FireEye, Inc.
Form 10-K
February 25, 2019
false--12-31FY20180001370880YesfalseLarge Accelerated FilerfalsefalseNoYesP3DP5DP5DP5D5P2YP1YP1YP1YP4YP1Y250300025250000.000110000000000187105000199612000100013708802018-01-01 2018-12-31 0001370880 2019-02-20 0001370880 2018-06-29 0001370880 2018-12-31 0001370880 2017-12-31 0001370880 2016-01-01 2016-12-31 0001370880 2017-01-01 2017-12-31 0001370880 feye:SubscriptionSupportandServicesMember 2017-01-01 2017-12-31 0001370880 feye:ProfessionalServicesMember 2017-01-01 2017-12-31 0001370880 feye:SubscriptionSupportandServicesMember 2016-01-01 2016-12-31 0001370880 feye:SubscriptionSupportandServicesMember 2018-01-01 2018-12-31 0001370880 feye:ProfessionalServicesMember 2018-01-01 2018-12-31 0001370880 feye:ProfessionalServicesMember 2016-01-01 2016-12-31 0001370880 us-gaap:AdditionalPaidInCapitalMember 2016-01-01 2016-12-31 0001370880 us-gaap:TreasuryStockMember 2015-12-31 0001370880 feye:SeriesAConvertibleSeniorNotesMember 2018-01-01 2018-12-31 0001370880 2015-12-31 0001370880 us-gaap:AdditionalPaidInCapitalMember 2018-01-01 2018-12-31 0001370880 us-gaap:CommonStockMember 2017-12-31 0001370880 us-gaap:RetainedEarningsMember 2018-12-31 0001370880 us-gaap:TreasuryStockMember 2018-12-31 0001370880 us-gaap:RetainedEarningsMember 2017-12-31 0001370880 us-gaap:CommonStockMember 2018-12-31 0001370880 us-gaap:AdditionalPaidInCapitalMember 2017-01-01 2017-12-31 0001370880 us-gaap:CommonStockMember 2018-01-01 2018-12-31 0001370880 us-gaap:AccumulatedOtherComprehensiveIncomeMember 2016-01-01 2016-12-31 0001370880 us-gaap:TreasuryStockMember 2016-12-31 0001370880 us-gaap:RetainedEarningsMember 2018-01-01 2018-12-31 0001370880 us-gaap:CommonStockMember 2017-01-01 2017-12-31 0001370880 us-gaap:RetainedEarningsMember 2017-01-01 2017-12-31 0001370880 us-gaap:AccumulatedOtherComprehensiveIncomeMember 2016-12-31 0001370880 us-gaap:CommonStockMember 2016-12-31 0001370880 us-gaap:AccumulatedOtherComprehensiveIncomeMember 2015-12-31 0001370880 us-gaap:CommonStockMember 2015-12-31 0001370880 us-gaap:TreasuryStockMember 2017-12-31 0001370880 2016-12-31 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:AdditionalPaidInCapitalMember 2018-01-01 2018-12-31 0001370880 us-gaap:RetainedEarningsMember 2016-12-31 0001370880 us-gaap:CommonStockMember 2016-01-01 2016-12-31 0001370880 feye:ISIGHTSecurityMember us-gaap:AdditionalPaidInCapitalMember 2016-01-01 2016-12-31 0001370880 feye:InvotasInternationalCorporationMember us-gaap:CommonStockMember 2016-01-01 2016-12-31 0001370880 us-gaap:AdditionalPaidInCapitalMember 2017-12-31 0001370880 feye:InvotasInternationalCorporationMember 2016-01-01 2016-12-31 0001370880 us-gaap:AccumulatedOtherComprehensiveIncomeMember 2017-12-31 0001370880 us-gaap:AdditionalPaidInCapitalMember 2015-12-31 0001370880 us-gaap:AdditionalPaidInCapitalMember 2016-12-31 0001370880 us-gaap:AccumulatedOtherComprehensiveIncomeMember 2017-01-01 2017-12-31 0001370880 us-gaap:RetainedEarningsMember 2016-01-01 2016-12-31 0001370880 us-gaap:AccumulatedOtherComprehensiveIncomeMember 2018-01-01 2018-12-31 0001370880 us-gaap:RetainedEarningsMember 2015-12-31 0001370880 feye:ConvertibleSeniorNotesdue2024Member 2018-01-01 2018-12-31 0001370880 feye:ISIGHTSecurityMember us-gaap:CommonStockMember 2016-01-01 2016-12-31 0001370880 us-gaap:AccumulatedOtherComprehensiveIncomeMember 2018-12-31 0001370880 feye:InvotasInternationalCorporationMember us-gaap:AdditionalPaidInCapitalMember 2016-01-01 2016-12-31 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:AdditionalPaidInCapitalMember 2018-01-01 2018-12-31 0001370880 us-gaap:AdditionalPaidInCapitalMember 2018-12-31 0001370880 feye:ISIGHTSecurityMember 2016-01-01 2016-12-31 0001370880 us-gaap:AccountingStandardsUpdate201409Member us-gaap:RetainedEarningsMember 2015-12-31 0001370880 srt:RestatementAdjustmentMember us-gaap:AccountingStandardsUpdate201409Member 2017-01-01 2017-12-31 0001370880 srt:ScenarioPreviouslyReportedMember 2017-01-01 2017-12-31 0001370880 srt:ScenarioPreviouslyReportedMember 2016-01-01 2016-12-31 0001370880 srt:RestatementAdjustmentMember us-gaap:AccountingStandardsUpdate201409Member 2016-01-01 2016-12-31 0001370880 us-gaap:AccountingStandardsUpdate201409Member us-gaap:RetainedEarningsMember 2017-12-31 0001370880 us-gaap:PrepaidExpensesAndOtherCurrentAssetsMember feye:DeferredCommissionsMember 2017-12-31 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember 2018-06-30

0001370880 feye:DepositsandOtherLongtermAssetsMember feye:DeferredCostsofRevenueMember 2018-12-31
0001370880 feye:TheEmailLaundryMember 2017-10-01 2017-10-31 0001370880 srt:MinimumMember
us-gaap:AccountingStandardsUpdate201602Member us-gaap:ScenarioForecastMember 2019-01-01 0001370880
us-gaap:PrepaidExpensesAndOtherCurrentAssetsMember feye:DeferredCommissionsMember 2018-12-31
0001370880 feye:DepositsandOtherCurrentAssetsMember feye:DeferredCommissionsMember 2018-12-31
0001370880 2018-04-01 2018-06-30 0001370880 feye:X15SoftwareInc.Member 2018-01-01 2018-01-31
0001370880 srt:MaximumMember us-gaap:AccountingStandardsUpdate201602Member
us-gaap:ScenarioForecastMember 2019-01-01 0001370880 feye:SeriesAConvertibleSeniorNotesMember
us-gaap:ConvertibleNotesPayableMember 2018-05-31 0001370880
us-gaap:PrepaidExpensesAndOtherCurrentAssetsMember feye:DeferredCostsofRevenueMember 2018-12-31
0001370880 us-gaap:PrepaidExpensesAndOtherCurrentAssetsMember feye:DeferredCostsofRevenueMember
2017-12-31 0001370880 feye:DepositsandOtherLongtermAssetsMember feye:DeferredCostsofRevenueMember
2017-12-31 0001370880 feye:DepositsandOtherCurrentAssetsMember feye:DeferredCommissionsMember
2017-12-31 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember
2018-04-01 2018-06-30 0001370880 feye:SeriesAConvertibleSeniorNotesMember
us-gaap:ConvertibleNotesPayableMember 2018-05-01 2018-05-31 0001370880
us-gaap:SoftwareDevelopmentMember 2018-01-01 2018-12-31 0001370880 srt:RestatementAdjustmentMember
us-gaap:AccountingStandardsUpdate201409Member 2017-12-31 0001370880
srt:ScenarioPreviouslyReportedMember 2017-12-31 0001370880 us-gaap:FurnitureAndFixturesMember 2018-01-01
2018-12-31 0001370880 srt:MaximumMember feye:ComputerEquipmentandSoftwareMember 2018-01-01
2018-12-31 0001370880 srt:MaximumMember us-gaap:MachineryAndEquipmentMember 2018-01-01 2018-12-31
0001370880 srt:MinimumMember feye:ComputerEquipmentandSoftwareMember 2018-01-01 2018-12-31
0001370880 srt:MinimumMember us-gaap:MachineryAndEquipmentMember 2018-01-01 2018-12-31 0001370880
srt:MinimumMember 2018-01-01 2018-12-31 0001370880 srt:MaximumMember 2018-01-01 2018-12-31
0001370880 us-gaap:FairValueInputsLevel3Member 2017-12-31 0001370880
us-gaap:FairValueInputsLevel3Member 2018-12-31 0001370880
us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2017-12-31 0001370880
us-gaap:USTreasurySecuritiesMember us-gaap:FairValueInputsLevel1Member 2017-12-31 0001370880
us-gaap:FairValueInputsLevel1Member us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2017-12-31
0001370880 us-gaap:FairValueInputsLevel1Member us-gaap:CommercialPaperMember 2018-12-31 0001370880
us-gaap:FairValueInputsLevel2Member 2018-12-31 0001370880 us-gaap:FairValueInputsLevel2Member
us-gaap:CommercialPaperMember 2018-12-31 0001370880 us-gaap:MoneyMarketFundsMember 2017-12-31
0001370880 us-gaap:USTreasurySecuritiesMember 2017-12-31 0001370880 us-gaap:FairValueInputsLevel3Member
us-gaap:CommercialPaperMember 2017-12-31 0001370880 us-gaap:USGovernmentAgenciesDebtSecuritiesMember
2018-12-31 0001370880 us-gaap:FairValueInputsLevel1Member 2017-12-31 0001370880
us-gaap:USTreasurySecuritiesMember 2017-12-31 0001370880 us-gaap:FairValueInputsLevel2Member
us-gaap:USTreasurySecuritiesMember 2018-12-31 0001370880 us-gaap:USTreasurySecuritiesMember 2018-12-31
0001370880 us-gaap:FairValueInputsLevel1Member 2018-12-31 0001370880 us-gaap:MoneyMarketFundsMember
us-gaap:FairValueInputsLevel1Member 2018-12-31 0001370880 us-gaap:FairValueInputsLevel1Member
us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2018-12-31 0001370880
us-gaap:FairValueInputsLevel2Member us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2018-12-31
0001370880 us-gaap:USTreasurySecuritiesMember 2018-12-31 0001370880 us-gaap:FairValueInputsLevel2Member
2017-12-31 0001370880 us-gaap:USTreasurySecuritiesMember us-gaap:FairValueInputsLevel2Member 2017-12-31
0001370880 us-gaap:FairValueInputsLevel2Member us-gaap:USTreasurySecuritiesMember 2017-12-31 0001370880
us-gaap:MoneyMarketFundsMember us-gaap:FairValueInputsLevel3Member 2017-12-31 0001370880
us-gaap:CommercialPaperMember 2017-12-31 0001370880 us-gaap:FairValueInputsLevel2Member
us-gaap:CorporateDebtSecuritiesMember 2018-12-31 0001370880 us-gaap:USTreasurySecuritiesMember
us-gaap:FairValueInputsLevel1Member 2018-12-31 0001370880 us-gaap:FairValueInputsLevel1Member
us-gaap:CorporateDebtSecuritiesMember 2017-12-31 0001370880 us-gaap:MoneyMarketFundsMember
us-gaap:FairValueInputsLevel2Member 2017-12-31 0001370880 us-gaap:FairValueInputsLevel1Member
us-gaap:USTreasurySecuritiesMember 2018-12-31 0001370880 us-gaap:USTreasurySecuritiesMember

us-gaap:FairValueInputsLevel3Member 2018-12-31 0001370880 us-gaap:CorporateDebtSecuritiesMember
2018-12-31 0001370880 us-gaap:CorporateDebtSecuritiesMember 2017-12-31 0001370880
us-gaap:MoneyMarketFundsMember 2018-12-31 0001370880 us-gaap:FairValueInputsLevel3Member
us-gaap:CorporateDebtSecuritiesMember 2018-12-31 0001370880 us-gaap:FairValueInputsLevel3Member
us-gaap:CorporateDebtSecuritiesMember 2017-12-31 0001370880 us-gaap:FairValueInputsLevel3Member
us-gaap:USTreasurySecuritiesMember 2017-12-31 0001370880 us-gaap:FairValueInputsLevel2Member
us-gaap:CorporateDebtSecuritiesMember 2017-12-31 0001370880 us-gaap:MoneyMarketFundsMember
us-gaap:FairValueInputsLevel3Member 2018-12-31 0001370880 us-gaap:FairValueInputsLevel1Member
us-gaap:USTreasurySecuritiesMember 2017-12-31 0001370880 us-gaap:FairValueInputsLevel3Member
us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2018-12-31 0001370880
us-gaap:FairValueInputsLevel3Member us-gaap:USTreasurySecuritiesMember 2018-12-31 0001370880
us-gaap:FairValueInputsLevel2Member us-gaap:CommercialPaperMember 2017-12-31 0001370880
us-gaap:FairValueInputsLevel3Member us-gaap:CommercialPaperMember 2018-12-31 0001370880
us-gaap:CommercialPaperMember 2018-12-31 0001370880 us-gaap:FairValueInputsLevel2Member
us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2017-12-31 0001370880
us-gaap:MoneyMarketFundsMember us-gaap:FairValueInputsLevel2Member 2018-12-31 0001370880
us-gaap:FairValueInputsLevel1Member us-gaap:CommercialPaperMember 2017-12-31 0001370880
us-gaap:MoneyMarketFundsMember us-gaap:FairValueInputsLevel1Member 2017-12-31 0001370880
us-gaap:USTreasurySecuritiesMember us-gaap:FairValueInputsLevel2Member 2018-12-31 0001370880
us-gaap:USTreasurySecuritiesMember us-gaap:FairValueInputsLevel3Member 2017-12-31 0001370880
us-gaap:FairValueInputsLevel3Member us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2017-12-31
0001370880 us-gaap:FairValueInputsLevel1Member us-gaap:CorporateDebtSecuritiesMember 2018-12-31
0001370880 us-gaap:FairValueInputsLevel2Member us-gaap:SeniorNotesMember 2018-12-31 0001370880
us-gaap:CashAndCashEquivalentsMember us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2018-12-31
0001370880 us-gaap:CashAndCashEquivalentsMember us-gaap:USTreasurySecuritiesMember 2018-12-31
0001370880 us-gaap:ShortTermInvestmentsMember us-gaap:USTreasurySecuritiesMember 2018-12-31 0001370880
us-gaap:ShortTermInvestmentsMember us-gaap:CorporateDebtSecuritiesMember 2018-12-31 0001370880
us-gaap:CashAndCashEquivalentsMember 2018-12-31 0001370880 us-gaap:ShortTermInvestmentsMember
us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2018-12-31 0001370880
us-gaap:CashAndCashEquivalentsMember us-gaap:CorporateDebtSecuritiesMember 2018-12-31 0001370880
us-gaap:ShortTermInvestmentsMember 2018-12-31 0001370880 feye:PrivateCompanyMember 2018-12-31
0001370880 feye:PrivateCompanyMember 2017-12-31 0001370880 us-gaap:ShortTermInvestmentsMember
us-gaap:CorporateDebtSecuritiesMember 2017-12-31 0001370880 us-gaap:CashAndCashEquivalentsMember
us-gaap:CommercialPaperMember 2017-12-31 0001370880 us-gaap:ShortTermInvestmentsMember 2017-12-31
0001370880 us-gaap:ShortTermInvestmentsMember us-gaap:USGovernmentAgenciesDebtSecuritiesMember
2017-12-31 0001370880 us-gaap:CashAndCashEquivalentsMember
us-gaap:USGovernmentAgenciesDebtSecuritiesMember 2017-12-31 0001370880
us-gaap:CashAndCashEquivalentsMember 2017-12-31 0001370880 us-gaap:CashAndCashEquivalentsMember
us-gaap:USTreasurySecuritiesMember 2017-12-31 0001370880 us-gaap:CashAndCashEquivalentsMember
us-gaap:CorporateDebtSecuritiesMember 2017-12-31 0001370880 us-gaap:ShortTermInvestmentsMember
us-gaap:USTreasurySecuritiesMember 2017-12-31 0001370880 us-gaap:ShortTermInvestmentsMember
us-gaap:CommercialPaperMember 2017-12-31 0001370880 us-gaap:FurnitureAndFixturesMember 2018-12-31
0001370880 us-gaap:MachineryAndEquipmentMember 2018-12-31 0001370880
us-gaap:MachineryAndEquipmentMember 2017-12-31 0001370880 us-gaap:LeaseholdImprovementsMember
2018-12-31 0001370880 feye:ComputerEquipmentandSoftwareMember 2018-12-31 0001370880
feye:ComputerEquipmentandSoftwareMember 2017-12-31 0001370880 us-gaap:FurnitureAndFixturesMember
2017-12-31 0001370880 us-gaap:LeaseholdImprovementsMember 2017-12-31 0001370880
feye:X15SoftwareInc.Member 2018-01-11 2018-01-11 0001370880 feye:TheEmailLaundryMember 2017-10-20
0001370880 feye:CleanCommunicationsLimitedMember 2017-10-20 0001370880 feye:X15SoftwareInc.Member
2018-01-11 0001370880 feye:CleanCommunicationsLimitedMember
us-gaap:TechnologyBasedIntangibleAssetsMember 2017-10-20 2017-10-20 0001370880

feye:TheEmailLaundryMember 2017-10-20 2017-10-20 0001370880 us-gaap:TradeNamesMember 2017-12-31 0001370880 feye:ContentMember 2017-12-31 0001370880 us-gaap:ContractBasedIntangibleAssetsMember 2018-12-31 0001370880 us-gaap:DevelopedTechnologyRightsMember 2017-12-31 0001370880 us-gaap:CustomerRelationshipsMember 2017-12-31 0001370880 us-gaap:CustomerRelationshipsMember 2018-12-31 0001370880 feye:ContentMember 2018-12-31 0001370880 us-gaap:TradeNamesMember 2018-12-31 0001370880 us-gaap:NoncompeteAgreementsMember 2017-12-31 0001370880 us-gaap:NoncompeteAgreementsMember 2018-12-31 0001370880 us-gaap:DevelopedTechnologyRightsMember 2018-12-31 0001370880 us-gaap:ContractBasedIntangibleAssetsMember 2017-12-31 0001370880 2016-08-01 2016-08-31 0001370880 us-gaap:EmployeeSeveranceMember 2018-01-01 2018-12-31 0001370880 us-gaap:FacilityClosingMember 2017-01-01 2017-12-31 0001370880 us-gaap:EmployeeSeveranceMember 2018-12-31 0001370880 us-gaap:EmployeeSeveranceMember 2017-01-01 2017-12-31 0001370880 us-gaap:FacilityClosingMember 2018-01-01 2018-12-31 0001370880 us-gaap:FacilityClosingMember 2018-12-31 0001370880 us-gaap:FacilityClosingMember 2016-12-31 0001370880 us-gaap:EmployeeSeveranceMember 2017-12-31 0001370880 us-gaap:EmployeeSeveranceMember 2016-12-31 0001370880 us-gaap:FacilityClosingMember 2017-12-31 0001370880 feye:ProductandRelatedSubscriptionandSupportMember 2018-12-31 0001370880 feye:ProductandRelatedSubscriptionandSupportMember 2017-12-31 0001370880 feye:ProfessionalServicesMember 2017-12-31 0001370880 feye:ProfessionalServicesMember 2018-12-31 0001370880 2021-01-01 2018-12-31 0001370880 2019-01-01 2018-12-31 0001370880 2020-01-01 2018-12-31 0001370880 2022-01-01 2018-12-31 0001370880 2021-01-01 2018-01-01 2018-12-31 0001370880 2022-01-01 2018-01-01 2018-12-31 0001370880 2019-01-01 2018-01-01 2018-12-31 0001370880 2020-01-01 2018-01-01 2018-12-31 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember 2018-12-31 0001370880 feye:SeriesBConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2017-12-31 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2018-12-31 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2017-12-31 0001370880 feye:SeriesBConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2018-12-31 0001370880 feye:SeriesBConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2015-06-01 2015-06-30 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember 2018-01-01 2018-12-31 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember 2018-05-24 2018-05-24 0001370880 feye:SeriesBConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2015-06-30 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember 2018-05-24 0001370880 us-gaap:ConvertibleNotesPayableMember 2018-01-01 2018-12-31 0001370880 feye:DebtLiabilityComponentMember us-gaap:ConvertibleNotesPayableMember 2015-06-30 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2015-06-30 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember us-gaap:MeasurementInputDiscountRateMember 2018-05-31 0001370880 feye:DebtEquityComponentMember us-gaap:ConvertibleNotesPayableMember 2015-06-30 0001370880 2015-06-01 2015-06-30 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:DebtInstrumentRedemptionPeriodOneMember us-gaap:ConvertibleNotesPayableMember 2018-05-24 2018-05-24 0001370880 feye:DebtEquityComponentMember us-gaap:ConvertibleNotesPayableMember 2018-12-31 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember us-gaap:MeasurementInputDiscountRateMember 2018-05-24 0001370880 feye:DebtLiabilityComponentMember us-gaap:ConvertibleNotesPayableMember 2018-05-24 0001370880 feye:SeriesBConvertibleSeniorNotesMember us-gaap:DebtInstrumentRedemptionPeriodTwoMember us-gaap:ConvertibleNotesPayableMember 2015-06-01 2015-06-30 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:DebtInstrumentRedemptionPeriodTwoMember us-gaap:ConvertibleNotesPayableMember 2018-05-24 2018-05-24 0001370880 us-gaap:ConvertibleDebtMember feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2018-05-01 2018-05-31 0001370880 feye:DebtLiabilityComponentMember us-gaap:ConvertibleNotesPayableMember 2018-12-31 0001370880 feye:SeriesBConvertibleSeniorNotesMember us-gaap:DebtInstrumentRedemptionPeriodOneMember us-gaap:ConvertibleNotesPayableMember 2015-06-01 2015-06-30 0001370880 us-gaap:CommonStockMember 2018-12-31 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember

2018-05-24 0001370880 feye:ConvertibleSeniorNotesdue2024Member us-gaap:ConvertibleNotesPayableMember
2018-06-05 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember
2018-01-01 2018-12-31 0001370880 feye:SeriesBConvertibleSeniorNotesMember
us-gaap:ConvertibleNotesPayableMember 2018-01-01 2018-12-31 0001370880
feye:SeriesBConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2016-01-01 2016-12-31
0001370880 feye:SeriesBConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember 2017-01-01
2017-12-31 0001370880 feye:SeriesAConvertibleSeniorNotesMember us-gaap:ConvertibleNotesPayableMember
2016-01-01 2016-12-31 0001370880 feye:SeriesAConvertibleSeniorNotesMember
us-gaap:ConvertibleNotesPayableMember 2017-01-01 2017-12-31 0001370880 feye:SoftwareandServicesMember
2018-12-31 0001370880 us-gaap:ConvertibleDebtMember 2018-12-31 0001370880 us-gaap:EmployeeStockMember
2017-12-31 0001370880 us-gaap:EmployeeStockMember 2018-12-31 0001370880
us-gaap:StockCompensationPlanMember 2018-12-31 0001370880 us-gaap:StockCompensationPlanMember
2017-12-31 0001370880 us-gaap:ConvertibleDebtMember 2017-12-31 0001370880
us-gaap:ConvertiblePreferredStockMember 2018-12-31 0001370880 2018-01-01 2018-09-30 0001370880
us-gaap:ConvertiblePreferredStockMember 2017-12-31 0001370880 feye:A2013StockOptionPlanMember
2017-12-31 0001370880 feye:A2013StockOptionPlanMember 2018-01-01 2018-12-31 0001370880
us-gaap:EmployeeStockOptionMember feye:A2013StockOptionPlanMember 2018-01-01 2018-12-31 0001370880
feye:A2013StockOptionPlanMember 2018-12-31 0001370880 us-gaap:EmployeeStockMember 2018-01-01
0001370880 feye:RestrictedCommonStockRestrictedStockAwardsOrRestrictedStockUnitsMember 2016-01-01
2016-12-31 0001370880 us-gaap:EmployeeStockMember 2018-01-01 2018-12-31 0001370880
feye:RestrictedCommonStockRestrictedStockAwardsOrRestrictedStockUnitsMember 2018-01-01 2018-12-31
0001370880 feye:A2013StockOptionPlanMember us-gaap:SubsequentEventMember 2019-01-01 0001370880
feye:RestrictedCommonStockRestrictedStockAwardsOrRestrictedStockUnitsMember 2017-01-01 2017-12-31
0001370880 us-gaap:CostOfGoodsProductLineMember 2016-01-01 2016-12-31 0001370880
us-gaap:RestructuringChargesMember 2016-01-01 2016-12-31 0001370880
us-gaap:GeneralAndAdministrativeExpenseMember 2018-01-01 2018-12-31 0001370880
us-gaap:SellingAndMarketingExpenseMember 2016-01-01 2016-12-31 0001370880
us-gaap:SellingAndMarketingExpenseMember 2017-01-01 2017-12-31 0001370880
us-gaap:ResearchAndDevelopmentExpenseMember 2017-01-01 2017-12-31 0001370880
us-gaap:ResearchAndDevelopmentExpenseMember 2016-01-01 2016-12-31 0001370880
us-gaap:SellingAndMarketingExpenseMember 2018-01-01 2018-12-31 0001370880
feye:CostofGoodsServicesMember 2018-01-01 2018-12-31 0001370880 us-gaap:RestructuringChargesMember
2017-01-01 2017-12-31 0001370880 us-gaap:GeneralAndAdministrativeExpenseMember 2017-01-01 2017-12-31
0001370880 us-gaap:RestructuringChargesMember 2018-01-01 2018-12-31 0001370880
feye:CostofGoodsServicesMember 2017-01-01 2017-12-31 0001370880
us-gaap:GeneralAndAdministrativeExpenseMember 2016-01-01 2016-12-31 0001370880
us-gaap:ResearchAndDevelopmentExpenseMember 2018-01-01 2018-12-31 0001370880
us-gaap:CostOfGoodsProductLineMember 2018-01-01 2018-12-31 0001370880 feye:CostofGoodsServicesMember
2016-01-01 2016-12-31 0001370880 us-gaap:CostOfGoodsProductLineMember 2017-01-01 2017-12-31 0001370880
us-gaap:EmployeeStockMember 2017-01-01 2017-12-31 0001370880 us-gaap:EmployeeStockMember 2016-01-01
2016-12-31 0001370880 srt:MinimumMember us-gaap:EmployeeStockMember 2016-01-01 2016-12-31 0001370880
srt:MaximumMember us-gaap:EmployeeStockMember 2017-12-31 0001370880 srt:MinimumMember
us-gaap:EmployeeStockMember 2016-12-31 0001370880 srt:MinimumMember us-gaap:EmployeeStockMember
2018-01-01 2018-12-31 0001370880 srt:MaximumMember us-gaap:EmployeeStockMember 2016-12-31 0001370880
srt:MaximumMember us-gaap:EmployeeStockMember 2018-12-31 0001370880 srt:MaximumMember
us-gaap:EmployeeStockMember 2018-01-01 2018-12-31 0001370880 srt:MaximumMember
us-gaap:EmployeeStockMember 2016-01-01 2016-12-31 0001370880 srt:MinimumMember
us-gaap:EmployeeStockMember 2017-01-01 2017-12-31 0001370880 srt:MinimumMember
us-gaap:EmployeeStockMember 2018-12-31 0001370880 srt:MaximumMember us-gaap:EmployeeStockMember
2017-01-01 2017-12-31 0001370880 srt:MinimumMember us-gaap:EmployeeStockMember 2017-12-31 0001370880
us-gaap:DomesticCountryMember 2018-12-31 0001370880 us-gaap:DomesticCountryMember

