Enterprise Strategy Group™
by TechTarget

WHITE PAPER

Using a CNAPP to Incorporate Security Throughout the Software Development Lifecycle

How to Use a Cloud-native Application Protection Platform (CNAPP) to Manage, Monitor, and Protect Software Applications

By Melinda Marks, Practice Director, Cybersecurity
Enterprise Strategy Group

September 2024

Contents

Executive Summary

As organizations use innovative technologies to optimize productivity and gain a competitive advantage, they have moved to cloud-native development processes to scale rapidly. However, it can be difficult for security teams to support enterprise applications that are often distributed across public and private cloud platforms and on-premises data centers. They need to ensure that they can consistently apply security controls to minimize security risk while rapidly detecting and responding to threats or attacks.

Also, as developers use continuous integration and continuous development (CI/CD) processes to quickly build, deploy, and update applications, security teams need to support them without slowing things down. But this is difficult because developers have moved to automated toolchains and processes when building their applications with microservices architectures using VMs, containers, serverless functions, and Kubernetes for orchestration. Security teams are challenged when supporting ephemeral assets across dynamic cloud environments because of the complexity and challenges in supporting rapid scale and growth. The higher volume and speed of releases means that it's easy to deploy security issues across these complex environments.

Organizations also realize the consequences a security breach can have on their business; many have already faced the negative impacts, including financial, brand reputation, downtime, customer loyalty, and data loss. Unfortunately, traditional security tools created to protect on-premises data centers and endpoints do not necessarily work for cloud infrastructure and cloud-native applications. While organizations typically have multiple security tools in place—including tools for setting policies, testing and scanning tools to catch and remediate misconfigurations and vulnerabilities, and tools to monitor running applications for security issues—they have faced challenges keeping up with the scale of releases and their associated security alerts. Although their solutions may generate needed alerts, organizations face cybersecurity incidents because it is difficult and time-consuming to analyze results and prioritize needed remediation actions in time to prevent or stop attacks.

As a result, organizations are turning to cloud-native application protection platforms (CNAPPs) for a unified, integrated approach to secure and protect cloud-native applications across the software development lifecycle, from development to production. Whereas using multiple tools from different vendors make it challenging for security teams to gain a complete view of risk, CNAPPs consolidate previously siloed capabilities, including container and configuration scanning, cloud security posture management (CSPM), infrastructure-as-code (IaC) scanning, runtime vulnerability assessment, and cloud workload protection.

This paper explores the benefits of adopting a CNAPP and what organizations should look for in an effective solution. Security teams need real-time visibility in their applications and possible attack surfaces. They also need to better incorporate security tools and processes into development processes without friction or disruption.

Organizations can also use a CNAPP to simplify processes to continuously meet compliance regulations such as HIPAA, PCI, and GDPR, leveraging automated compliance monitoring and reporting and enforcing security policies tied to those regulatory requirements.

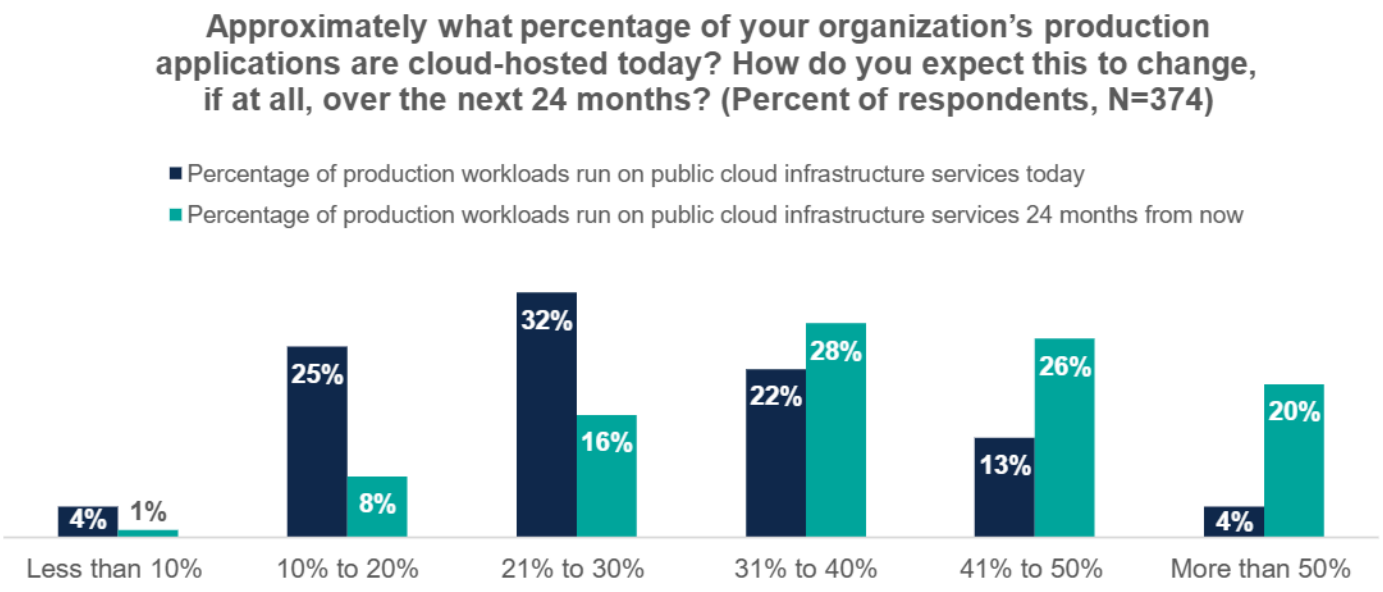
By having a centralized integrated approach correlating data and findings from multiple, previously siloed tools, a CNAPP gives security teams the context they need to work efficiently. This enables teams to effectively manage risk and respond rapidly to stay ahead of threats and attacks, reducing the number of security incidents that can damage their business.

