2023

CISO

Survival Guide

Emerging Trends From the Startup Landscape

Presented by cisco investments

in partnership with FORGEPOINT NIGHTDRAGON TEAM8™

Table of Contents

Foreward

For today's enterprises, the constant battle of identifying and preventing attacks from anywhere and everywhere can seem nearly impossible to overcome. With the types of attacks ever expanding and the number of security solutions growing by the hour, CISOs and security leaders are eager to understand what is around the corner and how to prepare.

In order to help with the often arduous task of keeping up with the evolving dynamics of cybersecurity, **Cisco Investments** and our partners **Forgepoint Capital**, **NightDragon**, and **Team8** have joined forces to issue this comprehensive guide. The **2023 CISO Survival Guide Report** explores the possible future of the cybersecurity industry as it pertains to identity management, data protection, software supply chain integrity, and ongoing cloud migration.

The report features **one-on-one CISO interviews, insights on emerging innovation trends, and a specially commissioned Foundry Research report** with 100 IT security decision-makers from over 15 different industries. What we wanted were the fundamental industry pain points. What we got were our marching orders for the year ahead.

We are grateful to Foundry Research, an IDG Inc. company, for their comprehensive investigative efforts. We thank our venture capital partners, as well as all the CISOs and security leaders, who so generously contributed their time, objectivity, and insights. And lastly, we thank **all the dauntless pioneers we meet in this space every day** – the startups that inspire us and take us to the next level together.

Cisco Investments and our partners are excited to release the **2023 CISO Survival Guide: Emerging Trends from the Startup Landscape.**

We hope you find this insightful.

Happy exploring.

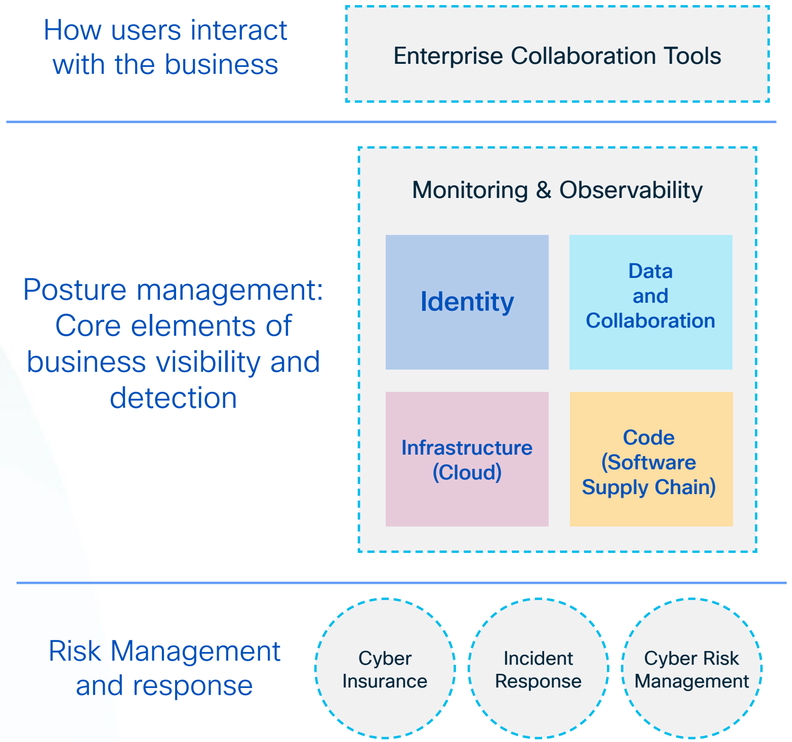
Securing the Enterprise

Enterprises today face an interesting dilemma: on one hand, they rely on connectedness to enable productivity and growth, but on the other, this very connectedness invites breach contagion. The two are inversely related, forcing organizations to walk a fine line between boom and backlash. Attack corridors stemming from infrastructure, applications, users, identities, and data besiege the modern workplace, while API entrenchment exacerbates the attack surface. Yet, this is the cost of progress.

Unwilling to accept that innovation must mean insecurity, four of the cybersecurity industry's most active investors plumbed the minds of CISOs in the trenches to discover how increasing shared collaboration could also decrease shared risk and technical debt in 2023.

Cisco Investments, **Forgepoint Capital, NightDragon**, and **Team8** collaborated on a robust qualitative and quantitative research investigation to uncover how modern enterprises should be secured given the uniquely evolving cyber challenges.

The modern enterprise is borderless and requires tailored security controls. In collaboration with leading CISOs, we co-developed a simple framework for understanding how modern enterprises can be effectively secured today:



- Employees use modern enterprise collaboration tools to gain universal access to resources and are no longer bound to a location or a device.
- CISOs need to define the security posture of **identities, data,** and **code (Software Supply Chain)** that are now distributed across a hybrid infrastructure (on prem, public cloud, private cloud, SaaS, PaaS, etc.).
- In addition to defining the security posture of these elements, CISOs need to have a way to **monitor** and **measure** the effectiveness of these controls to mitigate cybersecurity risk.
- Lastly, organizations need a holistic approach to cyber risk management including cyber insurance and incident response.

Executive Summary

- **The lack of a unified platform across Identity Access Management (IAM), Identity Governance and Administration (IGA), and Privileged Access Management (PAM) results in a balkanized Identity topology within enterprises.** CISOs today define this as a critical pain point and a desired focus for future innovation. In the present state, manual tuning is required to tailor these solutions to customer environments, increasing friction and adding cycles at a time when increasing security risks demand greater efficiency.
- **Cloud Infrastructure Entitlements Management (CIEM) is gradually gaining prominence as a spend priority for customers.** Many are actively leveraging Cloud Security Providers' (CSP) native offerings.
- **Acronyms are proving to be a bane.** CISOs are voicing their frustration with an unchecked proliferation of acronyms. Every week sees the creation of a new Identity category/acronym without an accompanying use case or technological differentiation. This trend imposes cycles for CISOs to vet and unpack these purportedly new categories only for them to discover they are a rehash of existing solutions. A more welcome approach would focus on core use cases (such as adaptive application access, privileged Identity, or developer access) and demonstrate differentiation on priority axes (such as ease of deployment, breadth of coverage, rich integrations, etc.).

cisco investments

Identity
Introduction

In an era of expanding technologies, proliferating applications, and decentralizing work lows, the issue of Identity management has never been more business critical. Organizations today operate with an unprecedented amount of data in play. However, that reality comes with the responsibility to always secure access to that data.

Organizations need help finding their footing on the Identity path as the digital enterprise evolves. Finding **hybrid-compatible solutions, securing SaaS, and retooling legacy architectures** to the pace of passwordless platforms are just a few of the challenges they face. Consolidating vendors and balancing the cost of unified solutions with the tradeoff of manageable oversight are other considerations companies must bear going forward.

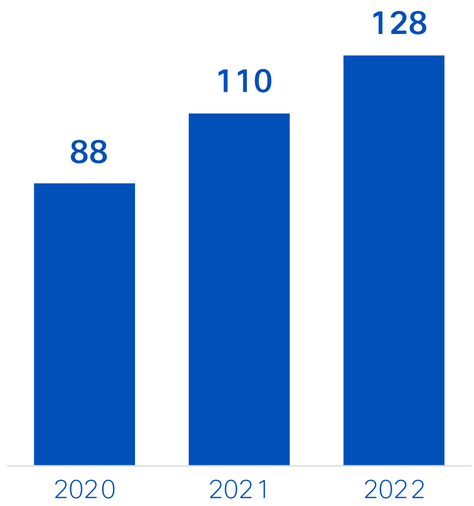
Identity is part of an ongoing trend cycle, and 2023 finds the industry engrossed in a number of innovations.

- Zero trust is forging ahead with new initiatives in passwordless identification
- Continuous access management is surging to the forefront of operational needs
- New technologies are arising as inquisitive startups build solutions to new problems

Cisco invests across a wide range of Identity-related assets, including Cloud, Identity Governance and Administration (IGA), Privileged Access Management (PAM), SaaS apps, Active Directory, and Identity Threat Detection and Response (ITDR). The net yield of our partnership with emerging companies within these fields is a keener scope into the Identity security problems of today, and a firmer grasp on the technologies required to fix them tomorrow. These include solutions that provide cloud-native access for the hybrid worker, hardened privilege identities, continuous access within SaaS apps, and more.

The overall impact of these changes is a push toward stronger authentication as enterprises realize they can't take anything for granted. What was sufficient security for on-premises architectures is not enough in the cloud. What was once protected by an entryway at the perimeter now requires continuous authentication at each checkpoint. And what was once 'secured' by assumption is now guarded by the principle of least privilege.

Identity Security Financing Transactions (2020-2022)



Source: Pitchbook, Momentum Partners

Identity

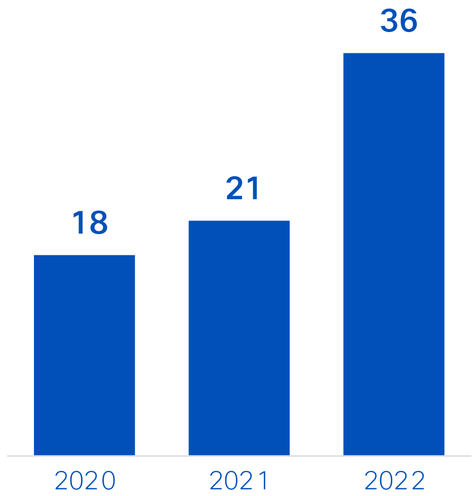
(Introduction continued)

The enterprise landscape is changing, and so is the Identity environment that underpins it. Identity security measures doggedly follow that trend, and this year's report provides a cross-sampling of the many ways those evolutions take place.

Continuous, future-proof Identity management is a journey, and CISOs are at the helm. We hope the knowledge CISOs glean from this guide will help to contextualize Identity within the broader expanse of ultimate security goals.

As digital enterprises expand in scope and size, the challenge of securing all assets via the Identities that access them becomes an increasingly complex problem. Through discovering, supporting, and partnering with emerging technology startups in this space and sharing what is found, Cisco seeks proactive ways to deliver on its promise: If it's connected, it's protected.

Identity Security M&A Transactions (2020-2022)



Source: Pitchbook, Momentum Partners

cisco investments

Identity
Startup Landscape

The Identity landscape is a diverse ecosystem with emerging technologies and exciting innovations. **Cisco Investments** purposefully invests in and supports best-in-class companies that provide strong Identity security, including **AppOmni, Oort** and **Elevate Security**.

These companies and their peers are shaping the intersection of Identity (role), users, and policy. As the industry trends toward a more simplified, frictionless, and continuous approach, these startups show us what is possible.

Together, they are advancing innovation across the Identity and zero-trust landscape in the areas of passwordless and continuous access, converging authentication/governance/privileged access, end-to-end multi-cloud Identity detection and response, continuous SaaS-app security, account takeover and session hijack prevention, active and cloud directory security, to name a few.

