Cybersecurity
INSIDERS

2023

Cloud Security Report

How organizations are leveraging cloud security strategies, technologies, and tools for operational excellence

CHECK POINT™

YOU DESERVE THE BEST SECURITY

Introduction

The rapidly evolving cloud landscape presents organizations with complex challenges in effectively managing and securing their cloud infrastructure, necessitating the adoption of comprehensive solutions to mitigate risks and safeguard critical assets.

This 2023 Cloud Security Report is based on a comprehensive survey of 1052 cybersecurity professionals in April 2023, to gain insights and reveal trends in cloud security management, highlighting the pressing challenges faced by organizations and providing guidance for enhancing cloud security posture.

Key Survey Findings Include:

- **Multi-Cloud Security Challenges and Concerns:** As cloud adoption is increasing, with 39% of respondents having more than 50% of their workloads in the cloud, a majority of organizations struggle with the skills gap for cloud security deployment (58%) and ensuring data protection (52%) in multi-cloud environments. Security concerns remain high, with 76% of respondents being extremely or very concerned about cloud security.
- **Cloud Security Incidents:** 24% of respondents experienced a public cloud-related security incident, with misconfigurations, account compromises, and exploited vulnerabilities being the top incident types.
- **Cloud Configuration and Security Policy Management:** 62% of organizations use cloud-native tools for configuration management, while 29% utilize dedicated CSPM solutions. A significant 72% of users have to access three or more separate security solutions to configure their cloud policies, causing cloud management and security issues. A substantial 70% of organizations have six or more security policies in place.
- **DevSecOps, CIEM, and Unified Security Management:** 37% of respondents have adopted DevSecOps in some parts of their organization, while 19% have a comprehensive program in place. 40% use CIEM as part of their CSPM, and 90% of respondents favor a single cloud security platform for simplified management.

We would like to thank Check Point for supporting this important industry research project. We hope you'll find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

Cloud Security Concerns

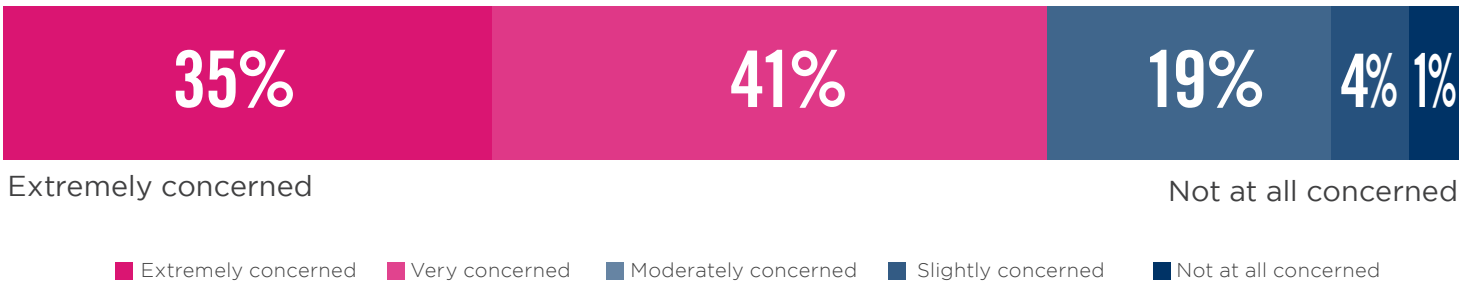
The evolution of cloud security has been turbulent, often manifesting in bursts of revolutionary changes, and continues to be a major concern for cybersecurity professionals. Starting over is seldom an option, and most organizations have likely expanded their IT and security capabilities gradually, leading to a combination of a la carte cloud and on-premises configurations. Trying to manage a variety of point tools has led to decreased visibility and an additional layer of complexity, which continues to create concern.

According to the survey, 76% of respondents are either extremely or very concerned about cloud security. This highlights the urgent need for a shift in the way we are securing the cloud infrastructure.

To address these security concerns, organizations should adopt a comprehensive cloud security solution, like a Cloud Native Application Protection Platform (CNAPP), that provides complete visibility across the entire cloud infrastructure, securing applications from development to production.

How concerned are you about the security of public clouds?

76% of organizations are extremely or very concerned about cloud security



Cloud Incidents Reality

As the attack surface of cloud-native applications increases and assailants target misconfigurations across the entire cloud infrastructure, organizations continue to experience security-related incidents at the same rate year over year. Twenty-four percent of respondents reported experiencing a public cloud-related security incident in the last 12 months.

Public cloud security incidents come in various forms and can have far-reaching consequences. The top three types of incidents reported among cybersecurity professionals are wrongly configured resources or accounts (19%), account compromises (16%), and exploited vulnerabilities (16%).

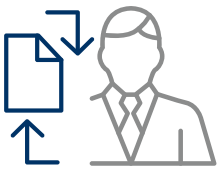
Did your organization experience a public cloud related security incident in the last 12 months?

If yes, what type of incident was it?

19%
Wrongly configured resource or account

16%
Account compromise

16%
Vulnerability exploited



13%
Data or files shared inappropriately by a user

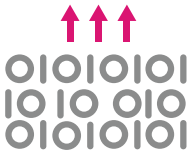
Malware infection 11% | Data or files downloaded to an unsafe device 10% | Data or files uploaded to an unsanctioned cloud resource 9% | Other 6%

Top Cloud Threats

Regardless of whether an organization has suffered a security incident so far, the following findings align closely with the overall experience in the industry. When it comes to the top security threats, we see that misconfiguration of the cloud platform or wrong setup ranks highest at 59%, followed by exfiltration of sensitive data (51%), insecure interfaces/APIs (51%), and unauthorized access (49%). This demonstrates that a significant portion of organizations are still vulnerable to cloud security threats, in particular, misconfigurations and access control. The findings also emphasize the importance of proper configurations, robust account protection, and timely vulnerability management.

