Scrut Automation

Cloud Security 101: Challenges and Best Practices

Scrut Automation

Contents

Abstract

In the modern digital landscape, data is the lifeblood of organizations, and cloud computing stands as the cornerstone of its storage and management. As we delve into the complexities of cloud security in 2023, it becomes evident that data's significance is matched only by the challenges it poses.

With the rapid shift of workloads to the cloud, the rise of multi-cloud strategies, and the growth of cloud storage and Software as a Service (SaaS), security has never been more crucial.

Challenges abound, from staffing and data protection complexities to integration hurdles and the need to keep pace with an ever-changing technological landscape.

This eBook explores the critical role of empirical data and statistical evidence in shaping our understanding of cloud security. It also outlines sourcing options for cloud security services, including native tools, managed services, and third-party vendors.

Within this resource, we will also examine obstacles to cloud security, ranging from staffing constraints to budget limitations and evolving compliance requirements.

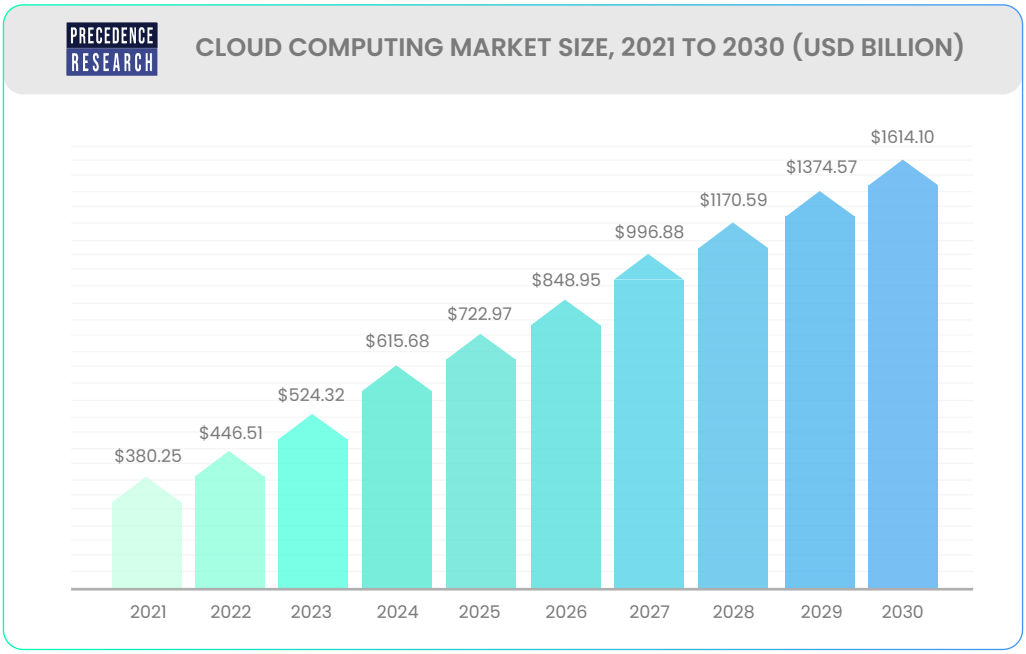
The eBook concludes by outlining best practices for cloud security and compliance management, emphasizing risk assessment, identity management, data encryption, security monitoring, and proactive vulnerability management. Staying informed and adaptable is key to successfully navigating the cloud landscape and ensuring the safeguarding of digital assets in our data-driven world.

Introduction

Data is the new-age oil. The success or failure of an organization is based on its capacity to collect, process, and use the right information at the right time.

As the data collection is increasing with time, it is becoming almost impossible to store and manage all this data physically on-site. Enter cloud service providers.

The cloud computing market is one of the fastest-growing markets in the world today. *Precedence Research* predicts that the global cloud computing market, which was $446.51 billion in 2022, will reach $1614.10 billion by 2030.



Source: Precedence Research

Be it individuals or corporations, everyone uses cloud computing for storing their data. For instance, Gmail gives access to free cloud storage when a user creates an email account with them.

Corporations use cloud computing on a much larger scale to store applications and data. With the increase in remote work, artificial intelligence, and machine learning, cloud computing has scaled greater heights.

Although cloud computing is inevitable at this stage of development in modern technology, it doesn't come without its limitations.

One of the biggest challenges in cloud computing is maintaining cloud security.

Cloud security should not be an afterthought but should be prioritized before even an organization decides to store its data in a cloud.

In addressing the challenges of cloud security, it is crucial to rely on empirical data and statistical evidence to make informed decisions. Anecdotal information and assumptions can lead to misguided security strategies that may prove inadequate in the face of evolving threats.

