2021

CISO
Survival Guide

Emerging Trends From the Startup Landscape

presented by **cisco investments**   in partnership with   **NORWEST** VENTURE PARTNERS   **YL VENTURES**   **ForgePoint** CAPITAL

Table of Contents

Introduction

At Cisco, a core mission is to protect what's new and what's next. We've committed to not just building the best in-house end-to-end security solutions, but also to embracing tech outside our four walls.

Because of our long history as investors and acquirers, our strong connections with other venture capital firms, and our long-standing relationships with CISOs at enterprises all over world, we have a unique vantage point to offer insights and recommendations to CISOs.

I'm excited to present what we've learned in the second edition of the **Cisco Investments** CISO Survival Guide to Emerging Trends From the Startup Ecosystem. To author the 2021 edition, we decided to partner closely with three leading cybersecurity venture capital firms – **ForgePoint Capital**, **Norwest Venture Partners**, and **YL Ventures**.

Armed with insights from CISO roundtables, one-on-one CISO interviews, and an extensive survey we commissioned IDG to produce, which reached over 100 CISO and security leaders, our teams deconstructed four major trends in cybersecurity: Secure Access Service Edge (SASE); DevSecOps; Privacy & Compliance; and Security Automation. We collaborated closely over a six-month time frame, challenged each other and our own thesis multiple times, and leveraged learnings across our collective 50+ cybersecurity investments to filter signal from noise.

We synthesized our collective assessment of critical use cases, spending patterns, future-proof architectures, promising start-ups, and best practices across the four once-in-a-generation technology trends identified above. In the process, we identified some important best practices for embracing startup tech in general.

Cisco Investments is delighted to present the 2021 edition and is grateful to our venture capital partners who made it happen.

Happy reading, and let us know if you're interested in participating in next year's CISO Survival Guide.

Janey Hoe
VP at Cisco Investments

Executive Summary

- While Secure Access Secure Edge (SASE) is still early in its adoption lifecycle, almost all respondents (98%) see clear benefits for it and are committed to directing future spend towards it.

- Among SASE pillars, Zero Trust Network Access (ZTNA) and Cloud-Native Firewalls are key priorities. Most enterprises have already embraced cloud-based Secure Web Gateway (SWG) and view cloud-native security controls along with adaptive user access as critical focus areas.

- CISOs recommend creating "fusion centers" of SecOps and NetOps teams and committing to a multi-year roadmap for implementing SASE.

SURVIVAL
GUIDE

SASE
Cisco Investments

Introduction

The traditional models of networking and network security are under stress from hybrid compute environments, diverse user roles and access, as well as massive device sprawl, among other factors. Ensuring a consistent experience across these fragmented use cases is driving the adoption of SASE.

At its core, SASE architecture mandates that security and networking controls are enforced at the source of all data and traffic. It also works to ensure that every user and location enjoys consistently secure, low latency Internet that's comparable to the experience in the corporate HQ. A SASE approach thus differs from the "traditional" model where traffic is backhauled to Corporate IT, security and networking policies are applied, and the resulting decision is sent back to the source.
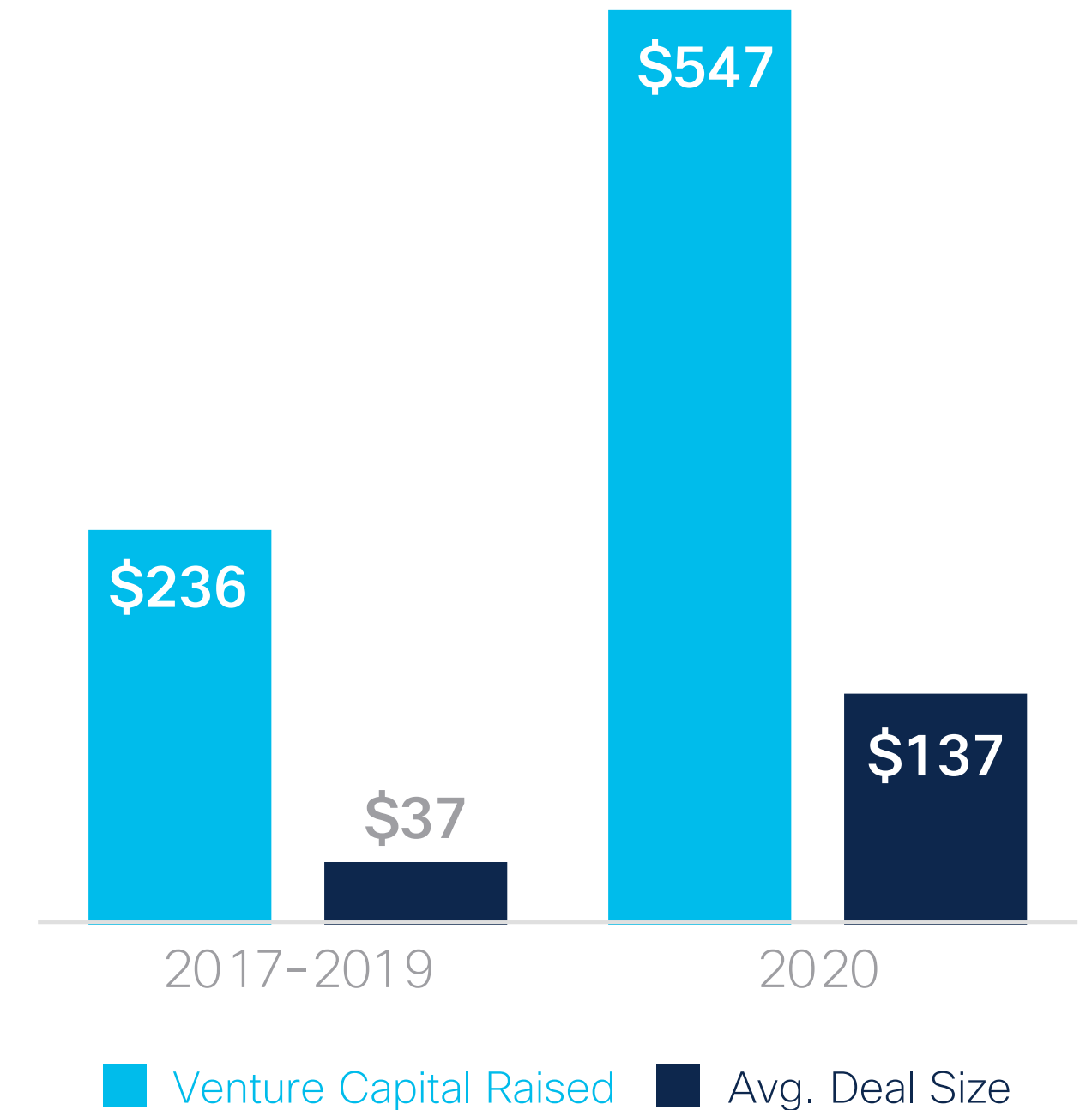
Enabling SASE requires stitching a unified fabric across security controls including Secure Web Gateway, DNS, and CASB. It also necessitates embedding Networking (SD-WAN) in the architecture. The role of SD-WAN in SASE is pivotal, as it allows users to access the web by using the web (i.e., eliminate centralized backhauling).

While SASE is early in its adoption lifecycle, many enterprises are increasingly prioritizing spend on the SASE roadmap.

Distributed users, disparate devices, data and app sprawl, as well as evolving compliance requirements are some of the biggest motivating factors for this commitment. To what extent varies across organizations, as each SASE journey is different. Secure Cloud Edge, ZTNA, Cloud Firewall, and Secure SD-WAN are just some of the current control points within SASE, with secure user access, granular data controls, and policy emerging as future tenets. There's enough interest around these use cases that SASE-related venture capital increased significantly in 2020. Such growth was driven by large raises on a few select companies. Additionally, both acquisitions and investments in SASE-focused companies have remained robust over the last three years.

Even so, some enterprises are holding back in their SASE journeys. Some are reluctant to consolidate spending with a limited set of cybersecurity platforms and are instead spending across multiple platforms. This won't aid them in the long run. SASE involves multiple stakeholders across security and networking. As such, a unified SASE architecture will require customers to stand up "fusion centers" – having security, networking, and IT infrastructure buyers in one pod – like in DevSecOps.

SASE- related Venture Capital Raised and Avg. Deal Size ($M)

Bar chart showing:
- 2017–2019: Venture Capital Raised $236, Avg. Deal Size $37
- 2020: Venture Capital Raised $547, Avg. Deal Size $137

Legend: ■ Venture Capital Raised ■ Avg. Deal Size

SASE M&A Volume since 2018: **$2.2bn**

SASE VC Volume since 2018: **$1.1bn**

CLOUDGENIX
daptiv
luminate
silver peak
Skyhigh

bitglass
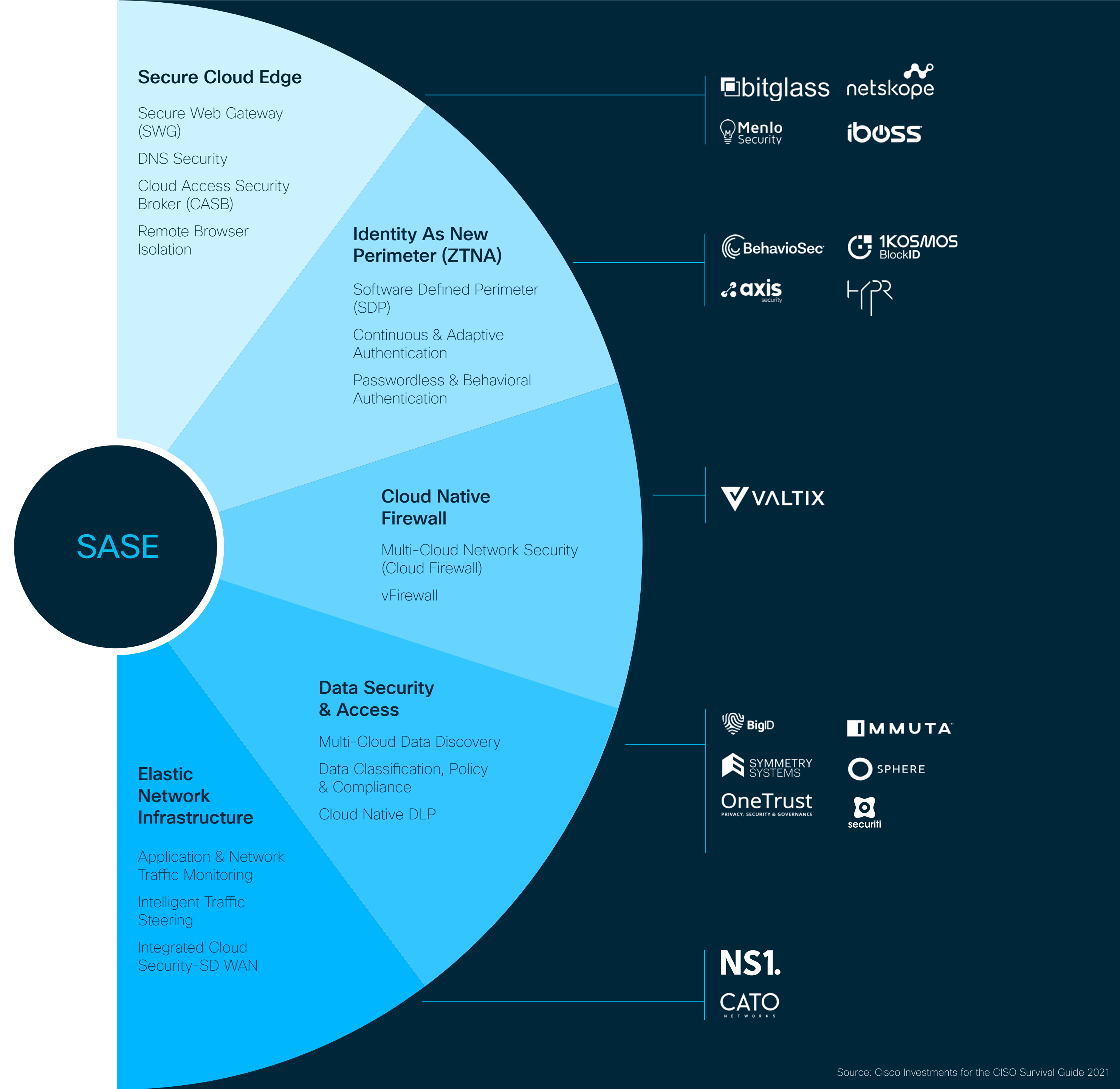netskope
CATO
Menlo Security
iboss
NS1.

Startup Landscape

Since SASE subsumes multiple security control points, we decided to break down the SASE landscape into five categories and showcase representative security startups.

We would be remiss to not mention that there are scaled platform players who cut across the different pillars of SASE. Those players include Cisco, where we're investing in companies like **Valtix**, **Securiti**, **NS1**, and **BehavioSec** to enable integration of cloud-native technologies within scaled architectures.

For the purposes of this report, however, we are focusing on startups defined as companies that are privately held with no IPO or acquisition, that are early in their company journey, and that are disrupting traditional methods or mindsets by bringing a new solution to market.

SASE

Secure Cloud Edge

Secure Web Gateway (SWG)

DNS Security

Cloud Access Security Broker (CASB)

Remote Browser Isolation

bitglass netskope
Menlo Security iboss

Identity As New Perimeter (ZTNA)

Software Defined Perimeter (SDP)

Continuous & Adaptive Authentication

Passwordless & Behavioral Authentication

BehavioSec 1KOSMOS BlockID
axis security HYPR

Cloud Native Firewall

Multi-Cloud Network Security (Cloud Firewall)

vFirewall

VALTIX

Data Security & Access

Multi-Cloud Data Discovery

Data Classification, Policy & Compliance

Cloud Native DLP

BigID IMMUTA
SYMMETRY SYSTEMS SPHERE
OneTrust
PRIVACY, SECURITY & GOVERNANCE securiti

Elastic Network Infrastructure

Application & Network Traffic Monitoring

Intelligent Traffic Steering

Integrated Cloud Security-SD WAN

NS1.
CATO
NETWORKS

What We're Hearing from CISOs

SASE
# Survey Results

ZTNA a top spending priority.

