Enterprise Strategy Group | Getting to the bigger truth.™

Automate the Protection of Cloud-native Workloads Against Dynamic Attacks

Enabling Agility of Workloads in Legacy and Modern Environments

Melinda Marks, Senior Analyst

JUNE 2022

CONTENTS

Introduction

Organizations are moving workloads and applications to the cloud for faster product delivery and innovation. They can use state-of-the-art technologies from cloud service providers (CSPs) without having to worry about setting up or maintaining hardware or underlying infrastructure. This frees them up to modernize software development processes leveraging microservices architectures.

But what does this mean for security? As we gain speed and flexibility, security is more important than ever. As organizations deliver services and applications through the cloud, it's important to protect them across environments—whether they are on-premises, in the cloud, or in hybrid environments. With the speed of cloud deployments, security teams need a centralized way to automate security and workload protection. This is the only way to scale security for cloud-native environments, especially as threats are rapidly evolving, creating an ever-increasing attack surface for attackers to target.

A unified approach is needed to realize the business benefits of speed and agility while protecting applications and resources across cloud environments. In this eBook, we'll explore the move to the cloud, the security challenges that organizations are facing, and how to best protect workloads from rapidly evolving threats.

Back to Contents

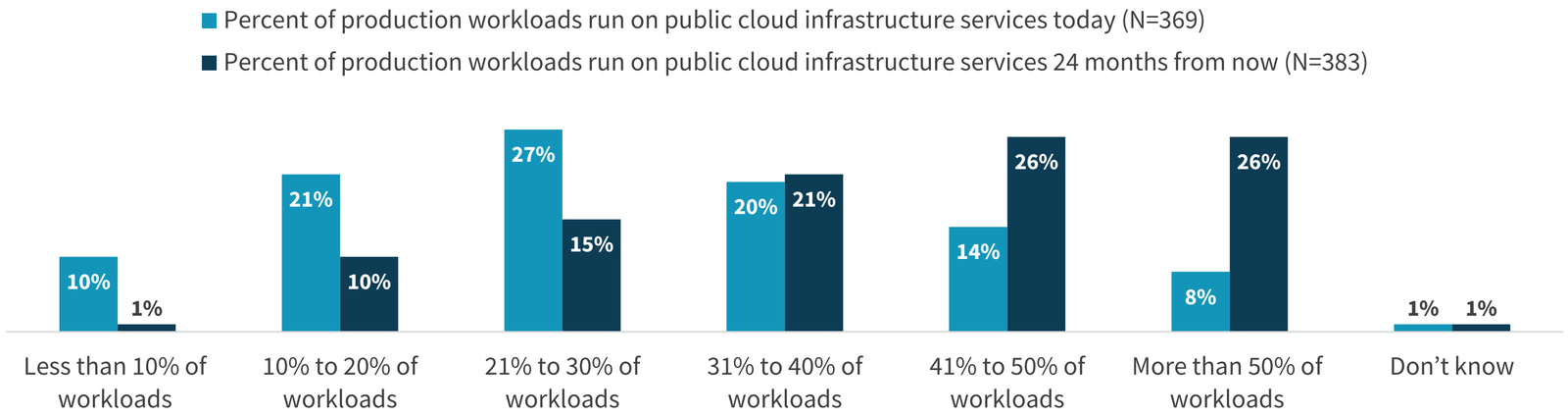
Moving Workloads to the Cloud

Organizations today realize the competitive advantage they can gain by leveraging cloud services.

Utilizing the cloud provider's state-of-the-art technology and services enables them to provision infrastructure and develop applications faster, without having to worry about the underlying infrastructure or maintenance. Cloud services also offer economies of scale, with pay-as-you-go models.

But this means a dynamic and changing attack surface that legacy security solutions cannot address. It requires a new approach that can secure the workloads in cloud environments.

Percentage of production server workloads run on public cloud infrastructure services today and 24 months from now.



48%

of organizations reported having a cloud-first policy.

43%

Consider cloud and on-premises approaches equally.

