Enterprise Strategy Group™ by TechTarget

State of DevSecOps and Cloud Security Platforms:

Scaling Security Practices to Accommodate Cloud-native Application Development

Melinda Marks | Practice Director

ENTERPRISE STRATEGY GROUP

FEBRUARY 2025

Research Objectives

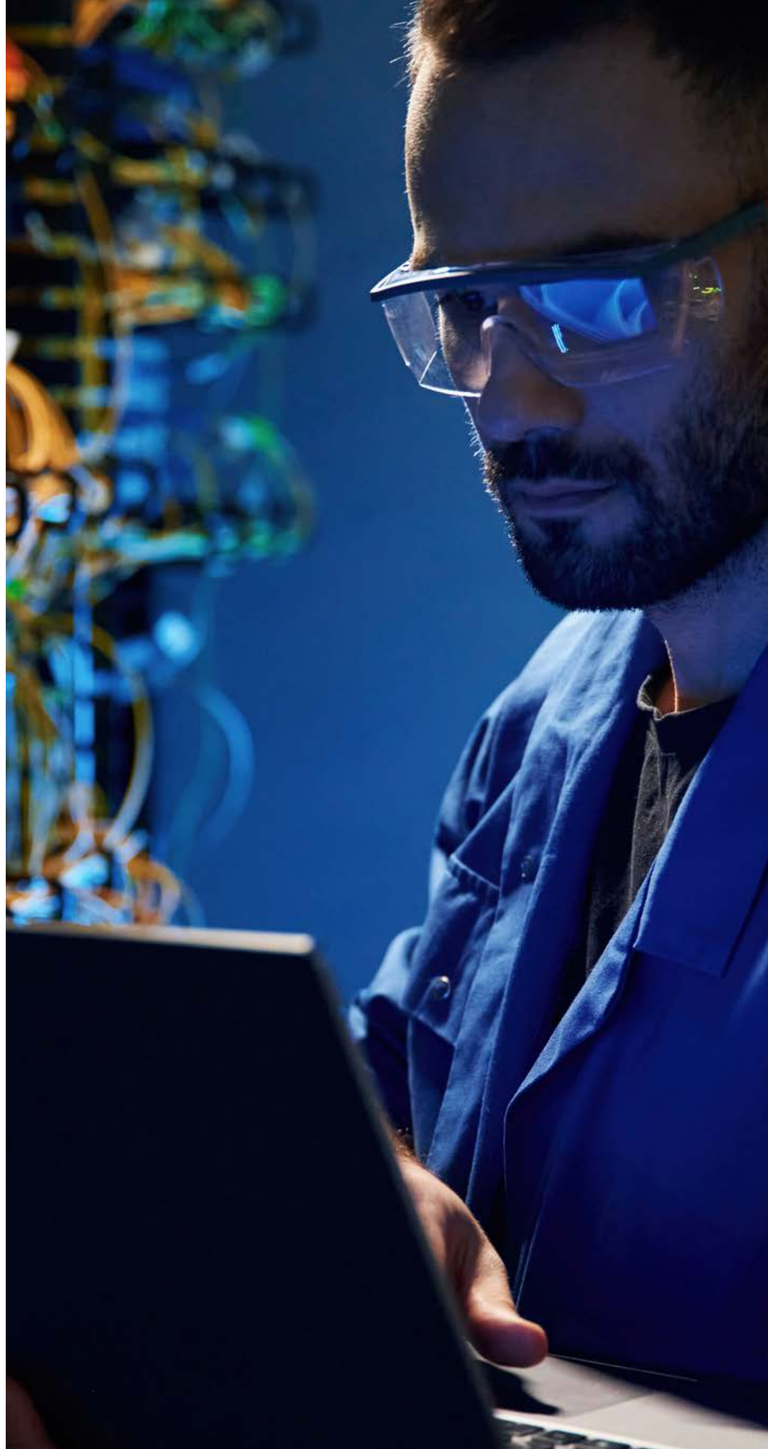
As organizations today face pressure to boost their productivity and scale while efficiently optimizing resources, they are increasingly utilizing cloud services to deliver cloud-native applications. Cybersecurity teams recognize the impact of security incidents on their cloud-native applications, including application downtime, business disruption, compliance fines, and negative brand reputation. They need effective cybersecurity solutions that address security risk from development to deployment to ensure security teams can support business growth.

The efforts to modernize application development utilizing cloud services are focused on optimizing efficiency for growth and scale. However, having separate, siloed security tools that work in different parts of the software development lifecycle works against the speed and efficiency that organizations are trying to achieve. As a result, organizations need to look for ways to gain unified visibility and control to efficiently manage risk and rapidly respond to threats and attacks by incorporating security into DevOps processes (DevSecOps) and utilizing cloud security platforms.

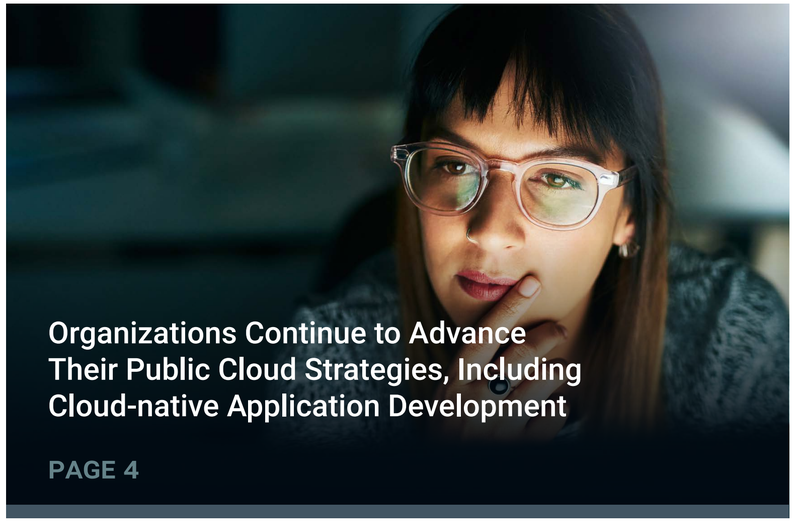
To gain insights into these trends, Informa TechTarget's Enterprise Strategy Group surveyed 373 IT, cybersecurity, and application development professionals in North America (US and Canada) responsible for evaluating or purchasing cloud security technology products and services.

THIS STUDY SOUGHT TO:

- **Establish** cloud-native application development adoption trends and the subsequent influence on supporting security strategies.
- **Track** the progress and maturity of organizations' cloud-native security programs.
- **Understand** the challenges organizations face incorporating security into developer processes, mitigating security risk, and detecting and responding to threats and attacks.
- **Highlight** buying patterns and key stakeholders influencing DevSecOps and cloud security platform investments.



Key Findings

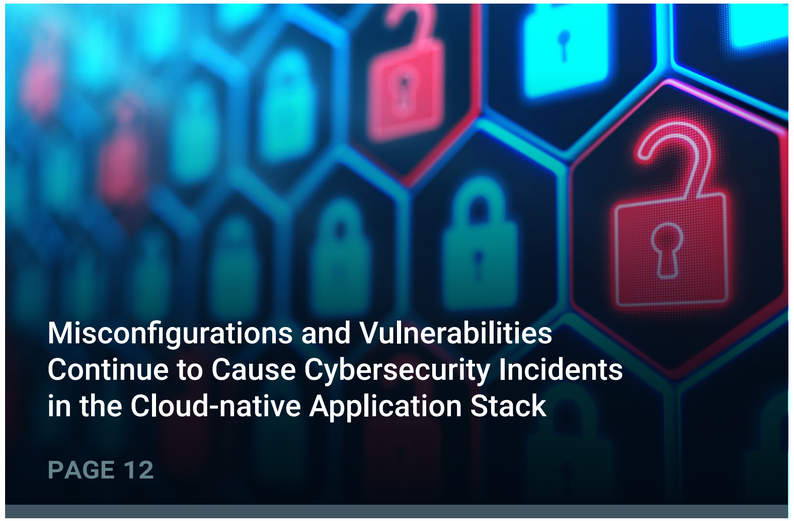


Organizations Continue to Advance Their Public Cloud Strategies, Including Cloud-native Application Development

PAGE 4

Challenges Managing Cloud-native Applications Across Environments Persist

PAGE 9



Misconfigurations and Vulnerabilities Continue to Cause Cybersecurity Incidents in the Cloud-native Application Stack

