

Information Security

Q2 2020





Contents

Q2 2020 news and updates	3
Executive summary	4
Key takeaways	6
Leading use cases for AI & ML in infosec	7
VC activity	11
Infosec market map	12
Segment deep dives	13
Network security	13
Application security	26
Data security	38
Identity & access management	47
Endpoint security	58
Security operations	70
Supplemental materials	81

Contact

Research

Brendan Burke

Senior Analyst, Emerging Technology
brendan.burke@pitchbook.com

Data

Matthew Nacionales

Data Analyst

Design

Mara Potter

Junior Graphic Designer

Caroline Suttie

Junior Graphic Designer

This Emerging Technology Research report is updated on a quarterly basis to reflect changes in venture capital deal activity and other market related updates deemed valuable by the research analyst.



Q2 2020 news and updates

VC ACTIVITY

- Infosec companies raised \$1.9 billion in VC funding across 104 deals in Q2 2020, continuing strong deal flow.
- Q2 2020 deal value was driven by large deals in the identity & access management, data security, and security operations segments, which typically lag network security and endpoint security in funding.
- Deals with disclosed valuations featured loftier median early- and late-stage VC valuations, though a lower proportion of valuations were disclosed relative to 2019.
- COVID-19 has caused a flight to quality in infosec, with more late-stage VC deals than early-stage deals completed in 2020 through H1.

Q2 2020 M&A ACTIVITY

- VC exit activity remained weak in Q2, with only 14 deals and \$173.0 million in disclosed deal value, both the lowest quarterly results since Q4 2016.
- **Microsoft's** \$165.0 million acquisition of IoT security vendor **CyberX** led the quarter's M&A activity; this valuation suggests continued shakeout in IoT security due to **CyberX's** high level of VC funding.
- **VMware** and **Zscaler** completed tuck-in cloud security acquisitions in Q2, demonstrating that incumbents are searching for bargains in key product categories.

NEWS

- **June 17: Palo Alto Networks** announced three new products—a next-generation firewall embedding machine learning, cloud container firewalls, and an IoT security platform. These new products leverage recent acquisitions and are indicative of the priority areas for the company's customer base.
- **June 2:** Hacker organization REvil began auctioning stolen data on the dark web, a sign that the prolific ransomware group may present additional business risk along with the threat of ransom payments.
- **May 19:** The 2020 Verizon Data Breach Investigations Report found that the leading threat actions across 2,907 data breaches were phishing, credential theft, data misdelivery, and misconfiguration.¹

1: "2020 Data Breach Investigations Report," Verizon, 2020.

A NOTE ON COVID-19

We believe COVID-19 is not substantially hurting security department budgets. One survey indicates that only 12% of security leaders are decreasing their budgets, while 26% of both enterprise CISOs and SMBs are planning to increase their security budgets.² We believe macro business challenges have not compromised security budgets, and this stability had led to continued growth opportunities. Security startups are adapting to the shifting priorities of security leaders, emphasizing secure service edges for remote work, insider threat detection, and third-party risk management.

2: "The CISO Current Report Q2, 2020," YL Ventures, 2020; "Business survey 2020," Analysys Mason, 2020.



Executive summary

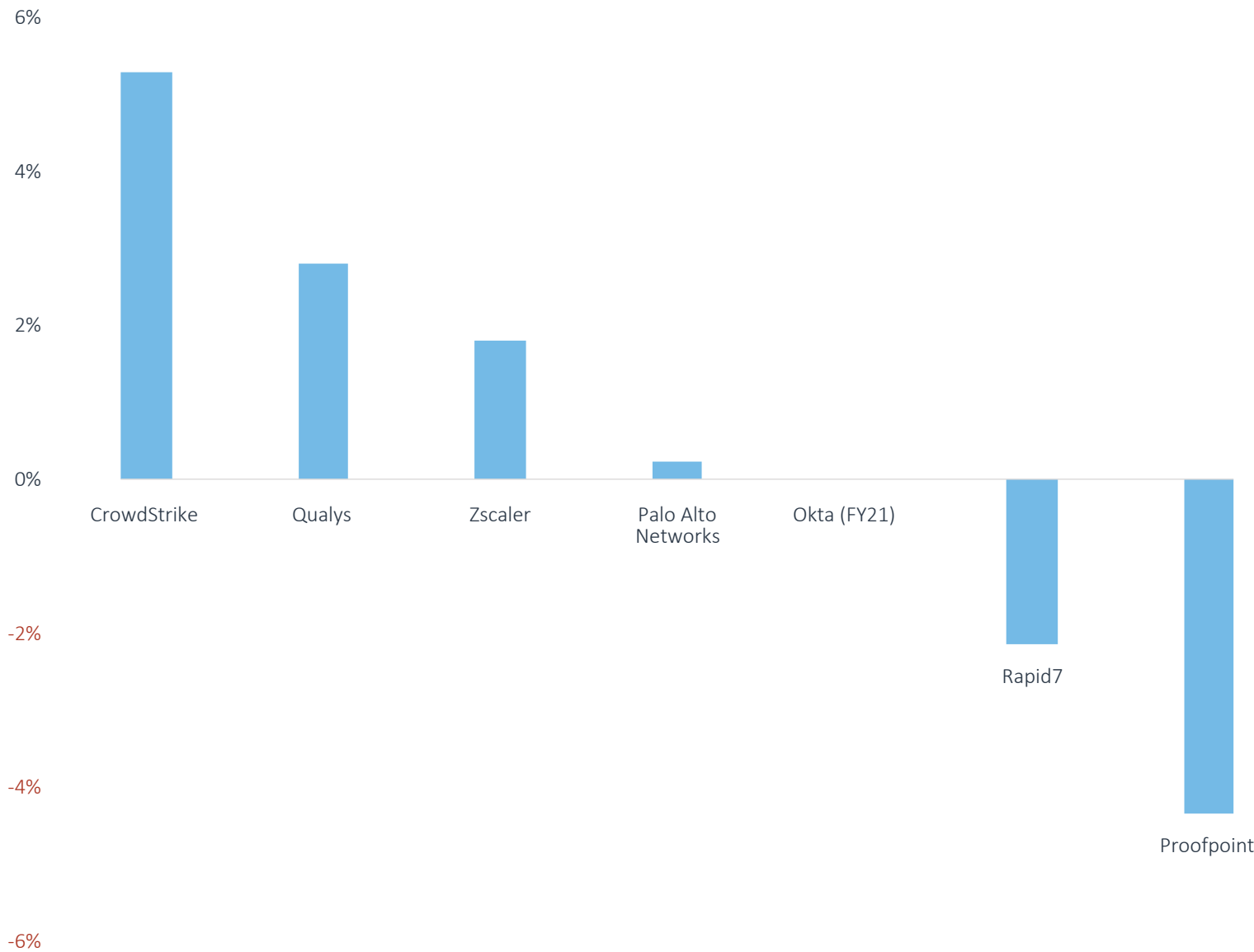
Information security (infosec) refers to technology and services that protect enterprises from digital threats to business operations.³ The infosec industry evolves constantly as new threats arise, generating innovation opportunities for legacy vendors and startups alike. As the industry is principally concerned with the protection of enterprise data, infosec has become a subset of enterprise SaaS that is increasingly delivered through the cloud with a subscription business model. We believe this shift has made the industry more resilient to economic downturns, since customers are locked into recurring revenue contracts and face high switching costs. For this reason, we believe that, despite the COVID-19 crisis, growth will likely continue in security software in 2020.

Leading infosec incumbents have maintained or improved their revenue forecasts for 2020 as of Q1 earnings despite the COVID-19 pandemic. This includes **CrowdStrike**, **Zscaler**, **Qualys**, and **Palo Alto Networks**. Even companies that decreased their revenue forecasts maintained positive growth forecasts for the full year, suggesting that infosec has a better outlook than IT overall. In our sample, only Fortinet withdrew its forecast. In addition, many companies were able to maintain revenue growth through Q1 2020. We believe infosec companies are experiencing increased demand for their products as a result of digital transformation, reflecting further enterprise security budget growth and positioning them to continue M&A in strategic areas.

We estimate the infosec vertical to be a \$124.0 billion market in CY 2020, a flat total YoY, and expect strong growth to resume in 2021. While this estimate may fall short of others, most market size estimates include firewall equipment, consumer security, and other product segments with limited disruption potential. Our estimate includes the \$70.2 billion

³: The term “infosec” is interchangeable with the PitchBook platform’s cybersecurity vertical. Infosec is more commonly used by practitioners in the enterprise market, while cybersecurity may apply to governments as well.

Figure 1.
Change in 2020 revenue guidance for public information security vendors (Q4 2019-Q1 2020)



Source: Company 10-Q disclosures



EXECUTIVE SUMMARY

managed security services market, which we expect will cede market share to software over the next five years. Based on these estimates, we anticipate this market will grow to \$162.6 billion by 2023 at a 9.5% CAGR in a coronavirus-induced recession scenario. Some segments may face decreased spending in 2020, though other segments are likely to sustain their growth trajectories, including network security, endpoint security, and data security. We expect a recovery would drive demand for infosec technologies to defend broader enterprise surface areas including home networks, multi-cloud environments, and mobile device networks, benefiting longer-term investments in application security, network security, data privacy, and identity & access management.

PE firms had a slow second quarter, with only one buyout completed. We believe, however, that they are positioned to take advantage of discounted infosec assets in a recovery. The most active infosec PE firm, Thoma Bravo, has nearly \$10.0 billion in PE dry powder as of September 30, 2019, suggesting that the firm will be able to continue conducting substantial buyouts when there is a clearer economic outlook. We believe Thoma Bravo, Warburg Pincus, Francisco Partners, and TPG Capital are actively pursuing platform strategies in the space. PE firms are well positioned to conduct buyouts of infosec assets at decreased valuations.

COVID-19 has caused a flight to quality in infosec, with more late-stage VC deals than early-stage deals completed through H1 2020 and resilient deal value. Overall, our thesis that infosec will outperform enterprise SaaS in fundraising is on pace to be correct, with H1 2020 achieving 60% of the total deal value realized in 2019, compared to 56% for B2B technology more broadly as shown in our Q2 2020 PitchBook-NVCA Venture Monitor.

Given the sophistication of the enterprise infosec buyer—typically a company’s Chief Information Security Officer (CISO)—the industry is segmented based on the product

types most commonly required when protecting the enterprise. Each segment carries unique competitive dynamics and market opportunities and reveals a variety of growth opportunities in this industry. We segment the venture ecosystem into the following categories:

- Network security
- Application security
- Data security
- Identity & access management
- Endpoint security
- Security operations

These segments naturally overlap in an enterprise network, though vendor technologies typically operate at one of these layers. For example, an identity & access management platform may be used to protect a mobile app if it grants access to the app for certain users but would not be considered an application security company because it does not specifically address vulnerabilities within the application codebase. Due to the unique challenges of each layer of the stack, infosec companies typically specialize within one of these segments and integrate with other point solutions to provide comprehensive security. Enterprises then build a stack of point solutions from each of those categories, creating redundancies at each layer. For this reason, we believe diversified investment portfolios can be built within infosec addressing each segment of the market.



Key takeaways

Emerging threat surfaces are driving enterprise demand for infosec innovation. Emerging enterprise technologies carry unique vulnerabilities that attackers can exploit. As a result, each infosec segment has opportunities in protecting emerging threat surfaces including:

- Cloud-native applications and databases
- IoT/operational technology devices
- Third-party technology vendors
- Remote employee devices

Secondary opportunities exist in mobile security, web security, and email security, all of which have become more important due to COVID-19. Due to these emerging risks, startups are increasingly focused on individual threat surfaces. Simultaneously, incumbents are building comprehensive secure network architectures, commonly referred to as SASE (secure access service edge), that can defend the full scope of cloud-native and distributed endpoints and filling gaps in their product suites via M&A. We believe startups targeting these vulnerabilities can become market leaders, even as incumbents race to improve their own capabilities.

The “shift left” opportunity has materialized and may create multiple unicorns. We believe this “shift left” in application security (i.e. introducing security software at the beginning of application development instead of a final step in the process) has the potential to open a new market. The shift left can help startups compete against incumbents’ unified platforms that address the full extent of network and endpoint vulnerabilities. We believe adoption rates of DevOps-friendly security tools are improving as developers identify user-friendly tools through open-source business models. Given the increasing relevance of container and serverless security

to application performance, developers are looking for security integrations for their code bases and migrating to open-source or open-core solutions. The recent VC mega-deals (\$100 million+) for **Snyk** and **SentinelOne** demonstrate the potential for valuation growth in this niche.

Security teams require optimization through security tool orchestration and alert correlation. Security teams are often understaffed and overworked due to the high number of alerts flooding enterprises. Tool sprawl has led to an average of 75 security tools being used at an enterprise, with nearly each one generating frequent alerts and requiring configuration and policy management (see security operations industry drivers on page 72). Network traffic analysis and application security tools are emerging as the next wave of tool sprawl, further challenging security teams, operations teams, and developers to manage an entirely different set of alerts for vulnerabilities in runtime applications on distributed networks.

Investors should exhibit caution when evaluating the product-market fit of infosec startups. The primary security risks enterprises face are credential theft, phishing attacks, and web application injection attacks.⁴ While organizations can address these problems without AI threat detection and dark web activity tracking, many startups tend to market these kinds of aggrandized solutions and do not directly address market needs for more basic enterprise security functions. For growth-stage companies, we believe a focus on operational problems within security teams—which generally pertain to security log management and interaction with other business units (including developers)—can best enable scale. This report introduces the key problem areas in infosec and maps out the most highly funded VC-backed companies in each. We expect the segments that address the most urgent problems for security teams to perform the best going forward.

4: “2019 Data Breach Investigations Report,” Verizon, May 2019



Leading use cases for AI & ML in infosec

Role of AI & ML in recent outlier security exits

Artificial intelligence and machine learning (AI & ML) have become commonplace in infosec startup pitches, with varying commercial results based on the application of the technology. We believe ML has become a substantial value driver for security startups and has been a common denominator for outlier security exits in endpoint security, application security, and security operations (see Figure 2 at right). Our Q1 2020 Emerging Tech Research: Artificial Intelligence & Machine Learning report highlights the role of ML in **CrowdStrike**’s upward margin migration and eventual outstanding growth trajectory and public performance. More broadly, our research has found that advanced approaches to AI & ML in specific data-rich use cases have been a common denominator in recent unicorn exits, showing infosec to be one of the leading applications of AI & ML in the modern enterprise. These exits have been unevenly distributed across segments, demonstrating that some security datasets are better suited to effective AI & ML approaches than others.

Outstanding exits for ML-integrated infosec vendors have occurred in endpoint security, application security, identity & access management, and security operations. In endpoint security, **Cylance**, **CrowdStrike**, and **Armis** have collected massive datasets of endpoint device behaviors and file types that can be used to train ML models. In particular, malware classification has emerged as a use case for which Big Data is available and

Figure 2.
Recent ML-integrated infosec VC exits

COMPANY	CLOSE DATE	SEGMENT	EXIT SIZE (\$M)	ACQUIRER/ INDEX	VALUATION STEP-UP
Armis	February 11, 2020	Endpoint security	\$1,100.0	Insight Partners, CapitalG, DFJ Growth	N/A
Shape Security	January 24, 2020	Identity & access management	\$1,000.0	F5 Networks	14.3x*
Twistlock	July 9, 2019	Application security	\$378.1	Palo Alto Networks	27.3x**
CrowdStrike	June 12, 2019	Endpoint security	\$6,075.4	NASDAQ	22.4x
Demisto	March 28, 2019	Security operations	\$560.0	Palo Alto Networks	46.7x**
Cylance	February 21, 2019	Endpoint security	\$1,400.0	Blackberry	10.8x*

Source: PitchBook, *company disclosures, **Hampton Partners



LEADING USE CASES FOR AI & ML IN INFOSEC

ML can produce accurate estimates. **Cylance** employs deep neural networks while **Armis** and **CrowdStrike** use more limited ML approaches such as gradient-boosted trees and statistical models. In other segments, startups have leveraged large datasets of security alerts (**Demisto**), application behavior (**Twistlock**) and online fraud attempts (**Shape Security**). ML integration has been a necessary but insufficient condition for billion-dollar exits in infosec in recent years.

ML has not yet contributed the same level of outcomes in network security and data security, suggesting ML may have varying applications across different layers of the security value chain. Fundamentally, AI & ML are best applied in use cases where automation can be driven via the use of robust training data, and we observe automation to have varying satisfaction among security teams. Not all datasets are equal as some data must be updated on a continuous basis to build new features. Since hackers are constantly innovating novel attacks against emerging threat surfaces, we believe adversarial behavior data is a perishable data source. As a result, AI & ML has been met with dissatisfaction and low usage in threat intelligence and detection. In the SANS Institute's Cyber Threat Intelligence survey, ML for threat intelligence produced dissatisfaction for 58% of security professionals. We believe this stems from the shifting approaches of adversaries, which makes attacker behavior challenging to predict via ML models. While specific file-based attacks and common attack patterns can be predicted via ML, developing novel insights into new types of attacks can be a limitation for weak ML approaches.

AI & ML priority areas

While AI & ML is not the only way to automate security functions, we believe that the automation priorities for security leaders can be promising areas for AI & ML applications. Industry surveys reveal that security teams' highest priority for automation is the reduction of alert fatigue. The top three automation requirements identified by SANS Institute survey on automation are directly related to improving the handling of alerts and incidents including workflow automation, threat investigations, and threat data correlation (see Figure 3 on page 9).⁵ A Capgemini survey found that over 80% of security leaders use AI for threat detection and prediction.⁶ These functions are most commonly addressed by endpoint detection & response, SIEM, and SOAR platforms. We believe AI is best applied to measure network activity baselines to help identify anomalous behavior and previously identified attacker behaviors. The high penetration of AI technologies in this niche can benefit new entrants with innovative approaches to data collection and correlation.

Among startups, the development of graph databases is generating outstanding technical outcomes. Graph databases use ML to find correlations between data points and label data for predictive analytics. In security, graph databases are used to correlate the activity across an organization's endpoints to malicious activity. **CrowdStrike**'s graph database has been used to crowdsource billions of events per day into a cloud-based endpoint detection model that can be applied to new customers. In Q2 2020, **Cybereason** leveraged its graph database to achieve the highest rating in endpoint protection platforms in leading

5: "2020 SANS Automation and Integration Survey," SANS Institute, May 2020.

6: "Reinventing Cybersecurity with Artificial Intelligence," Capgemini Research Institute, July 2019.



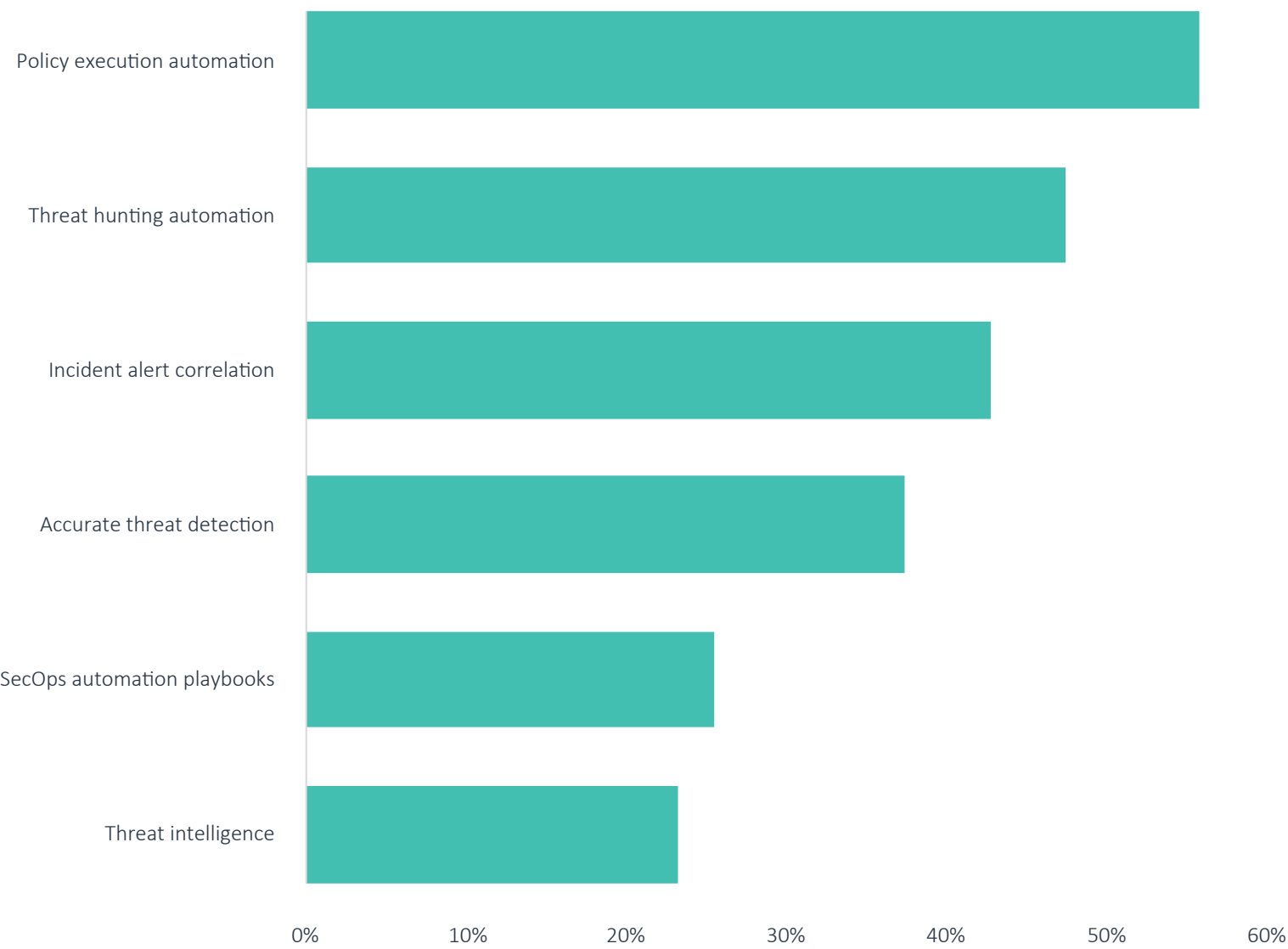
LEADING USE CASES FOR AI & ML IN INFOSEC

testing firm **NSS Labs**’ Advanced Endpoint Protection comparative test, including best-in-class performance on complex attacks such as phishing and targeted malware. While other vendors in this test use AI & ML, **Cybereason** has been able to generate outstanding performance based on an ML-first graph database approach, positioning it to capture market share in endpoint protection, much as **CrowdStrike** has in endpoint detection & response.

Critically, we believe AI & ML systems are better able to determine predictive relationships from defender data rather than attacker data. Enterprise traffic’s predictable flows can be compared to known attacker behavior and clear anomalies. Some retuning of models must occur as enterprise perimeters expand, but we believe the expansion of computing power and flexibility of graph databases can enable AI & ML to continuously learn from the patterns of the enterprise itself, rather than the attackers outside the enterprise. AI-first startup **Darktrace** is shifting to this approach with its AI Cyber Analyst product.

Some startups have been able to outperform based on the level of AI & ML innovation in their architecture. Many startups claim to embed AI & ML without incorporating innovative approaches to data collection, instead relying on existing databases that may not be optimized for AI & ML. Furthermore, AI & ML does not always play a core role in the correlation of threat data and automation of responses, serving instead as an optimizer for analytics in narrow use cases. Figure 4 on page 10 outlines the use cases in which we believe sufficient data exists to power impactful AI & ML applications along with examples of leading startups with genuine AI & ML innovation.

Figure 3.
Leading infosec automation priorities (% of respondents)



Source: "2020 SANS Automation and Integration Survey," SANS Institute, May 2020
Note: N = 1,060 security professionals



INDUSTRY OVERVIEW: LEADING USE CASES FOR AI & ML IN INFOSEC

Figure 4.
Leading AI & ML use cases in infosec and representative startups

Network security	Application security	Identity & access management	Data security	Endpoint security	Security operations
Network intrusion detection Darktrace Vectra ExtraHop IronNet Blue Hexagon MixMode	Cloud workload runtime protection automation Aqua Security vArmour StackRox	Fraud prevention Riskified Signifyd Sift Forter Ravelin Fraugster	Data mapping BigID Egnyte Securiti.ai Nightfall	OT/IoT device behavior baselining Ordr Bastille Networks AdaptiveMobile	Risk scoring SecurityScorecard Kenna Security CYR3CON
				Anti-phishing automation Ironscale Inky PhishCloud	Security orchestration, automation & response (SOAR) Simplify LogicHub
	Bot detection PerimeterX Salt Cequence Security			Malware detection SentinelOne Cybereason Deep Instinct	Security log correlation Sumo Logic Exabeam BigPanda Stellar Cyber

Source: PitchBook

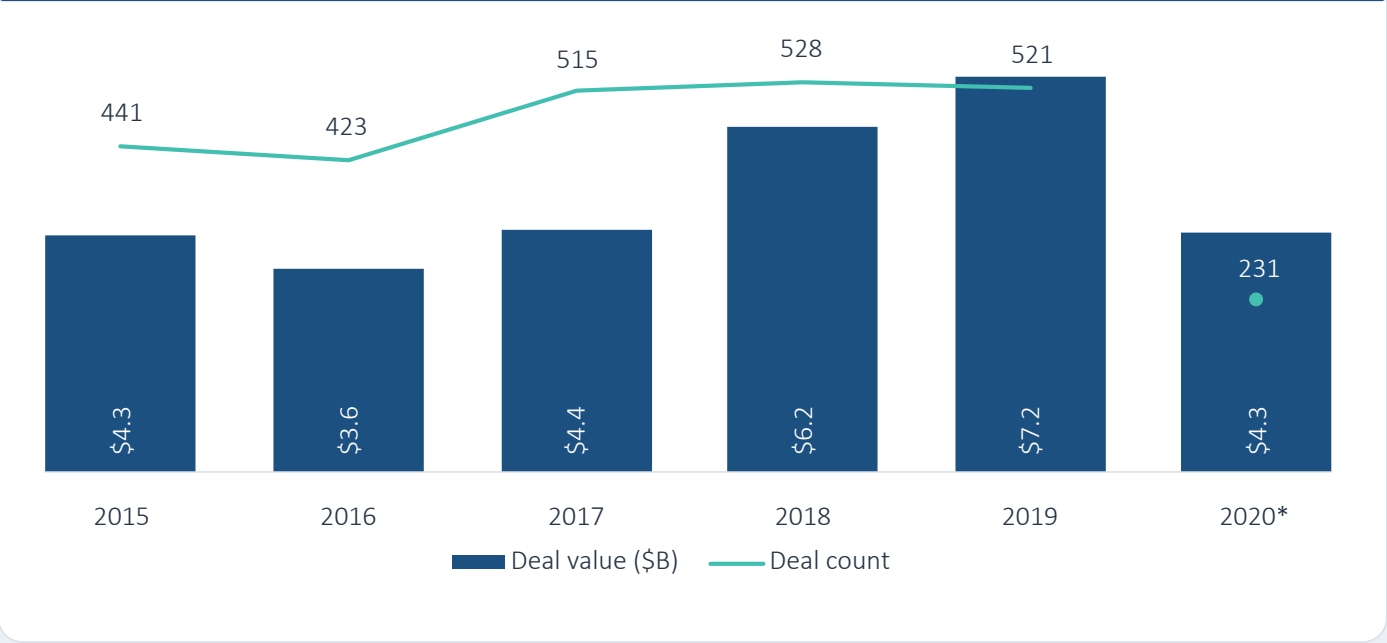


VC activity

Infosec companies raised \$1.9 billion in VC funding across 104 deals in Q2 2020, continuing strong deal flow in the face of the pandemic. We have not observed a significant drop in deal value because of COVID-19, demonstrating the resilience of the vertical to economic pressures. Deal value in Q2 2020 was driven by large deals in identity & access management, data security, and security operations, segments that typically lag network security and endpoint security in funding. Identity & access management deal activity has been driven by innovation in both fraud prevention and identity governance & administration, while security operations has primarily been driven by security risk assessment & management. In H1 2020, 86 late-stage deals were completed compared to 82 early-stage deals and 63 seed deals. In no previous year have late-stage deals been the leading source of deal flow. Q2 2020 maintained high deal value across a decreasing number of deals, with VC investment on pace to exceed 2019’s record total.

