



# **Security Software**

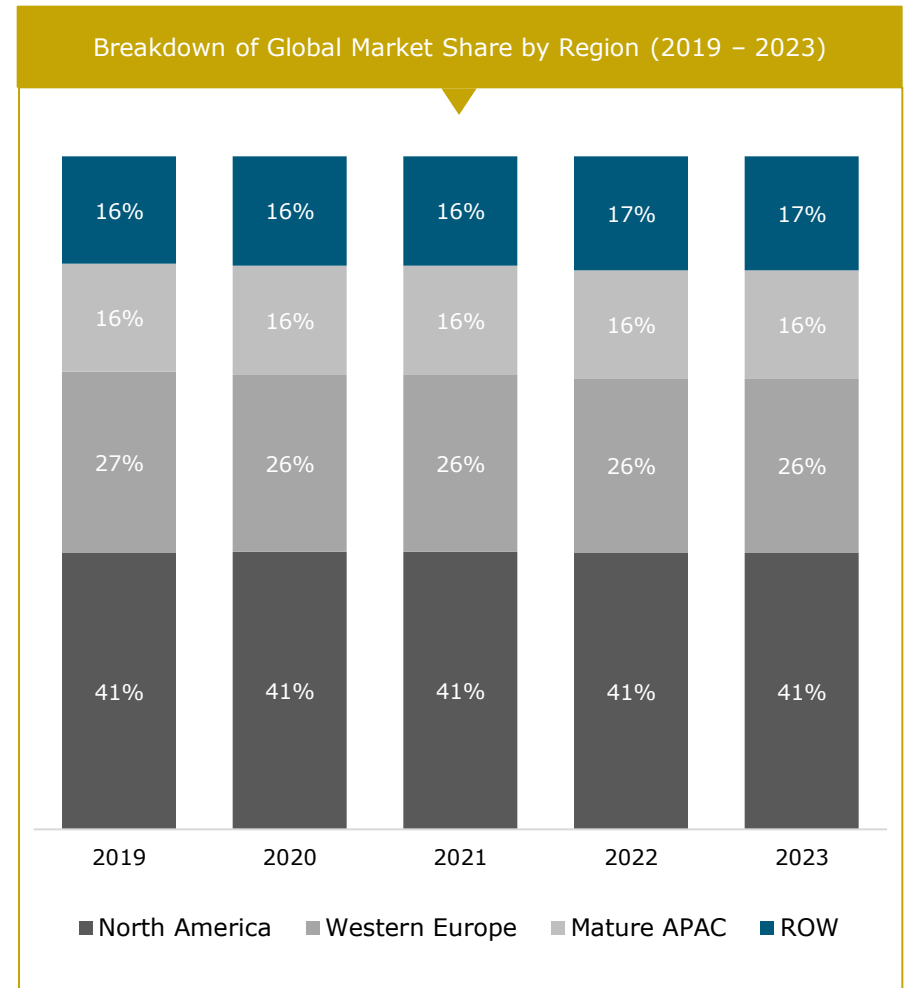
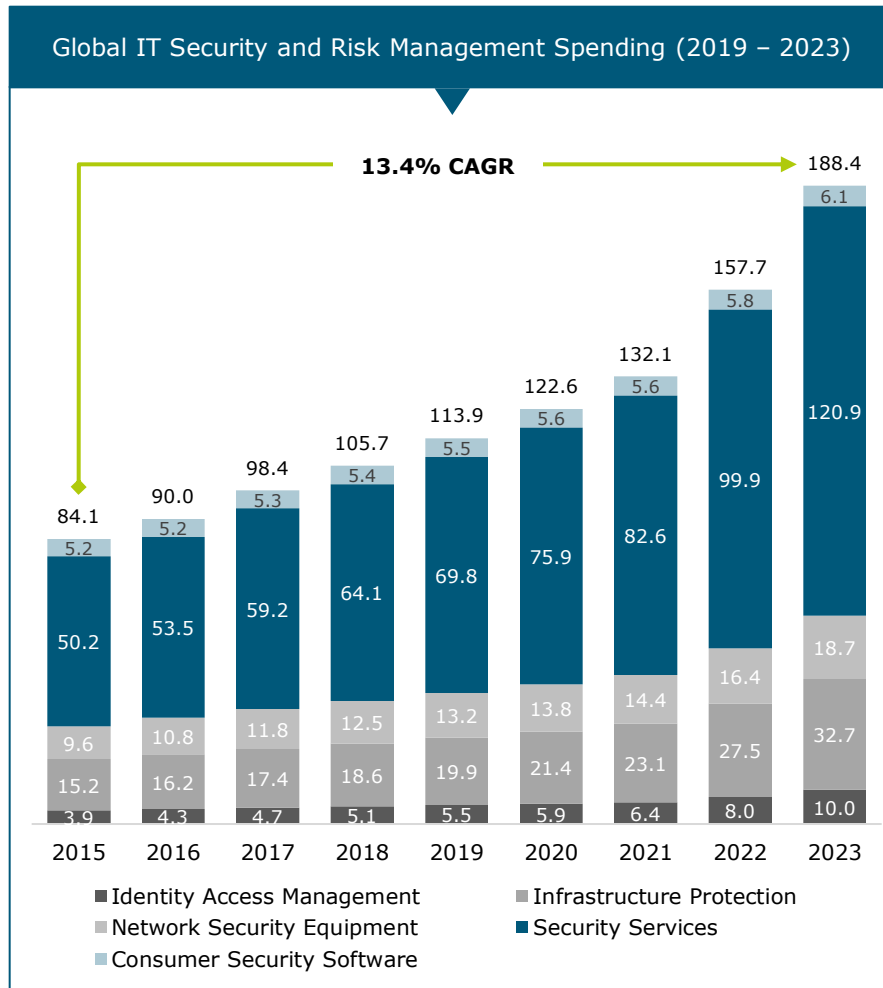
*Industry Overview Highlights*

