algosec

WHITE PAPER

Cloud Network Security Report 2025

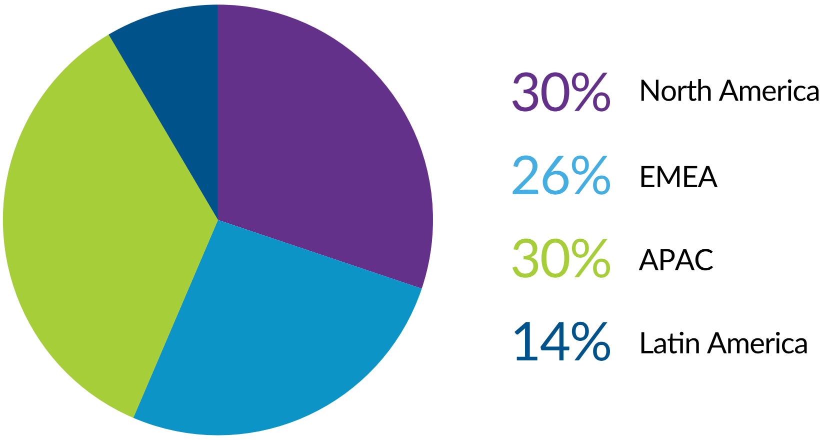
Contents

algosec

Purpose of this report

This report delivers key findings from a global industry survey conducted in July 2025. With insights collected from over 300 leading computer security experts, it provides a comprehensive overview of current trends and significant challenges in maintaining robust cloud computing system security.

Cloud security challenges



This report is designed for professionals responsible for securing organizational and enterprise level computer systems, particularly those leveraging cloud infrastructure. We engaged with leading experts to capture the current landscape of cloud security. Our findings are detailed below:

2025 cloud security challenges

Despite concerted efforts to protect cloud environments, organizations continue to encounter significant challenges. These include:

- Identifying and remediating vulnerabilities
- Achieving comprehensive visibility across their cloud infrastructure
- Ensuring consistent policy enforcement

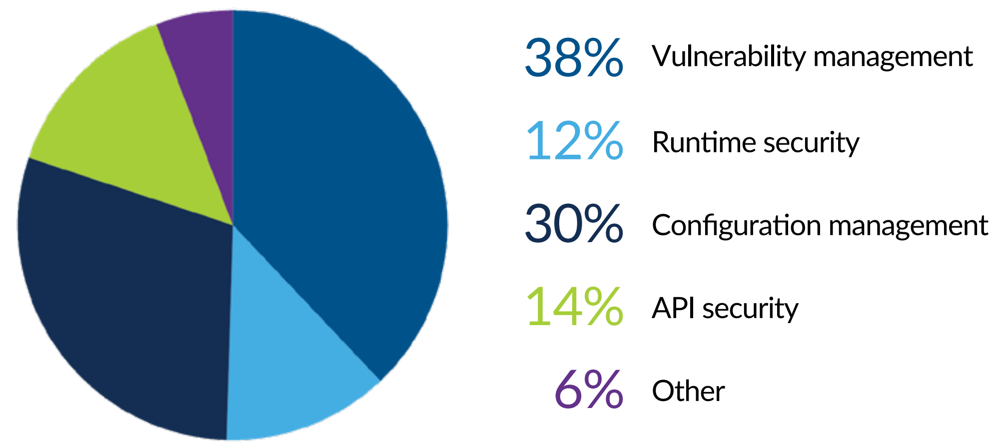
However, there is positive news. Many organizations are realizing substantial cost savings through enhanced cloud security measures. An increasing number of businesses are adopting multi-vendor firewall strategies, which, while strengthening defenses, underscore the critical need for centralized management solutions. Furthermore, security professionals are shifting their focus towards protecting business applications rather than solely the network perimeter. A growing number of teams are also implementing automated tools to manage security policies and ensure adherence to compliance regulations, leading to faster operations and reduced risks.

This report will elucidate these crucial trends, providing actionable insights to enhance your cloud network security and guide best practices.