Cloud, DevOps, and CIAM

Provides cloud native access and policy for the hybrid workforce and consumer

1KOSMOS
Opal
CLOUDENTITY
ORY
BEYOND IDENTITY
SILVERFORT
ELISITY
STRATA
ConductorOne
STYTCH
CURITY
transmit security
Magic
TRUSONA
AUTOTIX

Modern IGA

Delivers a modern Identity, Governance, and Compliance solution

SAVIYNT
BalkanID
SECURENDS

PAM & CIEM

Hardens privileged identities and cloud infrastructure entitlements

ermetic
britive
Procyon
SPHERE
sonraí SECURITY

SaaS-app and CTA

Secures access to and within SaaS Apps and enables Continuous Trusted Access

AppOmni
Control.
ADAPTIVE SHIELD
grip
OBSIDIAN
Island

End-to-End ITDR

Identifies risky users and detects Identity threats and vulnerabilities

Constella INTELLIGENCE
QOMPLX:
AUTHMIND
Authomize
Elevate Security
OORT

Cloud & Active Directory

Provides bespoke security for on-premises and cloud directory

jumpcloud
semperis

Identity
What We're Hearing from CISOs

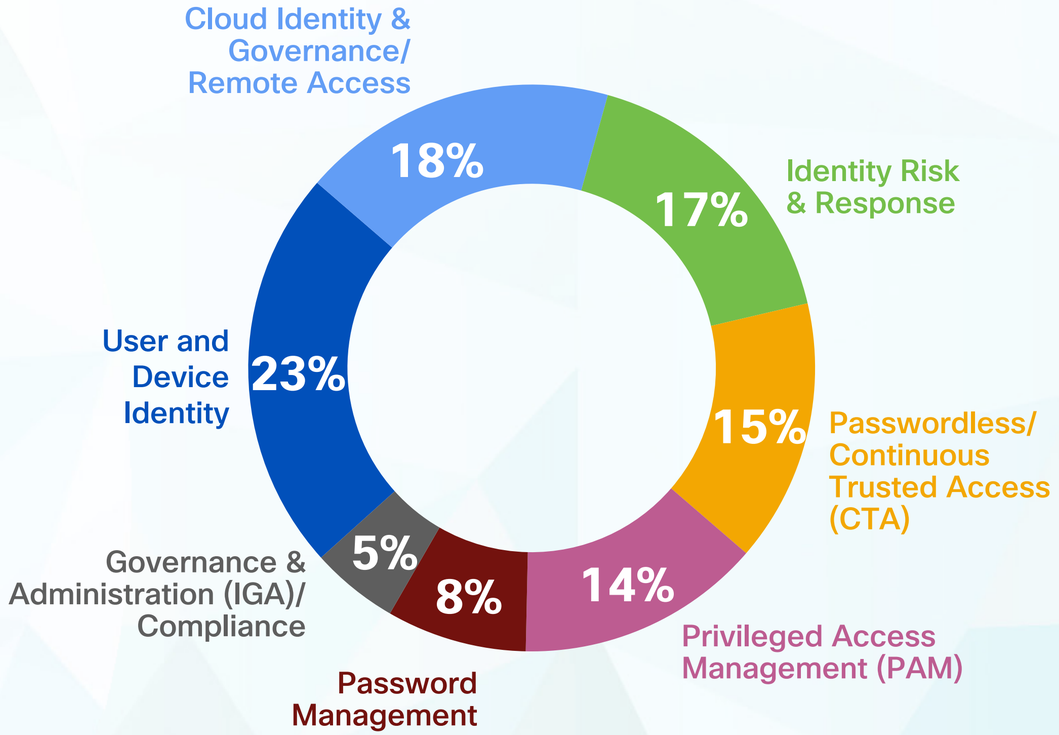
85% Identity is a Critical or High Priority

IT decision-makers prioritize Identity and Access management investments more highly than other security solutions.

23% User and Device Identity management is a top priority, within Identity

However, a notable level of even distribution in spending priorities across Identity, suggests the need for a comprehensive approach to overall Identity management strategies.

Top Spending Priorities Within Identity



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Identity

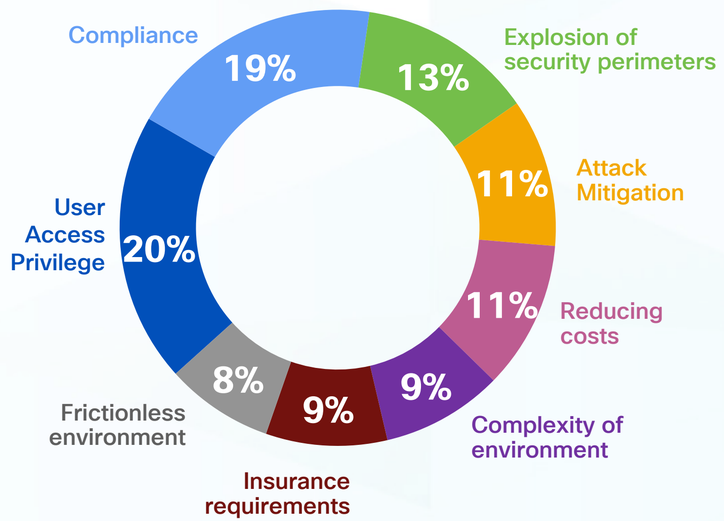
(What We're Hearing from CISOs continued)

39%

User Access Privilege and Compliance drive investment

Additionally, recognition of security perimeter explosion (13%) as a driving factor highlights the growing complexity of modern threat landscapes and the need for robust Identity solutions.

Top Motivators Driving Identity Investment Plans

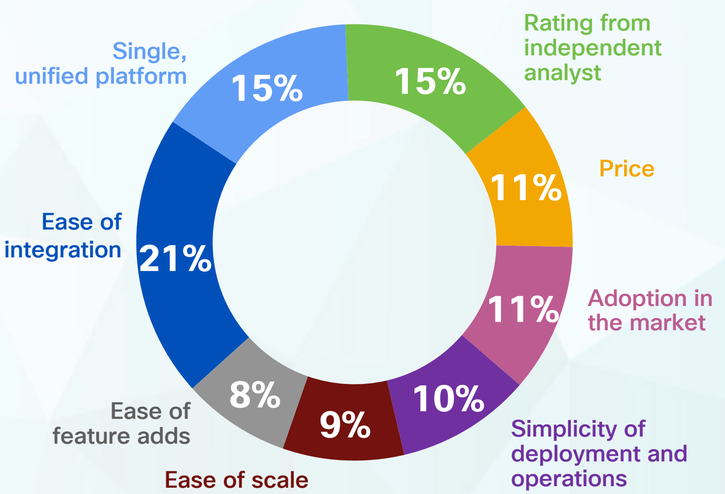


21%

Ease of integration is key

In addition to seeking solutions that offer seamless integration, other top considerations include having a single unified platform and ratings from an independent analyst.

Top Criteria for Selecting a Modern Next-Gen Identity Platform



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Identity

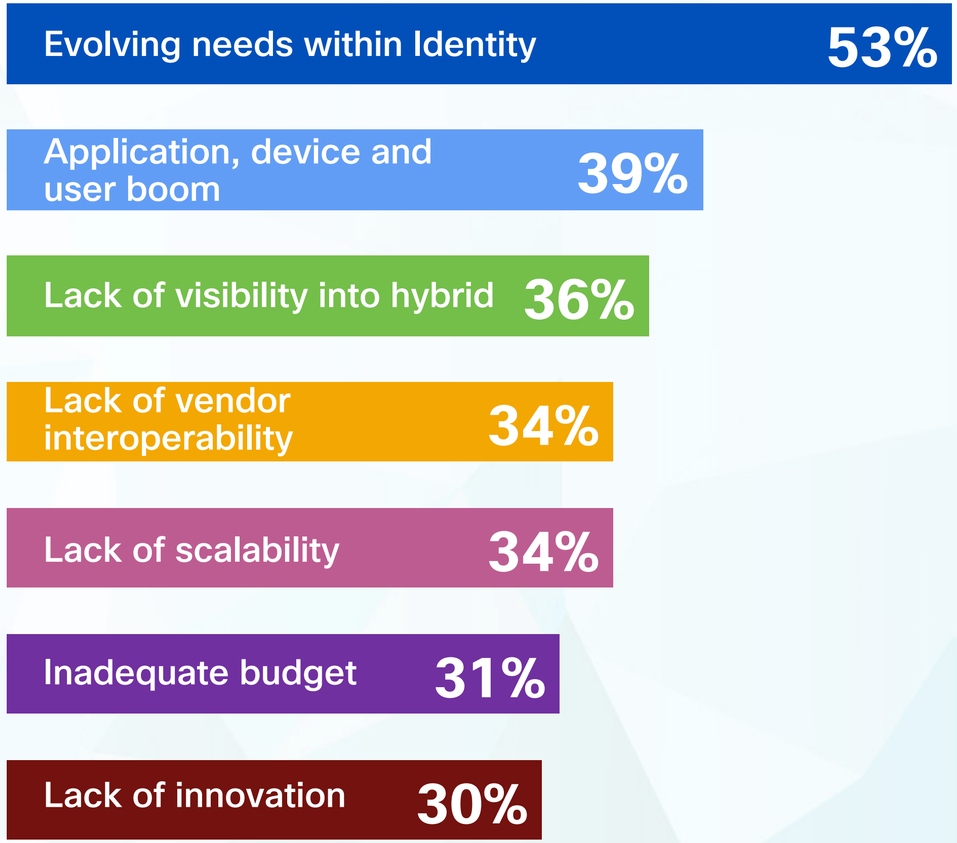
(What We're Hearing from CISOs continued)

53%

Evolving Identity needs is a challenge

Additionally, more than one-third cite the exponential increase in applications, devices, and users as a challenge for Identity solutions, indicating the increasing complexity of managing access for a growing number of users.

Top Challenges in Meeting Access and Management Goals



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Identity

What This Means for CISOs

What Your Peers Are Saying

Don’t be afraid of new technologies

Don’t be afraid of jumping into new security platforms. It’s easy to fear downtime, a learning curve, or just the pain of transition, but the progression toward zero-trust initiatives is often more user-friendly than you think.

> “What I’ve seen with new technologies is that everyone is afraid of them, but when you start putting them in place, there’s much less to be afraid of than CISOs initially thought. So, I think that the fear of adoption is much higher than the actual noise around adopting it.”
>
> – Larry Lidz
> CX Cloud CISO, **Cisco**

Look beyond the entry points

Being able to track users and devices as they navigate the modern digital enterprise is paramount to securing those navigations later. When it comes to Identity, the full picture is required: Who is using what, when, and where across the enterprise? It is important to be able to distinguish credentialed employees accessing a work SaaS app from their own device, from an attacker using stolen credentials. Only through understanding the holistic health of your Identity landscape can proper remediations take place.

> “We need to understand the full story, and part of that story takes place under the users’ credentials. Security teams need to understand what actions are being taken. What pathways from account to account are being exploited? Being able to understand that full picture is paramount.”
>
> – Paul Curylo
> CISO, **Inova Health**

Identity

(What This Means for CISOs continued)

Less is more with zero trust

When the problem is steeped in complexity, the solution must be simplicity. While niche products and vendors serve a specific purpose, CISOs increasingly want one tool to consolidate the disparate aspects of Identity — such as IAM, end-to-end ITDR, modern IGA, PAM, and CIEM — and make continuous authentication simpler in the process. With the right combination of vendors and technologies, zero-trust architecture does not have to be complicated to be effective.

> “To me, complexity is the enemy of security. Leaning on a smaller number of vendors and keeping the architecture as simple as you can to operate it, and still meet your security controls and capabilities, is preferred. I also hope and expect, in the future, to leverage more artificial intelligence in innovating in the IAM space to help overcome the challenges of complexity within your organizational structures and overall lack of standardization.”
>
> – Duc Lai
> CISO, **University of Maryland Medical System**

Don’t forget about the non-negotiables

If zero-trust solutions aren’t streamlined and optimized for highly regulated industries, they will be forced to take a back seat to compliance and workability. While zero trust is seen as an ideal solution, regulatory requirements and operability are necessary. IAM solutions need to be able to integrate and keep pace with industry non-negotiables.

> “For me, zero trust has to leverage my current existing Identity store process. It must work with the governance and compliance requirements and let me leverage that. [And] if it makes it harder on the user, it will get zero buy-ins.”
>
> – Alan Berry
> CISO, **Centene Corporation**

Identity

(What This Means for CISOs continued)

Innovation is still ongoing

Zero-trust solutions are far from complete. While extensive, they are not exhaustive, and work still remains to be done to integrate critical security goals with existing on-premises and legacy methodologies. Thankfully, these problems have not gone unnoticed. We see more innovation on the horizon and this underscores the importance of evaluating startups and emerging technologies regularly.

> “From an IAM perspective, [organizations] still face challenges. Right now, there are a lot of rudimentary and manual solutions for provisioning and un-provisioning, managing permissions between users and entities, and even between machine to machine. These operations can be costly for organizations to give the right access to the right person at the right time, which is the goal of IAM. We need more innovation in this space. I’m interested in anything that provides or supports an auto-configuration model or AI assistance for humans.”
>
> – Jean-Sebastien Pilon
> VP of Security Operations, **Desjardins**

Identity

Bobby Singh
CISO, Toronto Stock Exchange

One CISO's Identity Management Journey

Bobby Singh is the CISO at the Toronto Stock Exchange, the 10th largest exchange in the world and the third largest in North America based on market capitalization. He shares how TSX navigates the changing Identity landscape in a hybrid environment where appetite for innovation is offset by the regulatory demands of the finance industry.

As the Chief Information Security Officer (CISO) of the Toronto Stock Exchange, like many other CISOs, I find myself navigating the complex realm where on-premises and cloud-based migrations intersect. This is a critical junction where choosing the right Identity solution can be a daunting task, especially with a multitude of vendors vying for attention. Being part of a well-established industry adds an extra layer of complexity, as legacy architectures are deeply ingrained and non-negotiable. And when you factor in the stringent regulations surrounding a stock exchange, the challenges I face are further amplified.

IDENTITY LANDSCAPE CHALLENGES

The Identity Management industry has seen a lot of progress, but I believe it has a long way to go. The glut of vendors in the space — literally dozens that often provide similar services — is itself, challenging. As an example, we use three different Identity solutions at TSX to cover Multifactor Authentication (MFA), Identity Governance and Administration (IGA) and Privileged Access Management (PAM). Additionally, when it comes to deployment, many Identity solutions require a very heavy lift and steep learning curve for teams. These behemoths leave much to be desired when it comes to management and contextualization.

