PitchBook

EMERGING TECH RESEARCH

Information Security Overview

Industry and taxonomy update with latest VC activity

2023

Published June 16, 2023

Contents

Institutional Research Group

Analysis

Brendan Burke Senior Analyst, Emerging Technology
brendan.burke@pitchbook.com
pbinstitutionalresearch@pitchbook.com

Data

Matthew Nacionales Data Analyst

Publishing

Report designed by **Megan Woodard**, **Julia Midkiff**, and **Joey Schaffer**

Published on June 16, 2023

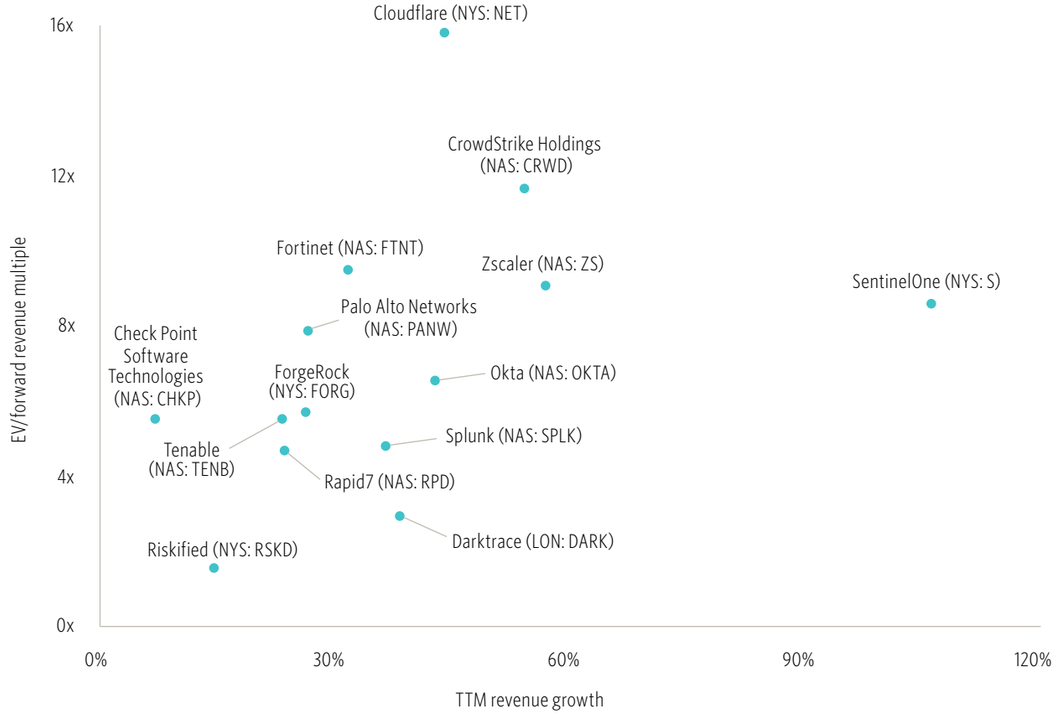
For previous updates as well as our complete information security research, please see the designated analyst workspace on the PitchBook platform.

Vertical overview

Information security (infosec) companies remain high growing and highly valued relative to other IT companies. Of the 42 public pure-play infosec companies we track, 22 recorded over 20% revenue growth in the most recent trailing 12-month (TTM) period. Expectations for these companies remain heightened, with 14 companies sitting above the median EV/forward revenue multiple of the Bessemer Venture Partners NASDAQ Emerging Cloud Index, as of May 31, 2023. Cloudflare and CrowdStrike both sit above 10x, demonstrating their trajectory toward creating iconic companies in separate segments of infosec. Cloudflare's rapid pace of innovation and profitability contribute to the highest multiple valuation among cloud stocks, showing the value of emerging themes such as zero-trust network access.

Startup innovation remains encouraged by inquisitive acquirers and expanding problem spaces. Chief information security officers (CISOs) have little clarity on the leading threats facing their organizations. In a survey by Proofpoint, 1,600 CISOs were asked for the biggest threats they face across attack types. Eight attack types received between 26% and 33% of votes, including email fraud, insider threats, cloud breaches, distributed denial of service, supply chain attacks, ransomware, and malware.[1] This dispersion encourages CISOs to spread their efforts broadly across organizational culture and hygiene. Similarly, infosec incubator Team8 identifies eight themes driving CISO activity from their network of 350 executives, including cloud, resilience, operations, internet of things (IoT), identity & access management data, application security, and training, to paraphrase.[2] Infosec organizations remain complex in their priorities, with no technical panaceas presenting themselves. This tension encourages incumbents to pursue M&A across segments.

Key pure-play infosec incumbents' financial performance by forward revenue multiple and trailing revenue growth*



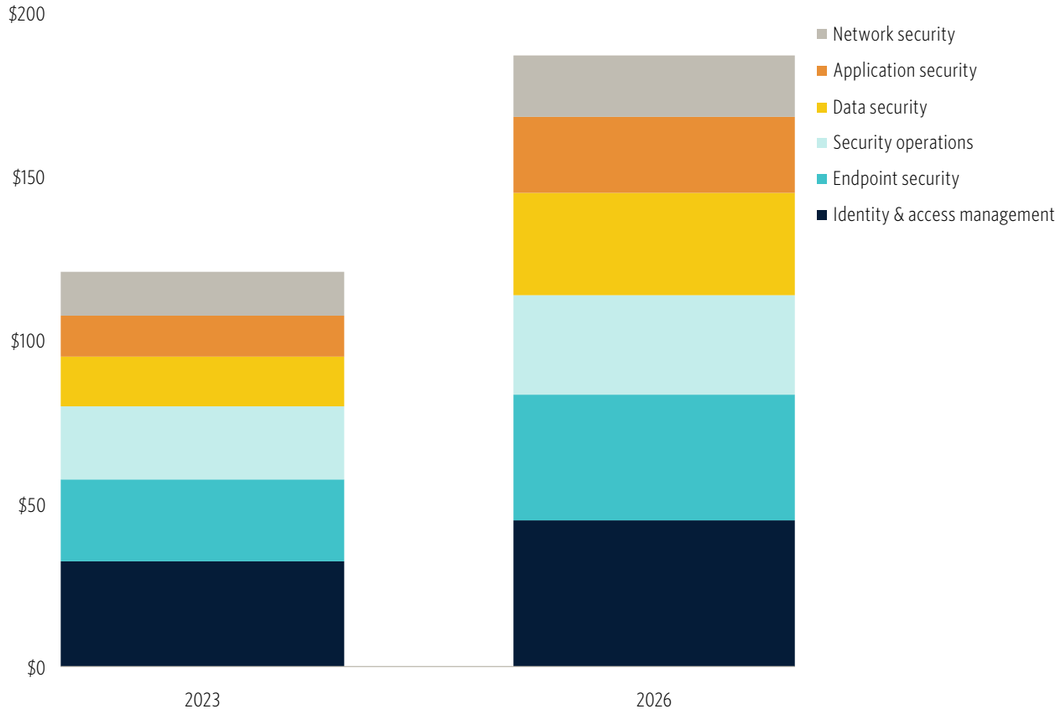
Source: PitchBook • Geography: North America & Europe • *As of May 31, 2023

1: "Voice of the CISO 2023," Proofpoint, May 9, 2023.
2: "Announcing Team8's 2023 Cyber Themes," Team8, Aaron Dubin, February 22, 2023.

Nation-state activities promise to roil the infosec waters further in years ahead. An increasingly polarized world portends escalating cross-border attacks, digital espionage, and misinformation campaigns aimed at destabilizing rival nations. These attacks make critical infrastructure a primary target of cyberattacks. The Russian-Ukraine war yielded targeted attacks on US critical infrastructure from state-backed entities, and recent threat research finds similar initiatives from China-based threat groups. In 2022, according to Microsoft threat research, critical infrastructure received 40% of nation-state cyberattacks, up from 20% in 2021.[3] Governmental focus on cybersecurity is likely to persist between political administrations given the military urgency of fortification. This focus yields standards and regulations that can have a transformative impact on the industry.

In this context, infosec spending is likely to rise robustly in any economic environment. In Morgan Stanley Research's Q4 2022 Chief Information Survey, 19.0% of executives marked security software as least likely to reduce spending in 2023—up from 15.0% in Q3—while no executives reported that it was most likely to receive cuts.[4] No other category received more than 10.3% of responses, including cloud computing, data analytics, and artificial intelligence & machine learning (AI & ML). An IDC survey also confirms that security is the category most immune to budget reduction in IT departments. We estimate the serviceable addressable market for infosec startups will reach $126.7 billion in 2023, led by endpoint security and identity & access management (IAM). This market size estimate includes startup-relevant software categories within the vertical's broader $219.6 billion market. Industry revenue growth is on pace to be up year-over-year, reaching 15.8% growth for software spending. We forecast a 14.5% CAGR out to 2026, and this growth is estimated to result in a 14.5% CAGR out to 2026, and this growth is estimated to result in a $190.3 billion market.

Infosec software market size estimate ($B)*



Source: PitchBook • Geography: Global • *As of May 31, 2023

3: "Microsoft Digital Defense Report 2022," Microsoft Security, Tom Burt, November 4, 2022.
4: "US Tech: 4Q22 CIO Survey," AlphaWise and Morgan Stanley Research, January 11, 2023.

Information security landscape

Threat surfaces

1. Cloud-based web applications & services
2. Corporate-owned endpoints
3. On-premise network
4. On-premise databases
5. On-premise data center servers
6. Employee-owned endpoints
7. Cloud-based databases
8. IoT devices/sensors
9. Industrial control systems

Product segments

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

Information security VC ecosystem market map

Click to view the 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.

Application security

Cloud workload protection platforms

STACKPATH, aqua, varmour, Uptycs, ionir, ISOVALENT, weaveworks, TIGERA, Rezilion, Kubescape

DevOps security platforms

snyk, Contrast, VERACODE, MEND, SECURE CODE WARRIOR, BIONIC, cycode, AKEYLESS, GitGuardian, qwiet AI

Web application protection

SALT, imperva, CHEQ, noname, HUMAN, perimeter 81, virsec, ONAPSIS, CORO, ActiveFence

Web3 security

Fireblocks, LEDGER, Chainalysis, CERTIK, Aleo, polysign, Quantstamp, Hedera, HALBORN, Shyft

Security operations

Log ingestion & SIEM

securonix, BigPanda, exabeam, logz.io, panther, HUNTERS, EclecticIQ, cynet, Stairwell

Managed security services

ARCTIC WOLF, PENTERA, Coalition, BlueVoyant, deepwatch, expel, CIRCADENCE, BISHOPFOX, AUTOMOX, envelop

Security risk assessment & management

SecurityScorecard, Vanta, Synack, interos, Comply Advantage, cowbell, BITSIGHT, IMMERSIVELABS, hackerone, Kiteworks

Security orchestration, automation & response

SWIMLANE, tines, ACALVIO, torq, CYWARE, revelstoke, seemplicity, CARDINALOPS, cloudcover, Push

Data security

Data privacy & compliance

onetrust, DRATA, semperis, BigID, veza, securiti, EGNYTE, TrustArc, VERY GOOD SECURITY, DATAGRAIL

Data protection & encryption

rubrik, Acronis, COHESITY, Own{backup}, druva, SCALITY, PRIVITAR, {tokenex}, code42, virtru

Database monitoring & loss prevention

DIGITAL GUARDIAN, IMMUTA, VERA, Nightfall, JSONAR, sertainty, CybelAngel, CYBERHAVEN, egress, Cyral

Identity & access management

Access management

jumpcloud, BetterCloud, OBSIDIAN, plainID, Cyolo, strongdm, britive, prismo, ClearSkye, clerk

Fraud prevention

ĀURA, Socure, FORTER, Trulioo, Signifyd, quantexa, feedzai, onfido, incode, Pindrop

Identity governance & administration

transmit, ID.me, SAVIYNT, Prove, BioCatch, BEYOND IDENTITY, veriff, DASHLANE, HYPR

Information security VC ecosystem market map

Click to view the interactive market map on the PitchBook Platform.

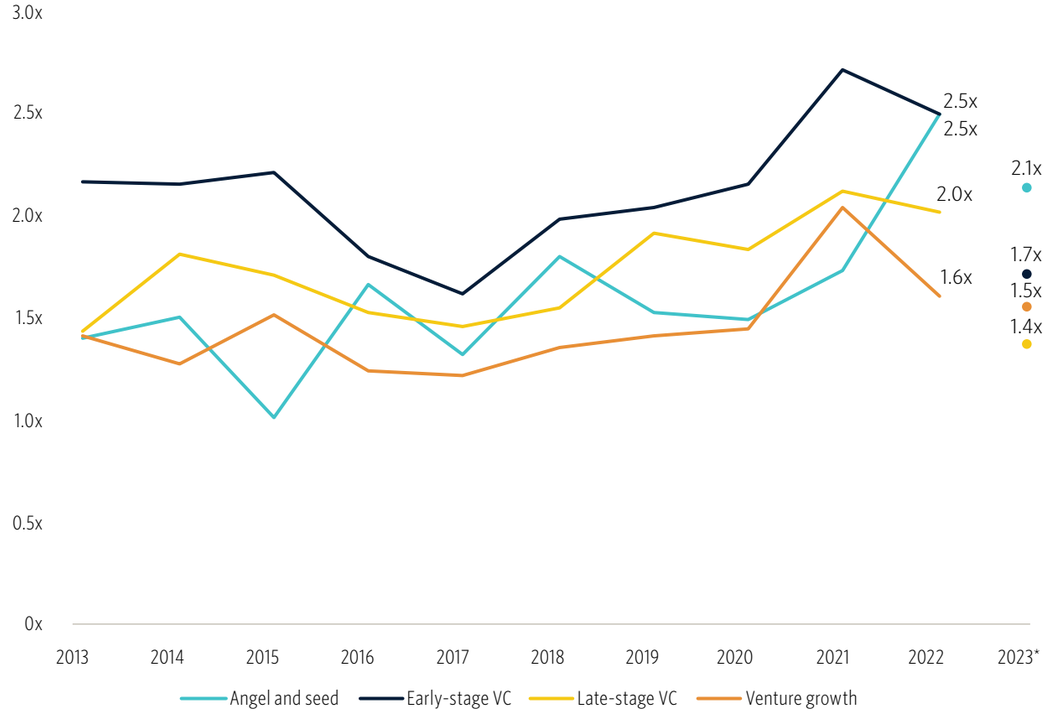
Market map is a representative overview of venture-backed or growth-stage providers in each segment. Companies listed have received venture capital or other notable private investments.

