Cybersecurity
INSIDERS

2024

CLOUD SECURITY REPORT

TREND MICRO™

Introduction

Cloud security continues to be a critical concern as organizations increasingly leverage multi-cloud environments to drive business growth and innovation. While cloud technologies offer substantial benefits, they also present significant challenges, including complex security management, evolving compliance requirements, and a worsening threat landscape.

This 2024 Cloud Security Report, based on a comprehensive survey of over 400 IT and cybersecurity professionals across Europe, aims to unveil the current state of cloud security, identify prevalent challenges, and gather insights into the effectiveness of existing security strategies. This project was designed to provide actionable insights that guide organizations in enhancing their cloud security measures and practices.

Key Survey Findings:

- **Security Incidents:** A significant 42% of organizations reported experiencing security incidents related to public cloud usage in the last year, highlighting the continued risk in cloud environments. Respondents identified unauthorized access (59%) and data security breaches (61%) as the biggest security threats, highlighting critical areas for strengthening security measures.
- **Single Cloud Security Platform:** Survey respondents confirm the benefits of a single cloud security platform and dashboard, with 96% expressing that it would greatly aid in managing and configuring policies to protect data across their cloud infrastructures.
- **API Security Risk:** Nearly half of the respondents (49%) emphasized the importance of securing APIs, identifying these as prevalent points of vulnerability.
- **Incident Response:** 61% of participants acknowledged the need for automated incident response mechanisms to effectively address security incidents.

We extend our gratitude to Trend Micro for their valuable contributions to this report. Their dedication to advancing cloud security has been instrumental in developing this comprehensive analysis. We are confident that the insights and recommendations detailed in this report will prove useful to readers striving to secure their cloud environments.

Best,

Holger Schulze
Founder, Cybersecurity Insiders

Cybersecurity INSIDERS

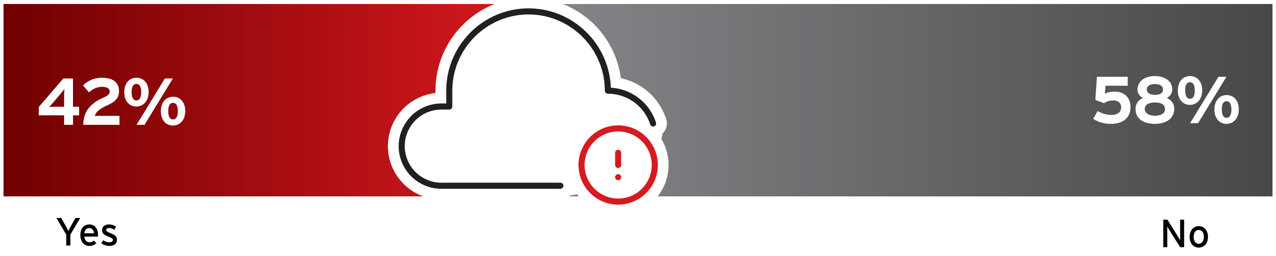
Cloud Security Incidents on the Rise

Understanding the frequency and nature of security incidents related to public cloud usage is vital for organizations to evaluate their cloud security posture and the practical challenges they face in protecting their cloud environments against evolving threats.

According to the survey results, a notable 42% of organizations reported experiencing security incidents related to public cloud usage in the past year (an increase from 36% in our 2023 report). This significant figure underscores the ongoing risks and vulnerabilities inherent in public cloud environments.

The most common types of incidents reported include unauthorized access and account compromise (26%), data security breaches (24%), and malware-related incidents (20%), which suggests a critical need for enhanced access controls and data protection measures.

Has your organization experienced any security incidents related to public cloud usage in the last 12 months?



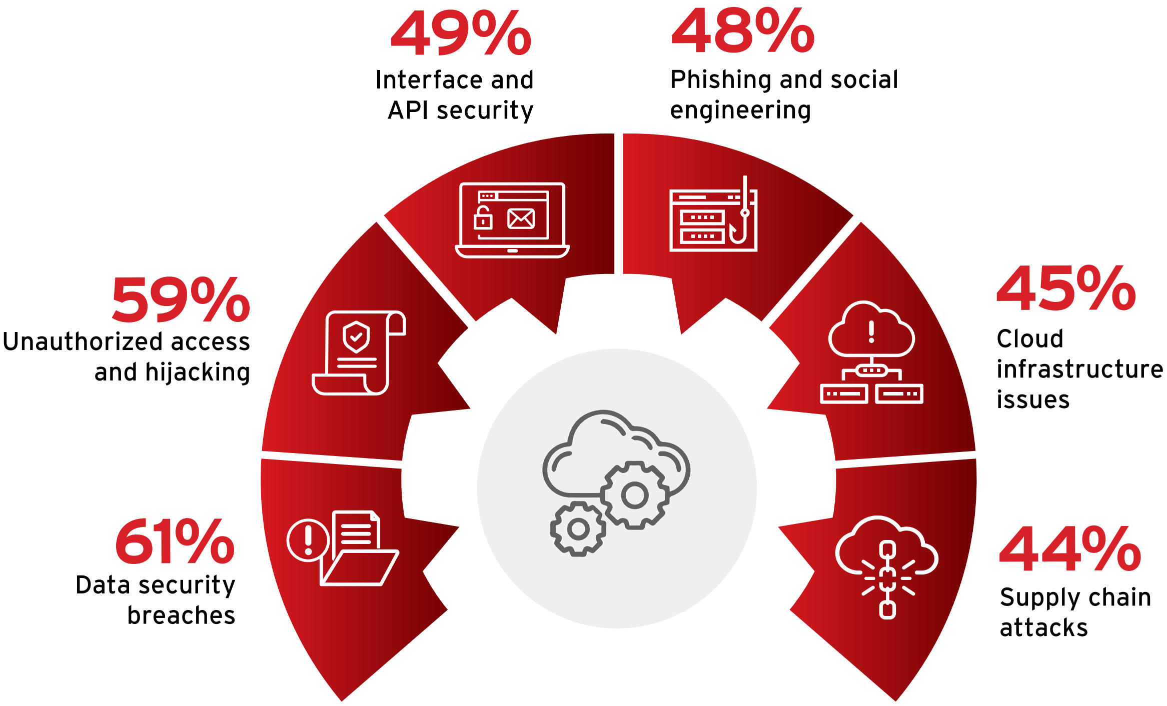
To address these challenges, organizations should focus on enhancing their security measures around user authentication, access control, and data encryption. Implementing a robust cloud security strategy that includes automated threat detection and response capabilities can significantly reduce the incidence of security breaches. Utilizing solutions that provide real-time monitoring and proactive threat hunting can help organizations proactively manage potential security issues.

Understanding the Cloud Threat Landscape

Understanding the most significant security threats in public clouds is essential for organizations to effectively tailor their defensive strategies. The types of threats organizations face can directly guide the development of more focused and effective security measures.

From the survey, data security breaches were considered the top security threat, with 61% of respondents highlighting this concern that encompassed issues such as data exfiltration and exposure due to misconfiguration. This issue is closely followed by unauthorized access and hijacking, noted by 59% of respondents, emphasizing the vulnerability of cloud services to unauthorized intrusions. API security also stood out, with 49% identifying it as a major vulnerability, highlighting the critical need to secure communication endpoints to prevent breaches. These findings echo survey insights about incidents related to unauthorized access and data breaches. This consistency highlights the ongoing challenge of safeguarding sensitive data and securing access points against unauthorized users.

What do you consider the biggest security threats in public clouds?



Organizations need to increase their visibility into cloud operations to promptly identify and address vulnerabilities and attacks. Implementing least privilege access and robust data governance frameworks can greatly reduce the risk of data breaches and unauthorized access. Additionally, adopting a security framework that integrates advanced threat detection and automated response solutions can add an essential layer of security, mirroring best practices in cloud security management. These strategies not only protect against identified threats but also bolster the overall security posture by preparing organizations to respond proactively to potential security incidents.

