PitchBook

EMERGING TECH RESEARCH

Information Security

Q4 2020

Contents

Credits & contact

RESEARCH

Brendan Burke

Senior Analyst, Emerging Technology

brendan.burke@pitchbook.com

DATA

Matthew Nacionales

Data Analyst

DESIGN

Julia Midkiff and **Kelilah King**

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. The previous quarterly report can be accessed **here.**

Q4 2020 news and updates

VC ACTIVITY

- Infosec VC deal activity set a record in 2020 with $9.9 billion invested across 626 deals, a 16.1% increase in deal value despite an 8.6% decline in deal count.
- Late-stage VC deals outnumbered early-stage and angel & seed VC deals for the first time since 2010, indicating a flight to quality in infosec investing and challenging conditions for startup fundraising.
- VC deal value was led by fraud prevention, data privacy & compliance, managed security services, and endpoint security, which all raised over $700 million in funding in 2020.

Q4 2020 EXIT ACTIVITY

- VC exit value set a record with $18.3 billion in 2020, although exit count declined for the first time since 2016.
- In Q4, **Palo Alto Networks** (NYSE: PANW) continued its high M&A activity with an $800.0 million acquisition of endpoint security vendor **Expanse**. **CrowdStrike** (NASDAQ: CRWD) also solidified its presence as an acquirer with its $96.0 million acquisition of zero trust networking startup **Preempt Security**.
- After an active quarter for IPOs in Q3, no IPOs occurred in Q4. We predict that five infosec unicorns will go public in 2021.

NEWS

- **December 8, 2020: FireEye** (NASDAQ: FEYE) reports suffering a **SolarWinds** (NYSE: SWO) IT monitoring software supply chain attack resulting in theft of penetration testing tools, which was later associated with Russia-based threat actors. The vulnerability was later found to affect 18,000 of **SolarWinds**' customers.
- **November 9, 2020:** Video conferencing leader **Zoom** (NASDAQ: ZM) settled with the Federal Trade Commission over a claim of misleading customers about end-to-end encryption, including agreeing to additional security measures.
- **October 28, 2020: FireEye** (NASDAQ: FEYE) identified a leading European ransomware group it called UNC1878 that primarily targets hospitals, retirement communities, and medical centers, delivering malware via email phishing attacks.

TRENDS & OBSERVATIONS

Definitive industry trends identified in our Q3 report, including extended detection & response (XDR), secure access service edge (SASE), and DevOps security (also known as DevSecOps), are developing into commercially relevant packages. In XDR, vendors are starting to offer integrated endpoint scanning and automated incident response software, posing direct challenges to SIEM (security information and event management) and SOAR (security orchestration, automation, and response) vendors. In SASE, incumbent vendors have developed nearly comprehensive offerings via M&A, and leading private company **Netskope** has formed partnerships with challengers **CrowdStrike** (NASDAQ: CRWD), **Okta** (NASDAQ: OKTA), and **Proofpoint** (NASDAQ: PFPT) to offer a comprehensive solution. In DevSecOps, the **SolarWinds** breach serves as a catalyst for software vendors to improve their secure software development tooling. Vendors are increasingly addressing the entire software development lifecycle.

Executive summary

Information security (infosec) refers to technology and services that protect enterprises from digital threats to business operations.[1] 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. Infosec growth surprised to the upside in 2020 and is poised for even higher double-digit growth in 2021 in response to increasing digital transformation and increased nation-state threats.

We estimate the infosec vertical to have reached $148.2 billion in 2020 as the industry has been able to increase spending during the pandemic, and we expect low double-digit 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 not addressed by most infosec startups. Our estimate includes the $73.9 billion 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 $206.9 billion by 2024 at a 9.7% CAGR. We expect high economic growth in 2021 to 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.

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. 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.

1: 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.

Key takeaways

DevOps adoption of security practices is accelerating through the pandemic. Industry surveys find that the percentage of developer teams integrating security in multiple phases of the software development lifecycle increased in 2020 during the COVID-19 pandemic, unlocking opportunities for developer-focused security in each segment. Despite this increased integration of practices, commercial tools remain relatively underpenetrated. The **SolarWinds** software supply chain heightens the importance of secure code in third-party applications. 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 two VC mega-deals ($100 million+) for **Snyk** in 2020 demonstrate the potential for valuation growth in this niche.

Endpoint security and network security are experiencing convergence of point solutions into XDR and SASE. XDR unifies endpoint security and security operations tools to automate responses to alerts across threat surfaces. SASE unifies network security and identity & access management to connect both remote workers and offices directly to the cloud. Both trends have resulted in commercial product offerings and are testing product-market fit going into 2021. Furthering the trend outlined in our Q3 update, SASE and XDR continued to be M&A drivers in Q4. **CrowdStrike** (NASDAQ: CRWD) made a SASE-related acquisition with its $96.0 million acquisition of zero trust networking startup **Preempt Security**. **FireEye** (NASDAQ: FEYE) expanded its XDR suite with a $186.0 million acquisition of log ingestion & SIEM startup **Respond Software**. Startups have new opportunities to build ground-up solutions in each space and capture market share from legacy incumbents.

Passwordless authentication is rapidly emerging as the next wave of identity & access management. Microsoft (NASDAQ: MSFT) reported a 50% increase in the use of its passwordless tools in 2020 and forecast widespread adoption in 2021. IT teams nearly universally believe that a passwordless experience is likely at their organizations in the future. Benefiting from a partnership with **Microsoft** (NASDAQ: MSFT), **Beyond Identity** achieved a 2.5x deal size step-up within eight months, indicating that passwordless authentication is becoming the next wave of identity verification after multifactor authentication. **Averon**, **TruU**, and **Secret Double Octopus** have also achieved high valuation growth in this niche over the past two years.

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.[2] 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 security operations 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.

2: "2020 Data Breach Investigations Report," Verizon, May 2020.

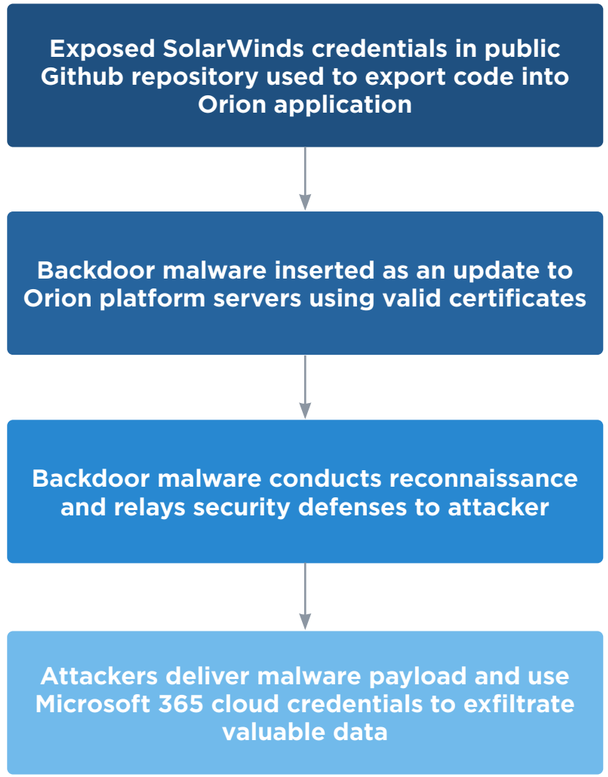
Industry overview: SolarWinds attack implications

The Sunburst attack via **SolarWinds** network monitoring software highlights systemic weaknesses in cybersecurity and will have ramifications for security vendors. The Sunburst attack refers to the malware deployed in SolarWind's Orion application via a backdoor in its software, enabling data exfiltration from **SolarWinds**' customers. Both corporations and government departments are implicated among 18,000 **SolarWinds** customers. The attack has been connected to sophisticated nation-state actors. While nation-state actors are not responsible for most breaches, this breach underscores that all corporations and governments must be protected against sophisticated espionage.

The breach exposes the vulnerabilities of open-source and application codebases, since **SolarWinds** was found to have leaked credentials in a public Github repository. Open-source codebases can host hidden secrets within otherwise generic scripts. These leaked credentials were likely used to install a backdoor application and deliver malware that evaded detection. The malware appeared to be legitimate code, using signed certificates. Action is required from both software vendors and customers to ensure that software supply chains do not become attack vectors. Both cultural and technical changes will be encouraged to ensure that software applications are secure and sensitive data is protected. We believe that existing priorities including threat surface visibility will be reinforced, and some priorities will increase in importance for both software customers and vendors. While no authoritative forensic report of the breach has been issued, we believe that security researchers have broad consensus on some steps the attackers took (see right).

Figure 2.

Reported attack vector of Sunburst software supply chain attack



Source: CrowdStrike, FireEye, Microsoft, SaveBreach, Symantec

Priorities for software customers:

- **Third-party vendor security audits:** Increasing reliance on SaaS applications for business-critical functions creates nonlinear risk for enterprises since each new SaaS application can be used to breach the enterprise and move laterally to other applications. Third-party risk assessment remains a manual process typically offered through professional services on a quarterly or annual basis. Startups are bringing increased velocity and visibility to third-party risk assessments and will offer improvements to enterprise customers.
- **Vulnerability assessment:** Up-to-date inventory of IT assets and centralized ability to block and patch third-party applications are critical capabilities for security teams. Automation of this process is common using advanced scanning agents. While this niche is mature commercially, enterprises will likely assign additional resources to it.
- **Cloud workload and identity behavioral analysis:** Attackers targeted sensitive data in cloud environments using high-privileged accounts with cloud access. Customers should be able to conduct behavioral analysis on cloud users to detect abnormal behavior as is common with endpoint security.

Priorities for software vendors:

- **DevOps security:** Software vendors will increasingly be pushed to prove the hygiene of their software supply chain via software composition analysis and security monitoring integration. An open-source composition analysis of SolarWind's Orion application may have revealed an unverified repository that could have suggested remediation. Adoption of DevOps security across the software development lifecycle, especially at the open-source repository selection phases, remains uneven, offering growth opportunities for DevOps security vendors.
- **Application monitoring:** Runtime application security protection (RASP) and cloud workload monitoring can detect abnormalities from normal behavior. In this case, these tools may have been able to detect the installation of the backdoor or the malware payload itself.
- **Threat hunting software:** Attackers first breached **SolarWinds** in October 2019, according to the company, suggesting they were able to dwell in their applications and deliver malware for over a year. Threat hunting is still primarily a manual process involving professional services, creating challenges to find patient attackers. Automated threat hunting can supplement limited security teams in investigating abnormal application behavior.

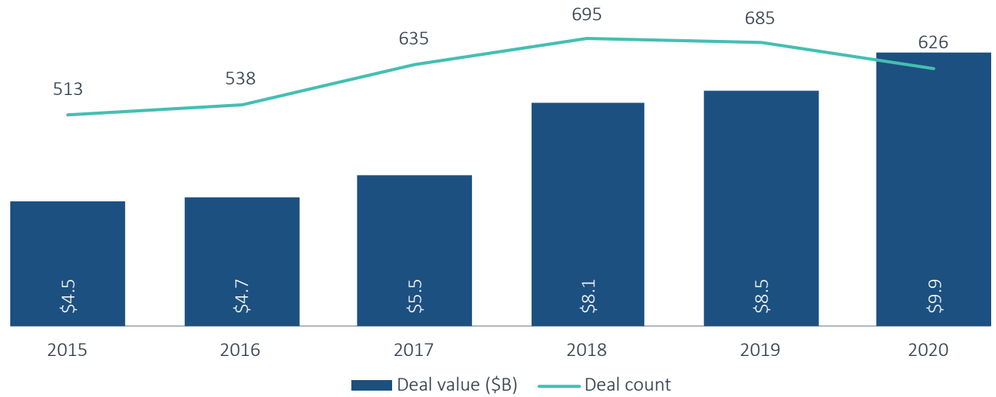
The **SolarWinds** attack highlights the essential role of application security in modern defense, since neither endpoint nor network security would have been sufficient to detect the attack in progress. The attack was delivered through a software application and spread further than a single organization as a result. Application security is a newer and less adopted category of infosec, although we believe enterprises have increasingly been focusing on it. This attack will likely catalyze adoption of application security tools on both customer and vendor sides. We believe that application security will grow over 20% per year from 2021 to 2024 as a result.

VC activity

Infosec was insulated from the pandemic both commercially and from an investment perspective in 2020. Infosec VC deal activity set a record in 2020 with $9.9 billion invested across 626 deals, a 16.1% increase in deal value despite an 8.6% decline in deal count. US technology VC deal value increased 14.0% by comparison, suggesting that infosec was a relatively more attractive sector during the year. The pandemic had its greatest harmful effects on early-stage deals. Late-stage VC deals outnumbered both early-stage and angel & seed VC deals for the first time since 2010, underscoring the flight to quality in infosec investing and challenging conditions for startup fundraising. VC deal value was led by fraud prevention, data privacy & compliance, managed security services, and endpoint security, which all raised over $700 million in funding in 2020. All of those categories except data privacy & compliance feature high-end total addressable markets, suggesting that market size is a primary driver of VC deal activity.

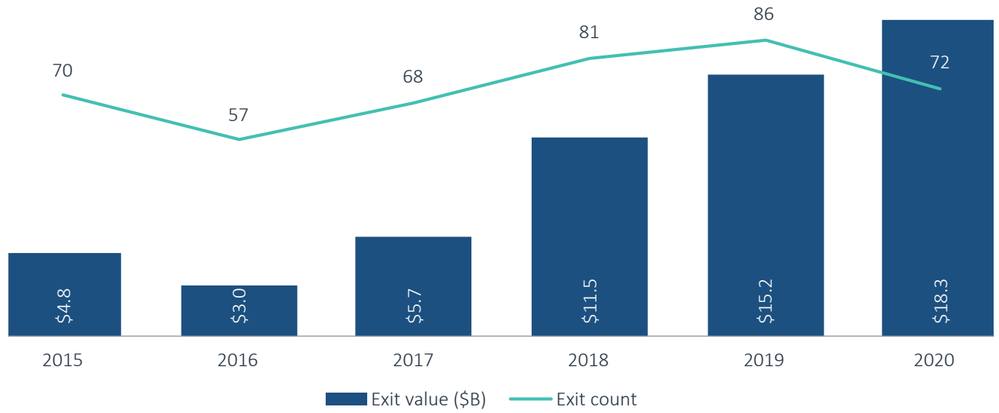
VC exit value set a record with $18.3 billion, although exit count declined for the first time since 2016. Acquisition count declined 19.3% from 62 to 50, with some incumbents showing weakness in their businesses and M&A appetite. In Q4, **Palo Alto Networks** (NYSE: PANW) advanced its leading M&A position with an $800.0 million acquisition of endpoint security vendor **Expanse**. SASE and XDR continued to be M&A drivers. **CrowdStrike** (NASDAQ: CRWD) made a SASE-related acquisition and established its presence as an acquirer with its $96.0 million acquisition of zero trust networking startup **Preempt Security**. **FireEye** (NASDAQ: FEYE) expanded its XDR suite with a $186.0 million acquisition of **Respond Software**. XDR and SASE are justifying substantial acquisition values for incumbents developing strategies to address them. After an active quarter for IPOs in Q3, no IPOs occurred in Q4. We predict that five infosec unicorns will go public in 2021.

Figure 5. INFOSEC VC DEAL ACTIVITY



Source: PitchBook | Geography: North America & Europe

Figure 6. INFOSEC VC EXIT ACTIVITY



Source: PitchBook | Geography: North America & Europe

Infosec VC ecosystem market map

Click to view interactive market map on the PitchBook Platform

Market map is a representative overview of venture-backed or growth-stage providers in each segment. Companies listed have received venture capital or other notable private investments.

Security operations

Managed security services

ARCTIC WOLF · BlueVoyant · CIRCADENCE · Coalition · expel · Prevalent · bugcrowd · deepwatch · AUTOMOX · CYGILANT

Log ingestion & SIEM

exabeam · bigpanda · illusive · Attivo NETWORKS · EclecticIQ · logdna · SECURONIX · LOGPOINT · Cynet · panther

Security risk assessment & management

BITSIGHT · Accellion · Synack · SecurityScorecard · hackerone · CyberGRX · KENNA Security · Comply Advantage · RISKIQ · THREATQUOTIENT

Security orchestration, automation & response

Siemplify · SWIMLANE · ACALVIO · LogicHub · Tines

Network security

Cloud security

netskope · Lacework · bitglass · ARMOR · CloudPassage · Guardicore · WIZ · ANOMALI · threat stack · SHIELDX · sonraí SECURITY · CLOUDKNOX · censornet. · JUPITERONE · bridgecrew

Network security (cont.)

Network detection & response

DARKTRACE · VECTRA · ZEROFOX · IronNet · corelight · FLASHPOINT · ExtraHop · INTSIGHTS · BLUEHEXAGON · CYCOGNITO

Secure networking

illumio · CATO NETWORKS · Menlo Security · iboss · 128 TECHNOLOGY · packetfabric · dispersive · Tempered · perimeter 81 · GARRISON

Data security

Database monitoring & loss prevention

IONIC · CipherCloud · IMMUTA · SecurityONE · CybelAngel · egress · UNBOUND · GEMINI · global velocity · ALTR

Data privacy & compliance

OneTrust PRIVACY, SECURITY & TRUST · BigID · EGNYTE · TrustArc · VERY GOOD SECURITY · DATAVANT · SECURITI.ai · ClearDATA · InCountry · semperis · TRANSCEND · Skyflow · wirewheel · Aware · ETHYCA

Data protection & encryption

druva · Acronis · PRIVITAR · CODE42 · Ledger

Application security

Web application protection

onapsis · perimeterx · NAMOGOO · SALT · detectify · CEQUENCE SECURITY · appdetex · virsec · sqreen

Cloud workload protection platforms

STACKPATH · varmour Relationships Matter · aqua · ionir · StackRox · weaveworks · TIGERA · Uptycs · CAPSULE8 · ISOVALENT · INTEZER · K2 CYBER SECURITY · CLOUDENTITY · deepfence · NeuVector

DevOps security platforms

snyk · CONTRAST SECURITY · LYNX · WhiteSource · FOSSA · AURORALABS · ShiftLeft · NowSecure · anchore · ZERONORTH

Endpoint security

IoT/OT security

TANIUM · DRAGOS · nexthink · Plume · silent circle · MOCANA · PSafe · CLAROTY · AXONIUS · Vdoo · KOOLSPAN · NOZOMI NETWORKS · ordr · wandera · MEDIGATE

Endpoint security (cont.)

