Enterprise Strategy Group™ by TechTarget

WHITE PAPER

Fueling Business Growth With Security Across Hybrid and Multi-cloud Environments

Efficiently Manage Security to Support Digital Transformation

By Melinda Marks, Practice Director, Cybersecurity
Enterprise Strategy Group

October 2023

This Enterprise Strategy Group White Paper was commissioned by Cisco and is distributed under license from TechTarget, Inc.

Contents

Introduction 3
Security Challenges Associated With Digital Transformation 3
- Increased IT Complexity 4
- Increasing Movement of Applications to Cloud Environments 5
- Managing Security Posture Across Multi-cloud Environments 5
- A Wide Range of Security Incidents 7
- Too Many Siloed Tools and Data 8
- Overprovisioned Network Access 10

Introducing Cisco Cloud Protection Suite 11
Conclusion 12

Introduction

Organizations today are under pressure to digitally transform to optimize productivity and gain a competitive advantage. To do this, they are increasingly moving applications to cloud services to speed up software development without having to worry about provisioning servers or hardware. They also must support remote work to provide flexibility for employees and growing teams. On their digital transformation journeys, organizations face increased IT complexity with distributed applications across hybrid and multi-cloud environments, as well as the need to support a distributed workforce.

This creates new demands for security to ensure it can scale to support applications across environments and fully enable business growth. It requires security to support applications and users across diverse environments, which each have their own platform architectures, features, and capabilities. Security teams also need the flexibility to scale to support changing business needs, including organic growth and acquisitions.

But they face numerous challenges adapting their security strategies to keep up with the increasing usage of cloud services and cloud-native development. This is due to visibility challenges with the ephemeral nature of cloud resources and infrastructure that can be quickly scaled up or down. It is also difficult to keep up with the increased productivity of developers and to prevent exposure to threats as access and permissions proliferate.

While many organizations try to address these challenges by using multiple security solutions or platforms, they frequently face security incidents from common issues, including misconfigurations or overprovisioned access. Blind spots and gaps between tools also create visibility challenges. Additionally, while their tools might alert them about security vulnerabilities, security teams often fail to prioritize and remediate critical issues in time to protect their applications from attacks. As assets and applications proliferate across cloud environments, these challenges only multiply.

Security teams need an effective strategy to secure applications across environments, providing pervasive visibility and access protection supporting the mobility of workloads. This paper explores the key elements for an effective application security approach with the flexibility to support rapid business growth and its demands for hybrid and multi-cloud environments.

Organizations should look for a flexible approach that supports security teams, regardless of their skillsets, to provide full visibility of assets for efficient vulnerability remediation and a zero trust approach to protect applications from attack across all environments. It should include rapid detection of security issues, along with the contextual insight and threat intelligence to prioritize actions that will have the strongest impact on risk mitigation. It should also provide simplified, centralized ways to set policies to safeguard assets.

With an approach that addresses applications and access across their interconnected, dynamic multi-cloud and hybrid environments, security teams can optimize resources and operations to effectively manage risk and rapidly respond to threats. This enables security teams to efficiently scale to support rapid development and business growth.