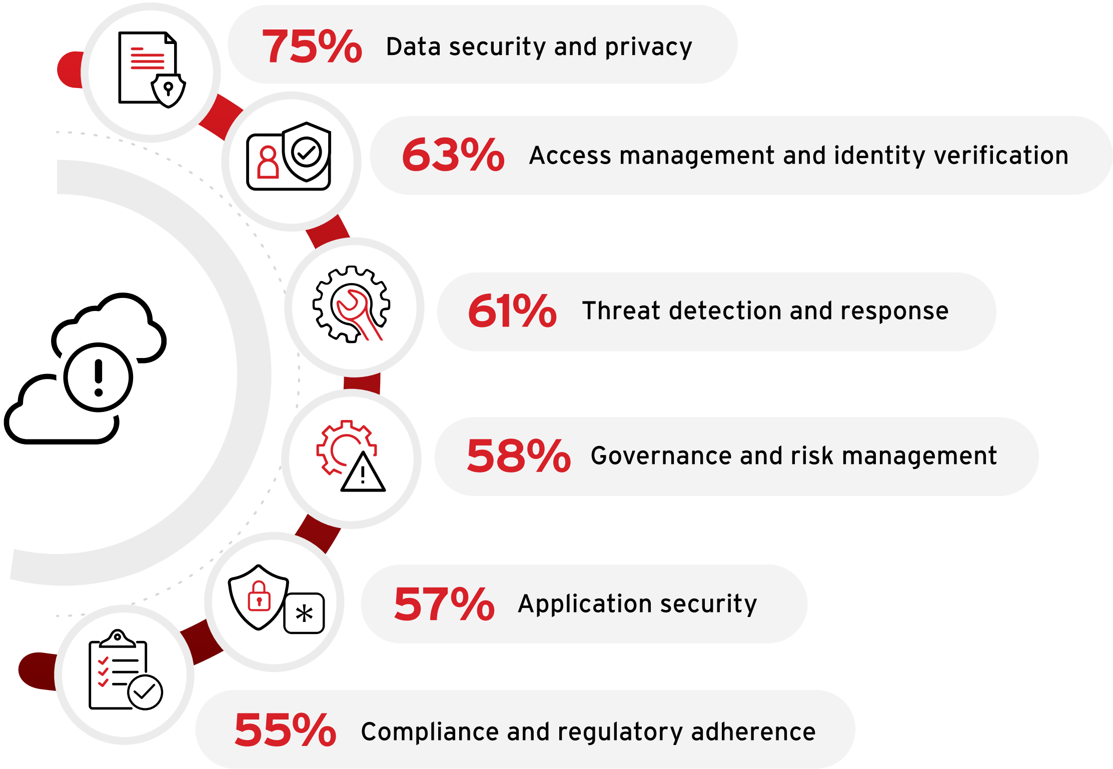
Additional responses include: Insider threats and targeted attacks 40% | Malware and ransomware 38% | Service disruptions and attacks 37% | Device security 24%

Cloud Security Priorities

As organizations continually adapt to the evolving landscape of cyber threats, understanding security priorities helps align security strategies and resource allocation to the most critical areas of concern.

The survey indicates a strong emphasis on data security and privacy, with an overwhelming 75% of respondents marking it as a top priority. This emphasis is a direct response to the prevalent concerns over data breaches and unauthorized access previously discussed. Following closely, identity and access management is prioritized by 63% of respondents, underscoring the critical role of secure authentication and access controls in preventing unauthorized access. Threat detection and response also emerged as a key concern, with 61% of participants identifying it as a priority, reflecting the urgent need for robust mechanisms to quickly identify and mitigate cyber threats.

What are your top cloud security priorities?



75% Data security and privacy

63% Access management and identity verification

61% Threat detection and response

58% Governance and risk management

57% Application security

55% Compliance and regulatory adherence

Organizations should enhance their data protection strategies and invest in advanced identity management solutions to address these priorities effectively. By integrating real-time threat detection systems and automated response mechanisms, they can significantly improve their capability to preemptively counteract potential security incidents. These measures are integral to a comprehensive cloud security strategy that incorporates best practices designed to foster a resilient and adaptive security posture, reflective of industry-leading approaches to cloud security.

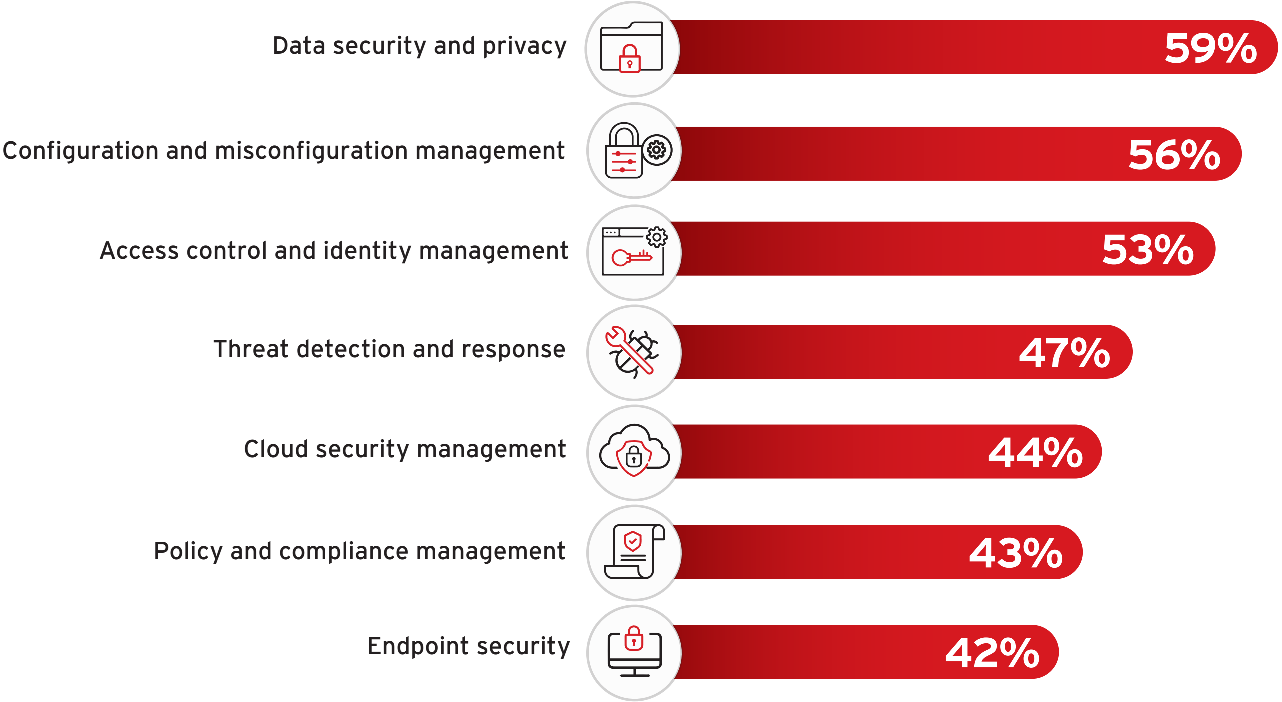
Additional responses include: Infrastructure and resource security 51% | Disaster recovery and business continuity 48% | User education and awareness 45% | Cloud migration and integration 37%

Navigating Cloud Security Challenges

Implementing cloud security and managing day-to-day operations involves addressing a variety of challenges that can impact the effectiveness and efficiency of security measures. Understanding these challenges is essential to developing strategies that create a robust security posture and ensure the resilience of cloud environments.

Survey respondents highlight data security and privacy as their top operations challenge, cited by 59%, reflecting ongoing concerns about protecting sensitive information—a theme that has consistently emerged in earlier responses related to security priorities and significant threats. Configuration and misconfiguration management was also noted as a significant concern, cited by 56% of participants, reflecting concerns over cloud service configurations that can lead to risks around unauthorized access and interface vulnerabilities. Access control and identity management, identified by 53% as a key challenge, further underscores the critical need for robust mechanisms to manage who can access what resources within the cloud, which is closely aligned with the priority given to access management.

