ESG a division of TechTarget

Enterprise Strategy Group | Getting to the bigger truth.™

Closing the Cloud Security Readiness Gap

Gaining Consistency Across Disparate Environments

Doug Cahill, Vice President and Group Director

JUNE 2021

Google Cloud

GLOBAL

Partner of the Year

Security

2020

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.

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.

Back to Contents

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.

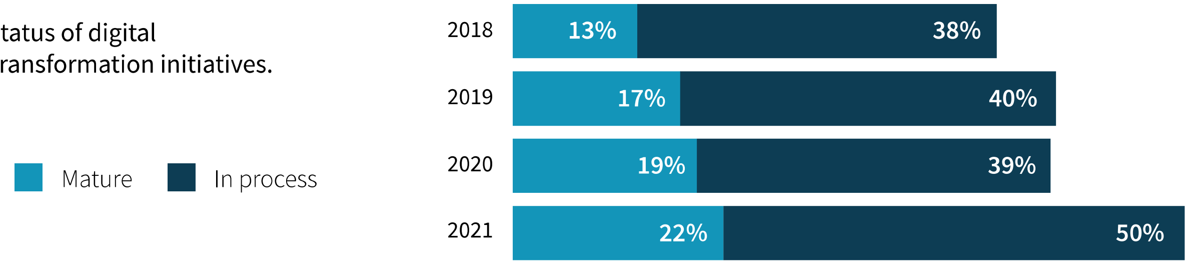
The Drivers of Cloud Adoption

Digital transformation is accelerating as organizations recognize increasing operational efficiency and shift to work-from-home strategies for the foreseeable future.

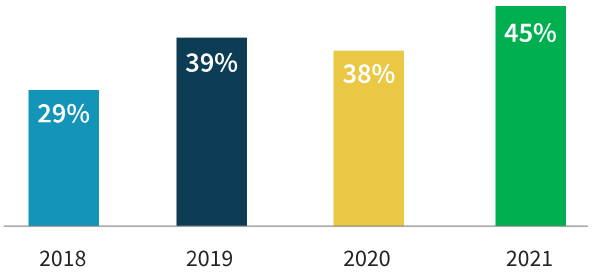
Digital transformation initiatives and cloud-first policies are on the rise

The need to digitally transform business operations is leading many organizations to adopt a cloud-first policy through which new IT initiatives are often expedited by the use of cloud applications and services. The need to support remote work has been another catalyst for the adoption of cloud applications and services.

Status of digital transformation initiatives.



Growth in cloud-first policies.



> “The need to digitally transform business operations is leading many organizations to adopt a cloud-first policy…”

Source: ESG Master Survey Results: *2021 Technology Spending Intentions Survey*, December 2020.

Back to Contents

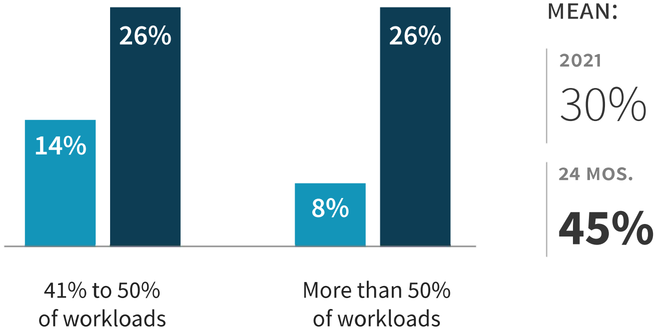
Production server workloads are shifting to public clouds

The increase in the use of cloud services is resulting in a notable increase in those organizations who are consuming infrastructure-as-a-service (IaaS) platforms. This expansion of IaaS usage includes an increase in the percentage of production server workloads being deployed in public cloud platforms.

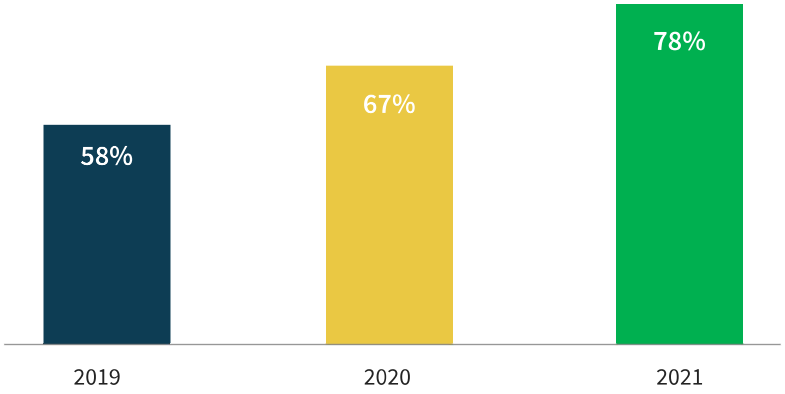
Production workloads deployed in a public cloud.

🟦 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)



Organizations using infrastructure-as-a-service (IaaS) platforms.



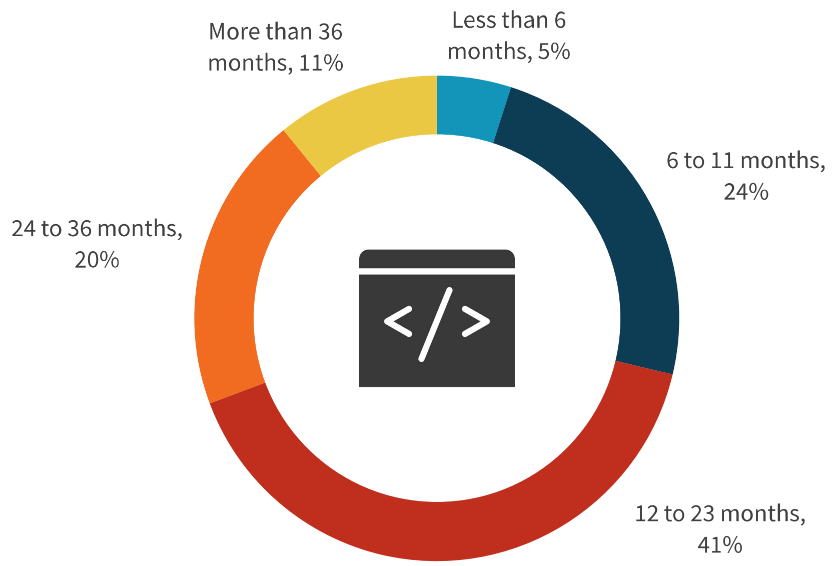
Source: ESG Master Survey Results: *2021 Technology Spending Intentions Survey*, December 2020.

