2022

Cybersecurity INSIDERS

AWS CLOUD SECURITY REPORT

Fidelis Cybersecurity

INTRODUCTION

Cloud environments are increasingly complex, while threats continually evolve. This trend makes simplified cybersecurity imperative to meet both operations and compliance requirements. To close security gaps, organizations are looking for unified cybersecurity platforms to better manage complexity and maintain both visibility and control.

The 2022 AWS Cloud Security Report is based on a comprehensive survey of 578 cybersecurity professionals to reveal how AWS user organizations are responding to evolving cloud security threats, and what tools and best practices cybersecurity leaders prioritize as their cloud infrastructures mature.

Key survey findings include:

- Virtually all organizations in our survey have some public cloud footprint. While AWS is still the predominant cloud provider, a majority of organizations (87%) use two or more cloud providers.
- More than two of three organizations (67%) use between three to six different dashboards to configure cloud security policies, significantly increasing the cost and complexity of managing security across multi-cloud environments.
- Ninety-five percent of organizations agree that it would be helpful to have a single cloud security platform with a single dashboard to configure all policies needed to consistently and comprehensively protect data across their cloud footprint.
- Eighty-one percent of organizations have an intermediate to leading cloud maturity level. However, despite this growing maturity level with the cloud, consistent with previous years, 95% of security professionals are moderate to extremely concerned about the security of public clouds, signaling a need for adoption of better security tools and practices.
- Fifty-eight percent of organizations state that they will deploy a new cloud security solution in the coming year.

We would like to thank Fidelis Cybersecurity for supporting this important research.

We hope you find this report informative and helpful as you continue your efforts in securing your journey into the cloud.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

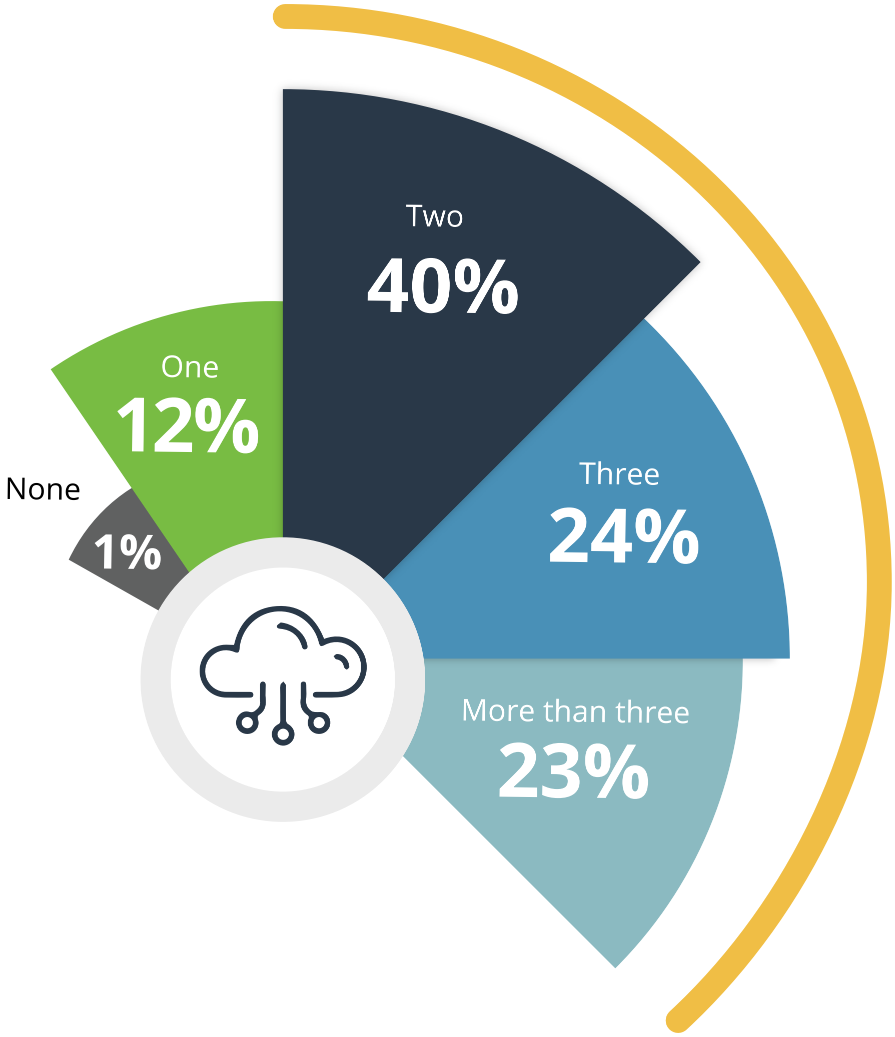
Cybersecurity
INSIDERS

CLOUD DEPLOYMENT STRATEGIES

Virtually all organizations now have some public cloud footprint. While AWS is still the predominant cloud provider, an overwhelming majority of organizations (87%) use two or more cloud providers.

However, the more cloud providers an organization uses, the more inherently complex the infrastructure becomes. The addition of multiple cloud-native security tools compounds challenges for security teams. These solutions add their proprietary methods and dashboards for policy/rule configuration, along with varying techniques and cadences for monitoring, reporting, and remediating security issues.

How many cloud providers does your organization currently use?



87% of organizations that are in the cloud use two or more cloud providers

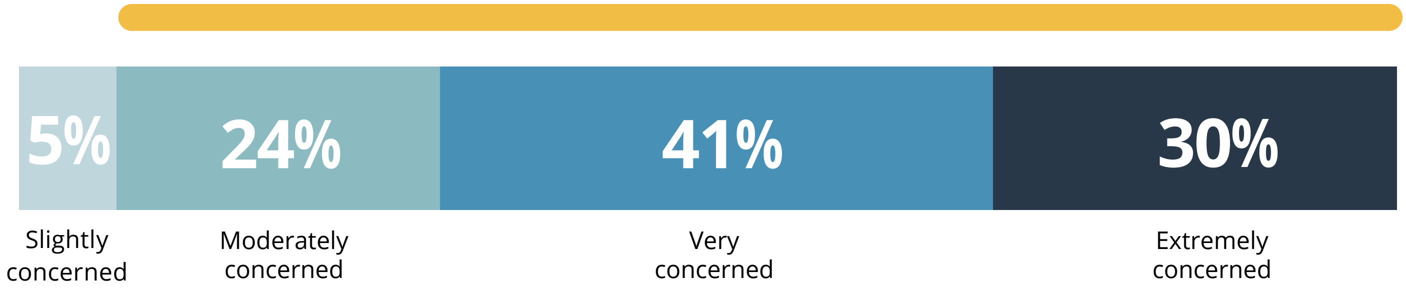
Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

