Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

The Maturation of Cloud-native Security:

Securing Modern Applications and Infrastructure

Doug Cahill, Vice President and Group Director

MARCH 2021

TABLE OF CONTENTS

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.

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

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

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

Research Highlights

Containers play a leading role in a heterogenous stack deployed across single and multi-clouds with serverless functions on the horizon. Container adoption has grown appreciably over the last two years with serverless functions being used largely on a limited basis. The term “cloud native” can be a misnomer since the use of Kubernetes for elastic container orchestration is enabling many organizations to provision on-premises private clouds.

Program maturity gaps result in inconsistency, misconfigurations, and visibility gaps. In addition to increasing cost and complexity, the use of environment-specific cybersecurity controls contributes to an inability to implement centralized policies. Such policies will require a clear understanding of the threat models specific to cloud-native applications and infrastructure. Additionally, a cloud security visibility gap has been a common refrain, one perennially headlined by the need to better understand the configuration of cloud-resident workloads and services.

A diverse threat model is driving the need for an integrated defense-in-depth strategy. A lack of attention to IAM basics joins externally facing workloads subject to port scanning, overly permissive accounts targeted by bad actors, and unauthorized access to services via open ports as the most commonly detected types of cloud misconfigurations. The diversity of the threat landscape is often brought to bear against cloud-native applications and infrastructure, which highlights the need for an integrated defense-in-depth approach.

The shift from a bottoms-up to a top-down approach is increasing the role of IT ops. Because different types of cloud-native controls are required for different layers of the stack and stages of the lifecycle, multiple stakeholders are involved in defining requirements and conducting the technical evaluations. As cloud-native applications gain critical mass and become a substantial portion of the IT footprint, companies are merging the related security responsibilities with their central security teams.

Automation via SDLC integration spans the application lifecycle. The need to keep pace with the elastic, dynamic nature of cloud-native applications and infrastructure makes automation a strategic tenet of cloud security programs. Current and planned secure DevOps use cases are being implemented across the application lifecycle by embracing both a shift-left approach and DevSecOps automation to provide runtime protection.

The requirement for breadth of coverage and depth of functionality is leading the consolidation of point tools into integrated platform modules. More than half of respondents indicated their organizations intend to leverage integrated platforms to enable a centralized approach to securing heterogenous cloud-native applications deployed across distributed clouds in the next 12-24 months. The broader adoption of IaaS/PaaS services along with further development and deployment of cloud-native applications is resulting in an increase in cloud-native security spending.

Back to Contents

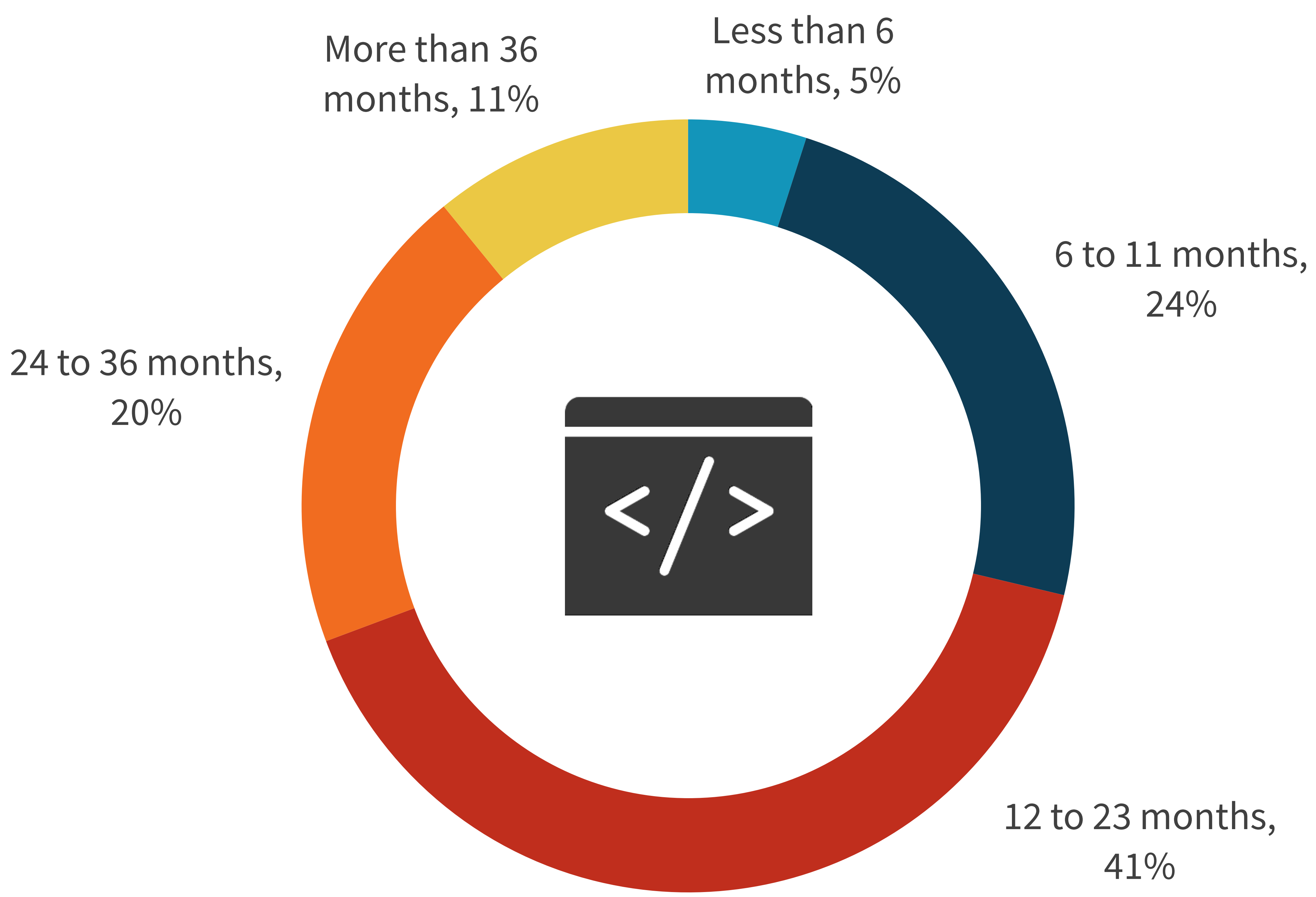
Cloud-native Environments

Containers play a leading role in a heterogenous stack deployed across single and multi-clouds with serverless functions on the horizon.

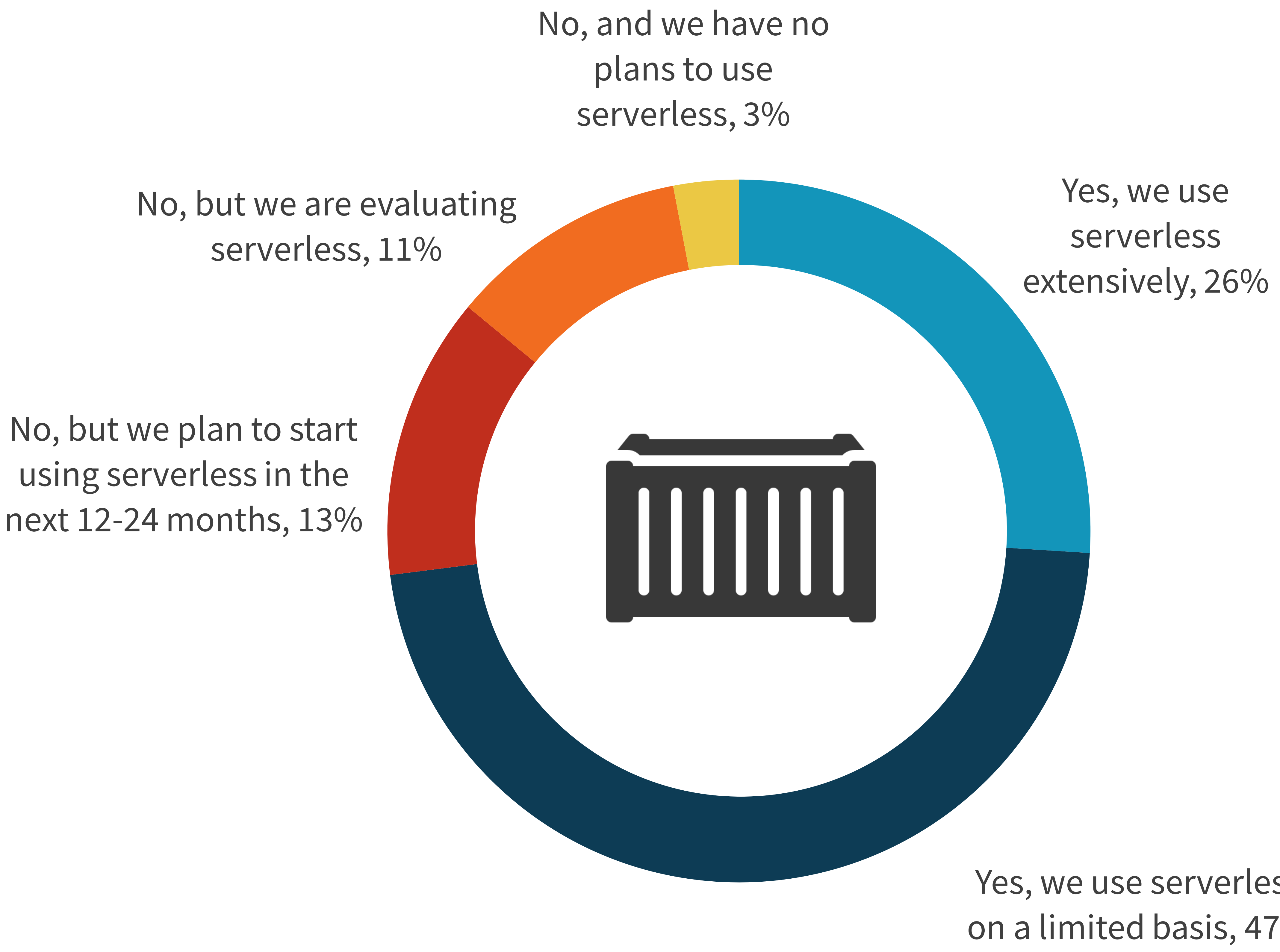
Containers, and now serverless functions, are underpinning microservices-based cloud-native applications

Container adoption has grown appreciably over the last two years with serverless functions being used largely on a limited basis. However, those project teams that have had containers deployed in production for more than two years are more likely to be using serverless functions extensively, a leading indicator of the future composition of cloud-native applications.

Length of time production apps have run on containers.



Use of serverless in application code.