us-gaap:ResearchMember 2018-12-31 0001370880 us-gaap:StateAndLocalJurisdictionMember
us-gaap:ResearchMember 2018-12-31 0001370880 us-gaap:StateAndLocalJurisdictionMember 2018-12-31
0001370880 feye:UnvestedRestrictedStockAwardsAndRestrictedStockUnitsMember 2016-01-01 2016-12-31
0001370880 us-gaap:EmployeeStockMember 2017-01-01 2017-12-31 0001370880
us-gaap:ConvertibleDebtSecuritiesMember 2017-01-01 2017-12-31 0001370880 us-gaap:StockOptionMember
2017-01-01 2017-12-31 0001370880 us-gaap:ConvertibleDebtSecuritiesMember 2018-01-01 2018-12-31
0001370880 us-gaap:EmployeeStockMember 2016-01-01 2016-12-31 0001370880
feye:ContingentlyIssuableSharesMember 2016-01-01 2016-12-31 0001370880
feye:UnvestedRestrictedStockAwardsAndRestrictedStockUnitsMember 2017-01-01 2017-12-31 0001370880
feye:UnvestedRestrictedStockAwardsAndRestrictedStockUnitsMember 2018-01-01 2018-12-31 0001370880
feye:ContingentlyIssuableSharesMember 2017-01-01 2017-12-31 0001370880 us-gaap:StockOptionMember
2016-01-01 2016-12-31 0001370880 us-gaap:ConvertibleDebtSecuritiesMember 2016-01-01 2016-12-31
0001370880 us-gaap:StockOptionMember 2018-01-01 2018-12-31 0001370880
feye:ContingentlyIssuableSharesMember 2018-01-01 2018-12-31 0001370880 us-gaap:EmployeeStockMember
2018-01-01 2018-12-31 0001370880 us-gaap:EMEAMember 2016-01-01 2016-12-31 0001370880
feye:OtherGeographicLocationMember 2017-01-01 2017-12-31 0001370880 feye:OtherGeographicLocationMember
2018-01-01 2018-12-31 0001370880 us-gaap:EMEAMember 2017-01-01 2017-12-31 0001370880 country:US
2016-01-01 2016-12-31 0001370880 srt:AsiaPacificMember 2016-01-01 2016-12-31 0001370880 country:US
2018-01-01 2018-12-31 0001370880 srt:AsiaPacificMember 2018-01-01 2018-12-31 0001370880
us-gaap:EMEAMember 2018-01-01 2018-12-31 0001370880 country:US 2017-01-01 2017-12-31 0001370880
feye:OtherGeographicLocationMember 2016-01-01 2016-12-31 0001370880 srt:AsiaPacificMember 2017-01-01
2017-12-31 0001370880 feye:ProductandRelatedSubscriptionandSupportMember 2016-01-01 2016-12-31
0001370880 feye:CloudSubscriptionandManagedServicesMember 2018-01-01 2018-12-31 0001370880
feye:CloudSubscriptionandManagedServicesMember 2016-01-01 2016-12-31 0001370880
feye:ProductandRelatedSubscriptionandSupportMember 2017-01-01 2017-12-31 0001370880
feye:ProductandRelatedSubscriptionandSupportMember 2018-01-01 2018-12-31 0001370880
feye:CloudSubscriptionandManagedServicesMember 2017-01-01 2017-12-31 0001370880 feye:OneResellerMember
us-gaap:SalesRevenueNetMember us-gaap:CustomerConcentrationRiskMember 2017-01-01 2017-12-31 0001370880
feye:OneResellerMember us-gaap:SalesRevenueNetMember us-gaap:CustomerConcentrationRiskMember
2016-01-01 2016-12-31 0001370880 feye:OneDistributorMember us-gaap:SalesRevenueNetMember
us-gaap:CustomerConcentrationRiskMember 2018-01-01 2018-12-31 0001370880 feye:OneResellerMember
us-gaap:SalesRevenueNetMember us-gaap:CustomerConcentrationRiskMember 2018-01-01 2018-12-31 0001370880
feye:OneDistributorMember us-gaap:SalesRevenueNetMember us-gaap:CustomerConcentrationRiskMember
2017-01-01 2017-12-31 0001370880 feye:OneDistributorMember us-gaap:SalesRevenueNetMember
us-gaap:CustomerConcentrationRiskMember 2016-01-01 2016-12-31 0001370880 us-gaap:NonUsMember
2017-12-31 0001370880 country:US 2017-12-31 0001370880 us-gaap:NonUsMember 2018-12-31 0001370880
country:US 2018-12-31 xbrli:shares iso4217:USD iso4217:USD xbrli:shares xbrli:pure feye:reporting_segment
feye:days feye:day feye:claim feye:vote_per_share

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

x **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES**

EXCHANGE ACT OF 1934
For the fiscal year ended December 31, 2018

or

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE
o SECURITIES EXCHANGE ACT OF 1934
For the transition period from to

Commission File Number 001-36067

FireEye, Inc.

(Exact name of registrant as specified in its charter)

Delaware	**20-1548921**
(State or other jurisdiction of incorporation or organization)	**(I.R.S. Employer Identification Number)**

601 McCarthy Blvd.
Milpitas, CA 95035
(408) 321-6300
(Address, including zip code, and telephone number, including area code, of registrant's principal executive offices)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	**Name of each exchange on which registered**
Common Stock, par value $0.0001 per share	The NASDAQ Global Select Market

Securities registered pursuant to Section 12(g) of the Act:
None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes x No ¨

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ¨ No x

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes x No ¨

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes x No ¨

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. x

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” “smaller reporting company,” and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	x	Accelerated filer	¨
Non-accelerated filer	¨	Smaller reporting company	¨
		Emerging growth company	¨

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ¨

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ¨ No x

As of June 29, 2018, the last business day of the registrant’s most recently completed second fiscal quarter, the aggregate market value of the registrant’s common stock held by non-affiliates was approximately $2.9 billion, based on the closing sales price of such stock reported for such date on The NASDAQ Global Select Market. This calculation does not reflect a determination that persons are affiliates for any other purposes.

The number of outstanding shares of the registrant’s common stock was203,093,510 as of February 20, 2019.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant’s Proxy Statement for the2019 Annual Meeting of Stockholders to be filed with the Securities and Exchange Commission within 120 days after the end of the registrant’s fiscal year endedDecember 31, 2018 are incorporated by reference into Part III of this Annual Report on Form 10-K.

		Page
	PART I	
Item 1.	Business	6
Item 1A.	Risk Factors	13
Item 1B.	Unresolved Staff Comments	39
Item 2.	Properties	39
Item 3.	Legal Proceedings	39
Item 4.	Mine Safety Disclosures	39
	PART II	
Item 5.	Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities	40
Item 6.	Selected Consolidated Financial Data	42
Item 7.	Management's Discussion and Analysis of Financial Condition and Results of Operations	44
Item 7A.	Quantitative and Qualitative Disclosures About Market Risk	67
Item 8.	Financial Statements and Supplementary Data	68
Item 9.	Changes in and Disagreements With Accountants on Accounting and Financial Disclosure	104
Item 9A.	Controls and Procedures	104
Item 9B.	Other Information	106
	PART III	
Item 10.	Directors, Executive Officers and Corporate Governance	107
Item 11.	Executive Compensation	107
Item 12.	Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters	107
Item 13.	Certain Relationships and Related Transactions, and Director Independence	107
Item 14.	Principal Accountant Fees and Services	107
	PART IV	
Item 15.	Exhibits, Financial Statement Schedules	108
Item 16.	Form 10-K Summary	112
	Signatures	113

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K, including the sections entitled “Business,” “Risk Factors,” and “Management’s Discussion and Analysis of Financial Condition and Results of Operations,” contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. The words “believe,” “may,” “will,” “potentially,” “estimate,” “continue,” “anticipate,” “i “could,” “would,” “project,” “plan” “expect,” the negative and plural forms of these words and similar expressions that convey uncertainty of future events or outcomes are intended to identify forward-looking statements. These forward-looking statements include, but are not limited to, statements concerning the following:

- the evolution of the threat landscape facing our customers and prospects;
- our ability, and the effects of our efforts, to educate the market regarding the advantages of our security solutions;
- our ability to continue to grow revenues;
- our future financial and operating results;
- our business plan and our ability to effectively manage our growth and associated investments;
- our beliefs, forecasts and objectives for future operations;
- our ability to expand our leadership position in advanced network security;
- our ability to attract and retain customers and to expand our solutions footprint within each of these customers;
- our expectations concerning customer retention rates, as well as expectations for the value of subscriptions and services renewals;
- our ability to maintain our competitive technological advantages against new entrants in our industry;
- our ability to timely and effectively scale and adapt our existing technology;
- our ability to innovate new products and solutions and bring them to market in a timely manner;
- our ability to maintain, protect, and enhance our brand and intellectual property;
- our ability to expand internationally;
- the effects of increased competition in our market and our ability to compete effectively;
- cost of revenue, including changes in costs associated with products, subscriptions, manufacturing and customer support;
- operating expenses, including changes in research and development, sales and marketing, and general and administrative expenses;
- anticipated income tax rates;
- potential attrition and other impacts associated with restructuring;
- sufficiency of cash to meet cash needs for at least the next 12 months;
- our ability to generate cash flows from operations and free cash flows;
- our ability to capture new, and renew existing, contracts with the United States and international governments;
- our expectations concerning relationships with third parties, including our manufacturers, channel and technology alliance partners and logistics providers;
- the release of new products and solutions;
- economic and industry trends or trend analysis;
- the attraction, training, integration and retention of qualified employees and key personnel;
- future acquisitions of or investments in complementary companies, products, subscriptions or technologies; and
- the effects of seasonal trends on our results of operations.

These forward-looking statements are subject to a number of risks, uncertainties, and assumptions, including those described in “Risk Factors” included in Part I, Item 1A and elsewhere in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment, and new risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties, and assumptions, the forward-looking events and circumstances discussed in this Annual Report on Form 10-K may not occur, or

unanticipated events or circumstances that we did not foresee may materialize, either of which could cause actual results to differ materially and adversely from those anticipated or implied in our forward-looking statements.

You should not rely upon forward-looking statements as predictions of future events. Although we believe that the expectations reflected in our forward-looking statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Moreover, neither we nor any other person assumes responsibility for the accuracy and completeness of the forward-looking statements. We undertake no obligation to update publicly any forward-looking statements for any reason after the date of this Annual Report on Form 10-K to conform these statements to actual results or to changes in our expectations, except as required by law.

You should read this Annual Report on Form 10-K and the documents that we reference in this Annual Report on Form 10-K and have filed with the SEC as exhibits to this Annual Report on Form 10-K with the understanding that our actual future results, levels of activity, performance and events and circumstances may be materially different from what we expect.

PART I

Item 1. Business

General

We provide comprehensive intelligence-based cybersecurity solutions that allow organizations to prepare for, prevent, investigate, respond to and remediate cyber attacks. Our portfolio of cybersecurity products and services is designed to minimize the risk of costly cyber security breaches by detecting and preventing advanced, targeted and other evasive attacks, as well as enabling more efficient management of security operations, including alert management, investigation and response when a breach occurs. We accomplish this through the integration of our core competitive advantages in solutions and services that adapt to changes in the threat environment through a cycle of intelligence-driven innovation. Our core competitive advantages include:

- Our technologies, including our machine-learning, behavioral-based, and rules-based threat detection, analysis and correlation technologies, combined with our proprietary Multi-vector Virtual Execution ("MVX") engine,
- Our intelligence on threats and threat actors based on the continuous flow of machine-, attacker- and victim-based attack data from our global network of threat sensors and virtual machines, as well as threat intelligence gathered by our security analysts, consultants and incident responders, and
- Our accumulated security expertise derived from responding to thousands of significant breaches over the past decade.

Our threat detection and prevention products encompass appliance-based, virtual and cloud solutions for web security, email security and endpoint security. These products are complemented by our cloud-based threat intelligence, security analytics and security automation and orchestration technologies, as well as our managed security services, cybersecurity consulting and incident response offerings. In combination, our solutions and services enable a proactive approach to cybersecurity that extends across the threat management lifecycle to minimize the risk of costly cybersecurity breaches.

We have organized our cybersecurity solutions in a hub and spokes model designed to integrate machine-generated threat data from our detection and prevention products with our analytics, response and orchestration technologies delivered through our Helix cybersecurity operations platform. Helix is designed to enable more efficient security operations by correlating security and event data across an organization’s environment to determine which threats present the greatest risk, automating repetitive security processes, and providing tools and workflows to investigate alerts and respond to attacks. The Helix cloud-based interface presents a unified view of an organization’s attack surface, including on-premise and cloud environments, and provides the contextual threat intelligence and threat management tools to enable a rapid response.

We were founded in 2004 to address the inability of signature-based security solutions to detect the new generation of dynamic, stealthy and targeted cyber attacks, known as advanced persistent threats. To meet the challenges of detecting these previously unknown threats, for which there were no signatures, we developed our MVX engine, a purpose-built virtual machine-based threat detection and analysis engine. MVX works in conjunction with our intelligence-driven analysis ("IDA") technologies in our network, email and endpoint security solutions to detect and block attacks that evade detection by signature-based security solutions. Our approach allows us to detect both known and unknown threats while minimizing costly false positive alerts. In addition to providing customers with high fidelity alerts on cyber attacks, MVX generates a continuous flow of real-time, anonymized “victim-based” threat data to FireEye through our Dynamic Threat Intelligence ("DTI") cloud.

In December 2013, we acquired Mandiant, a leading provider of advanced endpoint security products and security incident response management solutions. As a result of the Mandiant acquisition, we expanded our threat intelligence to include contextual information on cyber attackers’ tools and techniques, augmented our threat detection technologies with additional detection and forensic capabilities, and added a comprehensive suite of incident response and other cyber related professional services.

Since the Mandiant acquisition, we have expanded our business from a narrow focus on the detection of advanced persistent threats to helping our customers detect and prevent all types of cyber attacks and improve their resilience to new cyber threats using our technologies, intelligence and expertise. Additionally, our threat researchers correlate the attack data from our network, email, and endpoint security solutions with the intelligence on adversaries generated by our global network of security researchers and consultants. This deep knowledge of the threat environment and

attacker tools and techniques is used to adapt our detection and analysis engines to new attack techniques and to develop new features and use cases for our security solutions.

In the first quarter of 2017, we introduced our FireEye Helix cybersecurity operations platform. Helix integrates security alerts from our network, email and endpoint security solutions, as well as data from other information technology and cybersecurity solutions, with our advanced threat intelligence, threat analytics, and orchestration capabilities to enable more efficient security operations. The cloud-based Helix user interface provides a unified, customized view of an organization's attack surface, and includes pre-determined threat response "playbooks" based on Mandiant expertise and best practices. Helix allows security analysts to prioritize critical alerts, hunt for new threats, and rapidly pivot from detection to response to reduce the business impact of an attack.

As of December 31, 2018, we had approximately 7,700 end-customers, including more than 50% of the Forbes Global 2000. Our customers include leading enterprises in a diverse set of industries, including telecommunications, technology, financial services, public utilities, healthcare and oil and gas, as well as leading U.S. and international governmental agencies.

For 2018, 2017 and 2016, our revenue was $831.0 million, $779.6 million and $706.0 million, respectively, representing year-over-year growth of 7% for 2018 and 10% for 2017, and our net losses were $243.1 million, $285.2 million and $485.4 million, respectively.

We were incorporated in Delaware in February 2004 under the name NetForts, Inc., and changed our name to FireEye, Inc. in September 2005. Our principal executive offices are located at 601 McCarthy Blvd., Milpitas, California 95035, and our telephone number is (408) 321-6300. Our website is www.fireeye.com. Information contained on, or that can be accessed through, our website is not incorporated by reference into this report, and you should not consider information on our website to be part of this report. Our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K and amendments to reports filed or furnished pursuant to Sections 13(a) and 15(d) of the Securities Exchange Act of 1934, as amended, are available free of charge on the Investor Relations portion of our website as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC. The SEC maintains an Internet site that contains reports, proxy and information statements and other information regarding issuers that file electronically with the SEC at www.sec.gov. The contents of these websites are not incorporated into this filing.

Investors and others should note that we announce material financial information to our investors using our investor relations website (https://investors.fireeye.com), SEC filings, press releases, public conference calls and webcasts. We use these channels, as well as social media, to communicate with the public about our company, our services and other issues. It is possible that the information we post on social media could be deemed to be material information.

Our Cybersecurity Solutions and Services

Our solutions are designed to address cybersecurity requirements for small-to-mid sized enterprises, remote offices, large enterprises, governments and service providers. Customers may choose to deploy our detection and prevention solutions on optimized appliances hardware, on virtual appliances, as a cloud-based service, or in hybrid deployments of all three options. All our detection and prevention solutions include subscriptions to our DTI cloud and support offerings, which are priced either as a percentage of the appliance hardware or as an all-inclusive subscription. Subscriptions are typically offered for one- or three-year terms. We typically invoice customers for the full term of subscriptions up-front. Our Helix cybersecurity platform, threat analytics, and Managed Defense security-as-a-service offerings are offered in one- or three-year subscriptions and are priced based on appropriate use metrics. These subscriptions are invoiced either for the full term of the subscription up front or annually, based on customer preference. Professional services are invoiced according to pre-determined contract terms for consulting services and on a time-and-materials basis for incident response. We recognize professional services revenue as our services are delivered.

Product, Subscription and Support

Threat Detection and Prevention Solutions. Our detection and prevention solutions utilize our advanced threat detection software, including our IDA technologies and MVX engine, to identify suspicious content embedded in Internet and network traffic, emails, software downloads and other data transfers and electronic communications. Our portfolio encompasses solutions for network security, email security, and endpoint security that are available in a variety of form factors and deployment options.

- ***Network security solutions.*** Our network security solutions utilize our IDA technologies and MVX engine in a two-phase approach to detect, validate and block advanced, targeted and other evasive attacks hidden in Internet traffic, as well as threats embedded in internal network traffic. Our network security solutions may be deployed at the network perimeter, in conjunction with signature- and policy-based defenses, such as network firewalls to detect and validate attacks missed by those products. Additionally, our network security solutions may be deployed at the network core, across network segments or in front of servers to detect threats embedded in internal network traffic, such as ransomware. Our network security solutions require up-to-date dynamic threat intelligence and software support to maintain high detection efficacy. Customers may choose to purchase our network security software, dynamic threat intelligence, and support in a single “all inclusive” subscription, with optional appliance hardware, or

they may purchase pre-configured appliance hardware with the required dynamic threat intelligence and support subscriptions priced as a percentage of the appliance hardware. Our network security solutions integrate with our email and endpoint security solutions through our Central Management System ("CMS") or our Helix security operations platform to correlate threat intelligence and protect against multi-vector, blended attacks.

Integrated network security. Our integrated network security appliances combine our IDA rules and correlation engines and our MVX engine in a single, standalone appliance to secure a single Internet access point. Customers may choose to deploy integrated network security on our optimized appliance hardware, or on a virtual appliance, with capacity scaling from 50 megabits per second to multiple gigabits per second of throughput.

Distributed network security. In November 2016, we updated our advanced detection software to enable our IDA detection technologies to be deployed separately from our MVX engine without performance degradation. This allowed our IDA technologies to be deployed at multiple Internet access points in distributed, cloud and hybrid environments, using physical or virtual appliances known as Smart Nodes. Suspicious traffic detected by network sensors is submitted to a centrally shared MVX

service over an encrypted connection. Distributed network security customers can choose to host the shared MVX service in their private cloud or utilize the FireEye-hosted Cloud MVX service.

Network forensics. Our network forensics appliances capture, store and index full network packets at rapid speeds to allow organizations to investigate and resolve security incidents.

- ***Email security solutions.*** Our email security solutions detect and stop spear phishing, ransomware, sender impersonation, credential phishing, typo-squatting, and other email-based attacks. We offer our email security solution in a Server Edition with multiple deployment options, or as a cloud-based service. Both versions utilize our URL detection platform and our MVX engine to inspect emails for zero-day exploits, malicious URLs, behavioral anomalies, and other malware hidden in attachments. If an attack is confirmed, the malicious email is quarantined for further analysis and deletion. Our email security solutions integrate with FireEye network security through our CMS or our Helix security operations platform to protect against multi-vector, blended attacks.

Email Security - Server Edition is an on-premises appliance-based solution that can be deployed with an integrated MVX engine or in a distributed architecture with a centralized, private cloud MVX service.

Email Security - Cloud Edition is a FireEye-hosted version of our email security solution designed to integrate with cloud-based email systems such as Microsoft Office 365 with Exchange Online Protection and Google Mail. Email Security - Cloud Edition provides the same advanced correlation, analytics and MVX threat validation as Email Security - Server Edition, and also includes anti-spam and antivirus protection to defend against conventional signature-based threats.

- ***Endpoint security solutions.*** Our endpoint security solutions consist of a centralized management application, available through an on-premise appliance or as a cloud-based user interface, and lightweight endpoint agents deployed on desktops, laptops and other end-user devices. The solutions combine a signature-based endpoint protection platform with advanced endpoint detection and response capabilities to provide a comprehensive detection, protection and response solution in a single endpoint agent. The endpoint security agent also enables rapid containment and collects forensic data necessary for post-breach investigation and analysis of attacks. Our endpoint security solutions integrate with our email and endpoint security solutions through our CMS or our Helix security operations platform to correlate threat intelligence and protect against multi-vector, blended attacks.

Customer Support and Maintenance Services. We offer technical support on our solutions. We provide multiple levels of support and have regional support centers located across the globe to help customers solve technical challenges they may encounter. In addition to post-sales support activities, our support organization works with our product management and engineering teams to ensure the attainment of defined pre-requisite quality levels for our products and services prior to release.

Security Orchestration, Analytics and Management Solutions

- ***Central Management System.*** Our Central Management System manages the overall deployment and integration of our on-premise network, email and endpoint security solutions by unifying reporting, configuration, and threat intelligence sharing. Customers generally purchase one or more CMS appliances to manage multiple FireEye detection and prevention appliances.

FireEye Security Orchestrator. Our FireEye Security Orchestrator ("FSO") accelerates and simplifies security operations by coordinating the response to critical alerts across the security and IT infrastructure using customized workflows, granular permissions, and bi-directional command and control plug-ins for many popular security and infrastructure products. FSO also provides an investigative dashboard and is a core enabling technology for the Helix cybersecurity platform.

FireEye Helix. Our FireEye Helix security operations platform combines security alerts generated by our network, email and endpoint security solutions, as well as third-party security and IT products, with our contextual threat intelligence, threat analytics, and orchestration capabilities within a unified cloud-based interface. Helix enriches raw security event data with our contextual threat intelligence and our built-in analytics to identify and prioritize critical alerts. Helix also serves as an investigative platform with case management and workflow tools, as well as pre-loaded playbooks to automate and orchestrate the response across an organization. Helix also provides detailed reporting for compliance purposes.

Threat Intelligence Subscriptions

-

Dynamic Threat Intelligence Cloud. Our DTI cloud is a bi-directional cloud-based service that collects, correlates and anonymizes machine-generated security data from our network, email and endpoint security solutions. DTI also distributes updated threat detection and prevention algorithms and software updates to our network, email and endpoint security solutions based on new threat intelligence and an evolving attack landscape. A subscription to our DTI cloud is required for all network, email and endpoint security solutions.

- ***FireEye Threat Intelligence*** is a subscription service based on our active monitoring of attacker personas, including nation-state sponsored groups. The resulting intelligence on adversaries is codified in reports and distributed through our Threat Intelligence portal to enable organizations to proactively defend against new and emerging cyber threats before an attack is launched.

On-Demand and Managed Service Subscriptions

- ***Managed Defense*** is a technology-enabled managed detection and response service that utilizes our latest adversary, machine-based, and victim threat intelligence to detect, investigate, and proactively hunt for known and previously undetected threats in our customers' environments.
- ***Expertise-on-Demand*** is a prepaid annual subscription that provides flexible, pay-per-use access to our threat intelligence and expertise as microservices. Customers purchase packages of units based on their anticipated needs and use the units to purchase threat intelligence and services at pre-determined unit values. Revenue is recognized in either the Cloud subscription and Managed services category or the Professional services category when the units are utilized, or upon expiration. Unused units expire one year after purchase.

Professional Services

- ***Incident response, compromise assessments and related security consulting services.*** Our cybersecurity experts help customers identify and remediate cyber breaches. Additionally, we offer security program assessments and planning, provide litigation support, and perform forensic analyses. These consulting services are marketed under the Mandiant brand.
- ***Cyber Threat Intelligence Services.*** Cyber threat intelligence services design and build cyber threat intelligence processes and solutions within customers' security operations.
- ***Training.*** We offer training services to our customers and channel partners through our training department and authorized training partners.

For contributions to total revenue by significant category of revenues, see "Management's Discussion and Analysis of Financial Condition and Results of Operations" included in Part II, Item 7 of this Annual Report on Form 10-K.

Our Technologies

We have developed proprietary technologies related to threat detection, virtual machine-based threat analysis, endpoint protection, and security orchestration. Our technologies leverage intelligence about threat actors' tools and techniques, gathered through our incident response engagements and our network of security researchers, to adapt to new threats and changes in the threat environment. We believe these technologies, combined with our threat intelligence and security expertise, differentiate our products and services.

Advanced Threat Detection and Prevention Technologies. At the core of our detection and protection capabilities for our network, email and endpoint security solutions is our proprietary, purpose-built MVX engine and our IDA technologies. Our IDA technologies include advanced correlation and analytics engines, our MalwareGuard machine-learning detection engine, behavior- and rules-based detection modules, and signature matching capabilities. These detection technologies work in conjunction with our MVX engine and our Helix-based analytics to detect suspicious content and confirm malicious behavior in the targeted virtual environment. This allows our network, email and endpoint security solutions to provide high fidelity detection of known and unknown threats with negligible false-positive rates. We have built our IDA and MVX engine technologies over 10 years of research and development, and we believe they represent a significant competitive advantage for us. They first identify suspicious flows using intelligence-driven rules and analysis, including machine-learning and behavioral analysis, and then, through a separate process, use our MVX engine to determine whether such suspicious flows are malicious. Our detection technologies can be deployed on a single integrated appliance, as a cloud-based service, or in a hybrid appliance/cloud architecture.