Finding 1 Major challenges in cloud security

Securing cloud networks is paramount. Our research indicates that many organizations face similar formidable obstacles. Cloud systems are inherently complex, introducing a distinct set of difficulties. So, what constitute today's top challenges in the cloud?

Cloud security challenges

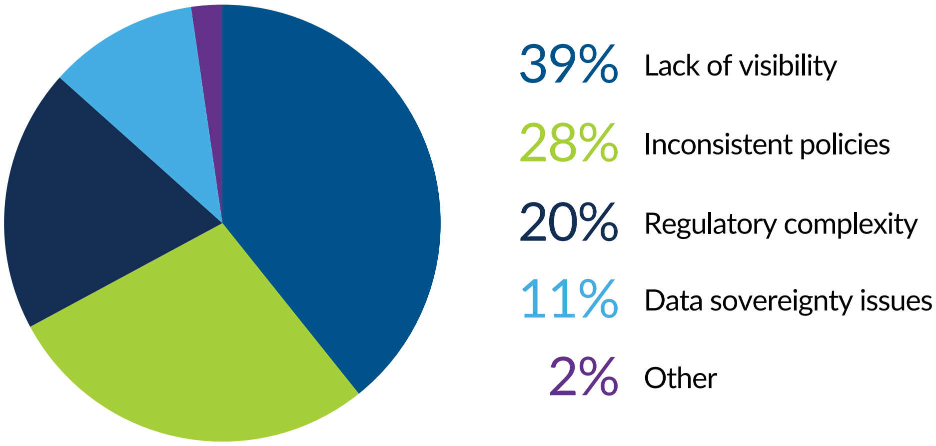


Vulnerability management remains a top concern

The foremost challenge, reported by **37.9%** of companies, is vulnerability management. This necessitates the identification and remediation of security weaknesses. Cloud environments are characterized by their rapid evolution and continuous integration of new components. Consequently, maintaining comprehensive awareness of potential security weaknesses across diverse elements, such as virtual machines and software containers, presents a significant challenge. Additionally, the timely patching of these vulnerabilities can be impeded by concerns regarding compatibility or potential operational disruptions.

Challenges in achieving comprehensive visibility

What is your biggest challenge in ensuring consistent data security and compliance across your multi-cloud environment?



39.3% of companies report difficulty gaining complete insight into their cloud operations, specifically citing "Lack of visibility" as their primary challenge in ensuring consistent data security and compliance across multi-cloud environments. This lack of clear oversight into cloud systems, data flows, and user activities severely impedes threat detection, configuration error remediation, and the overall understanding of application interdependencies. Without adequate visibility, proactive problem resolution becomes considerably more difficult.

Inconsistent policy enforcement

For **27.9%** of companies, a significant hurdle is maintaining uniform security policies across their disparate cloud systems, referring to this as "Inconsistent policies." When policies lack consistency, the potential for misconfigurations increases, leading to security drift. This creates security gaps and complicates overall management. Ensuring policy alignment across all environments is crucial for robust protection.

Navigating regulatory complexity and data location concerns

Approximately **19.5%** of companies find it challenging to comply with diverse security regulations (e.g., HIPAA for health information, PCI DSS for credit card data), citing "Regulatory complexity." They also express concerns about data residency across various cloud providers and national borders, with **11.1%** specifically citing "Data sovereignty issues." Adherence to these regulations demands meticulous planning and continuous monitoring.

Securing Application Programming Interfaces (APIs)

14.1% of respondents identified API security as a significant concern. APIs serve as digital connectors, facilitating communication between disparate applications and services. They are integral to cloud systems but can also present attractive targets for adversaries. Common issues include authentication vulnerabilities, excessive access privileges, or other inherent weaknesses. Given that APIs are frequently exposed to the internet, their robust security is vital.