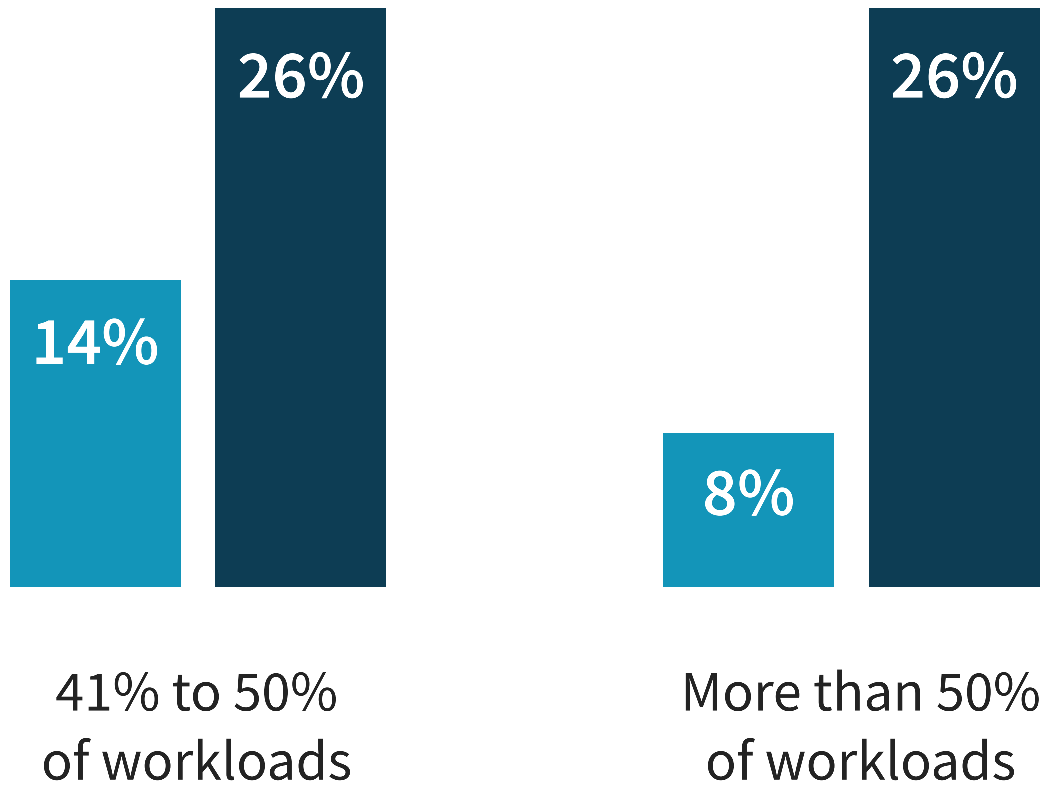
While some production workloads are shifting to public clouds, container portability affords location flexibility

The term “cloud native” is a misnomer insofar as today’s modern applications are not exclusive to public cloud platforms. The use of Kubernetes for elastic container orchestration is enabling many organizations to provision on-premises private clouds. As such, while some project teams may start off deploying containers in a public cloud environment, the flexibility of container portability provides options going forward to deploy across hybrid, multi-cloud environments.

Production server workloads in the cloud.

■ Percent of production workloads run on public cloud infrastructure services today (N=369)

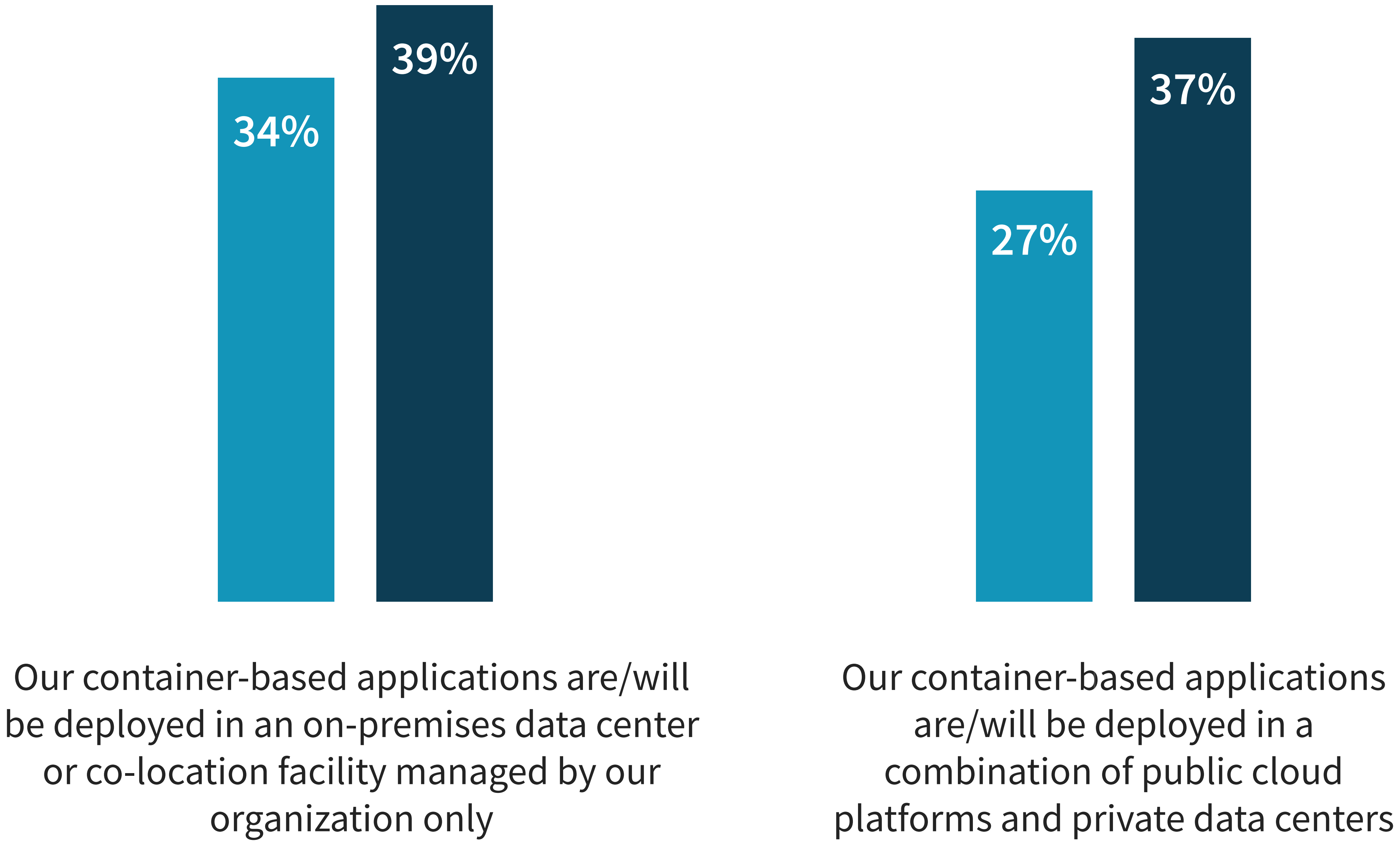
■ Percent of production workloads run on public cloud infrastructure services 24 months from now (N=383)



Container operation location approach.

■ Today (N=293)

■ 12-24 months from today (N=382)



Back to Contents

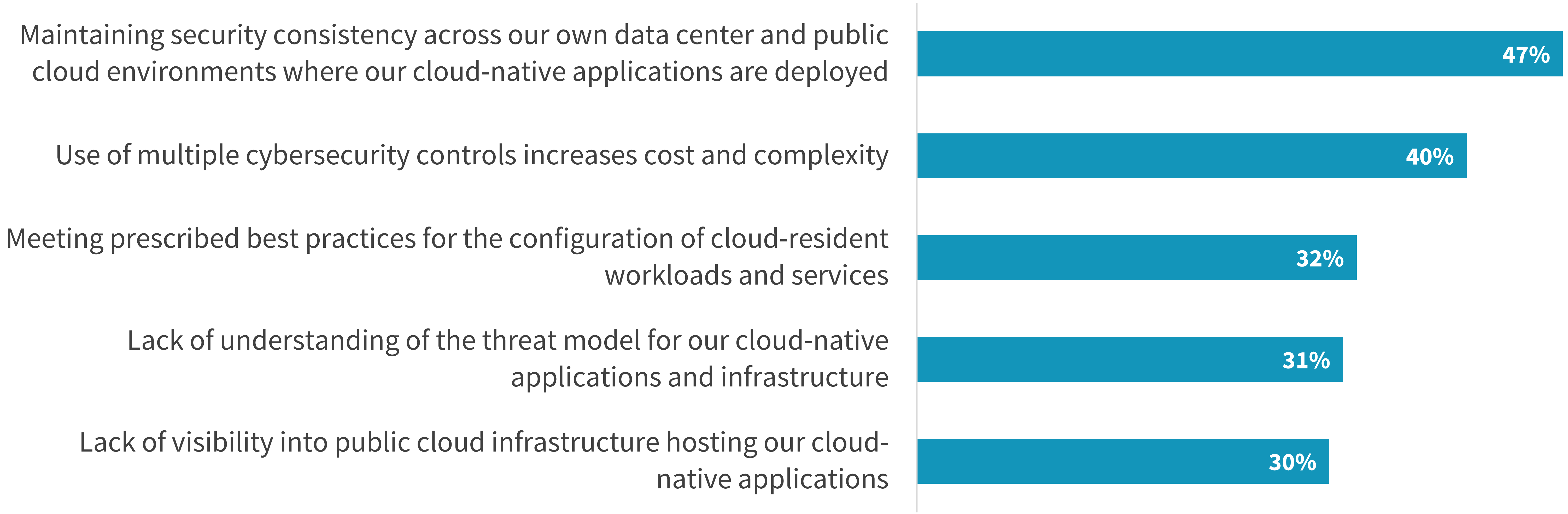
Cloud-native Security Challenges

Program maturity gaps result in inconsistency, misconfigurations, and visibility gaps.

The lack of security consistency across disparate environments highlights the need to evolve cybersecurity programs

In addition to increasing cost and complexity, the use of environment-specific cybersecurity controls contributes to an inability to implement centralized policies. Such policies will require a clear understanding of the threat models specific to cloud-native applications and infrastructure. Program maturation will come with experience as evidenced by the percent of organizations with containers in production for more than 2 years who reported that they have implemented a more robust set of automated policies.

Top five cloud-native app security challenges.