March 2020

**Growing equity, realizing value**

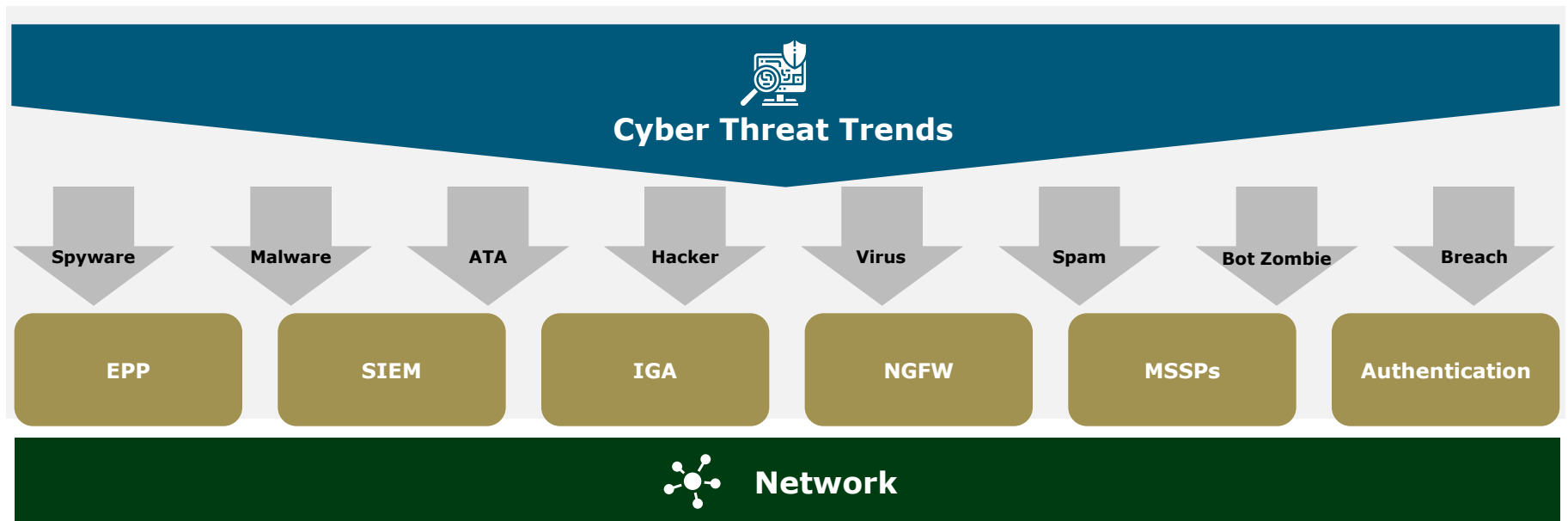
# Global IT Security and Risk Management Spending Is Expected To Grow At A 13.4% CAGR With Developed Markets Representing The Largest Spend