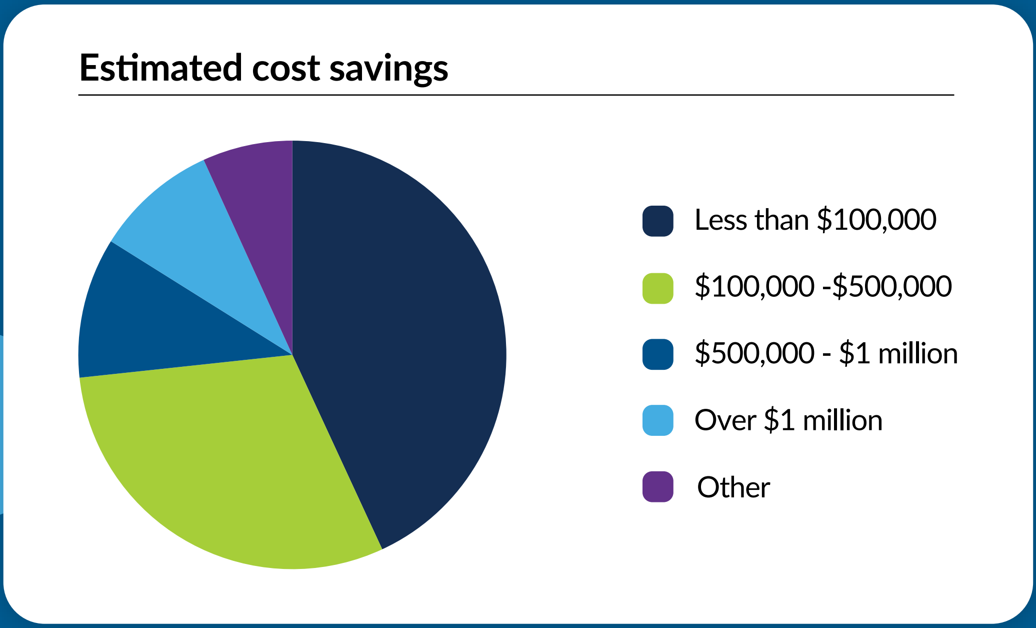
Effective configuration management

Finally, configuration management was frequently cited as a problem by **29.6%** of companies. Errors in setting up elements such as identity and access management, storage policies, or network rules are a primary source of security risks in the cloud. This underscores the critical importance of meticulous and organized configuration of cloud systems.

> Limited visibility into cloud assets, traffic, and user activity. This impacts us due to hard to detect unauthorized access or misconfigurations.
>
> **Anonymous survey response**

Finding 2 Cost savings through enhanced cloud security

Investing in cloud security extends beyond protection; it also represents a strategic financial decision. Our data demonstrates that organizations are realizing substantial cost savings by optimizing their cloud security posture.



Tangible financial benefits

The majority of companies, **43.1%**, reported annual cost savings or avoidance of less than $100,000 through improved cloud security. This indicates that even fundamental security enhancements can yield financial benefits.

Furthermore, the impact is more significant for many: **30.2%** of companies saved between $100,000 and $500,000, and **10.6%** saved between $500,000 and $1 million. A notable **9.3%** even achieved savings exceeding $1 million annually.

These substantial savings stem from several key factors:

Breach prevention
Robust security measures prevent costly incidents before they occur.

Reduced incident response costs
Stronger security minimizes the financial impact of security events when they do arise.

Operational automation
Leveraging intelligent tools for security tasks automates processes, saving time and resources.

Regulatory compliance avoidance
Adhering to regulations helps organizations avoid fines and penalties.

Thus, by prioritizing cloud security, organizations not only safeguard their information but also directly contribute to their financial health.

> Our cloud security improvements have helped reduce potential breach incidents, misconfiguration-related downtime, and compliance penalties-leading to an estimated cost avoidance in the $100K–$500K range. For clients, these improvements also translate into better trust and business continuity.
>
> **Anonymous survey response**

Finding 3 Firewall and microsegmentation strategies in the cloud

In securing cloud networks, organizations strategically deploy various firewall solutions and leverage sophisticated techniques for internal network partitioning, known as microsegmentation. Understanding these prevalent approaches can significantly inform and enhance your security planning.

Firewall deployments

Companies extensively utilize diverse firewall vendors to fortify their cloud perimeters and internal network segments. This multi-vendor approach aims to provide robust, layered defense capabilities.