88%

of respondents believe their cybersecurity program needs to evolve to secure their cloud-native applications and use of public cloud infrastructure

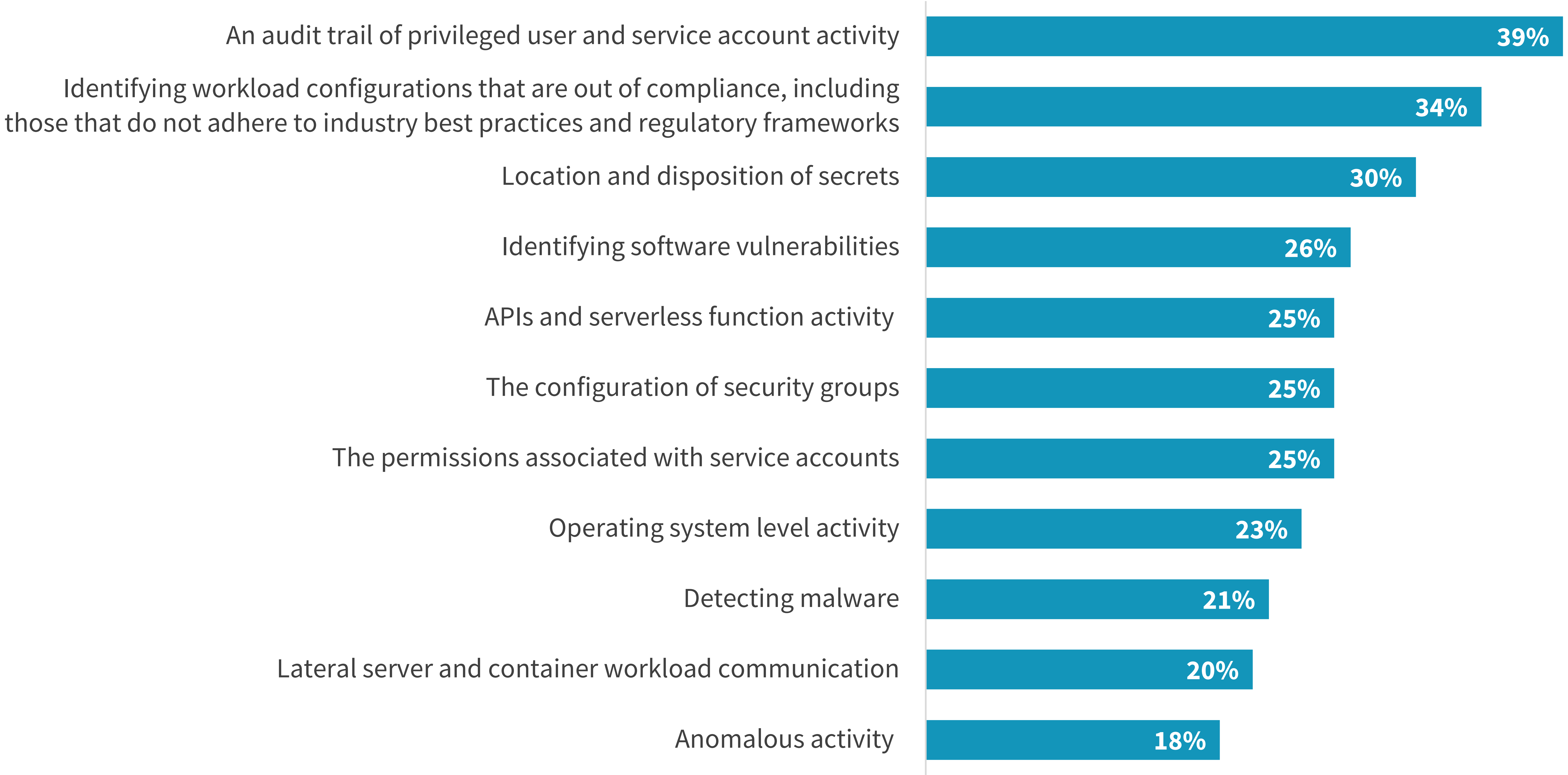
62%

report that 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 use of privileged accounts is the top priority for closing the cloud security visibility gap

A cloud security visibility gap has been a common refrain, one perennially headlined by the need to better understand the configuration of cloud-resident workloads and services. An increase in privileged cloud credential compromises has led to a need to monitor the activity of these accounts for anomalies that could be indicative of an account takeover (ATO) attack. Of particular concern are user credentials that have administrative access to cloud and orchestration management consoles and service accounts that serve as the identity context for production applications.

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



Back to Contents

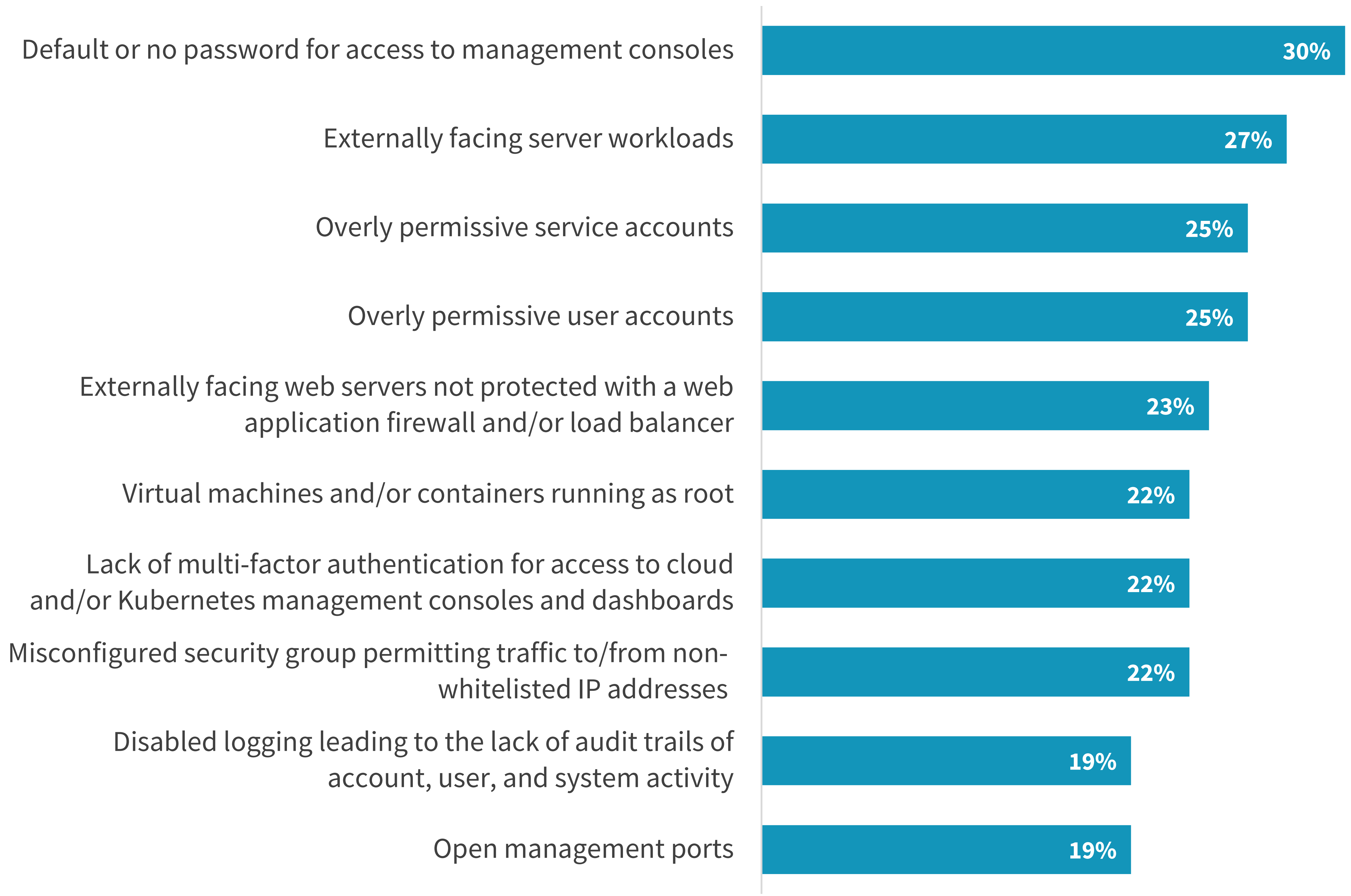
The Cloud-native Threat Landscape

A diverse threat model is driving the need for an integrated defense-in-depth strategy.

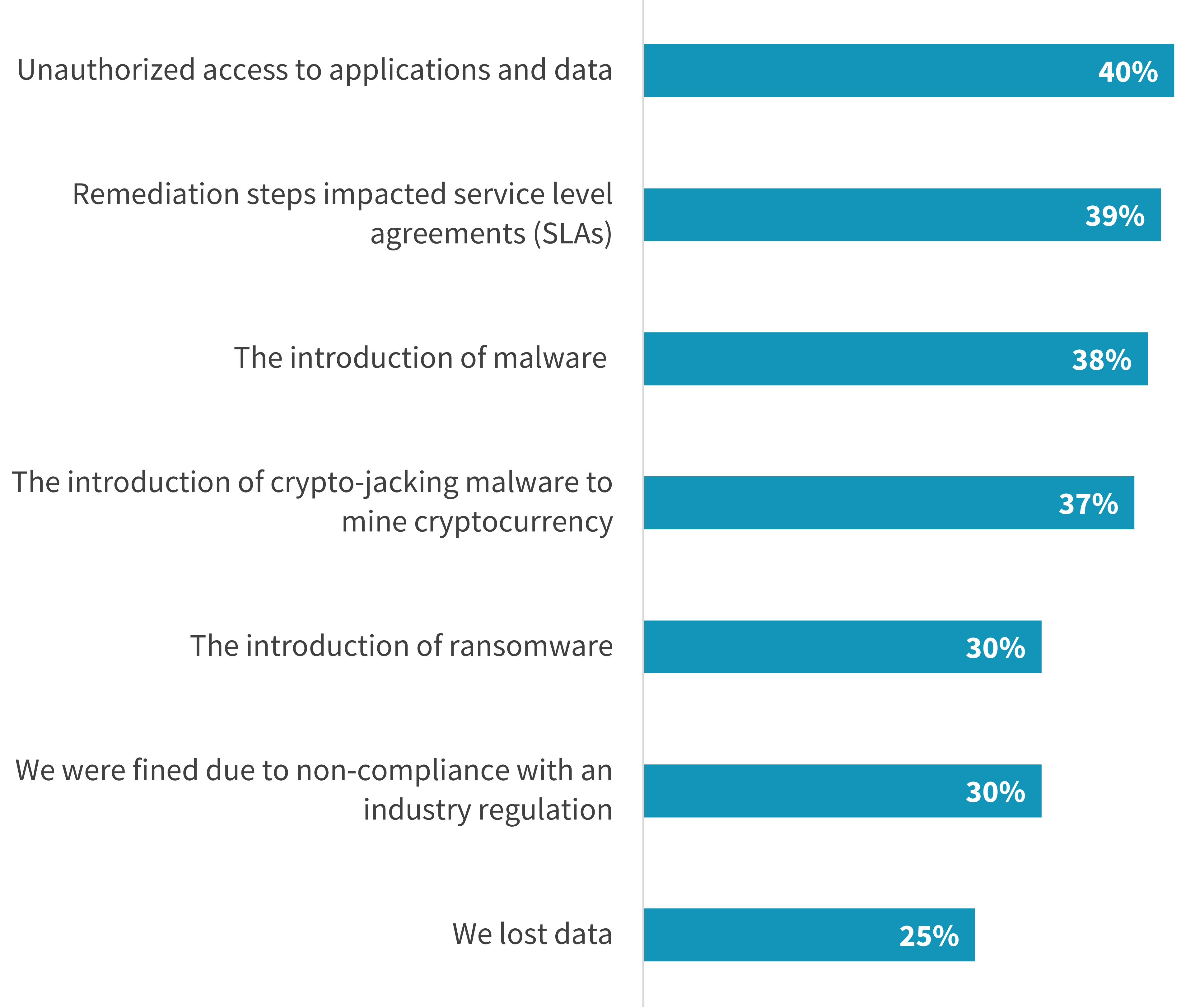
Identity and access management-related issues headline a series of misconfigured cloud services with serious ramifications

The most commonly reported types of cloud misconfigurations include those that spring from a disconcerting lack of IAM basics, such as the use of default passwords and lack of mult-factor authentication. These join other misconfigurations reported by respondents such as externally facing workloads subject to port scanning, overly permissive accounts targeted by bad actors, and unauthorized access to services via open ports. The ramifications have been serious – data compromises and the introduction of malware, including cryto miners and ransomware. The impact to SLAs indicates a need to automate updating infrastructure-as-code (IaC) templates via cloud security posture management (CSPM) controls.