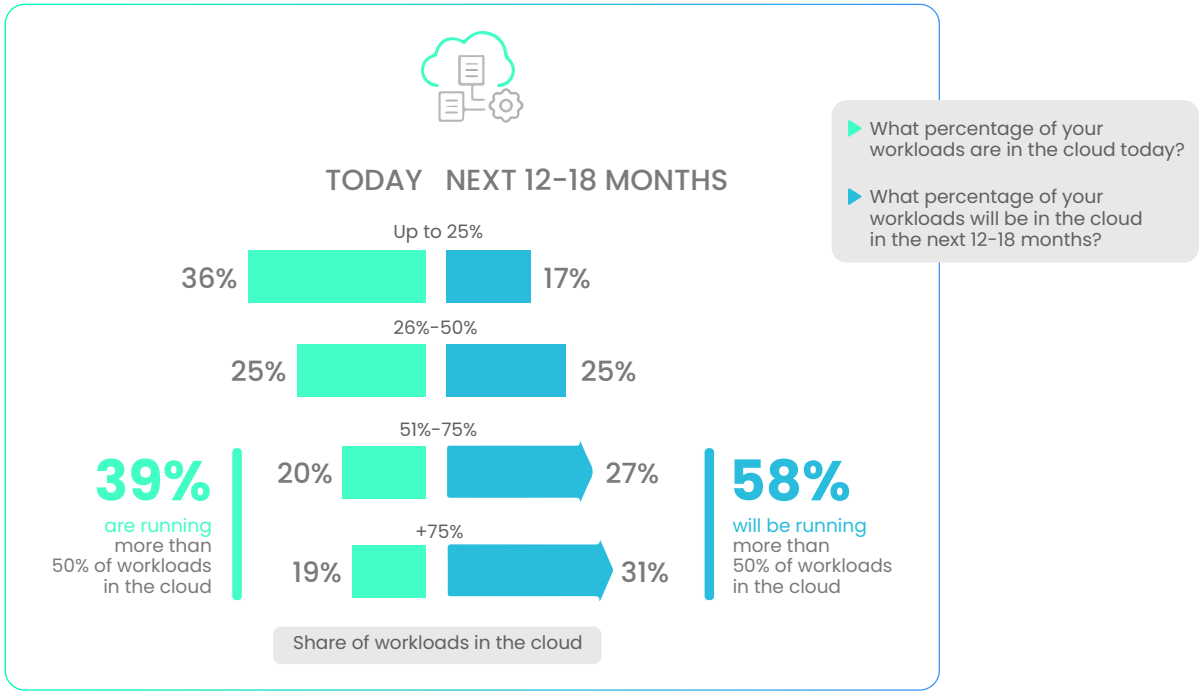
Statistical evidence allows us to identify trends, vulnerabilities, and patterns in cloud security incidents. It provides a foundation for evidence-based decision-making and helps organizations allocate resources effectively to mitigate risks. This paper underscores the significance of statistical evidence in shaping our understanding of cloud security.

In the subsequent sections, we will explore each of these reports in detail, emphasizing their contributions to the broader discussion of cloud security.

Cloud computing landscape in 2023

In order to understand the cloud computing landscape, one should first understand the amount of data that is already on the cloud and the data that will be stored on the cloud in the next 12-18 months.

The *ISC2 2023 Cloud Security Report* has published the following figures:



Source: ISC2 2023 Cloud Security Report

The same report also says that 72% of the respondents use multiple cloud providers to store their data, which means that multi-cloud security has precedence in the market.

There are various motivating factors that drive organizations to broaden their array of cloud service providers. These reasons encompass a desire for enhanced functionality, a strategic shift to diversify operations to bolster resilience, forming partnerships, ensuring service availability, and, notably, engaging in mergers and acquisitions. However, the findings of the study unequivocally demonstrate that the adoption of multi-cloud strategies is steadily on the rise.