42%

have ZTNA as top spending priority within SASE

Almost half (42%) of survey participants told us that zero-trust network access (ZTNA) was their top spending priority within SASE. This finding highlights how adaptability, a context-aware state, and continuous access are increasingly viewed as primary benefits of SASE. Behind ZTNA came cloud firewall capabilities at 23% of respondents.

At least a quarter of IT security budgets reserved for SASE

Most (55%) respondents told us that they intend to prioritize 25%-75% of their future IT security budget on SASE. CISOs wouldn't be setting aside this amount of budget if they didn't view SASE as urgent and critical for their enterprises going forward.
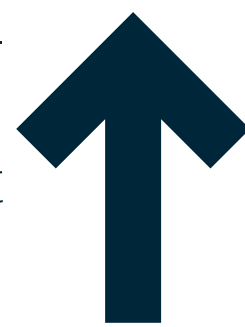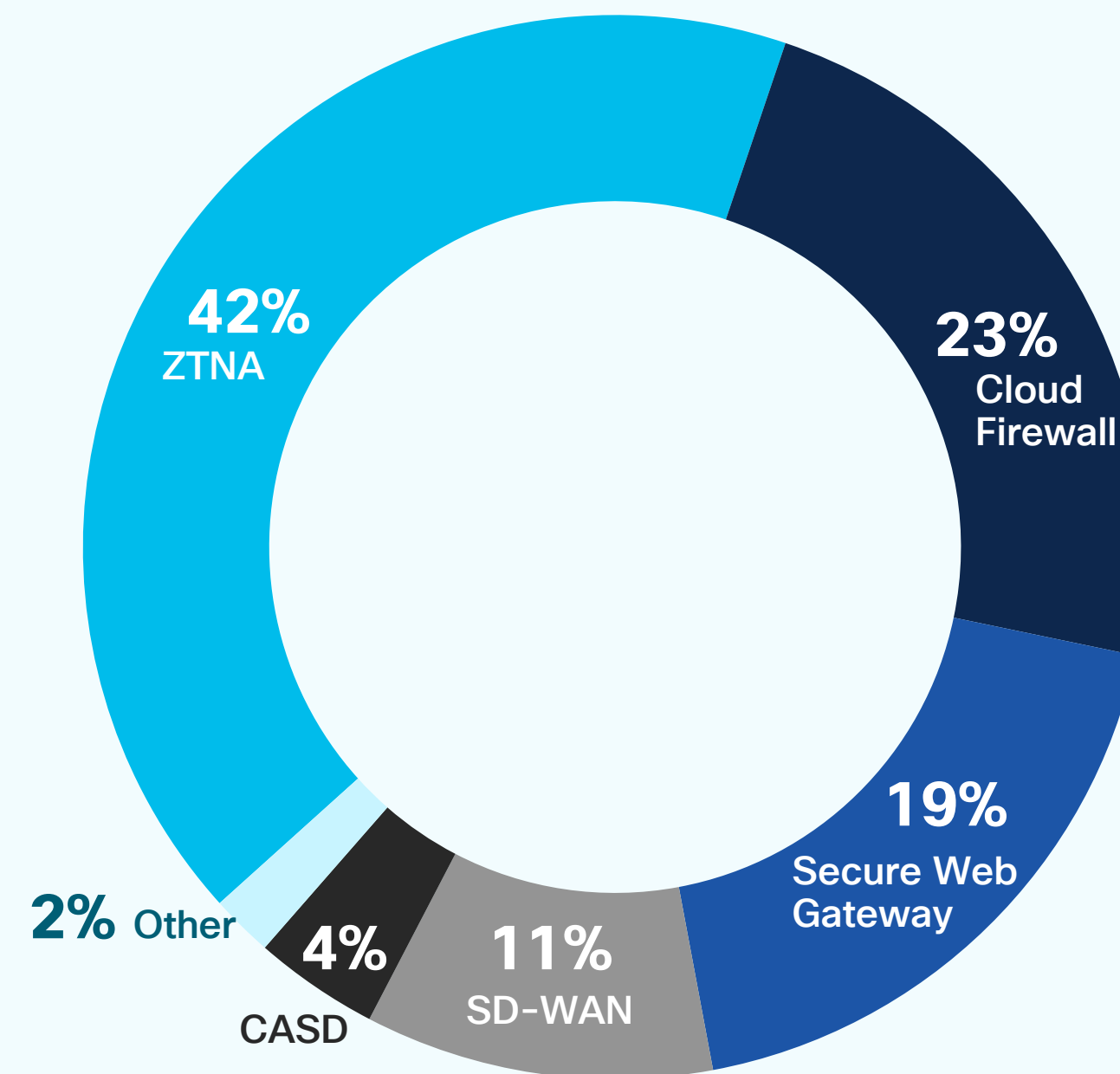
Up To
75%

intend to priortize their future IT security budget on SASE

Top Spending Priority within SASE
(among those who have adopted, have plans to adopt or are investigating SASE)

Zero-trust network access (ZTNA) is the top spending priority within SASE.

42%
ZTNA

23%
Cloud Firewall

19%
Secure Web Gateway

11%
SD-WAN

4%
CASD

2% Other

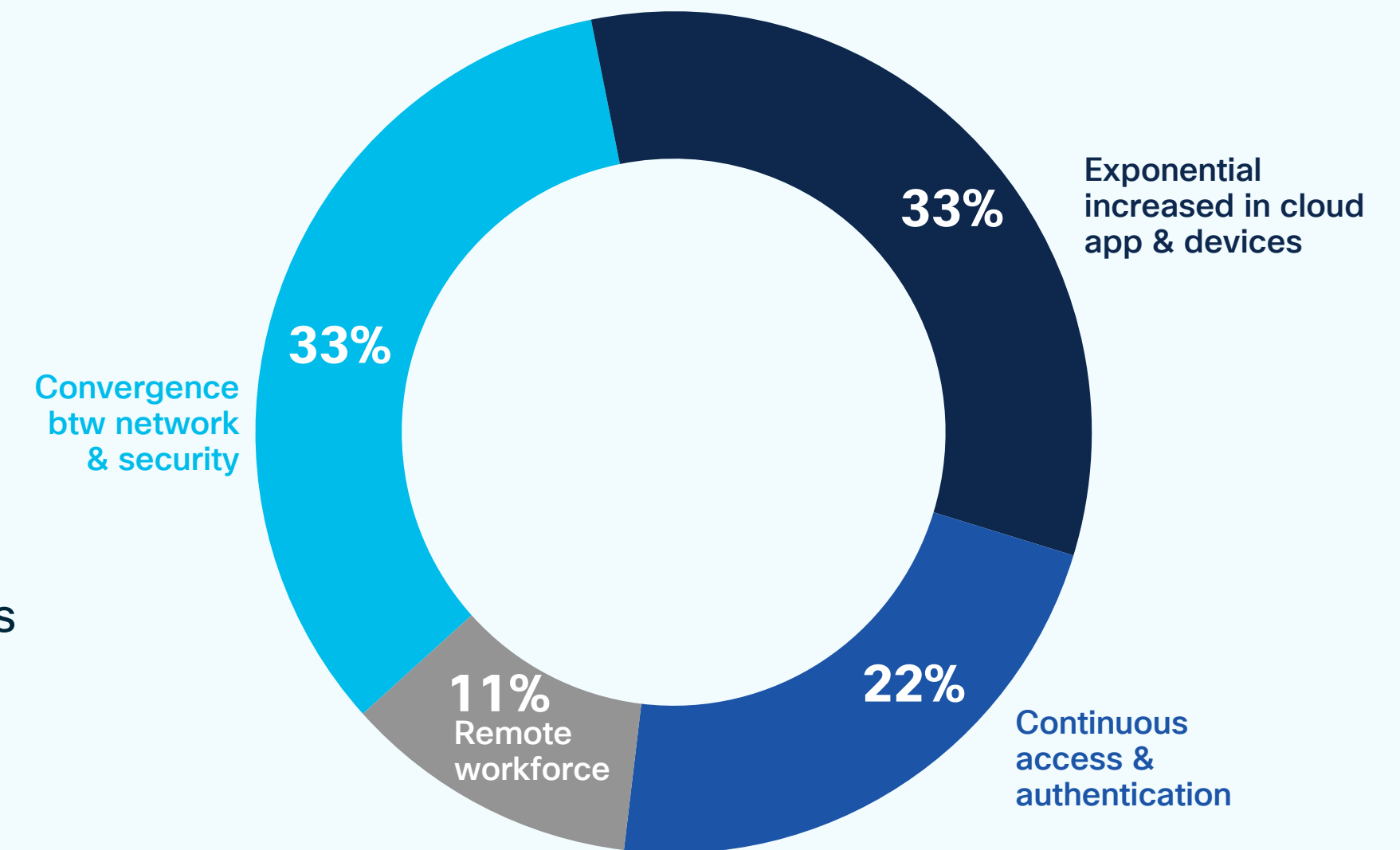# Convergence and complexity as top SASE drivers

98%
see clear benefits of SASE

We asked our survey participants to identify the top drivers for their SASE plans. The convergence between network and security areas tied with the exponential increase in cloud apps and devices at both 33%. In the process of asking this question, we also found out that 98% respondents have good visibility into SASEs benefits.

Implementation inhibited by maturity

We asked respondents to weigh in on what's inhibited their SASE implementation. Almost half (46%) identified a lack of mature architectures as a key factor. Hence, the need for a unified SASE architecture.

Motivators to Investigate/ Implement SASE
(among those who have adopted, have plans to adopt or are investigating SASE)

Respondents cite the convergence between network and security areas as the top driver for SASE plans.

- 33% Exponential increased in cloud app & devices
- 22% Continuous access & authentication
- 11% Remote workforce
- 33% Convergence btw network & security

Inhibitors to Implementing SASE

ASE implementation is most often delayed or inhibited by a lack of mature architectures.

- 46% Lack of mature architecture
- 25% Undefined/lack of spending budget
- 25% Multiple buying centers
- 3% Other
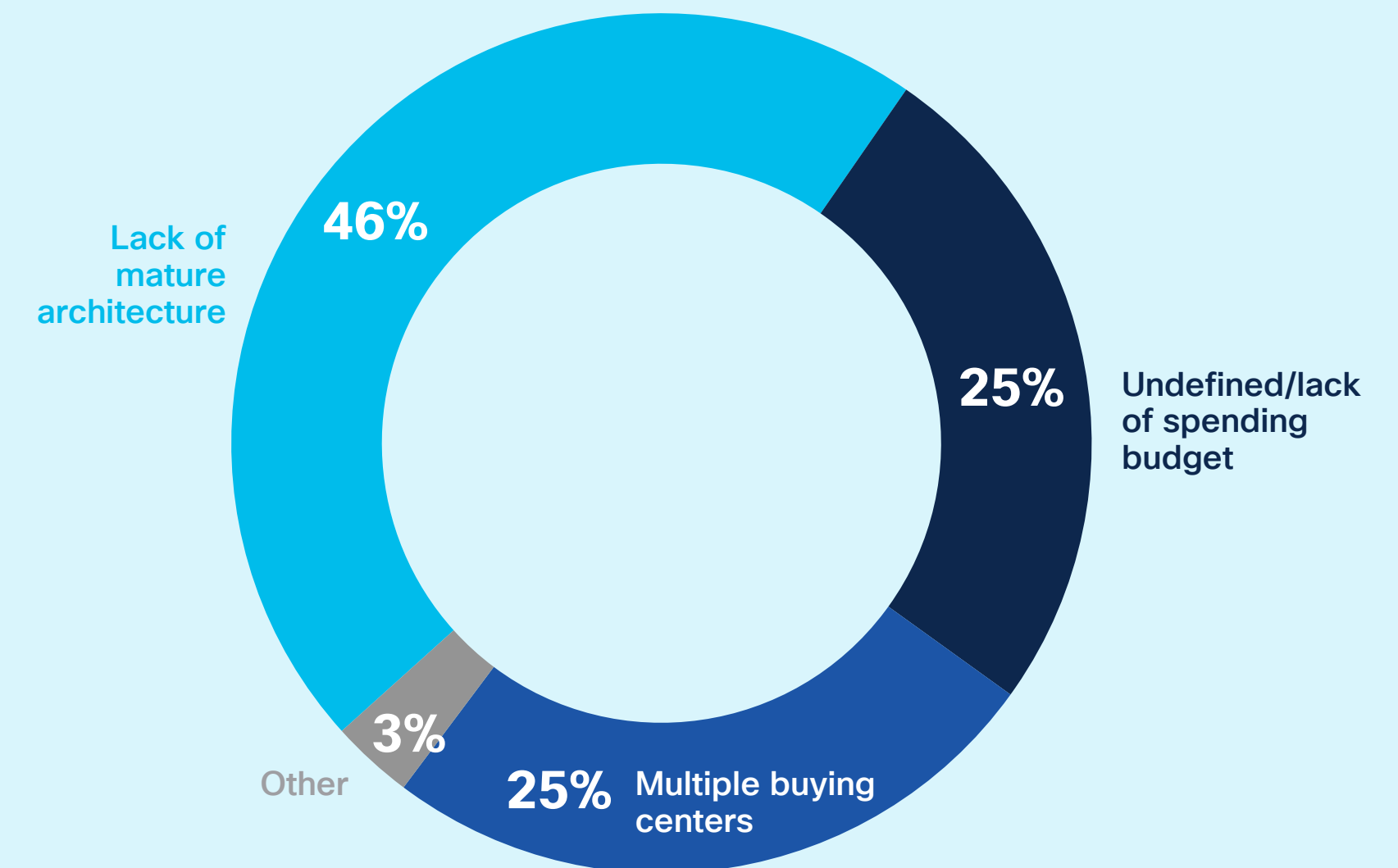
What This Means for CISOs

Advice from Your Peers

Start the journey today

Customers thus need to consider their regulatory and compliance environments when starting their SASE journeys. They also need to take the sophistication of their internal IT teams into account.

"SASE isn't a light-switch – it's a journey. So, start laying the groundwork and foundation today, or you're going to fall behind."

– **Jill Cochrane**
VP of Global Security Technology
at **MetLife**

Anchor SASE in ZTNA
Basic hygiene will go a long way in activating a SASE journey. It starts with foundational security measures such as MFA, identity, and access controls.

"Understand that – at its core – SASE is zero trust. We're talking about things like identity, authentication, access control, and privilege. Start there and then build out."

– Esmond Kane
CISO at **Steward Health**

Identify, inventory, and monitor data assets and userprivileges
You can't protect what you don't know about. That's why it's important to know what data you have, where it resides, and to what extent it's confidential and sensitive.

