algosec

Secure application connectivity.
Anywhere.

Whitepaper

The business case for AlgoSec Cloud Enterprise

Reducing costs and improving security in hybrid and multi-cloud environments

The business case for AlgoSec Cloud Enterprise (ACE)

Reducing costs and improving security in hybrid and multi-cloud environments

An AlgoSec Whitepaper

The rapid adoption of hybrid and multi-cloud environments has created unprecedented complexity for cloud network security teams. Organizations struggle to maintain visibility and control over sprawling cloud deployments, leading to increased risk of security breaches, compliance violations, and costly downtime. Traditional perimeter-based security models are no longer sufficient to protect dynamic applications and workloads distributed across diverse environments.

Cloud network security professionals face unprecedented challenges in today's complex hybrid and multi-cloud environments. As a cloud network security professional, you know that today's hybrid and multi-cloud environments are incredibly complex to secure. AlgoSec Cloud Enterprise (ACE) provides a unique application-centric approach that gives you the visibility, automation, and control needed to optimize your security posture, reduce risk, and demonstrate compliance. ACE maximizes ROI and frees your team to focus on strategic initiatives. ACE empowers organizations to confidently embrace the agility of the cloud while minimizing cloud network security risks and maximizing ROI. This white paper explores the financial benefits and security enhancements ACE delivers, making a compelling case for its adoption.

Consider the cost and severe consequences of hybrid and multi-cloud insecurity

The cost of insecurity in the cloud

Failing to secure your cloud environments can have severe consequences, impacting your organization's bottom line, your team's productivity, and your ability to meet compliance requirements.

Data breaches: The average cost of a data breach in 2024 reached $4.88 million globally and $9.36 million in the U.S. [IBM]. These costs include regulatory fines, legal expenses, compensation to affected individuals, and the loss of customer trust. ACE identifies assets that are inadvertently exposed to the internet, creating potential attack vectors for unauthorized access. By pinpointing these vulnerabilities, ACE enables security teams to implement corrective actions before they can be exploited, significantly reducing the risk of a successful breach.

Downtime: Downtime caused by security incidents can result in significant financial losses. The average cost of downtime across industries is estimated at $225,000 per day, with cyberattacks causing an average of 18 days of downtime [IDC]. ACE helps prevent downtime by offering

- **Vulnerability management:** ACE assesses the security posture of cloud environments, identifying misconfigurations, vulnerabilities, and exposed assets before they can be exploited. This proactive approach prevents attacks that could lead to downtime.
- **Application-centric security:** By focusing on application dependencies and connectivity, ACE allows for granular security policies that minimize the attack surface. This reduces the likelihood of successful attacks that disrupt application availability.

Compliance violations: Failing to comply with industry regulations like PCI DSS, HIPAA, and GDPR can result in substantial fines and penalties, often exceeding the average cost of a data breach. Organizations with significant compliance gaps face an average cost of $5.05 million [IBM]. ACE's application-centric approach proactively addresses compliance requirements by:

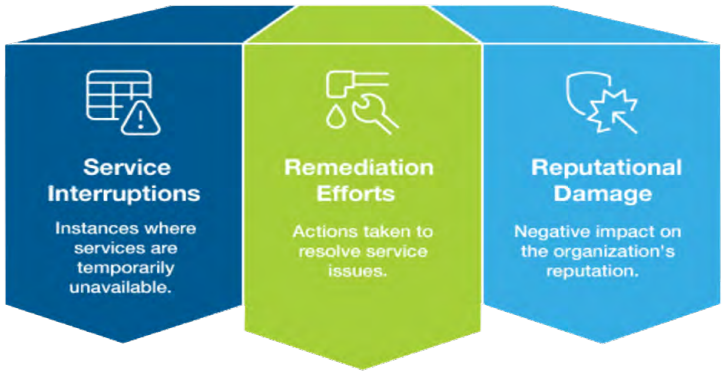
- **Compliance checks:** ACE monitors application configurations and network security policies to identify potential compliance violations, reducing manual effort and ensuring consistent enforcement.
- **Providing granular visibility:** ACE provides deep visibility into application traffic flows, security controls, and user access, enabling you to identify and address compliance gaps proactively.
- **Generating audit-ready reports:** ACE generates comprehensive reports that demonstrate compliance with specific regulatory requirements, streamlining audit processes and reducing audit preparation time.
- **Enforcing consistent security policies:** ACE ensures that security policies are consistently applied across all environments, minimizing the risk of inconsistencies that can lead to compliance violations.

Reduced IT security staff expenses: ACE's unified security management streamlines operations across hybrid environments, freeing IT staff from repetitive tasks and enabling them to focus on strategic initiatives. This increased efficiency translates to reduced staff expenses.