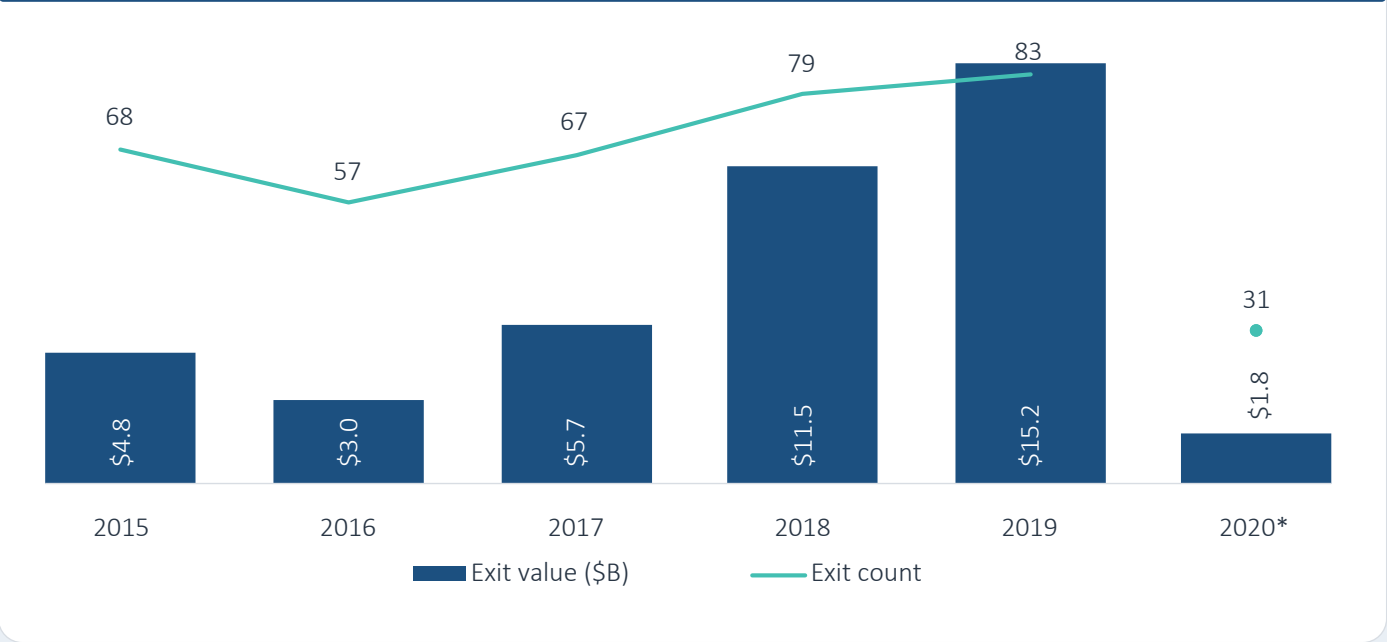
VC exit activity remained weak in Q2, with only 14 deals and \$173.0 million in disclosed deal value, both the lowest recordings since Q4 2016. The leading acquisition of the quarter was **Microsoft**’s \$165.0 million acquisition of IoT security vendor **CyberX**, a valuation that indicates a continued shakeout in IoT security. **CyberX** raised \$47.8 million before exiting, suggesting its exit was at a flat or down valuation. **Microsoft** has an established strategy in IoT security via its Azure Sphere product line yet continued the trend of acquisitions under \$200.0 million in IoT security, with the notable outlier of **Armis**. Tuck-in acquisitions were made in cloud security by **VMware** and **Zscaler**, demonstrating that incumbents are searching for bargains in key product categories benefiting from the remote work transition. PE and M&A deal counts fell in Q2, but we expect to see a rebound in those categories that will likely strongly affect infosec. The lack of investor focus on early-stage VC deals may create a shakeout in vendors in the industry once M&A activity resumes.

Figure 5. INFOSEC VC DEAL ACTIVITY



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Figure 6. INFOSEC VC EXIT ACTIVITY



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Infosec market map



Companies included are VC-backed, segmented by primary use case, and sorted by total capital raised.

SEGMENT DEEP DIVE

Network security



NETWORK SECURITY

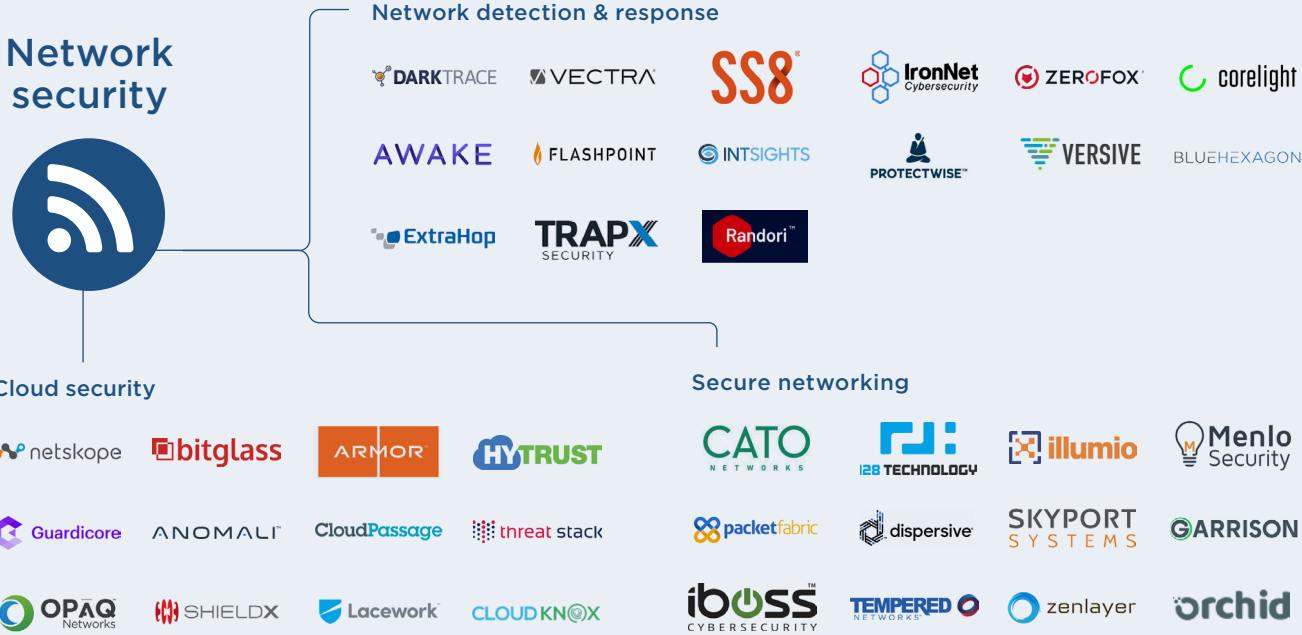
Overview

Network security includes software and hardware that protect enterprise network infrastructure from digital attacks. It focuses on the traffic entering the enterprise perimeter and moving laterally among network nodes. Components of network infrastructure that can be vulnerable to attack include:

- Servers
- On-premise and remote wireless networks
- Cloud environments
- Firewalls
- Routers and switches

The growth of cloud environments and remote networks have created new surfaces for attackers to target, driving innovation in network security. As a result, network security solutions increasingly provide protection for data at rest and in transit within hybrid and multi-cloud-based environments, as well as for data delivered through SaaS applications. For this reason, we expect the network security space to continue to grow through the pandemic-related crisis.

Enterprise perimeters are increasingly amorphous as employee devices are spread over diffuse wi-fi networks and legacy IT approaches are insufficient to ensure business continuity. Secure networking is essential for remote work, since employees must be able to gain access to cloud servers securely. Existing VPN solutions have performance issues and struggle to scale. Enterprises are shifting resources to the cloud, requiring companies to offer additional cloud security and network segmentation to securely facilitate the transfer.





NETWORK SECURITY

Subsegments include:

Cloud security: Software platforms and services that defend against breaches of public cloud environments. This subsegment includes the following technologies:

- Cloud access security brokers (CASBs)
- Cloud security posture management (CSPM)
- Cloud-based secure web gateways

Network detection & response: Platforms that detect risk exposure at the network level and identify threat actors attempting to breach the enterprise perimeter. This subsegment includes the following technologies:

- Network traffic analysis
- Threat intelligence platforms
- Network security policy management
- Network sandboxing
- Intrusion detection & prevention systems
- Network penetration testing tools
- Vulnerability assessment

Secure networking: Software-based secure network architectures beyond conventional firewalls and networking equipment including the following technologies:

- Secure web gateways
- Next-generation firewalls
- Software-defined wide-area networks (SD-WAN)
- Virtual private networks
- Browser isolation

Industry drivers

Shared responsibility for cloud security: The shift to cloud infrastructure requires an enhanced network security posture, as cloud providers do not take responsibility for customer data. Cloud hosts take responsibility only for security “of the cloud” while customers must secure all data “in the cloud.” AWS, for example, has a shared responsibility model for security, tasking the cloud customer with responsibility and management of the guest operating system, other associated application software, and the configuration of the AWS cloud firewall.

Prevalence of multi- and hybrid cloud environments: Hybridization of cloud environments and a trend toward multi-cloud strategies are creating new security complexities. One study shows that enterprises with a hybrid strategy combining public and private clouds grew from 51% in 2018 to 58% in 2019.⁷ Security is the third-most prevalent challenge with cloud deployments.

Malware delivery automation: Hackers are continuously increasing their activity, automating delivery of malware and responding quickly to new network vulnerabilities. In

7: “2020 State of the Cloud Report,” Flexera, 2020.



NETWORK SECURITY

2019, hackers infiltrated more than 17,000 websites by automatically scanning for exposed AWS S3 buckets with a technique called Magecart. Additionally, research has detected increasing automated attacks on cloud infrastructure with the intent of installing crypto-mining software.⁸

Market size

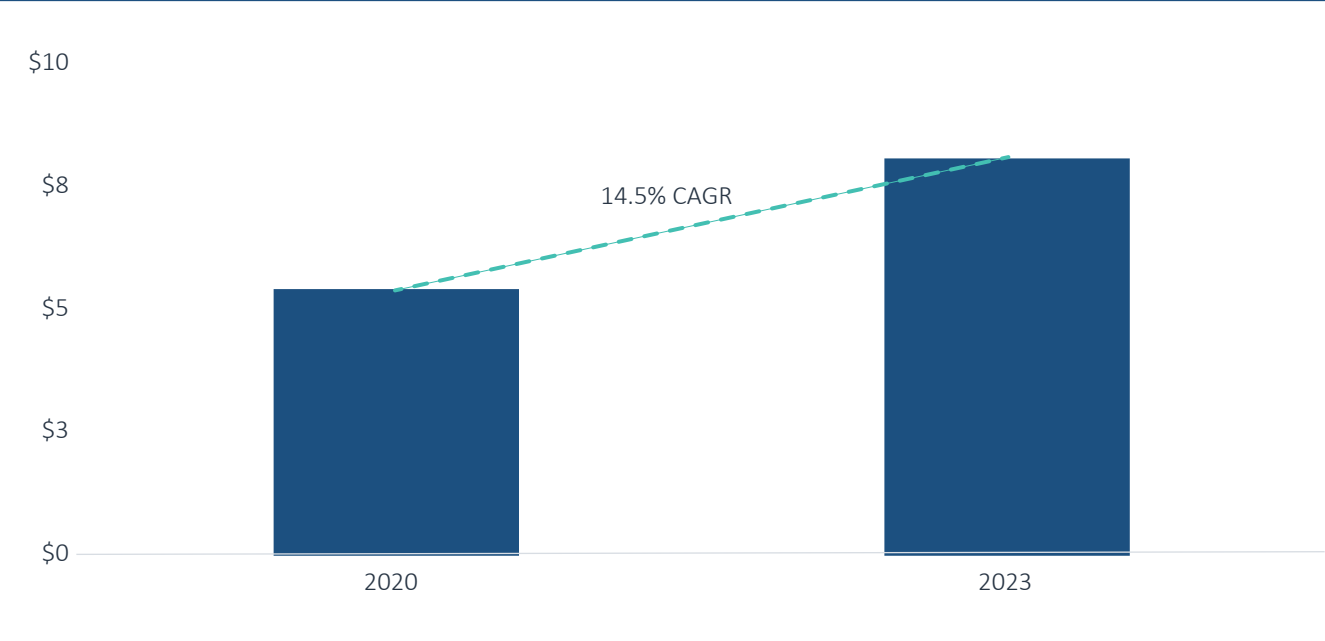
We estimate the network security market to be \$5.4 billion as of 2020. This market size includes CASBs, secure web gateways, and threat intelligence, and it excludes network firewall hardware and legacy intrusion detection systems. We forecast network security to grow more quickly than the overall infosec market at a 14.5% CAGR to an \$8.1 billion market in 2023, after accounting for flattened growth in 2020 resulting from the pandemic. We expect high growth to resume in 2021 as enterprises begin to invest in new IT infrastructure in a recovery scenario. Cloud security is still a small niche within network security, but we estimate it will be among the highest-growth infosec subsegments over the next three with a 38.9% CAGR. We believe enterprises will invest in network security as part of their remote workforce strategies.

Disruption potential

Startups can seize market share in network security from legacy firewall vendors, though all vendors in the space are adapting to cloud-based environments. We believe that **Symantec** lost market share in Secure Web Gateways in 2019 and both ZScaler and **Cisco** substantially improved their market positions from 2018 to 2019. This suggests

8: “Detecting Persistent Cloud Infrastructure/Hadoop/YARN Attacks Using Security Analytics: Moanacroner, X Bash,” Securonix, January 15, 2019.

Figure 7. NETWORK SECURITY MARKET SIZE (\$B)



Source: PitchBook | Geography: North America & Europe

Figure 8. COMMON INDUSTRY KPIS

Financial

- ARPU LTM
- Revenue mix (product/subscription/support)
- LTV/CAC

Operational

- Number of solutions purchased per customer
- Gartner magic quadrant
- Forrester Wave
- NSS security effectiveness
- NSS price performance



NETWORK SECURITY

that growth-stage technology companies can disrupt network security leaders but other public incumbents are improving their innovation in security. Furthermore, **Netskope** and **Bitglass** have become market leaders in the cloud access security brokers market as venture-backed companies, suggesting that startups may become leaders in burgeoning categories including cloud security posture management (CSPM) and network traffic analysis (NTA).

Business model

Network security products are typically bundled based on use cases including the following components:

- Fee per network user ranging from \$2 to \$30 for basic breach discovery and log management
- Maintenance and support costs
- Premium modules include mobile protection and data encryption
- One-time sales of infrastructure including Secure Web Gateways

VC activity

Network security had a weak quarter of VC deal activity, but the importance of secure networking to the overall infosec industry remained evident. We tracked only 12 deals and \$177.8 million invested in Q2 2020, the lowest quarterly totals since Q2 2018. Deal activity was led by **Cato Networks**, a secure SD-WAN vendor, which raised a \$77.0 million round

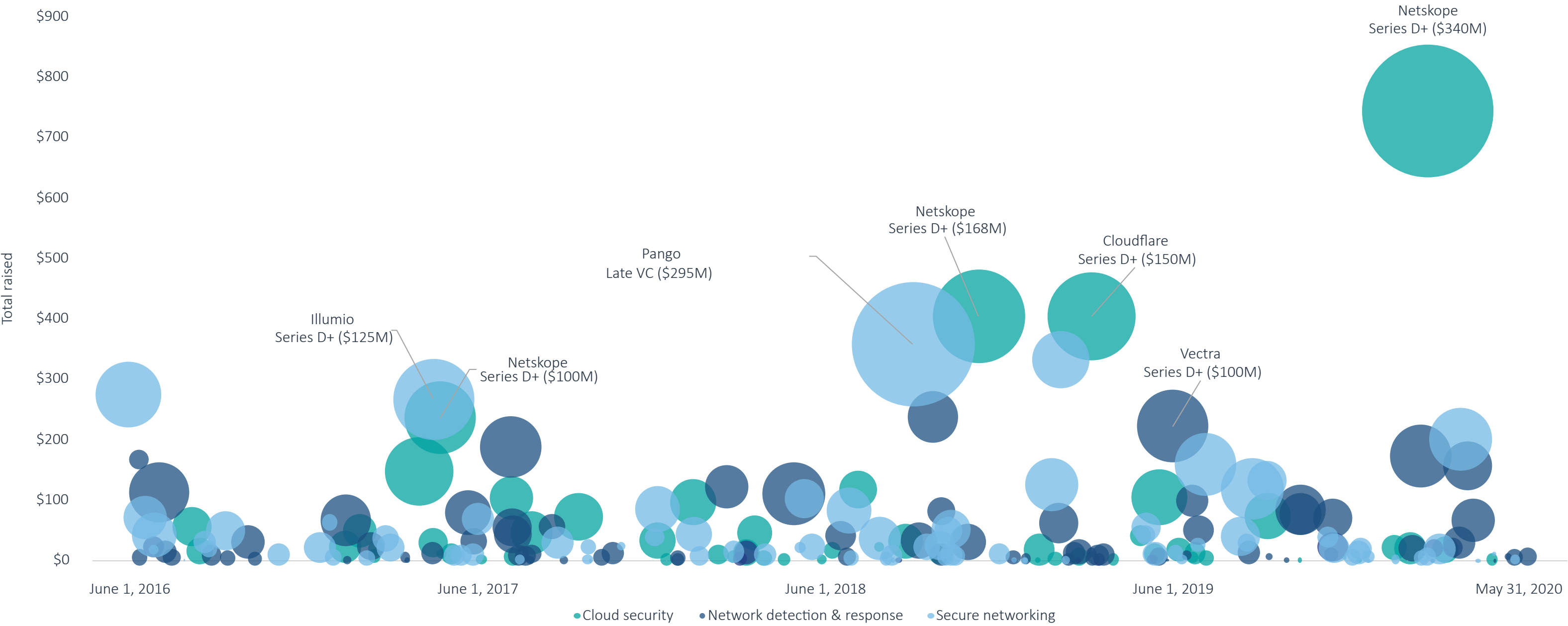
from prior investor Lightspeed Venture Partners and disclosed 220.0% bookings growth in 2019. **Cato Networks** stands to benefit from COVID-19 as security teams prioritize improving their remote work infrastructure. **Cato Networks** is facing stiff competition from **Cisco** and **Palo Alto Networks**, among others, but we believe the company has a competitive advantage in security architecture. Network detection & response showed weakness as **IronNet** had step-down from its latest round and secured PPP funding. **ExtraHop** also raised PPP funding, which suggests advanced network traffic analysis may be facing commercial challenges. We believe that while cloud security and secure networking are requirements in the current environment, network detection & response may be deferred, resulting in superior VC opportunities in the other two categories.

Network security VC exit activity remained muted; the only two VC exits in Q2 2020 were both acquisitions of cloud security startups by **Zscaler**. These purchases include **Cloudneeti**, an early-stage cloud security posture management startup, and **Edgewise Networks**, an early-stage secure networking startup. The early-stage nature of both companies at time of acquisition highlights the barriers to entry in the network security space. **Cloudneeti** supports configuration management for **Zscaler**'s existing public security product, while **Edgewise Networks** bolts onto **Zscaler**'s broader remote access product, enabling micro-segmentation of enterprise networks with zero-trust network access, a key functionality of emerging network architectures in remote work environments. These exits continue to reinforce our view that quality cloud security assets can be bought for under \$200.0 million, limiting upside potential for startups. There are numerous exit candidates in network detection & response, including **Darktrace**, **Vectra**, and **ExtraHop**. **Darktrace** is an IPO candidate that may have to delay its plans in the current economic environment.



NETWORK SECURITY

Figure 9.
Network security VC landscape (\$M)








Source: PitchBook
Note: The left axis indicates total VC raised as of deal date. Bubbles indicate amount raised.



NETWORK SECURITY

Figure 10.
Notable network security VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE (\$M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
 AWAKE	April 15, 2020	Network detection & response	\$35.6	Series C	Evolution Equity Partners	N/A
 netskope	February 27, 2020	Cloud security	\$340.0	Series G	Sequoia Capital	1.8x
 AXIADO	December 19, 2019	Secure networking	\$10.0	Early-stage VC	Orbit Venture Partners	2.6x
 corelight	October 17, 2019	Network detection & response	\$50.0	Series C	Accel, Insight Partners	2.3x
 128 TECHNOLOGY	September 12, 2019	Secure networking	\$30.0	Series D	N/A	1.1x

Source: PitchBook

Figure 11.
Notable network security VC exits






COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE (\$M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
 Cloud Conformity	October 21, 2019	Cloud security	\$70.0	Trend Micro	N/A	N/A
 Hillstone NETWORKS	September 30, 2019	Cloud security	N/A	N/A	N/A	5.4x
 CLOUDFLARE	September 13, 2019	Secure networking	\$3,875.2	NYSE	N/A	18.7x
 Meta Networks	May 7, 2019	Secure networking	\$120.0	Proofpoint	N/A	N/A
 REDSEAL	April 9, 2019	Cloud security	\$70.0	STG Partners	0.77x	N/A

Source: PitchBook



NETWORK SECURITY

Figure 12.
Key VC-backed network security companies





COMPANY	TOTAL VC RAISED (\$M)*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
 netskope	\$744.3	Cloud security	Next-gen Secure Web Gateway	Best-in-class DLP engine	Sequoia Capital, Accel, Lightspeed Ventures, ICONIQ Capital
 illumio	\$332.5	Secure networking	Adaptive Security Platform	Automatically detects anomalous attacks	JP Morgan Asset Management, BlackRock, General Catalyst, Andreessen Horowitz
 DARKTRACE	\$238.4	Network detection & response	Darktrace Antigena	Cloud-based AI threat detection	Vitruvian Partners, Insight Partners, KKR, Summit Partners, Talis Capital, Invoke Capital
 VECTRA	\$222.7	Network detection & response	Cognito platform	Automates security analysis of SaaS applications	TCV, Atlantic Bridge Capital, Accel, IA Ventures, Khosla Ventures
 CATO NETWORKS	\$202.0	Secure networking	Security as a service	All SD-WAN traffic decrypted and inspected	Lightspeed Ventures, Greylock Partners, Aspect Ventures, US Venture Partners
 ZEROFOX	\$173.4	Network detection & response	ZeroFOX Digital Risk Management Platform	Behavioral analytics for individual social media accounts	Intel Capital, Hercules Capital, Redline Capital Management, Silver Lake Management, Highland Capital Partners, NEA

Source: PitchBook | *As of June 30, 2020



NETWORK SECURITY

Figure 13.
Key network security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/REVENUE*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
 Symantec	Subsidiary of Broadcom	4.7x (acquisition multiple)	Cloud security, network vulnerability management & threat intelligence platforms	CloudSOC	Cloud service discovery and usage and policy violation
 McAfee	Owned by TPG Capital	N/A	Cloud security, network vulnerability management & threat intelligence platforms	McAfee Skyhigh Security Cloud	Cloud security posture management auditing and compliance
 Microsoft	NASDAQ: MSFT	10.7x	Cloud security, network vulnerability management & threat intelligence platforms	Microsoft Cloud App Security	Complex policies can be built with programming through a visual editor
 ORACLE	NYSE: ORCL	5.1x	Cloud security	Oracle CASB Cloud Service	Assesses SaaS and IaaS applications for common misconfigurations

Source: PitchBook | *As of June 30, 2020



NETWORK SECURITY

Opportunities

Network detection & response tools: A vendor survey indicates that the “new threats from existing threat actors” is the second leading area of increased spending behind cloud infrastructure.⁹ Network detection & response tools address new threats by installing sensors in network nodes to analyze network traffic and detect breaches using machine learning and behavioral analysis. Vendors can differentiate based on the level of remediation offered, since the alerts generated by these platforms typically require a SIEM platform to interpret and respond. IT teams can easily integrate them with existing network performance management solutions, leading to multiple insertion points within the IT organization. We believe **Darktrace**, **ExtraHop**, and **Vectra** can benefit from this trend with their machine learning-first approaches and face weak competition from incumbents including **Cisco**, **FireEye**, and **HPE**. **Darktrace** grew its revenue 79.0% to \$135.8 million in FY 2019, according to a Telegraph report.¹⁰ The category has been negatively affected by COVID-19 but is still approaching a \$1 billion market with strong YoY growth.

SD-WAN: Multi-cloud environments, third-party software vendors and IoT devices all introduce new risks to enterprise security. While on-premise firewalls are not well equipped to identify risks at the network edge and control access to the enterprise cloud, software-defined networks can solve this problem by identifying edge devices and isolating contaminated nodes from the broader network. Furthermore, IoT devices operate best within SD-WAN, which makes next-generation networks crucial for companies

deploying IoT at scale. SD-WAN can be deployed over large surface areas without routing traffic through hubs—increasing the efficiency of edge device communications—and can isolate compromised devices from other application traffic, improving the security of distributed endpoints. During COVID-19, enterprises are running into the limits of VPN capacity, which require employee communications to be routed to a central data center and then to the cloud. In response, companies are either upgrading their firewall capability or shifting to cloud-based SD-WAN. COVID-19 has hurt SD-WAN growth, decelerating from over 100% YoY in 2019 to nearly 20% as of Q2 2020.¹¹ Conventional SD-WAN relies on branch hardware that has faced supply chain challenges. We expect higher growth to resume in 2021. **Cato Networks** and **Zenlayer** have developed security-focused SD-WAN solutions that encrypt the tunnels between network locations, addressing the leading concern for this emerging architecture.

Cloud security posture management (CSPM): CSPM vendors provide software to help companies manage cloud deployments by detecting misconfigurations and implementing security policies across multi-cloud environments. While attacks on cloud security providers have not been proven to be more common than on-premise attacks, misconfiguring cloud deployments increases the risk of a breach. Research shows that nearly all cloud security failures stem from incorrect implementation policies related to cloud management, monitoring, and responsibility.¹² A recent vendor study has found that disclosed breaches attributed to cloud misconfigurations grew 42% YoY in 2019.¹³ Furthermore, cloud providers do not accept responsibility for customer data. Thus, although cloud providers offer security functionality, cloud customers must still utilize

9: Spends and Trends: SANS 2020 IT Cybersecurity Spending Survey, SANS Institute, Barbara Filkins and John Pescatore, January 28, 2020.

10: “Darktrace revenues top £100m ahead of coronavirus,” The Telegraph, April 2020

11: “STATFlash: How will COVID-19 impact SD-WAN?,” Vertical Systems Group, May 2020.

12: “Is the Cloud Secure?” Kasey Panetta, Gartner, March 27, 2018

13: “2020 Cloud Misconfigurations Report,” DivvyCloud, February 2020



NETWORK SECURITY

CSPM tools to ensure they configure their cloud deployments securely. Legacy security vendors may want to add CSPM technologies to their product suites, as evidenced by Trend Micro's recent acquisition of CSPM startup Cloud Conformity and **Rapid7**'s acquisition of **DivvyCloud**. Cloud security is the highest growth category in infosec and yet was only a \$500.0 million market in 2019.

Secure access service edge (SASE) platforms: The term "secure access service edge," first coined by Gartner, has become an explicit area of focus among organizations. Core components of SASE include:

- Wide area networks
- Secure web gateways
- Cloud access security brokers
- Cloud-native firewalls
- Zero trust network access

Fundamentally, these components represent a full shift in network security from on-premise firewalls to cloud-delivered security for distributed enterprise perimeters. This trend is disrupting a \$5.0 billion market in firewall appliance sales.¹⁴ Other estimates indicate that the enterprise penetration rate for a full stack of SASE solutions will increase from 5% in 2019 to 20% in 2023.¹⁵ As a result, we believe network security leaders including **Palo Alto Networks**, **Netskope**, and **Zscaler** are in the process of building full-stack SASE solutions via R&D and M&A, with **Zscaler** taking a lead in the category. **Palo**

14: Worldwide Quarterly Security Appliance Tracker, IDC, 2020

15: "The Future of Network Security Is in the Cloud," Gartner, August 2019.

Alto Networks' recent acquisition of **CloudGenix** for \$420.0 million was explicitly tied to improvement of their SASE capabilities, as the company shifts its product suite from firewall appliance sales to cloud-delivered security. We believe the competition to develop a full suite of solutions in this area is just beginning; the market is currently fragmented into vendors that specialize in one or two of the above categories, and vendors will continue with acquisitions to develop comprehensive capabilities. Furthermore, we believe COVID-19 will likely accelerate this trend as IT leaders replace on-premise firewall appliances.

Considerations

Innovative incumbents: The CASB market is saturated as incumbents aggressively buy and build solutions to maintain market share and relevancy despite disruptive challenges. The list of acquisitions in the CASB space is long and includes the following:

- **Palo Alto Networks**' acquisitions of Redlock and ShieldArc
- **Cisco**'s acquisition of **CloudLock**
- **McAfee**'s acquisition of Skyhigh Networks
- **Microsoft**'s acquisition of **Adallom**
- **Oracle**'s acquisition of Palerra
- **ProofPoint**'s acquisition of FireLayers
- **Symantec**'s acquisition of Blue Coat Systems
- **Forcepoint**'s acquisition of Imperva Skyfence



NETWORK SECURITY

Incumbents' willingness to innovate in this space should concern startups; they must move quickly if they are to stay far enough ahead to be considered for acquisition. We believe that large enterprise customers are more likely to opt for trustworthy leaders than disruptive startups in an uncertain economic environment. As infosec incumbents typically make acquisitions under \$500.0 million, their focus on this market can provide exit opportunities; however, it may limit upside potential for point solutions, which are less likely to file for an IPO. This could act as a headwind for highly funded cloud security startups.

Cloud providers crowding out startups: Cloud service providers are increasingly developing high-quality security tools for their customers to use in their deployments. **Microsoft**, Amazon, and Google have introduced data loss prevention (DLP) and security information and event management features to their public cloud environments that may compete with challengers such as **Netskope** and **Threat Stack**. While the limited liability of cloud providers for customer data will provide a compelling reason to deploy a third-party cloud security solution, cloud providers have a cost advantage in offering security services. We believe startups have not been able to scale cloud security posture management solutions due to competition with public cloud hosts and have sold at low valuations as a result.

Limited demand for advanced threat detection: By some estimates, 80% of attacks are conventional phishing attacks, yet many companies are designing threat hunting tools to track dark web activity and other sophisticated nation-state attacks. We believe this functionality may not achieve product-market fit at scale as discerning enterprises realize there is not a compelling ROI for advanced threat detection and as CISOs are more likely to allocate budget toward security operations and next-generation networking. We

believe that for startups such as **Darktrace**, **RiskIQ**, and **IronNet**, this product-market mismatch may contribute to limited demand.

AI & ML at a trough of disillusionment in the market: We believe CISOs and security engineers have low trust for AI-based solutions in the marketplace for several reasons. First, network-focused AI solutions often do not disclose their explainability, which refers to the transparency of the factors behind machine learning models. When users have visibility on the variables behind machine learning decisions, they can determine whether the model is adding value and tune the model to take actions in various scenarios. AI solutions on the market that do not offer explainability decrease their utility to security teams. Second, we believe AI-based solutions for unknown threat detection achieve well below 100% detection rates and have substantial false positive rates, creating reliability issues for security departments. Lastly, anomaly detection is not the ideal use case for AI or machine learning because, as novel network attacks are constantly developed, models trained on historical data can be inaccurate. We believe investors should be cautious of bold claims to detect zero-day threats with AI and should evaluate testing data on detection and false positive rates of those solutions.

