



Enterprise Strategy Group | Getting to the bigger truth.™

The Secure Cloud Configuration Imperative

The Central Role of Cloud Security Posture Management

Doug Cahill, Vice President and Group Director

SPRING 2021

PREPARED BY ESG FOR:



Research Objectives

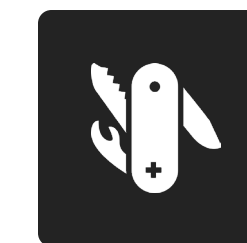
The composition of cloud-native applications is a mix of APIs, containers, VMs, and serverless functions continuously integrated and delivered. Securing these applications, the underlying infrastructure, and the automation platforms that orchestrate their deployment necessitates revisiting threat models, gaining organizational alignment, and leveraging purposeful controls. Additionally, as security and DevOps continue to converge, cloud security controls are being consolidated. Project teams are evolving from a siloed approach to a unified strategy to securing cloud-native applications and platforms. In parallel, vendors are consolidating cloud security posture management (CSPM), cloud workload protection (CWP), container security, and more into integrated cloud security suites, impacting buyer personas and vendor sales motions.

In order to gain insight into these trends, ESG surveyed 383 IT and cybersecurity professionals at organizations in North America (US and Canada) personally responsible for evaluating or purchasing cloud security technology products and services.

THIS STUDY SOUGHT TO:



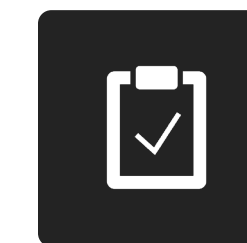
Assess the current and future composition and environments of cloud-native apps and infrastructure.



Gauge the state of organizational convergence, tool consolidation, and the emergence of platforms.



Explore the problem space with respect to operational challenges and the threat landscape.



Vet the go-forward strategy with respect to top priorities, spending intentions, and approaches for securing cloud-native environments.

RESEARCH HIGHLIGHTS

CLICK TO FOLLOW




THE CLOUD FOOTPRINT

The use of cloud services is increasingly strategic and heterogeneous.



THE CLOUD ATTACK SURFACE

Misconfigured services and a visibility gap have expanded the attack surface.



CONSEQUENCES OF MISCONFIGURATIONS

Misconfigurations lead to compromised data and the introduction of malware.



SPOTLIGHT: SHIFTING CSPM LEFT

Secure DevOps measures include automating scanning infrastructure-as-code (IaC) templates.



ESSENTIAL INVESTMENTS

Increased spending on cloud security controls is planned, with a preference for integrated platforms.



The Cloud Footprint

The use of cloud services is increasingly strategic and heterogeneous.

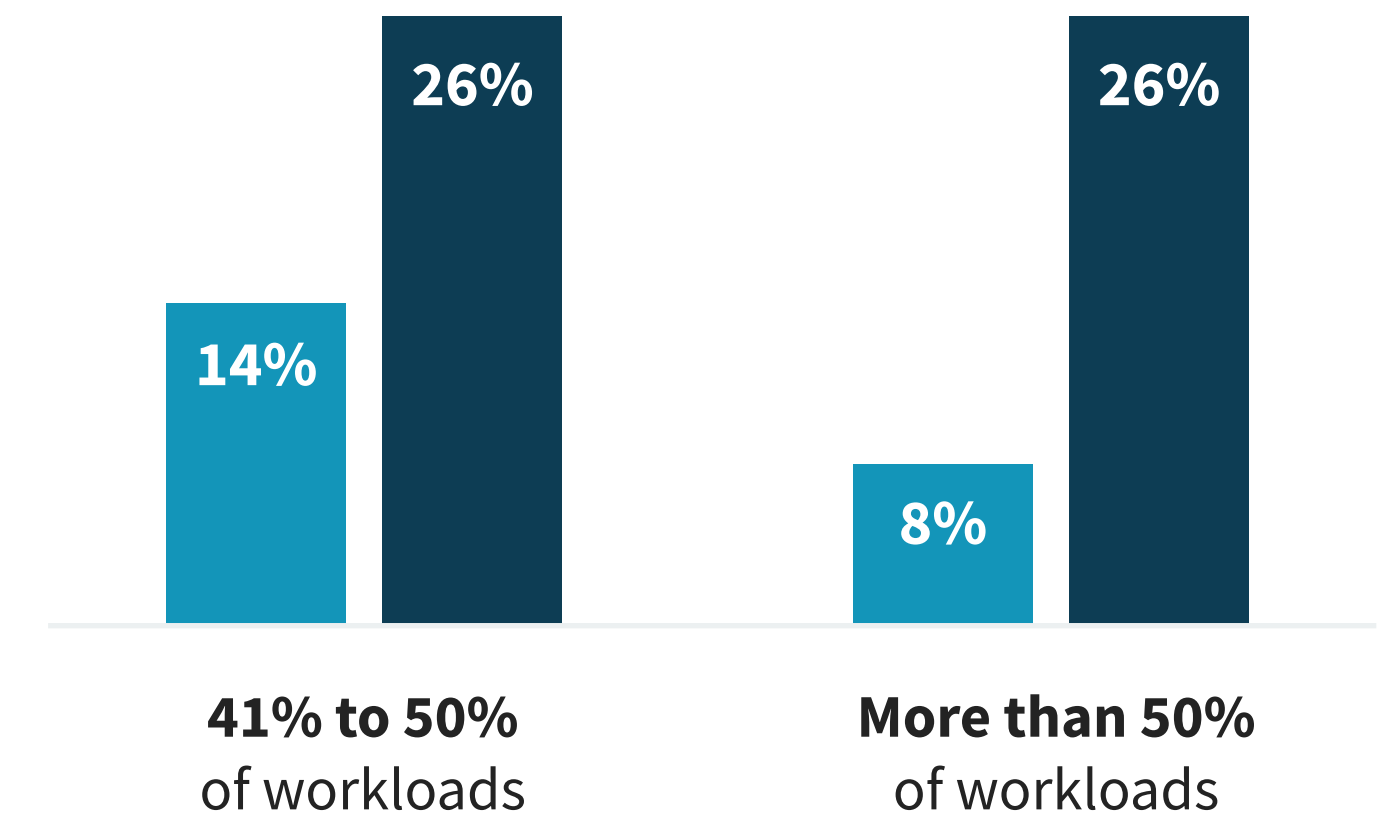
“**Securing such disparate environments** has led to a lack of consistent policies...”

Production workloads are shifting to multiple public clouds

The deployment of production server workloads across hybrid multi-clouds is introducing additional complexity, further challenging the ability to realize cybersecurity objectives. Securing such disparate environments has led to a lack of consistent policies, exposing enterprises to greater risk of data loss and cyber-attacks.

Production server workloads in the cloud.