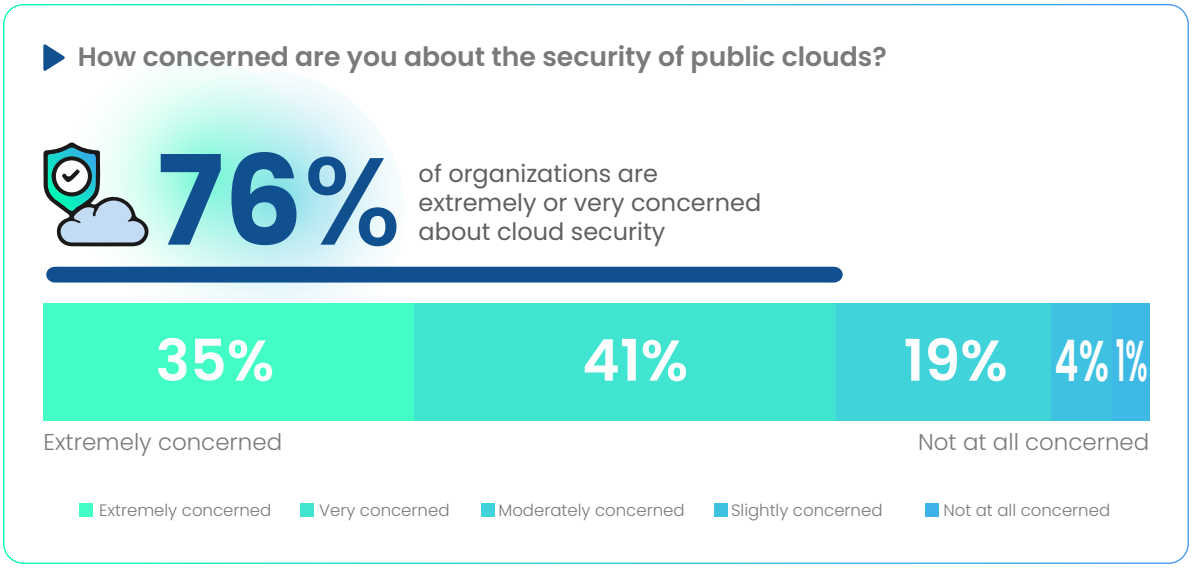
Thales 2023 Cloud Security Study reports that within two years, i.e., from 2021 to 2023, the average number of cloud infrastructure providers is up 35% - from 1.68 to 2.26.

With each additional cloud provider, there are new security controls and data protection models to understand and implement. Cloud users have to extend their existing operating processes further while understanding the constraints of the new environment.

There is growth in cloud storage on the one hand and in the use of software as a service (SaaS) on the other. While cloud storage is used to store data, SaaS reduces the on-premise application storage. The mean number of applications reported in use went from 69 in 2021 to 97 in 2023, a 41% increase, growing faster than regular cloud infrastructure (Thales).

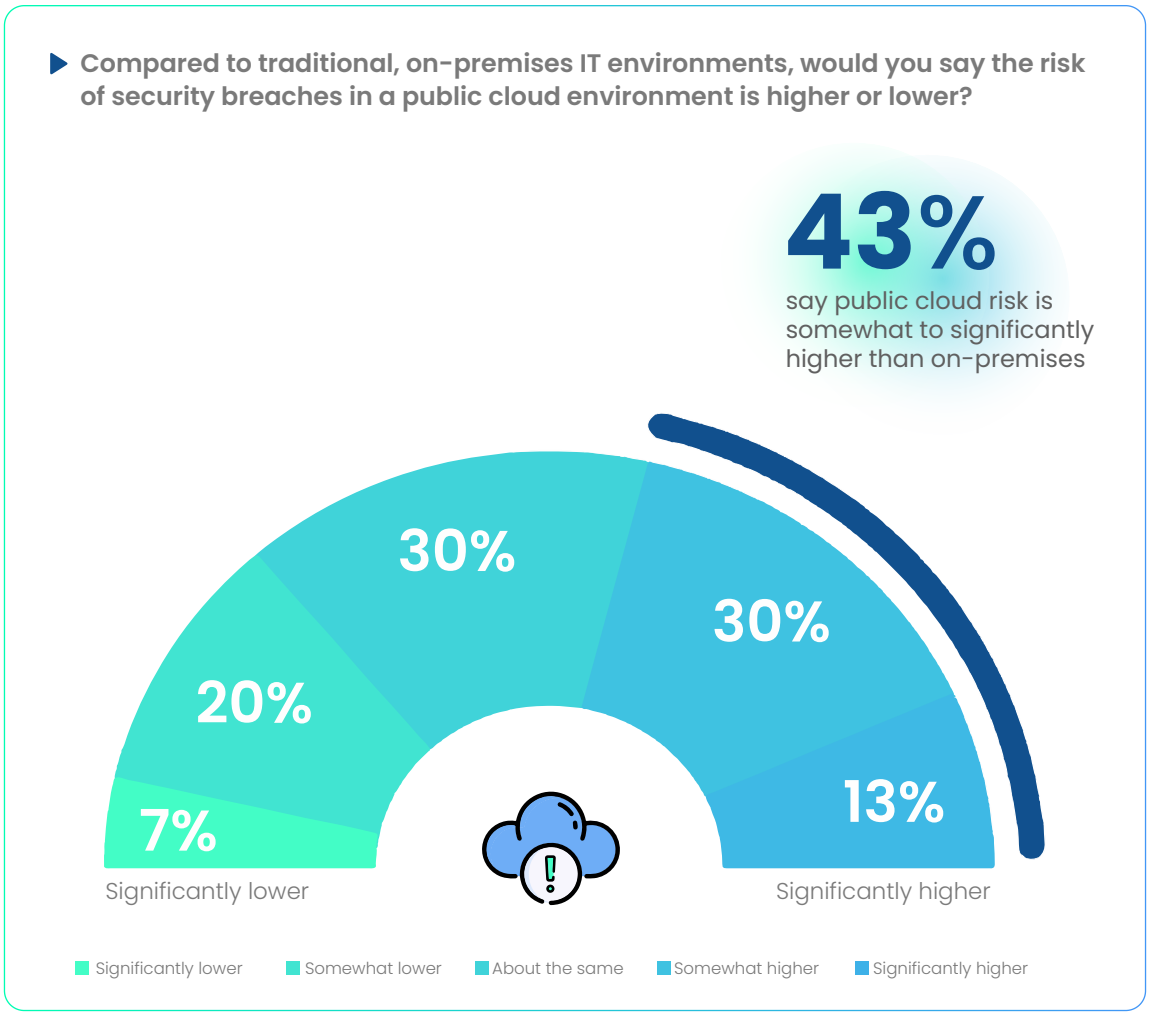
This extensive expansion translates to an increased management and security workload, with sensitive data dispersed across multiple locations. A majority of Thales survey participants (55%) acknowledge the growing complexity of securing data in the cloud, and this complexity may well be exacerbated by the rising number of cloud service providers.