Microsegmentation strategies

Beyond traditional firewalls, microsegmentation is crucial for granular control. This method involves dividing networks into smaller, isolated segments, allowing for precise security policies to be applied at the workload or application level. By restricting communication between these segments, it limits the lateral movement of threats and unauthorized access, significantly reducing the attack surface.

Strategic insights

Examining the prevalent choices in firewall technologies and microsegmentation methodologies offers valuable benchmarks for developing or refining your own comprehensive cloud security strategy. Implementing microsegmentation effectively requires meticulous planning, including mapping application dependencies and defining security policies. It enhances visibility, improves breach containment, and strengthens regulatory compliance.

Leading firewall vendors in the cloud

Our research identifies the most frequently utilized firewall vendors for cloud networks:

Palo Alto

This vendor is a prominent choice, adopted by **25.4%** of companies. It is frequently selected for its advanced threat detection capabilities, deep packet inspection, and granular control over applications.

Fortinet

Another strong contender, utilized by **19.9%** of companies. It is recognized for its extensive cloud platform compatibility, centralized management features, and comprehensive threat protection.

Azure

Microsoft Azure's native firewalls are employed by **17.7%** of companies, particularly those with significant investments in Microsoft's cloud services.

AWS

Similarly, Amazon Web Services (AWS) firewalls are used by **13.2%** of companies to secure their systems within the AWS cloud environment.

Checkpoint

This brand is used by **9.0%** of companies. It is particularly valued for hybrid cloud and on-premises deployments, as well as for advanced security requirements.

GCP

Google Cloud Platform (GCP) firewalls are utilized by **3.5%** of companies.

Approaches to microsegmentation

Microsegmentation is vital for achieving precise network control. Organizations adopt various strategies for its implementation:

Cisco
The most frequently reported solution, adopted by **42.8%** of companies.

Other Specialized Solutions
36.0% of companies employ other specialized microsegmentation tools.

Akimaii/Guardicore
Utilized by **13.5%** of companies.

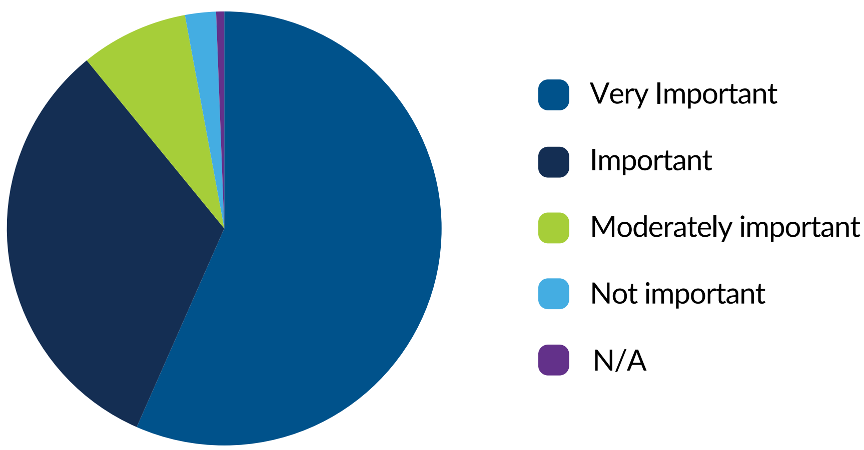
Illumio
Used by **7.7%** of companies.

This diverse adoption illustrates that organizations are leveraging both established vendors and specialized tools to address their microsegmentation requirements.

Finding 4 Policy management and automation adoption

Intelligent management of security policies and the strategic application of automation are crucial for developing robust and efficient cloud security postures. Our findings reveal how organizations are approaching these critical tasks.