Back to Contents

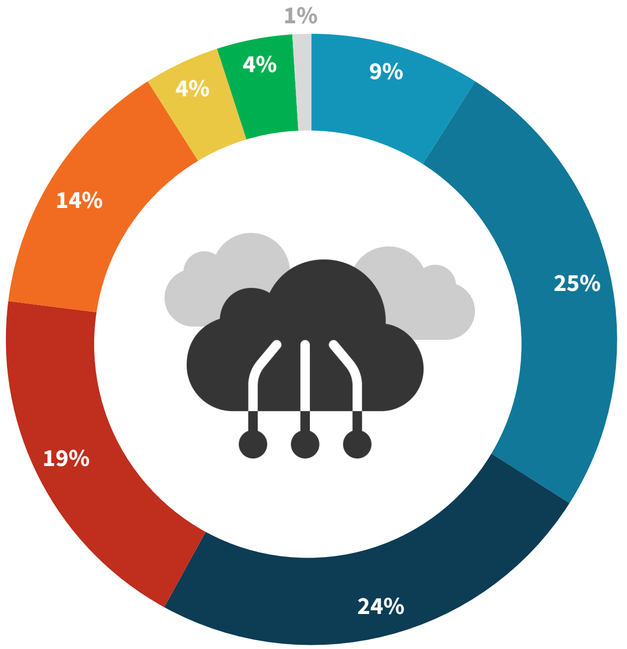
Leveraging Hybrid and Multi-cloud Environments

Organizations are most often leveraging infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) services from multiple CSPs.

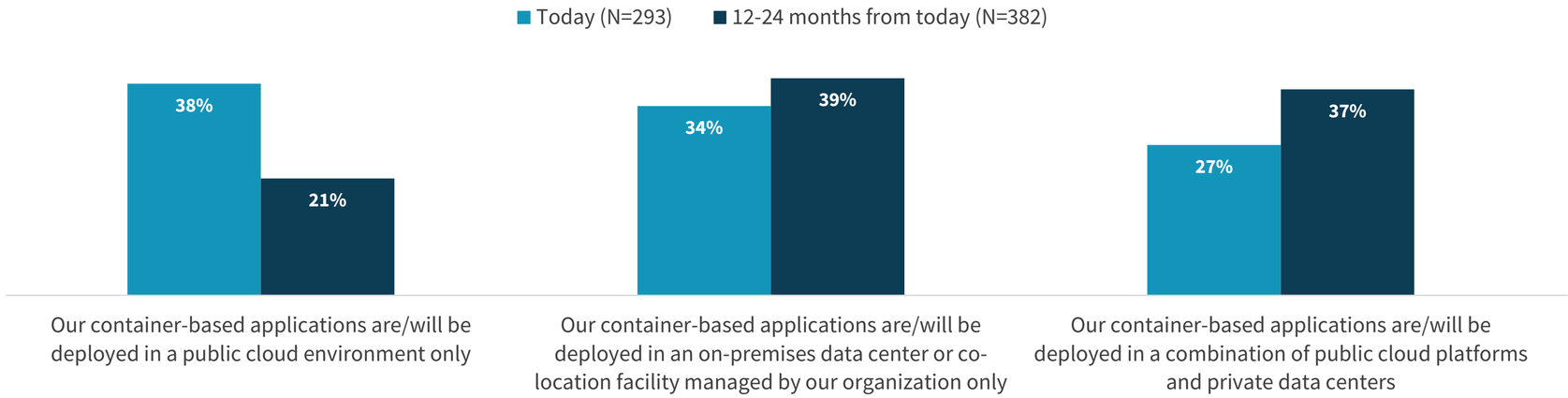
Factors such as the portability of modern software components, like containers, give developers the flexibility to utilize a variety of environments, including public clouds, private clouds, and hybrid environments.

This gives organizations the flexibility to put their applications in the environments that best accommodate their requirements, including service level agreements (SLAs) for performance and availability, storage services, ability to scale, cost of services, and other considerations.

Most organizations use multiple CSPs.



Container portability provides deployment flexibility.



