algosec

Secure application connectivity.
Anywhere.

Whitepaper

The cloud visibility imperative

A guide to defeating the unseen threat

The cloud visibility imperative

A guide to defeating the unseen threat

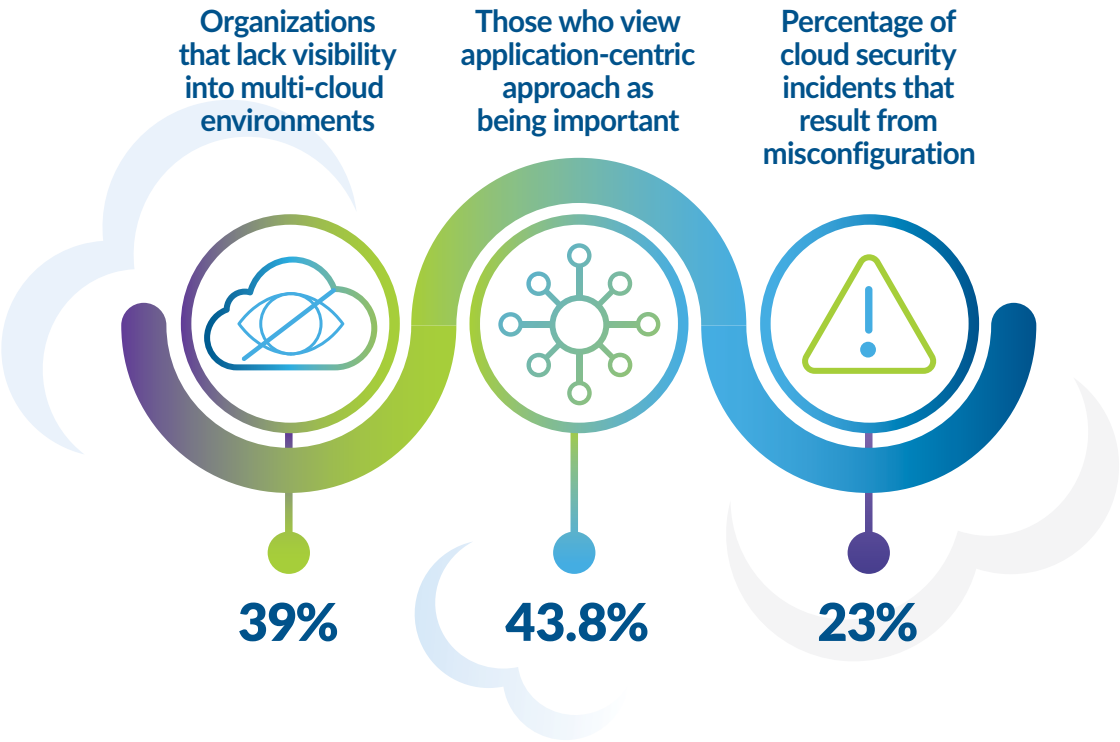
An AlgoSec Whitepaper

Your digital transformation is about agility and innovation, but with that speed comes a new challenge: a pervasive lack of visibility. While your security teams are focused on sophisticated threats, a more fundamental danger is looming in the unmonitored corners of your cloud. **AlgoSec's Cloud Network Security Report 2025** reveals that this lack of visibility is not merely a side effect of growth but has become the number one risk for enterprises today, leading to unpatched vulnerabilities, data exposure, and costly breaches that directly impact your business.

This paper will outline the core findings of our report and present a prescriptive framework to help you achieve total cloud visibility. By understanding and addressing the root causes of security blind spots, you can build a resilient security posture, protect your most critical assets, and defeat the unseen threat before it ever affects your bottom line.

Key takeaways:

- **39%** of organizations admit to lacking full visibility into their multi-cloud environments.
- **43.8%** of companies feel that an application-centric approach is 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..
- **Nearly 23%** of cloud security incidents are a result of cloud misconfiguration.



The state of cloud security in 2025

The cloud has enabled your business to innovate faster than ever before. Teams can now spin up new servers and applications in minutes, accelerating product development and go-to-market strategies. But this speed has created a massive security challenge. The sheer scale and dynamism of your multi-cloud environment are simply too vast for traditional, static security tools to manage effectively.

This disconnect means you're operating with critical blind spots. You can't protect what you can't see, and in the sprawling landscape of a typical enterprise cloud, there are more unmanaged, unmonitored, and unpatched assets than ever before. This is an issue that isn't solved by adding more firewalls or threat intelligence; it requires a fundamental shift in your approach, starting with achieving complete visibility.

The unseen threat: Findings from the Cloud Network Security Report 2025

Our recent report provides a clear, data-driven look at the hidden dangers lurking in the cloud. We surveyed hundreds of security leaders and found a direct correlation between visibility gaps and heightened security risk. The data unequivocally proves that the greatest threats to your business are often the ones you don't even know exist.

The data doesn't lie

- Our report found that a staggering 39% of organizations admit to a critical lack of full visibility, meaning their security teams lack full knowledge of what's running in significant parts of their cloud network.
- This lack of control has a direct and measurable impact on your risk profile. On average, it takes organizations too long to discover a new, unauthorized cloud asset, leaving a massive window of opportunity for attackers to exploit.
- The consequences are severe. Reports show that 23%of security incidents in the last year were directly linked to assets that were either unmonitored or riddled with misconfigurations.