Unified view importance

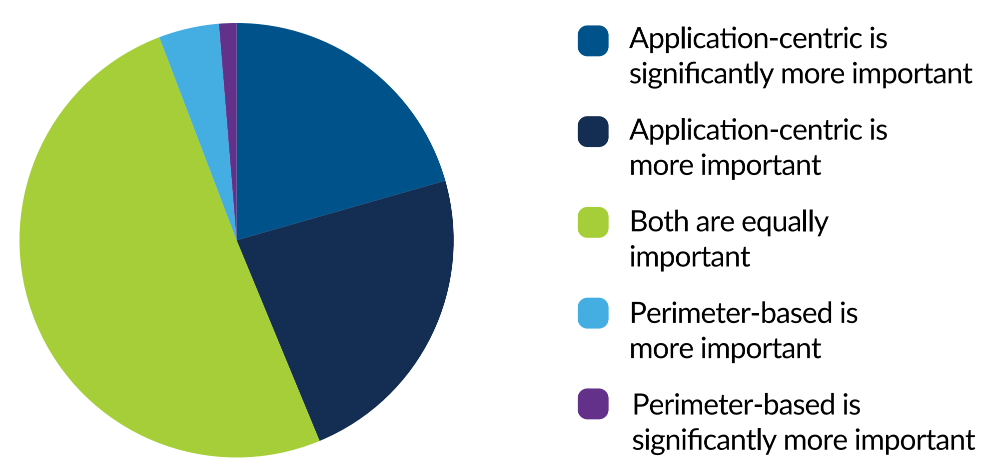


A substantial majority of respondents underscore the importance of a unified view for security policies across both on-premises and cloud-native environments. **56.6%** rated this as **Very Important**, and an additional **32.5%** considered it **Important**. This clearly indicates that a single, intuitive interface is critical. It aids in preventing errors, ensuring policy consistency, and significantly simplifying overall security management.

> Having a unified view of security policies across on-premises and cloud-native environments is critical for maintaining consistency, reducing misconfigurations, and ensuring compliance. It helps streamline security operations and simplifies incident response across the entire infrastructure.
>
> **Anonymous survey response**

Shifting towards application-centric security

Application-centric approach

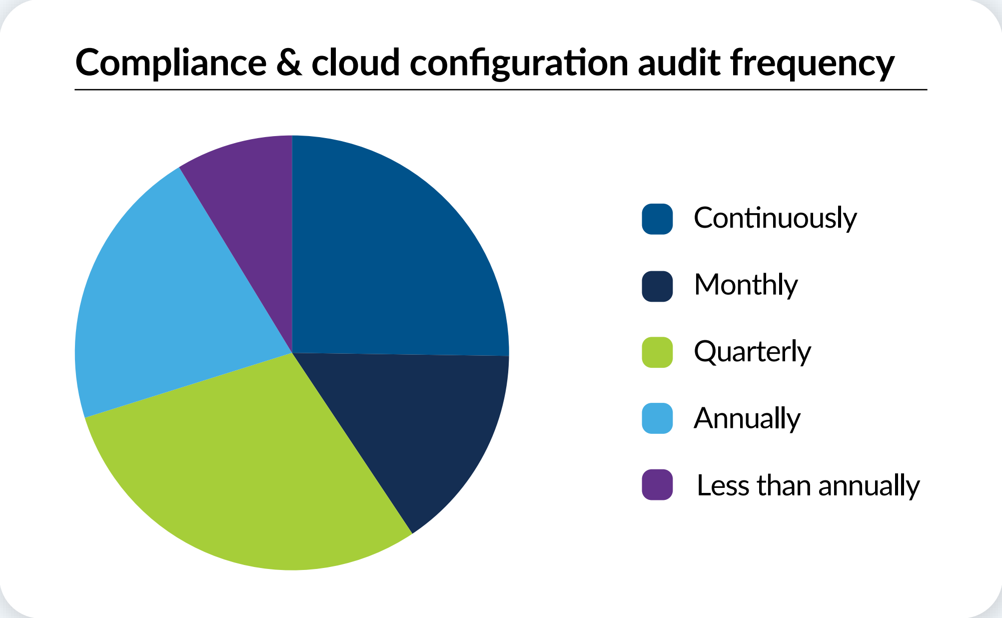


Regarding cloud-native security strategy, 50.5% of companies consider both an application-centric and a traditional perimeter-based approach to be equally important. However, there is a clear trend towards an application-centric methodology, with 23.2% deeming it more important and 20.6% classifying it as significantly more important. This reflects an understanding that in dynamic cloud environments, where applications are distributed and constantly evolving, security must be inherently integrated within the applications themselves. While traditional perimeter-based security remains relevant, it is increasingly complemented by granular application-level controls.