Back to Contents

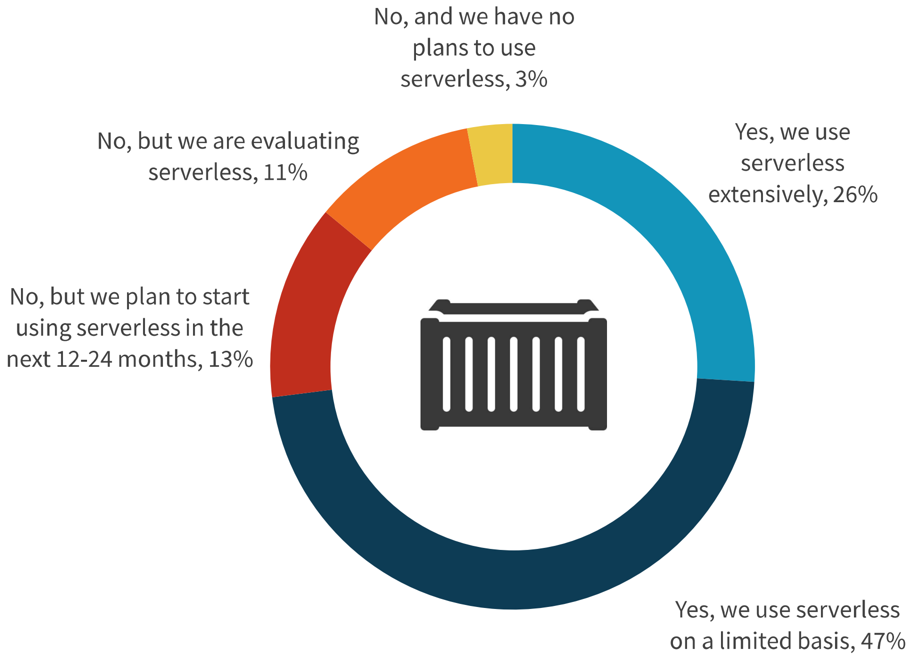
Containers, and now serverless functions, are underpinning microservices-based cloud-native applications

Container adoption has grown appreciably over the last two years, though serverless functions are currently 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.



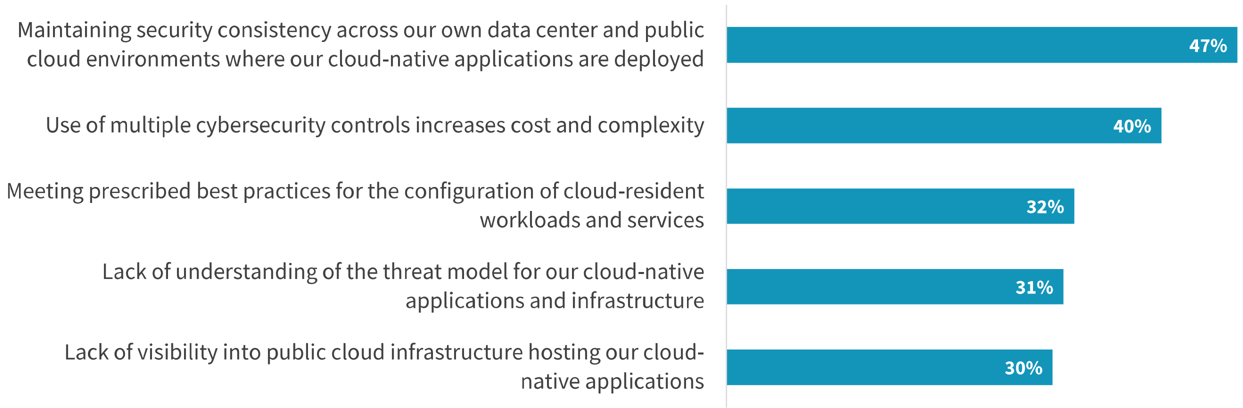
Adoption Ahead of Readiness

The rate at which organizations are expanding their use of cloud services has outpaced the maturity of cybersecurity programs, creating consistency and visibility challenges.

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.