The Identity-related challenges facing many large hybrid companies are amplified in an exchange. As a major banking center, we see a huge amount of data flowing in and out. We parse much of that data into the cloud for reporting purposes, historical analysis, and so on, and we use a lot of new technologies in that space. From an Identity viewpoint, SaaS and other cloud-based applications are easier to manage. They're written in a modern language with readily available APIs. At the same time, we've been around for a long time. The Toronto Stock Exchange opened in 1861 and our on-prem environment includes proprietary monolithic applications that were set up decades ago.

For a CISO, this presents a unique challenge: Do I build two different Identity stacks, one for SaaS and the cloud, and another for on-prem? There are solutions on the market that claim to do both, but when you look under the hood the reality is they do a much better job on the SaaS side than they do with your legacy applications in the on-prem environment.

HOW CISOS CAN NAVIGATE THE IDENTITY LANDSCAPE

This kind of technical debt impacts how aggressively CISOs can transition from legacy systems to modern zero-trust architectures. At TSX, we try to do a yearly assessment where we ask ourselves if we should modernize an application, look at a different solution, or merge it with something else. Sometimes you can't move as fast as you want to. You can't just rip off the legacy solutions like a Band-Aid and embrace the modern zero-trust architecture, because some of those monolithic on-premises applications are still needed and replacing them is too costly.

Identity

(One CISO's Identity Management Journey continued)

A lot of CISOs struggle with this. In some cases, they may have to carve out areas that won't have zero trust — areas that they manage separately, perhaps with an in-house, customized Identity solution, because of the technology they have in place for specific reasons. They simply don't have the luxury of creating an API that can manage it. That said, we've got to get to a point where it's more simplified for the end user. Technology and innovation are far enough along now that we can't use the excuses that we did 10 or 20 years ago when we could say the technology isn't there yet. That's just not true anymore.

Take passwordless authentication. Passwords were a reactive response to the cybersecurity needs of 30 years ago, but the future demands a better, more secure solution. Passwordless authentication aligns well with a zero-trust framework, simplifying access from any device, anywhere and enhancing the user experience. Our phones are always with us and have become an extension of our bodies. Whether we're logging in on our phone or another device, the phone, in a sense, is the password. There's no reason to have a separate password. This kind of device-centric authentication, along with cryptographic techniques, establishes trust based on the device itself, which reduces reliance on traditional passwords and enhances overall security.

It's time for us to leave the password era behind. I've got to be able to have an environment where any device, from anywhere, can access the organization, with no passwords along the way.

BEST PRACTICES AND LESSONS LEARNED

Take a strategic approach to zero-trust implementation. Before embarking on the zero-trust journey, be sure to do your homework. You can't just say, 'I'm going to do zero trust.' Take a step back and get a thorough understanding of the organization's environment. Conduct proper inventory assessments and build architectural principles early on. We first started talking about zero trust 10 years ago, but we only started our zero-trust implementation about one year ago. In shopping for Identity solutions, we made sure they would help us on our zero-trust journey. So, if you want to buy a solution today, make sure it has X, Y, and Z even if you're not going to use those capabilities immediately. You know you'll use them eventually, and if you get them now, you'll avoid a situation down the road where you suddenly must make significant investments or changes to get on the zero-trust journey.

Identity management platforms need to be hybrid compatible. At TSX, our focus on Identity management is deeply rooted in our hybrid environment. We recognize the significance of maintaining an agile and scalable Identity management posture. It is essential for us to strike a balance that caters to our legacy architectures while embracing the possibilities of the future. Network-based IAM tools are no longer suitable, yet fully cloud-based platforms often do not align with where

Identity

(One CISO's Identity Management Journey continued)

many organizations are today. It's important to seek solutions that bridge these two realms, prioritizing finding platforms that can seamlessly serve on-premises assets while enabling to ability to expand and leverage the cloud as you grow.

Partner with a select few vendors. Rather than put all our eggs in one basket, my preference is to partner with two or three key vendors who can provide solutions aligned with our zero-trust goals. Managing multiple vendors can be challenging and time-consuming. Selecting a few strategic vendors who can address most of your Identity management needs simplifies integration, reduces complexity, and enhances cost-effectiveness and overall efficiency. With so many vendors in the Identity management space, it's also essential to conduct comprehensive research and evaluations to find the most suitable solutions for your organization's specific requirements. Finally, consider a trusted partner for long-term collaboration as this can bring stability and continuity to your Identity management strategy.

Stay updated with industry trends. Stay informed about the latest advancements to ensure your Identity management strategy remains relevant and future-proof. That includes staying updated about emerging technologies, such as quantum computing, and their potential impact on traditional password complexity. Explore stronger cryptographic solutions, such as public key infrastructure, to ensure long-term security resilience against evolving threats. When it comes to scoping out emerging tech, my strategy is to begin with the end in mind. It's important you don't pick now and then try to make them bend to your vision later. This takes a lot of foreplaning and the best possible research on new technology solutions before you buy.

Executive Summary

- **CISOs are no longer tasked with security alone.** They are also now responsible for securely enabling overall collaboration and business operations. **Gartner** notes that 64% of board directors increasingly emphasize digital assets, and 88% recognize that cybersecurity poses a risk to the business, creating the perfect conditions for CISO leadership.
- **Controlling access to information remains the crux of cybersecurity,** with Data Identity and Privileged Access Management (PAM) being the top priority for CISOs. The global PAM solutions market is expected to increase from $2.7 million in 2020 to nearly $20 million in 2030, registering a 23.1% CAGR.
- **Data Access Control and Data Loss Prevention** are the top Data Security controls among CISOs.

Data and Collaboration

FORGEPOINT

Data and Collaboration

Introduction

In the digital era, enterprises struggle to extract value from large amounts of data. The modern CISO is tasked with being both gatekeeper and enabler, balancing data protection and data use.

Security leaders break down the vast data landscape into comprehensible focus areas to manage the load. Facilitating the secure, effective use of data can be distilled into **four pillars: data collaboration, data reliability, data privacy management, and data protection.**

While only some pillars are within the CISO budget, all are required to securely enable the modern enterprise.

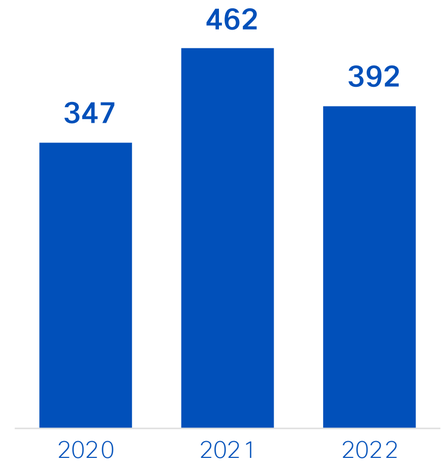
Siloed data with antiquated access controls complicates data governance and limits **data collaboration**. Technologies like data catalogs allow all businesses to locate and apply data governance controls on distributed data. In contrast, data collaboration tools look to eliminate the bottleneck of data access and to enable productivity without compromising Data Security.

Duplicated data sprawled throughout the enterprise often cannot be trusted as an upstream source for data-driven decisions. **Data reliability** — ensuring data is accurate and usable — is essential for both operational decision-making and advanced analytics.

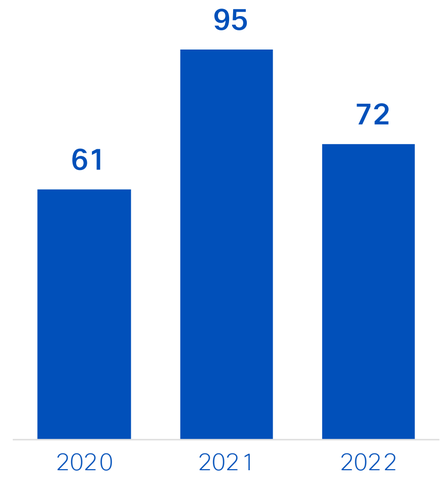
Data privacy regulations restrict how companies can collect, maintain, and analyze sensitive data. For effective **data privacy management**, enterprises must have governance, risk, and compliance controls to adhere to data privacy regulations and enable analytics on sensitive data.

In the modern extended enterprise, data is used by distributed teams across hybrid infrastructure, further obfuscating where your sensitive data is, where it is going, and who has access to it. **Data protection** means enterprises can find, categorize, and remediate access so that all data best serve their intended purpose.

Data and Collaboration Financing Transactions (2020-2022)



Data and Collaboration M&A Transactions (2020-2022)



Source: Pitchbook, Momentum Partners

cisco investments

Data and Collaboration
Startup Landscape

Over the last few years, numerous startups have stepped up to address data collaboration and security. **Forgepoint Capital** supports active players in this space, such as **Cinchy**, **Cyberhaven**, **Symmetry Systems**, **Truera**, and **WireWheel**.

Securing data access is securing the modern enterprise. The emerging startups dedicated to this endeavor are pushing advancements in

Data Collaboration, Data Reliability, Data Privacy Management, and Data Protection.

From our conversations with CISOs and technology leaders, we are encouraged to find that data collaboration, and the security of that exchange is increasingly a major priority — and that emerging technology companies are rising to meet related needs and challenges.

Data Collaboration

Enabling teamwork and productivity in the digital era (via hybrid, SaaS, multi-cloud)

DATA CATALOG

- Alation
- data.world
- Collibra
- stemma

DATA COLLABORATION

- cinchy
- habu
- Deep.BI
- tellius

Data Reliability

Ensuring data is accurate and usable, and produces high fidelity insights

DATA QUALITY

- Anomalo
- great expectations
- lightup
- MONTE CARLO
- SODA
- acceldata

ML / AI QUALITY

- arize
- fiddler
- Arthur
- truera

Data Privacy Management

Governance, risk, and compliance controls to adhere with data privacy regulations and enable analytics

DATA SUBJECT ACCESS RIGHTS

- BigID
- ethyca
- OneTrust
- Transcend
- wirewheel
- DATAGRAIL
- exterro
- securiti

DATA ENCRYPTION

- baffle
- Cape Privacy
- Duality
- ENVEIL
- Opaque systems

CONFIDENTIAL COMPUTING

- anjuna
- Fortanix
- EDGELESS SYSTEMS

Data Protection

Find and protect sensitive data

DATA SECURITY POSTURE MGMT

- SYMMETRY SYSTEMS
- securiti
- cyera
- MMUTA

DPL / DATA DETECTION AND RESPONSE

- CODE42
- cyberhaven
- Dig Security

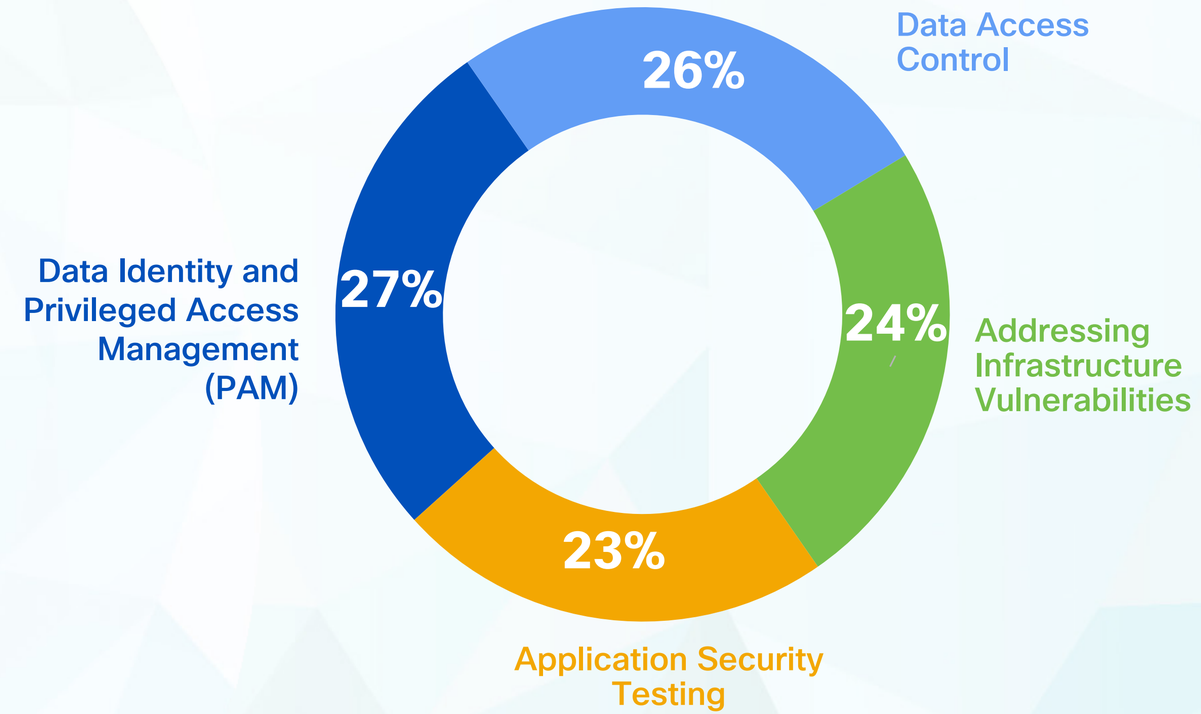
Data and Collaboration

What We're Hearing from CISOs

27% Data Identity and Privileged Access Management (PAM) top the spending list

When asked about their top security hygiene spending priority in 2023, most CISOs identified Data Identity and Privileged Access Management (27%) as the essential spending priority.