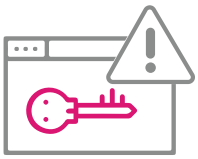
What do you see as the biggest security threats in public clouds?

59% Misconfiguration of the cloud platform/wrong setup

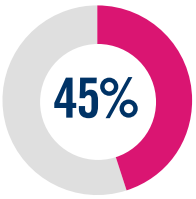


51% Exfiltration of sensitive data

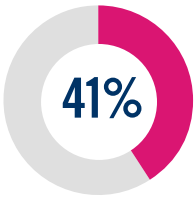
51% Insecure interfaces/APIs



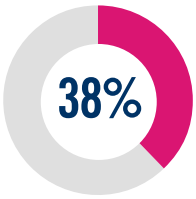
49% Unauthorized access



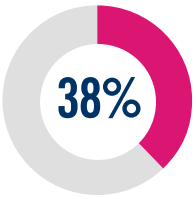
Hijacking of accounts, services, or traffic



External sharing of data



Malicious insiders



Malware/ ransomware

Foreign state-sponsored cyber attacks 37% | Denial of service attacks 31% | Cloud cryptojacking 21% | Theft of service 20% | Lost mobile devices 13% | Don't know/other 7%

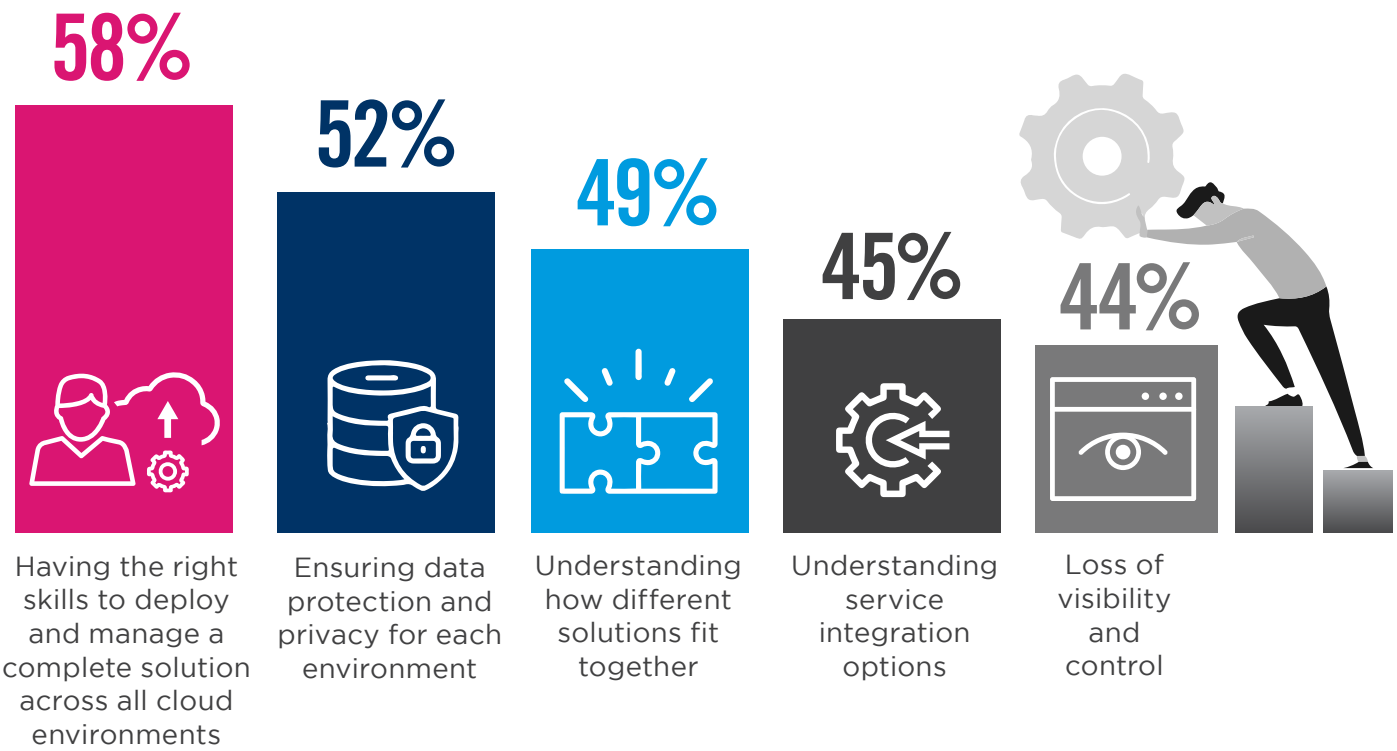
Multi-Cloud Security Challenges

The difficulties of safeguarding cloud workloads expand drastically with the addition of a multi-cloud environment. This is clearly shown by the four primary issues that organizations struggle with - all of which relate to having the right personnel and in-depth understanding of the separate cloud platforms.