Ten most common cloud misconfigurations in the past 12 months.



Results of cloud misconfigurations.

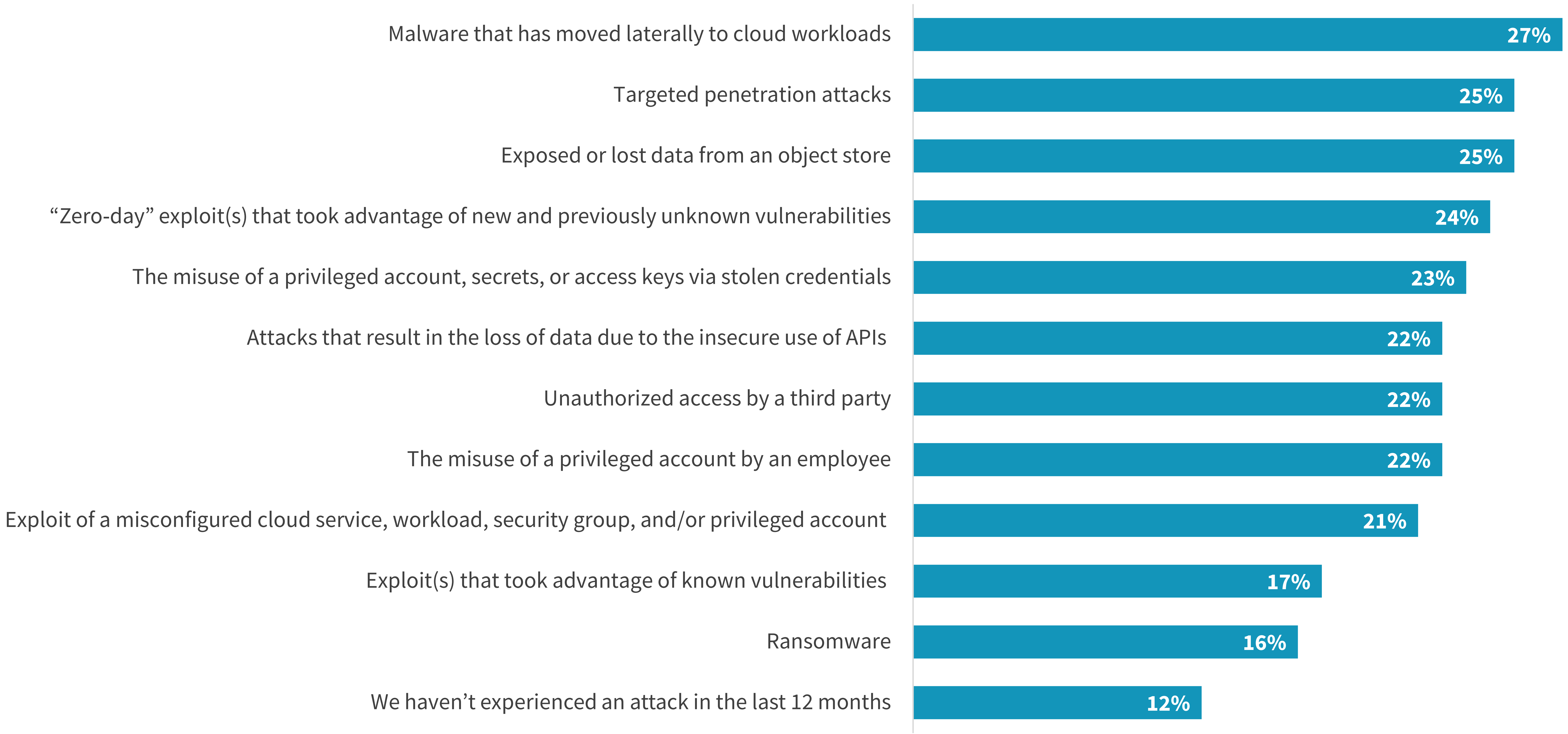


Back to Contents

A diverse range of attacks is centered on the exploitation of configuration and software vulnerabilities

The diversity of the threat landscape is often brought to bear against cloud-native applications and infrastructure. Indeed, only 12% of organizations reported not experiencing any cyber incidents targeting their cloud-native apps or infrastructure over the past year. This highlights the need for an integrated defense-in-depth approach. Such controls will enable a focus on hardened configurations, automation, segmentation, and the monitoring of accounts and services.

Cloud-native security incidents experienced in the last 12 months.



ONLY 12% report having **not** experienced an attack on their cloud-native apps and infrastructure over the last 12 months

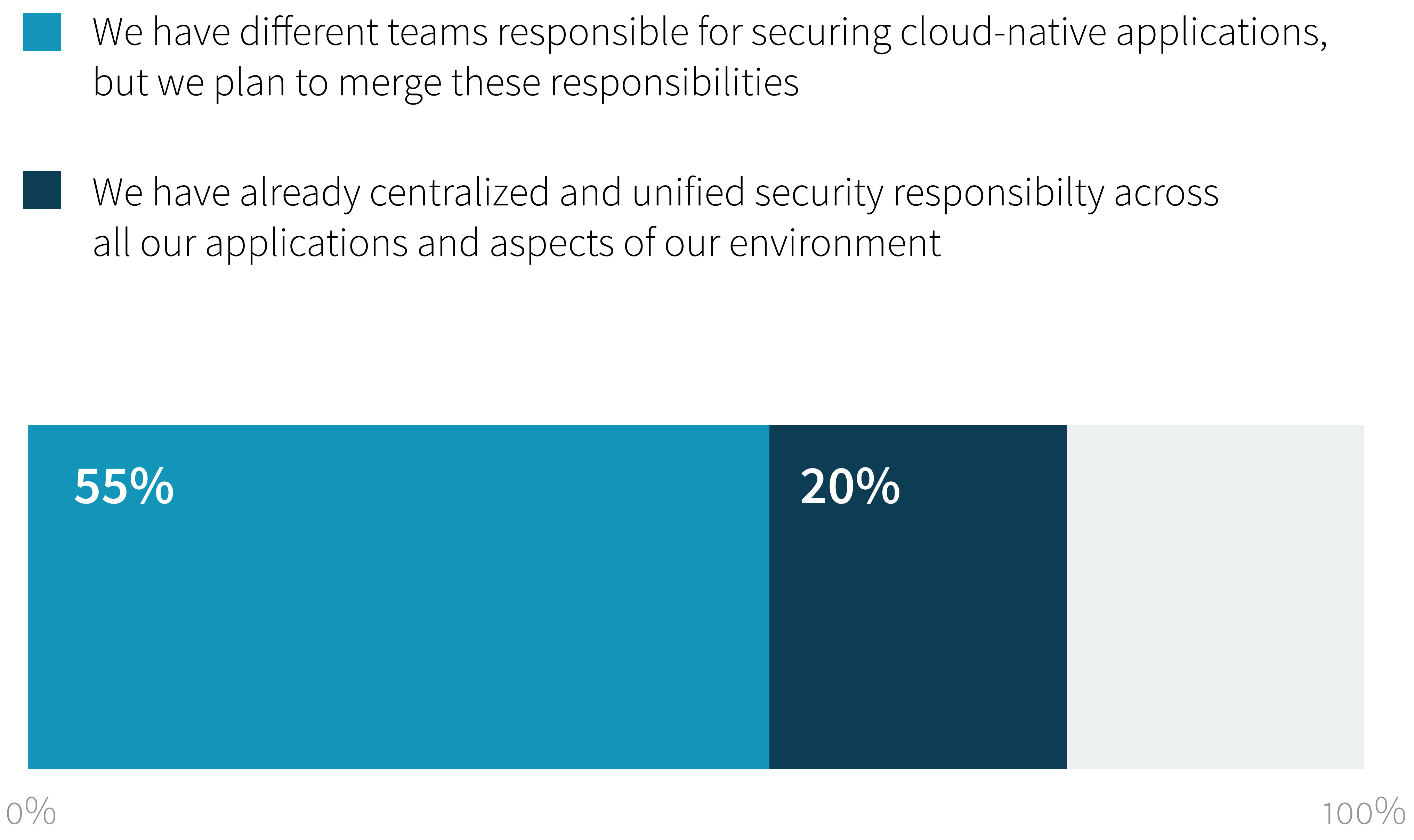
The People Who Secure Cloud-native Environments

The shift from a bottoms-up to a top-down approach is increasing the role of IT ops.