> In modern cloud-native architectures-especially with microservices, containers, and serverless-security needs to follow the application, not just the network perimeter. While perimeter-based controls (like firewalls and VPNs) are still relevant, we prioritize an application-centric approach for its ability to enforce fine-grained policies, identity-based access, and zero-trust principles at the workload level
>
> **Anonymous survey response**

Frequency of cloud configuration audits

To maintain consistency and regulatory adherence, organizations audit their cloud configurations with varying frequencies:



Quarterly:

29.5% of companies conduct audits on a quarterly basis.

Continuously:

A significant portion, **25.2%** of companies, continuously monitor their cloud configurations, indicating a proactive and real-time approach.

Annually:

21.1% of companies perform annual checks.

Monthly:

15.4% of companies conduct monthly audits.

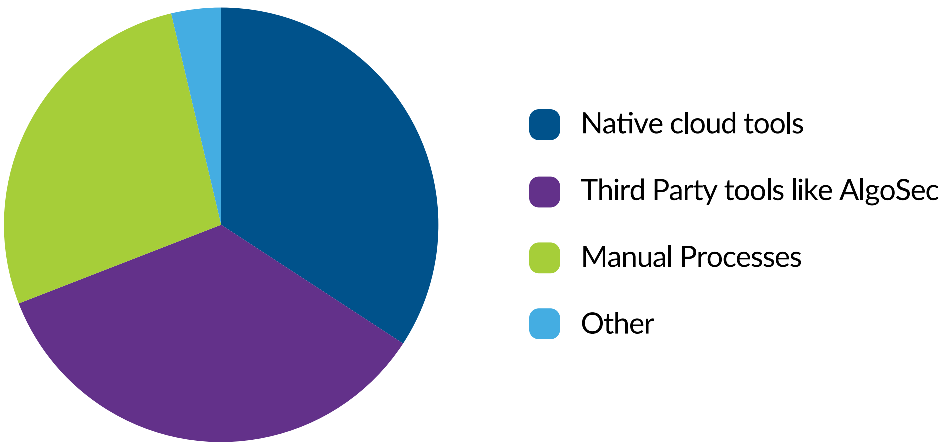
Less than annually:

Only **8.7%** of companies audit less frequently than once a year.

Ensuring consistent network security policy across multi-cloud environments

Maintaining consistent security policies across diverse cloud providers presents a complex challenge. Organizations employ several strategies:

How do you manage network security policy consistency across multiple cloud providers?



Third-party tools (e.g., AlgoSec)

The most common approach, utilized by **34.9%** of companies. This highlights the demand for solutions that provide cross-platform management capabilities.

Use best practices

Employed by **34.2%** of companies. This indicates a strong reliance on the security features integrated within each cloud platform.

Manual processes

Despite the push for automation, **27.2%** of companies still manage their security policies manually.

Integration of network security policy automation into compliance workflows

Organizations are increasingly automating their security checks, particularly for compliance purposes:

To what extent have you integrated network security policy automation into your compliance workflows?

17% Fully Integrated

34% Mostly Integrated

35% Partially Integrated

14% Not Integrated

Partially integrated

The largest segment, **35.2%** of companies, report partial integration of network security policy automation into their compliance workflows.

Mostly integrated

Another **33.6%** of companies are largely leveraging automation, signifying considerable progress.

Fully integrated

A strong **16.8%** of companies have fully integrated automated security checks, demonstrating a high degree of automation maturity for compliance. degree of automation maturity for compliance

Not integrated

14.4% of companies have not yet integrated automation in this area.

This data clearly indicates a strong industry trend towards utilizing automation to enhance efficiency, minimize human error, and ensure continuous adherence to critical regulations.