What are your primary challenges in managing day-to-day cloud security operations?



To navigate these challenges, organizations should prioritize automating security configurations and standardizing security policies to prevent misconfigurations and unauthorized access. Focusing on staff training and the adoption of advanced security technologies, such as those providing granular access controls and real-time data protection, can tackle these operational hurdles effectively. This approach not only mitigates immediate risks but also builds a stronger foundation for long-term security resilience, aligning with strategies that incorporate best practices for continuous monitoring and response.

Additional responses include: Shadow IT and unauthorized app usage 38% | Cloud integration and automation 35% | Resource allocation 32% | Operational agility and complexity 30% | DevSecOps practices 28%

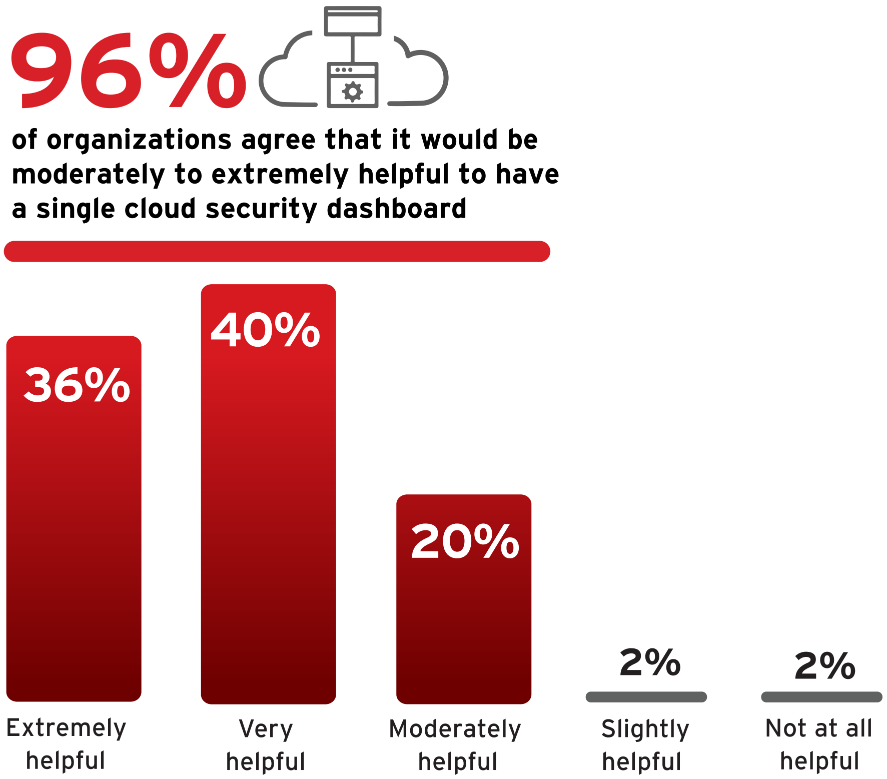
Streamlining Cloud Security Management

The need for a unified security management platform becomes increasingly important as organizations grapple with the increasing complexities of cloud environments. A single dashboard for managing security policies across all cloud services can greatly streamline operations and bolster the overall security posture.

Survey respondents overwhelmingly recognize the benefits of a single cloud security platform and dashboard, with an impressive 96% expressing that it would aid in managing and configuring policies to protect data across their cloud infrastructures.

This substantial agreement reflects the demand for more integrated and user-friendly security management tools in complex cloud infrastructures, where managing disparate systems can lead to inefficiencies and vulnerabilities.

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?



Organizations should consider the integration of a cloud security platform that provides a centralized management dashboard. Such platforms not only facilitate streamlined oversight of security policies but also markedly reduce the complexity associated with managing multiple security tools and boost the ability to swiftly respond to emerging threats. Centralized platforms also support improved compliance tracking and can significantly decrease the operational burdens of securing cloud environments during times of limited cloud expertise.

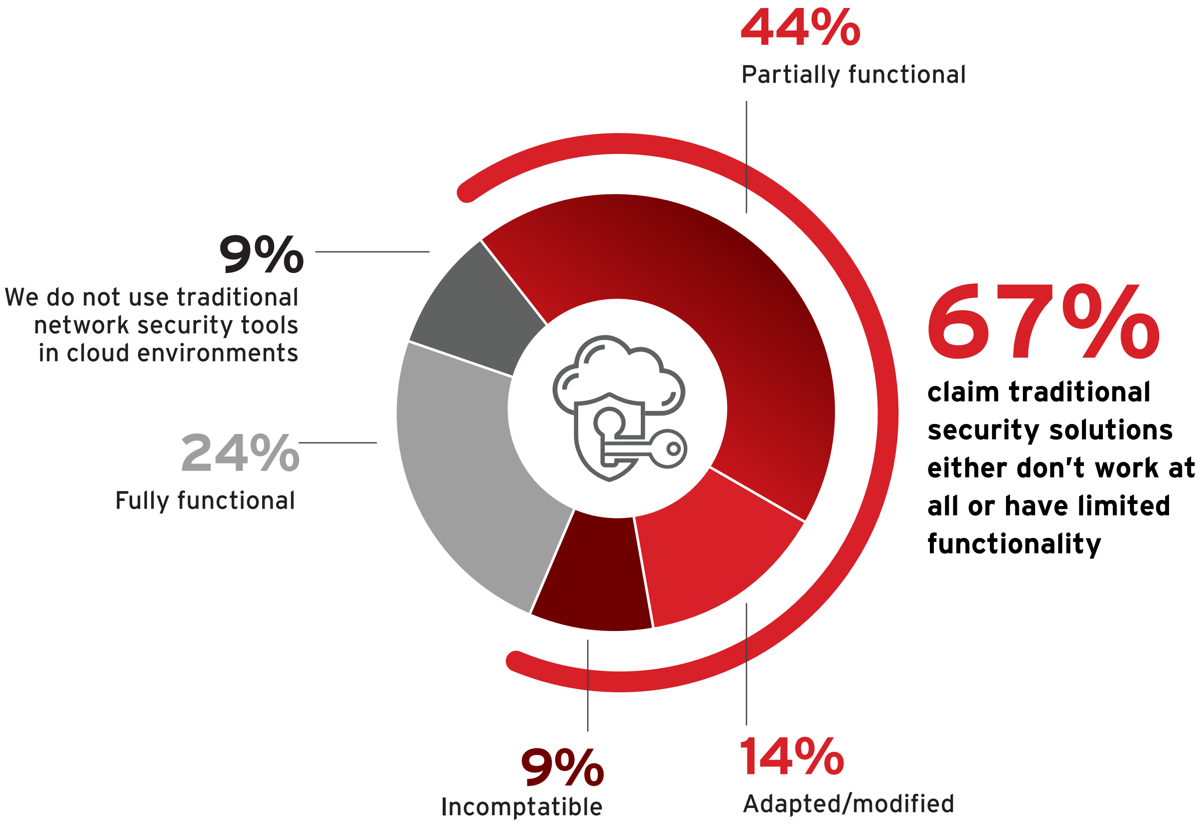
Adapting Security for the Cloud

The limited utility of traditional security tools and appliances in cloud environments is a critical issue as organizations migrate more of their operations and data to cloud platforms. This transition poses unique challenges and demands a nuanced approach to ensure that security measures remain effective.

From the survey, 44% of respondents report that their traditional security tools are only partially functional in cloud environments, indicating that while some features work, they face limitations. This highlights a common issue where legacy tools aren't fully equipped to handle the dynamic nature of cloud architectures.

Only 24% of respondents find their tools fully functional, suggesting that some organizations have successfully integrated their traditional tools with cloud infrastructures. However, 14% had to modify their tools for better cloud compatibility and 9% find their traditional tools completely incompatible.

How do your traditional security tools and appliances function in cloud environments?