Top Security Hygiene Spending Priorities



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Data and Collaboration

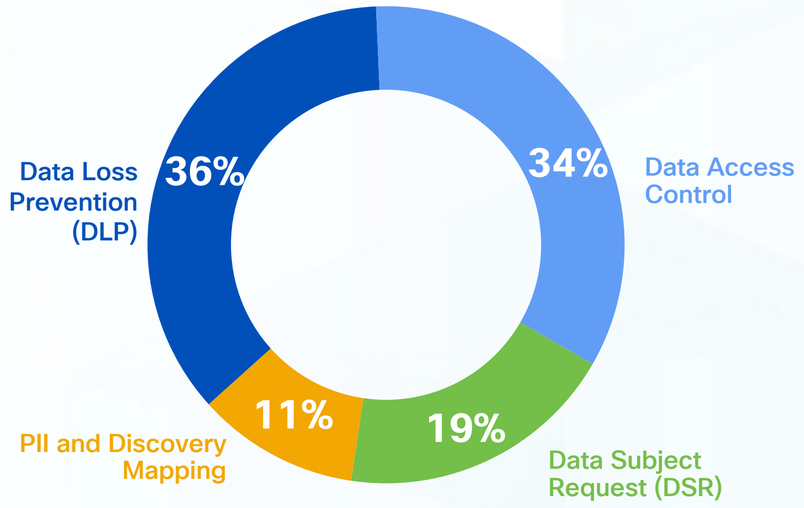
(What We're Hearing from CISOs continued)

70%

Data Loss Prevention and Data Access Control remain key priorities

CISOs place nearly equal importance on safeguarding sensitive data from loss, as they do maintaining control over data access. When asked about top data security focus, 70% of CISOs identified DLP and Data Access Control.

Top Data Security Priorities

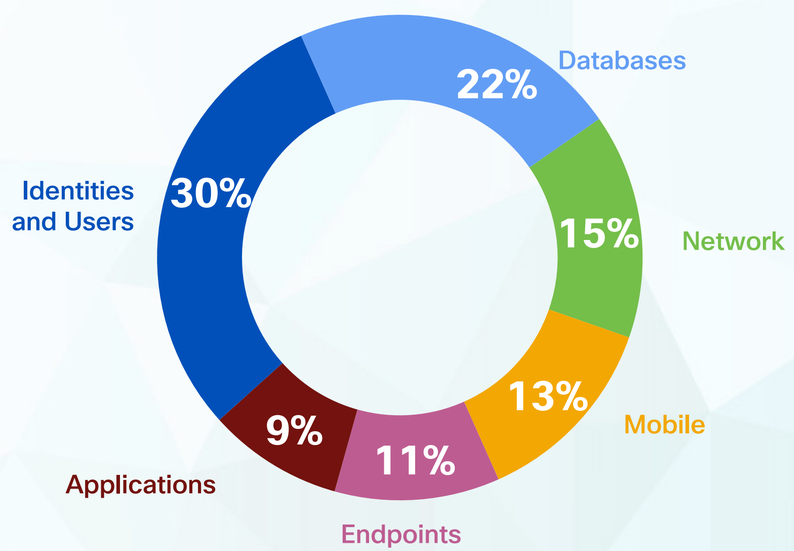


22%

Databases prove challenging to secure

When asked about the most difficult access control points to manage and protect, 22% of CISOs selected databases.

Most Difficult Assets to Protect and Manage



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Data and Collaboration

What CISOs are Saying

Data spans across Identity, infrastructure, and applications, thus requiring a team effort to control.

Data Security cannot hinder availability

The most straightforward cybersecurity building block in the book is the CIA triad (Confidentiality, Integrity, and Availability). Information is nothing without being accessible. It would be easy to defend Data Security in a vacuum. However, modern security solutions must respect modern applications' advancements in the ease of use and convenience while still securing sensitive assets. CISOs must strike a balance between locking down data and enabling its use.

> “Cybersecurity’s fundamental purpose is to control risk to information. But this must be balanced with the organization's ability to use the information, and ideally enable its efficient usage. After all, we are here to support the company’s success.”
>
> – George Webster
> Chief Security Architect, **HSBC**

The CISO as a business enabler

CISOs are increasingly seen as the hub of a critical wheel, rather than an oft-forgotten spoke. As C-suite executives and investors recognize that secure and fast innovation is a critical business driver amid a climate of increased regulation and corporate accountability, CISOs are expanding their leadership roles. Consequently, the modern CISO should no longer be seen as the naysayer but as the business enabler – advancing progress and productivity through secure, timely access to the right data and information by the right users and teams.

> “Security must not be seen as an impediment to the business ... security should always seek to safely enable the business. ‘How can we do this securely?’ is a much more effective and respected response than simply no.”
>
> – Yonesy Núñez
> Former CISO, **Jack Henry**

Data and Collaboration

Diego Souza
Global CISO, Cummins

One CISO's Data and Collaboration Journey

Diego Souza is the Global CISO at Cummins, Inc., a leading multinational power technology leader that specializes in diesel and alternative fuel engines and generators, and related components and technology. He shares perspective on the company's approach to data and collaboration.

Given the ever-evolving cybersecurity threats and the frequent occurrence of data breaches, it is imperative that organizations prioritize the safeguarding of sensitive data and information.

DATA AND COLLABORATION CHALLENGES AND OPPORTUNITIES

In today's global and connected business environment, there are numerous challenges that exist in data security and collaboration. As a multibillion dollar global power leader that manufactures diesel, natural gas, hybrid and electrified power engines, filtration, and generators, we serve customers in more than 190 countries through a network of 500+ distributors and 7500+ dealer locations. It can be difficult to ensure that sensitive information is protected from potential data leaks. Additionally, the emergence of generative AI and GPT technologies has brought about new concerns regarding data privacy and security. Furthermore, changing workforce dynamics can also have an impact on collaboration and information sharing within an organization. These operational issues must be carefully monitored to ensure that data security and collaboration are maintained at all times.

In addition to the challenges mentioned above, there are also plenty of data and collaboration opportunities for organizations in today's business landscape. For instance, the rise of remote work prompted by COVID has allowed for greater flexibility and cost savings industry-wide – and ushered in a host of enterprise solutions that help gather, process, and synthesize data to make better decisions. At Cummins, advancements in technology like predictive maintenance, over-the-air updates, and remote monitoring and diagnostics have enabled our teams to optimize performance while streamlining our operations and improving productivity. With the right strategies in place, businesses can take advantage of external and internal innovation opportunities while ensuring that data quality, security, and collaboration remain a top priority.

HOW CISOS CAN SECURE DATA WHILE ENABLING INNOVATION AND PRODUCTIVITY

CISOs need to balance the need to secure data with the need to enable innovation and productivity. They can do this by embracing a risk-based approach to security, using security automation and orchestration, adopting a zero-trust security model, and building a culture of security awareness and responsibility. They should also work closely with the business, be open to new technologies, and communicate effectively with stakeholders.

Emerging technologies such as AI, ML, blockchain, quantum computing, and 5G

Data and Collaboration

(One CISO's Data and Collaboration Journey continued)

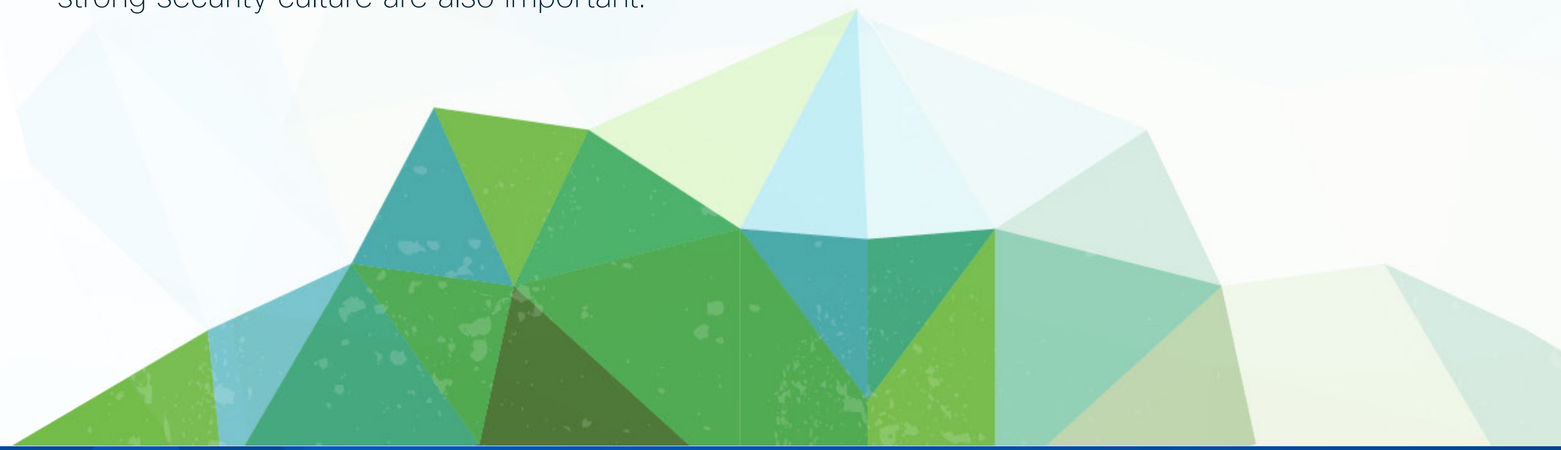
can help CISOs to protect organizations and data in a number of ways. These technologies can be used to automate security tasks, analyze data, store and track data, and improve the performance of security solutions. In addition, cloud computing, microsegmentation, and zero-trust security can also help to improve the security of organizations. However, it is important to note that no single technology can provide complete security. CISOs need to adopt a layered security approach that combines a variety of technologies to create a comprehensive security posture.

LESSONS LEARNED

As you develop, implement, and refine your cybersecurity strategy, it's important to keep a few best practices in mind. First, understand your organization's risk profile so that you can tailor your security strategy to your specific needs. Involve all stakeholders, including business, IT, and security teams, to ensure alignment with your overall goals. Use a risk-based approach to focus on the threats that pose the most significant risks. Implement security controls such as firewalls, intrusion detection systems, and access control lists, and monitor and test them regularly. Train your employees on cybersecurity best practices to identify and report suspicious activity.

Avoid ignoring the human factor, as human error is often the cause of cyberattacks. Don't be afraid to change your cybersecurity strategy as the threat landscape evolves, and ensure compliance with applicable regulations. Consider using a cybersecurity framework and seeking professional help if necessary. Stay up to date on the latest threats and leverage peer CISO networks to share and learn as much as possible.

CISOs need safeguards and legal protections to do their job effectively. This includes immunity from liability, access to all data, authority to make decisions without too much interference, and privacy protections. Ongoing training, support from management, and a strong security culture are also important.



Executive Summary

- As agile DevOps create a more rapid software development lifecycle, **enterprise security will only be as strong as its weakest link: the software supply chain**. However, there is an encouraging response to this industry's Achilles heel. Seven out of 10 respondents prioritize securing the software supply chain, and 96% will use or are considering relevant solutions within the next 12 months.
- **Compliance was identified as the top software supply chain pain point for participating executives**, with over half (55%) placing it among the top three concerns. This correlates with another trend of poor visibility into the development pipeline, making regulatory requirements difficult to enforce.
- **Companies need to not only think about vulnerable code** but develop and implement a holistic software supply chain strategy, which should include open source governance, delivery pipeline management, and an understanding of risk in third-party software. We are optimistic about continued innovations, funding, and interest, as 81% of those surveyed expect the priority of software supply chain security to increase over the next few years.