Outlook

Network detection & response platforms to face valuation pressure because of COVID-19: We believe network detection & response platforms are facing higher churn than other technologies during COVID-19 because of unclear value propositions and false positive rates. Given the difficulty of attaining perfectly accurate detection of threats within network traffic, organizations may prioritize more practical SASE tools. At the



NETWORK SECURITY

company level, **ExtraHop** has gone through layoffs and raised PPP funding, and **Darktrace** faces corporate governance concerns around its co-founders' legal battles. Companies in this segment are investing heavily in R&D, sales, and marketing and may be required to return to the capital markets at flat or down valuations or for venture debt.

Point solutions for hybridized cloud environments likely to be acquired before

becoming unicorns: Given the competitiveness of the CASB market and rapid evolution of cloud environments, we expect other incumbents will follow the recent trend of CSPM acquisitions. These acquisitions reinforced our view that few cloud security startups can achieve scale, but many are attractive acquisition targets. Startups such as **CloudPassage** and **Threat Stack** could be candidates to enhance the CASB offerings of other market leaders, including **Microsoft** and **McAfee**.

COVID-19 to catalyze a shift from VPN to SASE: We believe the pandemic-related crisis will catalyze a longer-term shift to distributed workforces as a part of normal business operations, as detailed in our recent **PitchBook Analyst Note: The Great Unlocationing**. Enterprises have extended their existing SaaS access controls and VPNs during the shift to remote work, but we believe these solutions are too limited to provide a secure enterprise perimeter. SaaS access controls fall subject to third-party risk—as evidenced by Zoom's false encryption statements—and VPNs have performance issues at scale. We believe IT departments will invest in new infrastructure in a recovery scenario to establish SD-WAN for all endpoints, create zero-trust network access for SaaS applications beyond the access controls provided by SaaS vendors, and shift on-premise networks to the cloud. This shift offers opportunities for startups to improve network security efficiency and policy management as incumbents attempt to create a comprehensive SASE offering.

SEGMENT DEEP DIVE

Application security



APPLICATION SECURITY

Overview

Application security includes technologies and services that address the vulnerabilities of software programs. Common vulnerabilities include data requests within applications, injection of malicious scripts into existing code, and contamination of log file entries and HTTP headers.

Subsegments include:

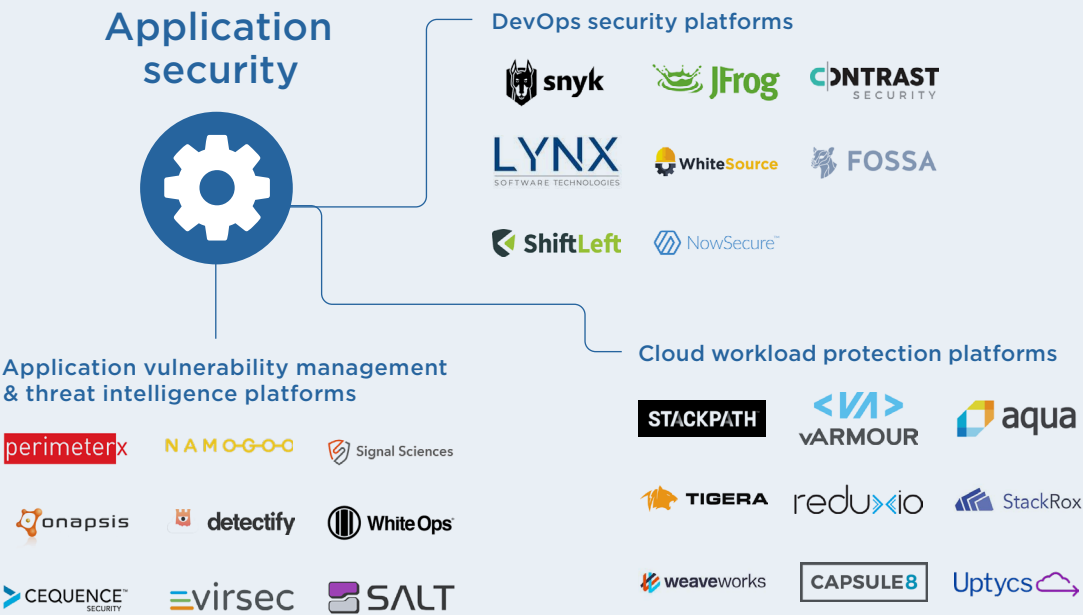
DevOps security platforms: These software tools enable software developers to embed security protections within their code, test their code’s vulnerabilities on a regular basis, and securely deploy application updates.

Cloud workload protection platforms: This emerging niche includes security protections for cloud-based applications and containers that increasingly house cloud-native applications.

Application vulnerability management and threat intelligence platforms: These platforms detect threats targeted at applications. Examples include web application firewalls, bot defense, and application penetration testing technologies.

Industry drivers

Cloud-native application development: There has been a growing use of cloud-based infrastructure for application development and deployment and expansion of container technologies in cloud environments. Container adoption is rising rapidly, with one survey indicating that 87% of companies running applications in container environments, up from





APPLICATION SECURITY

56% in 2017.¹⁶ Container security has become a leading concern for IT departments as a result.

Organizations prioritizing application security in CISO hiring: Application security expertise has become the leading priority for CISO hiring due to prioritization of DevOps and Agile processes by CIOs and CTOs, according to cybersecurity recruiting firm Recrewmint.¹⁷ Given the influential role of CISOs in security purchasing, this priority should lead to increased application security spending.

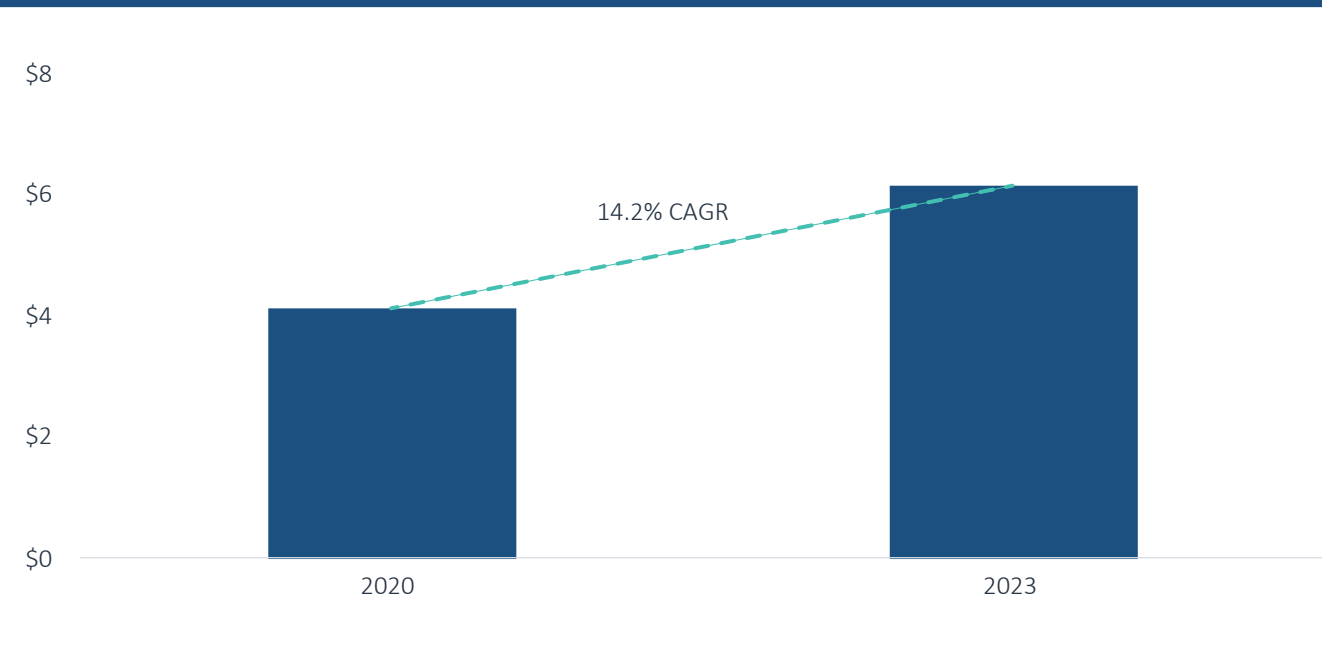
Web application data breaches: Security research indicates that web application data breaches constitute around 90% of the sample of hacking action vectors it investigated,¹⁸ suggesting that they are far more likely to be breached than network backdoors, VPNs, or third-party portals.

Market size

Given the immaturity of the application security market, we believe the space could contract slightly in 2020, considering decreased IT spending overall. Application security contains several emerging product categories that might be considered long-term investments rather than mission-critical priorities. For this reason, we believe the market may decline to around \$4.1 billion in 2020, with high growth resuming in 2021. By 2023, the market should stand at around \$6.2 billion propelled by a 14.2% CAGR. We still believe that cloud workload protection is one of the fastest-growing segments in infosec, though from a low base of \$1.0 billion in 2019. Beyond that subsegment, this estimate includes

16: “2019 Container Adoption Survey,” Portworx and Aqua Security, 2019.
17: “Digital Transformation Moves Application Security to the Top CISO/CSO Priority,” Andre Tehrani, June 2020.
18: “2020 Data Breach Investigations Report,” Verizon, 2020.

Figure 14. APPLICATION SECURITY MARKET SIZE (\$B)



Source: Gartner, Forrester, PitchBook | Geography: North America & Europe

Figure 15. COMMON INDUSTRY KPIS

Financial

- ARPU LTM
- Revenue mix (product/subscription/support)
- LTV/CAC

Operational

- Number of solutions purchased per customer
- Gartner magic quadrant
- Forrester Wave
- NSS security effectiveness
- NSS price performance



APPLICATION SECURITY

application security testing, vulnerability assessment, and web application firewalls, each of which may be deprioritized relative to open source tools, cloud host offerings, and consolidated toolchains in a recessionary environment.

Disruption potential

Application security has not historically been a priority for security teams due to the prevalence of firewalls. The shift toward application-centric enterprise infrastructure, which positions web applications as the most distant perimeter of the enterprise, has required additional focus on application security. Furthermore, the shift to agile software development, which enables the use of SaaS products throughout DevOps processes, has familiarized developers with the entire lifecycle of their apps, including security. As a result, DevOps security platforms are relatively new, having emerged within the last 10 years. As enterprises cut costs in a recessionary environment, we believe they will entrust more power to software developers to ensure applications are secure by default. With more technology being delivered as cloud services, application security can directly capture wallet share from security operations and network security budgets.

Business model

Application security can be delivered as an on-premise tool or through a subscription. Additional modules can be upsold on top of application testing platforms, including vulnerability management and intrusion monitoring. Testing tools are typically deployed on a per-user basis. For example, **Synopsys** charges around \$12,000 per year for five users for its static application testing product Coverity. DevOps security platforms'

runtime-based solutions can utilize consumption-based pricing in conjunction with cloud providers. **Aqua Security** has innovated this business model and offers strong upsell opportunities as the number of applications in production increases.

VC activity

After reaching a record quarterly VC deal value in Q1, venture investment into application security companies declined significantly in Q2, with only \$98.8 million invested across 13 deals. Cloud workload protection leader **Aqua Security** raised only a \$30.0 million Series D, a significant deal size step-down. Management claimed that the round was at a significant valuation step-up while announcing substantial layoffs. Previous investor M12 elected not to participate in the round. API security startup **Salt** demonstrated the high-growth potential in its space with a \$20.0 million Series A at a \$55.0 million pre-money valuation, disclosing strong growth through H1 2020. Funding for DevOps security platforms may be hurt by the pandemic, since developers may opt for open source tools given budget constraints. We believe Guardicore remains a strong candidate for a VC mega-deal in the space.

Application security VC exit activity remained low in Q2 2020, with only two acquisitions completed for DevOps security startups. **VMware** continued its security M&A strategy by acquiring **Octarine**, which has similar capabilities to **Twistlock** and **Aqua Security** in its integration of security policies into the CI/CD pipeline, as described in our **PitchBook Analyst Note: The Shift Left Market Opportunity for DevOps Security Tools**. **Octarine** focuses on container security, specifically Kubernetes, a space in which **Palo Alto Networks** has already made acquisitions. DevOps open source vendor SonarSource



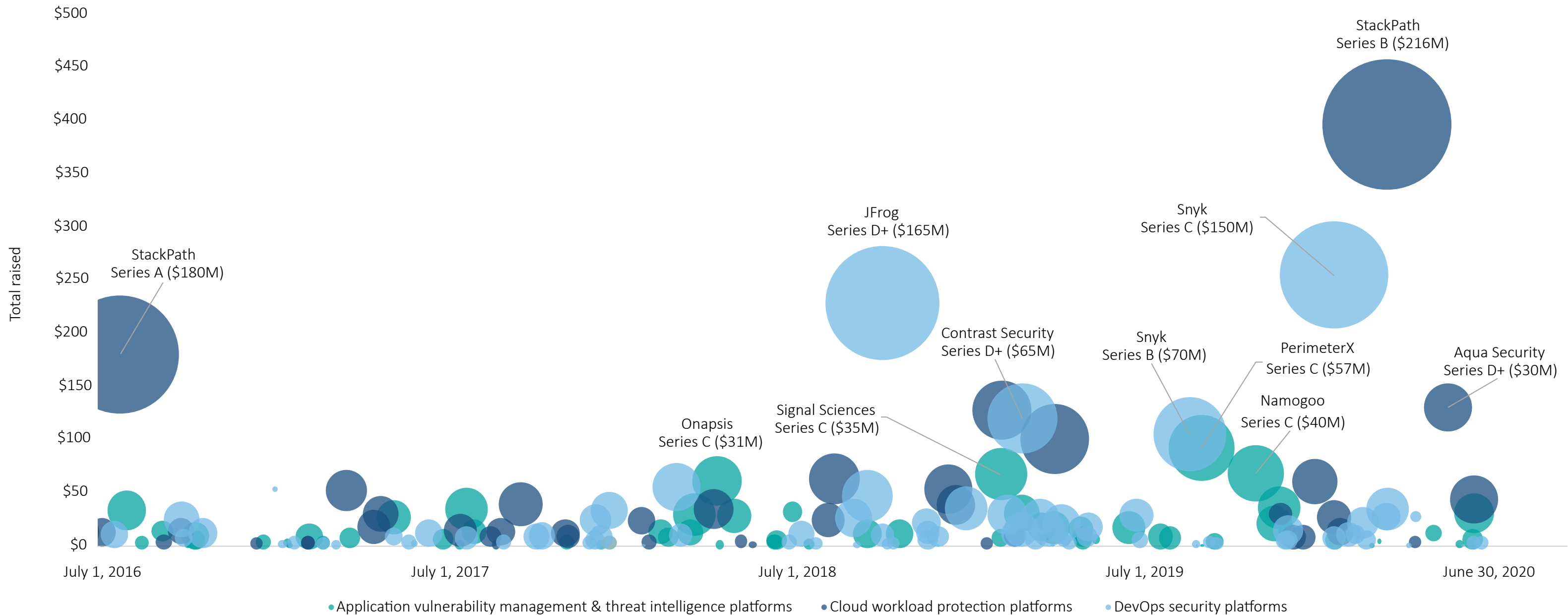
APPLICATION SECURITY

acquired application security testing startup **RIPS Technologies**, citing the speed and accuracy of its platform. **Synopsys** has built the most comprehensive developer security tool suite through M&A, and we believe competitors will be forced to keep up. We anticipated a busy year for application security M&A, but the coronavirus pandemic may mute this activity. A range of IT incumbents have interest in the space, including public network security vendors Fortinet, Check Point, **Cisco**, and **Zscaler**; endpoint security vendors **VMware** and **CrowdStrike**; application security testing vendors **Synopsys**, **Qualys**, and **Rapid7**; and application performance monitoring vendors **DataDog**, **Cisco**, **New Relic**, **Sumo Logic**, and **Dynatrace**. **Palo Alto Networks** has been aggressive in acquiring cloud workload protection platforms, and we expect other cloud security vendors to acquire assets in the space in the medium term.



APPLICATION SECURITY

Figure 16.
Application security VC landscape (\$M)








Source: PitchBook
Note: The left axis indicates total VC raised as of deal date. Bubbles indicate amount raised.








APPLICATION SECURITY

Figure 17.
Notable application security VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE (\$M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
 SALT	June 16, 2020	Application vulnerability management & threat intelligence platforms	\$20.0	Series A	N/A	3.0x
 aqua	May 20, 2020	Cloud workload protection platforms	\$30.0	Series D	Greenspring Associates	N/A
 snyk	January 21, 2020	DevOps security platforms	\$150.0	Series C	Stripes	2.8x
 GitGuardian	December 4, 2019	DevOps security platforms	\$11.9	Series A	Balderton Capital	4.1x
 perimeterx	September 4, 2019	Application vulnerability management & threat intelligence platforms	\$57.0	Series C2	Scale Venture Partners	2.6x

Source: PitchBook

Figure 18.
Notable application security VC exits

COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE (\$M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
 OCTARINE	May 27, 2020	DevOps security platforms	N/A	VMware	N/A	N/A
 Aporeto	December 23, 2019	Cloud workload protection platforms	\$144.1	Palo Alto Networks	N/A	N/A
 Protego	December 2, 2019	Cloud workload protection platforms	\$40.0	Check Point Software Technologies	4.00x	N/A
 Twistlock	July 9, 2019	Cloud workload protection platforms	\$378.1	Palo Alto Networks	N/A	27.3x**
 PURESEC <small>A PALO ALTO NETWORKS COMPANY</small>	May 28, 2019	DevOps security platforms	\$50.0	Palo Alto Networks	N/A	N/A

Source: PitchBook, **Hampton Partners



APPLICATION SECURITY

Figure 19.
Key VC-backed application security companies






COMPANY	TOTAL RAISED (\$M)	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
	\$254.5	DevOps security platforms	Open source security management	Tests vulnerabilities at the repository level and continuously monitors open source-based projects	Stripes, Accel, Boldstart Ventures, Canaan Partners
	\$228.0	DevOps security platforms	Xray	Software Composition Analysis integrates with JFrog repository manager	Insight Partners, VMware, Gemini Israel Funds
	\$100.3	Cloud workload protection platforms	Cloud Native Security Platform	Custom policy enforcement engine for virtual machines, containers, and serverless functions	Insight Venture Partners, Lightspeed Venture Partners, M12
	\$127.0	Cloud workload protection platforms	vArmour ApplicationController	Layer 7 inspection of cloud workload connections	AllegisCyber, NightDragon Security, Redline Capital Management, Citi Ventures, Columbus Nova Technology Partners, Menlo Ventures, Highland Capital Partners, Vanedge Capital
	\$119.6	DevOps security platforms	"Contrast Assess" Interactive Application Security Testing platform	Ease of use and customer support	Warburg Pincus, Battery Ventures, General Catalyst, Acero Capital
	\$91.5	Application vulnerability management & threat intelligence platforms	PerimeterX BotDefender	Best-in-class machine learning for application traffic analysis	Scale Venture Partners, Canaan Partners, Vertex Ventures, Data Collective

Source: PitchBook



APPLICATION SECURITY

Figure 20.
Key application security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/EBITDA*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
 SYNOPSYS®	NASDAQ: SNPS	43.2x	DevOps security platforms	Seeker Interactive Application Security Testing platform	Comprehensive suite of testing services
 MICRO FOCUS®	LON: MICRO	6.3x	DevOps security platforms	Fortify Application Security Testing platform	Out-of-the-box integrations for CI/CD tools
 VERACODE	Thoma Bravo portfolio company	N/A	DevOps security platforms	Greenlight	Ease of use and customer support
 CHECKMARX	K1 Investment Management portfolio company	N/A	DevOps security platforms	CxSAST	User-friendly code remediation suggestions
 imperva	Thoma Bravo portfolio company	4.7x EV/revenue CY 2018	DevOps security platforms	SecureSphere WAF	Strong customer support and bot mitigation

Source: PitchBook | *As of June 30, 2020



APPLICATION SECURITY

Opportunities

Application testing and development tools: DevOps has been a tailwind for the SaaS industry, with companies such as **Atlassian** and **Chef** helping power the DevOps process. Similarly, we believe the shift left (that is, the integration of security into the DevOps process) represents a unique opportunity for infosec startups. The shift left refers to security being employed earlier in the software production cycle and integrated into code itself. This differs from traditional application security, which is applied once the application is in production. While the opportunity to move security from a runtime service directly into the requirements, design, and development stages of application creation could improve security infrastructure, it presents new implementation challenges for technology departments. Even so, we have seen COVID-19 catalyze the shift in processes needed to drive change in secure DevOps and increased demand for startup products in the space. Startups focused on this opportunity are offering tools for developers to detect vulnerabilities within open-source codebases and integrating security policies into continuous deployment pipelines. We estimate this opportunity to have an \$11.5 billion addressable market based on current pricing and developer population. As a subset of this opportunity, software composition analysis (SCA) can be used to produce an inventory of all the open-source components of an application's code base and identify vulnerabilities within the code. Recently in this space, Vista Equity Partners bought out **Sonatype**, and **Snyk** raised the largest-ever Series C in the infosec industry. **WhiteSource** is an innovator in SCA, and we believe the company could be an attractive target for legacy application-testing vendors such as **Micro Focus**.

API security controls: APIs are a growing type of threat surface that is easy for developers to implement and enables them to transfer sensitive data between applications with common programming languages, powering ubiquitous tech companies including Twilio, Shopify, and Stripe. These application linkages, once breached, make it possible for hackers to exfiltrate data and move laterally. APIs can easily be integrated outside the typical software development lifecycle, giving existing security controls little visibility over API traffic. As a result, the Open Web Application Security Project (OWASP) has identified 10 vulnerabilities unique to APIs and have further recognized their role in the top 10 application security vulnerabilities overall. As a result, enterprises are in the early stages of evaluating standalone API security controls, which we believe could evolve into a \$1.0 billion market as APIs become more ubiquitous. Startups emerging at the early stage in this space include **Cequence Security**, **Salt**, **Tinfoil Security**, **42Crunch**, **imVision Technologies**, and **Wallarm**. **Salt**, **42Crunch**, and **Cequence Security** have achieved outstanding valuation step-ups at an early stage, suggesting early traction in this emerging market.

Application security orchestration and correlation (ASOC): As application security is an immature niche, a minority of enterprises employ multiple application security tools. As adoption grows, many of these tools will require integration and coordination beyond what existing security operations tools can provide. ASOC is an emerging category that has not yet received high commercial traction or significant VC funding. There are startups addressing the opportunity, including **Code Dx**, which integrates with software testing and runtime-protection tools to triage alerts and prioritize vulnerabilities for remediation by security teams. We believe some tool sprawl in application security is inevitable, and ASOC could become similar in size to SOAR at a nearly a \$1.0 billion market over the next five



APPLICATION SECURITY

years. COVID-19 should accelerate the need for remote workers to prioritize alerts given the reduced interaction of developers with security teams.

Considerations

Smaller problem size than endpoint penetration: Due to the immaturity of the application security market, startups may have difficulty scaling. Enterprises have existing budgets for endpoint and network technologies but may be less trusting of application security given its nascence. The market is smaller than other segments' markets, estimated at \$4.4 billion in 2019. Gartner forecasts a 10.6% growth rate for the segment in 2019, which, if extrapolated forward, means the segment could be the second-smallest infosec segment 2023. However, we believe this estimate may prove to be conservative as developers increasingly allocate budget to security tools.

Cloud security providers may offer competing products to startups: Amazon Web Services (AWS) offers a web application firewall (WAF) that can protect customer applications in runtime environments and may limit demand for third-party application security tools. AWS also offers RASP and APIs for developers to apply WAF rules to each application stack. While the product involves only applications running in AWS, which is estimated to have nearly 50% of the public cloud market, it demonstrates that cloud providers can offer competitive security solutions for cloud-native apps.

Uncertain product-market fit: Application security requires buy-in from IT departments, which tend to have different priorities from security departments. CTOs' priorities for their developers may not include incorporating security into the production environment, which

may limit a CISO's ability to integrate application security at the developer level, thereby reducing adoption. Security teams have difficulty implementing solutions in other business units, since they are obstacles to business objectives, which could increase the friction of the sales process for companies in this segment. Thus, uncertain product-market fit could put some solutions low on the IT priority list in a recessionary environment.

Outlook

Point solutions for cloud workload protection platforms to be acquired by cloud security providers: The rise of containerization may make cloud workload protection platforms essential additions to CASB product offerings. Recent acquisitions in this space by **Palo Alto Networks**, **McAfee**, and Check Point may be the first of many similar deals, as exemplified by **Cisco's** reported interest in acquiring **Signal Sciences**. The limited supply of container- and serverless-specific security solutions may put upward pressure on valuations as interest from strategic buyers increases. **Palo Alto Networks** has a history of paying high multiples for cutting-edge technologies, exemplified by its acquisition of Secdo for 45x its \$2.0 million in revenue and **Twistlock** for 27x revenue.¹⁹ These deals may set precedents for similarly high-priced acquisitions.

DevOps security to produce further unicorns: **Snyk's** ascendance to a unicorn valuation demonstrates the demand for DevOps security tools, which is further substantiated by **Auth0's** growth in identity & access management. We expect rapid growth in this area of infosec over the next three years, largely driven by venture-backed startups. The DevOps community can spur rapid adoption of best-of-breed tools and practices, as demonstrated

19: "M&A Market Report 2H 2018: Cybersecurity," Hampton Partners, 2018.



APPLICATION SECURITY

by the swift rise of containers. Emerging technologies that can eliminate development bottlenecks, including manual application security testing and penetration testing, and are delivered via open-source business models, which are likely to fuel growth in this niche.

Bot defense technologies may struggle to achieve unicorn status given the maturity of the

market: Web application bot defense includes vendors that focus on malicious web traffic carrying automated attacks. This subsegment of application vulnerability management vendors has less funding allocated to it relative to other segments of application security, possibly due to the strong incumbent positions of Distil Networks and Akamai Technologies. Bot defense vendor **PerimeterX** recently became the highest-valued startup in this field, raising a Series C at a \$197.0 million post-money valuation. We believe DevOps security tools and cloud workload protection platforms may have greater potential to create unicorns.

SEGMENT DEEP DIVE

Data security



DATA SECURITY

Overview

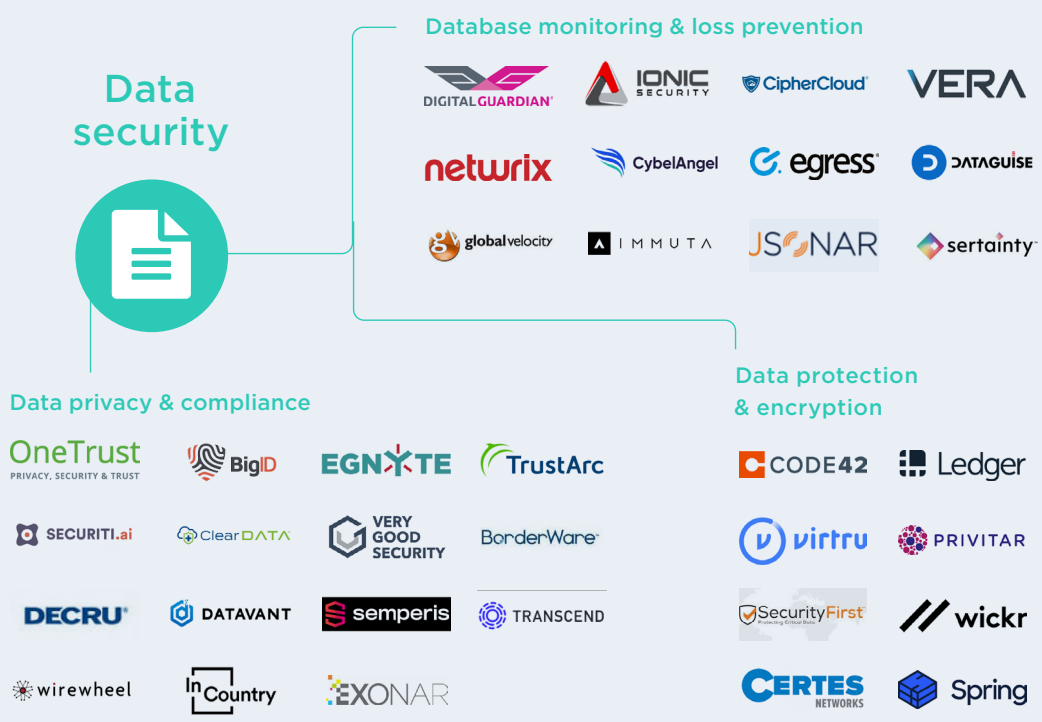
Data security uses monitoring, filtering, blocking, and remediating technologies to address the risks of inadvertent or accidental data loss and the exposure of sensitive data. As Big Data analytics become ubiquitous within enterprises and data-focused regulation increases, there is a growing need for data security platforms that can monitor access to databases and provide data loss back-up and protection services. Data security platforms integrate directly with databases to enable permission and authorization features, track the movement of data, encrypt data, and provide back-up copies of those databases.

Subsegments include:

Database monitoring & loss prevention: Companies that provide analytics of database activity including access, data in transit, and data at rest. These technologies allow users to block data exfiltration attempts at the database level. Related technologies include data loss prevention platforms (DLP), multi-party trust computation, and AI-based data monitoring.

Data protection and encryption: Companies that protect databases from intrusions and develop novel encryption algorithms and applications for data-in-transit. Related technologies include tokenization, distributed ledgers, and cryptocurrency security.

Data privacy and compliance: Companies that enable customers to address emerging data regulations including the EU’s General Data Privacy Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These platforms identify data that could violate specific policies, remediate those regulatory vulnerabilities, and generate reporting and documentation for audits. Many infosec companies claim to address a range of compliance issues, though this particular subsegment addresses platforms that have built-in compliance rules and specialized workflows to meet emerging governmental privacy regulations.





DATA SECURITY

Industry drivers

The rising quantity and cost of data breach incidents have propelled investment into this space. Regulations including GDPR and CCPA encourage enterprises to use third-party data security tools to ensure privacy, including database monitoring tools and secure data protection platforms. GDPR violations can cost up to 4% of revenue in fines, pushing enterprises to spend on data mapping solutions.