VC activity

Infosec VC funding in North America and Europe has remained consistently low since the market downturn in Q3 2022, reaching $2.5 billion across 127 deals in Q1 2023—nearly the same level as in Q3 and Q4 2022. Late-stage VC deal count exceeded both angel and seed and early-stage deal count yet again, demonstrating a concerning trend for early-stage startups. Deal volume fell too low to gain any reliable insights on valuations, yet only five VC megadeals closed, indicating that unicorns remain constrained in funding outside of venture debt. Leading specialist VC investors remained active in leading early-stage deals yet focused on seed and Series B investments, suggesting a preference for lower valuations. Wiz raised the outstanding round of the quarter, achieving a $10.0 billion pre-money valuation with a $300.0 million Series D. This deal surpasses Tanium for the highest VC valuation we have tracked in infosec, also surpassing Lacework's $8.3 billion valuation. Wiz has shown that outliers in revenue growth rates can be created in cloud security with excellent founding teams.

Disclosed exit value continued to dry up in Q1 2023, yet significant acquisitions continued. Data security posture management (DSPM) is a leading innovation theme for infosec startups—as covered in our Q1 2023 Infosec Report and RSA conference analyst note—given the ability of startups to combine cloud database scanning, access management, and data theft detection. This acquisition offers an outstanding 7.1x multiple on invested capital for seed investors in Polar Security, demonstrating the lack of cloud data controls in existing data security product portfolios. Media outlet Calcalist reported that DSPM startup Laminar is also receiving outsized acquisition offers from infosec leaders, including Datadog and Rubrik, showing that the niche will be a leading driver of M&A activity in the near term.[5] A low volume of deals suggests that consolidation is still in a holding pattern yet will likely follow on as a result of diminishing VC deal flow.

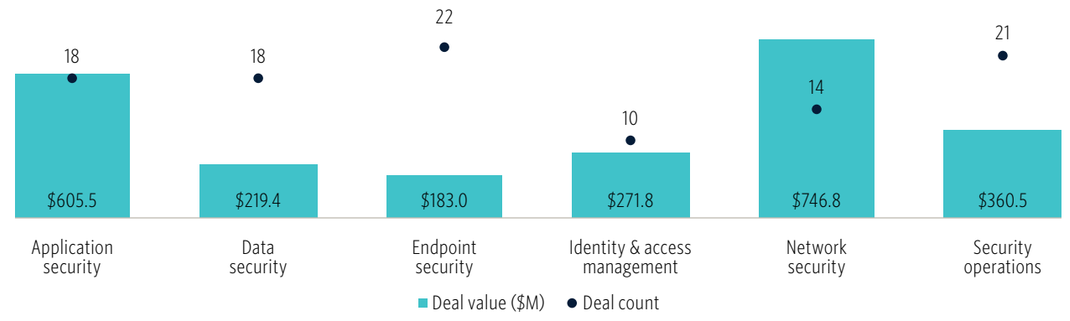
Median infosec VC pre-money valuation step-up by stage



Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

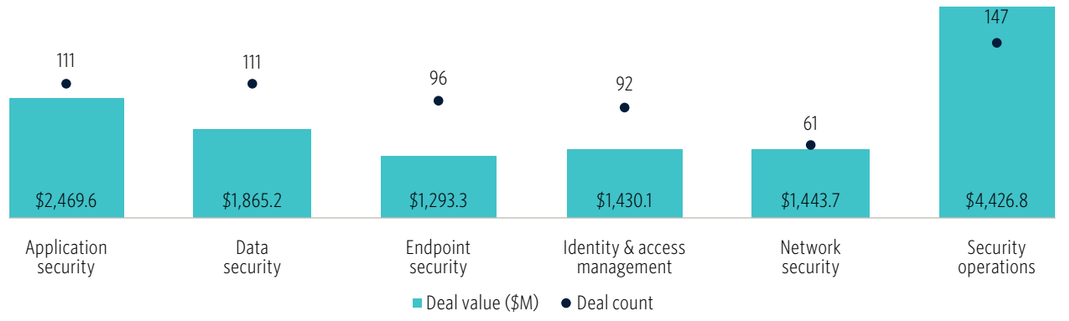
5: "Cloud Security Startup Laminar Set to Be Acquired for $200-250 Million," CTech by Calcalist, Meir Orbach, May 11, 2023.

Q1 2023 infosec VC deal activity by segment*



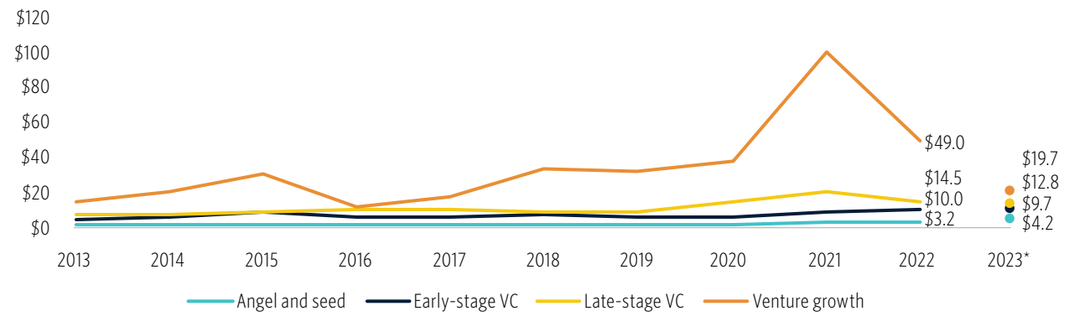
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

TTM infosec VC deal activity by segment*



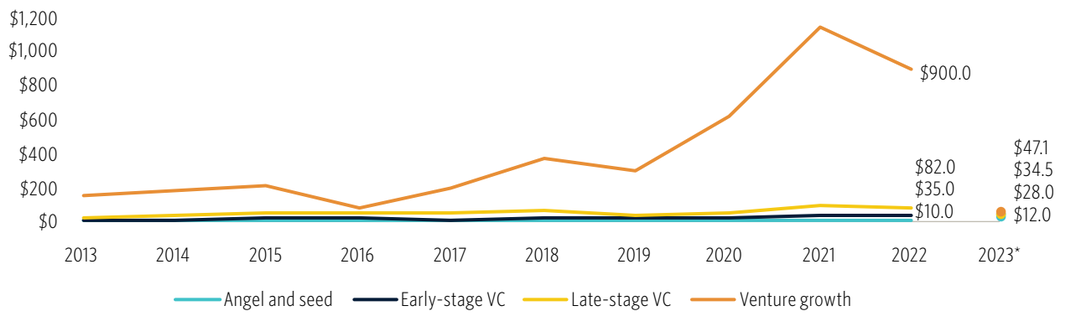
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Median infosec VC deal value ($M) by stage



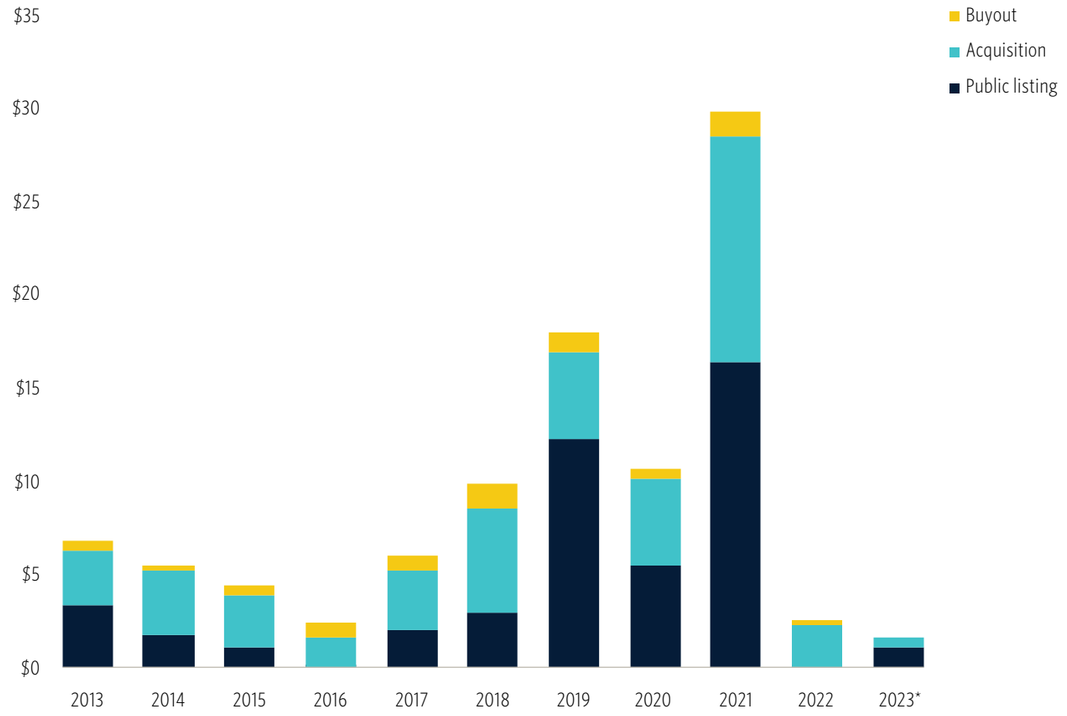
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

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



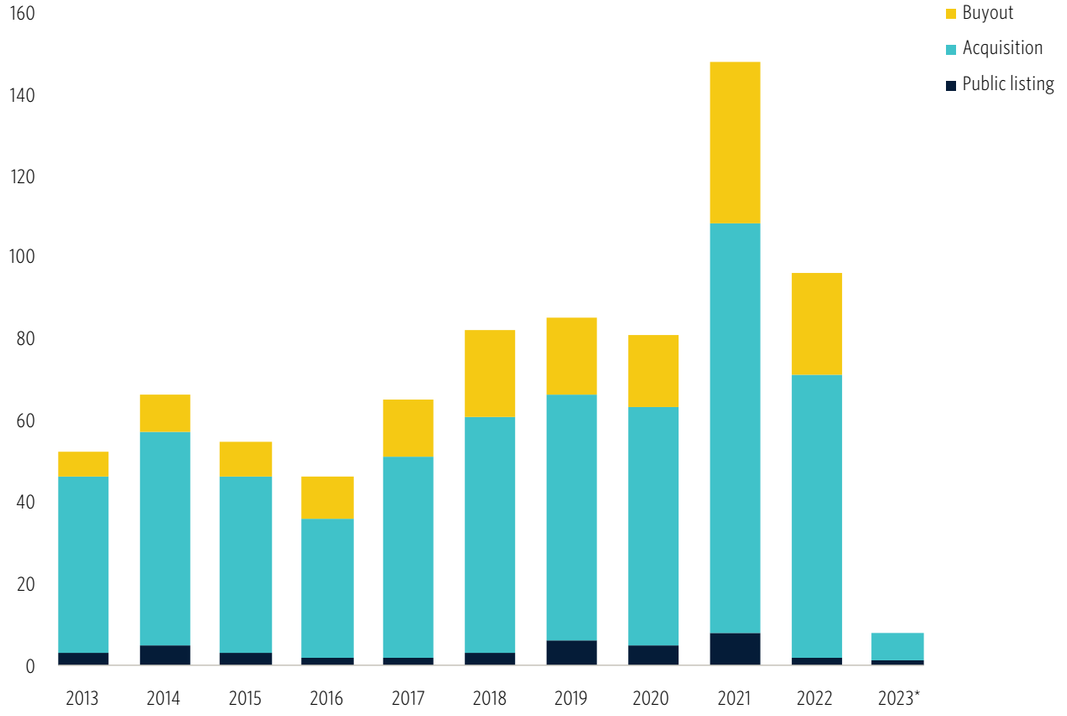
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Infosec VC exit value ($B) by type



Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Infosec VC exit count by type



Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Key Q1 2023 infosec VC exits by exit value ($M)*

Company	Close date (2023)	Exit size ($M)	Exit type	Subsegment	HQ location
HUB Security	January 1	$1,054.0	Reverse merger	Data protection & encryption	Tel Aviv, Israel
Axis Security	March 2	$500.0	M&A	Secure networking	Plano, US
Minerva Labs	March 15	$38.0	M&A	Endpoint protection, detection & response	Petah Tikva, Israel
Trustpage	January 19	N/A	M&A	Security risk assessment & management	Royal Oak, US
Confluera	March 22	N/A	M&A	Endpoint protection, detection & response	Palo Alto, US
Baffin Bay Networks	March 20	N/A	M&A	Network detection & response	Stockholm, Sweden
Foxpass	March 20	N/A	M&A	Secure networking	San Francisco, US
Anlyz	February 15	N/A	M&A	SOAR	Lewes, US

Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Segment overview

Application security

Open-source adoption shows a path to market for startups.