- Percent of production workloads run on public cloud infrastructure services **today** (N=369)
- Percent of production workloads run on public cloud infrastructure services **24 months from now** (N=383)



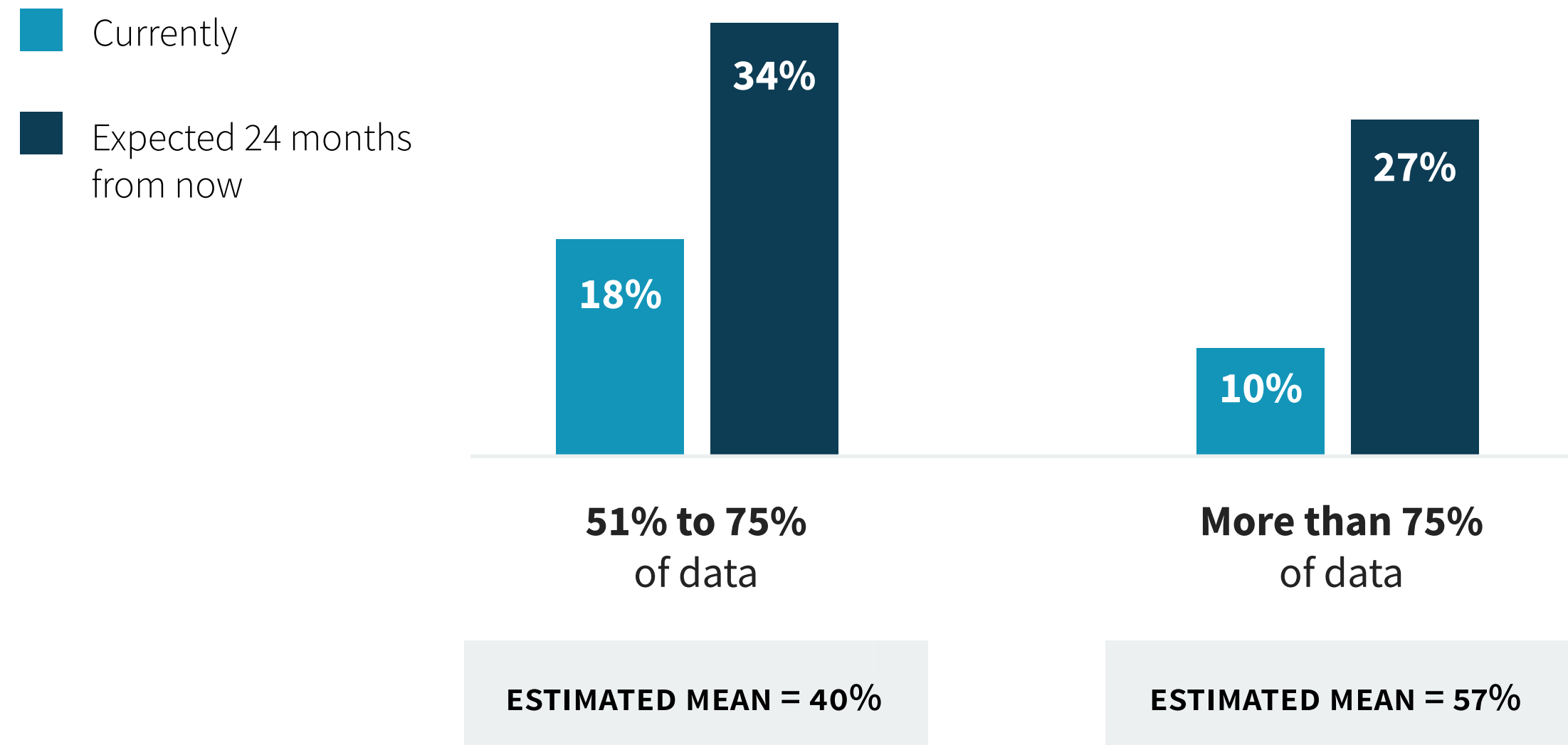
The average IaaS user leverages **3 unique CSPs**



Data, most of which is sensitive, is also shifting to public cloud

The expanding adoption of public cloud services is resulting in a notable projected increase in cloud-resident data. The use of public clouds for business-critical purposes is highlighted by the amount of cloud-resident data considered sensitive.¹ Where does that sensitive data live? Across both SaaS applications and IaaS/PaaS platforms.

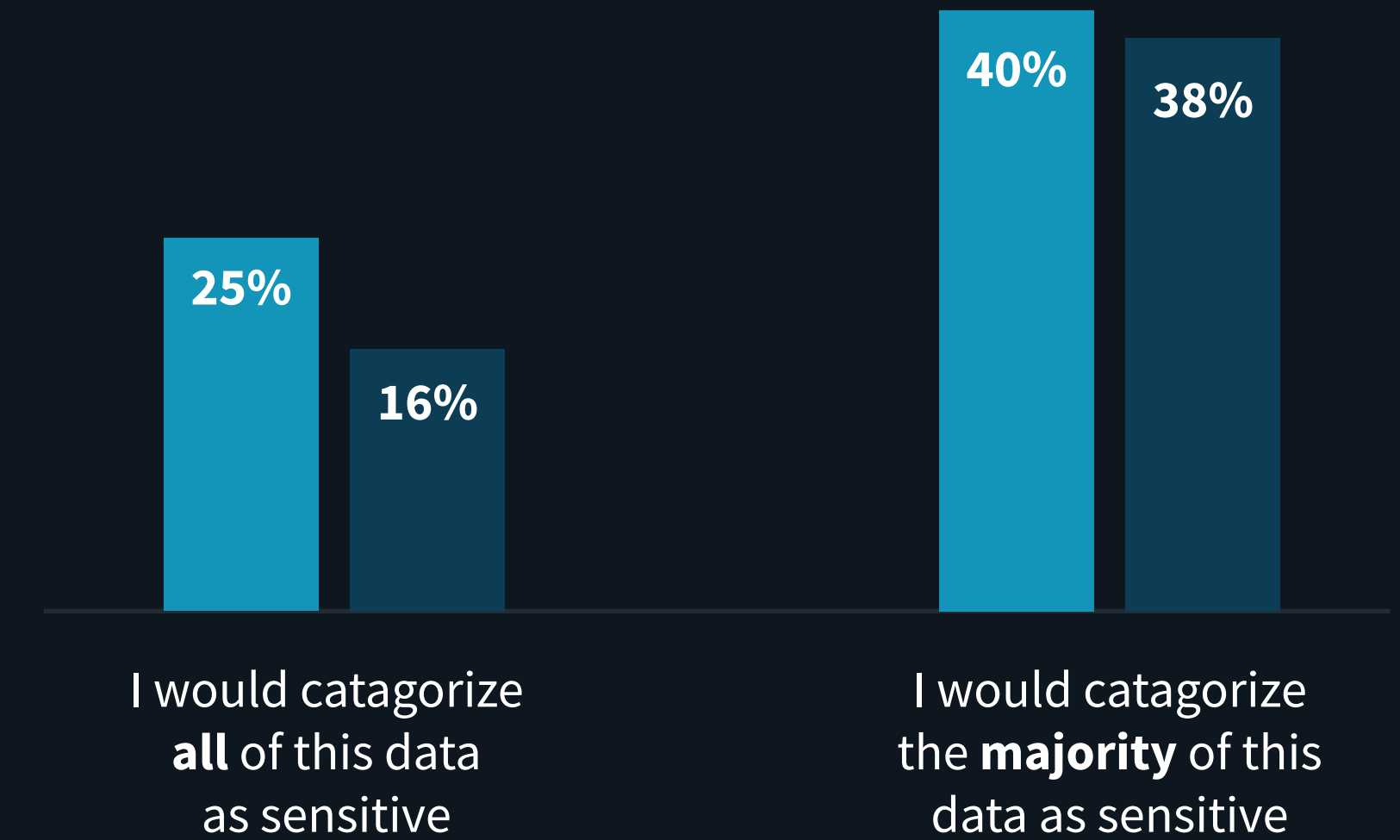
| Percent of data residing in the cloud.