Endpoint protection, detection and response

SentinelOne · cybereason · Lookout · GoSecure · deepinstinct · AGARI · AREA 1 · Malwarebytes · DTEX · QOMPLX:

Anti-phishing platforms

VadeSecure Predictive Email Defense · VALIMAIL · Abnormal Security · TESSIAN · AVANAN · Material · IRONSCALES THE POWER OF NOW · INKY · Armorblox · SLASHNEXT

Identity & access management

Access management

Auth0 · ForgeRock · JumpCloud Directory as a Service · BetterCloud · onelogin · OBSIDIAN · AlertEnterprise PHYSICAL | LOGICAL SECURITY CONVERGENCE · plainID THE AUTHORIZATION COMPANY · ALSID · Remediant

Fraud prevention

adjust · onfido · riskified · FORTER · pindrop · SIGNIFYD · BIOCATCH Less Friction. Less Fraud. · AURA · FEATURE SPACE · sift

Identity governance & administration

prove Formerly Payfone · BEYOND IDENTITY · dashlane · SECURE KEY · GRADIENT · ID.me · SAVIYNT · averon

SEGMENT DEEP DIVE

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.[3] 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 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.[4]

3: "2020 State of the Cloud Report," Flexera, 2020
4: "Detecting Persistent Cloud Infrastructure/Hadoop/YARN Attacks Using Security Analytics: Moanacroner, XBash," Securonix, January 15,

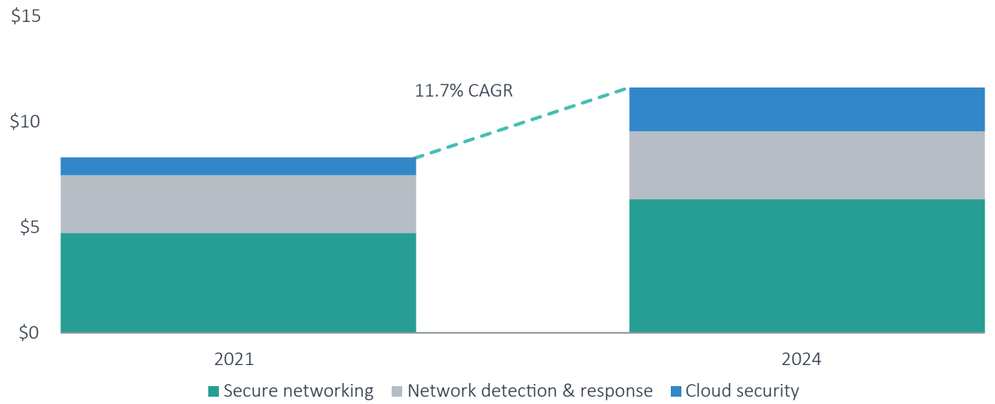
Market size

We estimate the network security market to reach $8.4 billion in 2021. This market size includes cloud security, secure web gateways, network detection & response, and legacy intrusion detection systems, excluding firewall hardware. We forecast network security to grow more quickly than the overall infosec market at an 11.7% CAGR to an $11.7 billion market in 2024. We expect high growth to resume in 2021 as enterprises 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 years with a 31.4% 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** (NASDAQ: ZS) and **Cisco** (NASDAQ: CSCO) substantially improved their market positions from 2018 to 2019. This suggests 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 broker 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).

Figure 7. NETWORK SECURITY MARKET SIZE ($B)



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

Figure 8. COMMON INDUSTRY KPIS FOR NETWORK SECURITY COMPANIES

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

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

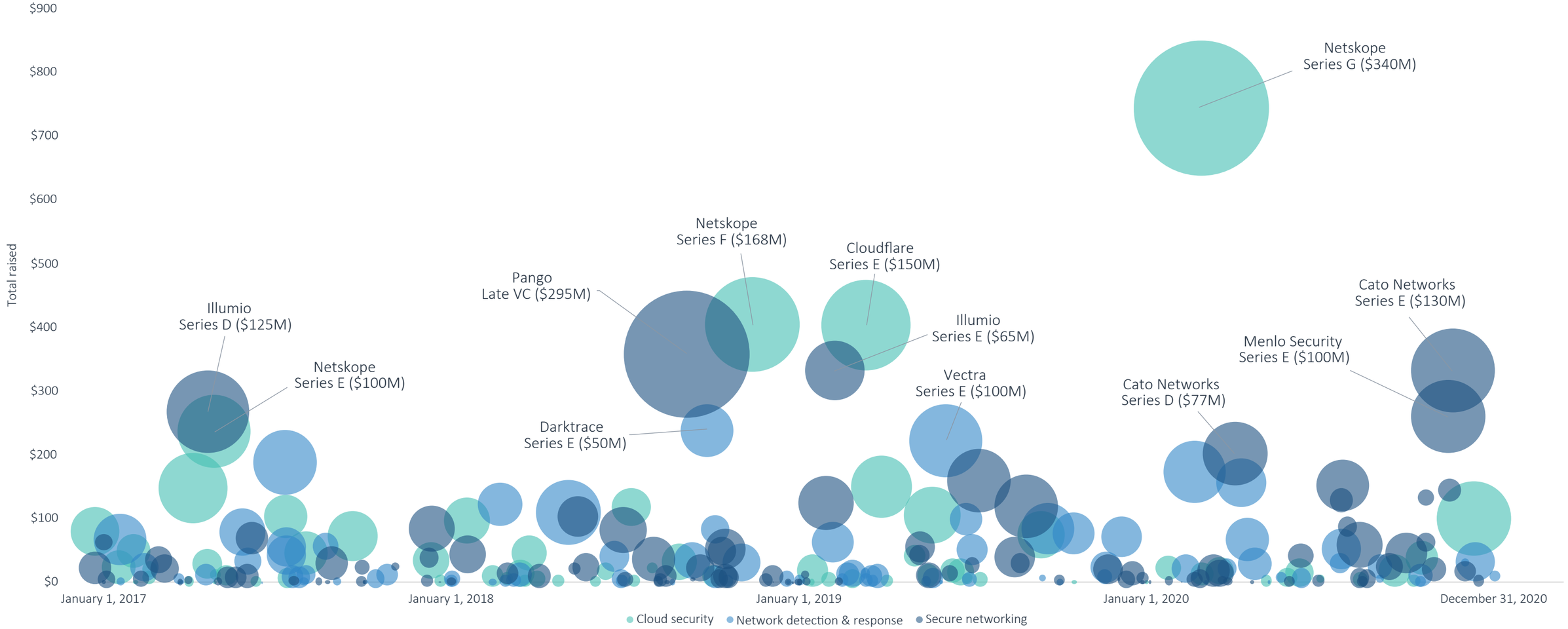
VC activity

VC activity in Q4 underscored the cloud security and SASE opportunities. In cloud security, high valuations were achieved by **Wiz** and **Orca Security**. **Wiz** achieved a $500.0 million post-money valuation in its Series A, primarily based on the experience of its founders, and **Orca** secured a 2.7x deal size step-up in only 7 months. Both startups offer vulnerability scanning for cloud environments. Cloud security is the fastest growing category in terms of end user spending and is supporting some of the highest valuation growth for the few startups that find product-market fit. In SASE, **Cato Networks** became a unicorn with a $130.0 million Series E. **Cato Networks** has layered security software onto an encrypted SD-WAN architecture and claimed to double revenue in 2020. We believe further high growth is ahead given strong growth forecasts for SD-WAN and SASE more broadly.

Zero trust network security approaches are continuing to drive M&A activity. The acquisitions of **Preempt Security** by **CrowdStrike** (NASDAQ: CRWD), **Fyde** by **Barracuda**, and **Odo** by **Check Point** (NASDAQ: CHKP) demonstrate high customer demand for zero trust network architecture. This technology is a critical component of SASE and has seen precedent acquisitions by **Zscaler** (NASDAQ: ZS), **Okta** (NASDAQ: OKTA), and **HPE** (NYSE: **HPE**) of **Edgewise Networks**, **ScaleFT**, and **Scytale**, respectively. In Q4, network detection & response vendor **Awake Security** was acquired by **Arista Networks** (NYSE: ANET). No acquisition value was disclosed, and given the company's fundraising history, we believe the company had not achieved scale. We have still not seen a venture-style exit from network detection & response startups. Cloud security startups have been challenged to scale given competition from hyperscalers and incumbents, resulting in a recent wave of early acquisitions in cloud security posture management (CSPM).

Figure 9.

Network security VC landscape ($M)



Source: PitchBook | Geography: North America & Europe

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
Wiz	December 9, 2020	Cloud security	$100.0	Series A	Insight Partners, Sequoia Capital, CyberStarts	N/A
Cato Networks	November 17, 2020	Secure networking	$130.0	Series E	Lightspeed Venture Partners	N/A
Menlo Security	November 12, 2020	Secure networking	$100.0	Series E	Vista Equity Partners	1.2x
Axiado	October 28, 2020	Secure networking	$10.9	Early-stage VC	Orbit Venture Partners	2.6x
Sonrai Security	October 15, 2020	Cloud security	$20.0	Series B	Menlo Ventures	1.9x

Source: PitchBook | Geography: North America & Europe

Figure 11.

Notable network security VC exits

COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE ($M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
Fyde	October 26, 2020	Cloud security	N/A	Thoma Bravo, Barracuda Networks	N/A	N/A
Awake Security	October 1, 2020	Network detection & response	N/A	Arista Networks	N/A	N/A
Odo	September 16, 2020	Cloud security	$30.0	Check Point Software Technologies	2.7x	N/A
OPAQ	July 20, 2020	Cloud security	$8.0	Fortinet	0.1x	N/A
Edgewise Networks	May 28, 2020	Cloud security	$30.7	Zscaler	0.8x	N/A

Source: PitchBook | Geography: North America & Europe

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, Andreesen 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 | Geography: North America & Europe

Figure 13.

Key network security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/FORWARD 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	NASDAQ: MCFE	4.1x	Cloud security, network vulnerability management & threat intelligence platforms	McAfee Skyhigh Security Cloud	Cloud security posture management auditing and compliance
Microsoft	NASDAQ: MSFT	11.0x	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	5.7x	Cloud security	Oracle CASB Cloud Service	Assesses SaaS and IaaS applications for common misconfigurations
Cloudflare	NYSE: NET	58.4x	Cloud security	Cloudflare DDoS Protection	Unlimited DDoS protection with low-friction user experience

Source: PitchBook | Geography: North America & Europe

Opportunities

Network detection & response tools: 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 integrate NDR tools with existing network performance management solutions, leading to multiple insertion points within the IT organization. The market crossed $1 billion in end user spending in 2020 and is forecast to grow at a 17.0% CAGR from 2021 to 2024. 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**.

Secure SD-WAN: Software-defined networks are converging with security software to give security vendors exposure to high growth in enterprise networking. Remote-worker devices, 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. 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 slowed SD-WAN growth, decelerating from over 100% YoY in 2019 to around 50% in 2020, with market research forecasts estimating 30-40% growth in 2021. The escalation of exit activity in this space in 2020, with **Palo Alto Networks** (NYSE: PANW)' acquisition of **CloudGenix** for $420.0 million and **HPE**'s acquisition of **Silver Peak** for $925.0 million, suggests that the space may produce a $1 billion+ outcome in the near term. **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.

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:

- Software-defined wide area networks (SD-WAN)
- 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.[5] Other estimates indicate that the enterprise penetration rate for a full stack of SASE solutions will increase from 5% in 2019

5: Worldwide Quarterly Security Appliance Tracker, IDC, 2020.

to 20% in 2023.[6] This has the potential to create a $10 billion market at a 20% adoption rate. As a result, we believe network security leaders including **Cisco** (NASDAQ: CSCO), Akamai (NASDAQ: AKAM), **Palo Alto Networks** (NYSE: PANW), **Netskope**, and **Zscaler** (NASDAQ: ZS) are in the process of building full-stack SASE solutions via R&D, M&A, and partnerships. with **Zscaler** (NASDAQ: ZS) taking a lead in the category. **Palo Alto Networks'** (NYSE: PANW) recent acquisition of **CloudGenix** for $420.0 million and **Cisco**'s $100.0 million acquisition of **Portshift** were explicitly tied to improvement of their SASE capabilities, as the companies shift their product suites from firewall appliance sales to cloud-delivered security. At the early stage, Elisity recently raised a Series A to bring a zero trust software-defined perimeter to market, showing that startups can build holistic solutions to this problem. 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.

Cloud Infrastructure Entitlement Management (CIEM): A leading cause for cloud breaches is overprivileging of cloud users. A range of business users including developers are granted access to all cloud resources they may need to deploy software. This access can be used by attackers or insiders to move laterally through cloud networks and access sensitive data, as evidenced by the Capital One breach. Given the risks of admin-level access and increased reliance on cloud resources, greater control over cloud identities is necessary. CIEM scans user permissions across cloud environments and enables review and remediation of excess privileges. This niche of cloud security is less susceptible to dominance by cloud providers than other cloud security products since user identities apply across on-premise and multi-cloud environments. The niche is being led by startups including **CloudKnox**, **Orkus** Security–which was acquired by identity governance & administration incumbent **Sailpoint**–Ermetic, **Sonrai**, and **Authomize**. Startups can differentiate based on the level of automated remediation they offer for policy enforcement. The niche's adjacency with access management offers greater potential for scale than most point solutions for cloud security.

Considerations

Innovative incumbents: The CASB market is saturated as incumbents aggressively buy and build solutions to maintain market share and relevancy despite disruptive challenges. 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** (NASDAQ: MSFT), **Amazon** (NASDAQ: AMZN), and **Google** (NASDAQ: GOOGL) 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

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

providers for customer data will provide a compelling reason to deploy a third-party cloud security solution, cloud providers have cost and customer data advantages 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.

Outlook

Network detection & response platforms to face consolidation: We believe network detection & response platforms are facing lower interest 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, enterprises may prioritize more practical SASE tools. The category is one of a few that has seen VC funding decline since 2017, signaling low investor interest, and deal value fell 19.9% in 2020 as unicorns did not raise further funding. Government and finance customers, the early adopters of the technology, may be insufficient to drive high growth at scale. The exit of **Awake Security** to **Arista Networks** may be the start of larger vendors in the space considering their strategic options. At the 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 face pressure to accept unfavorable exit terms.

Point solutions for CIEM and software security posture management (SSPM) 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 **CloudKnox** and **Obsidian Security** could be candidates to enhance the CASB offerings of other market leaders, including **Microsoft** (NASDAQ: MSFT) and **McAfee** (NASDAQ: MCFE).

COVID-19 to catalyze a shift from VPN to SASE: 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

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.

Web application protection 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 are running applications in container environments, up from 56% in 2017.[7] Container security has become a leading concern for IT departments as a result.

7: "2019 Container Adoption Survey," Portworx and Aqua Security, 2019.

APPLICATION SECURITY

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.[8]

Web application data breaches: Security research indicates that web application data breaches constitute around 70% of a sample of hacking action vectors,[9] suggesting that they are far more likely to be breached than network backdoors, VPNs, or third-party portals.

Market size

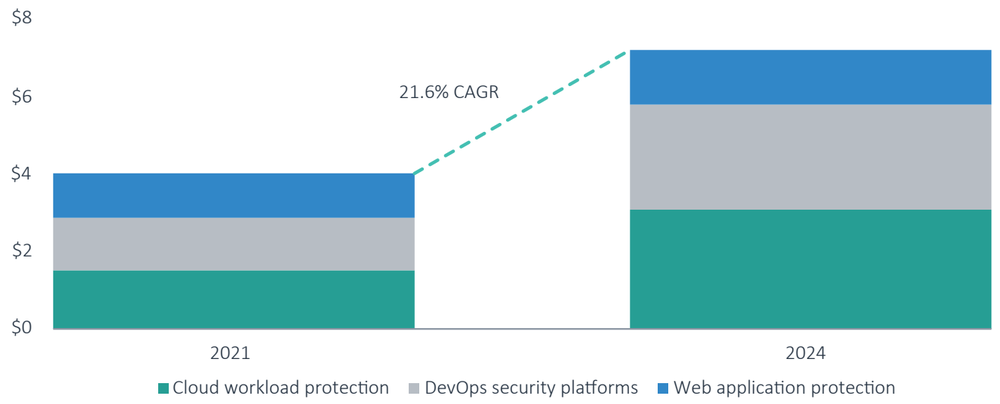
High growth in the relatively immature niche of application security is estimated to yield a $4.0 billion market in 2021, slightly down from our previous estimate due to a reassignment of vulnerability assessment tools to security operations. By 2024, the market is estimated to reach $7.2 billion at a 21.6% CAGR. We still believe that cloud workload protection is one of the fastest-growing segments in infosec, although from a low base of $1.3 billion in 2020. **Beyond** that category, this estimate includes application security testing, vulnerability assessment, and web application firewalls. We believe that an increased focus from DevOps practitioners on secure coding can create a S-curve in application security testing adoption and forecast 25.3% annualized growth in the category out to 2024.

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

8: "Digital Transformation Moves Application Security to the Top CISO/CSO Priority," Andre Tehrani, June 2020.
9: "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 FOR APPLICATION SECURITY COMPANIES

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

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 use 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.