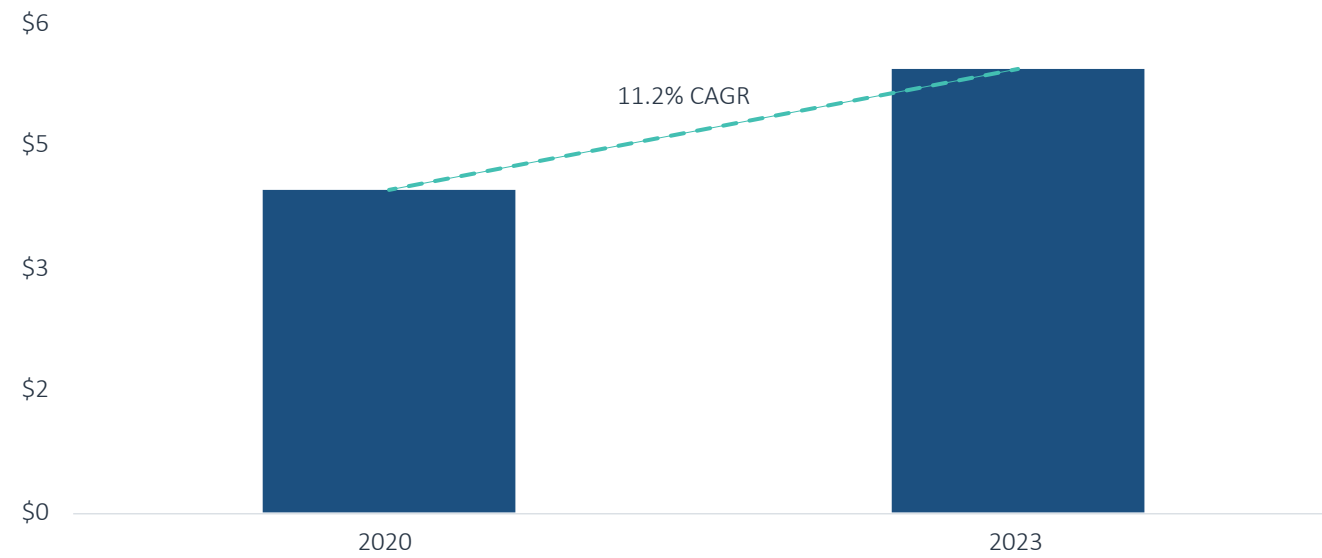
Market size

We believe the data security market may grow slightly in 2020 due to enterprises' dependence on database monitoring & loss prevention. While data privacy & compliance solutions are becoming more essential due to emerging regulations, standalone solutions may face slower adoption than we previously forecast. We expect growth to resume in 2021 at 11.2% CAGR to a \$5.4 billion market size by 2023. This market includes encryption, data loss prevention, data privacy management, and tokenization. The data privacy management software market grew 60% in 2019 to \$802.3 million, and we forecast a \$2 billion market by 2023, driven almost entirely by private companies.

Disruption potential

Emerging challenges to data encryption, including decreased cost of computing for attackers and quantum computing, make current forms of encryption less effective. Novel forms of encryption, such as the homomorphic and quantum forms that academic researchers are

Figure 21. DATA SECURITY MARKET SIZE (\$B)



Source: Gartner, PitchBook | Geography: North America & Europe

Figure 22. COMMON INDUSTRY KPIS

- Revenue mix
- Growth in cloud storage
- Number of platforms supported
- Number of application and database types
- Number of integrated storage and HCI types
- Number of operating environments
- NSS security effectiveness
- NSS total cost of ownership per protected mbps
- Gartner magic quadrant placement
- Forrester wave placement



DATA SECURITY

developing, are poised to disrupt the data security industry. Startups that commercialize this technology can gain traction among governments and financial institutions.

Startups have already built superior GDPR compliance platforms relative to incumbents. Incumbent DLP solutions did not provide the level of data mapping needed to comply with Article 30 of GDPR. As a result, three of the market leaders in the segment are startups **OneTrust**, **BigID**, and **Securiti.ai**, all of which have at least 5% market share despite the presence of SAP in the category. SAP recognized the deficiency of its product offering and has recently partnered with **BigID** for privacy management. This development illustrates the potential for new security requirements to cause market dislocations and create startup opportunities. These requirements can emerge from both regulation and changing enterprise infrastructure.

Business model

Data security is typically sold via a SaaS business model with pricing based on level of usage. For example, DLP subscriptions typically cost around \$15 to \$45 per user based on the level of managed services provided. Data privacy & compliance is billed as a SaaS subscription based on the size of the organization and the level of data discovery and mapping by the vendor. Pricing starts as low as \$1500 for an enterprise. Additional modules can be upsold including training, cookie management, and third-party risk management.

VC activity

Data security VC deal activity remained robust in Q2, with \$346.2 million raised across 18 deals in the quarter, continuing strong momentum from the last several quarters. Data privacy

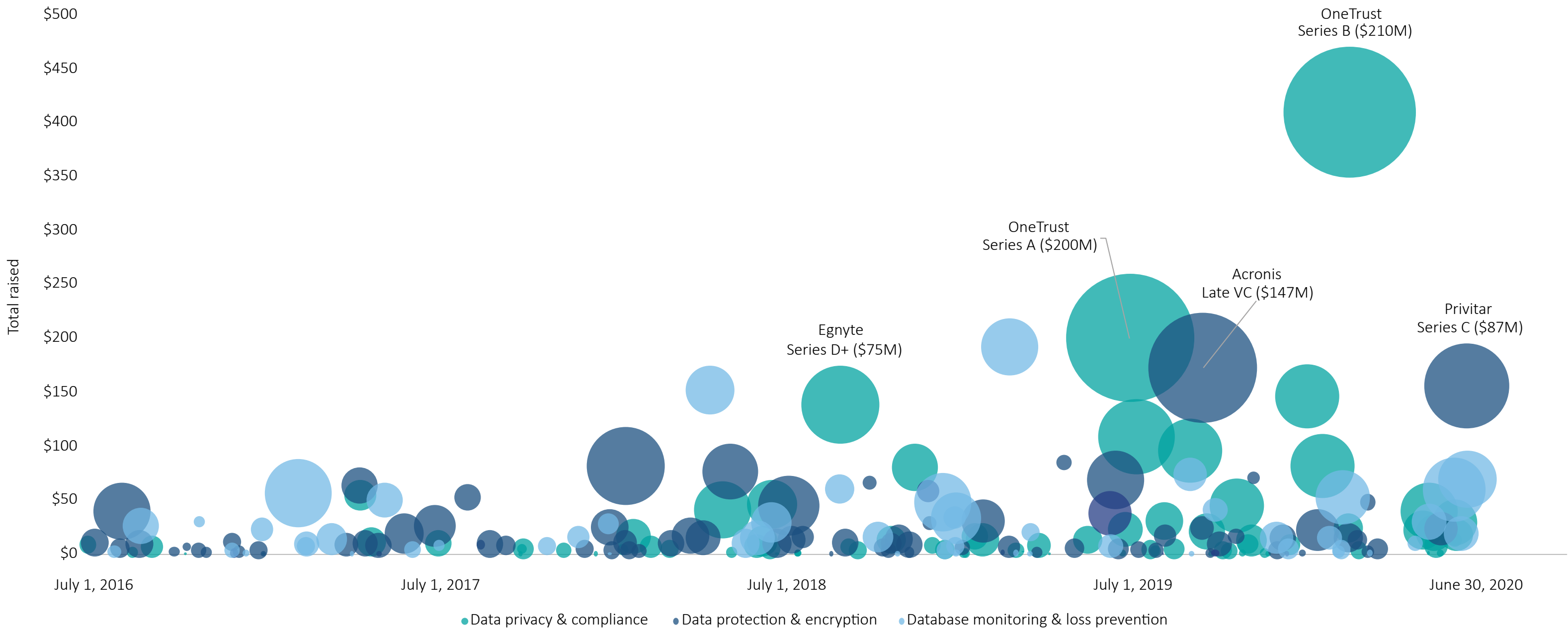
& compliance remained the main driver of deal flow, though database monitoring & loss prevention and data protection & encryption also had significant deals. Leading investors participated in deals with in this space, including Goldman Sachs, Insight Partners, Intel Capital, Accel, and Index Ventures. **Privitar**, a data protection platform, and jSonar, a database security platform, raised late-stage rounds at significant valuation step-ups from Warburg Pincus and Goldman Sachs, respectively, demonstrating high commercial traction. According to its investors, **Privitar**'s deal was primarily propelled by GDPR and CCPA compliance, and jSonar's by high adoption in large enterprises. **Transcend**, **Privacera**, and **Ethyca** raised Series A rounds with over \$30 million pre-money valuations. Data security has not been a leading source of deal activity nor exits in recent years, but this may change as startups bring new functionality to a dormant industry.

VC exit activity remained muted in Q2 for this segment. Recent transactions in data security have not exceeded \$100 million, suggesting companies in the segment are not gaining market traction and that these technologies are not critical for infosec incumbents. The one exit to close in Q2 was Genesis Global Trading's minor acquisition of London-based voIt, a digital asset custodian with advanced cybersecurity capabilities. This exit was atypical in its intention to create a prime brokerage with highly secure custodian services. Given the rapid growth in data privacy & compliance, we believe the large number of startups in the segment will likely form a pipeline for PE buyouts. The corporate M&A market in this niche has not yet crystallized, but we believe incumbents may be interested in adding growth via this adjacent segment over time.



DATA SECURITY

Figure 23.
Data security VC landscape (\$M)



Source: PitchBook
Note: The left axis indicates total VC raised as of deal date. Bubbles indicate amount raised.



DATA SECURITY

Figure 24.
Notable data security VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE (\$M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
 IMMUTA	June 23, 2020	Database monitoring & loss prevention	\$40.0	Series C	Intel Capital	1.7x
 PRIVITAR	June 22, 2020	Data protection & encryption	\$87.0	Series C	Warburg Pincus	2.3x
 TRANSCEND	June 10, 2020	Data privacy & compliance	\$25.0	Series A	Accel, Index Ventures	N/A
 JSNAR	June 9, 2020	Database monitoring & loss prevention	\$50.0	Series C	Goldman Sachs Merchant Banking Division	5.0x
 OneTrust <small>PRIVACY, SECURITY & TRUST</small>	February 20, 2020	Data privacy & compliance	\$210.0	Series B	Insight Partners, Coatue Management	1.9x

Source: PitchBook | *As of June 30, 2020

Figure 25.
Notable data security VC exits






COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE (\$M)	ACQUIRER/INDEX	VALUATION STEP-UP	VALUATION METRIC
 PERSEUS	February 1, 2020	Data privacy & compliance	N/A	HDI Global	N/A	N/A
 SHYFT	December 11, 2019	Data privacy & compliance	N/A	BitFury	N/A	N/A
 observe it	November 25, 2019	Database monitoring & loss prevention	\$214.0	Proofpoint	N/A	N/A
 BlueTalon	July 29, 2019	Database monitoring & loss prevention	N/A	Microsoft	N/A	N/A

Source: PitchBook | *As of June 30, 2020






DATA SECURITY

Figure 26.
Key VC-backed data security companies

COMPANY	TOTAL RAISED (\$M)	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
 OneTrust	\$410.0	Data privacy & compliance	Privacy program management	Ease of use for non-IT professionals	Coatue Management, Insight Partners
 IONIC SECURITY	\$192.1	Database monitoring & loss prevention	Machina data protection engine	Double the speed of other business VPNs	WndrCo, Goldman Sachs, Renn Global, Entrepreneurs Fund
 Acronis	\$173.0	Data protection & encryption	Active Protection	Integrates with data backup system to block ransomware attempts	Goldman Sachs, BlackRock, Kaplan Group Investments, RAA Ventures, Tennenbaum Partners
 PRIVITAR	\$155.5	Data privacy & compliance	Data privacy platform	Data de-identification	Warburg Pincus, Accel, Citigroup, Partech Partners
 BigID	\$146.2	Data privacy & compliance	Discovery Foundation	Classifies data in any environment	Scale Venture Partners, Tiger Global Management, Bessemer Venture Partners, ClearSky

Source: PitchBook | *As of June 30, 2020

Figure 27.
Key data security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/REVENUE*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
 FORCEPOINT <small>POWERED BY Raytheon</small>	Raytheon subsidiary	N/A	Database monitoring & loss prevention	DLP	Ease of use
 Symantec™	Broadcom subsidiary	4.7x (acquisition multiple)	Database monitoring & loss prevention, data protection & encryption	DLP, DLP Cloud Service for Email, DLP Cloud and Symantec CloudSOC	First integrated DLP and CASB for cloud data protection
 McAfee™	TPG Capital portfolio company	N/A	Database monitoring & loss prevention, data protection & encryption	McAfee Total Protection for DLP	Cost-effective suite of DLP solutions

Source: PitchBook | *As of June 30, 2020



DATA SECURITY

Opportunities

Blockchain: Blockchain technology can supplant conventional data protection technologies by distributing databases across a network. Storing data on a distributed ledger can make it nearly impossible for hackers to gain access due to the distributed encryption of the data. It is unclear whether fully decentralized public blockchains will be trusted for security purposes, and private permissioned blockchains may be able to gain more rapid adoption. Startups working on commercial products include R3, **Guardtime**, **Oasis Labs**, **Factom**, and Storj Labs. In a largely mature market, we believe blockchain security could be one of the few winner-take-all opportunities for startups.

Homomorphic encryption: Homomorphic encryption is the “holy grail” of the market but is years away from a commercially viable solution. It allows third parties to operate on encrypted data, removing the need to manage encryption keys, which is a vulnerability in data security platforms. Startups including **Enveil** and **Fortanix**, which refer to the technology as runtime encryption, have developed prototypes; however, the products suffer in practice from excessive compute requirements and are not suited to large databases.²⁰ Startups’ ability to define use cases for the technology while its compute requirements decline will determine its commercialization pathway. In terms of a response to the pandemic, the technology can be useful in protecting contact tracing data, which is feared to give location data to untrustworthy authorities, as well as analysis of genomic data to determine susceptibility to the virus. **Duality Technologies** is partnering with a US state-level government for homomorphic encryption for COVID-19 contact tracing and DARPA for machine learning studies on private genomic data, both of which could unlock new opportunities for HIPAA-compliant data analysis in a public

health-focused environment. Financial services enterprises have invested in this space via **Enveil**’s Series A, including Capital One Ventures, Bloomberg, and Mastercard.

GDPR and CCPA privacy regulation compliance technology: The New York Department of Financial Services Cybersecurity Regulation requires financial institutions to exceed industry standards of security, including encryption of sensitive data. Some incumbents, such as CommVault, have developed advanced products to meet the needs of these regulations. **Beyond** that, the wave of privacy regulations including GDPR and CCPA may require new data monitoring and encryption solutions to help consumer companies prove the security of their data to auditors. Leading GDPR enforcement agencies, including the UK Information Commissioner’s Office (ICO), have left compliance technologies up to the private sector, indicating that innovation is required to develop compliance processes for the rigorous standards. The ICO has actively engaged with Silicon Valley on compliance approaches, given the need to map data across enterprises and alert compliance teams when illegitimate data has been collected or transmitted. Given the uncertainty around these policies, growth-stage companies have the potential to tailor new products to meet compliance needs and work collaboratively with regulators to clarify enforcement mechanisms. Enterprises have rapidly escalated their data privacy compliance spending, with nearly all new spending going toward startups in the space.

Considerations

High barriers to entry: DLP is a mature market with dominant providers. Gartner stopped publishing a Magic Quadrant in the space in 2018 due to the lack of changes in the

²⁰: “The Cloud Encryption Handbook: Encryption Schemes and Their Relative Strengths and Weaknesses,” McAfee, July 2015.



DATA SECURITY

industry.²¹ **Microsoft**'s DLP policies for its exchange server and **Forcepoint**'s DLP have especially high market share. The maturity of the market raises concerns for highly funded VC-backed companies to achieve scale and justify their valuations.

Long time frame to adoption: We believe disruptive technologies that could drive increased value in the space are over five years from mainstream adoption. The field of infonomics, which assigns economic value to information, may drive more value to data security as information itself becomes a balance sheet asset. For now, there are no accounting conventions to determine the value of information, even as it represents a tangible asset. This is not likely to change soon. With blockchain and homomorphic encryption presumably over five years from mainstream adoption, incumbents are likely to stay ahead of the field in the medium term.

Emerging solutions may lack product-market fit: DLP solutions are not effective at blocking all attacks, as they typically deploy relatively simple data access policies, and hackers tend to find new ways around these defenses. For this reason, enterprises may not be willing to invest in emerging solutions in the space, instead focusing on blocking intrusions through endpoints and the network. While data has in many ways come to represent the crown jewels of many businesses, data security still may not be top of mind among CISOs' procurement priorities.

Outlook

Late-stage companies to be challenged by dampened funding environment: **Digital Guardian** has deferred an IPO for years, though we believe its recent PE growth and debt

rounds are unlikely to be sufficient to fuel its operations over the long term. While **Ionic Security** has received investment from prominent VC firms, it has struggled to increase its valuation or funding totals, and we believe secondary shares are available at a steep discount. Before the pandemic-related crisis, we believed these companies to be IPO candidates, though in an uncertain economy they may become PE buyout targets.

Cloud data security point solutions as acquisition targets for incumbents with CASB solutions: Data security startups are increasingly addressing the challenges of storing data in the cloud. With DLP and encryption acting as sources of competitive differentiation for CASB offerings, cloud DLP solutions such as those developed by **Code42**, **Vera**, and **Virtru** may be logical add-ons for CASBs with limited cloud DLP functionality, such as **Cisco** and **Forcepoint**. We expect these acquisitions would likely be in the typical range for infosec acquisitions at around \$200.0 million to \$500.0 million.

Data privacy & compliance and data protection & encryption startups as acquisition targets for financial services companies and telecom providers: Regulations may make it cost effective for financial and telecom companies that own consumer databases to acquire data privacy startups for strategic reasons. Companies with large stores of personal identifying information can benefit from integrating the latest data protection technologies both in terms of compliance and public perception. There is some precedent for strategic acquisitions in fraud prevention from financial institutions such as Capital One (**Conform**) and Goldman Sachs (**Final**) and in network security telecom leaders such as AT&T (**Vyatta**, **AlienVault**) and Verizon (**ProtectWise**, **Vidder**, **Niddel**). Furthermore, the acquisition of **Perseus Technologies** by HDI Global demonstrates there are synergies between insurance companies and data privacy vendors. Regulations may spur further acquisition activity in data privacy & compliance as well as encryption.

21: "The Cloud Encryption Handbook: Encryption Schemes and Their Relative Strengths and Weaknesses," McAfee, July 2015.

SEGMENT DEEP DIVE

Identity & access management



IDENTITY & ACCESS MANAGEMENT

Overview

Identity & access management (IAM) software enables management of employee and customer details as well as permissions across the enterprise network. It also provides maintenance of customer privacy preferences and provisioning of access to sensitive data for employees and third parties. This segment has grown in importance as enterprises have begun to substitute identity controls for firewall protections. IAM enables zero-trust access for approved identities, which can keep the network more secure than firewalls that rely on blacklisting known threats. We also include fraud prevention in this segment, which uses identity-based rules and data models including machine learning to block fraud, principally in ecommerce and retail.

Subsegments include:

Identity governance and administration (IGA): Platforms that manage access to information and applications based on pre-defined policies. We define this term more broadly than it is common definition to encompass all tools that enterprises use to segment access to their network, including both people and devices. Technologies within this subsegment include:

- Single sign on
- Password management
- Provisioning
- Privileged access management
- Entitlement management
- Access certification
- Directory management





IDENTITY & ACCESS MANAGEMENT

Fraud prevention: Technologies that detect and block fraudulent access requests and payments, which can be built from a database of legitimate identities and behaviors, making it part of the IAM segment. Technologies within this subsegment include online fraud detection and passwordless multifactor authentication.

Industry drivers

Expanding universe of enterprise devices: Workforces increasingly use multiple devices and network connections to connect to the enterprise network. Employee identities must be tracked across locations, devices, and cloud environments.

Ecommerce fraud: Ecommerce requires the management of customer identities across devices and has high potential for fraud. One study shows that online account takeover grew 79% in 2019.²²

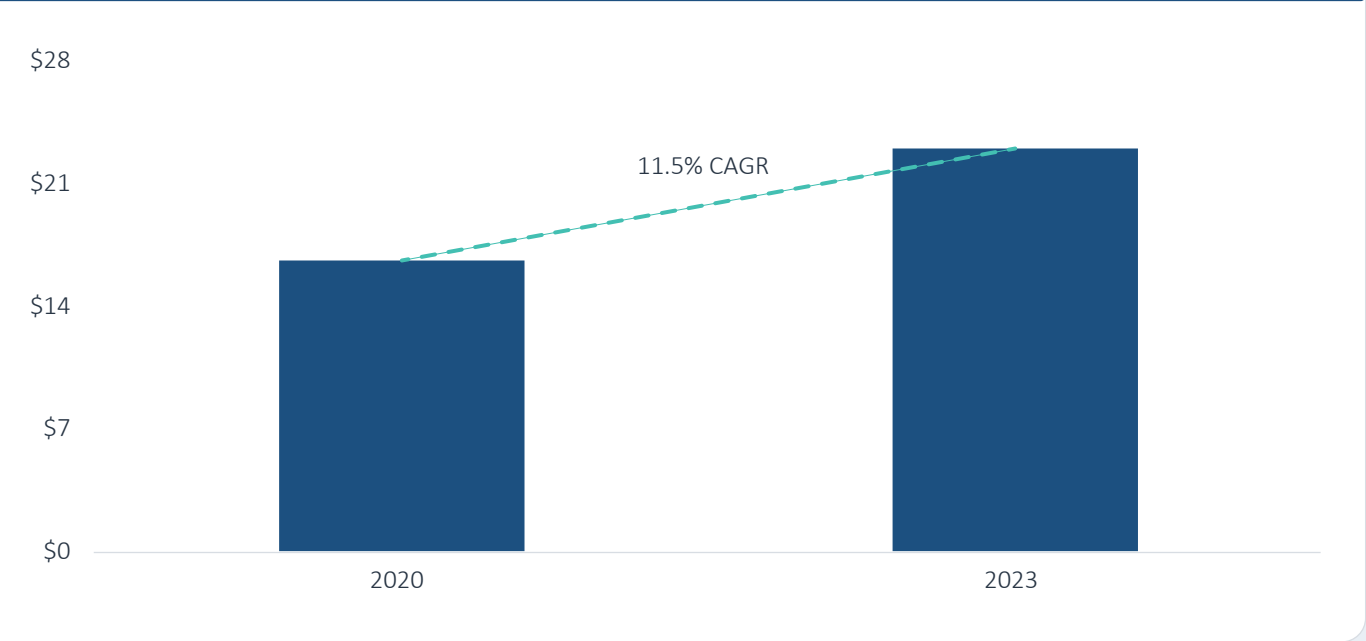
SaaS application growth: Enterprises are growing their use of SaaS applications and storage of sensitive data in those applications. Customers of IAM platform Okta use 88 apps on average, up 21% in three years.²³ Employee identities must be managed across all these applications and monitored for insider threats.

Market size

We expect the IAM market to grow slightly in 2020, as enterprises require identity governance and fraud prevention for remote workforces and ecommerce transactions,

22: “2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis,” Javelin, Krista Tedder & John Buzzard, April 7, 2020.
23: “Businesses at Work,” Okta, 2020.

Figure 28. IDENTITY & ACCESS MANAGEMENT MARKET SIZE (\$B)



Source: Gartner, Forrester, PitchBook | Geography: North America & Europe

Figure 29. COMMON INDUSTRY KPIs

Financial

- Subscription revenue growth
- Customer count growth
- Customers with over \$100,000/\$1 million in ACV
- Dollar-based retention rate
- Maintenance renewal rate

- 5-year purchase multiple

Operational

- Number of tests per release
- External compliance certifications
- Level of encryption
- Number of application integrations



IDENTITY & ACCESS MANAGEMENT

and for double-digit growth to resume in 2021. For this reason, we forecast the market to reach \$23.0 billion by 2023, representing a 11.5% CAGR from 2020, down from our Q4 2019 estimate of a \$27.8 billion market at a 12.3% CAGR. Fraud prevention is a high-growth subsegment within IAM, estimated to grow at a 16.6% CAGR from 2021 to 2023. Identity governance & administration should also likely expand in line with the broader infosec market, at around 9.5% from 2021.

Disruption potential

IAM predominantly relies on definition of access rules by IT and security teams, addressing both internal employee access and third-party interactions with the enterprise network. The definition of these rules is often a manual process that requires extensive configuration and is costly to install. The development of automated policy management tools that can interpret data about access requests and make policy changes in real time can save substantial operating costs in IAM configuration and enable enterprises to handle the complexity of ecommerce and IoT identities. The labor-intensive process used by many enterprises today can be streamlined and lead to decreased revenue losses through fraud and improved security through automatic access provisioning.

Business model

IAM models are simply based on the number of identities managed, though they can have license-style subscription fees for an entire enterprise. Okta per-user fees can start at \$12 annually for access management and range up to \$48 per user for lifecycle management. SailPoint charges a platform fee up to 7,500 users for \$50,000 per year.

VC activity

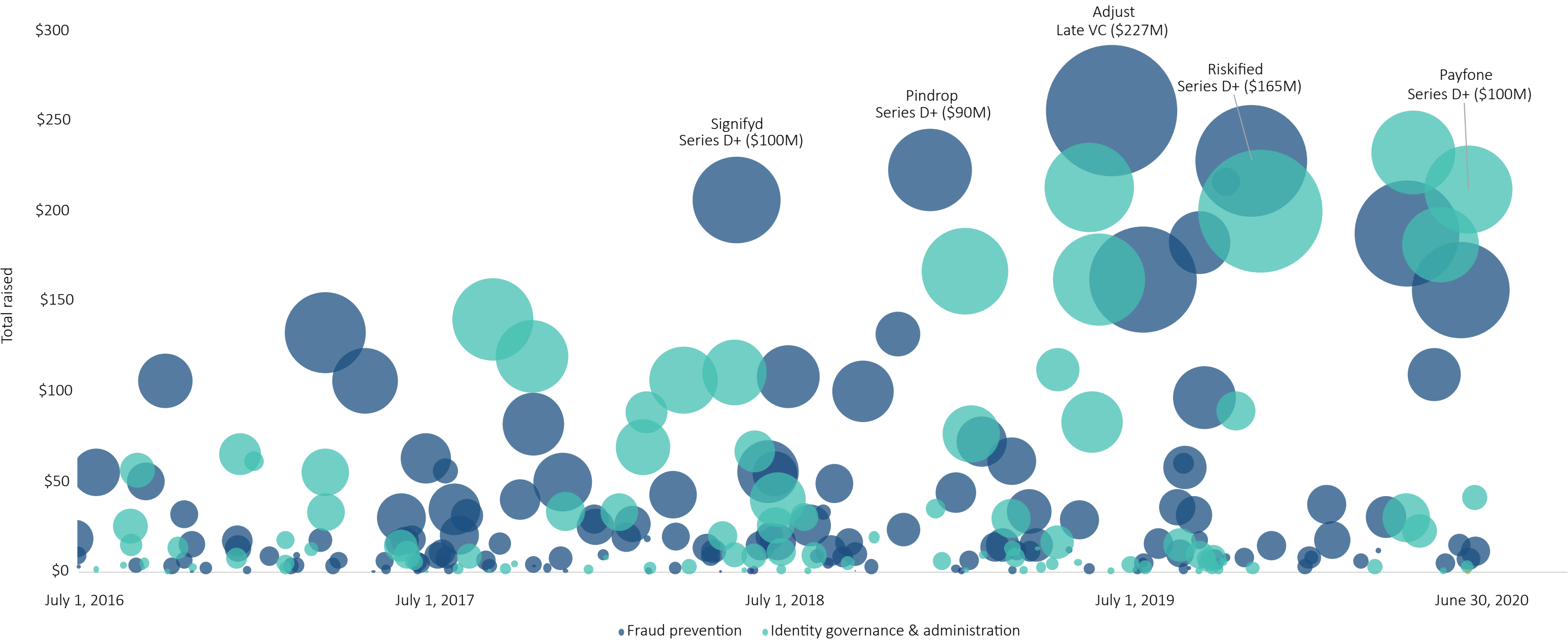
IAM had an outstanding quarter in terms of VC deal activity, with quarterly record deal value of \$658.8 million across 16 deals. COVID-19 has accelerated the ecommerce use case for fraud prevention, leading to substantial growth for startups addressing small merchants. Startups offering fraud prevention solutions naturally dominated venture investment into the IAM industry; three such companies closed mega-deals in Q2, including **BioCatch**, **NS8**, and **Payfone**. **NS8** raised \$123.0 million in a Series A from Lightspeed Venture Partners and AXA Venture Partners as it has already turned a profit and achieved 200% revenue growth in 2019. **Beyond Identity** raised a \$30.0 million Series A at a \$100.0 million pre-money valuation to eliminate passwords via cloud-delivered certificates, driven primarily by the quality of the team founding the company. Early-stage startup **Authomize** came out of stealth mode with \$6.0 million in seeding funding from M12, Entrée Capital, and Blumberg Capital to bring knowledge graphs to privileged access management, particularly for SMBs. Innovative approaches to both fraud prevention and identity governance & administration are finding traction in the market and driving high valuation growth.

After a strong Q1, exit activity within the IAM industry cooled Q2 with none tracked. IAM market leaders have not been active in M&A over the past three years, including Okta, **Microsoft**, **Saviynt**, **Visa**, and **American Express**. Despite the lack of demand, IAM has demonstrated consistent ability to produce unicorn exits, and we believe a pipeline of fraud prevention exits is building. **Riskified**, **Signifyd**, and **Sift** have reached valuations that suggest liquidity as a next step, with **Riskified** considering an IPO this year. We believe the high growth in fraud prevention, especially in the SMB segment, will stimulate further M&A activity in IAM going forward.



IDENTITY & ACCESS MANAGEMENT

Figure 30.
Identity & access management VC landscape (\$M)



Source: PitchBook
Note: The left axis indicates total VC raised as of deal date. Bubbles indicate amount raised.