Advanced Endpoint Validation and Containment. Our endpoint security solution includes proprietary technologies that enable (i) automatic creation of indicators of compromise coupled with rapid enterprise-wide search, (ii) exploit detection and prevention, (iii) malware detection and prevention, (iv) forensic data capture and (v) rapid containment and investigation for connected and unconnected endpoints. Additionally, we have developed our endpoint technologies to correlate and consume threat intelligence from our network-based security solutions.

Evolved Security Architecture and Security Orchestration. Our solutions are designed to operate as part of a comprehensive security architecture to defend organizations against today's cyber threats and minimize the business impact of cyber attacks. The ability to monitor all network traffic, as well as stored files and forensic data, is critical to detecting cyber threats that enter through multiple vectors and move laterally across the network. We combine this visibility with our dynamic, contextual and strategic threat intelligence, advanced analytics and case management tools in our Helix security operations platform to enable rapid, prioritized responses to critical alerts. Our security

orchestration tools and technologies integrate with Helix to extend security processes and response activities across the IT infrastructure.

Customers

Our customer base has grown to approximately 7,700 end-customers as of December 31, 2018, including more than 50% of the Forbes Global 2000. We provide products, subscriptions and services to customers of varying sizes, including enterprises, governmental agencies and educational and nonprofit organizations. Our customers include leading enterprises in a diverse set of industries, including telecommunications providers, financial services entities, Internet search engines, social networking sites, stock exchanges, electrical grid operators, networking vendors, oil and gas companies, healthcare and pharmaceutical companies and leading U.S. and international

governmental agencies. Our business is not dependent on any particular end-customer as no end-customer represented more than 10% of our revenue for any of the years ended December 31, 2018, 2017 or 2016. For the years ended December 31, 2018, 2017 and 2016, one reseller represented 15%, 13% and 12%, respectively, of our total revenue. For the years ended December 31, 2018, 2017 and 2016, one distributor represented 20%, 19% and 19% respectively, of our total revenue.

Backlog

Orders for our appliances, software, subscriptions and services are typically shipped and billed in their entirety shortly after receipt of the order, even when the delivery term for the subscription or service extends over multiple periods. These amounts are included in deferred revenue, although the timing of revenue recognition for subscriptions and services may vary depending on the contractual service period or when the services are rendered. In certain instances, a customer may request periodic billing on a multi-period subscription or service contract or we may not have a contractual right to bill at period end. In these instances, the amount billed is included in deferred revenue and the amount to be billed in the future periods is included in backlog. Subscription and services backlog has historically represented less than 3% of our annual deferred revenue and revenue. As a result, we do not believe that our backlog at any particular time is meaningful because it does not represent a material component of future revenue in any given period.

We expect that the amount of backlog relative to the total value of our contracts will change from year to year due to several factors, including the amount invoiced early in the contract term, the timing and duration of customer agreements, varying invoicing cycles of agreements and changes in customer financial circumstances. Accordingly, we believe that fluctuations in backlog are not always a reliable indicator of future revenues and we do not utilize backlog internally as a key management metric.

Sales and Marketing

Sales. Our sales organization consists of in-house sales teams who work in collaboration with external channel partners to identify new sales prospects, sell additional products, subscriptions and services, and provide post-sale support. Our field sales team is organized by territory and is responsible for enterprise and government accounts within their region. Our inside sales organization is responsible for sales to medium-sized and smaller organizations, and for renewal of existing subscriptions.

We also have a dedicated team focused on channel sales who manage the relationships with our value-added reseller and distributor partners and work with these channel partners to win and support customers. We believe this hybrid direct-touch sales approach allows us to leverage the benefits of broader market coverage provided by a reseller channel while maintaining a face-to-face connection with our customers, including key enterprise accounts.

We have also cultivated alliances with non-traditional partners to generate customer referrals and extend our technologies and sales coverage to new market segments. These relationships include relationships with insurance providers, large systems integrators, and managed service providers, and we have engaged in joint solution development with leading providers of engineering services, payment systems, and public cloud platforms.

Our sales organization is supported by sales engineers with deep technical domain expertise who are responsible for pre-sales technical support, solutions engineering for our customers, proof of concept work and technical training for our channel partners. Our sales engineers also act as the liaison between customers and our marketing and product development organizations.

As part of our sales strategy, we often provide prospective customers with our detection and prevention products for a short-term evaluation period, typically ranging from one week to several months. During this period, the prospective customer conducts evaluations with the assistance of our system engineers and members of our security research team. We believe that by providing proof of concept evaluations to potential customers, we are able to contrast the effectiveness of our solutions versus our competitors in identifying suspicious and potentially malicious content in their actual IT environments. For our cloud-based email security solutions, we allow customers to submit emails previously scanned by their existing email security provider for analysis by our advanced detection technologies. Additionally, our Mandiant consultants use our technologies and products in their incident response and consulting engagements, providing de facto proof of concept evaluations in the customer’s environment. Our sales cycle varies by industry and can be long and unpredictable, but is typical of large, complex enterprise sales cycles that can last several months or more. However, some transactions can close in a few weeks when an active breach is discovered.

Marketing. Our marketing is focused on building our brand reputation and market awareness for our solutions, driving customer demand and a strong sales pipeline, and working with our channel partners around the globe. Our marketing team consists primarily of corporate marketing, channel marketing, account/lead development, marketing operations and corporate communications. Marketing activities include demand generation, advertising, product launch activities, managing our corporate website and partner portal, trade shows and conferences, press and analyst relations, and customer awareness. We are also actively engaged in driving global thought leadership programs through blogs and media and developing rich content such as the global cyber map and threat reports.

Technology Alliance Partners

FireEye has built a robust ecosystem of Technology Alliance Partners who, through integration and joint go-to-market efforts, extend the breadth and depth of the cybersecurity and protection we deliver to customers. Spanning multiple technology categories, including network monitoring vendors, security information and event management vendors, network equipment vendors, forensic software vendors and web application firewall vendors, these partnerships provide for threat intelligence sharing, cross-vendor technology integrations,

and joint solution development. By helping to ease the complexity that organizations face when implementing multi-layered security solutions, our technology alliances facilitate integrated solution design, accelerate the time to realize value, and enhance our role as a strategic security partner.

Government Affairs

We maintain relationships with several governments around the globe. Our visibility into the threat landscape, knowledge of threat actors' activities, and thought leadership in defending against cyber threats has helped to shape the legislative, regulatory and policy environment to enhance these governments' individual and collective cyber posture. As part of this effort, we contribute to the evolving standard-making processes, help define best practices in various jurisdictions and help organizations of all sizes better understand the cyber threat landscape. We also help governments identify future needs and requirements. Through these and related activities, we engage on the front lines of emerging cybersecurity related public policy and use our knowledge and insight to improve the cybersecurity of our government and industry customers.

Manufacturing

The manufacturing of our security appliances is outsourced to principally one third-party contract manufacturer. This approach allows us to reduce our costs as it reduces our manufacturing overhead and inventory and also allows us to adjust quickly to changing customer demand. Our manufacturing partner assembles our products using design specifications, quality assurance programs, and standards that we establish, and it procures components and assembles our products based on our demand forecasts. These forecasts represent our estimates of future demand for our products based upon historical trends and analysis from our sales and product management functions as adjusted for overall market conditions.

Our primary contract manufacturer is Flex Ltd. ("Flex"). The manufacturing agreement we entered into with Flex does not provide for any minimum purchase commitments and had an initial term of one year, which automatically renews for one-year terms, unless either party gives written notice to the other party not less than 90 days prior to the last day of the applicable term. Additionally, this agreement may be terminated by either party (i) with advance written notice provided to the other party, subject to certain notice period limitations, or (ii) with written notice, subject to applicable cure periods, if the other party has materially breached its obligations under the agreement.

Research and Development

We invest substantial resources in research and development to enhance our detection, analysis and correlation engines, expand our threat intelligence, build add-on functionality to our products, and improve our core technologies. We believe that adapting our hardware, software and cloud-based technologies to changes in the threat environment is critical to maintaining and expanding our leadership in the cyber security industry. Our engineering teams have deep networking, security and data management expertise and work closely with our customers and our Mandiant consultants to identify current and future needs. Because our Mandiant consultants use our products in their incident response and compromise assessment engagements and provide continual feedback to our engineering teams on product performance, detection efficacy, evasion techniques and attack trends, we are able to adapt our solutions as the threat environment evolves.

In addition to our focus on platform expansion and enhancement, our research and development teams are focused on developing automation tools and machine learning techniques to reduce the time to discover and distribute new threat intelligence, as well as generate efficiencies in our services offerings. We are also investing in security platform management and orchestration capabilities to provide unified reporting, automated response, and security orchestration features to customers in a single dashboard.

We maintain research and development activities across the globe with teams located in Germany, India, Ireland, Japan, Singapore and the United States.

Competition

We operate in the intensely competitive IT security market which is characterized by constant change and innovation. Changes in the threat landscape and broader IT infrastructures result in evolving customer requirements for cyber security. Several vendors have either introduced new products or incorporated features into existing products that compete with our solutions. Our current and potential future competitors fall into six general categories:

•large networking vendors such as Cisco and Juniper that may emulate or integrate security features similar to ours into their own products;

•large companies such as IBM, Oracle and HPE that have acquired security solutions and have the technical and financial resources to bring competitive solutions to the market;

- independent security vendors such as Palo Alto Networks, Proofpoint and CrowdStrike that offer products or features that claim to perform similar functions to our platform;
- small and large companies, including new market entrants, that offer niche product solutions that compete with some of the features present in our platform;
- providers of traditional signature-based security solutions, such as Symantec and McAfee; and
- other providers of incident response and compromise assessment services.

As our market grows and a larger share of IT budgets is allocated to cybersecurity, it will attract more highly specialized vendors as well as larger technology vendors that may continue to acquire or bundle their products more effectively. The principal competitive factors in our market include:

- ability to deliver the combination of technology, intelligence and expertise necessary to combat the current threat landscape;
- ability to detect and prevent known and unknown threats by overcoming the limitations of signature-based approaches, while maintaining a low rate of false-positive alerts;
- scalability, throughput and overall performance of our detection and prevention technologies;
- visibility into all stages of an attack, especially the exploit phase;
- ability to consolidate features onto a single platform, thereby reducing the complexity of maintaining solutions from multiple vendors;
- the ability to integrate with third-party IT providers to enable an orchestrated solution of products and services that detect, prevent and resolve cybersecurity threats across multiple attack vectors;
- breadth and richness of the shared threat intelligence, including dynamic and contextual threat intelligence on cyber crime, cyber espionage, hacktivism, attacks on critical infrastructure and nation-state attacks;
- flexible deployment options, including on-premise appliances, cloud-based software or a hybrid of both, as well as "as-a-service" options;
- brand awareness and reputation;
- strength and effectiveness of sales and marketing efforts;
- product extensibility and ability to integrate with other technologies in the network infrastructure;
- ease of use and customer experience; and
- price and total cost of ownership.

We believe we compete favorably with our competitors on the basis of these factors as a result of the features and performance of our platform, the ease of integration of our products with network infrastructures, the breadth of our services and solution offerings and the relatively low total cost of ownership of our products. However, many of our competitors have substantially greater financial, technical and other resources, greater name recognition, larger sales and marketing budgets, deeper customer relationships, broader distribution, and larger and more mature intellectual property portfolios.

Intellectual Property

Our success depends in part upon our ability to protect our core technologies and intellectual property. We rely on, among other things, patents, trademarks, copyrights and trade secret laws, confidentiality safeguards and procedures, and employee non-disclosure and invention assignment agreements to protect our intellectual property rights. We file patent applications to protect our intellectual property and believe that the duration of our issued patents is sufficient when considering the expected lives of our products. We cannot assure you whether any of our patent applications will result in the issuance of a patent or whether the examination process will result in patents of valuable breadth or applicability. In addition, any patents that may issue may be contested, circumvented, found unenforceable or invalidated, and we may not be able to prevent third parties from infringing them. We also license software from third parties for integration into our products, including open source software and other software available on commercially reasonable terms.

We control access to and use of our proprietary software, technology and other proprietary information through the use of internal and external controls, including contractual protections with employees, contractors, end-customers and partners, and our software is protected by U.S. and international copyright, patent and trade secret laws. Despite our efforts to protect our software, technology and other proprietary information, unauthorized parties may still copy or otherwise obtain and use our software, technology and other proprietary information. In addition, we intend to

expand our international operations, and effective patent, copyright, trademark, and trade secret protection may not be available or may be limited in foreign countries.

Our industry is characterized by the existence of a large number of patents and frequent claims and related litigation regarding patent and other intellectual property rights. If we become more successful, we believe that competitors will be more likely to try to develop

products that are similar to ours and that may infringe our proprietary rights. It may also be more likely that competitors or other third parties will claim that our products infringe their proprietary rights. In particular, large and established companies in the IT security industry have extensive patent portfolios and are regularly involved in both offensive and defensive litigation. From time-to-time, third parties, including certain of these large companies and non-practicing entities, may assert patent, copyright, trademark, and other intellectual property rights against us, our channel partners, or our end-customers, whom our standard license and other agreements obligate us to indemnify against such claims. Successful claims of infringement by a third party, if any, could prevent us from distributing certain products or performing certain services, require us to expend time and money to develop non-infringing solutions, or force us to pay substantial damages (including, in the United States, treble damages if we are found to have willfully infringed patents), royalties or other fees. We cannot assure you that we do not currently infringe, or that we will not in the future infringe, upon any third-party patents or other proprietary rights. See “Risk Factors—Risks Related to Our Business and Our Industry—Claims by others that we infringe their proprietary technology or other rights could harm our business” for additional information.

Business Seasonality

For discussion of seasonal trends, see our quarterly results of operations discussion within "Management's Discussion and Analysis of Financial Condition and Results of Operations" included in Part II, Item 7 of this Annual Report on Form 10-K.

Employees

As of December 31, 2018, we had approximately 3,200 employees. None of our employees are represented by a labor organization or are a party to any collective bargaining arrangement. We have never had a work stoppage, and we consider our relationship with our employees to be good.

Item 1A. Risk Factors

Our operations and financial results are subject to various risks and uncertainties including those described below. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, also may become important factors that affect us. If any of the following risks or others not specified below materialize, our business, financial condition and results of operations could be materially adversely affected. In that case, the trading price of our common stock could decline.

Risks Related to Our Business and Our Industry

If the IT security market does not continue to adopt our security platforms, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations and financial condition would be harmed.

Our future success depends on market adoption of our unique approach to IT security. We are seeking to disrupt the IT security market with our security platforms. Our platforms interoperate with but do not replace most signature-based IT security products. Enterprises and governments that use signature-based security products, such as firewalls, intrusion prevention systems, or IPS, anti-virus, or AV, and Web and messaging gateways, for their IT security may be hesitant to purchase our security platforms if they believe that signature-based products are more cost effective, provide substantially the same functionality as our platforms or provide a level of IT security that is sufficient to meet their needs. Currently, many enterprises and governments have not allocated a fixed portion of their budgets to protect against next-generation advanced cyber attacks. As a result, to expand our customer base, we need to convince potential customers to allocate a portion of their discretionary budgets to purchase our platforms. However, even if we are successful in doing so, any future deterioration in general economic conditions may cause our customers to cut their overall IT spending, and such cuts may fall disproportionately on products and services like ours, for which no fixed budgetary allocation has been made. If we do not succeed in convincing customers that our platforms should be an integral part of their overall approach to IT security and that a fixed portion of their annual IT budgets should be allocated to our platforms, our sales will not grow as quickly as anticipated, or at all, which would have an adverse impact on our business, results of operations and financial condition.

Even if there is significant demand for security solutions like ours, if our competitors include functionality that is, or is perceived to be, better than or equivalent to that of our platforms, we may have difficulty increasing the market penetration of our platforms. Furthermore, even if the functionality offered by other IT security providers is different and more limited than the functionality of our platforms, organizations may elect to accept such limited functionality in lieu of adding products from additional vendors like us, especially if competitor offerings are free or available at a

lower cost.

In addition, changes in customer requirements could reduce customer demand for our security solutions. For example, if customers were to reduce their number of web egress points in order to reduce their cyber attack surface, they would not need to purchase as many of our Network Threat Prevention appliances, which currently account for the largest portion of our threat prevention product revenue. Similarly, if one or more governments share, on a free or nearly free basis, threat intelligence with other governmental agencies or organizations, such as critical infrastructure companies, then those agencies or organizations might have less demand for additional threat intelligence and may purchase less of our threat intelligence offerings.

If enterprises and governments do not continue to adopt our security platforms for any of the reasons discussed above or for other reasons not contemplated, our sales would not grow as quickly as anticipated, or at all, and our business, results of operations and financial condition would be harmed.

We have had operating losses each year since our inception, and may not achieve or maintain profitability in the future.

We have incurred operating losses each year since our inception, including net losses of $243.1 million, $285.2 million and $485.4 million during the years ended December 31, 2018, 2017 and 2016, respectively. Any failure to increase our revenue and manage our cost structure as we grow our business could prevent us from achieving or, if achieved, maintaining profitability. Even if we do achieve profitability, we may not be able to sustain or increase profitability on a quarterly or annual basis. If we are unable to become and remain profitable, the value of our company could decrease and our ability to raise capital, maintain our research and development efforts, and expand our business could be negatively impacted.

We face intense competition and could lose market share to our competitors, which could adversely affect our business, financial condition and results of operations.

The market for security products and services is intensely competitive and characterized by rapid changes in technology, customer requirements, industry standards, threat vectors and frequent new product introductions and improvements. We anticipate continued challenges from current competitors, which in many cases are more established and enjoy greater resources than us, as well as by new entrants into the industry. If we are unable to anticipate or effectively react to these competitive challenges, our competitive position could weaken, and we could experience a decline in our growth rate or revenue that could adversely affect our business and results of operations. Our competitors and potential competitors include large networking vendors such as Cisco Systems and Juniper Networks that may emulate or integrate security features similar to ours into their own products; large companies such as IBM, Oracle and HPE that have acquired security solutions in recent years and have the technical and financial resources to bring competitive solutions to the market; independent security vendors such as Palo Alto Networks, Proofpoint and CrowdStrike that offer products or features that claim to perform similar functions to our platform; small and large companies, including new market entrants, that offer niche product solutions that compete with some of the features present in our platform; providers of traditional signature-based security solutions, such as Symantec and McAfee; and other providers of incident response and compromise assessment services. Other IT providers offer, and may continue to introduce, security features that compete with our platform, either in stand-alone security products or as additional features in their network infrastructure products. Many of our existing competitors have, and some of our potential competitors could have, substantial competitive advantages such as:

- greater name recognition, longer operating histories and larger customer bases;
- larger sales and marketing budgets and resources;
- broader distribution and established relationships with channel and distribution partners and customers;
- greater customer support resources;
- greater resources to make acquisitions or enter into strategic partnerships;
- lower labor and research and development costs;
- larger and more mature intellectual property portfolios; and
- substantially greater financial, technical and other resources.

In addition, some of our larger competitors have substantially broader product offerings and may be able to leverage their relationships with distribution partners and customers based on other products or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing our products, subscriptions and services, including by selling at zero or negative margins, product bundling or offering closed technology platforms. Potential customers may also prefer to purchase from their existing suppliers rather than a new supplier regardless of product performance or features. As a result, even if the features of our platform are superior, customers may not purchase our products. In addition, new innovative start-up companies, and larger companies that are making significant investments in research and development, may invent similar or superior products and technologies that compete with our platform. Our current and potential competitors may also establish cooperative relationships among themselves or with third parties that may further enhance their resources. Further, as our customers refresh the security

products bought in prior years, they may seek to consolidate vendors, which may result in current customers choosing to purchase products from our competitors on an ongoing basis.

Some of our competitors have made or could make acquisitions of businesses that allow them to offer more competitive and comprehensive solutions. As a result of such acquisitions, our current or potential competitors may be able to accelerate the adoption of new technologies that better address end-customer needs, devote greater resources to bring these products and services to market, initiate or withstand substantial price competition, or develop and expand their product and service offerings more quickly than we do. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, and loss of market share.

If we are unable to compete successfully, or if competing successfully requires us to take costly actions in response to the actions of our competitors, our business, financial condition and results of operations could be adversely affected.

Real or perceived defects, errors or vulnerabilities in our products or services, the misconfiguration of our products, the failure of our products or services to block malware or prevent a security breach, or the failure of customers to take action on attacks identified by our products could harm our reputation and adversely impact our business, financial position and results of operations.

Because our products and services are complex, they have contained and may contain design or manufacturing defects or errors that are not detected until after their deployment. Our products also provide our customers with the ability to customize a multitude of settings, and it is possible that a customer could misconfigure our products or otherwise fail to configure our products in an optimal manner. Such defects and misconfigurations of our products could cause our products or services to be vulnerable to security attacks, cause them to fail to secure networks and detect and block threats, or temporarily interrupt the networking traffic of our customers. In addition, because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our products and services are unable to detect or prevent. Moreover, as our products and services are adopted by an increasing number of enterprises and governments, it is possible that the individuals and organizations behind advanced malware attacks will focus on finding ways to defeat our products and services. If this happens, our networks, products, services and subscriptions could be targeted by attacks specifically designed to disrupt our business and undermine the perception that our products and services are capable of providing superior IT security, which, in turn, could have a serious impact on our reputation as a provider of security solutions. In addition, defects or errors in our subscription updates or our products could result in a failure of our subscriptions to effectively update customers' hardware and cloud-based products. Our data centers and networks may experience technical failures and downtime, may fail to distribute appropriate updates, or may fail to meet the increased requirements of a growing installed customer base, any of which could temporarily or permanently expose our customers' networks, leaving their networks unprotected against the latest security threats. Moreover, our products must interoperate with our customers' existing infrastructure, which often have different specifications, utilize multiple protocol standards, deploy products from multiple vendors, and contain multiple generations of products that have been added over time. As a result, unanticipated failures could occur if a customer deploys our products in an untested configuration. Similarly, if we inadvertently update our products with an erroneous configuration or untested detection content, invalid detections or product downtime could occur. Any of these situations could result in negative publicity to us, damage to our reputation, declining sales, increased expenses and customer relations issues, and therefore adversely impact our business, financial position and results of operations.

If any of our customers becomes infected with malware after using our products or services, such customer could be disappointed with our products and services, regardless of whether our products or services blocked the theft of any of such customer's data or would have blocked such theft if configured properly. Similarly, if our products detect attacks against a customer but the customer has not permitted our products to block the theft of customer data, customers and the public may erroneously believe that our products were not effective. For any security breaches against customers that use our services, such as customers that have hired us to monitor their networks and endpoints through our own or our co-branded security operation centers, breaches against those customers may result in customers and the public believing that our products and services failed. Furthermore, if any enterprises or governments that are publicly known to use our products or services are the subject of an advanced cyber attack that becomes publicized, our other current or potential customers may look to our competitors for alternatives to our products and services. Real or perceived security breaches of our customers' networks could cause disruption or damage to their networks or other negative consequences and could result in negative publicity to us, damage to our reputation, declining sales, increased expenses and customer relations issues.

Furthermore, our products and services may fail to detect or prevent malware, ransomware, viruses, worms or similar threats for any number of reasons, including our failure to enhance and expand our products and services to reflect industry trends, new technologies and new operating environments, the complexity of the environment of our clients and the sophistication of malware, viruses and other threats. In addition, from time to time, firms test our products against other security products. Our products may fail to detect or prevent threats in any particular test for a number of

reasons, including misconfiguration. To the extent potential customers, industry analysts or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our products or services do not provide significant value, our reputation and business could be harmed. Failure to keep pace with technological changes in the IT security industry and changes in the threat landscape could adversely affect our ability to protect against security breaches and could cause us to lose customers. In addition, in the event that a customer suffers a cyber attack, we could be subject to claims based on a misunderstanding of the scope of our contractual warranties or the protection afforded by the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act").

Any real or perceived defects, errors or vulnerabilities in our products and services, or any other failure of our products and services to detect an advanced threat, could result in:

- a loss of existing or potential customers or channel partners;
- delayed or lost revenue and harm to our financial condition and results of operations;
- a delay in attaining, or the failure to attain, market acceptance;

- the expenditure of significant financial and product development resources in efforts to analyze, correct, eliminate, or work around errors or defects, to address and eliminate vulnerabilities, or to identify and ramp up production with alternative third-party manufacturers;
- an increase in warranty claims, or an increase in the cost of servicing warranty claims, either of which would adversely affect our gross margins;
- harm to our reputation or brand; and
- litigation, regulatory inquiries, or investigations that may be costly and further harm our reputation.

A network or data security incident against us, whether actual, alleged or perceived, may harm our reputation, create liability and adversely impact our financial results.

Increasingly, companies are subject to a wide variety of attacks on their networks on an ongoing basis. In addition to traditional computer "hackers," malicious code (such as viruses and worms), phishing attempts, employee theft or misuse, and denial of service attacks, sophisticated nation-state and nation-state supported actors engage in intrusions and attacks (including advanced persistent threat intrusions) and add to the risks to our internal networks, cloud deployed enterprise and customer facing environments and the information they store and process. We and/or our third-party service providers may face security threats and attacks from a variety of sources. Our data, corporate systems, third-party systems and security measures may be breached due to the actions of outside parties, employee error, malfeasance, a combination of these, or otherwise, and, as a result, an unauthorized party may obtain access to our data. Furthermore, as a well-known provider of security solutions, we may be a more attractive target for such attacks. A breach in our data security or an attack against our service availability, or that of our third-party service providers, could impact our networks or networks secured by our products and subscriptions, creating system disruptions or slowdowns and exploiting security vulnerabilities of our products, and the information stored on our networks or those of our third-party service providers could be accessed, publicly disclosed, altered, lost, or stolen, which could subject us to liability and cause us financial harm. Any actual, alleged or perceived breach of network security in our systems or networks, or any other actual, alleged or perceived data security incident we or our third-party service providers suffer, could result in damage to our reputation, negative publicity, loss of channel partners, customers and sales, loss of competitive advantages over our competitors, increased costs to remedy any problems and otherwise respond to any incident, regulatory investigations and enforcement actions, costly litigation, and other liability. In addition, we may incur significant costs and operational consequences of investigating, remediating, eliminating and putting in place additional tools and devices designed to prevent actual or perceived security incidents, as well as the costs to comply with any notification obligations resulting from any security incidents. Any of these negative outcomes could adversely impact the market perception of our products and subscriptions and end-customer and investor confidence in our company and could seriously harm our business or operating results.

Our results of operations may vary significantly from period to period, which could cause the trading price of our common stock to decline.

