Enterprise Strategy Group™
by TechTarget

Converging Cloud Security With Enterprise Security Operations

Driving Efficiency for Risk Management and Rapid Response

By Melinda Marks, Practice Director
Enterprise Strategy Group

February 2024

Contents

Executive Summary

Organizations continue to move production workloads to public cloud infrastructure to optimize efficiency and productivity and deliver software applications. This migration, however, places heavy demands on security, as more applications, data, and resources running in cloud environments increase overall risk, with higher chances for mistakes, greater attack surface area, and a rapidly evolving threat landscape.

Managing risk across multi-cloud environments is further complicated by the siloed nature of security practices, with proactive cloud security teams working separately from enterprise security operations (SecOps) teams. They use different tools with different data models or repositories feeding their views and dashboards, and they follow different processes when responding to issues.

Without a unified view of issues or activity and with data distributed across separate tools, cross-team collaboration becomes difficult. As a result, cloud security and SecOps practices can become highly inefficient and consume already scarce security talent. Without common views and workflows that bridge proactive and reactive security measures, it becomes difficult and time-consuming to reduce the backlog of unresolved security issues. This often creates a higher volume of open issues, leading to greater overall risk.

This is also damaging as organizations face threats and attacks. Critical cloud risk information derived from technologies such as attack path analysis and dynamic risk scoring cannot easily be shared across teams. As a result, teams often need to spend extra time and manual effort to determine the risk for each security finding and to devise the proper remediation strategy.

This paper examines the need to bridge the gap between proactive and reactive security with the convergence of cloud security—including posture management, compliance monitoring, and threat detection—and enterprise security operations solutions for rapid threat detection, investigation, and response.

Effective cloud security against cyberattacks requires a common data and operating platform to efficiently manage the full security lifecycle, from prevention and detection to investigation, response, and remediation. By converging cloud security with enterprise security operations, organizations gain the efficiency and cross-team collaboration needed to effectively manage risk and rapidly respond to critical issues in any cloud environment as development scales with cloud adoption.
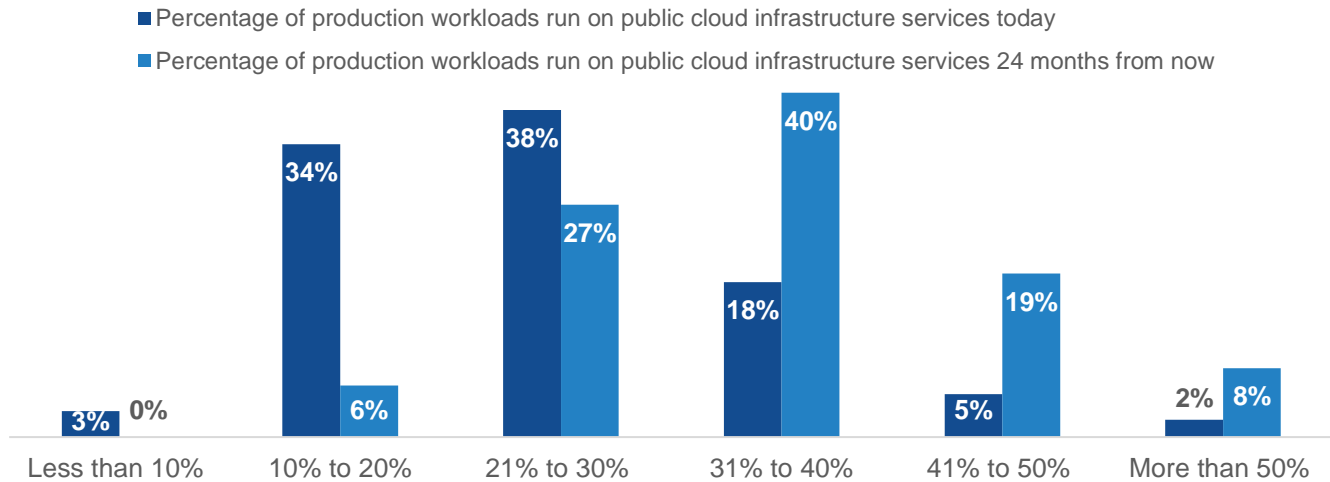
The Move to the Cloud Increases Risks

Organizations are increasingly moving production workloads to cloud-hosted infrastructure. In fact, research from TechTarget's Enterprise Strategy Group shows that, while only a quarter of organizations run more than 30% of their production workloads on public cloud infrastructure today, this is expected to increase dramatically over the next two years. Specifically, by 2025, nearly 7 in 10 organizations (67%) anticipate that more than 30% of their production workloads will run on public cloud infrastructure (see Figure 1).[1]

---

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

Figure 1. Cloud-hosted Production Applications Expected to Increase Over the Next Two Years

Approximately what percentage of your organization's production applications are cloud-hosted today? How do you expect this to change, if at all, over the next 24 months? (Percent of respondents, N=393)

■ Percentage of production workloads run on public cloud infrastructure services today
■ Percentage of production workloads run on public cloud infrastructure services 24 months from now

	Less than 10%	10% to 20%	21% to 30%	31% to 40%	41% to 50%	More than 50%
Today	3%	34%	38%	18%	5%	2%
24 months from now	0%	6%	27%	40%	19%	8%

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

As organizations move applications to cloud infrastructure, they need to ensure that security can scale to keep up so that they can efficiently and effectively manage the risks for their cloud-hosted applications and data.