Security Implications for the Move to Cloud-native Applications

Increasing Cloud Adoption with Modern Development Processes

Organizations are increasingly utilizing cloud services for digital transformation to raise software development productivity and scale; this enables them to focus resources on software development while using state-of-the-art cloud infrastructure from cloud service providers (CSPs). TechTarget's Enterprise Strategy Group research shows organizations are increasingly moving their production applications and workloads to public clouds (see Figure 1).[1]

Figure 1. Increasing Percentages of Production Workloads Run on Public Cloud Infrastructure



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

This enables them to increase productivity, streamlining the work needed to build and deploy software applications. Instead of setting up and managing hardware and infrastructure, organizations can focus on provisioning cloud infrastructure and workloads and building their software applications.

The cloud-native applications are typically built using a microservices architecture, connecting multiple services with any resources or data that it takes to run the applications that are connected via application programming interfaces (APIs). These can be easily deployed across different computing environments, including public or private clouds or on-premises data centers.

The research shows that most organizations host their applications across multiple cloud service providers, with the majority (66%) utilizing more than three CSPs (see Figure 2).[2]

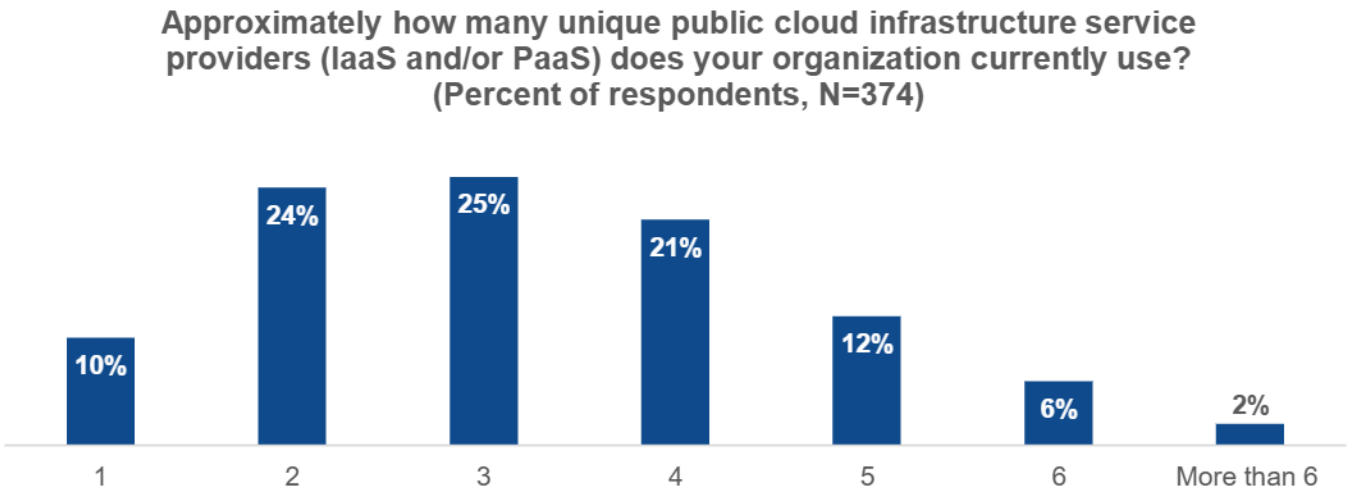
The reasons for using multiple CSPs vary, but most organizations choose CSPs aligned with application needs, business unit preferences, specialties within industries, or types of products.

Organizations have adopted DevOps processes to streamline and automate IT and operations. This empowers developers to efficiently provision and deploy their software applications instead of waiting for IT or operations to provision servers for them.

[1] Source: Enterprise Strategy Group Complete Survey Results, *2024 Cloud Security Platforms and DevSecOps*, June 2024.
[2] Ibid.

The research shows a majority (79%) are employing DevOps processes, including 34% who use it extensively, with an additional 9% planning to use DevOps processes and methodologies in the next 12-24 months to automate CI/CD processes.[3] With DevOps teams building CI/CD pipelines and workflows, developers can more quickly build and deploy their applications and then make software updates as needed. This is because they can efficiently work and collaborate by checking out code and checking it back in, with all changes made through the development pipeline.

Figure 2. Number of Unique CSPs



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

The Need to Adapt Security for Cloud-native Applications

Organizations moving workloads to the cloud need to adapt their security programs from traditional approaches. Instead of worrying about securing the hardware and computing infrastructure as they did for on-premises data centers, cloud computing offers a shared responsibility model in which the CSP is responsible for securing the cloud environment, while the organization must secure whatever it puts in the cloud, including the cloud infrastructure, workloads, and applications.

Securing the workloads organizations put in the cloud is often challenging for security teams adapting to cloud-native applications with loosely coupled microservices, connected to resources, such as data stores or other integrated applications. There are challenges with visibility and monitoring, as the assets are ephemeral and can be spun up and down on demand, often using containers or serverless functions, with Kubernetes orchestration. Also, while cloud-native development enables increased productivity, the higher speed and volume of releases and the

Adapting Security to Cloud-native Applications

The following properties of cloud-native applications pose challenges for security:

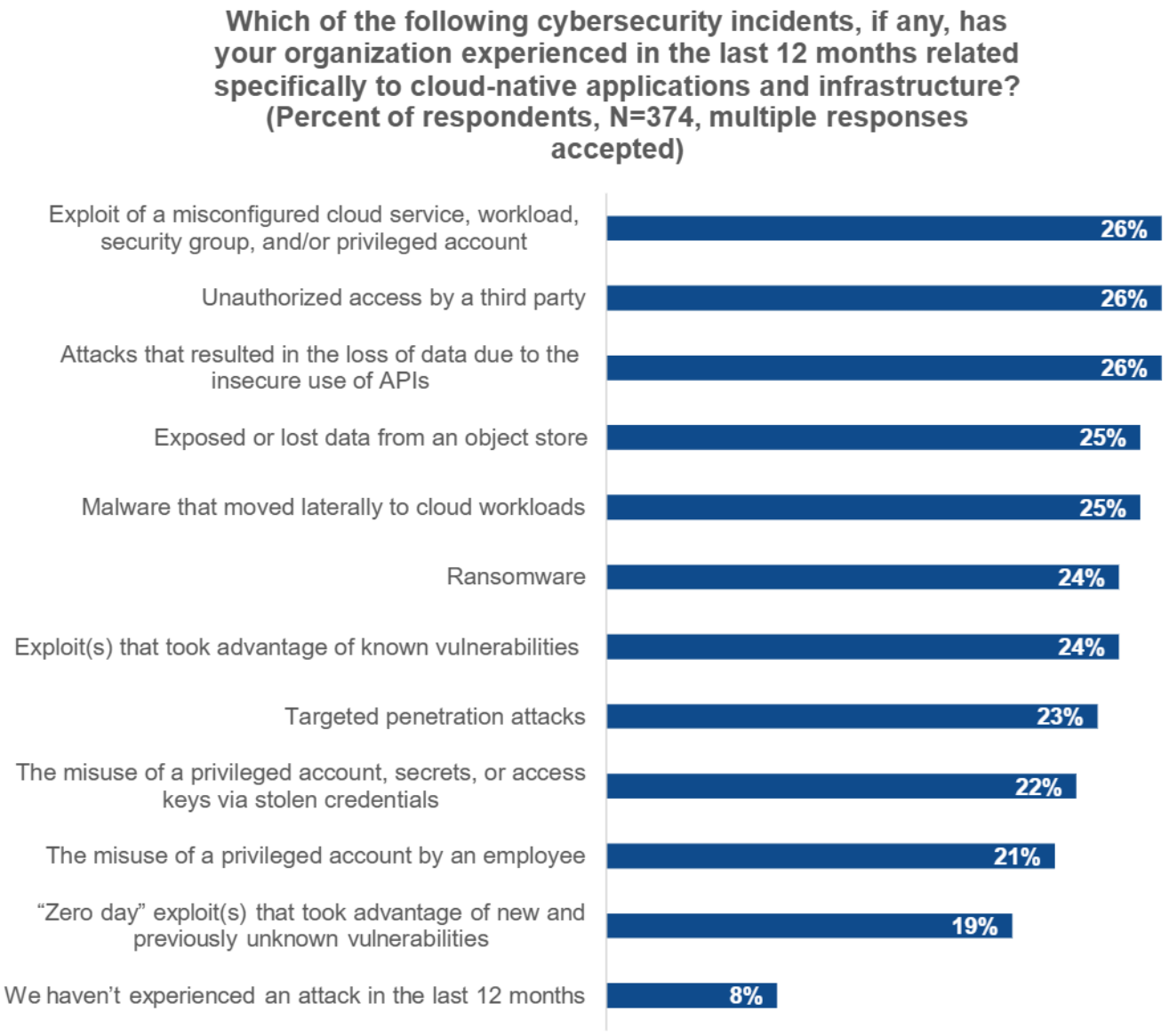
- Architected using loosely coupled microservices, via APIs.
- DevOps and CI/CD pipelines result in rapid, frequent updates.
- Dynamic workloads with Linux containers or serverless functions and Kubernetes orchestration.

[3] Ibid.

growth of development teams create more chances for mistakes that become vulnerabilities exposing organizations to risk of attacks.

The research shows that despite having security solutions deployed from early in development through runtime, a majority of organizations (92%) have suffered from cybersecurity incidents on their cloud-native applications over the past year (see Figure 3).[4]

Figure 3. Security Incidents Experienced in the Past 12 Months on Cloud-native Applications



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

These incidents were often caused by misconfigurations, including access and permission issues as well as application, service, and infrastructure configuration issues, often due to human error or mistakes. While respondents reported that they use a wide range of solutions to catch and remediate security issues, if the solutions

[4] Ibid.

are not integrated, they require time for teams to deploy, manage, and fine-tune to create the needed views of findings and results.

Organizations need a better way to manage risk with more context on which alerts need attention so they can prioritize needed remediation actions that have the highest impact on reducing security risk. Otherwise, organizations will continue to fall victim to security incidents despite heavy investments in security solutions.

Also, each tool generates alerts in silos, making it difficult to analyze and compare results, prioritize what needs attention, and determine remediation steps, including determining which owner can make the needed update or creating policies to set controls and guardrails to eliminate similar issues in the future.

The research showed multiple challenges related to keeping up with the speed and scale of cloud-native development, including:[5]

- 85% said their security team is challenged keeping up with the scale and pace of cloud-native development.
- 74% said they have multiple security tools in place but cannot remediate security issues fast enough to prevent incidents.
- 70% said their security team is overwhelmed with the number of tools they have to deploy and manage.

Organizations need a better way to manage risk with more context on which alerts need attention so they can prioritize needed remediation actions that have the highest impact on reducing security risk. Otherwise, organizations will continue to fall victim to security incidents despite heavy investments in security solutions.

