Enterprise Strategy Group™ by TechTarget

USING RUNTIME INSIGHTS FOR EFFECTIVE CLOUD SECURITY

Driving Efficiency with a Cloud-native Application Protection Platform to Support Innovation and Speed

Melinda Marks,
Senior Analyst

SEPTEMBER 2023

sysdig | aws

This Enterprise Strategy Group eBook was commissioned by Sysdig and is distributed under license from TechTarget, Inc.

Introduction

As organizations leverage state-of-the-art cloud services and modern software development processes for increased productivity and innovation, they need an efficient way to manage security risk and mitigate exposure to attacks as their development scales.

While IT teams are focused on scaling to meet business needs, security teams need a way to scale to support the growth of dynamic cloud workloads, services, and identities. Although organizations typically implement a number of solutions to ensure they have the coverage to identify security issues, they face security incidents if they are overwhelmed with alerts. Instead, organizations need the context to prioritize needed actions to remediate security issues in time to stay ahead of threats.

This eBook explores how organizations should leverage a consolidated platform that leverages runtime insights to effectively manage security risk. With visibility and context from runtime monitoring, organizations can drive efficiency across four essential areas:

Vulnerability management, reducing the time to triage alerts and remediate issues in order to stay ahead of threats and attacks.

Posture management, eliminating blind spots with contextual prioritization and consistency of governance for compliance.

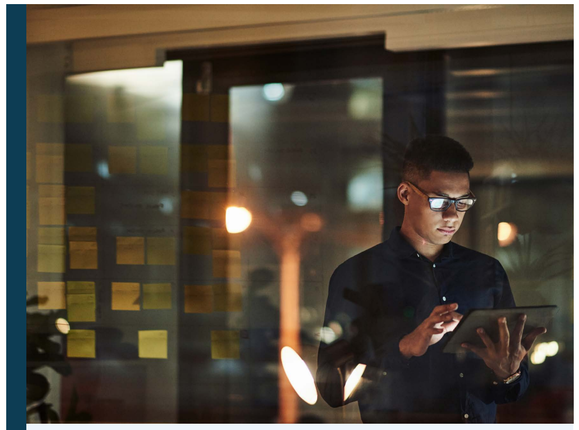
Permissions and entitlement management, understanding access and permissions to eliminate over-permissive identities and paths of attack.

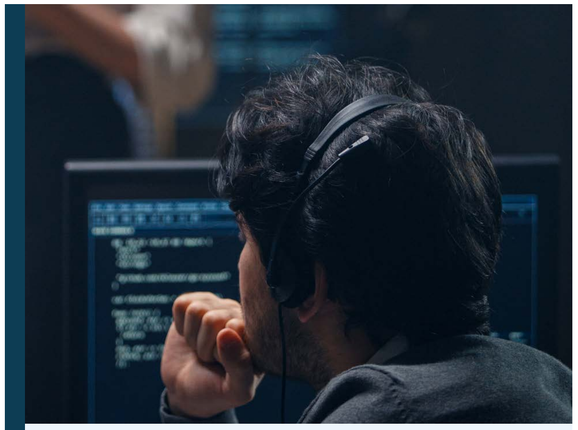
Threat detection and response, thoroughly monitoring applications and related resources to identify security issues and speed response.

BACK TO CONTENTS

CONTENTS

Click to follow





BACK TO CONTENTS

The Move to the Cloud

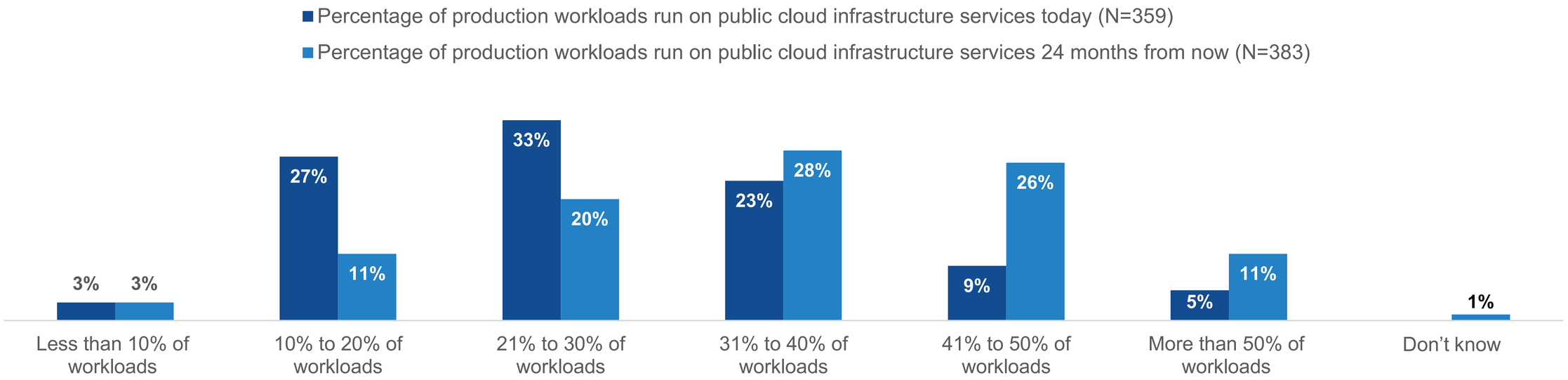
Moving Production Workloads to Public Clouds

As organizations are under pressure to boost productivity and drive innovation to serve their customers, they are increasingly moving production workloads to public cloud platforms. Research from TechTarget's Enterprise Strategy Group shows that nearly one in seven respondents report that more than 40% of their organization's applications run on public cloud infrastructure. This number is expected to more than double two years from now.

Cloud service providers like Amazon Web Services (AWS) provide 200+ services today that enable developers to build their applications with microservices architectures that can be deployed on elastic infrastructure in the cloud and spun up and down as needed, bringing new economies of scale and productivity. This enables companies of all sizes and across all industries to deliver software applications to their customers to better serve them and gain a competitive advantage. Organizations don't have to worry about the underlying infrastructure or maintenance, and they can take advantage of economies of scale with pay-as-you-go models.

As a result, our research shows that organizations are increasingly moving production workloads to the cloud.[1]

Figure 1. Percentage of Production Workloads Run on Public Cloud Infrastructure Services



1. Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023.