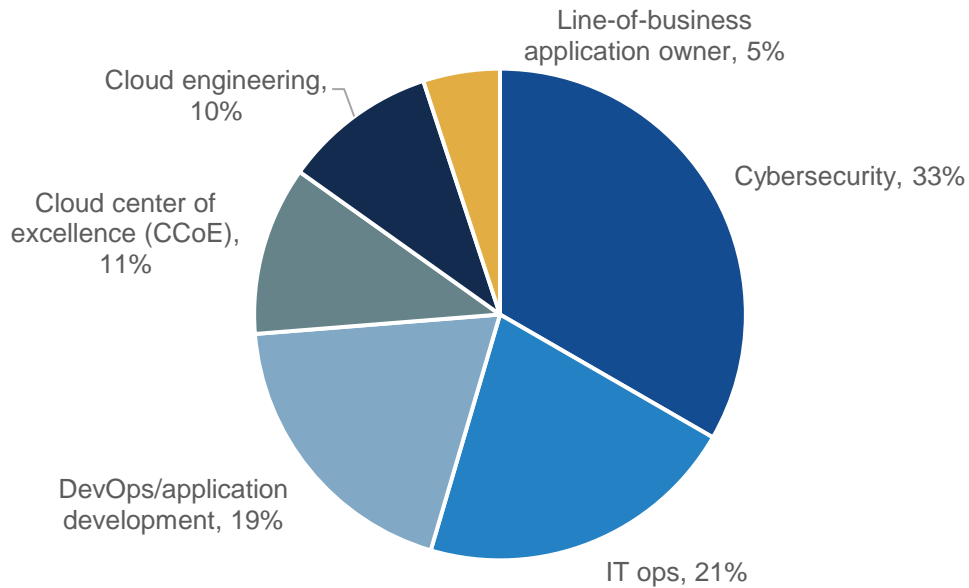## The Complexity of Managing Security Across Teams

Enterprise Strategy Group research shows that the responsibility for securing cloud-native applications and managing risks to the business may fall under several groups. For example, organizations may add cloud security skills and personnel to their existing IT and/or security teams, with dedicated responsibility for cloud, or it could fall to the cloud center of excellence, cloud engineering, or DevOps and developer teams (see Figure 2).[2]

These teams typically use cloud security posture management (CSPM) tools from their cloud service providers or security vendors to manage cloud-native security risk across cloud workloads, including gaining visibility of workloads and their related resources, checking for misconfigurations and security issues, and setting policies and controls to mitigate risk.

---

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

Figure 2. Security Responsibilities for Cloud-native Applications and Infrastructure

Which of the following groups are the budget holder and thus final decision maker for purchasing identity and access management products for securing access to your organization's cloud applications and services? (Percent of respondents, N=383)