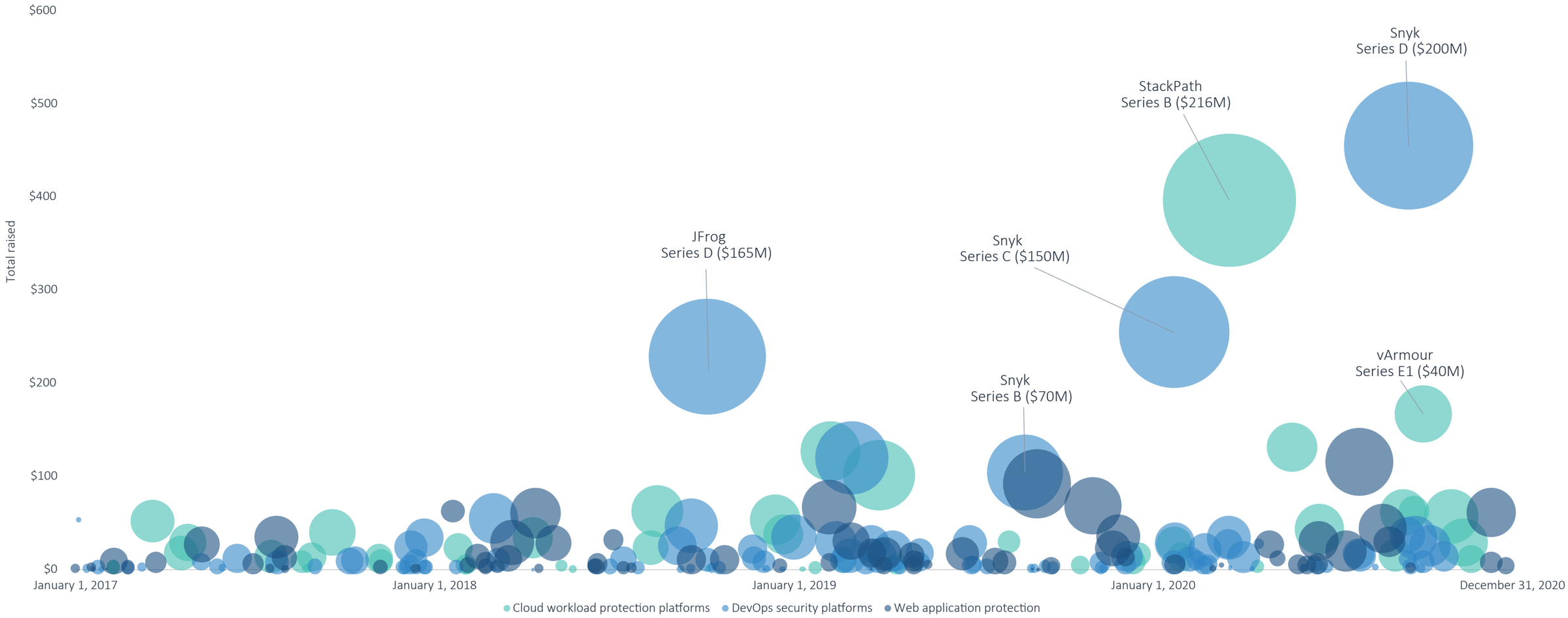
VC activity

The embryonic state of application security is creating primarily early-stage opportunities for leading VC investors. API security continued to be the hottest early-stage niche in application security, with **Salt Security** raising a Series B from **Sequoia Capital** 6 months after its Series A. **Sequoia Capital** also led a Series A for machine learning security (MLSec) startup **Robust Intelligence**, demonstrating the opportunity in protecting AI & ML algorithms in the next wave of computing. Infosec specialist investor **AllegisCyber** led a Series A for Deepfence, a cloud workload protection startup. The deal was led by former **McAfee** (NASDAQ: MCFE) CEO Dave Dewalt, who has remained a leader in security investing and consulting. Another specialist investor, ClearSky, co-led a Series A for DevOps security startup **Accurics**, joined by Intel Capital. VC opportunities in security exist across the DevOps lifecycle.

In Q4, acquisitions closed in web application protection, DevOps security, and cloud workload protection. **Cisco**'s acquisition of **Portshift** for $100.0 million demonstrates the urgency of container and serverless security to security incumbents. **Portshift** offers container and serverless software that is integrated across the software development lifecycle, addressing the horizontal integration opportunity addressed in our Q1 2020 analyst note on DevOps security. The size of this acquisition, after the company only raised a $5.3 million seed round in 2018, indicates a strategic premium to gain exposure to this emerging trend. A syndicate of leading infosec investors including Goldman Sachs, NightDragon, and ClearSky acquired web application protection startup **White Ops** for an undisclosed amount, citing the company's ability to defend web applications against fraud. The company has limited funding growth since its Series B in 2016, advancing our thesis that bot mitigation has limited demand. Italy-based DevOps security startup **Swascan** also exited for a low deal value. We have not seen an active M&A market for DevOps security startups emerge yet.

Figure 16.

Application security VC landscape ($M)



Source: PitchBook | Geography: North America & Europe

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 Security	December 8, 2020	Web application protection	$30.0	Series B	Sequoia Capital	1.6x
Deepfence	November 18, 2020	Cloud workload protection platforms	$9.5	Series A	AllegisCyber	4.5x
Robust Intelligence	October 21, 2020	DevOps security platforms	$11.0	Series A	Sequoia Capital	2.7x
vArmour	September 30, 2020	Cloud workload protection platforms	$40.0	Early-stage VC	N/A	1.2x
Snyk	September 15, 2020	DevOps security platforms	$200.0	Series D	Addition	2.0x

Source: PitchBook | Geography: North America & Europe

Figure 18.

Notable application security VC exits

COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE ($M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
White Ops	December 23, 2020	Web application protection	N/A	ClearSky, Goldman Sachs Merchant Banking Division, NightDragon Security	N/A	N/A
JFrog	September 16, 2020	DevOps security platforms	$3,549.7	N/A	8.3x	30.5x
Aporeto	December 23, 2019	Cloud workload protection platforms	$144.1	Palo Alto Networks	N/A	N/A
Protego Labs	December 2, 2019	Cloud workload protection platforms	$40.0	Check Point Software Technologies	4.0x	N/A
Twistlock	July 9, 2019	Cloud workload protection platforms	$378.1	Palo Alto Networks	N/A	27.3x**

Source: PitchBook, **Hampleton Partners | Geography: North America & Europe

Figure 19.

Key VC-backed application security companies

COMPANY	TOTAL VC RAISED ($M)	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
Snyk	$454.5	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
vARMOUR	$167.0	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
Aqua	$131.3	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
Contrast Security	$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
PerimeterX	$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 | Geography: North America & Europe

Figure 20.

Key application security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/FORWARD REVENUE	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
Synopsys	NASDAQ: SNPS	10.6x	DevOps security platforms	Seeker Interactive Application Security Testing platform	Comprehensive suite of testing services
Micro Focus	LON: MICRO	2.0x	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 (CY 2018)	DevOps security platforms	SecureSphere WAF	Strong customer support and bot mitigation

Source: PitchBook | Geography: North America & Europe

Opportunities

Application testing and composition analysis: We have seen COVID-19 catalyze the shift in processes and budgets needed to drive change in secure DevOps and increase demand for startup products in the space. From 2019 to 2020, the share of developer teams integrating security in multiple phases of the software development lifecycle increased from 63% to 70%, according to an industry survey.[10] A minority of teams integrate security in the build phase, which we believe still has room to double in adoption over the next several years. Even for organizations with mature security practices in their DevOps teams, tool adoption is uneven. According to a vendor survey, around 40% of mature DevOps security practices integrate static and dynamic application security testing, suggesting that the market is still relatively underpenetrated.[11]

Startups focused on this opportunity are offering tools for developers to detect vulnerabilities within open-source codebases and integrate security policies into continuous deployment pipelines. We estimate this opportunity to have an $9.2 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 D 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 present a growing type of attack vector that developers can easily implement. This 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 has further recognized its 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**, **42Crunch**, **imVision Technologies**, and **Wallarm**. **Salt**, **42Crunch**, and **Cequence Security** have achieved outstanding valuation step-ups at an early stage, while Traceable—founded by the former CEO of AppDynamics—achieved a $125.0 million pre-money valuation in its Series A, suggesting early traction in this emerging market. In January 2020, application security testing incumbent Synopsys acquired API security startup **Tinfoil Security**, suggesting that this capability may be strategic for application security vendors going forward.

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. We believe the market will remain fragmented, given that no vendor has a tenable claim to be a one-stop shop in application

10: "2020 State of DevOps Report," Puppet and CircleCI, November 2020.
11: "WhiteSource Report—DevSecOps Insights 2020," WhiteSource, September 30, 2020.

security. To address this pending tool sprawl, 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, and **ZeroNorth**, which has achieved a $40.0 million post-money valuation in its Series A. We believe some tool sprawl in application security is inevitable, and ASOC could become similar in size to SOAR at a nearly a $1 billion market over the next five years. COVID-19 should accelerate the need for remote workers to prioritize alerts given the reduced interaction of developers with security teams.

Machine learning security (MLSec): MLSec is under-addressed by startups and may create a new field of information security. ML carries its own security risks, including data poisoning, model theft, and reverse engineering. Current AI & ML processes integrate highly sensitive data in experimental and open-source environments without security experts involved in the process. Contrary to popular wisdom, the leading risk for AI practitioners by far is cybersecurity, according to a recent survey.[12] **Microsoft** (NASDAQ: MSFT) and Mitre recently launched a threat matrix for machine learning. Mitre's attack frameworks have been adoption drivers for cybersecurity tools more broadly and this framework might encourage ML operations teams to consider their defense-in-depth strategy, while giving vendors opportunities to align with the framework. **Microsoft** (NASDAQ: MSFT) finds that a new suite of application security tools will need to be implemented by ML development teams. Much as ML has raced ahead without incorporating DevOps, so it has made its models vulnerable by default. We believe that entrepreneurs are just beginning to address this opportunity head on, as evidenced by the recent seed and incubator rounds for **TrojAI**, **Neurocat** and **SafeRide Technologies**. In Q2, **Calypso AI**, the most advanced startup in this field that we have seen, raised a $13.0 million Series A from a syndicate of leading investors.

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 $4.7 billion in 2020. Gartner forecasts a 6.2% growth rate for the segment in 2020, which, if extrapolated forward, means the segment could be the second-smallest infosec segment in 2023.[13] However, we believe this estimate may prove to be conservative as DevOps teams increasingly allocate budget to security tools.

Cloud security providers may offer competing products to startups: Amazon (NASDAQ: AMZN) 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

12: "Global Survey: The State of AI in 2020," McKinsey Analytics, November 2020.

13: "Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020," Gartner, June 2020.

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** (NYSE: PANW), **McAfee** (NASDAQ: MCFE), **Cisco** (NASDAQ: CSCO), and **Check Point** initiated this trend, and Fastly's acquisition of **Signal Sciences** for $775.0 million demonstrates that security-adjacent vendors can support the trend as well. The limited supply of container- and serverless-focused security solutions may put upward pressure on valuations as interest from strategic buyers increases. **Palo Alto Networks** (NYSE: PANW) 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.[14] Recently, **Cisco** paid $100.0 million for container and serverless workload protection startup **Portshift** after its seed round. 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 by the swift rise of containers. Emerging technologies that can eliminate development bottlenecks, including manual application security testing and penetration testing, and have open-source business models are likely to fuel growth in this niche. In support of this trend, leading investors are developing investment theses in this space including **AllegisCyber**, NightDragon, Insight Partners, and Sapphire Ventures.

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 category 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. Deals in the space during the pandemic have not demonstrated strong deal sizes or valuation step-ups, suggesting the space is commercially challenged. **White Ops**' recent sale to a syndicate of VC firms demonstrates that bot mitigation may not be achieving commercial scale. We believe DevOps security tools and cloud workload protection platforms may have greater potential to create unicorns.

14: "M&A Market Report 2H 2018: Cybersecurity," Hampleton Partners, 2018.

SEGMENT DEEP DIVE

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.

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

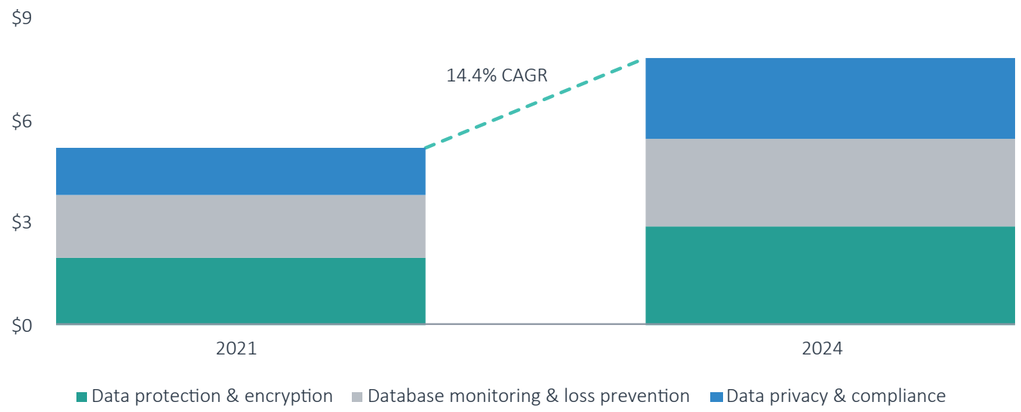
We forecast the market to reach $7.8 billion by 2024 at a 14.4% CAGR. This market includes encryption, data loss prevention, data privacy management, and tokenization. The data privacy management software market grew 60.3% in 2019 to $0.8 billion, and we forecast a $2.0 billion market by 2023, driven 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 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

Figure 21. DATA SECURITY MARKET SIZE ($B)



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

Figure 22. COMMON INDUSTRY KPIS FOR DATA SECURITY COMPANIES

- 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

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 $1,500 for an enterprise. Additional modules can be upsold including training, cookie management, and third-party risk management.

VC activity

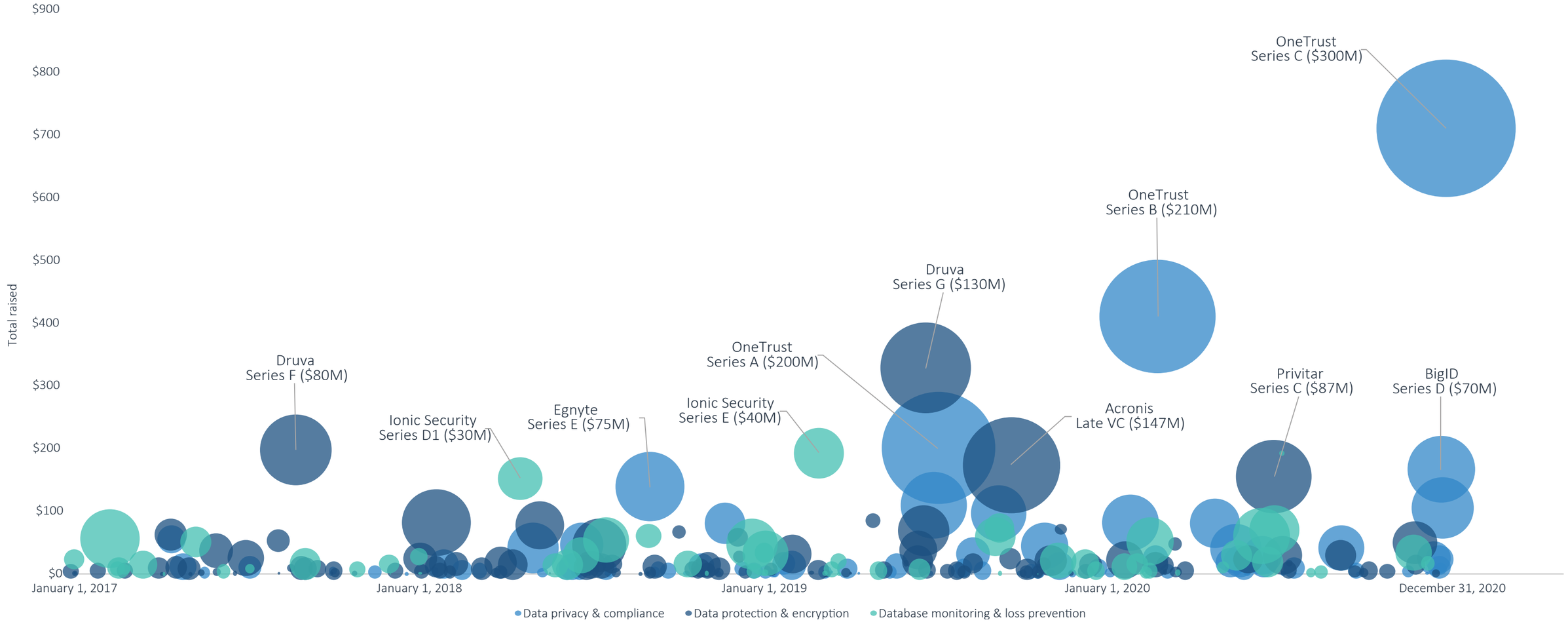
Data privacy & compliance has become one of the largest infosec categories in terms of VC funding due to rapid market size growth. In Q4, **OneTrust** raised its third mega-deal in 18 months from TCV, achieving a 1.8x valuation step-up to $4.8 billion pre-money in 10 months. **OneTrust** is progressing toward a winner-take-most solution in the emerging category of data privacy management. Its first-mover advantage and customer focus in the EU's GDPR (general data protection regulation) compliance are proving to be sustainable advantages.

In the same category, **Very Good Security** and **BigID** raised $60.0 million and $70.0 million rounds, respectively, with **BigID** reaching unicorn status at a 2.7x valuation-step up. At the early stage of this category, **Skyflow** emerged with a $97.5 million Series A post-money valuation to bring an outsourced privacy data vault to market, similar to the business model of **Very Good Security**. Capital is rushing into this category at high valuations, and the high growth phase is in full swing. Data protection & encryption and database monitoring & loss prevention are lagging behind, although there is a rising tide for innovative data security overall.

Q4 was active for data security exits with five, although none disclosed deal values. Imperva's acquisition of jSonar indicates that the data loss prevention category has become susceptible to disruption. The segment has seen neither significant growth nor innovation in recent years, with Gartner removing its Magic Quadrant for data loss prevention due to a lack of changes. We believe the lack of innovative incumbents has enabled startups to disrupt the market, particularly in data recovery and privacy. jSonar previously raised a Series C at a high valuation step-up at the outset of the pandemic, demonstrating that enterprises are increasing their data security spending while obtaining more sensitive data via digital transformation.

Figure 23.

Data security VC landscape ($M)



Source: PitchBook | Geography: North America & Europe

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

Figure 24.

Notable data security VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE ($M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
OneTrust	December 21, 2020	Data privacy & compliance	$300.0	Series C	TCV	1.8x
BigID	December 16, 2020	Data privacy & compliance	$70.0	Series D	Salesforce Ventures, Tiger Global Management	2.7x
Skyflow	December 8, 2020	Data privacy & compliance	$17.5	Series A1	Canvas Ventures	3.2x
InCountry	September 1, 2020	Data privacy & compliance	$33.0	Early-stage VC	Mubadala Capital-Ventures, Caffeinated Capital	6.6x
Immuta	June 23, 2020	Database monitoring & loss prevention	$40.0	Series C	Intel Capital	1.7x

Source: PitchBook | Geography: North America & Europe

Figure 25.