- The information security market grew 7.8% in revenue in 2019, with the Security Services segment recording the fastest growth at 8.9%; Gartner estimates the global market for IT security will exceed \$188.4 billion in 2023
- Developed regions such as North America and Western Europe will continue to dominate the global landscape in the foreseeable future as market spend across geographies is expected to remain consistent



Source: Gartner; Equiteq Analysis

# Increases In Cyber Attacks & Fraud Are Driving Spending On Security Software & Identity Management



More zero day attacks where attackers exploit unidentified vulnerabilities in a system – SMB’s with weaker security measures are increasingly the victims in these attacks

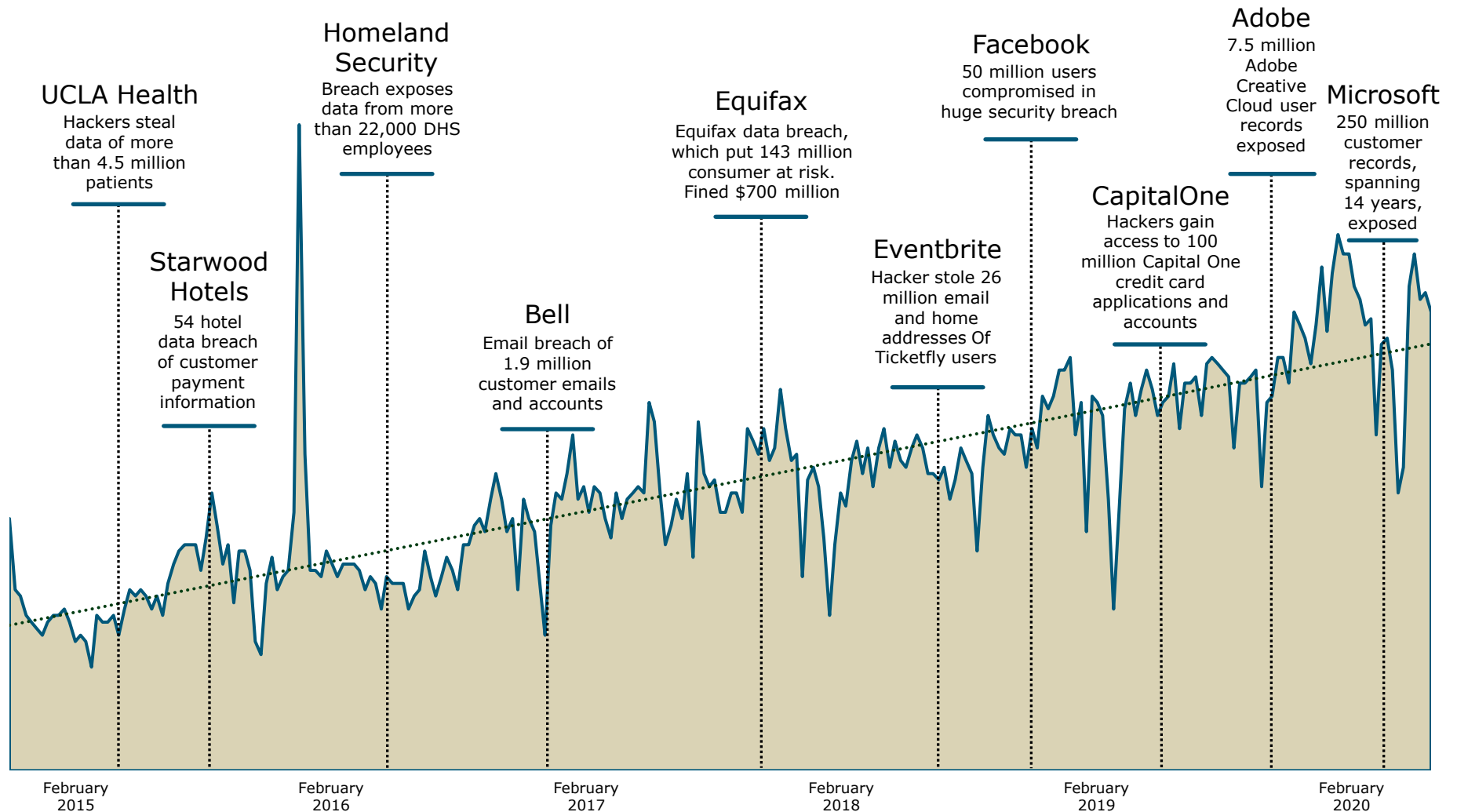
Focused targeted attacks and advanced persistent threats (APTs), where individuals or groups use significant resources and a more concerted effort to achieve their ends, have increased in occurrence