Back to Contents

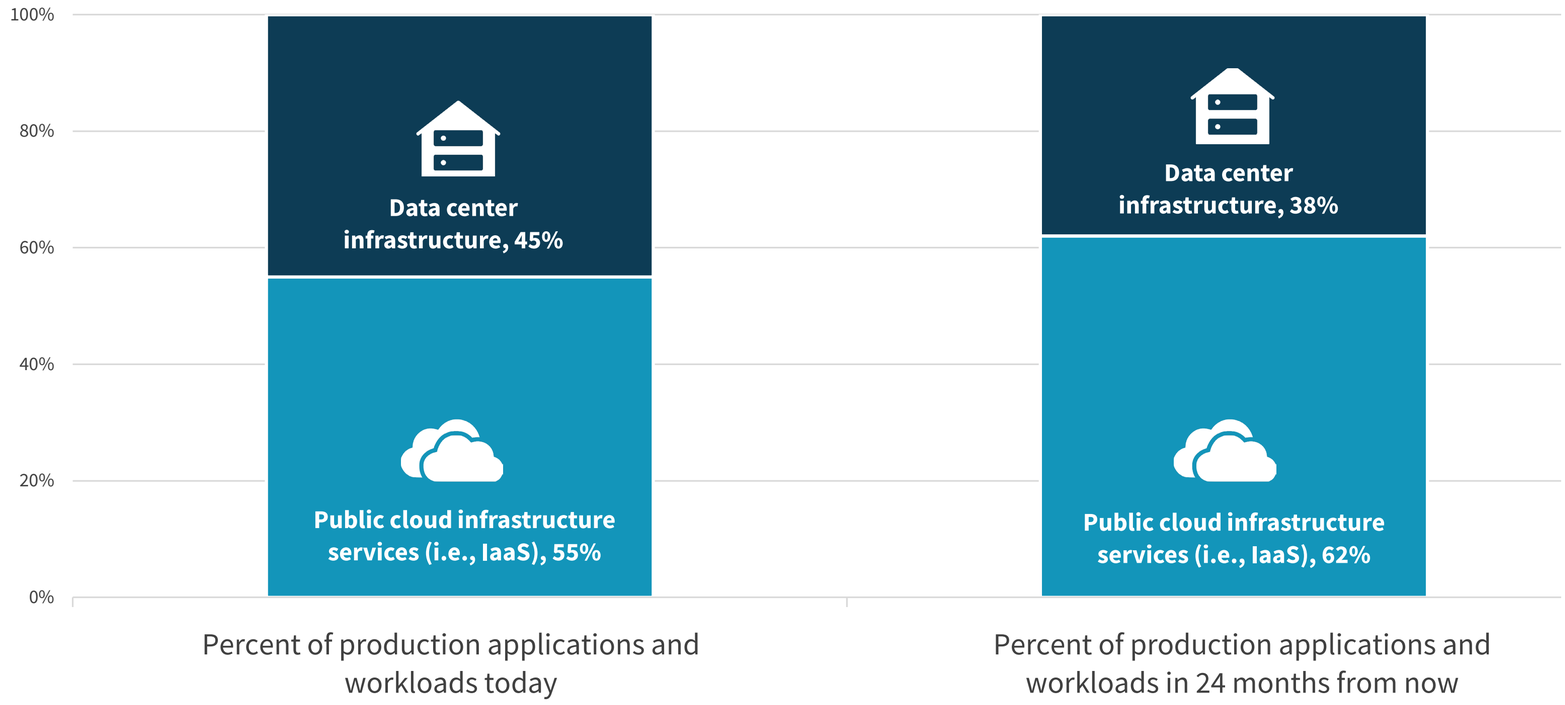
On-premises Applications Are Not Going Away

While organizations are increasingly leveraging cloud services to take advantage of modern software development practices, our research showed that they are still hosting applications in on-premises data centers.

So, security is tasked with managing security and compliance in ways that support and enable the business to host their workloads in multi-cloud and hybrid environments.

> “Our research showed organizations **are still hosting applications in on-premises data centers.**”

Breakdown of locations in which organizations’ applications and workloads run today and in 24 months.



Back to Contents

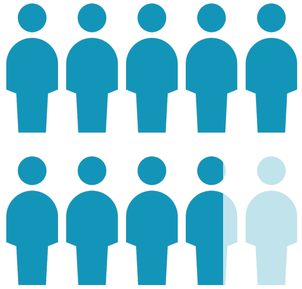
Challenges Managing Security Risk

With hybrid, multi-cloud environments now the norm, security is much more complex compared to the traditional security approach of perimeter protection.

This is due to:

- Dynamic and ephemeral infrastructure and resources being spun up and spun down with exposure through the internet.
- The scale of product releases and development teams.
- The lack of visibility to detect and block attacks on cloud-native applications.

Organizations now need workload-based protection that can be consistently applied across environments.



88%

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

87%

of respondents agree the differences between cloud-native applications and the rest of their apps and infrastructure require a different set of security policies and technologies.

88%

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

73%

of respondents agree 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.

62%

of respondents agree they lack cybersecurity personnel to sufficiently support all their DevOps and project teams.

Back to Contents

The Need for Better Protection of Workloads

Hosting workloads in the cloud helps companies serve more customers, but it also widens their exposure to threats.

Organizations report that they face many challenges protecting their workloads due to:

- The increase in the threat landscape.
- Lack of IaaS security skills.
- Difficulty responding to incidents and breaches.