Line-of-business application owner, 5%

Cloud engineering, 10%

Cloud center of excellence (CCoE), 11%

Cybersecurity, 33%

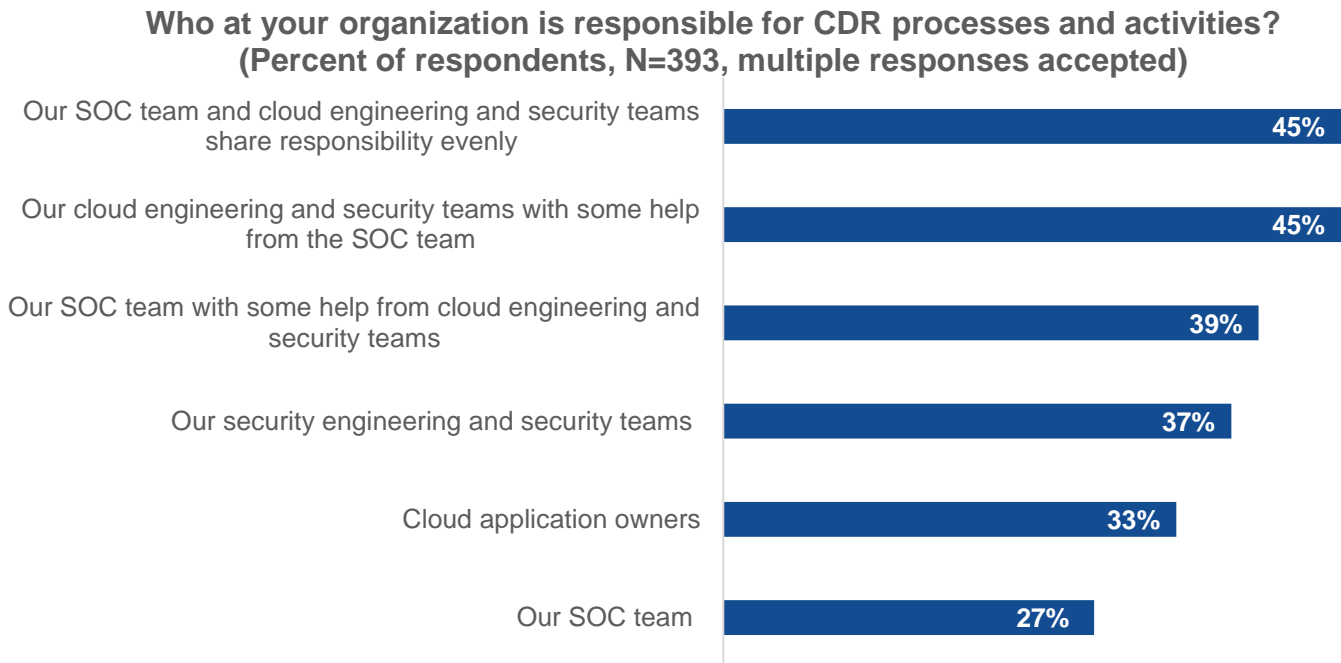DevOps/application development, 19%

IT ops, 21%

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

However, cloud threat detection, investigation, and response (CDR) typically involves the security operations center (SOC), staffed by security analysts who are typically responsible for detection and remediation of cyberthreats. They typically cover on-premises data centers, endpoints, and cloud environments. According to Enterprise Strategy Group research, SecOps teams typically work with the other teams, including security and cloud engineering teams, for CDR (see Figure 3).[3]

---

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

Figure 3. CDR Responsibilities Are Typically Shared Across Security, Cloud Engineering, and SOC

Who at your organization is responsible for CDR processes and activities?
(Percent of respondents, N=393, multiple responses accepted)

Our SOC team and cloud engineering and security teams share responsibility evenly	45%
Our cloud engineering and security teams with some help from the SOC team	45%
Our SOC team with some help from cloud engineering and security teams	39%
Our security engineering and security teams	37%
Cloud application owners	33%
Our SOC team	27%

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

Undoubtedly, there is additional complexity when managing security operations for cloud applications and infrastructure as compared with on-premises environments where applications and their owners are clearly mapped to physical infrastructure. This likely contributes to the difficulty in assigning accountability to the security challenges faced by organizations that are increasingly using cloud-hosted applications and infrastructure.
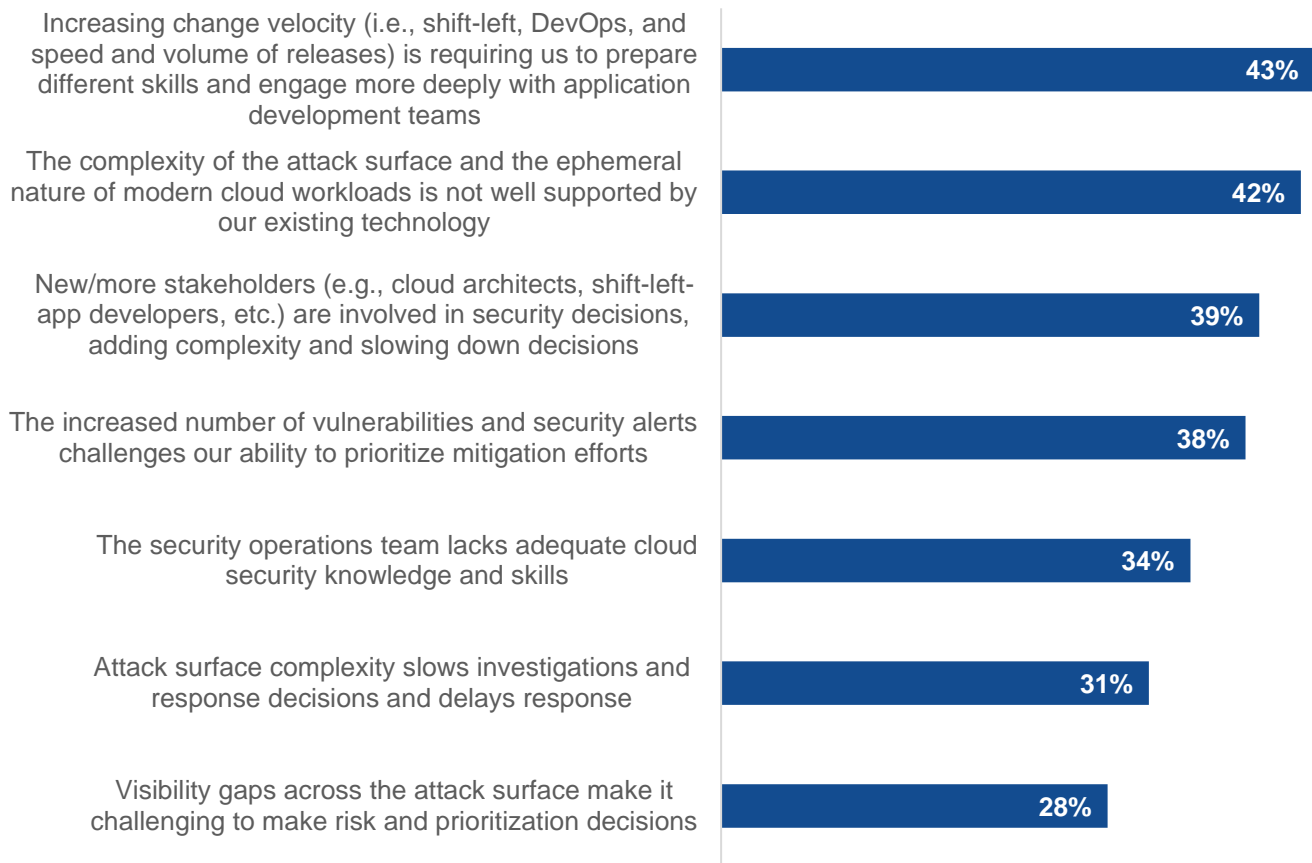
Siloed Tooling Creates Challenges for CDR