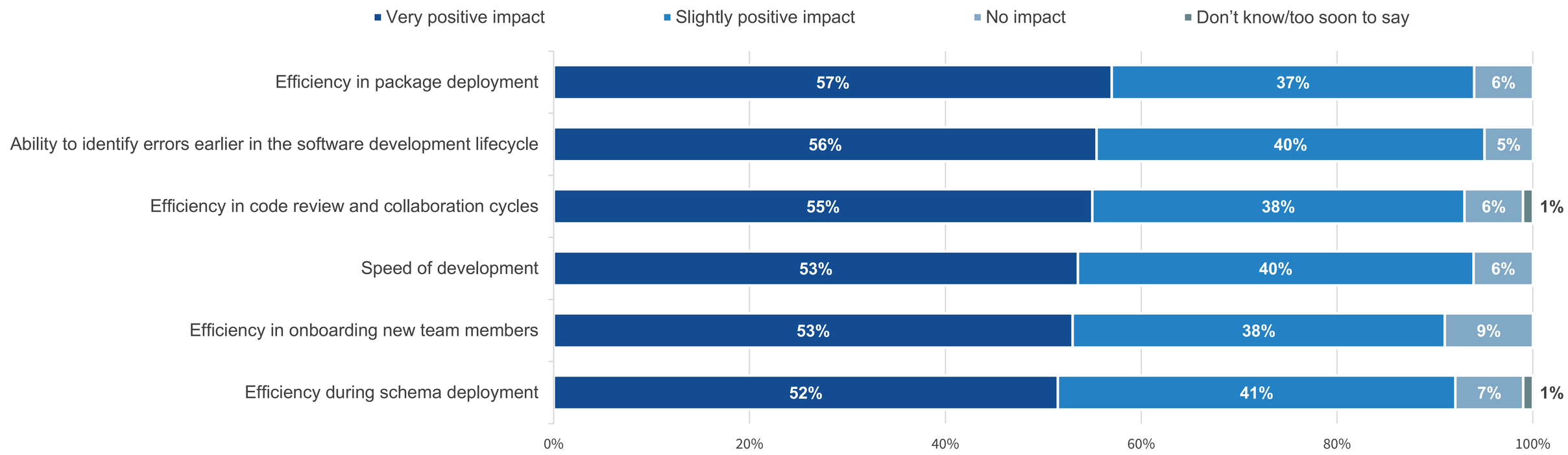
BACK TO CONTENTS

Increased Efficiency and Speed with Cloud-native Development

Organizations that have moved their applications to the cloud have realized many benefits that increase their efficiency for greater productivity.

This is due to enabling DevOps, where operations teams have shifted left to empower developers to provision their own infrastructure instead of waiting for IT or operations teams to provision servers or computing resources. Leveraging AWS, developers can work quickly and efficiently to deliver software applications, deploying them to the cloud. By utilizing continuous integration and continuous deployment (CI/CD) processes, they are able to collaborate and work more efficiently, with faster time to value than traditional application development methods.[2]

Figure 2. Positive Impacts of Cloud-native Development



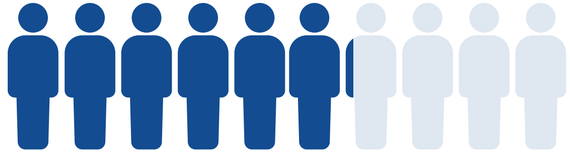
2. Source: Enterprise Strategy Group Research Report, *Cloud-native Applications,* May 2022.

BACK TO CONTENTS

Security Tops the List of Cloud Adoption Challenges

While most organizations (62%)[3] reported that they are migrating their existing applications to public cloud infrastructure for its benefits, they also reported that security and compliance are two of the biggest areas where they face cloud-native-application-related challenges.

Organizations need to support the speed, growth, and complexity of securing their cloud-native applications. They need an effective way to efficiently manage risk to support the demands of the business with the move to the cloud.[4]



62%

of organizations are migrating their **existing applications to public cloud infrastructure.**

Figure 3. Top 5 Challenges with Cloud-native Development

34%
Security

30%
Meeting and maintaining compliance requirements

29%
Lack of performance monitoring/observability

29%
Services purchased outside the purview of IT or other authorized decision makers

27%
Retaining full-featured functionality and capabilities

3. Source: Enterprise Strategy Group Researc Report, *Application Infrastructure Modernization Trends Across Distributed Cloud Environments,* March 2022.
4. Source: Enterprise Strategy Group Research Report, *Cloud-native Applications,* May 2022.

BACK TO CONTENTS

Challenges Scaling Security for the Cloud

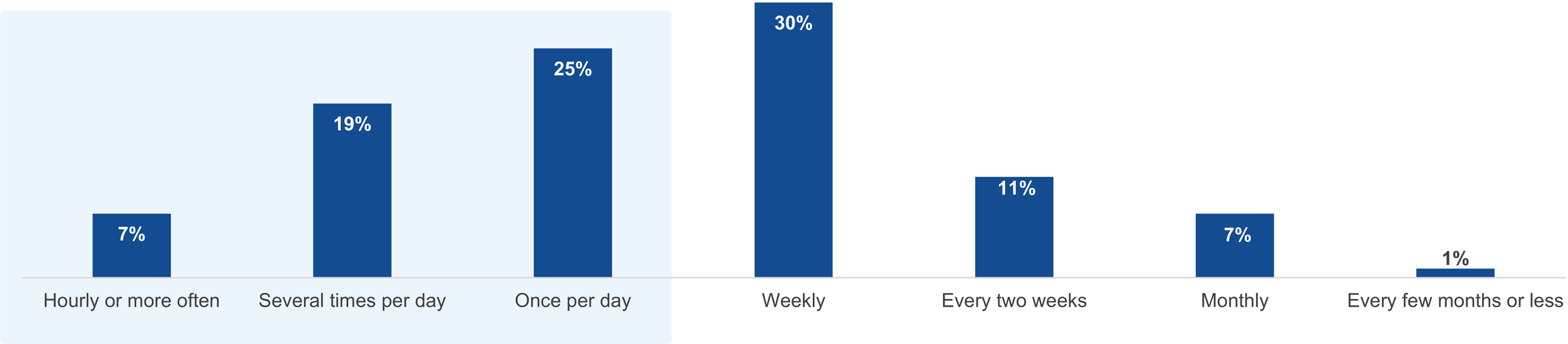
> “Most organizations are deploying new code to production daily, **making it difficult for security to scale to keep up with these faster development cycles.”**

Challenges Scaling Security with Increased Speed of Development

Traditional security teams were aligned with infrastructure provisioning and common waterfall development processes. An application developer would file a ticket, wait for someone from the IT or operations teams to provision a server, work to release software, and then issue updates over periods of months or even yearly.