Organizations' greatest public cloud infrastructure security challenges.

52%

An increase in the threat landscape

39%

An increase in the amount of IaaS usage at our organization

30%

My organization lacks the right level of IaaS security skills

28%

My organization lacks the right level of IaaS security staff

28%

Difficulty responding to security incidents and breaches

27%

Difficulty remaining compliant efficiently

23%

Ineffective security tools

21%

Insufficient budget

Back to Contents

The Added Complexity of Security Across Hybrid Environments

Gaining the visibility and control security teams need to manage modern software development processes proves challenging. Instead of dealing with monolithic applications, the dynamic microservices architectures are more difficult to protect without an understanding of the applications, their communications with resources, and their dependencies.

Security teams face multiple challenges, including:

- Managing configurations.
- Ensuring consistency of policies.
- Incorporating security and networking configuration best practices.

Ten biggest challenges for managing security across hybrid environments.

30%

Challenges ensuring/ maintaining proper configuration of cloud services

24%

Meeting and maintaining compliance with industry regulations across disparate cloud environments

24%

Lack of consistent security policies across different application architectures

21%

Incorporating security and networking configuration best practices into DevOps processes

20%

Lack of consistent security policies across the different parts of our environment

20%

Understanding the cloud security shared responsibility model

20%

Lack of visibility across the different parts of our environment

20%

Increasing total cost of ownership

18%

Increasing vendor management/complexity

14%

Inconsistent operational models across locations/ clouds

Back to Contents

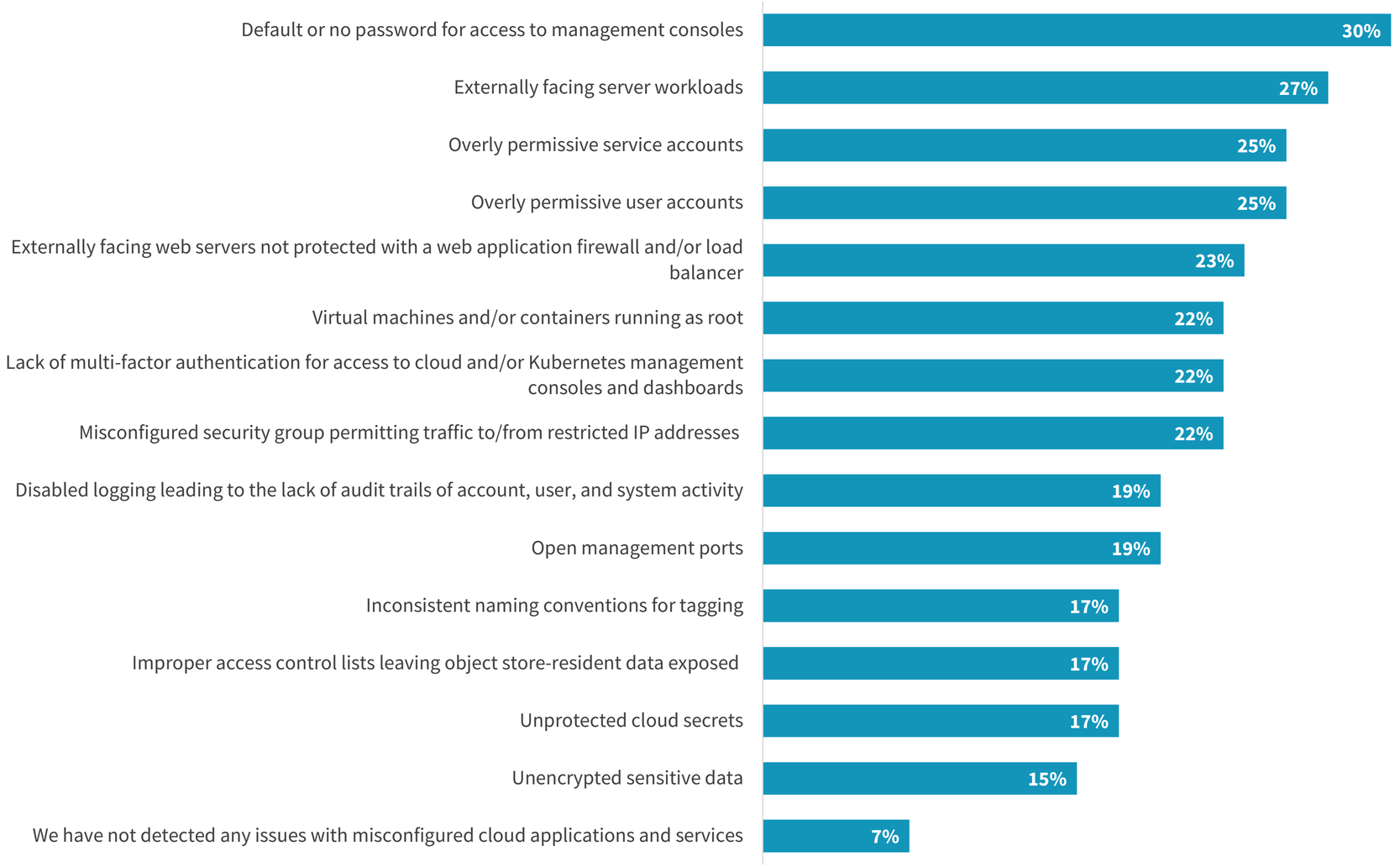
The Need for Consistent Policies and Controls