Security Challenges Associated With Digital Transformation

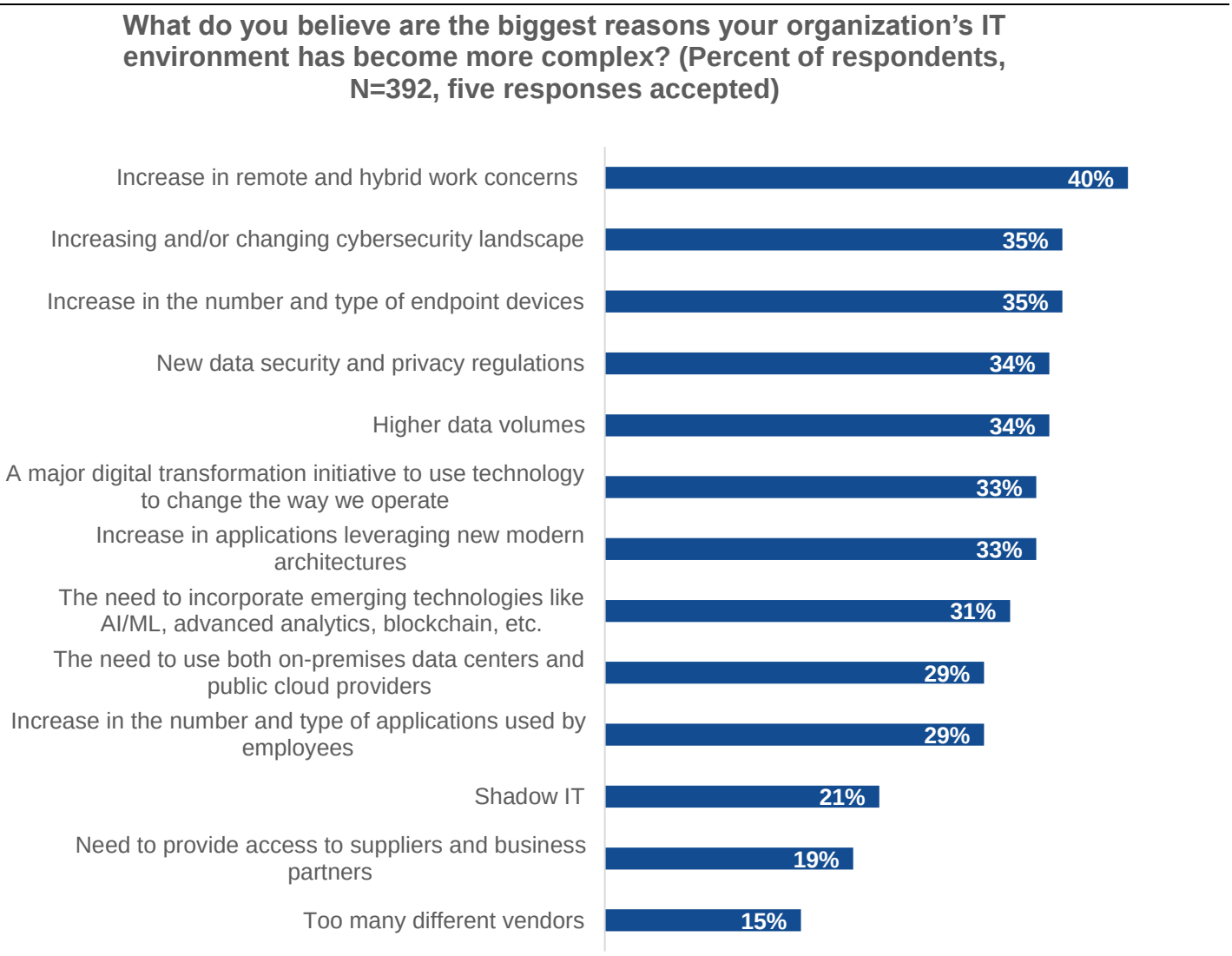
Research from TechTarget's Enterprise Strategy Group indicates a perfect storm of recent developments creating challenges for security teams. These include the increased complexity of IT environments, the proliferation of cloud-native applications from increased developer productivity, and visibility gaps across multiple public clouds, resulting in a wide range of security incidents. Security teams need an effective strategy to meet these challenges and enable the business to grow while ensuring their applications are secure and protected across different environments without requiring specialized skills.

© 2023 TechTarget, Inc. All Rights Reserved.

Increased IT Complexity

As organizations leverage digital transformation to increase productivity and gain a competitive advantage, it creates complexity and new demands on IT and security. Enterprise Strategy Group research shows that more than half (53%) of organizations say their IT environment is more complex or significantly more complex than it was two years ago.[1] Among those organizations, the top reason cited for the added complexity is the increase in remote and hybrid work (40%). Other top reasons for increased complexity include the changing cybersecurity landscape (35%), the increase in the number and types of endpoint devices (35%), new data security and privacy regulations (34%), and higher data volumes (34%). Further down the list, the need to use both on-premises data centers and public cloud providers was cited by 29% of respondents (see Figure 1).

Figure 1. Reasons for IT Complexity



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations can find effective ways to support growth and scale despite being challenged by these multiple areas of added complexity.