Where does that sensitive data live?

| Percent of cloud-resident data that is sensitive.

- Proportion of SaaS-resident data that is sensitive today (N=298)
- Proportion of IaaS/PaaS-resident data that is sensitive today (N=301)



¹Source: ESG Research Report, *Trends in Identity and Access Management: The Increasingly Cloud-driven Identity Landscape*, February 2021.

The Cloud Attack Surface

Misconfigured services and a visibility gap have expanded the attack surface.



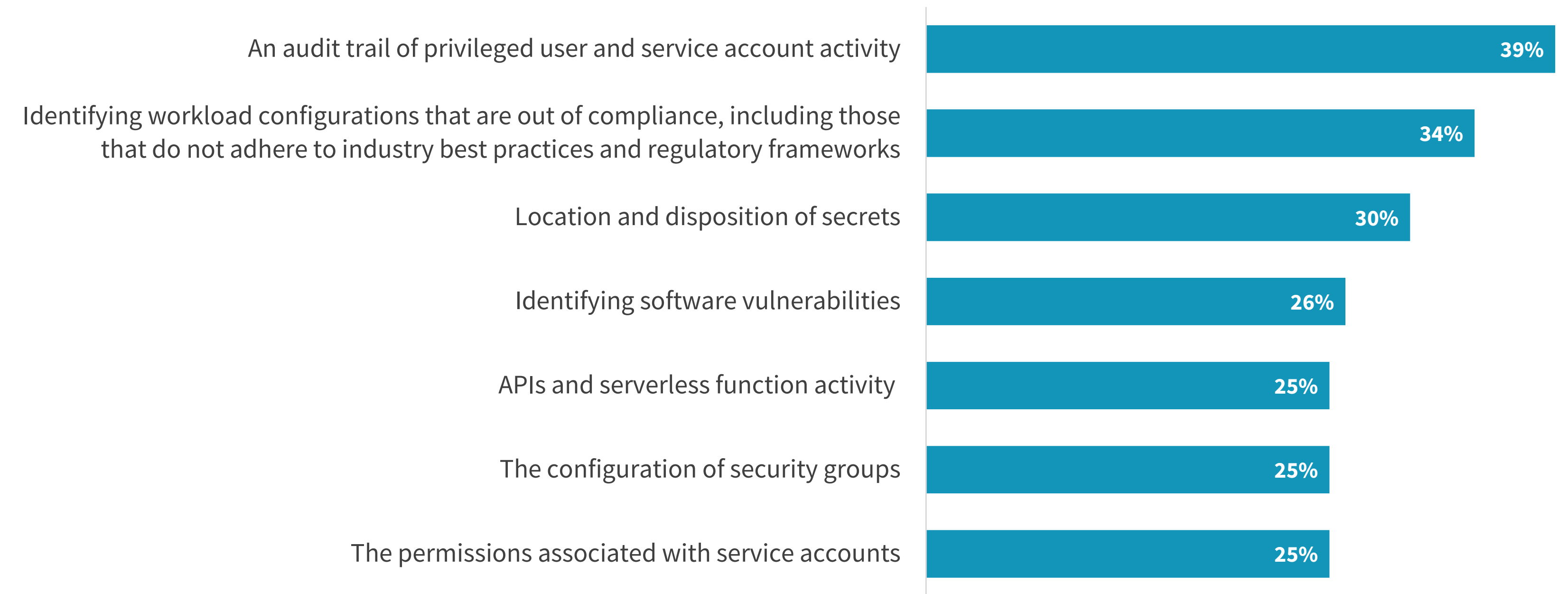
74%

of cybersecurity professionals believe the lack of access to the physical network and the dynamic nature of cloud-native applications and elastic infrastructure **create visibility blind spots, making security monitoring challenging.**

The cloud attack surface trifecta: visibility, access, and configurations

The abstract nature of public cloud platforms has created a need for greater visibility into the configuration of cloud services. An increase in the phishing of cloud credentials has led project teams to require a trail of the use of both privileged user and service accounts to detect potential account takeover (ATO) attacks. Improving visibility also entails vetting the configuration of server workloads against industry benchmarks and identifying the location of secrets such as API keys.

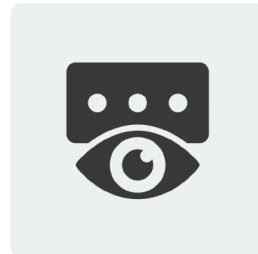
| Most important approaches to improving security visibility for cloud-native apps.



Access-related issues headline a series of misconfigured cloud services

Externally facing workloads subject to port scanning and open ports join a set of permission and access control-related issues. The prevalence of misconfigured cloud services, including insecure management consoles, serves as a call to action to treat cloud configuration management as a strategic imperative.

| **Ten most common** cloud misconfigurations in the past 12 months.



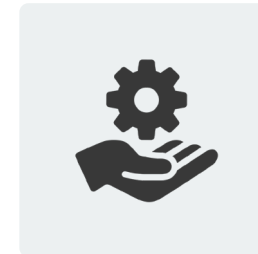
30%

Default or no password for access to management consoles



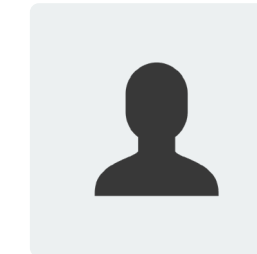
27%

Externally facing server workloads



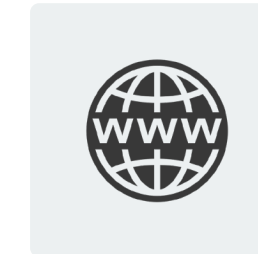
25%

Overly permissive service accounts



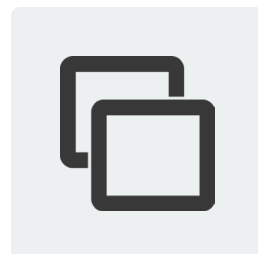
25%

Overly permissive user accounts



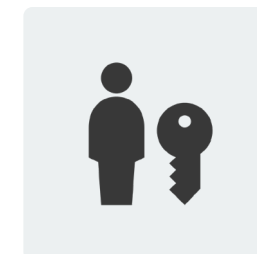
23%

Externally facing web servers not protected with a web application firewall and/or load balancer



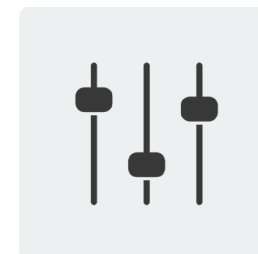
22%

Virtual machines and/or containers running as root



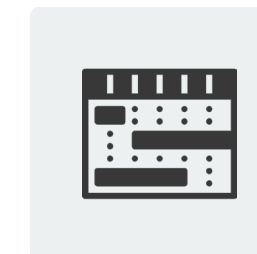
22%

Lack of multi-factor authentication for access to cloud and/or Kubernetes management



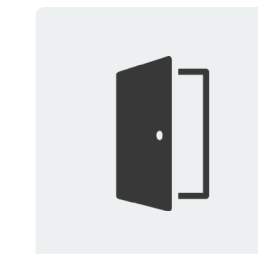
22%

Misconfigured security group permitting traffic to/from restricted IP addresses



19%

Disabled logging leading to the lack of audit trails of account, user, and system activity



19%

Open management ports

The Consequences of Misconfigurations

Misconfigurations lead to compromised data and the introduction of malware.