With cloud-native development processes, developers are empowered to provision their own infrastructure, build their applications, and deploy them to the cloud using continuous integration and continuous deployment (CI/CD) pipelines for rapid software releases and updates. In fact, most organizations are deploying new code to production daily, making it difficult for security to scale to keep up with these faster development cycles.[5]

Figure 4. Frequency of Deploying New Code to Production Environments



5. Source: Enterprise Strategy Group Research Report, *Cloud-native Applications,* May 2022

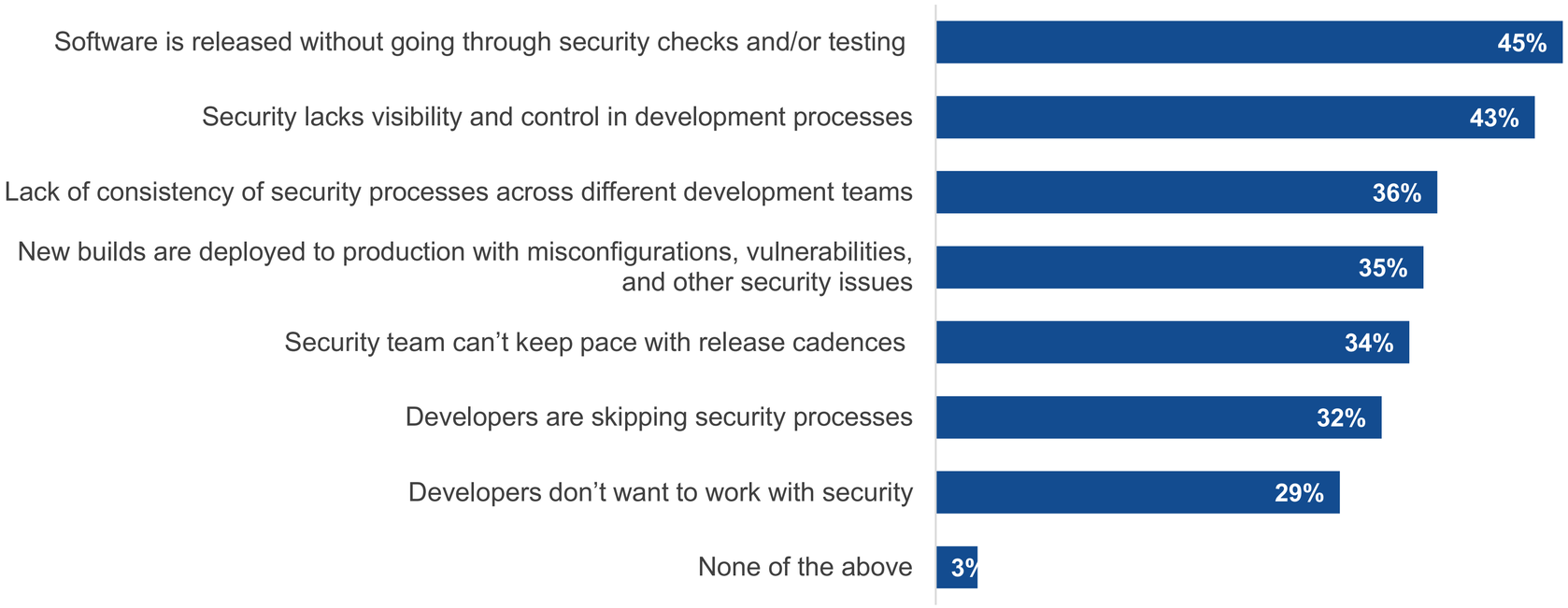
BACK TO CONTENTS

Increased Security Vulnerabilities

Security faces challenges keeping up with these faster development cycles. And all too often, security teams lack visibility into and control over development actions.

The result: Software is often released without going through security checks or testing. The new software builds are deployed with misconfigurations, vulnerabilities, and other security issues.[6]

Figure 5. Security Challenges from Faster CI/CD Development Cycles



THE RESULT:

Software is often released without going through security checks or testing. The new software builds are deployed with misconfigurations, vulnerabilities, and other security issues.

6. Source: Enterprise Strategy Group Research Report, *Walking the Line: GitOps and Shift Left Security*, November 2022

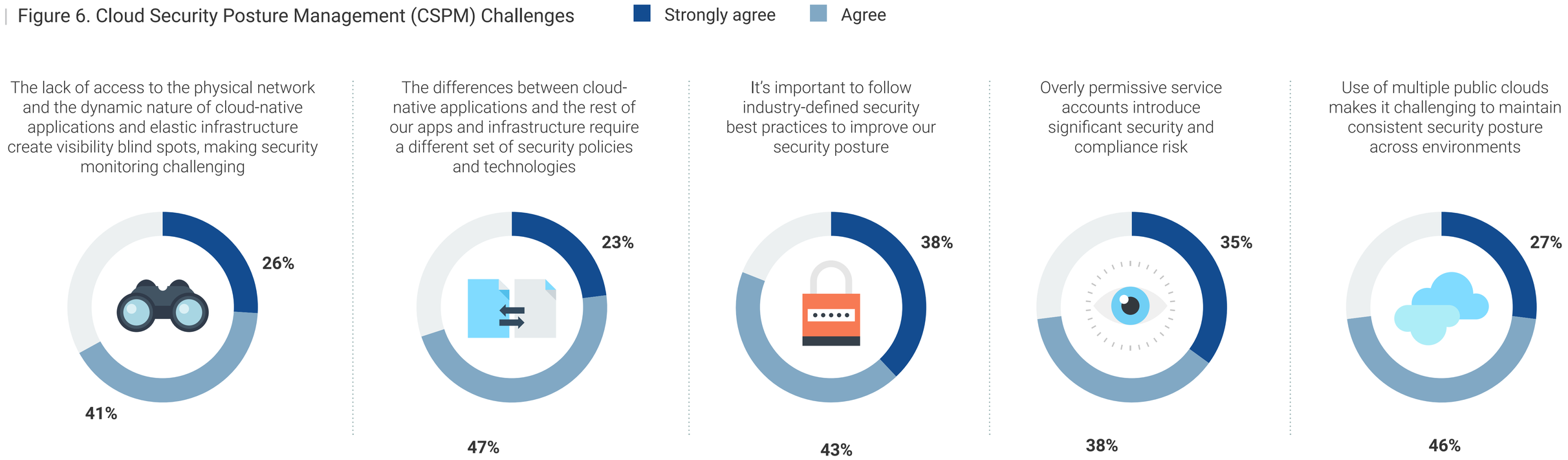
BACK TO CONTENTS

Cloud Security Posture Management (CSPM) Challenges

Organizations also realize that it is more difficult to manage their cloud security posture with the complexity of microservices-based applications with dynamic infrastructure and components.[7]

Ideally, security teams can work with developers to harden their applications with the right security controls and processes to prevent security issues from being deployed into production. Once they are deployed, the applications are more difficult to monitor, as they use ephemeral infrastructure and resources that are spun up and spun down on demand. Also, there is a bigger attack surface with exposed dynamic surfaces and nodes, and the infrastructure's security cannot be controlled by setting up a perimeter.