To navigate these challenges, organizations should prioritize investing in cloud-native security solutions that are designed to handle the dynamic and scalable nature of cloud environments. This often involves leveraging solutions that support automated security tasks, integrate with cloud services through APIs, and offer scalability to handle elastic workloads. The move to cloud-native security tools not only addresses compatibility issues but also enhances the ability to monitor and protect distributed assets with greater efficiency.

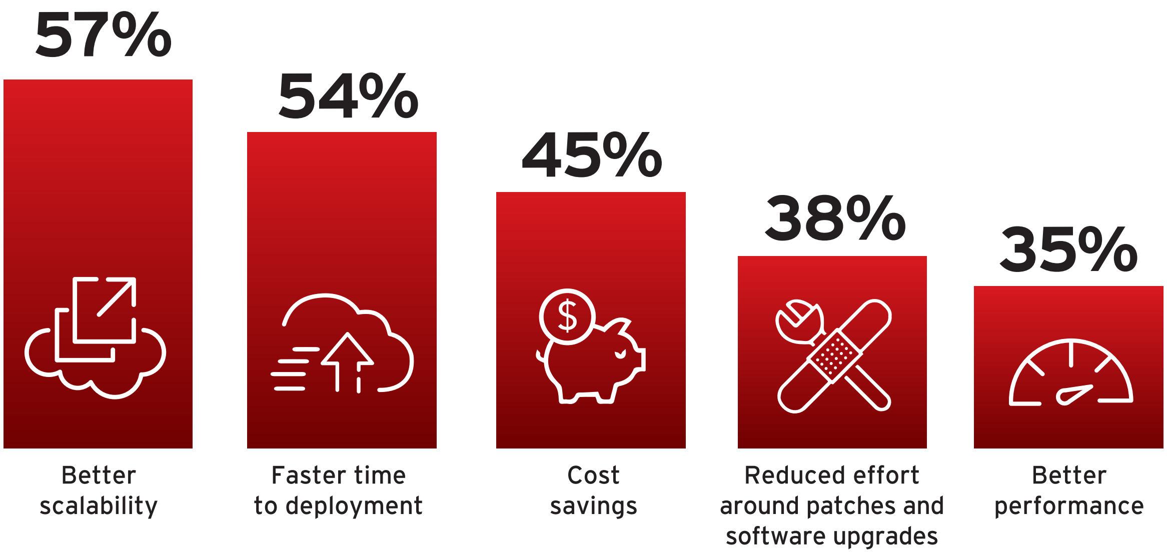
Drivers for Cloud-Based Security Solutions

Adopting cloud-based security solutions is driven by various strategic and operational factors that align with the evolving requirements of modern IT landscapes. As organizations look to enhance their security posture while also capitalizing on the agility and scalability of cloud technologies, understanding these drivers is essential for optimizing security investments.

The survey highlights several key motivations for considering cloud-based security solutions. The top driver is better scalability. cited by 57% of respondents, which reflects the need for solutions that can accommodate rapid business growth and fluctuating demands without compromising security. Closely following, 54% of respondents emphasize faster time to deployment, which is essential in today's fast-paced business environments where speed and agility are critical. Cost savings is also a significant consideration for 45% of participants, underscoring the economic benefits of cloud solutions in reducing total cost of ownership and operational expenses.

Furthermore, 38% of respondents appreciate the reduced effort around patches and upgrades, which can be more effectively managed in cloud environments through automated processes. Better security performance and easier policy management, noted by 35% of respondents, highlight the operational efficiencies and enhanced control over security policies that cloud solutions provide.

What are the main drivers for considering cloud-based security solutions?



Organizations looking to capitalize on these benefits should prioritize security solutions that offer flexibility, quick integration, and cost-effectiveness. The focus on scalability and rapid deployment aligns with the need for security frameworks that can adapt quickly to changing conditions without compromising on protection. Leveraging cloud-native features such as automation, real-time threat intelligence, and integrated management can dramatically enhance security efficacy and operational efficiency.

Additional responses include: Easier policy management 35% | Better visibility into user activity and system behavior 34% | Need for secure app access from any location 31% | Meet cloud compliance expectations 29% | Better uptime 27% | Reduction of appliance footprint in branch offices 24% Our data/workloads reside in the cloud (or are moving to the cloud) 21%

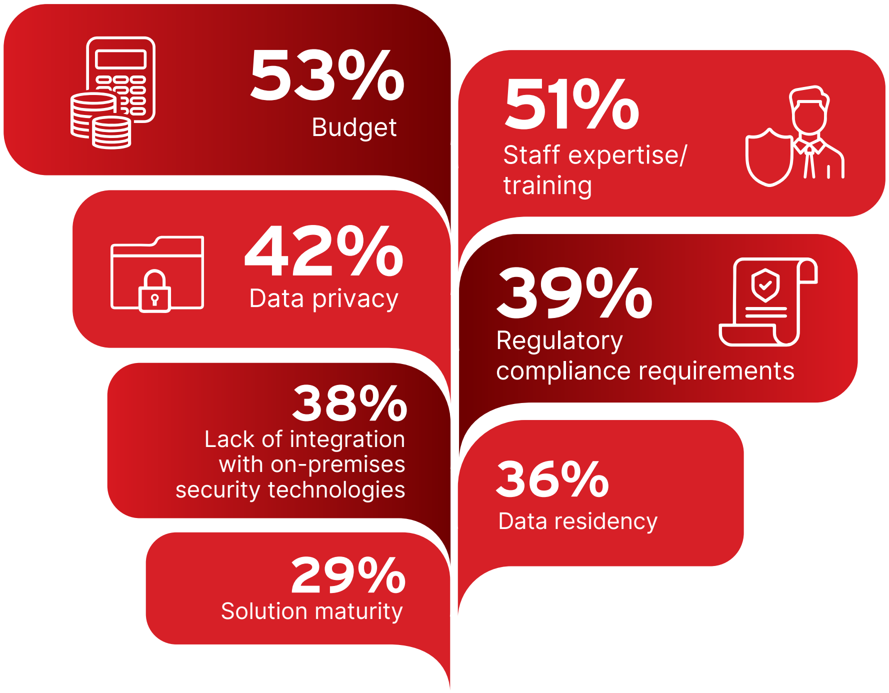
Barriers to Cloud Security Migration

Understanding the barriers to adopting cloud-based security solutions is essential to address the gaps between recognizing the benefits of such solutions and their actual implementation. These barriers highlight the challenges organizations face, informing strategies to mitigate them and enhance cloud adoption rates.

The survey identifies budget constraints as the primary barrier, reported by 53% of respondents. This suggests that despite the perceived cost savings of cloud solutions, initial investment and transition costs remain significant concerns.

Staff expertise and training, mentioned by 51% of respondents, points to a skills gap that must be bridged to manage cloud technologies effectively. Additionally, data privacy issues and regulatory compliance requirements, highlighted by 42% and 39% respectively, underscore the complexities of ensuring data security and adhering to regulatory and industry standards in cloud environments.

What are the main barriers to migrating to cloud-based security solutions?



To address these barriers, organizations should focus on strategic planning that includes budget allocation for cloud transitions and comprehensive training programs to upskill their workforce. Additionally, adopting cloud security solutions that offer robust compliance and data protection features can alleviate concerns related to data privacy and regulatory challenges. By focusing on these key areas, organizations can facilitate a smoother transition to cloud-based security solutions, ultimately strengthening their security posture and preparing them to tackle today's cybersecurity challenges more effectively.