Back to Contents

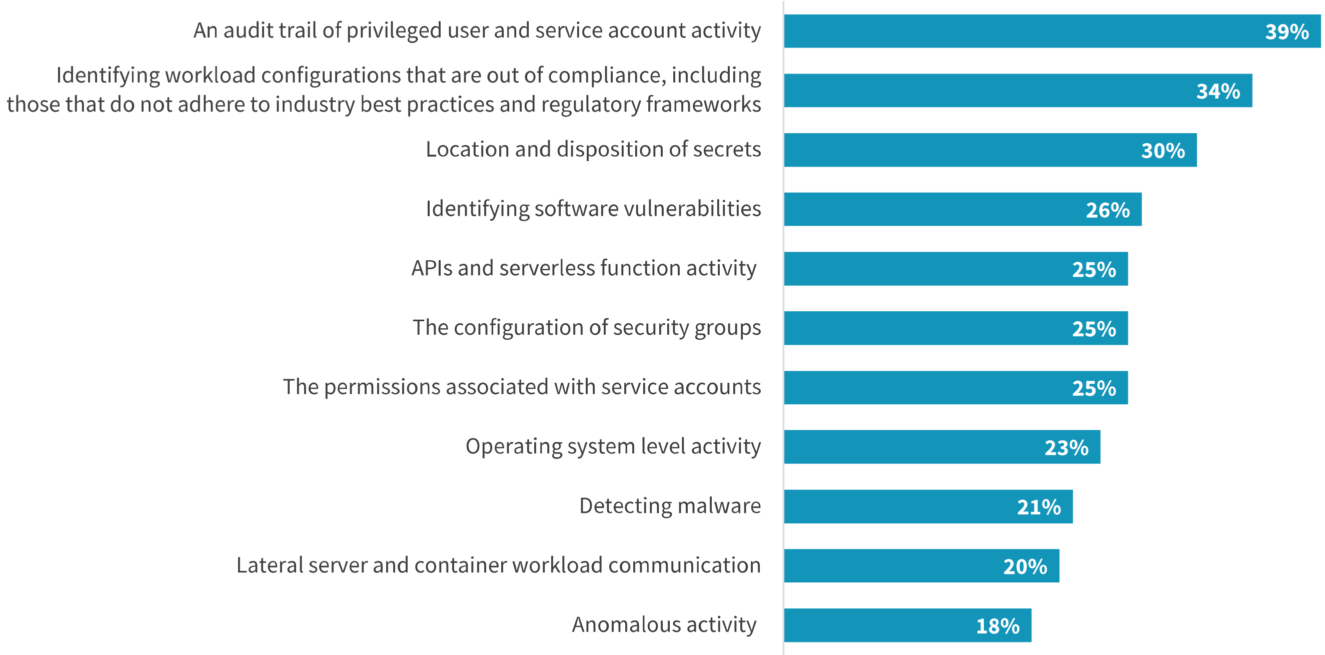
74%

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

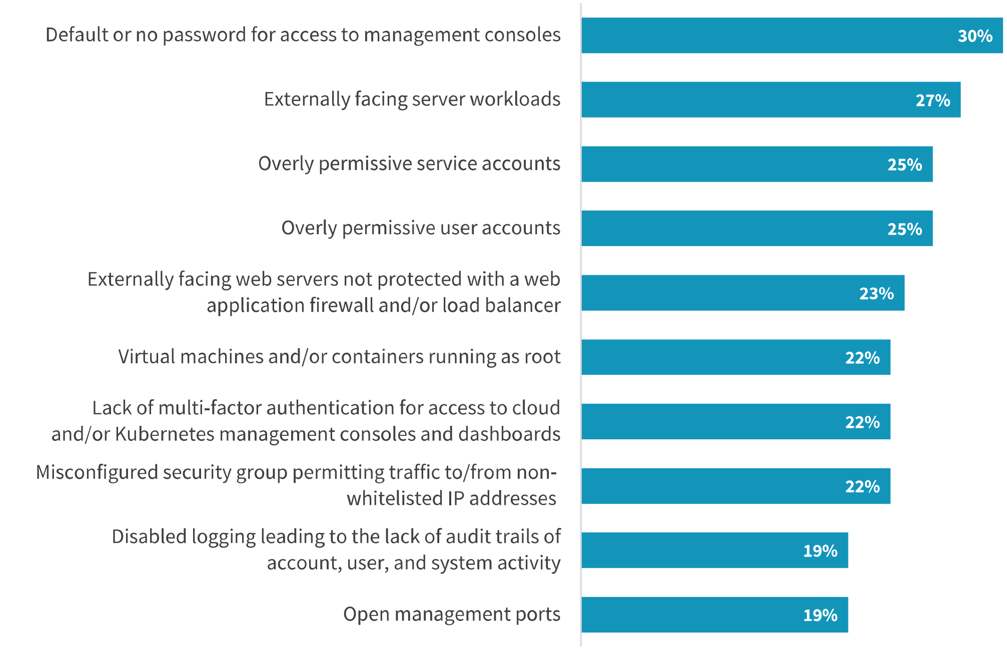
The Cloud Threat Landscape

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

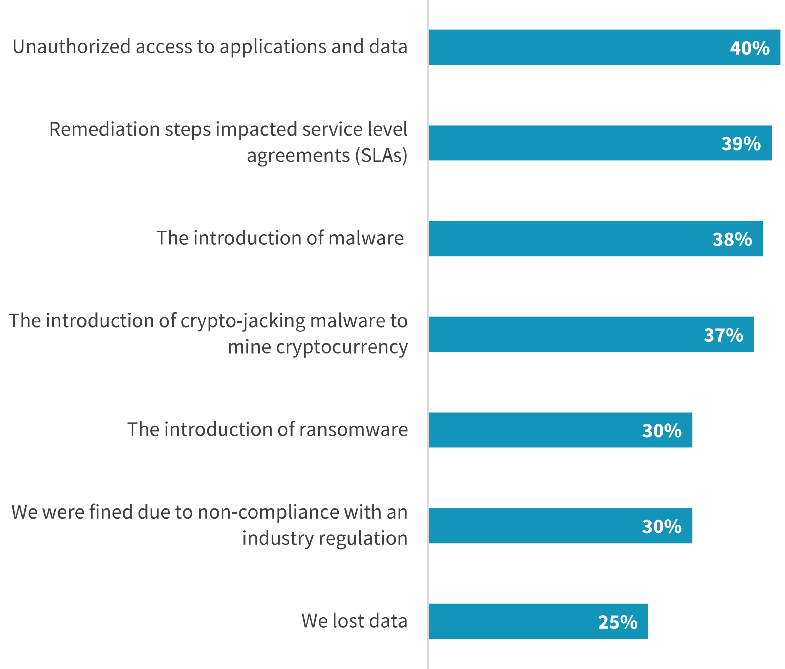
The frequency and ramifications of misconfigurations highlight the need for cloud security posture management

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 crypto 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.