Our results of operations have varied significantly from period to period, and we expect that our results of operations, including, but not limited to our GAAP and non-GAAP measures, will continue to vary as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including:

- our ability to attract new and retain existing customers or sell additional products and subscriptions to our existing customers;
- changes in our mix of products, subscriptions and services sold, including changes in multi-year subscriptions and support;
- the timing and success of new product, subscription or service introductions by us or our competitors;
- real or perceived reductions in our product efficacy by our customers or in the marketplace;
- the budgeting cycles, seasonal buying patterns and purchasing practices of customers;
- the timing of new contracts or shipments of our products and length of our sales cycles;
- changes in customer, distributor or reseller requirements or market needs;
- changes in the growth rate of the IT security market, particularly the market for threat protection solutions like ours that target next-generation advanced cyber attacks;
-

any change in the competitive landscape of the IT security market, including consolidation among our customers or competitors and strategic partnerships entered into by and between our competitors;

- the level of awareness of IT security threats, particularly advanced cyber attacks, and the market adoption of our platform;
- deferral of orders from customers in anticipation of new products or product enhancements announced by us or our competitors;
- our ability to successfully and continuously expand our business domestically and internationally;
- reductions in customer retention rates for our subscriptions and support;

- decisions by organizations to purchase IT security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
- any disruption in, or termination of, our relationships with channel partners;
- our inability to fulfill our customers' orders due to supply chain delays or events that impact our manufacturers or their suppliers;
- the timing and costs related to the development or acquisition of technologies or businesses or strategic partnerships;
- the lack of synergy or the inability to realize expected synergies, resulting from acquisitions or strategic partnerships;
- our inability to execute, complete or integrate efficiently any acquisition that we may undertake;
- increased expenses, unforeseen liabilities, or write-downs and any impact on our operating results from any acquisitions we consummate;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our products, subscriptions and services, or confronting our key suppliers, particularly our sole source suppliers, which could disrupt our supply chain;
- the cost and potential outcomes of future litigation;
- seasonality or cyclical fluctuations in our business;
- political, economic and social instability;
- future accounting pronouncements or changes in our accounting policies or practices;
- the amount and timing of operating costs and capital expenditures related to the expansion of our business; and
- increases or decreases in our revenues and expenses caused by fluctuations in foreign currency exchange rates.

Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other operating results from period to period. For example, as we offer more and more solutions through subscriptions and services, it becomes increasingly difficult for us to predict whether customers will purchase our solutions as a product, a subscription or a service. If customers purchase our solutions through subscriptions and services that have less profit associated with them than our products, our operating results could be harmed. Changes in the mix of offerings sold impacts the timing of recognition of revenue for our sales. Consequently, given the different revenue recognition policies associated with sales of our products, subscriptions and services, customers purchasing more of our subscription and services offerings and less of our product offerings than we anticipated could result in our actual revenue falling below our publicly announced guidance or the expectations of securities analysts and investors, resulting in a decline in our stock price.

As a result of this variability, our historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for these or other reasons, the market price of our common stock could fall substantially, and we could face costly lawsuits, including securities class action suits.

If we are unable to retain our customers, renew and expand our relationships with them, and add new customers, we may not be able to sustain revenue growth and we may not achieve or maintain profitability in the future.

From the year ended December 31, 2010 to the year ended December 31, 2018, our revenue grew from $11.8 million to $831.0 million, which represents a compounded annual growth rate of approximately 70%. Although we have experienced rapid growth in the past and currently have strong retention rates, we may not continue to grow in the future and our retention rates may decline. Any success that we may experience in the future will depend, in large part, on our ability to, among other things:

- maintain, renew and expand our existing customer base;
- win new customers to our solutions;
- increase revenues from existing customers through increased use of our products, subscriptions and services within their organizations;
- improve the capabilities of our products and subscriptions through research and development;
- continue to develop our cloud-based solutions;
- maintain the rate at which customers purchase our subscriptions and support;
- continue to successfully expand our business domestically and internationally; and

17

- successfully compete with other companies.

If we are unable to maintain consistent or increasing revenue growth or if our revenues decline, it may be difficult to achieve and maintain profitability and our business and financial results could be adversely affected. Our revenue for any prior quarterly or annual periods should not be relied upon as any indication of our future revenue or revenue growth.

If we are unable to sell additional products, subscriptions and services, as well as renewals of our subscriptions and services, to our customers, our future revenue and operating results will be harmed.

Our future success depends, in part, on our ability to expand the deployment of our platform with existing customers by selling them additional products, subscriptions and services, such as our FireEye Helix platform. This may require increasingly sophisticated and costly sales efforts and may not result in additional sales. In addition, the rate at which our customers purchase additional products, subscriptions and services depends on a number of factors, including the perceived need for additional IT security, general economic conditions, and our customers' level of satisfaction with our existing solutions they have previously purchased. If our efforts to sell additional products, subscriptions and services to our customers are not successful, our business may suffer.

Further, existing customers that purchase our platform have no contractual obligation to renew their subscriptions and support and maintenance services after the initial contract period, and given our limited operating history, we may not be able to accurately predict our retention rates. Our customers' retention rates may decline or fluctuate as a result of a number of factors, including the level of their satisfaction with our platform, our customer support, customer budgets and the pricing of our platform compared with the products and services offered by our competitors. If our customers renew their subscriptions, they may renew for shorter contract lengths or on other terms that are less economically beneficial to us. We cannot assure you that our customers will renew their subscriptions, and if our customers do not renew their subscriptions or renew them on less favorable terms, our revenue may grow more slowly than expected, not grow at all, or even decline.

We also depend on our installed customer base for future support and maintenance revenue. We offer our support and maintenance agreements for terms that generally range between one and five years. If customers choose not to renew their support and maintenance agreements or seek to renegotiate the terms of their support and maintenance agreements prior to renewing such agreements, our revenue may grow more slowly than expected, not grow at all, or even decline.

Recent, past and future acquisitions and investments could disrupt our business and harm our financial condition and operating results.

Our success will depend, in part, on our ability to expand our platform and grow our business in response to changing technologies, customer demands and competitive pressures. In some circumstances, we may decide to do so through the acquisition of complementary businesses and technologies rather than through internal development, including, for example, our acquisition of iSIGHT Security, Inc. (d/b/a iSIGHT Partners, Inc.) ("iSIGHT"), our acquisition of Invotas International Corporation ("Invotas"), our acquisition of Clean Communications Limited (d/b/a The Email Laundry) ("The Email Laundry") and our acquisition of X15 Software, Inc. ("X15").

The identification of suitable acquisition candidates can be difficult, time-consuming and costly, and we may not be able to successfully complete acquisitions that we target in the future. The risks we face in connection with acquisitions, including our acquisitions of iSIGHT, Invotas, The Email Laundry and X15 include:

- diversion of management time and focus from operating our business to addressing acquisition integration challenges;
- coordination of research and development and sales and marketing functions;
- integration of product and service offerings;
- retention of key employees from the acquired company;
- changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisition;
- cultural challenges associated with integrating employees from the acquired company into our organization;
- integration of the acquired company's accounting, management information, human resources and other administrative systems, as well as the acquired operations, technology and rights into our offerings, and any unanticipated expenses related to such integration;
-

the need to implement or improve controls, procedures, and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;

- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we don’t adequately address and that cause our reported results to be incorrect;
- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities;

- completing the transaction and achieving or utilizing the anticipated benefits of the acquisition within the expected timeframe, or at all;
- unanticipated write-offs or charges; and
- litigation or other claims in connection with the acquired company, including claims from terminated employees, customers, former stockholders or other third parties which may differ from or be more significant than the risks our business faces.

Our failure to address these risks or other problems encountered in connection with our past or future acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally. Future acquisitions could also result in dilutive issuances of equity securities. For example, in January 2016, we issued 1,793,305 shares of common stock in connection with our acquisition of iSIGHT; in February 2016, we issued 742,026 shares of common stock in connection with our acquisition of Invotas; in October 2017, we issued 259,425 shares of common stock in connection with our acquisition of The Email Laundry; and in January 2018, we issued 1,016,334 shares of common stock in connection with our acquisition of X15.

There is also a risk that future acquisitions will result in the incurrence of debt, contingent liabilities, amortization expenses, incremental operating expenses or the write-off of goodwill, any of which could harm our financial condition or operating results.

If we are unable to maintain successful relationships with our channel partners and technology alliance partners, or if our channel partners or technology alliance partners fail to perform, our ability to market, sell and distribute our platform will be limited, and our business, financial position and results of operations will be harmed.

In addition to our direct sales force, we rely on our indirect channel partners to sell and support our platform. We derive a substantial portion of our revenue from sales of our products, subscriptions and services through, or with the assistance of, our indirect channel, and we expect that sales through channel partners will continue to be a significant percentage of our revenue. We also partner with our technology alliance partners to design go-to-market strategies that combine our platform with products or services provided by our technology alliance partners.

Our agreements with our channel partners and our technology alliance partners are generally non-exclusive, meaning our partners may offer customers products from several different companies, including products that compete with ours. If our channel partners do not effectively market and sell our platform, choose to use greater efforts to market and sell their own products or those of our competitors, or fail to meet the needs of our customers, our ability to grow our business and sell our platform may be adversely affected. Our channel partners and technology alliance partners may cease marketing our platform with limited or no notice and with little or no penalty, and new channel partners require extensive training and may take several months or more to achieve productivity. The loss of a substantial number of our channel partners, our possible inability to replace them, or the failure to recruit additional channel partners could materially and adversely affect our results of operations. In addition, sales by channel partners are more likely than direct sales to involve collectability concerns, particularly in developing markets. Our channel partner structure could also subject us to lawsuits or reputational harm if, for example, a channel partner misrepresents the functionality of our platform to customers or violates applicable laws or our corporate policies.

Our ability to achieve revenue growth in the future will depend in part on our success in maintaining successful relationships with our channel partners, and in training our channel partners to independently sell and deploy our platform. If we are unable to maintain our relationships with these channel partners or otherwise develop and expand our indirect sales channel, or if our channel partners fail to perform, our business, financial position and results of operations could be adversely affected.

Fluctuating economic conditions make it difficult to predict revenue for a particular period, and a shortfall in revenue may harm our business and operating results.

Our revenue depends significantly on general economic conditions and the demand for products in the IT security market. Economic weakness, customer financial difficulties, and constrained spending on IT security may result in decreased revenue and earnings. Such factors could make it difficult to accurately forecast our sales and operating results and could negatively affect our ability to provide accurate forecasts to our contract manufacturers and manage our inventory purchases, contract manufacturer relationships and other costs and expenses. In addition, concerns regarding the effects of the U.K.'s decision to exit the EU, commonly referred to as "Brexit", uncertainties related to

changes in public policies such as domestic and international regulations, taxes or international trade agreements as well as geopolitical turmoil and other disruptions to global and regional economies and markets in many parts of the world, have and may continue to put pressure on global economic conditions and overall spending on IT security. General economic weakness may also lead to longer collection cycles for payments due from our customers, an increase in customer bad debt, restructuring initiatives and associated expenses, and impairment of investments. Furthermore, the continued uncertainty in worldwide credit markets, including the sovereign debt situation in certain countries in the EU may adversely impact the ability of our customers to adequately fund their expected capital expenditures, which could lead to delays or cancellations of planned purchases of our platform.

Uncertainty about future economic conditions also makes it difficult to forecast operating results and to make decisions about future investments. Future or continued economic weakness for us or our customers, failure of our customers and markets to recover from such

weakness, customer financial difficulties, and reductions in spending on IT security could have a material adverse effect on demand for our platform and consequently on our business, financial condition and results of operations.

If we fail to effectively manage our growth, our business, financial condition and results of operations would be harmed.

Although our business has experienced significant growth in the past, we cannot provide any assurance that our business will continue to grow at the same rate or at all. To improve our infrastructure, we continue to enhance our enterprise resource planning system, including revenue recognition and management software, and implement and enhance additional systems and controls. There is no assurance that we will be able to successfully scale improvements to our enterprise resource planning system or implement or scale improvements to our other systems, processes and controls in a manner that keeps pace with our growth or that such systems, processes and controls will be effective in preventing or detecting errors, omissions or fraud.

As part of our efforts to improve our internal systems, processes and controls, we have licensed technology from third parties. The support services available for such third-party technology are outside of our control and may be negatively affected by consolidation in the software industry. In addition, if we do not receive adequate support for the software underlying our systems, processes and controls, our ability to provide products and services to our customers in a timely manner may be impaired, which may cause us to lose customers, limit us to smaller deployments of our platform or increase our technical support costs.

Many of our expenses are relatively fixed, at least in the short term. If our projections or assumptions on which we base our projections are incorrect, we may not be able to adjust our expenses rapidly enough to avoid an adverse impact on our profitability or cash flows.

To manage this growth effectively, we must continue to improve our operational, financial and management systems and controls by, among other things:

- effectively hiring, training and integrating new employees, particularly members of our sales and management teams;
- further improving our key business applications, processes and IT infrastructure, including our data centers, to support our business needs;
- continuing to refine our ability to forecast our bookings, billings, revenues, expenses and cash flows;
- enhancing our information and communication systems to ensure that our employees and offices around the world are well coordinated and can effectively communicate with each other and our growing base of channel partners and customers;
- improving our internal control over financial reporting and disclosure controls and procedures to ensure timely and accurate reporting of our operational and financial results; and
- appropriately documenting and testing our IT systems and business processes.

These and other improvements in our systems and controls will require significant capital expenditures and the allocation of valuable management and employee resources. If we fail to implement these improvements effectively, our ability to manage our expected growth, ensure uninterrupted operation of key business systems and comply with the rules and regulations applicable to public reporting companies would be impaired, and our business, financial condition and results of operations would be harmed.

If the general level of advanced cyber attacks declines, or is perceived by our current or potential customers to have declined, our business could be harmed.

Our business is substantially dependent on enterprises and governments recognizing that advanced cyber attacks are pervasive and are not effectively prevented by legacy security solutions. High visibility attacks on prominent enterprises and governments have increased market awareness of the problem of advanced cyber attacks and help to provide an impetus for enterprises and governments to devote resources to protecting against advanced cyber attacks, such as testing our platform, purchasing it, and broadly deploying it within their organizations. If advanced cyber attacks were to decline, or enterprises or governments perceived that the general level of advanced cyber attacks have declined, our ability to attract new customers and expand our offerings within existing customers could be materially and adversely affected. A reduction in the threat landscape, for example, as a result of the 2015 cybersecurity agreement between China and the U.S., may reduce the demand from customers or prospects for our solutions, and therefore could increase our sales cycles and harm our business, results of operations and financial condition.

Disruptions or other business interruptions that affect the availability of our Dynamic Threat Intelligence ("DTI") cloud, our Helix platform, or other cloud-based products and services we offer or may offer could adversely impact our customer relationships as well as our overall business.

When a customer purchases one or more of our threat prevention appliances, it must also purchase a subscription to our DTI cloud for a term of one to three years. Our DTI cloud enables global sharing of threat intelligence uploaded by any of our customers' cloud-connected FireEye appliances. We also offer additional cloud-based platforms such as our Email Threat Prevention, Mobile Threat Prevention and Threat Analytics Platforms and provide security solutions through our own and our co-branded security operation centers.

Our customers depend on the continuous availability of our DTI cloud and other cloud-based products and services. Our cloud-based products and services are vulnerable to damage or interruption from a variety of sources, including damage or interruption caused by

fire, earthquake, power loss, telecommunications or computer systems failure, cyber attack, human error, terrorist acts and war. Our data centers and networks may experience technical failures and downtime, may fail to distribute appropriate updates, or may fail to meet the increased requirements of a growing customer base, any of which could temporarily or permanently expose our customers' networks, leaving their networks unprotected against the latest security threats or, in the case of technical failures and downtime of security operation centers, all security threats. In addition, there may also be system or network interruptions if new or upgraded systems are defective or not installed properly. Moreover, interruptions in our subscription updates could result in a failure of our DTI cloud to effectively update customers' hardware products and thereby leave our customers more vulnerable to attacks. Interruptions or failures in our service delivery could cause customers to terminate their subscriptions with us, could adversely affect our retention rates, and could harm our ability to attract new customers. Our business would also be harmed if our customers believe that our DTI cloud or other cloud-based products and services are unreliable.

In addition, we provide our cloud-based products and services through third-party data center hosting facilities located in the United States and other countries. While we control and have access to our servers and all of the components of our network that are located in our data centers, we do not control the operation of these facilities. The owners of the data center facilities have no obligation to renew their agreements with us on commercially reasonable terms, or at all. If we are unable to renew these agreements on commercially reasonable terms, or if one of our data center operators is acquired, we may be required to transfer our servers and other infrastructure to new data center facilities, and we may incur significant costs and possible service interruption in connection with doing so.

We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to hire, integrate, train and retain qualified personnel, including members for our board of directors, could harm our business.

Our future success is substantially dependent on our ability to hire, integrate, train, retain and motivate the members of our management team and other key employees throughout our organization, including key employees obtained through our acquisitions. Competition for highly skilled personnel is intense, especially in the San Francisco Bay Area and the Washington D.C. Area, where we have a substantial presence and need for highly skilled personnel. We may not be successful in hiring or retaining qualified personnel to fulfill our current or future needs, and potential changes in U.S. immigration and work authorization laws and regulations, including those that restrain the flow of technical and professional talent, may make it difficult to renew or obtain visas for highly skilled personnel that we have hired or are actively recruiting. We are also substantially dependent on the continued service of our existing engineering personnel because of the complexity of our platform. Our competitors may be successful in recruiting and hiring members of our management team or other key employees, including key employees obtained through our acquisitions, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. Also, to the extent we hire employees from mature public companies with significant financial resources, we may be subject to allegations that such employees have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product. In addition, we believe that it is important to establish and maintain a corporate culture that facilitates the maintenance and transfer of institutional knowledge within our organization and also fosters innovation, teamwork, a passion for customers and a focus on execution. From time to time, there may be changes in our management team resulting from the hiring or departure of executives. Any such changes may result in a loss of institutional knowledge and cause disruptions to our business. In addition, if we are not successful in integrating key employees into our organization, such failure could delay or hinder our product development efforts and the achievement of our strategic objectives, which could adversely affect our business, financial condition and results of operations.

Our employees, including our executive officers, work for us on an "at-will" basis, which means they may terminate their employment with us at any time. We do not maintain key person life insurance policies on any of our key employees. If one or more of our key employees resigns or otherwise ceases to provide us with their service, our business could be harmed.

If we do not effectively hire, integrate and train our direct sales force, we may be unable to add new customers or increase sales to our existing customers, and our business will be adversely affected.

We continue to be substantially dependent on our direct sales force to obtain new customers and increase sales with existing customers. There is significant competition for sales personnel with the skills and technical knowledge that

we require. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, integrating, training and retaining sufficient numbers of sales personnel to support our growth, particularly in international markets. New hires require significant training and may take significant time before they achieve full productivity. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. If we are unable to hire and train a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business will be adversely affected.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. As a result, our sales, billings and revenue are difficult to predict and may vary substantially from period to period, which may cause our results of operations to fluctuate significantly.

Our results of operations may fluctuate, in part, because of the resource intensive nature of our sales efforts, the length and variability of our sales cycle and the short-term difficulty in adjusting our operating expenses. Our results of operations depend in part on sales to

large organizations. The length of our sales cycle, from proof of concept to delivery of and payment for our platform, is typically three to nine months but can be more than a year. To the extent our competitors develop products that our prospective customers view as equivalent to ours, our average sales cycle may increase. Because the length of time required to close a sale varies substantially from customer to customer, it is difficult to predict exactly when, or even if, we will make a sale with a potential customer. As a result, large individual sales have, in some cases, occurred in quarters subsequent to or in advance of those we anticipated, or have not occurred at all. We are generally billing a number of large deals in any quarter, and the loss or delay of one or more of these large transactions in a quarter could impact our results of operations for that quarter and any future quarters for which revenue from that transaction is delayed. Furthermore, some sales (such as product sales) generally result in immediate recognition of revenue, while other sales, such as product subscription sales, require the recognition of revenue over periods of one year or longer typically. As a result of these factors, it is difficult for us to forecast our revenue accurately in any quarter based on our internal forecasts of billings. Because a substantial portion of our expenses are relatively fixed in the short term, our results of operations will suffer if our revenue falls below our expectations in a particular quarter, which could cause the price of our common stock to decline.

We rely on revenue from sales of products, subscriptions, and maintenance and support, and because we recognize revenue from most of these sales over the term of the relevant useful life or subscription period, downturns or upturns in sales are not immediately reflected in full in our results of operations.

Revenue from sales of our products, subscriptions, and maintenance and support accounts for a significant portion of our total revenue. New or renewal sales of subscription and maintenance and support contracts may decline or fluctuate as a result of a number of factors, including customers' level of satisfaction with our products and subscriptions, the actual or perceived efficacy of our security solutions, the prices of our products and subscriptions, the prices of products and subscriptions offered by our competitors or reductions in our customers' spending levels. If our sales of new or renewal subscription and service contracts decline, our revenue and revenue growth rate may decline and adversely affect our business. In addition, we recognize revenue from most of our security appliances sales ratably over the useful life, and we recognize revenue from our subscriptions and maintenance and support contracts revenue ratably over the term of the relevant contract period, which is generally between one to five years. As a result, much of the product, subscription and support revenue we report each quarter is derived from sales in prior quarters. Consequently, a decline in new or renewal sales in any one quarter will not be fully reflected in revenue in that quarter but will negatively affect our revenue in future quarters. Accordingly, the effect of significant decreases in the market acceptance of, or demand for, our intelligence-dependent security appliances, subscriptions or maintenance and support contracts may not be immediately apparent from our results of operations until future periods. Also, it is difficult for us to rapidly increase our revenue through additional sales in any period, as the majority of our revenue is derived from sales of our products, subscriptions and services sold in prior periods. Furthermore, any increases in the average term of our subscriptions or maintenance and support contracts would result in a longer revenue recognition period, and could reduce the amount of revenue recognized in each period.

The sales prices of our products, subscriptions and services may decrease, which may reduce our gross profits and adversely impact our financial results.

The sales prices for our products, subscriptions and services may decline for a variety of reasons, including competitive pricing pressures, discounts, a change in our mix of products, subscriptions and services, anticipation of the introduction of new products, subscriptions or services, introduction of new pricing and packaging or promotional programs. Competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the price of products or subscriptions that compete with ours or may bundle them with other products and subscriptions. Additionally, although we price our products and subscriptions worldwide in U.S. dollars, currency fluctuations in certain countries and regions may negatively impact actual prices that partners and customers are willing to pay in those countries and regions, or the effective prices we realize in our reporting currency. Furthermore, we anticipate that the sales prices and gross profits for our products will decrease over product life cycles. We cannot assure you that we will be successful in developing and introducing new offerings with enhanced functionality on a timely basis, or that our new product and subscription offerings, if introduced, will enable us to maintain our prices and gross profits at levels that will allow us to maintain positive gross

margins and achieve profitability.

If we do not accurately anticipate and respond promptly to changes in our customers' technologies, business plans or security needs, our competitive position and prospects could be harmed.

The IT security market has grown quickly and is expected to continue to evolve rapidly. Moreover, many of our customers operate in markets characterized by rapidly changing technologies and business plans, which require them to add numerous network access points and adapt to increasingly complex IT networks, incorporating a variety of hardware, software applications, operating systems and networking protocols. As their technologies and business plans grow more complex, we expect these customers to face new and increasingly sophisticated methods of attack. We face significant challenges in ensuring that our platform effectively identifies and responds to these advanced and evolving attacks without disrupting our customers' network performance. As a result of the continued rapid innovations in the technology industry, including the rapid growth of smart phones, tablets and other devices, the trend of "bring your own device" in enterprises, and the rapidly evolving Internet of Things ("IOT"), we expect the networks of our customers to continue to change rapidly and become more complex.

We have identified a number of new products and enhancements to our platform that we believe are important to our continued success in the IT security market, including our FireEye Helix platform and enhancements to our endpoint solution. There can be no assurance that we will be successful in developing and marketing, on a timely basis, such new products or enhancements or that our new products or enhancements will adequately address the changing needs of the marketplace. In addition, some of our new products and enhancements may require us to develop new hardware architectures that involve complex, expensive and time-consuming research and development processes. Although the market expects rapid introduction of new products and enhancements to respond to new threats, the development of these products and enhancements is difficult and the timetable for commercial release and availability is uncertain, as there can be significant time lags between initial beta releases and the commercial availability of new products and enhancements. We may experience unanticipated delays in the availability of new products and enhancements to our platform and fail to meet customer expectations with respect to the timing of such availability. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing, releasing and making available on a timely basis new products and enhancements to our platform, such as our FireEye Helix platform and enhancements to our endpoint solution, that can adequately respond to advanced threats and our customers' needs, our competitive position and business prospects will be harmed. Furthermore, from time to time, we or our competitors may announce new products with capabilities or technologies that could have the potential to replace or shorten the life cycles of our existing products. There can be no assurance that announcements of new products will not cause customers to defer purchasing our existing products.

Additionally, the process of developing new technology is expensive, complex and uncertain. The success of new products and enhancements depends on several factors, including appropriate component costs, timely completion and introduction, differentiation of new products and enhancements from those of our competitors, and market acceptance. To maintain our competitive position, we must continue to commit significant resources to developing new products or enhancements to our platform before knowing whether these investments will be cost-effective or achieve the intended results. There can be no assurance that we will successfully identify new product opportunities, develop and bring new products or enhancements to market in a timely manner, or achieve market acceptance of our platform, or that products and technologies developed by others will not render our platform obsolete or noncompetitive. If we expend significant resources on researching and developing products or enhancements to our platform and such products or enhancements are not successful, our business, financial position and results of operations may be adversely affected.

Our current research and development efforts may not produce successful products or enhancements to our platform that result in significant revenue, cost savings or other benefits in the near future, if at all.

We must continue to dedicate significant financial and other resources to our research and development efforts if we are to maintain our competitive position. However, developing products and enhancements to our platform is expensive and time consuming, and there is no assurance that such activities will result in significant new marketable products or enhancements to our platform, design improvements, cost savings, revenue or other expected benefits. If we spend significant resources on research and development and are unable to generate an adequate return on our investment, our business and results of operations may be materially and adversely affected.

If we are unable to increase sales of our platform to large organizations while mitigating the risks associated with serving such customers, our business, financial position and results of operations may suffer.

Our growth strategy is dependent, in part, upon increasing sales of our platform to large enterprises and governments. Sales to large customers involve risks that may not be present (or that are present to a lesser extent) with sales to smaller entities. These risks include:

- increased purchasing power and leverage held by large customers in negotiating contractual arrangements with us;
- more stringent or costly requirements imposed upon us in our support service contracts with such customers, including stricter support response times and penalties for any failure to meet support requirements;
- more complicated implementation processes;
- longer sales cycles and the associated risk that substantial time and resources may be spent on a potential customer that ultimately elects not to purchase our platform or purchases less than we hoped;
- closer relationships with, and dependence upon, large technology companies who offer competitive products; and

- more pressure for discounts and write-offs.

In addition, because security breaches with respect to larger, high-profile enterprises are likely to be heavily publicized, there is increased reputational risk associated with serving such customers. If we are unable to increase sales of our platform to large enterprise and government customers while mitigating the risks associated with serving such customers, our business, financial position and results of operations may suffer.