Notable data security VC exits

COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE ($M)	ACQUIRER/INDEX	VALUATION STEP-UP	VALUATION METRIC
JSonar	October 1, 2020	Database monitoring & loss prevention	N/A	Imperva, Thoma Bravo	N/A	N/A
Exostar	July 6, 2020	Data protection & encryption	$100.0	Thoma Bravo	N/A	N/A
ObserveIT	November 25, 2019	Database monitoring & loss prevention	$214.0	**Proofpoint**	N/A	N/A
Cognigo (Israel)	May 23, 2019	Data protection & encryption	$70.0	NetApp	N/A	N/A
ID Quantique	April 1, 2018	Data protection & encryption	$65.0	SK Telecom	N/A	N/A

Source: PitchBook, *Hampleton Partners | Geography: North America & Europe

Figure 26.

Key VC-backed data security companies

COMPANY	TOTAL RAISED ($M)	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
OneTrust	$710.0	Data privacy & compliance	Privacy program management	Ease of use for non-IT professionals	Coatue Management, Insight Partners
Ionic Security	$192.6	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	$166.2	Data privacy & compliance	Discovery Foundation	Classifies data in any environment	Scale Venture Partners, Tiger Global Management, Bessemer Venture Partners, ClearSky

Source: PitchBook | Geography: North America & Europe

Figure 27.

Key data security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/REVENUE	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
Forcepoint	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	NASDAQ: MCFE	4.1x	Database monitoring & loss prevention, data protection & encryption	**McAfee** Total Protection for DLP	Cost-effective suite of DLP solutions

Source: PitchBook | Geography: North America & Europe

Opportunities

Developer-friendly data vaults. The increased risk of data leaks, exemplified by the Capital One and **SolarWinds** breaches, is forcing hard choices for data security. CISOs are increasingly assuming they have been breached and are focusing on hardening databases, which had been a lower priority in recent years. One silver bullet is to outsource data storage to security vendors and access the data via secure APIs. As a template, Apple uses a "restricted access environment" to process data and remove personal identifying tags, resembling the basic architecture of a data vault. Data vault hosts can verify adherence to regulations and offer compliant access to data, transferring risk from the customer. Data backup is already a large industry, although it does not integrate with real-time streaming use cases. Startups are beginning to build modern data vaults, including **Very Good Security**, **Evervault**, and **Skyflow**. These emergent architectures—still at an early stage—would enable real-time analysis of private data stored offsite.

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.[15] 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 given use cases in customer data protection.

GDPR and CCPA privacy regulation compliance technology: 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 because of 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, led by **OneTrust**, **BigID** and **Securiti.ai**. A recent survey finds that nearly 33% of large US companies are planning to double their data privacy spending over the next year.[16]

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

16: "Future-Proofing Corporate Data Privacy: Budgeting and Solutions to Address Tomorrow's Compliance Challenges," FTI Consulting, May 2020.

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 industry.[17] **Microsoft's** (NASDAQ: MSFT) 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, although 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, 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 for both compliance and customer service. There is some precedent for strategic

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

acquisitions in fraud prevention from financial institutions such as Capital One (**Confyrm**) 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.

SEGMENT DEEP DIVE

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 denying 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:

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.

Identity governance & administration (IGA): Platforms that verify user identities based on corroboration of access requests with pre-defined policies. Technologies within this category include:

- Directory management
- Entitlement management
- Password management
- Provisioning

Access management (AM): Platforms that enforce permissions in runtime environments. Technologies within this category include:

- Access certification
- Single sign-on
- Privileged access management

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.[18]

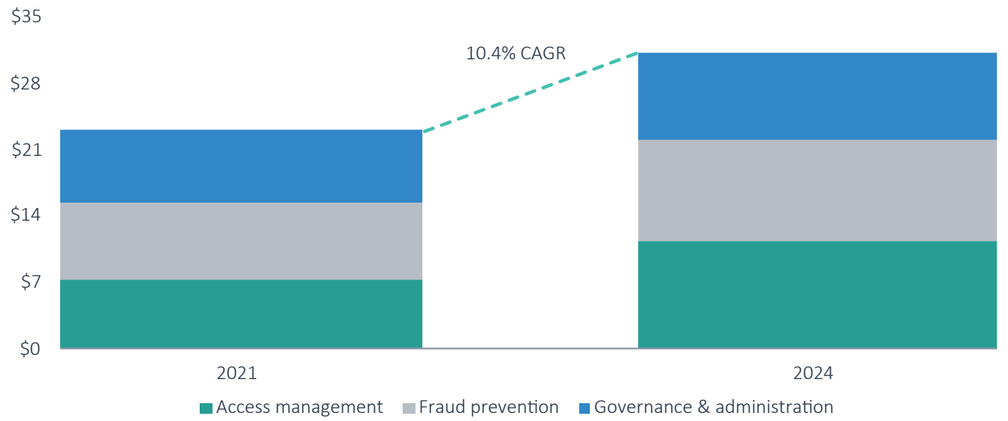
SaaS application growth: Enterprises are growing their use of SaaS applications and storage of sensitive data in those applications. Customers of IAM platform **Okta** (NASDAQ: OKTA) use 88 apps on average, up 21% in three years.[19] Employee identities must be managed across all these applications and monitored for insider threats.

Market size

IAM spending remained resilient in 2020 given enterprise requirements in identity governance and fraud prevention for remote workforces and ecommerce transactions, resulting in a $20.8

18: "2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis," Javelin, Krista Tedder & John Buzzard, April 7, 2020.
19: "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 FOR IDENTITY & ACCESS MANAGEMENT COMPANIES

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

billion market size estimate for the full year, making this the largest segment apart from security operations. Going forward, we forecast the market to reach $31.3 billion by 2024, representing a 10.4% CAGR from 2021. This estimate includes the IAM cornerstones of access management, identity governance & administration, privileged access management and authentication along with fraud prevention. Fraud prevention contributes a $7.3 billion market to 2020's total.

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 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** (NASDAQ: 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.

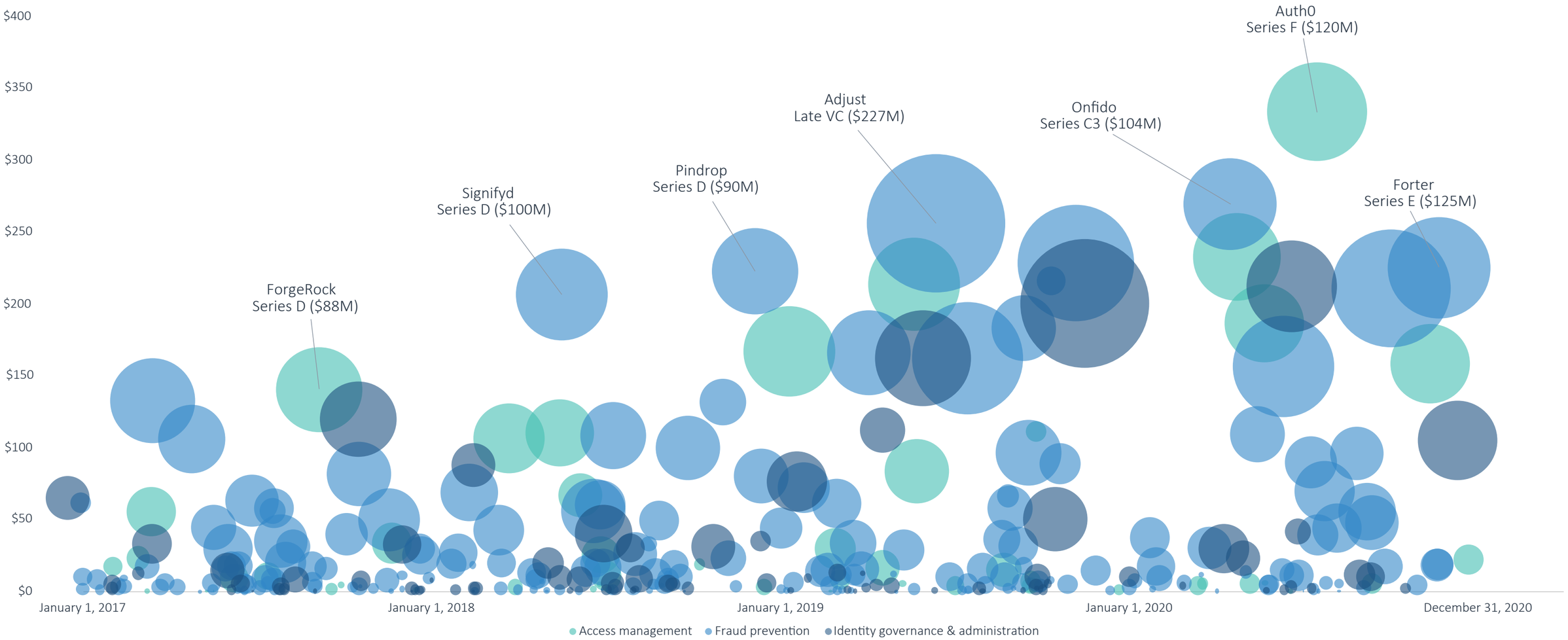
VC activity

IAM had a strong quarter of fundraising driven by large deals in each category with high step-ups. Fraud prevention vendor **Forter** became a unicorn with a 2.5x deal size step over its Series D in 2018. The company has become a leader in the emerging niche of chargeback guarantees and is demonstrating the potential for startups to achieve scale in this niche. In IGA, **Beyond Identity** achieved a 2.5x deal size step-up within 8 months, indicating that passwordless authentication is becoming the next wave of access control after multifactor authentication. **Beyond Identity**'s veteran founding team has enabled high valuation growth at an early stage. In access management, **JumpCloud** achieved a 2.6x valuation step-up to bring cloud-based identity management to midsize enterprises that are underserved by **Microsoft**'s (NASDAQ: MSFT) Active Directory. Identity is becoming the new perimeter in infosec, and enterprises are supporting high growth by disruptive startups.

Exit activity continued to be muted in this space, although **CrowdStrike**'s (NASDAQ: CRWD) entrance into zero trust demonstrated that access management is becoming more strategic for security incumbents. **CrowdStrike** (NASDAQ: CRWD) acquired access management startup **Preempt Security** for $96.0 million based on customer demand. Zero trust is an identity-based approach to access control that is bleeding into endpoint security and network security, given the limitations of antivirus and network traffic analysis to detect malicious behavior. Beyond this acquisition, IAM has seen little activity outside of fraud prevention, which can support both IPOs and acquisitions over $200 million. Access management and IGA have not yielded similar outcomes since **Duo Security**'s outlier exit to **Cisco** in 2018.

Figure 30.

Identity & access management VC landscape ($M)



Source: PitchBook | Geography: North America & Europe

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

Figure 31.

Notable identity & access management VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE ($M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
Beyond Identity	December 8, 2020	Identity authentication	$75.0	Series B	Koch Disruptive Technologies, New Enterprise Associates	2.3x
Forter	November 19, 2020	Fraud prevention	$125.0	Series E	Itai Tsiddon, Bessemer Venture Partners, Felix Capital	N/A
Mati	November 17, 2020	Fraud prevention	$13.3	Series A	Tribe Capital	3.8x
JumpCloud	November 10, 2020	Access management	$75.0	Early-stage VC	Blackrock Innovation Capital Group	2.6x
Alloy	September 5, 2020	Fraud prevention	$40.0	Series B	Canapi Ventures	3.8x

Source: PitchBook | Geography: North America & Europe

Figure 32.

Notable identity & access management VC exits

COMPANY	CLOSE DATE	SUBSEGMENT	EXIT SIZE ($M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
Preempt Security	October 1, 2020	Access management	$96.0	CrowdStrike	1.90x	N/A
Vesta Payment Solutions	May 28, 2020	Fraud prevention	$135.0	ACE & Company, Goldfinch Partners	N/A	N/A
Emailage	March 19, 2020	Fraud prevention	$480.0	LexisNexis Risk Solutions	2.23x	0.96x
Shape Security	January 24, 2020	Fraud prevention	$1,028.0	F5 Networks	0.96x	N/A
ZignSec	October 21, 2019	Identity authentication	$7.1	N/A	N/A	18.53x

Source: PitchBook | Geography: North America & Europe

Figure 33.

Key VC-backed identity & access management companies

COMPANY	TOTAL VC RAISED ($M)	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
Auth0	$333.5	Access management	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
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
Riskfied	$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**

Source: PitchBook | Geography: North America & Europe

Figure 34.

Key identity & access management incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/FORWARD REVENUE	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
Okta	NASDAQ: OKTA	42.1x	Access management	Single Sign-on	Ease of use for pre-built app integrations
SailPoint	NYSE: SAIL	13.4x	Identity governance & administration	IdentityIQ Access Management platform	Simple configuration
Microsoft	NASDAQ: MSFT	11.0x	Identity governance & administration	Azure Active Directory	Bundled with **Microsoft** 365 suite at a low cost
IBM	NYSE: IBM	2.2x	Identity governance & administration/fraud prevention	IBM Security Access Manager (IGA) and Pinpoint (Fraud Prevention)	Bundled package of access management and fraud prevention
Nice	TASE: NICE	10.4x	Fraud prevention	Actimize	Simple data integration tools

Source: PitchBook | Geography: North America & Europe

Opportunities

Passwordless identity provisioning: Research finds that brute force access or use of stolen credentials comprise more than 80% of hacking-related breaches,[20] 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. In 2020, **Microsoft** (NASDAQ: MSFT) has reported 50% growth in passwordless adoption in Azure Active Directory, suggesting that enterprises are growing comfortable with emerging security keys including biometrics and encryption devices.[21] A recent vendor survey finds that over 90% of IT and security professionals believe that a passwordless experience is likely for their organizations. The scale of **Duo Security**'s $2.4 billion exit to **Cisco** and the outperformance of **Okta** (NASDAQ: 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.

Identity-as-a-service: Offering IdaaS, which refers to cloud-native IGA through micro-services and APIs, enables developers to build 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** (NASDAQ: 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. **Okta** (NASDAQ: OKTA) recently was moved back in the Gartner magic quadrant for access management behind **Ping Identity** (NYSE: PING) and **Microsoft** (NASDAQ: MSFT) because of its limited integrations with directories and lack of support for customer identities. 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** (NASDAQ: 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.

ML-based chargeback guarantees: ML has become table stakes in fraud prevention, but legacy vendors struggle to tune their models to diverse customer environments and rely on human review and rules engines in many cases. ML models can be customized for different customer channels to achieve superior performance and offer guaranteed fraud reduction. Vendors with ensembles of multiple models can adapt to anomalous situations, and we believe startups are best positioned to address a range of customer types. Startups have already created a new category in chargeback guarantees, which is led by **Signifyd** and **Riskified**. Most vendors in the niche are private, are growing faster than the fraud prevention market overall, and have broken even financially, according to market research.[22] **Signifyd** has proven that manual review offers no improvement over its ML. Our prediction that multiple unicorns would be created in the space has been borne out by **Forter**'s Q4 Series E. Emerging entrants in the space include **Bolt Financial**, **Apruvd**, **Vesta Payment Solutions**, and **ClearSale**.

20: 2020 Verizon Data Breach Investigations Report, Verizon, 2020.
21: "A Breakthrough Year for Passwordless Technology," Microsoft, December 2020.
22: "Aite Matrix: Global Chargeback Guarantee Vendors," Aite Group, November 2020.

Considerations

Incumbent leadership in IGA: We see SailPoint and **Okta** (NASDAQ: 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** (NASDAQ: OKTA) has developed a cloud-first access management platform with growing functionality for developers.

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.

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.[23] 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.

Outlook

Consolidation likely in IDaaS: Legacy vendors such as **Microsoft** (NASDAQ: MSFT), **Oracle** (NYSE: ORCL), and IBM (NYSE: IBM) may find themselves falling behind **Okta** (NASDAQ: OKTA), **Ping Identity** (NYSE: PING), and **Sailpoint** in the IAM 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.

Passwordless authentication to create unicorns: Password management companies can achieve organic scale as evidenced by **1Password**, **Dashlane**, and **Duo Security**. **Duo Security** achieved unicorn status in its Series D before exiting. Startups in this space are just beginning their growth runways, and **Beyond Identity** appears poised to achieve unicorn status at a similar stage to **Duo Security**. **Averon**, **TruU**, and **Secret Double Octopus** have also achieved high valuation growth over the past two years. The support of **Microsoft** (NASDAQ: MSFT) for passwordless authentication should encourage a partner ecosystem that can support startups. Duo's partnership with **Microsoft** (NASDAQ: MSFT) Azure Active Directory was a catalyst for its growth, and **Beyond Identity** struck a similar partnership with **Microsoft** (NASDAQ: MSFT) in Q4.

Chargeback guarantee unicorns to go public: Our prediction that multiple fraud prevention unicorns would be created has actualized with **Forter**'s Series E. Going forward, we expect **Riskified** to test the public markets and may be joined by **Forter** and others. Ecommerce has become an outstanding public market theme with the outperformance of Shopify and **Amazon** (NASDAQ: AMZN), and fraud prevention unicorns offer additional exposure to this trend. Recently listed Palantir and C3.ai advertise their fraud detection capabilities in their prospectuses, demonstrating the appeal of the market to software vendors. Public companies in this space may offer high growth and outsized valuation multiples.

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

SEGMENT DEEP DIVE

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, and mobile device detection & response.

IoT/OT security: These solutions increase the visibility of distributed assets and enable security policy enforcement at the network edge. This subsegment includes mobile device management.

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.