Data security

Data security posture management offers a near-term opportunity before post-quantum and AI markets develop.

Endpoint security

The email security market remains ripe for disruption.

Identity & access management

The passwordless authentication market is starting to mature and benefit from new standards development.

Network security

Cloud security drives the highest valuations in infosec.

Security operations

Managed detection & response can yield growth at scale.

Application security

Overview

Application security encompasses 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. This market addresses the increasing focus on software supply chains, resulting from prominent ransomware attacks and open-source vulnerabilities.

Traditionally, infosec vendors have not addressed this opportunity, instead focusing on network traffic and endpoint operating systems. With cloud-native applications disrupting this infrastructure, a separate class of vendors has been trusted to protect applications deployed in the cloud, on the web, or on premises. As a result, this category has only existed for 10 to 15 years. Application security testing (AST) is served by a range of private companies, including Sonatype, Mend, and Veracode. Market leader Synopsys is not primarily a security vendor yet has become a leader in AST via M&A. Open-source scanning has emerged as a critical capability for these platforms over the past five years. Incumbents such as Palo Alto Networks, Cisco, and Rapid7 have made moves into application security over the past two years with the intent to unify security policies across the developer lifecycle. Additional capabilities are needed to protect high-value programs, including AI models and cryptocurrency blockchains.

Application security subsegments include:

- **Development operations (DevOps) security platforms:** Software tools that enable developers to embed security protections within their code, test their code's vulnerabilities on a regular basis, create a software bill of materials (SBOM), and securely deploy application updates.
- **Cloud workload protection platforms:** An emerging niche that includes security protections for cloud-based applications and containers that increasingly house cloud-native applications in production.
- **Web application protection platforms:** Platforms that detect threats targeted at web-based applications. Examples include web application firewalls (WAFs), machine learning security (MLSec), bot defense, and application penetration testing technologies.
- **Web3 security:** An emerging network paradigm that requires specialized identity management, asset custody, encryption, and malware detection software to protect a networking system that is centered on cryptocurrency tokens and blockchains, and that leverages decentralized finance (DeFi) to exchange value.

Industry drivers

- **Cloud-native application development:** Increasingly, cloud-based infrastructure has been used for application development and deployment as well as for expansion of container technologies in cloud environments. Container adoption is rising rapidly, with one survey indicating that 45% of databases and data services run on container service Kubernetes.[6] Container security has become a leading concern for IT departments as a result.

- **Open-source project adoption:** Security products are adopted by developers via open-source repositories and have been growing rapidly as security sophistication rises, rewarding product-led growth for application security vendors.

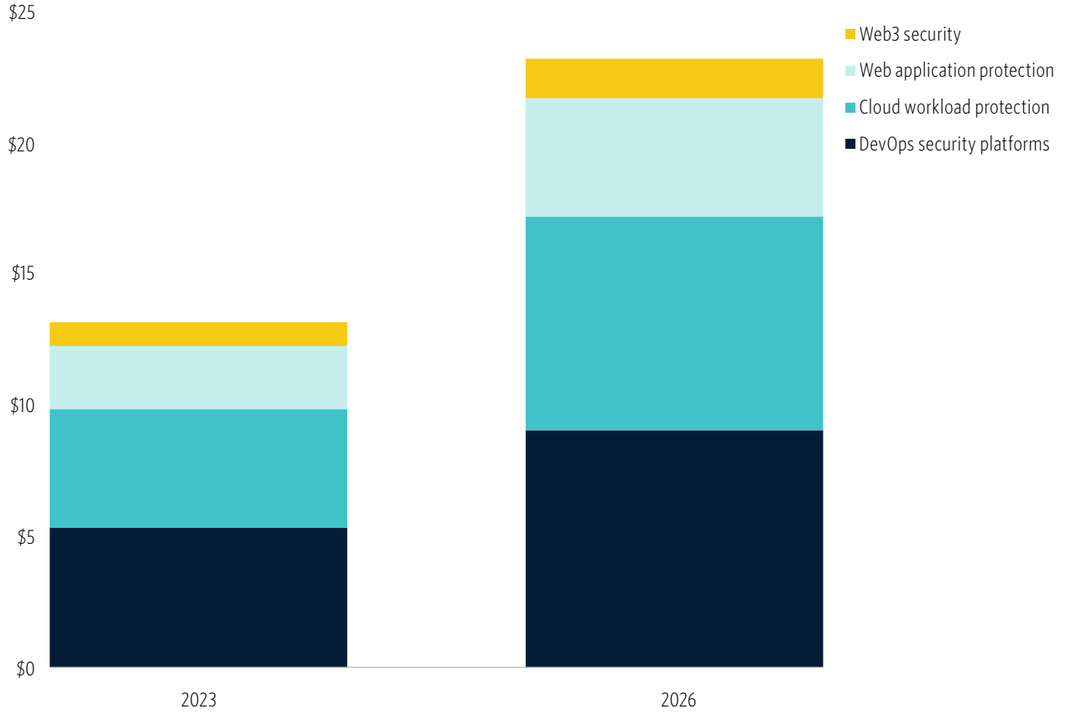
- **Web application data breaches:** Security research indicates that web application data breaches constitute around 70% of a sample of hacking action vectors, suggesting that they are far more likely to be breached than network backdoors, virtual private networks (VPNs), or third-party portals.[7]

Market size

High growth in the relatively immature niche of application security is estimated to yield an $13.1 billion market in 2023. By 2026, the market is estimated to reach $23.2 billion at a 20.8% CAGR. We believe that an increased focus from DevOps practitioners on secure coding has shifted the market up an S-curve in adoption and improved its outlook. Cloud workload protection has grown into a standalone $4.6 billion market with a high-growth forecast due to the necessity of protecting containers and serverless applications.

6: "2022 Container Adoption Survey," Portworx, 2022.
7: "2021 Data Breach Investigations Report," Verizon, 2021.

Application security market size estimate ($B)*



Source: PitchBook • Geography: Global • *As of May 18, 2023

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, Snyk charges around $3,100 annually per five users for its base bundle of software composition analysis and static application security testing. Container scanning and infrastructure-as-code policy integration, and cloud monitoring can be upsold to nearly triple the cost per user. DevOps security platforms' runtime-based solutions can use consumption-based pricing in conjunction with cloud providers. Aqua Security has pioneered this business model and offers strong upsell opportunities as the number of applications in production increases.

Opportunities

Cloud-native application protection platforms

Enterprise infrastructure is increasingly housed in cloud-native applications built by developers and hosted in public clouds. As a result, enterprise vulnerabilities increasingly stem from cloud assets and require novel solutions to detect and respond to cloud application threats. CNAPP is a term coined by Gartner to signify the consolidation of multiple cloud security point solutions including cloud workload protection, cloud security posture management (CSPM), cloud infrastructure entitlement management, and application security testing. This suite of tools is positioned as a successor to cloud access security broker (CASB), a category that provided guardrails for transmission of data to software-as-a-service (SaaS) applications.

Demand for consolidated cloud security solutions is driving rapid consolidation among application security testing, cloud workload protection, and CSPM. Vendors with cloud security platforms are acknowledging the limitations of their platforms to detect software supply chain vulnerabilities and are expanding into code testing. Check Point, Cisco, and Palo Alto Networks previously made acquisitions of cloud application testing startups including Bridgecrew, Cider Security, Portshift, and Spectral. All earned high premiums over their prior private valuations. These outsized valuations, along with rapidly accelerating exit counts, show the strategic value of a developer focus for cloud security.

Startups are beginning to scale with integrated platforms for application security orchestration, as much as endpoint detection & response (EDR) companies have done for malware analysis. In Q1 2022, Bionic raised a $65.0 million Series B led by prolific infosec investor Insight Partners. The company has developed a graphical user interface for tracking application dependencies and codebase vulnerabilities for applications in production. Because the software pulls insights from the application logic, the platform can scale alongside cloud vulnerability scanners. The company was founded by two former entrepreneurs-in-residence at YL Ventures, a leading infosec investor, demonstrating the investment opportunity in this category.

Cloud workload protection

Startups are driving open-source detection for Kubernetes monitoring via the extended Berkeley Packet Filter (eBPF) project. eBPF enables container monitoring without installing sensors within the kernel or root of the application. This monitoring occurs via a sandboxed application within Linux kernels that can run without editing. The technology offers the benefits of an agent without

needing to install a third-party solution, granting an unfair advantage to security companies leveraging them. The project is supported by Google and Microsoft, enabling compatibility with their cloud containers. Popularity of eBPF-based security projects has grown rapidly over the past two years, with new applications emerging from startup Isovalent's open-source project called Cilium. The space is led by Cilium and highly funded startups Aqua Security and Tigera.

Isovalent is achieving rapid growth and scale seen by open-source commercializers in other industries. The company was founded by the developers of the Cilium library at the heart of the eBPF project. It offers enterprise support for Cilium's service mesh, observability, runtime security, and networking services—a business model that has yielded outstanding results for open-source outliers such as Apache Spark (Databricks) and Kafka (Confluent). In Q3 2022, the company achieved an outstanding 3.0x valuation step-up in its Series B, resulting in a $280.0 million post-money valuation. In April 2023, the company launched its enterprise product in Microsoft Azure's marketplace, demonstrating the affinity between Microsoft and eBPF.

Software bill of materials

An SBOM offers an inventory of software components in an application for customers and future developers. The US National Telecommunications and Information Administration defines SBOM as "formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships."[8] The machine-readable aspect of this definition implies that software components must carry extensible metadata across different sources, enabling analysis by a variety of software programs and stakeholders. Several tools that we believe are core to formulating and translating these SBOMs include software composition analysis, application security testing, artifact repositories, and runtime application self-protection. Core open-source solutions include the Linux Foundation's SPDX, OWASP's CycloneDX, and NIST's Software Identification (SWID) Tags. Commercial solutions build on top of these frameworks to automate SBOM generation.

While the pace of DevOps security funding is down overall, early-stage activity is driving startups to secure the software supply chain. In Q2 2022, standout startup Chainguard raised a $50.0 million Series A at a 10.0x valuation step-up over its seed round. Sequoia Capital led the party round that included a raft of prominent angel investors—including the Chainsmokers—along with VCs. The founders come from the open-source community, particularly the Sigstore project for code signing. This project is part of the Open Source Security Foundation and has grown rapidly in contributors since launching at the end of 2020. At the seed stage, First Round Capital led a $4.5 million seed round for SBOM startup Manifest on the back of two new government contracts. SBOM startup Cybeats listed on the Canadian Stock Exchange, offering direct exposure to an early-stage company in this space.

8: "NTIA Multistakeholder Process on Software Component Transparency," NTIA, April 27, 2021.

Risks and considerations

Smaller market size than endpoint protection: 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. Application security leader Snyk initially addressed all developers yet found the small- and medium-sized business (SMB) segment costly to service and pivoted to the enterprise segment to gain marketing efficiency. This segment has not yet produced a $1 billion exit, demonstrating limited financial expectations for companies in this space.

Cloud security providers and content delivery network vendors may offer competing products to startups: Application security vendors appearing in Gartner's magic quadrant for web application and application programming interface (API) protection include Akamai, Cloudflare, Amazon Web Services (AWS), Fastly, F5 Networks, and Microsoft. Customers can use native application security tools from each of these vendors for applications running in their environments. AWS and Microsoft offer sophisticated cloud application controls as well, and together, they control a majority of cloud spending.

Uncertain product-market fit: Application security requires buy-in from IT departments, which tend to have different priorities from security departments. Chief technology officers' priorities for their developers may not include incorporating security into the application lifecycle, which may limit a CISO's ability to integrate application security at the developer level, thereby reducing adoption. Further, developers have proven to be a fickle customer base at scale, with limited ability to increase budgets for new tools. Security teams have difficulty implementing solutions in other business units because 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.

Data security

Overview

Data security uses encryption, monitoring, filtering, blocking, and remediating technologies to address the risks of inadvertent or accidental data loss and the exposure of sensitive data. As 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 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.

Data security 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), DSPM, and secure multiparty computation.

- **Data protection and encryption:** Companies that protect databases from intrusions and develop novel encryption algorithms and applications for data in transit. Related technologies include data backup & recovery, tokenization, distributed ledgers, and post-quantum cryptography.

- **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 reports and documentation for audits. Many infosec companies claim to address a range of compliance issues, however, this subsegment addresses platforms that have built-in compliance rules and specialized workflows to meet emerging governmental privacy regulations.

Industry drivers

- 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. Meta was recently assessed a €1.2 billion fine, the highest on record and the company's fifth in two years.

- Data backups are used to recover encrypted data in 70% of ransomware cases, while paying the ransom only recovers data in 46% of cases.[9] Additionally, data is stolen in 30% of ransomware cases. This trend encourages advanced data backup & recovery solutions.

- Quantum computing development risks the obsolescence of existing encryption methods over the next 15 years, encouraging innovation in post-quantum cryptography algorithms.

9: "The State of Ransomware 2023," Sophos, May 2023.