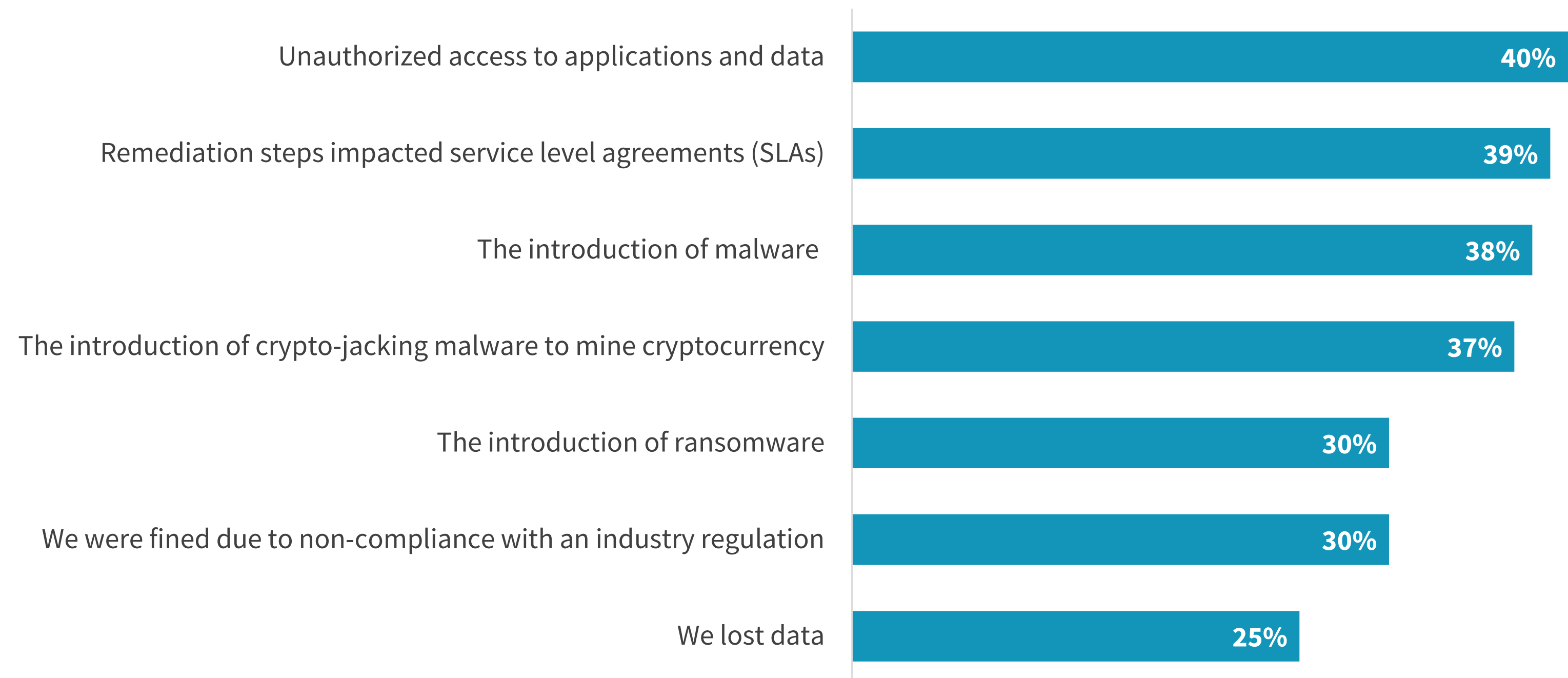
Misconfigured cloud services are often exploited by cyber-adversaries

Data compromises, failure to meet SLAs, and the introduction of malware highlight the need for greater attention to secure cloud configurations via the use of cloud security posture management (CSPM) controls. Malware that moves laterally, including crypto miners, is the top attack type against cloud-native environments.



Malware that moved laterally was the most common cloud-native security incident experienced in the last 12 months.

Results of cloud misconfigurations.



Challenges scoping roles lead to overly permissive accounts

The best practice of least privilege access (LPA) has been challenging to implement via the use of controls provided by cloud services providers.² The inability to do so leads to overly permissive user and services accounts, representing a highly vulnerable aspect of the cloud attack surface area.

| Roles and permissions for access to cloud services are difficult to manage with the native controls offered by the CSP.



²Source: ESG Research Report, *Trends in Identity and Access Management: The Increasingly Cloud-driven Identity Landscape*, February 2021.



The average organization estimates that

30%

of their human and non-human identities are **over-permissioned across cloud services.**