The Need for Faster Cloud Detection and Response

Organizations also need efficiency for security operations to react quickly to threats and attacks. Enterprise Strategy Group research on cloud threat detection, investigation. and response (CDR) showed security operations are challenged with the complexity of securing cloud-native applications.[6] This is due to factors, including the higher speed and volume of releases and the complexity of the attack surface with highly distributed applications with microservices-based architectures using dynamic, ephemeral resources (see Figure 4).

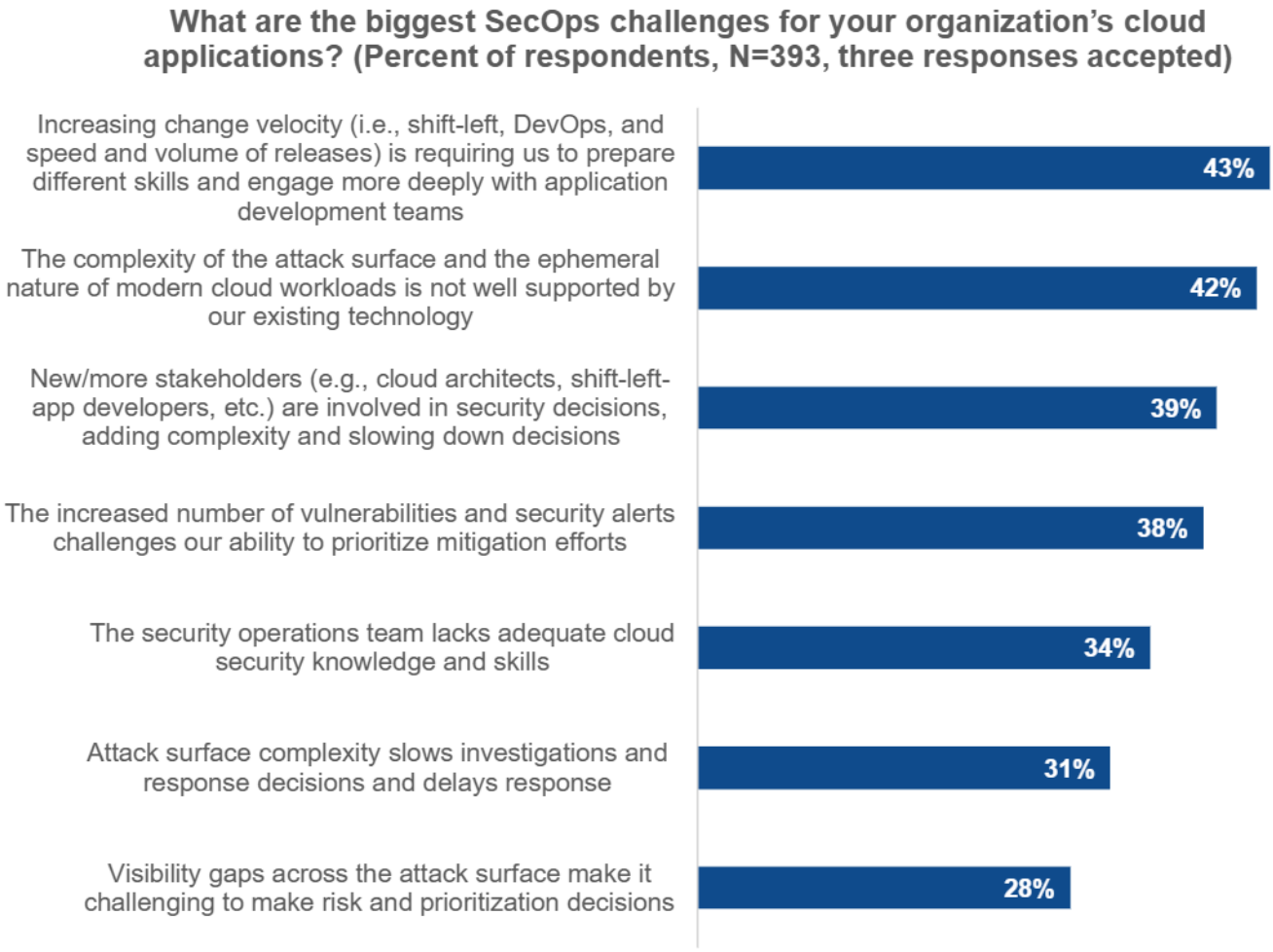
They also face challenges collaborating with more stakeholders across teams who may be involved in security processes. Each team may use siloed security tools and processes, with each tool generating separate alerts, making it difficult and time-consuming to handle the increasing volume of cloud application vulnerabilities.

Organizations reported that security operations teams are using a plethora of tools for cloud threat detection and response today that are separate from what cloud security and application security teams are using. For example, they may use extended detection and response (XDR) solutions, a dedicated SIEM (i.e., one dedicated to cloud security operations), a central SIEM (i.e., one with coverage that spans hybrid IT), third-party tools, CSP security tools, and dedicated CDR tools.

Also, typically, security teams have tried to extend existing security operations tools to the cloud, but they found that the differences mentioned earlier for cloud-native applications and the rest of their applications and infrastructure require different security policies and technologies. Also, 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.

[5] Ibid.
[6] Source: Enterprise Strategy Group Research Report, *Cloud Detection and Response*, December 2023.