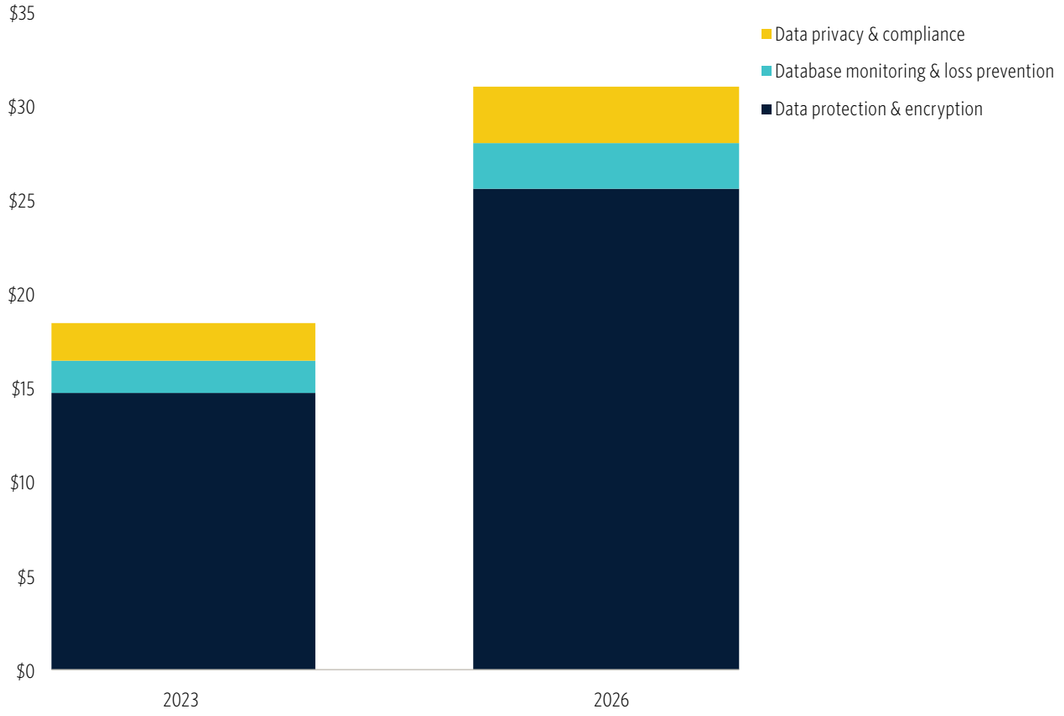
Market size

We expect the data security sector will reach a $17.5 billion market size in 2023 and estimate it will reach $29.6 billion by 2026 at a 19.1% CAGR. The data backup market contributes $12.5 billion of 2023's total, and we forecast that its market will reach $22.1 billion by 2026 at a 20.1% CAGR. Data security spending categories include encryption, data loss prevention, data privacy management, and tokenization. The data privacy management software market will reach $2.0 billion in 2023; we forecast a $3.1 billion market by 2026, driven almost entirely by private companies.

Business model

Data security is typically sold via a SaaS business model with pricing based on usage. For example, DLP subscriptions typically cost around $30 to $60 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. OneTrust's privacy essentials module costs a medium-sized business around $30,000 per year, and additional modules can be upsold, including modules for training, cookie management, and third-party risk management.

Data security market size estimate ($B)*



Source: PitchBook • Geography: Global • *As of May 18, 2023

Opportunities

Data security posture management

DSPM platforms identify cloud data repositories and discover sensitive data, enabling remediation to breaches, along with privacy. DSPM remains an immature market yet has large addressable budgets. Data privacy software has already increased to an $800.0 million market as of 2022, but it doesn't address fundamental security risks along with compliance. The data privacy market is led by startup vendors like OneTrust, although challengers—including BigID and DataGrail—are growing more quickly. BigID focuses on DSPM functionality, including data control orchestration. Further, DSPM benefits from the large market around cloud security, which has focused on cloud applications historically rather than databases. We believe DSPM can congeal into a $1 billion market over the next three years from an early stage.

Startups are being rewarded for market leadership in this nascent category with outsized early-stage rounds in a challenged market environment. In Q3 2022, both Dig and Open Raven achieved $120.0 million valuations in their Series A and Series B rounds, respectively. Dig focuses on data attack detection and response, offering the logical evolution of each new field of security visibility. This capability stands out for offering real-time detection of data changes, compared with periodic scans from cloud security tools. Its round was led by quantitative-focused VC investor SignalFire, which rates the company highly for the talent of its team.[10] Open Raven's round featured angel investors from Google Cloud and AWS, showing the value of its platform for hyperscalers.

Postquantum cryptography (PQC)

Quantum computing presents fundamental challenges to legacy encryption technologies that must be proactively addressed with novel algorithms. Not only can quantum computers theoretically decrypt our conventional encryption systems, but they can be used to take entire portions of the economy offline. In December 2022, the US government passed the Quantum Computing Cybersecurity Act, which guides federal agencies to prioritize data that will require protection from quantum computers. This bill is an initial stage of a process of postquantum modernization that may last until 2031, when post-quantum algorithms are intended to be deployed ubiquitously.

Regulated institutions are likely to invest in a stack of PQC techniques to provide defense in depth. Banks are already adopting PQC to guard against future risks, yet the uncertainty of quantum computers' strength means that no single algorithm can be trusted. Further, algorithms have been designed to protect specific data formats, including authentication and data communications. Even if the NIST approves one algorithm as a result of its testing, multiple algorithms will likely be used for different types of data, and thus multiple vendors will be supported. As a prior step, data mapping and PQC-compatible servers must be rolled out before algorithms can take hold, which may encourage an overhaul of IT infrastructure. The scale of this transformation can support a similar diversity of vendors to cloud.

10: "The Need for Real-Time Data Monitoring: Leading $34M for Dig Security," SignalFire, Jonathan Lim, September 14, 2022.

In Q1 2022, SandboxAQ spun out of Google to commercialize post-quantum algorithms with a $500.0 million investment that valued the company at $4.0 billion. The company has been selected by the NIST as a technology collaborator for the National Cybersecurity Center. Existing customers include telecom and healthcare giants, and partners include consulting firms Deloitte and EY. The company claims that customers should make the postquantum transition now to avoid "store-now, decrypt-later" attacks wherein attackers steal data to be decrypted once a sufficiently large quantum computer is developed. The scale of this company suggests that acquisitions and continued investment in the space are likely, even before NIST standards are finalized.

Risks and 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. Microsoft's DLP policies for its exchange server and Forcepoint's DLP have especially high market share. The maturity of the market raises concerns for highly funded VC-backed companies trying 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. Privacy-enhanced computing techniques like homomorphic encryption and zero-knowledge proofs may take time to develop due to the need for enhanced processing efficiency and research into compressed algorithms. We view these methods as unlikely to produce large companies until 2030.

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 and may instead focus on blocking intrusions through endpoints and the network. While in many ways data has come to represent the crown jewels of many businesses, data security still may not be top of mind among CISOs' procurement priorities. Products that align with cloud protection may fare better than on-premise databases.

Endpoint security

Overview

Endpoint security refers to the protection of data communicated through and stored in devices at the network edge, detection of attacks on edge devices, and responses to these attacks by utilizing forensic analysis and breach remediation. Endpoints include edge devices such as computers, phones, industrial equipment, and servers. Already one of the largest segments of the infosec market, this niche is experiencing sustained high growth as vendors bundle in cloud threat detection and IoT/operational technology (OT) protection capabilities. Former VC-backed companies such as CrowdStrike and SentinelOne are capturing market share from incumbents, including Trend Micro and Trellix (formerly known as McAfee).

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: endpoint protection platforms (EPP), EDR platforms, browser security, and extended detection & response (XDR).

- **IoT/OT security:** These solutions increase the visibility of industrial assets and enable security policy enforcement at the network edge. This subsegment includes firmware security, critical infrastructure threat detection, and mobile device management.

- **Anti-phishing platforms:** Software that monitors email and social media traffic for malicious files and behavior.

Industry drivers

- **Increasing volume of endpoint attacks:** The Log4j vulnerability affecting hundreds of millions of devices shows how workstations can have fundamental flaws that require visibility, patching, and threat-hunting solutions.

- **Emerging threat surfaces:** In recent years, the number of endpoint attack surfaces has multiplied, 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 a network point of entry.

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

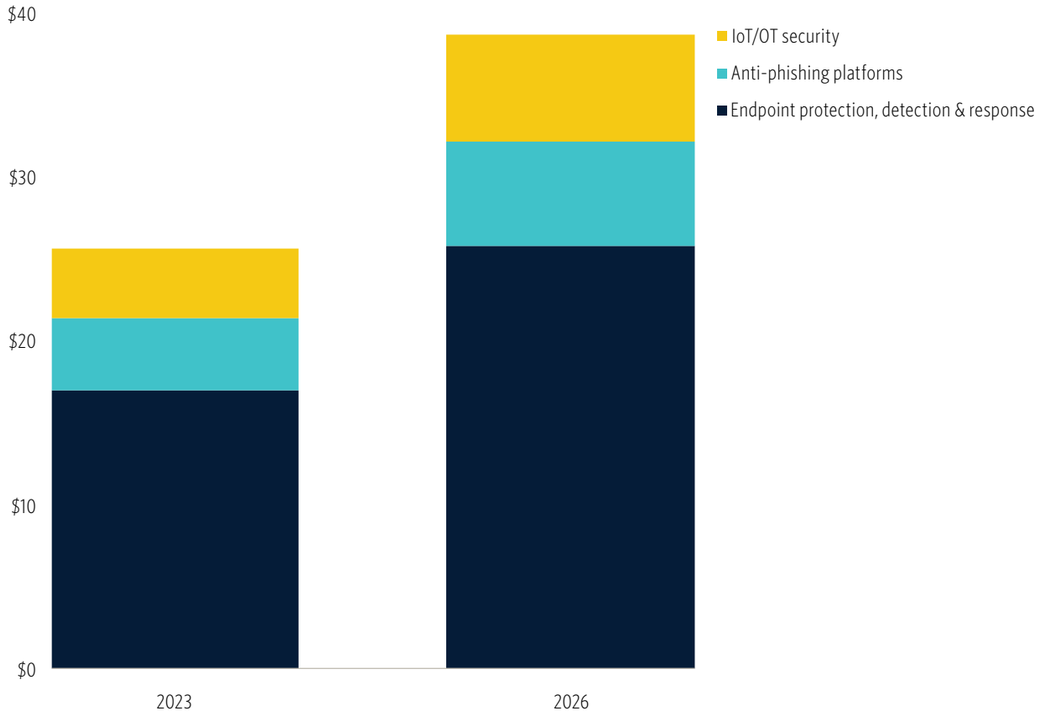
Market size

We estimate this market will grow to $25.6 billion in 2023 and forecast it will grow to $38.7 billion at a 15.1% CAGR by 2026. Endpoint protection, detection & response platforms dominate the segment, and we anticipate this category will grow to $25.9 billion by 2026. Cloud-delivered XDR remains a small niche with $0.6 billion on pace to be devoted to pure-play solutions in 2023. The IoT security market is forecast to grow as quickly at a 16.6% CAGR over the same timeframe, though the market remains small, at $4.1 billion as of 2023. The segment's growth will stem from more devices protected, as well as the addition of cloud assets as new endpoints for threat detection.

Business model

Endpoint protection, detection & response platforms, the largest subsegment within endpoint security, typically carry a subscription license fee on a per-endpoint basis, with additional upcharges for premium services such as threat hunting and vendor-managed detection and response. The price per endpoint tends to range from $30 to $70 per year. Solutions can be deployed through the cloud or on premise, with cloud services usually carrying higher prices and improved functionality.

Endpoint security market size estimate ($B)*



Source: PitchBook • Geography: Global • *As of May 18, 2023

Opportunities

Anti-phishing platforms

Consolidation in the email security space creates opportunities for VC to create the next wave of anti-phishing vendors. Over the past two years, three leading vendors have been bought by PE firms including McAfee, Symantec, Mimecast, Proofpoint, and Barracuda Networks. These firms contributed 54.2% market share in 2022 according to Gartner data.[11] Proofpoint is by far the market leader in this segment and was highly acquisitive prior to its $12.3 billion take-private by Thoma Bravo. PE may prioritize profitability above innovation and M&A, creating innovation opportunities for startups. Further exits include Avanan's sale to Check Point and Datto's sale to Kaseya. The resulting landscape contains few VC-backed vendors, generating opportunities for current startups to take market share.

Anti-phishing platform VC investment has continued to grow through the market downturn, as we tracked a record $360.5 million in 2022. Driving this investment have been megadeals for Abnormal Security and Material Security, which raised $210.0 million and $100.0 million, respectively, in Q2 Series C rounds. Material Security achieved a 4.5x valuation step-up, the sixth highest in a Series C that we tracked in all of infosec in 2022, led by Founders Fund and joined by a16z and Elad Gil. At the early stage, seed rounds demonstrate the opportunity to innovate in both the methods of phishing detection, as well as the attack vectors covered by it. In Q1 2023, Sublime Security reached a $40.0 million post-money valuation in its seed round led by Cisco-affiliated VC fund Decibel Partners—joined by leading infosec angels—to bring natural language AI to email analysis, along with crowdsourced email rules. These startups are well-positioned to build the future of email security.

Browser security

Secure enterprise browsers have presented an alternative to cloud-delivered secure browsing experiences offered by secure web gateway (SWG) vendors. Some SWGs incorporate browser isolation while offering web application control and endpoint configuration that can replicate the functions of secure browsers without the need to install a new program and change browser usage patterns. For this reason, secure browsers are most likely to be useful for unmanaged devices that don't have SWG controls layered on top. Secure browser startup Talon accepts SWG rules as part of its browser. Furthermore, the company's partnership with CrowdStrike to integrate endpoint detection & response demonstrates that secure browsers are likely to channel best-in-breed solutions rather than replacing them. Given this limited product-market fit, we believe that secure browsers will face challenges to meet outstanding expectations. If they do succeed in replacing SWGs, they can disrupt the $7.4 billion market for secure networking.