Organizations are using a plethora of tools for CDR today, including extended detection and response (XDR), 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, CSPM tools, and dedicated CDR tools.

This should make it easier for teams to detect security issues, including vulnerabilities, misconfigurations, access issues, anomalous activities, and lateral movement for threat detection, investigation, and response. So why are organizations facing security incidents and challenges with CDR? A deeper look at Enterprise Strategy Group research reveals the top SecOps challenges for CDR (see Figure 4).[4]

---

[4] Ibid.

Figure 4. Biggest SecOps Challenges for Cloud Applications

What are the biggest SecOps challenges for your organization's cloud applications? (Percent of respondents, N=393, three responses accepted)

Increasing change velocity (i.e., shift-left, DevOps, and speed and volume of releases) is requiring us to prepare different skills and engage more deeply with application development teams	43%
The complexity of the attack surface and the ephemeral nature of modern cloud workloads is not well supported by our existing technology	42%
New/more stakeholders (e.g., cloud architects, shift-left-app developers, etc.) are involved in security decisions, adding complexity and slowing down decisions	39%
The increased number of vulnerabilities and security alerts challenges our ability to prioritize mitigation efforts	38%
The security operations team lacks adequate cloud security knowledge and skills	34%
Attack surface complexity slows investigations and response decisions and delays response	31%
Visibility gaps across the attack surface make it challenging to make risk and prioritization decisions	28%

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

Increasing Change Velocity Requires Work With Application Development

Organizations are leveraging cloud services and modernizing their application development processes, using continuous integration and continuous delivery (CI/CD) to rapidly deliver applications and continuously update them with new capabilities, features, and/or corrections to their code. As application teams autonomously and rapidly produce new workloads or data stores in cloud environments, they may be introducing vulnerabilities. Also, as development teams scale, there is a higher chance for mistakes. This increases the risk of vulnerabilities that could be exploited by bad actors to compromise workloads or other assets in the cloud environment.

Does their SecOps and cloud security tooling give them sufficient visibility of these vulnerabilities to rapidly remediate and close security gaps—before applications are moved to production? Often they cannot, as SecOps tooling is still focused on detecting, investigating, and remediating threats—not vulnerabilities. The cloud security teams should be working closely with DevOps and development teams, but SecOps for cloud applications also requires working more closely with development to optimize response.

Attack Surface Complexity and Multiple Stakeholders

It is challenging for existing SecOps tools to support cloud environments because of the complexity of the attack surface, including APIs, access points, workloads, and developer tools. The needed cloud security data often resides within different security tools or cloud security platform tools used by multiple teams, including cloud security, application security, DevOps, and developer teams. This makes it difficult for SecOps tools to access and analyze the data and provide the needed context for security analysts.

While the cloud security teams may be working with other groups to help with risk and security posture management to prevent security issues and harden workloads against possible attacks, their tools are typically separate from the SecOps teams tools for investigation and response. In other words, there is no common data platform for cloud security and SecOps to drive efficiency for an effective, holistic security program.

A platform unifying posture management with threat detection and response combines prevention with rapid detection and response capabilities to improve collaboration and optimize efficiency.

Automation and assistive tools, including generative AI, can provide the full context and intelligence to mitigate risk and respond quickly to threats and attacks.