[1] Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

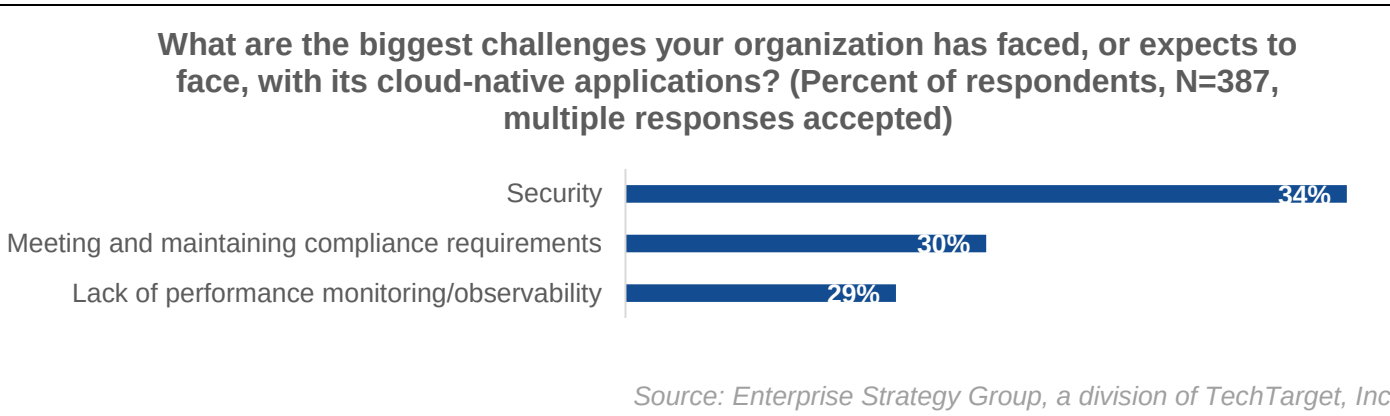
Increasing Movement of Applications to Cloud Environments

Organizations are also increasingly leveraging public cloud infrastructure to increase productivity and innovation with cloud-native development. They don't have to worry about the underlying infrastructure or maintenance, while they can benefit from economies of scale with pay-as-you-go models from cloud service providers (CSPs).

Enterprise Strategy Group application infrastructure modernization trends research shows 88% of the organizations surveyed run production workloads on public cloud infrastructure/platforms, and organizations are increasingly moving their production workloads to the cloud.[2] It also shows that those who have moved their applications to the cloud have realized many benefits, including greater agility, lower infrastructure costs, and faster deployment.

Cloud adoption also enables DevOps, which shifts operations left to empower developers to provision their own infrastructure instead of waiting for IT or operations teams to provision servers. Developers can work more efficiently, with faster time to value than traditional application development methods. However, with increased software development productivity, this creates security and compliance challenges for cloud-native applications.