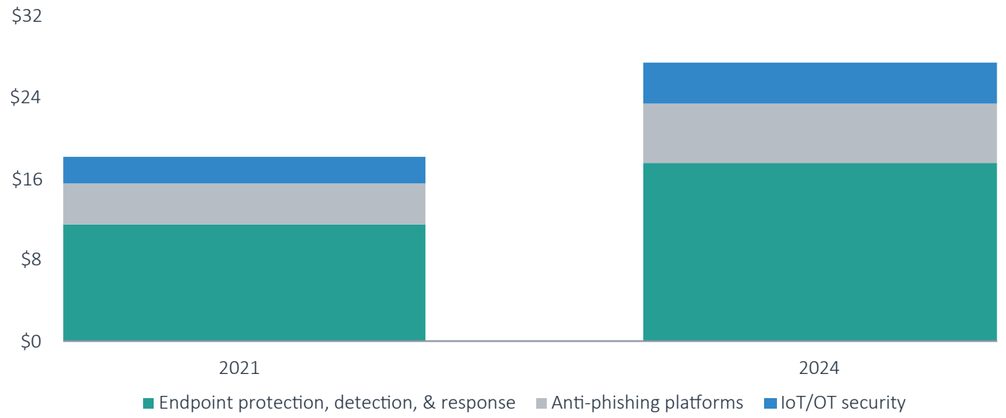
Emerging threat surfaces: The number of endpoint attack surfaces has multiplied in recent years, with mobile and IoT devices becoming indispensable parts of the enterprise. Attacks have been customized for each new attack surface, meaning that any device can be an entry point to the network.

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** (NASDAQ: CRWD) and **Carbon Black**.

Market size

We expect this market to grow to $15.8 billion in 2021, with mid-double-digit growth resuming. We forecast the market to grow to $27.6 billion at a 14.9% CAGR from 2021. Endpoint protection, detection & response platforms dominate the segment, and we anticipate the category will grow to $17.7 billion by 2024. The IoT security market is forecast to grow more quickly at a 16.0% CAGR over the same time frame, although the market remains small at $2.1 billion as of 2020, and this growth may be slowed by an

Figure 35. ENDPOINT SECURITY MARKET SIZE ($B)



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

Figure 36. COMMON INDUSTRY KPIS FOR ENDPOINT SECURITY COMPANIES

Financial

- Cloud revenue
- Customer count
- Orders over $100,000/ $1 million
- Average license order size ($)
- ARPU growth

Operational

- SaaS revenue %
- Maintenance renewal rate
- Number of incident response engagements annually
- Number of threat groups monitored

uneven recovery for the IoT industry. 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** (NASDAQ: MCFE) 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.

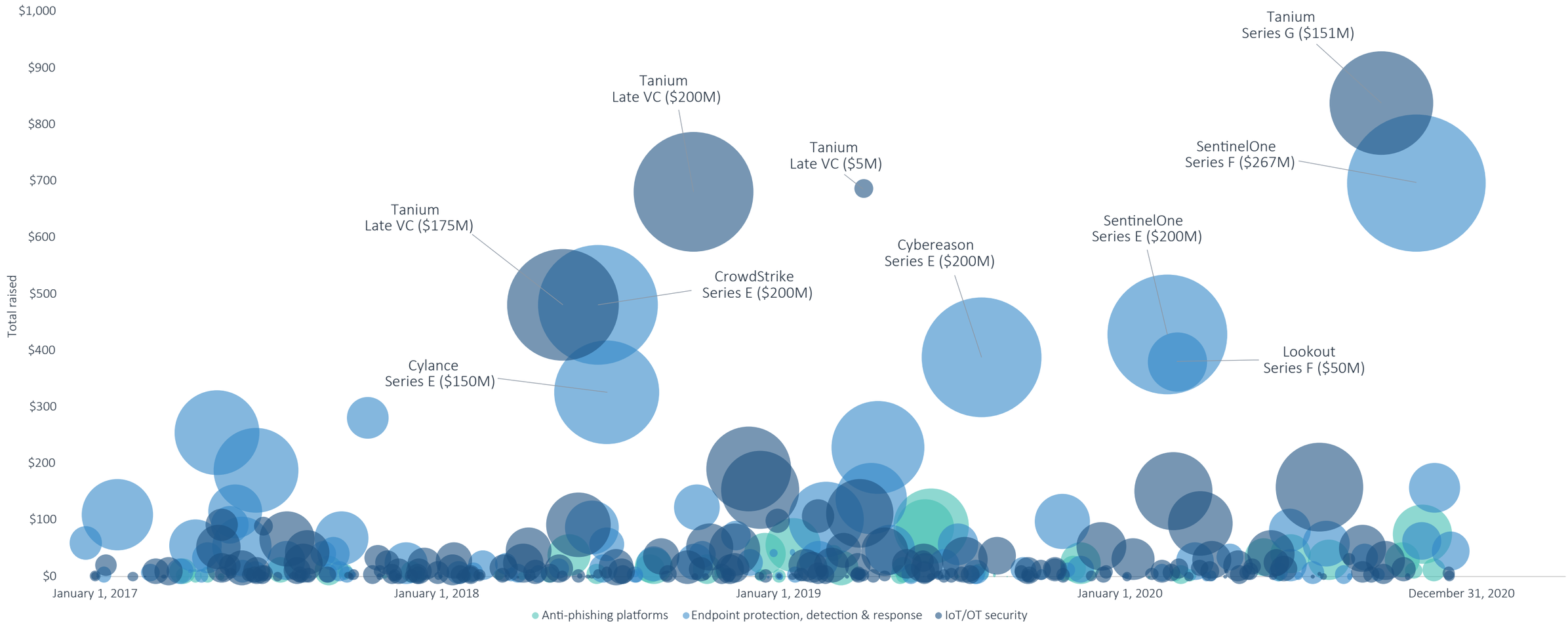
VC activity

This segment raised more than $600 million in Q4 due to mega-deals for endpoint detection & response unicorns **SentinelOne** and **Tanium**. The tripling of **SentinelOne**'s valuation in nine months demonstrates the high demand for endpoint and cloud security during the pandemic. **SentinelOne** demonstrates that endpoint detection & response vendors can integrate IoT security and cloud workload protection, tapping two of the highest-growing categories in infoSec. Unified endpoint management unicorn **Tanium** also raised a mega-deal as it continues to push out an IPO while capturing market share. Anti-phishing platform **Abnormal Security** achieved a 3.2x valuation step-up in a $50.0 million Series B, demonstrating that remote work has elevated the priority of email security.

A slow year for endpoint security exit activity picked up with the $800.0 million acquisition of **Expanse** by **Palo Alto Networks** (NYSE: PANW). This acquisition enables **Palo Alto Networks** (NYSE: PANW) to collect data from across enterprise threat surfaces for its XDR, security orchestration, and SOAR platforms. **Expanse** scans enterprise networks to give visibility over all internet-connected assets, of which enterprises typically have a limited view. While this acquisition is competitively priced at 11.9x EV/NTM revenue, the high exit value demonstrates that M&A can produce outstanding outcomes for startups aligned with incumbent strategies.

Figure 37.

Endpoint security VC landscape ($M)



Source: PitchBook | Geography: North America & Europe

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

Figure 38.

Notable endpoint security VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE ($M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
Abnormal Security	November 18, 2020	Anti-phishing platforms	$50.0	Series B	Menlo Ventures	3.2x
SentinelOne	November 11, 2020	Endpoint protection, detection and response	$267.0	Series F	Tiger Global Management	2.5x
Tanium	October 5, 2020	IoT/OT security	$150.5	Series G	Salesforce Ventures, TrueBridge Capital Partners, Fidelity Management & Research	N/A
Ironscales	August 10, 2020	Anti-phishing platforms	$23.0	Early-stage VC	K1 Investment Management, Jump Capital	1.0x
Dragos	July 31, 2020	IoT/OT security	$110.0	Series C	Koch Disruptive Technologies, National Grid Partners	2.2x

Source: PitchBook | Geography: North America & Europe

Figure 39.

Notable endpoint security VC exits

COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE ($M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/FORWARD REVENUE
Expanse	December 15, 2020	Endpoint protection, detection and response	$800.0	Palo Alto Networks	1.60x	11.9X*
CyberX	June 22, 2020	IoT/OT security	$170.0	Microsoft	N/A	5.07x
Armis (California)	February 7, 2020	IoT/OT security	$1,100.0	N/A	N/A	N/A
Indegy	December 2, 2019	IoT/OT security	$80.1	Tenable	N/A	N/A
Endgame	October 8, 2019	Endpoint protection, detection and response	$234.0	Elasticsearch	0.50x	N/A

Source: PitchBook, *Palo Alto Networks | Geography: North America & Europe

Figure 40.

Key VC-backed endpoint security companies

COMPANY	TOTAL VC RAISED ($M)	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
Tanium	$837.6	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
Sentinel One	$697.0	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 | Geography: North America & Europe

Figure 41.

Key endpoint security incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/FORWARD REVENUE	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
Crowdstrike	NASDAQ: CRWD	60.2x	Endpoint protection, detection & response	Falcon Platform	Bundled with managed threat hunting service
McAfee	NASDAQ: MCFE	4.1x	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 | Geography: North America & Europe

Opportunities

Operational technology (OT)/IoT security: In 2016, IoT devices were the vectors for major distributed denial-of-service (DDoS) attacks affecting PayPal, **Amazon** (NASDAQ: AMZN), Netflix, Spotify, and Twitter. New device vulnerabilities are discovered by security researchers on a constant basis, demonstrating that common devices and network protocols are vulnerable by default. 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. Vendors can specialize in each of these technologies to address different device types and enterprise requirements. In practice, each of these solutions is required to achieve defense-in-depth for an emerging threat surface.

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 by **Cisco**, **Palo Alto Networks** (NYSE: PANW), and **Tenable**, among others, 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, underscoring the variety of vendors that 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 specialists **Claroty** and **Dragos**.

XDR: Endpoint security has gone through clear shifts over time that have yielded opportunities to forward-thinking vendors. Over the past five years, endpoint protection has ceded ground to endpoint detection & response, which has further presaged the rise of managed detection & response. The fundamental catalyst behind these shifts is the failure of endpoint protection platforms to adequately detect breaches before malware is deployed on an endpoint, which requires increased visibility over endpoint behavior to detect and mitigate attacks in progress. Managed detection & response has been valuable in analyzing high volumes of endpoint alerts, although it is largely a manual process that is offered by both legacy managed service providers and technology companies such as **CrowdStrike** (NASDAQ: CRWD). The next phase of endpoint security is emerging as extended detection & response, which automates the detection & response phases of endpoint attacks. XDR offers an opportunity to replace not only outdated antivirus solutions, but also expensive and labor-intensive SIEM platforms. As a result, 70% of IT and security teams are planning to budget for XDR over the next 6-12 months, according to a vendor-supported market research survey.[24] Private vendors, including **Cybereason** and **SentinelOne** as well as new entrants **Hunters**, **Confluera**, and **Kognos**, stand to benefit from this.

Sophisticated anti-phishing solutions: Given the high degree of concern around COVID-19, hackers have created new phishing attacks, which refer to fraudulent

24: "The Impact of XDR in the Modern SOC," ESG, November 2020.

communications intended to steal data or install malware. COVID-19 has caused a spike in SMS- and social media-based attacks, often relating to COVID-19 tracking applications. 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 **Ironscales**, **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.[25] 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.

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** (NASDAQ: CRWD), **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.

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

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** may be a potential target, though the company is not likely to achieve unicorn status. In email, **Avanan** has developed solutions for several common vulnerabilities for **Microsoft** (NASDAQ: MSFT) Office 365 and thus may be a logical acquisition target for **Microsoft** (NASDAQ: MSFT).

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 **McAfee** (NASDAQ: MCFE) may face pressure to acquire automation-driven endpoint platforms as part of its XDR strategy or see its market share further erode. Because of the disruption potential in this market, EDR may produce further outlier exits after **CrowdStrike** (NASDAQ: CRWD).

SEGMENT DEEP DIVE

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 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

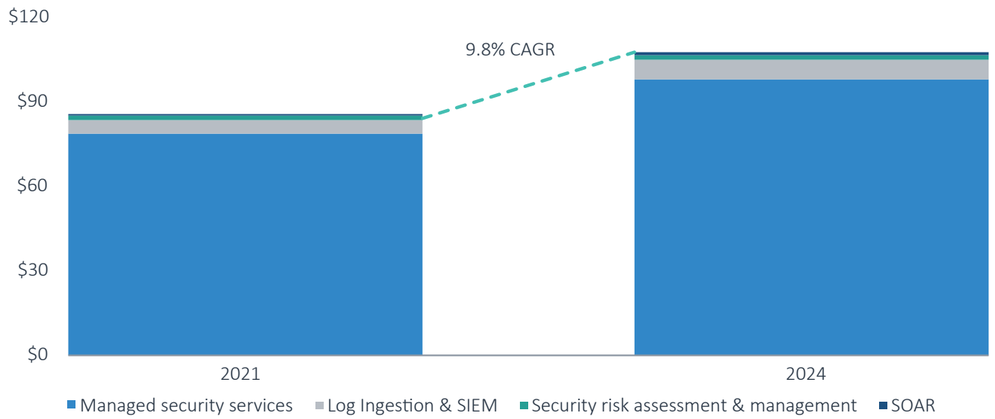
Security talent shortage: A shortage of security talent is driving CISOs to invest in software to handle alerts. A recent survey found that 44% of IT departments have a problematic shortage of cybersecurity skills at their organization.[26] This percentage dropped slightly for the first time since 2015.

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.[27] 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**.

26: "ESG Research Report: 2020 Technology Spending Intentions Survey," ESG Research, Bill Lundell, February 2020.
27: "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 FOR SECURITY OPERATIONS COMPANIES

Financial

- Cloud revenue
- Customer count
- Orders over $100,000/ $1 million
- Average license order size ($)
- ARPU growth

Operational

- SaaS revenue %
- Maintenance renewal rate
- Number of incident response engagements annually
- Number of threat groups monitored

Market size

We estimate the security operations market, exclusive of professional services, will amount to $16.0 billion in 2021. This estimate reflects 11.3% growth in 2021, and we forecast the market to become a $21.1 billion market in 2024, growing at a 9.8% CAGR. This market size reflects end-user spending in all four subsegments. Managed security services is the largest subsegment of the market, estimated to be $73.9 billion in 2020. 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 10.3% and 20.4% CAGRs, respectively. The high-growth forecast in SOAR is a primary reason for the subsegment's level of 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

Managed security service startups achieved high valuation step-ups in Q4. **Arctic Wolf** secured a 3.9x valuation step-up in seven months, becoming a unicorn with a $200.0 million investment led by Viking Global Investors. The company claimed 106% YoY growth in subscription revenue and attributed its growth to managed detection & response, which is also a leading driver of **CrowdStrike**'s (NASDAQ: CRWD) business. Deepwatch, which features managed detection & response in its product suite as well as a partnership with endpoint security unicorn **Cybereason**, secured a 3.3x valuation step-up in a round led by Goldman Sachs Growth Equity. Managed security services remain the largest market within infosec and are supporting high growth for cloud-native challengers.

Exit activity was led by **FireEye**'s (NASDAQ: FEYE) acquisition of SIEM startup **Respond Software** for $186.0 million. This acquisition continues the trend of incumbents acquiring security automation startups to offer XDR. Also in Q4, VMWare (NYSE: VMW) acquired

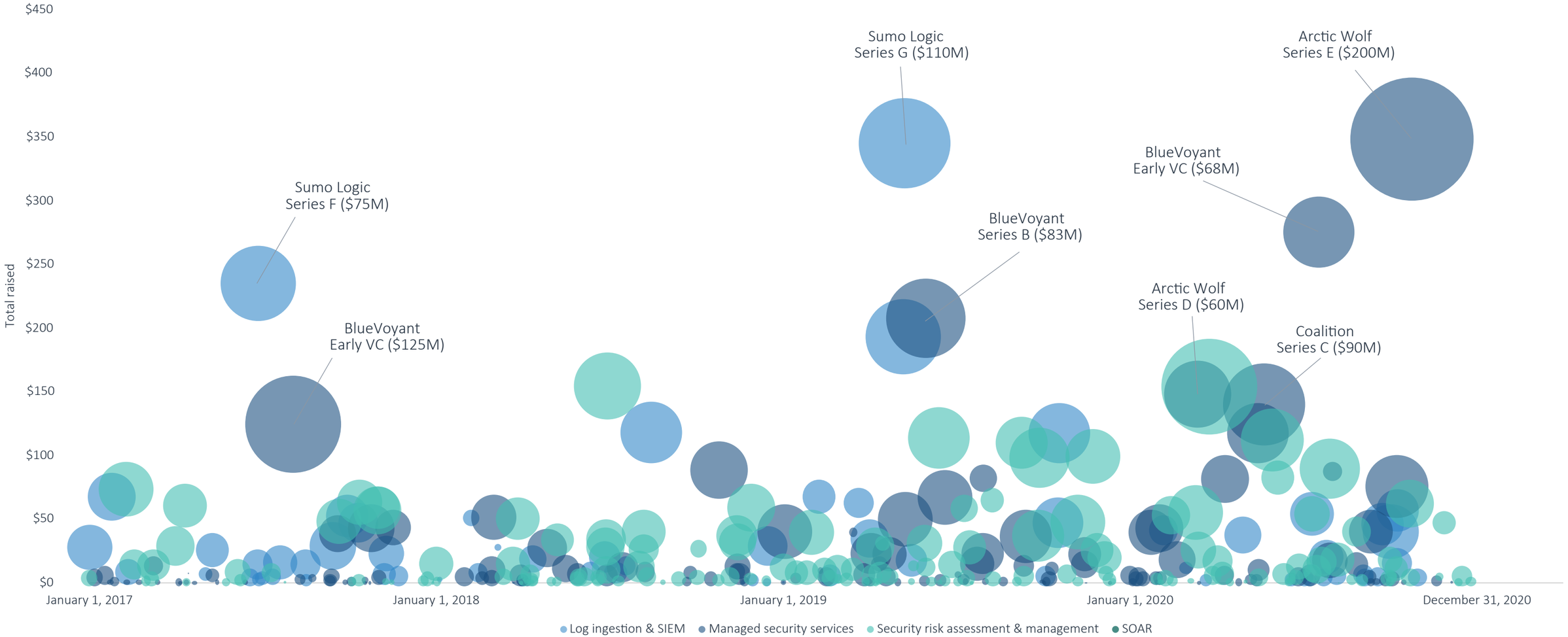
SECURITY OPERATIONS

SOAR startup **SaltStack** after its Series A in 2018, likely with a deal value under $100 million. Precedent acquisitions of XDR-relevant security operations startups were made by Fortinet (NASDAQ: FTNT) (Cybersponse), **Microsoft** (NASDAQ: MSFT) (**Hexadite**), **McAfee** (NASDAQ: MCFE) (Uplevel), and **Palo Alto Networks** (NYSE: PANW) (**Demisto**). XDR competitors **CrowdStrike** (NASDAQ: CRWD) and **Trend Micro** (TKS: 4704) may face pressure to make acquisitions in this space.