The survey findings show that 58% of respondents struggle with having the right skills to deploy and manage a complete solution across all cloud environments, while 52% face challenges in ensuring data protection and privacy for each environment. Other challenges include understanding how different solutions fit together (49%), understanding service integration options (45%), and loss of visibility and control (44%).

The complexity of securing multi-cloud environments and the diverse skill set required to manage them effectively are well underscored by these findings. Organizations should consider leveraging a comprehensive multi-cloud security solution that integrates with CSP tools to simplify management and reduce the need for specialized skills.

What are your biggest challenges securing multi-cloud environments?

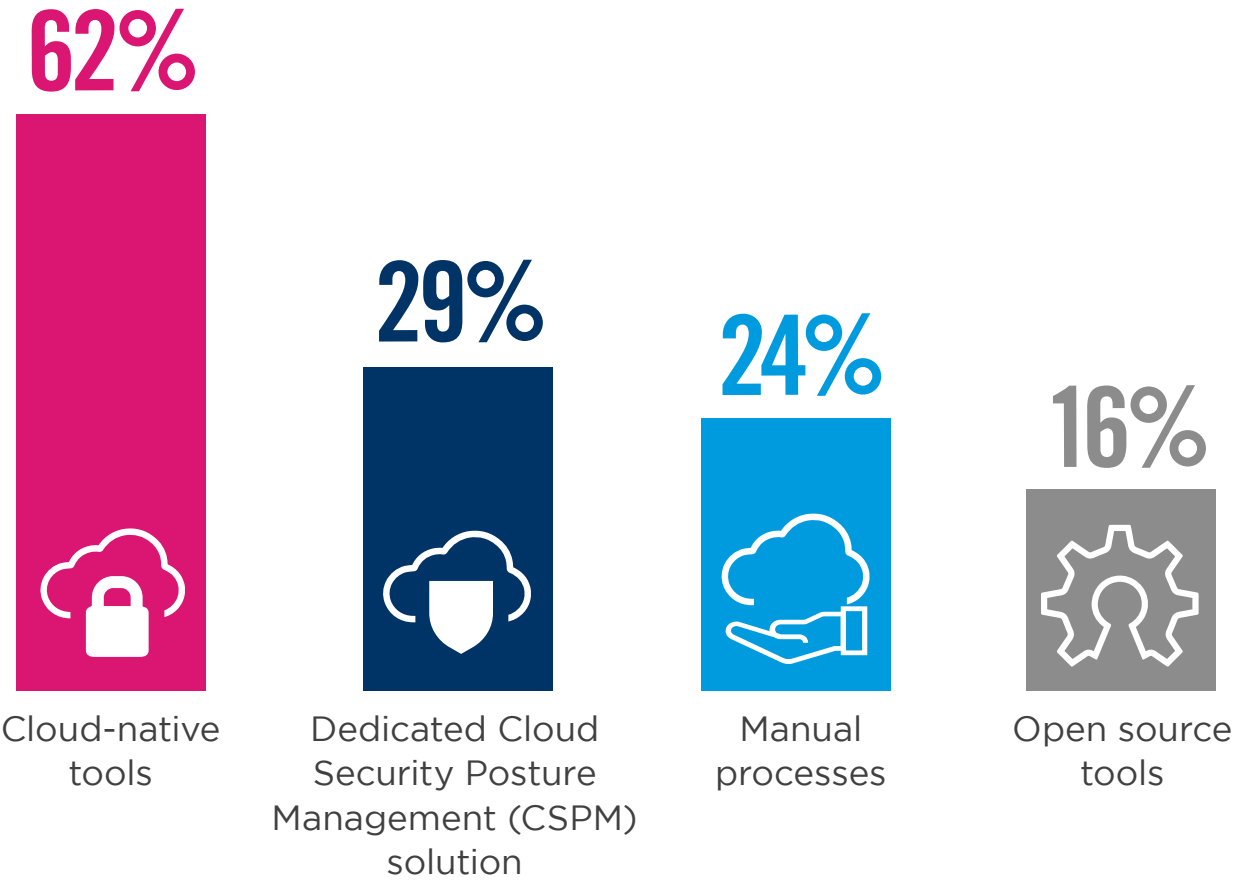


Keeping up with the rate of change 38% | Managing the costs of different solutions 37% | Providing seamless access to users based on their credentials 37% | Selecting the right set of services 36% | Other 3%

Managing Cloud Configurations

Organizations relying on cloud-based infrastructures often take advantage of the native security controls their Cloud Service Provider (CSP) offers for configuring and safeguarding cloud setups, and the survey results corroborate this. Most companies (62%) employ cloud-native tools for cloud configuration management and 29% opt for dedicated Cloud Security Posture Management (CSPM) solutions. However, many enterprises still cling to manual practices (24%), utilize open source tools (16%), or fail to adequately handle their configurations (13%).

How do you currently manage your cloud infrastructure configurations?



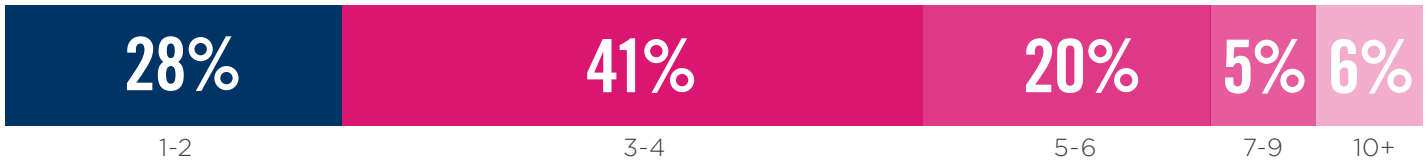
Not actively managing 13% | Other 4%

Security Configuration Overload

Maintaining security consistency across their data center and public cloud environments where cloud applications are deployed is a critical and growing issue for organizations. An overwhelming 72% of users must access three or more separate security solutions to configure enterprise cloud policies. Six percent of respondents reported using even ten or more separate solutions. This fragmentation in security can lead to increased complexity and potential gaps in protection. Security professionals also struggle to keep up with requirements and alerts, making it harder for security to be more proactive.