CLOUD SECURITY CONCERNS

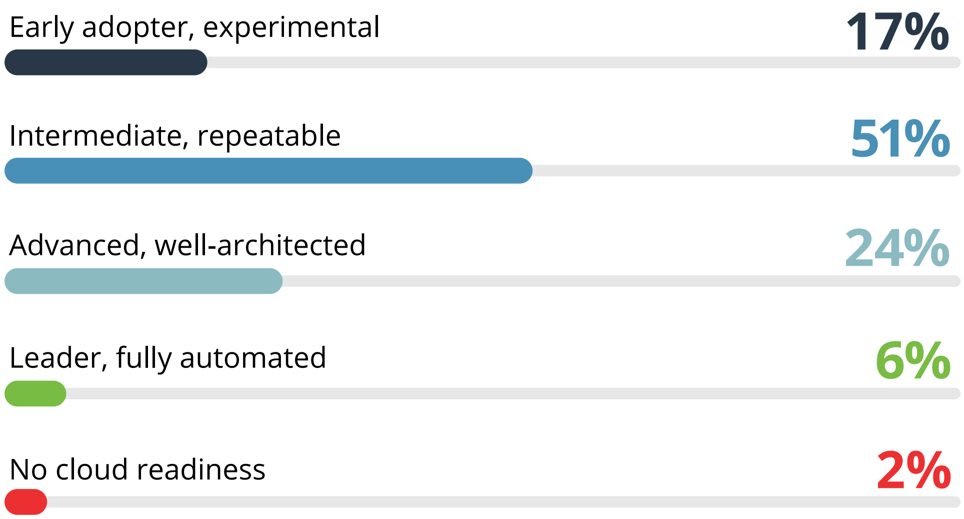
Eighty-one percent of organizations have an intermediate to leading cloud maturity level. However, despite this growing maturity level with the cloud, consistent with previous years, 95% of security professionals are moderately to extremely concerned about the security of public clouds. This continued trend signals a critical need for cloud security solutions that keep pace with increasingly complex environments and evolving threat landscapes.

How concerned are you about the security of public clouds?

95% organizations are concerned about cloud security, which is consistent with the findings over the past three years



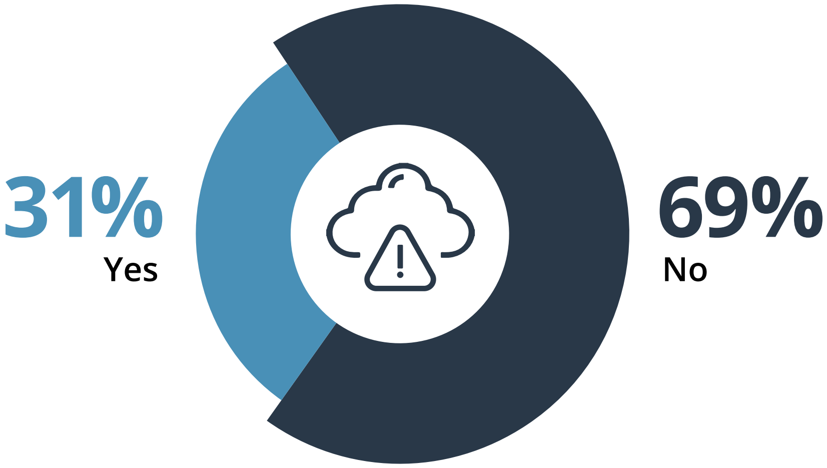
How would you describe your organization's cloud maturity level?



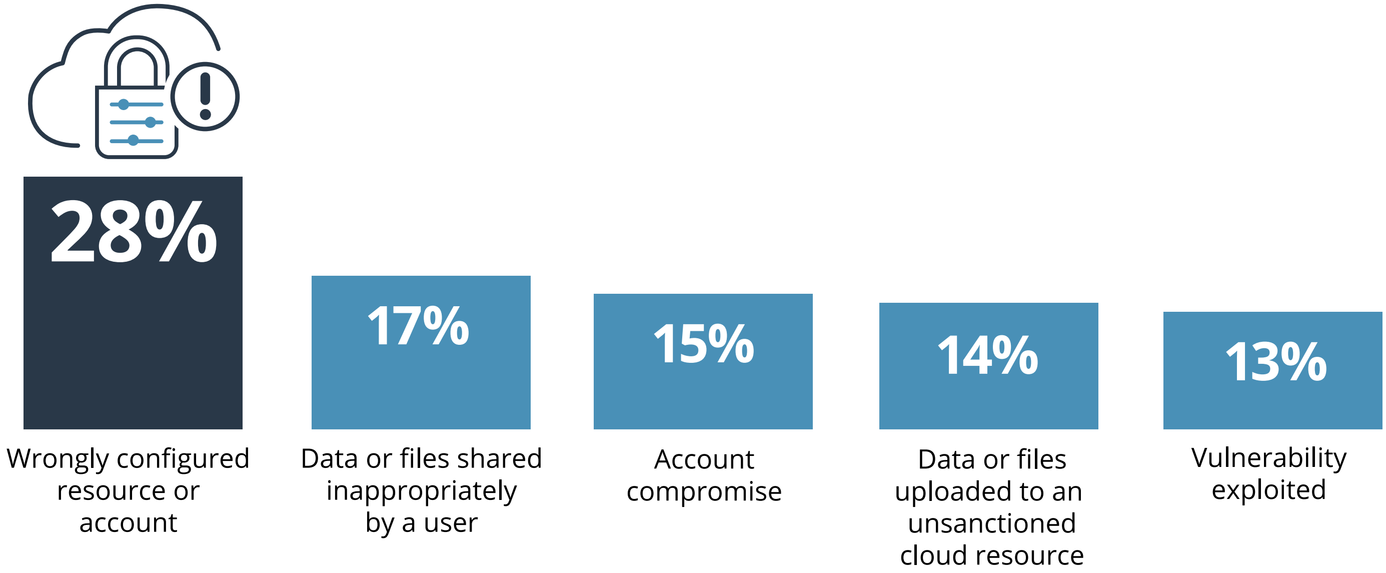
CLOUD SECURITY INCIDENTS

Security incidents happen. For the 31% of organizations that experienced a security incident in the cloud, misconfiguration was the leading cause (28%), followed by inappropriately shared data (17%) and account compromise (15%). Exploited vulnerabilities account for 13% of incidents, highlighting a need for automated compliance monitoring to catch common issues.

