algosec

Secure application connectivity.
Anywhere.

Whitepaper

Prediction over reaction

Enabling Zero Trust with AlgoSec Cloud Enterprise Attack Path Analysis

Prediction over reaction

Enabling Zero Trust with AlgoSec Cloud Enterprise Attack Path Analysis

An AlgoSec Whitepaper

The cloud security paradox

The agility of the cloud is being sabotaged by the fragility of its security.

For years, your team of multi-cloud security experts has been pushing the pace of digital transformation, adopting dynamic microservices, hybrid environments, and multiple cloud providers (AWS, Azure, GCP). Yet, the tools you rely on—many of them adapted from on-premise firewall management or designed merely to monitor cloud endpoints—simply cannot keep up.

This gap creates the **Cloud Security Paradox**: The more innovative and dynamic your environment becomes, the larger and more opaque your security risk grows.

The reactive gap: Why you can't afford to wait

Most security solutions offer a reactive view of the world. They answer the question: *What has already happened?* They analyze traffic flows, audit current settings, or flag misconfigurations after they are deployed. This is a game of continuous catch-up, and in the cloud, even a few minutes of exposure can lead to a material breach.

This reactive mindset creates a fundamental block for Zero Trust (ZT). You cannot enforce ZT principles (never trust, always verify) if your foundational network visibility is incomplete. Zero Trust requires absolute knowledge of every possible connection, but traditional tools only show the connections that have been observed.

The solution thesis: AlgoSec Cloud Enterprise (ACE) predicts the threat

ACE is engineered to bridge this reactive gap by shifting your security posture management from reaction to prediction.

ACE's unique Attack Path Analysis feature models the true, end-to-end network topology across your entire hybrid cloud estate. By revealing every single possible connection—both private and public—ACE uncovers the critical, hidden attack vectors and security policy errors that reactive tools miss, empowering your Zero Trust strategy and ensuring compliance from day one.

The limitations of traditional reactive security

For security and compliance experts, the shortcomings of current cloud security posture management (CSPM) and network flow analysis tools boil down to three dangerous realities: A blind spot for risk, policy overload, and a lack of contextual insight.

The blind spot of flow monitoring: observed vs. possible

The most common reactive tool is traffic analysis (flow logs, VPC Flow Logs, etc.). While useful for forensics, flow analysis introduces a massive security blind spot:

- **It only shows the connections that have occurred.** If a security group or firewall rule creates a path that an attacker hasn't exploited yet, flow data gives you a clean bill of health. This "Never Used" Risk—over-permissive rules that allow potential access—remains the biggest hidden exposure.
- Attackers don't follow observed traffic patterns; they exploit the possible paths opened by policy errors. Relying on flow data means you are consistently too late to prevent the breach.

Policy overload and dangerous policy drift

Multi-cloud security engineers face a management nightmare: policies across AWS Security Groups, Azure Network Security Groups (NSGs), on-prem firewalls, and Kubernetes network policies.

Ineffective change management across this fragmented landscape leads directly to policy drift, where:

- **Superfluous rules proliferate:** Legacy rules are left open "just in case," creating broad, unnecessary entry points.
- **Context is lost:** An engineer makes a seemingly benign change in one cloud that, when combined with a specific route table setting in another, inadvertently opens a critical lateral movement path.

This policy drift leads to compliance failures and, crucially, opens those critical hidden attack vectors that reactive tools are structurally incapable of finding.

The need for contextual analysis

Compliance teams and CISOs care less about the raw number of vulnerabilities reported and more about exploitable risk. Traditional CSPM delivers a list of thousands of misconfigurations. But which one is the most dangerous? Security is not about counting vulnerabilities; it's about mapping the context of exploitable paths from an attacker's perspective. Without this context, every patch cycle is a shot in the dark.

ACE's predictive power: How attack path analysis works

ACE's Attack Path Analysis feature is the definitive shift to a predictive model. Instead of looking backward at logs, ACE looks forward by modeling your entire network's security posture as a unified, connected graph.

The ACE paradigm: Prediction by modeling

ACE models the network by ingesting and analyzing the governing configuration elements—not the traffic—from every corner of your hybrid environment:

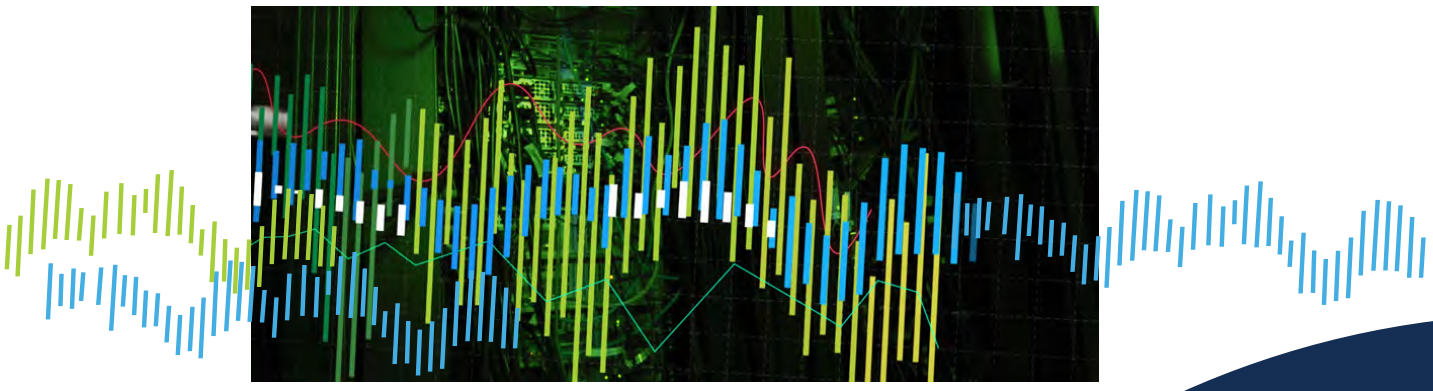
- Cloud security policies (security groups, NSGs, GCP firewalls)
- Network access control lists (NACLs)
- Route tables and transit gateway attachments
- Virtual private cloud (VPC) / virtual network (VNet) structures
- Hybrid connection points (VPNs, direct connects)
- Asset and identity inventory