How many separate security solutions do your users have to access to configure the policies that secure your enterprise's entire cloud footprint?

72% have to access 3 or more dashboards to configure their enterprise's cloud policies



Security solutions to configure policies

Cloud Security Policy Management

Security policies are the cornerstone of any effective cloud security strategy to ensure that access to cloud resources is properly managed, sensitive data is protected, and compliance requirements are met. Without proper policy procedures, organizations are vulnerable as security incidents become more frequent and complex. The survey data shows that a significant portion of respondents (70%) have six or more security policies. An alarming 26% even have 20 or more policies. However, a nontrivial number of respondents (30%) indicated having less than five policies in place, which may leave their cloud environments vulnerable to security breaches and data leakage.

How many security POLICIES does your organization have in place to secure access to and protect data in private and public cloud apps, and the web?

Additionally, managing security alerts is essential for prompt incident response. Cybersecurity professionals revealed that they get overwhelmed with alerts from multiple disparate tools. This alert fatigue creates confusion, bottlenecks, and blind spots, ultimately delaying the remediation of serious threats.

At what point do the security alerts you receive get overwhelming?

Achieving a balance between security and operational efficiency is key to effective cloud security policy management. Organizations should adopt a risk-based approach that prioritizes risks based on the full context of configuration risks, workload posture, network exposure, permissions, attack paths, and business priorities. Automation and orchestration tools can help streamline policy management, prioritize alerts, and ensure consistency across different cloud environments. Unifying security across these areas enables organizations to focus on the most critical alerts, use actionable insights from a contextual, effective risk management (ERM) engine, and utilize AI and risk scoring to reduce the attack surface. As a result, organizations are in a better position to act quickly when an issue arises.

Workloads in the Cloud

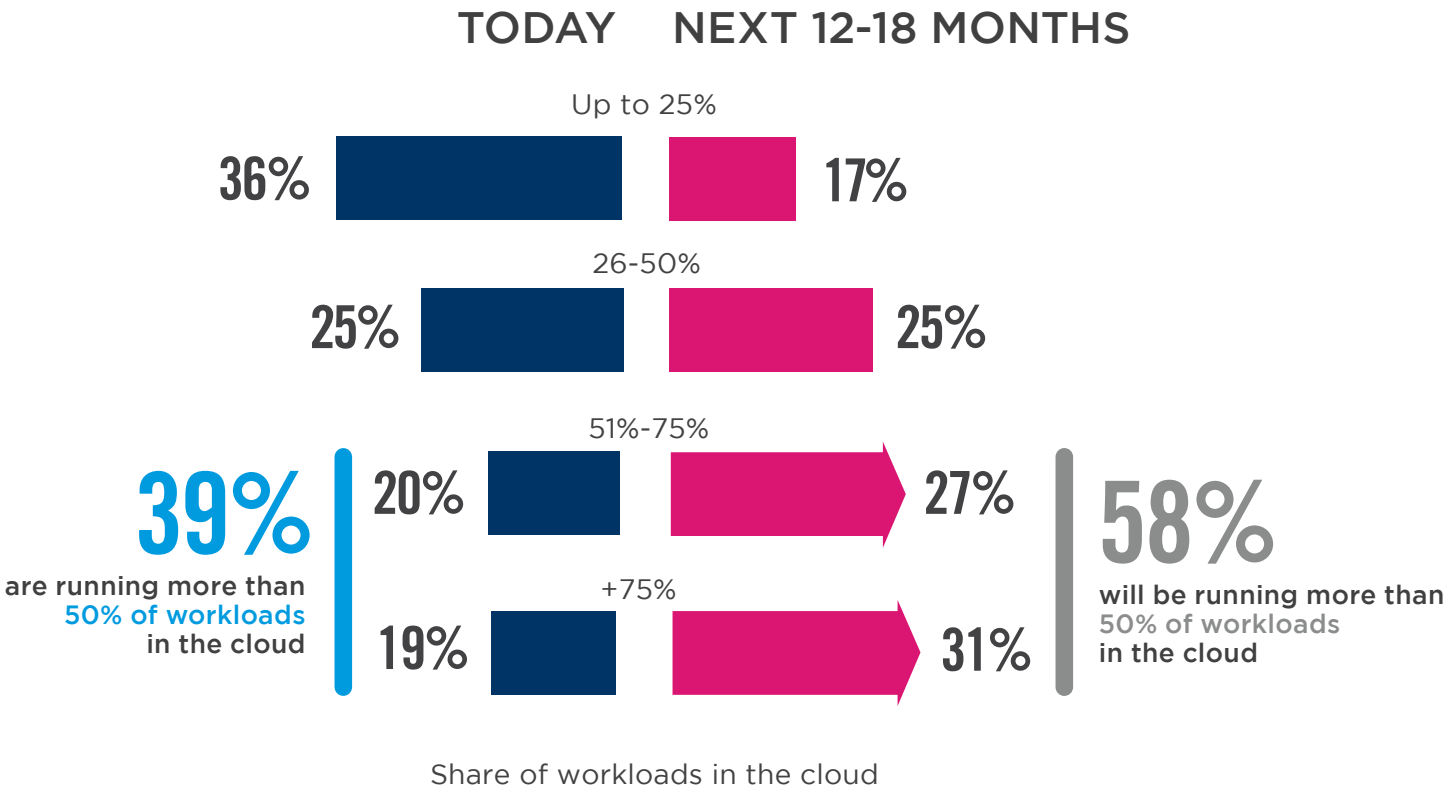
Moving workloads to the cloud is gaining momentum. Today, 39% of respondents have more than 50% of their workloads in the cloud (up 4 percentage points from last year).