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



If yes, what type of incident was it (select all that apply)?



Data or files downloaded to an unsafe device 10% | Malware infection 9% | Other 7%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

CLOUD NATIVE SECURITY VS INDEPENDENT

Sixty-two percent of organizations use native cloud security controls rather than an independent security vendor for their cloud security needs. The most important decision factors include cost (63%), solution complexity (58%), and ease of use (57%).

Do you prefer cloud native security controls or using an independent security vendor for your cloud security needs?

62%

Cloud native security controls

38%

Independent cloud security vendor

What criteria are most important to you when deciding between cloud native vs independent cloud security solutions?

63%

Cost

58%

Less solution complexity and already well integrated

57%

Ease of use

50%

Performance

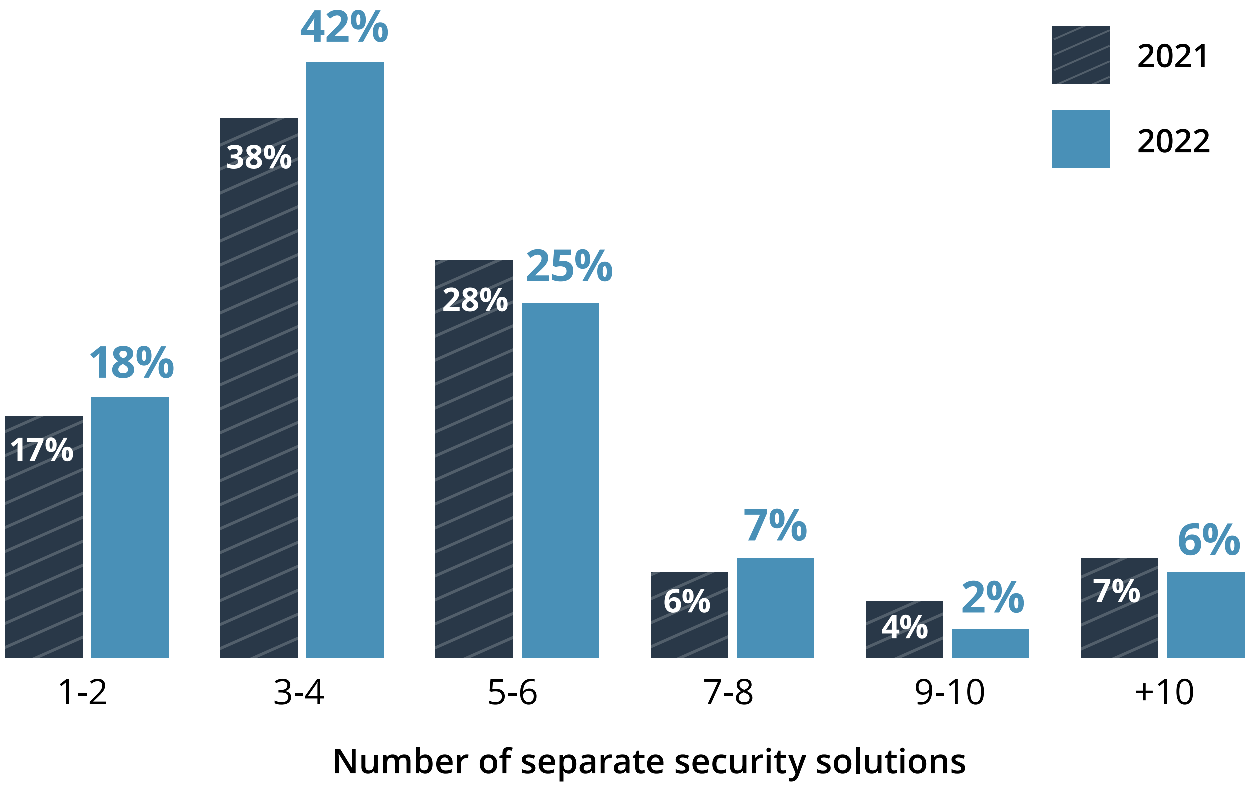
Quicker deployments 36% | No need to manage another vendor 31% | Cloud vendor security is good enough, why would I need anything else? 13% | Other 9%

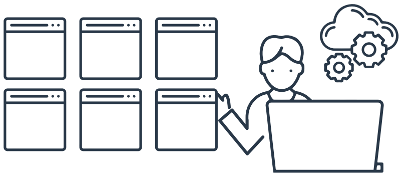
Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

SECURITY DASHBOARDS

More than two of three organizations (67%) use between three to six different dashboards to configure cloud security policies, significantly increasing the cost and complexity of managing security across multi-cloud environments. Utilizing multiple configuration solutions also negatively impacts security posture, highlighting the need for comprehensive security solutions for multi and hybrid cloud deployments.

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





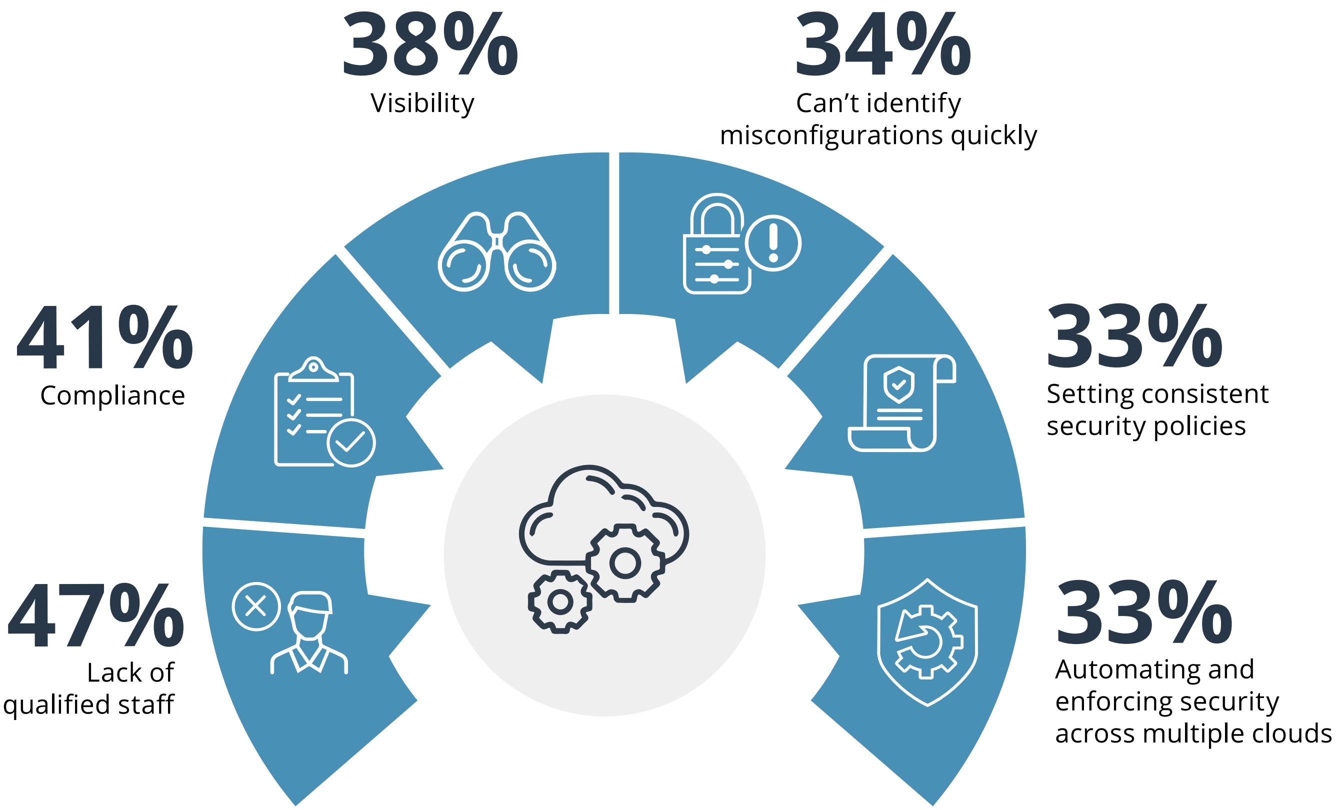
67% of organizations still use between **three to six different dashboards** to configure cloud security policies