Figure 2. Top Three Challenges Organizations Face With Cloud-native Applications



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

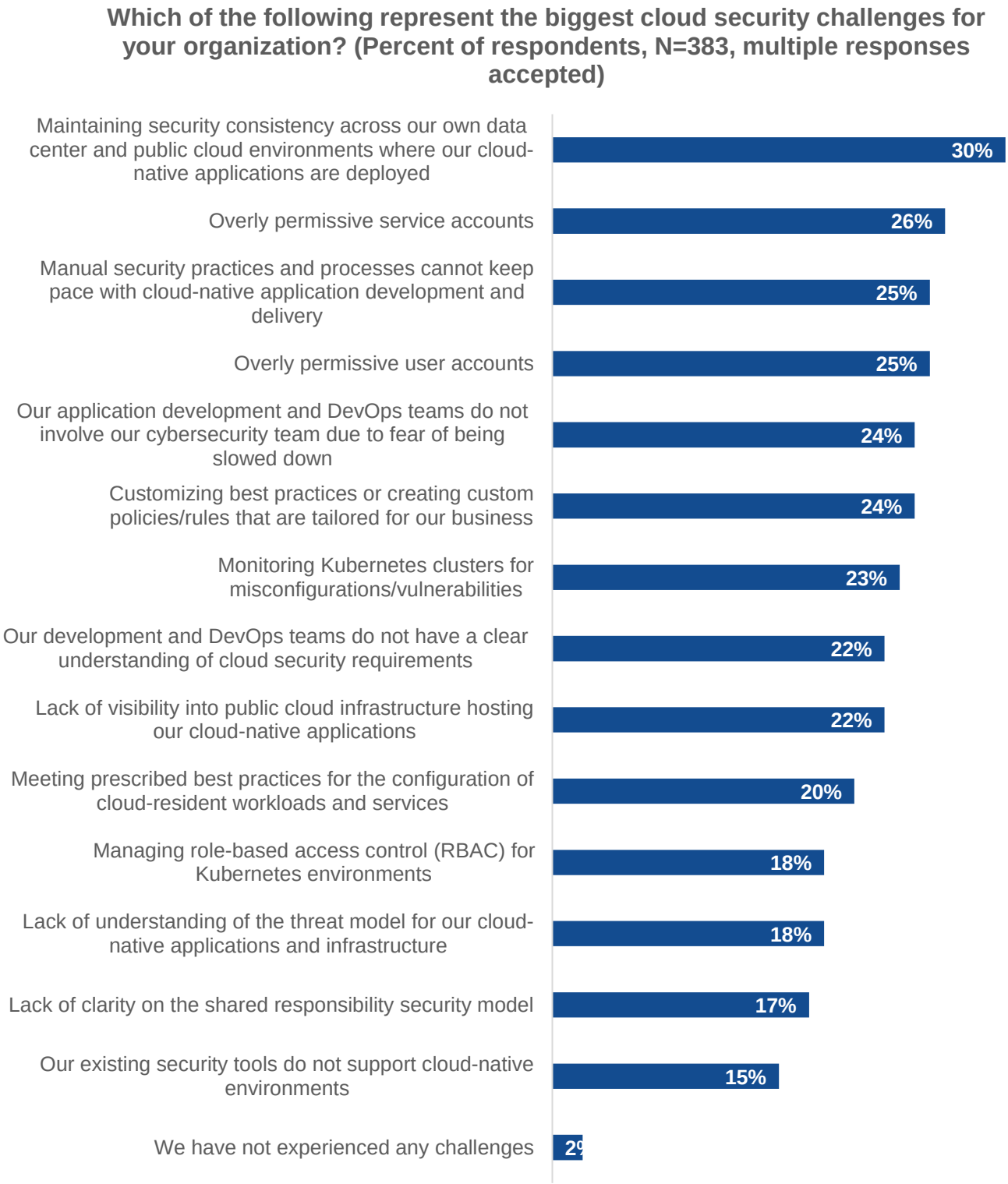
Organizations need an effective way to manage security risk to support the demands of the business to move to cloud-native development and deliver a higher volume and greater speed of releases. Security teams that can optimize efficiency to support this scale and growth, instead of impeding the adoption of newer technologies that can increase developer productivity and innovation, can play a strong role in enabling the business for better results.

Managing Security Posture Across Multi-cloud Environments

Supporting growth with cloud environments also requires security teams to support multi-cloud environments. Enterprise Strategy Group research on cloud security posture management shows that most organizations (94%) use multiple cloud infrastructure service providers, with the majority (69%) using three or more.[3] Although a majority of organizations (68%) said they have robust cloud security posture management solutions in place, they reported a variety of challenges, mainly around gaining the visibility and control they need to effectively manage risk across environments and teams, including achieving security consistency across their data center as well as their cloud environments (cited by 30%). Other challenges include overly permissive service and user accounts (cited by 25% and 26%, respectively), manual security practices and processes not keeping pace with the speed of cloud-native app delivery (25%), lack of involvement in and control over development processes (24%), lack of visibility into public cloud infrastructure (22%), and insufficient understanding of cloud-native threats (18%, see Figure 3).[4]

[2] Source: Enterprise Strategy Group Research Report, *Cloud-native Applications*, May 2022.
[3] Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023.
[4] Ibid.

Figure 3. Biggest Cloud Security Challenges for Organizations



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations need an effective approach that addresses these challenges to protect their applications across environments. This requires a way to gain visibility and control of the applications no matter where they reside, with a way to view them all as if they were in an interconnected, dynamic environment instead of separate environments. Bringing information together from multi-cloud and hybrid environments increases efficiency for security operations to mitigate risk and respond quickly to threats. This is the only way security can scale to support business growth with increasing cloud footprints.