"It's the data in the cloud that's scaring the bejeezus out of everybody. That's why you have to leverage SASE to solve for things like edge monitoring and data loss protection."

– CISO
at a multi-national universal bank

Create a "fusion center" of the right teams
It's important to establish a strong connective tissue between security and networking teams. This will enable you to embed security controls within network traffic.

"Close collaboration is key between the security and network or infrastructure teams to successfully take on SASE. We kicked off our own SASE engagement by bringing everyone together at an off-site location. Going around the room in an ice breaker fashion where each person would share a few things about themselves really helped create connections and reduce back-and-forth unproductive emails."

– Bryan McDowell
VP and CISO at **University Hospitals**

Leverage APIs for automation
Customers want best-in-breed solutions. As a result, security vendors need to build API-centric platforms that can integrate seamlessly across aisles.

"Look at areas where you can steer away from manual and instead leverage APIs to add capacity to teams, especially in areas like secure orchestration automation and response."

– Greg Kyrytschenko
Deputy CISO at **Guardian**

Thomas Doughty, CISO at Prudential

One CISO's
SASE Journey

Thomas Doughty has been the CISO at Prudential for more than a decade and a half. He told us how his SASE journey began when he realized that he wasn't pursuing an endgame or a deliverable. We trace this fascinating story below.

Gartner was the first to coin the term "SASE" back in 2019. As it so happens, the Prudential team was embarking on a journey towards evolved IAM and zero trust at that time. So, we came to encounter SASE in that frame of mind.

The interesting thing is that there was never a decision point where we said, "SASE in and of itself is a deliverable." That still rings true. Just as I did back then, I look at SASE as an enabler for the outcomes that we're trying to achieve as opposed to an objective in and of itself. In that mindset, I find it sometimes kind of odd to describe it as "an edge." **It's more of a necessary enabler to help us get to where we want to be, deliverable-wise and architecture-wise.**

As examples, our committed directions toward software and services-defined proxy, web application firewall, and closer to zero-trust private access solutions fall within the common definition of SASE. But none of these architectural choices

are about 'implementing SASE.' They're about increasing network efficiency, more elegantly integrating a mosaic of external services, and improving user experience.

Thus began our SASE journey. And so, I started asking myself, "How do we use SASE to get where we need to be as opposed to thinking of it as a destination itself?"

I quickly realized that we couldn't leverage SASE in a meaningful way without making it a joint effort involving different parts of the organization. So, I made sure that one of our first steps was to get the network folks and the CTO organization to help us cover our use of SASE. There are interdependencies, and we decided to interlace our strategy and plans accordingly. We spent the last 18 months really trying to make sure we're integrated and understanding where that integration is taking place. This has led us to a truly global perspective of investment.

What does that look like in practice? For one, it means there needs to be a closed loop of understanding what the business and application owners' requirements are. We can build a software-defined stack, and we can define this, but if we're not looking at this from the application owners' point of view or the business stakeholders' point of view, we need to figure out why.

That's my first piece of advice when it comes to embracing SASE. My second recommendation? Use SASE to avoid replication. We really want to avoid the operational risk of parallel or duplicate investments. The point is if you're not careful, it can be replicable in the new environment.

Finally, be ready to tackle data overload. Once upon a time, we didn't have enough data in terms of doing analytics. In a way, we have the opposite problem now. How do you tune out the noise? It's become more difficult in two ways. On the one hand, there are new attributes of data that those programs and analysts are not as familiar with, and it's going to take some time to get familiar with tuning them. The other piece is the idea that you've got overlap, so none of the old on-prem data sources and volumetric expansion that comes from them have gone away. It's a classic bubble problem. We've got to do both for some interim. And it's additive for that interim instead of transitional.

At the end of the day, SASE really isn't just a security discipline or a security question. **It's about changing – but more importantly embracing – what the fabric of your network architecture (and frankly your underlying application architecture) is as well as what you expect of it.**

Executive Summary

- Privacy and compliance remain top of mind due to regulations such as GDPR in the European Union, CCPA/CPRA in California, LGPD in Brazil, and new proposed legislation such as Bill C-11 in Canada. Currently, there are over 140 privacy laws globally, and the global regulatory landscape will only become more complex moving forward.

- With the public increasingly valuing privacy, data breaches now have measurable consequences in terms of eroding trust and brand value on top of monetary fines and civil damages.

- Data access control is the top privacy concern for nearly half of CISOs.

- Privacy is a mindset, so CISOs recommend building awareness across the entire organization through dedicated training and board-level visibility.

- Similar to SASE's convergence of networking and security, a new category of privacy engineering is emerging to manage data access, authorization, and other technical privacy controls "by design."

Privacy & Compliance

NORWEST | VENTURE PARTNERS

Introduction

The days of a neatly defined network perimeter seem so far away. Prior to 2020, hybrid environments already enabled employees, partners, and others to access corporate resources hosted in the cloud. Then the pandemic hit, and the shift to remote connectivity became essential for businesses to survive and thrive.

These developments have reshaped organizations' security focus—at least to a certain extent. For instance, there's the growing recognition that organizations can no longer concentrate on protecting devices, networks, and endpoints. These assets are just too dynamic in nature. In response, organizations are beginning to emphasize the need to protect their data itself.

Many are experiencing growing pains along the way. The reality is that many organizations don't know what data they have, where it's stored, who has access to it, and what it's used for. This doesn't bode well for business continuity. Organizations are under pressure from GDPR, the California Consumer Privacy Act (CCPA), and similar data privacy regulations around the world. If they don't adequately protect their data, they could face some big compliance fines—or worse, erosion of trust with their customers. Having robust privacy is foundational to ensuring good security – you cannot have good security without good privacy.

None of this is lost on VCs. That's why in 2020, over $800M was invested in privacy and compliance tech companies like **OneTrust**, **BigID**, and **Securiti**, according to Pitchbook data. Over the past two years, there has been a large volume of new company formation at the seed and Series A stage. Taken together, this activity signals a growing focus around helping organizations to consolidate their privacy and compliance efforts going forward.

Startup Landscape

Privacy and compliance startups generally fall into one of five primary categories.

1. **Data Access & Authorization**

2. **Privacy Platforms**

3. **Data Management**

4. **Compliance Automation & Asset Management**

5. **Workflow Automation**

SURVIVAL
GUIDE

Privacy & Compliance

Data Access & Authorization

Managing which individuals have access to data and what they are doing with that access

SPHERE · CLOUDENTITY · styra
ermetic · Authomize · britive
SYMMETRY SYSTEMS · CLOUDKNOX · Cyral
COOKIE.AI

Privacy Platforms

Identifying and discovering where data containing PII resides inside your organization

OneTrust · DATAGRAIL · BigID
PRIVACERA · TrustArc · securiti
ETHYCA · wirewheel
Relyance · satori

Data Management

Cloud data lakes, data governance, secure enclaves and data masking

IMMUTA · gretel · evervault
Collibra · dremio · Skyflow
PRIVITAR · Alation · OKËRA

Compliance Automation & Asset Management

Automating SOC 2 compliance and audit preparation, continuous user and endpoint management

Vanta · LAIKA · ANITIAN
Uptycs · JupiterOne · secureframe
DRATA · tugboat logic

Workflow Automation

Automating repetitive processes and privacy incident response

tines · TerraTrue · Transcend
DeepSee · usercentrics · BREACHRX
RadarFirst · osano

Source: Norwest Venture Partners for the CISO Survival Guide 2021

What We're Hearing from CISOs

Data access control a top priority

44%

say that data access control is top priority

We asked CISOs to name their top privacy priority. In response, nearly half (43.8%) of respondents said that data access control was their chief focus. That explains why VCs are investing in companies like **Cookie.AI**, a cloud-first data security platform which helps CISOs to answer the questions, "Who has access to what data?" and "What are they doing with that access?"

Access control is familiar to security, and it's just the beginning. Keeping bad guys out and letting in only those who are authorized to have access is essential, as security is foundational to privacy. Privacy goes much further and addresses how those who are authorized to have access handle personally identifiable information (PII).

Conflicting privacy policies and requirements the greatest challenge

The top challenge facing survey participants in their privacy and compliance program was conflicting interpretation of privacy regulations, policies, and requirements (43.2%). Privacy regulations tend to be principles-based and focus on the outcome (ie, the "what") that is expected.

Companies are given wide latitude to devise the "how" and methods to comply, which adds to confusion, conflict, and inconsistency. A central, authoritative voice (i.e., a Chief Privacy Office) is required to set clear standards and implementation guidance for a uniform application.

43%

say that conflicting interpretation is a top challenge

**34%**

say that identification is a top challenge

This was followed by the identification and location of PII (34.0%). As noted above, it is critical that business understand their data. If you don't know what you have, you can't properly protect or respect privacy. These results underscore how an evolving regulatory landscape is making it more difficult for organizations to understand and then fulfill their compliance obligations.

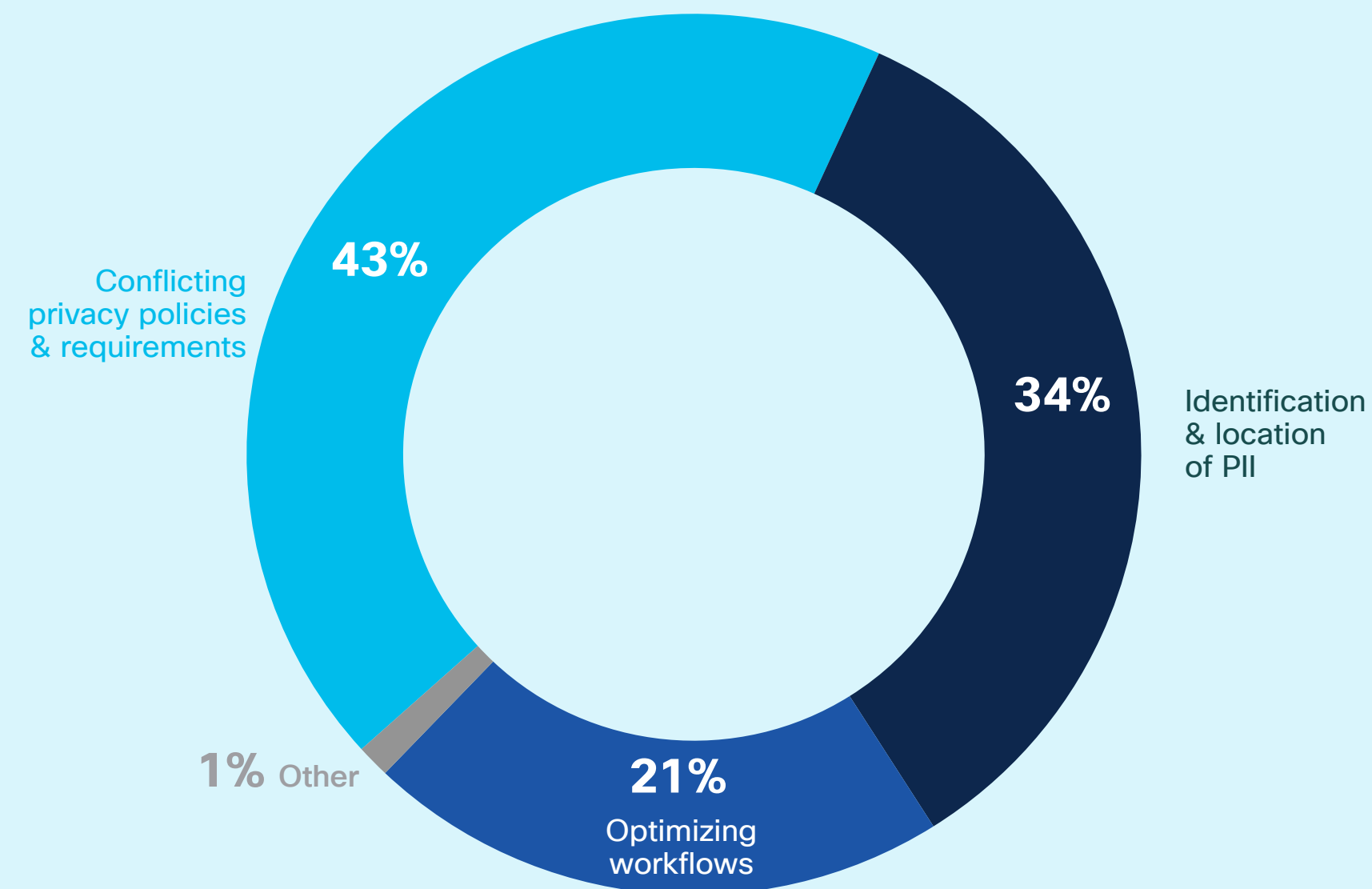# Privacy & Compliance
Survey Results

Top Privacy Priority
(among those who have adopted, have plans to adopt or are investigating SASE)

Data access control is the top privacy priority, followed closely by data subject right requests.