Secure browser startups Talon and Island have received funding to establish a new category of browser security. In Q3 2022, Island raised a $115.0 million Series B at a $1.2 billion pre-money valuation led by Insight Partners, along with Stripe and Sequoia Capital, after emerging from stealth in February 2022. The startup embeds security controls within a Google Chrome-like

11: "Market Share: Security Software, Worldwide, 2022," Gartner, May 2023.

browser. Also in Q3, Talon raised a $100.0 million Series A led by Evolution Equity Partners after its founding in 2021. Like Island, the startup embeds security controls within a Google Chrome-like browser. The startup was named "Most Innovative Startup" at the 2022 RSA Conference and has since reported heightened demand from customers. Its browser integrates multiple security controls, including data loss prevention, SaaS application monitoring, and zero-trust access control. New entrant Seraphic recently closed a seed round to offer browser-level controls that do not require installation of a new enterprise browser. These companies are likely to create a new category of endpoint protection and a promising vector for zero-trust network access.

Extended detection & response

The next phase of endpoint security is emerging in a product suite referred to as XDR, which automates the detection and response phases of enterprise breaches. XDR promises to consolidate the tool sprawl in security operations by aggregating logs from across enterprise IT environments and automating security responses to alerts. 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 analytics of endpoint behavior to detect latent malicious activity. Emerging IT assets including remote workstations, cloud workloads, and IoT devices require additional telemetry for analysis in cloud-based analytics systems.

XDR startups have multiple entry points yet should focus on cloud threat monitoring. In Q1 2023, early-stage XDR startup Confluera was acquired by XM Cyber. Confluera was founded as an advanced threat detection solution to advance the XDR field with a graphical user interface that tracks attacks as they develop across IT assets, allowing security teams to more quickly hunt threats and conduct forensic analysis. The acquisition is justified by Confluera's ability to support cloud workload protection, an adjacent category to endpoint detection & response. Early-stage startup Citadel Control Services brings NSA-developed reverse engineering technology to network traffic threat detection before it enters enterprise network and is gaining mindshare with managed detection & response service providers to add network telemetry for cloud services like Microsoft Azure to endpoint agents. The startup's software can detect the origin of network traffic with AI-generated threat queries and is capable of running in the cloud or on edge devices. We believe novel approaches like this can supplement the endpoint-focused behavioral analysis of incumbents.

Industrial cybersecurity

IoT/OT security software, including both internet-connected devices and industrial technology with limited connectivity, has emerged as a leading opportunity in the IoT vertical given the scale of the cybersecurity problem. Relative to other information security categories, IoT/OT security requires a unique stack of solutions to cover the device communication chain. IoT systems generally contain devices, communications gateways, and analytics applications. In OT, this chain, which contains disconnected network layers between these assets, is referred to as the Purdue model. Given the complexity of device types in large enterprises, a stack of security solutions is required to provide defense in depth, including device security, network & communication security, and vulnerability assessment. For further definitions of these segments, see our Q1 2021 PitchBook Analyst Note: Getting to the Root of IoT/OT Security.

Numerous IoT/OT security companies remain in the pipeline for exits and have continued to perform well. Given the stack of solutions required to provide layered defense, as well as the different device types, the space can support a range of large companies. In industrial control systems/OT security, Dragos plans to remain independent via an IPO and is thus not pursuing an acquisition. In IoT security, Armis was bought out in January 2020 and has since raised growth funding to pursue an IPO while expanding its product portfolio. Claroty, Axonius, and Nozomi Networks have raised self-proclaimed pre-IPO rounds. Given this pipeline, the category could be one of the leading drivers of upcoming public market exit value in all of enterprise software, pending a recovery in market conditions.

Risks and considerations

Customer churn: Constantly evolving threats may render new technologies obsolete and increase customer churn, and old systems may be retired if they cannot 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. In fact, a 2018 survey finds that over 50% of users are able to deploy such solutions in three months or less.[12] 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 are 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 Labs, and a benefit for others, such as Panda Security, which automates the creation of zero-trust policies, thereby removing a complex workload for security staff.

Crowded market: The highly competitive endpoint market is a difficult space in which to win market share. In recent years, numerous next-generation endpoint providers have challenged legacy vendors, such as CrowdStrike, Carbon Black, SentinelOne, 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. We believe this explains the muted exit performance of EPP and EDR companies in 2021 and recent down round for challenger Cybereason.

Automation can fail in practice: Machine learning (ML) 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.

12: "The 2018 State of Endpoint Security Risk," Ponemon Institute, September 20, 2018.

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 networks more secure than firewalls, which rely on denying known threats. We also include fraud prevention in this segment, which uses identity-based rules and data models like machine learning to block fraud, principally in e-commerce and retail.

Identity & access management 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, thus making it part of the IAM segment. Technologies within this subsegment include online fraud detection and identity verification.

- **Identity governance & administration (IGA):** Platforms that verify user identities based on corroboration of access requests with predefined policies. Technologies within this category include:
  - Directory management
  - Entitlement management
  - Password management
  - Passwordless authentication
  - 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.

- **E-commerce fraud:** E-commerce requires the management of customer identities across devices and has high potential for fraud. One study shows that 22% of consumers have been victims of account takeover.[13]

- **SaaS application growth:** Enterprises are growing their use of SaaS applications and storage of sensitive data in those applications. Tech enterprise customers of IAM platform Okta use 211 SaaS apps on average in 2023, up 8.2% from 2022.[14] Employee identities must be managed across all these applications and monitored for insider threats.

13: "Account Takeover 2021 Annual Report: Prevalence, Awareness and Prevention," Security.org, February 18, 2021.
14: "Businesses at Work," Okta, 2023.

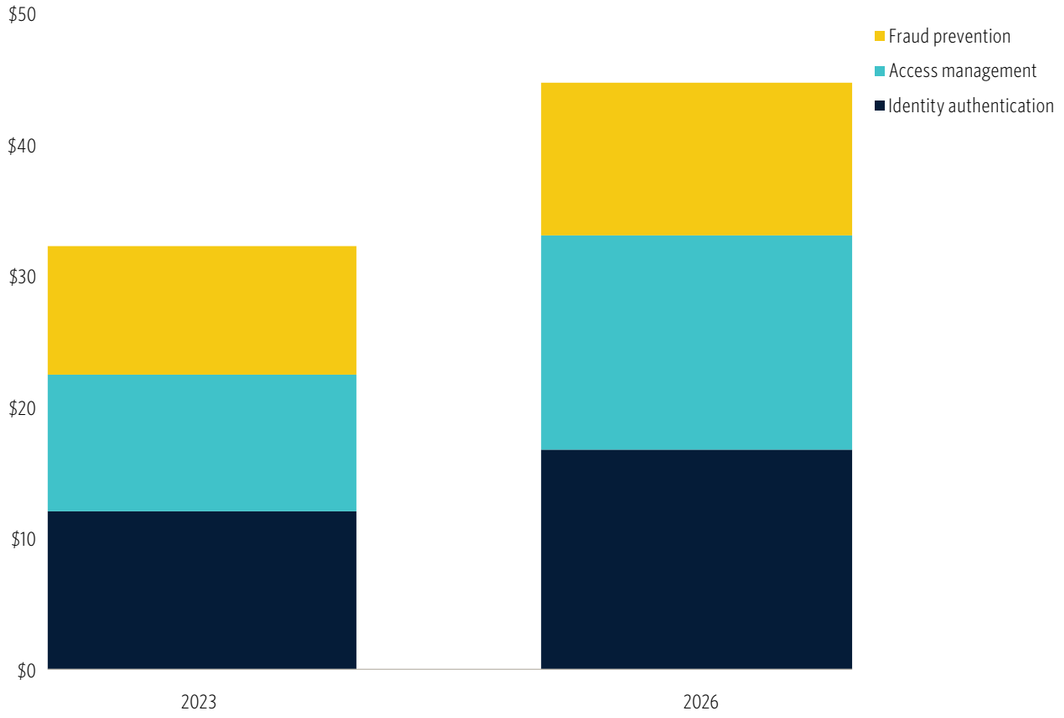
Market size

We estimate the IAM market to reach $32.2 billion in 2023, growing 11.7% over 2022. Going forward, we forecast the market to reach $44.8 billion by 2026 at a 11.6% CAGR. This estimate includes the IAM cornerstones of access management, identity governance & administration, and fraud prevention. Fraud prevention contributes an $9.8 billion market to 2023's total. We project access management software to achieve the highest growth by 2026, with a 16.4% CAGR.

Business model

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

Identity & access management market size estimate ($B)*



Source: PitchBook • Geography: Global • *As of May 18, 2023

Opportunities

Passwordless authentication

Passwordless identity governance & administration platforms can eliminate credentials theft while reducing IT maintenance costs for password provisioning. Research finds that credentials are sought by attackers in over 80% of web application breaches, thus making the presence of passwords an open target for organizations.[15] Multifactor authentication (MFA) and regular password updates help to address this problem but can slow productivity and leave the organization vulnerable to man-in-the-middle attacks, which refer to the capture of authentication tokens by attackers with access to vectors like mobile phones and email. Passwordless approaches can use the identity of the device that an employee is using and behavioral analytics on those devices to enable zero-factor authentication (ZFA) and seamlessly manage access in a zero-trust framework. The recent release of the FIDO2 standard has ushered in a new era of public-key cryptography for access management since users can bring cryptographic keys between devices with credentials called Passkeys.

Startups are winning large deals in this space as tech companies use passwordless products in both consumer-facing and internal use cases, supporting large companies in both areas. Both early-stage vendors Nok Nok and Beyond Identity cite a significant deployment with fintech giant Intuit yet for both customer and employee identities separately. A standout use case is onboarding third-party contractors to corporate resources. At the early stage, Token offers a smart ring for a novel form factor for hardware-based passwordless authentication. It announced $30.0 million in venture debt to expand its physical token production soon after legacy identity token vendor Yubico's $796.5 million public listing. This category can support a range of approaches and techniques across customer segments.

Fraud prevention

Fraud prevention includes technologies that detect and block fraudulent access requests and payments. It has emerged as a leading application of ML, given the outperformance of ML models when compared with manual transaction review. The market is broadly divided into fraud hubs and chargeback guarantee vendors. Fraud hubs bring a range of capabilities including rules engines, ML, case management systems, and managed services. They accept no liability for fraud and target large enterprises. Chargeback guarantee vendors use ML algorithms to automatically make fraud decisions and accept liability for fraud. They typically target SMB vendors. We estimate the fraud prevention market will reach $9.8 billion in 2023, growing at a 6.1% CAGR to a $11.7 billion market in 2026.

Startups are bringing advanced ML to a range of fraud-related use cases. ML models can be customized for different consumer channels to achieve superior performance and offer guaranteed fraud reduction. In addition to transaction review, customers are looking for assistance with account takeover, false bank declines, and policy abuse. Vendors with multiple models can adapt to anomalous situations across different transaction types, and we believe startups are in the best position to address a range of use cases.

15: "2022 Data Breach Investigations Report," Verizon, May 2022.

Fraud detection unicorns proliferated during the market boom and remain able to raise debt. In Q1 2023, Socure raised $95.0 million in venture debt from lenders including Silicon Valley Bank and JP Morgan Private Bank. This deal indicates that the company may not warrant valuation growth over its prior $4.5 billion private valuation yet has a mature business plan. Recently listed unicorn Riskified has seen its revenue growth slow, creating limited expectations for the rest of the market. There may be an opportunity for PE takeovers for large businesses in this space.

Machine identity management

Leading infosec investors acknowledge a gap in credentials management for machines, such as employee workstations, SaaS applications, and operational technology. At the early stage, Astrix Security has built a VPN for cloud-based machines to assess the security of their API connections and authorization tokens, citing 45x more non-human identities than humans. Fellow startup Qwerx demonstrated a key management solution for machines with focuses on operational security and successful customer deployments in national security. The startup takes a similar approach to early-stage startup Corsha, which brings a version of MFA to non-human identities via continuous rotation of a second public key. Leading VC investor CyberStarts has also disclosed a stealth investment in a machine identity startup along with the urgency of the challenge for security teams. Machine identities can be an essential part of endpoint breach mitigation, and we have seen startups such as BlastWave, Delinea, and Elisity succeed in this area yet not offer a winner-take-all solution.

Risks and considerations

Incumbent leadership in IGA: We see SailPoint, IBM, Okta, and Microsoft as leaders in IGA that are unlikely to cede market share in single sign-on and directory management to challengers. SailPoint has a cloud-architected IGA solution with a leading user experience and dominance in the large enterprise market. Okta has developed a cloud-first access management platform with growing functionality for developers and customers via its Auth0 acquisition. Microsoft's dominant position at the core of directories creates challenges for establishing a new system of record.

High competition in fraud prevention: At least a dozen competitive fraud prevention platforms offer 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: These solutions typically require system integrators to deploy IGA software, adding high upfront costs to subscription fees. Gartner estimates that 50% to 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.[16] 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.

16: "Magic Quadrant for Identity Governance and Administration," Gartner, Felix Gaehtgens, Kevin Kampman and Brian Iverson, February 21, 2018.

Network security

Overview

Network security includes software and hardware that protects enterprise network infrastructure from digital attacks. The segment 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, public cloud, and routers and switches. The growth of cloud environments and remote networks has created new surfaces for attackers to target, thus driving innovation in network security. As a result, network security solutions increasingly provide protection for data at rest and in transit within hybrid and multicloud-based environments, as well as for data delivered through SaaS applications. Enterprise perimeters are increasingly amorphous as employee devices are spread over diffuse wifi networks and legacy IT approaches are insufficient to ensure business continuity. Secure networking is essential for remote work, as employees must be able to securely gain access to cloud servers. Existing VPN solutions have performance issues and struggle to scale. Enterprises are shifting resources to the cloud, which requires 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 CASBs, CSPM, cloud vulnerability scanning, and cloud-based secure web gateways.