Seasonality may cause fluctuations in our revenue.

We believe there are significant seasonal factors that may cause us to record higher revenue in some quarters compared with others. We believe this variability is largely due to (i) our customers' budgetary and spending patterns, as many customers spend the unused portions of their discretionary budgets prior to the end of their fiscal years, and (ii) our sales compensation plans, which are typically structured around annual quotas and stair step commission rates. For example, we have historically recorded our highest level of revenue

in our fourth quarter, which we believe corresponds to the fourth quarter of a majority of our customers. Similarly, we have historically recorded our second-highest level of revenue in our third quarter, which corresponds to the fourth quarter of U.S. federal agencies and other customers in the U.S. federal government. Our growth rate over the last couple years may have made seasonal fluctuations more difficult to detect. If our rate of growth slows over time, seasonal or cyclical variations in our operations may become more pronounced, and our business, results of operations and financial position may be adversely affected.

Claims by others that we infringe their proprietary technology or other rights could harm our business.

Technology companies frequently enter into litigation based on allegations of patent infringement or other violations of intellectual property rights. In addition, patent holding companies seek to monetize patents they have purchased or otherwise obtained. As we face increasing competition and gain an increasingly higher profile, the possibility of intellectual property rights claims against us grows. From time to time, third parties have asserted, and we expect that third parties will continue to assert, claims of infringement of intellectual property rights against us. For example, on December 29, 2017, we executed Confidential Patent License Agreements with Finjan Holdings, Inc. ("Finjan"), whereby we resolved all pending litigation matters. Under the terms of the settlement agreement, we paid Finjan a one-time net cash settlement amount of $12.5 million in December 2017, in exchange for the resolution and settlement of all claims between FireEye and Finjan and for cross-licenses between the companies of certain issued patents and patent applications. Other security companies have paid amounts to the same plaintiff to license some of the patents asserted against us. Third parties may in the future also assert claims against our customers or channel partners, whom our standard license and other agreements obligate us to indemnify against claims that our products infringe the intellectual property rights of third parties. While we intend to increase the size of our patent portfolio, many of our competitors and others may now and in the future have significantly larger and more mature patent portfolios than we have. In addition, future litigation may involve patent holding companies or other patent owners who have no relevant product offerings or revenue and against whom our own patents may therefore provide little or no deterrence or protection. Any claim of intellectual property infringement by a third party, even a claim without merit, could cause us to incur substantial costs defending against such claim, could distract our management from our business and could require us to cease use of such intellectual property. Furthermore, because of the substantial amount of discovery required in connection with intellectual property litigation, there is a risk that some of our confidential information could be compromised by the discovery process.

Although third parties may offer a license to their technology or other intellectual property, the terms of any offered license may not be acceptable, and the failure to obtain a license or the costs associated with any license could cause our business, financial condition and results of operations to be materially and adversely affected. We may also be subject to additional fees or be required to obtain new licenses if any of our licensors allege that we have not properly paid for such licenses or that we have improperly used the technologies under such licenses. In addition, some licenses may be non-exclusive, and therefore our competitors may have access to the same technology licensed to us. If a third party does not offer us a license to its technology or other intellectual property on reasonable terms, or at all, we could be enjoined from continued use of such intellectual property. As a result, we may be required to develop alternative, non-infringing technology, which could require significant time (during which we could be unable to continue to offer our affected products, subscriptions or services), effort, and expense and may ultimately not be successful. Furthermore, a successful claimant could secure a judgment or we may agree to a settlement that prevents us from distributing certain products, providing certain subscriptions or performing certain services or that requires us to pay substantial damages, royalties or other fees. Any of these events could harm our business, financial condition and results of operations.

Because we depend on a limited number of manufacturers to build the appliances used in our platform, we are susceptible to manufacturing delays and pricing fluctuations that could prevent us from shipping customer orders on time, or on a cost-effective basis, which may result in the loss of sales and customers.

We depend on a limited number of third-party manufacturers, primarily Flextronics Telecom Systems, Ltd., as sole source manufacturers for our appliances used in our platform. Our reliance on third-party manufacturers reduces our control over the manufacturing process and exposes us to risks, including reduced control over quality assurance, product costs, product supply, upgrades and expansions and timing. Any manufacturing disruption by these third-party manufacturers could severely impair our ability to fulfill orders on time. If we are unable to manage our relationships

with these third-party manufacturers effectively, or if these manufacturers suffer delays or disruptions for any reason, experience increased manufacturing lead-times, capacity constraints or quality control problems in their manufacturing operations, or fail to meet our future requirements for timely delivery, our ability to ship products to our customers would be severely impaired, and our business and results of operations would be harmed.

Further, the portion of our appliances used in our platform that are sourced outside the United States may be subject to additional logistical risks or risks associated with complying with local rules and regulations in foreign countries. Significant changes to existing international trade agreements could lead to sourcing or logistics disruption resulting from import delays or the imposition of increased tariffs on our sourcing partners. For example, the United States and Chinese governments have each enacted, and discussed more potential, import tariffs. These tariffs, depending on their ultimate scope and how they are implemented, could negatively impact our business by increasing our costs and impair our ability to fulfill orders.

In addition, our reliance on third-party manufacturers exposes us to the risk that certain minerals, known as “conflict minerals,” that are contained in our products have originated in the Democratic Republic of the Congo or an adjoining country. As a result of the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the SEC adopted disclosure requirements for public

companies whose products contain conflict minerals that are necessary to the functionality or production of such products. Although the SEC has provided guidance with respect to a portion of the conflict minerals filing requirements that somewhat reduced the reporting required, we have incurred and expect to incur additional costs to comply with the disclosure requirements, including costs related to determining the source of the conflict minerals used in our products. Moreover, the implementation of these requirements could adversely affect the sourcing, availability and pricing of materials used in the manufacture of our products to the extent that there may be only a limited number of suppliers offering "conflict free" minerals that can be used in our products. There can be no assurance that we will be able to obtain such minerals in sufficient quantities or at competitive prices. We may also encounter customers who require that all of the components of our products be certified as conflict free. If we are not able to meet customer requirements, such customers may choose to not purchase our products, which could impact our sales.
Our third-party manufacturers typically fulfill our supply requirements on the basis of individual orders. We are subject to a risk of supply shortages and changes in pricing terms because we do not have long-term contracts with our third-party manufacturers that guarantee capacity, the continuation of particular pricing terms or the extension of credit limits. Our contract with our primary manufacturer permits it to terminate such contract at its convenience, subject to prior notice requirements. Any production interruptions for any reason, such as a natural disaster, epidemic, capacity shortages, or quality problems at one of our manufacturing partners would negatively affect sales of our products and adversely impact our business and results of operations.

We may be unable to protect our intellectual property adequately, which could harm our business, financial condition and results of operations.

We believe that our intellectual property is an essential asset of our business. We rely on a combination of patent, copyright, trademark and trade secret laws, as well as confidentiality procedures and contractual provisions, to establish and protect our intellectual property rights in the United States and abroad. The efforts we have taken to protect our intellectual property may not be sufficient or effective, and our trademarks, copyrights and patents may be held invalid or unenforceable. Any U.S. or other patents issued to us may not be sufficiently broad to protect our proprietary technologies, and given the costs of obtaining patent protection, we may choose not to seek patent protection for certain of our proprietary technologies. We may not be effective in policing unauthorized use of our intellectual property, and even if we do detect violations, litigation may be necessary to enforce our intellectual property rights. Any enforcement efforts we undertake, including litigation, could be time-consuming and expensive, could divert management's attention and may result in a court determining that our intellectual property rights are unenforceable. If we are not successful in cost-effectively protecting our intellectual property rights, our business, financial condition and results of operations could be harmed.

We incorporate technology from third parties into our products, and our inability to obtain or maintain rights to the technology could harm our business.

We incorporate technology from third parties into our products. We cannot be certain that our suppliers and licensors are not infringing the intellectual property rights of third parties or that the suppliers and licensors have sufficient rights to the technology in all jurisdictions in which we may sell our products. Some of our agreements with our suppliers and licensors may be terminated for convenience by them. If we are unable to obtain or maintain rights to any of this technology because of intellectual property infringement claims brought by third parties against our suppliers and licensors or against us, or if we are unable to continue to obtain such technology or enter into new agreements on commercially reasonable terms, our ability to develop and sell products, subscriptions and services containing such technology could be severely limited, and our business could be harmed. Additionally, if we are unable to obtain necessary technology from third parties, including certain sole suppliers, we may be forced to acquire or develop alternative technology, which may require significant time, cost and effort and may be of lower quality or performance standards. This would limit and delay our ability to offer new or competitive products and increase our costs of production. If alternative technology cannot be obtained or developed, we may not be able to offer certain functionality as part of our products, subscriptions and services. As a result, our margins, market share and results of operations could be significantly harmed.

Our products and subscriptions contain third-party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions.

Our products and subscriptions contain software modules licensed to us by third-party authors under "open source" licenses. The use and distribution of open source software may entail greater risks than the use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code. Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon the type of open source software we use. If we combine our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release the source code of our proprietary software to the public. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us.

Although we monitor our use of open source software to try to avoid subjecting our products and subscriptions to conditions, the terms of many open source licenses have not been interpreted by U.S. courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions will be effective. From time to time, we may face claims from third parties asserting ownership of, or demanding release

of, the open source software or derivative works that we developed using such software (which could include our proprietary source code), or otherwise seeking to enforce the terms of the applicable open source license. These claims could result in litigation. If we are held to have breached the terms of an open source software license, we could be required to seek licenses from third parties to continue offering our products on terms that are not economically feasible, to re-engineer our products, to discontinue the sale of our products if re-engineering could not be accomplished on a timely or cost-effective basis, or to make generally available, in source code form, our proprietary code, any of which could adversely affect our business, results of operations and financial condition.

U.S. federal, state and local government sales are subject to a number of challenges and risks that may adversely impact our business.

Sales to U.S. federal, state, and local governmental agencies have accounted for, and may in the future account for, a significant portion of our revenue. Sales to such government entities are subject to the following risks:

- selling to governmental agencies can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;
- government certification requirements applicable to our products may change and, in doing so, restrict our ability to sell into the U.S. federal government sector until we have attained the revised certification;
- government demand and payment for our products and services may be impacted by government shutdowns, public sector budgetary cycles, contracting requirements and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our products and services;
- we sell our platform to governmental agencies through our indirect channel partners, and these agencies may have statutory, contractual or other legal rights to terminate contracts with our distributors and resellers for convenience or due to a default, and any such termination may adversely impact our future results of operations;
- governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and results of operations, or institute fines or civil or criminal liability if the audit were to uncover improper or illegal activities; and
- governments may require certain products purchased by it to be manufactured in the United States and other relatively high-cost manufacturing locations, and we may not manufacture all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies.

Our ability to maintain customer satisfaction depends in part on the quality of our professional service organization and technical and other support services, including the quality of the support provided on our behalf by certain channel partners. Failure to maintain high-quality customer support could have a material adverse effect on our business, financial condition and results of operations.

Once our platform is deployed within our customers' networks, our customers depend on our technical and other support services, as well as the support of our channel partners, to resolve any issues relating to the implementation and maintenance of our platform. If we or our channel partners do not effectively assist our customers in deploying our platform, succeed in helping our customers quickly resolve post-deployment issues, or provide effective ongoing support, our ability to sell additional products, subscriptions or services as part of our platform to existing customers would be adversely affected and our reputation with potential customers could be damaged. Many larger organizations have more complex networks and require higher levels of support than smaller customers. If we fail to meet the requirements of our larger customers, it may be more difficult to execute on our strategy of upselling and cross selling with these customers. Additionally, if our channel partners do not effectively provide support to the satisfaction of our customers, we may be required to provide this level of support to those customers, which would require us to hire additional personnel and to invest in additional resources. It can take significant time and resources to recruit, hire, and train qualified technical support employees. We may not be able to hire such resources fast enough to keep up with demand. To the extent that we or our channel partners are unsuccessful in hiring, training, and retaining adequate support resources, our ability and the ability of our channel partners to provide adequate and timely support to our customers will be negatively impacted, and our customers' satisfaction with our platform will be adversely affected. Additionally, to the extent that we need to rely on our sales engineers to provide post-sales support, our sales productivity will be negatively impacted, which would harm our results of operations.

26

Our limited operating history makes it difficult to evaluate our current business and prospects and may increase the risk that we will not be successful.

We were founded in 2004, and our first commercially successful product was shipped in 2008. Since then, we have continued to expand our platform, both organically and through acquisitions, including through the addition of Mandiant Corporation's endpoint threat detection, response and remediation products; advanced threat intelligence capabilities; and incident response and security consulting services. The majority of our revenue growth began in 2010. Our limited operating history makes it difficult to evaluate our current business and prospects and plan for and model our future growth. We have encountered and will continue to encounter risks and uncertainties frequently encountered by emerging technology-based companies in developing markets.

If our assumptions regarding these risks and uncertainties are incorrect or change in response to changes in the IT security market, our results of operations and financial results could differ materially from our plans and forecasts. Although we have experienced rapid growth in the past, there is no assurance that such growth will continue. Any success we may experience in the future will depend in large part on our ability to, among other things:

- maintain and expand our customer base and the ways in which customers use our products and services;
- expand revenue from existing customers through increased or broader use of our products and services within their organizations;
- convince customers to allocate a fixed portion of their annual IT budgets to our products and services;
- improve the performance and capabilities of our platform through research and development;
- effectively expand our business domestically and internationally, which will require that we fill key management positions, particularly internationally; and
- successfully compete with other companies that currently provide, or may in the future provide, solutions like ours that protect against next-generation advanced cyber attacks.

If we are unable to achieve our key objectives, including the objectives listed above, our business and results of operations will be adversely affected and the fair market value of our common stock could decline.

Managing the supply of our products and their components is complex. Insufficient supply and inventory may result in lost sales opportunities or delayed revenue, while excess inventory may harm our gross margins.

Our third-party manufacturers procure components and build our products based on our forecasts, and we generally do not hold inventory for a prolonged period of time. These forecasts are based on estimates of future demand for our products, which are in turn based on historical trends and analyses from our sales and marketing organizations, adjusted for overall market conditions. In order to reduce manufacturing lead times and plan for adequate component supply, from time to time we may issue forecasts for components and products that are non-cancelable and non-returnable.

Our inventory management systems and related supply chain visibility tools may be inadequate to enable us to make accurate forecasts and effectively manage the supply of our products and product components. Supply management remains an area of increasing focus as we balance the need to maintain supply levels that are sufficient to ensure competitive lead times against the risk of obsolescence because of rapidly changing technology and customer requirements. If we ultimately determine that we have excess supply, we may have to reduce our prices and write-down inventory, which in turn could result in lower gross margins. Alternatively, insufficient supply levels may lead to shortages that result in delayed revenue or loss of sales opportunities altogether as potential customers turn to competitors' products that may be readily available. Additionally, any increases in the time required to manufacture or ship our products could result in supply shortfalls. If we are unable to effectively manage our supply and inventory, our results of operations could be adversely affected.

Because some of the key components in our products come from limited sources of supply, we are susceptible to supply shortages or supply changes, which could disrupt or delay our scheduled product deliveries to our customers and may result in the loss of sales and customers.

Our platform relies on key components, including a motherboard and chassis, which our third-party manufacturers purchase on our behalf from a sole source provider. The manufacturing operations of some of our component suppliers are geographically concentrated in Asia, which makes our supply chain vulnerable to regional disruptions. A localized health risk affecting employees at these facilities, such as the spread of a pandemic influenza, could impair the total volume of components that we are able to obtain, which could result in substantial harm to our results of

operations. Similarly, a fire, flood, earthquake, tsunami or other disaster, condition or event such as political instability, terrorist act, civil unrest or a power outage that adversely affects any of these component suppliers' facilities could significantly affect our ability to obtain the components needed for our products, which could result in a substantial loss of sales and revenue and a substantial harm to our results of operations.

We do not have volume purchase contracts with any of our component suppliers, and they could cease selling to us at any time. In addition, our component suppliers change their selling prices frequently in response to market trends, including industry-wide increases in demand, and because we do not have contracts with these suppliers, we are susceptible to price fluctuations related to raw materials

and components. If we are unable to pass component price increases along to our customers or maintain stable pricing, our gross margins and results of operations could be negatively impacted. If we are unable to obtain a sufficient quantity of these components in a timely manner for any reason, sales of our products could be delayed or halted or we could be forced to expedite shipment of such components or our products at dramatically increased costs, which would negatively impact our revenue and gross margins. Additionally, poor quality in any of the sole-sourced components in our products could result in lost sales or lost sales opportunities. If the quality of the components does not meet our or our customers' requirements, if we are unable to obtain components from our existing suppliers on commercially reasonable terms, or if any of our sole source providers cease to remain in business or continue to manufacture such components, we could be forced to redesign our products and qualify new components from alternate suppliers. The resulting stoppage or delay in selling our products and the expense of redesigning our products could result in lost sales opportunities and damage to customer relationships, which would adversely affect our business and results of operations.

If we fail to adequately protect personal information or other information we process or maintain, our business, financial condition and operating results could be adversely affected.

A wide variety of provincial, state, national, and international laws and regulations apply to the collection, use, retention, protection, disclosure, transfer and other processing of personal data. These data protection and privacy-related laws and regulations are evolving and may result in ever-increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. For example, the European Union General Data Protection Regulation, which became fully effective on May 25, 2018, imposes more stringent data protection requirements than previously effective European Union data protection law and provides for penalties for noncompliance of up to the greater of €20 million or four percent of worldwide annual revenues.

Evolving and changing definitions of personal data and personal information within the European Union, the United States, and elsewhere, especially relating to classification of IP addresses, machine identification, location data and other information, may limit or inhibit our ability to operate or expand our business, including limiting technology alliance partners that may involve the sharing of data.

California recently enacted legislation, the California Consumer Privacy Act ("CCPA"), that will, among other things, require covered companies to provide new disclosures to California consumers, and afford such consumers new abilities to opt-out of certain sales of personal information, when it goes into effect on January 1, 2020. The CCPA was amended on September 23, 2018, and it remains unclear whether any further modifications will be made to this legislation or how it will be interpreted. We cannot yet predict the impact of the CCPA on our business or operations, but it may require us to modify our data processing practices and policies and to incur substantial costs and expenses in an effort to comply.

Even the perception of privacy or information security concerns, whether or not valid, may harm our reputation, inhibit adoption of our products by current and future customers, or adversely impact our ability to hire and retain workforce talent. If our security measures are or are believed to be inadequate or breached as a result of third-party action, employee negligence, error or malfeasance, product defects, social engineering techniques or otherwise, and this results in, or is believed to result in, the disruption of the confidentiality, integrity or availability of our systems or networks or any data we process or maintain, or the loss, destruction or corruption of such data, we could incur significant liability, we could face a loss of revenues, and our business may suffer and our reputation and competitive position may be damaged. Additionally, our service providers may suffer, or be perceived to suffer, data security breaches or other incidents that may compromise data stored or processed for us that may give rise to any of the foregoing.

Our actual or perceived failure to adequately comply with applicable laws and regulations, or to protect personal data and other data we process or maintain, could result in regulatory investigations and enforcement actions against us, fines, penalties and other liabilities, imprisonment of company officials and public censure, claims for damages by customers and other affected individuals, required efforts to mitigate or otherwise respond to incidents, litigation, damage to our reputation and loss of goodwill (both in relation to existing customers and prospective customers), any of which could have a material adverse effect on our operations, financial performance and business. Even the perception of privacy, data protection or information security concerns, whether or not valid, may harm our reputation and inhibit adoption of our products and subscriptions by current and future customers.

Our technology alliance partnerships expose us to a range of business risks and uncertainties that could have a material adverse impact on our business and financial results.

We have entered, and intend to continue to enter, into technology alliance partnerships with third parties to support our future growth plans. Such relationships include technology licensing, joint technology development and integration, research cooperation, co-marketing activities and sell-through arrangements. We face a number of risks relating to our technology alliance partnerships that could prevent us from realizing the desired benefits from such partnerships on a timely basis or at all, which, in turn, could have a negative impact on our business and financial results.

Technology alliance partnerships require significant coordination between the parties involved, particularly if a partner requires that we integrate its products with our products. This could involve a significant commitment of time and resources by our technical staff and their counterparts within our technology alliance partner. The integration of products from different companies may be more difficult than we anticipate, and the risk of integration difficulties, incompatible products and undetected programming errors or defects may be higher than the risks normally associated with the introduction of new products. It may also be more difficult to market and sell products

developed through technology alliance partnerships than it would be to market and sell products that we develop on our own. Sales and marketing personnel may require special training, as the new products may be more complex than our other products.

We invest significant time, money and resources to establish and maintain relationships with our technology alliance partners, but we have no assurance that any particular relationship will continue for any specific period of time. Generally, our agreements with these technology alliance partners are terminable without cause with no or minimal notice or penalties. If we lose a significant technology alliance partner, we could lose the benefit of our investment of time, money and resources in the relationship. In addition, we could be required to incur significant expenses to develop a new strategic alliance or to determine and implement an alternative plan to pursue the opportunity that we targeted with the former partner.

If our estimates or judgments relating to our critical accounting policies are based on assumptions that change or prove to be incorrect, our results of operations could fall below our publicly announced guidance or the expectations of securities analysts and investors, resulting in a decline in our stock price.

The preparation of financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as provided in the section entitled "Management's Discussion and Analysis of Financial Condition and Results of Operations," the results of which form the basis for making judgments about the carrying values of assets, liabilities, equity, revenue and expenses that are not readily apparent from other sources. In general, if our estimates, judgments or assumptions related to our critical accounting policies change or if actual circumstances differ from our estimates, judgments or assumptions, our results of operations may be adversely affected and could fall below our publicly announced guidance or the expectations of securities analysts and investors, resulting in a decline in our stock price. Significant assumptions and estimates used in preparing our consolidated financial statements include those related to assets, liabilities, revenue, expenses and related disclosures.

We are exposed to the credit risk of some of our distributors, resellers and customers and to credit exposure in weakened markets, which could result in material losses.

Most of our sales are on an open credit basis. Although we have programs in place that are designed to monitor and mitigate these risks, we cannot assure you these programs will be effective in reducing our credit risks, especially as we expand our business internationally. If we are unable to adequately control these risks, our business, results of operations and financial condition could be harmed.

Our failure to raise additional capital or generate the significant capital necessary to expand our operations and invest in new products could reduce our ability to compete and could harm our business.

We intend to continue to make investments to support our business growth and may require additional funds to respond to business challenges, including the need to develop new products and enhancements to our platform, improve our operating infrastructure or acquire complementary businesses and technologies. Accordingly, we may need to engage in equity or debt financings to secure additional funds. If we raise additional equity financing, our stockholders may experience significant dilution of their ownership interests and the per share value of our common stock could decline. Furthermore, if we engage in additional debt financing, the holders of debt would have priority over the holders of common stock, and we may be required to accept terms that restrict our ability to incur additional indebtedness. We may also be required to take other actions that would otherwise be in the interests of the debt holders and force us to maintain specified liquidity or other ratios, any of which could harm our business, results of operations, and financial condition. If we need additional capital and cannot raise it on acceptable terms, we may not be able to, among other things:

- develop or enhance our products and subscriptions;
- continue to expand our sales and marketing and research and development organizations;
- acquire complementary technologies, products or businesses;
- expand operations, in the United States or internationally;
- hire, train and retain employees; or
- respond to competitive pressures or unanticipated working capital requirements.

Our failure to do any of these things could harm our business, financial condition and results of operations.

If our products do not effectively interoperate with our customers' IT infrastructure, installations could be delayed or cancelled, which would harm our business.

Our products must effectively interoperate with our customers' existing or future IT infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products from multiple vendors, and contains multiple generations of products that have been added over time. As a result, when problems occur in a network, it may be difficult to identify the sources of these problems. If we find errors in the existing software or defects in the hardware used in our customers' infrastructure or problematic network configurations or settings, we may have to modify our software or hardware so that our products will interoperate with our customers'

infrastructure. In such cases, our products may be unable to provide significant performance improvements for applications deployed in our customers' infrastructure. These issues could cause longer installation times for our products and could cause order cancellations, either of which would adversely affect our business, results of operations and financial condition. In addition, government and other customers may require our products to comply with certain security or other certifications and standards. If our products are late in achieving or fail to achieve compliance with these certifications and standards, or our competitors achieve compliance with these certifications and standards, we may be disqualified from selling our products to such customers, or may otherwise be at a competitive disadvantage, either of which would harm our business, results of operations, and financial condition.

Reliance on shipments at the end of each quarter could cause our revenue for the applicable period to fall below expected levels.

As a result of customer buying patterns and the efforts of our sales force and channel partners to meet or exceed their sales objectives, we have historically received a substantial portion of sales orders and generated a substantial portion of revenue during the last few weeks and days of each quarter. A significant interruption in our IT systems, which manage critical functions such as order processing, revenue recognition, financial forecasts, inventory and supply chain management, and trade compliance reviews, or our supply chain could result in delayed order fulfillment and decreased revenue for that quarter. If expected revenue at the end of any quarter is delayed for any reason, including the failure of anticipated purchase orders to materialize, our logistics or channel partners' inability to ship products prior to quarter-end to fulfill purchase orders received near the end of the quarter, our failure to manage inventory to meet demand, our inability to release new products on schedule, any failure of our systems related to order review, processing and licensing, or any delays in shipments based on trade compliance requirements (including new compliance requirements imposed by new or renegotiated trade agreements), our revenue for that quarter could fall below our expectations and the estimates of market analysts, which could adversely impact our business and results of operations and cause a decline in the trading price of our common stock.

We generate a significant amount of revenue from sales through resellers, distributors and end customers outside of the United States, and we are therefore subject to a number of risks associated with international sales and operations.

We have a limited history of marketing, selling, and supporting our platform internationally. As a result, we must hire and train experienced personnel to staff and manage our foreign operations. To the extent that we experience difficulties in recruiting, training, managing, and retaining international employees, particularly managers and other members of our international sales team, we may experience difficulties in sales productivity in, or market penetration of, foreign markets. We also enter into strategic distributor and reseller relationships with companies in certain international markets where we do not have a local presence. If we are not able to maintain successful strategic distributor relationships with our international channel partners or recruit additional channel partners, our future success in these international markets could be limited. Business practices in the international markets that we serve may differ from those in the United States and may require us to include non-standard terms in customer contracts, such as extended payment or warranty terms. To the extent that we enter into customer contracts in the future that include non-standard terms related to payment, warranties, or performance obligations, our results of operations may be adversely impacted.