Figure 6. Cloud Security Posture Management (CSPM) Challenges



7. Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023.

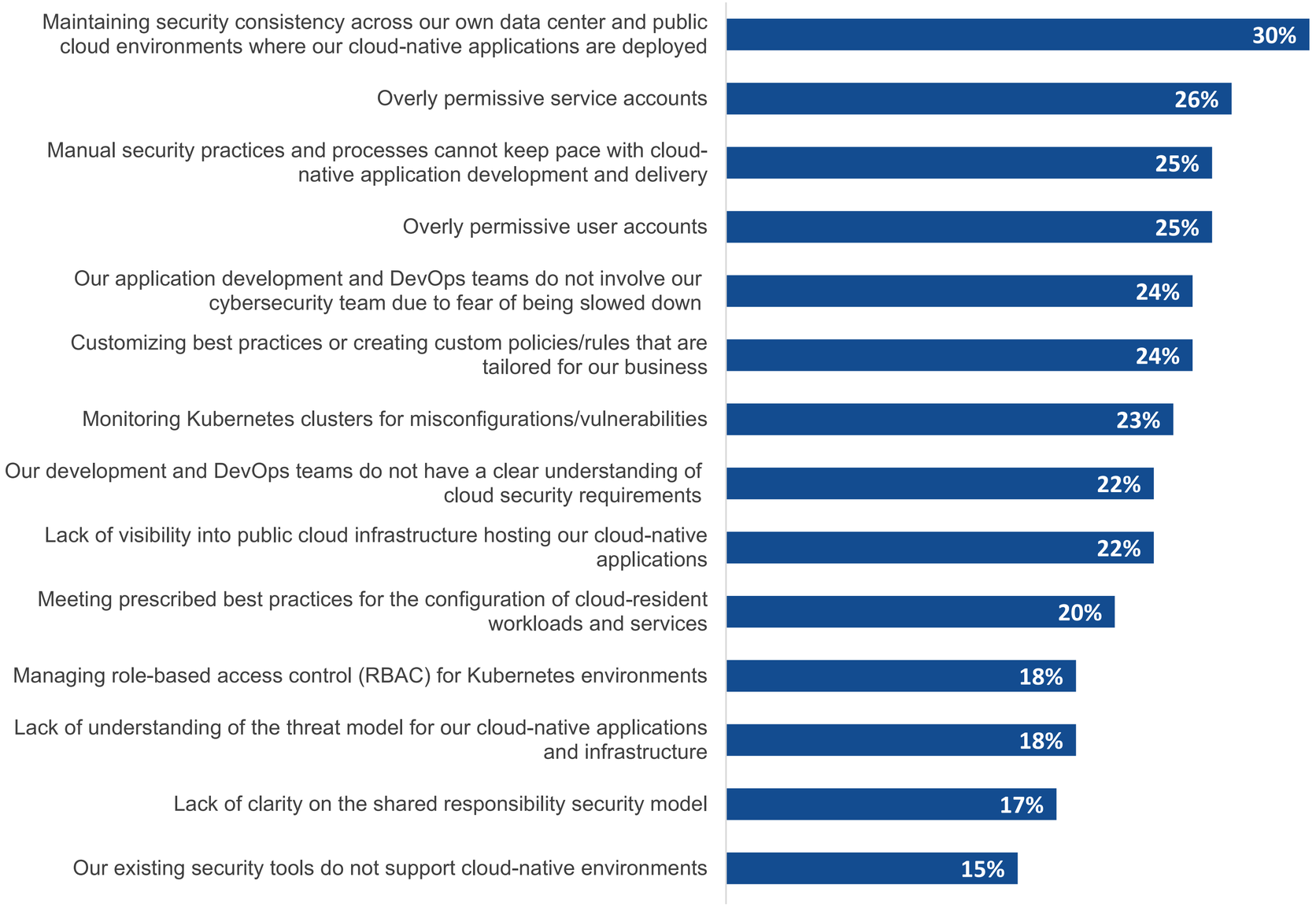
BACK TO CONTENTS

The Need for Visibility and Context to Scale

Organizations are facing security challenges related to scaling their cloud-native applications to manage risk.[8] Visibility is essential for gaining the context and understanding needed to drive efficient programs that make the best usage of proactive hardening and rapid response to threats and attacks.

For example, monitoring assets provides a clearer understanding of the exposure of resources, the location of the issue (the geographical region, cluster, container, or namespace), access and permission for points of entry or movement, and other information. This provides the context for preventative risk mitigation, such as setting up controls and security processes early in the software development lifecycle, to catch and fix issues before deploying applications to the cloud. Also, in runtime, when issues are detected, it gives them the context needed to prioritize remediation actions based on what needs attention in order to protect against attacks or threats or to minimize their impact.

Figure 7. Cloud-native Application Security Challenges



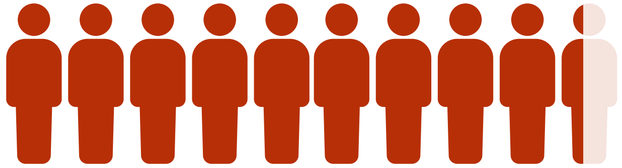
8. Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023.

BACK TO CONTENTS

Security Incidents on Cloud-Native Applications

We also see the need to more effectively monitor cloud workloads when we look at the wide range of attacks that organizations have experienced on their cloud applications.