- **Network detection & response:** Platforms that detect risk exposure in network traffic and identify threat actors attempting to breach the enterprise perimeter. This subsegment includes network traffic analysis, dark web threat intelligence platforms, and network security policy management.

- **Secure networking:** Software-based secure network architectures that go beyond conventional firewalls and networking equipment and include secure web gateways, next-generation firewalls, software-defined wide-area networks (SD-WAN), VPNs, and zero-trust network access.

Industry drivers

- Enterprises are trending toward full-scale replacements of VPNs with zero-trust-based secure access service edge (SASE) solutions. According to an industry survey, 51% of IT teams are planning to use SASE solutions to fully replace their existing VPN solutions for remote access. A further 35% are interested in such a replacement.[17]

- Public cloud vulnerabilities are expanding more rapidly than legacy solutions can detect and remediate them. Cloud security played central roles in recent breaches, including the Solarwinds supply chain attack and the Hafnium attack on Microsoft Exchange. In those cases, attackers were able to mimic legitimate cloud certificates. 40% of global enterprises have suffered at least one cloud breach over the past year, according to a vendor survey.[18] Cloud threat detection has emerged as a weakness for leading managed security service providers in customer feedback.

- Hybridization of cloud environments and a trend toward multicloud strategies are creating new security complexities. One study shows that individual enterprises use an average of 2.6 public clouds and 2.7 private clouds.[19] Security is the most prevalent challenge for advanced cloud users.

17: "A Guide to Adopting Secure Access Service Edge Network Security," Enterprise Strategy Group, March 2021.
18: "2022 Thales Cloud Security Study," Thales, March 2023.
19: "Flexera 2023 State of the Cloud Report," Flexera, March 2023.

Market size

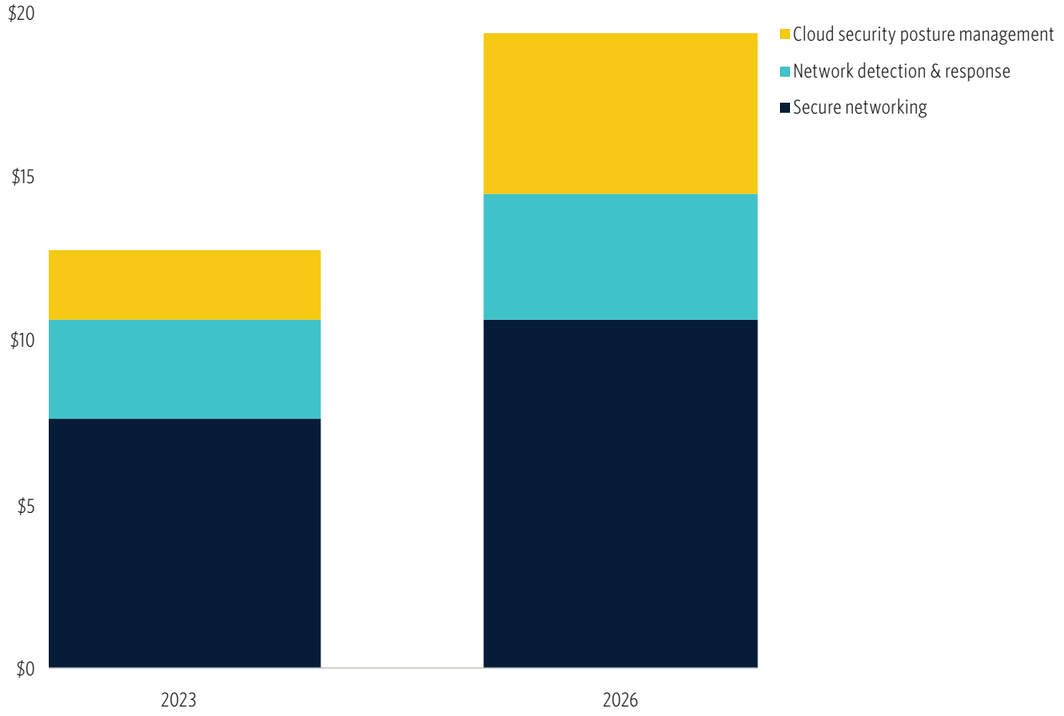
We estimate the network security market will reach $12.8 billion in 2023, accelerated by demand for zero-trust networking solutions. This market size includes cloud security, network detection & response, and secure networking software, and excludes firewall hardware. We forecast network security to grow more in line with the overall infosec market, at a 14.8% CAGR, to a $19.3 billion market in 2026. Cloud security is still a niche within network security, but we estimate it will be among the highest-growth infosec subsegments over the next three years, with a 31.3% CAGR. We estimate network detection & response and secure networking will grow in line with the market, at 14.4% and 11.7% CAGRs, respectively.

Business model

Network security products are typically bundled based on use case and can include the following components:

- Fee per network user, ranging from $2 to $50 for basic breach discovery and log management.
- Maintenance and support costs.
- Mobile protection and data encryption for premium modules.
- One-time sales of infrastructure, including secure web gateways.

Network security market size estimate ($B)*



Source: PitchBook • Geography: Global • *As of May 18, 2023

Opportunities

Secure service edge (SSE)

SSE refers to a shift in network security from on-premises firewalls and networking appliances to cloud-delivered access for distributed enterprise perimeters. Core components of SSE include secure web gateways, CASBs, and zero-trust network access. This definition excludes SD-WAN that are typically offered by non-security vendors, along with firewalls. The exclusion of networking hardware enables SaaS vendors to dominate this niche. These products are bundled together in a cloud-delivered networking solution that can supplant existing enterprise networking for distributed devices.

Product suites emphasize zero-trust approaches to network access. SSE platforms can enable zero-trust approaches by enforcing access control across cloud, web, and applications. Zero-trust networking is on pace to surpass VPN as the primary means of remote connections to the enterprise network. A global survey found that 94% of organizations are currently implementing zero-trust architecture models.[20] Further, most respondents believe that VPNs will be phased out in favor of zero trust. The primary commercial methods of implementing this model include Zero Trust Network Access and micro-segmentation. Private companies benefiting from this trend include Netskope, Perimeter 81, and Lookout.

In Q1 2023, Zero Networks raised a $20.3 million Series A to enable micro-segmentation with MFA, which is connected to assets at the network layer and will automatically turn on if risky behavior is detected. This approach adds friction to employee experiences if they are engaging in abnormal behavior yet offers smoother access than behavioral analytics software. Additionally, the approach may not work well against insider threats. The founder was a former product manager at Microsoft for the integration of EDR startup Hexadite, giving him insight into automated remediation products. We believe this capability will appeal to legacy CASB and secure web gateway vendors that have limited micro-segmentation capabilities.

Cloud vulnerability assessment

Cloud vulnerability assessment demonstrates the convergence of endpoint security and network security as a result of cloud transformation. Comprehensive visibility into hybrid and multicloud environments is becoming a higher priority as cloud resources become the new endpoints of enterprise networks. Even after a first wave of consolidation in cloud security, most security teams lack clarity on where sensitive data is being processed in the cloud. The ability to scan multicloud enterprise networks—especially containers and serverless scripts—for vulnerabilities remains a challenge for security teams. As a result, cloud security is the fastest-growing category in infosec, having grown 39.1% in 2023 to a $1.1 billion market with a 36.3% CAGR forecast to 2026.

VC megadeals for Orca Security, Lacework, and Wiz reflect a startup's ability to take advantage of outstanding spending growth. These startups are bringing agentless approaches to cloud scanning and promising universal coverage of multicloud environments. In Q1 2023, Wiz set a record for infosec startup post-money valuation at $10.3 billion. The company disclosed reaching $100.0 million ARR in Q3 2022 at a growth rate we believe exceeds 150%, suggesting that the ARR

20: "Eighty Percent of IT and Security Professionals List Zero Trust as a Priority, According to New Cloud Security Alliance Survey," Cloud Security Alliance, June 6, 2022.

multiple for this deal resembles the multiples granted before the market downturn. We have tracked similar revenue multiples for innovative AI companies, yet other information security unicorns have resorted to debt financing and down rounds to extend their runways. Wiz stands out in the cloud security market for its agentless cloud scanning approach, offering security and IT operations teams visibility into cloud resources that have amplified in complexity during the rapid digital transformation of the past three years. The company is expanding into cloud workload protection and data security posture management, demonstrating the opportunity to expand from the cloud.

Cloud infrastructure entitlement management (CIEM)

A leading cause for cloud breaches is overprivileged 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 gain access to sensitive data, as evidenced by the SolarWinds breach in 2020. Manual cloud permission management can take 80% to 100% of identity management teams' time, thus creating a need for external solutions. Further, cloud hosts offer little automation through cloud-native tools. Given the risks of administrator-level access and increased reliance on cloud resources, greater control over cloud identities is necessary.

CIEM platforms scan user permissions across cloud environments and enable review and remediation of excess privileges. This niche of cloud security is less susceptible to dominance by cloud providers than other cloud security products because user identities apply across on-premise and multicloud environments. Identity leaders have begun to make acquisitions in this space, including Rapid7 (DivvyCloud), Microsoft (CloudKnox), and SailPoint (Orkus Security). In Q4 2021, Sonrai Security raised a $50.0 million Series C at a 3.1x valuation step-up from strategic and specialist investors.

Three seed deals have closed in the space over the past year including for Arpio, ClearVector, and Acsense. Startups can differentiate based on the level of automated remediation they offer for policy enforcement. The space's adjacency with access management offers greater potential for scale than most point solutions for cloud security.

Risks and considerations

Innovative incumbents: The cloud security access broker 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. Network security leader Palo Alto Networks has achieved high growth with its Prisma Cloud product suite and renewed its commitment to M&A with its acquisition of cloud application security startup Cider. As other 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 cloud security startups without high VC funding.

Cloud providers crowding out startups: Cloud service providers are increasingly developing high-quality security tools for customers to use in their deployments. Microsoft, Amazon, and Google have all introduced DLP and security information and event management features to their public cloud environments that may compete with challengers such as Netskope and Lacework. While the limited liability of cloud providers for customer data will provide a compelling reason to deploy a third-party cloud security solution, cloud providers have cost and customer data advantages in offering security services. Startups have been unable to scale cloud security posture management solutions due to competition with public cloud hosts and have exited at low valuations as a result.

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, and 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 offering solutions to SMBs that are underserved by high-end infosec products.

Security operations 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 enterprise's value at risk in the 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, which includes software for managed detection & response. This subsegment also includes cybersecurity insurance underwriting.

Industry drivers

- **Security talent shortage:** A shortage of security talent is driving CISOs to invest in software to handle alerts.

- **Increasing alert volume:** 70% of security and IT teams indicate that they struggle to keep up with security alert volume.[21] These alerts are multiplying with increased telemetry into cloud and remote work environments.

- **Tool consolidation:** Most CISOs are now pursuing a tool consolidation strategy as of 2022, encouraging usage of managed services instead of adding new software vendors.

21: "SOC Modernization and the Role of XDR," ESG, June 2022.

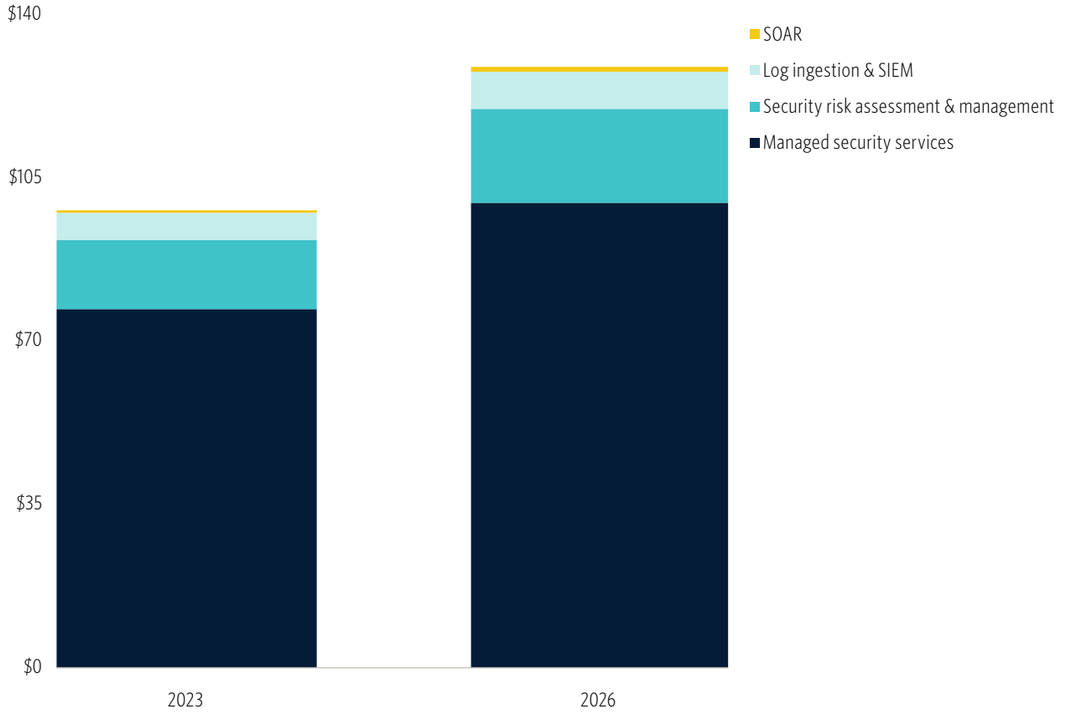
Market size

We estimate the security operations software market, exclusive of professional services, will amount to $22.1 billion in 2023. We forecast the market will grow to $30.2 billion in 2026 with a 11.0% 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 $76.9 billion in 2023. We expect VC-backed companies will capture market share in this subsegment, given the lack of technological innovation in the niche. We forecast SOAR to outpace the market at a 20.3% CAGR from a low base. Our outlook for SIEM has been muted by pressure from endpoint security vendors, leading us to forecast only a 9.1% CAGR out to 2026, resulting in a $7.3 billion market.