PAGE 12

Managing Application Security and Cloud Workload Controls Can Be Cumbersome, Which Could Be Mitigated via Consolidation

PAGE 15

Organizational Responsibilities for Securing Cloud-native Applications Vary but Generally Involve Cybersecurity Teams

PAGE 19

Increased Investments Are Expected in DevSecOps and Cloud Security Platforms

PAGE 22

BACK TO CONTENTS

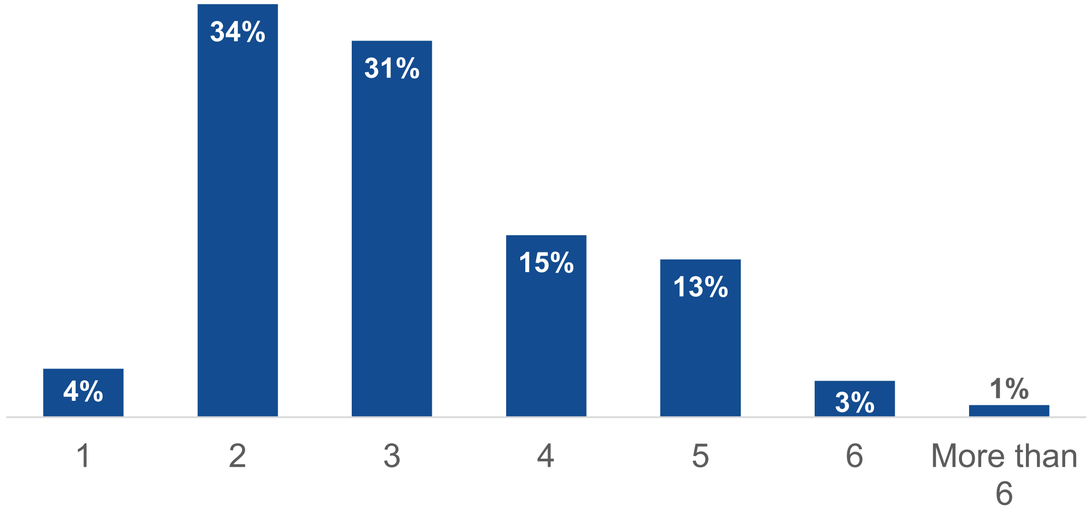
Organizations Continue to Advance Their Public Cloud Strategies, Including Cloud-native Application Development

Multi-cloud Strategies Are Pervasive and Create Challenges for Security Teams

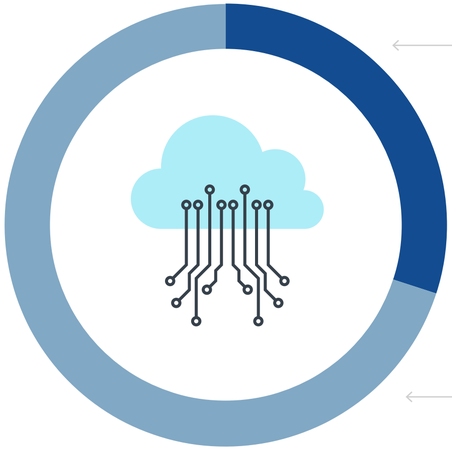
Organizations are utilizing cloud services to focus resources on building applications that they can easily develop and deploy in the cloud. The vast majority of those organizations using public cloud services leverage more than one unique cloud service provider (CSP), with nearly two-thirds using at least three. Among these multi-CSP organizations, 70% report having a primary CSP, with the balance using multiple in a meaningful way.

To protect their workloads in cloud environments, organizations have a shared responsibility with CSPs. It can be challenging for security teams to manage this when their organizations have workloads in multiple CSPs as each platform is architected differently, with diverse security features and capabilities. This can make it difficult for security teams to ensure consistent security controls and processes for workloads and applications across cloud and hybrid environments.

Number of unique CSPs in use.



How multiple CSPs are used.



30%

We use **multiple** IaaS or PaaS CSPs in a meaningful way

70%

We have **one primary** IaaS or PaaS CSP and use other IaaS or PaaS CSPs for small, discrete purposes

BACK TO CONTENTS

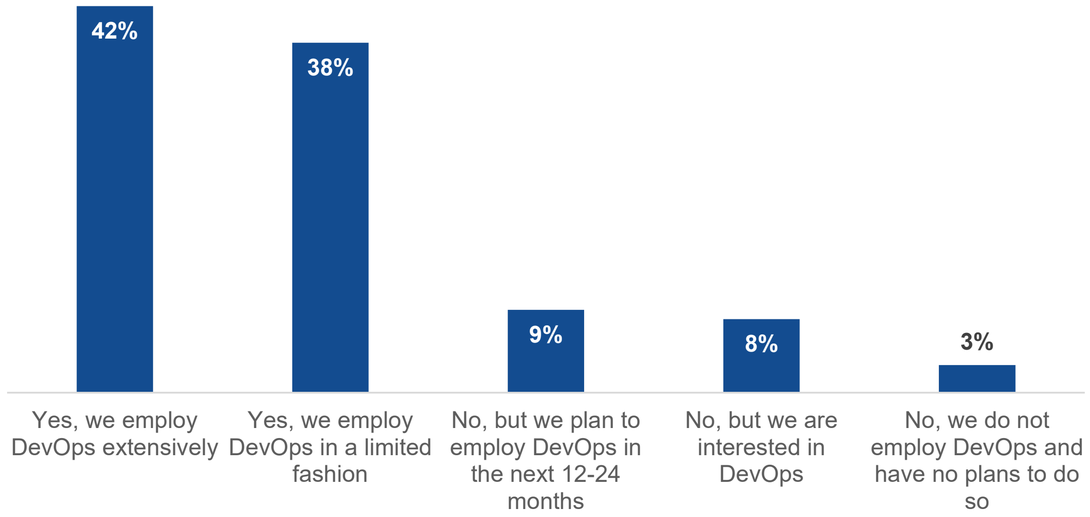
"One in five organizations are securing more than half of their production cloud-native applications via DevSecOps, **which is expected to jump to nearly two-thirds of organizations in 24 months."**

Increasing Usage of DevOps and DevSecOps Methodologies

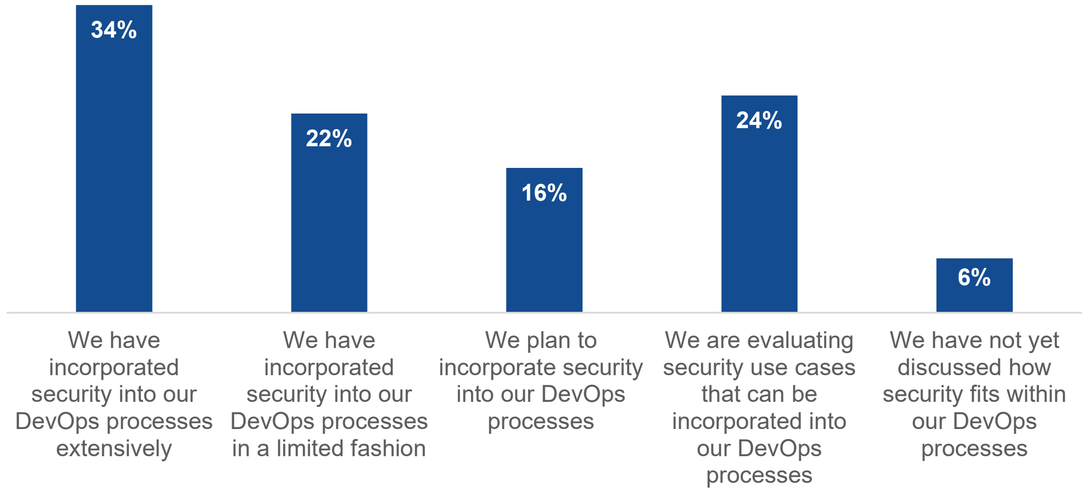
Organizations are continuing to adopt DevOps processes that streamline and automate IT and operations to efficiently provision and deploy software applications with continuous integration and continuous delivery (CI/CD) processes. A majority (80%) are employing DevOps processes, including 42% who utilize it extensively, with an additional 9% planning to use DevOps processes and methodologies in the next 12-24 months.