IDENTITY & ACCESS MANAGEMENT

Figure 31.
Notable identity & access management VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE (\$M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
 PAYFONE	June 18, 2020	Identity governance & administration	\$100.0	Series H	Apax Partners	N/A
 NS8	June 10, 2020	Fraud prevention	\$123.0	Series A	N/A	N/A
 ForgeRock	April 21, 2020	Identity governance & administration	\$92.5	Series E	Riverwood Capital	1.0x
 BIOCATCH Less Friction. Less Fraud.	April 15, 2020	Fraud prevention	\$145.0	Series E	Maverick Ventures, Bain Capital	N/A
 BEYOND IDENTITY	April 14, 2020	Identity governance & administration	\$30.0	Series A	Koch Disruptive Technologies, New Enterprise Associates	N/A

Source: PitchBook

Figure 32.
Notable identity & access management VC exits







COMPANY	CLOSE DATE	SUBSEGMENT	EXIT SIZE (\$M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
 emailage	March 19, 2020	Fraud prevention	\$480.0	LexisNexis Risk Solutions	2.23x	1.0x
 ZignSec	October 21, 2019	Identity governance & administration	\$7.1	NASDAQ Stockholm	N/A	18.5x
 simility	July 1, 2018	Fraud prevention	\$120.0	PayPal	2.27x	N/A
 ThreatMetrix	February 22, 2018	Identity governance & administration	\$813.6	RELX Group	N/A	N/A
 DUO	September 28, 2018	Identity governance & administration	\$2,350.0	Cisco Systems	2.01x	N/A

Source: PitchBook



IDENTITY & ACCESS MANAGEMENT

Figure 33.
Key VC-backed identity & access management companies

COMPANY	TOTAL VC RAISED (\$M)*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
 adjust	\$255.9	Fraud prevention	Fraud Prevention Suite	Data model-driven filtering	Highland Europe, Morgan Stanley, Sofina, Active Venture Partners, Target Partners
 ForgeRock	\$232.8	Identity governance & administration	Identity Platform	ML analysis of access vulnerabilities	Riverwood Capital, Accel, Meritech Capital, Foundation Capital
 riskified	\$228.1	Fraud prevention	Chargeback guarantee	Fraud model trained on billions of historical transactions and crowdsourced data	General Atlantic, Capital One Growth Ventures, Pitango Venture Capital, Qumra Capital
 pindrop	\$222.8	Fraud prevention	Phoneprinting technology	Analyzes over 1,300 audio features to validate caller profile	Vitruvian Partners, CapitalG, IVP, Andreessen Horowitz, Webb Investment Network, GRA Venture Fund
 SIGNIFYD	\$216.2	Fraud prevention	Guaranteed Fraud Protection	ML powers guaranteed anti-fraud for approved orders	Premji Invest, Bain Capital Ventures, Menlo Ventures, AllegisCyber
 Auth0	\$213.5	Identity governance & administration	Modern Identity Platform	APIs and SDKs for integration of access management with different development frameworks	Sapphire Ventures, Meritech Capital Partners, Trinity Ventures, Bessemer Venture Partners

Source: PitchBook | *As of June 30, 2020



IDENTITY & ACCESS MANAGEMENT

Figure 34.
Key identity & access management incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/REVENUE*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
	NASDAQ: OKTA	25.1x	Identity governance & administration	Single Sign-on	Ease of use for pre-built app integrations
	NYSE: SAIL	4.4x	Identity governance & administration	IdentityIQ Access Management platform	Simple configuration
	NASDAQ: MSFT	8.5x	Identity governance & administration	Azure Active Directory	Bundled with Microsoft 365 suite at a low cost
	NYSE: IBM	2.0x	Identity governance & administration/fraud prevention	IBM Security Access Manager (IGA) and Pinpoint (Fraud Prevention)	Bundled package of access management and fraud prevention
	TASE: NICE	5.9x	Fraud prevention	Actimize	Simple data integration tools

Source: PitchBook | *As of June 30, 2020



IDENTITY & ACCESS MANAGEMENT

Opportunities

Passwordless identity provisioning: Research finds that brute force access or use of stolen credentials comprise more than 80% of hacking-related breaches,²⁴ making the presence of passwords an intrinsic risk to organizations. Multifactor authentication and regular password updates help to address this problem but can slow productivity. Passwordless identity governance & administration platforms can eliminate credentials theft while reducing IT maintenance costs for password provisioning. These platforms use the identity of the device that an employee is using and analytics on the typical and approved behaviors of those devices to enable “Zero-Factor Authentication” and seamlessly manage access in a zero-trust framework. The scale of **Duo Security**’s \$2.4 billion exit to **Cisco** and the outperformance of Okta in single sign-on administration demonstrate the value of identity management to organizations, and we believe that passwordless management can produce similar outcomes. We expect the technology to become commonplace by 2023, at which time leading startups, including **Callsign**, **TruU**, **Beyond Identity**, **Secret Double Octopus**, **Hideez**, and **AnyLedger**, may be able to achieve scale.

Developer integrations with IGA platforms for hybrid identity deployments: Offering identity as a service (IdaaS), which refers to cloud-native IGA through micro-services and APIs, enables developers to build onsite solutions to unique identity needs. IAM has traditionally been a clunky on-premise solution but is increasingly delivered through the cloud. Even so, cloud-based solutions such as Okta do not work well with on-premise solutions, creating a gap for a point solution that allows developers to customize IAM solutions in hybridized environments. We believe remote access to corporate networks is

generally not designed to handle the uptick in capacity since COVID-19, and developers require flexible solutions to apply access rules to new services and APIs. Startups such as **ForgeRock** and **Auth0** have built API integrations that support hybrid cloud and onsite integrations. Okta has already closed an acquisition in the space with Stormpath, but those that have built a solution natively may prove more flexible and developer friendly.

Machine learning for fraud prevention: AI fraud prevention is an untapped frontier that may prove fundamentally better than legacy products. In network security, attacks are difficult to predict with historical data, which can be better suited to train models for fraud prevention due to the similarities of fraud attempts. Currently, machine learning is not being applied across customer channels to integrate disparate data streams. Many legacy vendors use a machine learning optimizer only on top of their existing rule-based systems, which is not as powerful as a ground-up machine learning-based approach. Startups such as **Feedzai** and **ThetaRay** have built fraud prevention engines driven by machine learning that have been able to compete with incumbents’ legacy products. Point solutions in this space have been acquisition targets for payments leaders, including Mastercard (**Konsensus**) and PayPal (**Simility**), and further acquisitions in the fintech space are possible.

Operational technology or IoT device management: The proliferation of IoT devices, referred to as operational technology in the infosec industry, requires advanced identity management solutions to ensure that a compromised device cannot contaminate the network. Many devices are put into use without security protection in place, with universal default usernames and passwords. Thus, hackers can simply log in to the device,

24: 2020 Verizon Data Breach Investigations Report, Verizon, 2020.



IDENTITY & ACCESS MANAGEMENT

gain access to its data, and move laterally through the network on which the device is registered. One survey indicates that 48% of a sample of 397 US executives reported suffering an IoT breach as a result of poor IAM.²⁵ Modern IAM service providers can reduce this threat by provisioning IoT devices and managing passwords. **ForgeRock** is taking advantage of this opportunity, and we believe additional innovation is needed.

Considerations

Incumbent leadership in IGA: We see SailPoint and Okta as leaders in IGA and unlikely to cede market share to challengers. Sailpoint has a cloud-architected IGA solution with a leading user experience and dominance in the large enterprise market. Okta has developed a cloud-first access management platform with growing functionality for developers. While these firms' market leadership may limit VC-backed challengers' ability to win market share, we see M&A potential as SailPoint and Okta look to incorporate additional technologies and capabilities.

High competition in fraud prevention: There are at least a dozen competitive fraud prevention platforms offering a range of features including behavior analysis and continuous risk assessment. We believe customers' different levels of risk tolerance support a more diverse ecosystem of vendors relative to security products, where the best feature sets tend to win. For this reason, we expect it will be difficult for private companies to achieve high market share and pricing power.

High switching costs for IAM solutions: IAM solutions typically require system integrators to deploy IGA software, adding high upfront costs to subscription fees. Gartner estimates

that 50%-200% of a three-year subscription can be spent in the first year on deployment costs due to the need to hire system integrators, making it onerous to switch vendors.²⁶ While this leads to high stickiness for IAM solutions with lesser risk of churn relative to other infosec segments, it also makes it harder to introduce disruptive solutions. For this reason, we believe IAM may ultimately consolidate around a few core vendors.

Outlook

Consolidation likely in IDaaS: Legacy vendors such as **Microsoft**, **Oracle**, and IBM may find themselves falling behind Okta and Sailpoint in the IGA space and make acquisitions to close the gap. **Auth0** is a likely acquisition target as incumbents recognize the shift left, though its latest funding round may have made an IPO more likely. While we view the IDaaS market as large enough to support IPOs, no startups appear to have gained the market leadership necessary to pursue such a route.

OT/IoT authentication and access control to be a winner-take-all space: Due to the poor quality of current IoT authentication, both the UK government and the National Institute of Standards and Technology (NIST) have published reports over the past 18 months calling for IoT security standards. While existing IAM solutions can manage user access to IoT devices using digital certificates, new technologies are needed to manage the access of each device to the network to prevent contamination of the network. **ForgeRock**, **Obsidian Security**, and **Rubicon Labs** all could develop a ground-up solution for the industry that applies public key infrastructure to manage the device certificates that have been created.²⁷ Each may be a tuck-in candidate for leading IoT security providers such as **Cisco** and **Gemalto**.

26: Gartner, "Magic Quadrant for Identity Governance and Administration," February 2018.

27: "New Research Project Aims to "Shrink" Public Key Infrastructure (PKI) Technology to Secure the IoT," Nexus Group, September 2017.

25: "Are Your Company's IoT Devices Secure? Internet of Things Breaches Are Common, Costly for US Firms," Altman Vilandrie & Company, n.d.



IDENTITY & ACCESS MANAGEMENT

Multiple fraud prevention unicorns likely to be created: Despite the competition in the market, its raw size means that innovative companies are likely to receive ample funding to unseat the incumbents. **Riskified** achieved this status in Q4 via its innovation in the chargeback guarantee niche of the market. Companies with machine learning technology, such as **Sift**, **Feedzai** and **ThetaRay**, can reach unicorn status by disrupting incumbents. **Feedzai** has already been named to the Tech Tour Growth 50, a list of the highest-growth companies in Europe in 2016 and 2017. The 2017 list also included **AlienVault**, **Darktrace**, Deliveroo, and SoundCloud. **Sift** and **ThetaRay** have also reported strong performance that may support loftier valuations.

SEGMENT DEEP DIVE

Endpoint security



ENDPOINT SECURITY

Overview

Endpoint security refers to the protection of data communicated through and stored in remote devices, detection of attacks on remote devices, and responses to these attacks by utilizing forensic analysis and remediating breaches. Endpoints include remote devices such as computers, phones, and servers. The endpoint market has traditionally addressed just the client side of the server but is currently expanding to cover the hosts as well, as cloud providers require endpoint protection on their servers to compete for client business. This niche is already one of the largest segments of the infosec market and may see consistent but slower growth than other subsegments.

Subsegments include:

Endpoint protection, detection & response platforms: Platforms that monitor endpoints for threats and remediate breaches through policy enforcement and patch management. This subsegment includes an array of product categories including:

- Endpoint protection platforms (EPP)
- Endpoint detection & response platforms (EDR)
- Email security
- Secure email gateways
- Mobile device detection & response

Edge device visibility & management solutions: Edge devices include IoT, operational technology (OT), and mobile devices. These solutions increase the visibility of distributed assets and enable security policy enforcement at the network edge. This subsegment includes mobile device management.





ENDPOINT SECURITY

Industry drivers

Increasing volume of endpoint attacks: While the types of endpoint attacks have not changed dramatically in recent years, the volume of phishing and malware attacks has increased rapidly as hackers automate new attacks and increase their efforts against small businesses.

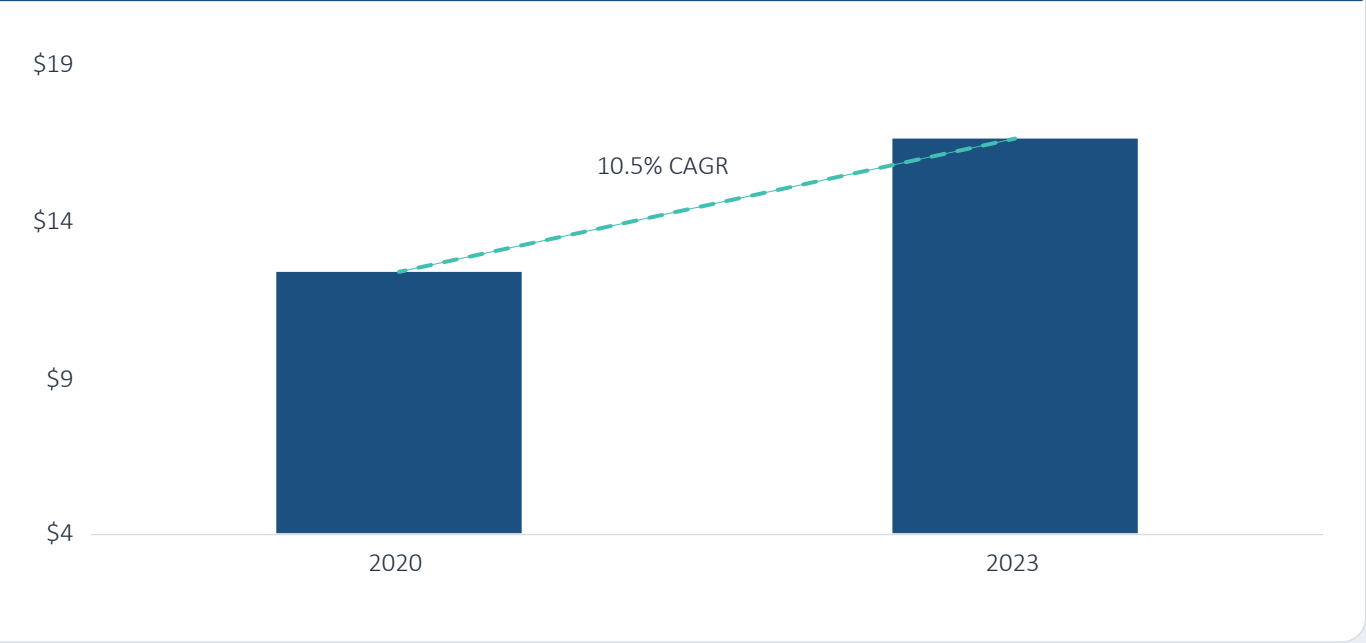
Emerging threat surfaces: The number of endpoint attack surfaces has multiplied in recent years, with mobile and IoT devices becoming indispensable parts of the enterprise. Attacks have been customized for each new attack surface, meaning that any device can be an entry point to the network.

Incumbent weakness: Incumbents have shown weakness in pushing updates to existing deployments, incorporating cloud and automation technologies, and addressing zero-day threats, which has created a shift to next-generation vendors such as **CrowdStrike** and Carbon Black.

Market size

The endpoint security market generated \$11.9 billion in sales in 2019. We expect this market to grow slightly in 2020 to \$12.4 billion, down from our original estimate, with high growth resuming in 2021. We forecast the market to nearly match our estimate in Q4 2019 for 2023 and grow to \$16.7 billion at a 10.5% CAGR from 2020. Endpoint protection, detection & response platforms dominate the segment, and we anticipate the industry will grow to \$9.8 billion by 2023. The IoT security market is forecast to grow more quickly at a 20.4% CAGR over the same time frame, though the market remains small at \$2.5billion as of 2020, and this

Figure 35. ENDPOINT SECURITY MARKET SIZE (\$B)



Source: IDC, Gartner, PitchBook | Geography: North America & Europe

Figure 36. COMMON INDUSTRY KPIS

Financial	Operational
<ul style="list-style-type: none">Cloud revenueCustomer countOrders over \$100,000/\$1 millionAverage license order size (\$)ARPU growth	<ul style="list-style-type: none">SaaS revenue %Maintenance renewal rateNumber of incident response engagements annuallyNumber of threat groups monitored



ENDPOINT SECURITY

growth may be slowed by an uncertain economic environment. In the long term, endpoint security will expand linearly with the number of devices deployed by enterprises across remote workforces and IoT.

Disruption potential

Improved threat hunting capabilities from startups and machine learning algorithms are disrupting the endpoint security market. Legacy endpoint security solutions can detect and quarantine attacks, but security analysts are required to conduct forensic analysis on those samples. Emerging services can use lightweight software agents to identify the nature of the attack in the wild and identify the appropriate response. Furthermore, machine learning is enabling improved detection and response capabilities, in contrast to the rules-based approaches of legacy EPPs. These innovations have created opportunity for startups to capture market share from leaders **McAfee** and **Symantec**. Endpoint security technology can be replaced in as little as three months with relatively simple IT integrations, resulting in low switching costs for enterprises to replace legacy technology with disruptive alternatives.

Business model

Endpoint protection, detection & response platforms, the largest subsegment within endpoint security, typically carries a subscription license fee on a per-endpoint basis with additional upcharges for premium services including threat hunting and vendor-managed detection and response.

The price per endpoint tends to range from \$30 to \$300 per year. Solutions can be deployed through the cloud or on-premise, with cloud services typically carrying higher prices and improved functionality.

VC activity

Endpoint security had a relatively weak Q2 in terms of VC deal activity, closing just 21 deals worth \$203.2 million in aggregate value. **Tanium** likely received an investment of \$100.0 million from Salesforce Ventures at a \$9.0 billion post-money valuation, but the deal size was not confirmed. This deal was joined by a partnership integrating **Tanium** into Salesforce Anywhere. Salesforce uses its CVC arm partly as an acquisition pipeline, making **Tanium** a target. **Upstream Security**, an automotive security platform, and **Inky**, an anti-phishing platform, achieved outsized deal size step-ups in Q2. Strategic investors in Renault-Nissan-Mitsubishi led the Upstream deal, likely improving the company's valuation. We identified **Inky** as a platform liable to benefit from increased phishing activity during COVID-19 in our **Q1 2020 PitchBook Analyst Note: The Ripple Effects of COVID-19 on Emerging Technologies**. It raised its round from Insight Partners, which has demonstrated willingness to pay high multiples for high-growth cybersecurity startups. We believe that an improved deal environment will bring high step-ups for EDR platforms experiencing high demand amid the pandemic.

VC exit activity in IoT security continued in Q2 2020 with **Microsoft's** acquisition of **CyberX**. The company's subsequent valuation of \$165.0 million illustrates a continued shakeout in



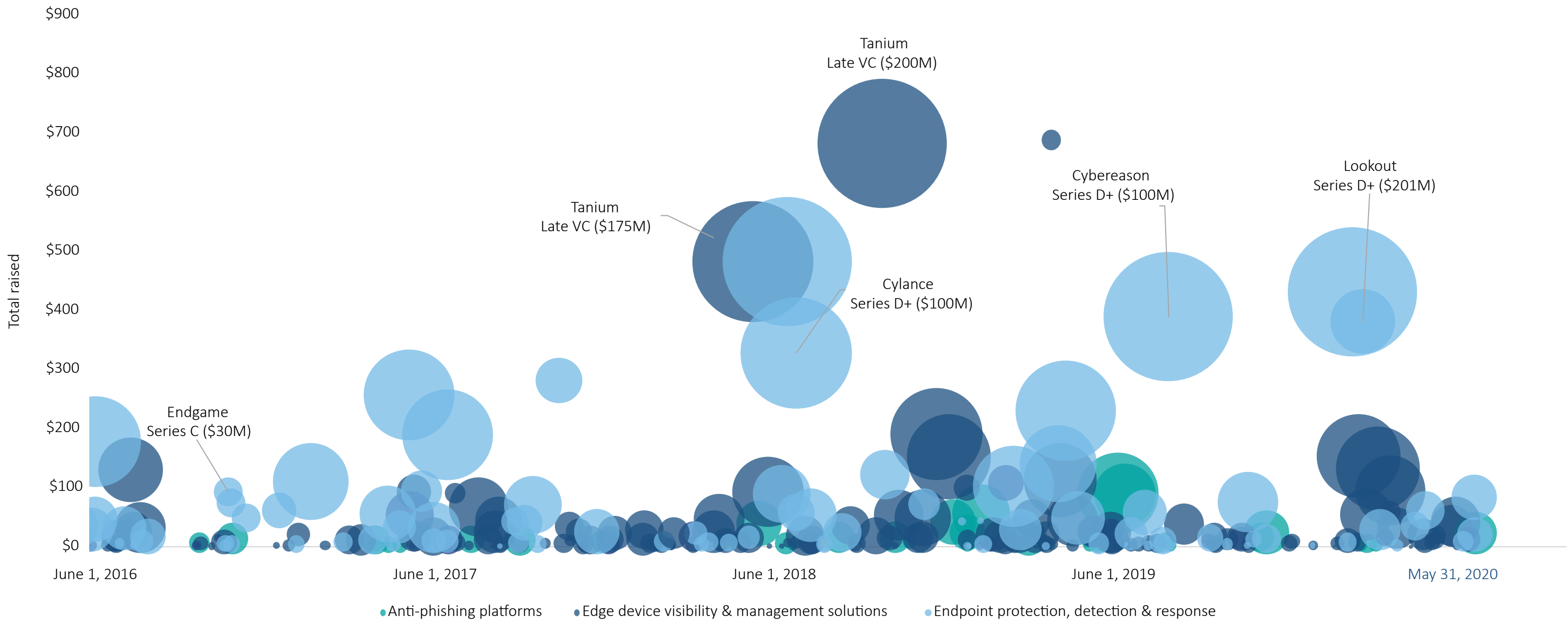
ENDPOINT SECURITY

IoT security. **CyberX** raised \$47.8 million before selling, suggesting that its exit was at a flat or down valuation for its late-stage investors. It has recently integrated machine learning threat detection capabilities and adds strategic value to **Microsoft**'s Azure Sphere product line. **Microsoft** is now able to deliver an integrated EDR platform for IoT devices, making it an increasingly formidable competitor in this space. **Armis**'s \$1.1 billion exit in Q1 appears to be an outlier given the high volume of IoT security exits under \$200.0 million in recent quarters. We believe the IoT security software market is still relatively small but addresses a major problem and can support further positive exits. Only two other minor acquisitions of endpoint security companies closed in Q2, but we believe that exit activity should resume at a high pace in a more certain investment environment.



ENDPOINT SECURITY

Figure 37.
Endpoint security VC landscape (\$M)



Source: PitchBook
Note: The left axis indicates total VC raised as of deal date. Bubbles indicate amount raised.








ENDPOINT SECURITY

Figure 38.
Notable endpoint security VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE (\$M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
 Upstream	June 9, 2020	Edge device visibility and management solutions	\$30.0	Series B	Renault-Nissan-Mitsubishi, Renault Venture Capital, Alliance Ventures	2.5x
 INKY®	June 4, 2020	Anti-phishing platforms	\$20.0	Series B	Insight Partners	1.9x
 AXONIUS	March 31, 2020	Edge device visibility and management solutions	\$57.6	Series C	Lightspeed Venture Partners	2.2x
 confluera	March 20, 2020	Endpoint protection, detection and response	\$20.0	Series B	Icon Ventures	1.9x
 ordr	March 5, 2020	Edge device visibility and management solutions	\$33.5	Series B	Battery Ventures	1.9x

Source: PitchBook

Figure 39.
Notable endpoint security VC exits




COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE (\$M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
 CYBERX	June 6, 2020	Edge device visibility and management solutions	\$165.0	Microsoft	N/A	4.9x
 ARMIS	February 11, 2020	Edge device visibility and management solutions	\$1,100.0	Insight Partners, CapitalG, DFJ Growth	N/A	N/A
 Indegy	December 2, 2019	Edge device visibility and management solutions	\$80.1	Tenable	N/A	N/A
 ENDGAME.	October 8, 2019	Endpoint protection, detection and response	\$234.0	Elasticsearch	0.50x	N/A
 CROWDSTRIKE	June 12, 2019	Endpoint protection, detection and response	\$6,075.4	NASDAQ	N/A	22.4x

Source: PitchBook



ENDPOINT SECURITY

Figure 40.
Key VC-backed endpoint security companies





COMPANY	TOTAL VC RAISED (\$M)*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
 TANIAM	\$687.1	Edge device visibility & management solutions	Tanium Asset and Tanium Discover	Enables quarantine of rogue assets including offline assets	Wellington Management, TPG, IVP, T. Rowe Price, Andreessen Horowitz, EP Executive Press
 SentinelOne	\$430.0	Endpoint protection, detection & response	Endpoint Protection Platform	Bundles EDR, EPP, and behavioral protection	Insight Partners, Redpoint Ventures, Third Point Ventures, Tiger Global Management, UpWest Labs
 cybereason	\$388.4	Endpoint protection, detection & response	Endpoint Detection & Response	Correlation engine to combine common endpoint alerts into single alert	SoftBank, Spark Capital, Charles River Ventures
 Lookout	\$380.7	Endpoint protection, detection & response	Mobile Endpoint Security	User-friendly integrations with SIEM and Mobile Device Management solutions	T. Rowe Price, Andreessen Horowitz, Index Ventures, Accel
 VENAFI	\$190.0	Edge device visibility & management solutions	TrustAuthority device monitoring platform	Continuous device discovery across virtual, cloud and IoT infrastructure	TCV, Intel Capital, QuestMark Partners, Silver Lake Management, Foundation Capital

Source: PitchBook | *As of June 30, 2020



ENDPOINT SECURITY

Figure 41.
Key endpoint security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/REVENUE*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
 CROWDSTRIKE	NASDAQ: CRWD	22.7x	Endpoint protection, detection & response	Falcon Platform	Bundled with managed threat hunting service
 McAfee™	TPG subsidiary	N/A	Endpoint protection, detection & response	Endpoint Security	Policy orchestration tool
 Symantec™	Broadcom subsidiary	4.7x (acquisition multiple)	Endpoint protection, detection & response	Symantec Endpoint Protection	Bundles malware protection, EDR, system hardening and deception tool
Carbon Black.	VMware subsidiary	9.9x (acquisition multiple)	Endpoint protection, detection & response	Cb Response	Proprietary data streaming technology enables cloud-based threat hunting analytics
 SOPHOS	Thoma Bravo subsidiary	5.4x (acquisition multiple)	Endpoint protection, detection & response	Intercept X	Protects against most ransomware

Source: PitchBook | *As of June 30, 2020



ENDPOINT SECURITY

Opportunities

Operational technology (OT)/IoT security: According to one survey, 92% of companies say that IoT will be important to their business in 2020,²⁸ making it a key growth market for security. In 2016, IoT devices were the vectors for major distributed denial-of-service (DDoS) attacks affecting PayPal, Amazon, Netflix, Spotify, and Twitter. Essential components of IoT security that may not be provided by the device vendor include penetration testing, end-to-end encryption, digital certificates for device authentication, integrity for boot process, updates and code signing, agentless device scanning, machine learning algorithms of typical device behavior based on industrial datasets, ICS/SCADA protocol integration for OT devices, and IoT network microsegmentation.

Because OT and IoT devices are deployed beyond the network perimeter, traditional EPPs do not always have visibility over those devices. Scanning technologies that can detect all devices with access to the network and implement policies outside the network can be essential for the deployment of large clusters of IoT devices. Acquisitions that closed in Q4 2019 illustrate how incumbents are pressured to acquire IoT security leaders. We believe **Darktrace** has generated a significant percentage of its \$135.8 billion in revenue from IoT network traffic analysis, emphasizing how many platforms can benefit from the growth of IoT devices. Furthermore, COVID-19 is pushing security departments to secure smart home devices, which requires innovative approaches such as those of **SAM Seamless Network**. In addition, OT devices that are not in constant communication with the internet but can access it may require distinct visibility scanners such as that developed by OT security specialist **Claroty**. We estimate 50% of IoT customers believe

they can protect their device fleets with existing security platforms, so demand may be suppressed by the recessionary environment in 2020.

Automation of endpoint security: Endpoint threats have historically required security analysts to manually review alerts. Automated platforms instead use a range of approaches including machine learning, correlation rules, statistics, and zero-trust lists. In a recent survey of large enterprises, AI-driven threat assessment and identification is ranked as the top defense concept prioritized by C-suite security leaders.²⁹ EDR challenger **SentinelOne** claims to offer full automation in threat detection, compared to **CrowdStrike**'s limited automation capabilities. **Cybereason**'s knowledge graph has produced the top-rated advanced EPP in **NSS Labs**' comparative test.³⁰ Given the high degree of customer turnover in the endpoint space, with **McAfee** losing market share due to an arduous update process, we believe endpoint challengers can gain market share much like **CrowdStrike** did. While legacy vendor Sophos and startup **Deep Instinct** offer endpoint threat detection based on deep learning, we believe this technology has not yet gained traction because of increased costs and overfit models.

Threat hunting automation: EPPs with active threat hunting, referred to as extended detection & response (XDR), can add value by identifying the presence of hackers before they deliver malware. Traditionally, endpoint platforms have integrated with SIEM platforms for alert triage, an approach that can cost valuable time while attackers are conducting reconnaissance in the network. To address this gap, threat hunting services identify hackers covertly monitoring an enterprise network and mitigate their attacks before they can achieve their objectives. Because hackers sometimes deploy advanced

29: "The Future of Cyber Survey," Deloitte, 2019.

30: "Endpoint Protection: Q2 2020 Comparative Ratings," NSS Labs, 2020.

28: "State of IoT Security Survey," Digicert, 2018.