44%
Data access control

35%
Data subject right (DSR) results

3%
Other

18%
PII discover & mapping
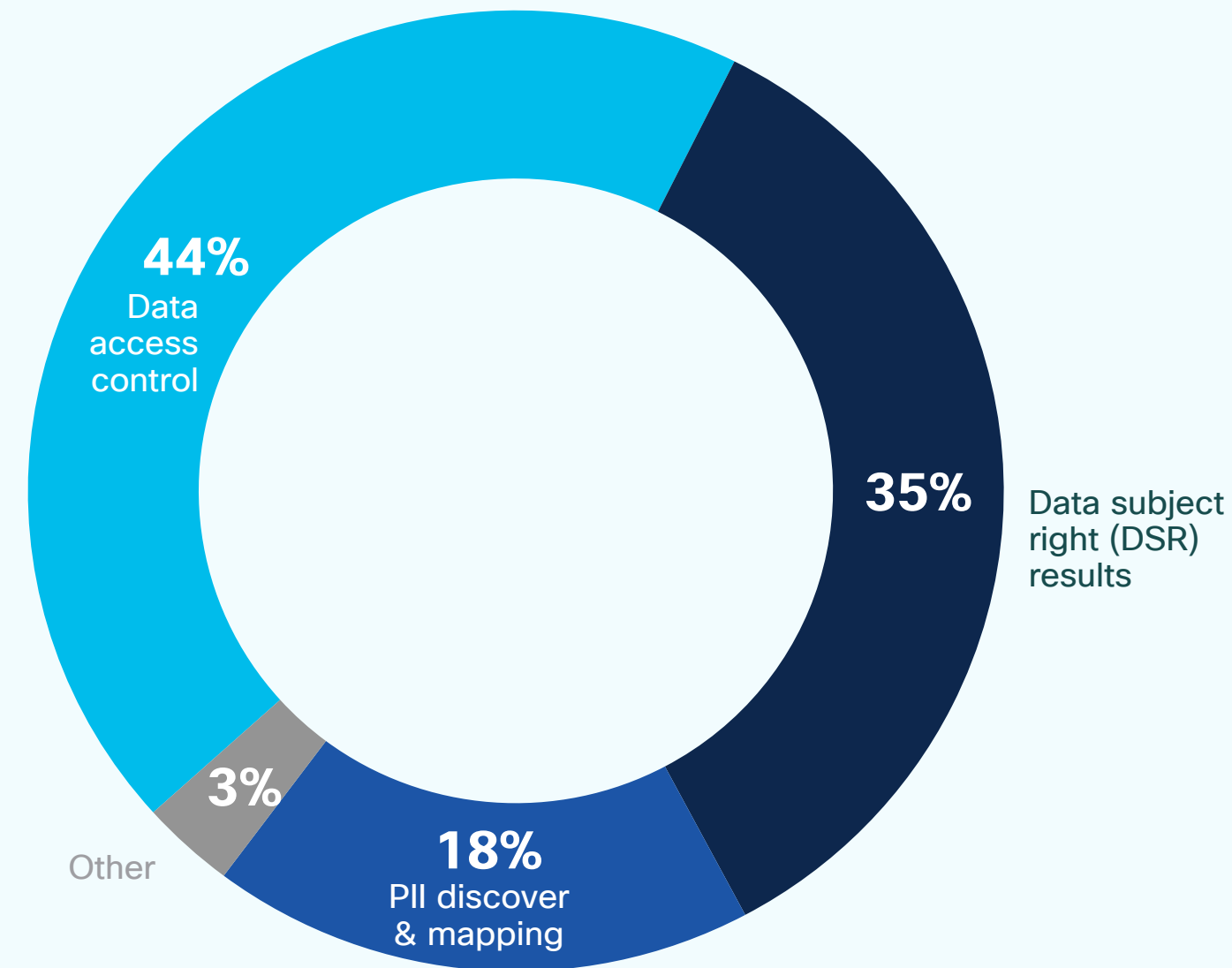
Challenges with Respect to Privacy and Compliance

Nearly one half cite conflicting privacy policies and requirements as their top privacy and compliance challenge.

43%
Conflicting privacy policies & requirements

34%
Identification & location of PII

1% Other

21%
Optimizing workflows

SURVIVAL GUIDE

Source: IDG survey for the CISO Survival Guide 2021

What This Means for CISOs

Advice from Your Peers

Partner closely with your privacy team and optimize for the long term

CISOs should partner with their Chief Privacy Officer. (If your company doesn't have one yet, advocate to get one.) Privacy is dependent on security, for sure, but it's also a distinct discipline in and of itself. In security, the focus is on the risk and impact to the company and its assets.

"**Building a robust privacy program will take years.** As such, creating a strong foundation by identifying where all PII is located and implementing north star privacy best practices is a great starting point."

– CISO
at a global financial firm

Privacy, on the other hand, considers the risk and impact to the individual. It is a fundamental human right. Protecting PII (security) is essential and necessary but not sufficient.

After speaking with numerous CISOs, we found that many took the below steps in their privacy journey:

• Work with the privacy team to understand and meet privacy's legal requirements for the geographies where they operate

• Map the data so they know what data they have and how it needs to be handled

• Build privacy into the development process and ensure it is always considered before a decision is made

• Work with customers and internal stakeholders to be transparent on how data is used and handled by the organization

• Embrace privacy training to continually build awareness

Privacy and compliance are ever-evolving as new regulations, guidance, and/or industry standards come online just about every other month. Startups are building next-generation solutions to track and tackle these changes. Exploring privacy and staying on top of privacy startup technology might help as you define your privacy programs.

Focus on people and process

Privacy, like cybersecurity, is a mindset. They are not just the responsibility of a single department but a shared responsibility for all who handle PII. With that said, tools and software might be necessary to execute and implement privacy standards consistently at scale, but investing in best-of-class tools alone does not guarantee protection. Before selecting a vendor, ensure that your internal business partners (e.g., engineering, IT, legal, procurement, etc.) are aligned on requirements, the desired outcome, and how the solution will be incorporated into existing workflows. Several start-ups and privacy compliance vendors, for example, have digitized the privacy impact assessment (PIA). Centralizing on a digitized platform provides consistency and holistic reporting, but unless processes are in place to drive traffic to the PIA and people who are knowledgeable about the processing activity and business purpose, the PIA tool is useless. As always, people, process, and technology are required for an effective compliance program.

"**No tool can fix a broken process.**"

– CISO
at a multi-national engineering firm

Build privacy awareness at the board level

Security and privacy both need to be regularly discussed by the Board. Privacy is not just required for compliance, with potential fines of up to 4% of gross revenue and executive incarceration in some jurisdictions. It is also central to trust, brand, and market access. Failure to properly address privacy may limit a company's ability to sell and may have a material, negative impact on revenue. (e.g., EU customers subject to GDPR are not able to buy and use products without appropriate protections, features, and functionality for privacy.) There are over 130 countries with omnibus privacy legislation that are generally aligned with GDPR on core values and individual rights. If your business handles PII, you must be able to demonstrate PII is properly protected and individual rights to their data respected. Privacy is a business imperative that warrants Board-level visibility and oversight. (GDPR requires the data protection officer to report directly to the "highest management level" of the company.)

"**Ensure that security and privacy initiatives are represented at the Board level. While most companies track compliance through the audit committee, having full Board awareness for privacy and security goals will help you ask for the resources you need to implement programs.**"

– CISO
at a regional healthcare system

Patrick Joyce, CISO at Medtronic

One CISO's Privacy & Compliance Journey

Patrick Joyce is vice president and chief security officer (CISO & CSO) at Medtronic. He has been with the company since 2005, serving in a variety of senior IT, security, and audit leadership roles.

How have you approached privacy and compliance?

In the world of security and privacy, there are a significant number of gray areas. GDPR and similar privacy legislation around the world call for a risk-based approach to compliance. Oftentimes, the answer to questions related to how to address a particular privacy requirement or what the level of appropriate risk is, "It depends." Take GDPR's "data minimization" principle (Article 5(c)), for example. "[P]ersonal data shall be… adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." What is appropriate will depend on the circumstances and reason for collection. As such, it will vary greatly. Your treating physician will need your name and the sensitive PII in your medical record. Medical researchers, on the other hand, can work with de-identified aggregate data, and they don't need PII.

As with many companies, GDPR and other regulations catalyzed the need for all of us to better understand what kind of data we have, what applications it lives in, where it's stored, how it's protected, and who has access to it.

Security is foundational to privacy. You cannot have privacy without good security. Therefore, it is important to ensure you have the appropriate control frameworks and audit cadence to both assess and address privacy risks.

How have you implemented privacy controls?

We have worked closely with leaders across the company to not only locate and secure sensitive personal data but to also analyze whether they truly need the data or not. Privacy is a mindset first and should be a deeper responsibility that every stakeholder and handler of PII feels ownership and responsibility over. For example, before we make a decision to store data, we ask the business, **"How critical is it to have this data? Can you learn what you need another way?"** We looked for vendors who could help us on this journey and found startups who were rethinking data privacy and access controls.

What advice would you give to a CISO that is early in their privacy journey?

Start by building awareness and education throughout the entire organization. There are many real-world examples where personal data has been exposed through a breach. Creating empathy on the ramifications of data loss to us as individuals is important and helps make privacy real. Privacy is as much a human behavioral risk as it is a technical issue. The decisions made on how to handle personal data and who to share it with have consequences to real people. **Humans are the weakest link. Most employees aren't security experts**; they might end up clicking on a link without considering whether it's suspicious. Therefore, to build privacy awareness at Medtronic, we require all employees to complete ongoing privacy training in addition to our continual security awareness and training.

Executive Summary

- DevSecOps is relatively nascent compared to some of the other trends discussed in this guide. With that being said, we are witnessing a growing emergence of DevSecOps startups.

- The role of security teams is changing when it comes to DevOps security practices, and security policies as code are already very prevalent.

- In support of DevSecOps, CISOs are actively expanding software-driven security policies, adopting security tools for developers, and applying security tools and methods across the entire scope of the DevOps pipeline.

DevSecOps

YL VENTURES

Introduction

The "need for speed" at the core of DevOps has exposed organizations to greater risk. A faster development lifecycle means coding mistakes that could interrupt developers' workflow or expose customers' data. It also means challenges for security teams to do their jobs in a way that doesn't inhibit breakneck software delivery speed.

Many organizations have responded by bringing DevOps and security together under DevSecOps. This set of products and practices enables security, development, and operations teams to collaborate around secure application development in modern development environments without sacrificing speed.

DevSecOps is still relatively nascent compared to some of the other trends discussed in this guide. That makes it difficult to clearly understand the current state of the DevSecOps market. But it's possible to gain some insight by looking to Application Security, a market of which DevSecOps is a part.
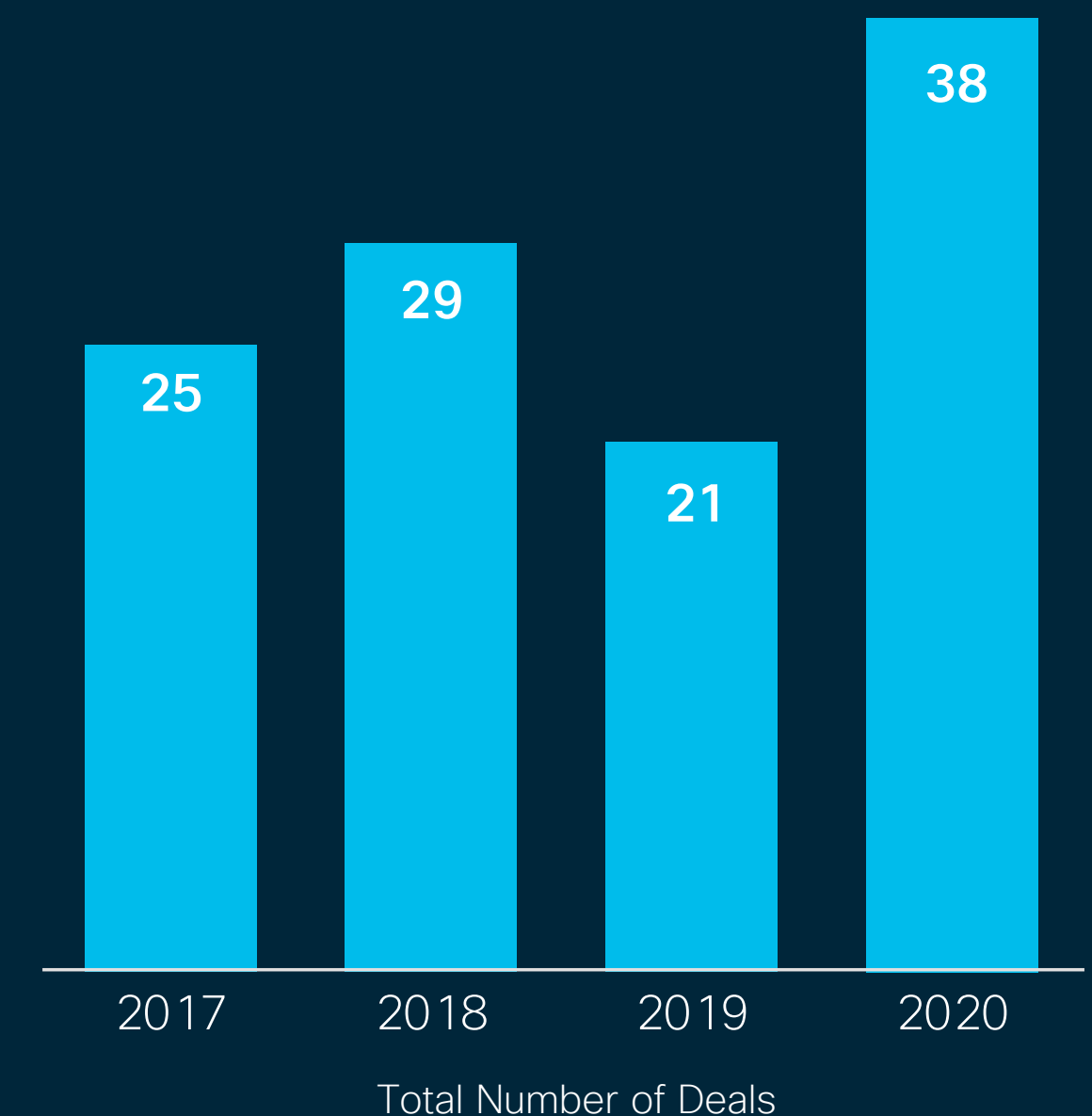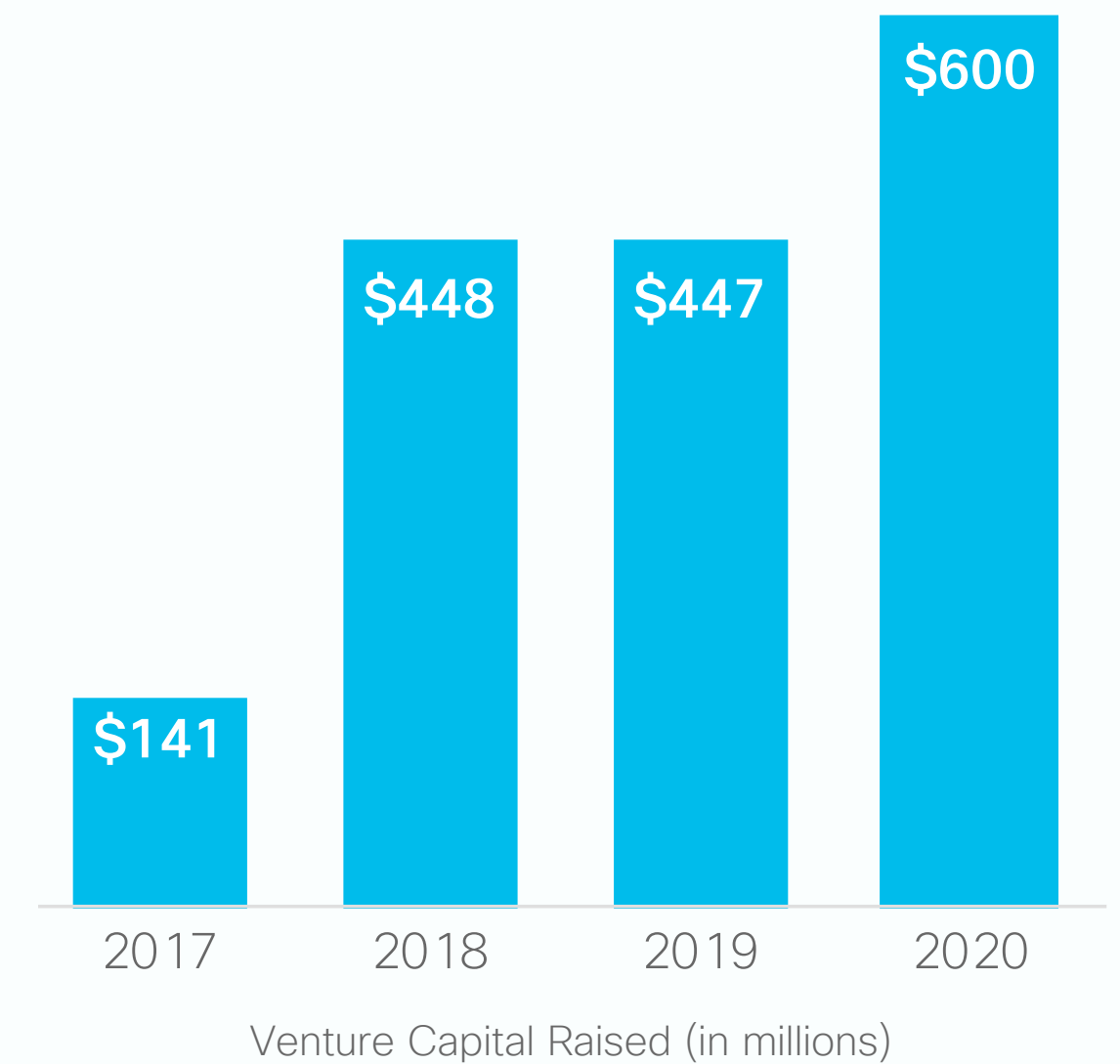
There was rise in Application Security investment from $141 million in 2017 to $600 million in 2020, according to