Political and ideological driven cyber attacks are ushering in a new wave of “hacktivism”

Malware authors are writing more ransomware, a form of malware that denies access to a system until a user pays a “ransom”

New suspect URLs hosting compromising malware, exploits, or codes are gaining more realistic appearances

# The Number Of Searches For "Cybersecurity" Has Been Steadily Growing With The Breaches



Source: Google Trends; Equiteq Analysis

# Changing Industry Dynamics Have Opened New Vulnerabilities As Businesses Focus On Cloud, Mobile, Social And Information/Big Data



## Cloud

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Metered service

### Vulnerabilities:

- Consolidation of large quantities of data in one place leads to more opportunities for outsiders to exploit
- Employee rogue projects
- Malicious insiders



## Social

- Web-based platforms
- Increased use of popular social media and networking sites Facebook, Instagram, Twitter, Pinterest, among others
- Creates need for mobile access and depends on cloud for scale and access

### Vulnerabilities:

- Threats via careless employees, BYOD, and fraudsters
- Increased use of social engineering (i.e. phishing) to steal confidential information



## Mobile

- Growing capabilities
- Growing number of mobile devices
- No more border between personal and professional
- No more border between home and office

### Vulnerabilities:

- "Eavesdropping" malware
- Bring your own device (BYOD)
- Malicious applications
- Increase in privacy leaks and premium number fraud



## Information / Big Data

- Increasing amounts of information
- Organizations are now able to probe larger, non-traditional datasets (like social media feeds) for valuable information

### Vulnerabilities:

- More APTs and social tactics risks
- Also opportunities: SIEM, network monitoring, user authentication, identity management, fraud detection, IPS, DLP; and governance, risk, and compliance (GRC)

# Adoption of Cloud Systems Poses Serious Threats



## Cloud Systems

Data Breach	Rogue Projects	GRC Concerns	Malicious Insiders	Account or Service Hijacking
<ul style="list-style-type: none"> <li>• Large quantities of data creates an attractive target</li> <li>• More vulnerability points</li> <li>• Targeted attacks and incursions via Internet-facing devices</li> <li>• Four stages of a typical breach:               <ol style="list-style-type: none"> <li>1. Incursion</li> <li>2. Discovery</li> <li>3. Capture</li> <li>4. Exfiltration</li> </ol> </li> </ul>	<ul style="list-style-type: none"> <li>• Inferior cloud infrastructures open up security risks</li> <li>• Employees engage in rogue cloud situations</li> <li>• Employees turn to cloud networks when their IT departments cannot accommodate projects on their networks</li> <li>• Unauthorized use of cloud applications</li> <li>• Lack of adequate monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• Rush to move to cloud based systems</li> <li>• Companies fined for various violations of privacy</li> <li>• Inability to locate information</li> <li>• Inability to monitor various regulations including HIPAA, COBIT, SOX, EU GDPR FFIEC, among others</li> <li>• Organizations need to ensure new cloud systems have “touch points” within finance and legal departments</li> </ul>	<ul style="list-style-type: none"> <li>• Amplified threat of malicious insiders</li> <li>• Lack of visibility</li> <li>• Insider gains visibility to extraordinary amounts of sensitive data</li> <li>• Malicious insiders face little risk of threat or detection</li> <li>• Open to many vulnerabilities</li> <li>• Companies who rely only on a cloud service provider for security are at the greatest risk</li> </ul>	<ul style="list-style-type: none"> <li>• Methods like phishing and fraud to gain access to confidential accounts</li> <li>• Recycling of usernames and password</li> <li>• Stolen credentials</li> <li>• Ability to skew data and wreak havoc client database</li> <li>• Prohibit credential sharing and invest in stronger IAM software</li> </ul>