Among those using or planning to use DevOps, more than half (56%) have incorporated security into these processes, also known as DevSecOps, and another 16% plan to do so. Today, one in five organizations are securing more than half of their production cloud-native applications via DevSecOps, which is expected to jump to nearly two-thirds of organizations in 24 months.

Do organizations use a DevOps methodology to automate CI/CD processes?



Usage of DevSecOps to secure cloud-native applications.

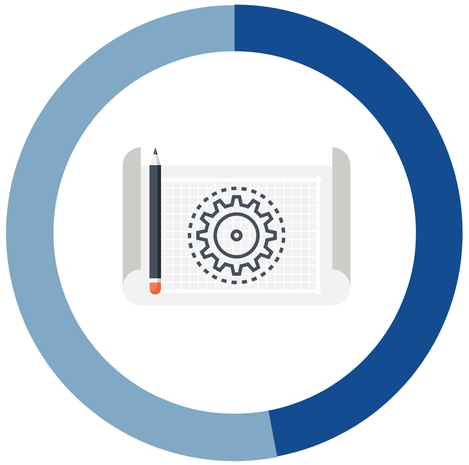


BACK TO CONTENTS

Security Teams Are Increasingly Responsible for DevSecOps

Effective DevSecOps requires organizations to incorporate security early in development processes. However, improvement is needed in this area, as currently only 53% of organizations said it is always incorporated early. To foster progress, security teams need to drive the efforts to incorporate security earlier in the development phase. The good news is that this advancement is evident in the fact that nearly half (48%) of organizations identify cybersecurity team members as typically having the responsibility for incorporating security early in development processes.

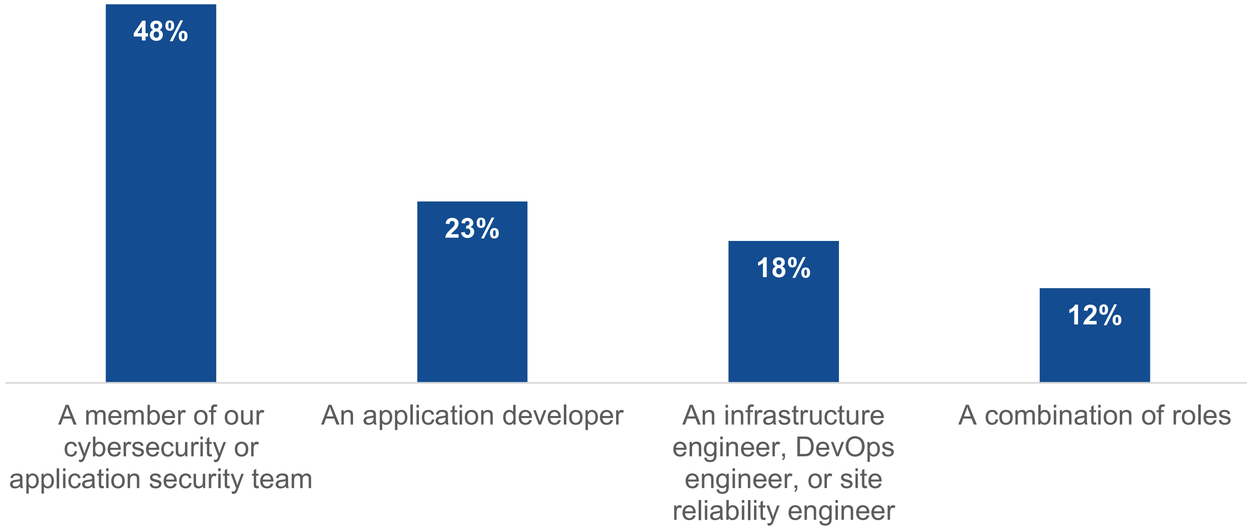
Frequency with which security processes are incorporated *early* into development processes.



53%
Our security processes are **always** incorporated early in development processes

47%
Our security processes are **sometimes** incorporated early in development processes

Group responsible for incorporating security early into development processes.

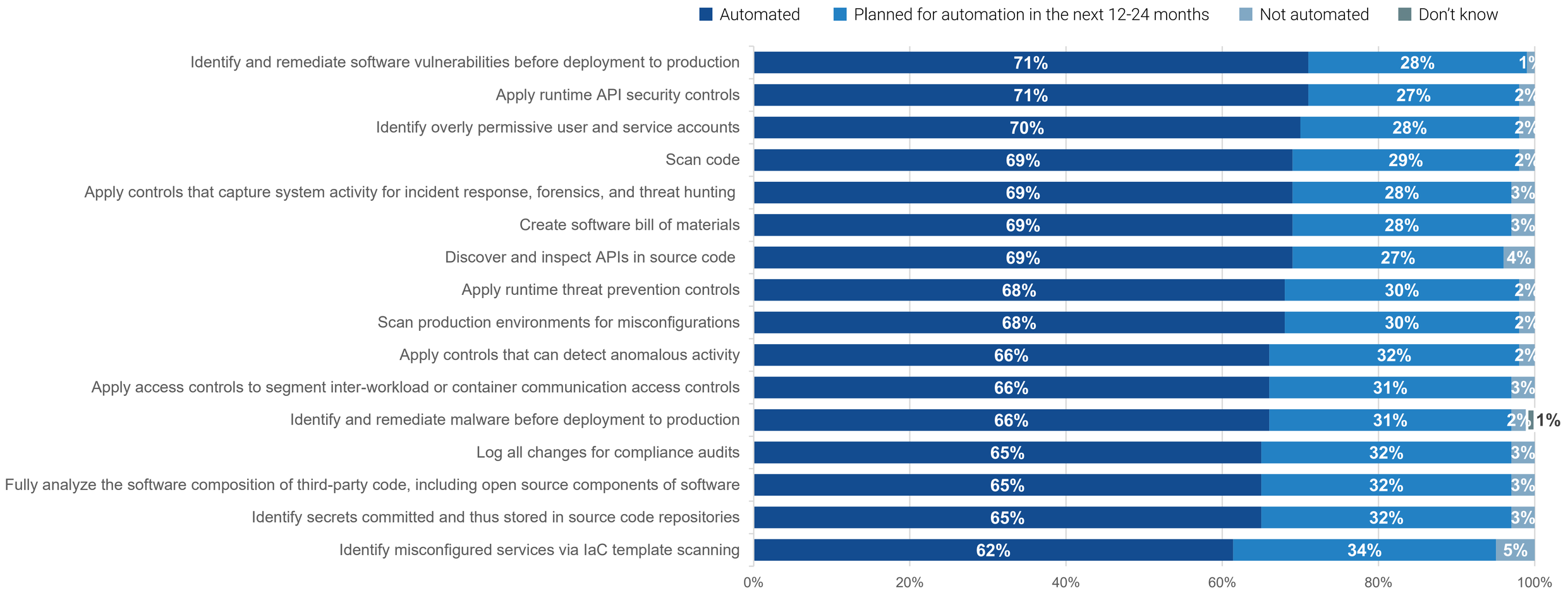


BACK TO CONTENTS

Security Practices Automated via DevOps Integration

How are organizations implementing DevSecOps? Most organizations—specifically, more than six in ten across the board—have automated a wide variety of security practices via integration within their DevOps tools and processes, and at least another quarter of organizations are planning to do so in the next 24 months.

Security practices that have been automated via integration with DevOps tools and processes.