Additionally, our international sales and operations are subject to a number of risks, including the following:

- greater difficulty in enforcing contracts and managing collections, as well as longer collection periods;
- higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for our international operations;
- fluctuations in exchange rates between the U.S. dollar and foreign currencies in markets where we do business, such as the British Pound Sterling, which experienced a sharp decline in value compared to the U.S. dollar and other currencies;
- management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of our platform that may be required in foreign countries and any changes in trade relations and restrictions as a result of the 2016 U.S. presidential election;

- greater risk of unexpected changes in foreign and domestic regulatory practices, tariffs and tax laws and treaties, including regulatory and trade policy changes adopted by the current administration;
- compliance with anti-bribery laws, including, without limitation, compliance with the U.S. Foreign Corrupt Practices Act of 1977, as amended, the U.S. Travel Act and the UK Bribery Act 2010, violations of which could lead to significant fines, penalties and collateral consequences for our Company;
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;
- the uncertainty of protection for intellectual property rights in some countries;
- foreign exchange controls or tax regulations that might prevent us from repatriating cash earned outside the United States;

- general economic, political and social conditions in these foreign markets, including the perception of doing business with U.S. based companies and changes in regulatory requirements that impact our operating strategies, access to global markets or hiring;
- political and economic instability in some countries, such as those caused by the 2016 U.S. presidential election and the referendum on June 23, 2016, in which voters in the U.K. approved an exit from the EU ("Brexit"), and, in March 2017, began the process to leave the EU by April 2019; and
- double taxation of our international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which we operate.

Further, the interpretation and application of international laws and regulations in many cases is uncertain, and our legal and regulatory obligations in foreign jurisdictions are subject to frequent and unexpected changes, including the potential for various regulatory or other governmental bodies to enact new or additional laws or regulations or to issue rulings that invalidate prior laws or regulations.

For example, "Brexit" could also lead to further legislative and regulatory changes. A Data Protection Act that substantially implements the European Union's General Data Protection Regulation has been implemented in the United Kingdom, effective in May 2018. It is unclear, however, how United Kingdom data protection laws or regulations will develop in the medium to longer term, and how data transfers to and from the United Kingdom will be regulated. In particular, the United Kingdom's anticipated exit from the EU in March 2019 to effectuate Brexit could require us to make additional changes to the way we conduct our business and transmit data from the EU into the United Kingdom.

Additionally, with regard to transfers of personal data from our European customers and employees to the U.S., we have self-certified under the EU-U.S. Privacy Shield Framework and a related program, the Swiss-U.S. Privacy Shield Framework, in addition to in certain cases using model contracts approved by the European Commission. With regard to transfers of personal data from one FireEye entity to another, we have put into place inter-company standard contractual clauses. The U.S.-EU Privacy Shield and such model contracts have been challenged and may be suspended, invalidated or modified. It is uncertain that the U.S.-EU Privacy Shield or such model contracts will continue to remain intact and serve as an appropriate means for us to meet European requirements for personal data transfers from the EEA or Switzerland to the United States. Developments in the legal landscape affecting the transfer of personal data from the EEA may cause us to find it necessary or desirable to modify our data handling practices, and may serve as a basis for our personal data handling practices, or those of our customers and vendors, to be challenged and may otherwise adversely impact our business, financial condition and operating results.

These and other factors could harm our ability to generate future international revenue and, consequently, materially impact our business, results of operations and financial condition.

We are exposed to fluctuations in currency exchange rates, which could negatively affect our financial condition and results of operations.

Our sales contracts are denominated in U.S. dollars, and therefore our revenue is not subject to foreign currency risk. However, strengthening of the U.S. dollar increases the real cost of our products, subscriptions and services to our customers outside of the United States, which could lead to delays in the purchase of our products and services and the lengthening of our sales cycle. In addition, we are incurring an increasing portion of our operating expenses outside the United States. These expenses are denominated in foreign currencies and are subject to fluctuations due to changes in foreign currency exchange rates.

Additionally, Brexit resulted in an adverse impact to currency exchange rates, notably the British Pound Sterling which experienced a sharp decline in value compared to the U.S. dollar and other currencies. A significantly weaker British Pound Sterling compared to the U.S. dollar could have a significantly negative effect on our financial condition and results of operations.

We do not currently hedge against the risks associated with currency fluctuations but may do so in the future.

Failure to comply with governmental laws and regulations could harm our business.

Our business is subject to regulation by various U.S. federal, state, local and foreign governmental agencies, including agencies responsible for monitoring and enforcing employment and labor laws, workplace safety, product safety, environmental laws, consumer protection laws, anti-bribery laws (including the U.S. Foreign Corrupt Practices Act and the U.K. Anti-Bribery Act), import/export controls, federal securities laws and tax laws and regulations. In certain

jurisdictions, these regulatory requirements may be more stringent than those in the United States. Noncompliance with applicable regulations or requirements could subject us to investigations, sanctions, mandatory product recalls, enforcement actions, disgorgement of profits, fines, damages, civil and criminal penalties, injunctions or other collateral consequences. If any governmental sanctions are imposed, or if we do not prevail in any possible civil or criminal litigation, our business, results of operations, and financial condition could be materially adversely affected. In addition, responding to any action will likely result in a significant diversion of management's attention and resources and an increase in professional fees. U.S. regulations surrounding our operating activities in foreign jurisdictions are not always consistent with, and at times are in contravention to, the local regulations or laws in such jurisdictions. Enforcement actions and sanctions could harm our business, reputation, results of operations and financial condition.

We are subject to governmental export and import controls that could subject us to liability or impair our ability to compete in international markets.

Our products are subject to U.S. export controls, specifically the Export Administration Regulations and economic sanctions enforced by the Office of Foreign Assets Control. We incorporate standard encryption algorithms into our products, which, along with the underlying technology, may be exported outside of the U.S. only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of an encryption registration and classification request. Furthermore, U.S. export control laws and economic sanctions prohibit the shipment of certain products and services to countries, governments, and persons targeted by U.S. sanctions. While we have taken precautions to prevent our products and services from being exported in violation of these laws, in certain instances in the past we shipped our encryption products prior to obtaining the required export authorizations and/or submitting the required requests, including a classification request and request for an encryption registration number, resulting in an inadvertent violation of U.S. export control laws. As a result, in February 2013, we filed a Voluntary Self Disclosure with the U.S. Department of Commerce's Bureau of Industry and Security, or BIS, concerning these potential violations. In June 2013, BIS notified us that it had completed its review of this matter and closed its review with the issuance of a warning letter. No monetary penalties were assessed. Even though we take precautions to ensure that our channel partners comply with all relevant regulations, any failure by our channel partners to comply with such regulations could have negative consequences, including reputational harm, government investigations and penalties.

In addition, various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our products or could limit our customers' ability to implement our products in those countries. Changes in our products or changes in export and import regulations may create delays in the introduction of our products into international markets, prevent our customers with international operations from deploying our products globally or, in some cases, prevent the export or import of our products to certain countries, governments or persons altogether. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such regulations, could result in decreased use of our products by, or in our decreased ability to export or sell our products to, existing or potential customers with international operations. Any decreased use of our products or limitation on our ability to export to or sell our products in international markets would likely adversely affect our business, financial condition and results of operations.

Our business is subject to the risks of earthquakes, fire, power outages, floods and other catastrophic events, and to interruption by man-made problems such as terrorism or armed conflicts.

Natural disasters or other catastrophic events, including earthquakes, fires, floods, significant power outages, telecommunications failures and cyber attacks, may cause damage or disruption to our operations, international commerce and the global economy, and thus could have a material adverse impact on our business, results of operations, and financial condition. Our corporate headquarters and servers hosting our cloud services are located in California, a region known for seismic activity. Customer data could be lost, significant recovery time could be required to resume operations and our financial condition and operating results could be adversely affected in the event of a natural disaster or other catastrophic event. In addition, natural disasters and other catastrophic events could affect our supply chain, manufacturing vendors, or logistics providers' ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. In the event that our or our service providers' information technology systems or manufacturing or logistics abilities are hindered by any of the events discussed above, shipments could be delayed, resulting in missed financial targets, such as revenue and shipment targets, for a particular quarter. In addition, acts of terrorism, armed conflicts and other geo-political unrest could cause disruptions in our business or the business of our supply chain, manufacturers, logistics providers, partners, or customers or the economy as a whole. Any disruption in the business of our supply chain, manufacturers, logistics providers, partners or end-customers that impacts sales at the end of a fiscal quarter could have a significant adverse impact on our financial results. All of the aforementioned risks may be further increased if the disaster recovery plans for us and our suppliers prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, the loss of customers or the delay in the manufacture, deployment or

shipment of our products, our business, financial condition and results of operations would be adversely affected.

If we fail to comply with environmental requirements, our business, financial condition, results of operations and reputation could be adversely affected.

We are subject to various environmental laws and regulations including laws governing the hazardous material content of our products and laws relating to the collection and recycling of electrical and electronic equipment. Examples of these laws and regulations include the EU Restrictions on the Use of certain Hazardous Substances in Electronic Equipment Directive and the EU Waste Electrical and Electronic Equipment Directive as well as the implementing legislation of the EU member states. Similar laws and regulations have been passed or are pending in China, South Korea and Japan and may be enacted in other regions, including in the United States, and we are, or may in the future be, subject to these laws and regulations.

Our failure to comply with past, present, and future laws could result in reduced sales of our products, substantial product inventory write-offs, reputational damage, penalties, and other sanctions, any of which could harm our business and financial condition. We also expect that our products will be affected by new environmental laws and regulations on an ongoing basis. To date, our expenditures for environmental compliance have not had a material impact on our results of operations or cash flows, and although we cannot predict the

future impact of such laws or regulations, they will likely result in additional costs and may increase penalties associated with violations or require us to change the content of our products or how they are manufactured, which could have a material adverse effect on our business, results of operations and financial condition.

Uncertainties in the interpretation and application of the 2017 Tax Cuts and Jobs Act could materially affect our tax obligations, effective tax rate and operating results.

On December 22, 2017, the U.S. government enacted comprehensive tax legislation commonly referred to as the Tax Cuts and Jobs Act of 2017 (the "Tax Act"). The Tax Act makes broad and complex changes to the U.S. tax code. The changes include, but are not limited to, reducing the U.S. federal corporate tax rate from 35% to 21%, imposing a mandatory one-time transition tax on certain unrepatriated earnings of foreign subsidiaries, imposing certain additional limitations on the use of deferred tax assets, introducing bonus depreciation that will allow for full expensing of qualified property, eliminating the corporate alternative minimum tax ("AMT"), and changing how existing AMT credits can be realized. The U.S. Department of Treasury has broad authority to issue regulations and interpretative guidance that may significantly impact our tax obligations, effective tax rate and our results of operations. The Tax Act will likely be subject to ongoing technical guidance and accounting interpretation, which we will continue to monitor and assess. Although we cannot predict the nature or outcome of such future technical guidance and accounting interpretation, they could adversely impact our tax obligations, effective tax rate and results of operations. In addition, it is uncertain if, and to what extent, various states will conform to the new tax law and foreign countries will react by adopting tax legislation or taking other actions that could adversely affect our business.

If we do not achieve increased tax benefits as a result of our corporate structure, our operating results and financial condition may be negatively impacted.

We generally conduct our international operations through wholly-owned subsidiaries and report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. In 2013, we completed the reorganization of our corporate structure and intercompany relationships to more closely align our corporate organization with the expansion of our international business activities. Although we anticipate achieving a reduction in our overall effective tax rate in the future as a result of this reorganized corporate structure, we may not realize any benefits. Our intercompany relationships are subject to complex transfer pricing regulations administered by taxing authorities in various jurisdictions. The relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur, and our position were not sustained, we could be required to pay additional taxes, interest and penalties, which could result in one-time tax charges, higher effective tax rates, reduced cash flows and lower overall profitability of our operations. In addition, if the intended tax treatment of our reorganized corporate structure is not accepted by the applicable taxing authorities, changes in tax law negatively impact the structure or we do not operate our business consistent with the structure and applicable tax laws and regulations, we may fail to achieve any tax advantages as a result of the reorganized corporate structure, and our future operating results and financial condition may be negatively impacted. In addition, we continue to evaluate our corporate structure in light of current and pending tax legislation, and any changes to our corporate structure may require us to incur additional expenses and may impact our overall effective tax rate.

We could be subject to additional tax liabilities.

We are subject to U.S. federal, state, local and sales taxes in the United States and foreign income taxes, withholding taxes and transaction taxes in numerous foreign jurisdictions. Significant judgment is required in evaluating our tax positions and our worldwide provision for taxes. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination is uncertain. In addition, our tax obligations and effective tax rates could be adversely affected by changes in the relevant tax, accounting and other laws, regulations, principles and interpretations, including those relating to income tax nexus, by recognizing tax losses or lower than anticipated earnings in jurisdictions where we have lower statutory rates and higher than anticipated earnings in jurisdictions where we have higher statutory rates, by changes in foreign currency exchange rates, or by changes in the valuation of our deferred tax assets and liabilities. We may be audited in various jurisdictions, and such jurisdictions may assess additional taxes, sales taxes and value-added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have a material adverse effect on our operating results or cash flows in the period for which a determination is made.

Our ability to use our net operating losses to offset future taxable income may be subject to certain limitations. In general, under Section 382 of the Internal Revenue Code of 1986, as amended (the "Code"), a corporation that undergoes an “ownership change” is subject to limitations on its ability to utilize its pre-change net operating losses, or NOLs, to offset future taxable income. Our existing NOLs may be subject to limitations arising from previous ownership changes. Future changes in our stock ownership, some of which are outside of our control, could result in an ownership change under Section 382 of the Code and adversely affect our ability to utilize our NOLs in the future. Furthermore, our ability to utilize NOLs of companies that we may acquire in the future may be subject to limitations. There is also a risk that due to regulatory changes, such as suspensions on the use of NOLs, or other unforeseen reasons, our existing NOLs could expire or otherwise be unavailable to offset future income tax liabilities. For these reasons, we may not be able to utilize a material portion of the NOLs reflected on our balance sheet, even if we attain profitability.

Risks Related to Our Convertible Senior Notes

We are leveraged financially, which could adversely affect our ability to adjust our business to respond to competitive pressures and to obtain sufficient funds to satisfy our future growth, business needs and development plans.

We have substantial existing indebtedness. In June 2015, we issued $460.0 million principal amount of 1.000% Convertible Senior Notes due 2035 (the "Series A Notes") and $460.0 million principal amount of 1.625% Convertible Senior Notes due 2035 (the "Series B Notes" and, together with the Series A Notes, the "2035 Notes"). During the three months ended June 30, 2018, we issued $600.0 million aggregate principal amount of 0.875% Convertible Senior Notes due 2024 (the "2024 Notes" and, together with the 2035 Notes, the "convertible notes") and repurchased approximately $340.2 million aggregate principal amount of certain of the 2035 Notes. As a result, as of December 31, 2018, we had approximately $1.2 billion aggregate principal amount of convertible notes outstanding. The degree to which we are leveraged could have negative consequences, including, but not limited to, the following:

- we may be more vulnerable to economic downturns, less able to withstand competitive pressures and less flexible in responding to changing business and economic conditions;
- our ability to obtain additional financing in the future for working capital, capital expenditures, acquisitions, general corporate or other purposes may be limited;
- a substantial portion of our cash flows from operations in the future may be required for the payment of the principal amount of our existing indebtedness when it becomes due; and
- we may elect to make cash payments upon any conversion of the convertible notes, which would reduce our cash on hand.

Our ability to meet our payment obligations under our convertible notes depends on our ability to generate significant cash flow in the future. This, to some extent, is subject to general economic, financial, competitive, legislative, and regulatory factors as well as other factors that are beyond our control. There can be no assurance that our business will generate cash flow from operations, or that additional capital will be available to us, in an amount sufficient to enable us to meet our debt payment obligations and to fund other liquidity needs. If we are unable to generate sufficient cash flow to service our debt obligations, we may need to refinance or restructure our debt, sell assets, reduce or delay capital investments, or seek to raise additional capital. If we were unable to implement one or more of these alternatives, we may be unable to meet our debt payment obligations, which could have a material adverse effect on our business, results of operations, or financial condition.

The conditional conversion feature of each series of convertible notes, if triggered, may adversely affect our financial condition and operating results.

In the event the conditional conversion feature of a series of convertible notes is triggered, holders of such series of convertible notes will be entitled to convert their convertible notes at any time during specified periods at their option. If one or more holders of such convertible notes elect to convert their convertible notes, unless we elect to satisfy our conversion obligation by delivering solely shares of our common stock (other than paying cash in lieu of delivering any fractional share), we would be required to settle a portion or all of our conversion obligation through the payment of cash, which could adversely affect our liquidity. In addition, even if holders of such series of convertible notes do not elect to convert their convertible notes, we could be required under applicable accounting rules to reclassify all or a portion of the outstanding principal of such series of convertible notes as a current rather than long-term liability, which would result in a material reduction of our net working capital.

The accounting method for convertible debt securities that may be settled in cash, such as the convertible notes, is subject to changes that could have a material effect on our reported financial results.

In May 2008, the Financial Accounting Standards Board, which we refer to as FASB, issued FASB Staff Position No. APB 14-1, Accounting for Convertible Debt Instruments That May Be Settled in Cash Upon Conversion (Including Partial Cash Settlement), which has subsequently been codified as Accounting Standards Codification 470-20, Debt with Conversion and Other Options, which we refer to as ASC 470-20. Under ASC 470-20, an entity must separately account for the liability and equity components of the convertible debt instruments (such as the convertible notes) that may be settled entirely or partially in cash upon conversion in a manner that reflects the issuer’s economic interest cost. The effect of ASC 470-20 on the accounting for each series of convertible notes is that the equity component is required to be included in the additional paid-in capital section of stockholders’ equity on our consolidated balance

sheet and the value of the equity component would be treated as original issue discount for purposes of accounting for the debt component of such series of convertible notes. As a result, we will be required to record a greater amount of non-cash interest expense in current periods presented as a result of the amortization of the discounted carrying value of the convertible notes to their face amount over the term of the convertible notes. We will report lower net income in our financial results because ASC 470-20 will require interest to include both the current period's amortization of the debt discount and the instrument's non-convertible coupon interest for such series of convertible notes, which could adversely affect our reported or future financial results and the trading price of our common stock.

In August 2016, the FASB issued ASU 2016-15, Statement of Cash Flows (Topic 230): Classification of Certain Cash Receipts and Cash Payments (a consensus of the Emerging Issues Task Force). This standard clarifies how certain cash receipts and payments should be classified in the statement of cash flows, including the cash settlement for each series of our convertible notes. Upon cash settlement,

repayment of the principal amount will be bifurcated between cash outflows for operating activities for the portion related to accreted interest attributable to debt discounts arising from the difference between the coupon interest rate and the effective interest rate, and financing activities for the remainder. This will require us to classify the $310.4 million of accreted interest as cash used in operating activities in our consolidated financial statements upon cash settlement, which could adversely affect our future cash flow from operations.

In addition, under certain circumstances, convertible debt instruments (such as the convertible notes) that may be settled entirely or partly in cash are currently accounted for utilizing the treasury stock method, the effect of which is that any shares issuable upon conversion of any series of convertible notes are not included in the calculation of diluted earnings per share except to the extent that the conversion value of such series of convertible notes exceeds their principal amount of such series of convertible notes. Under the treasury stock method, for diluted earnings per share purposes, the transaction is accounted for as if the number of shares of common stock that would be necessary to settle such excess conversion value, if we elected to settle such excess in shares, are issued. We cannot be sure that the accounting standards in the future will continue to permit the use of the treasury stock method. If we are unable to use the treasury stock method in accounting for the shares issuable upon conversion of the convertible notes, then our diluted earnings per share would be adversely affected.

Transactions related to our convertible notes may affect the market price of our common stock.

The conversion of any of our series of convertible notes, if such conversion occurs, will dilute the ownership interests of then-existing stockholders to the extent we deliver shares upon conversion of any of the convertible notes. Any sales in the public market of the common stock issuable upon such conversion could adversely affect prevailing market prices of our common stock. In addition, the existence of the convertible notes may encourage short selling by market participants because any conversion of the convertible notes could be used to satisfy short positions, or anticipated conversion of the convertible notes into shares of our common stock could depress the price of our common stock.

In addition, in connection with our issuance of the 2024 Notes, we entered into capped call transactions (the "capped call transactions") with certain financial institutions (the “option counterparties”). The capped call transactions are expected generally to reduce the potential dilution to our common stock upon any conversion of the 2024 Notes and/or offset any cash payments we are required to make in excess of the principal amount of such 2024 Notes converted, as the case may be, with such reduction and/or offset subject to a cap. From time to time, the option counterparties or their respective affiliates may modify their hedge positions by entering into or unwinding various derivative transactions with respect to our common stock and/or purchasing or selling our common stock or other securities of ours in secondary market transactions prior to the maturity of the 2024 Notes. This activity could cause a decrease in the market price of our common stock.

We are subject to counterparty risk with respect to the capped call transactions.

The option counterparties to our capped call transactions are financial institutions, and we will be subject to the risk that one or more of the counterparties may default or otherwise fail to perform, or may exercise certain rights to terminate, their obligations under the capped call transactions. Our exposure to the credit risk of the option counterparties will not be secured by any collateral. Adverse global economic conditions may result in the actual or perceived failure or financial difficulties for financial institutions, including one or more of our option counterparties. If an option counterparty becomes subject to insolvency proceedings, we will become an unsecured creditor in those proceedings with a claim equal to our exposure at that time under our transactions with that option counterparty. Our exposure will depend on many factors but, generally, our exposure will increase if the market price or the volatility of our common stock increases. In addition, upon a default or other failure to perform, or a termination of obligations, by an option counterparty, we may suffer adverse tax consequences and more dilution than we currently anticipate with respect to our common stock. We can provide no assurances as to the financial stability or viability of the option counterparties.

Risks Related to Ownership of Our Common Stock

If securities or industry analysts do not publish research or reports about our business, or publish inaccurate or unfavorable research reports about our business, our share price and trading volume could decline.

The trading market for our common stock, to some extent, depends on the research and reports that securities or industry analysts publish about us or our business. We do not have any control over these analysts. If one or more of

the analysts who cover us should downgrade our shares or change their opinion of our shares, industry sector or products, our share price would likely decline. If one or more of these analysts ceases coverage of our Company or fails to regularly publish reports on us, we could lose visibility in the financial markets, which could cause our share price or trading volume to decline.

We may fail to meet our publicly announced guidance or other expectations about our business and future operating results, which would cause our stock price to decline.

We have provided and may continue to provide guidance about our business and future operating results. In developing this guidance, our management must make certain assumptions and judgments about our future performance. Furthermore, analysts and investors may develop and publish their own projections of our business, which may form a consensus about our future performance. Our business results may vary significantly from such guidance or that consensus due to a number of factors, many of which are outside of our control, and which could adversely affect our operations and operating results. Such factors may include the possibility that interpretation, industry

practice, and accounting guidance may continue to evolve during the early stages of adoption of Accounting Standard Update 2014-09, Revenue from Contracts with Customers (Topic 606) ("ASC 606"). Furthermore, if we make downward revisions of our previously announced guidance, or if our publicly announced guidance of future operating results fails to meet expectations of securities analysts, investors or other interested parties, the price of our common stock would decline.

The price of our common stock has been and may continue to be volatile, and the value of your investment could decline.

The trading price of our common stock has been volatile since our initial public offering, and is likely to continue to be volatile. The price of our common stock during the last twelve months has ranged from $14.20 to $20.61 as measured through February 20, 2019, and the last reported sale price on February 20, 2019 was $16.67. The trading price of our common stock may fluctuate widely in response to various factors, some of which are beyond our control. These factors include:

- whether our results of operations, and in particular, our revenue growth rates, meet the expectations of securities analysts or investors;
- actual or anticipated changes in the expectations of investors or securities analysts, whether as a result of our forward-looking statements, our failure to meet such expectation or otherwise;
- announcements of new products, services or technologies, commercial relationships, acquisitions or other events by us or our competitors;
- changes in how customers perceive the effectiveness of our platform in protecting against advanced cyber attacks or other reputational harm;
- publicity concerning cyber attacks in general or high profile cyber attacks against specific organizations;
- price and volume fluctuations in the overall stock market from time to time;
- significant volatility in the market price and trading volume of technology and/or growth companies in general and of companies in the IT security industry in particular;
- fluctuations in the trading volume of our shares or the size of our public float;
- actual or anticipated changes or fluctuations in our results of operations;
- litigation involving us, our industry, or both;
- regulatory developments in the United States, foreign countries or both;
- general economic conditions and trends;
- natural disasters or other catastrophic events;
- sales of large blocks of our common stock or substantial future sales by our directors, executive officers, employees and significant stockholders; and
- departures of key personnel.

In addition, if the market for technology stocks or the stock market in general experiences a loss of investor confidence, the trading price of our common stock could decline for reasons unrelated to our business, results of operations or financial condition. The trading price of our common stock might also decline in reaction to events that affect other companies in our industry even if these events do not directly affect us. In the past, following periods of volatility in the market price of a company’s securities, securities class action litigation has often been brought against that company. The price of our common stock has been highly volatile since our IPO in September 2013, and beginning in June 2014, several lawsuits alleging violations of securities laws were filed against us and certain of our current and former directors and executive officers. Any securities litigation could result in substantial costs and divert our management’s attention and resources from our business. This could have a material adverse effect on our business, results of operations and financial condition.

Sales of substantial amounts of our common stock in the public markets, or sales of our common stock by our executive officers and directors under Rule 10b5-1 plans, could adversely affect the market price of our common stock.

Sales of a substantial number of shares of our common stock in the public market, or the perception that such sales could occur, could adversely affect the market price of our common stock and may make it more difficult for you to sell your common stock at a time and price that you deem appropriate. In addition, certain of our executive officers and directors have adopted, and other executive officers and directors may in the future adopt, written plans, known as

“Rule 10b5-1 Plans,” under which they have contracted, or may in the future contract, with a broker to sell shares of our common stock on a periodic basis to diversify their assets and investments. Sales made by our executive officers and directors pursuant to Rule 10b5-1, regardless of the amount of such sales, could adversely affect the market price of our common stock.

The issuance of additional stock in connection with financings, acquisitions, investments, our stock incentive plans, conversion of our convertible notes or otherwise will dilute all other stockholders.

Our amended and restated certificate of incorporation authorizes us to issue up to 1,000,000,000 shares of common stock and up to 100,000,000 shares of preferred stock with such rights and preferences as may be determined by our board of directors. Subject to compliance with applicable rules and regulations, we may issue shares of common stock or securities convertible into our common stock from time to time in connection with a financing, acquisition, investment, our stock incentive plans, the conversion of our convertible notes or otherwise. For example, in January 2016, we issued 1,793,305 shares of common stock in connection with our acquisition of iSIGHT; in February 2016, we issued 742,026 shares of common stock in connection with our acquisition of Invotas; in October 2017, we issued 259,425 shares of common stock in connection with our acquisition of The Email Laundry; and in January 2018, we issued 1,016,334 shares of common stock in connection with our acquisition of X15. In addition, we issued $920.0 million aggregate principal amount of 2035 Notes, of which approximately $579.8 million aggregate principal remains outstanding, and we issued $600.0 million aggregate principal amount of the 2024 Notes during the three months ended June 30, 2018. Any future issuances could result in substantial dilution to our existing stockholders and cause the trading price of our common stock to decline.