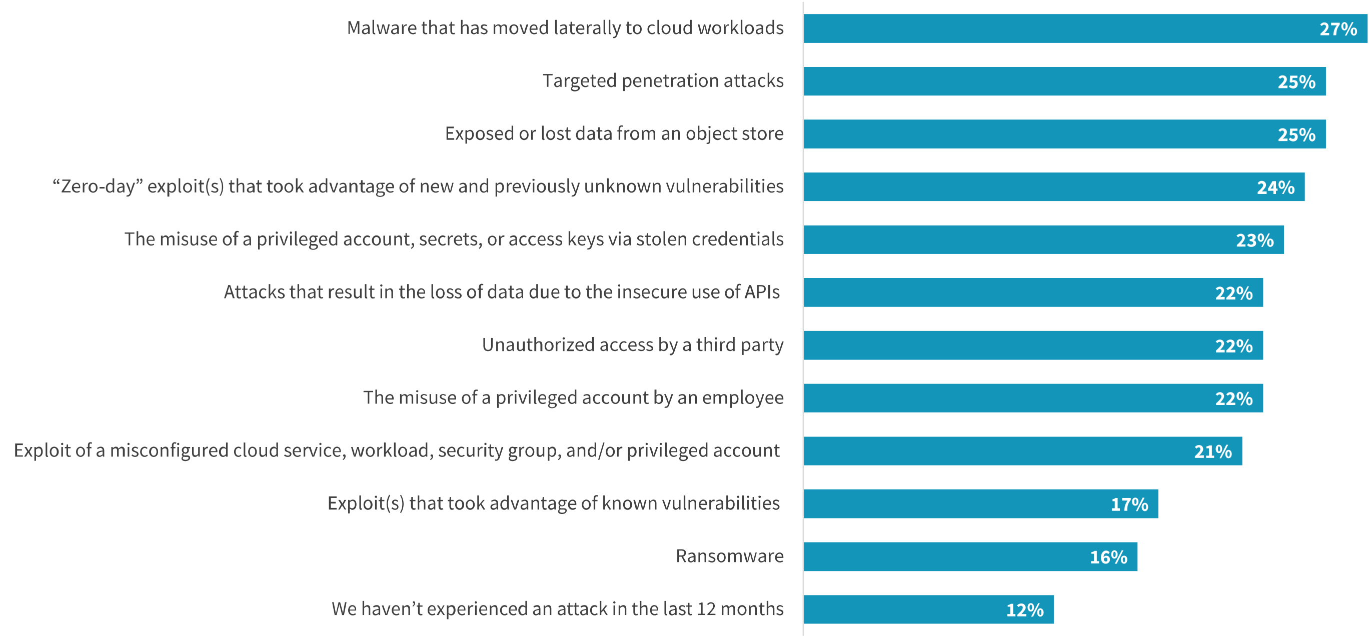


Back to Contents

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

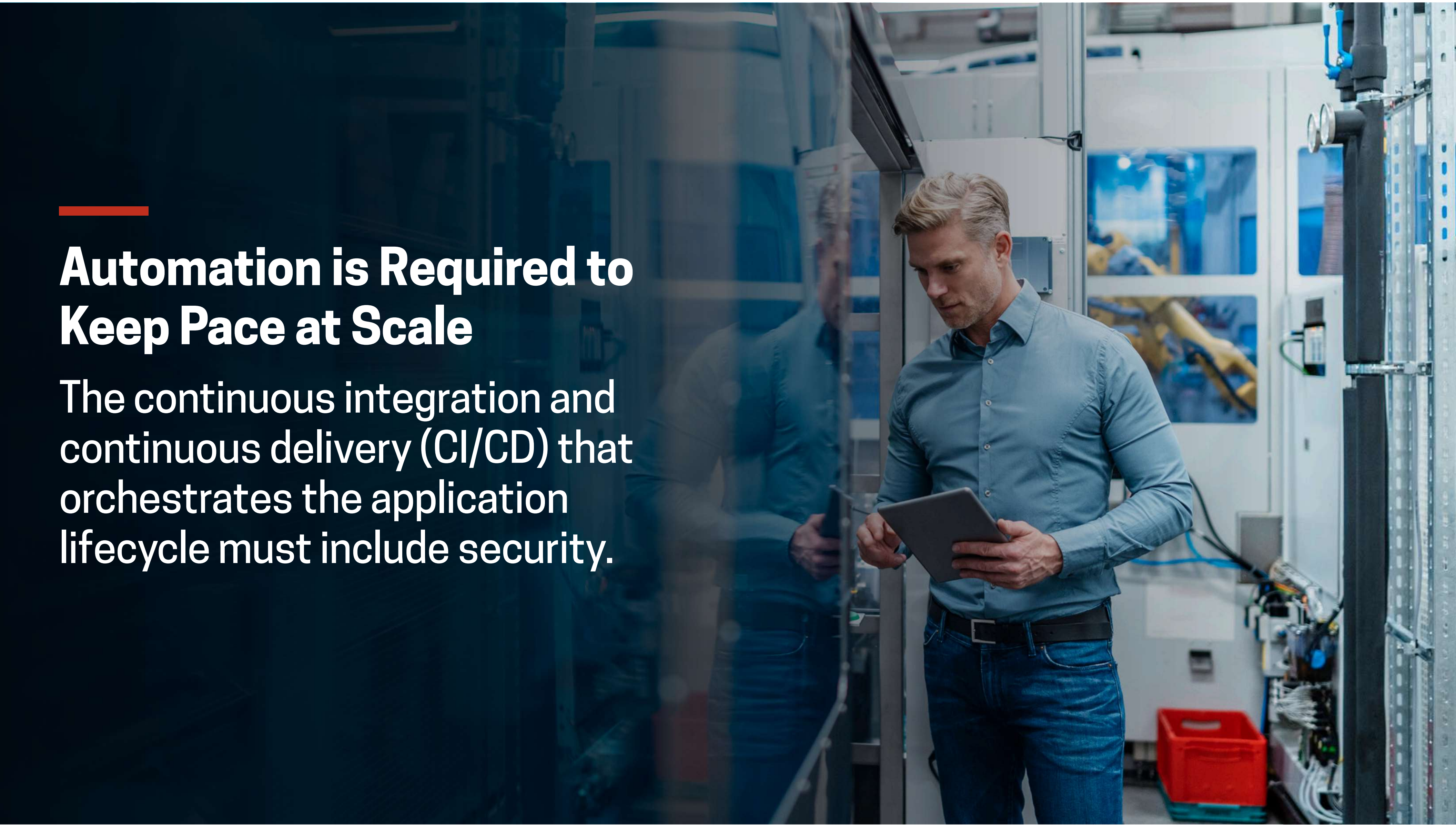
A variety of cyber attacks are often brought to bear against cloud-native applications and infrastructure. Indeed, only 12% of organizations reported not experiencing any cyber-incidents targeting their cloud-native apps or infrastructure over the past year. This highlights the need for an integrated 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.

Back to Contents



Automation is Required to Keep Pace at Scale

The continuous integration and continuous delivery (CI/CD) that orchestrates the application lifecycle must include security.