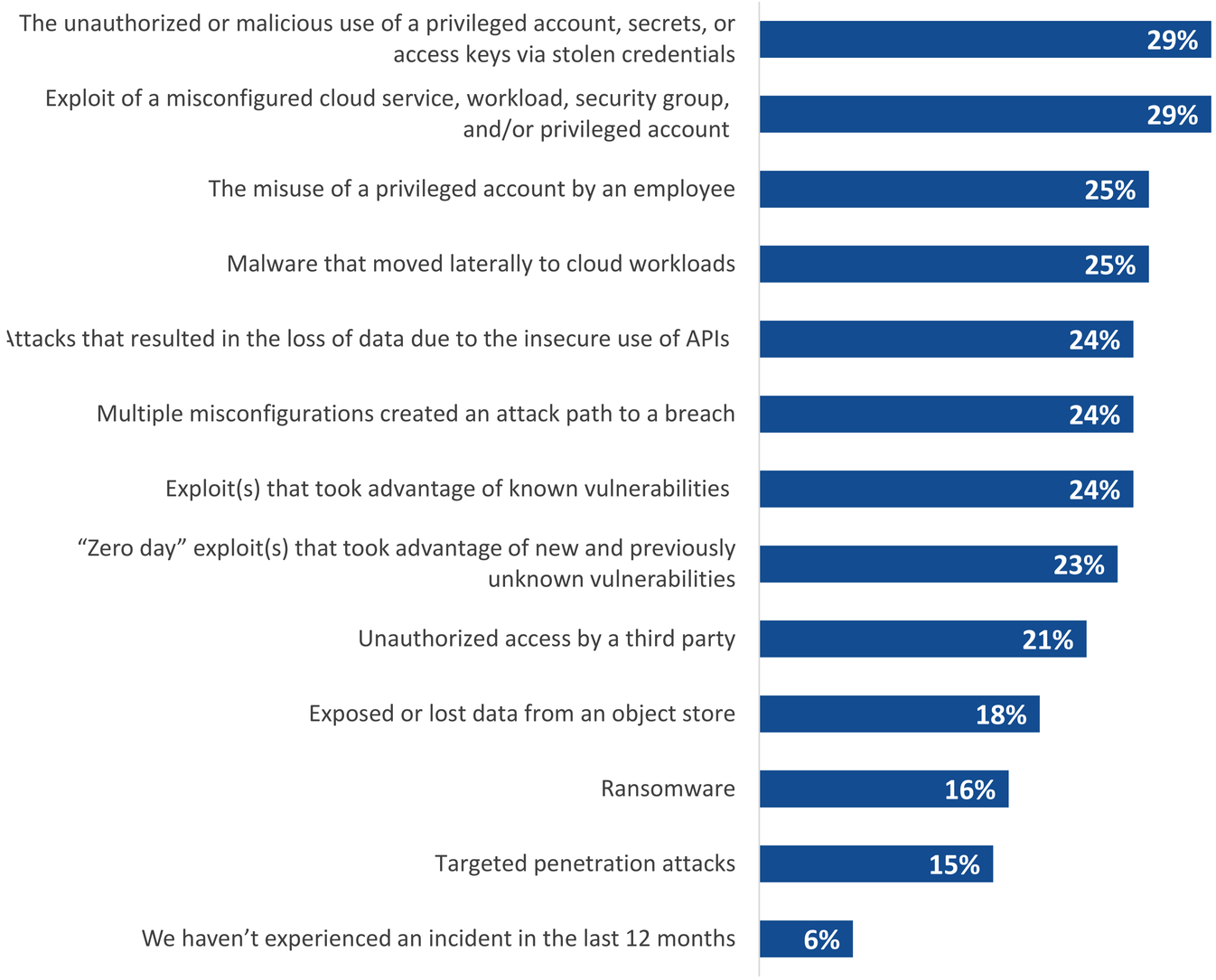
Most are the result of identity and access issues or misconfigurations. When security issues are detected, organizations need the context to remediate issues, beginning with those that have the highest impact on reducing risk.



94%

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

Figure 8. Cloud-native Security Incidents Experienced in the Last 12 Months



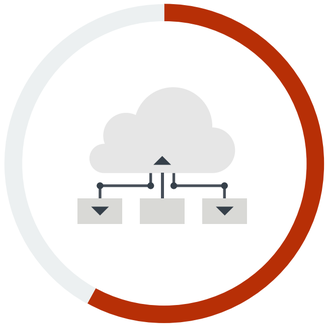
BACK TO CONTENTS

The Impacts of Unmitigated Misconfigurations

Although organizations have security solutions in place, they report suffering a wide range of incidents and related consequences from misconfigurations.[9]

These include the introduction of crypto-jacking malware to mine cryptocurrency, impacted SLAs, unauthorized access to apps and data, compliance fines, malware, ransomware, and data loss.

Although their tools may alert them on security issues, organizations still may not be able to take the needed actions to remediate the misconfigurations in time to protect against an attack.



97%

of organizations **detected at least one misconfigured cloud application in the last 12 months.**

Figure 9. Impacts of Cloud Application Misconfigurations

9. Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023

BACK TO CONTENTS

The Importance of Cloud Infrastructure Entitlement Management (CIEM)

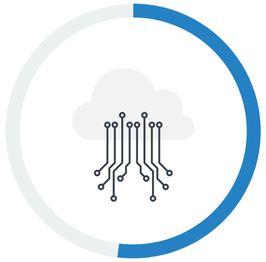
A majority of organizations recognize the role of entitlements in exposing them to more risk with a broader attack surface.[10]

It is easy for developers to set up entitlements for access privileges and connections to resources for team collaboration while building applications. However, overprovisioned or unused entitlements expose them to risk and compliance issues.

Instead of manually checking and analyzing entitlements to determine changes needed to reduce risk, organizations should look to a CIEM solution to mitigate risk and better meet compliance regulations. A CIEM solution maps entitlements and their relationships with applications and resources to make it easy to eliminate unneeded access points without impacting application performance.

37%

of respondents **have failed an audit** due to cloud entitlements.



52%

of respondents said entitlements **played a central role** in exposing their cloud environment.

89%

of respondents said **CIEM is very important or critical** in reducing security risk.

10. Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023.