CheckPoint 2023 Cloud Security Report states the following figure about the cloud security concerns of organizations.



Source: Checkpoint 2023 Cloud Security Report

When Check Point respondents were asked whether their organization had experienced a public cloud-related security incident in the last 12 months, 24% of them said yes. When it comes to cloud security posture, 95% of organizations are moderate to extremely concerned.



Source: Checkpoint 2023 Cloud Security Report

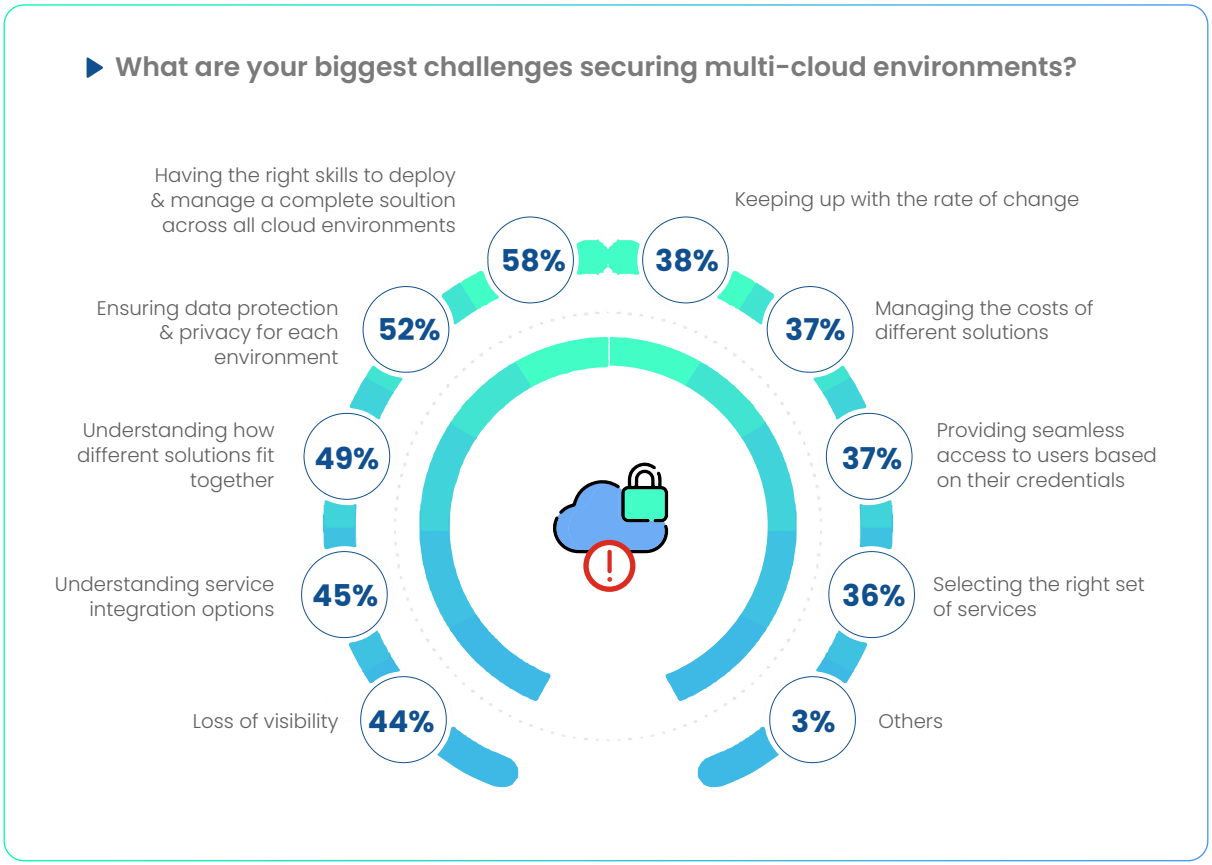
Real-time statistics in security operations are vital for swiftly addressing challenges. They help prioritize alerts, detect anomalies and advanced threats, enable rapid incident responses, and provide insights into evolving threat trends.