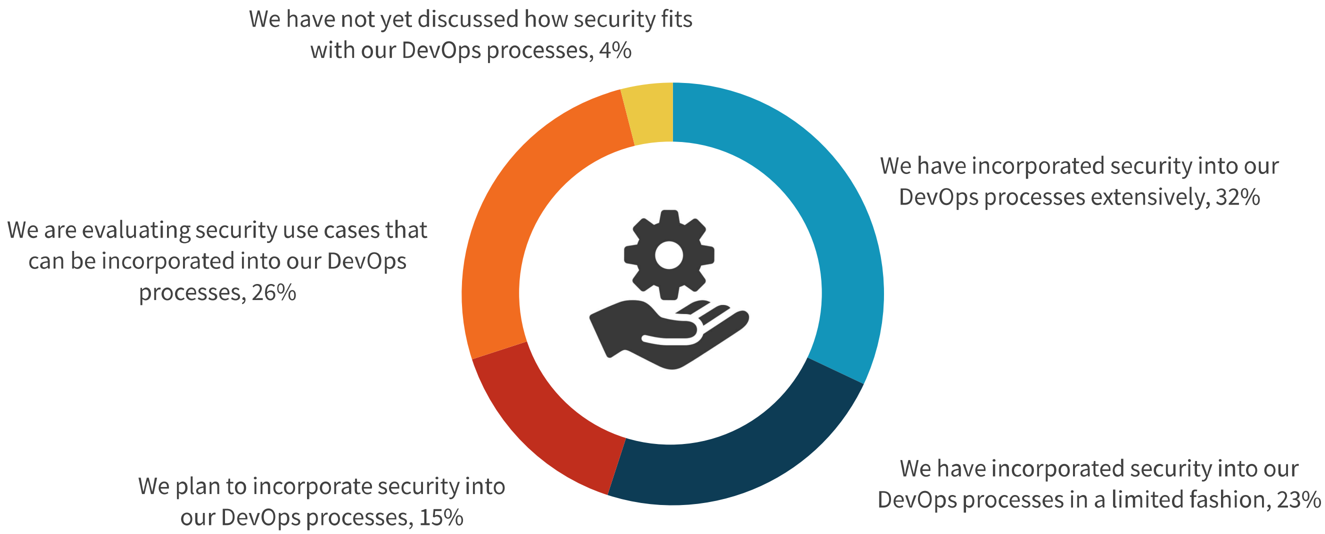
41%

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

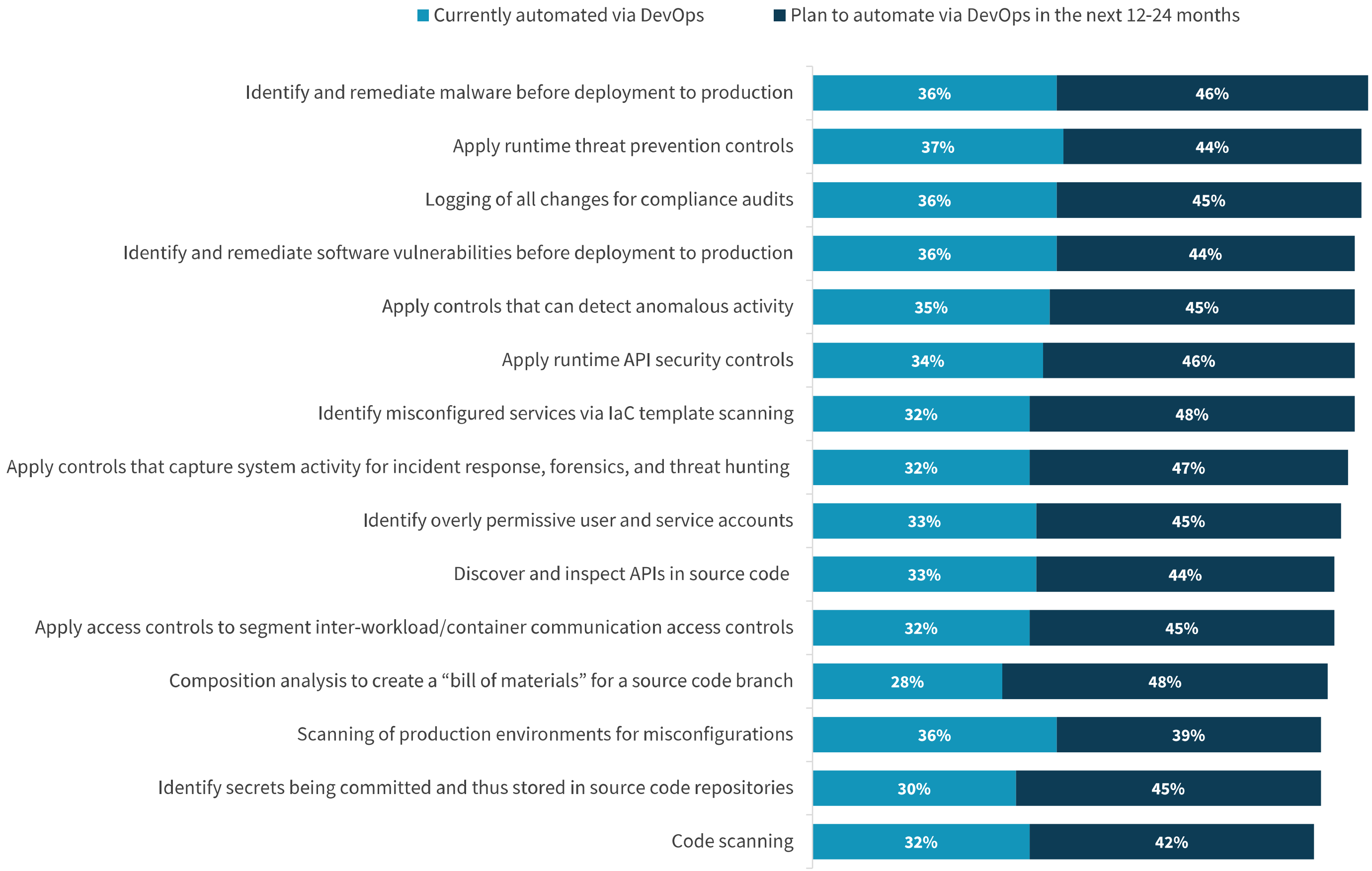
The need to keep pace with the elastic, dynamic nature of cloud-native applications and infrastructure makes automation a strategic tenet of cloud security programs. As a result, the ability to integrate cloud-native security controls into the tools that manage the software development lifecycle (SDLC), 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