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

OPERATIONAL SECURITY HEADACHES

We asked cybersecurity professionals about their biggest operational, day-to-day headaches when protecting cloud workloads. While cloud-native security tools offer beneficial coverage of their environments, the more complex a multi-cloud environment grows, the more challenging it is to keep an organization secure. The biggest challenges security professionals highlighted include a lack of qualified staff (47%), followed by compliance (41%) and visibility issues (38%).

What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

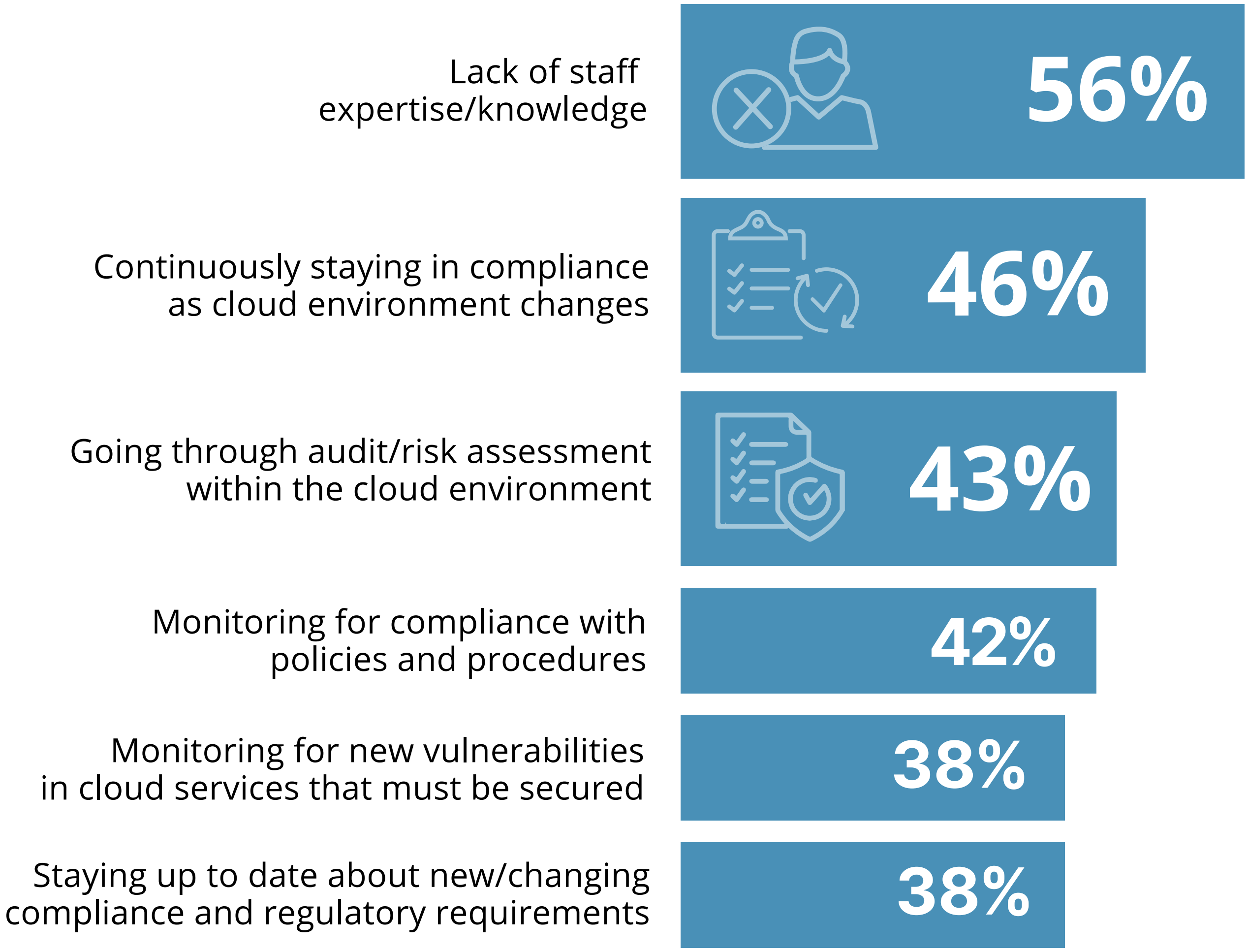


Implementing continuous and automated security controls in the cloud 32% | Complex cloud to cloud/cloud to on-prem security rule matching 28% | Setting the correct user access privileges 28% | Lack of integration with on-prem security technologies 27% | Securing access from personal and mobile devices 26% | Security can't keep up with the pace of changes to new/existing applications 26% | Justifying more security spending 26% | Securing traffic flows 25% | Remediating threats 25% | No automatic discovery/visibility/control to infrastructure security 24% | Reporting security threats 23% | Understanding network traffic patterns 23% | Lack of feature parity with on-prem security solution 15% | No flexibility 5% | Not sure/Other 8%

CLOUD COMPLIANCE CHALLENGES

Cloud compliance presents additional challenges, which increase significantly with the number of cloud providers. Fifty-six percent of cybersecurity professionals cite an increase in staffing challenges with diverse cloud implementations. For every cloud provider, security staff must understand the organization's security policies and compliance requirements and how to implement those policies. Knowledge of CIS benchmarks and cloud security best practices across multiple cloud providers is also required.