Figure 4. Biggest SecOps Challenges for Cloud Applications

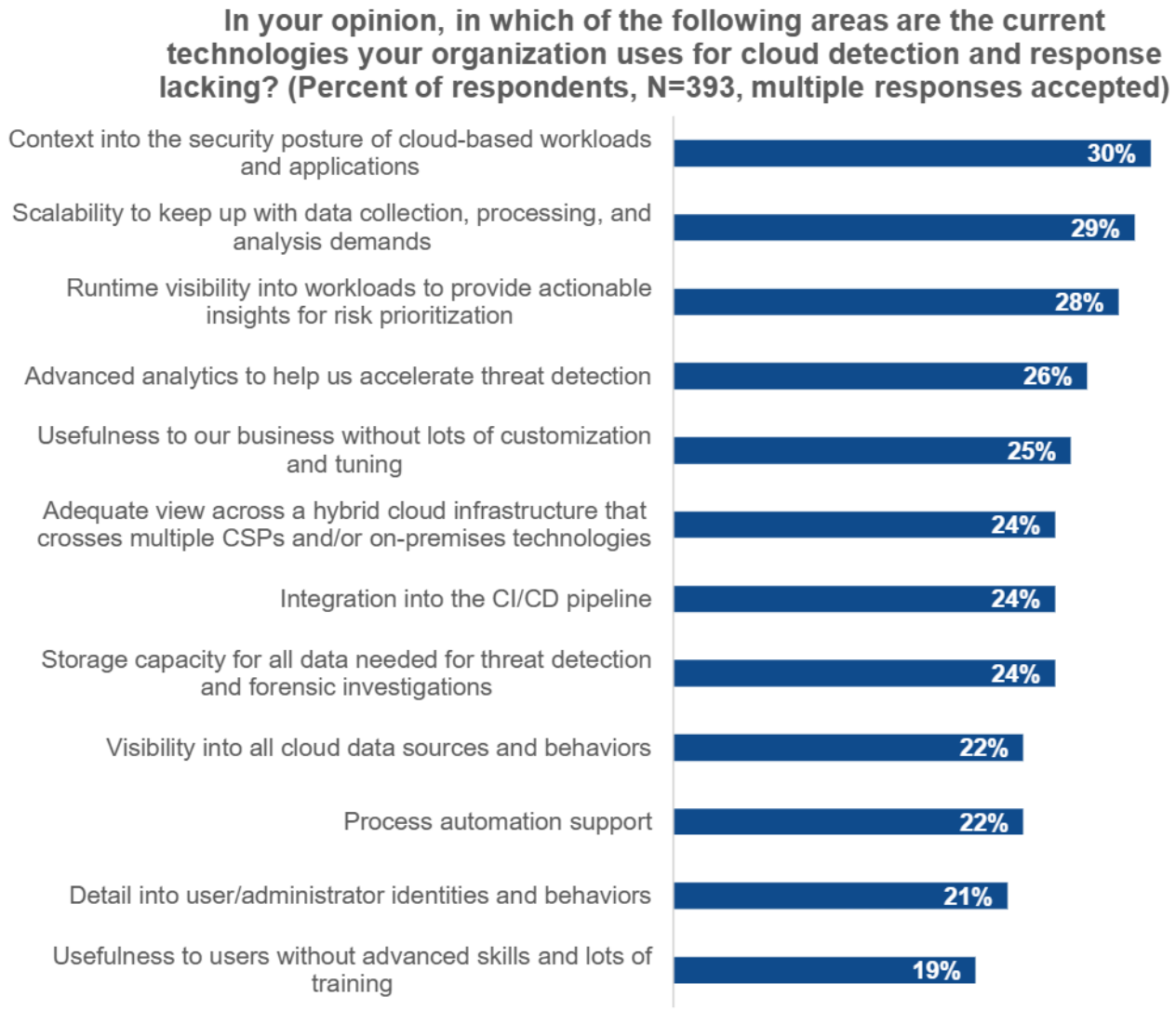


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

This has led to additional tool proliferation in areas like cloud security posture management, network segmentation, and anomaly detection. The research shows that despite their use of multiple tools, organizations have found that cloud security demands greater scale, rapid data analysis, and more process automation for detection and response. As a result, organizations recognize the need for improvements with cloud-based security posture context, scalability, runtime visibility into risk prioritization, advanced analytics, and intuitive business value for effective cloud detection and response (see Figure 5).[7]

[7] Ibid.