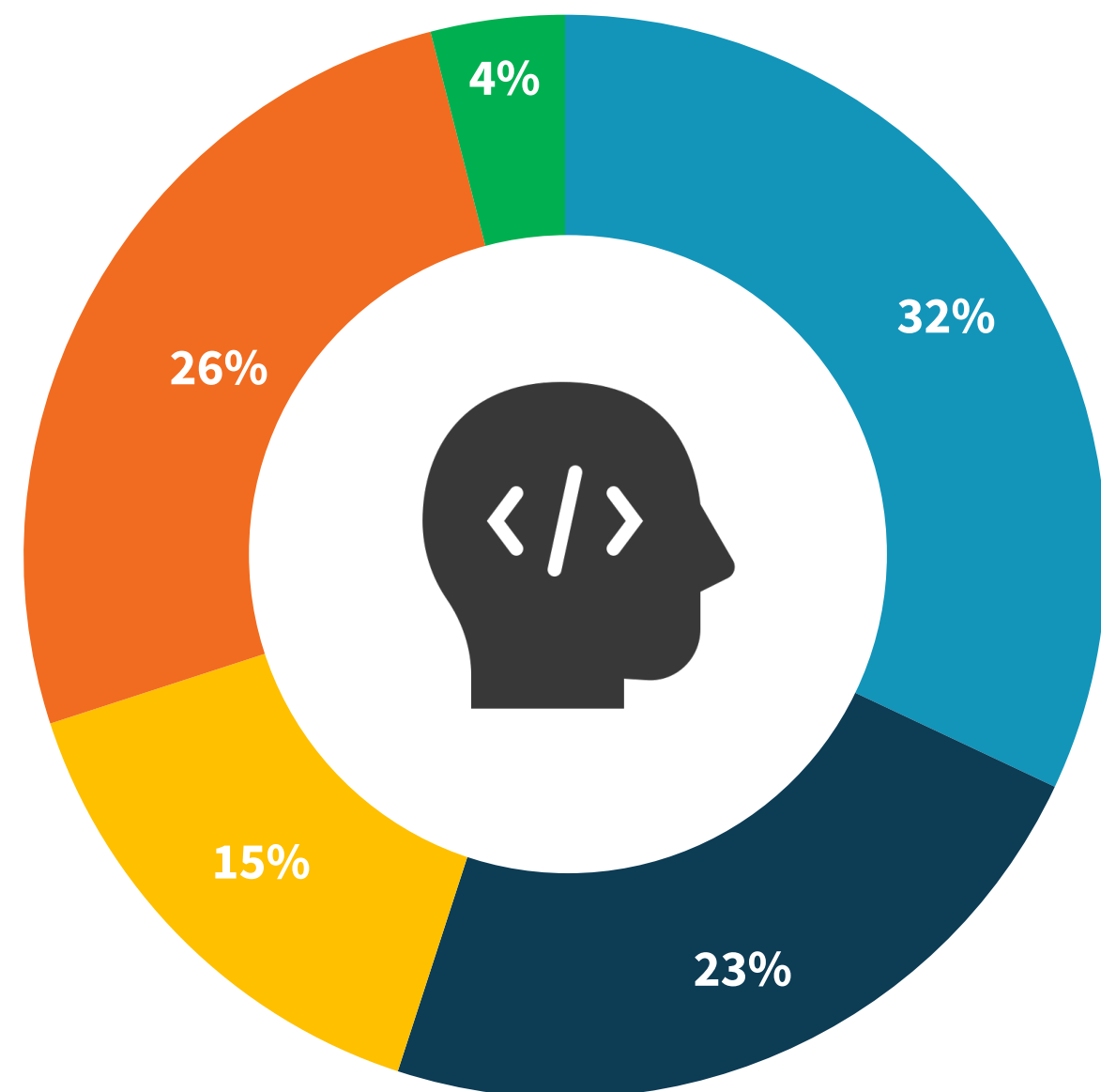
Spotlight: Shifting CSPM Left

Secure DevOps measures include automating scanning infrastructure-as-code (IaC) templates.

The need to scale via automation is driving secure DevOps practices

The speed at which cloud-native applications are delivered to production via continuous integration and continuous delivery (CI/CD) processes necessitates the inclusion of security controls. Fortunately, security measures are now being incorporated into DevOps processes as a means to keep pace at scale.

| Integration of security processes and controls via DevOps processes.



- We have incorporated security into our DevOps processes extensively
- We have incorporated security into our DevOps processes in a limited fashion
- We plan to incorporate security into our DevOps processes
- We are evaluating security use cases that can be incorporated into our DevOps processes
- We have not yet discussed how security fits with our DevOps processes



41%

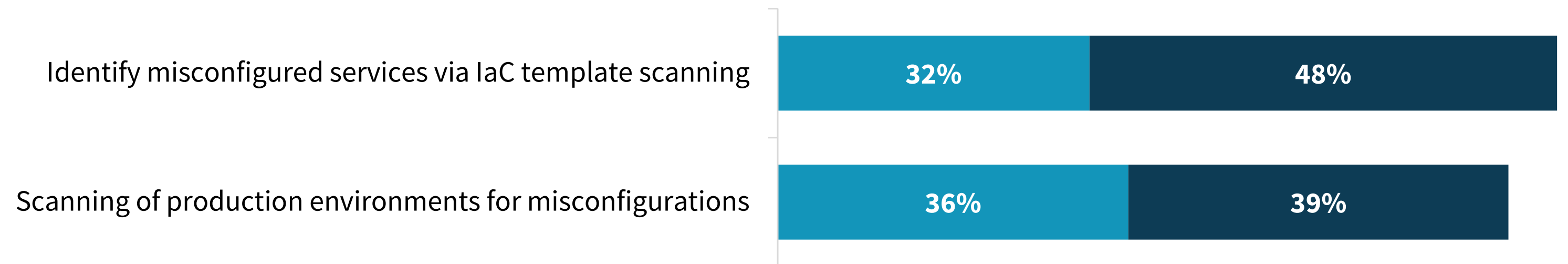
say automating the introduction of controls and processes via integration with the software development lifecycle and CI/CD tools is a top priority.

Automating cloud security posture management via DevSecOps

Current and planned DevSecOps use cases span the cloud-native application lifecycle, including addressing misconfigured cloud services in production and pre-deployment by scanning infrastructure-as-code (IaC) templates. As a result, more production cloud-native applications will be secured via DevSecOps practices over time.

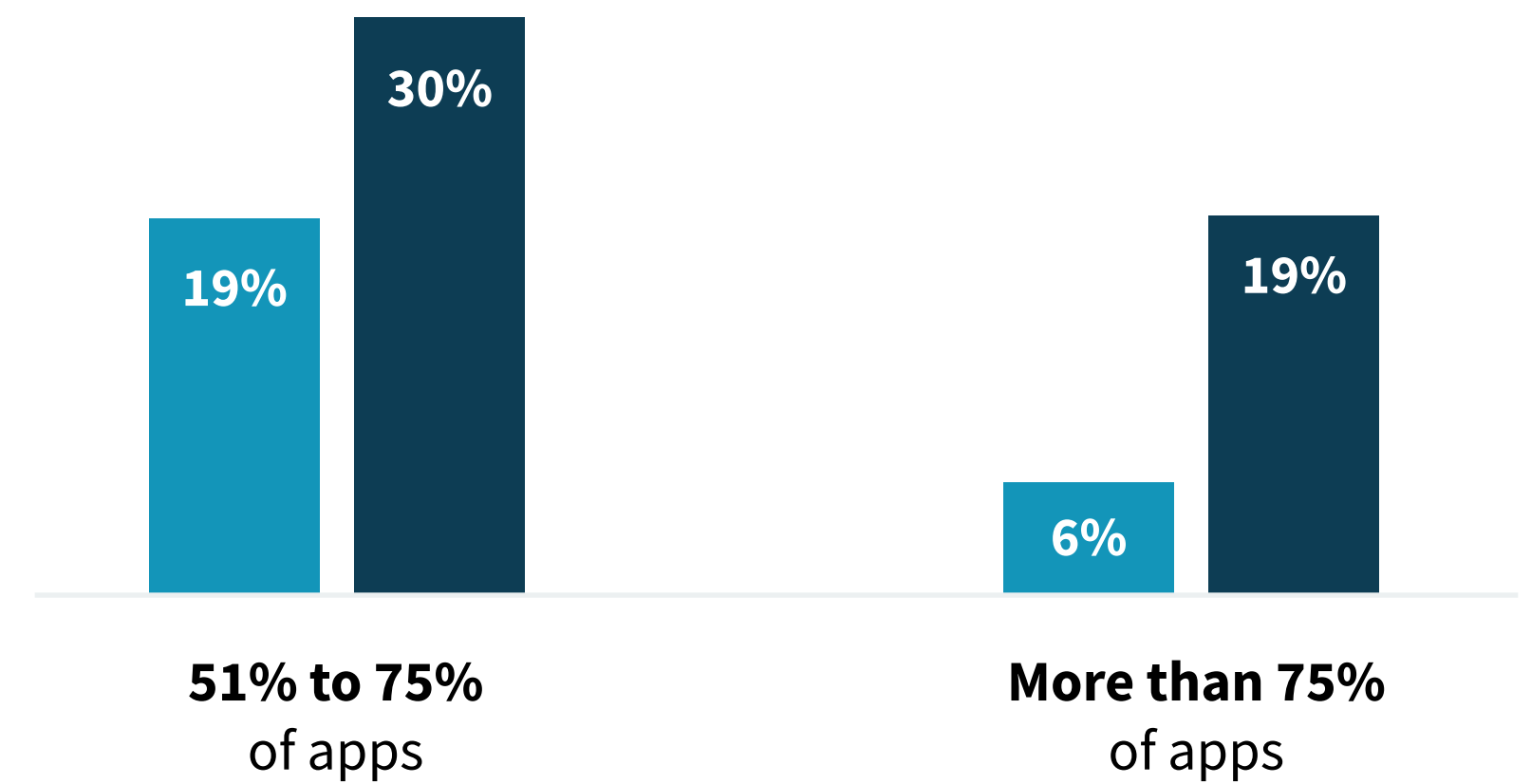
Security practices automated via integration with DevOps.