ENDPOINT SECURITY

persistent threats for weeks or months before they can be detected, threat hunting is becoming an essential upgrade for endpoint customers and has allowed **CrowdStrike** to increase its net dollar retention rate to the best among publicly traded SaaS companies. Emerging startups such as **ReversingLabs** have automated threat hunting, closing the gap between SIEM and endpoint platforms. Early-stage company **Confluera** is addressing multiple market gaps by delivering continuous threat monitoring with a graphical user interface that tracks attacks as they develop, allowing security teams to more quickly threat hunt and conduct forensic analysis. The company raised a Series B in Q2 a year after emerging from stealth. Another early-stage startup **Hunters** has partnered with **CrowdStrike** to bring automated threat hunting to **CrowdStrike**'s managed threat hunting service, highlighting the need for more efficient threat hunting services. While the market is crowded, demand is high for improvements in threat detection times.

Sophisticated anti-phishing solutions: Given the high degree of concern around COVID-19, hackers have created new phishing attacks, which refer to fraudulent communications intended to steal data or install malware. A prominent version of these phishing attacks is disguised as a COVID-19 tracker, mimicking popular resources such as the Johns Hopkins COVID-19 map. We believe that the anti-phishing market is mature but that existing tools do not utilize predictive analytics to determine zero-day phishing attacks. Furthermore, legacy tools require extensive custom configurations that are too complex for SMBs. Because of the increasing percentage of sensitive information transmitted by email instead of in-person communications, we believe enterprises may adopt advanced anti-phishing capabilities offered by emerging startups including **Ironscapes**, **Avanan**, and **Inky**. On the early side, **PhishCloud** has developed a self-

learning platform that visually highlights phishing attempts to employees across email, social media, and the broader internet, taking the burden off of security teams to review suspicious links.

Considerations

Customer churn: Constantly evolving threats may render new technologies obsolete and increase customer churn, and old systems can be retired if they do not keep up. The benefits of endpoint security depend on its ability to address emerging threats in malware, phishing, and ransomware more quickly and effectively than incumbents. EPP and EDR systems can be deployed rapidly; a recent survey finds that over 50% of users are able to deploy such solutions in three months or less.³¹ We believe speed of implementation is critical for firms seeking to quickly upgrade their ability to detect and respond to advanced threats, and providers that cannot move swiftly risk significant loss of market share.

Security staff skillsets a limitation on product-market fit: Despite advanced feature sets and automation capabilities, emerging endpoint solutions often require manual supervision to address alerts and false positives, which can reduce the actual addressable market for some emerging vendors. Existing IT and security staff may not have the skills needed to effectively use sophisticated solutions. This dynamic has been both a challenge for some vendors, such as Carbon Black and Kaspersky Lab, and a benefit for others, such as Panda Security, which automates the creation of zero-trust policies, removing a complex workload for security staff.

31: "State of Endpoint Security Risk," Ponemon Institute, 2018.



ENDPOINT SECURITY

Crowded market: The endpoint market is highly competitive and a difficult space in which to win market share. Numerous next-generation endpoint vendors have challenged legacy vendors in recent years, including **CrowdStrike**, Carbon Black, and **Cylance**. As these newer entrants have established market leadership, it may be difficult for the next wave of challengers to gain a foothold in the marketplace, which we believe helps explain the muted exit performance of EPP and EDR companies as of late.

Automation can fail in practice: Machine learning models are trained on historical data and use linear correlations to make decisions about new incidents. For this reason, they are not foolproof against future attacks and can both create false positives and miss zero-day attacks. We believe AI-infused threat intelligence has become a source of disillusionment among CISOs, and companies with innovative automation technologies in this area may not necessarily gain traction.

Outlook

Consolidation in mobile and email security: We believe mobile and email point solutions will be acquired by larger EPP providers. Emerging threat surfaces create pressure for incumbents to expand the number of endpoints covered. **Symantec**'s acquisition of **Skycure** was an early example of an incumbent addressing an emerging threat surface through an acquisition. Mobile and email security startups are not likely to scale organically and should see continued M&A activity in the near term. In mobile, **Zimperium** and MobileIron may be potential targets, though they are not likely to achieve unicorn status. In email, **Avanan** has developed solutions for several common vulnerabilities for **Microsoft** Office 365 and thus may be a logical acquisition target for **Microsoft**.

A shakeout in IoT security to continue: IoT security startups may sell earlier than they intended given the challenging environment created by the pandemic. We believe **Sentryo** may have acknowledged these difficulties by selling to **Cisco** after its Series A. Investors should expect a depressed IoT market to be reflected in the valuations they accept for IoT security startups. **Armis** has provided a counterpoint to this thesis, but we believe that the deal may prove to be an outlier in this stressed environment, especially given the limited appetite for IoT-specific solutions. Additional network and endpoint security vendors may join other incumbents in pursuing IoT and OT security from startups including **Mocana**, **Nozomi Networks**, **Claroty**, and **VDOO**.

EDR startups to organically gain market share and scale: Given the high customer churn in the endpoint space, we believe startups have the potential to disrupt incumbents and achieve scale. As there is little moat between companies in the subsegment, emerging platforms such as **SentinelOne**, **Ziften**, and **Cybereason** should be able to continue growing. We believe **Symantec** and **McAfee** may face pressure to acquire automation-driven endpoint platforms or else see their market share erode. Because of the disruption potential in this market, EDR may produce further outlier exits after **CrowdStrike**.

SEGMENT DEEP DIVE

Security operations



SECURITY OPERATIONS

Overview

Security operations technology aids the critical functions of the enterprise’s security operations center (SOC) or equivalent entity in utilizing the tools mentioned earlier in this report. These functions can include:

- Quantification of security risks
- Security alert management
- Integration and coordination of security tools at all levels of the kill chain
- Tracking the performance of security technologies

The role of a separate layer of operations technology becomes important when enterprises have dozens of security tools that must speak to each other and provide actionable information for the security team. Furthermore, managed services permit 24/7 monitoring and administration of a security center. These managed service offerings allow for the SOC to be outsourced while opening the SMB markets that are often viewed as afterthoughts in the traditional infosec market.

Subsegments include:

- **Log ingestion and security information & event management (SIEM):** Platforms that enable the analysis of security log data from multiple sensors across endpoints in the network
- **Security orchestration, automation & response (SOAR):** Platforms that automatically respond to security log data, including orchestration of the full stack of incident response and remediation solutions





SECURITY OPERATIONS

- **Security risk assessment & management:** Platforms that measure the vulnerability of various enterprise threat surfaces and in some instances quantify the value at risk to the enterprise in case of a breach
- **Managed security services:** Services that provide security analysts on a contractual basis to remotely carry out the work of a security team, some of which include software for managed detection and response

Industry drivers

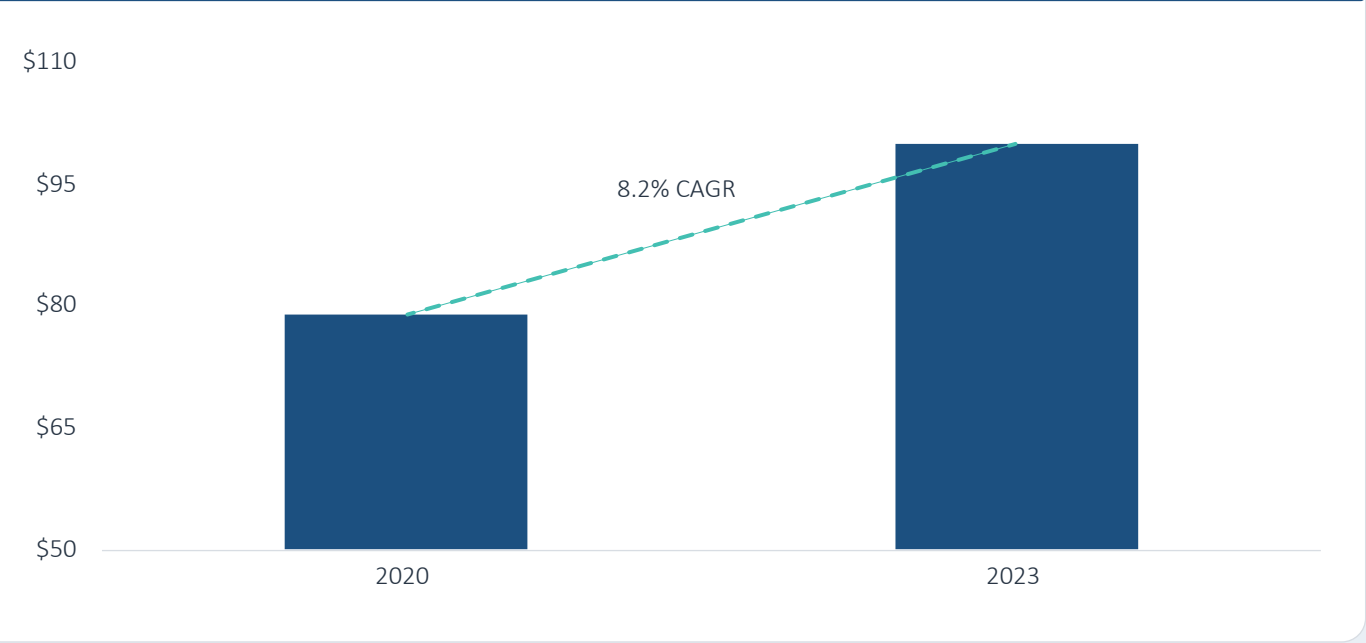
Security talent shortage: A shortage of security talent is driving CISOs to invest in software to handle alerts. A recent survey found that 44% of IT departments have a problematic shortage of cybersecurity skills at their organization.³² This percentage dropped slightly for the first time since 2015.

Increasing alert volume: The number of publicly disclosed security breaches increased 60.3% from 4,223 in 2016 to 6,773 in 2017 and set further highs in 2018 and 2019.³³ These breaches create security workflows that must be managed by security operations software or by managed security services.

Tool sprawl: The proliferation of security tools necessitates more automation and orchestration solutions. “The average enterprise uses 75 security tools,” according to Stephan Chenette, CTO and co-founder of **AttackIQ**.

32: “ESG Research Report: 2020 Technology Spending Intentions Survey,” ESG Research, Bill Lundell, February 2020.
33: “2019 Year End Report: Data Breach QuickView,” Risk Based Security, 2020.

Figure 42. SECURITY OPERATIONS MARKET SIZE (\$B)



Source: Gartner, PitchBook | Geography: North America & Europe

Figure 43. COMMON INDUSTRY KPIS

Financial	Operational
<ul style="list-style-type: none">• Cloud revenue• Customer count• Orders over \$100,000/\$1 million• Average license order size (\$)• ARPU growth	<ul style="list-style-type: none">• SaaS revenue %• Maintenance renewal rate• Number of incident response engagements annually• Number of threat groups monitored



SECURITY OPERATIONS

Market size

In 2019, security operations represented the largest infosec segment at \$78.9 billion. We expect the market to continue growing in 2020 and to become a \$100.9 billion market by 2023, growing at an 8.2% CAGR in that time frame. This market size reflects end-user spending in all four of the subsegments we outlined for the security operations segment. At \$70.2 billion, the managed security services space was the largest contributor to the market as of 2019 given the prevalence of outsourced security services. We expect VC-backed companies to capture market share in this subsegment given the lack of technological innovation in the niche. We forecast SIEM and SOAR to outpace the market at 12.2% and 17.4% CAGRs, respectively. The high-growth forecast in SOAR is a primary reason for the subsegment's high levels of VC and M&A activity.

Disruption potential

The security operations industry is dominated by managed security services companies that rely on manpower to streamline the security workflows of client portfolios. These companies face the same limitations as internal security teams in responding to cascades of security alerts and often do not have unique IP to address them. Because they rely on a limited supply of labor, they can charge high prices based on the level of service they provide. Startups can automate the work of managed services companies, saving enterprises on the cost of security services and enabling them to gain massive increases in efficiency across a constantly escalating number of threats.

Business model

Security operations business models differ by product. SOAR platforms are based on SaaS subscriptions for security analysts. **Demisto**, for example, starts pricing at \$50,000 per analyst. SIEM platforms are charged based on log data capacity and can cost a large enterprise \$250,000 annually. Risk assessment products can have one-time charges for self-assessments and then recurring payments for users to analyze a dashboard of risk ratings. Third-party risk analysis platforms charge based on the number of vendors and benefit from increases in the number of vendors at use within the enterprise.

VC activity

Q2 was an outstanding quarter in terms of security operations VC deal activity, with \$411.3 million invested across 21 deals. Security operations startups are benefiting from increased SMB budgets, which lean on technology vendors to support understaffed security teams. We have continued to see low activity in SIEM and SOAR, and startups in those segments could be challenged by a dampened funding environment.

Three companies closed deals of \$50 million or more, including **Coalition**, a cyberinsurance provider; **Synack**, a penetration testing platform; and **Expel**, a tech-enabled managed security services provider. **Coalition** and **Synack** achieved significant valuation step-ups with these latest VC infusions, suggesting that the companies are achieving high growth through the pandemic. **Coalition** reportedly grew its logo count by 600% YoY. **Synack** benefits from the remote work trend because it connects ethical



SECURITY OPERATIONS

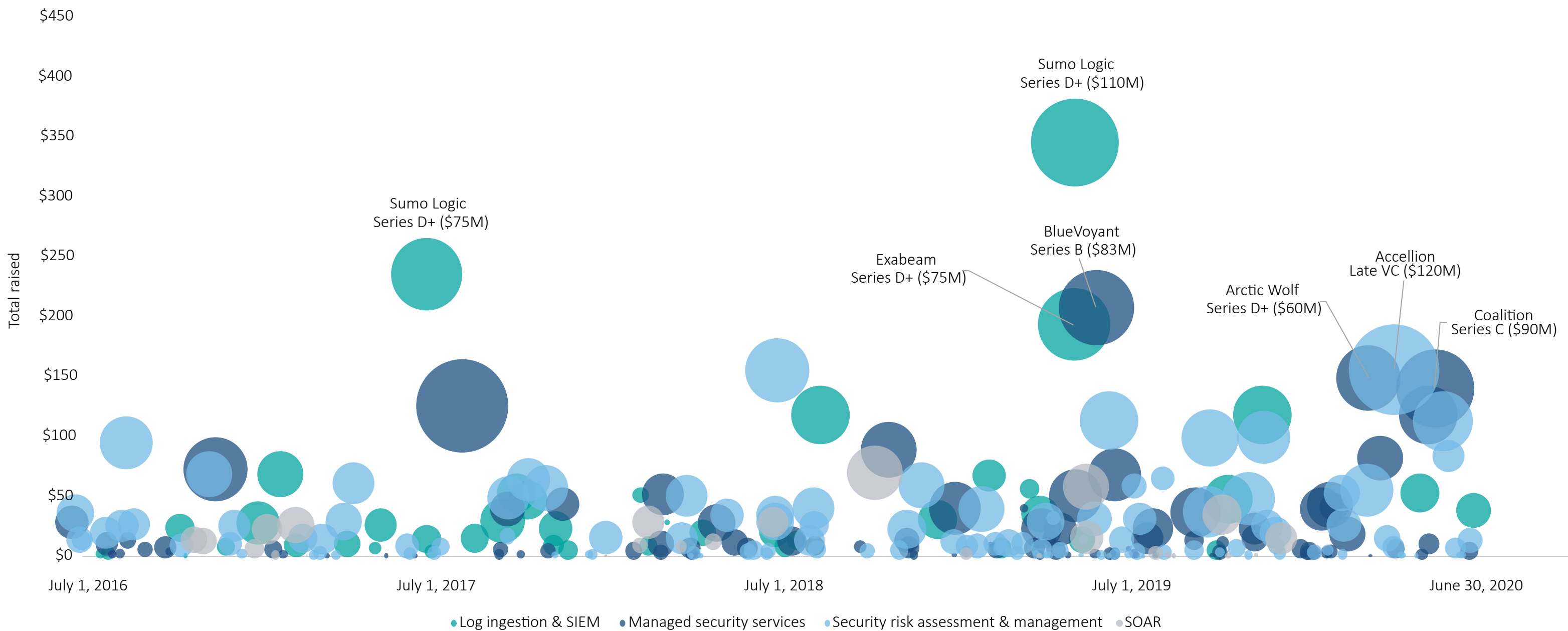
hackers with enterprises and has been experiencing increased demand during the pandemic. CapitalG led **Expel**'s \$50.0 million Series D, which we believe signals a strong product-market fit given the firm's recent exits in **CrowdStrike**, **Cloudflare**, and **Zscaler**.

We tracked only two exits in Q2, suggesting acquisition activity in the security operations segment will be muted through the remainder of 2020. SOAR startup **Swimlane** bought smaller SOAR startup **Syncurity** in what was likely an acqui-hire. As a result, we believe that **Swimlane** is slightly better positioned to take advantage of the SOAR market's high growth forecast with the additional incident response IP. **Cronus Cyber**, an automated penetration testing platform, sold to universal platform vendor **Orchestra Group** after raising just a few early-stage VC rounds. We believe that automated penetration testing is an emerging technology with a nascent market. In a recovery scenario, incumbents may find value in SOAR startups, so we would expect to see further acquisitions in the space. The large rounds in security risk assessment & management platforms will likely draw acquisition interest from managed security services vendors to improve their technology capabilities.



SECURITY OPERATIONS

Figure 44.
Security operations VC landscape (\$M)



Source: PitchBook
Note: The left axis indicates total VC raised as of deal date. Bubbles indicate amount raised.



SECURITY OPERATIONS

Figure 45.
Notable security operations VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE (\$M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
 Synack	May 28, 2020	Security risk assessment & management	\$52.0	Series D	C5 Capital, B Capital Group	2.2x
 Coalition™	May 20, 2020	Managed security services	\$90.0	Series C	Valor Equity Partners	3.1x
 expel™	May 13, 2020	Managed security services	\$50.0	Series D	CapitalG	1.6x
 bugcrowd <small>#1 Crowdsourced Security Company</small>	March 23, 2020	Managed security services	\$30.0	Series D	Rally Ventures	1.2x
 ARCTIC WOLF	March 11, 2020	Managed security services	\$60.0	Series D	Stereo Capital, Blue Cloud Ventures	1.2x

Source: PitchBook

Figure 46.
Notable security operations VC exits







COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE (\$M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
 SYNCURITY <small>Built by Analysts. For Analysts.</small>	April 16, 2020	SOAR	N/A	Swimlane	N/A	N/A
 J A S K	November 4, 2019	Log Ingestion & SIEM	N/A	Sumo Logic	N/A	N/A
 » VERODIN™	May 28, 2019	Security risk assessment & management	\$264.9	FireEye	2.63x	N/A
 tufin	April 11, 2019	SOAR	\$439.6	NYSE	N/A	6.3x
 DEMISTO	March 28, 2019	SOAR	\$560.0	Palo Alto Networks	2.57x	N/A

Source: PitchBook



SECURITY OPERATIONS

Figure 47.
Key VC-backed security operations companies

COMPANY	TOTAL VC RAISED (\$M)*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
 sumo logic	\$345.2	Log ingestion & SIEM	Cloud SIEM	Integrated with IT log management	Battery Ventures, Sapphire Ventures, DFJ Growth, IVP, Sequoia Capital, Accel, Sutter Hill Ventures
 BlueVoyant	\$207.5	Managed security services	Managed Detection and Response	24/7 outsourced security operations center	Fiserv, 8VC, DNS Capital, Winton Ventures
 exabeam	\$193.0	Log ingestion & SIEM	Incident Response and Automation	Cost savings from unlimited data lake	Lightspeed Venture Partners, Sapphire Ventures, Cisco Investments, Icon Ventures, Norwest Venture Partners, Aspect Ventures
 BITSIGHT	\$154.4	Security risk assessment & management	BitSight for Third-Party Risk Management	Security Ratings	Warburg Pincus, GGV Capital, Comcast Ventures, Menlo Ventures, Singtel Innov8, Commonwealth Capital Ventures
 ARCTIC WOLF	\$148.5	Managed security services	Security as a service	Managed detection & response	Stereo Capital, Blue Cloud Ventures, Australia Future Fund, Sonae IM, Redpoint Ventures, Lightspeed Venture Partners
 Coalition™	\$140.0	Managed security services	Cyber-insurance	Bundled security services and insurance policies	Felicis Ventures, Ribbit Capital

Source: PitchBook | *As of June 30, 2020



SECURITY OPERATIONS

Figure 48.
Key security operations incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/REVENUE*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
	NASDAQ: SPLK	13.5x	SIEM & SOAR	Security Intelligence Platform	Powerful monitoring functionality bundled with other IT data collection use cases
	NYSE: DELL	1.0x	SIEM & SOAR	SecureWorks	Bundles SIEM, network monitoring, EDR and behavior analysis
	NYSE: IBM	2.2x	SIEM & SOAR, managed security services	QRadar	Marketplace contains IBM and third-party integrations
	TPG Subsidiary	N/A	SIEM & SOAR	Enterprise Security Manager	Modern architecture using Kafka and Elasticsearch

Source: PitchBook | *As of June 30, 2020



SECURITY OPERATIONS

Opportunities

SOAR: SOAR technologies can take advantage of security skill shortage. SOAR platforms can integrate the numerous security tools that enterprises use. They automatically respond to security events aggregated by SIEM solutions and execute basic playbooks such as patching and policy enforcement. The SIEM solutions on the market now require full-time staff to manage, and SOAR can free these limited workers to pursue higher-value patching and configuration work. COVID-19 hiring freezes have intensified this need. We believe **Palo Alto Networks**' recent acquisition of **Demisto** demonstrates the blue sky in this subsegment. Emerging leaders within this niche include VC-backed **DF Labs**, **Swimlane**, and **Siemplify**. Other VC-backed companies such as **Exabeam**, **Respond Software**, and **SaltStack** may benefit as incumbent vendors make acquisitions in the space.

Security risk assessment tools: Security risk assessment tools scan an enterprise's network for threat surfaces and determine the value at risk if those surfaces are breached. They can enable CISOs to make a greater case for infosec funding from CIOs and CEOs, thus increasing demand. Furthermore, as boards increasingly create infosec committees, risk assessment and cyber-insurance will become necessary investment areas. VC-backed companies including **RiskLens**, **SecurityScorecard**, and cyber-insurer **Coalition** stand to benefit from this trend. We believe that the area will advance with further innovation in business impact modeling.

Small to medium-sized businesses: The SMB market could prove lucrative for VC-backed companies that are developing outsourced SOC solutions aiming to capture market share from established managed security service providers. We believe mid-sized enterprises

are increasingly seeking turnkey managed detection and response systems in addition to traditional monitoring services. A survey indicates that 26% of US SMBs plan to increase their security budgets as a result of remote work.³⁴ Startups can benefit by offering turnkey software platforms to “switch on” a 24/7 SOC and baked-in managed detection & response with little integration work. SOC-as-a-service companies that could capitalize on these trends include **Expel**, **deepwatch**, and **Cygilant**. SOC-as-a-service providers could also be attractive add-ons for incumbent managed security service providers with limited managed detection and response capabilities.

Considerations

Crowded SIEM and SOAR markets and rapidly innovating incumbents: SIEM is a mature market with numerous point solution vendors. For example, **Sumo Logic**, an IT vendor, integrates SIEM with its log management platform. Incumbents such as Splunk, through its Phantom acquisition, and IBM have developed in-house SOAR solutions. RSA uses a white-labeled **Demisto** SOAR. Because of the competition, even well-funded SIEM/SOAR startups may struggle to achieve scale. **Demisto** is a leader in the market and yet did not achieve unicorn status, suggesting that the market's upside potential may be limited.

SaaS vendors disrupting managed security services: While mid-sized enterprises can benefit from outsourcing their security operations centers, larger enterprises have the staffing to take advantage of lightweight SaaS tools with analytics and managed services functionality. For example, **CrowdStrike** offers managed detection and response in addition to its automated threat detection platform, limiting the amount of service needed. While

34: “Business Survey 2020: The COVID-19 Pandemic Will Accelerate the Cyber-Security Spend of SMBs in the USA,” Analysys Mason, June 2020.



SECURITY OPERATIONS

most CISOs likely need either a SIEM for their security tools or SOC as a service, they presumably do not need both, and we believe the software approach is likely to win.

COVID-19 to delay security operations platforms installations: SIEM platforms can take months to integrate at a time when organizations are not pursuing long-term investments. Furthermore, legacy products have gained reputations as labor-intensive and expensive. This could challenge startups that prioritize SIEM data or put SOAR on top of SIEM alerts. Going forward, enterprises could seek to bundle IT log management with SIEM to save costs and deployment time, a capability offered by larger vendors including Splunk and **Sumo Logic**.

Outlook

Incumbents to continue adding SOAR capabilities to their product suites through M&A: **Palo Alto Networks** was not a leader in SIEM and yet paid a high price for **Demisto** to enhance its SOAR capabilities at 27.3x revenue. Fortinet recently continued the trend with its cost-effective purchase of **CyberSponse**. We expect that SIEM leaders will enhance their product portfolios and identify several automation providers including **Exabeam**, **Siemplify**, **Swimlane**, **Respond Software**, and **SaltStack**. Incumbents requiring such a solution include Thoma Bravo's LogRhythm and **Micro Focus**, among others. SOAR startups may receive compelling acquisition offers early in their development.

Automation of security operations centers to accelerate: We believe the COVID-19 pandemic will push enterprises toward adoption of SOAR platforms, SIEM platforms with automation features, and automated incident response platforms for both network and endpoint security. The SOAR market is still small, and many enterprises focus on integrating tools internally instead of seeking solutions externally. Companies also rely heavily on

managed security service providers that reduce the need for automation. We believe cost savings and frozen security budgets will lead to offsetting managed security services with automation features. SOAR platforms cannot replace security analysts, but they can make them more efficient and address the increasing alerts that will come from remote work and cloud environments.

Pure-play software vendors to challenge analyst-reliant managed security service providers: VC-backed startups in managed security services leverage both software and professional services to provide 24/7 monitoring. While some of these startups have attracted substantial funding to scale their models, the growing volume of new threats and the ongoing infosec skills shortage could tip the scales in favor of nimbler pure-play software solutions. We believe investors should scrutinize the operating leverage of managed security service providers as the higher-margin profile of pure-play software startups will merit higher valuations.

Supplemental materials



SUPPLEMENTAL MATERIALS

Select company analysis



Founded in 2012	Leader in the Gartner Magic Quadrant for CASB, Forrester Wave for Cloud Security Gateways and IDC MarketScape Worldwide Cloud Security Gateways Vendor Assessment
Over 1,000 employees in four offices globally	Last financing post-money valuation: \$2.8B Last financing: Raised \$340M in a Series G
Total raised: \$744M	Lead investors: Sequoia Capital, Lightspeed Venture Partners, Iconiq Capital, Accel

Business overview

Netskope has developed market leadership in cloud security despite incumbents’ arms race to add CASB functionality. Its **Netskope** Security Cloud is an enterprise security platform that provides cloud usage governance. The platform protects SaaS, cloud user identities and internet traffic and optimizes for multi-cloud environments with network, endpoint and application security across the entire cloud stack. As a result, its cloud layer oversees the full range of all network activity. The platform utilizes ML algorithms for

threat detection and data loss prevention (DLP). Its proprietary content delivery network can route customers to their cloud environments without backhauling through a corporate VPN, a critical capability for the remote work transition that is being enabled by Secure Access Service Edge (SASE) architecture. In Q2, **Netskope** has shown the ability to benefit from remote work via integration with **Microsoft** Teams and partnerships with Okta, **CrowdStrike** and Proofpoint. The company reported 80% growth in enterprise customers in 2019.

Management

The **Netskope** management and board of directors has substantial experience at publicly traded companies that we believe increases the likelihood the company is pursuing an IPO. CEO and co-founder Sanjay Beri was formerly VP and GM at Juniper Networks’ secure access business unit. CFO Drew del Matto held the same position at Citrix and Fortinet. The board includes the former CEO of **Symantec** Enrique Salem. We view this as a relatively experienced bench that may help the company succeed as a public company.

Competitive differentiation

As a leader in the field, **Netskope** competes with other CASBs, principally **Symantec**, **Bitglass** and **McAfee**. As an early mover in the space in 2012, **Netskope** developed a full stack approach to PaaS and SaaS security earlier than competitors, which have had to



SUPPLEMENTAL MATERIALS

Select company analysis



stitch together point solutions to address the full cloud stack. As it has innovated, its DLP engine has become a superior offering to other CASBs, in line with DLP-only vendors. Further, the company has recently announced a zero-trust application security product that moves it into an adjacent segment and an edge infrastructure that allows it to incorporate IoT devices in low connectivity environments. Due to these developments, we believe that **Netskope**, **Palo Alto Networks** and **Zscaler** are emerging as vendors with the most advanced product suites for SASE. Unlike some competitors, we believe **Netskope** is limited in its ability to govern devices outside of the enterprise. For this reason, it must be complemented with an IAM or application security solution to ensure that unmanaged devices do not become attack vectorsfor the cloud.

Outlook

After **Netskope**’s Series G, we believe the company may become a private acquirer of startups in security operations, with an IPO likely in the medium term. The company has joined an elite group of late-stage software companies kept private by Sequoia Capital, including Stripe, Robinhood and Snowflake. We believe the company is well-positioned to build a full SASE stackand could benefit from acquisitions in cloud workload protection, IoT security and third-party risk management. We also believe the company is well-positioned to fill gaps in its product suite before IPO. The company is on track to scale to the size of other network security incumbents that are valued at \$10 to \$20 billion.