Which part of the cloud compliance process is the most challenging?



Scaling and automating compliance activities 29% | Applying/following the Shared Responsibility Model 22% | Data quality and integrity in regulatory reporting 22% | Not sure/other 6%

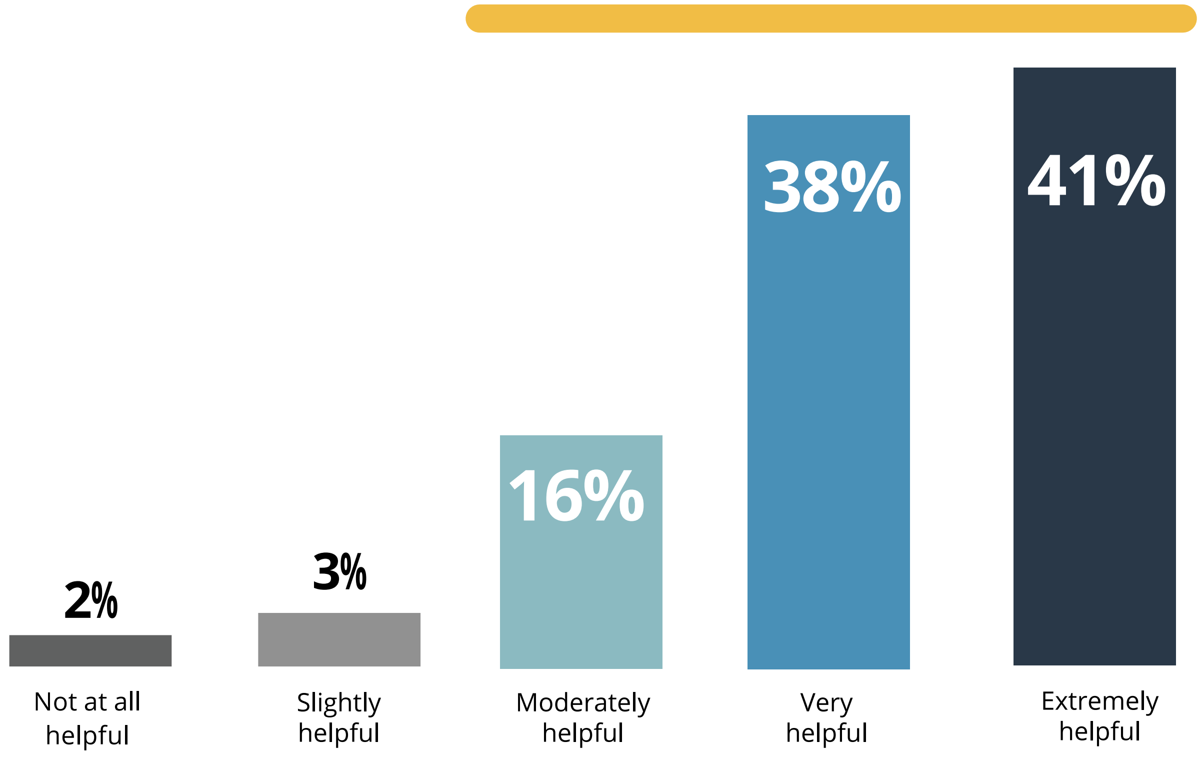
SINGLE CLOUD SECURITY PLATFORM

We asked cyber professionals how helpful it would be to have a unified cloud security platform with a single dashboard. Security leaders overwhelmingly see the value in such a solution. Ninety-five percent of organizations agree that it would be moderately to extremely helpful to have a single cloud security platform with a dashboard to configure all policies needed to consistently and comprehensively protect data across their cloud footprint.

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?

95%

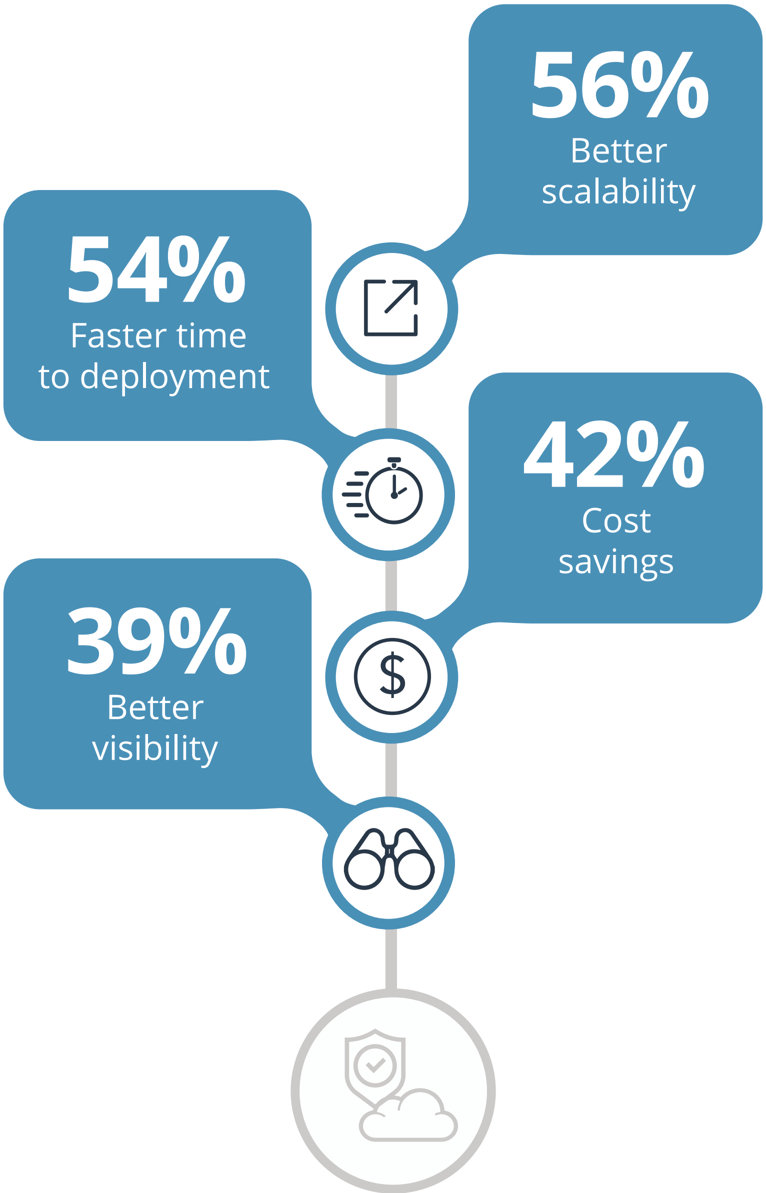
of organizations agree that it would be moderately to extremely helpful to have a single cloud security dashboard



CLOUD-NATIVE SECURITY DRIVERS

Unified security solutions that are made in the cloud, for the cloud, solve many of the key challenges around multi-cloud security. Issues addressed by a unified solution include visibility, scalability, and deployment speed, and they can even reduce costs. Our survey participants confirm that the biggest drivers for cloud-based security solutions include better scalability (56%), faster time to deployment (54%), and cost savings (42%).