- Lower security tool costs: In many cases, ACE can replace existing security tools, leading to significant savings on licensing and maintenance.
- Decreased incident response costs: By proactively identifying and prioritizing remediation of misconfigurations and risks, ACE reduces the number of security incidents. This, in turn, minimizes the time and resources required for investigation, remediation, and recovery, resulting in lower incident response costs.

Operational disruptions

Security incidents cause operational disruptions that can cripple an organization. These disruptions range from service interruptions impacting customer service and supply chains, to resource-draining remediation efforts that pull IT staff away from strategic work. Beyond these direct costs, the reputational damage of a security breach can lead to customer churn and market share loss.



Service interruptions: Security incidents can disrupt critical business operations, impacting customer service, productivity, and supply chain processes. ACE assesses your cloud security posture, identifying and mitigating vulnerabilities and misconfigurations before they can be exploited. This proactive approach helps prevent security incidents that could lead to service interruptions.

Remediation efforts: Responding to security incidents and remediating vulnerabilities can consume significant time and resources, diverting IT staff from strategic initiatives. ACE prioritizes remediation efforts based on risk, allowing you to focus on the most critical vulnerabilities first. This ensures that the most important systems and applications are protected, minimizing the impact of potential incidents.

Reputational damage: Security breaches can severely damage an organization's reputation, leading to customer churn and loss of market share. ACE helps you establish a security posture that inspires confidence, strengthens customer relationships, and protects your business reputation.

The evolving challenges of cloud security

As a cloud network security professional, you're constantly facing new and evolving challenges. Here are some of the key issues you need to address:

- **Complexity and visibility:** ACE provides unified visibility across all environments (AWS, Azure, GCP). Security teams struggle to gain a holistic view of their security posture, lacking a "single pane of glass" to monitor and control security across all environments. ACE addresses this challenge by providing unified visibility into application connectivity and security controls across all cloud and on-premises environments, simplifying management and enabling a comprehensive understanding of the organization's security posture.
- **Dynamic environments:** Constant changes in cloud infrastructure and applications make traditional security models obsolete. ACE overcomes this limitation with its cloud-native architecture and automated discovery capabilities. It continuously monitors and adapts to changes in the cloud environment, ensuring that security policies remain relevant and effective.
- **Cloud-native threats:** The rise of cloud-native technologies like serverless computing (AWS Lambda, Azure Functions), containerization (Docker, Kubernetes), and microservices architectures introduces new attack vectors. ACE provides specialized security capabilities to address these cloud-native threats. Its application-centric approach enables granular control over security groups, container and serverless deployments, while its threat detection engine is constantly updated to identify and respond to emerging cloud-native attacks.
- **Shared responsibility model misunderstandings:** Confusion about the division of security responsibilities between providers and customers leaves organizations vulnerable. ACE helps clarify these responsibilities by providing visibility into the customer's security domain and automating key security tasks, ensuring that organizations fulfill their obligations under the Shared Responsibility Model.
- **Skills gap:** The shortage of cloud security professionals makes it difficult to manage security effectively. ACE streamlines routine tasks and reduces the reliance on manual processes and specialized expertise. This allows organizations to maximize the efficiency of their existing security teams and focus their resources on strategic initiatives.

Limitations of traditional security approaches

Traditional security tools and strategies simply weren't designed for the dynamic and distributed nature of today's cloud environments. This leaves your organization vulnerable to new threats and makes it difficult to manage security effectively. Several key limitations highlight this:

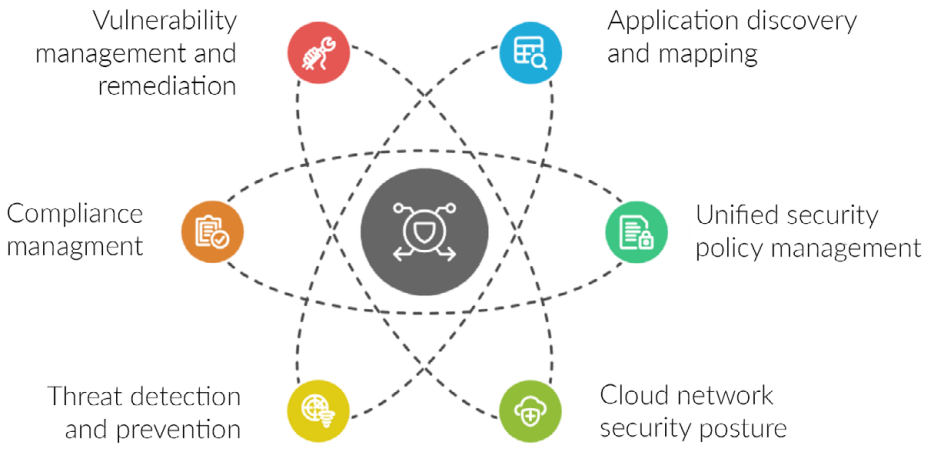
- **Demise of the perimeter:** Traditional security models rely heavily on the concept of a well-defined network perimeter. In the cloud, however, this perimeter has become porous and often non-existent. Applications and data reside across multiple environments, making it impossible to establish a clear boundary. Firewalls and VPNs, the cornerstones of traditional security, are no longer sufficient to protect against threats that originate from within or bypass the perimeter.
- **Siloed security and management complexity:** Hybrid and multi-cloud environments often involve a mix of different cloud platforms (AWS, Azure, GCP) and on-premises infrastructure. Managing security across these diverse environments with disparate, siloed security tools creates significant complexity. Security teams struggle to maintain consistency, visibility, and control, leading to increased risk of misconfigurations, vulnerabilities, and security breaches.