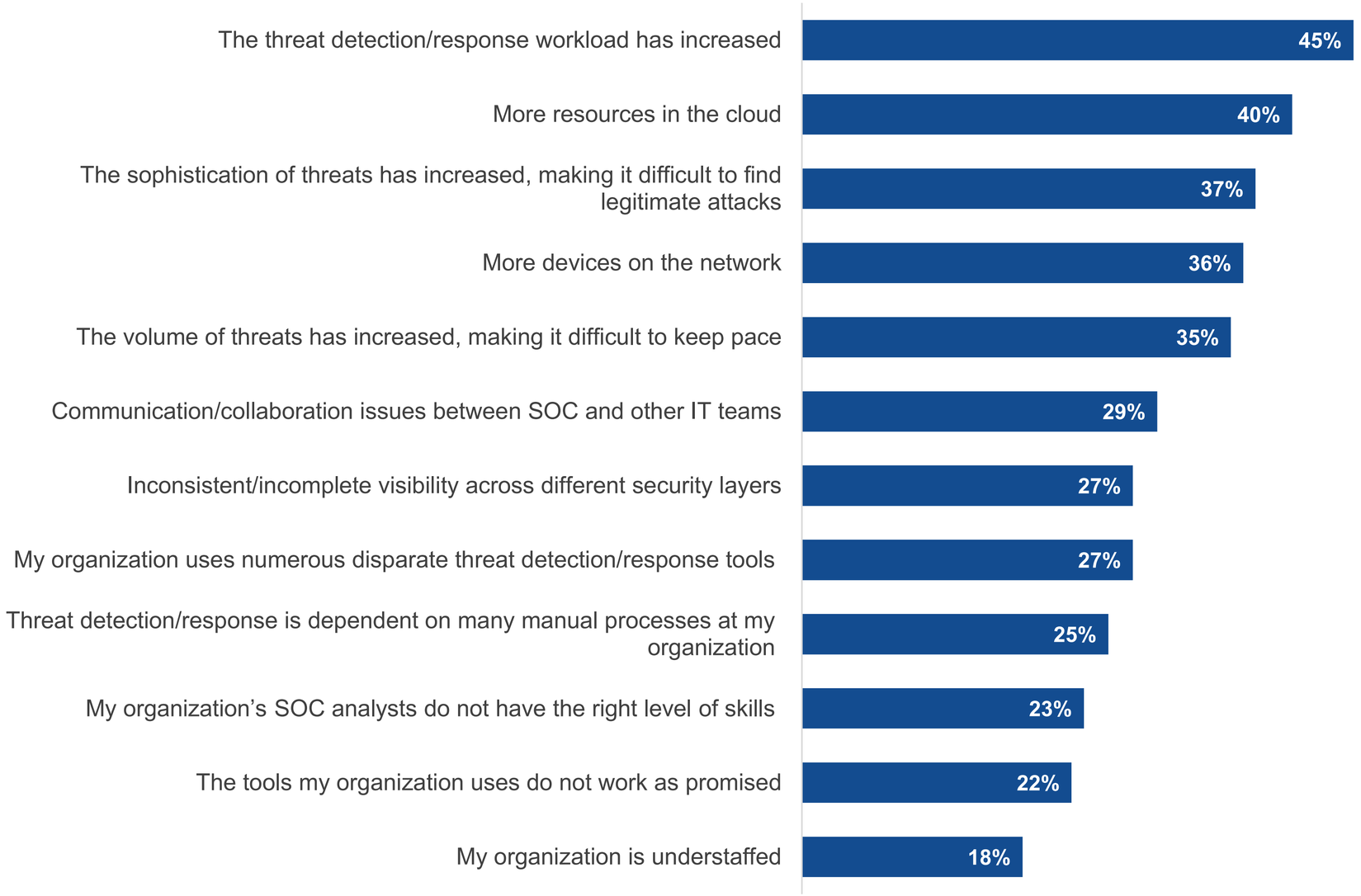
BACK TO CONTENTS

Increased Complexity Creates Threat Detection and Response Challenges

Organizations also struggle with threat detection and response due to challenges with monitoring, including addressing increasing workloads and the dynamic, distributed nature of modern applications.[11]

Threats can now exploit vulnerabilities across different layers of the cloud-native threat stack, making it crucial to monitor the infrastructure thoroughly in real time to accurately identify issues. Also, organizations need solutions that can optimize efficiency across teams, providing them with the context and understanding to make faster decisions, while also facilitating better communication and collaboration for rapid response.

Figure 10. Challenges Organizations Face Today with Threat Detection and Response



11. Source: Enterprise Strategy Group Research Report, *The Evolving Role of Network Detection and Response*, March 2023.

BACK TO CONTENTS

Challenges Managing Multiple, Siloed Tools

Organizations also face challenges when they use multiple, siloed tools.[12] While these tools help detect security issues, teams can't remediate issues in time to prevent incidents, and they waste time chasing multiple alerts and false positives. They also bring other challenges, including requiring training and time to deploy and manage them.

As a result, organizations are moving to consolidated platforms that integrate capabilities while providing context to prioritize needed actions for efficient remediation.

Figure 11. Issues with Managing Multiple Security Tools from Disparate Vendors

45%
Each security technology demands its own training, implementation, management, and operations, straining my organization's resources

36%
It is difficult to get a complete picture of our security status using many disparate security technologies

33%
The security staff has to aggregate results from independent security technologies, making overall security operations complex and time consuming

30%
My organization doesn't have enough staff or skills to manage our security technologies appropriately

21%
We need different solutions for different infrastructure environments, which are managed by separate teams, creating operational inefficiencies

16%
Purchasing from a multitude of security vendors adds cost and purchasing complexity to my organization

15%
All our security products generate high volumes of security alerts, making it difficult to prioritize and investigate security incidents

"75% of smaller organizations **buy from 1 to 10 cybersecurity vendors, while nearly half of enterprises have more than 10.**

12. Source: Enterprise Strategy Group Research Report, *Technology Perspectives from Cybersecurity Professionals,* May 2022.

BACK TO CONTENTS

Using a Platform Approach That Leverages Runtime Insights

The Majority of Organizations Are Integrating Their Security Platforms

Enterprise Strategy Group research shows that organizations are moving away from multiple tools in favor of platform approaches with integrated technologies.

They are looking to platforms to consolidate information and telemetry from multiple sources to save them the time of having to analyze and triage alerts across multiple tools.[13]

They also need a centralized way to consistently apply the controls and security processes to reduce risk across their cloud workloads as development teams grow.

Figure 12. Preference for Integrated Security Technology Platforms

24%
My organization tends to purchase best-of-breed security products

38%
My organization tends to purchase integrated security technology platforms rather than best-of-breed products

15%
My organization tends to purchase best-of-breed security products today, but we will be transitioning to purchasing integrated security technology platforms over the next few years

23%
Don't know

13. Source: Enterprise Strategy Group Research Report, *Technology Perspectives from Cybersecurity Professionals*, May 2022..

BACK TO CONTENTS

Figure 13. Level of Integration between Cloud Security Monitoring Solutions and Development Processes

41%

They are well integrated - when an issue is found, there is an option for auto-remediation and/or the developer can immediately fix the issue.

44%

There is some integration - when an issue is found, the monitoring tool can deliver information to the developer owner to facilitate remediation.

15%

They are not integrated at all - when the monitoring tools find an issue, there is work involved to determine who can make the coding revision to remediate the issue.