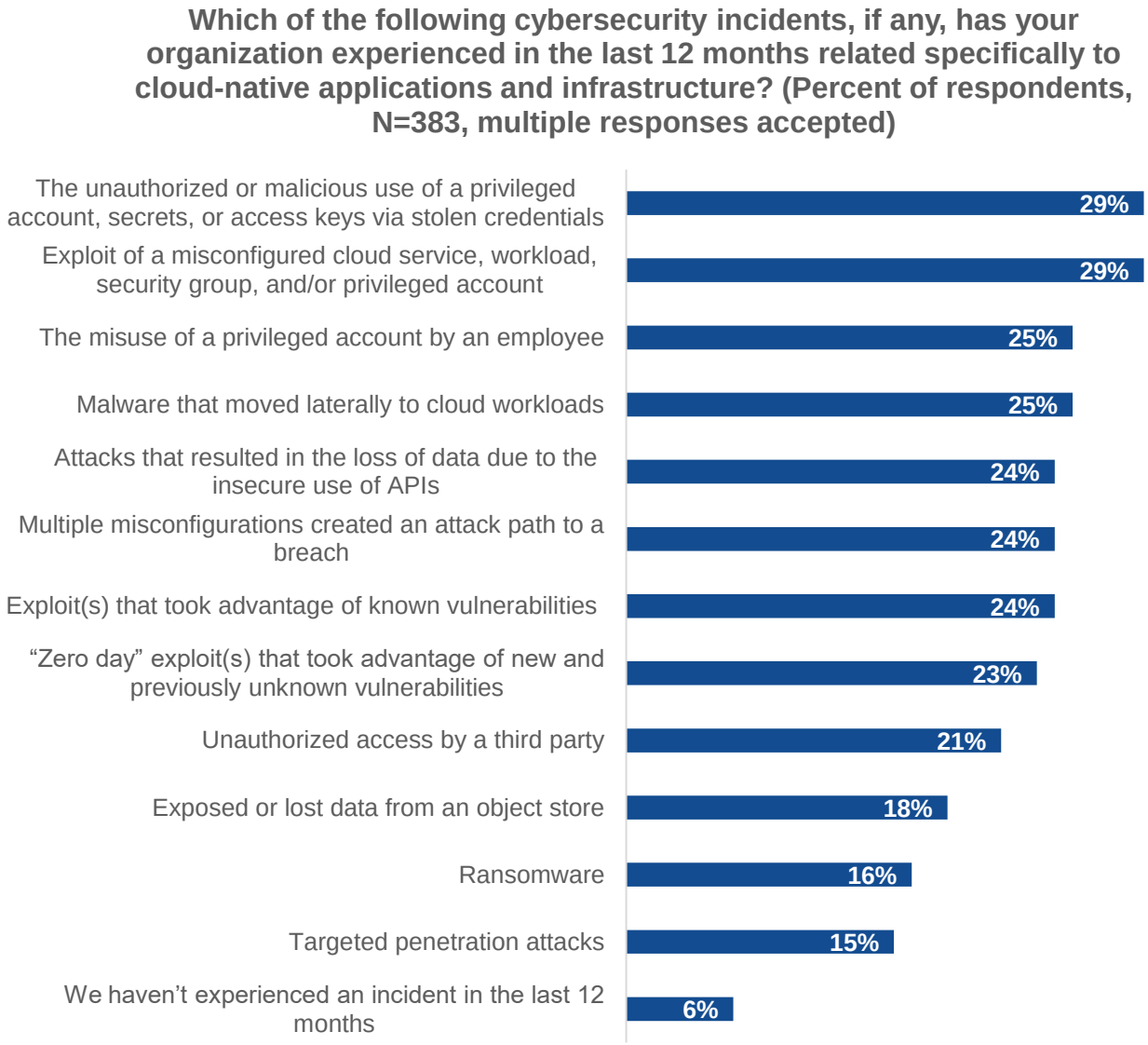
A Wide Range of Security Incidents

Although organizations typically have multiple security solutions in place, most of them have experienced security incidents involving their cloud-native applications or infrastructure. Specifically, the research shows that 94% of organizations reported facing security incidents with attacks and/or lateral movement in the past 12 months ranging from stolen credentials (29%), to misconfiguration exploitation (29%), to data loss via insecure use of APIs (24%), to ransomware (16%, see Figure 4).[5]

These occurred either because the organizations were unaware of their exposure to risk or because they were unable to remediate security issues in time to prevent or contain incidents. This underscores the need for visibility across environments, as well as the need for a platform approach to drive efficient security operations prioritizing actions that have the highest impact on risk reduction.