Q4 continued to validate our views that the SIEM & SOAR markets have been challenged in 2020 and than incumbents will seek cost-effective assets via M&A to bolster their automation efforts.

Figure 44.

Security operations VC landscape ($M)



Source: PitchBook | Geography: North America & Europe

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

Figure 45.

Notable security operations VC deals

COMPANY	CLOSE DATE	SUBSEGMENT	DEAL SIZE ($M)	STAGE	LEAD INVESTOR(S)	VALUATION STEP-UP
Arctic Wolf	October 22, 2020	Managed security services	$200.0	Series E	Viking Global Investors	3.9x
4iQ	October 20, 2020	Security risk assessment & management	$30.0	Series C	ForgePoint Capital, Benhamou Global Ventures	N/A
Illusive Networks	October 7, 2020	Log ingestion & SIEM	$24.0	Series B1	Citi Ventures, **Cisco** Investments, and Spring Lake Partners	N/A
deepwatch	October 7, 2020	Managed security services	$53.0	Early-stage VC	Goldman Sachs Growth Equity	3.3x
DefenseStorm	August 25, 2020	Security risk assessment & management	$11.9	Series B	Georgian Partners	1.5x

Source: PitchBook | Geography: North America & Europe

Figure 46.

Notable security operations VC exits

COMPANY	CLOSE DATE	SUBSEGMENT	EXIT VALUE ($M)	ACQUIRER/INDEX	VALUATION STEP-UP	EV/TRAILING REVENUE
Respond Software	November 18, 2020	Log ingestion & SIEM	$186.0	**FireEye**	2.48x	N/A
Sumo Logic	September 17, 2020	Log ingestion & SIEM	$1,845.6	N/A	1.56x	11.97x
Recorded Future	May 30, 2019	Security risk assessment & management	$780.0	Insight Partners	3.12x	N/A
Verodin	May 28, 2019	Security risk assessment & management	$264.9	**FireEye**	2.63x	N/A
Tufin	April 11, 2019	SOAR	$439.6	N/A	N/A	6.30x

Source: PitchBook, Hampleton Partners | Geography: North America & Europe

Figure 47.

Key VC-backed security operations companies

COMPANY	TOTAL VC RAISED ($M)	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION	LEAD INVESTORS
Arctic Wolf	$348.5	Managed security services	Security as a service	Managed detection & response	Viking Global Investors, Stereo Capital, Blue Cloud Ventures, Australia Future Fund, Sonae IM, Redpoint Ventures, Lightspeed Venture Partners
BlueVoyant	$275.5	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
Coalition	$140.0	Managed security services	Cyber-insurance	Bundled security services and insurance policies	Felicis Ventures, Ribbit Capital

Source: PitchBook | Geography: North America & Europe

Figure 48.

Key security operations incumbents

COMPANY	PRIVATE/PUBLIC STATUS	EV/FORWARD REVENUE*	SUBSEGMENT	KEY PRODUCTS	PRODUCT DIFFERENTIATION
Splunk	NASDAQ: SPLK	12.3x	SIEM & SOAR	Security Intelligence Platform	Powerful monitoring functionality bundled with other IT data collection use cases
Dell	NYSE: DELL	1.1x	SIEM & SOAR	SecureWorks	Bundles SIEM, network monitoring, EDR and behavior analysis
IBM	NYSE: IBM	2.2x	SIEM & SOAR, managed security services	QRadar	Marketplace contains IBM and third-party integrations
McAfee	NASDAQ: MCFE	4.1x	SIEM & SOAR	Enterprise Security Manager	Modern architecture using Kafka and Elasticsearch

Source: PitchBook | Geography: North America & Europe

Opportunities

Third-party security rating services (SRS): In the aftermath of the **SolarWinds** breach, enterprises will need to prioritize the cyber hygiene of third-party relationships. Third-party security assessments are typically conducted quarterly or annually and can be manual processes of reviewing an audit checklist. In the case of **SolarWinds**, however, an annual review may not have exposed the vendor's lax software security practices. More broadly, a recent vendor survey finds that 80% of medium-to-large enterprises have suffered a third-party data breach over the past 12 months.[28] Ongoing cloud-native security checks can identify issues more quickly and address what is becoming a board-level problem. **CyberGRX** and **SecurityScorecard** have scaled to $290.0 and $410.0 million post-money valuations, respectively, in this space to periodically assess vendor risk, and Black Kite (formerly known as **NormShield**) recently achieved a $25.0 million Series A pre-money valuation to bring near real-time assessment of vendor compliance. We believe the space hasn't seen substantial technical innovation and lacks integrations with risk management software, and that continuous software scanning will be required to manage a high volume of vendor relationships. After Mastercard's acquisition of **RiskRecon**, this space could become attractive for M&A from both managed service providers and XDR incumbents.

Cloud SIEM: A minority of SIEM instances are delivered via the cloud currently, although we believe the vast majority will be over the next several years. SIEM platforms currently require dedicated staff and complex integrations with on-premise systems. As a result, they can be the most expensive tool in the security stack, although they do not typically offer automated remediation. Leading incumbent **Splunk** (NASDAQ: SPLK) is struggling through a cloud transition, reporting an 11% revenue loss in Q3 2020. In endpoint security, we have seen the transition from a legacy product to a cloud-delivered product drive customer churn toward cloud-first solutions, and we believe similar potential exists in the $4.5 billion SIEM market. Recently NASDAQ-listed challenger **Sumo Logic** (NASDAQ: SUMO) acquired SIEM startup Jask to launch a Cloud SIEM and began to win large deals with the product in late 2020. At the early stage, **Panther Labs** emerged as a cloud SIEM contender with a $15.0 million Series A led by Lightspeed Venture Partners, demonstrating that a leading security investor sees disruption opportunity in the mature SIEM niche. **Panther Labs** focuses on alerts from cloud environments, an area that existing SIEM solutions are poorly positioned to address. We believe that the SIEM market may bifurcate into cloud SIEM for sophisticated security teams and XDR solutions for mid-sized enterprises going forward.

SMB managed services: 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 market research survey indicates that 26% of US SMBs plan to increase their security budgets as a result of remote work.[29] 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.

28: "Supply Chain Cyber Risk: Managing Cyber Risk Across the Extended Vendor Ecosystem," BlueVoyant, September 2020.

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

Considerations

Crowded SIEM and SOAR markets and rapidly innovating incumbents: SIEM is a mature market with numerous point solution vendors. For example, **Sumo Logic** (NASDAQ: SUMO), an IT vendor, integrates SIEM with its log management platform. Incumbents such as **Splunk** (NASDAQ: SPLK), through its **Phantom Cyber** acquisition, and IBM (NYSE: 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** (NASDAQ: CRWD) offers managed detection and response in addition to its automated threat detection platform, limiting the amount of service needed. While 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.

Outlook

Incumbents to continue adding SOAR capabilities to their product suites through M&A: **Palo Alto Networks** (NYSE: PANW) was not a leader in SIEM and yet paid a high price for **Demisto** to enhance its SOAR capabilities at 46.7x revenue. **VMware** (NYSE: VMW) and **FireEye** (NASDAQ: FEYE) recently continued this trend with acquisitions of **SaltStack** and **Respond Software**, respectively. We expect that SIEM leaders will enhance their product portfolios and identify several automation providers including **Exabeam**, **Siemplify**, and **Swimlane**. 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 manage security service providers as the higher-margin profile of pure-play software startups will merit higher valuations.

Supplemental materials

Select company analysis

Founded in
2012

Over
1,000
employees in four offices globally

Total raised:
$744M

Leader in the Gartner Magic Quadrant for CASB, Forrester Wave for Cloud Security Gateways and IDC MarketScape Worldwide Cloud Security Gateways Vendor Assessment

Last financing post-money valuation: $2.8 billion

Last financing: Raised $340.0 million in a Series G

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 via a secure web gateway 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 Q3, **Netskope** has shown the ability to benefit from remote work via integration with **Microsoft** (NASDAQ: MSFT) Teams and partnerships with **Okta** (NASDAQ: OKTA), **CrowdStrike** (NASDAQ: CRWD) and **Proofpoint**. The company reported 80% growth in logo count 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 (NASDAQ: FTNT). 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**,

SUPPLEMENTAL MATERIALS

Select company analysis

Bitglass and **McAfee** (NASDAQ: MCFE). 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 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 makes it a leader in the emerging SASE category 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** (NYSE: PANW) and **Zscaler** (NASDAQ: ZS) 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 vectors for 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 stack, and could benefit from M&A in cloud workload protection.

Financing history

SERIES G

February 6, 2020

Total raised ($M):
$340.0

Pre-money valuation ($M):
$2,460

Investors:
Sequoia Capital (lead), Canada Pension Plan Investment Board, Public Sector Pension Investment Board, Existing Investors

SERIES F

November 13, 2018

Total raised ($M):
$167.8

Pre-money valuation ($M):
$1,225

Investors:
Lightspeed Venture Partners (lead), Accel. Base Partners, Geodesic Capital, ICONIQ Capital, Omega Venture Partners, Sapphire Ventures, Social Capital

SERIES E

April 27, 2017

Total raised ($M):
$100.0

Pre-money valuation ($M):
$425.0

Investors:
Lightspeed Venture Partners (lead), Accel (lead), Dell Technologies Capital, Geodesic Capital, ICONIQ Capital, Sapphire Ventures

SERIES D

September 3, 2015

Total raised ($M):
$75.0

Pre-money valuation ($M):
$275.0

Investors:
Iconiq Capital (lead). Accel, Lightspeed Venture Partners, New York Life Ventures, Social Capital, ICONIQ Capital

SERIES C

May 15, 2014

Total raised ($M):
$35.0

Pre-money valuation ($M):
$150.0

Investors:
Accel (lead), Lightspeed Venture Partners, Social Capital

SERIES B

October 3, 2013

Total raised ($M):
$21.0

Pre-money valuation ($M):
$54.0

Investors:
Lightspeed Venture Partners, Social Capital

Select company analysis

CONTRAST SECURITY

Founded in
2014

About
277
employees in five offices globally

Total raised:
$120M

Visionary in Gartner Magic Quadrant for application security testing

Strong performer in Forrester Wave for runtime application self-protection

Last financing post-money valuation: $480.0 million

Last financing: Raised $65.0 million 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. In Q4, Contrast announced a holistic Application Security Platform that moves the company toward software composition analysis and application security orchestration & correlation (ASOC). **Contrast**'s growth metrics compare favorably to **CrowdStrike** (NASDAQ: CRWD), though at a lower revenue base. 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 Q4, Contrast hired a former Citrix executive as Chief Product Officer, lending public company experience to the executive team.

SUPPLEMENTAL MATERIALS

Select company analysis

CONTRAST SECURITY

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	March 1, 2018	September 28, 2016
Total raised ($M): $65.0	**Total raised ($M):** $30.0	**Total raised ($M):** $16.0
Pre-money valuation ($M): $415.0	**Pre-money valuation ($M):** $169.8	**Pre-money valuation ($M):** $64.0
Investors: Warburg Pincus (lead), Battery Ventures, Acero Capital, AXA Venture Partners, General Catalyst, M12	**Investors:** Battery Ventures (lead), Acero Capital, AXA Venture Partners, General Catalyst, In-Q-Tel, M12	**Investors:** General Catalyst (Lead), Acero Capital

SERIES A
June 25, 2014
Total raised ($M): $8.6
Pre-money valuation ($M): $12.8
Investors: Acero Capital

FINANCIAL METRIC	GROWTH YOY (FY18)
Annual recurring revenue	>120%
Net retention rate	>135%
Number of transactions $1 million or greater	500%

Source: Contrast Security

Select company analysis

Founded in
2013

About
650
employees in 33 countries

Total raised:
$213.5M

Visionary in Gartner Magic Quadrant for Access Management

Last financing valuation: $1.2 billion

Last financing: Raised $103.0 million in a Series E

Lead investors: Sapphire Ventures, Meritech Capital Partners, Trinity Ventures, Bessemer Venture Partners

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 customer-facing applications. 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. The company has a strong partnership with AWS IAM and recently added a partnership with Salesforce along with a strategic investment from Salesforce Ventures. In Q4, the company was ranked 156th in Deloitte's Fast 500 for its 3-year revenue CAGR, above other higher-valued unicorns including GitLab and **SentinelOne**.30

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

Co-founder and CEO Eugenio Pace was formerly principal lead program manager in technical guidance at **Microsoft** (NASDAQ: MSFT). Co-founder and CTO Matías Woloski was formerly an enterprise architect at Argentina-based Southworks and a professor of cloud computing. Thus far in 2021, the board has added former executives from **HPE**, SendGrid, and MuleSoft, giving the company the expertise necessary to pursue an IPO.

Competitors

Auth0 competes with access management leaders including **Okta** (NASDAQ: OKTA),

30: "2020 Technology Fast 500: Recognizing Growth & Innovation," Deloitte, November 2020.

Select company analysis

Microsoft (NASDAQ: MSFT), **Oracle** (NYSE: ORCL), IBM (NYSE: IBM) and **Ping Identity** (NYSE: PING). 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** (NASDAQ: 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** (NASDAQ: OKTA) focuses on employees.

Outlook

We believe **Auth0** is a strong IPO candidate given its high revenue growth and new board appointments. The company has announced that the company could IPO as early as 2022. Salesforce Ventures' recent investment in the company resembles its recent pre-IPO round in Snowflake, suggesting that the investor may see similar listing potential in **Auth0**, along with strategic synergy.

Financing history

SERIES F

July 14, 2020

Total raised ($M):
$120.0

Pre-money valuation ($M):
$1,800

Investors:
Salesforce Ventures (lead), DTCP, Founders Circle Capital, Bessemer Venture Partners, K9 Ventures, Meritech Capital Partners

SERIES E

May 20, 2019

Total raised ($M):
$103.0

Pre-money valuation ($M):
$1,057

Investors:
Sapphire Ventures (Lead), Bessemer Venture Partners, K9 Ventures, Meritech Capital Partners, Trinity Ventures, World Innovation Lab

SERIES D

May 15, 2018

Total raised ($M):
$55.2

Pre-money valuation ($M):
$465.0

Investors:
Sapphire Ventures (Lead), Bessemer Venture Partners, K9 Ventures, Meritech Capital Partners, Trinity Ventures, World Innovation Lab

SERIES C

March 14, 2017

Total raised ($M):
$30.0

Pre-money valuation ($M):
$220.0

Investors:
Meritech Capital Partners (Lead), Bessemer Venture Partners, K9 Ventures, Cygnus Capital, NTT Docomo Ventures, Telstra Ventures, Trinity Ventures

SERIES B

August 24, 2016

Total raised ($M):
$16.0

Pre-money valuation ($M):
$80.0

Investors:
Trinity Ventures (Lead), Bessemer Venture Partners, K9 Ventures, Silicon Valley Bank

SERIES A

June 24, 2015

Total raised ($M):
$6.9

Pre-money valuation ($M):
$27.4

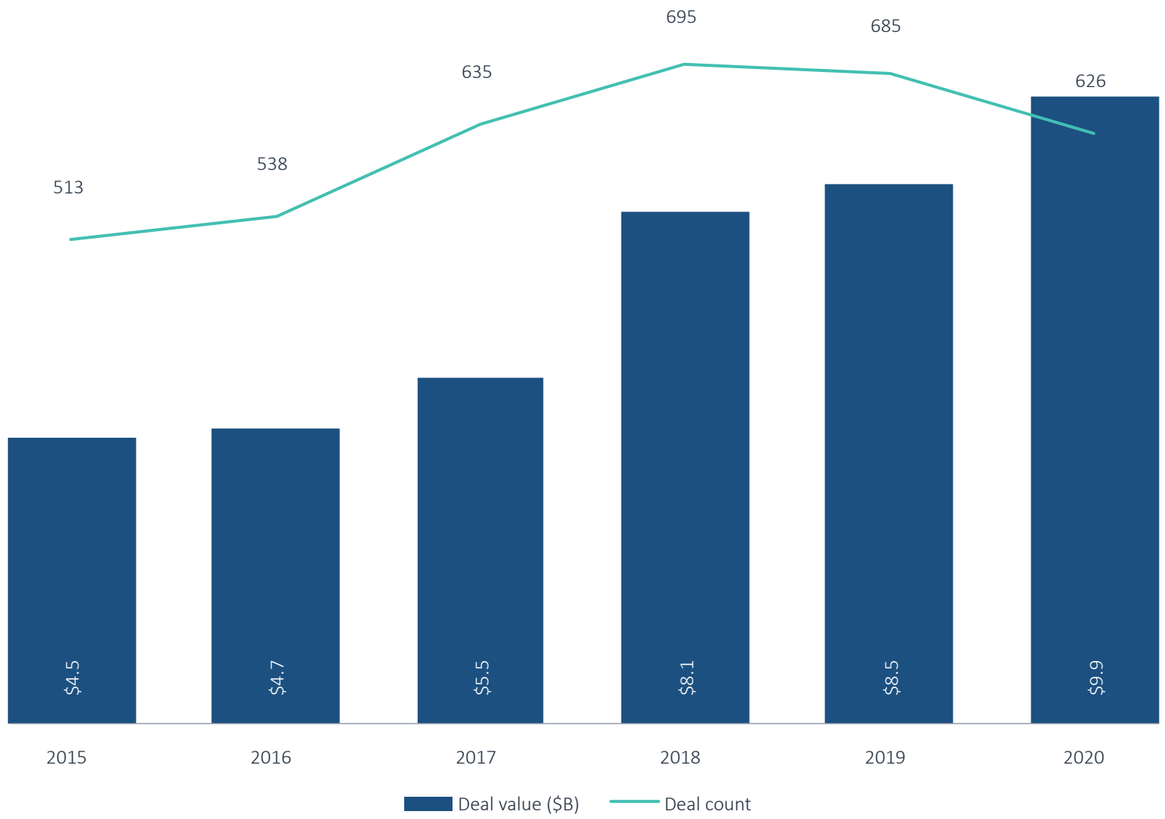
Investors:
Bessemer Venture Partners (Lead), Founders' Co-Op, K9 Ventures, NXTP Labs, Portland Seed Fund

SUPPLEMENTAL MATERIALS

Additional VC data

Figure 49.

Infosec VC deal activity



Source: PitchBook | Geography: North America & Europe

Figure 50.