■ Currently automated via DevOps
 ■ Plan to automate via DevOps in the next 12-24 months



Cloud-native applications secured via DevSecOps.

■ Percent of cloud-native production applications secured via DevSecOps **today**
■ Percent of cloud-native production applications secured via DevSecOps **24 months from now**



Essential Investments

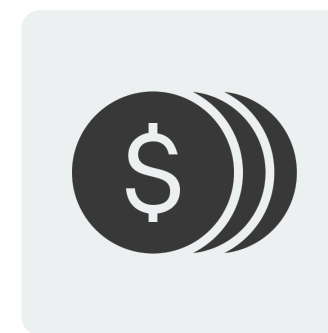
Increased spending on cloud security controls is planned, with a preference for integrated platforms.



Cloud security posture management (CSPM) tops cloud security investments

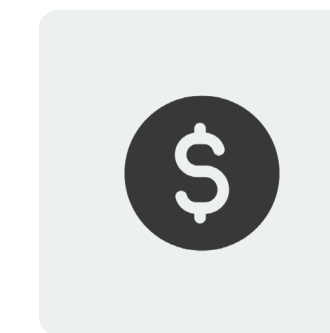
The internal development of cloud-native applications and increased usage of public cloud infrastructure is leading organizations to make essential investments. The top areas of incremental spending on cloud-native security focus on cloud security posture management and cloud workload security. This focus indicates a defense-in-depth approach that will require an integrated platform.

| Expected cloud-native app security spending change over the next 12 months.



27%

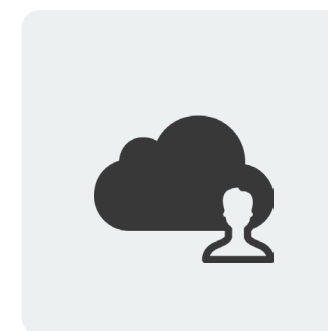
Increase substantially



52%

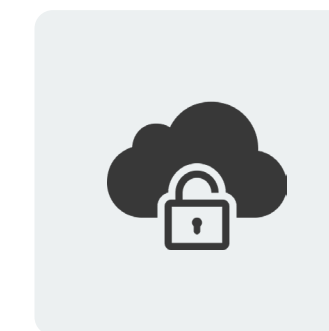
Increase slightly

| **Top three** cloud-native app security controls that will benefit from increased spending.



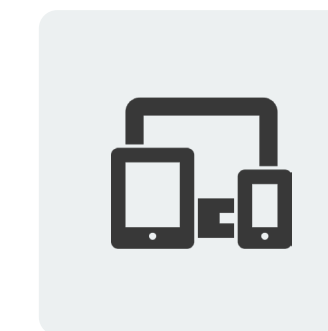
38%

Cloud security posture management



37%

Cloud workload protection platforms



36%

Endpoint detection and response for cloud-resident workload

The preference for consolidated controls will be met by integrated platforms

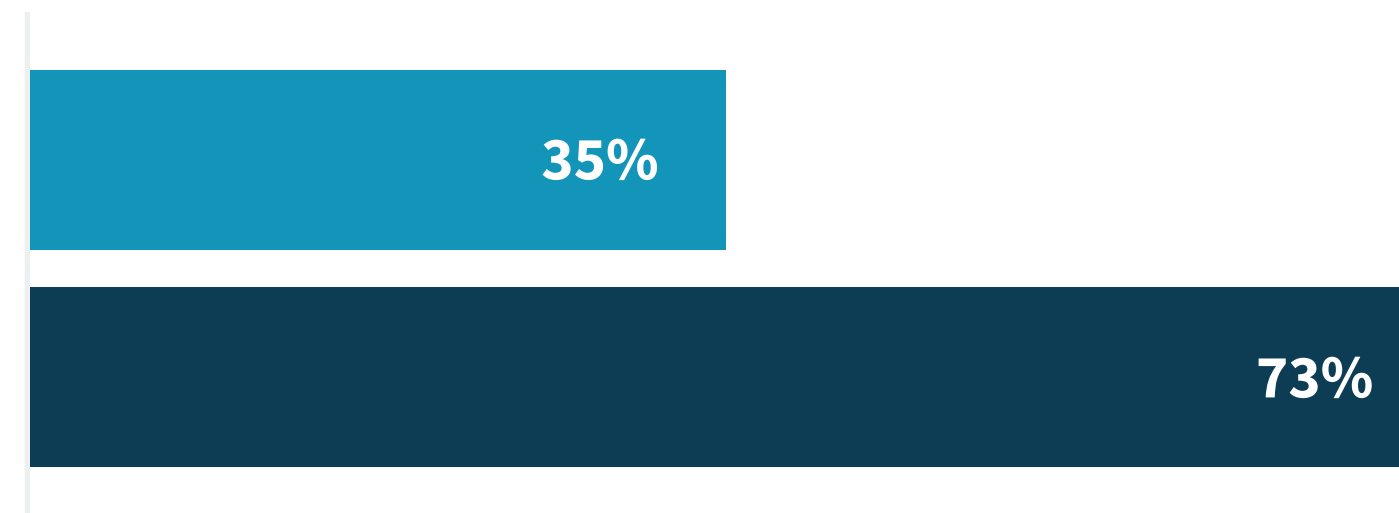
There is a strong preference to transition from silos of separate controls to an integrated cloud-native security platform. The shift to cloud-native application protection platforms (CNAPP) to meet this requirement is actively underway.

| Preferred security controls for protecting cloud-native applications and infrastructure.

■ Current approach

■ 24 months from now

We prefer a consolidated set of controls based on an integrated platform with convergence across environments (i.e., public cloud vs. on-premise) and server workload types



53%

plan to consolidate into an integrated platform within the next 12-24 months.