As workloads and cloud deployments grow and become more complex, the number of entitlements required to implement access control across multi cloud platforms grows as well. Adopting the principle of least privilege is crucial for strengthening the Zero Trust security model, protecting corporate cloud networks, and limiting an intruder's potential to traverse the infrastructure of a business.

It is essential to limit user, application, and system access to only what is required for employees to complete their work.

What percentage of your workloads are in the cloud today?

What percentage of your workloads will be in the cloud in next 12-18 months?

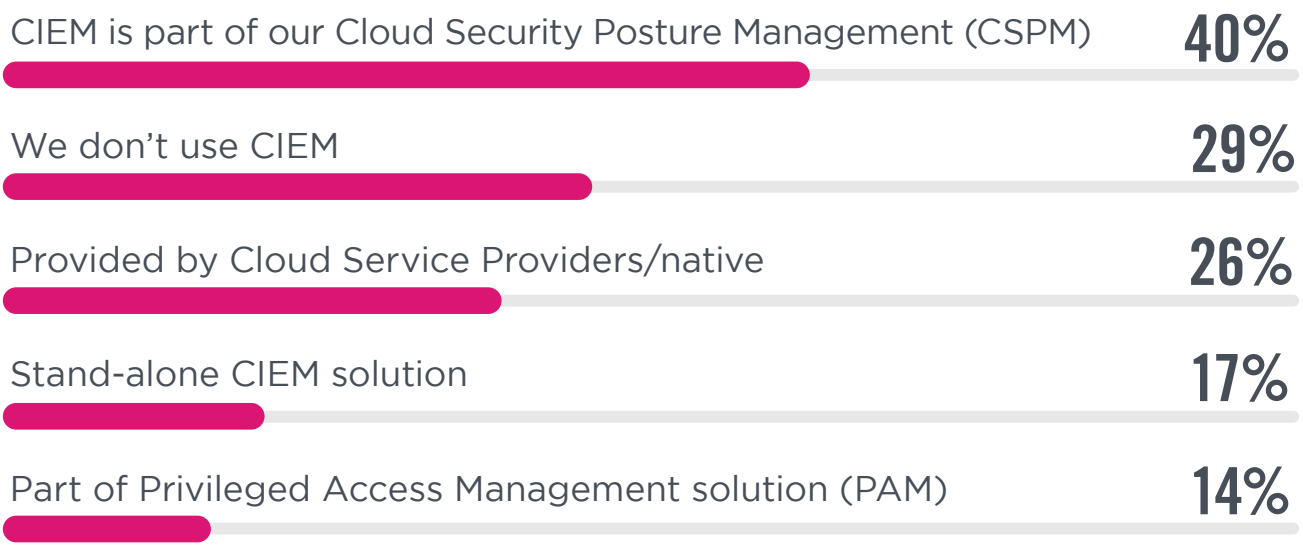


CIEM Adoption

Manually managing entitlements across multiple cloud infrastructures with thousands of permissions, actors, and resources is unrealistic and not scalable. CIEM solutions allow security teams to effectively manage user identities and access to cloud-based infrastructures and resources, while implementing the least-privileged access model. This ensures that the risk of attack due to excessive permissions is significantly reduced.

According to the survey, 40% of respondents use CIEM as part of their Cloud Security Posture Management (CSPM), while 26% rely on Cloud Service Providers or native CIEM solutions. However, 29% of surveyed professionals do not use CIEM today, suggesting there is room for significant growth in CIEM adoption. To enhance their cloud security posture, organizations should consider incorporating CIEM into their CSPM or explore dedicated CIEM solutions with robust capabilities, ensuring seamless integration with CSPM and helping organizations manage their cloud infrastructure entitlements more effectively.

How does your organization use CIEM?

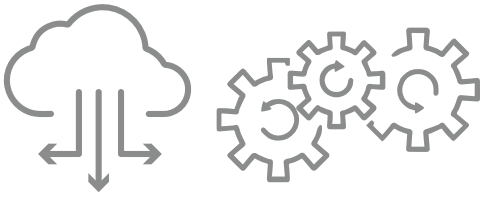


DevSecOps Adoption

As DevSecOps integration becomes increasingly important, we asked cybersecurity professionals about their organization's stance on DevSecOps. According to the survey, 37% of organizations have adopted DevSecOps in some parts of their organization, and 22% are considering its adoption. Only 19% have a comprehensive DevSecOps program in place (up 3 percentage points from last year).

We expect to see significant growth in the adoption of DevSecOps as organizations improve security practices throughout the software development lifecycle and implement solutions that provide automated security checks and proactive protection to ensure secure application deployment and development.

What is your organization's current position on DevSecOps?