Business model

Security operations business models differ by product. SOAR platforms are based on SaaS subscriptions for security analysts. 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 in use within the enterprise.

Security operations market size estimate ($B)*



Source: PitchBook • Geography: Global • *As of May 18, 2023

Opportunities

Compliance automation

SOC 2 completion is becoming a requirement for secure software supply chains. The standard can take less time than comparable standards, including ISO 27001 and the Federal Risk and Authorization Management Program. It has also become more popular among US tech companies because it demonstrates controls relevant to software companies; ISO 27001 can apply across industries and is more popular outside of the US. According to a vendor survey, two-thirds of small technology businesses have SOC 2 certification or plan to achieve it over the next two years, while only half plan to achieve ISO 27001.[22] By any measure, the share of companies that have achieved SOC 2 remains low, and in the US, the certification is a priority for more companies than those that have achieved it, making SOC 2 software a growth market going forward.

Startups solving SOC 2 compliance are among the fastest growing in infosec overall. In Q3 2022, Drata became a unicorn in its Series B with a $100.0 million deal led by ICONIQ Growth at a 7.1x valuation step-up after its founding in 2020 and emerging from stealth in January 2022. The company has become a leader in SOC 2 compliance with advanced software features, including an automated inventory of physical and virtual assets based on a set of APIs. The company also addresses more established standards, including ISO 27001, the Health Insurance Portability and Accountability Act of 1996, and the Payment Card Industry Data Security Standard. Co-founder Adam Markowitz sold his startup Portfolium to Instructure for $43.0 million in 2019. The company claims to have acquired hundreds of customers after two years in the market, demonstrating the product-market fit for SOC 2 automation.

22: "2022 State of Startup Security Report," Vanta, February 2022.

Exposure management

Exposure management, as coined by Gartner, should feature multiple software components, including vulnerability assessment, security control validation, and attack surface scanning.[23] Vulnerability assessment is a conventional product category that includes risk identification and prioritization based on lists of known common vulnerabilities and exposures that can be detected via software scanning. These scans depend on routine surveys of known assets. In contrast, attack surface scanning discovers internet-connected assets via APIs to identify gaps in security controls and existing vulnerability assessment scans. Validation refers to testing the effectiveness of existing security controls on internet-connected assets, including pen testing and attack simulation. Complementary features in this category include digital risk protection, security rating services, and application security testing.

We estimate that the serviceable addressable market for exposure management will incorporate the $1.8 billion vulnerability assessment market and the $6.0 billion risk management market, growing at an 11.3% CAGR to a $10.7 billion market in 2025. For vulnerability assessment vendors, incorporating exposure management features allows them to expand their addressable market by up to 4x if they can offer more comprehensive risk management software.

The trend toward outside-in scanning can accelerate startup results. Bishop Fox was founded in 2005 yet did not close a Series B until Q4 2022, when the company achieved a 6.1x valuation step-up resulting in a $600.0 million post-money valuation. It raised a Series A from infosec specialist VC Forgepoint Capital in 2019. The company pivoted from a services model to software in 2018 and

23: "Innovation Insight for Attack Surface Management," Gartner, March 2022.

now stands out as a leader in the attack surface management market, as determined by market research firm GigaOm.[24] Its platform achieves high coverage and accuracy in detection of internet-connected assets with a combination of ML and manual review. Exposure management has created an M&A trend, as outlined in our Q3 2022 Information Security Report. Threat detection incumbents require enhanced external scanning capabilities to protect against nation-state threats and monitor shifting enterprise perimeters. In Q1 2023, ZeroFox acquired LookingGlass Cyber Solutions to continue this theme. Security services remains a competitive differentiator for security operations despite promises of full automation from software-only startups.

Managed detection & response (MDR)

MDR evolved as a combination of endpoint security software and incident response to offer 24/7 threat monitoring services via an outsourced security operations center. These security operations centers are staffed by security analysts. MDR includes managed EDR software, incident response services, and managed threat hunting. Midsize enterprises are increasingly seeking turnkey managed detection & response systems, in addition to traditional monitoring services. Enterprises are circling back to managed security services in a time of budget constraints, thus creating a large addressable market for vendors that is relatively insulated from economic uncertainty.

This category is now anecdotally the fastest-growing niche in managed security services, though limited market size data has been collected on offerings in the space. Frost & Sullivan estimates that the space grew at 64.0% in 2021 from a base that we believe falls between $500 million and $2 billion.[25] It estimates a 34.0% CAGR over the next several years, aligning with other high-growth categories of infosec, including cloud security and zero-trust networking. The managed security services market looms as a much larger market than software but with lower growth; it incorporates consulting, IT outsourcing, implementation, and hardware support. Disruption of this market can produce large businesses.

Managed security services VC funding held up in 2022, reaching $1.9 billion after $2.1 billion in 2021. In Q4 2022, Arctic Wolf raised a $401.0 million debt round from Owl Rock Capital Group. The deal value was the largest we have tracked in the managed security services segment, surpassing Coalition's $250.0 million Series F from June. Arctic Wolf's revenue grew 46.0% in 2022, from $183.0 million to $256.0 million, according to Gartner data, and the company rapidly grew headcount.[26] It has expanded into valuable adjacencies, including cloud security and exposure management.[27] Earlier-stage startup Blumira is continuing triple-digit revenue growth by commercializing a detection & response platform for managed service providers (MSPs) that want to offer MDR services. 700% growth in MSP business led the company to raise a $15.0 million Series B from leading specialist investor Ten Eleven Ventures, demonstrating the importance of the services channel and a focus on SMB customers for tech startups.

Threat intelligence

Threat intelligence products collect data about infosec attacks and other IT risks. This data can serve as an input to security analytics software for matching to actual enterprise log data. It can also be used to create threat models for organizations in designing their security programs and practices. Mature security organizations can acquire more than 10 feeds of threat intelligence such

24: "GigaOm Radar for Attack Surface Management v1.0," GigaOm, February 28, 2022.
25: "Frost Radar™: Global Managed Detection and Response Market, 2022," Frost & Sullivan, May 2022.
26: "Market Share: Managed Security Services, Worldwide, 2022," Gartner, April 2023.
27: For a definition of exposure management, see our Q3 2022 Information Security Report.

as open-source, government, corporate information sharing, and commercial sources. Software solutions include machine readable threat intelligence (MRTI) feeds that are interpretable by threat detection software. Use cases of threat intelligence include alert correlation, attack simulation, threat detection rules, digital risk protection, and query generation for threat hunting. The market for pure-play threat intelligence remains small, on pace to reach $2.9 billion in 2023, yet is growing quickly at 17.2%, with catalysts to continue high growth going forward. We believe that threat intelligence will also be a value driver for the $17.0 billion EDR market, along with the $76.9 billion managed security services segment.

Late-stage managed security services startups use threat intelligence to differentiate their products. In Q1 2022, Bluevoyant raised a $250.0 million Series D. Focusing on domain name attacks, the company stands out in the market for digital risk protection and has become a leader in this space along with Rapid7 and Microsoft. The company has built customized detection toolsets for emerging threats, including a sample of HermeticWiper malware used by Russia against Ukraine. This approach to customized threat intelligence may be difficult to scale yet is likely to be adopted by small and medium-sized business security teams with limited additional threat feeds. Leading specialist investor Ten Eleven Ventures recently found opportunity in this space leading a $20.0 million Series B for Blackbird.AI to aggregate threat intelligence on disinformation campaigns, which represent an emerging form of social engineering that can yield harmful effects similar to cyberattacks. New forms of threats can yield new business opportunities.

Risks and considerations

Crowded SIEM and SOAR markets and rapidly innovating incumbents: SIEM is a mature market with numerous point solution vendors. For example, Sumo Logic—an IT vendor—integrates SIEM with its log management platform yet struggled to scale before a PE exit. Incumbents such as IBM and Splunk, through its Phantom Cyber acquisition, have developed in-house SOAR solutions. RSA uses a white-labeled Demisto SOAR. In Q1 2022, Google acquired SOAR vendor Siemplify and threat intelligence startup Foreseeti to add to its security operations product Chronicle. Because of the consolidation that has occurred in this market, 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.

Software vendors disrupting managed security services: While midsize enterprises can benefit from outsourcing their security operations centers, larger enterprises have the staffing to take advantage of lightweight SaaS tools with analytics and managed services functionality. For example, CrowdStrike offers managed detection & response, in addition to its automated threat detection platform, limiting the amount of service needed. Further XDR can ingest data from SIEMs and carry out value-added tasks including threat correlation and patching. 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.

Appendix

Top VC-backed infosec companies by total VC raised to date*

Company	Category	VC ($M) raised to date	Post-money valuation ($M)
Lacework	Cloud security	$1,857.4	$8,300.0
Netskope	Cloud security	$1,445.3	$7,500.0
Fireblocks	Web3 security	$1,227.9	$8,000.0
Securonix	Log ingestion & SIEM	$2,388.1	$8,000.0
Snyk	DevOps security platforms	$1,071.0	$7,400.0
OneTrust	Data privacy & compliance	$970.0	$5,500.0
1Password	Identity governance & administration	$950.1	$6,800.0
Rubrik	Data protection & encryption	$926.5	$3,300.0
Wiz	Cloud security	$921.0	$10,300.0
Arctic Wolf	Managed security services	$899.5	$4,300.0

Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Top VC investors in infosec companies in 2022*

Name	Deal count
Accel	14
Sequoia Capital	14
Tiger Global Management	13
SYN Ventures	11
Gula Tech Adventures	11
Cisco Investments	11
Forgepoint Capital	10
Ten Eleven Ventures	10
Team8	10
Andreessen Horowitz	10

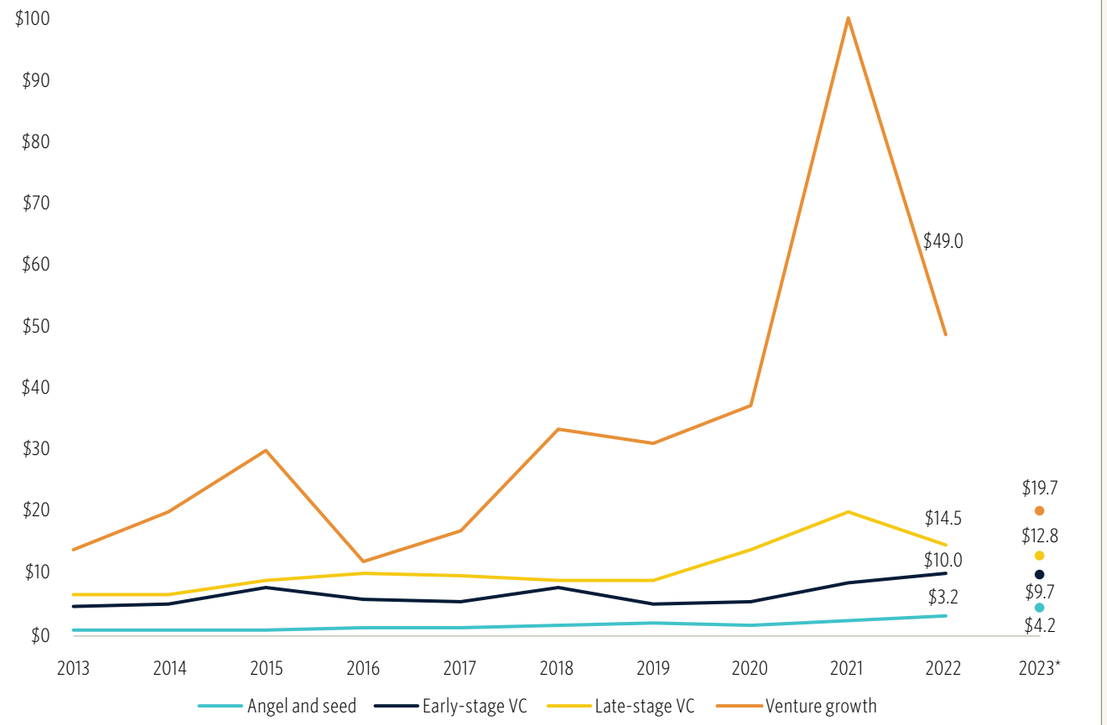
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Top strategic acquirers of infosec companies 2020-2022*

Name	Deal count
Fortra	10
CISO Global	9
Deloitte	9
Accenture	7
Microsoft	6
Palo Alto Networks	6
Meriplex Communications	6