Finding 5 The impact of AlgoSec Cloud Enterprise (ACE)

The provided data did not include specific quantitative feedback regarding AlgoSec Cloud Enterprise (ACE) usage or its benefits. Therefore, this section reiterates qualitative insights from existing reports.

For organizations utilizing AlgoSec Cloud Enterprise (ACE), feedback consistently indicates significant improvements in cloud network security.

Key improvements with ACE

Users of ACE frequently report substantial benefits across critical security domains:

Enhanced visibility and risk control

A primary advantage of ACE is its provision of a centralized view for security policies across various cloud systems and hybrid environments. This empowers teams to readily identify and rectify security gaps, understand application interdependencies, and swiftly detect risky firewall rules or misconfigurations that might otherwise go unnoticed.

Automated policy management and compliance

ACE is highly praised for its automation capabilities, including policy validation, change management, and compliance reporting. This significantly accelerates operations, drastically reduces manual errors, and consistently supports adherence to important regulations.

Increased operational efficiency

The tool's ability to streamline change requests, facilitate rapid and secure deployment of new security features, and optimize security policies contributes directly to greater operational efficiency.
This translates into reduced manual effort and faster, more reliable security updates.

AlgoSec Cloud Enterprise typically impacts an organization's cloud network security posture in several positive ways, such as:

Improved visibility
It provides centralized visibility into security policies across multiple cloud environments, helping identify and close security gaps faster.

Policy consistency
Ensures consistent security policy enforcement across hybrid and multi-cloud environments, reducing misconfigurations.

Automation & efficiency
Automates policy analysis, change management, and compliance reporting, which speeds up workflows and reduces human errors.

Compliance assurance
Helps maintain continuous compliance with regulatory standards by providing audit-ready reports and real-time policy validation

Risk reduction
By proactively identifying risky firewall rules and misconfigurations, it lowers the chances of security incidents and breaches

Anonymous survey response

AlgoSec Cloud Enterprise has significantly impacted our organization's cloud network security posture by addressing key challenges in managing complex, hybrid, and multi-cloud environments

Anonymous survey response

Highlighted features

When asked about the most valuable components of AlgoSec Cloud Enterprise, users frequently cited:

- **Unified security policy management**
  Centralized control over security rules across disparate systems.
- **Application-centric visibility and risk mapping**
  Deep insights into application behavior correlated with security risks.
- **Automated change management**
  Streamlined and automated processes for
- **Compliance and risk reporting**
  Comprehensive reports demonstrating regulatory adherence and risk posture.
- **Policy cleanup and optimization**
  Identification and elimination of obsolete or overly permissive rules to enhance security.

While the majority of users express high satisfaction, some noted they are still in the evaluation phase or have not yet fully utilized all features, occasionally due to a greater focus on on-premises systems than cloud environments. Nevertheless, the overarching message is clear: **AlgoSec Cloud Enterprise significantly strengthens cloud network security by providing superior visibility and advanced automation tools.**

Conclusion

The landscape of cloud network security is evolving rapidly and becoming increasingly complex. We hope this report has provided valuable insights and validated current industry trends.

The data unequivocally shows that vulnerability management **(37.9%),** achieving comprehensive visibility **(39.3%)**, and maintaining consistent policies **(27.9%)** remain the foremost challenges for organizations. Crucially, the findings also highlight that proactive security improvements yield significant financial benefits.

Looking forward, there is a widespread demand for a unified approach to managing security policies across all cloud systems and hybrid environments **(56.6% Very Important, 32.5% Important)**. The industry is clearly shifting towards an application-centric security focus, with **50.5%** acknowledging the equal importance of both application-centric and perimeter-based approaches, and a notable segment prioritizing the former. Furthermore, the increasing adoption of automated tools for security policy and compliance management **(33.6% mostly integrated, 16.8% fully integrated)** represents a smart and effective strategy for boosting efficiency and mitigating risks.

Solutions like AlgoSec Cloud Enterprise are instrumental in this evolution by enhancing visibility, automating critical tasks, and simplifying compliance. By concentrating on these key areas-centralized management, application-centric security, and automation-organizations can construct a resilient and future-ready network security plan.