Pitchbook data. Several companies contributed to this growth of private capital. For instance, developer–first security company **Snyk** became a cybersecurity unicorn in January 2020 when it announced that it had raised **$150 million in Series D financing**, after which it continued to raise a **$200M Series E financing** during the same year.

M&As in the Application Security domain fluctuated over the same period, generating a total of $2.5 billion between the years 2017–2020, according to Pitchbook data. The acquisitions of two companies fueled this rise. One of them was **Checkmarx**, a leading static analysis security testing company which was **acquired** by **Hellman & Friedman** for $1.15 billion.

Despite its relative novelty, many organizations are already taking DevSecOps to heart. Most have implemented "security as code," and others are working to transition their security teams from applying application security practices to a position of providing governance and guidance. This work lays the foundation for organizations to shift security everywhere in the DevOps pipeline.

Capital raised in the Application Security domain:

2017	2018	2019	2020
$141	$448	$447	$600

Venture Capital Raised (in millions)

2017	2018	2019	2020
25	29	21	38

Total Number of Deals

Startup Landscape

Four segments stand out to us in the DevSecOps sector.

DevSecOps

Code Security

Scan code to detect vulnerabilities or issues affecting code security

CONTRAST SECURITY · PortSwigger · SECURE CODE WARRIOR
NowSecure · WhiteSource · snyk
ShiftLeft · FOSSA

Securing Developer Enviroments

Manages security configurations and check for risk posture

cycode · enso · concourse labs
NowSecure · apiiro · oak9
GitGuardian · accurics ·
BLUBRACKET · Spectral · SECURE CODE WARRIOR

Code Detection & Response

Secures application code form potential and actual attacks through attack detection

SALT · noname · acunetix
accurics · NowSecure
CEQUENCE SECURITY · CONTRAST SECURITY

Security Policy as Code

Uses codified policies and automated enforcement to protect from threats and disruption

build.security · styra · OSO
Aserto · apolicy
accurics

Source: Norwest Venture Partners for the CISO Survival Guide 2021

What We're Hearing from CISOs

DevSecOps
Survey Results

Most strive to become focused on governance

We asked respondents what challenges they foresee or have experienced with developers using security tools. Nearly all (93%) of them mentioned the task of bringing a governance focus into app development. Security analysts, architects, and other practitioners are increasingly less hands-on in using application security products. They're providing policies and structures to developers, who increasingly own the operation of security tools.

93%
challenged to transition to being governance focused in app dev

Security as code is already a big trend

Security-policy-as-code (SPC) is the practice of writing code to manage and automate security policies. We asked our respondents about the different SPCs that they've implemented. Only 3% of respondents said that they do not implement security as code, and as such, security as code is already a big trend.
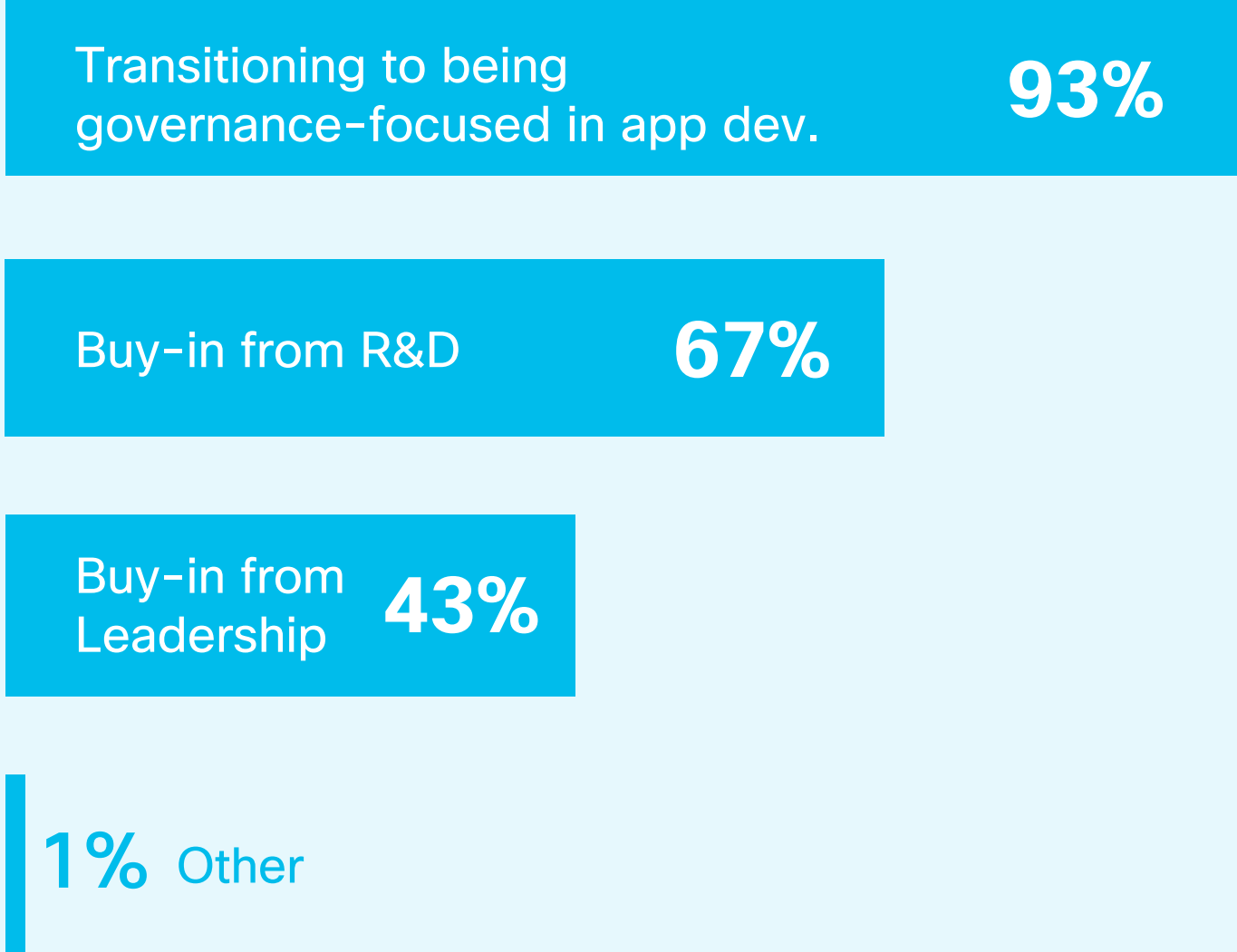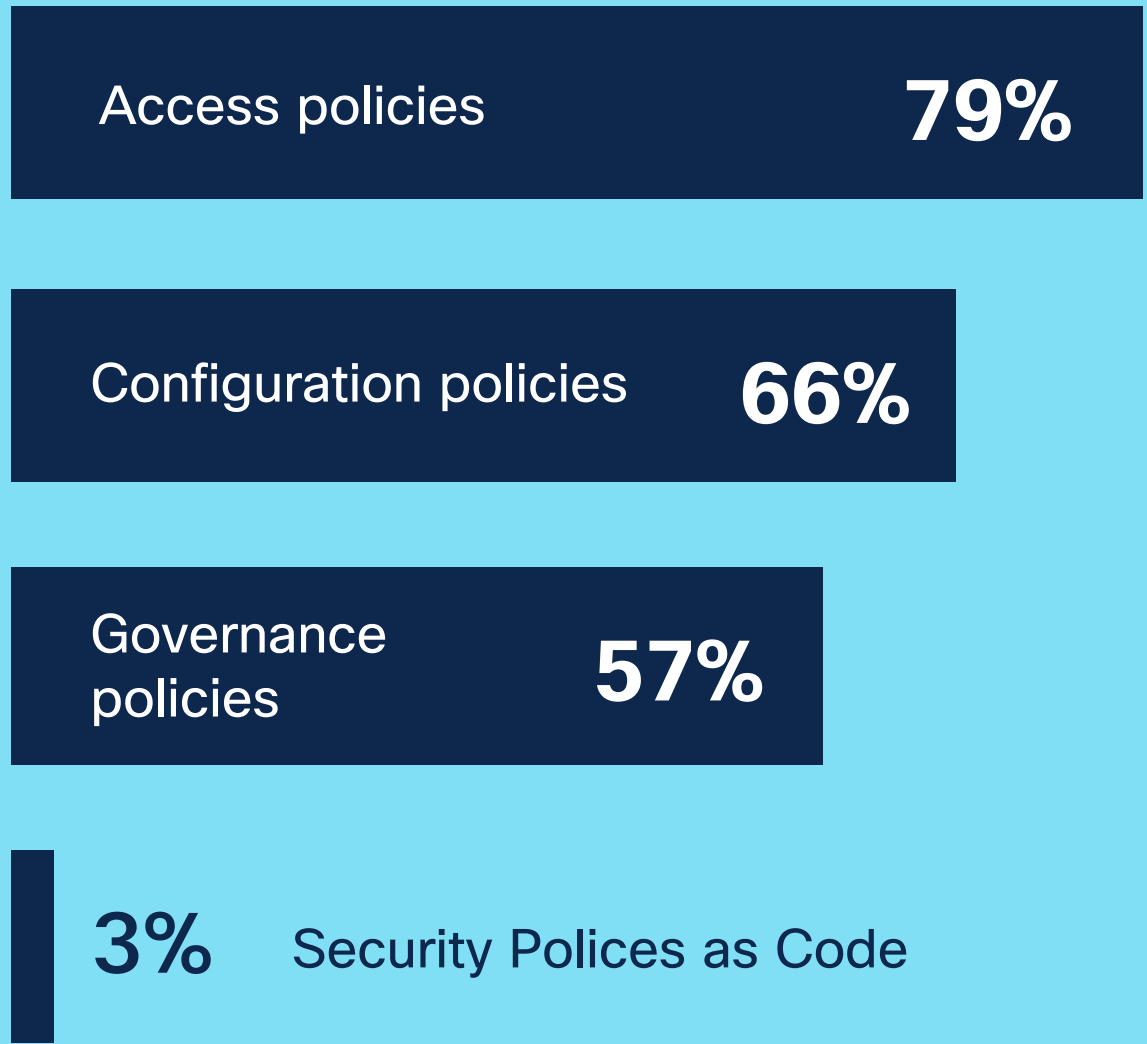
97%
implement some form of SPC

Challenges with the Use of Security Tools by Developers

Transitioning to a focus on governance during the development process is the top challenge with developer use of security tools.

Transitioning to being governance-focused in app dev.	**93%**

Buy-in from R&D	**67%**

Buy-in from Leadership	**43%**

1% Other

Implementation of Security Policies as Code

The use of security policy as code is prevalent in respondents' organizations; access policies are cited as the top implementation.

Access policies	**79%**

Configuration policies	**66%**

Governance policies	**57%**

3% Security Polices as Code

Source: IDG survey for the CISO Survival Guide 2021

What This Means for CISOs

Advice from Your Peers

Adopt security tools for developers

Until recently, application security was carried out in a "top down" approach, with security teams imposing security methodologies, tools, and practices on developers. Nowadays, application security is moving to R&D. This necessitates a "bottom-up" approach where developers measure security success and apply security controls.

"In order to effectively implement security tools for developers, it is essential to make developers accountable for security functions. Security should be guiding developers in explaining tool functionality, creating SLAs for security, and providing data sources and customer requirements."

— Andy Ellis
Operating Partner at YL Ventures and former CSO at **Akamai**

Adopt security-policy-as-code
(AKA software-driven security governance)
When setting security policies, using all sorts of security mechanisms as code enables better security governance. That's the reality of modern development environments that are increasingly complex and code-driven. It makes sense for security to keep pace by becoming software-driven and automated itself.

Shift from "shift-left" to "shift everywhere"
The old "shift-left" approach mentality aims at applying security controls at an earlier stage of the development lifecycle. By contrast, "shift everywhere" involves injecting security wherever we can overall in the pipeline. It's a nascent approach, though some companies are beginning to adopt it into certain sections of their DevSecOps pipelines.