- **Lack of agility and automation:** Traditional security approaches are often manual and time-consuming. They lack the agility and automation necessary to keep pace with the rapid pace of cloud innovation and the dynamic nature of cloud workloads. This can lead to security bottlenecks, slowing down application development and deployment, and hindering business agility.

- **Application-centricity imperative:** Traditional security focuses primarily on protecting the network infrastructure. However, in the cloud, applications are the primary target for attackers. A more effective approach requires shifting the focus from the network perimeter to the application itself. This means understanding application dependencies, network connectivity, and security requirements, and implementing security controls tailored to each application.

AlgoSec Cloud Enterprise: A modern approach

ACE is designed specifically for cloud network security professionals like you. It provides the tools and capabilities you need to overcome the challenges of securing hybrid and multi-cloud environments.



Key capabilities and benefits:

- **Application discovery and mapping:** ACE automatically discovers and maps application dependencies and connectivity across all environments, providing a comprehensive view of application relationships and potential vulnerabilities.
  - **Benefit:** Improved visibility, reduced attack surface, and enhanced understanding of application risk.
- **Unified security policy management:** ACE streamlines security policy management across hybrid and multi-cloud environments, ensuring consistent security posture and reducing manual effort.
  - **Benefit:** Streamlined operations and consistent security
- **Cloud network security posture:** ACE continuously unmatched network security posture: over 150+ network security policy risks checks including customized risks enabling unique segmentation or zero trust policy enforcement.
  - **Benefit:** Proactive risk mitigation, continuous compliance, and reduced exposure to threats.
- **Threat detection and prevention:** ACE maps cloud network security risks to applications, enabling an understanding of which critical business applications are most vulnerable.
  - **Benefit:** Reduced incident impact, faster threat response, and enhanced protection against emerging threats.

- **Compliance management:** ACE facilitates compliance checks, generates audit-ready reports, ensures consistent policy enforcement, simplifies audits and reduces compliance costs.
  - **Benefit:** Simplified audits, reduced compliance costs, and improved adherence to regulatory requirements.

- **Vulnerability and remediation:** ACE proactively identifies and prioritizes vulnerabilities based on business impact, enabling security teams to focus on the most critical threats. It also prioritizes remediation, minimizing downtime and reducing the risk of exploitation.
  - **Benefit:** Proactive risk reduction, minimized downtime, and efficient use of security resources.

Conclusion

The adoption of hybrid and multi-cloud environments has undeniably transformed the way organizations operate, offering unparalleled flexibility and scalability. However, this transformation has also introduced a new era of security challenges, demanding a modern approach to protect critical assets and data. As this white paper has demonstrated, traditional security models are no longer sufficient to address the complexities of cloud environments.

Cloud network security professionals face a daunting task: securing dynamic workloads, maintaining visibility across diverse platforms, and keeping pace with evolving threats, all while managing limited resources and a growing skills gap. Failing to address these challenges can lead to significant financial losses, operational disruptions, and reputational damage.

AlgoSec Cloud Enterprise offers a compelling solution. By providing an application-centric approach, comprehensive visibility, and powerful automation capabilities, ACE empowers security teams to:

- **Reduce risk:** Proactively identify and mitigate vulnerabilities, misconfigurations, and threats.
- **Improve compliance:** Automate compliance checks, generate audit-ready reports, and ensure consistent security policy enforcement.
- **Optimize security posture:** Gain a holistic view of security across all environments and streamline security operations.
- **Lower costs:** Reduce IT security staff expenses, consolidate security tools, and minimize incident response costs.

ACE is more than just a security tool; it's a strategic enabler that allows organizations to confidently embrace the agility and scalability of the cloud while ensuring robust security and maximizing ROI.

Ready to take control of your cloud security?

- **Request a personalized demo of ACE today:** See firsthand how ACE can help you overcome your cloud security challenges and achieve your security goals.

Don't let cloud security complexity hold you back. Embrace the future of security with AlgoSec Cloud Enterprise.

algosec