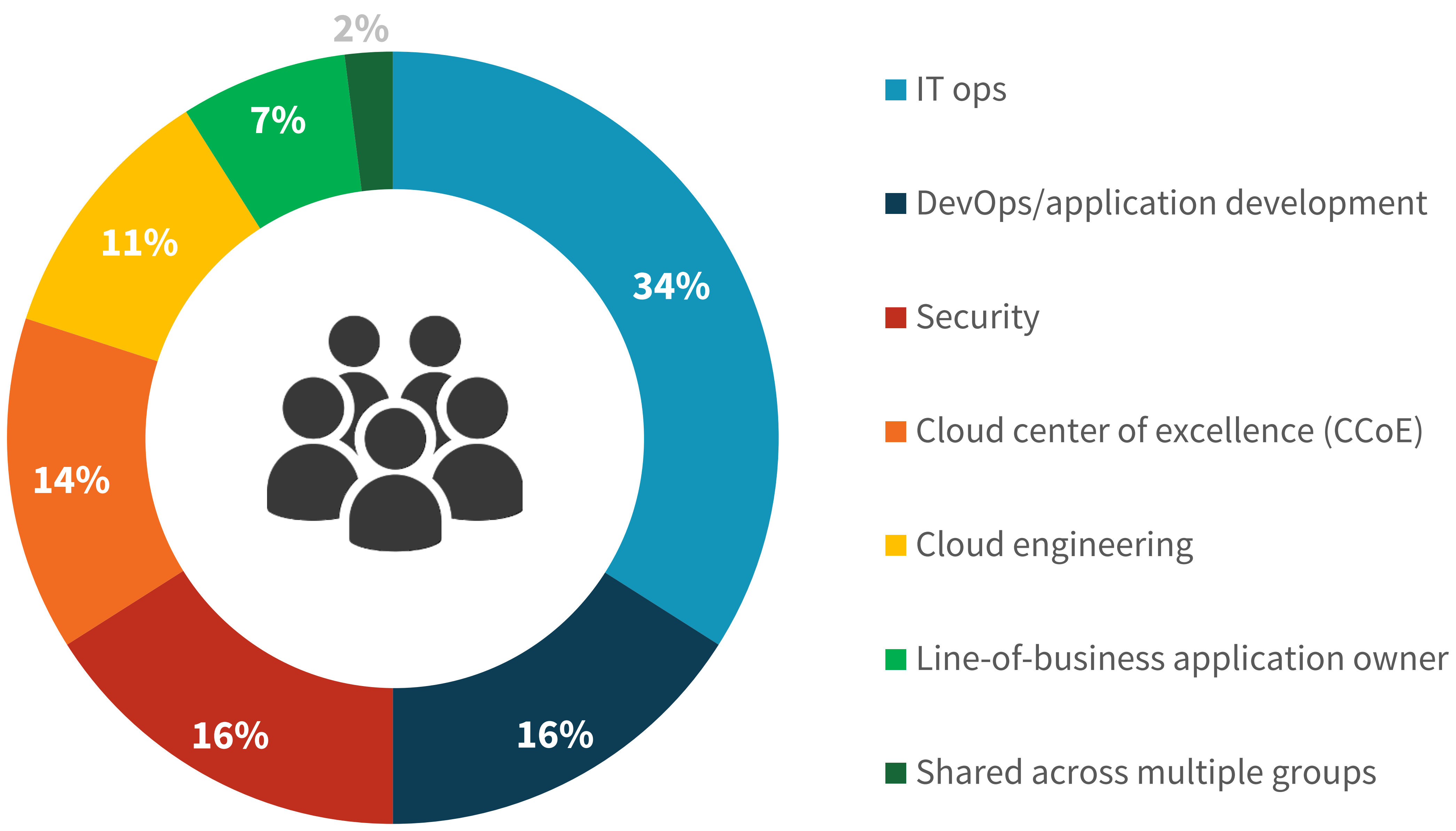
Plans to centralize and unify security by merging teams is elevating IT ops role in cloud-native security

As cloud-native applications gain critical mass and become a substantial portion of the IT footprint, companies are merging the related security responsibilities with their central security teams. This evolution is driving a shift from a project-team-led bottoms-up approach to a top-down approach for greater consistency across projects and environments.

Personnel approach to securing cloud-native apps and infrastructure.



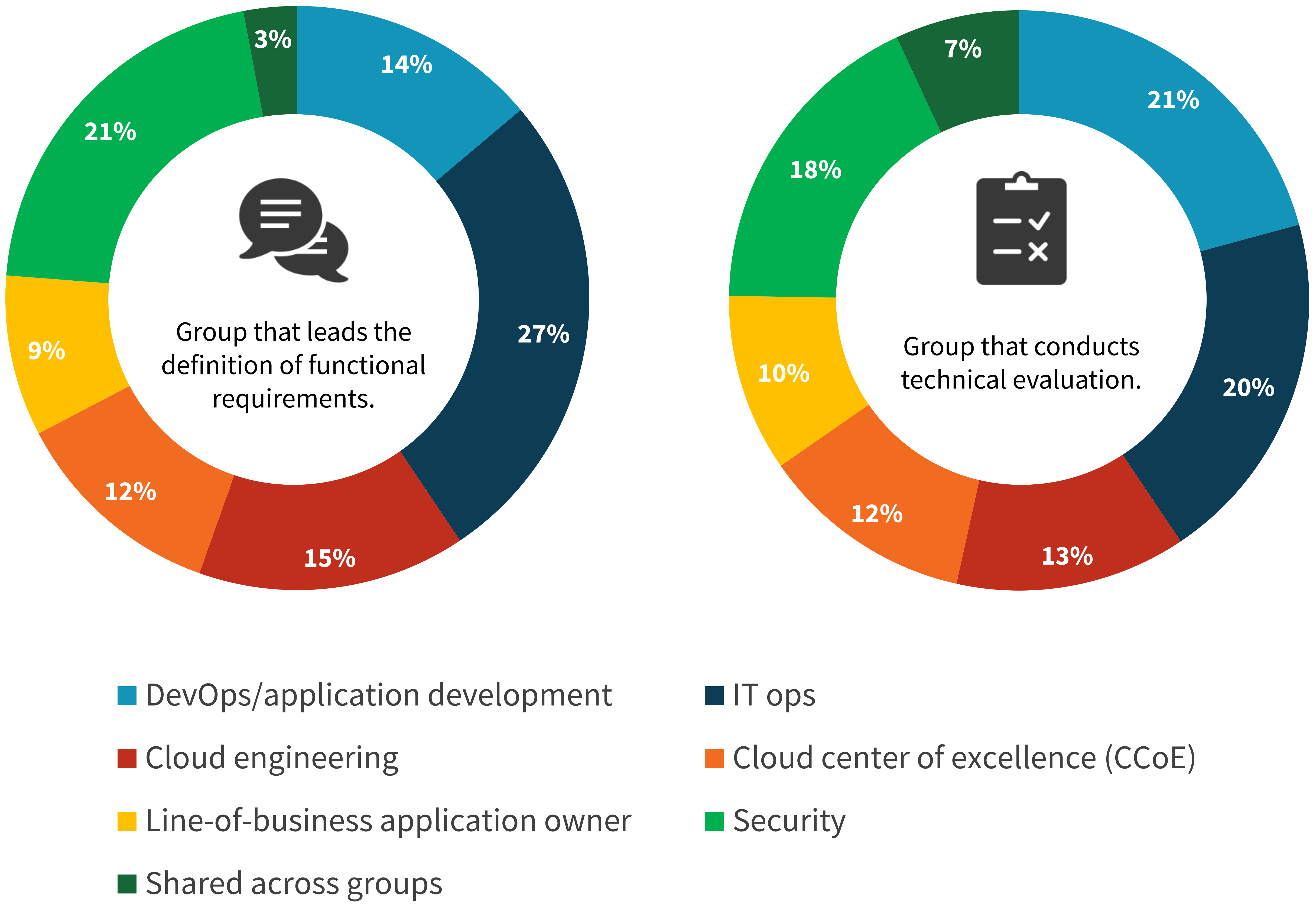
Group with primary responsibility of securing cloud-native apps and infrastructure.

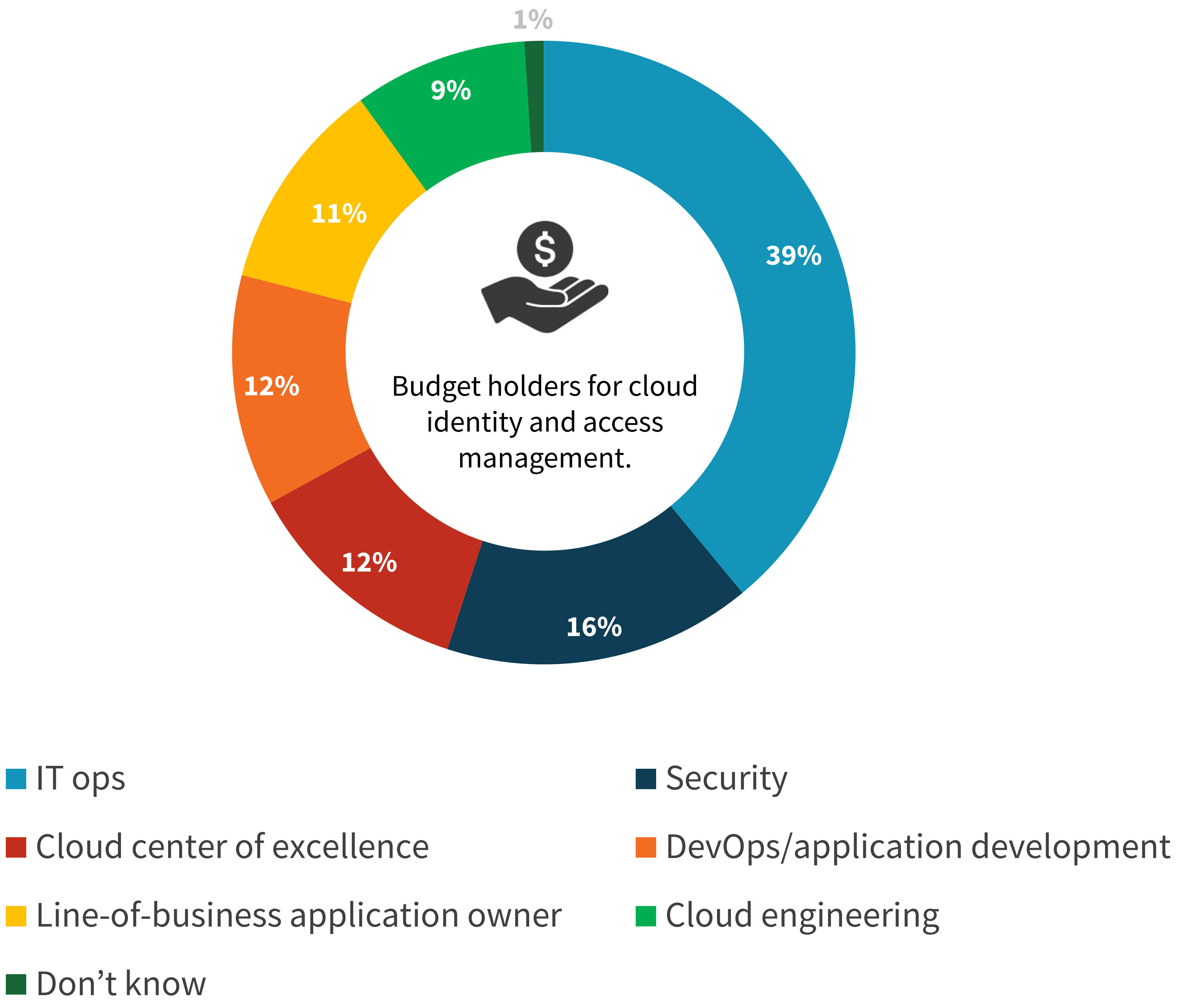


Back to Contents

Selecting and procuring cloud-native security controls is an IT ops-led team sport

Because different types of cloud-native controls are required for different layers of the stack and stages of the lifecycle, multiple stakeholders are involved in defining requirements and conducting the technical evaluations. With cloud-native applications serving business-critical functions, the choice of controls to protect them has become a strategic decision, a buying process that is now being led more often than before by IT ops or security teams.