Financing history

<div><div>SERIES G</div><div>February 6, 2020</div><div>Total raised (\$M): \$340</div><div>Pre-money valuation (\$M): \$2,460</div><div>Investors: Sequoia Capital (lead), Canada Pension Plan Investment Board, Public Sector Pension Investment Board, Existing Investors</div></div>	<div><div>SERIES F</div><div>November 13, 2018</div><div>Total raised (\$M): \$167.8</div><div>Pre-money valuation (\$M): \$1,225</div><div>Investors: Lightspeed Venture Partners (lead), Accel. Base Partners, Geodesic Capital, ICONIQ Capital, Omega Venture Partners, Sapphire Ventures, Social Capital</div></div>	<div><div>SERIES E</div><div>April 27, 2017</div><div>Total raised (\$M): \$100</div><div>Pre-money valuation (\$M): \$425</div><div>Investors: Lightspeed Venture Partners (lead), Accel (lead), Dell Technologies Capital, Geodesic Capital, ICONIQ Capital, Sapphire Ventures</div></div>
<div><div>SERIES D</div><div>September 3, 2015</div><div>Total raised (\$M): \$75</div><div>Pre-money valuation (\$M): \$275</div><div>Investors: Iconiq Capital (lead), Accel, Lightspeed Venture Partners, New York Life Ventures, Social Capital, ICONIQ Capital</div></div>	<div><div>SERIES C</div><div>May 15, 2014</div><div>Total raised (\$M): \$35</div><div>Pre-money valuation (\$M): \$150</div><div>Investors: Accel (lead), Lightspeed Venture Partners, Social Capital</div></div>	<div><div>SERIES B</div><div>October 3, 2013</div><div>Total raised (\$M): \$21</div><div>Pre-money valuation (\$M): \$54</div><div>Investors: Lightspeed Venture Partners, Social Capital</div></div>



SUPPLEMENTAL MATERIALS

Select company analysis



Founded in 2014	Visionary in Gartner Magic Quadrant for application security testing
About 277 employees in five offices globally	Strong performer in Forrester Wave for runtime application self-protection
Total raised: \$120M	Last financing post-money valuation: \$480M Last financing: Raised \$65M in a Series D Lead investors: Warburg Pincus, Battery Ventures, General Catalyst, Acero Capital

Business overview

Contrast has developed a novel approach to security testing that enables it to run in a wider variety of production environments than legacy solutions. **Contrast** offers interactive application security testing (IAST) that automatically analyzes software composition on a continuous basis. The testing agent works within the application and, unlike static or dynamic security testing, does not generate attacks for testing from an external component, instead analyzing the code itself for known vulnerabilities.

The test embeds runtime application self-protection (RASP) scanners that travel with the application between cloud environments. The company is benefiting from regulatory tailwinds as the NIST Cybersecurity Framework revisions include IAST as a recommendation, though the novelty of the technology may not make it a high-growth category during COVID-19. **Contrast**’s growth metrics compare favorably to **CrowdStrike**, though at a lower revenue base (see page 85). Their net retention rate would rank among the leaders of publicly traded security companies as would ARR growth. The growth of large transactions highlights demand among large enterprises for DevOps security tools. We believe these fundamentals provide justification for the 108% valuation step-up in just one year, a meteoric rise for a late-stage VC valuation.

Leadership

Contrast’s leadership team have all led companies through acquisitions, suggesting that **Contrast** will be well positioned for an acquisition as well. CEO Alan Naumann was formerly CEO at VC-backed 41st Parameter Inc. until its acquisition by Experian. Before that, Naumann was CEO of CoWare until its acquisition by **Synopsys**. Co-founder and CTO Jeff Williams was formerly co-founder and CEO of Aspect Security, an application security consulting company acquired by Ernst & Young. In Q2, the board added a former sales executive from AppDynamics, which achieved a \$3.7 billion exit to **Cisco**.



SUPPLEMENTAL MATERIALS

Select company analysis



Competitors

Contrast competes with web application firewall vendors via its RASP solution and some application security testing vendors via its IAST solution. Its RASP solution is portable and so can travel with applications between cloud environments, unlike web application firewalls, which apply static rules across applications. **Contrast** leads the market in interactive application security testing (IAST), though it does not offer conventional static, dynamic or runtime security testing. Market leader **Synopsys** offers a full suite of testing tools whereas **Contrast** only offers IAST and software composition analysis, making it a complement to leading vendors rather than a substitute. The agent-based approach of IAST allows the software to be more accurate down to the line of code than static or dynamic testing. **Contrast** has an advantage in software composition analysis and views itself as a compliment to leading incumbents including **Synopsys**, Checkmarx, and **Micro Focus**.

Outlook

We view **Contrast** as a prime acquisition candidate for growth-starved incumbents in application security testing. DevOps security has not seen high acquisition activity outside of **Synopsys**'s roll-up and PE has stepped in to acquire high growth companies in the space. We believe **Contrast** could be a candidate for a "private IPO" round to keep it private given the interest of PE and growth equity firms in the DevOps security space.

Financing history

SERIES D	SERIES C	SERIES B
February 28, 2019 Total raised (\$M): \$65 Pre-money valuation (\$M): \$415 Investors: Warburg Pincus (lead), Battery Ventures, Acero Capital, AXA Venture Partners, General Catalyst, M12	March 1, 2018 Total raised (\$M): \$30 Pre-money valuation (\$M): \$169.8 Investors: Battery Ventures (lead), Acero Capital, AXA Venture Partners, General Catalyst, In-Q-Tel, M12	September 28, 2016 Total raised (\$M): \$16 Pre-money valuation (\$M): \$64 Investors: General Catalyst (Lead), Acero Capital
SERIES A	FINANCIAL METRIC	GROWTH YOY (FY18)
June 25, 2014 Total raised (\$M): \$8.6 Pre-money valuation (\$M): \$12.8 Investors: Acero Capital	Annual recurring revenue	>120%
	Net retention rate	>135%
	Number of transactions \$1 million or greater	500%

Source: **Contrast Security**



SUPPLEMENTAL MATERIALS

Select company analysis



Founded in 2013	Visionary in Gartner Magic Quadrant for Access Management
	Last financing valuation: \$1.2B
About 650 employees in 33 countries	Last financing: Raised \$103M in a Series E
	Lead investors: Sapphire Ventures, Meritech Capital Partners, Trinity Ventures, Bessemer Venture Partners
Total raised: \$213.5M	

Business overview

Auth0 builds market leading developer tools for IAM solutions. **Auth0** offers APIs and SDKs to developers to build single sign-on (SSO), multi-factor authentication and passwordless logins and customize them to unique enterprise environments. The solution resembles strategies used by Stripe or Twilio in that developers have access to simple code-based integrations that embed the service within existing systems. The company has a freemium model in which most of its customers pay nothing for just a few logins per

day using its tools. It has announced several key commercial milestones including a record quarter in Q4 2019 and 70% growth in sales and new customers. The company has added employees during COVID-19 and we believe the company is continuing to grow through the pandemic.

We believe **Auth0** can maintain a high expansion rate and potentially increase its growth as it benefits from burgeoning demand for identity solutions in remote workforces. As developers embed security earlier in the development process and deploy more applications internally, **Auth0**'s tools can be directly embedded in apps from the requirements phase and scaled across large user bases.

Leadership

With less commercial experience than other high growth infosec companies, we believe **Auth0**'s management team nevertheless has the technical expertise to build a competitive DevOps solution to identity management. Co-founder and CEO Eugenio Pace was formerly principal lead program manager in technical guidance at **Microsoft**. Co-founder and CTO Matías Woloski was formerly an enterprise architect at Argentina-based Southworks and a professor of cloud computing. This team has positioned the company to technically innovate, though it may require more executive-level industry experience to achieve an IPO.



SUPPLEMENTAL MATERIALS

Select company analysis



Competitors

Auth0 competes with access management leaders including Okta, **Microsoft**, **Oracle**, IBM and Ping Identity. We believe **Auth0** has the most advanced developer tools on the market, supporting a variety of developer frameworks with its library of application programming interfaces and software development kits. While **Auth0** lacks the SaaS application pre-integrations of market leader Okta, this is in part by design—it allows developers to build their own integrations. Further, the company enables authentication for enterprise customers, while Okta focuses on employees. This focus likely decreases the addressable market the security budget for developer teams, which has not been defined in a majority of DevOps teams.

Outlook

While we believe **Auth0** could be an IPO candidate if it can accelerate its revenue growth, more executive-level hiring would be a stronger sign the company is moving in that direction. The company has announced that the company could IPO as early as 2022. **Auth0** should be able to maintain growth in a recessionary environment and could be a candidate for private IPO funding from growth equity firms.

Financing history

SERIES E	SERIES D	SERIES C
May 20, 2019 Total raised (\$M): \$103 Pre-money valuation (\$M): \$1,057 Investors: Sapphire Ventures (Lead), Bessemer Venture Partners, K9 Ventures, Meritech Capital Partners, Trinity Ventures, World Innovation Lab	May 15, 2018 Total raised (\$M): \$55.2 Pre-money valuation (\$M): \$465 Investors: Sapphire Ventures (Lead), Bessemer Venture Partners, K9 Ventures, Meritech Capital Partners, Trinity Ventures, World Innovation Lab	March 14, 2017 Total raised (\$M): \$30 Pre-money valuation (\$M): \$220 Investors: Meritech Capital Partners (Lead), Bessemer Venture Partners, K9 Ventures, Cygnus Capital, NTT Docomo Ventures, Telstra Ventures, Trinity Ventures
SERIES B	SERIES A	
August 24, 2016 Total raised (\$M): \$16 Pre-money valuation (\$M): \$80 Investors: Trinity Ventures (Lead), Bessemer Venture Partners, K9 Ventures, Silicon Valley Bank	June 24, 2015 Total raised (\$M): \$6.9 Pre-money valuation (\$M): \$27.4 Investors: Bessemer Venture Partners (Lead), Founders' Co-Op, K9 Ventures, NXTP Labs, Portland Seed Fund	



SUPPLEMENTAL MATERIALS

Additional VC data

Figure 49.
Infosec VC deal activity

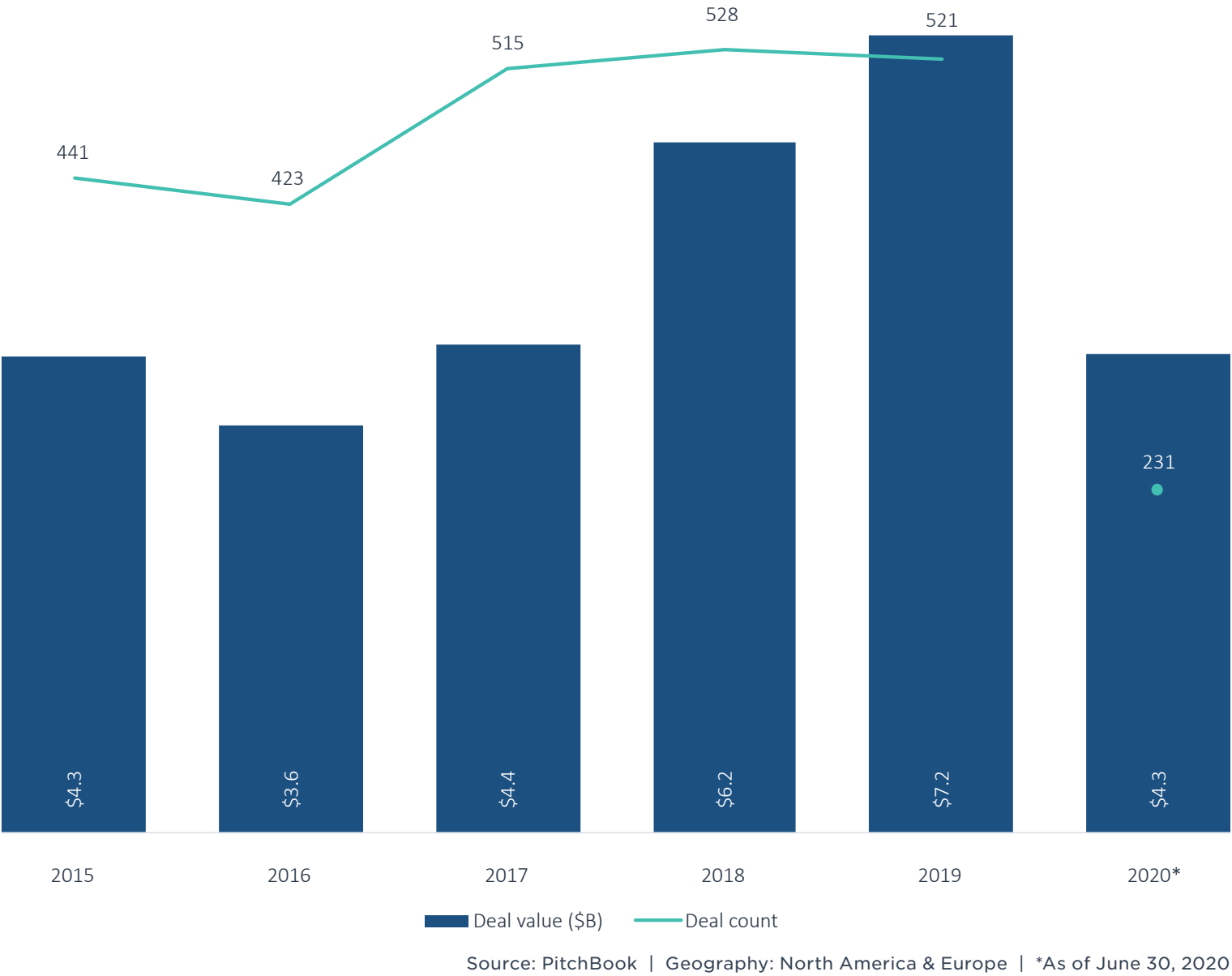


Figure 50.
Notable infosec VC deals

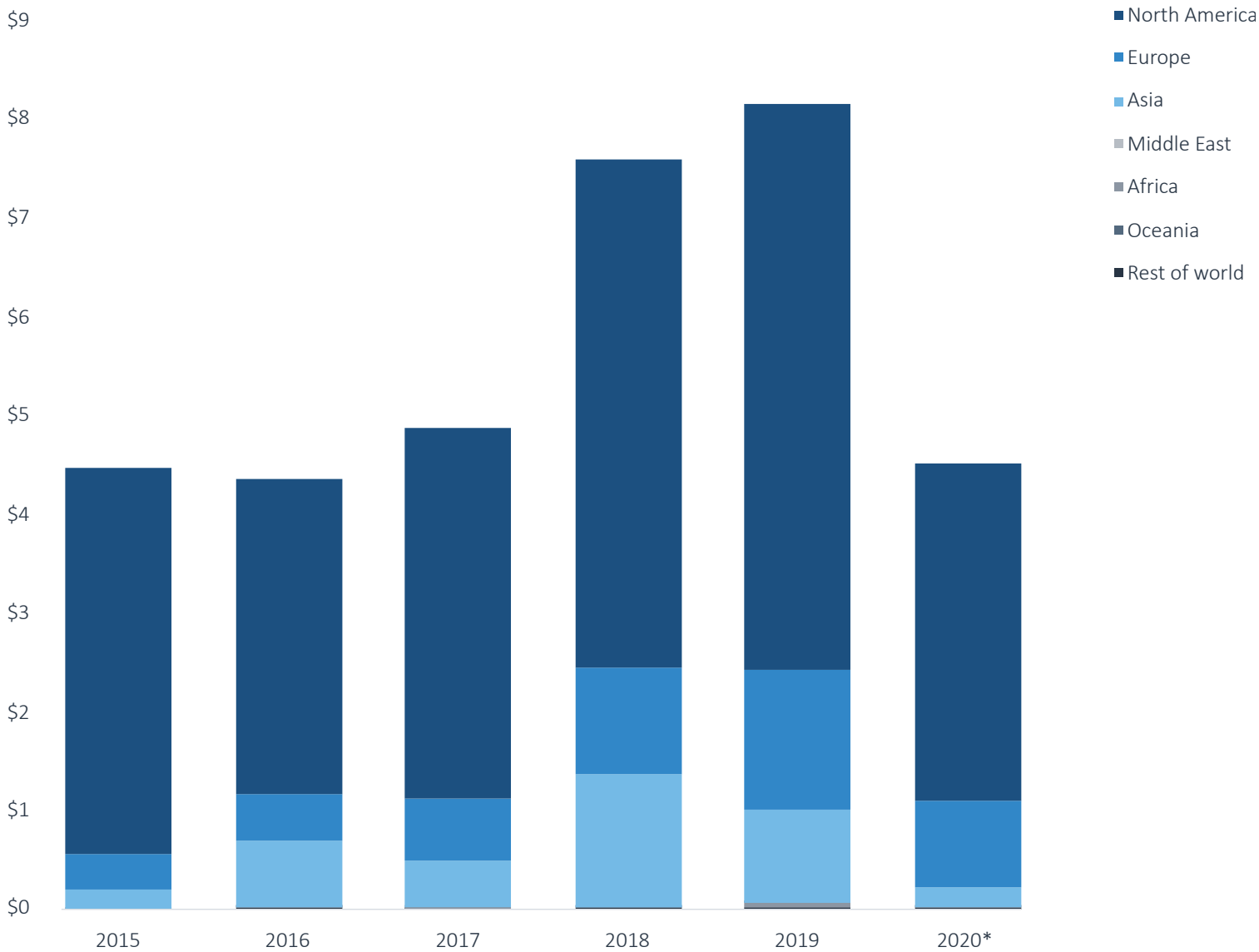
COMPANY	CLOSE DATE	DEAL SIZE (\$M)	POST-MONEY VALUATION (\$M)*
Netskope	February 6, 2020	\$340.0	\$2,800.0
Pango	September 5, 2018	\$295.0	N/A
Tenable	November 10, 2015	\$250.0	\$550.0
adjust	June 12, 2019	\$227.0	N/A
AirWatch	May 16, 2013	\$225.0	\$1,000.0
StackPath	March 17, 2020	\$216.0	N/A
OneTrust	February 20, 2020	\$210.0	\$2,700.0
Lookout	February 12, 2015	\$200.7	\$1,600.7
1Password	November 14, 2019	\$200.0	N/A
OneTrust	July 3, 2019	\$200.0	\$1,300.0

Source: PitchBook | *As of June 30, 2020



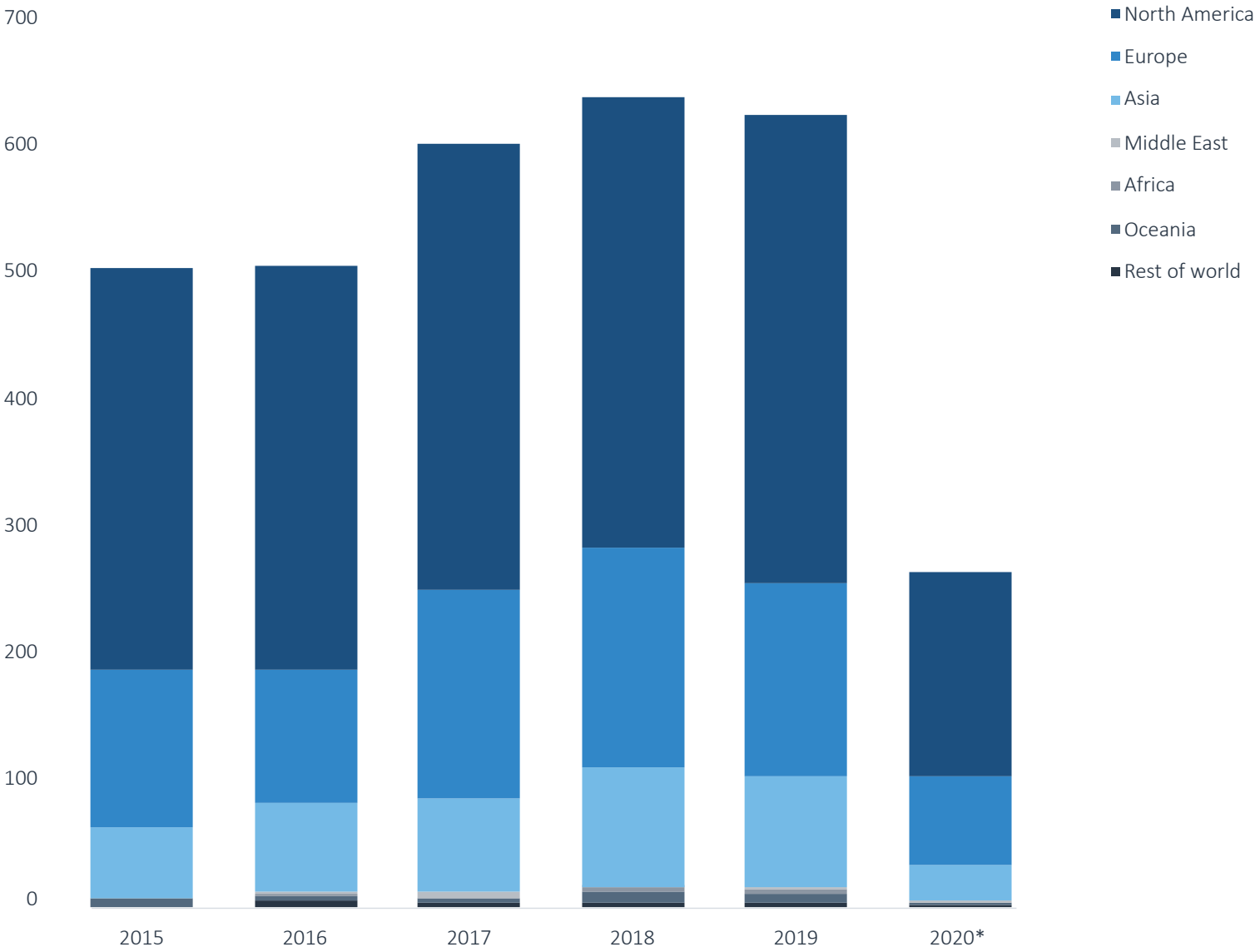
SUPPLEMENTAL MATERIALS

Figure 51.
Infosec VC deals (\$) by region



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Figure 52.
Infosec VC deals (#) by region

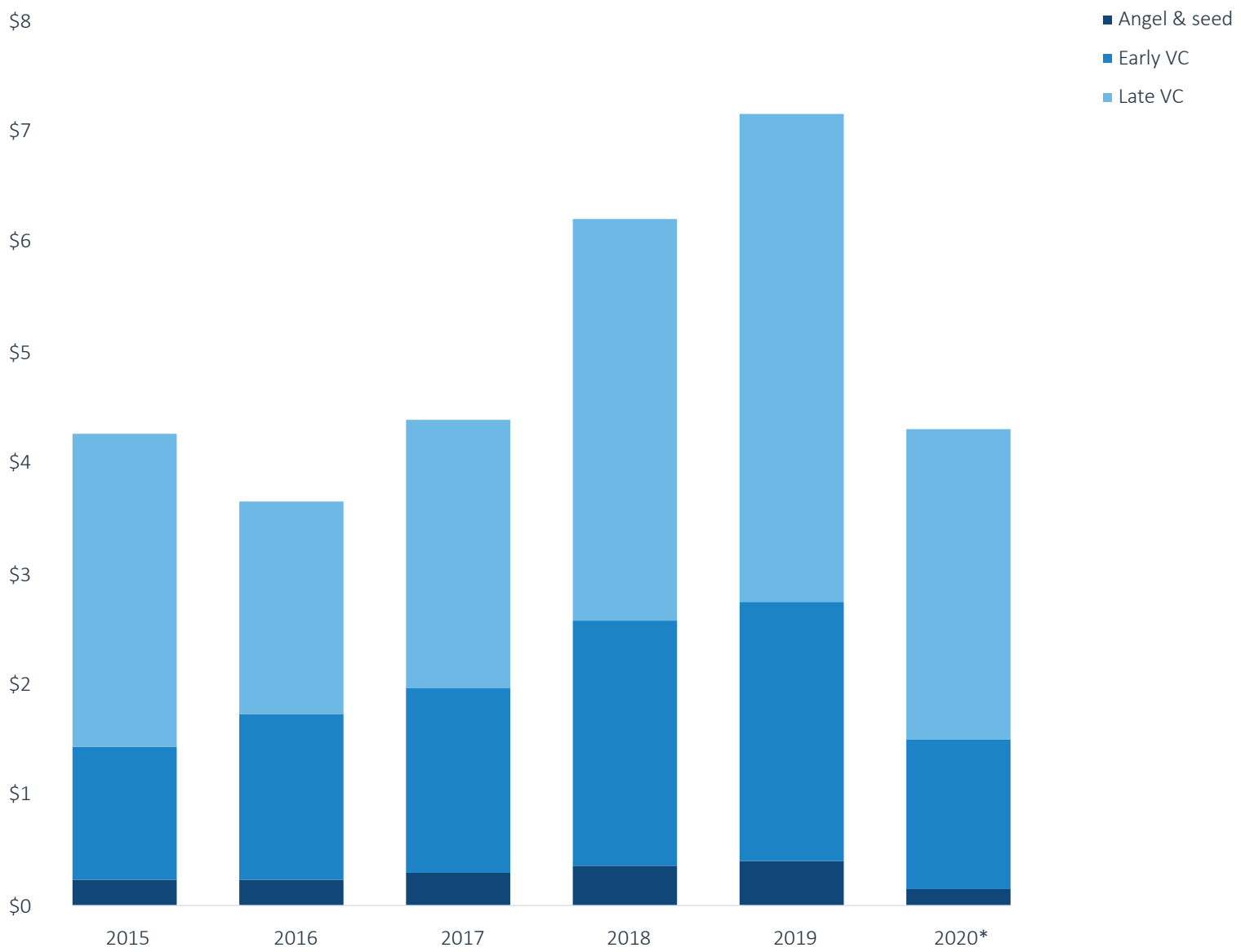


Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020



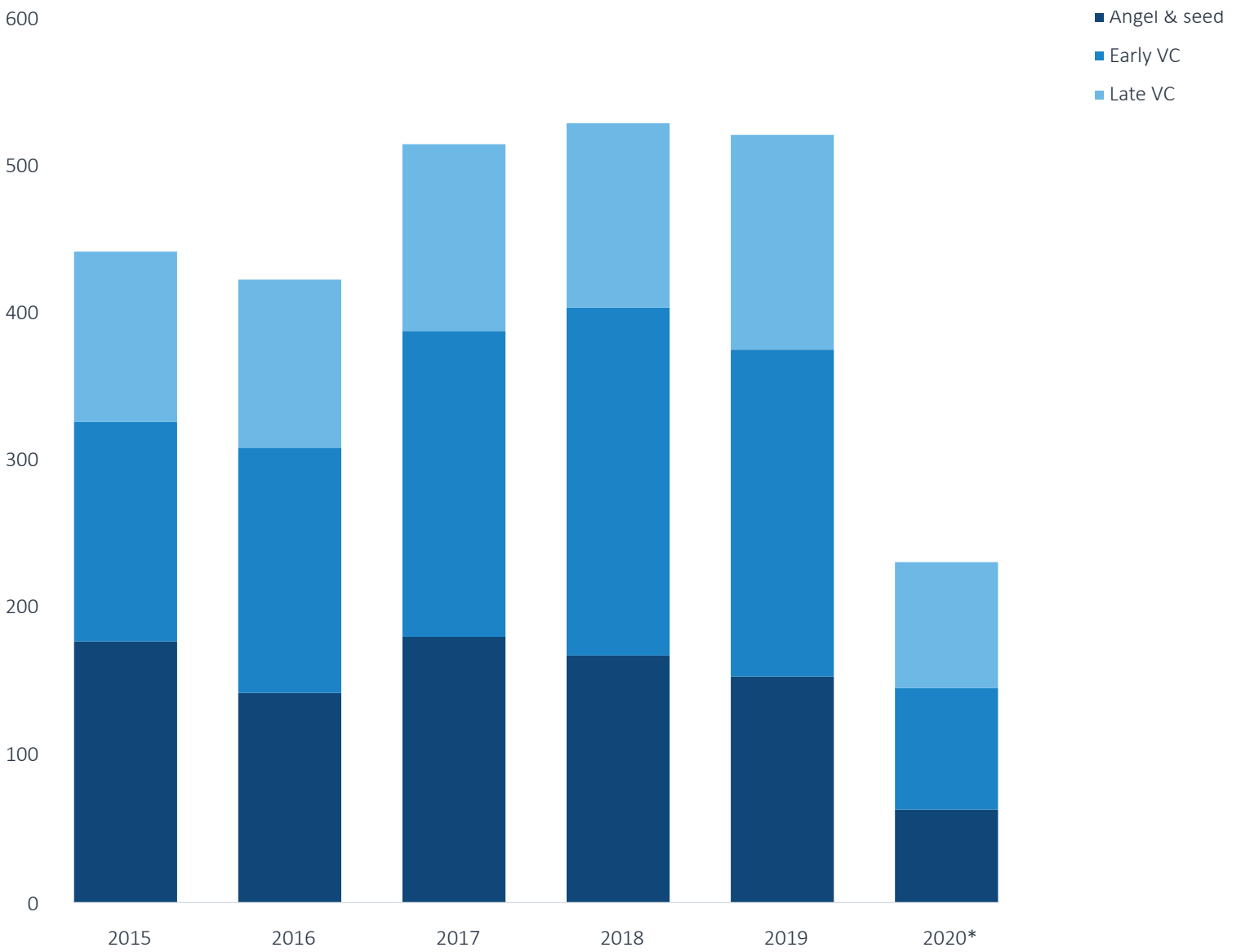
SUPPLEMENTAL MATERIALS

Figure 53.
Infosec VC deals (\$) by stage



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Figure 54.
Infosec VC deals (#) by stage