Integrating Security Monitoring with Development Processes

Enterprise Strategy Group research also shows that organizations are investing in solutions that leverage runtime application monitoring integrated with secure development processes to facilitate efficient remediation.[14]

By using insights from runtime, developers can prioritize critical security issues based on exposure and usage, instead of wasting time on an issue that doesn't matter, such as fixing a software package that is not in use. This helps both for preventative hardening and for faster response to remediate new vulnerabilities, attacks, or threats.

It also optimizes efficiency for both development and security teams, reducing remediation time for developers and reducing the number of issues materializing in production for security teams to address.

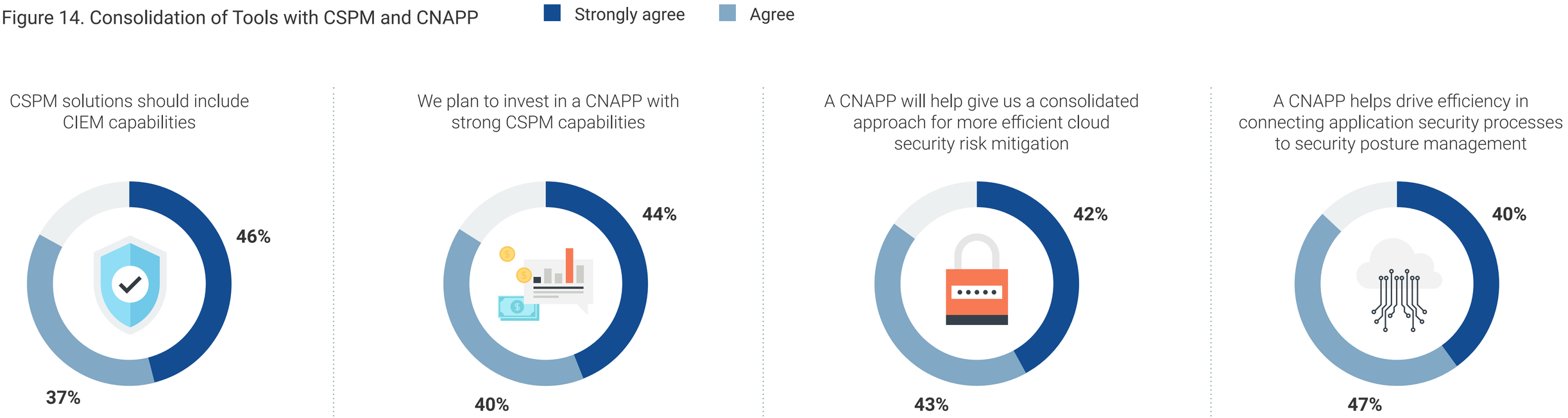
14. Source: Enterprise Strategy Group Research Report, *Walking the Line: GitOps and Shift Left Security,* November 2022.

BACK TO CONTENTS

Using a Platform for Efficiency

Organizations are looking to cloud-native application protection platforms (CNAPPs) to integrate cloud security monitoring with application security and DevOps processes. Most organizations believe the CNAPP should integrate CSPM and CIEM capabilities, as this will drive efficiency to proactively mitigate risk, while enabling efficient response to threats and attacks for effective cloud application protection.[15]

Figure 14. Consolidation of Tools with CSPM and CNAPP



15. Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023.

BACK TO CONTENTS

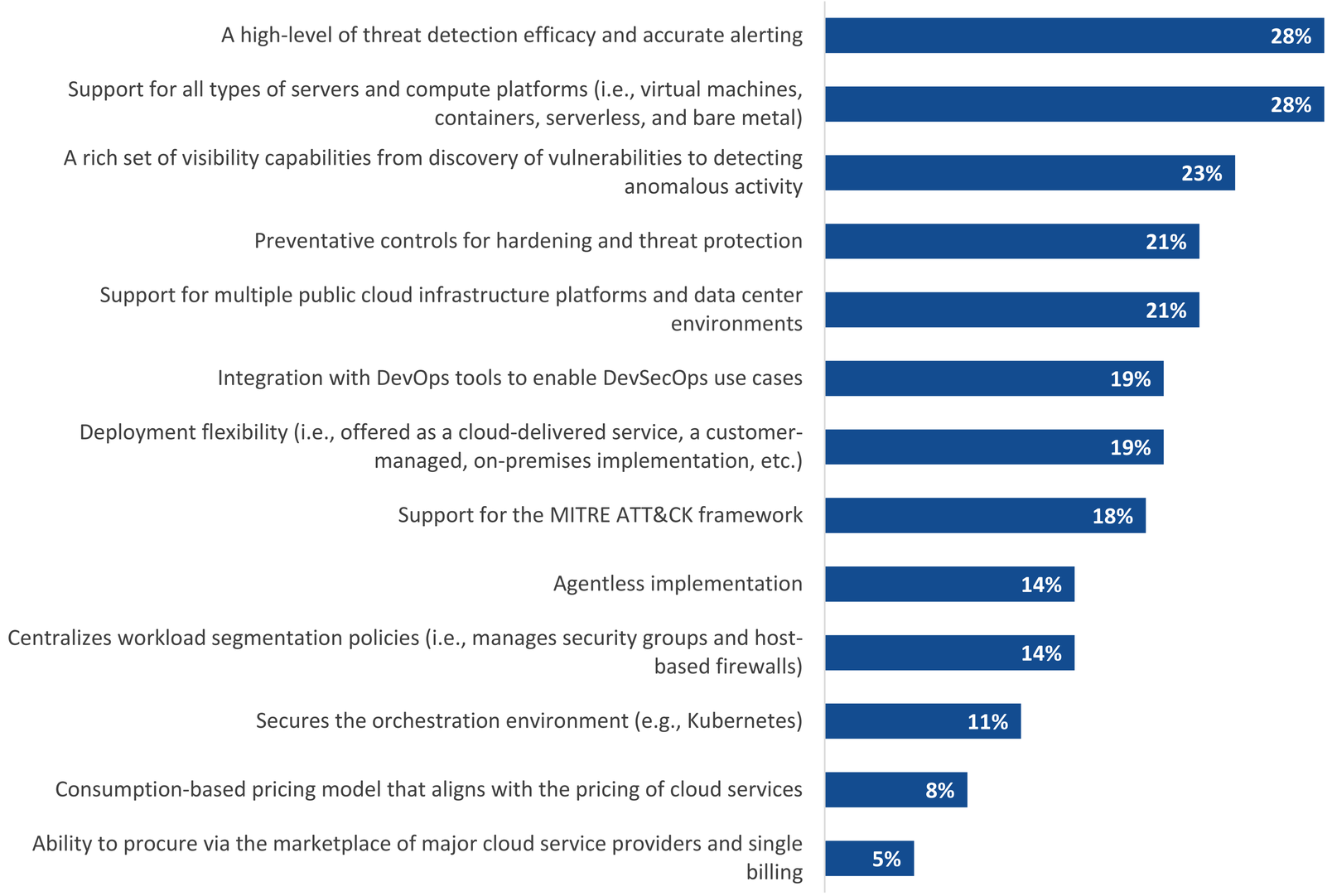
Key CNAPP Attributes

Enterprise Strategy Group research shows that organizations are looking for a CNAPP that will enable their security team to scale to support rapid growth.