Additional responses include: Sunk cost into on-premises tools 26% | Integrity of cloud security platform 22% | Limited control over encryption keys 20% | Scalability and performance 14%

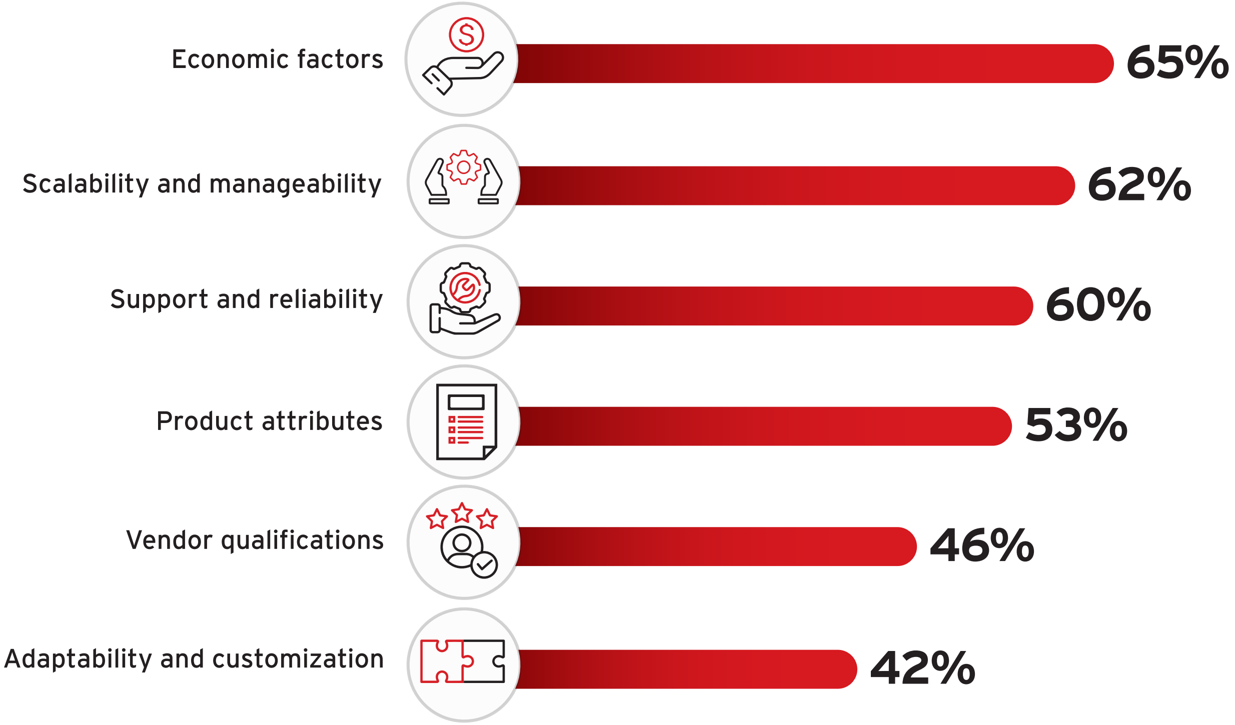
Selecting Cloud Security Solutions

Selecting the right cloud security solutions is a critical decision for organizations aiming to enhance their security posture while maintaining operational efficiency and cost-effectiveness. As organizations navigate the barriers to cloud adoption, understanding the criteria they consider when evaluating cloud security solutions becomes crucial.

Economic factors are the most significant consideration, with 65% of respondents emphasizing cost, contract terms, and overall value for money. This is consistent with budget constraints as a major barrier to cloud security migration noted earlier, highlighting the need for cost-effective solutions that do not compromise on quality or functionality. Scalability and manageability, cited by 62% of participants, reflects the necessity for solutions that can grow and adapt with the organization, a response to the dynamic nature of cloud environments and their security needs.

Support and reliability are crucial, as highlighted by 60% of respondents who emphasize the need for dependable service and robust support to maintain effective security measures. Additionally, 53% of respondents value product attributes such as functionality, performance, and ease of use, indicating that organizations are seeking solutions that fulfill their security requirements and are also user-friendly and efficient in operation.

What criteria do you consider most important when evaluating a cloud security solution?



Organizations should carefully consider these criteria to choose solutions that not only offer technical compatibility and robust security features but that also align with broader business and operational goals. Achieving a balance of these factors can significantly enhance the effectiveness of cloud security implementations and support long-term organizational security strategies.

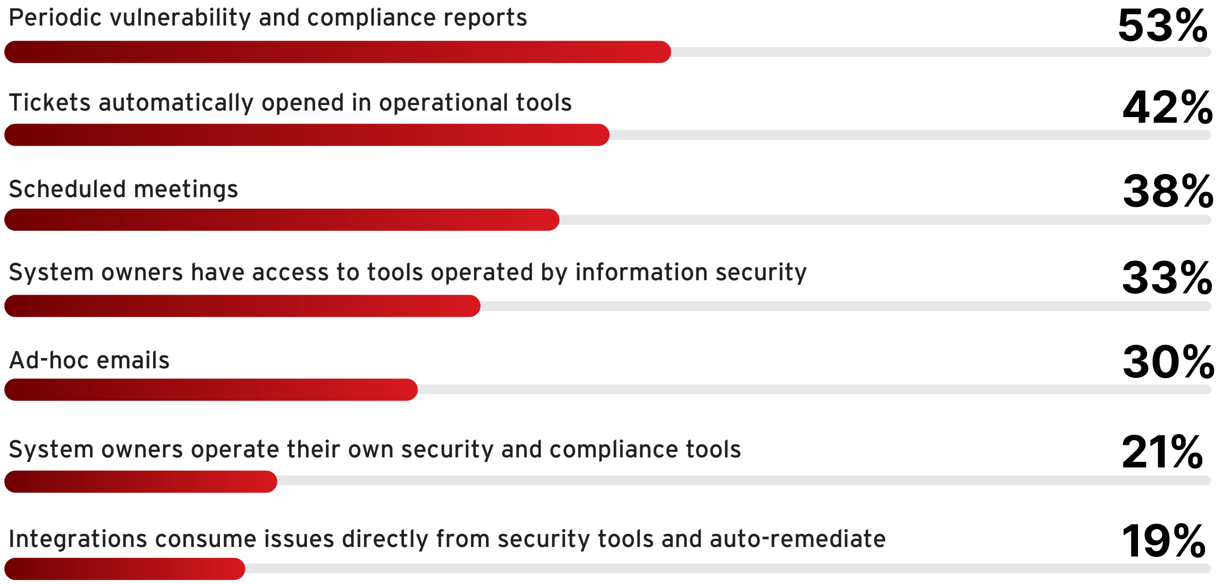
Strategies for Remediation of Security and Compliance Issues

As organizations refine their criteria for selecting cloud security solutions, understanding how they manage the remediation of security and compliance issues becomes equally important. Effective remediation is critical for maintaining cloud security integrity and ensuring that threats and vulnerabilities are addressed promptly and efficiently.

The survey responses reveal that periodic vulnerability and compliance reports are the primary method for managing remediation, utilized by 53% of organizations. This approach is aligned with the need for continuous monitoring and reporting mechanisms that enable organizations to stay ahead of potential security breaches and compliance issues.

Automatic ticket opening in operational tools like Jira or ServiceNow, employed by 42% of respondents, underscores the trend towards automation in security processes, enabling faster and more reliable responses to identified issues. Additionally, scheduled meetings for remediation management, utilized by 38% of respondents, illustrate the importance of regular communication and coordination among security teams to address vulnerabilities collaboratively. This is especially relevant in complex cloud environments where configuration and misconfiguration management pose ongoing challenges.

What are your primary methods for managing remediation of security and compliance issues with system owners?



Integrating these remediation strategies with cloud-native security solutions can boost their effectiveness. For example, leveraging advanced cloud security platforms that provide automated compliance checks and integrate seamlessly with incident response tools can streamline the remediation process. These platforms can offer comprehensive visibility across cloud environments, which is crucial for detecting and addressing security issues proactively. Incorporating best practices such as the principle of least privilege and regular security audits into the remediation process can further strengthen cloud security. These practices help in minimizing the attack surface and ensuring that the security measures are robust and responsive to evolving threats.