As development teams grow and scale with rapid product releases, it is difficult to ensure secure development processes are in place, and there is a higher chance for mistakes and misconfigurations.

ESG research shows a range of misconfigurations detected, from access-related issues, to externally facing workloads subject to port scanning, to open ports, to open secrets.

Organizations are looking for ways to reduce the risk from misconfigurations that should be preventable with the right controls in place.

Issues associated with misconfiguration of cloud applications or services detected by organizations in the last 12 months.



Back to Contents

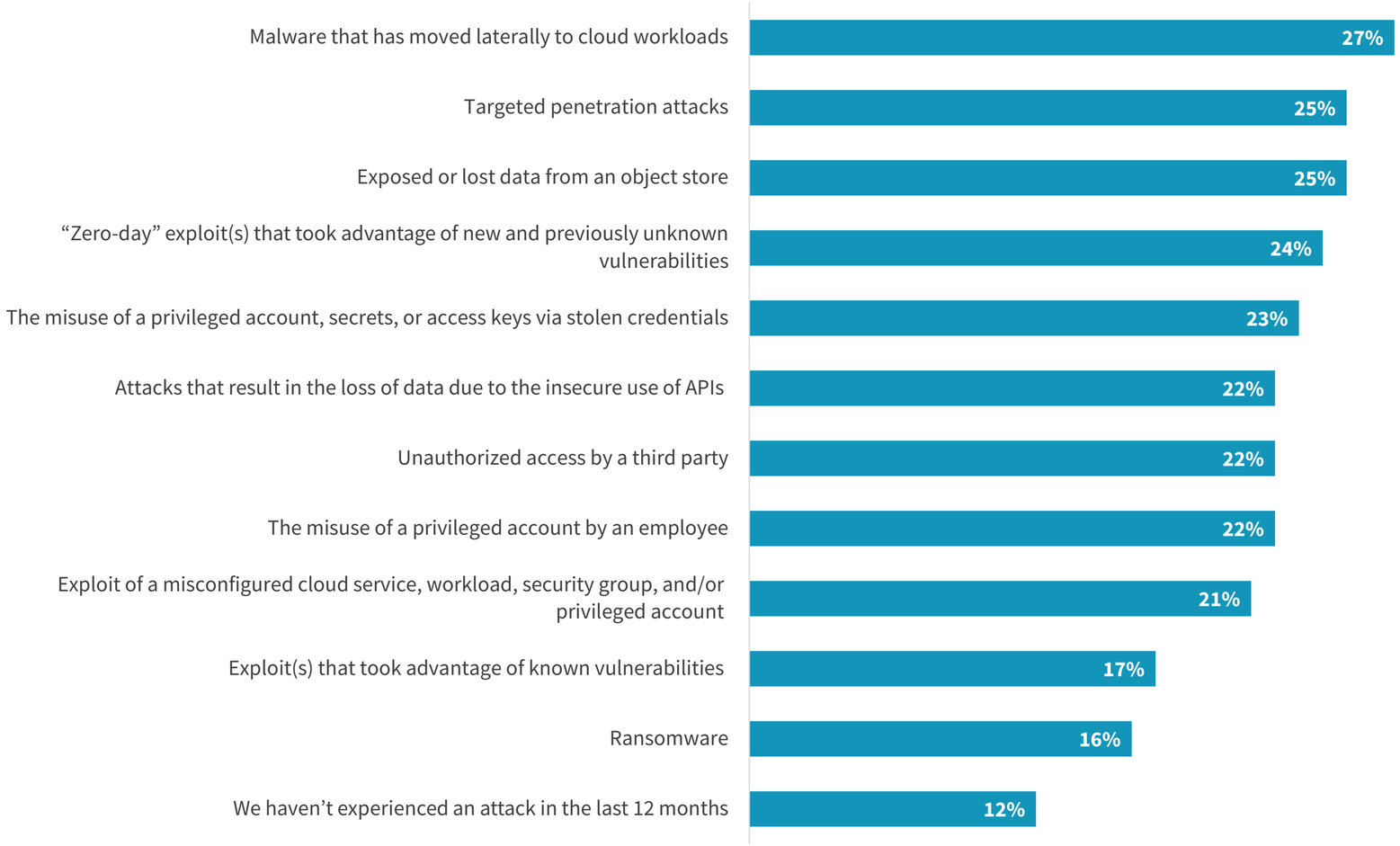
The Cloud-native Threat Landscape