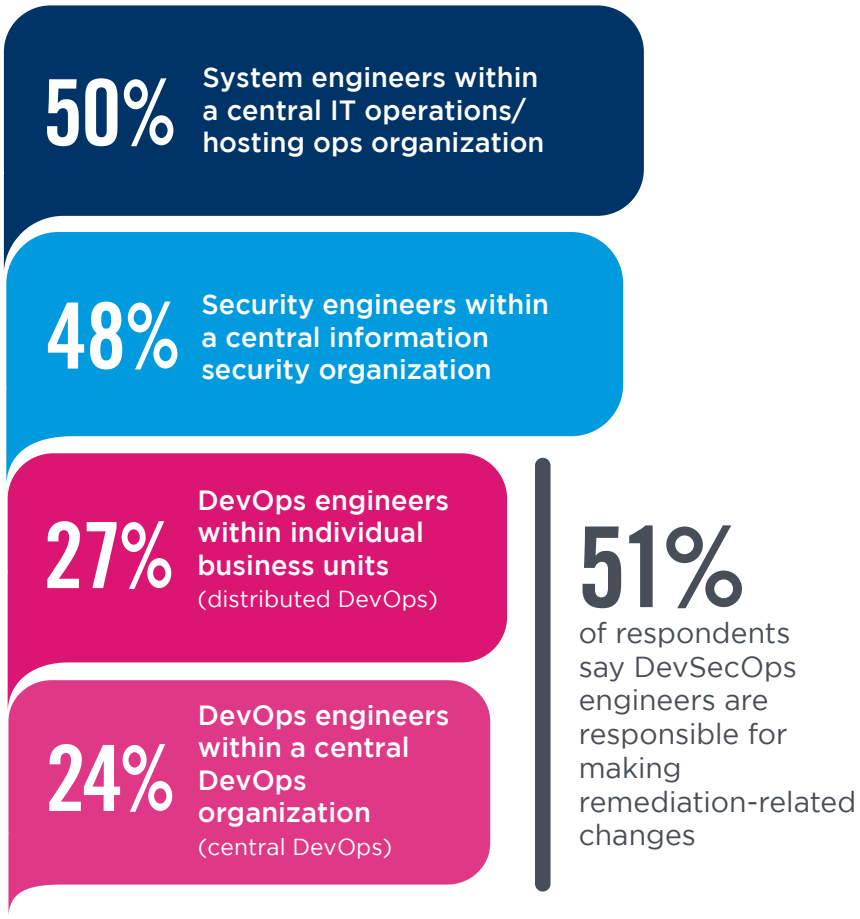


Other 4%

Responsibility for Changes

Developers are an integral part of the operational process. Finding a developer-centric approach that enforces security policies throughout the software development lifecycle without creating friction for developers is key. This will require that organizations have the necessary context to identify, prioritize, and remediate risks within the software supply chain. Today, 48% of respondents work in organizations where security engineers within a central information security organization decide what tools to use, and 51% of respondents work within organizations where DevSecOps engineers make system changes to remediate security compliance problems.

Who is accountable for actual technical changes to systems that are required to remediate security or compliance problems?