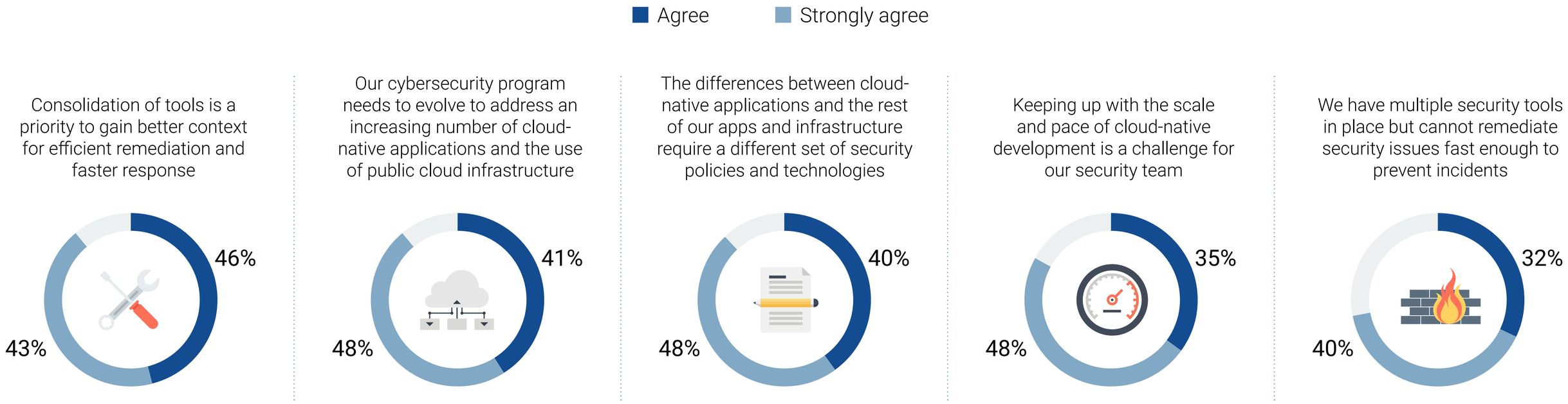
BACK TO CONTENTS

Challenges Managing Cloud-native Applications Across Environments Persist

Cloud-native Security Sentiment

When asked about cloud-native security, organizations' sentiments tend to prioritize consolidation as well as acknowledge the increase in cloud-native applications and use of public cloud infrastructure. Indeed, statements from respondents indicate the need for security solutions that provide efficiency so teams can scale to support cloud-native development with actions like consolidating tools, meeting the requirements of cloud-native applications running in cloud environments, keeping up with a faster pace of development, and gaining the context needed for rapid remediation.

Cloud-native security sentiments.



BACK TO CONTENTS

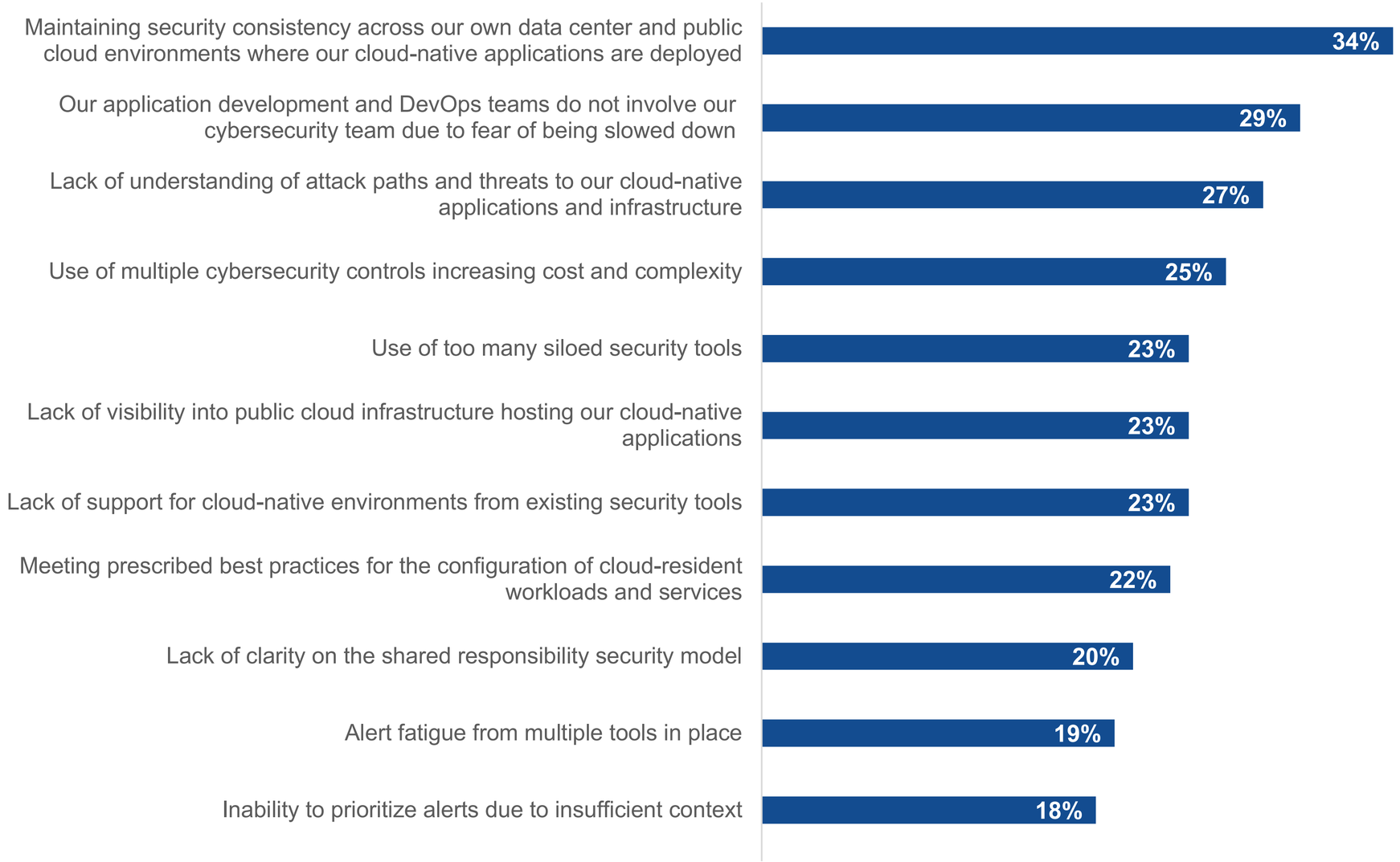
Lack of Consistency and Collaboration Top Cloud-native Application Security Challenges

Organizations face a variety of challenges related to ensuring security in cloud-native environments can scale without adversely impacting productivity.

Organizations are looking at how to maintain consistency across environments, which often requires tools from third-party security vendors to help them manage the security of applications across their multiple cloud environments.

They also need solutions that help teams work more efficiently so they are not disruptive to development processes.

Biggest cloud-native application security challenges.



BACK TO CONTENTS

Misconfigurations and Vulnerabilities Continue to Cause Cybersecurity Incidents in the Cloud-native Application Stack

Cloud-native Cybersecurity Incidents

The vast majority (94%) of organizations have experienced cybersecurity incidents specifically stemming from cloud-native applications and infrastructure in the last 12 months.

Although the highest percentage reported falling victim to "zero day" exploits taking advantage of new and previously unknown vulnerabilities, many of the incidents were the result of misconfigurations or issues that could have been thwarted with prevention and hygiene; several also related to catching issues earlier via automated testing or better controls and policies.

Cybersecurity incidents experienced in the last year related specifically to cloud-native applications and infrastructure.

"**Zero day**" exploit that took advantage of new and previously unknown vulnerabilities

29%

Attack that resulted in the loss of data due to the **insecure use of APIs**

27%

Targeted **penetration** attacks

26%

Exploit of a **misconfigured** cloud service, workload, security group, and/or **privileged account**