Software Supply Chain

NIGHTDRAGON

Software Supply Chain
Introduction

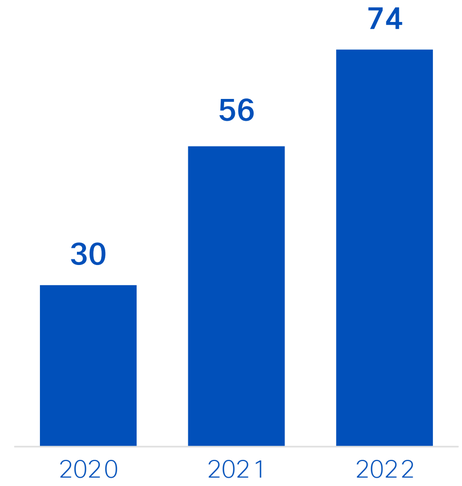
Over the last two years, attacks and vulnerabilities such as Log4j, SolarWinds, and Kaseya have opened our eyes to the risks lurking in our software supply chain. Additionally, we have seen supply chain attacks more recently at Fortra, 3CX, Progress Software and many others. According to the **2022 Verizon Data Breach Report**, 62% of intrusion incidents in the past year were due to vulnerabilities exploited in the software supply chain. These incidents have led to highly disruptive cyberattacks, not only for the directly impacted business but also for the vendors with whom they have a customer or partner relationship. As an example, Log4j allowed attackers to remotely take over computers around the world by inserting malicious code and exposing hundreds of thousands of systems to attack or ransomware. Given the widespread use of this open source library, these issues may continue to cause problems for decades.

Software supply chain risks did not emerge overnight. Today, 90% of IT leaders leverage open source code, which is largely developed outside of their control. Meanwhile, **according to one report**, 98% of applications analyzed included open source software libraries, expanding their threat landscape dramatically. Agile software development operations have drastically accelerated the pace and frequency of new features and capabilities, bringing many benefits in terms of innovation but also introducing potential new cycles of risk. Additionally, an increasingly distributed workforce and the use of cloud-native systems make it even more difficult to gain visibility and correct issues that may arise.

Regulators have noticed this rising risk and are actively discussing or rolling out new requirements for securing the software supply chain. Secure by Design efforts and Software Bill of Materials (SBOM) initiatives, in particular, have gained traction over the past year from government officials.

As we've looked to raise defenses against rising software supply chain risk, we've found current security approaches to be fragmented and insufficient. Legacy solutions fail to identify subtle threats sown throughout the lifecycle of the software supply chain. While they assess code at snapshots in time, they fail to account for the iterative nature of the software development process. Constant, continuous processes are needed to capture the entire risk spectrum. Code-level solutions fail to

Software Supply Chain Financing Transactions (2020-2022)



Source: Momentum Cyber

Software Supply Chain

(Introduction continued)

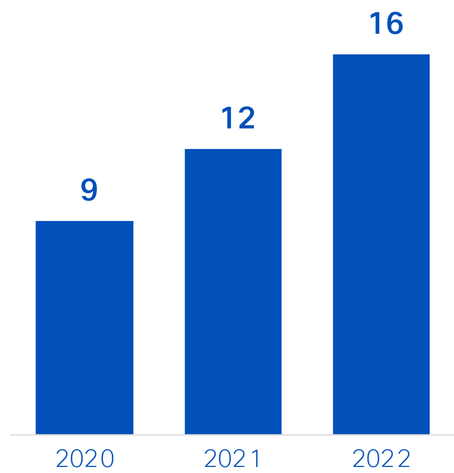
identify broader risks associated with the software delivery pipeline, such as access management, malicious behavior detection, and other risks beyond vulnerable code.

To gain control over the spread of software supply chain risks, organizations need to think strategically about their software supply chain and focus on solutions that can identify, manage, and address the risks quickly, continuously, and at scale. Categories such as code vulnerability and scanning, open source governance, delivery pipeline posture management, and third-party risk management have emerged to help mitigate different aspects of the software supply chain risk spectrum.

Several innovative vendors have emerged to help secure different areas of the software supply chain, such as **Endor**, **Fossa**, **Ox Security**, **Tidelift**, and **Interos**. These are just several of the innovative players NightDragon sees in the market, all of which you will meet in the pages ahead.

While each of these companies address use cases that sit at different levels of market maturity, we believe the next generation of solutions will move beyond assessing code risks at a point in time and move towards more end-to-end solutions, to secure the entire software development lifecycle. To the extent organizations are willing to embrace the convergence of developers and security teams, major strides will be made in continuous software supply chain security management. While an 'all-in-one platform' is yet to emerge, the pieces are starting to take shape and mature.

Software Supply Chain M&A Transactions (2020-2022)



Source: Momentum Cyber

Software Supply Chain
Startup Landscape

The software supply chain security ecosystem is a patchwork of established and emerging technologies designed to carry the burden of delivery pipeline oversight for the expanding digital enterprise. The key challenge within the development lifecycle space is achieving end-to-end software supply chain visibility while continuing to benefit from the innovation and speed provided by third-party code (including open source) while operating a distributed workforce.

To that end, **NightDragon** is excited to partner with innovative startups in this space, especially as the market category and opportunity continues to grow. Through our purview in the ecosystem, **we are beginning to see distinct categories materialize** around code vulnerability scanning and remediation, software supply chain platform security, code-to-cloud pipeline integrity, and SaaS-based software supply chain visibility as they nest within these four concepts.

Code Vulnerability and Scanning

Scanning for known in-house and open-source code vulnerabilities throughout the software lifecycle from development to production

- sonatype
- snyk
- STACKHAWK
- Contrast SECURITY
- Semgrep

Open-Source Governance

Managing risk associated with open-source code

- anchore
- Chainguard
- TIDELIFT
- ENDOR LABS
- FOSSA
- mend.io

Delivery Pipeline Posture Management

Continuously monitoring the security posture across the software development lifecycle

- apiiro
- LEGIT SECURITY
- Rezilion
- OX
- cycode
- ArmorCode

Third-Party Risk Management

Assessing and triaging third-party cyber risks

- BLACK KITE
- interos
- BISHOPFOX
- whistic
- REVERSING LABS
- CyberGRX

Software Supply Chain

What We're Hearing from CISOs

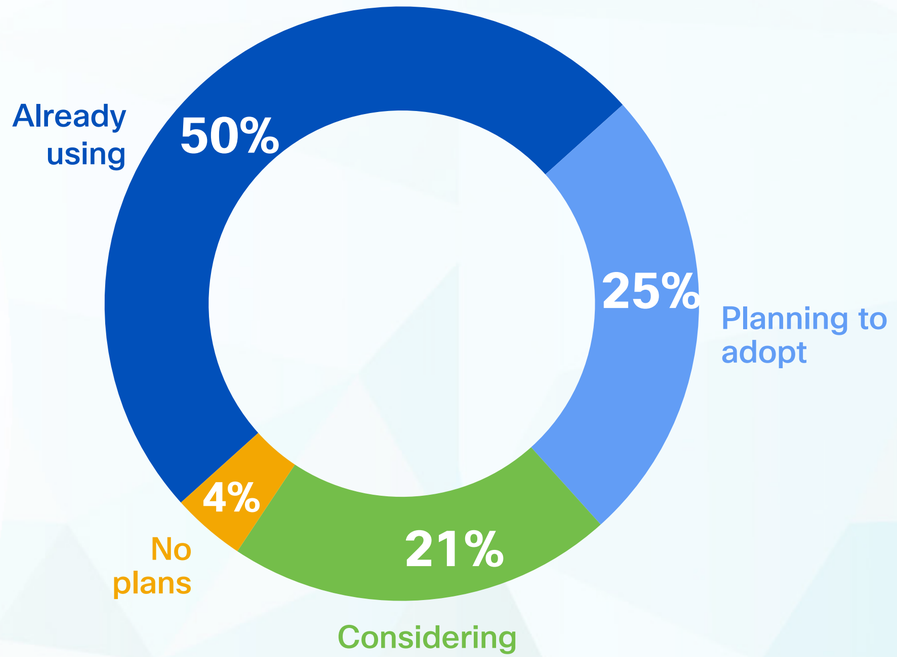
70% Software supply chain security a top investment

When asked about security investments, 70% of IT decision-makers are prioritizing software supply chain.

96% Software supply chain security solution implementation

Nearly every respondent is using or considering software supply chain security solutions in the next 12 months.

Use of Software Supply Chain Security Solutions Over the Next 12 Months



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Software Supply Chain

(What We're Hearing from CISOs continued)

81%

Expectation of an increasing priority

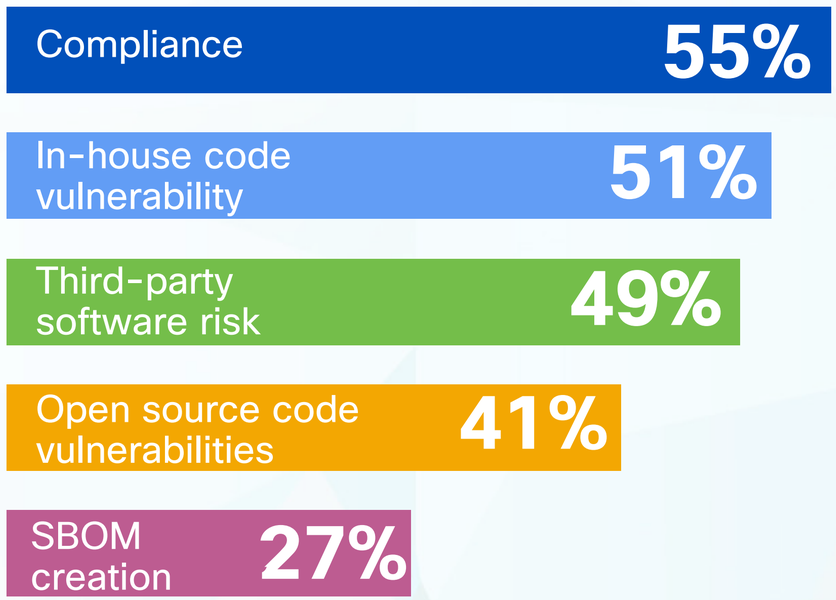
Nearly all – 81% – of executive IT decision-makers expect software supply chain security to increase as a priority within the next 3-5 years.

55%

Compliance concerns identified as a top Software Supply Chain pain point

When asked to identify the top pain point about the software supply chain, over half (55%) of our survey participants placed Compliance in the top three.

Top Vulnerabilities/Pain Points Around the Software Supply Chain



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Software Supply Chain

What This Means for CISOs

What Your Peers Are Saying

CISOs need full visibility into the development pipeline

You can't defend what you can't see. As the CI/CD pipeline continues to grow in complexity, CISOs need end-to-end visibility into each element of the development lifecycle before they can mitigate supply chain instances. Without cohesive, unified supply chain security solutions, teams rely on 'compensating controls.'

> "Third parties are a black box to us."
>
> – CISO
> Top 10 Medical Insurance Company

> "The biggest challenge for a CISO is that there's not an easy tool to prevent [a supply chain attack]; you have to really pivot to compensating controls ... The CISO ideally has a button that tells them, 'This library or this software – where are they in our environment? Which ones are at the highest risk?' I think visibility is a key thing that CISOs have to focus on. If they don't have that, the rest of the [security controls] are secondary. You first have to understand what you have and where you're exposed."
>
> – Brad Jones
> CISO, **Seagate Technology**

Software Supply Chain

(What This Means for CISOs continued)

Hold third parties to the same standards

The need for rapid interconnectivity can make vendors a 'black box' for teams looking to identify third-party software risks. Third parties within an ecosystem should be held to the same security controls as the rest of the enterprise.

> "If you look at what's happened over the last three to four years, the majority of software supply attacks have been from third party off-the-shelf tools. We don't have an understanding of what those third parties are using within their code. We have no visibility to that until something happens. If they're in our environment, why are we not holding them to the standards that we do our own organization?"
>
> – CISO
> Top 10 Medical Insurance Company

Software Supply Chain

(What This Means for CISOs continued)

Proliferating pipelines, standardized solutions

As more development pipelines proliferate, organizations need standardized, automated platforms that manage one of the key elements of supply chain posture risk: the exponential growth of the attack surface. Distinct environments have led enterprises toward disparate solutions; there is room in the market for a unified approach.

