algosec

WHITE PAPER



The enterprise guide to cloud security: A holistic approach

Contents

Executive summary 2

Why security is tricky in the cloud 3

Cloud network security: Stopping bad traffic 4

- Preventing unnecessary internet access 4
- Controlling lateral movement 5
- Ensuring proactive traffic prevention 6
- AlgoSec cloud security: Inherently proactive 6

Beyond network security 7

- Misconfigurations 7
- How AlgoSec ensures cloud misconfiguration remediation 7

Limitations of cloud-native security tools 8

Compliance and governance 9

- How AlgoSec makes you cloud security audit-ready 9

Complex application surface 10

- How AlgoSec drives application-centric cloud security 10

Building a secure cloud enterprise 11

Choosing a cloud security platform: Capabilities you need 12

Why AlgoSec for cloud security? 13

Conclusion 14

algosec

Executive summary

Cloud technologies are forever changing how businesses operate. By 2028, the cloud will be "a business necessity," with companies shovelling a whopping $679 billion into cloud services last year alone. There's no denying that the cloud is transformative, but equally evident is the magnitude of risk that the cloud poses.

Cloud security risks aren't the same as what enterprises had to deal with in legacy IT environments. Security is inherently trickier in the cloud, and businesses need to adopt a unique approach to deal with potent cloud threats.

In this white paper, we'll explore in detail why security in the cloud is so challenging, what security issues businesses need to look out for, why legacy tools aren't effective anymore, and how a platform like AlgoSec is the key to building a secure cloud enterprise.



algosec

Why security is tricky in the cloud

To keep cloud environments safe today, businesses need to completely revamp their security approach. This means shelving outdated on-premises security tools and tactics in favor of a modern, unified approach.

Today, cloud-based IT environments consist of highly dynamic and ephemeral resources, distributed architectures, and decentralized models, sourced from a smorgasbord of cloud service providers. Staying on top of what shared responsibility model each cloud provider follows is a task in itself.

Widespread cloud adoption has eroded traditional network perimeters, giving way to new ones, namely, applications, data, and identities. With so many fast-paced and short-lived resources being spun up in developer-driven cultures, cloud security visibility becomes a major hurdle.

Companies need to move beyond traditional fortress models of IT security and focus on models that prioritize application visibility. That doesn't mean merely seeing the applications; it means monitoring, controlling, and securing applications based on deeper cloud and business contexts.

What complicates matters further is the relentless flood of internal and external security risks. The cloud threat landscape is more menacing than ever, and cloud-native vulnerabilities stemming from high-octane development environments provide adversaries with multiple gateways to sensitive data.

The outcome? A surge in cloud incidents and an alarming number of data breaches across enterprises.

Breach-related financial setbacks ballooned in 2024, with the average incident hovering just under $5 million. The total cost of damages to organizations caused by cyberattacks is estimated to reach $10.5 trillion this year. Parallelly, cloud compliance and governance have become more demanding, with regulators and supervisors putting cloud operations under the microscope.

> **With the risk of data breach damages, reputational ruin, operational disruptions, and regulatory fines constantly looming, now is the time for enterprises to enhance their cloud security resilience. Untangling the intricacies of contemporary cloud network security is a good place to start.**

Cloud network security: Stopping bad traffic

In the past, network security included intrusion detection systems, firewalls, and antivirus software. Now, the focus needs to be on the true makeup of your cloud attack surface, which consists of applications, users, and data. Specifically, companies need to map and secure connectivity flows and understand how data moves between applications and through and beyond cloud environments.

Here are three of the most important steps businesses can take to reinforce network security and optimize cloud risk management.

Preventing unnecessary internet access

In cloud environments, there's always a risk of inadvertent exposure to the outside world. Sometimes, default configurations of cloud resources like virtual machines, serverless functions, containers, or storage buckets allow outbound internet traffic. If security operations (SecOps) cloud teams and other security personnel are late in catching those, it can lead to data breaches and compliance violations.

For example, if an AWS S3 bucket with sensitive PHI has unrestricted public access, threat actors can siphon off data without the enterprise knowing. Over time, this could lead to HIPAA fines, reputational damage, and a massive blow to the bottom line.