Figure 5. Areas Lacking for Cloud Detection and Response

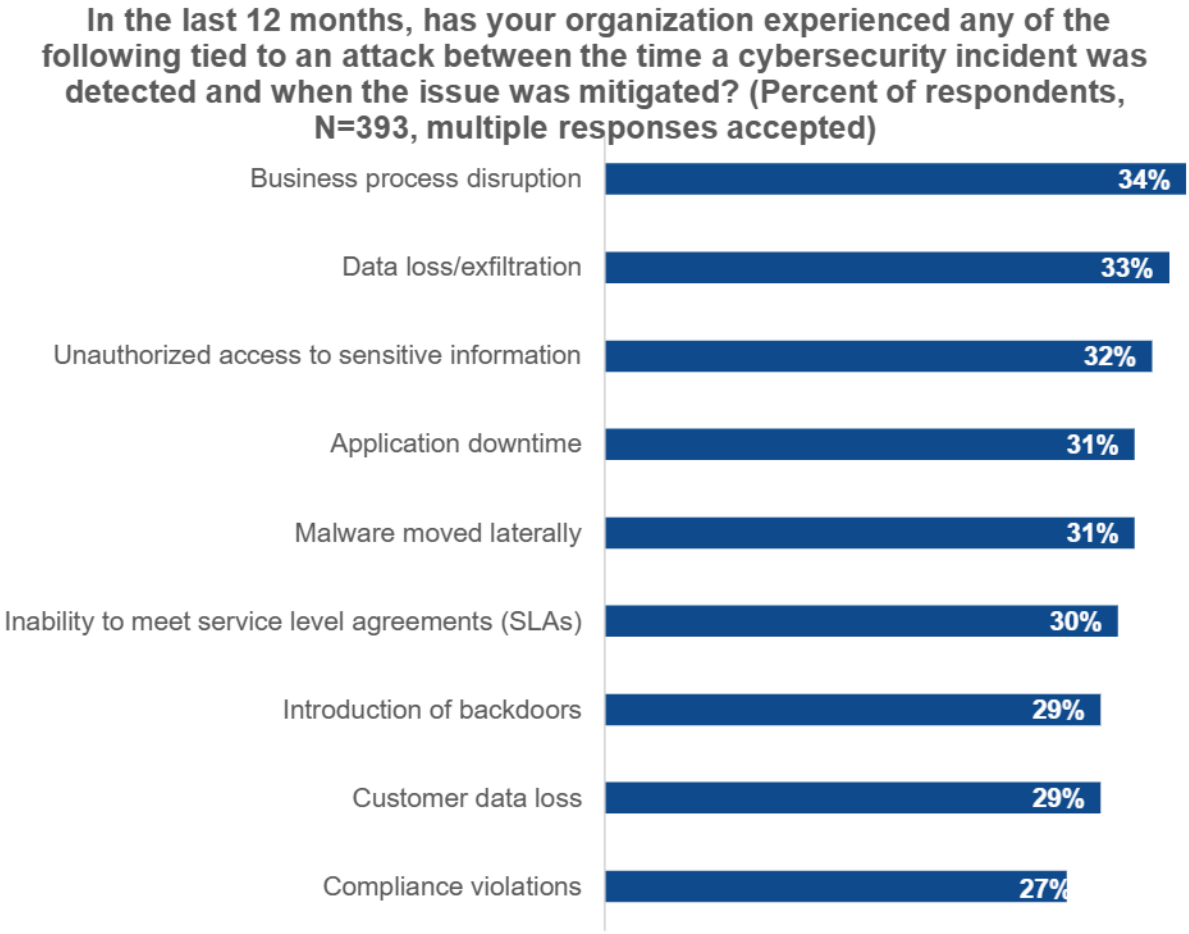


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

While organizations use various detection and response solutions, these mechanisms can experience significant challenges with data ingest, data normalization, correlation, and analysis, especially if needing to context switch between multiple tools. The delays enable attacks to advance and carry out malicious objectives before security teams are even aware of a threat.

In fact, the research also shows the need for efficiency and faster response times. When asked about the problems suffered between when incidents were detected and when the issues were mitigated, organizations suffered a range of impacts from delays, including business process disruption and application downtime, data loss or exfiltration, unauthorized access to sensitive information, customer data loss, and compliance violations (see Figure 6).

Figure 6. Impacts Occurring During Response Time



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

These incidents have strong impacts on the business and company reputation, so security leaders are seeking a better approach to ensure that they can support scale and growth.

This likely drives the interest we see in CNAPPs to consolidate tools for better visibility, greater context comparing results across tools, and increased efficiency to prioritize needed remediations. The right solution can better incorporate security tools and processes into development to help teams remediate security issues before the applications are deployed, or at least before an attacker can identify the exposure or vulnerability, and helps teams prevent security incidents.

Consolidating Cloud-native Security With a CNAPP

CNAPP Key Capabilities

We've reviewed how developers have gained advantages with modernized processes for automation, ease of deployment, and orchestration of cloud-native applications. But we've also seen how security teams have struggled keeping up. Security leaders recognize the need to take a proactive and more holistic approach to monitoring, managing, and protecting their cloud-native applications to prevent security issues and to respond quickly if they do occur.

CNAPPs have emerged as unified, tightly integrated sets of security and compliance capabilities designed to secure and protect cloud-native applications. Most CNAPPs are cloud-based, as-a-service offerings, with integrations into runtime cloud environments and development pipeline tools used by the development organization.

Having an effective solution in place makes security a valuable partner for other teams, including IT, operations, and business owners, who can align to ensure application resilience and security and enable business growth.

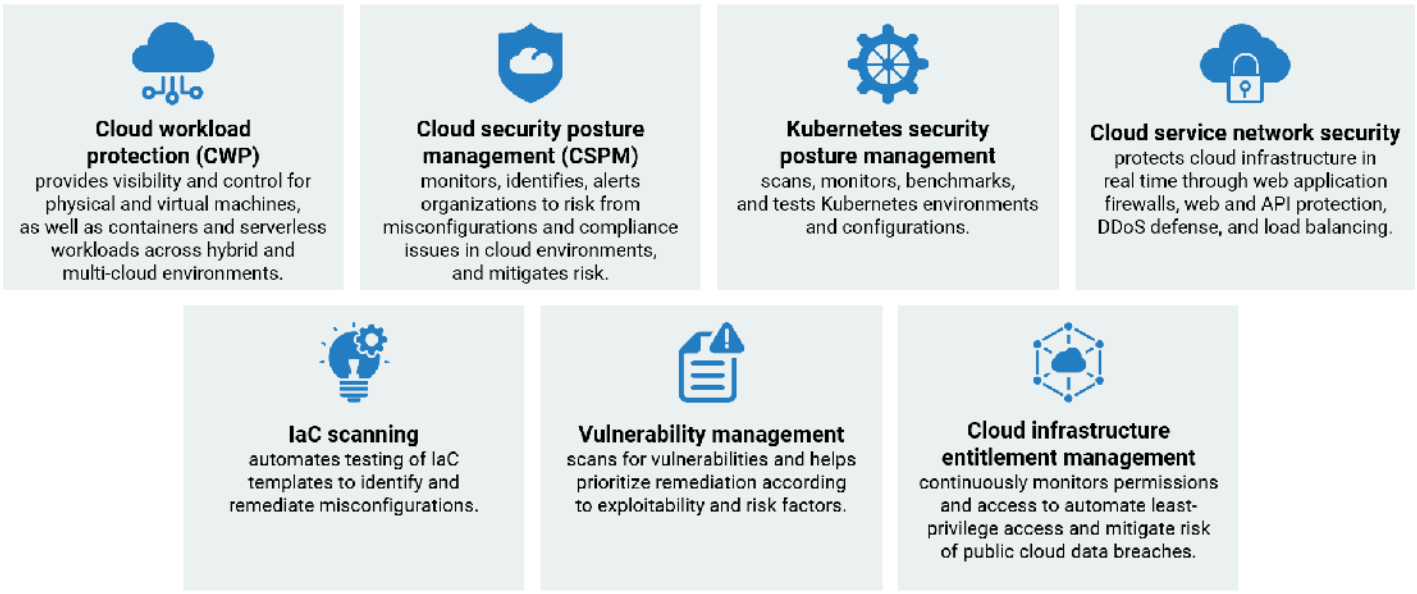
While the capabilities continue to be defined and vendor CNAPP offerings may vary, organizations should look for solutions that can integrate visibility, assessment, and remediation by leveraging DevOps processes to better integrate security to mitigate risk.