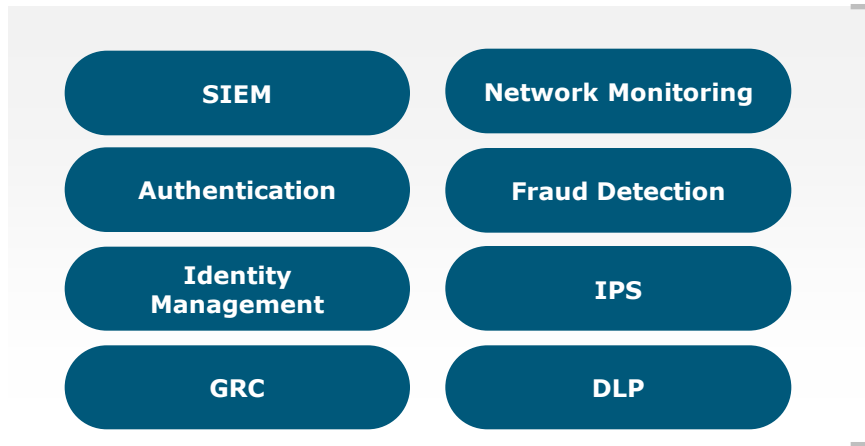
# Penetration Of Mobile Devices In The Enterprise Have Opened Unforeseen Vulnerabilities That Require Innovative Solutions



# The Emergence Of Big Data Opens The Door To New Security Measures



- Tremendous amounts of big data
- Data stored and managed in advanced databases (No SQL, Hadoop, etc)
- BI and advanced analytics needed to interpret





- Full 360-degree view of an organization and potential security risks
- Big data-driven security models
- Network monitoring and SIEM with the ability to process increasing amounts of information
- Greater depth to user profiles, for accurate baseline behavior
- Unification of behavioral and click-stream analysis



- By 2020, over one-third of all data will live in or pass through the cloud <sup>(1)</sup>
- In 2020, data production is estimated to be 44 times greater than it was in 2009; experts estimate a 4,300 percent increase in annual data generation by 2020. Advanced persistent threats (APTs) are more organized and deceptive attacks that require significant resources and are carried out over a prolonged period of time<sup>(1)</sup>



# Increased Use Of Social Media Calls For Additional Protection

 <b>Social Threats</b>			 <b>Social Protection</b>	
Social Engineering	Malware	Media & Business	Layered Security	User Level
<ul style="list-style-type: none"> <li>• Increase in spam and phishing</li> <li>• Phishers trick victims into divulging valuable information</li> <li>• Users taken to websites asking for the disclosure of information</li> <li>• Rise in “vishing,” where attackers task a victim with calling a phone number instead of clicking a link</li> </ul>	<ul style="list-style-type: none"> <li>• Malware connects with social media networks rather than customary C&amp;C servers</li> <li>• Lure victims into clicking on malicious links or downloads</li> <li>• Advanced targeted attacks</li> <li>• Successful attacks feed off one another</li> </ul>	<ul style="list-style-type: none"> <li>• Posts by employees on social media networks accidentally reveal sensitive information</li> <li>• Leverage company media pages to lure in new victims</li> <li>• Exposes businesses to potential lawsuits by reckless employees</li> <li>• BYOD allows criminals access to company information through social media account breaches</li> </ul>	<ul style="list-style-type: none"> <li>• EPP should have antivirus IDS/IPS, Firewall, and Application Control capabilities</li> <li>• Enforcing secure SSL connections to make phishing and other social media attacks more difficult</li> <li>• MSSPs to tag hosts and provide a higher level of security for social media users</li> </ul>	<ul style="list-style-type: none"> <li>• Trade-off between benefits of social media and security</li> <li>• Train employees on the appropriate use of social media</li> <li>• Limit the amount of personal data available online to avoid social engineering attacks</li> <li>• Consider all links before clicking to avoid threatening malware</li> </ul>