By calculating the *intersection* of all these rules, ACE builds a comprehensive, mathematical map of all possible connections—a definitive view of your actual attack surface.

Mapping every connection: East-west and north-south

ACE delivers two dimensions of critical, predictive visibility:

- **North-south security (external exposure):** ACE identifies all exposed assets by simulating an attack coming from the public internet. It traces every path that can lead from an external source to your sensitive environments, flagging exposed resources and exploitable external entry points.
- **East-west security (the Zero Trust focus):** This is the core of predictive Zero Trust enablement. ACE maps all lateral movement pathways across VPCs, hybrid links, and cloud regions. Since approximately 80% of major breaches involve internal lateral movement after an initial compromise, revealing these unintended East-West paths allows you to proactively enforce segmentation and least privilege before the attacker moves.



Revealing the true, exploitable risk

ACE takes policy mapping a critical step further by correlating policy data with threat intelligence:

- **Vulnerability chain analysis:** This is the ultimate predictive feature. ACE integrates external vulnerability data (CVEs) with the policy map. It doesn't just say, 'You have a vulnerable host.' It says, in plain language: *'Path A exists from the internet to your production database because of this over-permissive security group rule, which allows access to a host running a server with this specific, exploitable vulnerability (CVE-202X-XXXX).'* This allows security teams to prioritize fixes based on exploitability, not just presence.
- **Automated policy error identification:** ACE automatically flags and reports every over-permissive rule (like Any/Any or overly broad port ranges) that violates least-privilege principles, giving multi-cloud engineers the exact fix needed to right-size policies for Zero Trust.

The visualization advantage

ACE reduces investigation time from days to minutes by presenting complex, multi-hop attack paths—which might span five different clouds or hybrid devices—in a single, intuitive visual map. This visualization is key for communicating risk clearly to both technical teams and compliance officers.

Empowering Zero Trust from day one

Zero Trust is a journey, but it's often stalled by the massive effort required for the foundational step: gaining complete, auditable visibility into all network pathways. ACE transforms ZT from an aspirational goal into an achievable mandate.

ACE as the Zero Trust foundation: identify and protect

ACE's predictive analysis is used to directly execute the critical initial phases of a Zero Trust implementation:

Phase 1 Discovery (Identify the attack surface)

Before implementing micro-segmentation, you must know what needs to be segmented. ACE provides the definitive, mathematically validated map of every connection. This visibility is essential for understanding your blast radius and defining precise micro-perimeters, eliminating the guesswork that plagues most ZT projects.

Phase 2 Policy right-sizing (protect with least privilege)

The primary goal of ZT is least privilege. By leveraging the Automated Policy Error Identification (III.C.2), multi-cloud security engineers can instantly identify and narrow over-permissive security group rules (which the system previously flagged) to only the necessary connections. This proactive rule-tightening prevents lateral movement and drastically shrinks the attack surface without waiting for an incident.

Continuous Zero Trust assurance and compliance

The challenge of ZT is maintaining it in a DevOps-driven environment. ACE provides the continuous feedback loop necessary for assurance:

- **Potential risk monitoring:** ACE monitors the *potential* attack surface (not just observed activity). If a new deployment, IaC template, or policy change accidentally re-introduces a forbidden East-West attack vector or violates a defined security control, ACE flags it. This allows for proactive remediation before the change is merged or deployed.
- **Preventing compliance drift:** For compliance experts, ACE delivers auditable proof of segmentation integrity. Whether you are required to adhere to PCI-DSS, HIPAA, or internal segmentation standards, ACE provides continuous verification that network controls remain effective and have not drifted due to organic cloud evolution. This turns a complex, periodic audit into an ongoing, demonstrable compliance posture.

Stop chasing traffic logs. Start eliminating attack paths.

Reactive cloud security is a fundamentally losing strategy in the era of multi-cloud complexity and dynamic microservices. Tools that rely on traffic logs and post-facto audits will always leave hidden attack vectors exposed.

ACE transforms your security posture by providing predictive visibility into every possible connection, empowering your team to eliminate risk and enforce Zero Trust principles proactively.

Your next step: See the hidden paths in your environment

The most powerful way to understand the difference between reactive and predictive security is to see it applied to your unique environment.

Request a live predictive demo: Schedule a personalized session where our security architect will focus on identifying the five most critical hidden attack paths currently lurking in 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