Additionally, real-time data aids in ensuring regulatory compliance. In essence, real-time statistics are crucial for maintaining effective security measures and adapting to dynamic threats.

So, what are the challenges faced in the security operations of the cloud landscape?

Challenges faced in the multi-cloud security landscape in 2023

Let's look at the graph first (data by *Fortinet 2023 Cloud Security Report*), then understand each of the challenges in detail:



Source: Fortinet 2023 Cloud Security Report

Lack of qualified staff

Finding and retaining skilled cybersecurity professionals who are well-versed in multi-cloud security can be difficult. The rapidly evolving nature of cloud technology requires constant learning and adaptation, making it challenging to keep up with the latest security threats and best practices.

Palo Alto The State of Cloud-native Security 2023 Report found that organizations have largely distributed responsibility for designing and implementing cloud security policies and procedures to individual teams (78%). However, nearly half (47%) of respondents report that the majority of their workforce does not understand their security responsibilities. 75% of respondents also reported a higher-than-usual rate of turnover in DevOps roles.

Ensuring data protection and privacy for each environment

Managing data protection and privacy compliance across multiple cloud environments can be complex. Each cloud provider may have its own set of security controls and compliance requirements. Ensuring that data is consistently protected and in compliance with regulations like GDPR, HIPAA, or CCPA across all environments is a significant challenge.

Understanding how different solutions fit together

Organizations often adopt multiple security solutions and tools from different vendors to secure their multi-cloud environments. Integrating these solutions effectively and ensuring they work seamlessly together can be a major challenge. 76% of Palo Alto respondents say the number of cloud security tools they use creates blind spots. It's crucial to avoid redundancy and gaps in security coverage.

Understanding service integration options

Cloud providers offer various services and features, each with its own security options and configurations. Understanding how these services can be securely integrated into your organization's architecture and applications is a complex task. Misconfigurations can lead to security vulnerabilities.

Did you know that almost a fourth of the organizations (24%) faced security incidents in the last 12 months (ISC2)? The same report also calls misconfiguration a leading cause for these incidents, followed by account compromise and exploited vulnerabilities.

Loss of visibility and control

As data and applications are distributed across multiple cloud providers, there can be a loss of visibility and control. Organizations may struggle to gain a unified view of their security posture across all environments. This lack of visibility can make it difficult to detect and respond to security incidents promptly.

78% of Palo Alto respondents agree that cloud security needs more out-of-the-box visibility and risk prioritization filtering with minimal learning

Keeping up with the rate of change

The cloud technology landscape evolves rapidly, with new features, services, and security threats emerging frequently. Staying up-to-date with these changes and adapting security measures accordingly is an ongoing challenge. Organizations need to have a proactive approach to monitoring and implementing security updates and best practices to address emerging threats.

Managing the costs of different solutions

Adopting multiple security solutions from different vendors can lead to increased costs. Each solution may come with its own licensing, maintenance, and support fees. Managing these costs while ensuring optimal security coverage can be a financial challenge.

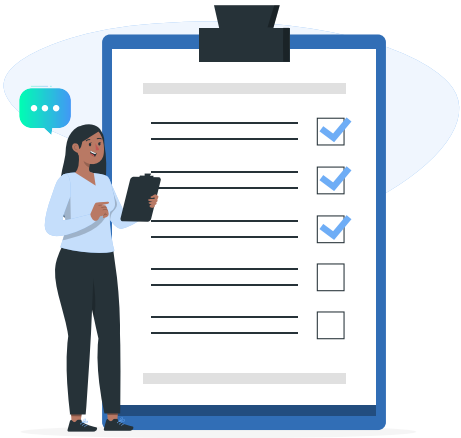
Providing seamless access to users based on their credentials

Implementing identity and access management (IAM) solutions that provide seamless and secure access to users based on their credentials across multiple cloud environments can be complex. Achieving a unified and consistent authentication and authorization process is essential for both security and user experience.