Cadence of Security Remediation

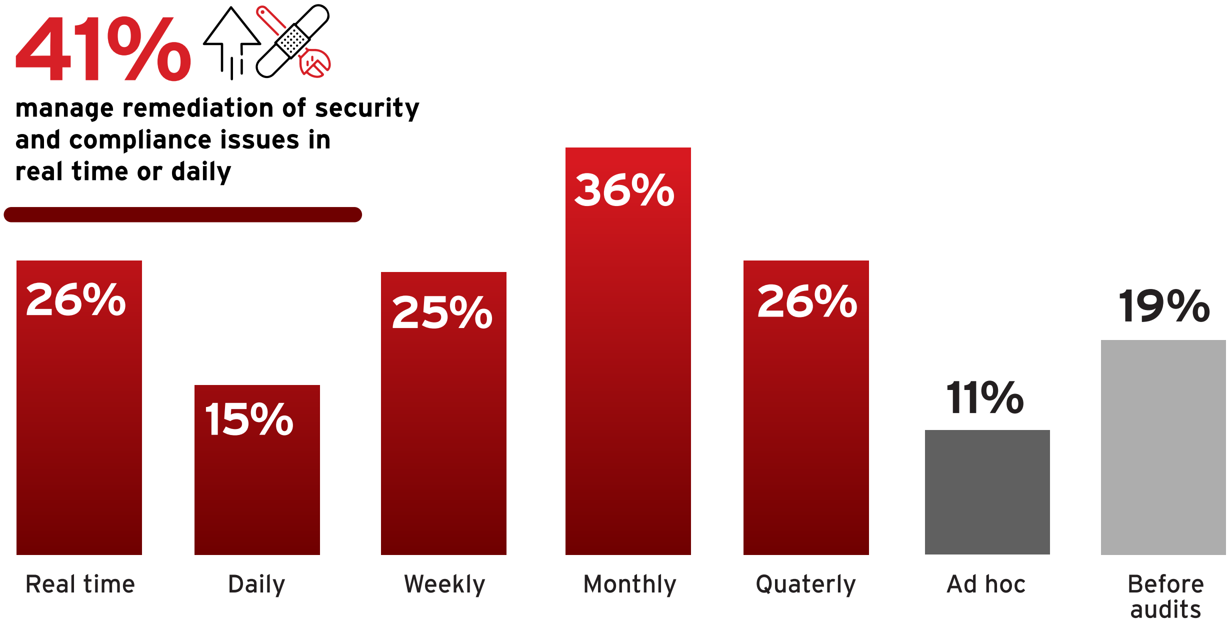
Building on the discussion about how organizations manage the remediation of security and compliance issues, it's essential to examine the cadence at which these remediations are conducted. A structured remediation schedule ensures that risks and vulnerabilities are addressed consistently and that security measures are reinforced regularly to counteract the evolving threat landscape.

According to the survey, the most frequent approach to remediation management is daily or even real-time remediation of security and compliance issues, at 41% collectively.

This is followed by 36% of organizations that execute a monthly cadence. This periodic approach allows organizations to regularly assess and address vulnerabilities without overwhelming system operations, balancing responsiveness with manageability. Weekly reviews are also common, with 25% of respondents adhering to this schedule, indicating a need for more frequent oversight in environments with higher transaction volumes or sensitive operations.

Interestingly, 30% of organizations handle remediation on an ad-hoc basis (11%) or before audits (19%), suggesting that while they have systems in place for regular checks, they adopt a more reactive approach to security threats.

Outside of critical vulnerabilities, what is the cadence for managing remediation of security and compliance issues with system owners? (Select all that apply)



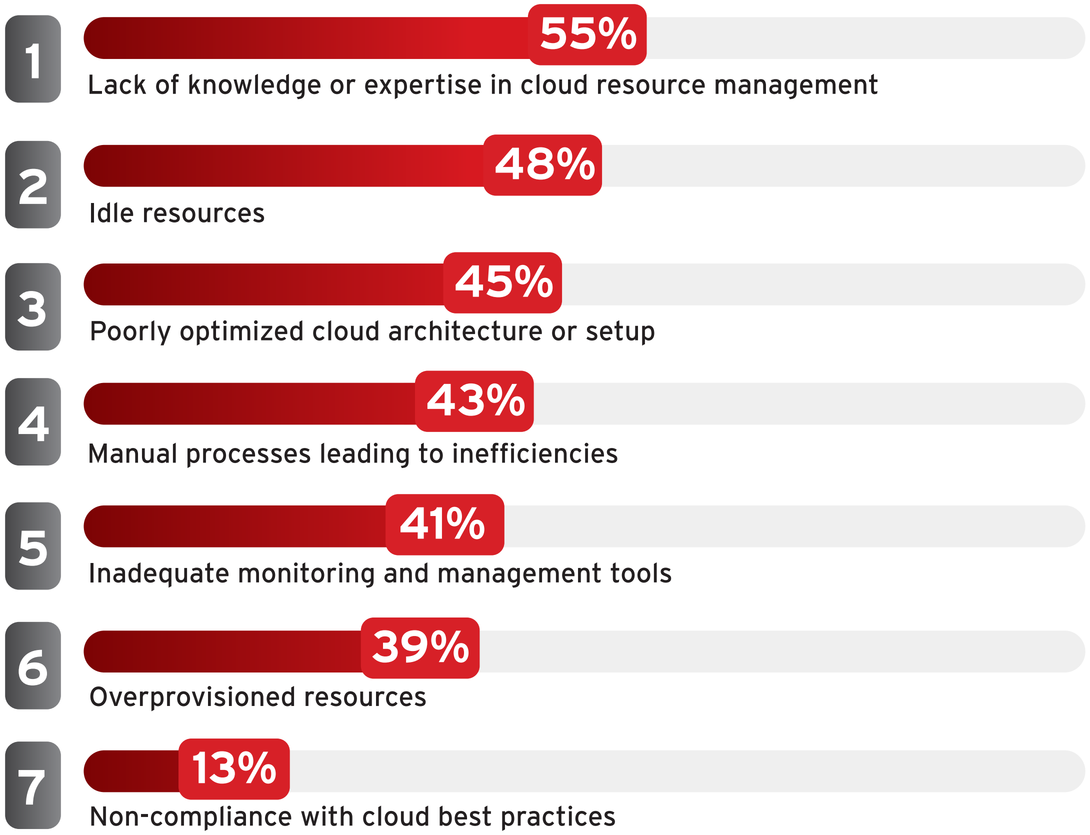
To optimize the effectiveness of their remediation processes, organizations might consider aligning their remediation cadence with the risk levels of different systems and the nature of the threats they face. For instance, more critical systems might require weekly reviews, while others might suffice with a monthly check. Adopting flexible, yet systematic approaches to remediation can help organizations maintain robust security without overwhelming their resources. This also encourages a proactive, automated stance in security management, where threats are addressed swiftly and efficiently, minimizing potential damage.

Curbing Cloud Resource Waste

The continuity of streamlining operational efficiency extends into the management of cloud resources. Efficient resource utilization is not only pivotal for reducing costs but also for enhancing the overall performance of cloud operations. Understanding the factors contributing to cloud waste is essential for devising effective strategies to mitigate it.

Survey responses identify a lack of knowledge or expertise in cloud resource management as the most significant contributor to cloud waste, noted by 55% of respondents. This challenge ties into previous concerns about staff expertise, underscoring the importance of continuous education and training in cloud technologies for efficient cloud management. Idle resources, cited by 48% of respondents, and poorly optimized cloud architecture, highlighted by 45%, also contribute significantly to cloud waste. These issues mirror the configuration and misconfiguration management challenges discussed earlier, where proper configuration is vital for optimizing resource use and securing the cloud environment.

Which of the following factors contribute to cloud waste in your organization?



To combat cloud waste, organizations should focus on enhancing their cloud management practices by investing in training programs that elevate the cloud competency of their workforce. Implementing automated resource management tools that can dynamically adjust resources based on load and usage patterns can also markedly reduce waste. Additionally, conducting regular audits to identify and decommission underutilized or redundant resources can lead to more efficient cloud utilization and cost savings.