Organizations have faced a wide range of attacks on their cloud-native applications, making it clear that they need to take steps to reduce their security risk. With so many attacks leveraging configuration- and access- related issues, as well as exploiting known vulnerabilities, organizations need a better approach to managing security risk.

88%

of organizations experienced cyber-attacks on their cloud-native applications and infrastructure in the past year.

Cybersecurity incidents related to cloud-native applications and infrastructure experienced in the last 12 months.



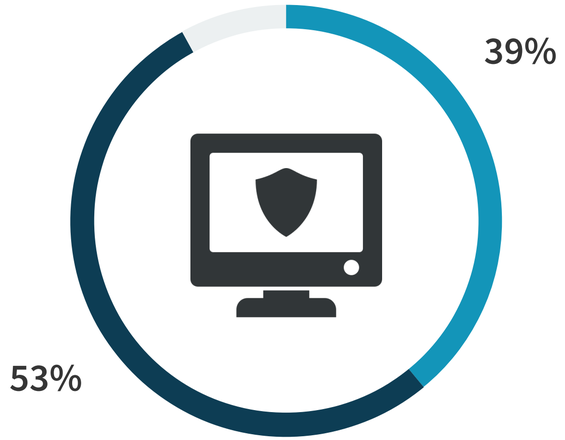
Back to Contents

Protecting Workloads Across Environments

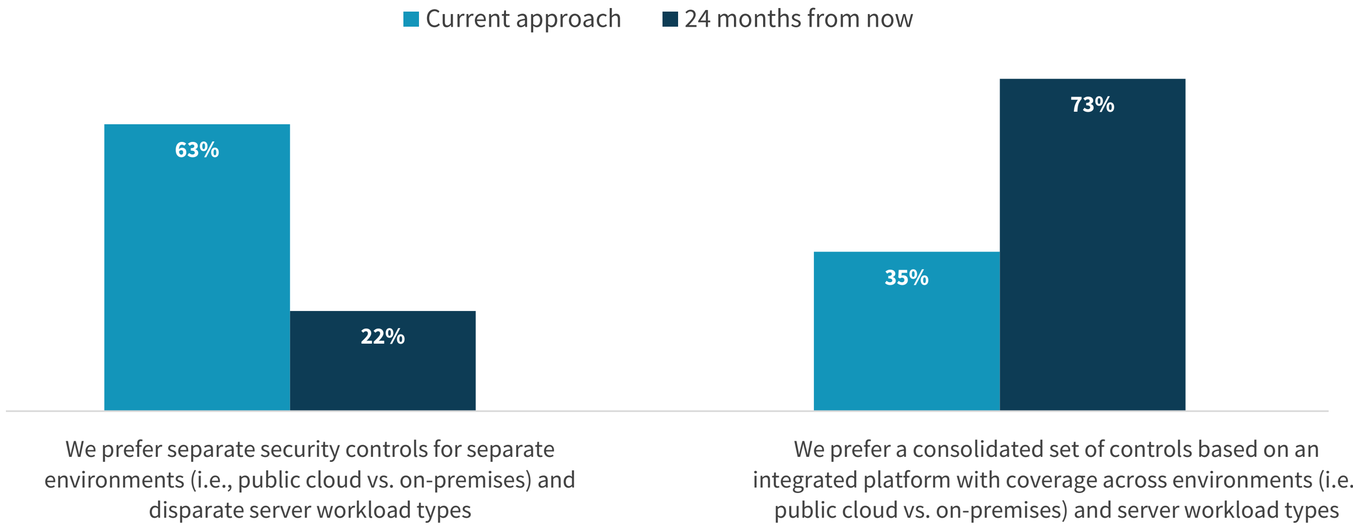
Organizations want an approach that gives them centralized visibility and control in order to scale security to protect the applications and data across environments.