26%

Misuse of a privileged account **by an employee**

25%

Unauthorized access by a third party

25%

Exploit that took advantage of **known vulnerabilities**

24%

Exposed or lost data from an **object store**

24%

Misuse of a privileged account, secrets, or access keys via stolen credentials

24%

Malware that moved laterally to cloud workloads

22%

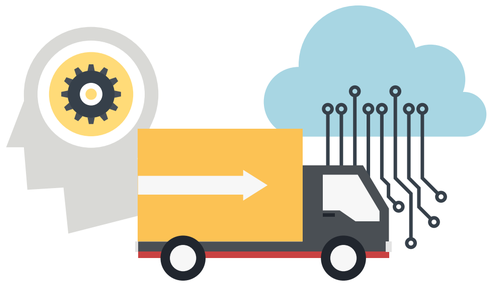
Ransomware

22%

We haven't experienced an attack in the last 12 months

6%

BACK TO CONTENTS



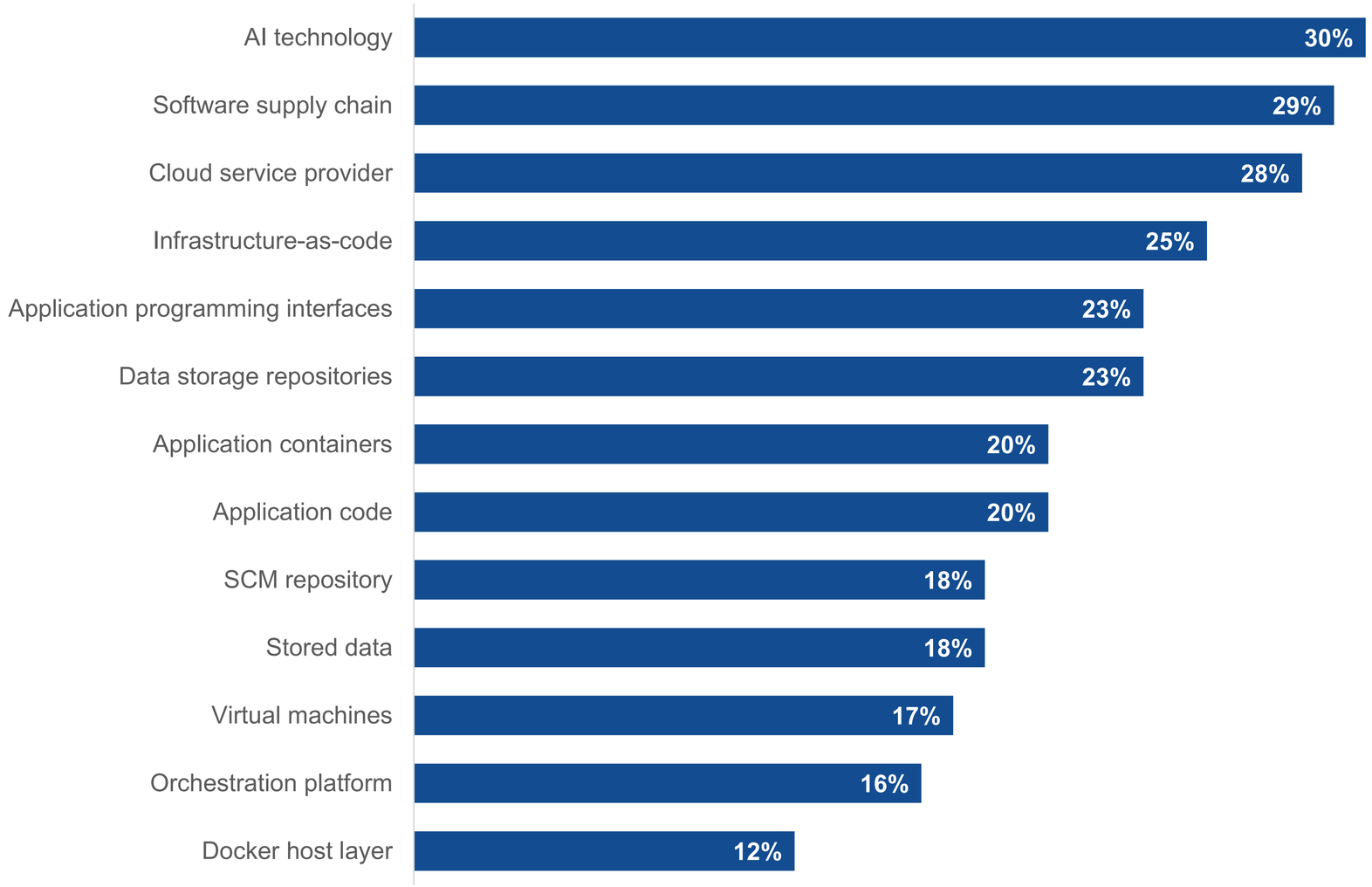
AI, the Software Supply Chain, and CSPs Are Most Susceptible to Compromise

Organizations are also worried about multiple elements of the cloud-native application stack.

As organizations increasingly adopt AI, it is not surprising that AI is the most commonly cited concern.

Teams are also worried about other areas scaling rapidly, including the software supply chain, cloud service provider infrastructure, IaC, and APIs.

Elements of the cloud-native application stack most susceptible to compromise.



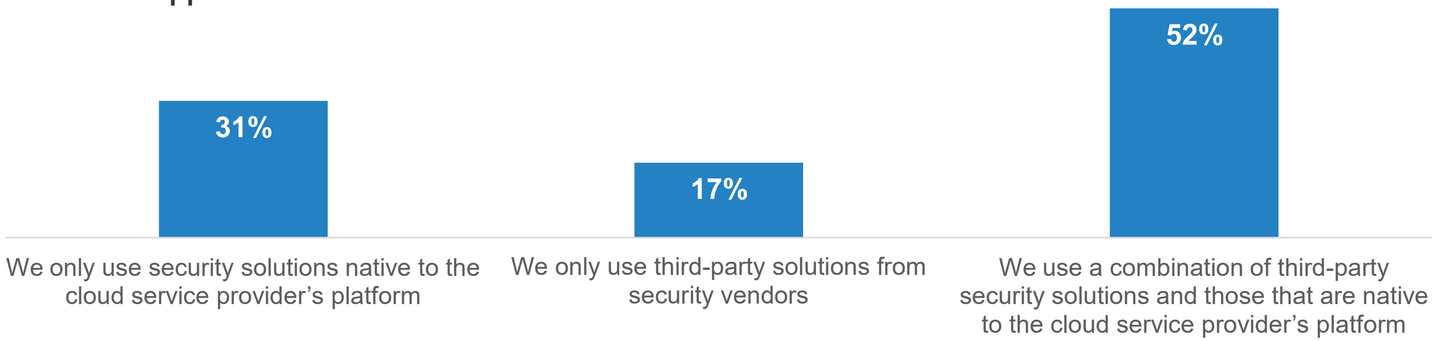
BACK TO CONTENTS

Managing Application Security and Cloud Workload Controls Can Be Cumbersome, Which Could Be Mitigated via Consolidation

Most Use a Combination of Tools From CSPs and Third-party Security Vendors

Although a high percentage of organizations indicated that they have a primary CSP, less than one-third (31%) *only* use security solutions from CSPs. The rest use either *only* third-party security solutions from security vendors or a combination of tools from the CSP and security vendors.

Types of solutions employed to secure cloud-native applications.

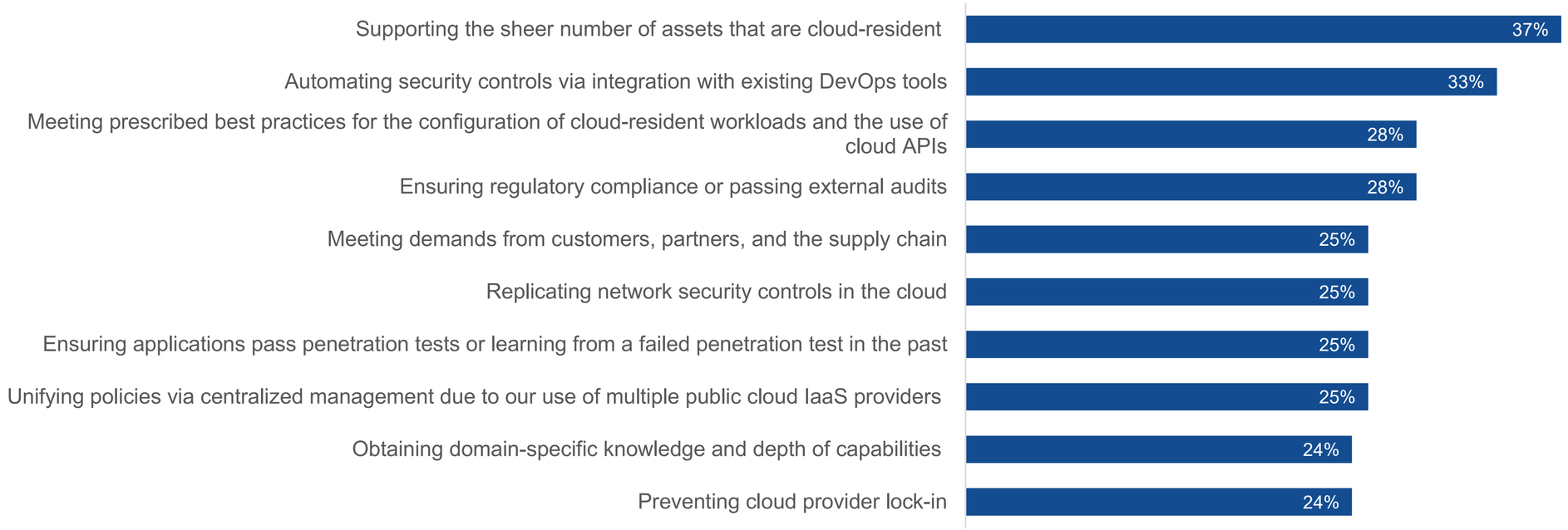


Organizations turning to third-party security vendors are looking for easier management to help their security teams support growth and scale.