[5] Ibid.

Figure 4. Types of Security Incidents Involving Cloud-native Applications and Infrastructure Over the Past Year



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Too Many Siloed Tools and Data

Another challenge for organizations is the frequent use of multiple, siloed tools across IT, network, and security teams, which slows down security operations. While traditional application security utilizes multiple security products to ensure coverage, with testing and monitoring to detect security issues, it doesn’t scale for cloud-native applications and the increasing speed of development cycles to keep adding multiple separate tools that generate alerts without the context to determine how to prioritize needed actions.

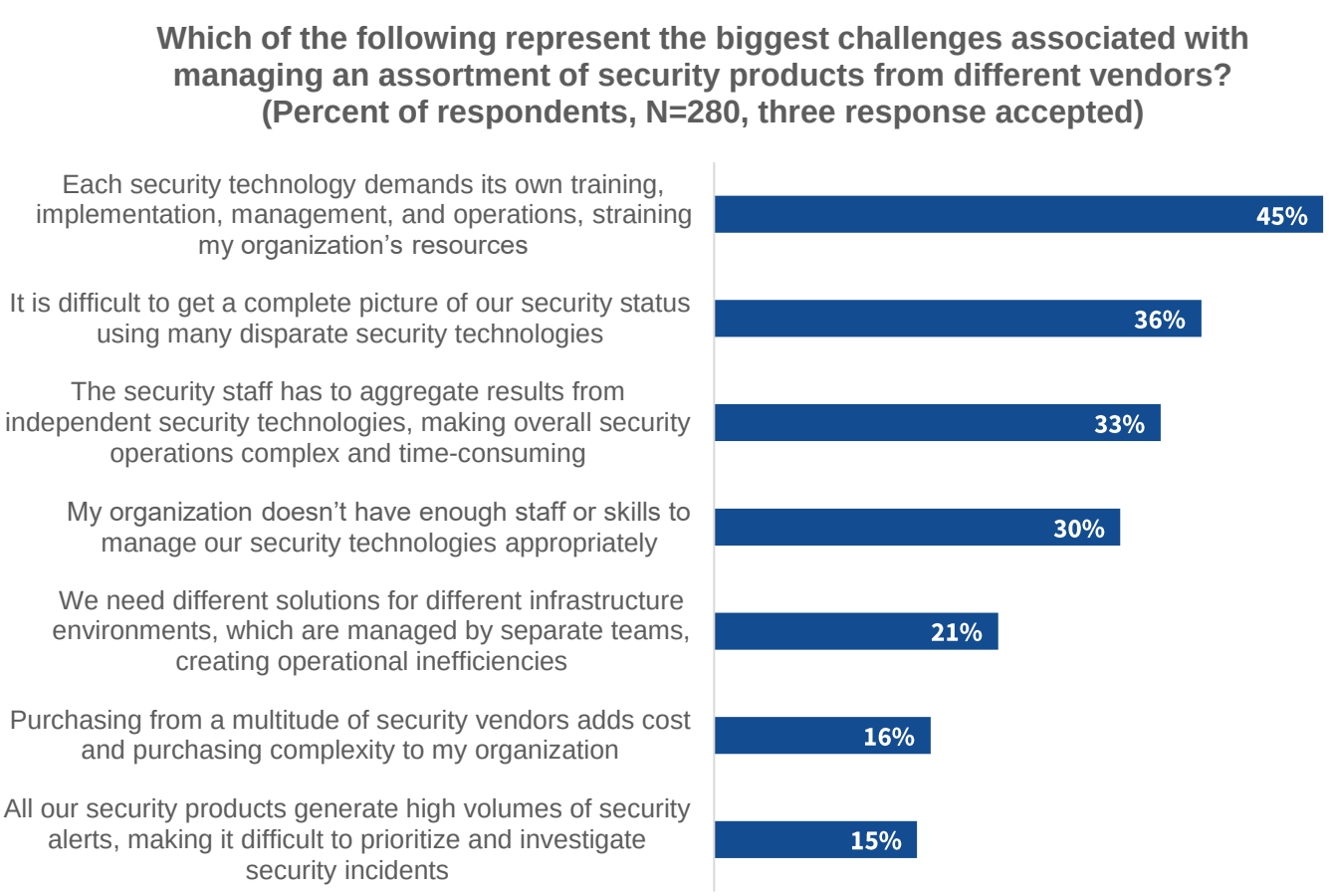
33% Reported Aggregating Results From Multiple Security Products As a Major Challenge