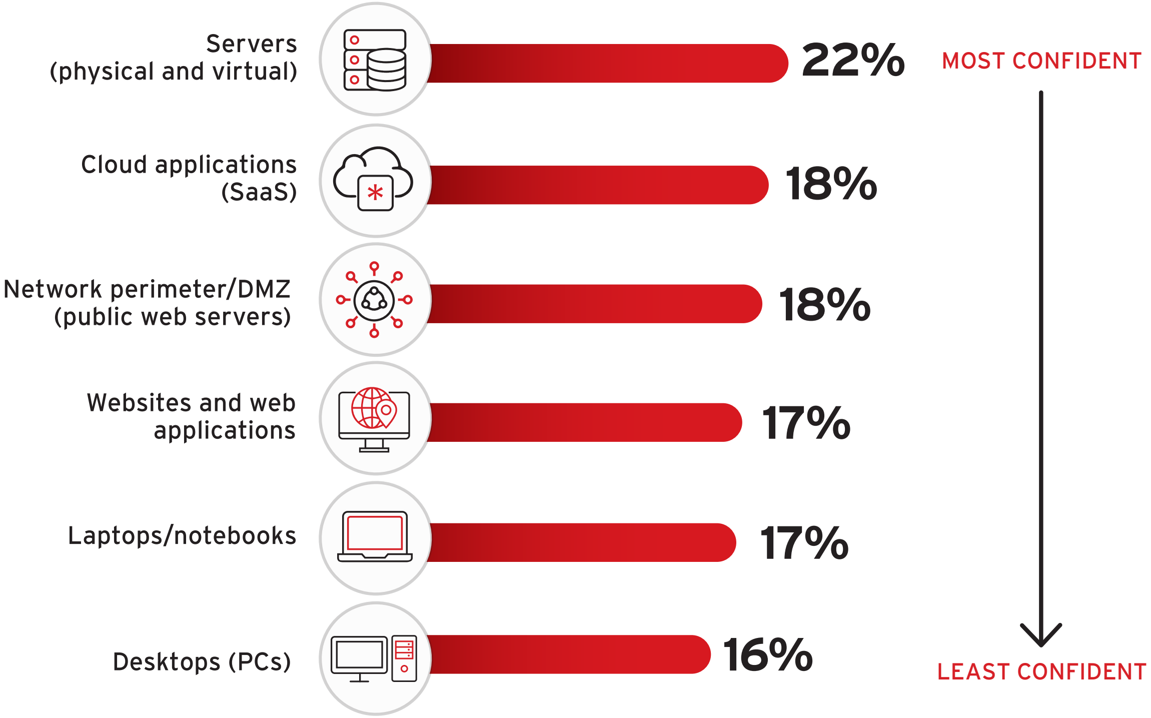
Securing Critical Cloud Components

Reevaluating where IT and cybersecurity professionals place their confidence in securing various cloud components is essential for understanding and addressing potential vulnerabilities within cloud security frameworks.

The survey results indicate varying levels of confidence in security across different cloud components. While ranked at the top of the list, only 22% of IT professionals report confidence in securing servers, both physical and virtual.

This indicates ongoing challenges and potential vulnerabilities in securing these critical components of cloud architecture, which are often targets for sophisticated cyber attacks due to their crucial roles in cloud operations and data exchange.

Of the following components, which are you confident in being able to secure in the cloud?



To enhance security where confidence is lower, organizations should invest in specialized training and advanced security technologies that cater specifically to these areas. Strengthening API security with rigorous access controls, encryption, and regular audits, and enhancing IaaS/PaaS security through comprehensive monitoring and incident response strategies are essential. Adopting integrated security solutions that provide visibility across all cloud components can also help organizations maintain a robust security posture, adhering to best practices that advocate for a comprehensive and proactive approach to cloud security.

Additional responses include: Cloud infrastructure 13% | Containers 13% | Datastores 12% | Application programming interfaces (APIs) 11% | Mobile devices 10% | Industrial Control System (ICS) / SCADA devices 7% | Internet of Things (IoT) 3%

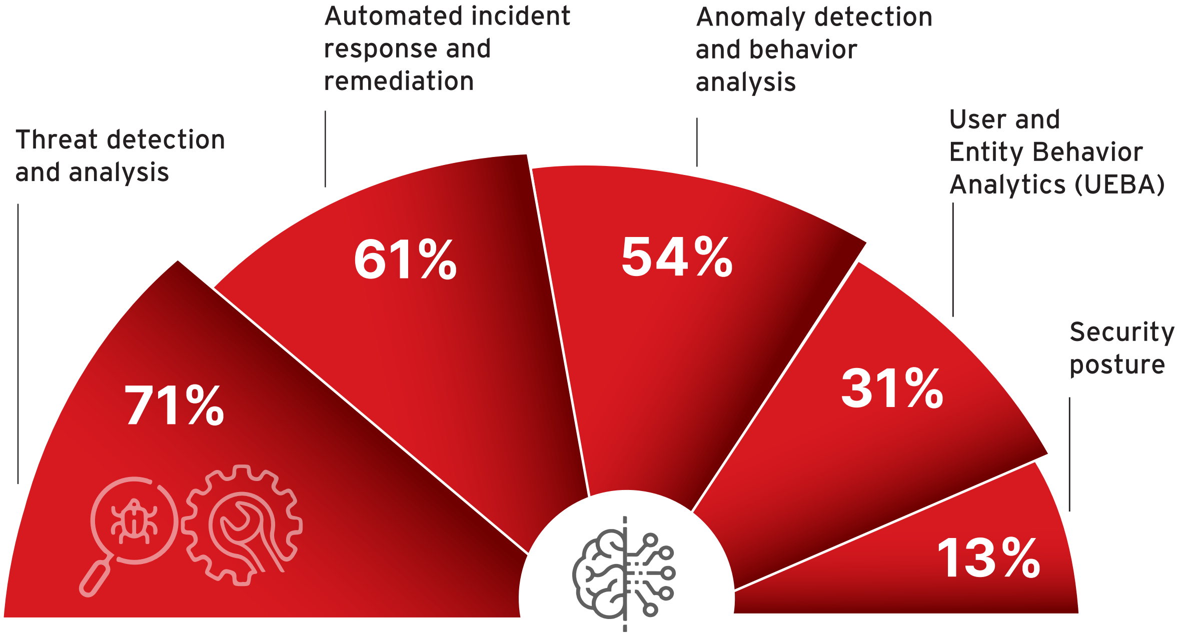
AI-Security Priorities

The integration of Artificial Intelligence (AI) in cloud security is a critical enhancement to cybersecurity strategies. This shift is mirrored in the preferences expressed by IT and cybersecurity professionals regarding which AI-driven features they consider most valuable for ensuring robust security across their cloud environments.

Threat detection and analysis is identified as the most valuable AI-driven feature, with 71% of respondents recognizing its importance. This highlights the critical role AI plays in identifying and analyzing emerging threats in real time, a necessity in the dynamic cloud environment where threat landscapes evolve rapidly. Automated incident response and remediation, valued by 61% of respondents, underscores the need for swift, automated actions that reduce the time from threat detection to response, thereby enhancing the overall security resilience. Anomaly detection and behavior analysis, chosen by 54%, further demonstrates the reliance on AI to understand and predict unusual behaviors within cloud systems that could indicate security breaches.

Less prioritized but still significant, User and Entity Behavior Analytics (UEBA) and security posture management are seen as valuable by 31% and 13% of respondents, respectively. These technologies play essential roles in fine-tuning the security measures based on user behavior and maintaining the overall health and security readiness of cloud infrastructures.

Which AI-driven cloud security features do you consider most valuable?



Incorporating these AI features supports a more proactive security posture, aligning with the previously discussed emphasis on enhancing threat detection and incident management capabilities. For organizations, the focus should be on adopting cloud security solutions that integrate these AI functionalities seamlessly to provide a sophisticated, layered defense mechanism. This approach is not only about leveraging technology but also about ensuring it works cohesively within the broader security infrastructure to effectively address specific vulnerabilities and threats.