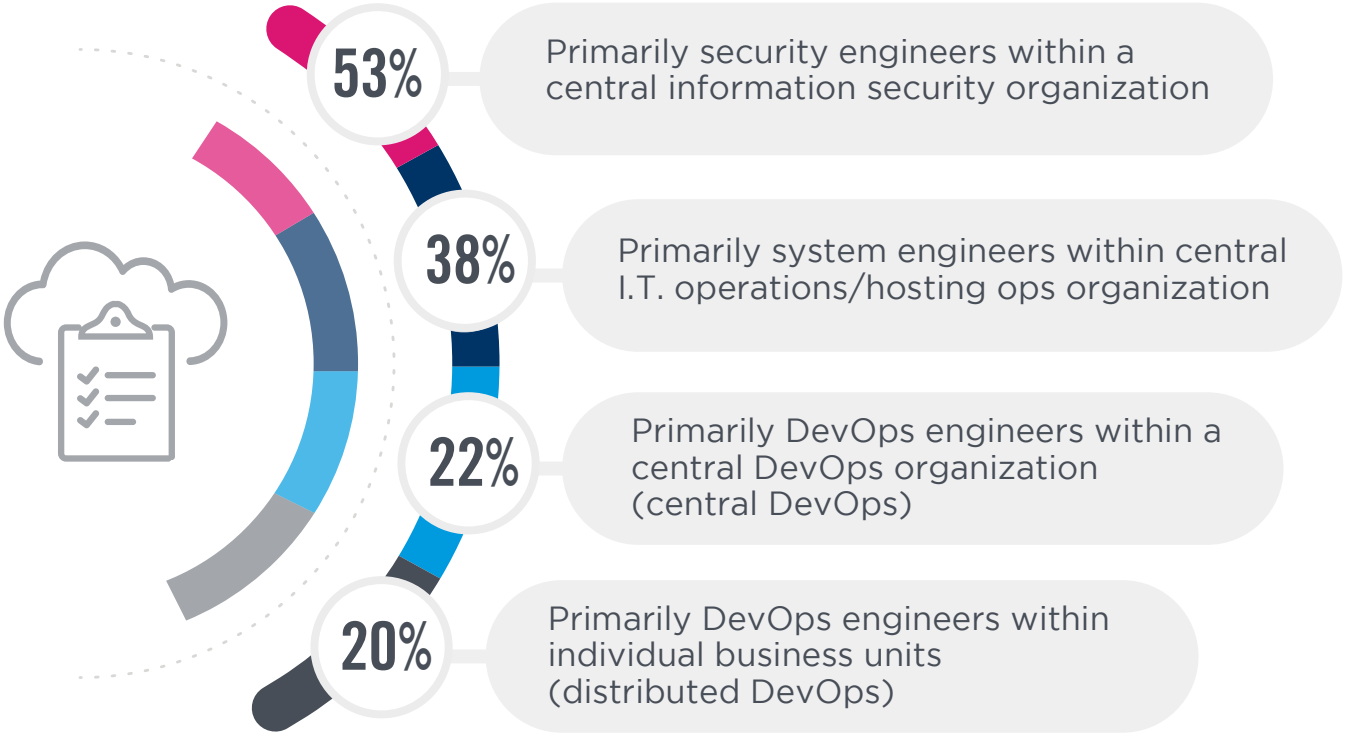
Other 4%

Security Control Decisions

Identifying who makes decisions on security technology implementation is essential for effective security control. According to the survey, 53% of respondents reported that primarily security engineers within a central information security organization make these decisions, while 38% said system engineers within central IT operations/hosting ops organizations are responsible. Decisions were also attributed to DevOps engineers within a central DevOps organization (22%) and those within individual business units (20%).

Developers and DevOps teams are integral to both cloud security and daily cloud operations. They also play a pivotal role in decision-making on tool usage and system modifications for security compliance. Given their central role, it's important for organizations to adopt a 'developer-first' approach when selecting cloud technology. Organizations should foster collaboration and clear communication among decision-makers not only to ensure effective security control, but to increase adoption and empower all stakeholders to prevent and remediate security and compliance issues more efficiently.

Given that information security organizations typically establish security control requirements and standards, who actually makes decisions on what technologies are used to implement security control requirements and standards?



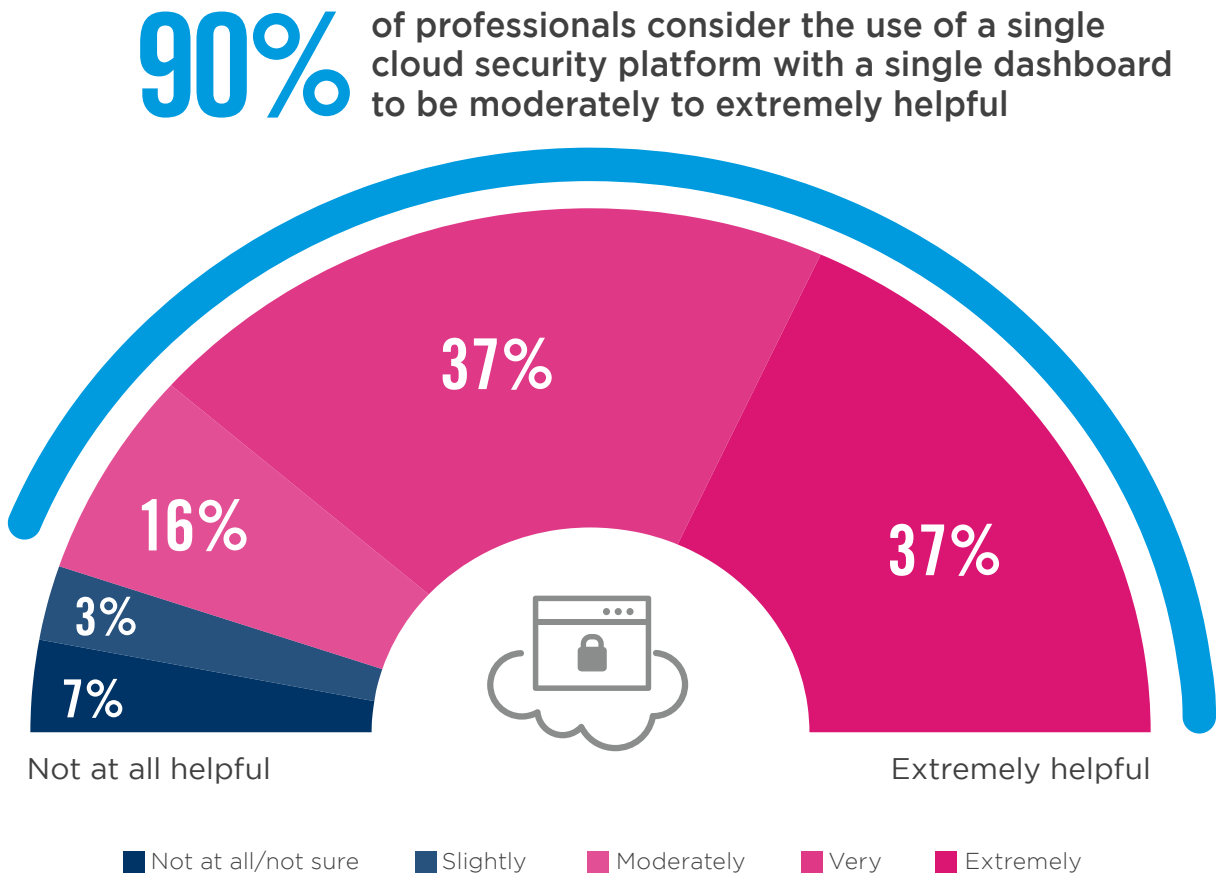
Other 9%

Unified Cloud Security Management

Better integrating features such as code scanning, effective risk management, and CIEM are key building blocks for mitigating risk and employing Zero Trust across the board. A single cloud security platform with a single dashboard can greatly simplify policy management and data protection. In our survey, an overwhelming 90% of respondents favor the idea of a single cloud security platform.