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

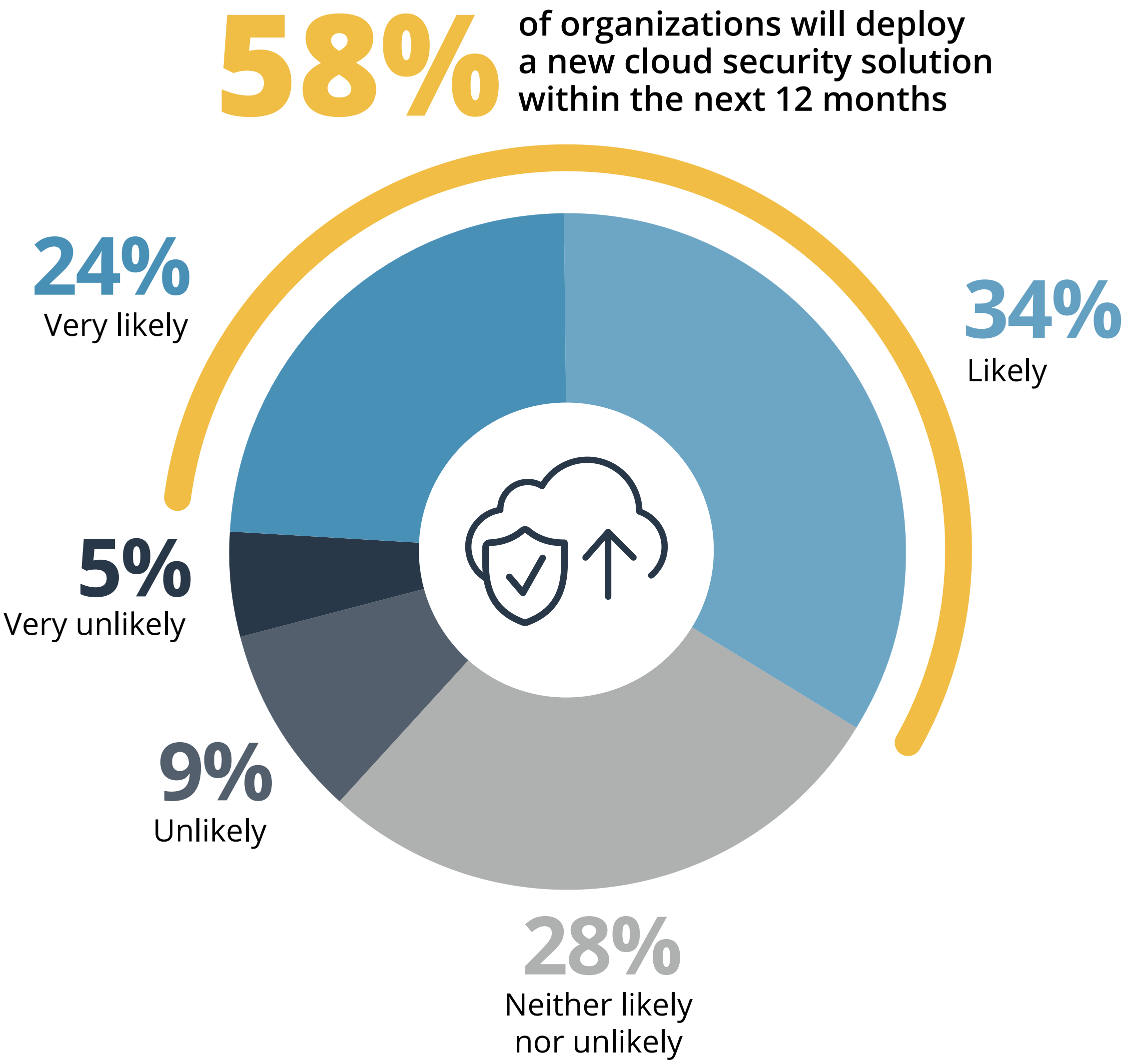


Meet cloud compliance expectations 38% | Better performance 35% | Our data/workloads reside in the cloud (or are moving to the cloud) 34% | Easier policy management 33% | Better uptime 33% | Need for secure app access from any location 32% | Reduction of appliance footprint in branch offices 26% | Other 1%

CLOUD SECURITY INVESTMENT

If you're looking into a new cloud security solution, you're not alone. Fifty-eight percent of organizations are finding new ways to implement cloud security in the next 12 months.

How likely is your organization to deploy a new cloud security solution within the next 12 months?