A CNAPP should help security teams identify and remediate vulnerabilities as early as possible in the software development lifecycle, accelerate remediation, and provide consistent and continuous security and compliance monitoring.

Traditionally, tools have been siloed with three things: build-time security policies, application security testing tools to catch and remediate issues before applications are deployed, and cloud security posture management and cloud monitoring tools to catch issues in runtime.

Instead, a CNAPP solution helps security teams integrate their program from build time to run time for a full software development lifecycle approach. A CNAPP is defined as a cloud security solution that provides full-stack security through multiple components (see Figure 7).

Figure 7. CNAPP Components



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

The key value proposition for CNAPP solutions is to deliver an integrated set of capabilities for visibility and control to optimize collaboration among security, business, and IT teams, from setting policies and automating security testing processes, to CSPM and CDR capabilities.

Having an effective solution in place also makes security a valuable partner for other teams, including IT, operations, and business owners, who can align to ensure application resilience and security and enable business growth.

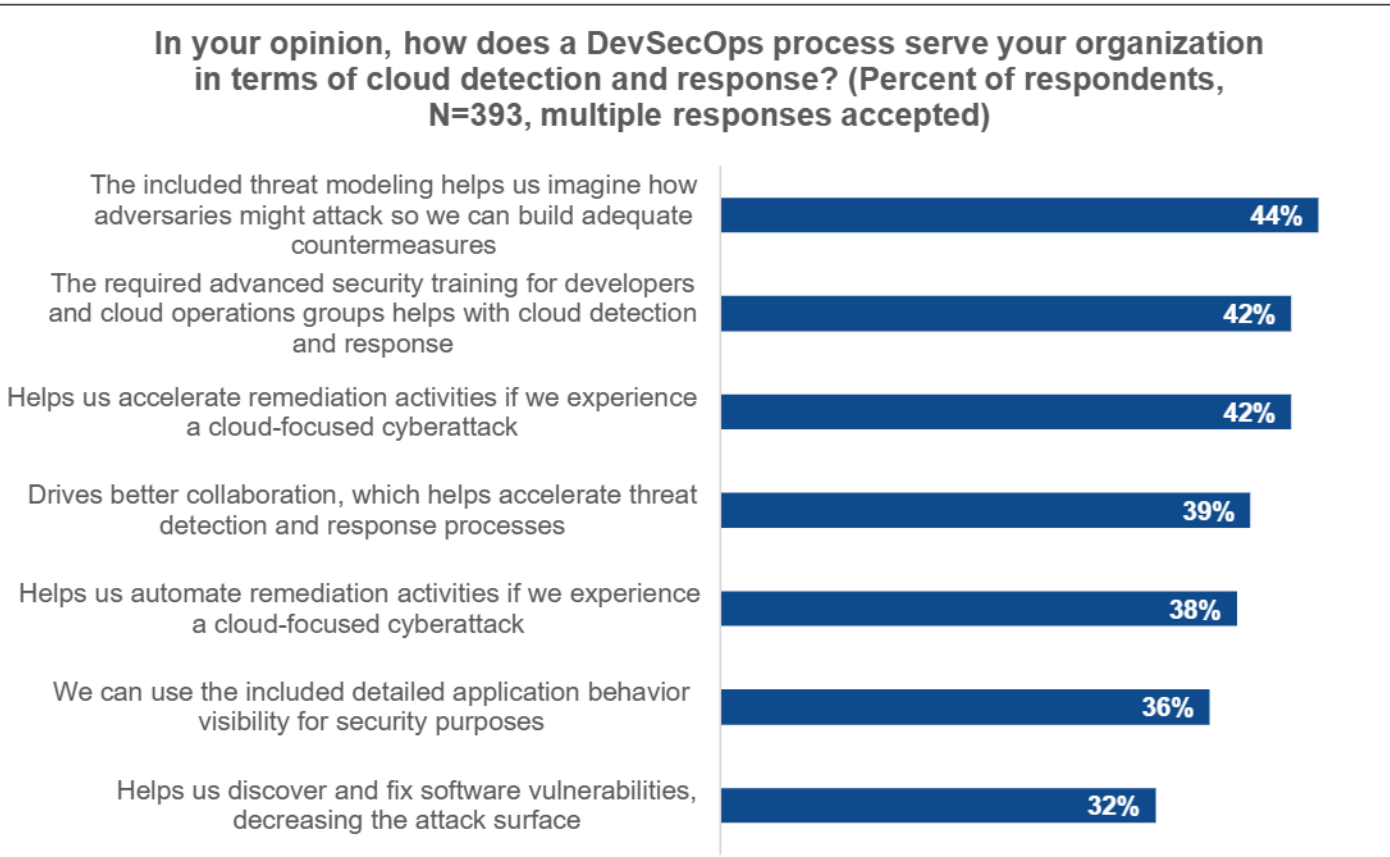
The Importance of the Platform in Integrating Security

Organizations need to look for a platform that gathers and normalizes data from multiple sources, including data from CSPs and multiple security capabilities and tools, to provide a single source of truth to help drive efficiency across the full security lifecycle.