Real-world examples:

- **The "forgotten" asset:** A development team for a new product deploys a temporary test virtual machine in their Azure environment. After performance testing is complete, the team moves on to other priorities and forgets to decommission it. The VM remains active for months, unpatched and unmonitored, while falling outside the security team's standard scan policies. An attacker performing routine port scans finds the VM, exploits a known vulnerability in its outdated operating system, and uses it as a beachhead to move laterally into the production environment. This scenario is not only common but highlights a direct threat to your business continuity.
- **The "shadow IT" risk:** A marketing team, in a rush to launch a new campaign, signs up for an unapproved SaaS application that integrates with cloud storage. The marketing employee connects the app to an AWS S3 bucket containing sensitive customer data. Without guidance from the security team, they use overly permissive permissions, and the bucket is publicly exposed. Because the security team has no visibility into this unsanctioned application, a critical data breach goes unnoticed until it's too late. This shows how a lack of visibility can lead to a critical data breach from an unexpected source.

This shows how a lack of visibility can lead to a critical data breach from an unexpected source.

How visibility fails: Root causes of blind spots

Achieving total visibility isn't as simple as flipping a switch. The blind spots in your cloud environment are a symptom of fundamental architectural and operational challenges:

- **Decentralized DevOps:** Modern DevOps practices empower your teams to deploy and manage their own infrastructure, but this can bypass your traditional security gates. New assets are often created and then forgotten, leading to a sprawling and unaccountable network that you can't fully secure.
- **Multi-cloud sprawl:** When you use multiple cloud providers—AWS, Azure, GCP, and more—you are forced to grapple with different APIs, security tools, and data formats. This makes it virtually impossible for your security team to get a unified view of your entire environment without a centralized solution.
- **The rise of shadow IT:** The ease of spinning up cloud resources and subscribing to SaaS applications has created a new security nightmare. When your business units or individual employees bypass official IT channels, they create unmanaged endpoints that you cannot see or protect.
- **Cloud misconfigurations:** With thousands of configuration options, even a small error—like an open S3 bucket or an overly permissive firewall rule—can expose your sensitive data. These misconfigurations are difficult to track manually and often go undetected until a breach occurs.

A framework for total cloud visibility

Defeating the unseen threat requires a proactive, automated, and unified approach. A comprehensive cloud visibility framework is built on three core pillars designed to empower your team and secure your business:

Pillar 1 Automated asset discovery and inventory

What it is: This is the foundational layer. You need a solution that continuously scans and maps every single asset in your multi-cloud environment, from VMs and containers to serverless functions and APIs. It must work in real time, not just in scheduled scans, to keep pace with the dynamic nature of your cloud.

Actionable step: Implement a tool that integrates directly with all of your cloud providers to build a complete, real-time inventory of all your cloud resources.

Pillar 2 Continuous security posture monitoring

What it is: After you see the assets, you must know their state. This pillar involves continuously monitoring for misconfigurations, policy violations, and compliance drift against established security standards. This moves your team from a reactive, incident-driven security model to a proactive, preventative one.

Actionable step: Use a solution that automatically identifies and alerts on misconfigurations, providing you with a unified view of your security posture across the entire multi-cloud estate.

Pillar 3 Unified dashboard and alerting

What it is: This is your single pane of glass. This final pillar consolidates all of the data from asset discovery and posture monitoring into one, intuitive dashboard. Instead of your team sifting through fragmented alerts from different clouds, they can see all vulnerabilities and risks in one place, reducing alert fatigue and enabling faster, more coordinated responses.

Actionable step: Centralize all your cloud security data into a single, actionable dashboard with integrated alerting to empower your team to focus on high-priority threats.

Case study: An anonymous cloud security story

Scenario: A large financial services firm relied on a decentralized, multi-cloud strategy for its development teams.

The challenge: Due to the rapid pace of development, several unused development VMs were left running with default passwords in their Azure environment. Because these were considered non-production assets, they were excluded from routine security scans and did not appear on any central dashboard. This created a critical, undetected vulnerability that put the firm's data and reputation at risk. An attacker scanned for open ports, found one of these forgotten VMs, and gained a foothold. From there, they began to perform reconnaissance.

The solution: The finance firm implemented a new visibility solution that provided a complete, real-time inventory of their cloud assets across both AWS and Azure. Within hours, the solution discovered the abandoned VMs and immediately flagged them as high-risk due to their open ports and misconfiguration.

The outcome: The security team received an immediate alert, isolated the compromised VMs, and contained the threat before the attacker could move laterally. The outcome was a prevented breach, saving the company from potential data loss, regulatory fines, and brand damage. The team now has a unified, real-time view of every asset, ensuring they can protect what was once unseen.

The path forward

The findings of the **Cloud Network Security Report 2025** are clear: without complete visibility, your cloud is not secure. The unseen threat is not a future problem—it's here today, exploiting the blind spots created by your rapid, decentralized cloud growth.

By adopting a framework focused on automated discovery, continuous monitoring, and unified dashboards, you can move from a reactive to a proactive security posture. The first step to protecting your assets is to see them. It's time to shine a light on the unseen.

Schedule a demo today

To learn more and take the first step toward total cloud visibility, visit AlgoSec.com.

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

The AlgoSec platform enables the world's most complex organizations to gain visibility, reduce risk, achieve compliance at the application-level and process changes at zero-touch across the hybrid network.

Over 1,800 of the world's leading organizations trust AlgoSec to help secure their most critical workloads across public cloud, private cloud, containers, and on-premises networks.

algosec