Back to Contents

The Processes of Cloud-native Security

Automation via SDLC integration spans the application lifecycle.

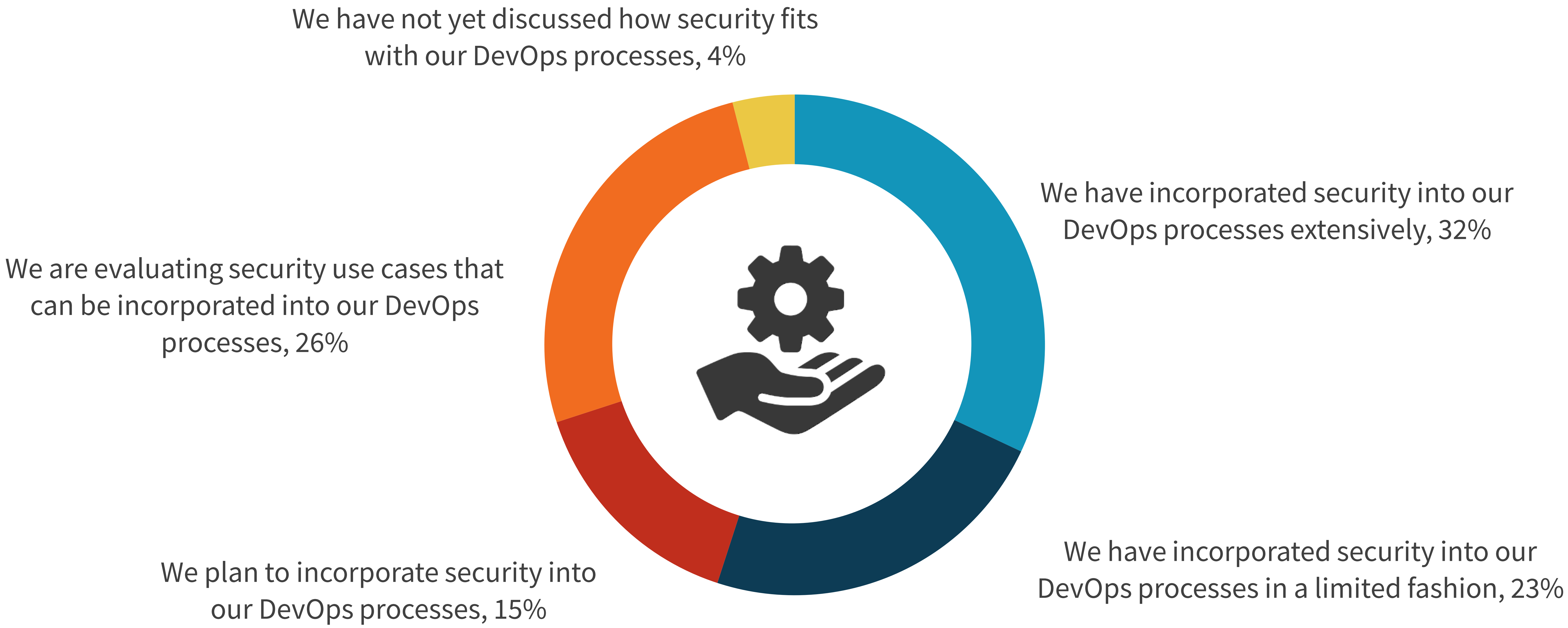
41%

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

The automation imperative is driving the integration of security into DevOps

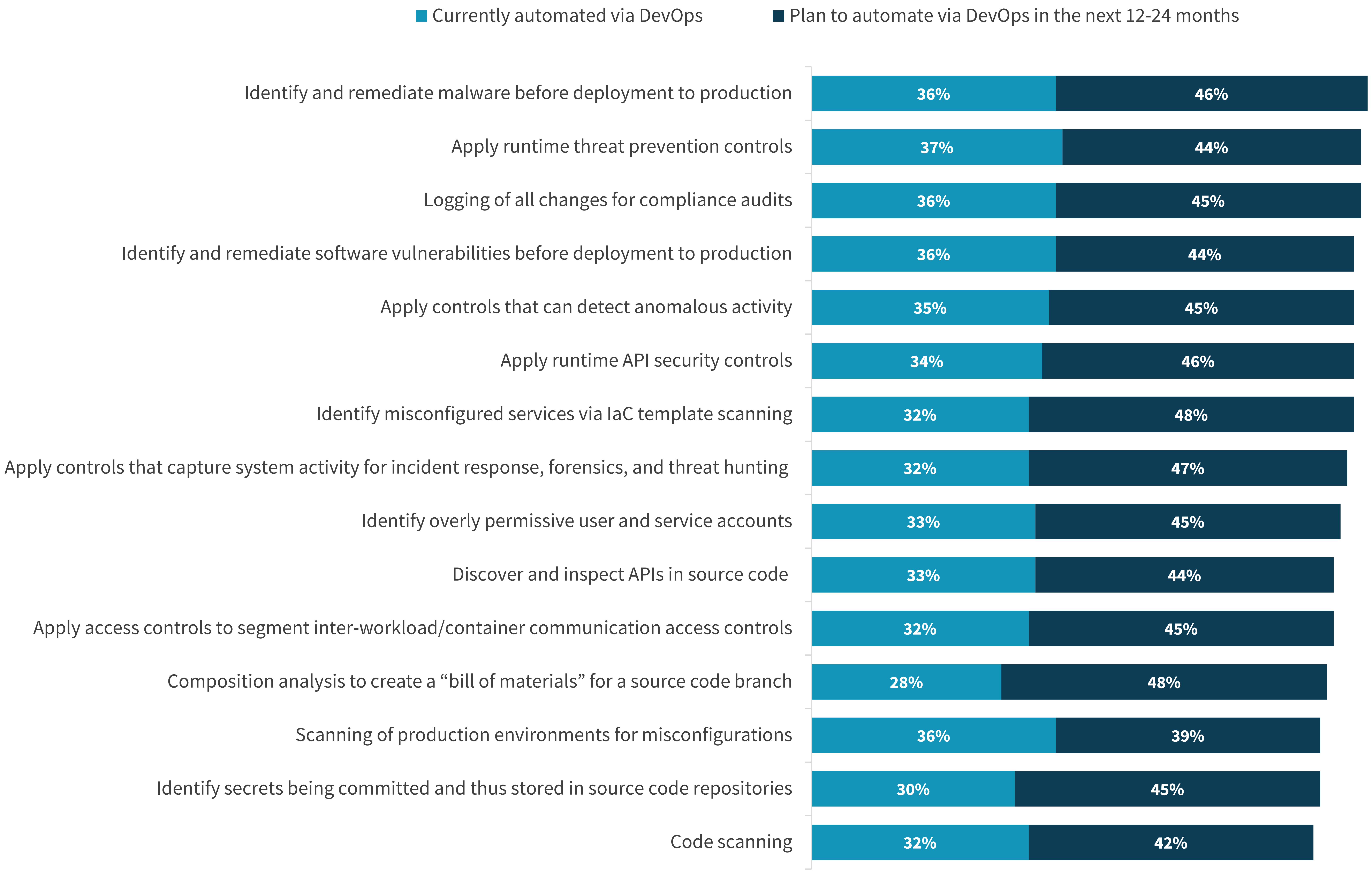
The need to keep pace with the elastic, dynamic nature of cloud-native applications and infrastructure makes automation a strategic tenet of cloud security programs. As a result, the ability to integrate cloud-native security controls into the tools that manage the software development lifecycle (SDLC), including the continuous integration and continuous delivery (CI/CD) stages, is a must-have requirement for such products.

Integration of security processes and controls via DevOps processes.



Back to Contents

Security practices automated via integration with DevOps.



As DevSecOps use cases expand across the lifecycle, more cloud-native applications will be protected

Current and planned secure DevOps use cases are being implemented across the application lifecycle, from the development stage to build and integration into delivery and production, which will result in an increase in those production cloud-native applications being protected via DevSecOps practices. This full lifecycle approach embraces both a shift-left approach and DevSecOps automation as a means for runtime protection.

Percent of cloud-native apps secured via DevSecOps

MEANS:

2021:	24 MONTHS FROM NOW:
38%	**51%**

Back to Contents

Technology: Cloud-native Security Controls

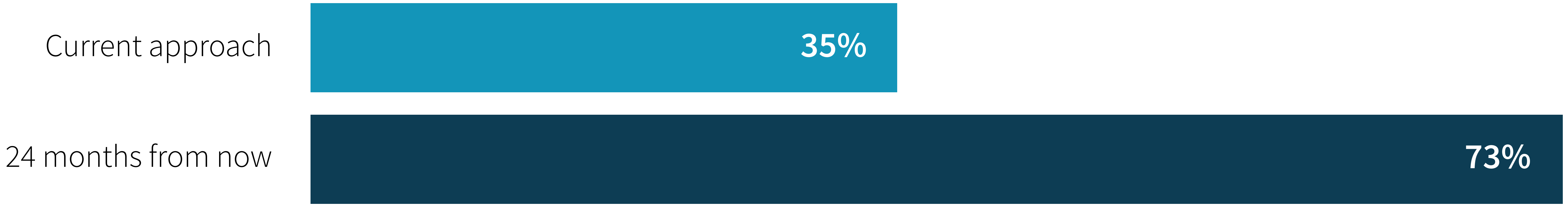
The requirement for breadth of coverage and depth of functionality is leading the consolidation of point tools into integrated platform modules.

