algosec

Secure application connectivity.
Anywhere.




# Cutting the kill chain
## Shifting the advantage from the attacker to the architect

### A personal note

My name is Iris, and if you've spent any time in a modern SOC, you know the feeling of the defender's dilemma. We are currently living in an era where an adversary only needs to be right once - finding that one forgotten peering connection or overly permissive security group - while we, the architects, have to be right every single time, across every rack, VPC, and container. This paper is about changing that math. It's about moving away from chasing pings and toward a state where we own the map, and by extension, the outcome.

### 1. The asymmetry of modern defense

In the traditional security model, we built walls. We knew where the data lived, and we knew where the perimeter was. In 2026, the perimeter hasn't just moved; it has effectively dissolved. With the average enterprise managing over 200 cloud accounts alongside a robust on-premises core, the surface area for an attack is now effectively infinite.

Today's most pressing challenge isn't a lack of alerts - it's the alert deluge. Most SOC teams are trapped in a reactive cycle, chasing isolated telemetry. You see an unauthorized login in an Azure region; ten minutes later, you see a strange API call in AWS. Without a unified view, these are just noise. But in reality, they are often the first two steps of a hybrid kill chain designed to move laterally into your private data center.

Proactive defense is no longer a luxury for the highly regulated; it is the only way to shorten the dwell time of an adversary who is already operating within your environment.

### The pathway to hybrid security

1. **The hybrid manifesto:**
   Establishing the architectural truths of hybrid security. Coming soon;
2. **Cutting the kill chain:**
   Shifting from alerts to visual, cross-estate risk mapping.
3. **Attack path blueprint:**
   Tactical steps for remediating hybrid vulnerabilities.
4. **AI prompt playbook:**
   Putting natural language automation to work for your team.
5. **The trinity demo:**
   A live masterclass in unified execution.
6. **Migration mapping blueprint:**
   The final framework for secure application mobility.

## 2. Anatomy of the hybrid kill chain

Attackers don't think in silos. They don't care where your Cloud Team's responsibility ends and your Network Team's begins. They thrive in the seams - the messy transition points between cloud-native frontends and on-premises backends.

**The hybrid reality gap:** Imagine a scenario where a public-facing web server in a public cloud is compromised. The attacker exploits a lack of micro-segmentation to move laterally. They find a VPN or ExpressRoute connection that was opened for a temporary migration three months ago. From there, they traverse into your on-premises environment, reaching a legacy Oracle database containing your customer's PII.

If you can only see half the network, you cannot cut this chain. You might stop the compromised web server, but the ghost rule in the firewall still exists, and the path to your crown jewels remains open for the next exploit.

## 3. The solution: Predictive attack path analysis

To defend a hybrid estate, we must stop reacting and start simulating. This requires a shift to predictive attack path analysis.

Instead of waiting for an alert to trigger, we should be asking **"What If?"** every day.

- **What if one of my clouds is compromised? Can an attacker reach my environment?**
- **What if this user's IAM role is hijacked? Which databases do they have a path to?**

By identifying your crown jewels first and working backward, you can map every possible entrance. Manual path analysis in a hybrid environment is a mathematical impossibility - the permutations are too high. True proactive defense requires an automated engine that understands the specific syntax of every router, switch, and cloud security group in the path.

## 4. Unified defense with AlgoSec Horizon

This is where AlgoSec Horizon changes the game. It acts as the central intelligence layer - the Brain - that unifies your entire security estate into a single, cohesive fabric.

### On-premise mastery: Change management & FireFlow

Proactive defense begins with ensuring you don't make the problem worse. Horizon automates the risk-check process. Before a change is ever deployed to a physical firewall, Horizon simulates the impact. If a requested rule opens a high-risk attack path to a sensitive zone, the system flags it immediately. It moves change management from a manual ticket-approval process to a continuous, automated compliance engine.

### Cloud-Native Visibility: Horizon ACE (AlgoSec Cloud Enterprise)

You cannot defend what you cannot see. Horizon integrates deeply with cloud-native fabrics through the Horizon ACE engine. It pulls in security groups and NSGs to provide a non-siloed view. It treats a cloud security group with the same rigor as a hardware firewall, ensuring that your universal translator understands the intent of the policy, regardless of the vendor.

Beyond native cloud settings, ACE provides full-spectrum management for Cloud Firewalls (such as AWS Network Firewall or Azure Firewall) as well as virtual appliances from leading vendors. It treats these cloud-resident firewalls with the same rigor as on-premise hardware, ensuring your universal translator understands the intent of the policy regardless of the vendor. Whether you are managing a native cloud security group or a high-performance virtual firewall, ACE gives you a single, unified point of control.

### The lens: Application visualization (Horizon AppViz)

Technical IP-to-IP paths are useful for engineers, but they are meaningless to the business. Horizon AppViz translates these complex network maps into application-centric views.

## 5. Seeing the solution in action: Overcoming the seams

To truly understand how we cut the kill chain, we must address two of the main friction points in hybrid defense: communication silos and compliance exhaustion. We have paired this white paper with two critical demonstrations:

- **Video 8: The language barrier:** This video illustrates how the universal translator logic works in real-time. By bridging the gap between cloud-native JSON and legacy CLI, it ensures that a security policy meant to cut an attack path is accurately spoken to every device in the chain, leaving no room for manual translation errors that attackers love to exploit.
- **Video 2: The audit panic:** Proactive defense and compliance are two sides of the same coin. This demonstration shows how maintaining a clean, visualized kill-chain map allows you to move from panic to proof. When an auditor asks how you prevent lateral movement, you don't show them a spreadsheet; you show them a live, automated defense fabric.

## 6. Cutting the link: Practical remediation

Once we identify an attack path, the goal is intent-based blocking. Horizon doesn't just point out a vulnerability; it identifies the point of least resistance - the most effective place to break the chain.

**Technical example:** Horizon identifies a path from a cloud-native frontend to an on-premise DB. Instead of suggesting you fix the whole network, it identifies the specific rule in a legacy firewall or the specific Security Group in the cloud that facilitates the lateral move. It then provides the remediation steps to close that gap without breaking the application's legitimate traffic.

## Summary: Reclaiming the high ground

The audit panic is a symptom of a reactive architecture. By moving to a unified, proactive model with AlgoSec Horizon, you move toward a state of continuous compliance.

You cannot cut the kill chain if you can only see half the network. Unification is the only path forward. By bridging the gap between your on-premises core and your cloud-native future, you stop being a responder and start being an architect.

**Welcome to the Fabric.**

**Iris** AlgoSec

© AlgoSec Inc. All rights reserved. AlgoSec and the AlgoSec logo are registered trademarks of AlgoSec Inc.
All other trademarks used herein are the property of their respective owners.