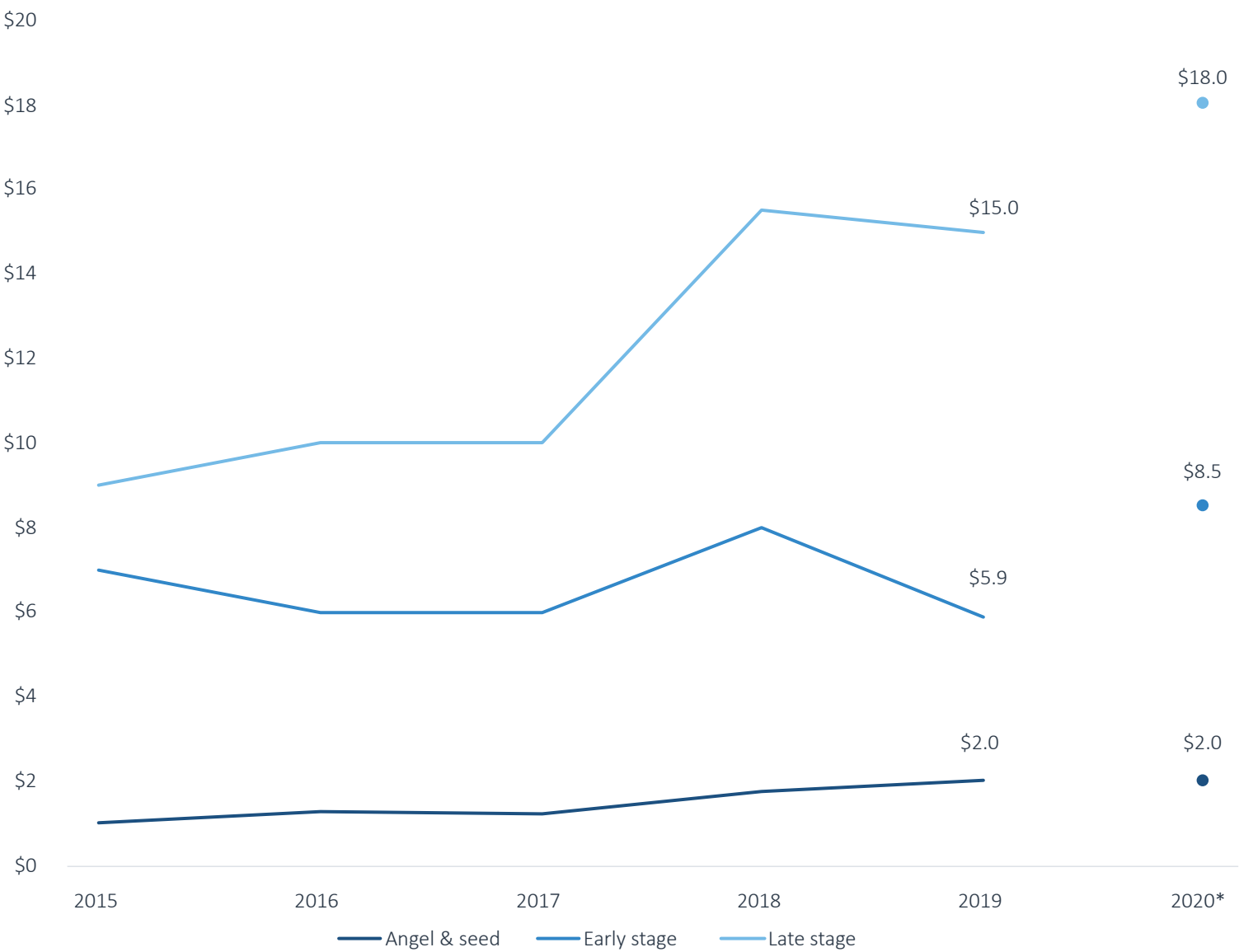


Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020



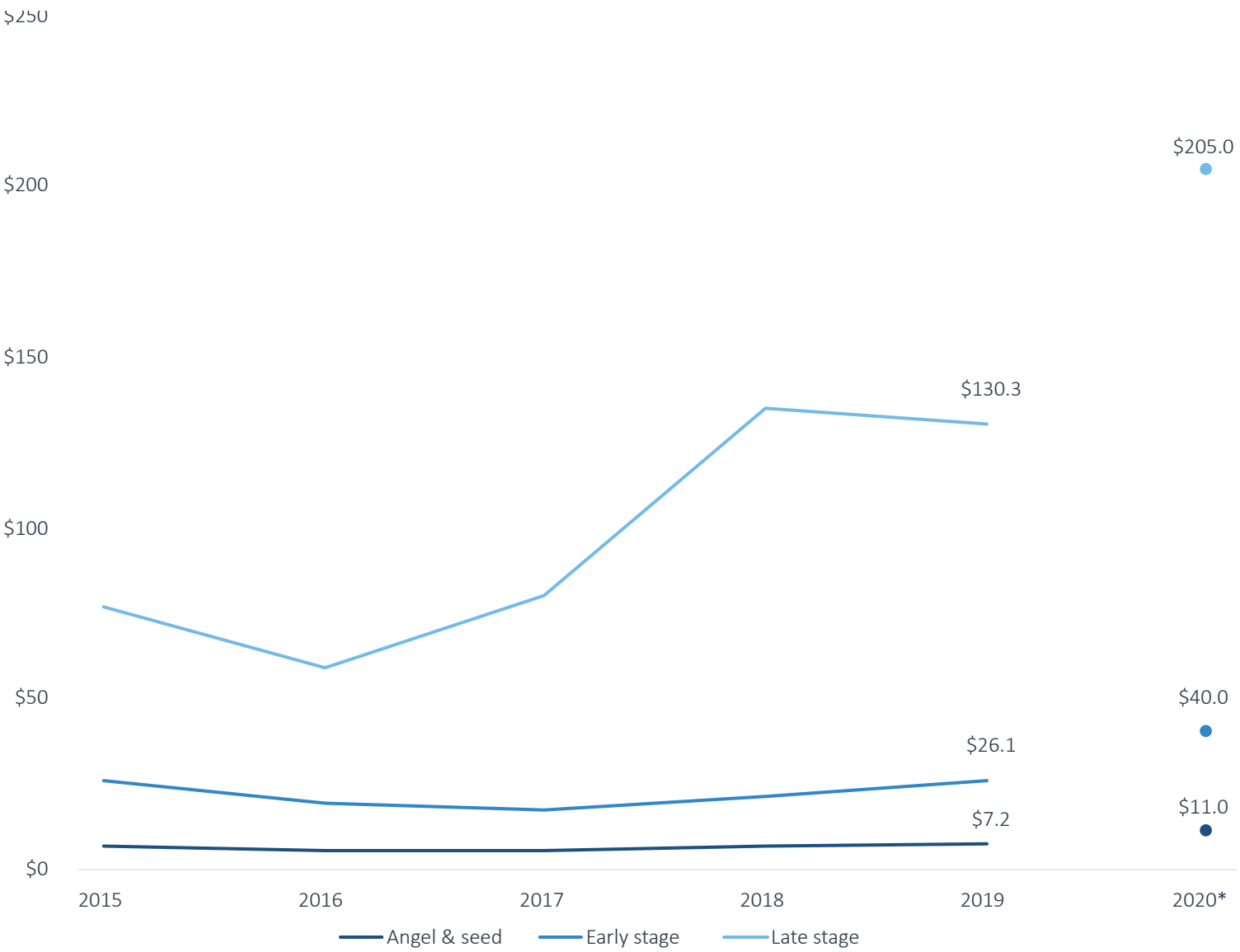
SUPPLEMENTAL MATERIALS

Figure 55.
Median infosec VC deal size (\$M) by stage



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Figure 56.
Median infosec VC pre-money valuation (\$M) by stage

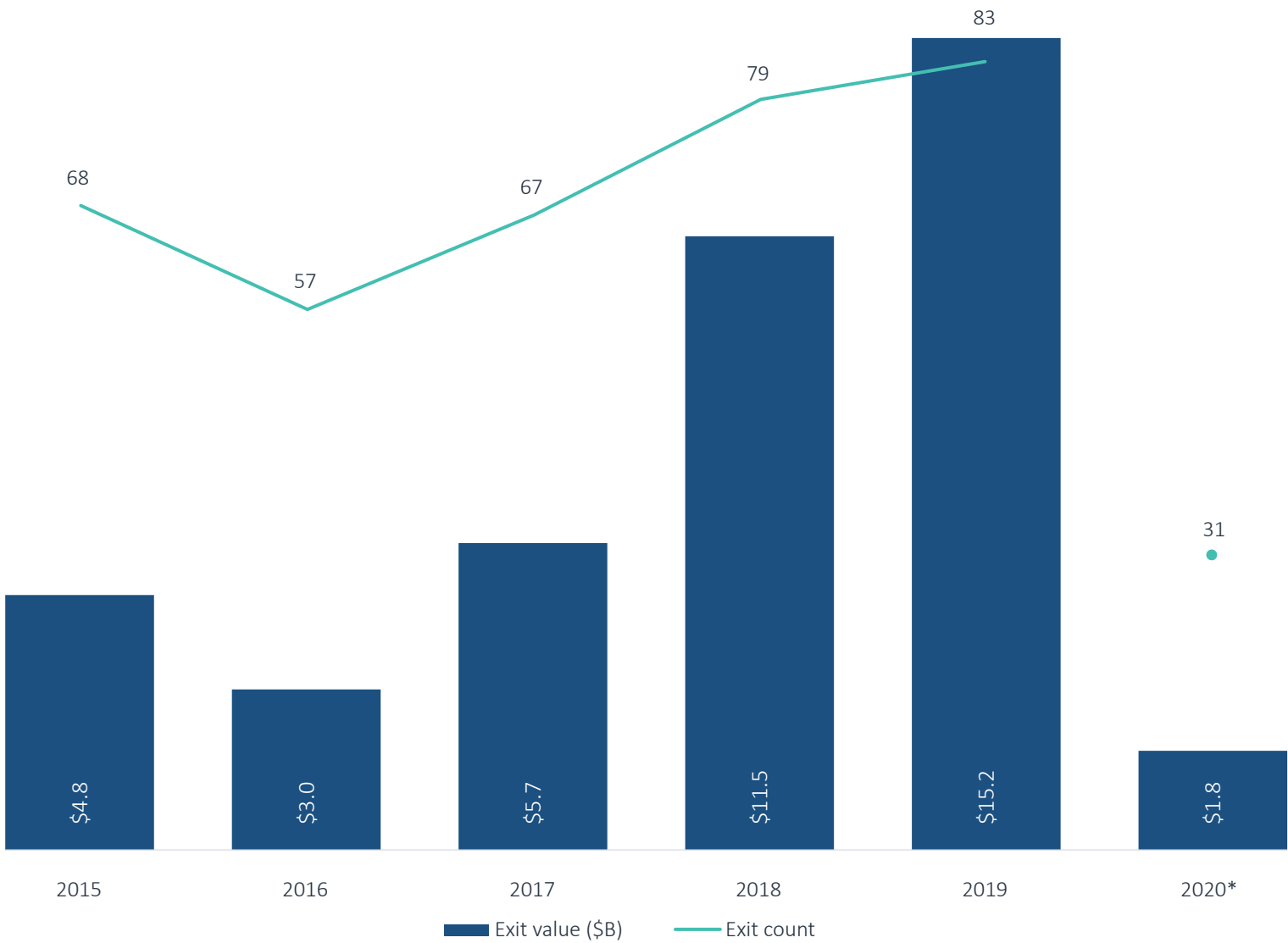


Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020



SUPPLEMENTAL MATERIALS

Figure 57.
Infosec VC exit activity



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Figure 58.
Notable infosec VC exits

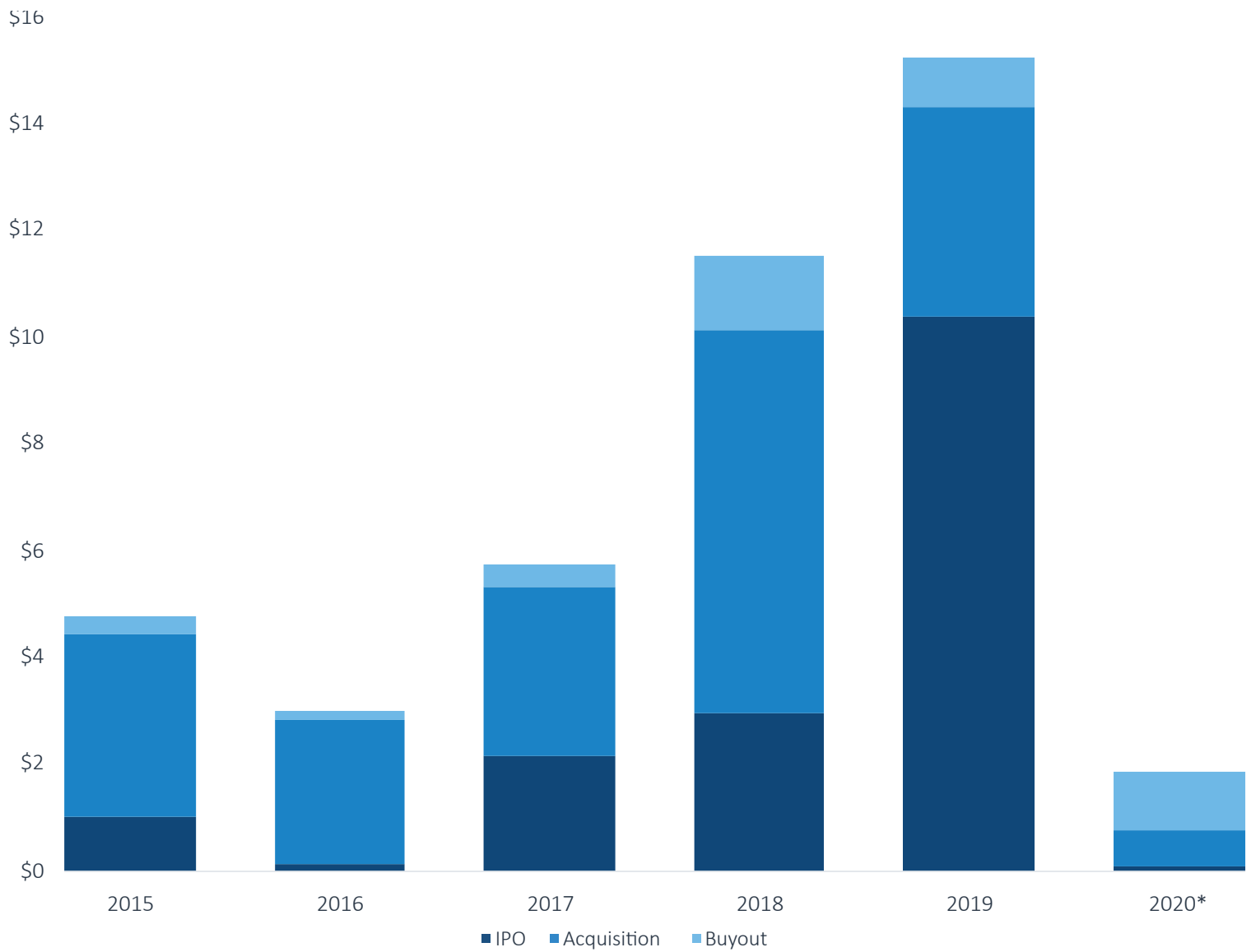
COMPANY	CLOSE DATE	EXIT TYPE	EXIT SIZE (\$M)
CrowdStrike	June 12, 2019	IPO	\$6,075.4
Cloudflare	September 13, 2019	IPO	\$3,875.2
Duo Security	September 28, 2018	M&A	\$2,350.0
Tenable	July 26, 2018	IPO	\$1,844.1
AT&T Cybersecurity	August 22, 2018	M&A	\$1,600.0
Cylance	February 21, 2019	M&A	\$1,400.0
Armis	February 11, 2020	Buyout/LBO	\$1,100.0
VMware	May 4, 2018	IPO	\$1,098.7
ThreatMetrix	February 22, 2018	M&A	\$813.6
Recorded Future	May 30, 2019	Buyout/LBO	\$780.0

Source: PitchBook



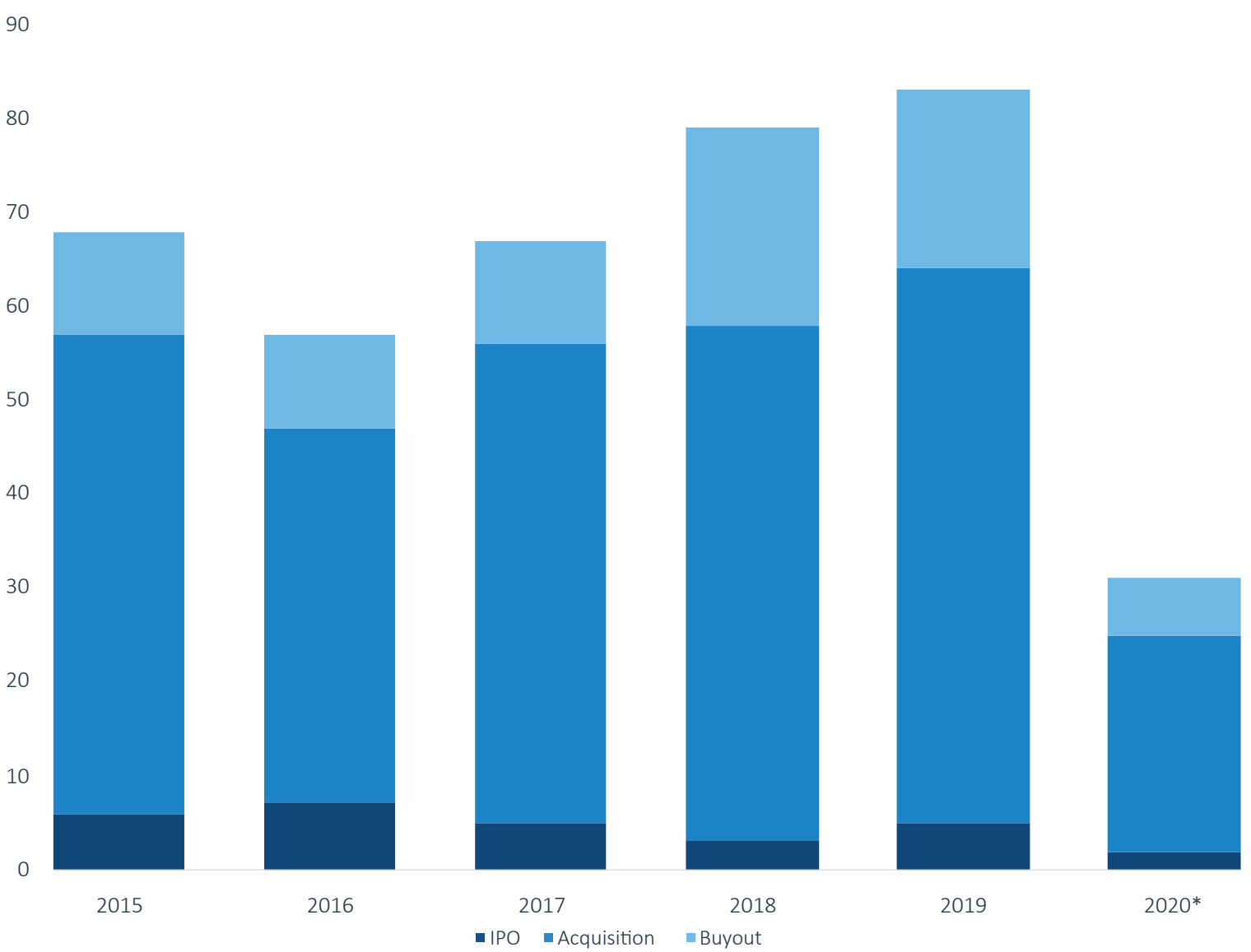
SUPPLEMENTAL MATERIALS

Figure 59.
Infosec VC exits (\$) by type



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Figure 60.
Infosec VC exits (#) by type



Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020



SUPPLEMENTAL MATERIALS

Figure 61.
Top VC investors in infosec by deal count since 2017

INVESTOR NAME	DEAL COUNT
Accel	38
Dell Technologies Capital	29
New Enterprise Associates	28
Bessemer Venture Partners	28
Lightspeed Venture Partners	25
ClearSky	25
ForgePoint Capital	24
Intel Capital	24
Battery Ventures	23

Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020

Figure 62.
Top PE investors in infosec by deal count since 2017

INVESTOR NAME	DEAL COUNT
Thoma Bravo	18
TA Associates Management	9
Insight Partners	9
Kohlberg Kravis Roberts	8
Marlin Equity Partners	7
H.I.G. Capital	7
Francisco Partners	7
ABRY Partners	7
Pamplona Capital Management	7

Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020



SUPPLEMENTAL MATERIALS

Figure 63.
Top 10 VC-backed infosec companies by VC raised

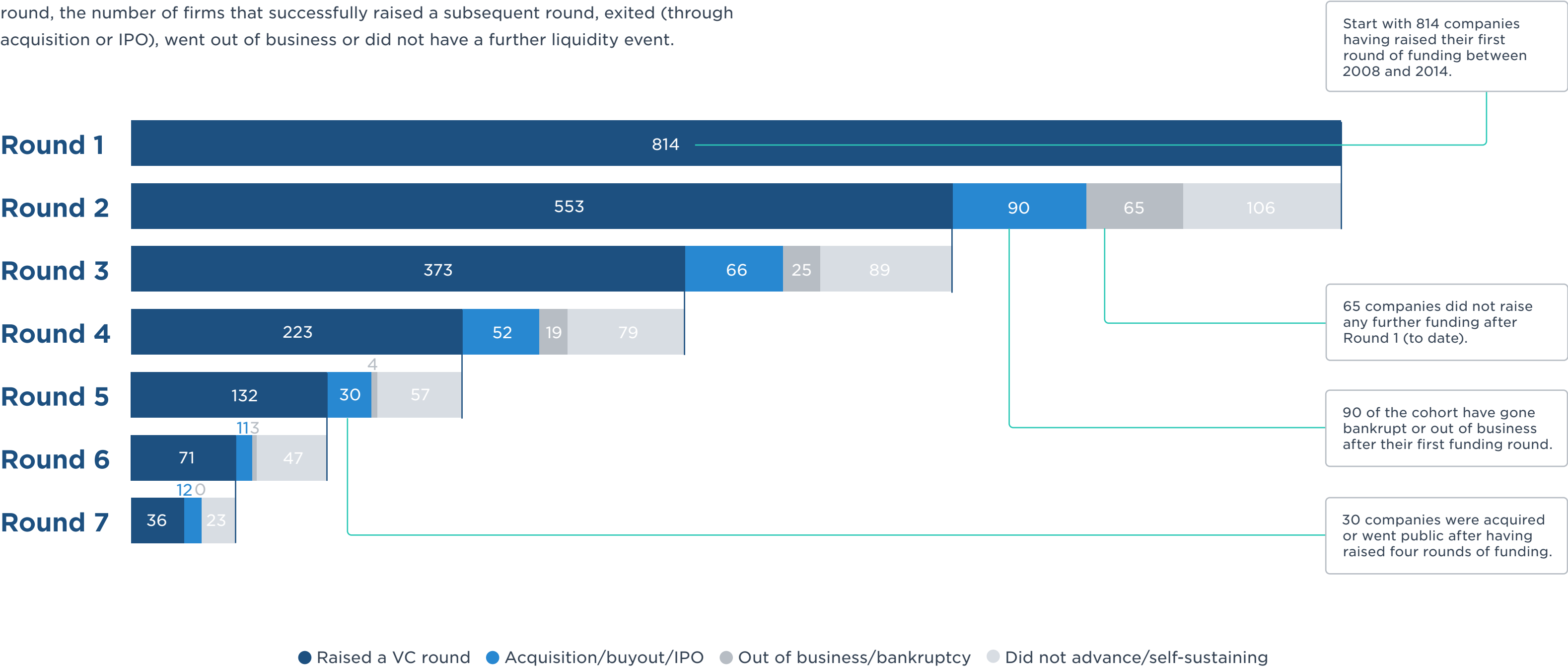
COMPANY	SEGMENT	SUBSEGMENT	COUNTRY	TOTAL VC RAISED (\$M)
Netskope	Network security	Cloud security	US	\$744.3
Tanium	Endpoint security	Edge device visibility & management solutions	US	\$687.1
SentinelOne	Endpoint security	Endpoint detection, response & protection	US	\$430.0
OneTrust	Data security	Data privacy & compliance	US	\$410.0
StackPath	Application security	Cloud workload protection platforms	US	\$396.0
Cybereason	Endpoint security	Endpoint detection, response & protection	US	\$388.4
Lookout	Endpoint security	Endpoint detection, response & protection	US	\$380.7
Pango	Network security	Secure networking	US	\$358.2
Sumo Logic	Security operations	Log ingestion & SIEM	US	\$345.2
Illumio	Network security	Secure networking	US	\$332.5

Source: PitchBook | Geography: North America & Europe | *As of June 30, 2020



Infosec VC funnel

This VC funnel uses PitchBook data to analyze the VC funding life cycle by highlighting, by round, the number of firms that successfully raised a subsequent round, exited (through acquisition or IPO), went out of business or did not have a further liquidity event.





SUPPLEMENTAL MATERIALS

Buyers list

Figure 64.
Top strategic acquirers since 2017

INVESTOR NAME	DEAL COUNT
Palo Alto Networks	9
Accenture	9
NortonLifeLock	8
HelpSystems	6
Convergint Technologies	6
Cisco Systems	6
j2 Global	6
NuMSP	5
Proofpoint	5
VMware	5

Source: PitchBook | *As of June 30, 2020



SUPPLEMENTAL MATERIALS

Glossary

Attack types

Ransomware: Blocks access to networks or encrypts data and requests a ransom, typically over \$1 million and commonly paid in bitcoin.

Spyware: Covertly transmits data from the user's hard drive.

Viruses: Software that inserts itself into a program and becomes part of it or overwrites the host program, spreading to other computers communicating with the script.

Worms: Standalone program that enters a system and uses file transport systems to traverse the network and create copies of itself.

Trojan: A harmful piece of software that looks legitimate.

Bots: Infect a host and connect back to a central server; commonly infects web applications and IoT devices.

Phishing: Sending fraudulent communications to steal data or install malware. It is the most common cyberattack.

Zero-day attack: Exploiting/attacking a computer software vulnerability that is unknown to the parties protecting the network before a patch or solution is implemented (day 0 is referred to as the day that the vulnerability is discovered).

Distributed Denial of Service (DDoS): A type of cyber-attack in which an attacker makes a network resource unavailable to users by flooding the targeted machine with excessive

requests to overload the system and prevent normal use. DDoS attacks create traffic from many different sources, usually accomplished with bots, so the attack can't be stopped by blocking one source.

SQL injection: An attack that has become increasingly common on big datasets. An attacker inserts a SQL query to the database via the input data from the client to server. The attacker can then expose the database, modify the data, shutdown the database and in some cases move laterally into the network.

Hacker types

Hacktivists: Activists that breach systems to advance an ideological agenda.

Malicious insiders: An employee with a malicious motivation to breach their employer's system.

White hat: Ethical hackers that remove malicious viruses or carry out penetration tests to help enterprises harden their defenses.

Red hat: Retributive hackers that attack malicious hackers.

Black hat: Malicious attackers often in pursuit of financial gain. These hackers are often sophisticated, highly educated programmers that develop automated attack patterns, differentiated from "script kiddies" that use simplistic open source methods to launch discrete attacks.



SUPPLEMENTAL MATERIALS

Glossary

Gray hat: neutral hackers with mixed motives. They comprise the majority of hackers and do not usually hack for malicious purposes.

Selected product types

Virtual private network (VPN): A VPN extends a private network across a public network, enabling users to send and receive data as if their devices were connected directly to the private network. Uses an encrypted layered tunneling protocol to ensure security.

Data loss prevention (DLP): Software that detects potential data breaches and prevents them through monitoring, detecting and blocking sensitive data across the network and endpoints. Includes firewalls, antivirus, intrusion detection systems (IDSs), machine learning algorithms for abnormal activity, honeypots, etc.

Security information and event management (SIEM): Provides real-time analysis of security alerts generated by applications and network hardware. Involves log management/data aggregation, correlation of events, alerting about these correlated events, dashboards, retention and compliance of data, etc.

Homomorphic encryption (HE): Methodology that enables enterprises to operate on sensitive, encrypted data—such as personal data—without decrypting it, exposing it to algorithms, processing systems, or analysts. The user submits an encrypted query and the search engine computes an encrypted answer without looking at the plain text query. HE lets cloud computing customers secure their cloud data while it's in use and ensures that only authorized users, not the cloud provider—can view the data.

Cyber kill chain

Information breaches are carried out through a “kill chain,” the military term for the process used by an enemy to carry out an attack first coined by Lockheed Martin. Multiple steps are required for data breaches to occur, and security teams must be prepared to defend against attacks at each step. The range of functions required to execute an attack creates opportunities for vendors to block multiple attack vectors. Successful vendors operate at each level of the kill chain as security buyers create a stack of security solutions to ensure the management of each vulnerability.

Perimeter breach: Attackers typically breach networks via threat surfaces that communicate with the web.

Deliver malware: Once hackers breach an enterprise, they generally attempt to deliver a payload of malware into the enterprise's system. As malware often alters code within applications, the principal defenses to these injections reside within the programs themselves.

Command and control of networks: Once malware is delivered, it moves laterally through a network, encrypts data and can prevent users from accessing their own data.

Data exfiltration: Data protection solutions can ensure that even if attackers take control of a network, they will not have access to sensitive data.

About PitchBook Emerging Tech Research

Independent, objective and timely market intel

As the private markets continue to grow in complexity and competition, it's essential for investors to understand the industries, sectors and companies driving the asset class.

Our Emerging Tech Research provides detailed analysis of nascent tech sectors so you can better navigate the changing markets you operate in—and pursue new opportunities with confidence.

©2020 by PitchBook Data, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, and information storage and retrieval systems—without the express written permission of PitchBook Data, Inc. Contents are based on information from sources believed to be reliable, but accuracy and completeness cannot be guaranteed. Nothing herein should be construed as any past, current or future recommendation to buy or sell any security or an offer to sell, or a solicitation of an offer to buy any security. This material does not purport to contain all of the information that a prospective investor may wish to consider and is not to be relied upon as such or used in substitution for the exercise of independent judgment.

Additional research

Artificial Intelligence &
Machine Learning
[Brendan Burke](#)
brendan.burke@pitchbook.com

Cloudtech & DevOps
[Paul Condra](#)
paul.condra@pitchbook.com

Fintech
[Robert Le](#)
robert.le@pitchbook.com

Foodtech
[Alex Frederick](#)
alex.frederick@pitchbook.com

Health & Wellness Tech
[Kaia Colban](#)
kaia.colban@pitchbook.com

Information Security
[Brendan Burke](#)
brendan.burke@pitchbook.com

Insurtech
[Robert Le](#)
robert.le@pitchbook.com

Internet of Things (IoT)
[Brendan Burke](#)
brendan.burke@pitchbook.com

Mobility Tech
[Asad Hussain](#)
asad.hussain@pitchbook.com

Supply Chain Tech
[Asad Hussain](#)
asad.hussain@pitchbook.com