Actionable recommendations for blocking undesired traffic cloud-wide

1

Adopt a network segmentation cloud approach

In cloud environments, there's always a risk of inadvertent exposure to the outside world. Sometimes, default configurations of cloud resources like virtual machines, serverless functions, containers, or storage buckets allow outbound internet traffic. If security operations (SecOps) cloud teams and other security personnel are late in catching those, it can lead to data breaches and compliance violations.

2

Develop strong egress filtering cloud strategies

Disable any default or misconfigured settings that enable unrestricted outbound network traffic. Establish an allowlist of destinations that network traffic can travel to, and restrict everything else.

3

Leverage network access control lists (NACLs) and security groups

to implement specific rules around incoming and outgoing traffic. For example, enterprises can only allow traffic from certain Classless Inter-Domain Routing (CIDR) blocks.

Controlling lateral movement

If an adversary manages to infiltrate enterprise cloud environments, their next step usually involves moving laterally to escalate attacks or access more sensitive data. In the cloud, the smallest misconfiguration in a VM or an API can be used by attackers to gain an initial foothold before escalating privileges. Any open connection across an enterprise's cloud architecture can result in large-scale disasters.

Actionable recommendations for preventing lateral movement in the cloud



Implement zero trust principles and controls across cloud environments

This includes continuous authorization, multi-factor authentication (MFA), and access based on the principle of least privilege. Zero trust cloud network security presupposes that all users are dangerous, which means that all lateral movement will be flagged as potentially dangerous.



Decouple and isolate applications and services

using business logic and the specifics of the current cloud architecture. Business criticality is another important factor to consider when isolating cloud applications. The more granular an enterprise cloud is, the harder it is for adversaries to move from one segment to another.



Introduce robust monitoring and logging mechanisms

that provide comprehensive real-time insights into enterprise cloud estates. Pay close attention to an unusual number of access requests or spikes in network traffic, both of which are indicators of compromise.

Ensuring proactive traffic prevention

Reactive cloud security in today's threat landscape is a ticking time bomb. One of the most important steps to secure enterprise cloud networks is adopting a proactive cloud security approach. In the simplest terms, this means uncovering and addressing problems before they develop into full-blown incidents.

To ensure proactive cloud security, businesses need cloud security solutions that leverage AI-driven automation capabilities. Cloud security automation can help companies and their security teams keep pace with the speed of cloud environments and threats.

Actionable recommendations for achieving proactive cloud security

Replace a perimeter-based cloud security approach with a policy-based approach.

A policy-based cloud security strategy helps eliminate security siloes and nurture a more unified rules-based model. To introduce policies effectively, accurately, and at scale, businesses should automate policy enforcement and management.

Build compliance requirements from standards like PCI DSS, HIPAA, and GDPR

into security controls and policies. This will ensure that anomalous behavior or any cloud activity that strays from compliance baselines will be flagged and mitigated before it matures into security or noncompliance incidents.

Implement real-time detection and response mechanisms

that continuously evaluate traffic, spot suspicious patterns and behaviors, and provide mitigation suggestions. This will proactively address vulnerabilities and misconfigurations (e.g., unrestricted inbound /outbound ports or unsecured APIs) that might trigger excessive, noncompliant, or risky data exchanges.

AlgoSec cloud security: Inherently proactive

To adopt a truly proactive cloud security approach, enterprises need the right tools. All of AlgoSec's capabilities—policy simulation, risk analysis, automated change validation, continuous compliance checks, remediation recommendations, and more—are built to support proactive cloud security strategies. The platform essentially ensures businesses are always a few steps ahead of cloud risks.

By moving on from reactive cloud security approaches with AlgoSec, companies will see improvements across critical cloud security metrics like mean-time-to-detection and mean-time-to-resolution, data breach costs, volume of noncompliance incidents, and operational productivity and efficiency.

Beyond network security

Network security is a major part of the cloud security puzzle, but the complexities of the cloud don't end at the network. Businesses have numerous other cloud-native hurdles to overcome before they can truly unlock the cloud's transformative benefits.

Some of the biggest issues include misconfigurations, ineffective tools, compliance challenges, and the inability to effectively protect applications.

These obstacles to cloud security are further exacerbated because companies often lack cross-cloud visibility, hybrid cloud integration, vendor-agnostic policy orchestration, and the business context required to prioritize risks across their diverse environments. Those are precisely the gaps that AlgoSec is built to bridge.

This section will shed light on specific cloud challenges and touch on how AlgoSec can solve them.