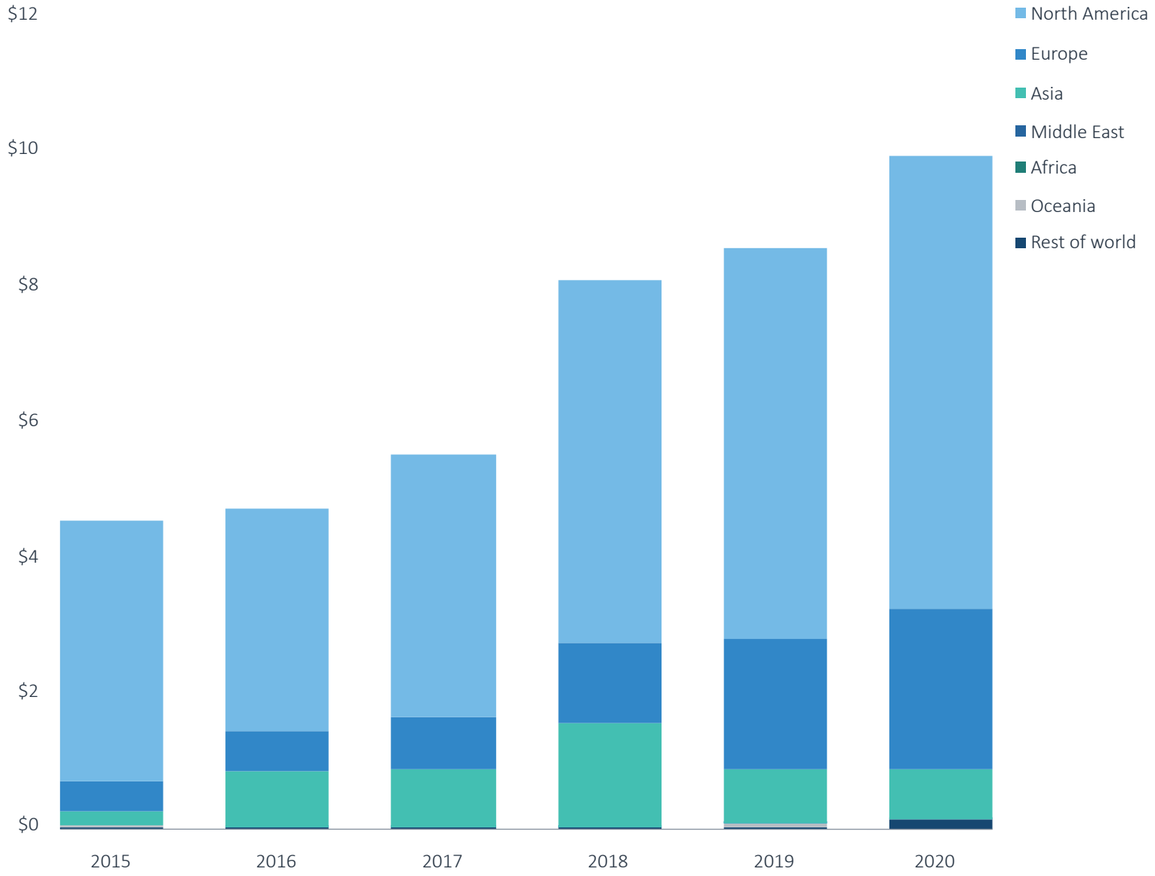
Notable infosec VC deals

COMPANY	CLOSE DATE	DEAL SIZE ($M)	POST-MONEY VALUATION ($M)*
Netskope	February 7, 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 | Geography: North America & Europe

Figure 51.

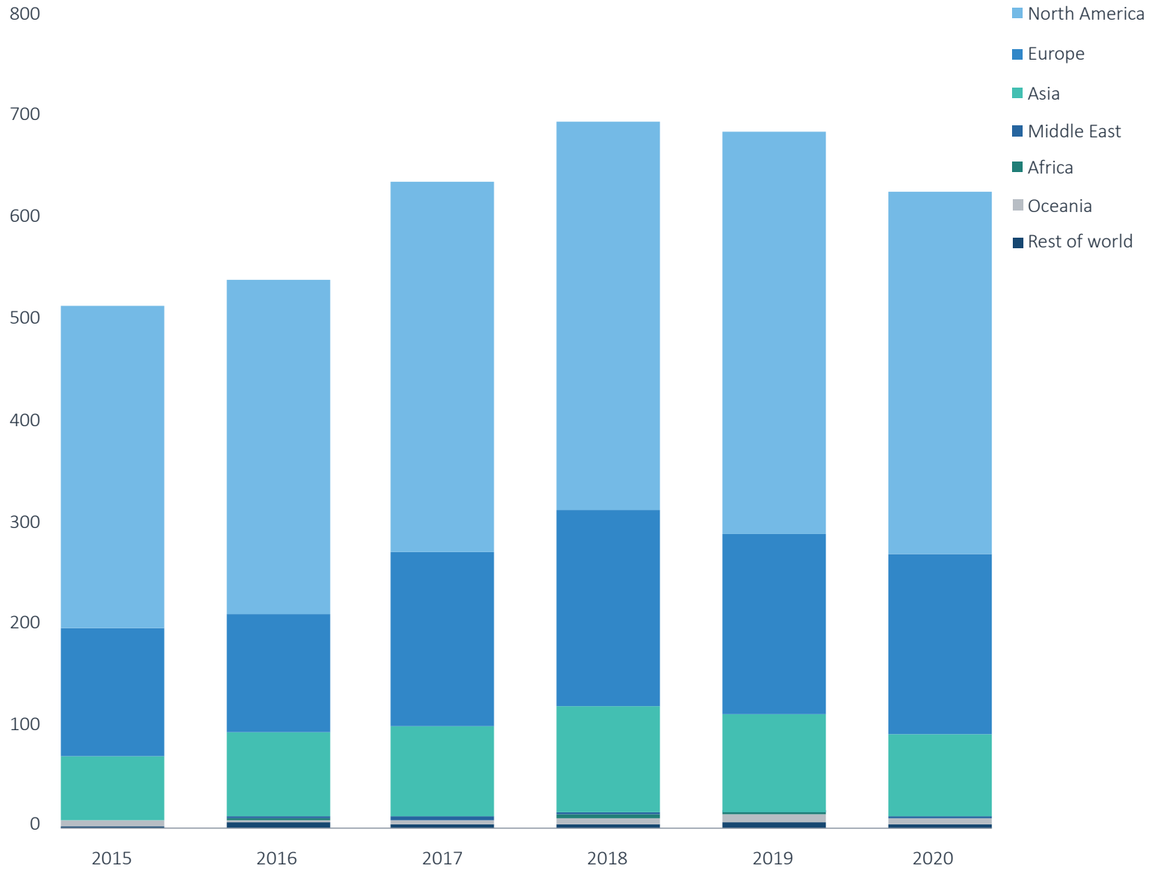
Infosec VC deals ($B) by region



Source: PitchBook | Geography: North America & Europe

Figure 52.

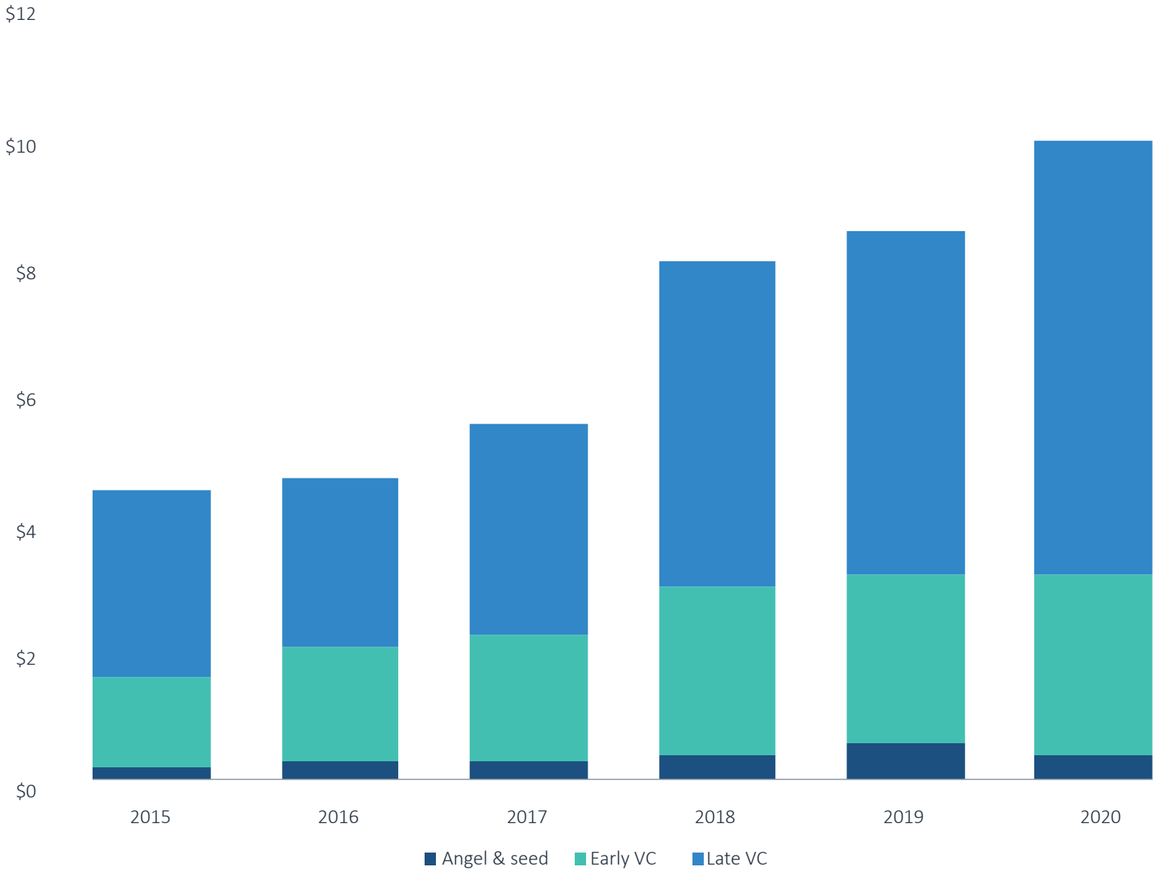
Infosec VC deals (#) by region



Source: PitchBook | Geography: North America & Europe

Figure 53.

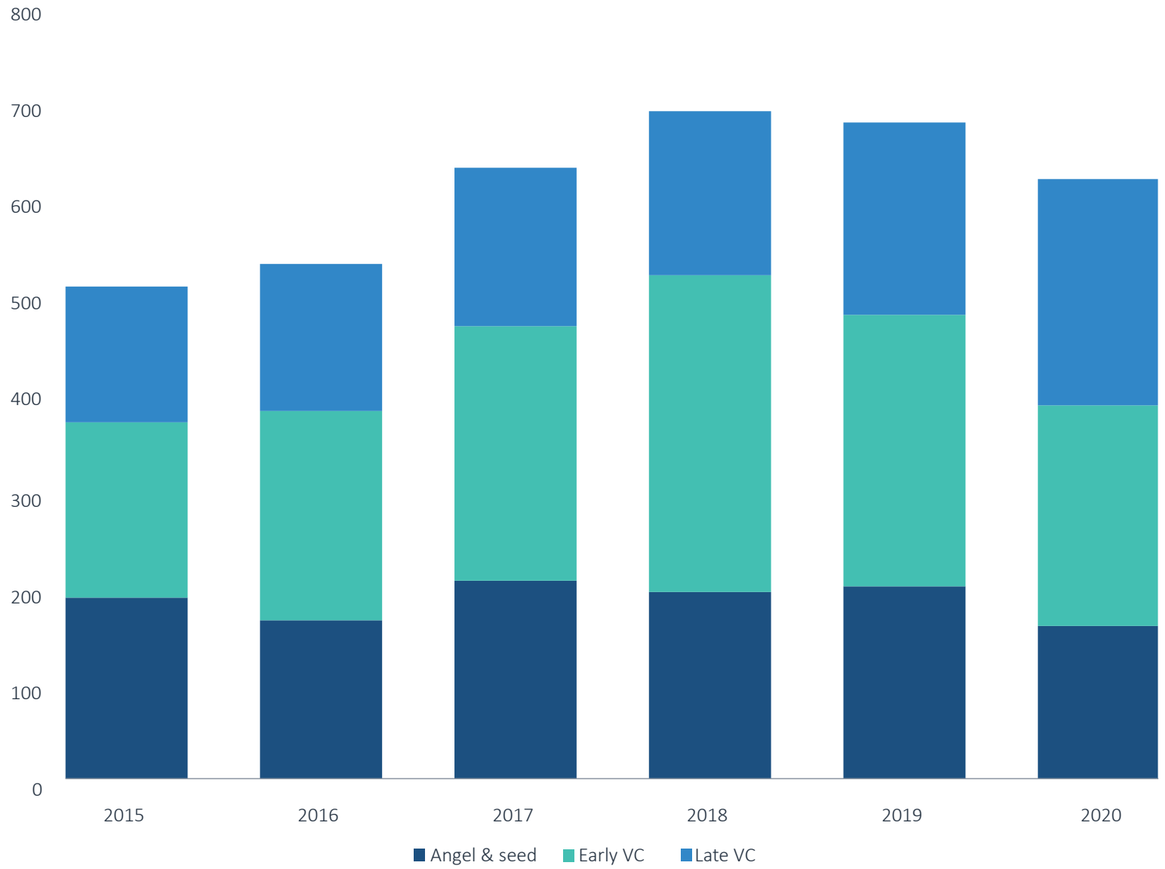
Infosec VC deals ($B) by stage



Source: PitchBook | Geography: North America & Europe

Figure 54.

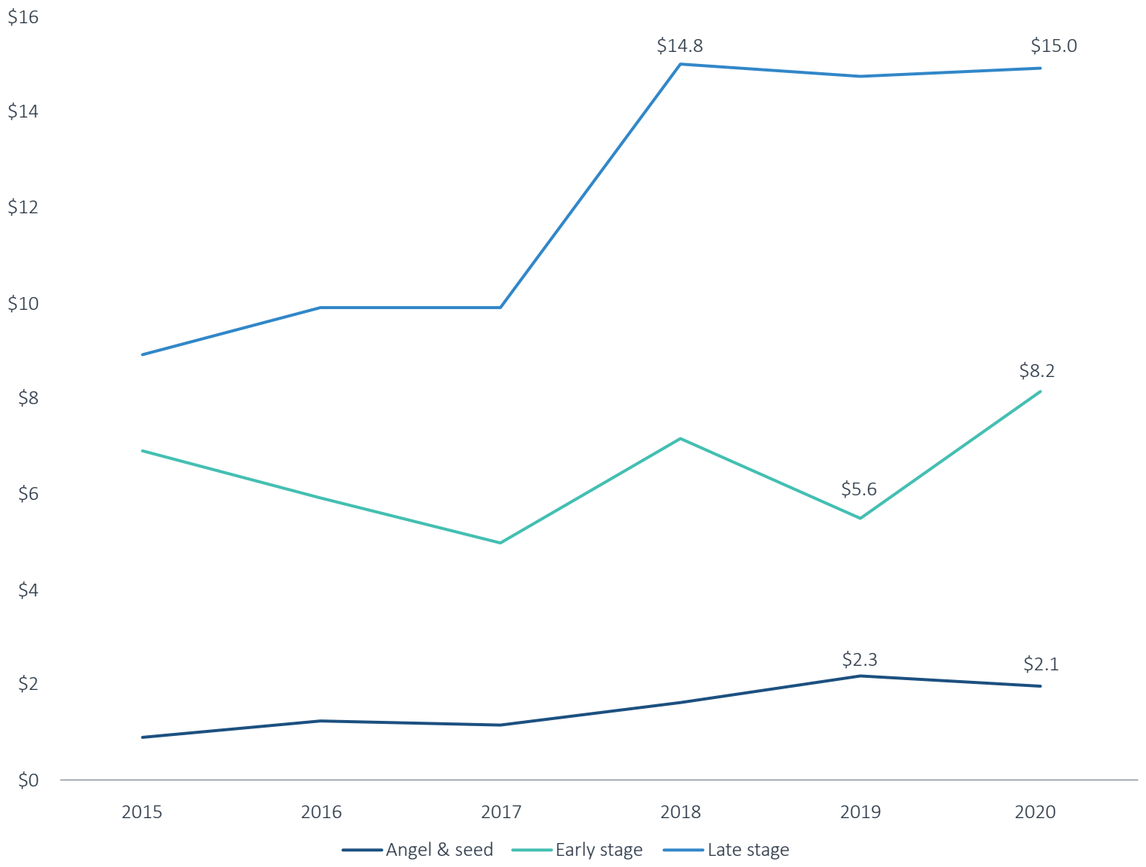
Infosec VC deals (#) by stage



Source: PitchBook | Geography: North America & Europe

Figure 55.