We do not intend to pay dividends for the foreseeable future.

We have never declared or paid any dividends on our common stock. We intend to retain any earnings to finance the operation and expansion of our business, and we do not anticipate paying any cash dividends in the future. As a result, you may only receive a return on your investment in our common stock if the market price of our common stock increases.

The requirements of being a public company may strain our resources, divert management’s attention and affect our ability to attract and retain qualified board members.

As a public company, we are subject to the reporting requirements of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), the listing requirements of the NASDAQ Stock Market and other applicable securities rules and regulations. Compliance with these rules and regulations has increased and will continue to increase our legal and financial compliance costs, has made and will continue to make some activities more difficult, time-consuming or costly, and has increased and will continue to increase demand on our systems and resources. Among other things, the Exchange Act requires that we file annual, quarterly and current reports with respect to our business and results of operations and maintain effective disclosure controls and procedures and internal control over financial reporting. In order to maintain and, if required, improve our disclosure controls and procedures and internal control over financial reporting to meet this standard, significant resources and management oversight may be required. As a result, management’s attention may be diverted from other business concerns, which could harm our business and results of operations. Although we have already hired additional employees to comply with these requirements, we may need to hire even more employees in the future, which will increase our costs and expenses. We are subject to the independent auditor attestation requirements of Section 404 of the Sarbanes-Oxley Act ("Section 404"), enhanced disclosure obligations regarding executive compensation in our periodic reports and proxy statements, and the requirements of holding a nonbinding advisory vote on executive compensation and stockholder approval of any golden parachute payments not previously approved. While we were able to determine in our management's report for fiscal 2018 that our internal control over financial reporting is effective, as well as provide an unqualified attestation report from our independent registered public accounting firm to that effect, we have and will continue to consume management resources and incur significant expenses for Section 404 compliance on an ongoing basis. In the event that our Chief Executive Officer, Chief Financial Officer, or independent registered public accounting firm determines in the future that our internal control over financial reporting is not effective as defined under Section 404, we could be subject to one or more investigations or enforcement actions by state or federal regulatory agencies, stockholder lawsuits or other adverse actions requiring us to incur defense costs, pay fines, settlements or judgments and causing investor perceptions to be adversely affected and potentially resulting in a decline in the market price of our stock.

In addition, changing laws, regulations and standards relating to corporate governance and public disclosure are creating uncertainty for public companies, increasing legal and financial compliance costs, and making some activities more time consuming. These laws, regulations and standards are subject to varying interpretations, in many cases due

to their lack of specificity, and as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. We intend to invest resources to comply with evolving laws, regulations, and standards, and this investment will increase our general and administrative expense and a diversion of management's time and attention from revenue-generating activities to compliance activities. If our efforts to comply with new laws, regulations, and standards are unsuccessful, regulatory authorities may initiate legal proceedings against us and our business may be harmed.

We also expect that these new rules and regulations will make it more expensive for us to obtain and maintain director and officer liability insurance, and in the future, we may be required to accept reduced coverage or incur substantially higher costs to obtain coverage. These factors could also make it more difficult for us to attract and retain qualified executive officers and members of our board of directors, particularly to serve on our audit committee and compensation committee.

In addition, as a result of our disclosure obligations as a public company, we have reduced strategic flexibility and are under pressure to focus on short-term results, which may adversely impact our ability to achieve long-term profitability.

We are obligated to maintain proper and effective internal control over financial reporting. We may not complete our analysis of our internal control over financial reporting in a timely manner, or this internal control may not be determined to be effective, which may adversely affect investor confidence in our Company and, as a result, the value of our common stock.

We are required, pursuant to the Exchange Act, to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting. This assessment will need to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting, as well as a statement that our auditors have issued an attestation report on our internal controls.

While we were able to determine in our management's report for fiscal 2018 that our internal control over financial reporting is effective, as well as provide an unqualified attestation report from our independent registered public accounting firm to that effect, we may not be able to complete our evaluation, testing, and any required remediation in a timely fashion or our independent registered public accounting firm may not be able to formally attest to the effectiveness of our internal control over financial reporting in the future. During the evaluation and testing process, if we identify one or more material weaknesses in our internal control over financial reporting that we are unable to remediate before the end of the same fiscal year in which the material weakness is identified, we will be unable to assert that our internal controls are effective. If we are unable to assert that our internal control over financial reporting is effective, or if our independent registered public accounting firm is unable to attest to the effectiveness of our internal controls or determine we have a material weakness in our internal controls, we could lose investor confidence in the accuracy and completeness of our financial reports, which would cause the price of our common stock to decline.

Our charter documents and Delaware law, as well as certain provisions of our convertible notes, could discourage takeover attempts and lead to management entrenchment, which could also reduce the market price of our common stock.

Our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that could delay or prevent a change in control of our Company. These provisions could also make it difficult for stockholders to elect directors who are not nominated by the current members of our board of directors or take other corporate actions, including effecting changes in our management. These provisions include:

- a classified board of directors with three-year staggered terms, which could delay the ability of stockholders to change the membership of a majority of our board of directors;
- the ability of our board of directors to issue shares of preferred stock and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquiror;
- the exclusive right of our board of directors to elect a director to fill a vacancy created by the expansion of our board of directors or the resignation, death or removal of a director, which prevents stockholders from being able to fill vacancies on our board of directors;
- a prohibition on stockholder action by written consent, which forces stockholder action to be taken at an annual or special meeting of our stockholders;
- the requirement that a special meeting of stockholders may be called only by our board of directors, the chairperson of our board of directors, our Chief Executive Officer or our President (in the absence of a Chief Executive Officer), which could delay the ability of our stockholders to force consideration of a proposal or to take action, including the removal of directors;
- the requirement for the affirmative vote of holders of at least $66\,^{2}/_{3}\%$ of the voting power of all of the then outstanding shares of the voting stock, voting together as a single class, to amend the provisions of our amended and restated certificate of incorporation relating to the management of our business (including our classified board structure) or certain provisions of our amended and restated bylaws, which may inhibit the ability of an acquiror to effect such amendments to facilitate an unsolicited takeover attempt;
-

the ability of our board of directors to amend the bylaws, which may allow our board of directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquiror to amend the bylaws to facilitate an unsolicited takeover attempt; and

- advance notice procedures with which stockholders must comply to nominate candidates to our board of directors or to propose matters to be acted upon at a stockholders' meeting, which may discourage or deter a potential acquiror from conducting a solicitation of proxies to elect the acquiror's own slate of directors or otherwise attempting to obtain control of us.

In addition, as a Delaware corporation, we are subject to Section 203 of the Delaware General Corporation Law, which may prohibit large stockholders, in particular those owning 15% or more of our outstanding voting stock, from merging or combining with us for a specified period of time. Additionally, certain provisions of our convertible notes could make it more difficult or more expensive for a third party to acquire us. The application of Section 203 or certain provisions of our convertible notes also could have the effect of

discouraging, delaying or preventing a transaction involving a change in control of us. Any of these provisions could, under certain circumstances, depress the market price of our common stock.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

Our corporate headquarters is located in Milpitas, California where we currently lease approximately 190,000 square feet of space under lease agreements that expire during the year ended December 31, 2027. We maintain additional offices throughout the United States and various international locations, including, but not limited to, Australia, Dubai, Germany, India, Ireland, Japan, Singapore and the United Kingdom. We believe that our current facilities are adequate to meet our ongoing needs, and that, if we require additional space, we will be able to obtain additional facilities on commercially reasonable terms.

Item 3. Legal Proceedings

The information set forth under "Litigation" in Note 10 contained in the "Notes to Consolidated Financial Statements" in Part II, Item 8 of this Annual Report on Form 10-K is incorporated herein by reference.

Item 4. Mine Safety Disclosures

Not applicable.

PART II

Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

Market Information

Our common stock, $0.0001 par value per share, began trading on The NASDAQ Global Select Market on September 20, 2013, where its prices are quoted under the symbol “FEYE.”

Holders of Record

As of December 31, 2018, there were 97 holders of record of our common stock. Because many of our shares are held by brokers and other institutions on behalf of stockholders, we are unable to estimate the total number of stockholders represented by these record holders.

Stock Performance Graph

The following performance graph shall not be deemed “filed” for purposes of Section 18 of the Exchange Act or otherwise subject to the liabilities under that Section, and shall not be deemed to be incorporated by reference into any of our filings under the Securities Act of 1933, as amended ("the Exchange Act"), except as shall be expressly set forth by specific reference in such filing.

The following graph compares the cumulative total return of our common stock with the total return for the Standard & Poor's 500 Index and the Standard & Poor's Information Technology Index from December 31, 2013 through December 31, 2018. The graph assumes that $100 was invested on December 31, 2013 in our common stock, the Standard & Poor's 500 Index and the Standard & Poor's Information Technology Index, and assumes reinvestment of any dividends. The stock price performance on the following graph is not necessarily indicative of future stock price performance.

	12/13	12/14	12/15	12/16	12/17	12/18
FireEye, Inc.	$100.00	$72.41	$47.56	$27.29	$32.56	$37.17
S&P 500	$100.00	$113.69	$115.26	$129.05	$157.22	$150.33
S&P Information Technology	$100.00	$120.12	$127.23	$144.85	$201.10	$200.52

Dividend Policy

We have never declared or paid, and do not anticipate declaring or paying in the foreseeable future, any cash dividends on our capital stock. Any future determination as to the declaration and payment of dividends, if any, will be at the discretion of our board of directors, subject to applicable laws, and will depend on then existing conditions, including our financial condition, operating results, contractual restrictions, capital requirements, business prospects, and other factors our board of directors may deem relevant.

Recent Sales of Unregistered Securities

There were no sales of unregistered securities during the period covered by this Annual Report on Form 10-K, other than those previously reported in a Quarterly Report on Form 10-Q or in a Current Report on Form 8-K.

Issuer Purchases of Equity Securities

No shares of our common stock were repurchased during the three months ended December 31, 2018.

Securities Authorized for Issuance Under Equity Compensation Plans

See Part III, Item 12 of this Annual Report on Form 10-K regarding information about securities authorized for issuance under our equity compensation plans.

Item 6. Selected Consolidated Financial Data

The following selected historical financial data should be read in conjunction with Part II, Item 7, “Management’s Discussion and Analysis of Financial Condition and Results of Operations,” and our financial statements and the related notes appearing in Part II, Item 8, “Financial Statements and Supplementary Data,” of this Annual Report on Form 10-K to fully understand the factors that may affect the comparability of the information presented below.

The statements of operations data for the years ended December 31, 2018, 2017 and 2016 and the balance sheet data as of December 31, 2018 and 2017 are derived from our audited financial statements appearing in Part II, Item 8, “Financial Statements and Supplementary Data,” of this Annual Report on Form 10-K. The statements of operations for the years ended December 31, 2015 and 2014 and the balance sheet data as of December 31, 2016, 2015 and 2014 are derived from audited financial statements not included in this Annual Report on Form 10-K. Our historical results are not necessarily indicative of the results to be expected in the future.

For the years ended December 31, 2017 and 2016, we have adjusted certain of the following financial data as a result of adoption of ASC 606 in the first quarter of the year ended December 31, 2018. Financial data for the years ended December 31, 2015 and 2014 has not been adjusted to reflect the adoption of ASC 606. See Note 1 contained in the "Notes to Consolidated Financial Statements" included in Part II, Item 8 of this Annual Report on Form 10-K for further information regarding our impact of adoption of ASC 606.

	Year Ended December 31,				
	2018	2017*	2016*	2015	2014
	(In thousands, except per share data)				
Consolidated Statements of Operations Data:					
Revenue:	$830,950	$779,648	$705,995	$622,967	$425,662
Cost of revenue:[1]	272,475	271,647	271,083	233,204	175,093
Total gross profit	558,475	508,001	434,912	389,763	250,569
Operating expenses:[1]					
Research and development	254,142	243,273	279,594	279,467	203,187
Sales and marketing	380,962	379,278	437,519	476,166	401,151
General and administrative	105,773	125,549	139,791	141,790	121,099
Restructuring charges	—	—	27,630	—	4,327
Total operating expenses	740,877	748,100	884,534	897,423	729,764
Operating loss	(182,402)	(240,099)	(449,622)	(507,660)	(479,195)
Interest income	16,033	9,323	6,582	2,935	713
Interest expense	(56,426)	(49,766)	(47,869)	(27,116)	(26)
Other expense, net	(14,804)	(10)	(3,247)	(3,284)	(1,936)
Loss before income taxes	(237,599)	(280,552)	(494,156)	(535,125)	(480,444)
Provision for (benefit from) income taxes	5,524	4,632	(8,721)	4,090	(36,654)
Net loss attributable to common stockholders	$(243,123)	$(285,184)	$(485,435)	$(539,215)	$(443,790)
Net loss per share attributable to common stockholders, basic and diluted	$(1.27)	$(1.60)	$(2.97)	$(3.50)	$(3.12)
Weighted-average shares used to compute net loss per share attributable to common stockholders	190,803	177,757	163,211	154,120	142,176

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

(1) Includes stock-based compensation expense as follows:

	2018	2017	2016	2015	2014
	(In thousands)				
Stock-Based Compensation Expense:					
Cost of revenue	$28,362	$32,656	$31,903	$31,023	$17,925
Research and development	49,503	56,720	64,755	68,329	28,968
Sales and marketing	47,592	46,766	57,750	73,286	66,773
General and administrative	28,218	30,194	43,343	49,793	38,186
Restructuring	—	—	1,144	—	—
Total stock-based compensation expense	$153,675	$166,336	$198,895	$222,431	$151,852

	As of December 31,				
	2018	2017*	2016*	2015	2014
	(In thousands)				
Consolidated Balance Sheet Data:					
Cash and cash equivalents	$409,829	$180,891	$223,667	$402,102	$146,363
Total assets	$2,696,078	$2,458,837	$2,526,092	$2,441,473	$1,758,881
Total deferred revenue	$934,828	$910,100	$927,749	$526,998	$352,543
Total long-term debt	$962,577	$779,578	$741,980	$706,198	$—
Total stockholders' equity	$650,394	$632,216	$710,006	$1,044,372	$1,250,828

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with our financial statements and related notes appearing elsewhere in this Annual Report on Form 10-K. In addition to historical financial information, the following discussion contains forward-looking statements that reflect our plans, estimates and beliefs. Our actual results could differ materially from those contained in or implied by any forward-looking statements. Factors that could cause or contribute to these differences include those under "Risk Factors" included in Part I, Item 1A or in other parts of this Annual Report on Form 10-K.

Overview

We provide a broad portfolio of cybersecurity solutions and services that allow organizations to prepare for, prevent, respond to and remediate cyber attacks. Our products include detection and prevention solutions for network, email and endpoint security, forensics appliances, security orchestration software, subscription-based threat intelligence and analytics solutions, and our Helix security operations platform. These products are complemented by our technology-enabled Managed Defense security service and our Mandiant incident response and cyber security consulting services.

Our Business Model

We generate revenue from sales of our network, email and endpoint security solutions, our security orchestration software, our cloud-based threat intelligence subscriptions, our managed security service, our Helix security operations platform, and our Mandiant professional services. We disaggregate our revenue into two main categories: (i) product, subscription, and support and (ii) professional services. For the years ended December 31, 2018, 2017 and 2016, product, subscription and support revenue as a percentage of total revenue was 83% for each period. Revenue from professional services was 17% of total revenue for each period.

Within the Product, subscription and support category, we provide supplemental data to distinguish between solutions that are deployed on-premise (or in hybrid on-premise/cloud configurations), and solutions and Managed services that are delivered entirely through the cloud. Security solutions deployed on-premise (or in hybrid on-premise/cloud configurations) are included in the Product and related subscription and support sub-category, and solutions without an on-premise component are included in the Cloud subscription and Managed services sub-category. For the years ended December 31, 2018, 2017 and 2016, Product and related subscription and support revenue as a percentage of total revenue was 60%, 62% and 62%, respectively. Revenue from Cloud subscription and Managed services was 23%, 21% and 21% for the years ended December 31, 2018, 2017 and 2016, respectively.

Revenue in the Product and related subscription and support sub-category consists primarily of revenue from sales of our network, email and endpoint security solutions that are deployed on the customer's premise, either as an integrated security appliance or in distributed hybrid on-premise/cloud configurations. Both deployment options are available on pre-configured appliance hardware or as virtual appliance software, and include FireEye IDA and MVX detection technologies, our DTI cloud updates, and support services.

Integrated and distributed solutions deployed on virtual appliances are offered as an "all inclusive" capacity-based subscription that includes our IDA and MVX technologies (distributed deployments include a shared MVX service), DTI cloud updates, and support services. There is no limit to the number of virtual appliances a customer can deploy, and capacity can be distributed throughout the network as needed. Subscription revenue is recognized ratably over the contractual term, typically one to three years. Customers purchasing our network and email security subscriptions have the option of purchasing our appliance hardware at additional cost, but are not required to do so.

Integrated network and email security solutions can also be deployed on pre-configured appliance hardware purpose-built for FireEye security solutions with scalable throughput from 50 megabits per second to multiple gigabits per second. Integrated security appliances are delivered with pre-installed IDA and MVX detection technologies and require subscriptions to our DTI cloud updates and support services, which are priced at 20% of the appliance price per year. Subscription terms are typically one to three years and include a material right of renewal. The majority of our installed base of network and on-premise email security customers purchased our solutions under this pricing model.

Since our network, email and endpoint security solutions require regular DTI cloud and software updates to maintain detection efficacy, physical and virtual security appliances and the related DTI cloud and support subscriptions are considered a single performance obligation, whether deployed as an integrated appliance or in a distributed hybrid

on-premise/cloud configuration.

As a single performance obligation, revenue from sales of appliance hardware and related subscriptions is recognized ratably over the contractual term, typically one to three years. Such contracts typically contain a material right of renewal option that allows the customer to renew their DTI cloud and support subscriptions for an additional term at a discount to the original purchase price of the single performance obligation. For contacts that contain a material right of renewal option, the value of the performance obligation allocated to the renewal is recognized ratably over the period between the end of the initial contractual term and end of the estimated useful life of the related appliance and license.

Revenue in the Cloud subscriptions and Managed services sub-category consists primarily of revenue from sales of our cloud-based email security, our threat analytics platform (either standalone or within the Helix security operations platform), our standalone threat

intelligence subscriptions and our Managed Defense managed detection and response service. Revenue from our Cloud subscriptions and Managed services is recognized ratably over the contractual term, generally one to three years.

A small portion of our revenue in the product and related subscription and support revenue is derived from the sale of our network forensics appliances and our central management system ("CMS") appliances. These appliances are not dependent on regular security intelligence updates, and revenue from these appliances is therefore recognized when ownership is transferred to our customer, typically at shipment.

Sales of our network, email, and endpoint security solutions, cloud subscriptions, and managed services, initially increase our deferred revenue. Deferred revenue from our product, subscription and support sales totaled $868.0 million and $859.5 million as of December 31, 2018 and 2017, respectively. The increase in deferred revenue from our product, subscription and support sales in 2018 compared to 2017 reflected strong subscription renewals by enterprise-class customers for our network, email and endpoint security products and increases in sales of our Cloud subscriptions and Managed services, partially offset by a decrease in sales of our appliance hardware compared with prior periods. Our retention rate of enterprise-class customers with subscriptions and support contracts expiring in the 12 months ended December 31, 2018 was consistent with historical retention rates.

To complement our product, subscription and support solutions, we offer professional services, including incident response and other security consulting services, to our customers who have experienced a cyber security breach or desire assistance assessing the resilience of their networks. The majority our professional services are offered on a time and materials basis, through a fixed fee arrangement, or on a retainer basis. Revenue from professional services is recognized as services are delivered. Revenue from our Expertise-on-Demand micro-services and some pre-paid professional services is deferred and revenue is recognized when services are delivered. Deferred revenue from professional services as of December 31, 2018 and 2017 was $66.8 million and $50.6 million, respectively.

Key Business Metrics

We monitor the key business metrics set forth below to help us evaluate growth trends, establish budgets, measure the effectiveness of our sales and marketing efforts, and assess operational efficiencies. We discuss revenue and gross margin below under “Components of Operating Results.” Deferred revenue, billings (a non-GAAP metric), net cash flow provided by (used in) operating activities, and free cash flow (a non-GAAP metric) are discussed immediately below the following table (in thousands, except percentages).

	Year Ended or as of December 31,		
	2018	2017*	2016*
Product, subscription and support revenue	$687,382	$645,965	$584,885
Professional services revenue	143,568	133,683	121,110
Total revenue	$830,950	$779,648	$705,995
Year-over-year percentage increase	7 %	10 %	
Gross margin percentage	67 %	65 %	62 %
Deferred revenue, current	$556,815	$546,615	$508,718
Deferred revenue, non-current	$378,013	$363,485	$419,031
Billings (non-GAAP)	$855,678	$761,999	$822,787
Net cash provided by (used in) operating activities	$17,381	$17,640	$(14,585)
Free cash flow (non-GAAP)	$10,125	$(26,139)	$(50,899)

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

Deferred revenue. Our deferred revenue consists of amounts that we have the right to invoice, but have not yet been recognized into revenue as of the end of the respective period. The majority of our deferred revenue consists of the unamortized balance of deferred revenue from previously invoiced sales of our security appliance hardware, and non-cancelable contracts for subscriptions to our network, email and endpoint security solutions, threat intelligence, managed services and support and maintenance contracts. Invoiced amounts for such contracts can be for multiple years, and we classify our deferred revenue as current or non-current depending on when we expect to recognize the related revenue. If the deferred revenue is expected to be recognized within 12 months it is classified as current, otherwise, the deferred revenue is classified as non-current. We monitor our deferred revenue balance because it represents a significant portion of revenue to be recognized in future periods.

Billings. Billings are a non-GAAP financial metric that we define as revenue recognized in accordance with generally accepted accounting principles ("GAAP") plus the change in deferred revenue from the beginning to the end of the period, excluding deferred revenue assumed through acquisitions. We consider billings to be a useful metric for management and investors, as a supplement to the corresponding GAAP measure, because billings impact our deferred revenue, which is an important indicator of the health and visibility of trends in our business and represents a significant percentage of future revenue. However, it is important to note that other companies, including companies in our industry, may not use billings, may define billings differently, may have different billing frequencies, or may use other financial measures to evaluate their performance, all of which could reduce the usefulness of billings as a comparative measure. A reconciliation of billings to revenue, the most directly comparable financial measure calculated and presented in accordance with GAAP, is provided below (in thousands):

	Year Ended December 31,		
	2018	2017*	2016*
Revenue	$830,950	$779,648	$705,995
Add: Deferred revenue, end of period	934,828	910,100	927,749
Less: Deferred revenue, beginning of period	910,100	927,749	789,870
Less: Deferred revenue assumed through acquisitions	—		21,087
Billings (non-GAAP)	$855,678	$761,999	$822,787

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

We have provided disaggregation of our billings in the table below (in thousands):

	Year Ended December 31,		
	2018	2017*	2016*
Product and related subscription and support	$451,973	$414,809	$499,038

Cloud subscription and Managed services	243,903	194,939	188,664
Professional Services	159,802	152,251	135,085
Billings (non-GAAP)	$855,678	$761,999	$822,787

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

Net cash provided by (used in) operating activities. We monitor net cash provided by (used in) operating activities as a measure of our overall business performance. Our net cash provided by (used in) operating activities performance is driven in large part by sales of our products and from up-front payments for both subscriptions and support and maintenance services. Monitoring net cash provided by (used in) operating activities enables us to analyze our financial performance without the non-cash effects of certain items, such as depreciation, amortization, amounts deemed repayment of convertible senior notes attributable to accreted debt discount and stock-based compensation costs, thereby allowing us to better understand and manage the cash needs of our business.

Free cash flow. Free cash flow is a non-GAAP financial measure we define as net cash provided by (used in) operating activities, the most directly comparable GAAP financial measure, plus amounts deemed to be repayment of accreted debt discount on repurchased convertible senior notes, less purchases of property and equipment and demonstration units. We consider free cash flow to be a liquidity measure that provides useful information to management and investors about the amount of cash generated by our business when excluding deemed repayment of accreted debt discount on repurchased convertible notes and that, after the purchases of property and equipment and demonstration units, can be used by us for strategic opportunities, including investing in our business, making strategic acquisitions and strengthening our balance sheet. However, it is important to note that other companies, including companies in our industry, may not use free cash flow, may calculate free cash flow differently, or may use other financial measures to evaluate their performance, all of which could reduce the usefulness of free cash flow as a comparative measure. A reconciliation of free cash flow to cash flow provided by (used in) operating activities is provided below (in thousands):

	Year Ended December 31,		
	2018	**2017**	**2016**
Cash flow provided by (used in) operating activities	$17,381	$17,640	$(14,585)
Add: deemed repayment of convertible senior notes attributable to accreted debt discount	43,575	—	—
Less: purchase of property and equipment and demonstration units	50,831	43,779	36,314
Free cash flow (non-GAAP)	$10,125	$(26,139)	$(50,899)
Net cash used in investing activities	$(48,517)	$(59,323)	$(189,696)
Net cash provided by (used in) financing activities	$260,074	$(1,093)	$25,846

Factors Affecting our Performance

Market Adoption. We rely on market education to raise awareness of today's cyber attacks and articulate the need for our security solutions and services. Our prospective customers often do not have a specific portion of their IT budgets allocated for advanced security solutions that address the next generation of cyber attacks. Additionally, the market for security operations platforms such as FireEye Helix is in the early stages of development.

We invest heavily in sales and marketing efforts to increase market awareness, educate prospective customers and drive adoption of our products, subscriptions and services. This market education is critical to creating new IT budget dollars or allocating more of existing IT budget dollars to advanced threat protection and security operations management solutions and, in particular, our solutions and the FireEye Helix platform. The degree to which prospective customers recognize the mission critical need for advanced threat protection solutions and security operations management solutions, including our FireEye Helix platform, will drive our ability to acquire new customers and increase renewals and follow-on sales opportunities, which, in turn, will affect our future financial performance.

Sales Productivity. Our sales organization consists of in-house sales teams who work in collaboration with external channel partners to identify new sales prospects, sell additional products, subscriptions and services, and provide post-sale support. Our sales teams are organized by territory to target large enterprise and government customers, who typically have sales cycles that can last several months or more. We have also expanded our inside sales teams to work with channel partners to expand our customer base of small and medium enterprises, or SMEs, as well as manage renewals of subscription and support contracts.

Newly hired sales and marketing employees typically require several months to establish prospect relationships and achieve full sales productivity. In addition, although we believe our investments in market education have increased awareness of us and our solutions globally, sales teams in certain international markets may face local markets with

limited awareness of us and our solutions, or have specific requirements that are not available with our solutions. All of these factors will influence the timing and overall levels of sales productivity, impacting the rate at which we will be able to convert prospects to sales and drive revenue growth.