"In the future, software-driven approaches will be an essential component of security governance. Much of how we build technology today is highly automated, but unfortunately, many security teams haven't caught up and are stuck in onerous manual processes. Security needs to embrace software-driven security governance to catch up to modern application development practices."

— Sounil Yu
CISO & Head of Research at **JupiterOne**

"Shifting security controls across all points in the DevOps pipeline is now possible, as more security functions are carried out as software. Software-driven security controls automate security and are easily replicated across the pipeline."

— Andy Ellis
Operating Partner at YL Ventures and former CSO at Akamai

23

Anonymous, CISO at a high-growth and cloud-native SaaS company

One CISO's DevSecOps Journey

When you are building the security practice of a cloud-native and high-growth SaaS company, you are inevitably going to be at the heart of DevSecOps practices and technologies. This CISO built a developer-focused Application Security program from the ground up. We're happy to share their growth story.

The ever-changing Application Security landscape requires a process of constantly updating workflows between security, operations, and development. That's the only way to catch up with modern development environments and practices. The challenge is even greater when you're the CISO of a company whose sole product is software, as applications are a core component of what the business is all about.

As such, it was very clear to me from the onset how embedded in the development lifecycle my team and stack needed to be. It was also clear just how crucial cooperation between R&D, security, and operations would be going forward.

In thinking about how to build a DevSecOps infrastructure, I decided to first deploy security tools for developers to scan code as it's submitted to GitHub. We implemented some tools that are designed to specifically search for issues and vulnerabilities such as OWASP's Top 10 as well as other weaknesses and coding issues.

A big issue that many security leaders encounter when it comes to DevSecOps is the extent to which developers and R&D will be motivated and cooperate with security controls for code. I was happy to realize our developers were extremely supportive of what we as the security team were trying to do and promote. They've implemented security tools really well. This reflects just how vital it was for us to design tools and methodologies with minimum impact on engineers. Nothing is ever perfect, of course, and we did receive some pushback, but it was not substantial.

Looking back on my journey, the biggest piece of advice I have is to try to continuously understand engineering workflows and to integrate into them. Do not force engineers to change workflows. In fact, try to minimize the need of engineers to add more steps into their processes, and don't slow them down or cause friction.

My second piece of advice would be to prioritize security-policy-as-code. We're very much focused on this right now. If R&D is continuously being automated, so should security teams. The focus should be on doing this in a way that enables us to use code for security controls at scale.

Lastly, I would advise CISOs to apply security controls across the entire development pipeline. We're trying to instill the use of security controls each step of the way. We scan the CI/CD every day, and we use penetration testing and as well as a bug bounty program at the backend for code that's already in production. As each individual control will have a certain success rate, you want to have controls at every checkpoint.

Ultimately, DevSecOps is not just about bringing in the best tools to contend with modern development practices and environments. **It is about building a relationship and collaborating with development, from individual contributors to R&D leadership.** It's also about bringing the DevOps team on board the security train. As security teams are no longer the sole proprietor of security, collaboration and partnership are key to a successful DevSecOps program.

Executive Summary

- Every organization is adopting automation at each layer of defense based on their organization's business model and security program maturity. Many CISOs identified inventorying network assets and protecting databases as priority areas, though overall automation across the security stack is happening at different rates and focus areas.

- While DevSecOps solutions are "shifting left" and "shifting everywhere," overall financing has "shifted right" towards detecting and responding. This is reflective of startup innovation "shifting right" to address the needs of the industry during and post incident.

- The security industry is evolving in multiple categories at once due to significant, new, and expanding changes impacting the modern organization – from increased breach disclosure guidelines to privacy to public cloud to DevSecOps and recent expansion in employees working from home.

Automation

Introduction

While every CISO has a different expectation of what needs to be automated, there are typically three factors at play that underly all automation needs.

The first is resource constraints. Security skills are rapidly evolving with the threat landscape, a trend which is compounded by pandemic-accelerated digital transformation and remote work. Indeed, a remote workforce introduces new challenges for IT and security practitioners given an ever-changing attack surface, remote-work infrastructure and devices, and new threats. Organizations are realizing that they can augment some skills with technology to improve productivity and streamline operations.

The second point is the amount of noise that security practitioners must deal with. Even the most experienced practitioners don't have the capacity to address every alert or notification. Technology is better at processing large amounts of data and identifying patterns. Automation makes it possible to prioritize.

The third factor is speed. Time matters in cybersecurity and in the ability to quickly respond to potential incidents. The most effective solutions oftentimes aren't the most technically advanced. They're just faster.

PROTECT
# #1
automation priority

These factors all shape where CISOs direct their automation focus. To illustrate, we looked at cybersecurity financing aligned with the five functions of NIST's Cybersecurity Framework – "Identify," "Protect," "Detect," and "Respond/Recover" – to observe which areas are attracting more venture capital dollars and, by proxy, startup innovation. Investment in "Protect"-focused companies received the greatest amount of investment in 2021 YTD at 31%. This was followed closely by investment in "Identify" and "Detect" at 29% and 27%, respectively. "Respond/Recover" received the least amount at 13%.

IDENTIFY
#2
automation priority

These statistics highlight how organizations each experience unique challenges in the "Identify," "Protect," "Detect," and "Respond/Recover" cybersecurity phases. It's this variability that shapes what an organization's automation journey looks like.

Investing in innovation over time saw the largest shift from protecting to detecting incidents.

	2019	2020	YTD 2021	
Respond/Recover	11%	11%	13%	
Detect	10%	19%	27%	
Protect	52%	42%	31%	
Identify	28%	28%	29%	
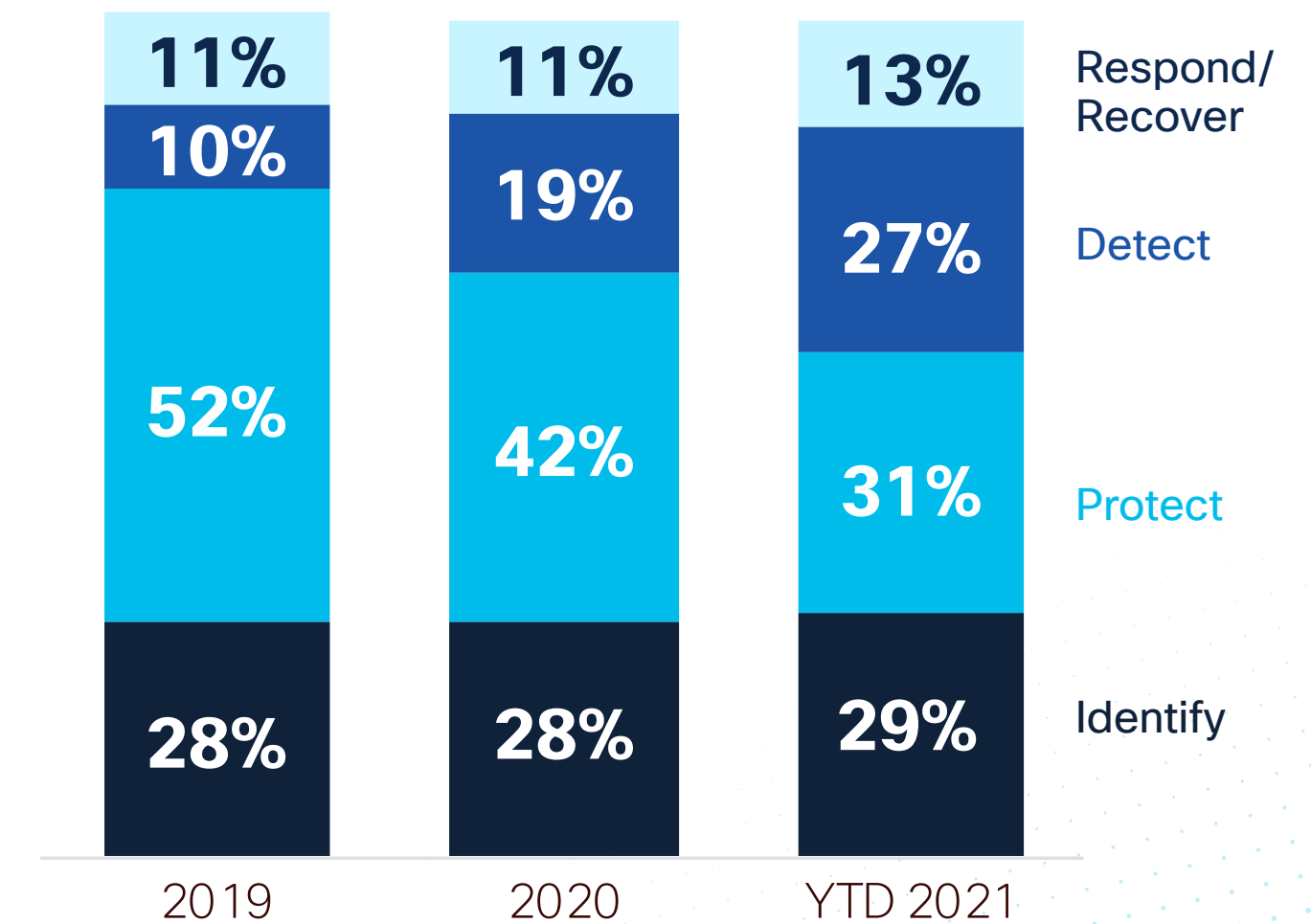
Startup Landscape

We used the NIST Cybersecurity Framework to classify automation-focused startups into four categories.

IDENTITY

DATA

APPLICATION

NETWORK

ENDPOINT

Identify

- 1KOSMOS BlockID
- AXONIUS
- exabeam
- FLASHPOINT
- JUPITERONE.
- loginradius
- panaseer
- SPHERE
- Strata
- RUMBLE
- Remediant
- THREATQUOTIENT
- VULCAN.
- BISHOPFOX

Protect

- ANITIAN
- BehavioSec
- Cynet
- CLOUDENTITY
- concourse labs
- exabeam
- NowSecure
- panaseer
- SYMMETRY SYSTEMS
- BAYSHORE Industrial Network Security

Detect

- AREA 1.
- Constella INTELLIGENCE
- Dtex systems
- exabeam
- HUNTRESS
- IronNet
- REVERSING LABS
- THREATQUOTIENT
- Uptycs
- Hunters

Respond/Recover

- CYSIV
- exabeam
- CyberCube
- IDExperts
- Own {backup}

What We're Hearing from CISOs

Network the most difficult asset to identify

60%

see the network as the most difficult to inventory

We heard from CISOs that they need the most help with managing their network and identities. More than half (60%) believe the network is the most difficult to inventory. Shadow IT isn't going away, and the proliferation of applications, data, and endpoints only makes it harder. That's why IT asset management companies leverage automation and integrations to discover assets, identify risk areas, validate against security policies, and enforce these policies.

Databases the protection priority for organizations

CISOs identified databases as a top priority when it comes to protection. Data is the crown jewel of modern organizations, and losing data is the difference between security "incident" and "breach." To gain an accurate understanding of an organization's risk profile, CISOs need visibility into what data they have, where it is stored, and who has access. This is easier said than done. Data is spread out between data stores, databases, and data lakes, and it is constantly pooled into a large network of applications hosted in multiple data centers. Automating data classification and correlation can help you figure out how your data is used, accessed, and managed.

CISOs most concerned about detecting phishing attacks

We heard from CISOs that automation has been most helpful with the detection of phishing attacks and application vulnerabilities. Phishing is the #1 attack vector for organizations, resulting in nine out of 10 breaches. The rising volume and sophistication of attacks has been a struggle for security practitioners. To help organizations, next-generation email security solutions like **Area 1**, **Abnormal**, and **Material Security** leverage automated triage and detection for both traditional and cloud email providers.

Blocking threats the lowest-hanging fruit for automation post incident

Respond is the function that leverages automation the least, as each remediation will be unique to an attack and the affected underlying environment. That said, CISOs told us that automation can most help with blocking the threat from causing further damage and connecting the dots with integrations.

Data and applications the most critical assets for post-incident restoration

We heard from CISOs that data and applications are the highest priority assets to restore post incident. These are critical areas in getting people back to work. An employee may be able to switch workstations, but they can't do that with their data. As a result, data protection solutions including backup & recovery are critical to business continuity and ransomware defense.