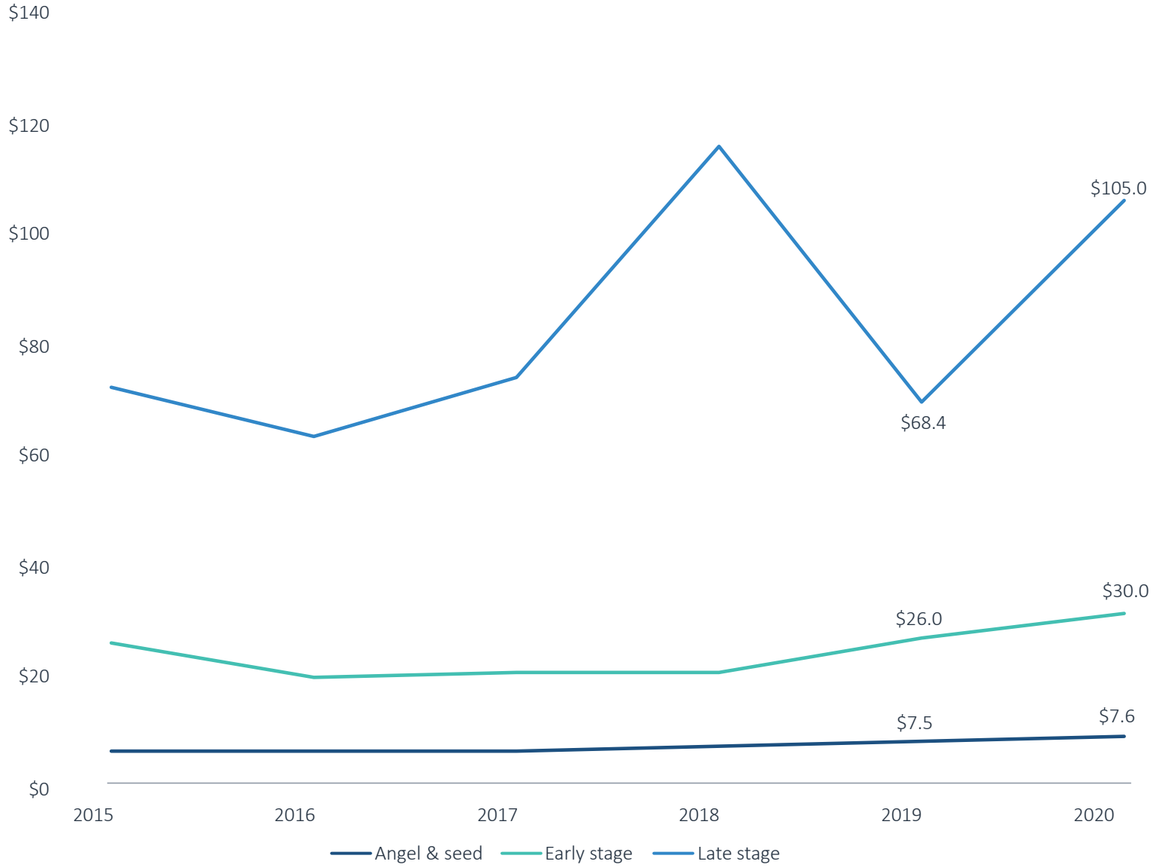
Median infosec VC deal size ($M) by stage



Source: PitchBook | Geography: North America & Europe

Figure 56.

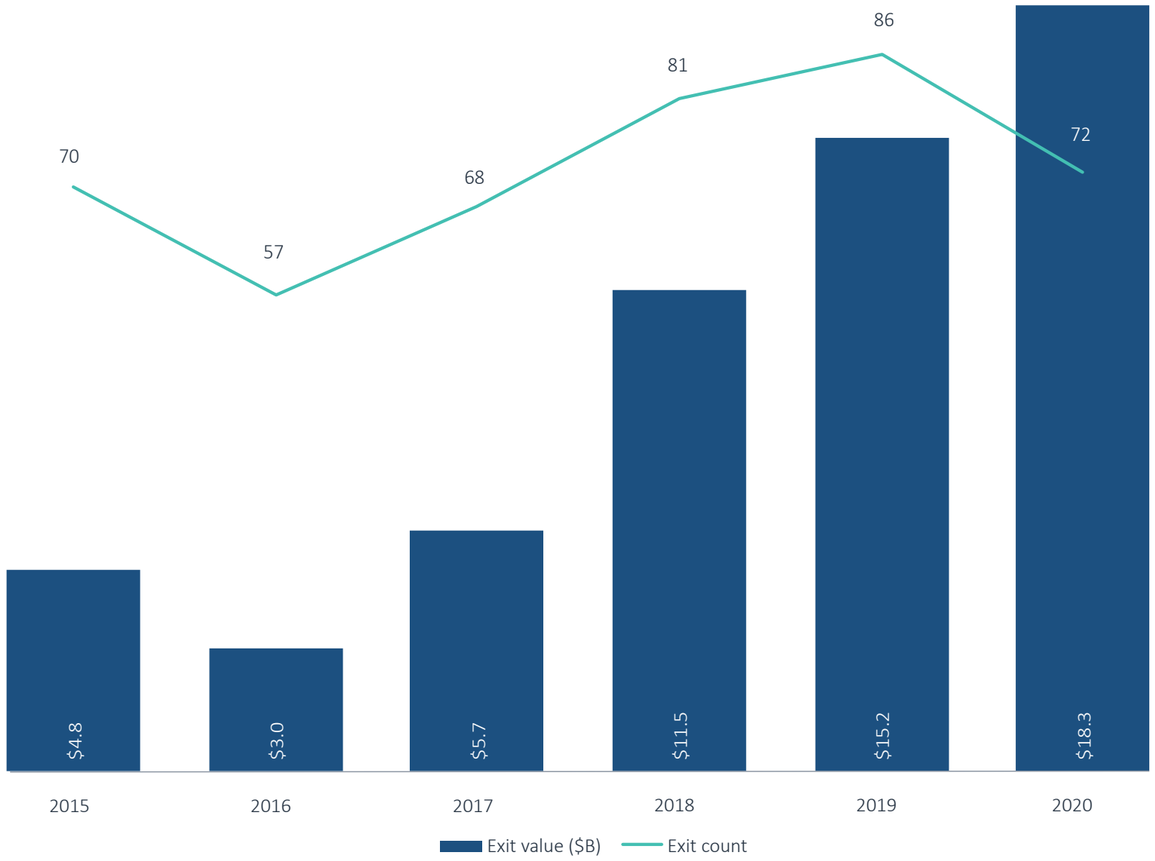
Median infosec VC pre-money valuation ($M) by stage



Source: PitchBook | Geography: North America & Europe

Figure 57.

Infosec VC exit activity



Source: PitchBook | Geography: North America & Europe

Figure 58.

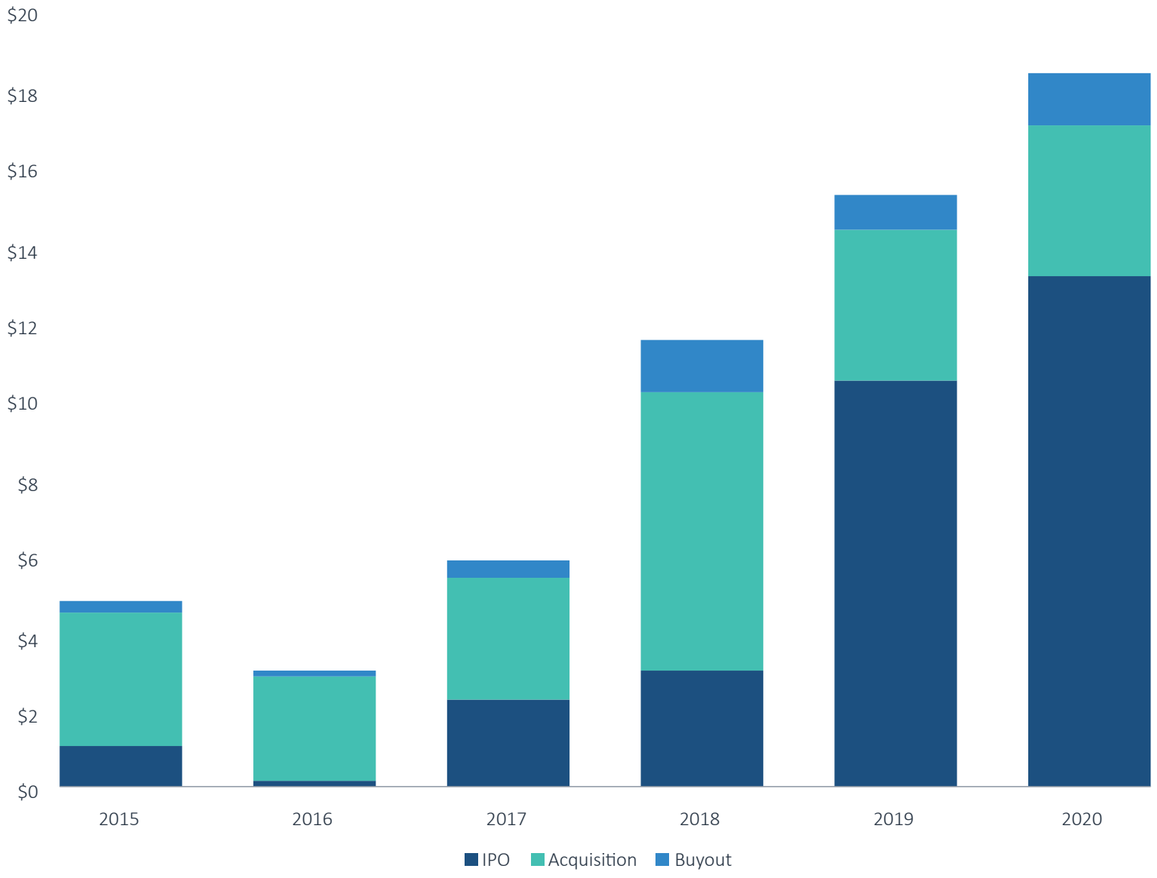
Notable infosec VC exits

COMPANY	CLOSE DATE	EXIT TYPE	EXIT SIZE ($M)
CrowdStrike	June 12, 2019	IPO	$6,075.4
Cloudflare	September 13, 2019	IPO	$3,875.2
JFrog	September 16, 2020	IPO	$3,549.7
Palo Alto Networks	July 20, 2012	IPO	$2,536.9
Duo Security	September 28, 2018	M&A	$2,350.0
FireEye	September 20, 2013	IPO	$2,045.9
Sumo Logic	September 17, 2020	IPO	$1,845.6
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

Source: PitchBook | Geography: North America & Europe

Figure 59.

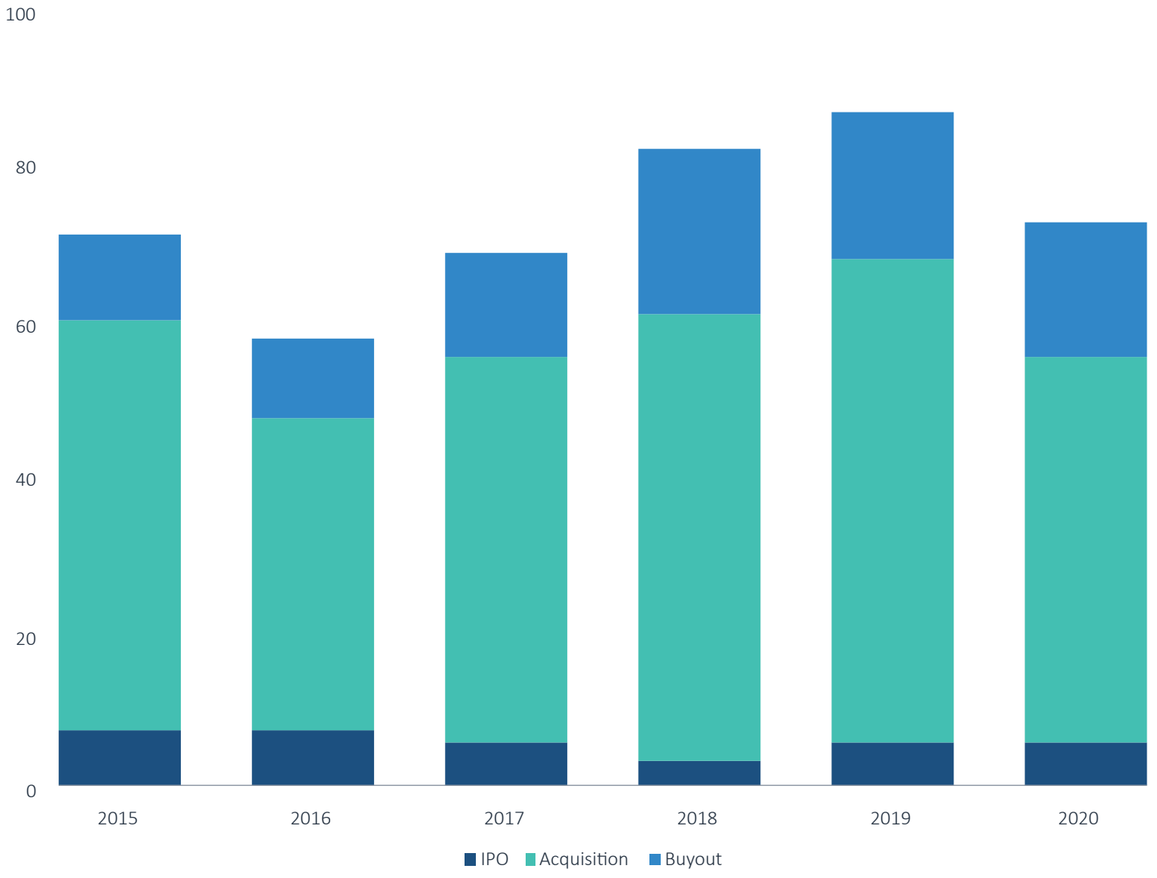
Infosec VC exits ($B) by type



Source: PitchBook | Geography: North America & Europe

Figure 60.

Infosec VC exits (#) by type



Source: PitchBook | Geography: North America & Europe

Figure 61.

Top VC investors in infosec by deal count since 2017*

INVESTOR NAME	DEAL COUNT
Accel	42
Bessemer Venture Partners	33
Dell Technologies Capital	30
ForgePoint Capital	30
Lightspeed Venture Partners	30
New Enterprise Associates	30
Paladin Capital Group	29
ClearSky	28
Intel Capital	27

Source: PitchBook | Geography: North America & Europe
*including VC firms and CVC investor type

Figure 62.

Top PE investors in infosec by deal count since 2017*

INVESTOR NAME	DEAL COUNT
Thoma Bravo	24
TA Associates Management	15
Insight Partners	13
Kohlberg Kravis Roberts	9
ABRY Partners	8
Pamplona Capital Management	8
H.I.G. Capital	8
Marlin Equity Partners	8

Source: PitchBook | Geography: North America & Europe
*including PE/Buyout, Growth/Expansion, Mezzanine Investor Type

Figure 63.

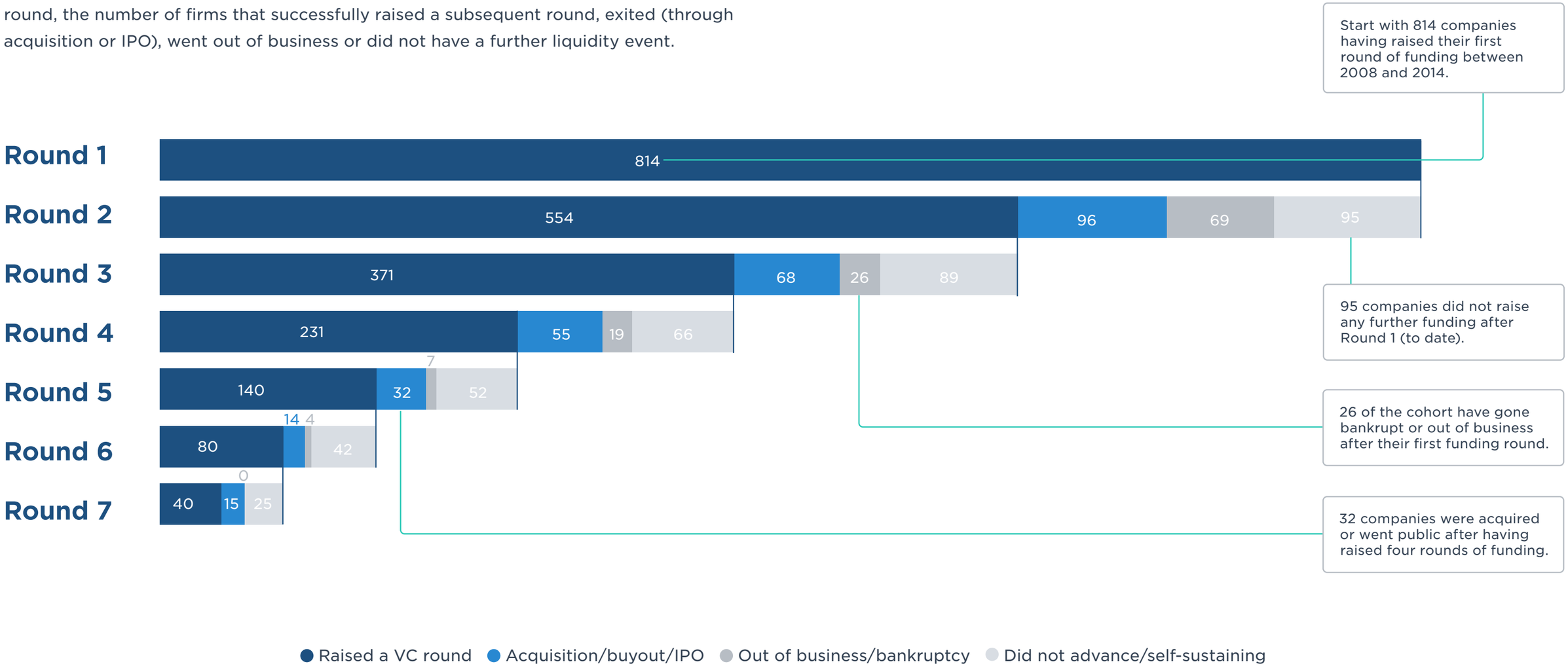
Top 10 VC-backed infosec companies by VC raised

COMPANY	SEGMENT	SUBSEGMENT	COUNTRY	TOTAL VC RAISED ($M)*
Tanium	Endpoint security	IoT/OT security	US	$837.6
Netskope	Network security	Cloud security	US	$744.3
OneTrust	Data security	Data privacy & compliance	UK	$710.0
SentinelOne	Endpoint security	Endpoint Protection, detection and response	US	$697.0
Snyk	Application security	DevOps security platforms	US	$454.5
StackPath	Application security	Cloud workload protection platforms	US	$396.0
Cybereason	Endpoint security	Endpoint protection, detection and response	US	$388.4
Lookout	Endpoint security	Endpoint protection, detection and eesponse	US	$380.7
Arctic Wolf	Security operations	Managed security services	US	$348.5
Auth0	Identity & access management	Access management	US	$333.5

Source: PitchBook | Geography: North America & Europe

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.



Buyers list

Figure 64.

Top strategic acquirers since 2016*

INVESTOR NAME	DEAL COUNT
Accenture	12
Palo Alto Networks	11
NortonLifeLock	9
Convergint Technologies	7
HelpSystems	7
j2 Global	7
Cisco Systems	7
Proofpoint	7
VMware	6
Fortinet	6

Source: PitchBook | Geography: North America & Europe
*including corporation, corporate development, PE-backed company, VC-backed company

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.

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.

Additional research

Agtech
Alex Frederick
alex.frederick@pitchbook.com

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