Retention Rates. New or existing customers who purchase our appliance-based network, email, or endpoint security solutions are required to purchase a one to three year subscription to our DTI cloud and support and maintenance services. New or existing customers who purchase our network forensic appliances or our CMS management appliances are required to purchase support and maintenance services for a term of one to three years. Customers who purchase our network, email or endpoint security subscriptions (with or without appliance hardware), and our cloud subscriptions or managed services typically purchase contracts of one to three years duration.

Since we expect that our existing customers are likely to expand their deployments and purchase additional solutions from us over time, we believe our customer retention rate is an important metric to measure the long-term value of our customer agreements. We define retention rate as the percentage of customers at the end of the previous period that are up for renewal in the current period that remain customers at the end of the current period on a trailing twelve month basis. We believe our ability to maintain strong customer retention rates will have a material impact on our future sales of our security solutions and services and therefore our future financial performance.

Follow-On Sales. After the initial sale to a new customer, we focus on expanding our relationship with the customer to sell additional products, subscriptions and services. To grow our revenue, it is important that our customers make additional purchases of our products, subscriptions and services. Sales to our existing customer base can take the form of incremental sales of network, email and endpoint security solutions, cloud subscriptions, managed services, and professional services either to deploy our platform into additional parts of their network to protect additional threat vectors, or to extend their internal security resources with our managed and professional security services. Our opportunity to expand our customer relationships through follow-on sales will increase as we add new customers, broaden our product portfolio with additional subscriptions and services and enhance the functionality of our existing products and the Helix platform. Follow-on sales lead to increased revenue over the lifecycle of a customer relationship and can significantly increase the return on our sales and marketing investments. With many of our large enterprise and government customers, we have realized follow-on sales that were multiples of the value of their initial purchases.

Components of Operating Results

Revenue

We generate revenue from the sales of our products, subscriptions and services. As discussed further in “Critical Accounting Policies and Estimates-Revenue from Contracts with Customers” below, revenue is recognized when a contract has been entered into with a customer, the performance obligation(s) is(are) identified, the transaction price is determined and has been allocated to the performance obligation(s) and only then for each performance obligation after we have satisfied that performance obligation.

- *Product, subscription and support revenue*. Our product, subscription and support revenue is generated from sales of our network, email, and endpoint security solutions deployed on the customer's premise (or in a hybrid on-premise/cloud deployment), as well as cloud subscriptions and managed services. We combine our virtual and physical appliances and software licenses with the mandatory subscriptions to our DTI cloud updates and support services as a single performance obligation. As a result, we recognize revenue for this single performance obligation ratably over the contractual term. Contracts containing this single performance obligation typically contain a material right of renewal option. For contracts that contain a material right of renewal option, the allocated value of the performance obligation is recognized ratably over the period between the end of the initial contractual term and the end of the estimated useful life of the related appliance and license. Significant judgment is required in estimating the useful life of our intelligence dependent appliances and assessing the material rights associated with such products. Revenue from our Cloud subscription and Managed services is recognized ratably over the contractual term, typically one to three years.
- *Professional services revenue*. Professional services, which includes incident response, compromise assessments, and other security consulting services, are offered on a time-and-material basis, through a fixed fee arrangement, or on a retainer basis. We recognize the associated revenue as the services are delivered. Some professional services and our Expertise-on-Demand micro-services are prepaid, and revenue is deferred until services are delivered.

Cost of Revenue

Our total cost of revenue consists of cost of product, subscription and support revenue and cost of professional services revenue.

- *Cost of product, subscription and support revenue.* Cost of product, subscription and support revenue primarily consists of costs paid to our third-party contract manufacturers for our appliances, other costs in our manufacturing operations department, and personnel costs associated with maintaining our Dynamic Threat Intelligence updates and our global customer support operations. Personnel costs associated with our operations and global customer support organizations consist of salaries, benefits, bonuses and stock-based compensation. Overhead costs consist of certain facilities, depreciation and information technology costs. Our cost of product, subscription and support revenue also

includes product testing costs, shipping costs and allocated overhead costs. If revenue from sales of product, subscriptions and support declines, the cost of product, subscription and support revenue may increase as a percentage of product, subscription and support revenue due to the fixed nature of a portion of these costs. Additionally, our appliance related cost of goods sold are capitalized and amortized on a systematic basis that is consistent with the pattern of transfer to which the asset relates.

- *Cost of professional services revenue.* Cost of professional services revenue primarily consists of personnel costs for our services organization and allocated overhead costs. If sales of our professional services decline or we are unable to maintain our changeability rates, our cost of professional services revenue may increase as a percentage of professional services revenue.

Gross Margin

Gross margin, or gross profit as a percentage of revenue, has been and will continue to be affected by a variety of factors, including our average selling prices, the mix of products and services sold, the mix of revenue among products, subscriptions and services and manufacturing costs. We expect our gross margins to fluctuate over time depending on these factors.

Operating Expenses

Our operating expenses consist of research and development, sales and marketing and general and administrative expenses. Personnel costs are the most significant component of operating expenses and consist of salaries, benefits, bonuses, stock-based compensation and, with regard to sales and marketing expense, sales commissions. Operating expenses also include allocated overhead costs consisting of certain facilities, depreciation and information technology costs.

- *Research and development.* Research and development expense consists primarily of personnel costs and allocated overhead. Research and development expense also includes prototype related expenses. We expect research and development expense to increase in absolute dollars but to remain flat as a percentage of total revenue.
- *Sales and marketing.* Sales and marketing expense consists primarily of personnel costs, incentive commission costs and allocated overhead. Commission costs are capitalized and amortized based on the useful life amortization period taking into consideration the pattern of transfer to which the asset relates and the expected renewal periods during which renewal commissions are not commensurate with the initial commissions paid. When initial commissions are higher than (not-commensurate with) renewal commissions, we recognize the incremental portion of initial commissions over an estimated renewal period. The commensurate portion will be recognized over the same period as the initial revenue arrangement to which it relates.

Sales and marketing expense also includes costs for market development programs, promotional and other marketing activities, travel, depreciation of proof-of-concept evaluation units and outside consulting costs. These costs are recognized as incurred. We expect sales and marketing expense to remain relatively flat in absolute terms, but decrease as a percentage of total revenue.

- *General and administrative*. General and administrative expense consists of personnel costs, professional service costs and allocated overhead. General and administrative personnel include our executive, finance, human resources, facilities and legal organizations. Professional service costs consist primarily of legal, auditing, accounting and other consulting costs. We expect general and administrative expense to remain relatively flat in absolute terms, but to decrease as a percentage of total revenue.

Interest Income

Interest income consists of interest earned on our cash and cash equivalent and investment balances. We have historically invested our cash in money-market funds and other short-term, high quality securities. We expect interest income to vary each reporting period depending on our average investment balances during the period, types and mix of investments and market interest rates.

Interest Expense

Interest expense consists primarily of interest at the stated rate (coupon) and amortization of discounts and issuance costs relating to our convertible notes.

Other Income (Expense), Net

Other income (expense), net includes gains or losses on the disposal of fixed assets, gains or losses from our equity-method investment, gains or losses on the extinguishment of convertible notes, foreign currency re-measurement gains and losses and foreign currency transaction gains and losses. We expect other income (expense), net to fluctuate depending primarily on foreign exchange rate movements.

Provision for (Benefit from) Income Taxes

Provision for income taxes primarily relates to income taxes payable in foreign jurisdictions in which we conduct business, withholding taxes, and state income taxes in the United States. The provision is offset by tax benefits primarily related to the reversal of valuation allowances previously established against our deferred tax assets. Should the tax benefits exceed the provision, then a net tax benefit from income taxes is reflected for the period. Income in certain countries may be taxed at statutory tax rates that are lower than the U.S. statutory tax rate. As a result, our overall effective tax rate over the long-term may be lower than the U.S. federal statutory tax rate due to net income

being subject to foreign income tax rates that are lower than the U.S. federal statutory rate.

Results of Operations

The following tables summarize our results of operations for the periods presented and as a percentage of our total revenue for those periods. The period-to-period comparison of results is not necessarily indicative of results for future periods.

	Year Ended December 31,		
	2018	2017*	2016*
	(In thousands)		
Revenue:			
Product, subscription and support	$687,382	$645,965	$584,885
Professional services	143,568	133,683	121,110
Total revenue	830,950	779,648	705,995
Cost of revenue:			
Product, subscription and support	188,301	190,786	192,659
Professional services	84,174	80,861	78,424
Total cost of revenue	272,475	271,647	271,083
Total gross profit	558,475	508,001	434,912
Operating expenses:			
Research and development	254,142	243,273	279,594
Sales and marketing	380,962	379,278	437,519
General and administrative	105,773	125,549	139,791
Restructuring charges	—	—	27,630
Total operating expenses	740,877	748,100	884,534
Operating loss	(182,402)	(240,099)	(449,622)
Interest income	16,033	9,323	6,582
Interest expense	(56,426)	(49,766)	(47,869)
Other expense, net	(14,804)	(10)	(3,247)
Loss before income taxes	(237,599)	(280,552)	(494,156)
Provision for (benefit from) income taxes	5,524	4,632	(8,721)
Net loss attributable to common stockholders	$(243,123)	$(285,184)	$(485,435)

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

	Year Ended December 31,		
	2018	2017*	2016*
	(Percent of total revenue)		
Revenue:			
Product, subscription and support	83 %	83 %	83 %
Professional services	17	17	17
Total revenue	100	100	100
Cost of revenue:			
Product, subscription and support	23	25	27
Professional services	10	10	11
Total cost of revenue	33	35	38
Total gross profit	67	65	62
Operating expenses:			
Research and development	31	31	40
Sales and marketing	46	49	62
General and administrative	13	16	20
Restructuring charges	—	—	4
Total operating expenses	89	96	126
Operating loss	(22)	(31)	(64)
Interest income	2	1	1
Interest expense	(7)	(6)	(7)
Other expense, net	(2)	—	0
Loss before income taxes	(29)	(36)	(70)
Provision for (benefit from) income taxes	1	1	(1)
Net loss attributable to common stockholders	(29)%	(37)%	(69)%

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

Comparison of the Years Ended December 31, 2018 and 2017

	Year Ended December 31,								
	2018			2017*			Change		
	Amount	% of Total Revenue		Amount	% of Total Revenue		Amount	%	
	(Dollars in thousands)								
Revenue:									
Product, subscription and support	$687,382	83	%	$645,965	83	%	$41,417	6	%
Professional Services	143,568	17		133,683	17		9,885	7	
Total revenue	$830,950	100	%	$779,648	100	%	$51,302	7	%
Product, subscription and services by type:									
Product and related subscription and support	$498,992	60	%	$479,521	62	%	$19,471	4	%
Cloud subscription and Managed services	188,390	23		166,444	21		21,946	13	
Total Product, subscription and support	$687,382	83	%	$645,965	83	%	$41,417	6	%
Revenue by geographic region:									
United States	$523,150	63	%	$521,232	67	%	$1,918	—	%
EMEA	135,736	16		116,205	15		19,531	17	
APAC	122,516	15		105,196	13		17,320	16	
Other	49,548	6		37,015	5		12,533	34	
Total revenue	$830,950	100	%	$779,648	100	%	$51,302	7	%

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

Product, subscription and support revenue increased by $41.4 million, or 6%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The increase was comprised of product and related subscription and support revenue of $19.5 million and cloud subscription and managed services of $21.9 million. The increase in product and related subscription and support revenue was primarily due to an increase in the amortization of deferred revenue for subscription and support associated with prior period sales of our on-premise network, email and endpoint security solutions, as well as subscription and support renewals. The increase in cloud subscriptions and managed services reflected increased amortization of deferred revenue associated with sales of our threat intelligence subscriptions, our cloud-based email security, our Helix network operations platform, and our Managed Defense managed security service.

We are experiencing a shift in customer buying patterns away from the deployment of security solutions on new appliance hardware in favor of virtual, cloud and hybrid security solutions. This has resulted in a continuing decline in our sales of appliance hardware for our network, email and endpoint security solutions. As a result, the amortization of deferred revenue associated with prior appliance sales exceeded additions to deferred revenue from new appliance sales, and the amount of deferred revenue associated with our appliances declined in 2018. We expect the decline in deferred revenue associated with appliance hardware will continue, which will result in reduced amortization of appliance revenue in future periods. This decline is offset by increased sales of our cloud subscriptions and managed services, as well as sales of our network, email and endpoint security subscriptions and renewals of prior subscription and support contracts.

Given the expansion of our customer base, our new subscription pricing model for on-premise, and hybrid on-premise/cloud network, email and endpoint security, and our high retention rate for enterprise-class customers, we expect revenue from the amortization of deferred revenue associated with renewals of our network, email, and endpoint security solutions, our cloud subscriptions and our managed services to increase as a percentage of our total revenue. Our retention rate of enterprise-class customers with subscriptions expiring in the 12 months ended December 31, 2018 remained strong.

Professional services revenue increased by $9.9 million, or 7%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The increase is primarily driven by revenues from incident response services and an increase in billable hours due to more engagements and professional services personnel as compared to the

same period in 2017.

Our international revenue increased $49.4 million, or 19%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The increase reflects growth in sales from our international regions compared to prior periods as we expanded our international market presence, which resulted in an increase in revenue amortized from deferred revenue.

	Year Ended December 31,					
	2018		2017*		Change	
	Amount	Gross Margin	Amount	Gross Margin	Amount	%
	(Dollars in thousands)					
Cost of revenue:						
Product, subscription and support	$188,301		$190,786		$(2,485)	(1)%
Professional services	84,174		80,861		3,313	4
Total cost of revenue	$272,475		$271,647		$828	— %
Gross margin:						
Product, subscription and support		73 %		70 %		
Professional services		41 %		40 %		
Total gross margin		67 %		65 %		

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

The cost of product, subscription and support revenue decreased $2.5 million, or 1%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The decrease in cost of product, subscription and support revenue was primarily the result of declining appliance hardware sales, partially offset by an increase in software licenses and network costs associated with increased subscription and support sales.

The cost of professional services revenue increased $3.3 million, or 4%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The increase in cost of professional services revenue was primarily driven by a $5.9 million increase in personnel costs and a $1.3 million increase in travel costs due to higher headcount, partially offset by a $3.5 million decrease in depreciation as compared to the same period in 2017.

Gross margin was higher for the year ended December 31, 2018 compared to the year ended December 31, 2017, due to increased gross margins for product, subscriptions and support and professional services. The increased product, subscription and services margin reflected a higher mix of higher margin subscriptions. The increase in professional services margin was primarily driven by higher billable utilization of our professional services personnel.

	Year Ended December 31,					
	2018		2017*		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Operating expenses:						
Research and development	$254,142	31 %	$243,273	31 %	$10,869	4 %
Sales and marketing	380,962	46	379,278	49	1,684	0
General and administrative	105,773	13	125,549	16	(19,776)	(16)
Total operating expenses	$740,877	89 %	$748,100	96 %	$(7,223)	(1)%
Includes stock-based compensation expense of:						
Research and development	$49,503		$56,720			
Sales and marketing	47,592		46,766			
General and administrative	28,218		30,194			
Total	$125,313		$133,680			

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

Research and Development

Research and development expense increased $10.9 million, or 4%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The increase was primarily due to a $10.6 million increase in personnel costs for headcount increase, a $1.7 million increase in professional services costs, a $5.3 million increase in software and web hosting costs, and a $0.9 million increase in

53

travel costs, partially offset by a decrease in stock-based compensation charges of $7.2 million. The increase in headcount was as a result of increased investment in research and development for future product and subscription offerings.

Sales and Marketing

Sales and marketing expense increased by $1.7 million, or 0.4%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The increase was primarily due to an increase in personnel costs of $4.7 million associated with increased headcount, an $0.8 million increase in stock-based compensation expense and a $4.7 million increase in marketing programs and associated travel costs, partially offset by a $6.2 million decrease in commission expense as a result of non-order related payouts in 2017, and a $2.7 million decrease in amortization of intangibles.

General and Administrative

General and administrative expense decreased $19.8 million, or 16%, during the year ended December 31, 2018 compared to the year ended December 31, 2017. The decrease was primarily due to a $14.0 million decrease in net legal settlement costs and related legal costs incurred in 2017, a $1.4 million decrease in consulting services primarily related to implementation of ASC 606 adoption, a $1.5 million decrease in professional services costs, a $1.8 million decrease in bad debt expense, and a $2.0 million decrease in stock-based compensation charges, partially offset by a $1.0 million increase in personnel costs due to increased headcount.

	Year Ended December 31,		Change	
	2018	2017	Amount	%
	(Dollars in thousands)			
Interest income	$16,033	$9,323	$6,710	72%

Interest income increased for the year ended December 31, 2018 compared to the year ended December 31, 2017, primarily due to an increase in interest rates resulting in a higher rate of return on our investments.

	Year Ended December 31,		Change	
	2018	2017	Amount	%
	(Dollars in thousands)			
Interest expense	$56,426	$49,766	$6,660	13%

Interest expense for the year ended December 31, 2018 increased compared to the year ended December 31, 2017 due to greater amortization of discount and issuance costs on our previously issued 2035 Notes and the issuance of the 2024 Notes during the year ended December 31, 2018.

	Year Ended December 31,		Change	
	2018	2017	Amount	%
	(Dollars in thousands)			
Other expense, net	$14,804	$ 10	$14,794	147,940%

The increase in other expense, net during the year ended December 31, 2018 compared to the year ended December 31, 2017 was primarily due to the loss on extinguishment of a portion of the 1.000% Convertible Senior Notes due 2035 (the “Series A Notes”) in the amount of $10.8 million and foreign currency transaction losses of $3.3 million during the year ended December 31, 2018.

	Year Ended December 31,	
	2018	2017
	(Dollars in thousands)	
Provision for (benefit from) income taxes	$5,524	$4,632
Effective tax rate	(2.3)%	(1.6)%

54

The provision for income taxes increased for the year ended December 31, 2018 compared to the year ended December 31, 2017. The increase in the provision was primarily due to an increase in estimated tax liability related to foreign operations. We continue to maintain a full valuation allowance on all of our U.S. deferred tax assets. The tax expense for the years ended December 31, 2018 and December 31, 2017 was primarily comprised of income taxes in foreign jurisdictions and withholding taxes.

Comparison of the Years Ended December 31, 2017 and 2016

	Year Ended December 31,							
	2017*		2016*		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Revenue:						
Product, subscription and support	$645,965	83 %	$584,885	83 %	$61,080	10%
Professional Services	133,683	17	121,110	17	12,573	10
Total revenue	$779,648	100 %	$705,995	100 %	$73,653	10%
Product, subscription and services by type:						
Product and related subscription and support	$479,521	62 %	$437,238	62 %	$42,283	10%
Cloud subscription and Managed services	166,444	21	147,647	21	18,797	13
Total Product, subscription and support	$645,965	83 %	$584,885	83 %	$61,080	10%
Revenue by geographic region:						
United States	$521,232	67 %	$490,802	70 %	$30,430	6 %
EMEA	116,205	15	93,832	13	22,373	24
APAC	105,196	13	90,682	13	14,514	16
Other	37,015	5	30,679	4	6,336	21
Total revenue	$779,648	100 %	$705,995	100 %	$73,653	10%

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

Product, subscription and support revenue increased by $61.1 million, or 10%, during the year ended December 31, 2017 compared to the year ended December 31, 2016. The increase was comprised of a $42.3 million, or 10%, increase in product and related subscription and support revenue and an $18.8 million, or 13%, increase in cloud subscription and managed services. The increase in product and related subscription and support revenue was primarily due to an increase in the amortization of deferred revenue associated with prior period sales and renewals of our network, email, and endpoint security solutions, including appliance hardware. The increase in cloud subscription and managed services revenue was primarily due to the amortization of deferred revenue associated with growing sales of our cloud subscriptions, including threat intelligence subscriptions, our cloud-based email security, and our Helix network operations platform.

Given our expanding customer base and high retention rate of enterprise-class customers, we expect revenue from the amortization of deferred revenue related to renewals to increase as a percentage of our total revenue. Our retention rate for enterprise class customers, expiring in the 12 months ended December 31, 2016 remained strong.

Professional services revenue increased by $12.6 million, or 10%, during the year ended December 31, 2017 compared to the year ended December 31, 2016. The increase reflected growth in sales in our international regions in prior periods as we expanded our international market presence, which resulted in an increase in revenue amortized from deferred revenue.

Our international revenue increased $43.2 million, or 20%, during the year ended December 31, 2017 compared to the year ended December 31, 2016, which reflected our increasing international market presence.

	Year Ended December 31,					
	2017*		2016*		Change	
	Amount	Gross Margin	Amount	Gross Margin	Amount	%
	(Dollars in thousands)					
Cost of revenue:						
Product, subscription and support	$190,786		$192,659		$(1,873)	(1)%
Professional Services	80,861		78,424		2,437	3
Total cost of revenue	$271,647		$271,083		$564	— %
Gross margin:						
Product, subscription and support		70 %		67 %		
Professional Services		40 %		35 %		
Total gross margin		65 %		62 %		

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

The cost of product, subscription and support revenue decreased $1.9 million, or 1%, during the year ended December 31, 2017 compared to the year ended December 31, 2016. The decrease in cost of product, subscription and support revenue was primarily driven by fewer product shipments and lower average product cost per unit, partially offset by greater inventory reserves.

The cost of professional services revenue increased $2.4 million, or 3%, during the year ended December 31, 2017 compared to the year ended December 31, 2016. The increase in cost of professional services revenue was primarily due to a $1.9 million increase in professional services and consulting costs, and a $1.2 million increase in software and hosting costs, partially offset by a $0.7 million decrease in amortization of intangibles.

Gross margin was higher for the year ended December 31, 2017 compared to the year ended December 31, 2016, due primarily to an increase in product, subscription and support and professional services revenue, while the total cost of revenue remained relatively constant as compared to the same period in 2016.

	Year Ended December 31,					
	2017*		2016*		Change	
	Amount	% of Total Revenue	Amount	% of Total Revenue	Amount	%
	(Dollars in thousands)					
Operating expenses:						
Research and development	$243,273	31 %	$279,594	40 %	$(36,321)	(13)%
Sales and marketing	379,278	49	437,519	62	(58,241)	(13)
General and administrative	125,549	16	139,791	20	(14,242)	(10)
Restructuring charges	—	—	27,630	4	(27,630)	(100)
Total operating expenses	$748,100	96 %	$884,534	126 %	$(136,434)	(15)%
Includes stock-based compensation expense of:						
Research and development	$56,720		$64,755			
Sales and marketing	46,766		57,750			
General and administrative	30,194		43,343			
Restructuring charges	—		1,144			
Total	$133,680		$166,992			

*Certain prior period amounts have been adjusted as a result of adoption of ASC 606.

the year ended December 31, 2017 compared to the year ended December 31, 2016. The decrease was primarily due to a $26.9 million net decrease in personnel costs, which included an $8.0 million decrease in stock-based compensation charges, as well as a $3.7 million reduction as a result of higher capitalized software development costs primarily related to our Helix offering, a

$1.8 million decrease in allocated facility and IT costs, a $1.6 million decrease

in telecommunications costs, a $1.3 million decrease in professional service vendor costs and a $1.2 million decrease in depreciation expense, partially offset by a $2.6 million increase in data hosting costs. The decreases were primarily driven by lower headcount and cost optimizations as a result of our 2016 restructuring activities.

Sales and marketing expense decreased $58.2 million, or 13%, during the year ended December 31, 2017 compared to the year ended December 31, 2016. The decrease was primarily due to a $34.6 million decrease in personnel costs, which included an $11.0 million decrease in stock-based compensation charges, a $8.9 million decrease in commissions, a $7.3 million decrease in allocated facility and IT costs, a $3.9 million decrease in marketing programs, a $3.9 million decrease in depreciation expense associated with demonstration units and a $3.5 million decrease in travel expense. The decreases were primarily driven by lower headcount and cost optimizations from our 2016 restructuring activities.

General and administrative expense decreased $14.2 million, or 10%, during the year ended December 31, 2017 compared to the year ended December 31, 2016. The decrease was primarily due to a $19.1 million decrease in personnel costs, which included a $13.1 million decrease in stock-based compensation charges, that was primarily driven by lower headcount and cost optimizations from our 2016 restructuring activities, a $2.5 million decrease due to a charge related to the change in fair value of the contingent earn-out liability recognized in fiscal 2016, and a $1.6 million decrease in professional service vendor costs due primarily to lower acquisition-related costs, partially offset by $12.5 million in net legal settlement costs.

we incurred restructuring charges of approximately $27.6 million, primarily related to a 10% reduction in our workforce, the consolidation of certain real estate facilities and impairment of certain assets under our August 2016 restructuring plan. We incurred no restructuring expenses during the year ended December 31, 2017.

	Year Ended December 31,		Change	
	2017	2016	Amount	%
	(Dollars in thousands)			
Interest income	$9,323	$6,582	$2,741	42%

year ended December 31, 2017 year ended December 31, 2016

	Year Ended December 31,		Change	
	2017	2016	Amount	%
	(Dollars in thousands)			
Interest expense	$49,766	$47,869	$1,897	4%

expense for the year ended December 31, 2017 increased compared to the year ended December 31, 2016 due to greater amortization of discount and issuance costs on our 2035 Notes.

	Year Ended December 31,		Change	
	2017	2016	Amount	%
	(Dollars in thousands)			
Other expense, net	$10	$3,247	$(3,237)	(100)%

The decrease in other expense, net during the year ended December 31, 2017 compared to the year ended December 31, 2016 was primarily due to greater foreign currency transaction gains during the year ended December 31, 2017.

57

	Year Ended December 31,	
	2017	2016
	(Dollars in thousands)	
Provision for (benefit from) income taxes	$4,632	$(8,721)
Effective tax rate	(1.6)%	1.8 %

We recorded a tax expense for the year ended December 31, 2017 compared to a tax benefit for the year ended December 31, 2016. The change to a tax expense in 2017 is primarily due to the reversal of a valuation allowance in connection with the acquisitions of iSIGHT and Invotas included in 2016, which was not included in 2017. We continue to maintain a full valuation allowance on all of our U.S. deferred tax assets. The tax expense for the year ended December 31, 2017 was primarily comprised of income taxes in foreign jurisdictions and withholding taxes.

Quarterly Results of Operations

The following unaudited quarterly statements of operations data for each of the eight quarters in the period ended December 31, 2018 have been prepared on a basis consistent with our audited annual financial statements included in this Annual Report on Form 10-K and include, in our opinion, all normal recurring adjustments necessary for the fair presentation of the financial information contained in those statements. Our historical results are not necessarily indicative of the results that may be expected in the future. The following quarterly financial data should be read in conjunction with our audited financial statements and the related notes included in this Annual Report on Form 10-K.

	Three Months Ended							
	December 31, 2018	September 30, 2018	June 30, 2018	March 31, 2018	December 31, 2017*	September 30, 2017*	June 30, 2017*	March 31, 2017*
	(Dollars in thousands)							
Revenue:								
Product, subscription and support	$178,827	$ 175,653	$167,429	$165,473	$170,965	$163,174	$158,097	$153,729
Professional Services	38,706	35,998	35,267	33,597				