Increased Number of Vulnerabilities

When vulnerabilities are detected by the cloud security team and passed to SecOps, it results in too many alerts to assess and prioritize, often at a massive scale. Enterprise Strategy Group research shows that organizations often must wade through hundreds or thousands of security findings each month. The result: High percentages of alerts must be ignored because teams don't have time to investigate them (see Figure 5).[5]

---

[5] Ibid.

Figure 5. High Volume of Alerts Resulting in High Percentages of Alerts Ignored

Within your organization's cloud environment(s), approximately how many security alerts would you estimate that your organization generates on a monthly basis? (Percent of respondents, N=393)

Fewer than 50	50 to 250	251 to 1,000	1,001 to 5,000	More than 5,000
8%	28%	43%	19%	2%
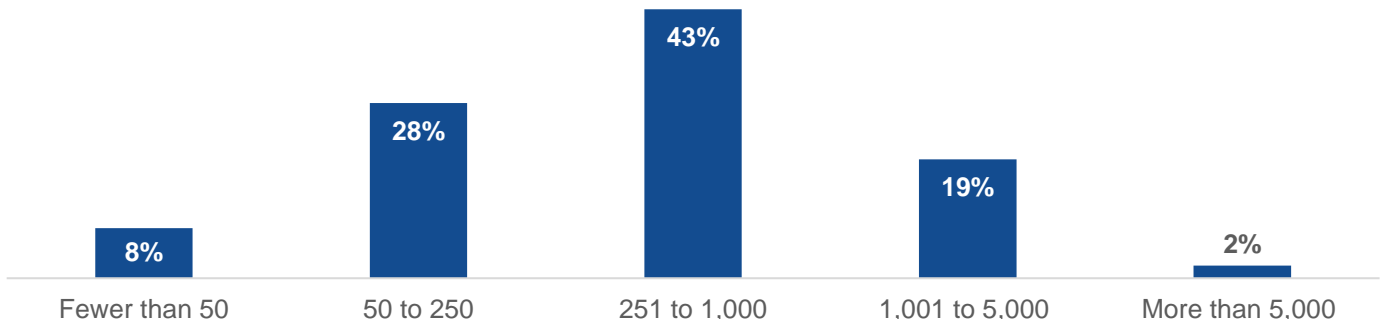
Approximately what percentage of the overall volume of security alerts in your organization's cloud environment(s) do you believe your organization/MSP ignores because it is impractical to investigate every

Less than 10%	10% to 25%	26% to 50%	51% to 75%	More than 75%
6%	22%	48%	22%	2%
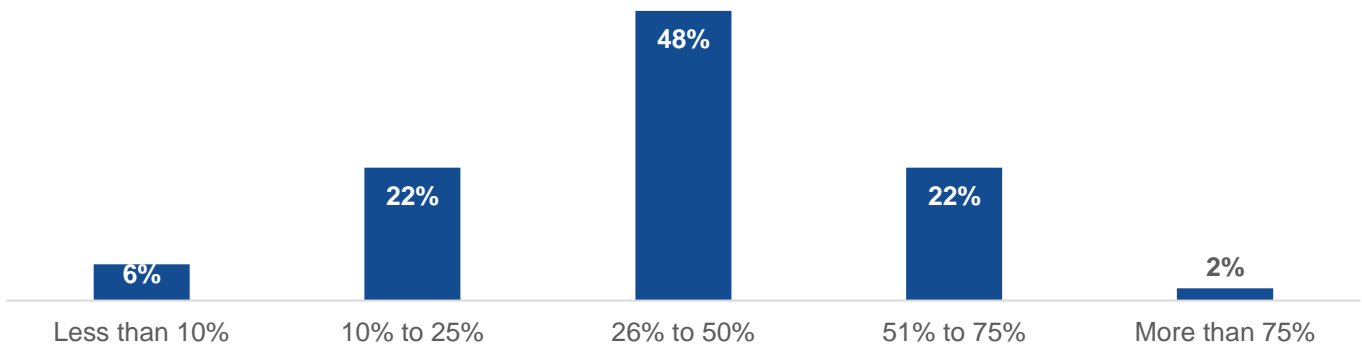
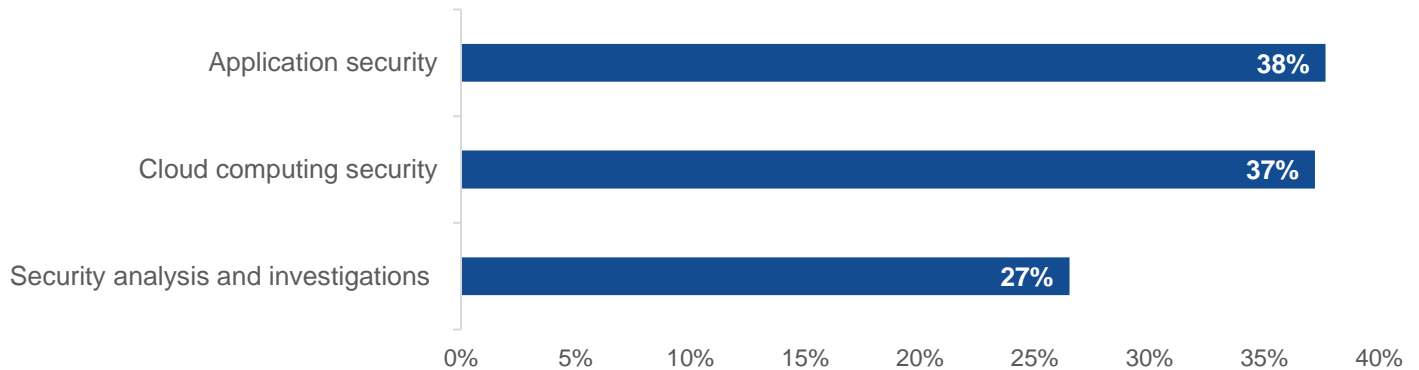*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