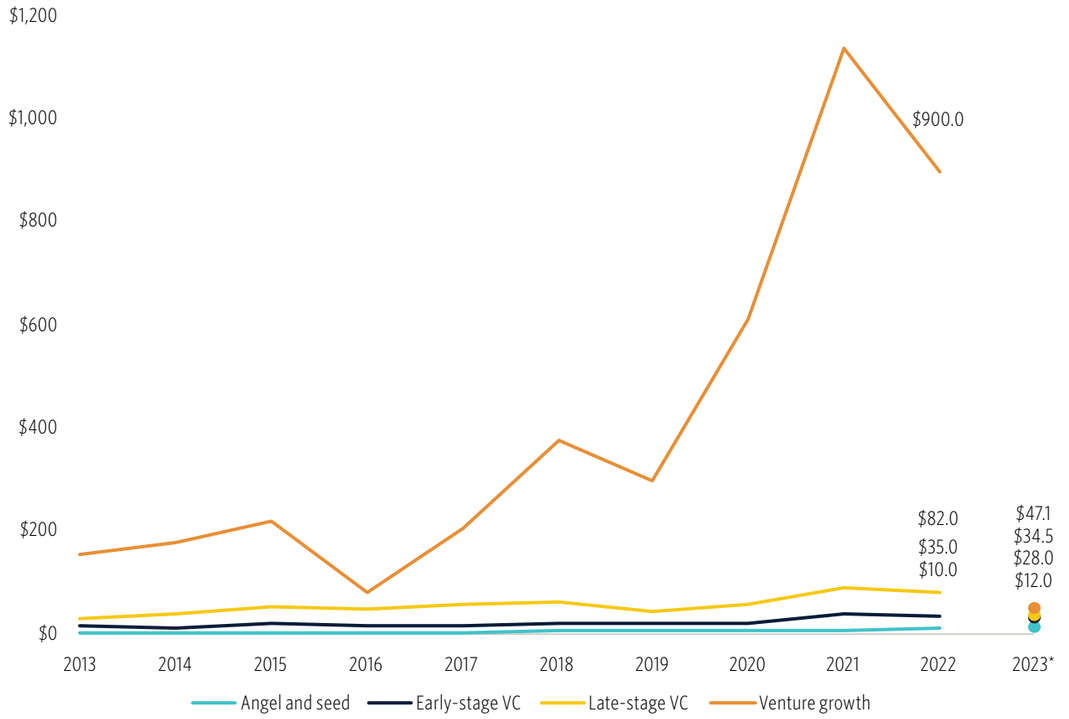
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Median infosec VC deal value ($M) by stage



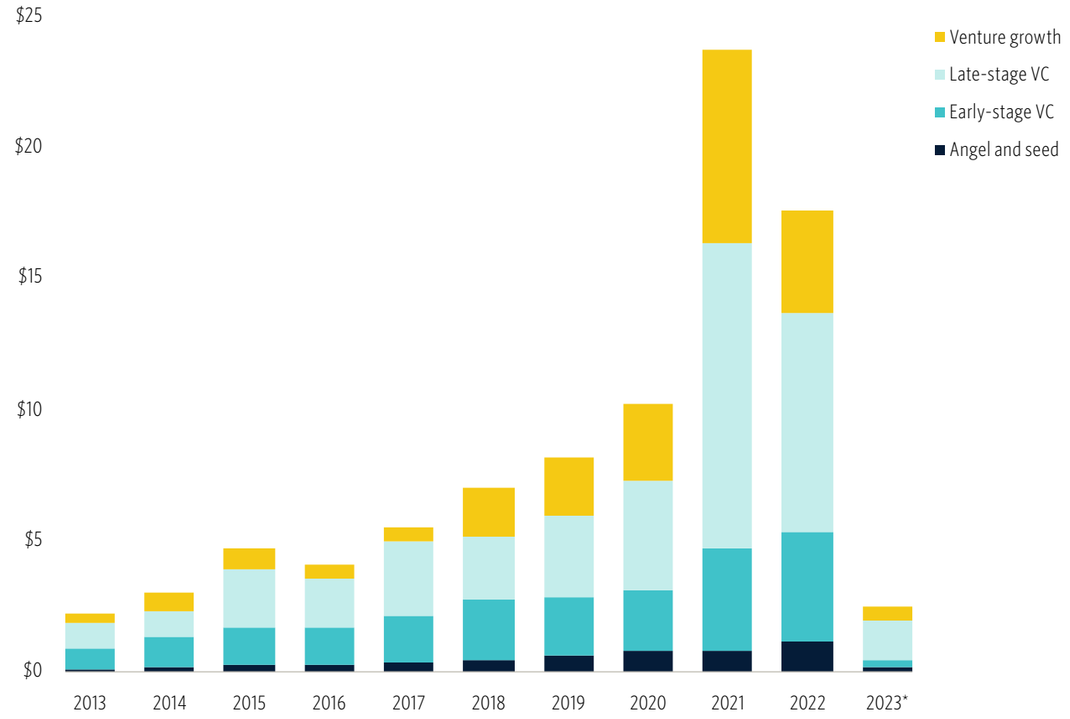
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

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



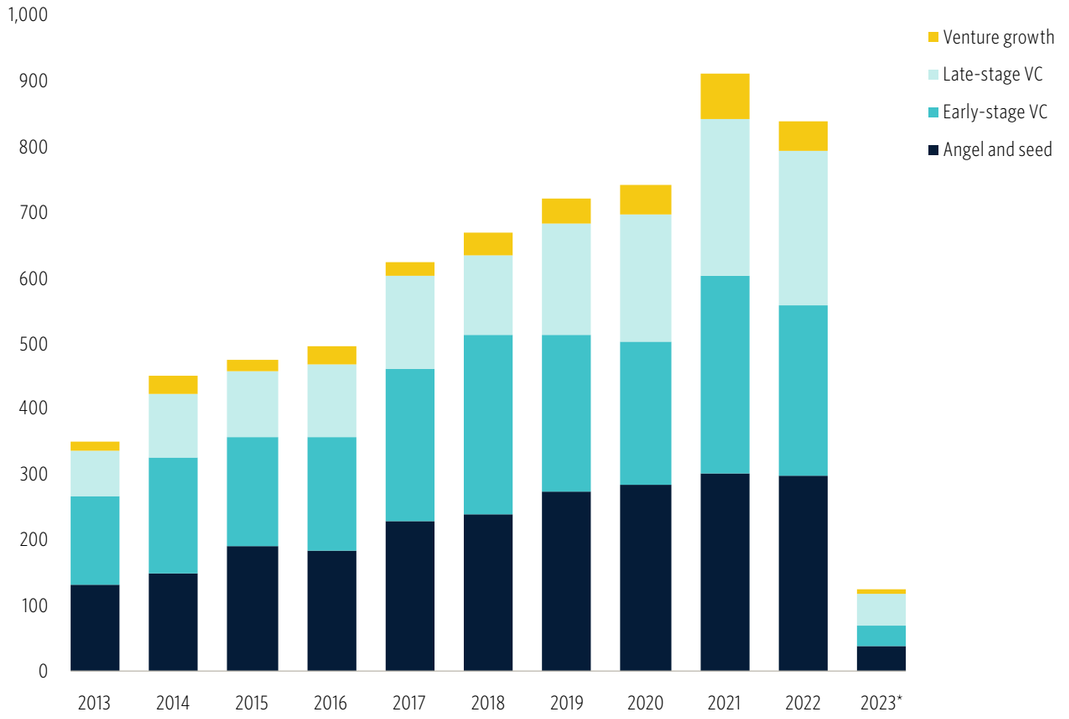
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Infosec VC deal value ($B) by stage



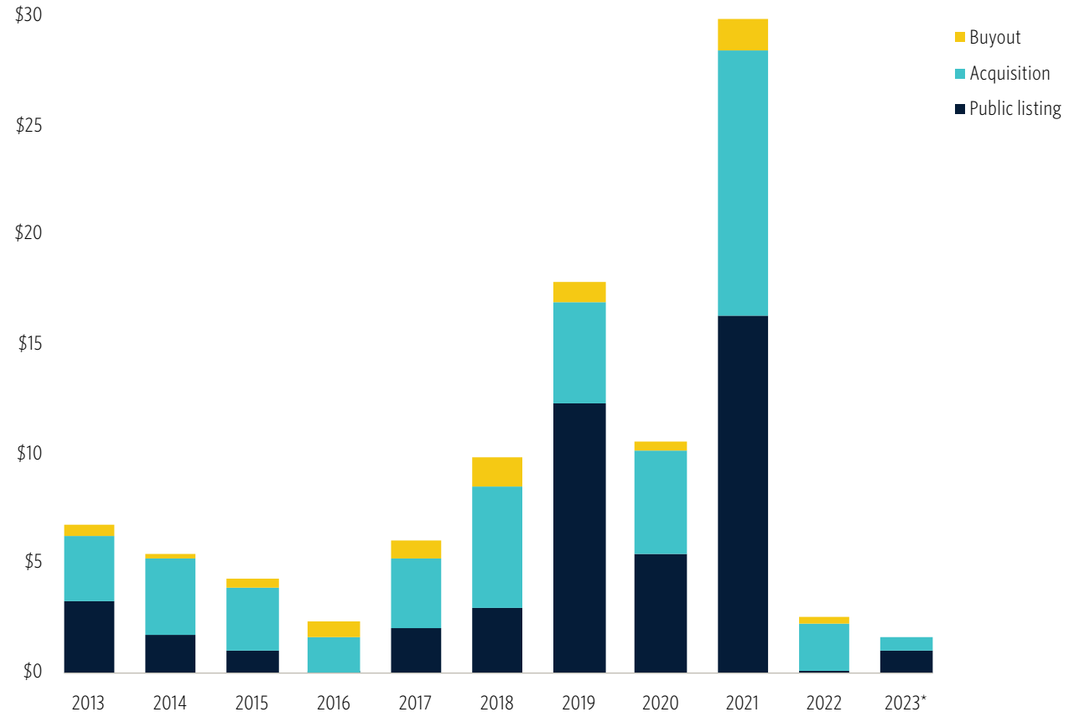
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Infosec VC deal count by stage



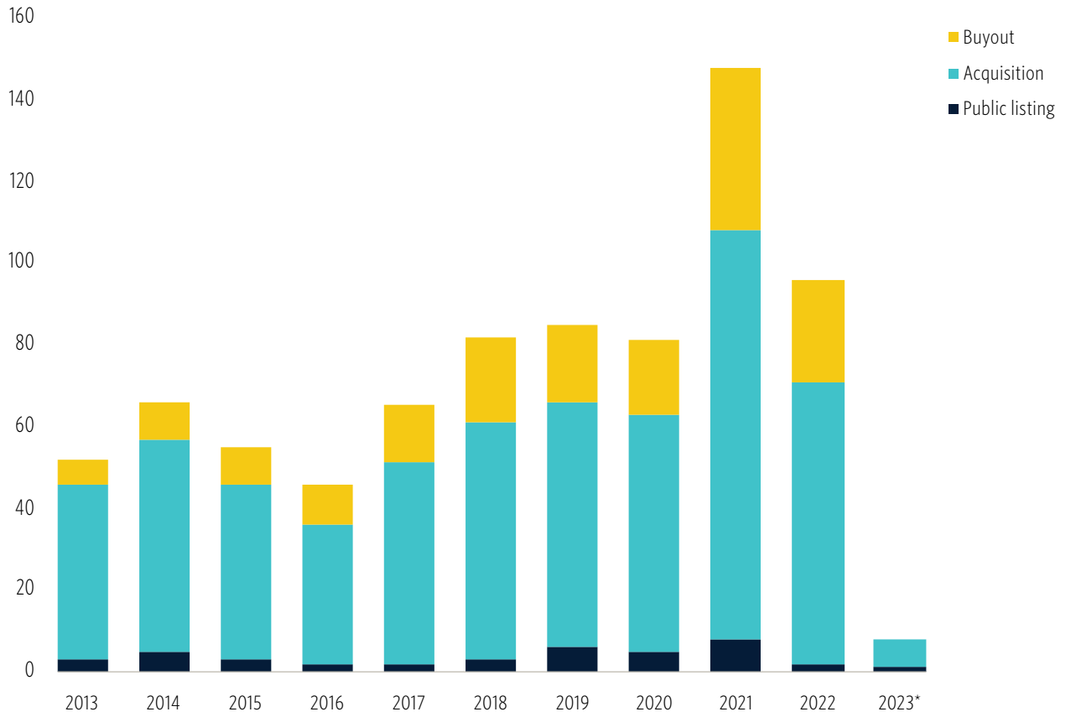
Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Infosec VC exit value ($B) by type



Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

Infosec VC exit count by type



Source: PitchBook • Geography: North America & Europe • *As of March 31, 2023

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.

PitchBook Data, Inc.

John Gabbert Founder, CEO

Nizar Tarhuni Vice President, Institutional Research and Editorial

Paul Condra Head of Emerging Technology Research

Additional research

Eric Bellomo
eric.bellomo@pitchbook.com
Gaming
E-Commerce

Brendan Burke
brendan.burke@pitchbook.com
Internet of Things
Information Security
Artificial Intelligence & Machine Learning

Aaron DeGagne
aaron.degagne@pitchbook.com
Medtech
Digital Health

Alex Frederick
alex.frederick@pitchbook.com
Agtech
Foodtech

Jonathan Geurkink
jonathan.geurkink@pitchbook.com
Supply Chain Tech
Mobility Tech

Derek Hernandez
derek.hernandez@pitchbook.com
Enterprise SaaS

Ali Javaheri
ali.javaheri@pitchbook.com
Emerging Spaces

Robert Le
robert.le@pitchbook.com
Insurtech
Crypto

John MacDonagh
john.macdonagh@pitchbook.com
Carbon & Emissions Tech
Clean Energy Tech

Rebecca Springer
rebecca.springer@pitchbook.com
Healthcare Services
Healthcare IT

Rudy Yang
rudy.yang@pitchbook.com
Enterprise Fintech
Retail Fintech

Coming soon
Biotech
Pharmatech