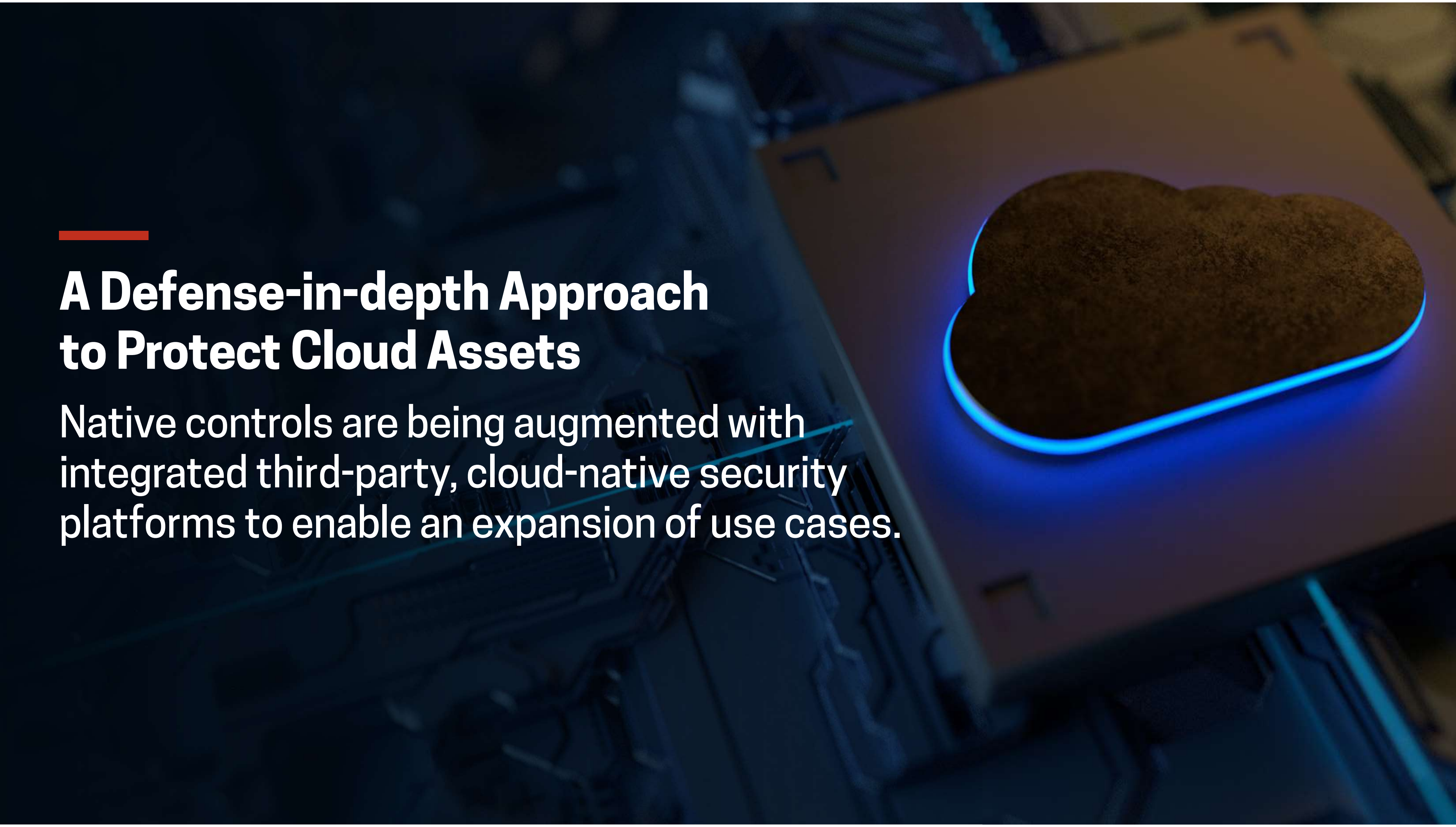
Current and planned secure DevOps use cases are being implemented across the application lifecycle, from the development stage to build and integration into delivery and production, which will result in an increase in those production cloud-native applications being protected via DevSecOps practices. 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

MEAN:

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

Back to Contents



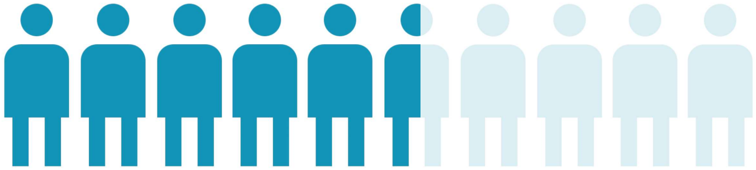
A Defense-in-depth Approach to Protect Cloud Assets

Native controls are being augmented with integrated third-party, cloud-native security platforms to enable an expansion of use cases.

The need for consistency is driving the consolidation of controls

The strategic imperative to unify security policies across disparate environments is driving the need to leverage both native controls and integrated cloud-native application protection platforms (CNAPP). The shift to controls based on an integrated platform will allow project teams to address the cost and complexity associated with using separate controls for separate environments.

Current types of controls used to secure cloud-native applications.



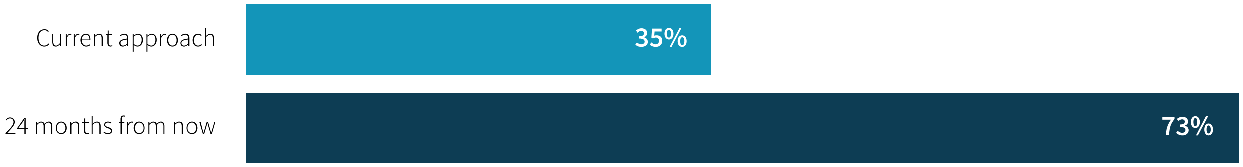
57%

use a combination of third-party security controls and those that are native to the cloud service provider's platform.

MAY 2019: 38%

Preferred types of controls to secure.