This helps security teams gain the context they need to efficiently address and remediate critical issues, including understanding the issue and its possible impact, assessing overall risk for the organization, determining the right owner, and driving the needed mitigation action, including steps to further reduce risk, such as setting new policies.

When multiple teams can utilize the platform, it drives goal alignment and efficiency across the software development lifecycle, from helping developers and application security teams secure applications before they are deployed to helping security operations teams rapidly remediate issues or speed up threat investigations and response. For example, the research showed that SecOps teams recognize the benefits of incorporating security processes into development (DevSecOps) to drive efficiency and speed for more effective cloud detection and response (see Figure 8).[8]

Figure 8. How DevSecOps Helps With Cloud Detection and Response



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

Also, as multiple teams, including IT and operations, set policies, a common platform can optimize efficiency and reduce duplication of work. Threat modeling and an understanding of how attackers could utilize exposures with attack path analysis also helps drive efficient remediation to reduce risk and thwart attacks.

[8] Ibid.

Organizations should look for a CNAPP that provides:

- **A centralized platform with integrated capabilities** to gather data and telemetry from multiple sources; normalizing the data with comparisons for greater context helps prioritize alerts and needed remediation to improve security operations efficiency.
- **Centralized management for setting security policies and controls** for cloud-native applications across environments, leveraging automation to minimize tedious manual tasks.
- **Complete visibility with full coverage** of all applications, application performance, resource use, and security threats, from development to runtime, to help IT and security teams quickly detect issues.
- **Rapid remediation for threat detection and response** helps teams more easily identify and remediate security threats in real time with speed and accuracy.
- **Automated compliance monitoring and reporting** helps teams proactively and continuously adhere to regulations instead of scrambling periodically for audits; this ensures organizations meet compliance requirements and avoid fines or legal actions.

Using a CNAPP with these key capabilities can help security teams effectively collaborate with other teams to support cloud-native development to enable business growth.

Harnessing the Power of AI

Organizations need the right solutions to help teams work efficiently; reduce tedious, manual work; and fully leverage staff resources. Enterprise Strategy Group research shows that organizations most commonly face a skill shortage in cybersecurity, with 45% of organizations saying they have a problematic shortage of cybersecurity and cloud security skills.[9]

There is an opportunity for CNAPPs to use AI to eliminate tedious manual tasks so security teams can optimize efficiency. For example, CNAPPs can utilize machine learning to process and analyze large volumes of data and recommend or automate needed remediation or blocking actions; they can also employ generative AI to assist with detection and response, including forensics investigation queries. The stronger the capabilities, the more data can be considered for the full context and intelligence to drive needed outcomes, mitigate risk, and respond quickly to threats and attacks.

Using SentinelOne Singularity Cloud Security for a Comprehensive AI-powered CNAPP

Organizations are using Singularity Cloud Security to gain complete visibility of cloud-native applications, combining agentless insights and visibility with real-time, agent-based threat protection and response to deliver a comprehensive, AI-powered CNAPP. It enables teams to optimize efficiency to support scale and growth, providing:

- **Instant visibility and coverage** for full discovery and monitoring of cloud assets for vulnerabilities across computing environments to discover and remediate vulnerabilities in cloud-native applications without the need to install agents.
- **Comprehensive CNAPP capabilities supporting secure development**, including IaC scanning, container and Kubernetes security posture management, policy controls, secrets and cloud credential leakage detection, malware scanning, and compliance monitoring and reports.
- **AI-powered insights and protection with Purple AI,** which analyzes and correlates data and automates remediation or blocking to defeat attacks as they happen to protect cloud-native applications.

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

- **Automated red teaming with offensive security engine to stay ahead of attacks**, leveraging Verified Exploit Paths™ to safely simulate attacks on cloud infrastructure and analyze the data; this verifies possible attack paths and identifies vulnerabilities that are exploitable and ensures needed remediations are prioritized.
- **A unified platform that optimizes efficiency to stop or mitigate incidents** by consolidating and normalizing native and third-party security data into Singularity Data Lake for a unified source of truth. This is useful for root cause analysis and blast radius analysis for rapid response, as incidents may start on premises and cut across endpoints, identities, and cloud infrastructure.
- **Simplified compliance and reporting** to continuously keep up with industry regulations.

Conclusion

As organizations increasingly leverage cloud services and cloud-native development processes to increase productivity and best serve their customers, security needs an effective approach that can support rapid growth and scale. Security teams have been challenged to adapt their security programs to meet the needs of cloud-native applications with faster development lifecycles and are facing difficulties monitoring and securing highly dynamic, microservices-based applications with ephemeral infrastructure and resources. Organizations have also made the mistake of adding multiple siloed tools—which generate too many alerts to process—and are falling victim to attacks because they could not address security vulnerabilities in time.

As organizations turn to CNAPPs to consolidate their previously siloed tools to more effectively manage risk, they should consider SentinelOne Singularity Cloud Security. It provides a unified AI-powered security platform that gathers and normalizes data from multiple sources to deliver AI-powered insights and protections. Organizations can leverage the platform to easily gain full visibility of applications across environments, better incorporate security into development processes, and utilize its offensive security capabilities, including Verified Exploit Paths. It helps security teams optimize efficiency and ensure that they can scale to protect their cloud-native applications and support business growth.

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