They are looking for automation to save their teams from tedious, time-intensive tasks, as well as help with compliance, audits, and meeting customer demands.

It is important that these solutions help security teams manage across environments, including multiple CSPs and hybrid environments.

Drivers for using third-party security solutions.

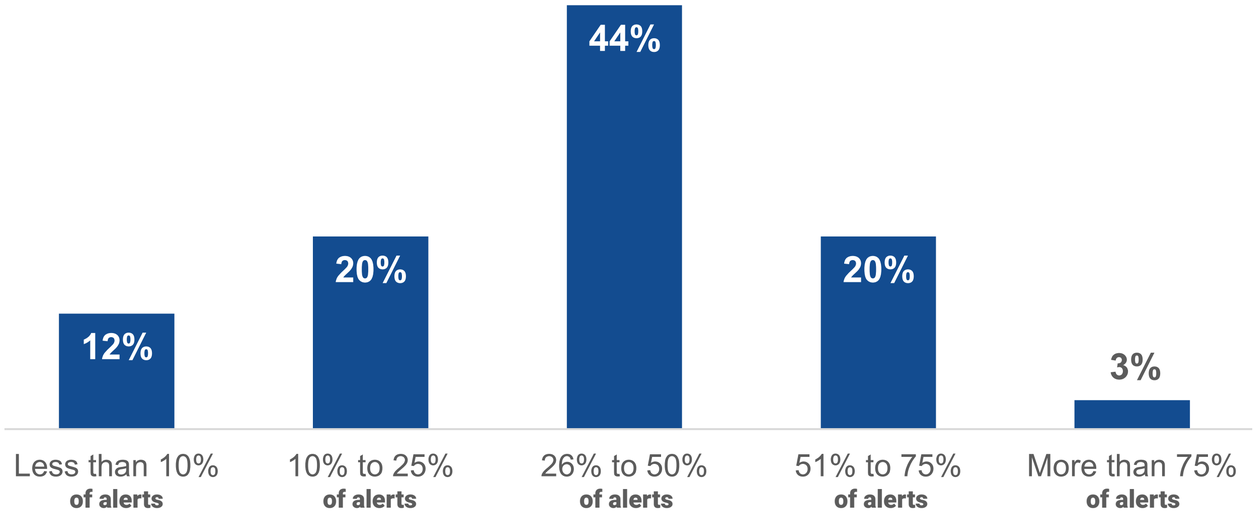


BACK TO CONTENTS

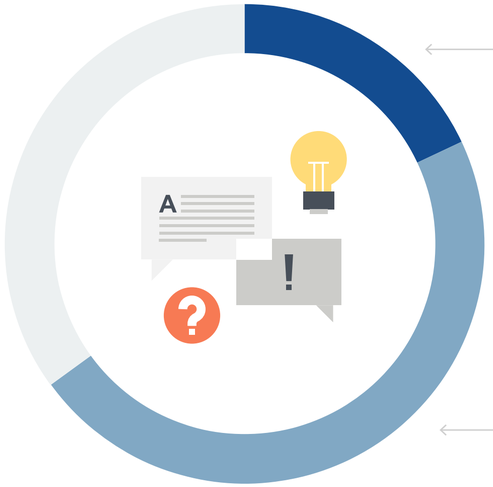
The Need to Prioritize Security Alerts

Another driver for third-party security tools is helping teams prioritize alerts. When security teams are inundated with security alerts, it difficult to prioritize and subsequently address the alerts that may lead to incidents. Indeed, the majority of organizations report ignoring more than one-quarter of their security alerts. To make matters worse, nearly two-thirds (65%) have seen an increase in security alerts coming from their cloud environments over the past year.

Percentage of cloud environment security alerts that organizations ignore.



Change in rate of cloud environment security alerts in the past year.



18%
The number of alerts has **increased significantly**

47%
The number of alerts **has increased**

BACK TO CONTENTS

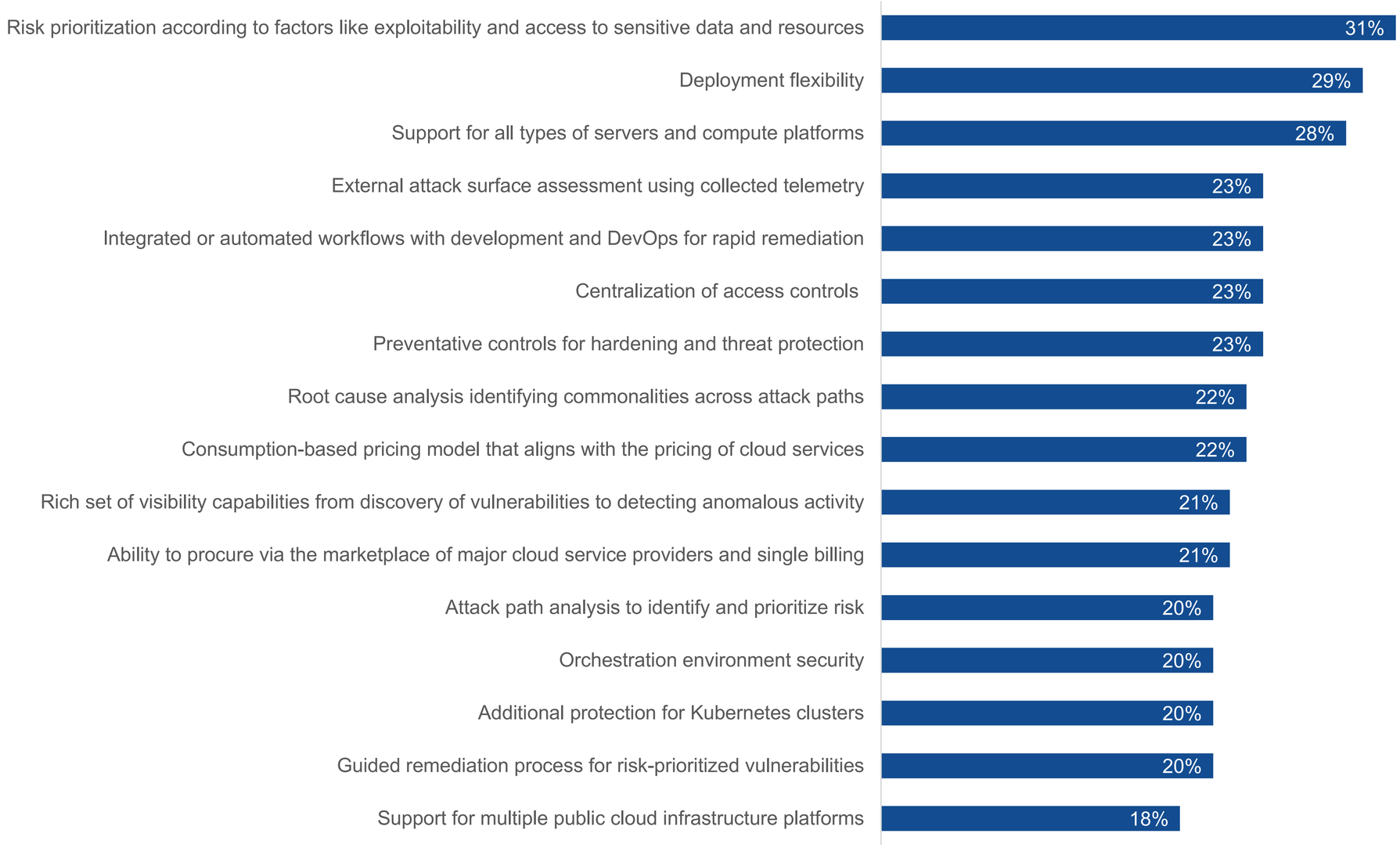
Top Attributes for a Cloud-native Application Security Solution

The top three most attractive attributes of a cloud-native application security product indicate a need to standardize security management for cloud-native applications across environments:

1. **Risk prioritization.**
2. **Deployment flexibility.**
3. **Support for multiple server types and platforms.**

Organizations further selected a wide variety of features needed for a comprehensive cloud-native application security program. These range from preventative controls to capabilities driving faster responses to threats and attacks.