Security Operations Lacks Cloud Knowledge and Skills

According to Enterprise Strategy Group research, the top SecOps challenges include a lack of cloud knowledge and skills, as security operations teams may be less experienced in conducting forensic investigations and rapid threat detection and response for ephemeral workloads and resources in dynamic cloud environments. Our research report *The Life and Times of Cybersecurity Professionals Volume IV* also highlighted the top three areas for cybersecurity skills gaps: 37% of organizations cited cloud computing security, 38% cited application security, and 27% cited security analysis and investigations (see Figure 6).[6]

---

[6] Source: Enterprise Strategy Group Complete Survey Results, *The Life and Times of Cybersecurity Professionals Volume VI*, August 2023.

Figure 6. Top Cybersecurity Skills Shortages

**In which of the following areas, if any, would you say that your organization has the most significant shortage of cybersecurity skills?
(Percent of respondents, N=215, three responses accepted)**

Category	Percent
Application security	38%
Cloud computing security	37%
Security analysis and investigations	27%

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

Organizations need to embrace technologies to address the skills gaps and enable staff to work efficiently without needing specialized skills. For example, SecOps requires full visibility of and information on who owns different assets or resources, as well as information on risk levels, to prioritize needed actions.
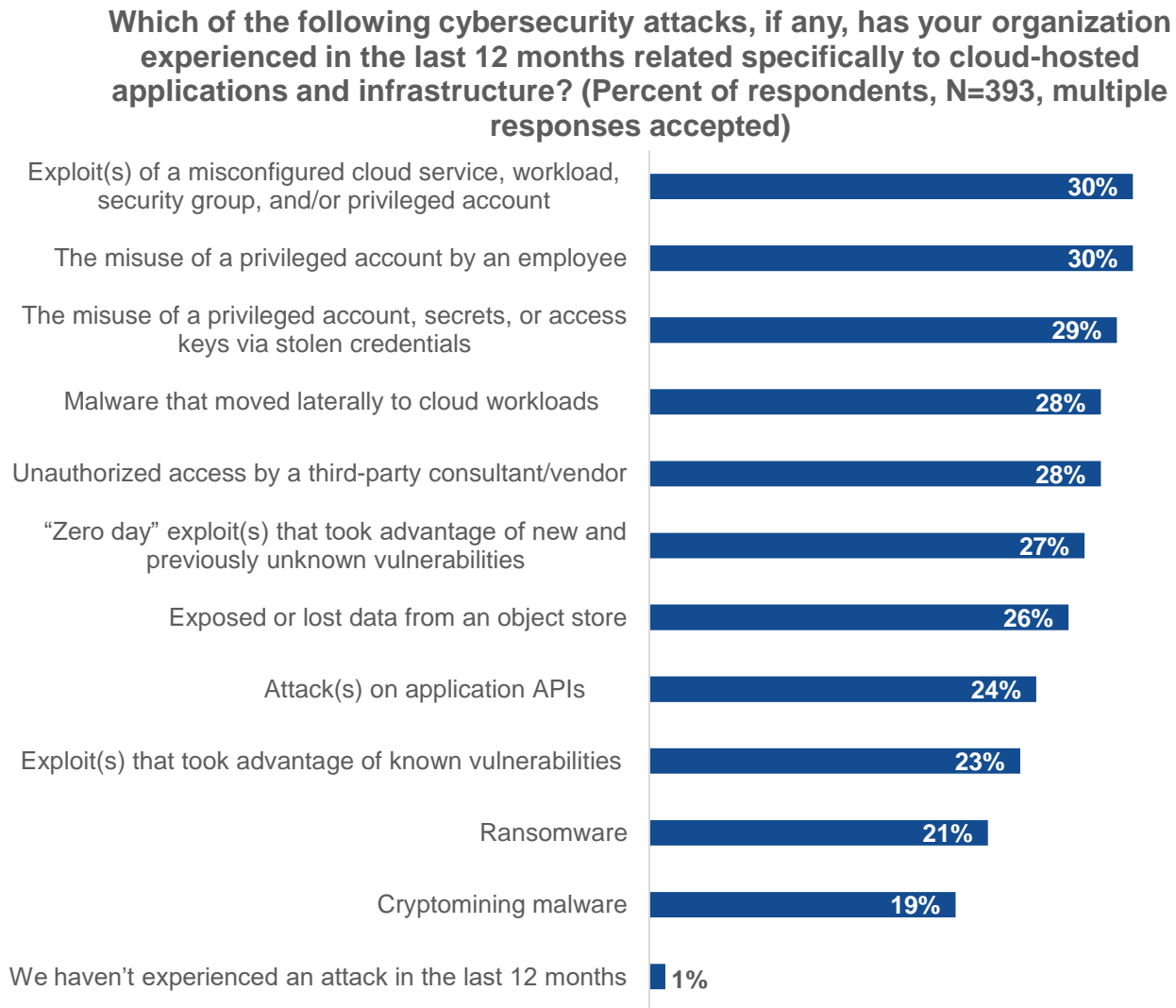
Having a common platform utilizing multiple sources of data, enriched with needed contextual information, can provide a clearer picture of risk and necessary actions for rapid response. This could help security analysts respond to high-risk, cloud-specific threats and vulnerabilities more quickly and efficiently.