Consolidation to integrated cloud-native security platforms is underway

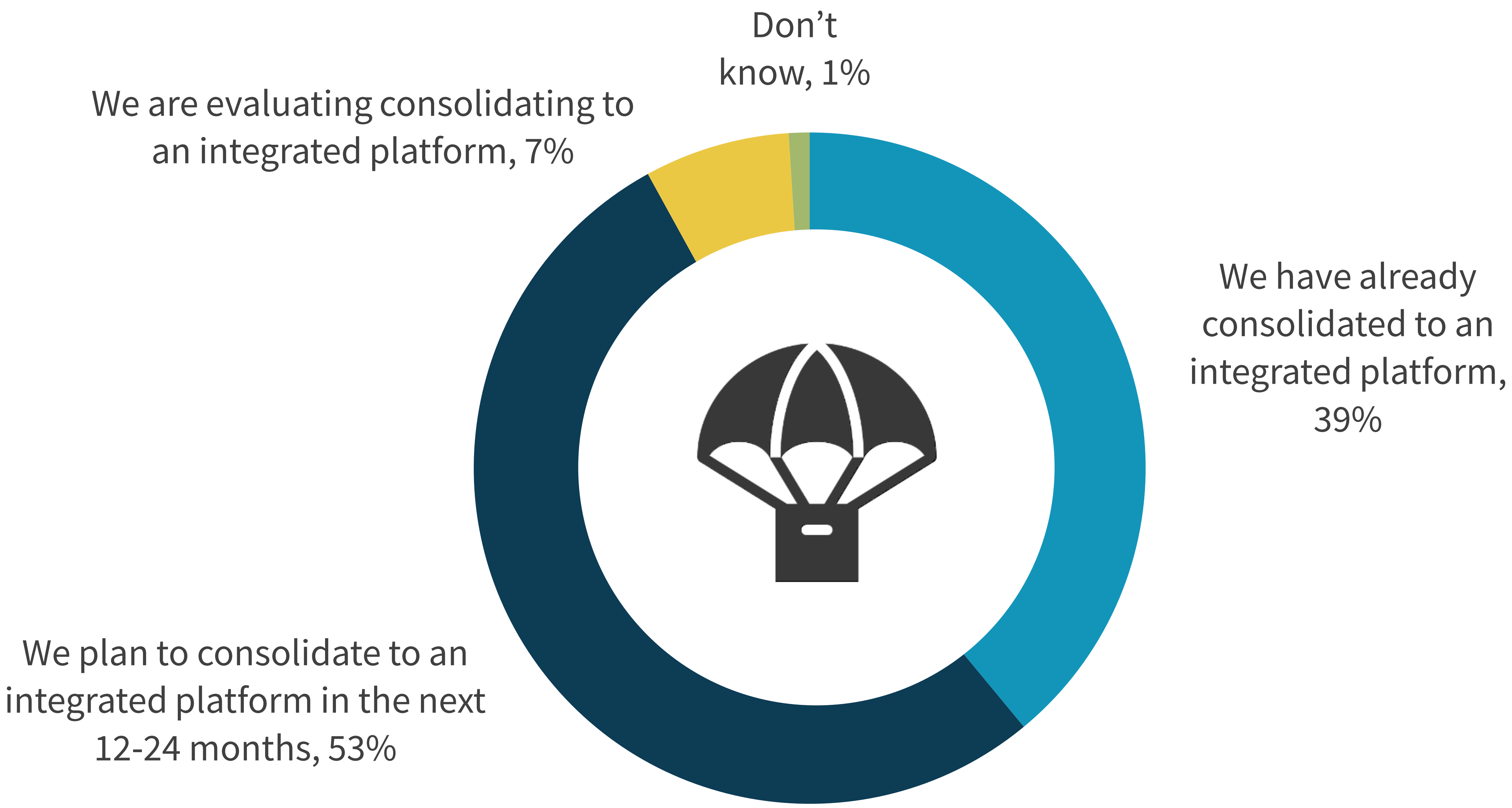
While many have opted for separate controls for separate environments and server workload types, there is a clear preference moving forward for integrated platforms to enable a centralized approach to securing heterogenous cloud-native applications deployed across distributed clouds. In fact, more than half of respondents indicated their organizations intend to consolidate to an integrated platform in the next 12-24 months.

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

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



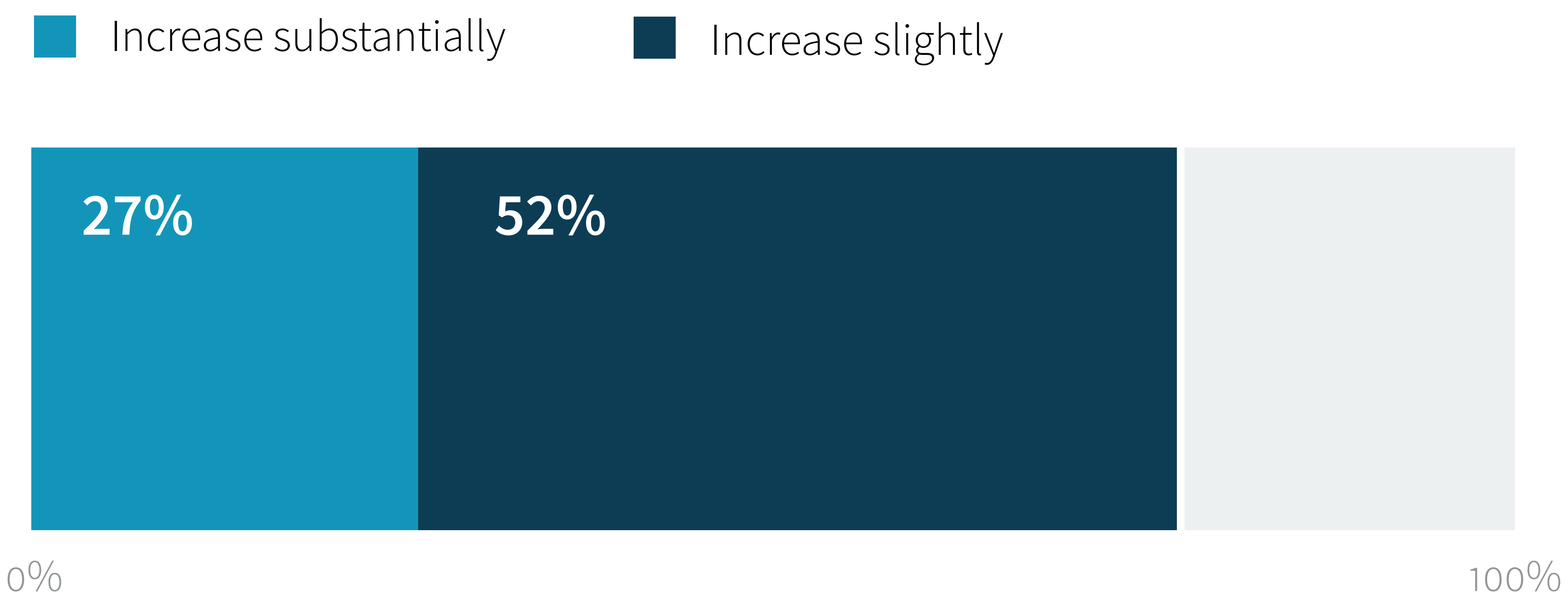
Plans for deploying an integrated platform to protect cloud-native applications and infrastructure.



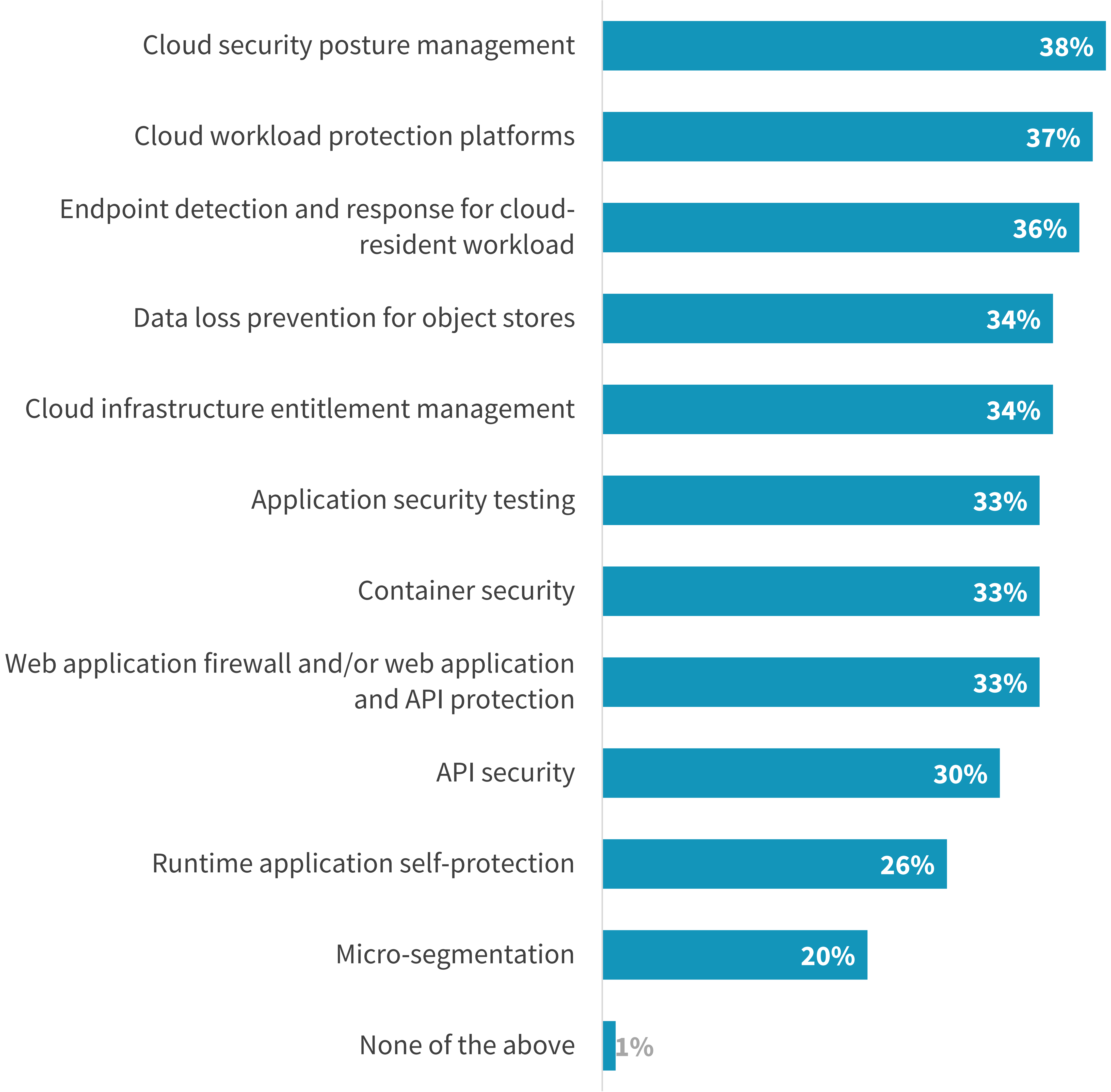
Appreciable investments will be made to close the cloud security maturity gap

The transition from remote work to the hybrid workplace is driving incremental adoption in IaaS/PaaS services and cloud-native applications. This broader adoption of IaaS/PaaS services along with further development and deployment of cloud-native applications is resulting in an increase in cloud-native security spending. Such investments will be made on functional modules now being integrated into cloud-native application protection platforms (CNAPP) headlined by CSPM and CWPP. The projected increase in EDR for cloud-resident workloads is part of broader XDR initiatives that will allow SOC teams to gain greater visibility into cloud-native apps and infrastructure.

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



Cloud-native app security controls that will benefit from increased spending.



McAfee

In responding to a digital transformation mandate most organizations are leveraging the agility, elasticity, and innovation velocity of public cloud providers, either solely or in conjunction with their private data centers and private clouds in a hybrid manner. All organizations want to unleash the productivity and creativity of their developers to rapidly develop and deploy compelling cloud-native applications. And all organizations want to ensure that their data, workloads, and resources in these cloud-native applications are safe and regulatorily compliant.