When security staff has to collate data from several independent security technologies, overall security operations becomes overly complex and time-consuming.

Developers and security teams can't keep up with the high number of alerts from multiple products. Also, separate tools are often built in different languages, making it difficult to analyze their results for the context needed to prioritize what needs attention. Further, each tool might generate alerts or false positives that would waste time to address.

Enterprise Strategy Group research shows that managing multiple tools creates challenges for cybersecurity staff, including the need for training and time to deploy and manage each tool, cited by 45% of respondents. Organizations also reported that it is difficult to get a complete picture of security status from separate tools (36%) and that aggregating the results from the separate tools creates more work for security staff (33%, see Figure 5).[6]

Figure 5. Challenges of Managing Multiple Security Products



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[6] Source: Enterprise Strategy Group Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

As a result, organizations are moving to products and services that work across CSPs to gather needed data and present it holistically. This helps security teams more effectively manage security risk, including efficient vulnerability management, attack surface management, and attack path analysis for a better understanding of security exposure.

A Unified Platform Across Hybrid and Multi-cloud Environments Can Provide:

- Least privilege access, with centralized controls stopping lateral movement.
- Pervasive visibility into asset discovery and attack path management for all applications, workloads, and resources.
- High-fidelity insights, actions, and priorities for SecOps teams, providing security posture from a single source of truth.

Overprovisioned Network Access

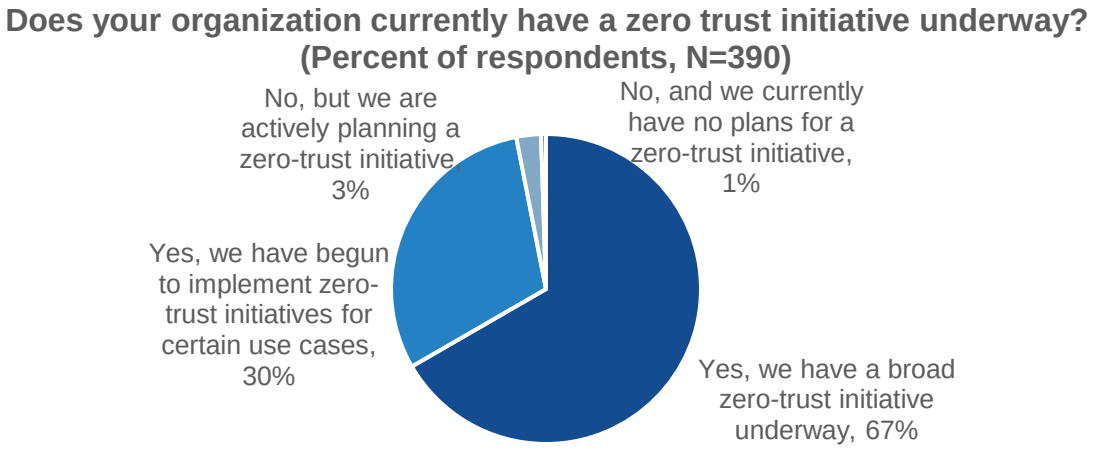
Managing identities and secure access also plays a key role in security program effectiveness. This is because cloud-native development makes it easy for organizations and their developers to deploy their applications to the cloud and make them available for customers, employees, and partners. Once deployed to the cloud, the applications are available for the intended users, but access needs to be managed properly to mitigate risk and exposure that could put company and customer data at risk. In other words, in the cloud, there is no perimeter to protect workloads; identity and access form the perimeter.