> “In some organizations, I've seen 800 pipelines. That makes it much harder to deploy [security controls] versus one pipeline or one product per pipeline. We have a different vendor for static, dynamic, and open source. How do I stitch this together? And how do I stitch it together when there's another pipeline coming, and there's another cloud environment coming? I can easily get 100 times the work and it’s all got to be relatively quick. So, the question is, how do I standardize? I think focusing on automation is key.”
>
> – Grant Bourzikas
> CSO, **Cloudflare**

Software Supply Chain

Gary Hayslip
CSO, SoftBank

One CISOs Software Supply Chain Journey

Securing the software supply chain has become more challenging as development decentralizes and security teams lose full pipeline visibility. The problem can be even more difficult in the cloud. Gary Hayslip, CSO of telecommunications giant SoftBank, shares insights into the ongoing journey to secure the software supply chain.

As the CSO of a company that's 100% in the cloud, I must do more than worry about securing the software supply chain. As a result, I've been able to identify a lot of industry pain points around the issue, as well as a personal/professional opinion on where startups need to take us going forward.

When you have a lot of SaaS apps going in different directions, you need to vet each one. Unfortunately, that means following the chain up to the vendor, their code source, the nature of the product, and how well those data analytics programs can keep all that data safe (once it's parsed and ready for analysis). There's a lot to keep track of, and you must do it the hard way.

There's also the issue of compliance. Many of these companies are highly regulated, which brings problems when simplifying the development pipeline. As much as they want to dip into these OS libraries and make their jobs easier, organizations with a lot of red tape can't take that risk. So that means no open source software, no libraries that aren't managed, and no repositories that aren't up to date. It makes the job considerably harder, but you can't take that risk.

What these organizations end up doing, then, is tracking down SBOMs (Software Bill of Materials) manually and asking for SOC 2 letters and audits. They look to third-party vetting. They do a lot of penetration testing, including the apps, the code, and the libraries. They make security adjustments along the way. It's a whole song and dance, but unfortunately, it's what needs to be done at this point.

Startups know this. The market is inundated with new code-scanning solutions, for example. So much so that it can be hard to tell one from the other. What is needed is something to pull it all together.

I think there is a definite space in the industry for a unified platform. I would love to see one that notifies you of supply chain threats, such as which vendors were affected, which vulnerabilities were exploited, and which patches were available. All of that.

And I see the market heading in that direction. People are now spinning up platforms that fix four or five problems instead of just one that you'll have trouble integrating later. I see unified software supply chain solutions as the way to cut through all the noise in this space.

The industry is now saturated with single-use-case software supply chain tools, which is a good start. But the ones I think will pull ahead are the ones that know the pain points — complexity, too many tools and processes, not enough visibility — and tackle them in a way that pulls them all together and integrates with what companies already have.

Executive Summary

- **Cloud adoption has reached a tipping point.** By 2025, **more than 85%** of enterprises are expected to embrace a cloud-first approach. With the rising adoption of cloud infrastructure, primarily multi-cloud, **cloud security is now high on a CISO's priority list**. According to Gartner, cloud security spend will reach approximately $6 billion by the end of 2023, making it the category with the **strongest growth** in security spending.
- While current posture solutions are essential, most of them are preventative, leaving room for attackers and unknown vulnerabilities. The CNAPP (Cloud-Native Application Protection Platform) concept aims to improve posture management by preventing misconfigurations, enforcing best practices, and monitoring for policy violations.
- We believe that in the modern era of increasing cloud attacks, **a holistic cloud security program is needed.** Such a program should address both the 'left side of the boom' (preventive measures, posture) and the 'right side of the boom' (real-time and post-incident measures such as detection, investigation, response, and recovery).

Cloud Security

TEAM8™

Cloud Security
Introduction

Within three years, **nearly all (95%)** new workloads are projected to be deployed in the cloud, over triple the amount of just two years ago. Eight out of 10 organizations **(80%) are hybrid**, and the **same percentage** adopt a multi-cloud approach. The cloud adoption rate is so high that Gartner expects cloud spending to approximate $6 billion by the end of 2023, exceeding 45% of all enterprise IT spending.

Not ones to be left behind, **attackers are shifting to the cloud as well.** As evidence, **88% of IT and cybersecurity professionals** reported experiencing an attack on cloud-native apps and infrastructure. A few notorious examples are the Uber, Capital One, and Imperva breaches.

The issue of cloud security management has never been more prescient, as the dramatic spike in cloud usage increases the need for dedicated cloud security solutions.

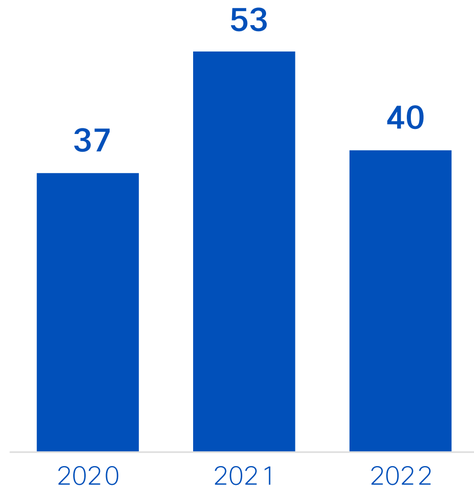
The cloud environment creates new complexity and challenges, leaving security defenders exposed to diverse threats, especially in multi-cloud organizations.

- Security teams are unfamiliar with the terrain.
- Cloud-based assets are more accessible and discoverable, making it far easier for an attacker to map cloud-based environments automatically.
- The flattened cloud attack surface leaves it exposed to more automated attack techniques.
- The cloud's central control plane enables swift and easy access to the most sensitive assets, giving attackers with the proper permissions the "keys to the kingdom."
- The amount of telemetry is skyrocketing, resulting in a lot of noise, high costs, and sub-optimal ROI.

Not surprisingly, the most significant problem for many organizations is misconfiguration. Meanwhile, just as many organizations lack the expertise to detect security flaws or deal with cloud events.

The evolution of cloud security tools for IaaS (Infrastructure as a Service) started with CSPM (Cloud Security Posture Management) and CWPP (Cloud Workload Protection Platform). These then expanded to a **broader CNAPP concept**, which also included CIEM (Cloud Infrastructure Entitlements

Cloud Security Financing Transactions (2020-2022)



Source: Pitchbook, Momentum Cyber

Cloud Security

(Introduction continued)

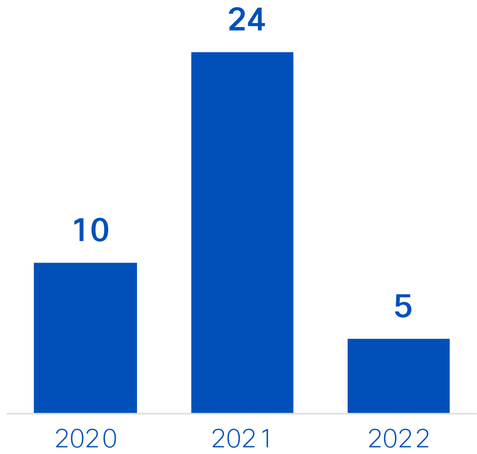
Management) capabilities. **The CNAPP concept addressing the 'left side of the boom' aims to improve posture management by preventing misconfigurations, enforcing best practices, and monitoring for policy violations.**

Increased cloud usage also means an increase in the amount of data that needs to be secured in the cloud. As organizations juggle dozens of data asset types between multiple cloud environments, this raises many new challenges. DSPM (Data Security Posture Management) tools address these challenges by protecting sensitive data, enabling organizations to understand where the data stores reside, and staying compliant.

Yet these tools do not go far enough. While many solutions can point to security hygiene gaps ('left of the boom'), the ability to detect in **real time** that something has happened – and discover the who, what, and where – is still lacking. In addition, CSPs (Cloud Service Providers) and cloud security tools often provide too many logs and alarms, making the meaning difficult to separate from the noise. Hence, their security value is limited. This leads **modern security operations (SOC) teams to seek dedicated real-time and 'right of the boom' solutions which address the issues of cloud detection, investigation, and response.**

We believe that detection and response tools based on legacy approaches (designed for on-prem infrastructure) are insufficient to meet the demands of an entirely new architecture in the cloud. A bespoke solution like CDR (Cloud Detection and Response) as part of CIRA (Cloud Investigation and Response Automation) technology is required to enable security operations teams to automate, visualize, and simplify cloud incident triage and minimize attack impact through rapid response.

Cloud Security M&A Transactions (2020-2022)



Source: Pitchbook, Momentum Cyber

cisco investments

Cloud Security
Startup Landscape

To understand the solutions emerging in the cloud security startup landscape, we first have to understand the problems that precipitated them.

In response to limited visibility, systemic misconfiguration, compliance vulnerabilities, overwhelming and uncontextualized alerts, and stymied detection and response capabilities, a few adventurous startups have committed to tackling the problem of end-to-end cloud security.

Innovative companies like **Orca**, **Lacework**, **Ermetic**, **Dig**, **Securiti** and **Gem** are all making exciting advancements in their respective areas of CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platform), CIEM (Cloud Infrastructure Entitlement Management), DSPM (Data Security Posture Management), and CDR (Cloud Detection and Response).

Together, these pillars – CNAPP (CSPM, CWPP, CIEM), DSPM, and CDR (as part of the CIRA technology) – form the foundation of a holistic cloud security program. **Team8** is proud to be part of building and investing in emerging technology startups in the cloud security space, creating a more transparent, proactive, and unified approach.

Cloud Security

What We're Hearing from CISOs

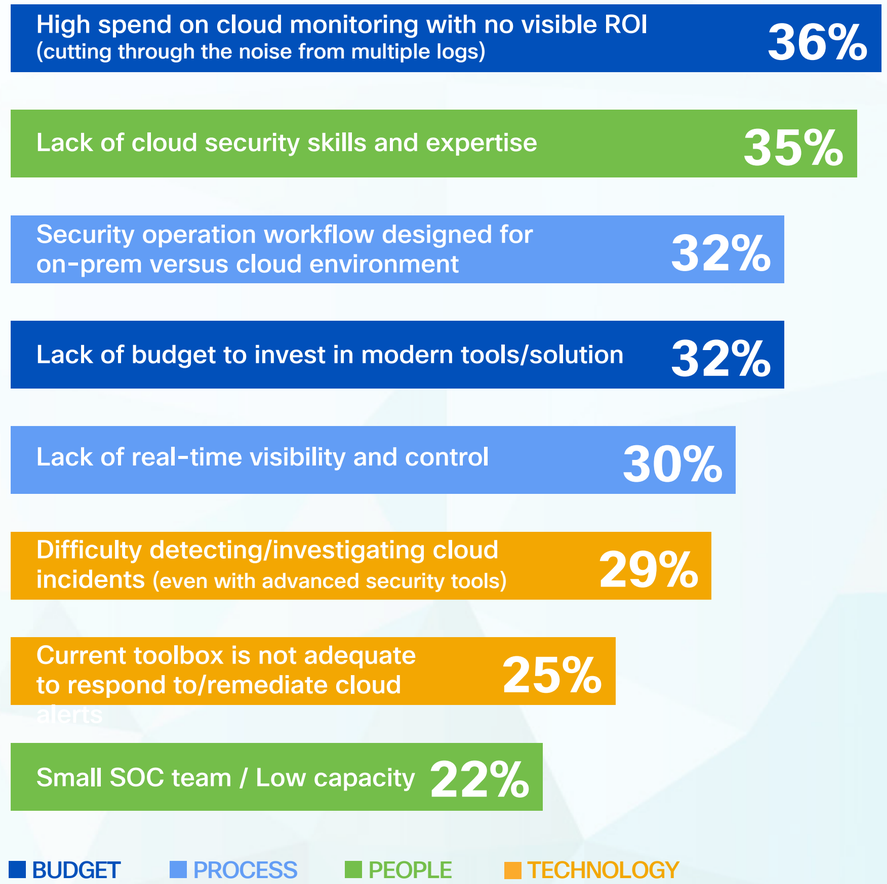
84% Majority of organizations prioritize cloud adoption

These results underline the growing trend towards workloads in the cloud, with 22% of organizations operating entirely in the cloud.

36% High spend on cloud security monitoring as top pain point

While high spend was the top callout, low variance of all the main challenges reflects low maturity in the cloud security space.