Only 14% of respondents say that they control all of their encryption keys in their cloud environments (Thales).

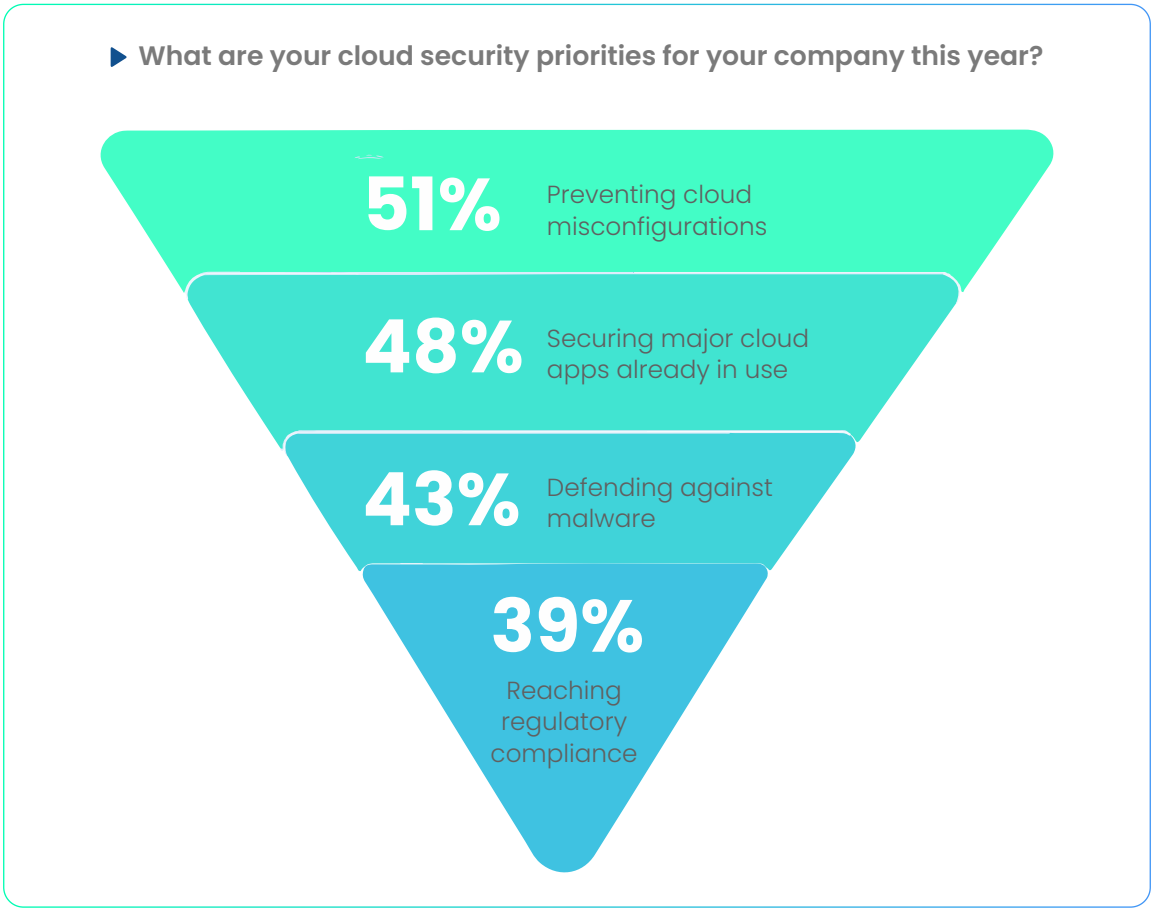
Selecting the right set of services

Choosing the appropriate cloud services and features for your specific security needs can be challenging. Different cloud providers offer a wide array of services and selecting the right ones that align with your security requirements and budget is critical. 77% of organizations struggle to identify what security tools are necessary to achieve their objectives (Palo Alto). Overprovisioning or underutilizing services can impact both security and costs.