# Selected M&A Transactions

Date	Acquirer	Target	Target Business Description	EV (\$mm)
2/18/2020	<b>AlpInvest Partners, Ontario Teachers Pension Plan, STG</b>	<b>RSA</b>	Offers services for cyber threat detection and response, identity and access management, online fraud prevention, and governance, risk and compliance	\$2,075
2/6/2020	<b>Advent International</b>	<b>Forescout</b>	Offers solutions that provide the ability to see devices, including non-traditional devices, and connects to the network and enforce policy-based control of these devices	\$1,786
12/30/2019	<b>Broadcom</b>	<b>Bay Dynamics</b>	Offers a cyber risk analytics platform that analyzes cyber security related data collected by an organization, makes sense of the data, and communicates the risk insights to the right people to facilitate informed decision making	-
12/19/2019	<b>f5</b>	<b>Shape</b>	Developer of enterprise-based application security technology designed to defend the web and mobile applications and APIs from fraud, abuse and attack	\$1,028
11/25/2019	<b>Palo Alto Networks</b>	<b>Aporeto</b>	Develops cloud-native security solutions for deploying and operating cloud-native applications that focus on machine-based micro-segmentation	\$150
11/3/2019	<b>Proofpoint</b>	<b>Observe It</b>	Threat management platform focused on endpoint agent and data risk analytics	\$225
10/25/2019	<b>Fortinet</b>	<b>enSilo</b>	Developer of a comprehensive endpoint security platform designed to combine next-generation antivirus with post-infection data protection capabilities	-
10/14/2019	<b>Thoma Bravo</b>	<b>Sophos</b>	Provides cloud-enabled end-user and network security solutions primarily focused on the securitization of end-point assets	\$3,925
8/22/2019	<b>VMware</b>	<b>Carbon Black</b>	Provides security solutions in the United States and internationally. Its security cloud platform captures, records, and analyzes unfiltered endpoint data	\$2,060
8/8/2019	<b>Broadcom</b>	<b>Symantec</b>	Offers Norton security solutions as a subscription service providing protection for devices against malware, viruses, adware, and ransomware on various platforms; and LifeLock identity theft protection solution that provides identity monitoring	\$10,700