Top Pain Points Within Cloud Security



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Cloud Security

(What We're Hearing from CISOs continued)

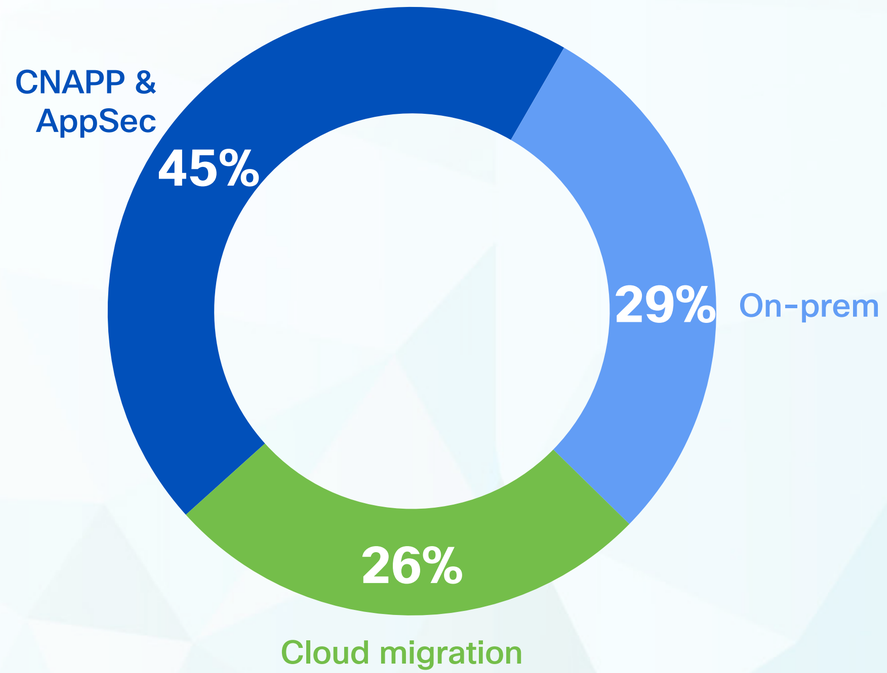
74% Identify investigation capabilities and lack of visibility in the cloud as top technology challenges

Other challenges include complex log collection, too many alterts, and delayed breach response.

45% of the cloud security operation budget is allocated from CNAPP and AppSec budgets

Besides CNAPP, over 50% of the budgets allocated to cloud security operations are coming from on-premise protection platforms and cloud migration budgets.

Areas of Budget from Which Cloud Security Operations Budget is Allocated



Source: Foundry Research, MarketPulse Survey for Cisco, Feb. 2023

Cloud Security

What This Means for CISOs

What Your Peers Are Saying

Cloud challenges and opportunities

While not without its obstacles, the cloud also inherits a significant number of security contributions. Thanks to its inherent agility, cloud-based security capabilities can remediate a number of gaps as quickly as they arise. The cloud's hyperconnectivity also acts as a business enabler, and cloud users can host assets free from traditional boundaries – great for scalability and innovation. However, this same expansiveness also creates a burden for security. As we move into this new world of 'anywhere data,' we must adopt new security strategies to match.

> "The main advantages of the cloud are that everything is configurable as code, and you can change the way anything is set up rapidly. When thinking purely in terms of security, you can fix almost anything as soon as you find it or within a very short amount of time thereafter."
>
> – Justin Berman
> VP of Core Technology, CISO
> Thirty Madison

Cloud Security

(What This Means for CISOs continued)

Uniform visibility and governance a top challenge

While cloud use is nearly ubiquitous, it's still very much the 'wild west' when it comes to governance. Similar to the early days of the internet, we are just past the honeymoon phase and are reaching the point where formal frameworks are needed. As companies move between public, private, and hybrid cloud environments, and most organizations use multiple cloud providers, it **creates real pain of visibility and requires cloud-specific knowledge that's missing today.** Visibility and governance alongside policy alignment will be key to improving security and efficiency.

> "The real challenges in multi-cloud are: First, the governance of all the different cloud assets – whether it's a third-party application, or through a Software as a Service (or an Infrastructure as a Service) like AWS or Google. Second, how to make sure that policy is synonymous across all these different types of cloud environments."
>
> – Richard Barreto
> CISO, **Progress**

Cloud Security

(What This Means for CISOs continued)

On-prem skills struggle to keep pace

The on-prem legacy toolset is woefully limited when it comes to the very fast, ephemeral, and extensive nature of the cloud. Furthermore, CISO organizations are not immune to the cloud skills shortage, leading to difficulties in finding gaps, prioritizing them, and remediating. Cloud posture tools provide a holistic map of existing vulnerabilities and misconfigurations, but it's not enough, and the organization still remains vulnerable to potential attacks. These issues become even more critical when a cloud incident unfolds, and there is an urgent need to detect, contain, investigate, and respond.

> "Security skills have historically been in short supply. The rapid migration to the cloud is not just underpinned by the migration to a new form of infrastructure, but a new way of constructing applications and systems, which requires a change in methodology and technology for security teams. This means we need to re-train people on the new model, which further exacerbates the talent challenges we face."
>
> – Charles Blauner
> Former CISO, **Citigroup**

> "Cloud posture management vendors are good at finding the vulnerabilities or gaps in security. But now when your systems are exposed to the public on the internet, you have to fix those things very quickly. If not, you're setting yourself up for some additional risks."
>
> – Richard Barreto
> CISO, **Progress**

Cloud Security

Tyson Kopczynski
Former SVP & CISO, Oportun

One CISO's Cloud Security Journey

Tyson Kopczynski is the former CISO of Oportun, where he worked for nine years during the company's migration from on-prem to cloud. Here he speaks about the challenges, advantages, skills, tools, and mindsets needed to be successful in your cloud journey.

> "You need to embrace the cloud. If you approach the journey from an on-prem perspective, with your standard InfoSec approach, you will fail miserably."

CHALLENGES AND OPPORTUNITIES

The cloud is dynamic, ephemeral, and forever moving faster. This is by design, considering that companies want to deploy applications that are highly scalable, flexible, and resilient. The challenge is that traditional information security practices can't keep up. After all, those practices were born on-premises and are highly manual in nature — which is the antithesis of what in the cloud is increasingly driven by code. On the other hand, the nature of the cloud also brings some security advantages provided we are willing to adapt. To start, security itself can also be driven by code, guardrails, and automation. Secondly, if embraced to its fullest, the cloud is highly distributed, immutable, and ephemeral — which gives us the cyber resiliency we're all after.

The multi-cloud approach also poses a great challenge, especially for smaller teams. Each provider does things in a different way, so you have to understand those nuances to really grasp how to manage, configure, and secure the cloud properly. To avoid dealing with the finer-grained details of each provider, enterprises are looking for an agnostic abstraction plane to build on top of any Cloud Service Provider. The advantage is, once again, a certain amount of resiliency by using the benefits of one Cloud Service Provider against the benefits of others.

CLOUD SECURITY TOOLS

The old enterprise tools don't translate well to the cloud environment. However, the issue of tool proliferation is 10x worse in the cloud than on-prem because everyone has generated so many different point solutions for every problem. What we want is a single platform that we can plug in and that can handle a variety of use cases — to act as a Swiss Army knife.

The tools in the modern cloud security stack should be plugged into your software development lifecycle, enabling out-of-the-box security capabilities. But even on a more basic level, the cloud services themselves should be secure out of the box. For example, resources spun up in AWS should be secure by default.

The cloud security stack should include pen-testing tools, vulnerability management

Cloud Security

(One CISO's Cloud Security Journey continued)

tools, IaC, CSPM, CIEM, DSPM, and SOC tools (like SIEM or SOAR), which include both cloud detection and response capabilities as well as log management and log aggregation.

Our current challenge, however, is that we have too many tools, so our focus right now is getting our teams to most effectively use a single set of tools, and really leverage and optimize what we are paying for. For example, how do you know you're collecting the right logs from the cloud and the very manual process of building your use cases so that your SIEM can leverage it? If a vendor can do this for you, then you can spend more time ensuring the use cases you have chosen are the most effective.

SECURITY TEAMS' SKILLSET AND KNOWLEDGE

Current security teams do not have the needed skill set to deal with cloud security, which is another big challenge. We need more and more people that understand and write code, understand how to configure the tools using code, and understand how things fit together.

There is a generic shift-left in the cloud. With security as code, infrastructure as code, and compliance as code, the cloud has become very engineering focused. Hence, cloud-based security tools need to relate to those relevant personas. The old vendors don't really understand how things work in the cloud, and they are now acquiring new tools to adjust.

The next generation of tools will be born-in-the-cloud platforms, which will intrinsically understand developers and code. **Security teams will become more like platform teams. They need to become a part of the value stream where they are actually providing services back to the developers' teams to be consumed.**

Executive Summary

Perhaps there has never been a better time for companies to have a finger on the pulse of emerging security technology. The rapid pace of digitization necessitates constant improvement in security research, and continual threat evolution drives ongoing innovation. Cultivating relationships with tech startups is critical.

- CISOs want to see more unified — less niche — offerings that can simplify disparate functions, workflows, and use cases.
- Cloud-only emerging technologies may warrant adoption in conjunction with traditional technologies as many companies retain on-premises or hybrid environments.
- Executives are turning to startups with a 'design partner' mindset and taking a proactive role in creating the solutions they want to see.

Embracing Startup Tech

Embracing Startup Tech

What CISOs are Saying

Striking a balance

Many organizations are still steeped in traditional technology. While this might be necessary in some industries, companies that keep an eye on up-and-coming solutions have a distinct advantage over those who don't. Staying abreast of yearly developments within the startup landscape will help decision-makers make informed choices that lead to a well-rounded security stack.

> “While we prioritize mature technologies due to the nature of healthcare and patient care, we recognize the importance of emerging tech and strive for a balance between the two. Staying on top of innovation and emerging technologies is critical to keeping our infrastructure secure.”
>
> – Duc Lai
> CISO, **University of Maryland Medical System**

Collaborate to innovate

Sometimes the right answer is still out there. As experienced organizations partner with emerging technology firms, the chances of finding or creating effective solutions improve. Established companies have a foundational understanding of the pain points that come from limited security solutions of generations past; savvy new startups have the agility to quickly spin out new solutions. This close collaboration speeds time to market for new technologies that solve legacy problems.

> “Protecting information cannot be an afterthought but must be a fundamental part of data. Protection should flow with the information as an attribute. It’s going to require new products and potentially new solution sets. To achieve this, we need to collaborate with emerging tech. It’s important we evaluate and push the boundaries of innovation to come up with a solution.”
>
> – Paul Curylo
> CISO, **Inova Health System**

Embracing Startup Tech

Alan Berry
CISO, Centene Corporation

A CISO's Advice on Leveraging Technology Startups

Sourcing emerging technology is like scouting for the next superstar athlete. It takes skill, knowledge, and experience to identify the best talent before they become a household name. We sat down with Alan Berry, CISO of Centene Corporation, to learn how to best draw startup engagement into their organizations.

Having had the chance to lead in large organizations, I can attest that **no matter how good you are, you can always improve.** That's especially true of security. The problem is that the gears can get turning and business can operate so fast that there's little time to reflect and innovate. That's why we've deliberately invested in startups over the years. I think embracing emerging technology is an integral part of staying agile as a corporation. However, as fundamental as these types of relationships are, they require some navigating. **I'll share what I've learned as a CISO about working with startups over the years,** hoping these kinds of relationships will only grow stronger.

ON ENGAGING NEW TECH

Before jumping into new technology, **we like to canvass opinions**. One of the primary ways we do this is through roundtables of startups within the security space. We regularly work with a small number of VCs, who identify possible companies that may meet our security needs. The VC then sets up one-on-one calls with the startup. Personal meetups have been invaluable for us. Prior to the pandemic, we hosted a VC at our headquarters a couple times a year. They curated a small slate of candidate companies and brought their founders to us for briefings and exploratory sessions. This gives us a chance to have the kind of productive discussions that are just hard to come by over a video call. The return value to the company is direct engagement with not just my team, but other local CISOs in our St. Louis region. The validation of the startup's vision and direction provides invaluable insights and helps guide their development and investment.

DEVELOP PERSONAL RELATIONSHIPS

This ties into another one of our strategies – **maintaining personal relationships with the VCs.** Because we've put in the work, I can reach out to them when I have a need, and they reach back when they have something interesting. That way, I know I'm always up to date. This also gives the VC a trusted partner with whom they can meet their goals in the most time-efficient way. Startups want to tackle impossible problems and they need to understand the problems CISOs are facing today. By establishing a good two-way rapport with the VC and startup community, the entire cybersecurity ecosystem improves measurably. In that way, we're ensuring we're not only at the forefront of emerging technologies but also contributing our experiences to help shape them.

Embracing Startup Tech

(A CISO's Advice on Leveraging Technology Startups continued)

BE PREPARED TO GIVE ADVICE

When it comes to being a 'design partner' to startups, it's important to keep a few things in mind. Their product development depends largely on you, so you want to **make sure you have the cycles before jumping in.** We mostly invest that kind of commitment in an area where nobody else on the market can offer the capability we're looking for. And we guard our time jealously, since that is the most valuable resource I have. I can only engage as a design partner with one company at a time.