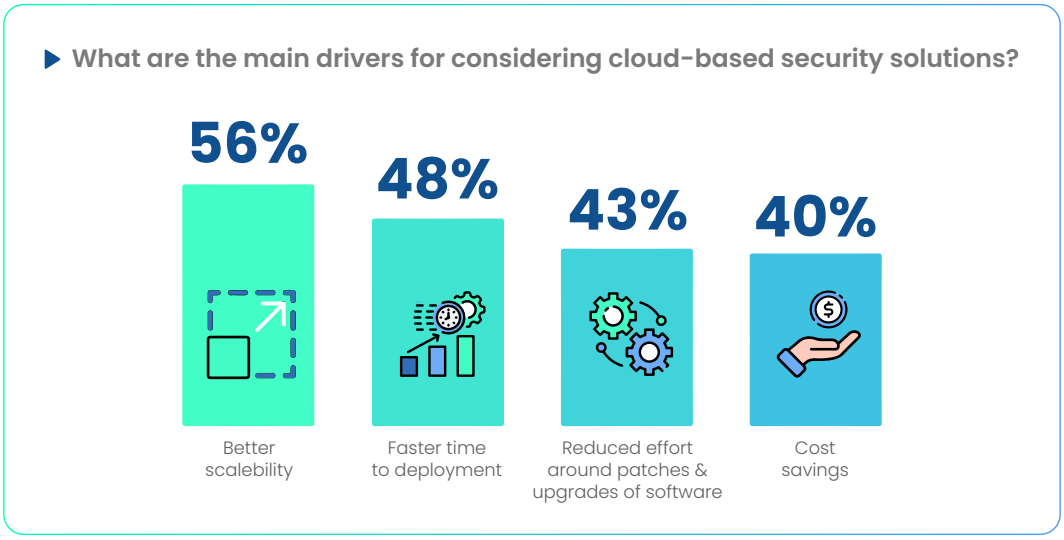
Cloud security priorities

Security experts are employing their cloud budgets judiciously to tackle the most critical threats and issues that jeopardize business operations. Here are some of the studies. Data source: Fortinet.



Source: Fortinet 2023 Cloud Security Report

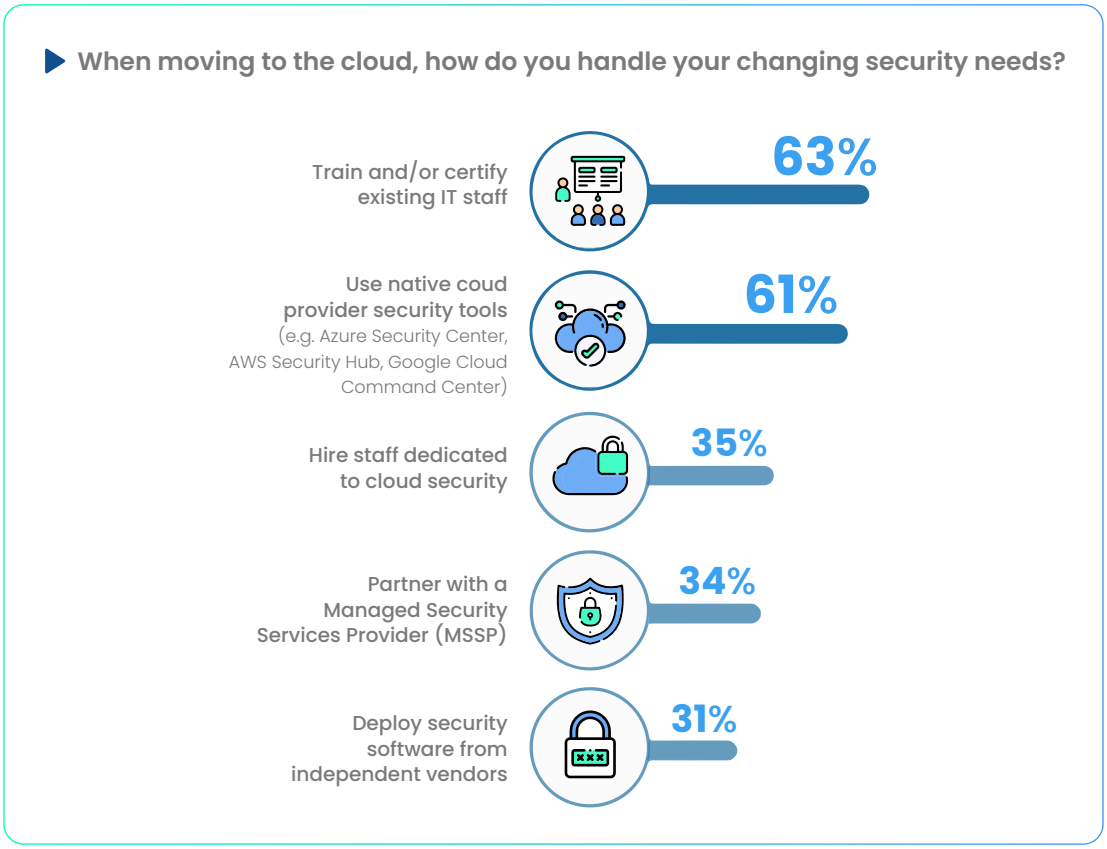
The cloud empowers organizations to access the same benefits for their security services as they do for their applications and workloads. According to Fortinet data,



Source: Fortinet 2023 Cloud Security Report

Best practices for cloud security

ISC2 asked their subjects about how they would handle changing security needs while moving to a cloud-based environment. Here is what they had to say.