The top attributes show the need for increased visibility and monitoring for high efficacy in threat detection and alerting. A CNAPP also needs to help organizations stay ahead of threats by identifying vulnerabilities and security issues across the cloud-native tech stack so they can mitigate security risk and exposure, while speeding response time to stay ahead of attacks and threats.[16]

This requires insights from visibility and monitoring in runtime to provide the context to drive efficient remediation across security and development teams.

Figure 15. Most Important CNAPP Attributes



16. Source: Enterprise Strategy Group Research Report, *Technology Perspectives from Cybersecurity Professionals*, May 2022.

BACK TO CONTENTS

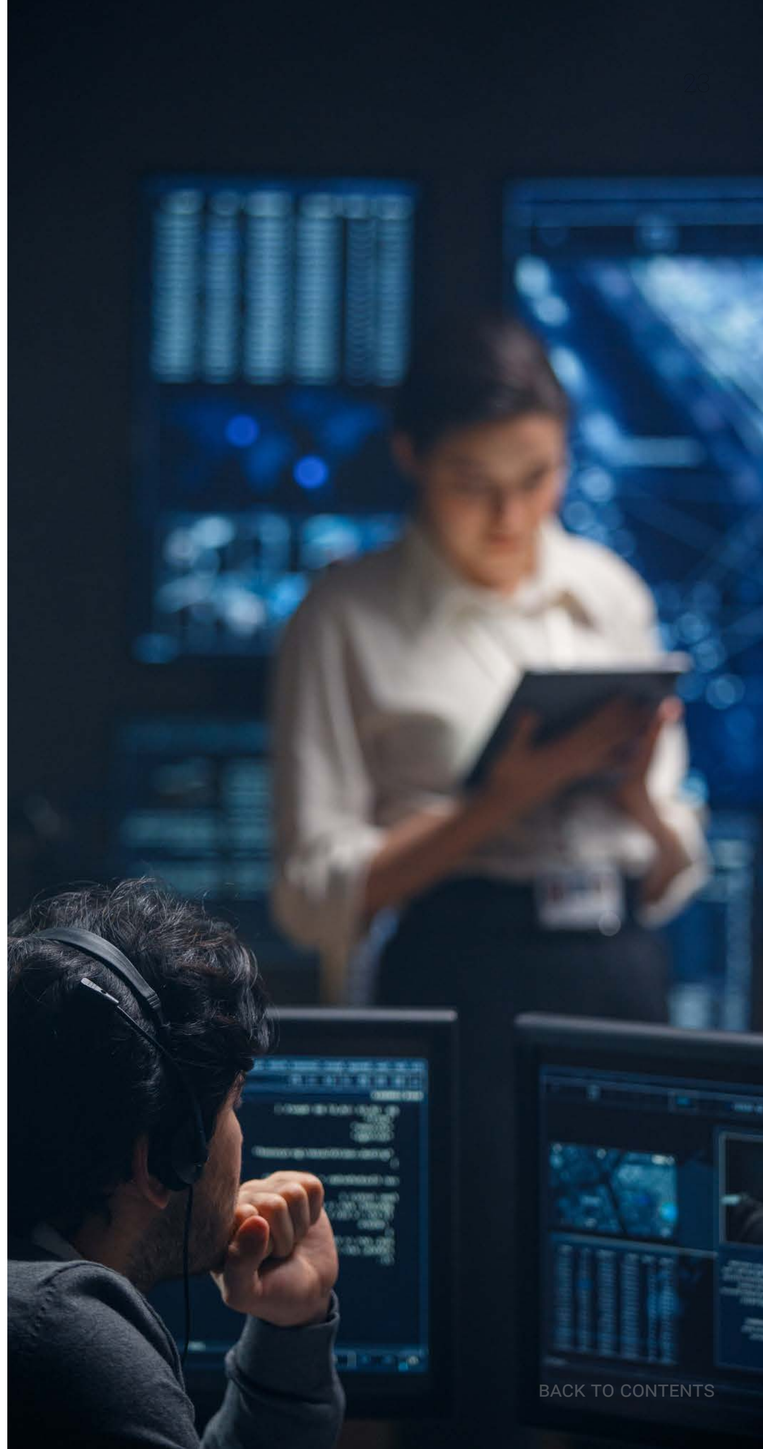
Conclusion

Using Sysdig on AWS for an Effective CNAPP That Leverages Runtime Insights

Organizations can use Sysdig to provide secure innovation on AWS, including Amazon ECS, Amazon EKS, and AWS Fargate. Leveraging deep runtime insights from the widely adopted Falco open source tool created by Sysdig as a security monitoring solution for hosts, containers, Kubernetes, and the cloud, the Sysdig CNAPP provides efficient detection, prioritization, and remediation for in-use vulnerabilities, misconfigurations, and permissions to prevent unauthorized access and attacks.

It provides:

- **Streamlined vulnerability management, reducing noise and prioritizing actions that have a high impact on reducing risk.**
- **Simplified CSPM with configuration management and compliance for standards and regulations.**
- **Reduced attack surface with CIEM to reduce risk from overprovisioned permissions and access.**
- **Faster threat detection and response with real-time monitoring, machine learning, and policies, while capturing detailed activity records for efficient investigation and response.**



BACK TO CONTENTS

sysdig | aws

Sysdig helps companies secure and accelerate innovation in the cloud. Powered by runtime insights, the cloud security platform stops threats in real time and reduces vulnerabilities by up to 95%. Rooted in runtime, the company created Falco, the open source solution for cloud threat detection. By knowing what is running in production, Dev and security teams can focus on the risks that matter most. From shift left to shield right, the most innovative companies around the world rely on Sysdig to prevent, detect, and respond at cloud speed.

Click below to learn more about Sysdig cloud security powered by runtime insights with AWS cloud services.

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

TechTarget's 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.

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.