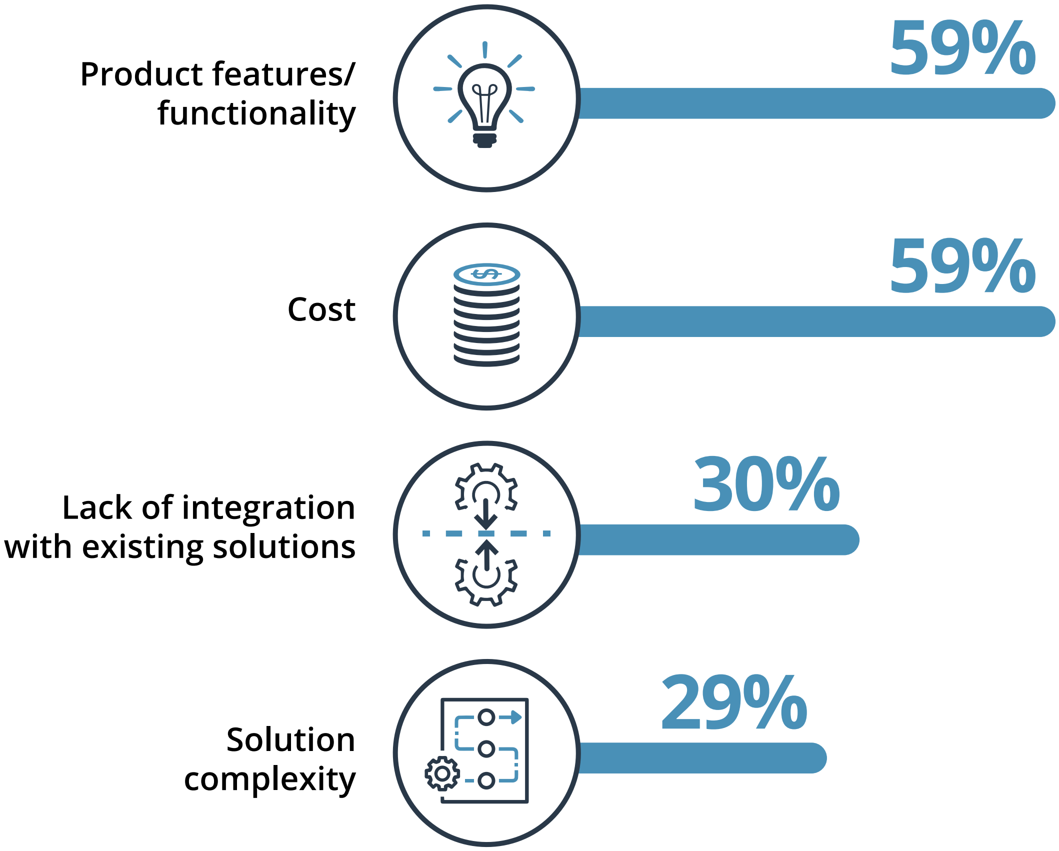


Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

SWITCHING CLOUD SECURITY VENDORS

Product features (59%) and cost (59%) are the main reasons cybersecurity professionals consider switching cloud security vendors. Additional considerations include lack of integration with existing solutions (30%) and solution complexity (29%). A unified cloud security solution can normalize controls across infrastructures as multi-cloud installations increase. Benefits include reducing costs by eliminating vendor contracts, providing improved integration with existing workflows regardless of the cloud provider, and significantly easing deployment and operational management complexities.

What are the main reasons why you would consider switching to a new cloud security vendor?



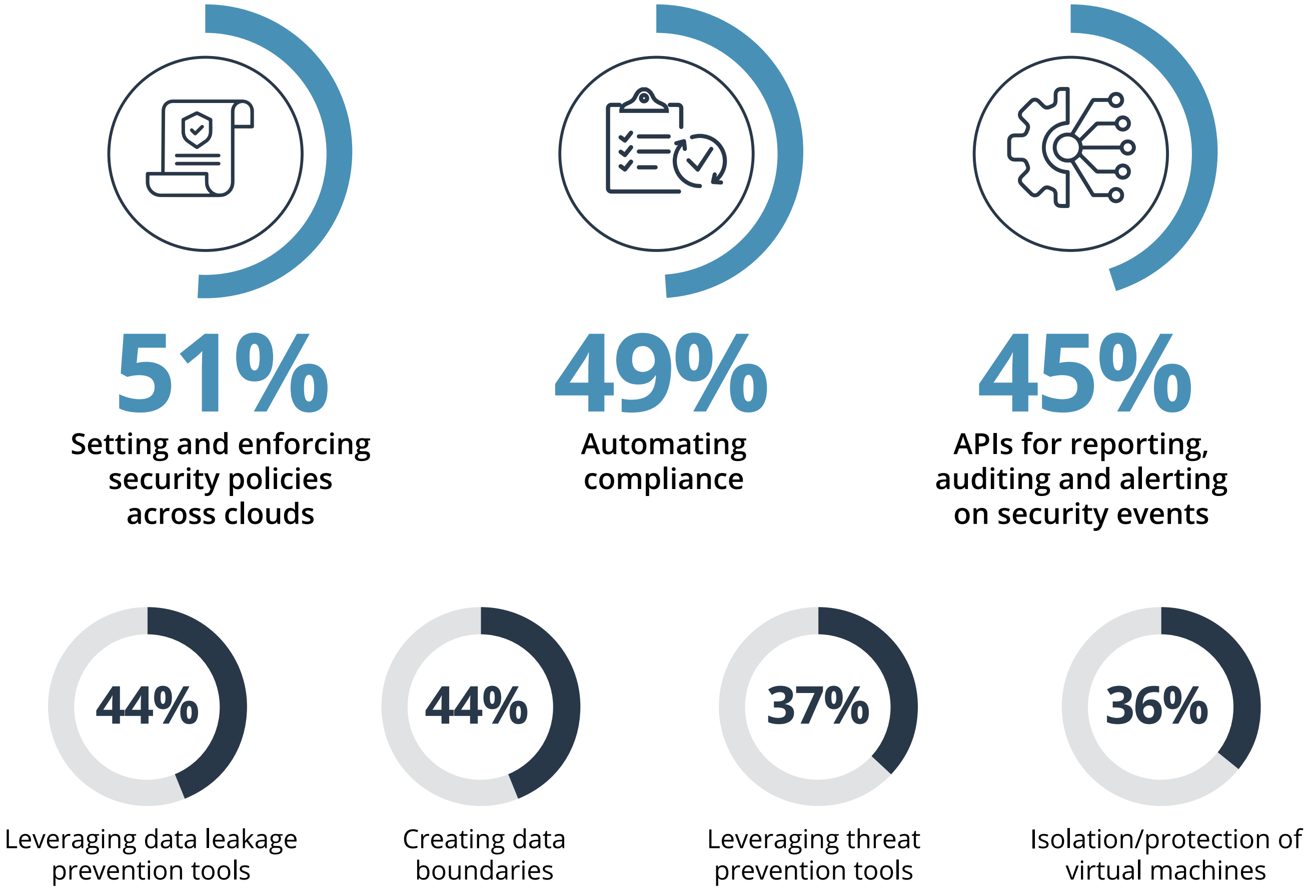
Support issues 27% | Poor product performance 24% | Contract/term 22% | Lack of scalability 20% | Provider inflexible in offering new/ requested features 19% | Lack of ability to customize 19% | Lack of comprehensive, consistent protections 19% | Lack of ease of use 19% | Too many false positives 16% | Stalled/complicated deployments 16% | Too many point solutions to manage 14% | Migrating to a Managed Service 14% | Provider's willingness to adapt and support our specific use case 14% | Inflexible terms / contract rigidity 13% | Too complicated to add new data feeds 9% | Customer reviews 8% | Other 4%

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

CLOUD CONFIDENCE

We asked cybersecurity professionals which security controls would most increase their confidence in adopting public clouds. The ability to set and enforce security policies across multiple clouds tops the list of security controls to increase confidence (51%), closely followed by automating compliance (49%) and APIs for reporting, auditing, and alerting on security events (45%).