Misconfigurations

As volatile as the threat landscape currently is, one of the biggest cloud security vulnerabilities comes from inside enterprise environments. We're talking about misconfigurations, which are essentially just suboptimal or inadequate settings on cloud resources.

Here are some example misconfigurations businesses are likely to come across in their cloud:

- **Excessive access privileges**
- **Exposed storage buckets/data**
- **Suboptimal encryption**
- **Outdated and unpatched applications**
- **Poor credential hygiene**
- **Incomplete logging/monitoring**
- **Unrestricted inbound traffic**
- **Firewall misconfigurations**

How AlgoSec ensures cloud misconfiguration remediation

Major incidents can stem from cloud misconfigurations. AlgoSec addresses these by providing complete visibility into cloud environments, preventing the number of users who can make configuration changes, and optimizing change management.

Most importantly, AlgoSec furnishes enterprises with the deep context needed to know which misconfigurations are critical. For example, a seemingly small misconfiguration that can lead adversaries to business-critical data should be treated as a high-risk threat. AlgoSec makes sure you know which misconfigurations can cause the most damage to your organization.

Limitations of cloud-native security tools

Cloud-native security tools can be immensely useful for enterprises to deal with various threats and attacks. For example, cloud workload protection (CWP), runtime application self-protection (RASP), and cloud security posture management (CSPM) are all essentials of cloud security, but if they're disjointed and ungoverned, it can cause tool sprawl and security silos.

Another major deficiency of many major cloud security tools, especially in heterogeneous tool stacks, is context. Without accurate business and workload contexts, organizations will struggle to identify which issues pose the biggest threat to business-critical processes, resources, and data.

Lastly, businesses can end up commissioning extra tools to address gaps in their existing tool stack. While the objective of using more cloud-native tools is to optimize threat detection and remediation, there's always the risk of tool sprawl, which can be a security threat in and of itself.

How AlgoSec breaks down tool silos

AlgoSec understands that disjointed security tools are themselves major cloud vulnerabilities. That's where AlgoSec's strong integration capabilities come into play, as it can seamlessly integrate with leading cloud-native tools. This includes network security tools, cloud platforms, SIEM and SOAR tools, change management systems, vulnerability scanners, and DevSecOps cloud security tools.



algosec

Compliance and governance

Navigating the contemporary compliance landscape is another major headache for enterprises, especially those in heavily regulated industries and regions. Standards like GDPR, HIPAA, and PCI DSS have to be followed to a tee, and new compliance standards and obligations constantly add to the tangle.

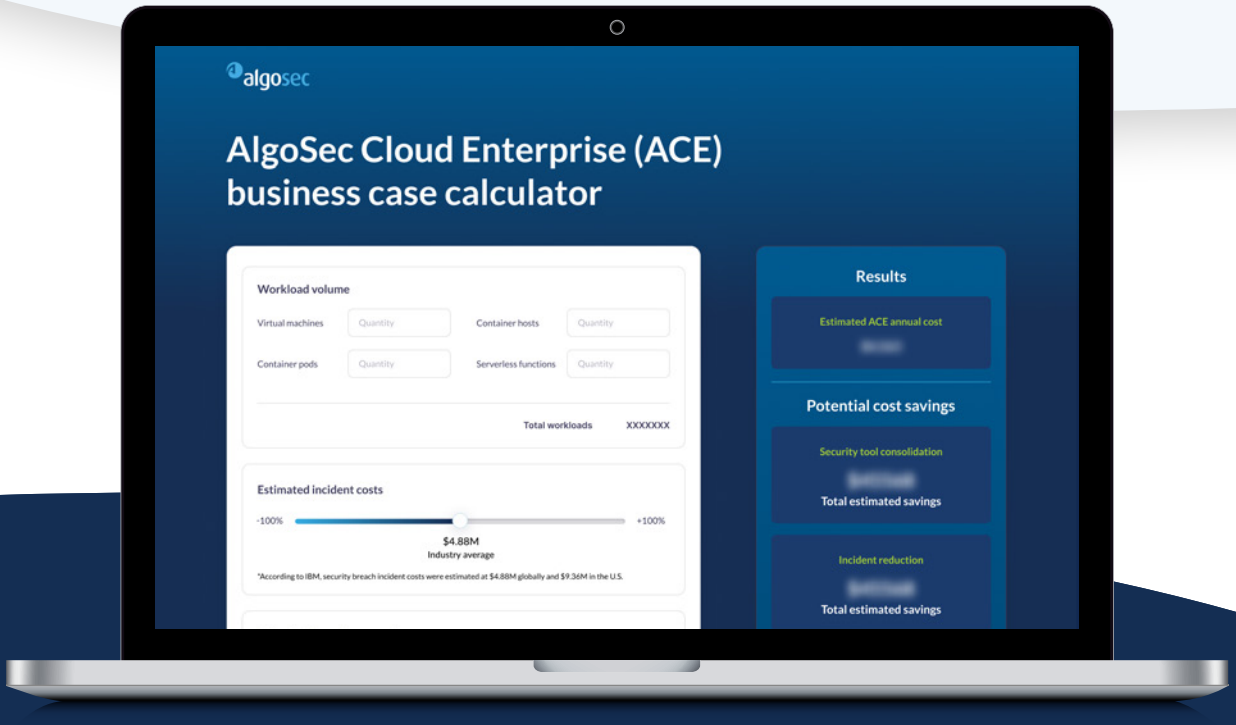
Now more than ever, businesses are in need of automated compliance checks, thorough logging for audits, and mechanisms to ensure that policies are consistently enforced. Automation helps boost a company's overall compliance posture, both by enforcing compliance guardrails and providing audit-ready documentation.