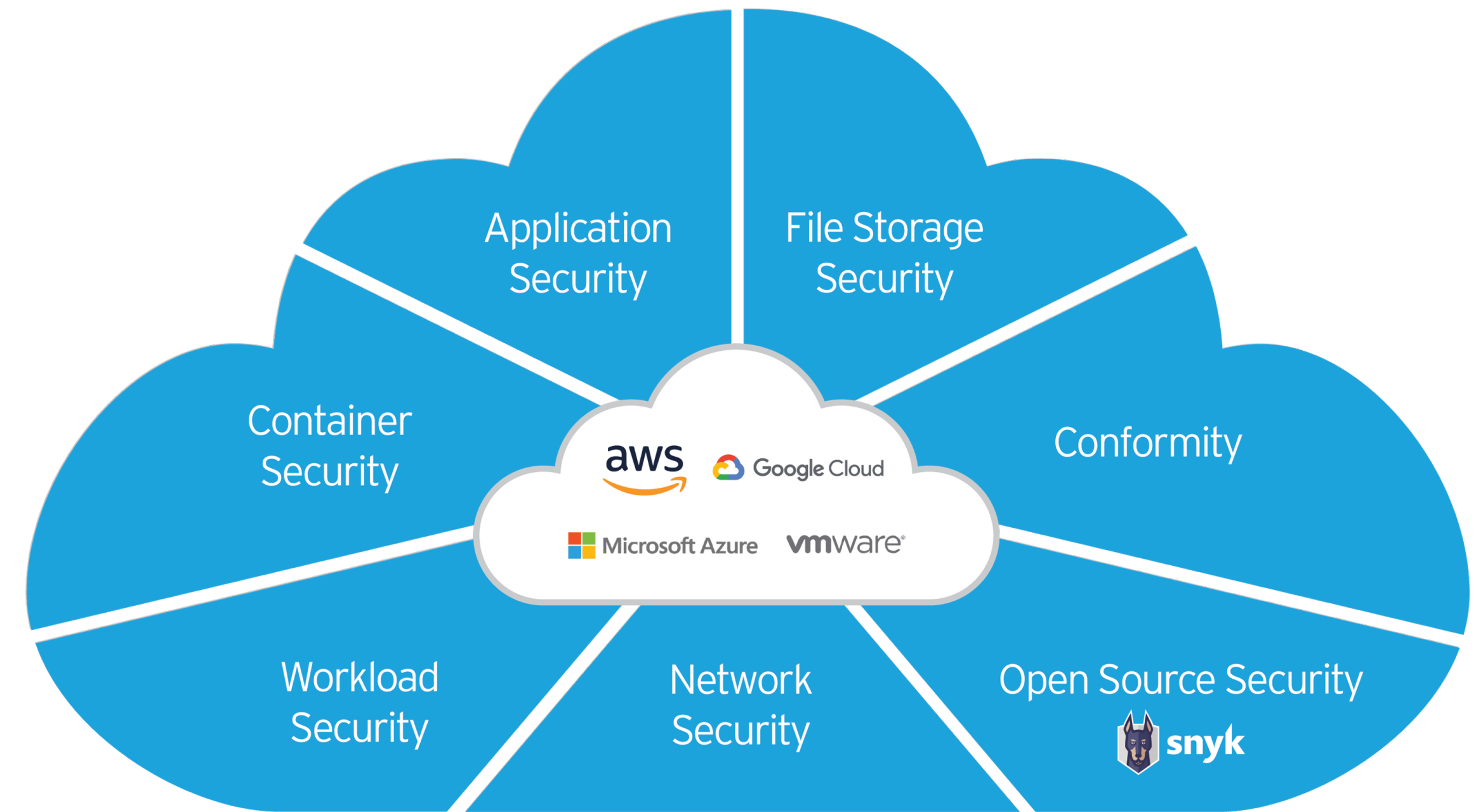


Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and innovation, Trend Micro enables resilience for customers by providing security solutions across the cloud and IT infrastructure. Optimized for the cloud and designed to simplify security via automation, Trend Micro Cloud One™ delivers world-class security in a single platform, helping you migrate to the cloud and innovate securely with compliance.

[FIND OUT YOUR SECURITY POSTURE](#)

ABOUT ESG

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.