Source: CIQ; Pitchbook; Equiteq Analysis

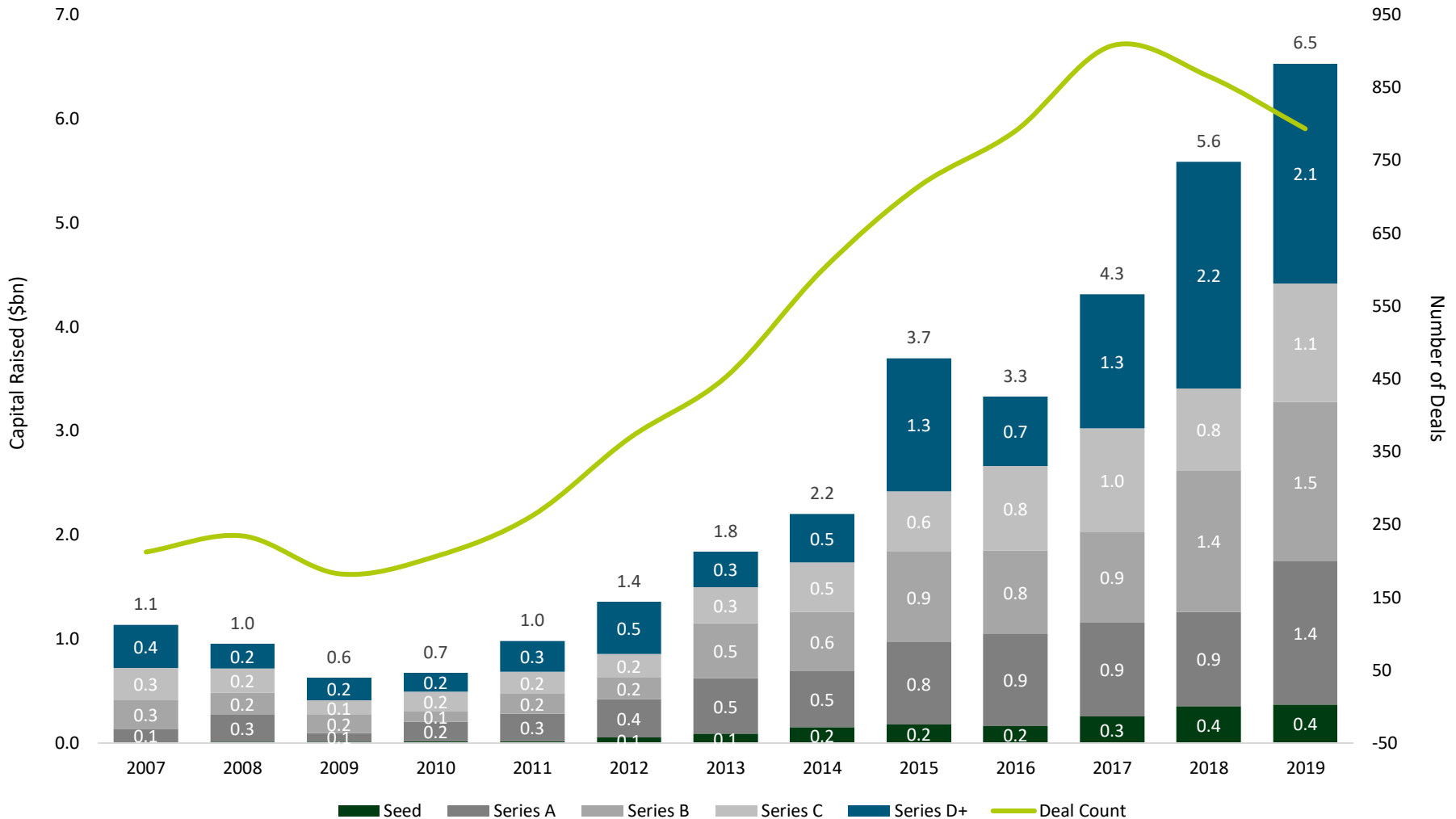
# Selected Capital Raises

Date	Financial Sponsor	Target	Transaction Overview
2/20/2020	<b>Coatue Management, Insight Venture Partners</b>	<b>OneTrust</b>	OneTrust has received \$210mm in its series B round of funding co-led by existing investor, Insight Venture Partners, and new investor, Coatue Management
1/9/2020	<b>Ballast Point Ventures</b>	<b>Abacode</b>	Abacode received \$5mm in a round of funding led by new investor Ballast Point Ventures. The transaction also included participation from other investors. Sean Barkman of Ballast Point Ventures L.P. joined company's board of directors
12/5/2019	<b>Costanoa Venture Capital, Crane Venture Partners, Vertex Ventures</b>	<b>Cyberhaven</b>	Cyberhaven raised \$13mm in its series A round of funding co-led by Vertex Ventures and Costanoa Venture Capital
11/25/2019	<b>Alsop Louie Partners, CIT, Inner Loop Capital, Working Lab Capital</b>	<b>RunSafe Security</b>	RunSafe Security issued 10,795,138 series A preferred shares at a price of \$0.84 per share for gross proceeds of \$9mm
11/14/2019	<b>Accel Partners, Slack Fund, WndrCo Holdings</b>	<b>1Password</b>	1Password received \$200mm in its series A round of funding led by new investor Accel Partners. The transaction also included participation from new investors Slack Fund and WndrCo Holdings
11/12/2019	<b>Signalfire</b>	<b>CloudVector</b>	CloudVector raised more than \$5mm in its seed round of funding led by new investor Signalfire. The transaction also included participation from other investors
11/6/2019	<b>Arthur Ventures, Build Group, Gula Tech Adventures</b>	<b>Cybrary</b>	Cybrary received \$10mm in funding. The company issued convertible preferred shares in the transaction and issued securities pursuant to exemption provided under Regulation D
7/29/2019	<b>Intel Capital</b>	<b>Trinity Cyber</b>	Security startup Trinity Cyber raised \$23mm in funding from Intel Capital to build out a service it claims is an entirely new approach to cybersecurity: stealth interception of external threats
7/11/2019	<b>Insight Venture Partners</b>	<b>OneTrust</b>	OneTrust received \$200mm in its series A round of funding led by new investor Insight Venture Partners
6/12/2019	<b>Elephant Partners, KKR, TenEleven Ventures</b>	<b>KnowBe4</b>	KnowBe4 issued 1,270,379 convertible preferred shares at issue price of \$236.15 per share for gross proceeds of \$300mm

Source: CIQ; Pitchbook; Equiteq Analysis

# VC Funding for Cyber Security Companies

Total VC funding for cyber security companies increased 17% YoY to reach \$6.5bn in 2019 while funding per deal increased 28% over the same period indicating significant interest for new players in the space



Source: Pitchbook; Equiteq Analysis

# Equiteq

*Growing equity, realizing value*

***New York – London – Paris – Singapore – Sydney***

122 East 42nd Street, Suite 3500

New York, NY 10168

Phone: (212) 256-1120

[www.equiteq.com](http://www.equiteq.com)



*Securities offered through Equiteq Securities LLC, member FINRA/SIPC.*