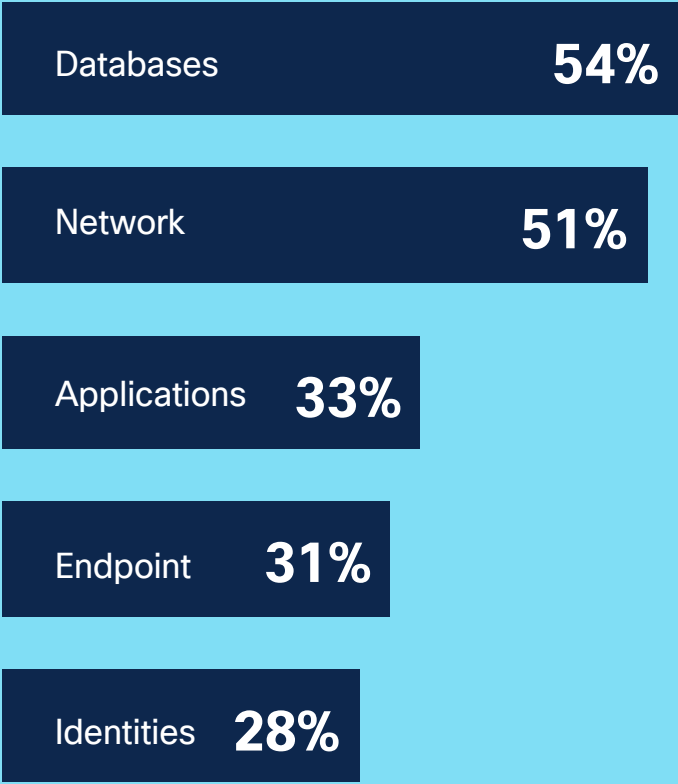# Automation
Survey Results

IDENTITY: Which assets are the most difficult to inventory?
(Select two)

Within the identity aspect of the NIST cybersecurity framework, network assets are the most difficult to inventory.

|	
Network	**60%**
Identities	**40%**
Applications	**39%**
Endpoint	**32%**
Mobile	**26%**
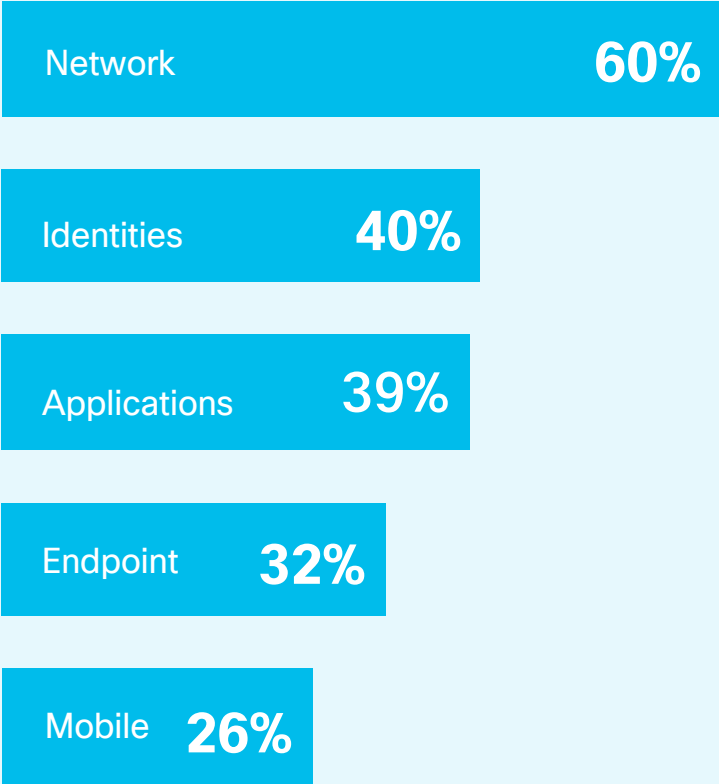
PROTECT: Which asset is at the top of your threat model?
(Select two)

Within the category of protection, networks and databases are at the top of the threat model.

|	
Databases	**54%**
Network	**51%**
Applications	**33%**
Endpoint	**31%**
Identities	**28%**

SURVIVAL
GUIDE

CISCO investments

DETECT: What automation has been most effective in detections?
(Select two)

With respect to automating detection, application and phishing have been most effective.

|	
Phishing	**56%**
Application	**55%**
Endpoint/EDR/EPP	**46%**
Identity	**40%**
1% Other	
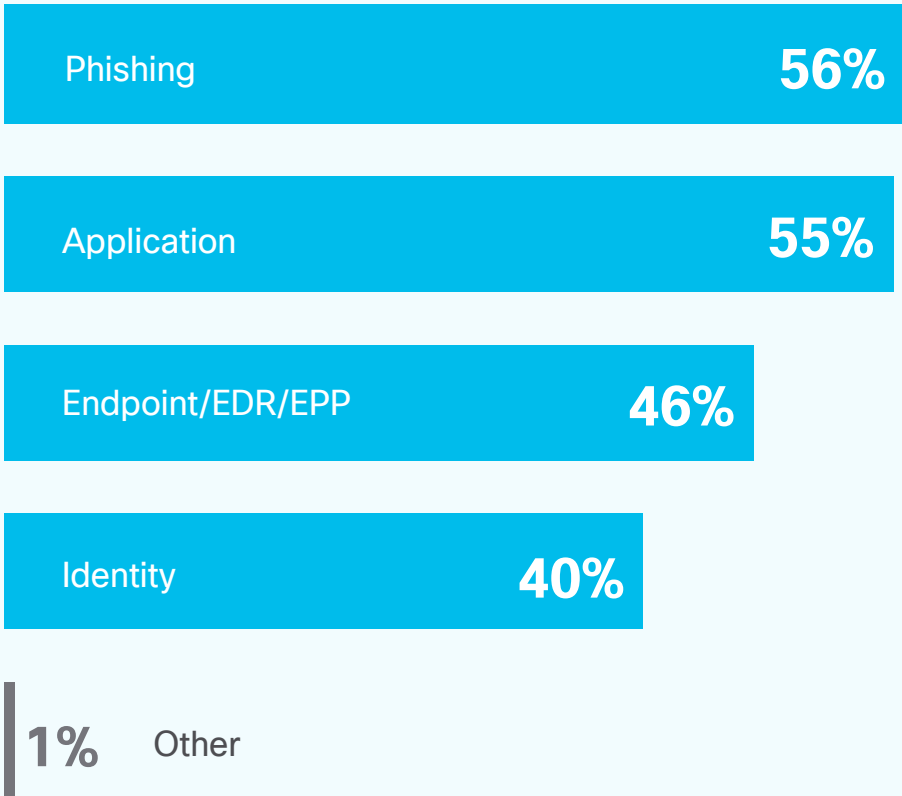
RESPOND: What is the low-hanging fruit for automation post-incident?
(Select two)

Integrations, blocking the threat, and communication are all areas ripe for applying automation post-incident.

Blocking the threat	**54%**
Integrations	**52%**
Communications	**51%**
Legal	**36%**
4% Other	
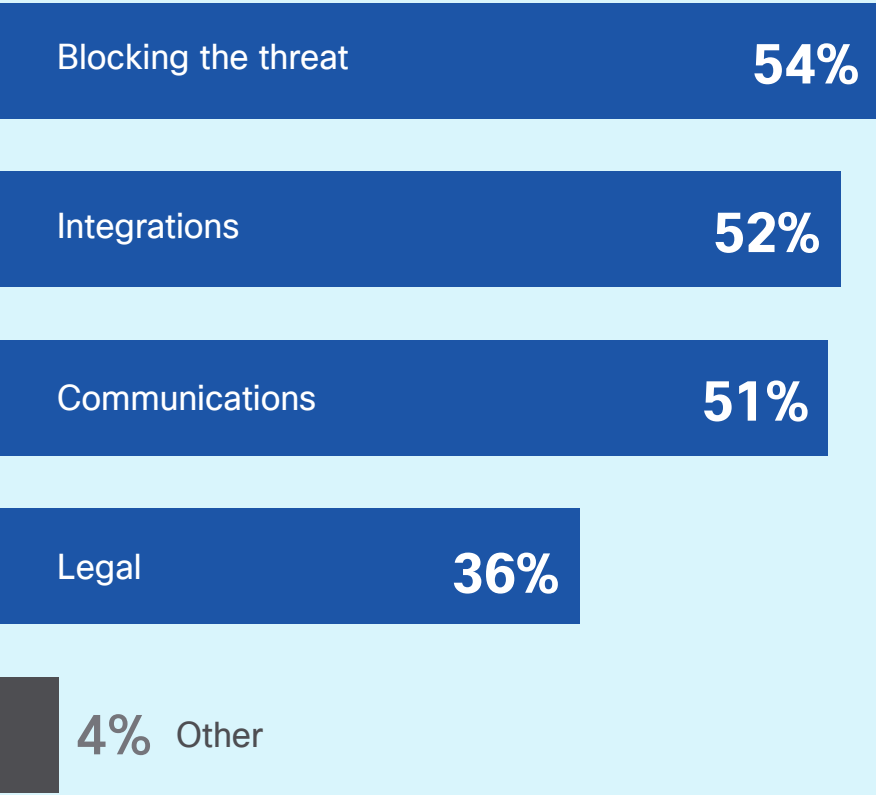
If everything was to go down, what would you focus on?
(Select two)

Respondents have difficulty prioritizing what they would focus on first if everything were to go down; data is at the top of the list.
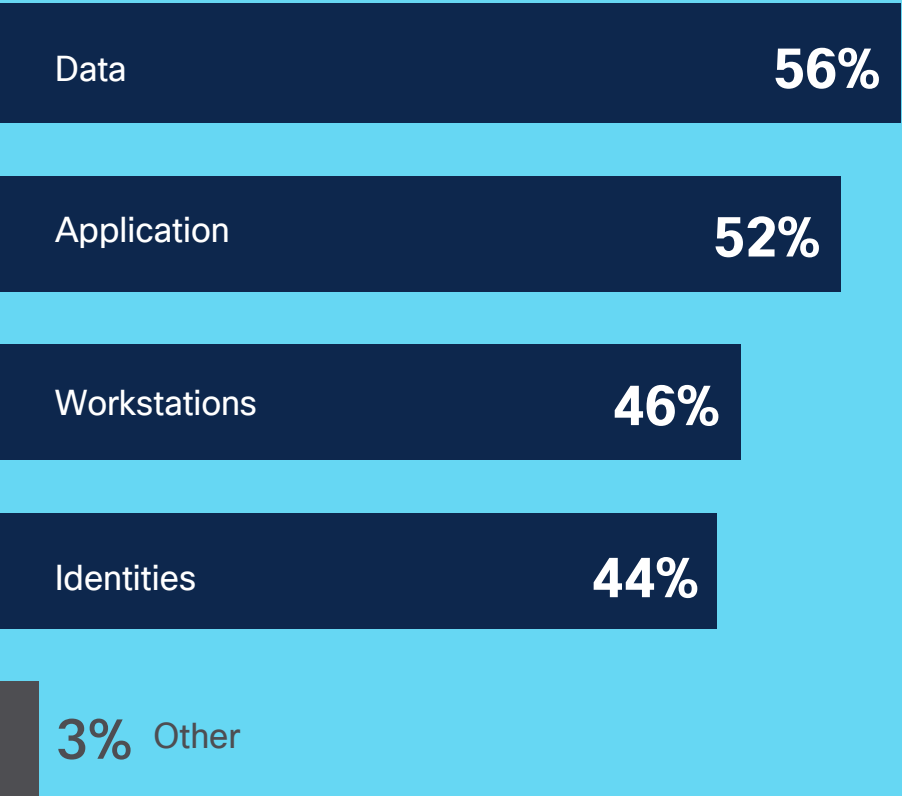
Data	**56%**
Application	**52%**
Workstations	**46%**
Identities	**44%**
3% Other	

SURVIVAL GUIDE

Source: IDG survey for the CISO Survival Guide 2021

What This Means for CISOs

Advice from Your Peers

Identify and automate repetitive tasks first
Automation can help your skilled workers spend more time doing interesting things that have a meaningful impact on your organization's security posture. Identify where the most repetitive tasks are, especially if you're already thinking about scaling your team.

"**Rules-based automation can help you achieve higher levels of quality** with more predictable output and processes. Less operational overhead will be needed to respond to outages or rework. You'll be able to get more out of security teams when removing these tasks, and it'll make it easier to scale with the resources you already have."

– CISO
at a Fortune 100 financial services company

Create a framework to assess the blast radius if an asset is compromised
Network assets were identified in the survey as the most difficult to inventory. This is an area where you may be missing things without even realizing. In any inventory project, it's important to layover the blast radius if an asset is compromised or there's an outage, as determined by what type of data it holds, who has access, etc. From there, you can begin to reduce your attack surface.

Leverage automation to identify misconfigurations, particularly for the cloud
Organizations adopting the public cloud or moving towards a DevOps model will likely have fewer guardrails and controls in place than before. These companies could quickly become exposed by an intentional or accidental misconfiguration. Automation can help detect and remedy these risks before they become a problem.

"While every environment is different, **figuring out your blast radius is a critical piece** of proactive security where automation can help."

– CISO
at a Fortune 100 retail company

"**Automation can help** with application and infrastructure misconfigurations."

– CISO
at a Fortune 100 healthcare company

Adam Ely, CISO at a multinational financial services corporation

One CISO's
Automation Journey

Identify

When I inventory, I look at what is exposed outside of the company first. I want to know whether it's a company network or IP space, exposed applications in infrastructure. **Those things are the low hanging fruit.** They're the first things that attackers can go after, so there's less resistance and controls simply because they have access.

Protect

When I think about protection, identity is the first thing that I think about because identity is a key to everything. If I lose control of an employee's identity, an attacker has access to anything that that person had access to. That could be the databases, applications, and everything else.

Detect

I'd put automation with detecting application infrastructure vulnerabilities like Bishop Fox's CAST higher up than email-based threats because that's been more effective. Then I would put log and security event analysis.

Respond

We automate a playbook that the actual responder goes through post incident. We'll have an institutional review board (IRB) that looks across the organization and across all endpoints. We automate those steps, kicking off multiple tools, pipelining into the integrations, and taking actions specifically on the host where they've been found positive. The responders don't have to click through so many steps when it's already predictable what you're going to do when you find certain problems.

Recover

If we're talking a recoverable, one-day event, I'm going to go 1) identity, 2) data, and 3) application. Without identity, no one can log into anything. Springing up the apps doesn't matter. In some businesses, I might just focus on getting data access if that's a company that can purely run off the raw data. But I don't know many businesses that can do that. Then I think about what my attack surface looks like and what I can reduce. **What can I quickly cut off and limit access to trusted devices or trusted network partners? How can I quickly reduce that attack surface?** From there, I go into security posture, patching, updates, and all the other things everybody has to talk about.

Executive Summary

- While nearly all CISOs (99%) are interested in working with startups to meet new security challenges and fill gaps in their technology stack, more than half lack a formal process for sourcing and evaluating startup technology.

- Internal innovation teams and analyst reports are some of the most effective routes to identifying and sourcing startup technology.

- To successfully engage startups, CISOs recommend developing a proactive method for sourcing and taking a "design partner" mentality.

Embracing Startup Tech
Cisco Investments

Introduction

In previous sections, we broke down four emerging trends and identified some of the startups who are breaking new ground in these spaces. The next question becomes: how do today's CISOs engage these startups, weave them into an end-to-end architecture, and create successful, long-term partnerships?

It's no secret that working with startups comes with unique benefits – particularly agility and forward-thinking solutions. However, they also come with their own unique challenges that today's enterprises may not be structured to overcome. In our role, we've learned that these challenges aren't actually barriers but in fact opportunities to become more innovative and flexible.

What We're Hearing from CISOs

CISOs all for embracing startup tech, but challenges exist

99%

of organizations open to working with a security startup

Nearly all (99%) respondents to our survey reported that their organizations were open to working with a security startup; however, most (56%) survey participants said that they don't have a formal assessment process for looking at the latest and newest tech in this sector. Some CISOs go to events, while others use recommendations from their partners. They don't have a dedicated team or concerted effort for making this happen.