How AlgoSec makes you cloud security audit-ready

A unified platform like AlgoSec provides the numbers and metrics required for cloud security reporting. This helps businesses stay on top of every potential security, compliance, or risk management audit. The platform will generate reports to demonstrate compliance with numerous standards, including PCI DSS, SOX, HIPAA, GDPR, and ISO/IEC 27001.

Interested in knowing the exact benefits of using AlgoSec, including quantifiable risk reduction and how to boost ROI?

Check out our ROI calculator



Complex application surface

Today, applications are an enterprise's primary assets. They're also the main target for threat actors. In complex and dynamic cloud environments, businesses may find it difficult to map connectivity flows and gain complete visibility across application architectures. As a result, it's not always straightforward to arrive at the root cause of performance and security issues.

Businesses need to do more than just introduce new capabilities; they need to completely shift to an application-centric cloud security approach. This means driving DevSecOps security initiatives that cover security risks all the way from code to runtime environments.

How AlgoSec drives application-centric cloud security

For AlgoSec, robust cloud security is synonymous with robust application security.

Applications are enterprise engines, meaning they are almost always under attack. AlgoSec's application discovery and management capabilities ensure companies have a complete top-down view of every application across their environments and connectivity flows.

By using AlgoSec, businesses can reinforce application security while boosting application performance.



Building a secure cloud enterprise

To mitigate the broad spectrum of cloud risks that we highlighted in this paper, organizations need a comprehensive cloud security platform that provides unified control across all cloud and on-premises environments. Crucially, it needs to do so from a single, unified dashboard. A tool like this drives home the "single source of truth" model, where everything an organization needs to get a clear picture of its cloud security is interconnected, contextualized, and accessible via a single pane.

But achieving unified control with a comprehensive cloud security platform delivers more than complete visibility. A unified platform is the secret to cloud security orchestration and automation, both of which are must-haves to deal with the threats companies face today.

Higher degrees of automation and orchestration also help organizations deal with the global cloud security skills gap. They help you do more with less, empowering you to tackle the world's most complex cloud security challenges without needing an army of specialists.



Choosing a cloud security platform: Capabilities you need

How can enterprises identify the best cloud security product from a reliable provider? Here's a list of priority features to keep an eye out for:

Total unrestricted observability across cloud networks

Automated network security policy management, including policy-as-code (PaC) security

Continuous and automated compliance checks

Complete visibility across the application surface, including connectivity flows and dependencies

Automated configuration drift detection and configuration management

Seamless cross-cloud capabilities

Multi-cloud firewall management



AlgoSec has all these features and more, all built into a single platform. In the next section, we'll provide further details as to why AlgoSec is the cloud security powerhouse businesses need.

Why AlgoSec for cloud security?

AlgoSec Cloud Enterprise (ACE) is the optimal platform to empower enterprises to secure and streamline their cloud operations. With ACE, enterprises can:

Gain total command and oversight over complex and adaptive hybrid and multi-cloud environments.