LEARN MORE

About ESG

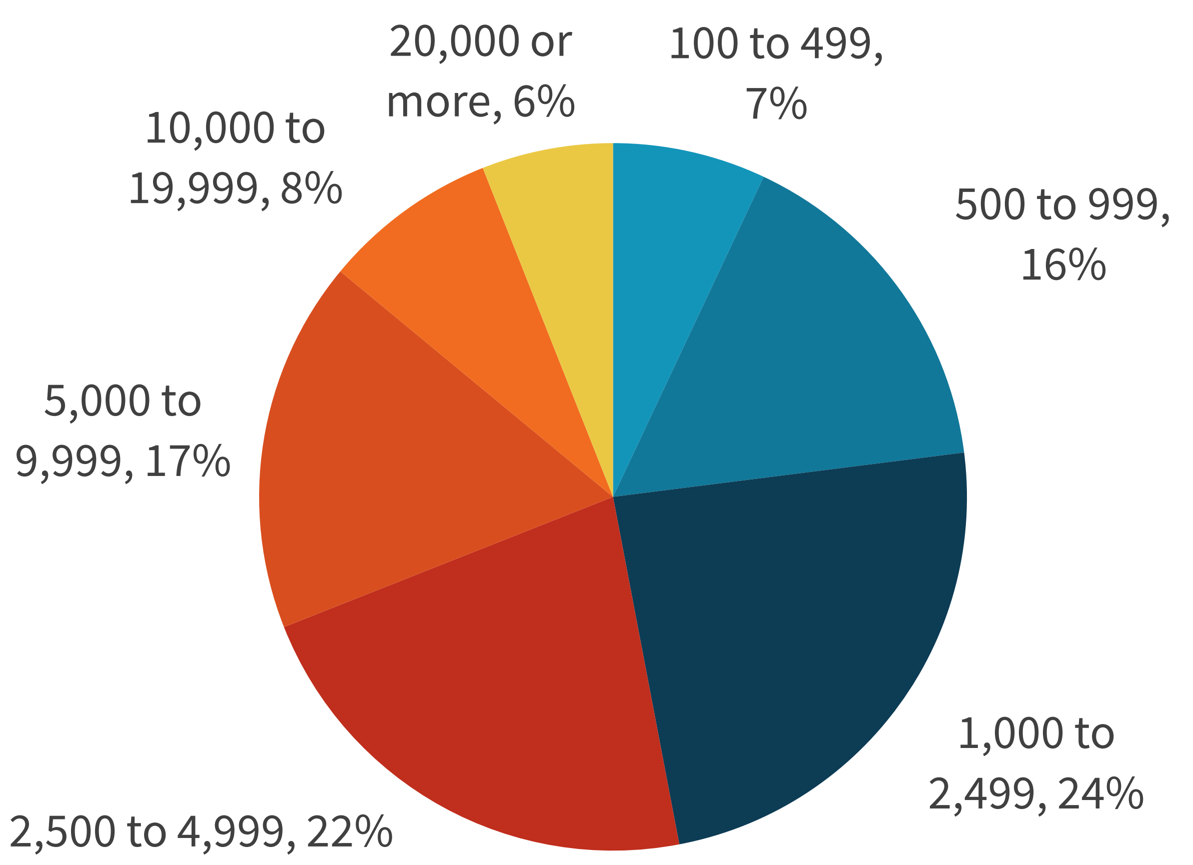
Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

Research Methodology

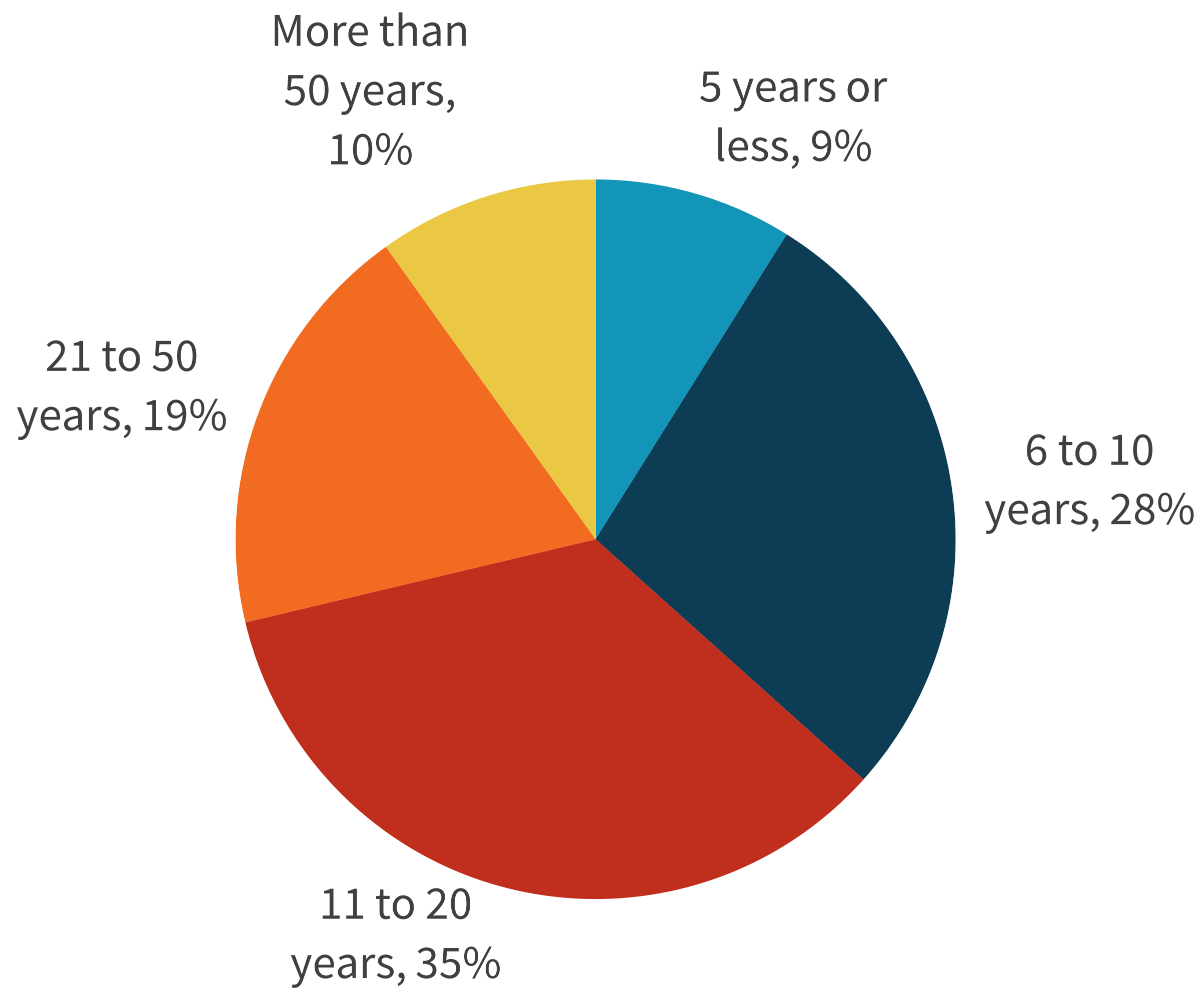
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between December 7, 2020 and December 26, 2020. To qualify for this survey, respondents were required 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.

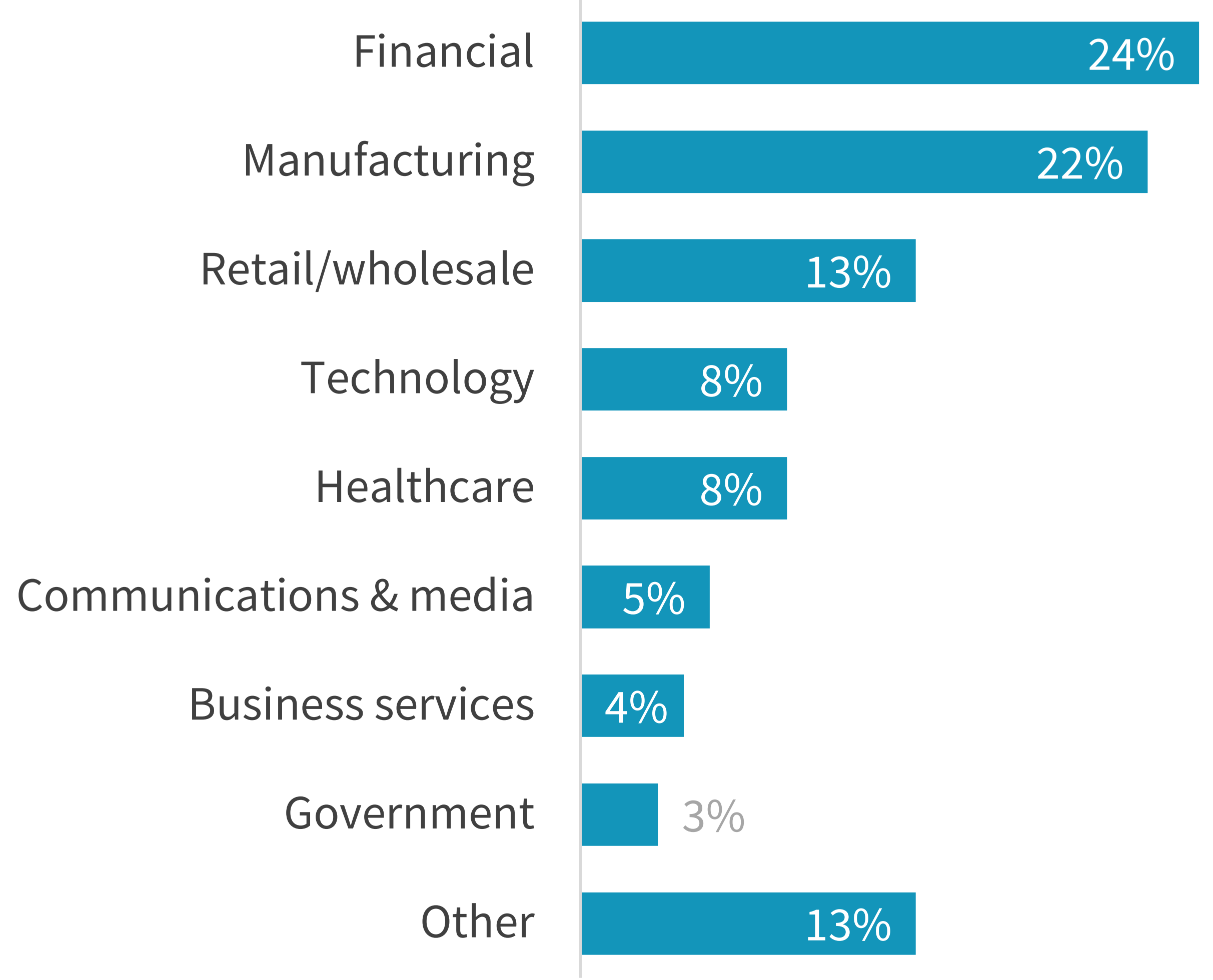
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



Back to Contents

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.