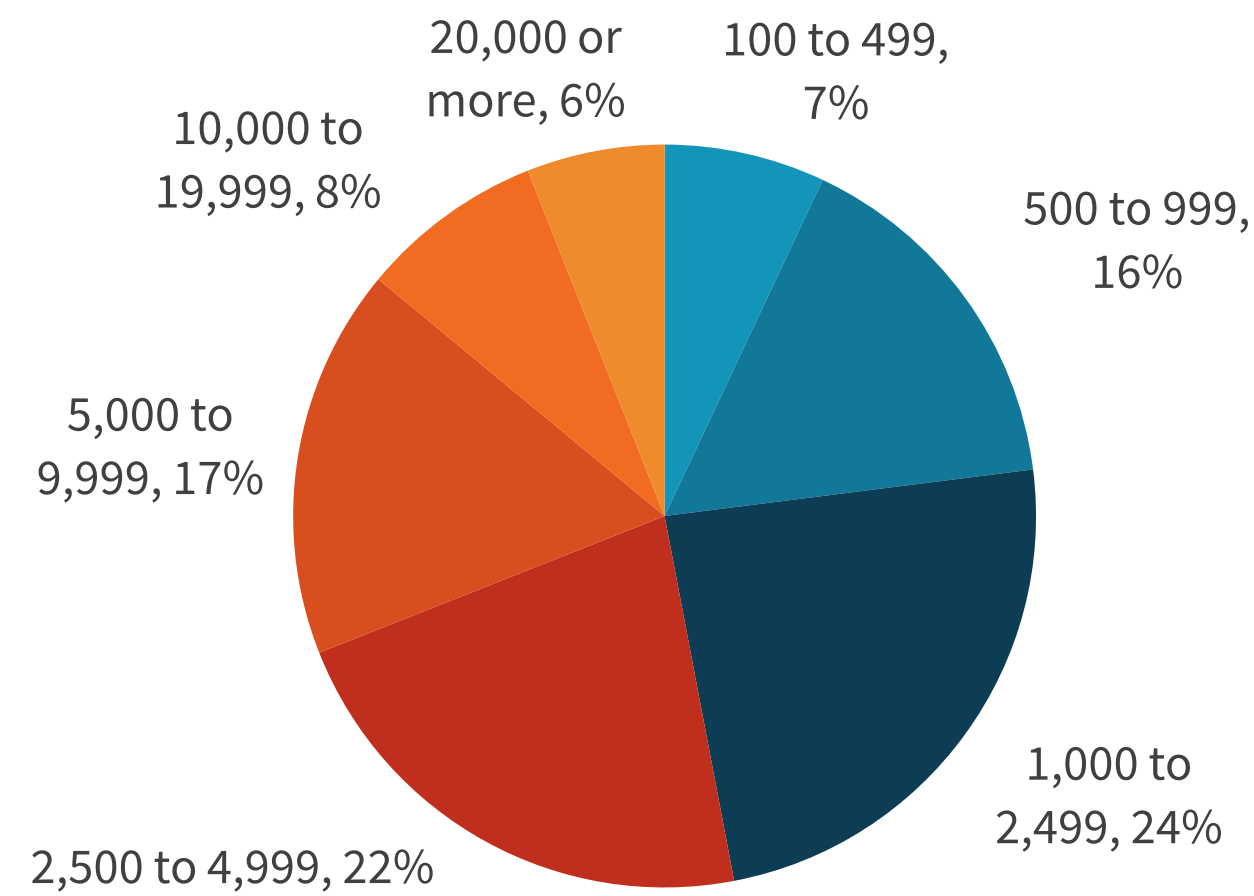
Trend Micro Cloud One™

Research Methodology and Demographics

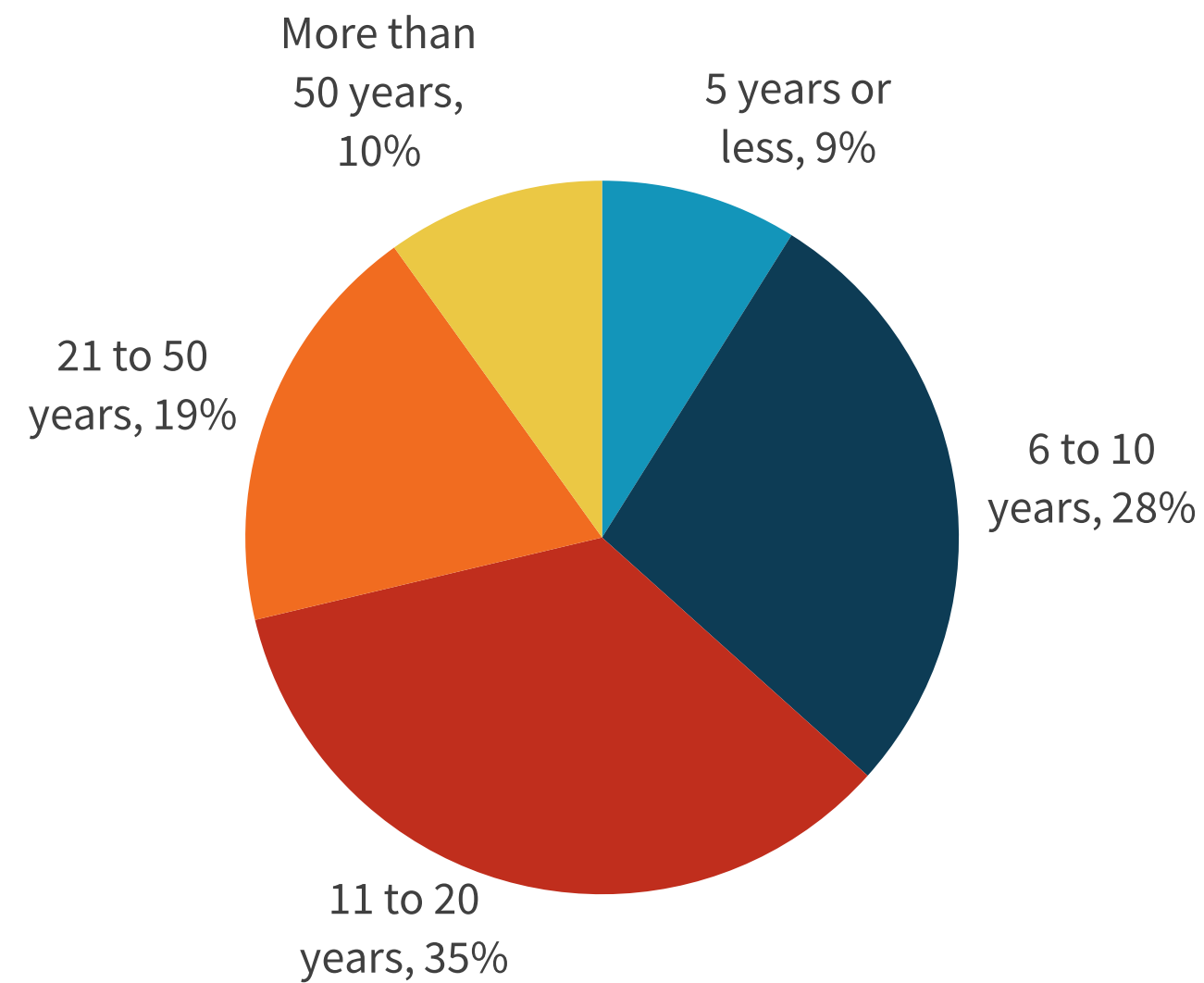
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between December 7, 2020 and December 26, 2020. To qualify for this survey, respondents were required to be IT and cybersecurity professionals personally responsible for evaluating or purchasing cloud security technology products and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 383 IT and cybersecurity professionals.

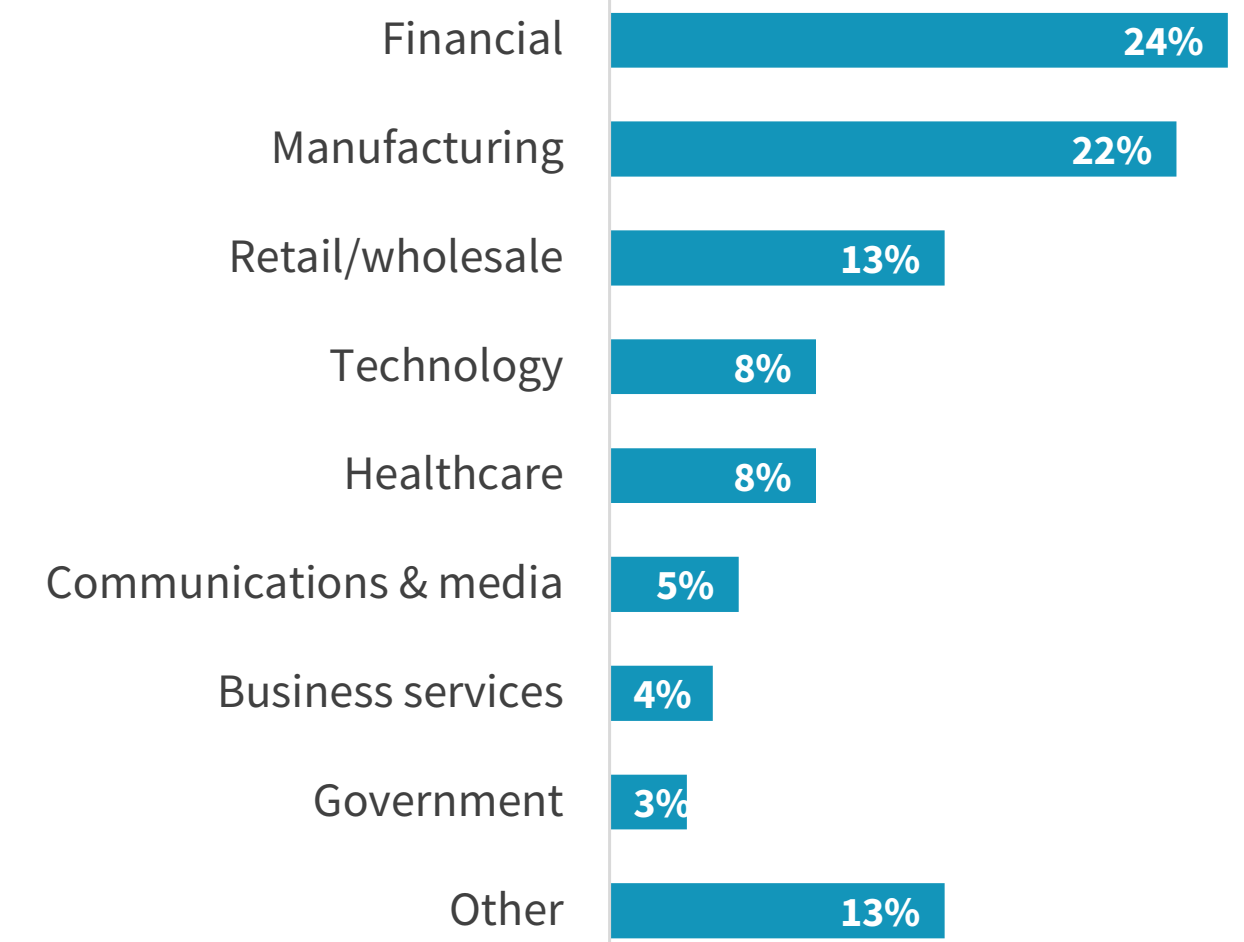
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2021 TechTarget, Inc. All Rights Reserved.