Most attractive attributes of a comprehensive cloud-native application security product offering.



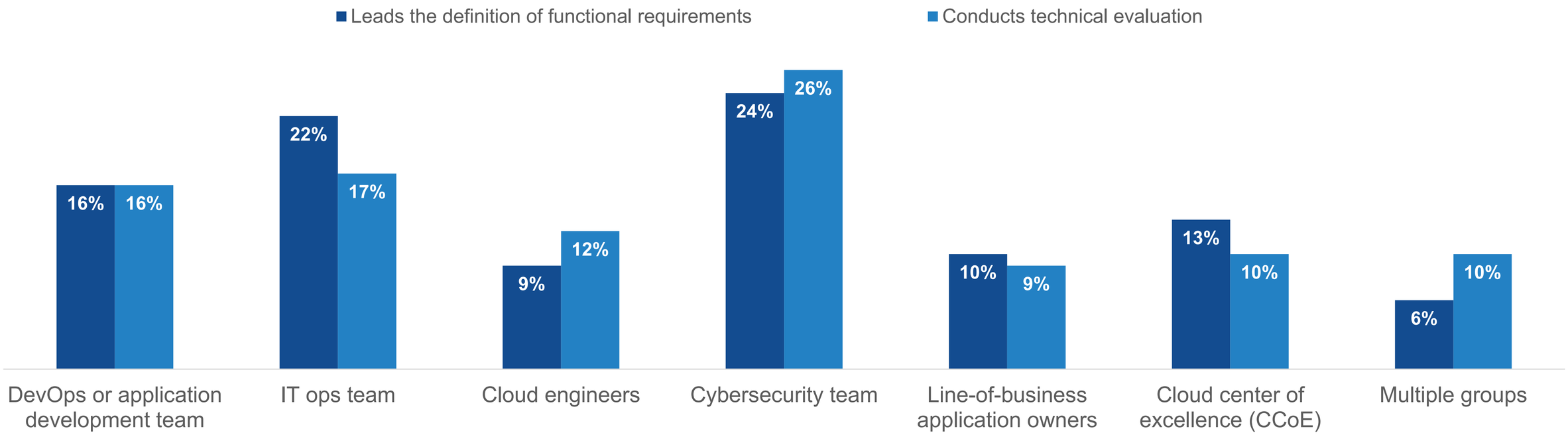
BACK TO CONTENTS

Organizational Responsibilities for Securing Cloud-native Applications Vary but Generally Involve Cybersecurity Teams

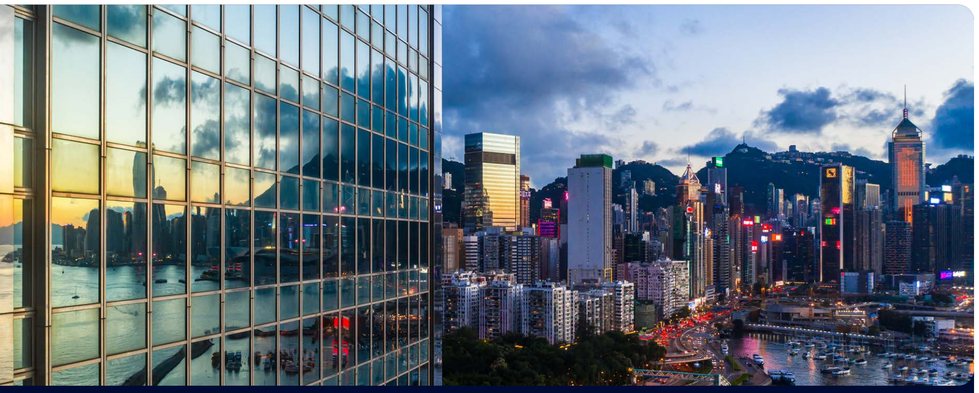
Defining Functional Requirements and Conducting Technical Evaluations

While different groups may lead the definition of functional requirements and conduct the technical evaluation for cybersecurity controls for cloud-native applications and infrastructure, those tasks are most commonly the responsibility of cybersecurity teams. This is also related to the need for multiple groups to set policies, which is indicative of requirements for cloud-native security tools to have flexibility to support multiple teams and ideally enable collaboration across teams to drive efficiency and reduce duplicative efforts.

Groups involved with evaluation processes for cloud-native application and infrastructure cybersecurity controls.



BACK TO CONTENTS



Multiple Groups Are Involved in Setting and Executing Cloud-native Application Security Controls

Multiple groups are involved in implementing and supporting the cybersecurity controls tasked with securing cloud-native applications. Not surprisingly, cybersecurity teams are most often involved, but to drive efficiency, a common platform should be used that allows multiple groups to set controls. Security teams need a way to gain additional visibility and control to best mitigate risk.

Groups that implement and operate the cybersecurity controls that secure cloud-native applications.

Cybersecurity team

58%

IT ops team

47%

DevOps or application **development** team

38%

Cloud engineers

29%

Cloud **center of excellence**

26%

Line-of-business **application** owners

16%

BACK TO CONTENTS

Increased Investments Are Expected in DevSecOps and Cloud Security Platforms

Majority Expect Increased Investments in Cloud Security Platforms and DevSecOps

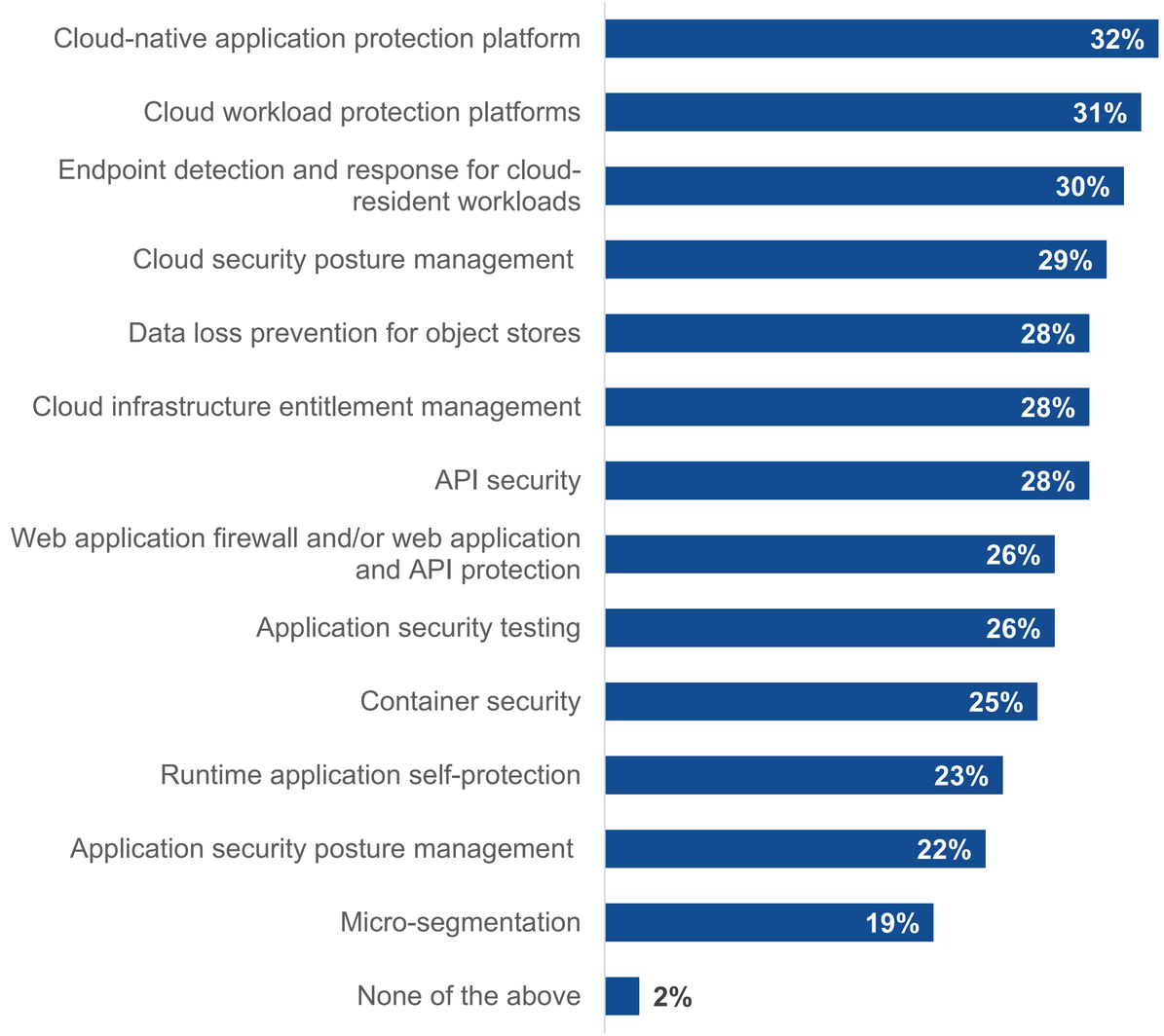
More than three-quarters (79%) of organizations plan to increase their investments in cloud security platforms and DevSecOps over the next 12 months. This includes investments across a wide variety of areas, including cloud-native application protection platforms, cloud workload protection platforms, endpoint detection and response, posture management, API security, and application security solutions.