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



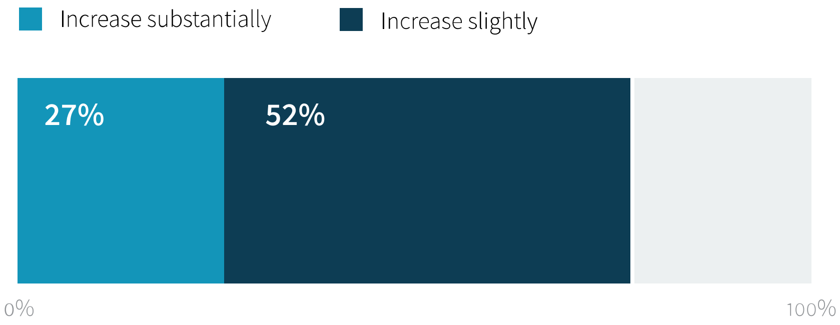
Back to Contents

Investments to close cloud security readiness gap

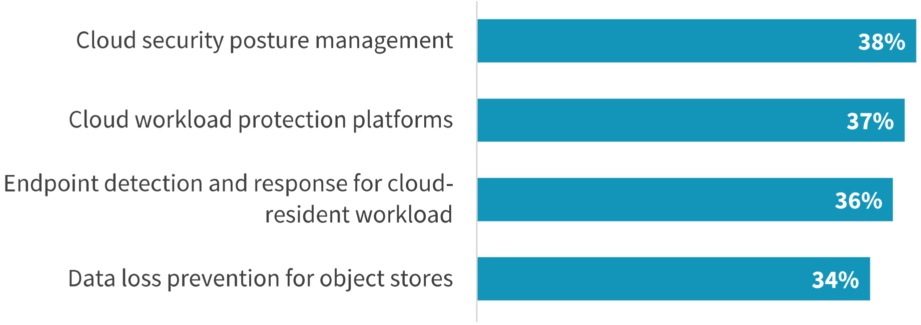
Organizations are planning appreciable investments in cloud security to fund incremental purchasing of core modules on a cloud-native application platform (CNAPP), including cloud security posture management (CSPM) and cloud workload protection (CWP) controls. These investments will enable an expansion of cloud security controls, including microsegmentation and endpoint detection and response (EDR), to enable the SOC to gain greater visibility into cloud-native apps and infrastructure.

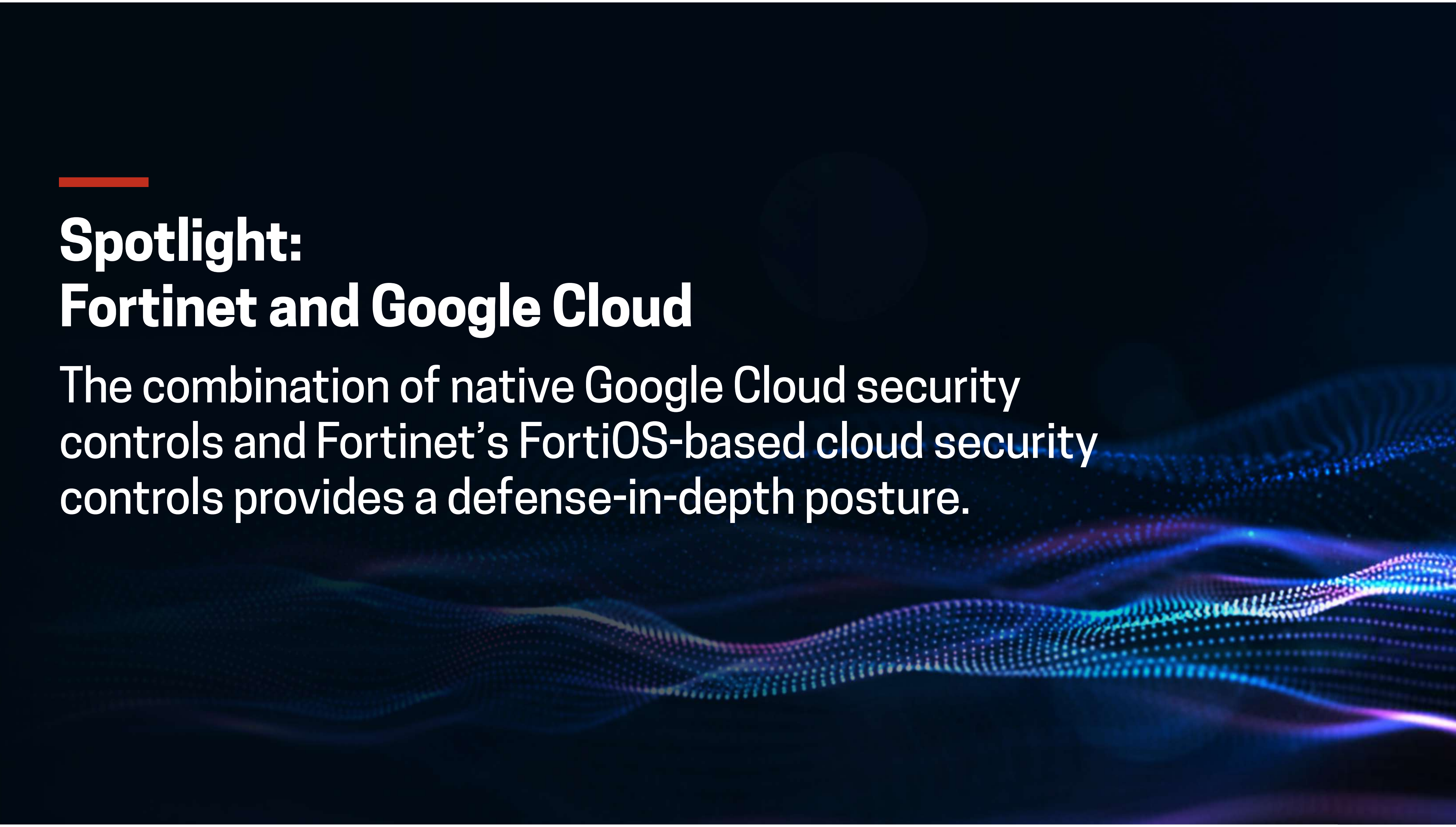
> ***"These investments will enable an expansion of cloud security controls..."***

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



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





Spotlight:
Fortinet and Google Cloud

The combination of native Google Cloud security controls and Fortinet’s FortiOS-based cloud security controls provides a defense-in-depth posture.