Source: ISC2 2023 Cloud Security Report

According to Palo Alto, despite the deployment of multiple security tools, enterprises have still encountered significant security incidents, revealing shortcomings in the effectiveness and efficiency of their response efforts. A mere 10% of respondents possess the capability to detect, contain, and resolve threats within an hour. Approximately 39% have reported an uptick in the number of breaches, while more than 30% noted a notable increase in intrusion attempts and unplanned downtime.

Additionally, a substantial 68% of organizations are unable to identify a security incident within an hour, and once detected, 69% struggle to respond to the threat in under an hour.

In summary, the landscape of security threats and incidents is becoming increasingly challenging to both identify and mitigate.

Source: Palo Alto The State of Cloud-native Security 2023 Report

Going forward, maintaining cloud security and compliance in 2023 requires a proactive and comprehensive approach.

Here are some best practices to help organizations effectively secure their cloud environments:


Risk assessment & security strategy


Identity & access management


Data encryption


Security monitoring & logging


Vulnerability management


Compliance management


Incident response plan


Patch & configuration management


Employee training & awareness


Backup & disaster recovery


Third-party security


Automation & orchestration

Regular audits & assessments


Cloud-native security tools


Stay informed

Risk assessment and security strategy

- Begin with a thorough risk assessment to identify potential vulnerabilities and compliance requirements specific to your organization.
- Develop a cloud security strategy that aligns with your business objectives and includes policies, procedures, and guidelines.

Identity and access management (IAM)

- Implement strong identity and access controls, including multi-factor authentication (MFA) and role-based access control (RBAC).
- Regularly review and update permissions to ensure the least privilege access.

Data encryption

- Encrypt sensitive data both in transit and at rest using strong encryption methods.
- Utilize encryption services provided by your cloud provider and manage encryption keys securely.

Security monitoring and logging

- Set up robust monitoring and logging systems to track user and system activities.
- Implement automated alerting for suspicious or unauthorized activities.

Vulnerability management

- Regularly scan for vulnerabilities in your cloud infrastructure and applications.
- Prioritize and remediate vulnerabilities promptly to reduce the attack surface.

Compliance management

- Understand and adhere to industry-specific regulations and compliance standards relevant to your organization (e.g., GDPR, HIPAA, PCI DSS).
- Continuously monitor and audit your cloud environment to ensure compliance.

Incident response plan

- Develop a well-defined incident response plan that outlines roles, responsibilities, and procedures for addressing security incidents.
- Conduct regular incident response exercises to test the effectiveness of the plan.

Patch and configuration management

- Keep all cloud resources, operating systems, and software up to date with security patches.
- Implement secure configuration practices for cloud services to mitigate risks associated with misconfigurations.

Employee training and awareness

- Provide ongoing cybersecurity training for your staff to raise awareness about security best practices.
- Encourage a security-conscious culture within your organization.

Backup and disaster recovery

- Regularly back up critical data and establish a disaster recovery plan to ensure business continuity in case of data loss or service disruptions.

Third-party security

- Vet and monitor third-party vendors and their security practices, especially if they have access to your cloud environment or data.

Automation and orchestration

- Leverage automation and orchestration tools to streamline security tasks and responses to incidents.

Regular audits and assessments

- Conduct regular security audits and assessments to evaluate the effectiveness of your cloud security measures.

Cloud-native security tools

- Explore and use cloud-native security tools and features provided by your cloud provider to enhance security.

To sum it all up

This eBook highlights the pivotal role of data in today's world, where cloud computing is paramount. Cloud computing is expanding rapidly, but it also presents security challenges that demand evidence-based solutions.

We have explored five key reports, offering real-world insights into cloud security. The cloud landscape is evolving, with multi-cloud strategies on the rise and data storage growing.

Challenges in 2023 include staffing issues, data protection complexities, and integration hurdles. Organizations source cloud security services from various options, including native tools, managed services, and third-party vendors.

Third-party solutions are gaining trust for their capabilities. Obstacles to cloud security often involve human resources and budgets, but investments are increasing.

Priorities revolve around misconfiguration prevention and securing cloud-based applications. Compliance management remains a challenge, necessitating staff training and vigilant monitoring.

Best practices encompass risk assessment, strong identity management, data encryption, security monitoring, and proactive vulnerability management. Staying informed and agile is key to cloud security success in 2023.

By following these practices, organizations can confidently navigate the evolving cloud landscape, ensuring the safety and compliance of their digital assets in today's data-driven world.