They need a unified, easy-to-manage solution to consistently apply the policies, technologies, and controls they need to reduce risk across their cloud workloads as development scales.

Stages of procuring and deploying an integrated platform.



Security control preference for protecting cloud-native applications and infrastructure



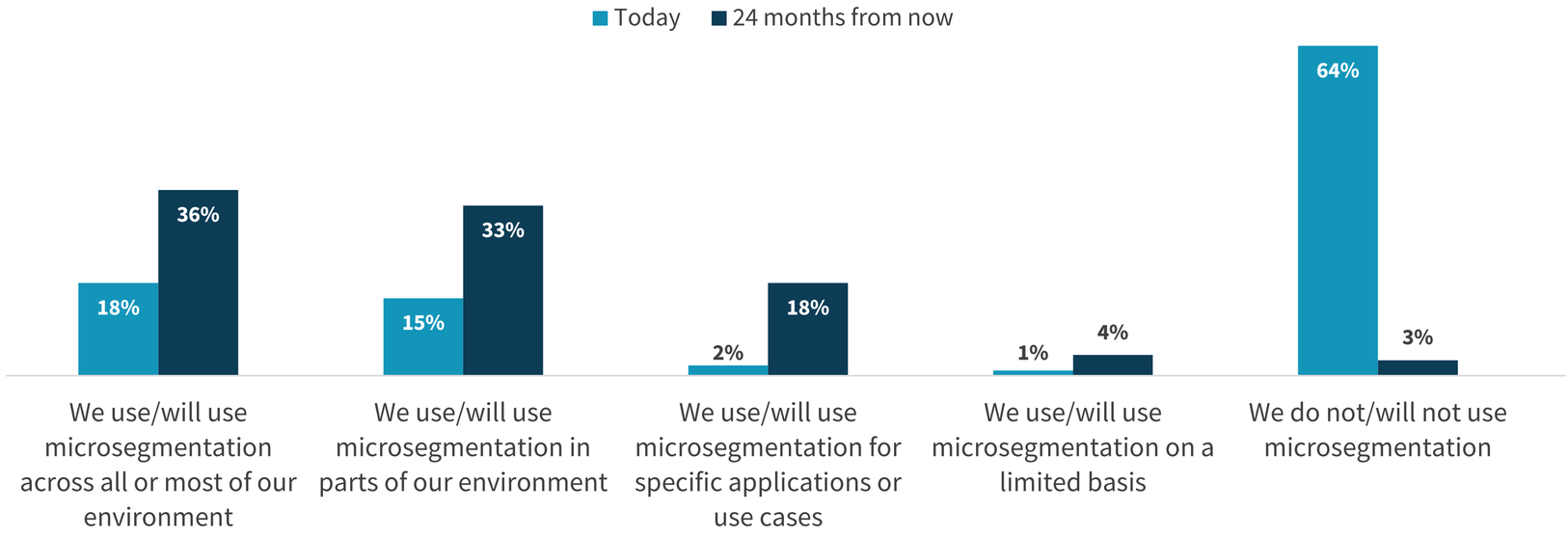
Back to Contents

Microsegmentation Is Becoming Critical to Stop or Contain Incidents

Organizations realize the need to protect workloads from threats and typically look at ways to isolate them by segmentation. But network segmentation is limited with coarse-grained segmentation via access control lists and virtual LANs. While our research shows that organizations find that microsegmentation is useful in cases, such as securing traffic between public infrastructure and on-premises data centers or remote sites, organizations need microsegmentation to provide more granular controls needed for dynamic cloud environments with changing attack surfaces. This helps organizations quickly act to isolate and protect workloads. While microsegmentation usage is limited today, most organizations have come to realize its importance and are planning to implement it in the next 24 months.

> “Most organizations have come to realize microsegmentation’s importance **and are planning to implement it in the next 24 months.”**

Organizations’ usage of and plans for microsegmentation.