Expected spending change for cloud security platforms and DevSecOps over the next year.

31%
Increase **substantially**

48%
Increase **slightly**

Areas of increased security spending due to cloud adoption.

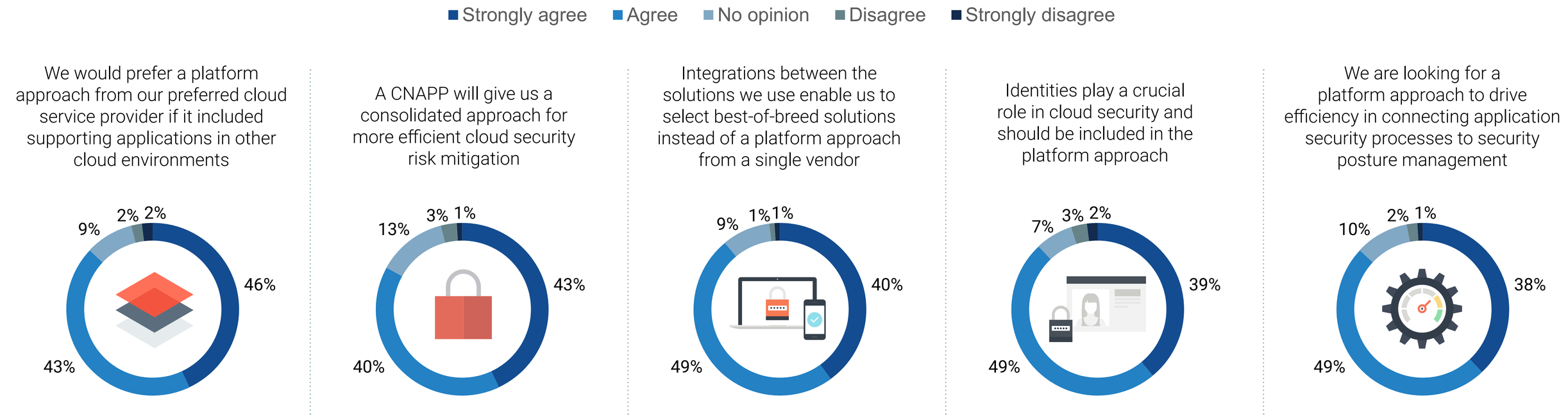


BACK TO CONTENTS

Organizations Seek Integrations and Platform Approaches

While organizations indicated they are looking for platform approaches, there is also strong sentiment for integrated best-of-breed tools. The broader capabilities of platform tools and integrations can give teams more comprehensive visibility and better context for risk prioritization so they can drive efficiency to support scale. Organizations believe a CNAPP will help but also seek capabilities such as identity security.

Views on cloud security tool consolidation and platform approaches.



BACK TO CONTENTS

LevelBlue

ABOUT

LevelBlue provides cloud security expertise and services, helping organizations innovate and migrate to the cloud safely. We reduce risk, increase visibility and control, and ensure continuous compliance with regulatory requirements. As a leading cloud security solution provider, we offer managed services and consulting for network and cloud security, exposure and vulnerability management, managed detection and response, and governance, risk, and compliance. LevelBlue supports your operational resilience and helps you mitigate risk and foster digital innovation. With a large, always-on global presence, we set the standard for cybersecurity, enhancing your resources so you can focus on the business.

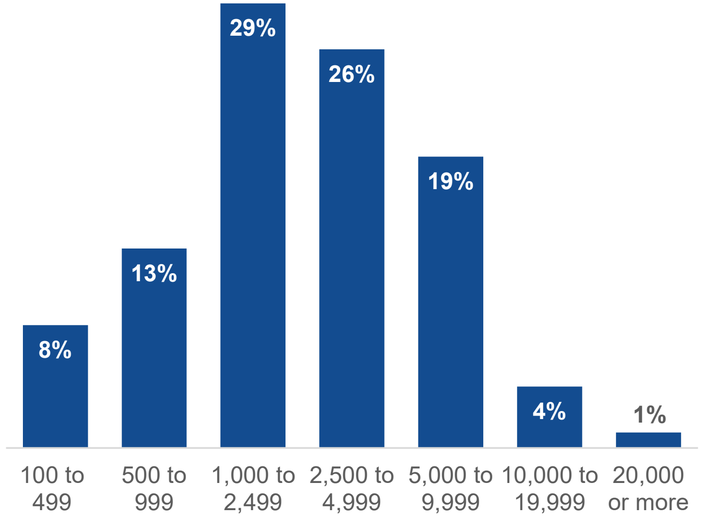
LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

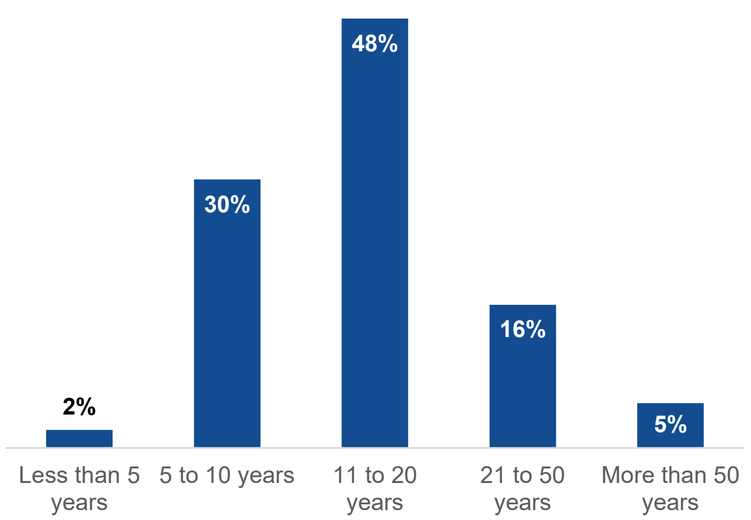
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America between December 11, 2024, and December 18, 2024. To qualify for this survey, respondents were required to be 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 373 IT, cybersecurity, and application development professionals.

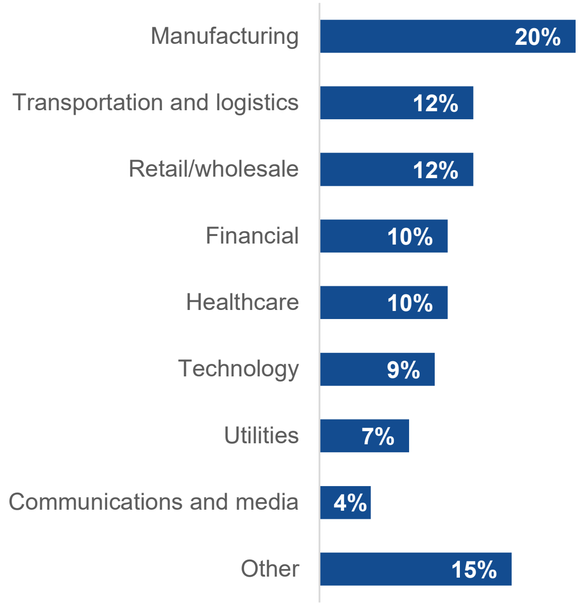
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



BACK TO CONTENTS

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.