Which of the following security controls would most increase your confidence in adopting public clouds?

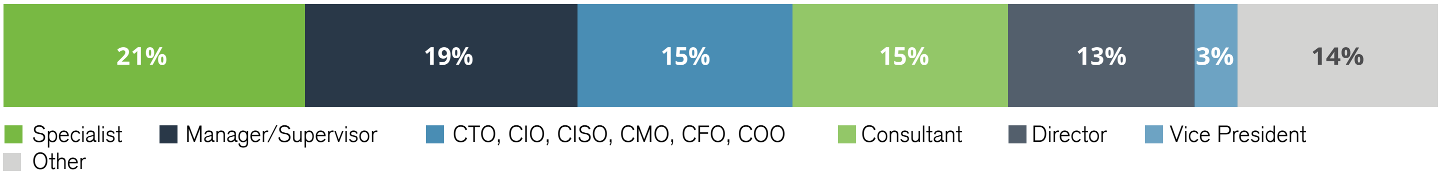


Limiting unmanaged device access 34% | Protecting workloads 32% | Proxying traffic for real-time security at accesss 25% | Other 2%

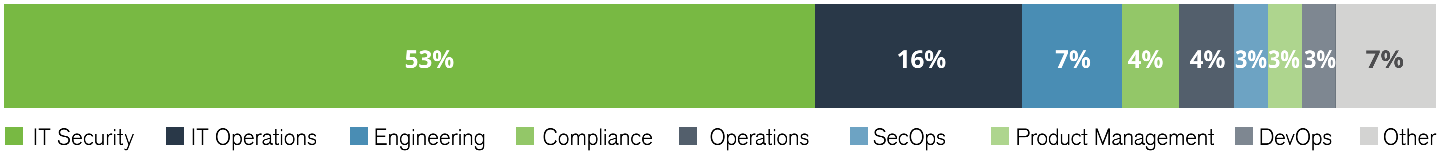
METHODOLOGY & DEMOGRAPHICS

This AWS Cloud Security Report is based on the results of a comprehensive online survey of 578 cybersecurity professionals, conducted in June 2022, to gain deep insight into the latest trends, key challenges, and solutions for cloud protection. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

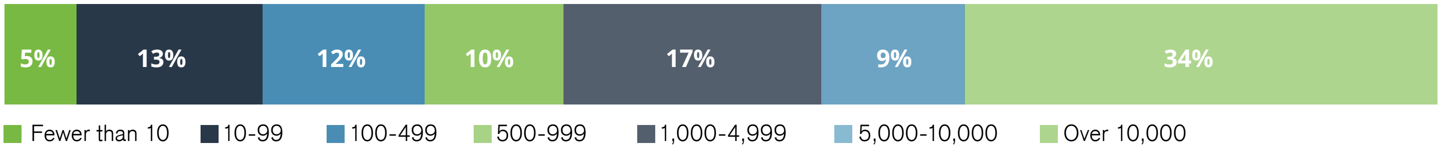
CAREER LEVEL



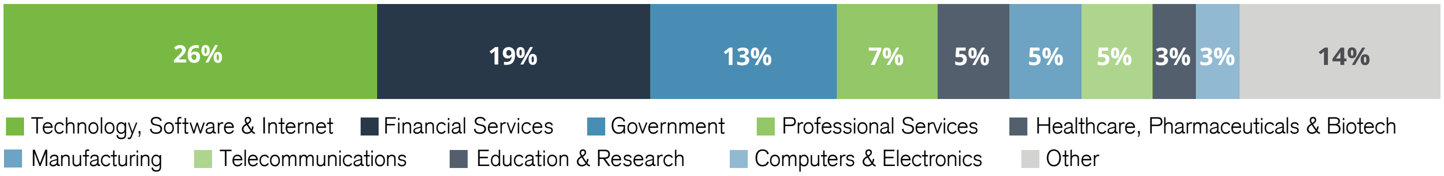
DEPARTMENT



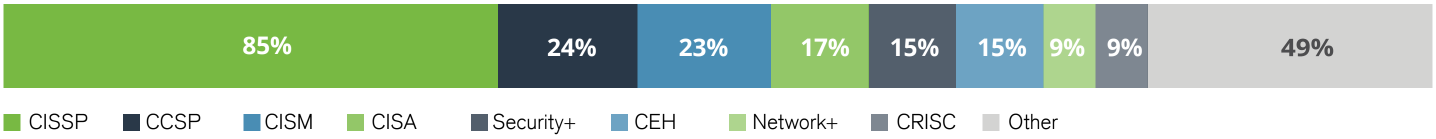
COMPANY SIZE



INDUSTRY



SECURITY CERTIFICATIONS HELD



Copyright © 2022 Cybersecurity Insiders. All Rights Reserved.

Fidelis® Cybersecurity

Safeguard your cloud infrastructure and keep up with the cloud-speed of digital transformation. Fidelis CloudPassage Halo® is a comprehensive cloud security platform that unifies and automates cybersecurity and maintains continuous compliance across IaaS, PaaS, servers, and containers. This fast, scalable, and cost-effective platform integrates directly into cloud environments to work seamlessly across any mix of public, private, hybrid, and multi-cloud environments, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform. Fidelis Halo provides layers of protection that close gaps, accelerate security deployment, and increase visibility and control no matter which cloud service providers you use, while extending the same protections to your on-premises servers and virtual environments. It scales dynamically and automatically with your cloud footprint, keeping ahead of new assets and workloads, configuration changes, and containerized environments. With Fidelis Halo, you will stay ahead of configuration changes and policy violations—both innocent and malicious—with real-time alerting, API-level integration, and the ability to automate remediation.

About Fidelis Cybersecurity

Fidelis Cybersecurity®, the industry innovator in Active XDR and proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic asset discovery, multi-faceted context, and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. Fidelis Cybersecurity is dedicated to helping clients become stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide.

For more information, please visit **www.fidelissecurity.com.**

Cybersecurity

INSIDERS

Cybersecurity Insiders is a 500,000+ 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

Copyright © 2022 Cybersecurity Insiders. All Rights Reserved. Data can be reproduced or referenced as long as it is sourced and linked to www.cybersecurity-insiders.com.