Back to Contents

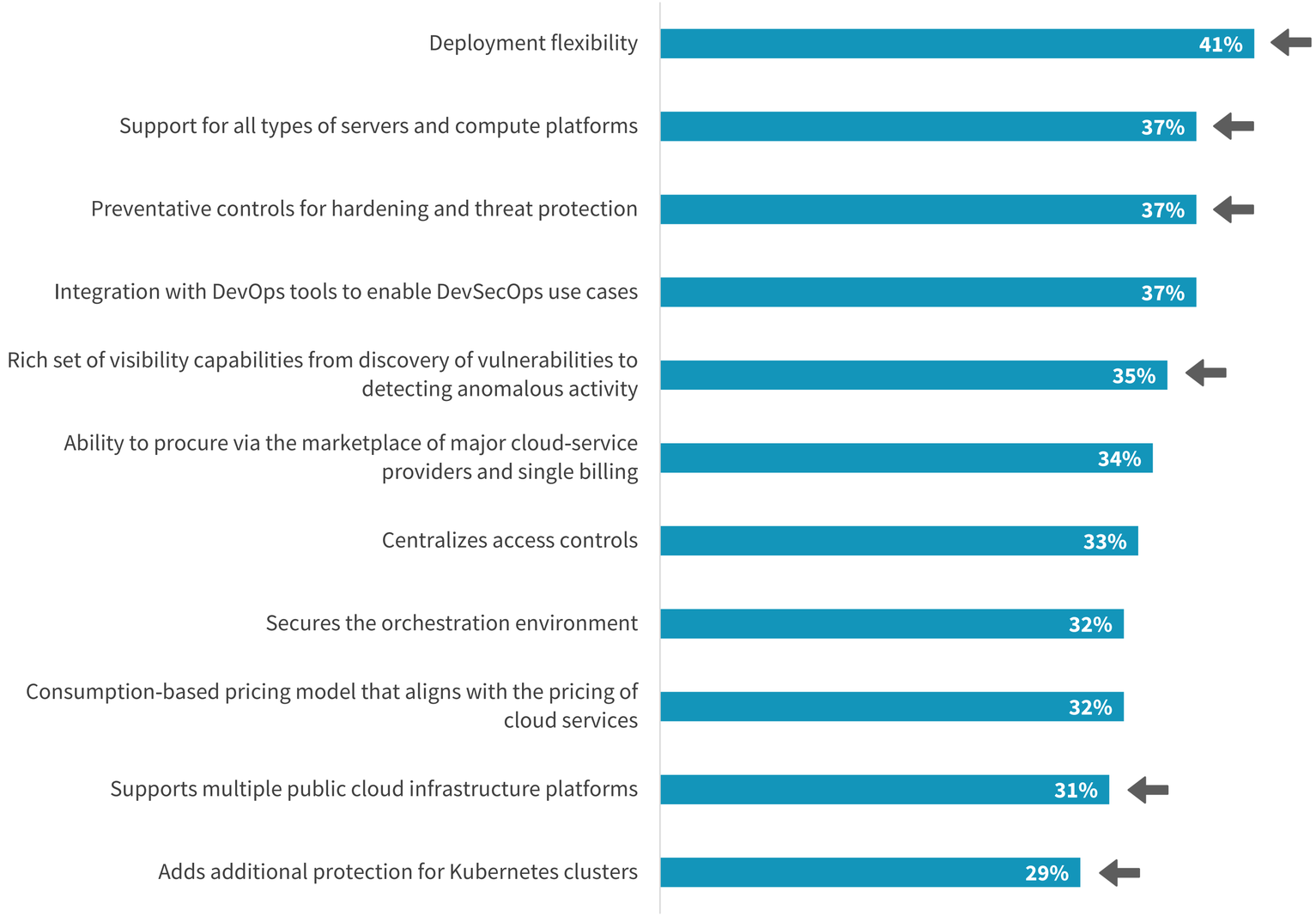
The Need for a Comprehensive Platform for Workload Protection

To keep up with the speed of development and to protect against evolving threats, organizations listed key attributes of comprehensive security platforms, including:

- Deployment flexibility.
- Support across servers and compute platforms.
- Preventative controls for hardening and threat protection.
- Centralized access controls.
- Protection across platforms.

By being able to put preventative measures in place, monitor for vulnerabilities and anomalous activities, and stop or contain any incidents with microsegmentation, organizations can protect their applications and workloads across hybrid environments. Whereas network-based solutions often have limited application context, application-centric controls can provide deep visibility into application behavior, providing protection in dynamic cloud environments.

Most attractive comprehensive cloud-native security platform attributes.



Back to Contents

TRUEFORT

TrueFort gives security teams the scalable workload protection platform they need to secure hybrid environments. Whether your workloads execute in the cloud, in virtual infrastructure, or on physical servers, TrueFort protects against advanced attacks with workload hardening, integrity monitoring, detection and response, and identity-based segmentation.

LEARN MORE

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.