Operational Convergence to Reduce Incidents and Their Impacts

Enterprise Strategy Group research shows that 99% of organizations suffered from cybersecurity incidents,[7] despite having multiple security tools and platforms in place. Many of the incidents stem from vulnerabilities—including misconfigured cloud services, workloads, security groups, or privileged accounts—access issues, or vulnerability exploits rather than highly sophisticated attacks (see Figure 7).

---

[7] Source: Enterprise Strategy Group Research Report: *Complete Survey Results: Cloud Detection and Response,* October 2023.

Figure 7. Cybersecurity Attacks on Cloud-hosted Applications Over the Past 12 Months

Which of the following cybersecurity attacks, if any, has your organization experienced in the last 12 months related specifically to cloud-hosted applications and infrastructure? (Percent of respondents, N=393, multiple responses accepted)

Exploit(s) of a misconfigured cloud service, workload, security group, and/or privileged account	30%
The misuse of a privileged account by an employee	30%
The misuse of a privileged account, secrets, or access keys via stolen credentials	29%
Malware that moved laterally to cloud workloads	28%
Unauthorized access by a third-party consultant/vendor	28%
"Zero day" exploit(s) that took advantage of new and previously unknown vulnerabilities	27%
Exposed or lost data from an object store	26%
Attack(s) on application APIs	24%
Exploit(s) that took advantage of known vulnerabilities	23%
Ransomware	21%
Cryptomining malware	19%
We haven't experienced an attack in the last 12 months	1%

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

This is a consequence of the lack of collaboration and efficiency between cloud security and SecOps teams. Even when the cloud security teams are generating alerts for these types of security issues, SecOps cannot determine which issues have the highest impact on risk. As a result, high-risk issues are not remediated in time to prevent the incidents, and, at worst, the high-risk issues remain open for too long, leading to more frequent compromise or lateral movement once there is a breach.

The research demonstrates that organizations have suffered serious impacts from longer response times, including business process disruption, data loss, unauthorized access to sensitive information, application downtime, malware movement, data loss, and compliance violations (see Figure 8).[8]

---

[8] Ibid.

Figure 8. Cybersecurity Attack Impacts Over the Past 12 Months

In the last 12 months, has your organization experienced any of the following tied to an attack between the time a cybersecurity incident was detected and when the issue was mitigated? (Percent of respondents, N=393, multiple responses accepted)