IT'S A TWO-WAY STREET

Finally, my advice for establishing strong working relationships with emerging technology companies: know the terrain. These startups are driven by their unwavering passion and dedication to their work, often putting in long hours – often without weekends – to innovate and excel. And they love what they do! Embrace the touchpoints that come with collaborating with startups and be receptive to their requests for feedback. The symbiotic relationship between enterprises and startups presents a unique opportunity for growth and innovation. We should adapt and evolve alongside them, recognizing their agility and fresh perspectives as assets to address legacy challenges. We must also not be offended or discouraged if the same startups are simply not willing or able to attack our problems. After all, they have to be able to generate revenue if they want to grow and improve.

By partnering with startups, established organizations can leverage these new innovative solutions, while bringing unparalleled expertise, fostering an environment of mutual learning and growth. Startups benefit from our experience and we (the enterprises) gain valuable insights from the startup ecosystem. Together, we can navigate the evolving threat landscape, drive innovation, and secure our organizations for the future.

Embracing Startup Tech

Daniel Barriuso
Chief Transformation Officer and former Global CISO
Santander Group

A CISO's vision on the value of partnerships and the startup ecosystem

Daniel Barriuso is the Chief Transformation Officer and former Global CISO at Santander Group, a leading commercial bank with 164 million customers across Europe, Latin America, and the US. He tells us about how he views the opportunities to partner with startups.

The CISO of today understands that when it comes to leveling cyber threats, organizations must look beyond their perimeter and combine efforts and resources with peers. We see a shift in how CISOs engage and **partner with innovative businesses. Looking at cyber threats and solutions from different perspectives is key to creating a more secure ecosystem.**

Startups often collaborate with academic institutions, other companies, and industry associations, creating opportunities for the cross-pollination of ideas and technologies. This can help CISOs gain a nuanced understanding of the threat landscape and access a wider range of solutions. Startups often have a nimble approach to applying technologies for new applications. They may be more willing to move fast and experiment with new ideas and customize for their clients. **This can help CISOs gain access to innovative technologies and solutions that may not yet be available from more established vendors.**

Over the past several years, Santander has successfully partnered with several Forgepoint Capital companies, leading to pilots and partnerships in key cybersecurity domains: Identity and Privileged Access Management, Automatic Pen-testing and Control testing, Cloud Security, Backup Protection and Recovery, Data Management and Advanced Detection, Frontier Cybersecurity, and Advanced Fraud Detection.

Cybersecurity and fraud are disciplines that are interrelated and integral to one another. Fraud events are increasingly digital and technology based. Effective fraud management requires deep technical expertise and a holistic understanding of the attack chain and cybersecurity. In addition, **capabilities to combat emerging fraud threats must rely on highly sophisticated technologies — particularly artificial intelligence** to automate responses and to be able to adapt and operate in real time.

At Santander, we've opted for a global fraud and cybersecurity model that helps the Group to have an integrated and agile vision. As part of this commitment, Santander has been working very closely with **Lynx Financial Crime Tech**, an innovative AI company that

Embracing Startup Tech

(A CISO's vision on the value of partnerships and the startup ecosystem continued)

grew out of a university center of innovation. Its advanced fraud detection and scoring platform can operate both on-premise and in the cloud to ensure flexible scaling, while incorporating artificial intelligence **capable of learning from the data received daily to adapt to both new fraud patterns and new payment methods. It is designed to analyze high volumes of transactions enriched by peers.** Lynx can detect fraud in real time with more than 3 billion analyzed transactions per month.

Moreover, **the emergence of the truly digital enterprise has made it crucial for organizations to have a robust next-generation Security Information and Event Management (SIEM) system in place.** With the increasing sophistication and frequency of cyber threats, it is essential to have complete visibility into systems, applications, user behavior, and threat intelligence to be able to correlate events, identify threats, and mitigate the risk of breaches. Real-time monitoring, advanced analytics, and machine learning enable faster and more accurate detection and response to threats. Herein lies greater opportunity to modernize the future of cyber.

These days, in the face of rapidly evolving challenges, it is essential to have a modern, agile, and integrated management of cybersecurity and fraud, combined with an innovative technology strategy. Partnering with startups building innovative solutions is critical in protecting your data, assets, and identities so that people, businesses, and society continue to prosper.

Conclusion

Partnering with emerging technology firms infuses new life into enterprise economies to stay ahead of the curve of constantly evolving threats. That said, with today's rapidly evolving startup landscape, organizations are confronted with a myriad of emerging technology solutions, making it imperative to sift through the noise and find the right security answers.

Cisco Investments is committed to navigating the emerging technology landscape, connecting CISOs with best-in-class solutions, and driving innovation in the security industry. We hope the release of our 2023 CISO Survival Guide offers valuable insights to supplement your area of interest with emerging expertise.

Contact us **here** to get involved and be a part of the ongoing conversation in shaping the future of security.

Contributing Authors

Cisco Investments

Cisco Investments is where inclusive innovation begins. When our visions align, we can build an inclusive future for everyone. We're committed to helping create a more diverse, global technology community, and are focused on accelerating innovation to the market. But we go further than investing. Strategy and thought leadership are at the forefront of everything we do. We provide you with access to our technology expertise and global customers to accelerate your growth. With us by your side, you will have a trustworthy partner and collaborator throughout your company-building journey.

cisco investments

Janey Hoe is a Vice President of Cisco Investments. Previously, she held multiple product management, technical marketing, and business development leadership roles at Cisco, operating multi-billion dollar product lines as well as pioneering new products in switching, security, data center, and video collaboration. Along with her team, she was recognized as a finalist for the Pioneer Award, the highest honor for innovation at Cisco.

Prasad Parthasarathi is Senior Director and Global Head of Cisco's Cybersecurity Investments and M&A practice. Prasad's strong M&A track record extends to large cap technology platforms such as HP and EDS, characterized by 25+ category defining investments, multiple successful exits, as well as landmark transactions such as Cisco's $2.4B acquisition of Duo Security and $14B sale of EDS to HP among others.

Neetta Shetty leads Cisco Investments' Portfolio Development function, where she helps portfolio companies accelerate their businesses and unlock their potential by harnessing Cisco's extensive go-to-market engine and global reach. With over a decade of experience at Cisco, Neetta held various business acceleration roles spanning the United States and the Asia Pacific, Japan, and China (APJC) region. In her prior role, she served as the Global Go-to-Market (GTM) leader for Cisco dCloud, playing a pivotal role in establishing and developing the GTM function for Cisco's largest cloud demo platform.

Soo Jin Park joined Cisco Investments in 2021 and focuses on acquisitions and investments in the Cybersecurity space. Prior to joining Cisco, Soo Jin was an investment banker at Jefferies Technology M&A group in New York, where he advised leading technology companies and private equity firms on M&A transactions.

Forgepoint Capital

Forgepoint Capital is a leading cybersecurity and digital infrastructure venture capital firm that invests in transformative companies protecting the digital future. With $1B+ AUM, the largest sector-focused investment team, and portfolio of nearly 40 companies, the firm brings over 100 years of proven company-building experience and its Advisory Council of more than 80 industry leaders to support entrepreneurs advancing innovation globally. Founded in 2015 and headquartered in the San Francisco Bay Area, Forgepoint is proud to partner with category-defining companies as they reach their market potential.

Leoncio "Leo" Casusol is Managing Director at Forgepoint. He is a seasoned technology leader and investor with over 20 years of executive experience building and operating large-scale global technology companies. His expertise in product development, infrastructure management, global operations, sales, business development, telecommunications, and government contracting has been successfully applied at startups as well as Fortune 20 companies. Prior to Forgepoint, Leo spent over two decades as the CIO at Cyxtera Technologies, Verizon Business, Terremark Worldwide, and Liquidity Services (Nasdaq: LQDT). Leo was also a founding member and technology architect for Quadrem US (acq. Ariba and subsequently acq. SAP). Leo holds an MBA from the Universidad Nacional de San Agustin and a BASc from the Universidad Católica de Santa Maria.

Reynaldo “Rey” Kirton is a Vice President at Forgepoint, where he focuses on data security and infrastructure, incident response, cyber risk management and resilience. Prior to Forgepoint, Rey worked at Harlem Capital, which invests in seed-stage, tech startups founded by women and minorities. He also worked at Altman Vilandrie & Co, where he managed over 30 operational and due diligence efforts for clients across North American, European, and Latin American markets. He began his career as a consultant with Cambridge Associates, where he provided capital markets research and portfolio allocation advice to private and institutional investors ranging from $50M to $3B in assets. Rey is a CFA Charterholder and holds an MBA from the Wharton School of the University of Pennsylvania and a BA from Harvard.

FORGEPOINT

NightDragon

NightDragon is an investment and advisory firm focused on growth and late-stage investments within the cybersecurity, safety, security and privacy industries. Its platform and vast industry network provide unparalleled threat insights, deal flow, market leverage and operating expertise to drive portfolio company growth and increase shareholder value. Founded by Dave DeWalt, the NightDragon team has more than 25 years of operational and market expertise leading technology companies such as Documentum, EMC, Siebel Systems (Oracle), McAfee, Mandiant, Avast and FireEye.

Morgan Kyauk is a Managing Director at NightDragon, bringing a wealth of experience leading M&A transactions for companies of all sizes - from late stage, pre-IPO companies to large, serial acquirers. Most recently, Morgan was the Vice President of Corporate Development at FireEye, where he was responsible for the evaluation, execution, and integration of all acquisition, investment, and strategic partnering activity for the company. Morgan has also held corporate development leadership roles at a variety of technology companies, including Dropbox, Juniper Networks, and HP. Morgan began his career advising technology companies on M&A activity while at Bank of America Merrill Lynch. Morgan received his MBA from Wharton and his bachelor's degree in Business Administration and Economics from the University of California, Berkeley.

Hannah Huffman is a Senior Associate at NightDragon. She is a former senior technology consultant from the mergers and acquisitions practice at Deloitte. Throughout her consulting career, she worked with various Fortune 50 and 500 companies. Hannah focused her time on executing successful mergers and divestures, managing large scale cloud and network transformations and performing the role of a product manager for software offerings and applications. Hannah received her bachelor's degree in Business Administration - Finance from the Mendoza College of Business at the University of Notre Dame. While at Notre Dame, she was a student-athlete on the Women's Basketball team reaching three Final Fours in her four-year career.

NIGHTDRAGON

Team8

Team8 is a venture group that builds and backs the most innovative technology companies in the fields of cybersecurity, data, fintech, and digital health. Team8 leverages deep domain expertise, cutting-edge technology, and first-hand company-building experience to partner with entrepreneurs in founding globally-successful companies.

TEAM8™

Amir Zilberstein is Managing Partner of Team8 Enterprise. Amir is also Chairman and Co-Founder of Claroty, a pioneer in the OT security market. Prior to Claroty, Amir co-founded Waterfall Security Solutions and Gita Technologies, and prior to that, he managed a team of exceptional researchers and developers in the Israeli elite technology unit 8200. Amir is the inventor and author of more than ten patents, most of which are in the field of cybersecurity.

Tom Sadon is a Director of Marketing at Team8, focused on product marketing initiatives in the fields of cyber security and data. Before joining Team8, Tom held various managerial product marketing positions at Cognyte and was a Director of Cyber Threat Intelligence at XM Cyber. Tom served as head of a department and product manager in the Israeli elite technology unit 8200 and the Israeli Prime Minister's Office for over a decade, with honors and awards.

Shirly Ozer is a Director of Strategy at Team8 focused on supporting the Team8 Enterprise foundry and portfolio companies' building process, from ideation to growth, in cybersecurity and data infrastructure domains. Before joining Team8, Shirly worked as a Strategy Manager at Deloitte, leading consulting projects for private and public sectors and advising C-level executives. Prior to that, Shirly served as an Intelligence Team Manager in the Israeli elite technology unit 8200.

This report is the result of the hard work, expertise, and collaboration among four Venture Capital groups, who share a common goal of helping Chief Information Security Officers engage security startups.

The team includes:

- **Amy Gerrie**, Portfolio Development Manager, Cisco Corporate Development
- **Danny Vivenzio**, Communications Manager, Cisco Corporate Development
- **Giselle Omar**, Marketing Manager, Cisco Corporate Development
- **Mofe Alege**, Associate, Cisco Corporate Development
- **Sarah Kuranda Vallone**, Vice President of Marketing and Communications, NightDragon
- **Tanya Loh**, Chief Marketing Officer, Forgepoint Capital

Special thanks are given to **Cisco's Security Business Group**, especially its leadership and communication teams, and **Wendy Nather**, the group's Advisory CISO, as well as **Dan DeSantis**, Director of CISO Advisory for Cisco GSSO and his advisory team.

CISCO

Investments

© 2023 Cisco Investments