Enhancing Cloud Security: Key Practices for Robust Defense

Effective management of cloud security is vital for protecting data, maintaining privacy, and ensuring continuous business operations. Drawing on survey insights and industry-leading approaches, here are essential practices to strengthen your cloud security management:

Implement Comprehensive Threat Detection: Adopting a holistic approach to threat detection is crucial. Incorporate systems that provide comprehensive monitoring across all cloud layers to detect and respond to threats promptly. With 71% of survey respondents recognizing the importance of AI-driven threat detection, this strategy emphasizes the necessity of leveraging advanced technologies to enhance security responsiveness and effectiveness.

Automate Incident Response: Automation of incident response is not just beneficial; it's essential for maintaining pace with the rapid evolution of the threat landscape. An impressive 61% of professionals advocate for automated response mechanisms to ensure quick and effective action against threats, highlighting the need for systems that can autonomously react to and mitigate potential breaches immediately.

Prioritize API Security: With 49% of survey participants concerned about API security, it's clear that protecting these critical interfaces is a priority. Implement rigorous security protocols, including regular audits, robust access controls, and continuous monitoring, to safeguard APIs against unauthorized access and ensure the integrity of data flows.

Strengthen Identity and Access Management: Effective management of access rights is vital for preventing unauthorized access, a major concern for 59% of respondents. Enhancing identity and access management systems with advanced multi-factor authentication methods and zero trust principles can significantly secure sensitive data and systems against illicit access attempts.

Conduct Regular Security Audits: Adopt continuous compliance monitoring and utilize cloud-native tools for regular security audits to align with regulatory requirements and address vulnerabilities. This practice is essential for maintaining an up-to-date security posture and ensuring all systems and policies adhere to the highest standards.

Invest in Targeted Security Training: As 80% of respondents believe additional training is necessary, investing in specialized education programs for your team is crucial. Tailor training to address the unique challenges of cloud security, ensuring personnel are equipped to handle the latest threats and security technologies effectively.

Optimize Resource Management: Efficient cloud resource management is highlighted by 55% of professionals as key to reducing operational costs and preventing resource wastage. Utilize intelligent tools that optimize cloud resource allocation, ensuring optimal performance without compromising security.

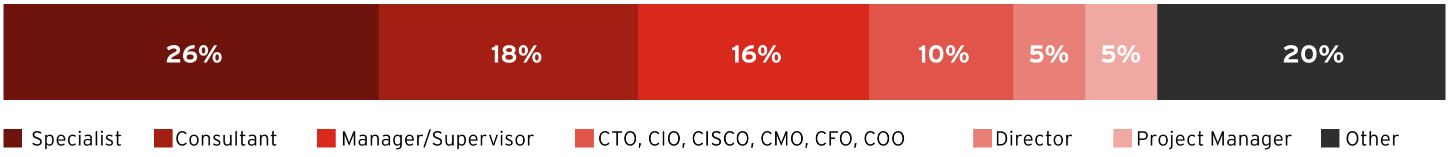
Adopt a Centralized Security Management Platform: A unified security management platform can greatly simplify the oversight of diverse cloud services. With 96% of respondents finding such a platform helpful, it's clear that centralizing security management helps with improving visibility across all cloud assets, simplifying the enforcement of security policies and accelerating response times.

These practices form the foundation of a proactive and resilient cloud security strategy, ensuring organizations can defend against today's dynamic threat environment while preparing for future challenges.

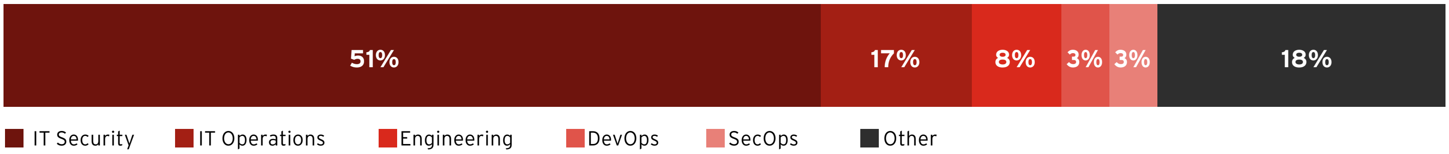
Methodology & Demographics

The 2024 Cloud Security Report is based on an extensive survey of 411 cybersecurity professionals conducted in June 2024. The study explored how cloud user organizations adopt the cloud, their perceptions of cloud security evolution, and the best practices IT cybersecurity leaders prioritize in their cloud transition. The respondents encompass technical executives and IT security practitioners, providing a balanced representation of organizations of diverse sizes across a wide range of industries.

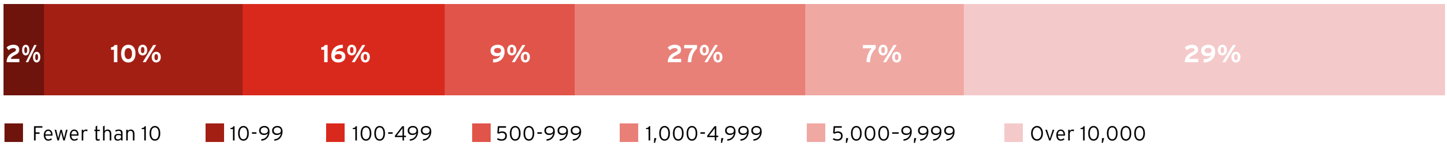
CAREER LEVEL



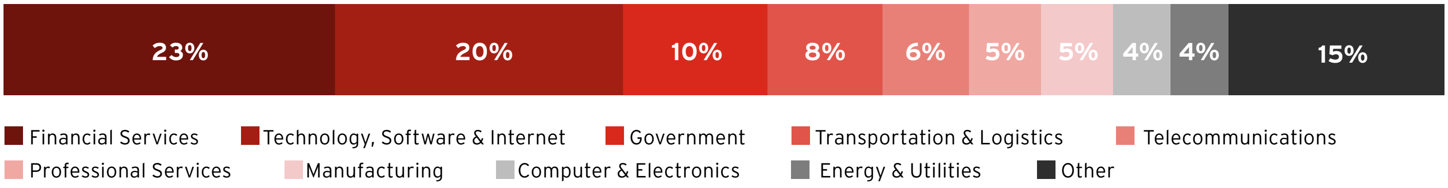
DEPARTMENT



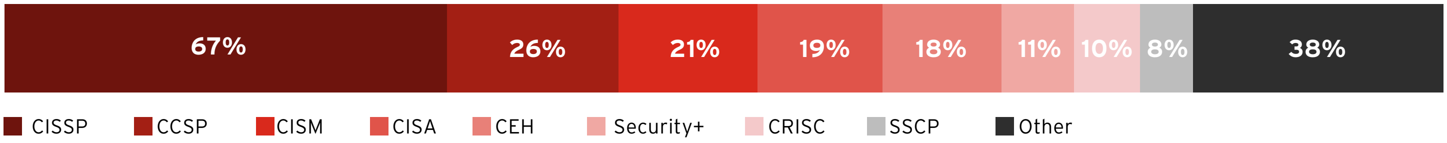
COMPANY SIZE



INDUSTRY



SECURITY CERTIFICATIONS HELD



TREND MICRO™

At Trend Micro, everything we do is about making the world a safer place for exchanging digital information.

As your business continues to navigate its cloud journey, moving from migration and optimization to cloud-native application development, your security challenges continue to evolve.

Trend Vision One – Cloud Security unites your cloud security teams with SecOps, ensuring protection across your entire cloud infrastructure. Whether you're just starting out or refining your approach, we help you stop threats swiftly and manage risk confidently. Our cutting-edge, AI-powered platform delivers deep visibility, early detection, rapid response, and risk reduction across varied hybrid cloud environments.

As a global cybersecurity leader, our platform, threat intelligence, and services are deployed by over 500,000 enterprise customers across 175 countries and recognized by third-party reviewers and industry analysts.

www.TrendMicro.com

Cybersecurity

INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at **info@cybersecurity-insiders.com** or visit **cybersecurity-insiders.com**