algosec

Secure application connectivity.
Anywhere.

Whitepaper

Stop hunting after the breach

Achieving proactive zero trust with AlgoSec Cloud Enterprise

Stop hunting after the breach

Achieving proactive zero trust with AlgoSec Cloud Enterprise

An AlgoSec Whitepaper

Your challenge

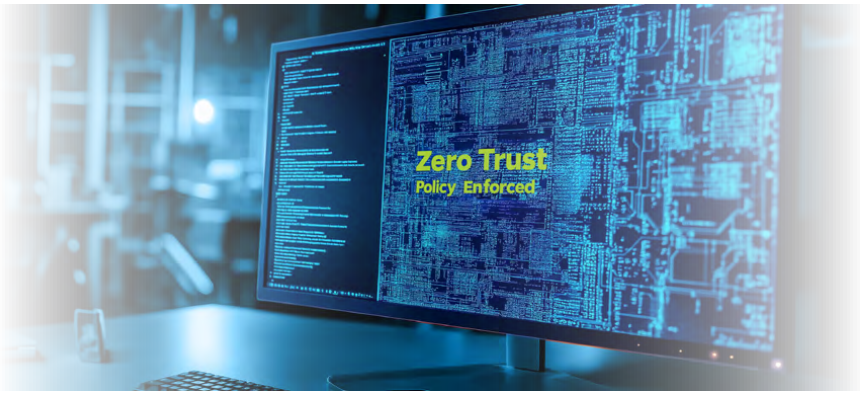
The rapid shift to cloud and hybrid infrastructure has created a security complexity headache. Your Virtual Private Clouds (VPCs) and security groups are constantly being updated, often leading to misconfigurations that create silent, exploitable attack paths. Traditional security, focused on checking traffic logs, only tells you after an attack or breach has occurred. You're constantly playing catch-up.

Your proactive solution

AlgoSec Cloud Enterprise (ACE) introduces Attack Path Analysis, a unique, proactive feature designed to put you back in control. It takes the policy expertise you already trust from AlgoSec and applies it to the cloud, performing a deep analysis to identify and visualize potential security flaws and misconfigurations before they are ever exploited.

Your result

With ACE, you can finally build true, proactive Zero Trust. You get continuous, configuration-based visibility that eliminates hidden risks, drastically shrinks your cloud attack surface, and ensures consistent security compliance across all your complex hybrid environments.



The High Cost of Reactive Security

Why traditional cloud security leaves you exposed

For too long, the security mantra has been "detect and respond." In the cloud world, this means relying on analyzing flow logs and active traffic—effectively, confirming a problem has already happened. This reactive approach forces your team into the stressful, resource-intensive role of "breach hunters" every time an alert fires. When attackers can exploit configuration gaps faster than you can find them, detection is simply not enough.

The headache of cloud complexity: Unintended open doors

Cloud agility is a double-edged sword. While rapid deployment is great for business, it also means your cloud environment is a constantly shifting maze of VPCs, routing rules, and security groups. A small oversight—a single overly broad rule—can unintentionally create a path from the public Internet directly to a sensitive database. Because cloud systems prioritize speed over inherent security, these misconfigurations are inevitable, leading to silent, exploitable vulnerabilities that accelerate the rate of costly data breaches.

Extending the trust you already have to the cloud

You already rely on AlgoSec to manage the complexity of your on-premise firewall and network security policies. ACE seamlessly extends this proven intelligence into your cloud domain. This bridges the trust you have in our policy analysis to your cloud-native configurations, ensuring that the same rigorous enforcement and compliance standards apply everywhere.

Introducing ACE connectivity analysis: Your shield of proactive zero trust

The shift: How ACE helps you stop hunting

The ACE Attack Path Analysis fundamentally shifts your security posture from forensic to preventative. Instead of analyzing what has happened (network traffic), we analyze what could happen (system configuration). Our core thesis empowers you to: If you can identify and close potential access paths before they are used, you can STOP Hunting After the Breach entirely.

What it is: Security modeling that predicts the attack

ACE doesn't just check for active connections; it delivers a comprehensive security model that maps the potential configuration weaknesses across your entire hybrid infrastructure. This powerful, unique capability allows you to pinpoint and fix mistakes before they become exploited, giving you true, proactive visibility across multi-cloud and on-premise deployments.

Zero Trust, Applied proactively

ACE makes true Zero Trust achievable. By meticulously identifying every potential access path and misconfiguration, your security team gains the visibility needed to enforce the principle of least privilege. You can confirm that connections are only possible when explicitly necessary, continuously verifying that your security policy intent matches the actual, configuration-based risk.

Deep dive: The two layers of the ACE difference

ACE's analysis is delivered through two integrated layers, ensuring comprehensive coverage from the network perimeter down to your core applications.

Layer 1 Seeing the network landscape (configuration health check)

This initial layer analyzes the system's configuration to uncover potential connectivity and inherent security risks, without needing volatile real-time traffic data.

Internet access check: Since nearly every external breach involves access from the Internet, we explicitly map the ability of your cloud assets to be reached from the public domain. This is your crucial first step in identifying breach points.

VPC analysis: ACE provides essential context by showing how many other VPCs can access a specific resource. If a resource has an unusually high number of inbound connections, it's flagged as a likely security misconfiguration risk, helping you prevent lateral movement by attackers.

Public IP visibility: You get a detailed, easy-to-read list of public IP addresses per VPC and account, instantly highlighting configuration errors that might be inadvertently exposing assets you intended to keep private.

Layer 2 Protecting your crown jewels (application focus)

The second layer takes the configuration risks identified in Layer 1 and maps them directly to your critical business applications, enabling application-centric risk prioritization.

Application exposure: This quickly identifies applications or network-facing components within them that were never intended to be public. For example, ACE will flag a mistake like a security group allowing all IPs for HSS sessions on a critical EC2 instance, confirming a direct application-level risk that needs immediate attention.

Internet-facing filter: Your team can immediately filter results to focus on the highest-priority threat: internet-facing applications. This ensures your limited remediation resources are spent addressing the most immediate, externally exposed risks first.

The outcome: Security, simplicity, and confidence

The unified hybrid view

The true competitive advantage of ACE is the ability to consolidate your security posture. By providing a Unified hybrid view, you can import cloud applications and have a single, authoritative platform for managing security policies and configurations across diverse infrastructures—from firewalls to cloud-native constructs. This eliminates frustrating operational silos and gives you one source of truth.

Unparalleled visibility for attack surface reduction

ACE gives you eyes where you need them most: deep inside your cloud configurations. By identifying and visualizing hidden attack paths, the platform empowers your team to proactively close network gaps and correct routing errors. This direct, preventative action leads to a significant and measurable reduction in your overall attack surface.

Simplified compliance and security posture

Stop wrestling with fragmented compliance checks across different cloud vendors (AWS, Azure, GCP). ACE provides a streamlined, consistent platform that manages connectivity and security compliance, ensuring you can maintain a high, auditable security posture effortlessly, no matter how fast your cloud footprint grows.

Stop hunting. Start eliminating.

The modern digital landscape demands more than reactive security. The complexity of the cloud demands a proactive solution that analyzes configuration risk before exploitation can occur.

ACE Attack Path Analysis leverages AlgoSec's trusted policy expertise to give your team the foresight needed to manage true Zero Trust proactively. It's time to move from hunting breaches to eliminating them.

Next Steps

Ready to stop hunting and start preventing? **Contact your AlgoSec representative today** to request a personalized demo and discover how ACE and its new Attack Path Analysis feature can eliminate hidden risks and secure your cloud environment.

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