Business process disruption	34%
Data loss/exfiltration	33%
Unauthorized access to sensitive information	32%
Application downtime	31%
Malware moved laterally	31%
Inability to meet service level agreements (SLAs)	30%
Introduction of backdoors	29%
Customer data loss	29%
Compliance violations	27%
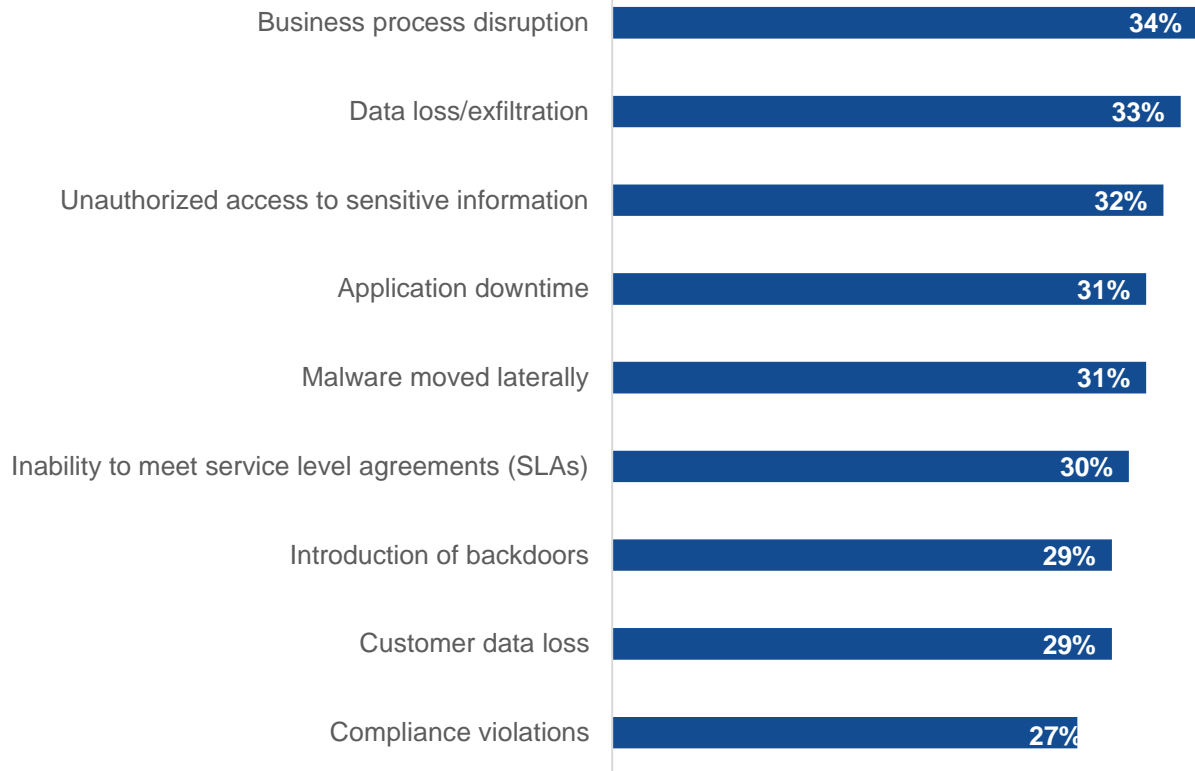
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Solution: Converge Enterprise Security Operations With Cloud-native Application Protection

Cloud security solutions need to bridge the gap between proactive and reactive security. This can only be accomplished by converging cloud security—including posture management, compliance monitoring, and threat detection—with enterprise security operations solutions for rapid threat investigation and response.

This requires a common data and operating platform to provide a single source of truth to drive efficiency across the full security lifecycle, from prevention and detection to investigation, response, and remediation. This enables coordination across teams, helping cloud security teams mitigate risk and deploy more secure applications, while enabling security operations to collaborate with teams to remediate critical issues. A unified platform will help security teams understand the issue and its possible impact, assess overall risk for the organization, determine the right owner, drive the needed mitigation action, and validate the success of the action and any other necessary steps to further reduce risk, such as setting new policies.

Using Google Security Command Center to Unite Cloud Security With Enterprise Security Operations

Google provides a complete multi-cloud security platform that converges cloud security and security operations capabilities into a single solution, powered by Mandiant threat intelligence and Google's Gemini AI. It helps unite teams so more expertise can be applied to high-risk issues, helping drive accountability for remediation. In addition, it provides:

- **Risk lifecycle management for security posture management.** A comprehensive and continuous view of cloud risks helps security teams drive actions by the *right* teams to address top risks.

- **Converged cloud security and security operations workflows.** A unified data model enables a complete picture of activity, automatic grouping of incidents based on correlation analysis, and common workflows to optimize efficiency across teams.

- **Rapid response for threat investigation, leveraging AI and advanced analytics.** The latest, frontline threat intelligence from Mandiant, along with generative AI capabilities, infuse the superior analytic capabilities that enable rapid threat investigation and response.

- **Assignment of cases and playbooks for the right analysts.** Correct assignment makes immediate remediation and corrective actions possible.

The solution also optimizes efficiency by:

- Helping teams collaborate so more people can be enlisted to address high-risk issues and events.

- Sharing security data to better understand and address root causes.

- Driving faster, more effective remediation actions.

- Providing a holistic view of risk.

- Automating response actions.

Conclusion

As organizations continue to move their workloads to the cloud, security teams have been challenged to manage their overall risk posture across cloud environments. They also struggle to deliver efficient and effective cloud threat detection and response. Organizations need a solution with strong tooling that integrates cloud security with enterprise security operations to dismantle the tool-driven silos that separate teams today.

Google Security Command Center provides a converged approach, providing a unified data model and platform to help security teams understand where they are most at risk and efficiently remediate the issues that are creating these risks. It is powered by Mandiant threat intelligence to catch new and novel threats and infuses Google AI to reduce toil on security teams, while upskilling IT professionals so they can keep their organizations safe.

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