Looking at the cloud-native security challenges and incidents mentioned earlier, many are related to identity and access issues. This is because it is easy to overprovision access to facilitate rapid development, but if not properly managed, increased access expands the attack surface and an organization's exposure to risk by leaving applications open to attack or making it easy for an attacker to move laterally after penetrating a system.

Implementing a zero trust network access (ZTNA) approach helps protect applications by ensuring that every access request is verified before connections are made, enabling security teams to minimize the likelihood and impact of an incident. So if a workload or application is compromised, a zero trust environment would prevent accessing or egressing data. Enterprise Strategy Group research shows that a vast majority of organizations (97%) either have or are in the process of implementing zero trust initiatives to ensure they can better protect their workloads across environments.[7]

[7] Source: Enterprise Strategy Group Complete Survey Results, *2023 SASE Series: SSE Leads the Way Toward SASE*, August 2023.

Figure 6. Percentage of Organizations Adopting Zero Trust Initiatives



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

However, organizations face challenges implementing least privilege access for their applications across multi-cloud and hybrid environments, including facilitating collaboration between IT, operations, and security teams; providing secure access from a range of devices; managing costs; ensuring data security, maintaining performance; and providing comprehensive visibility and reporting.

Therefore, organizations should look for a solution that satisfies both hybrid and multi-cloud environments, integrating a zero-trust aproach. Such a solution would help organizations mitigate risk while optimizing operational efficiency, helping IT, networking, and security teams to protect their applications across environments.

Introducing Cisco Cloud Protection Suite

The Cisco Cloud Protection Suite delivers a modern application security approach with end-to-end security for hybrid and multi-cloud application environments. From bare metal to cloud-native, the Cloud Protection Suite provides customers with holistic application security, safeguarding workloads across environments—on prem and in the cloud.

Cisco Cloud Protection offers the following:

- **Comprehensive hybrid and multi-cloud security.** With Cisco's Cloud Protection Suite, users can efficiently and effectively manage security risk across environments.
- **Pervasive visibility into all assets.** Providing a clear view of every network, application, and cloud asset enables organizations to validate security posture and prioritize risks to the business.
- **Consistency across environments.** Cisco's suite facilitates the application of security frameworks, controls, and compliance policies to mitigate risk and meet industry best practices.
- **Optimized remediation efficiency.** Cisco's suite utilizes risk scoring powered by data science for prioritization of vulnerabilities that pose real risk across the hybrid environment.
- **Application protection.** Safeguarding traffic across the network, clouds, and VPCs, the suite enables consistent and accurate macro- and micro-segmentation across environments.
- **Least privilege access with a zero trust approach.** Cisco Cloud Protection leverages ZTNA to protect workloads on prem and in the cloud, reducing the attack surface area and preventing lateral movement.

Using the Cisco Cloud Protection Suite to manage application security across cloud environments, customers can:

- Reduce operational overhead and optimize resources.
- Mitigate security risk by prioritizing vulnerabilities according to risk.
- Facilitate meeting compliance regulations.
- Respond more quickly to threats with comprehensive visibility.
- Enable digital transformation to support business growth.

Conclusion

As organizations increasingly move workloads to the cloud to optimize productivity, security teams face challenges protecting their applications across environments and keeping up with business growth. The complexity of supporting applications across hybrid and multi-cloud envrionments while enabling cloud migration or even repatriation requires a unified, flexible approach.

The Cisco Cloud Protection Suite provides an effective way for security teams to manage application security across multiple clouds and data centers. By providing comprehensive visibility and least privilege access control, it provides a holistic and effective method for securing assets and applications across the entire environment. Offering a cohesive way to manage risk with automation, consistency across envrionments, and consolidated security tools, also reduces manual tasks to optimize efficiency across IT, network, and security teams.

With Cisco Cloud Protection Suite, security teams are better equipped to support business growth and digital transformation, including scaling development teams, adoption of new technologies, and mergers and acquisitions that keep businesses competitive.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

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

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, 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.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com