By embracing a CNAPP platform approach and devoting resources to automation, scaling, and risk management, organizations can address and achieve the full life cycle protection requirements of cloud native applications, from development to production.

How helpful would it be to have a single cloud security platform with a single dashboard where you could configure all of the policies needed to protect data consistently and comprehensively across your cloud footprint?



Best Practices for Cloud Security Management

As organizations continue to adopt cloud technologies, ensuring the security of their cloud infrastructure is paramount. The following best practices, derived from key survey findings, provide actionable insights for organizations looking to enhance their cloud security posture and address the management challenges associated with multi-cloud environments:

Embrace a platform approach: Utilize a comprehensive, integrated cloud security platform to ensure consistency, visibility, and control across multi-cloud environments, thereby reducing complexity and minimizing the chances of misconfigurations.

Prioritize automation: Leverage automation to scale security operations, streamline processes, and reduce manual work, ultimately minimizing human errors and enhancing security posture while addressing skills shortages and knowledge gaps.

Adopt DevSecOps principles: Integrate security into the development and operations lifecycle to achieve continuous security and compliance, promoting collaboration between development, operations, and security teams.

Implement a Zero Trust model: Enforce strict access controls and verification for users, devices, and applications, regardless of their location or relationship with the organization.

Implement a robust CIEM solution: Utilize a comprehensive Cloud Identity and Entitlement Management (CIEM) solution to manage access roles and entitlements, mitigating the risk of unauthorized access and data breaches.

Focus on context and intelligence: Develop a system that provides the necessary context to identify, detect, and prioritize threats, minimizing alert fatigue and enabling a more effective response to security incidents.

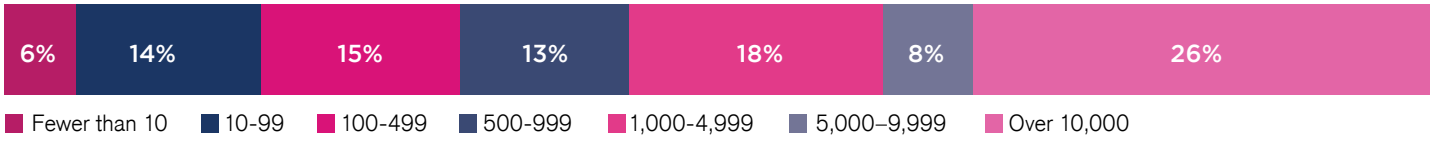
Methodology & Demographics

The 2023 Cloud Security Report is based on an in-depth survey of 1052 cybersecurity professionals conducted in April 2023. This research provides insights and trends in cloud security management, highlighting the threats and pressing challenges organizations face while providing guidance for enhancing cloud security posture. Participants span various roles - from technical and business executives to hands-on IT security practitioners, representing a balanced mix of organizations of different sizes across various industries.

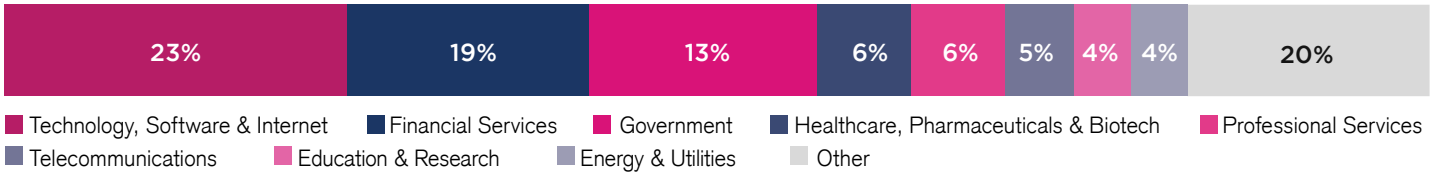
CAREER LEVEL

DEPARTMENT

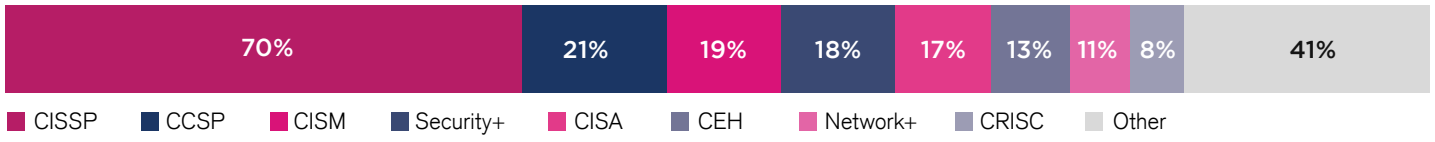
COMPANY SIZE



INDUSTRY



SECURITY CERTIFICATIONS HELD



YEARS OF EXPERIENCE

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry-leading catch rate of malware, ransomware, and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network, and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Process efficiencies and increased network agility are driving SaaS, PaaS and IaaS technology adoption at a rapid pace. This new infrastructure is also presenting businesses with a unique set of security challenges. Check Point CloudGuard provides unified cloud native security for all your assets and workloads, giving you the confidence to automate security, prevent threats, and manage posture – everywhere – across your multi-cloud.

www.checkpoint.com

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 600,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com