56%

don't have formal assessment process

Internal experts, analyst reports favored by CISOs

30%

use internal experts as main source for finding startups

Our survey found that internal experts were the most-cited source for finding and engaging with high-quality startups at 30% of CISOs. This was followed by the use of analyst reports at 28%. CISOs are turning to these sources because that's what they probably have immediate access to. They don't have the time or resources to look at emerging tech in a more formal way.

CISOs most interested in working with startups on automation

Three-quarters or more indicate interest in working with startups in the areas of automation (83%), privacy and compliance (77%), and DevSecOps (74%). More than one-half (54%) would consider working with a startup for SASE.

83%

interested in working with automation

What This Means for CISOs

Advice from Your Peers

Make sourcing a deliberate effort

CISOs can miss out on some exciting opportunities if they just react to whatever they're hearing. It's more productive to be proactive and create a regular cadence for "looking ahead." This can take the form of scheduling recurring meetings with a VC to meet with startups. Ideally, it can involve having someone to track innovation for them.

"As CISOs, we have limited time, but it's essential to find a regular cadence to stop, pay attention, and look at what's coming next. For us, that means monthly calls with a trusted VC and our leadership team to identify emerging trends and top startups. Those insights are precious."

– Brian Akers,
CISO at **KeyBank**

Strike a balance between emerging and mature technologies

There's not a perfect ratio between new and legacy technology that will works for every organization. Instead, it's about regularly assessing your company's priorities and risk tolerance to identify what makes the most sense at the time.

Find startups that partner with mature vendors

It's impossible for CISOs to assess the ever-changing startup landscape on their own. Instead, CISOs can partner with mature vendors – such as Cisco – that have an idea about how startups' technologies will work with their existing solutions. It'll be even easier for them if their organizations are already using solutions provided by the mature vendor.

Frame yourself as a design partner

Startups are small and agile, which means they can quickly adapt to their customers' evolving needs. But CISOs can't tap into this opportunity automatically. They need to be willing to work with the startup and provide feedback to help retool their products to meet today's enterprise needs.

"You have to strike the right balance between mature and emerging technologies, and be ready to constantly adjust. Having a nimble approach helps ensure you are adapting to shifting business priorities as well as preparing for external factors that may force immediate change, like with the COVID-19 pandemic. As a CISO when you look at your security tech stack, you want to ensure that you are adopting leading-edge technology, while identifying areas of overlap to drive optimization and efficiencies that best support your business' transformation."

– Trina Ford,
Former CISO, **AECOM**

"Over the last several years, I've seen CISOs focus on consolidating and relying on companies that they already have established relationships with to make acquisitions that plug tech holes. It's easier to have a handful of strategic partnerships as opposed to trying to navigate the entire marketplace and put the pieces together ourselves."

– Jason Lish
CISO at **Lumen Technologies**

"When I go to an early-stage startup, it would be wrong for me to expect a fully-formed product. What I need is a product that meets a minimum viable use case, and then I have to be willing to work as a design partner with that startup to get it to be everything I need it to be."

– Dustin Wilcox
CISO at **Anthem**

Dustin Wilcox, CISO at Anthem

A CISO's Journey of Embracing Startup Tech

When it comes to engaging the startup ecosystem, Dustin Wilcox, CISO at Anthem, is a pro. We sat down with him to learn more about his hard-won lessons learned on sourcing and engaging startup tech.

If you're a CISO in the enterprise space, you probably have decades worth of experience. Here's the problem, though: that great experience doesn't necessarily tee you up for what's next. Our familiarity with protecting on-premise, data center-centric architectures doesn't automatically put us in a position to understand areas where best practices are still being defined such as cloud, digital, APIs, and AI. As CISOs, we can't rely on our same old standard toolbox.

This became apparent in 2014. Back then, I was the CISO at Centene, and cloud was quickly becoming the hottest trend in IT. Our teams were asking us to be more cloud-native, agile, and innovative, but there was no clearly defined path or "how-to" guide to this emerging tech space. There were no "best practices."

The answer? We were going to have to define them. I realized this would be the greatest opportunity I would ever have in my career to get it right from the beginning — to stop trying to fix legacy architectures but instead think about security by design. It was a wake-up call for me that I should be leaning into early-stage innovation and the venture capital space.

Like many other CISOs, I attended security conferences and tried to keep my ears open for new companies with relevant use cases. After that wake-up call, though, I became more diligent by establishing a regular cadence with a few trusted venture capital organizations, making yearly pilgrimages to Tel Aviv's startup hotbed, and eventually becoming an advisor and later a general partner at SixThirty.

I realized that **by leaning in, I became better equipped to identify relevant emerging trends and answer the tough questions about where we needed to make changes to our security strategy.**

This journey has taught me some invaluable lessons that I'd like to share with my fellow CISOs. First: be a design partner. You're in a unique position to help startups understand what they need to be successful. Don't expect

startups to have everything solved from the beginning. Expect to help them solve a problem.

Second, accept that each engagement is different. I partnered with one Application Security startup that led to breakthroughs in how we think about the development lifecycle. Another partnership with an encryption company didn't pan out after a six-month proof of concept. **Not every project is successful, but every project will help your teams become more agile and disruptive.**

I'll leave you with this: as CISOs, we can spend all our time trying to read crystal balls, or we can be a driving force in shaping security's future. In my experience, that begins with embracing innovation and startup technology.

Conclusion

All of the startups we've mentioned in this report represent some of the best-in-breed solutions in the market today. But as we all know, having all of these amazing solutions means nothing if there's no integrated architecture. It would be like an orchestra having the best pianist, violinist, flutist, and horn players in the world but no conductor.

So, if you're a CISO who wants to learn more about emerging trends and our portfolios, you can **contact the Cisco Investments team** for additional assistance. We have dedicated team members whose full-time jobs are identifying the best and most trustworthy startups for today's enterprises.

Finally, if you'd like to contribute to the 2022 CISO Survival Guide, give us your information **here**!

This report is the product of some amazing people at four VCs who came together to help CISOs engage security startups. Special thanks to Ashley Sullivan, Ghezal Omar, Glen Fisher, Margo Mendez-Penate, Chris Dallmar, Sharon Seemann, Karen Smyth, and everyone else on our Marketing, Comms, and Operations teams who helped bring this report to life behind the scenes.

Contributing Authors

Cisco Investments

Cisco Investments is the corporate development and venture capital arm of Cisco that's responsible for investing in enterprise technology Series A and beyond. For over three decades, the team has made hundreds of direct investments in high-growth technology startups, with a current portfolio of 120+ companies across the globe. Their deal managers are domain experts responsible for both investments and M&A in security and applications, enterprise networking and cloud, mass-scale infrastructure, and more.

Janey Hoe is Vice President at Cisco Investments. Previously, she held multiple product management, technical marketing, and business development leadership roles at Cisco, operating multibillion-dollar product lines as well as pioneering new products in switching, security, data center, and video collaboration. Her work on TCP/IP performance improvements has been widely implemented and referenced. Janey holds a BS and MS in electrical engineering and computer sciences from U.C. Berkeley and MIT, respectively.
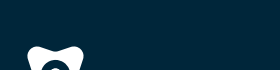
Prasad Parthasarathi is Director & Global Head for Cybersecurity Investments and M&A at Cisco Investments. His team is responsible for sourcing, qualifying, and transacting multi-stage venture investments as well as end-to-end M&A execution in Cybersecurity. Prior to Cisco, Prasad led multiple M&A transactions in large cap technology companies and was instrumental in EDS' $14B sale to HP. Prasad earned an MBA from Indian School of Business (ISB) Hyderabad and held Corporate Finance and Advisory stints in Singapore and India.

Neetta Shetty is Senior Manager and Head of the Cybersecurity Portfolio Development for Cisco Investments. In her role, Neetta's primary focus is bringing external innovation from startups together with internal opportunities with Cisco's customers, partners, and business functions. As a leader, Neetta is committed to fostering a world-class GTM engine for portfolio companies, building lasting relationships, and keeping a lens on tomorrow's disruptive technologies. Neetta has spent over a decade at Cisco working across APJC and the United States in various business acceleration roles. Neetta is passionate about mentoring women in STEM through Black Girls Code and Cisco University Programs. Neetta holds a B.S. Degree in Computer Science from Pune University.

.ıl CISCO **investments**

BehavioSec   exabeam   panaseer

dremio   FLASHPOINT   styra

RANGEFORCE   illusive   SECURE CODE WARRIOR

THREATQUOTIENT   SAFEGUARD CYBER   securiti

VALTIX   NS1.

Norwest Venture Partners

Norwest Venture Partners is an American venture and growth equity investment firm with more than $9.5 billion in capital under management. The firm targets early- to late-stage venture and growth equity investments across several sectors including cloud computing and information technology, Internet, software as a service, business and financial services, consumer, and healthcare. Headquartered in Palo Alto, California, Norwest has offices in San Francisco and subsidiaries in Mumbai, Bengaluru, and Herzelia. The firm has funded more than 600 companies since inception. The firm has 150+ active companies across its venture and growth equity portfolio.

Rama Sekhar focuses on early- to late-stage venture investments in enterprise and infrastructure including cloud, big data, DevOps, cybersecurity, and networking. Before joining Norwest in 2009, Rama was with Comcast Ventures, where he focused on investment opportunities in the enterprise and infrastructure sectors. Rama holds an MBA from the Wharton School of the University of Pennsylvania with a double major in finance and entrepreneurial management and a Bachelor of Science in electrical and computer engineering, with high honors, from Rutgers University.

Elaine Dai focuses on early to late-stage venture investments across a wide range of sectors at Norwest, with an emphasis on the enterprise and infrastructure spaces. Prior to joining Norwest, Elaine was an analyst at Microsoft, where she spent time at M12 (formerly known as Microsoft Ventures) and in the cloud and AI organization. Elaine previously held roles at Fidelity Investments and Citigroup. Elaine graduated from Harvard University with a Bachelor of Arts in economics.

NORWEST | VENTURE PARTNERS

COOKIE.AI   ermetic
exabeam   bitglass
Cynet   dremio
Uptycs   Dtex systems
SLASHNEXT   FOSSA
>_cmd

SURVIVAL GUIDE

YL Ventures

YL Ventures funds and supports brilliant Israeli tech entrepreneurs from seed to lead. Based in Silicon Valley and Tel Aviv, YL Ventures manages over $300 million and specializes in cybersecurity. YL Ventures accelerates the evolution of portfolio companies via strategic advice and U.S.-based operational execution, leveraging a powerful network of CISOs and global industry leaders. The firm's track record includes successful, high-profile portfolio company acquisitions by major corporations including Palo Alto Networks, Microsoft, CA and Proofpoint.

Sounil Yu is YL Ventures' former CISO-in-residence and is now the CISO & Head of Research at JupiterOne. In his role at YL Ventures, Sounil imparted his 30+ years of industry experience towards the firm's ideation support of up-and-coming entrepreneurs and amplifying the firm's value-add services to its portfolio companies. Previously, Sounil served as the chief security scientist at Bank of America, driving innovation to meet emerging security needs and develop alternative approaches to hard problems in security. Sounil is the creator of the highly influential Cyber Defense Matrix and the DIE Resiliency Framework, serves on the board of SCVX Corp and the FAIR Institute, teaches security as an adjunct professor, co-chairs "Art into Science: A Conference on Defense" and advises many startups.

Naama Ben Dov is an associate at YL Ventures who researches new investment opportunities, analyzes investments through thorough due diligence, and provides value-add to portfolio companies. Naama is a certified lawyer and previously articled in Amit, Pollak, Matalon Law firm's high tech and venture capital practice. She also served as an analyst in an elite technological intelligence unit of the Israeli Defense Forces.

YL VENTURES

cycode
build.security
enso
satori
VULCAN.
MEDIGATE
grip
orca security
Karamba Security
Hunters

ForgePoint Capital

ForgePoint Capital is the premier cybersecurity venture fund investing in transformative companies protecting the digital world. With $770 million of assets under management, the firm is one of the most active investors in early and growth-stage cybersecurity startups with over 25 global investments. Based in the San Francisco Bay Area, the firm partners with exceptional cybersecurity entrepreneurs, visionaries, and leaders worldwide.

Will Lin is a managing director and a founding team member at ForgePoint Capital. He has been an avid technology enthusiast for decades, building his first computer in elementary school and starting online businesses while completing his bachelor's degree at the University of California, Berkeley. Focusing on security startups for a decade, he has helped invest more than $150 million across 20+ cybersecurity companies to date.

Connie Qian is an investor at ForgePoint Capital focused on early-stage cybersecurity startups. Prior to joining ForgePoint, Connie spent time at Square in a role spanning strategic finance and business operations. She also spent several years in equity research at Goldman Sachs and Baird, developing deep expertise in the hardware and enterprise technology sectors. Connie earned a BS in Applied Economics from Cornell University and an MBA from the University of Pennsylvania's Wharton School.

Appendix

SASE

PORTFOLIO COMPANY	CISCO INVESTMENTS	FORGEPOINT	NORTHWEST	YL VENTURES
1Kosmos		●		
Atvo Networks		●		
Bayshore Networks		●		
BehavioSec	●	●		
Bitglass			●	
Cloudentity		●		
NS1	●			
Securiti	●			
Valtix	●			

Privacy & Compliance

PORTFOLIO COMPANY	CISCO INVESTMENTS	FORGEPOINT	NORTHWEST	YL VENTURES
CMD			●	
Constella		●		
Cookie.AI			●	
Dremio	●		●	
Ermetic			●	
SafeGuard Cyber	●			
Satori				●
Securiti	●			
Symmetry Systems		●		
WireWheel		●		

DevSepOps

PORTFOLIO COMPANY	CISCO INVESTMENTS	FORGEPOINT	NORTHWEST	YL VENTURES
Build Security				●
CMD			●	
Cycode				●
Enso				●
Fossa			●	
Secure Code Warrioor	●	●		
Styra	●			

Automation

PORTFOLIO COMPANY	CISCO INVESTMENTS	FORGEPOINT	NORTHWEST	YL VENTURES
Anitian		●		
Area 1 Security		●		
Bishop Fox		●		
Concourse Labs		●		
Cynet			●	
Cysiv		●		
Dtex			●	
Exabeam	●		●	
Flashpoint	●			
Hunters				●
Huntress Labs		●		
Illusive	●			
IronNet Cybersecurity		●		
Panaseer	●			
Slashnext			●	
Sphere		●		
Strata Identity		●		
ThreatQuotient	●			
Uptycs		●	●	
Vulcan				●