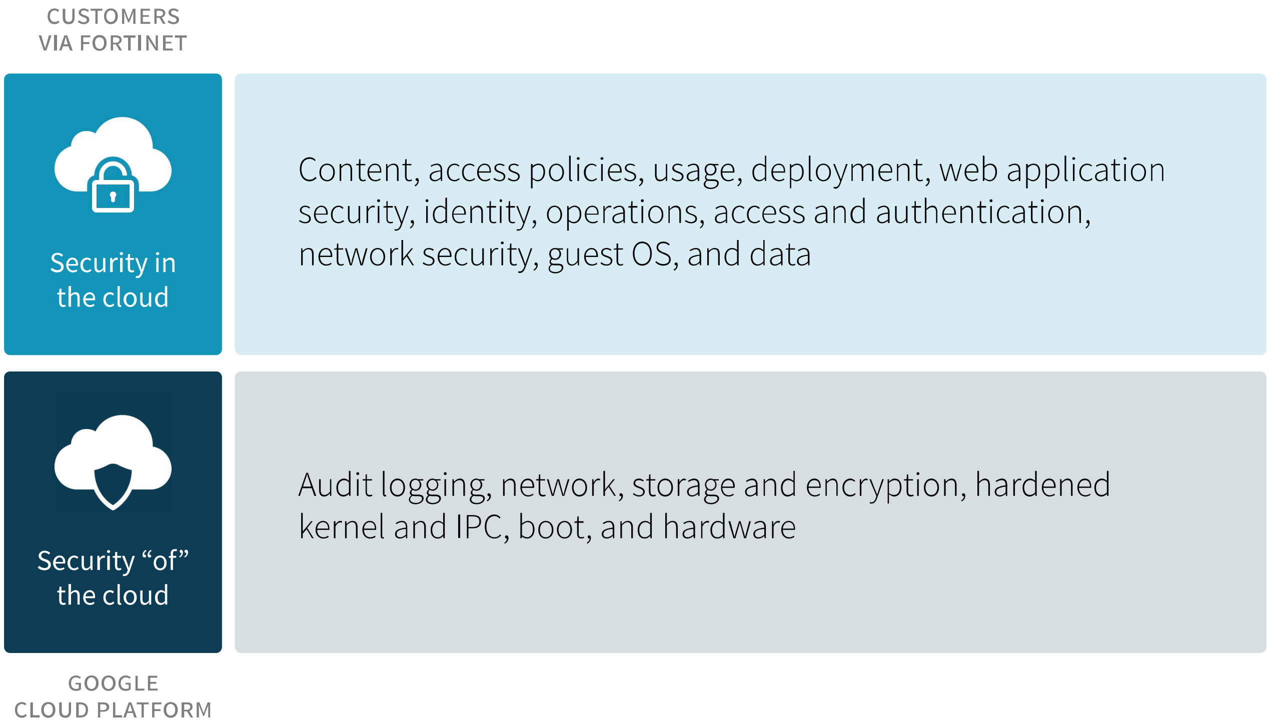
“Better Together” Entails Shared Responsibility

With Fortinet and Google, organizations can achieve a robust defense-in-depth posture when running workloads on Google Cloud.

Using security controls supplied by Fortinet and Google simultaneously reduces risk of overlooking potential security gaps.

Through Google’s Risk Reduction Program, customers can obtain cybersecurity insurance via Google’s partnerships with Allianz Global Corporate and Specialty (AGCS) and Munich Re.

Benefits not only include reduced risk but also potentially reduced costs with specialized cyber coverage.



CUSTOMERS VIA FORTINET

Security in the cloud

Content, access policies, usage, deployment, web application security, identity, operations, access and authentication, network security, guest OS, and data

Security “of” the cloud

Audit logging, network, storage and encryption, hardened kernel and IPC, boot, and hardware

GOOGLE CLOUD PLATFORM

Back to Contents

Fortinet Security Fabric

- The platform is designed to unify security technologies into a single system for providing defense-in-depth across on-premises and Google Cloud deployments.
- Consulting partners can help customers to develop a highly differentiable security practice to fill any combination of gaps in a customer's security posture.

Fortinet Partner Network

- Network of vetted distributors and resellers committed to providing world-class products, services, and technical support to Fortinet customers.
- Trained on the latest in Fortinet security offerings.
- Employing on-site Network Security Expert (NSE) Level 4 engineers for ensuring security in Google Cloud.

FORTINET®

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.

LEARN MORE

ABOUT ESG

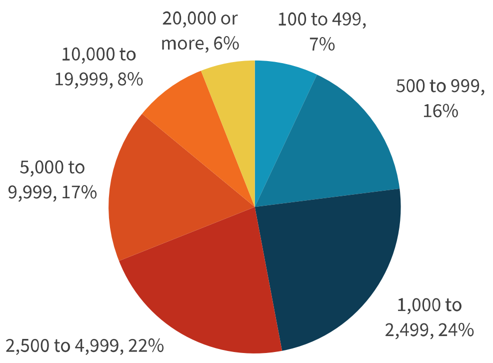
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology

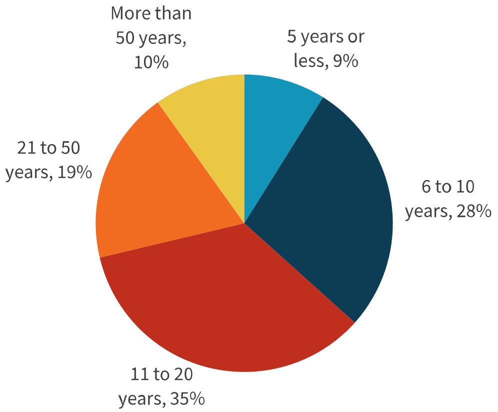
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between December 7, 2020 and December 26, 2020. To qualify for this survey, respondents were required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

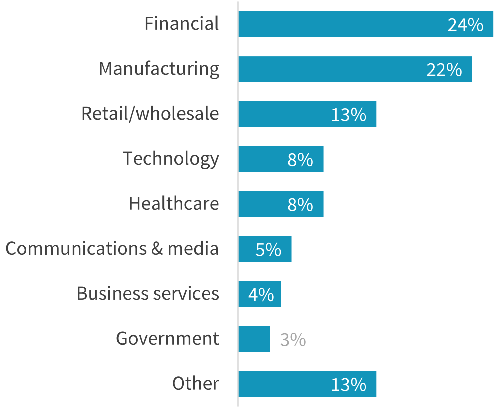
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



Back to Contents

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.

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.