Minimize cloud-native threats and ensure that your enterprise cloud network security posture is in top shape.

Navigate high volumes of cloud risks using prioritization based on severity levels and potential impact on business-critical services and applications.

Gain a comprehensive and contextual view of how cloud networks might inadvertently be internet-facing.

Ensure adherence to zero trust principles by achieving visibility of inadvertent or suspicious bilateral movement between networks.

Achieve centralized control over virtual cloud firewalls.

Fully automate your policy management lifecycle.



Conclusion

So what have we learned? The cloud is packed to the brim with exciting features and benefits, but businesses need to mitigate unique risks along the way. The cloud is inherently complex and requires a dedicated and proactive approach to deal with its security entanglements.

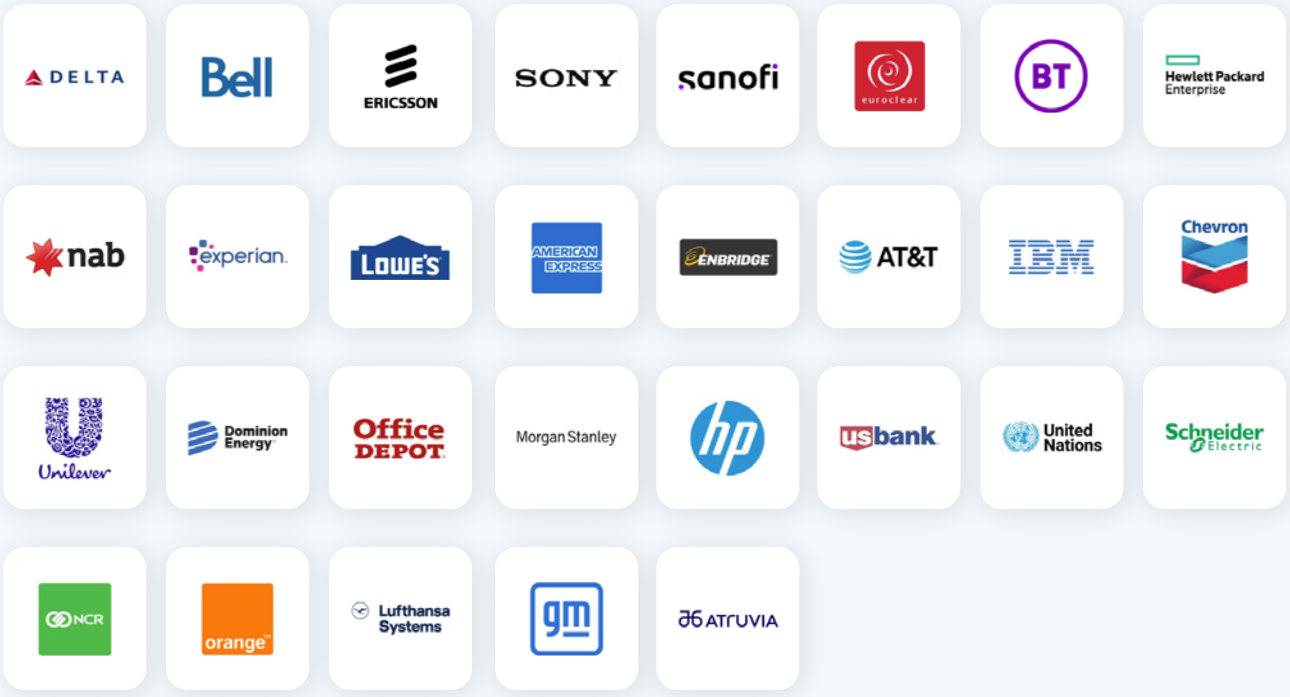
All in all, a proactive cloud security approach is only possible with an advanced platform like AlgoSec.

With ACE, businesses gain complete application visibility and protection, a robust network security posture, unified fortifications, and continuous compliance management. AlgoSec Cloud Enterprise is a powerful platform for all things cloud security—from streamlining cloud misconfiguration remediation to enforcing cloud security best practices.

With ACE, you'll significantly reduce the possibility of data breaches and keep your business-critical applications safe from any network security risks.

If you want to get a firsthand look at what 2,200 other companies have gained by using AlgoSec,

Get a demo now



algosec