algosec

Secure application connectivity.
Anywhere.



Partner solution brief
AlgoSec and AWS

aws PARTNER

As applications expand across AWS and on-premises environments, security policy becomes distributed across cloud-native controls, network firewalls, routing, and separate operating teams. AlgoSec connects AWS security context to application connectivity, risk, compliance, and governed change across the hybrid enterprise.

The problem

Organizations operating across hybrid environments must manage complex application connectivity across AWS and on-premises infrastructure. Without a unified view, risky access and internet exposure are difficult to identify and prioritize. Manual changes, compliance reviews, and incomplete dependency maps slow application delivery, complicate audits, and increase the risk of migration delays or outages.

The AWS and AlgoSec integrated solution

AWS provides scalable cloud infrastructure and native controls such as security groups, AWS Network Firewall, VPCs, and Transit Gateway. The Horizon ACE module from AlgoSec analyzes supported AWS networking, workload, and flow information.

The AlgoSec Horizon platform connects that cloud intelligence with application context and the broader network policy estate. Together, AWS and AlgoSec give cloud, network, security, and application teams one application-centric view to understand connectivity, prioritize exposure, and govern change.

Support safer AWS migration and modernization

Identify existing application dependencies before migration, understand the controls supporting each connection, and validate connectivity after workloads move. This reduces delayed cutovers, broken dependencies, and unnecessary access in the target environment.

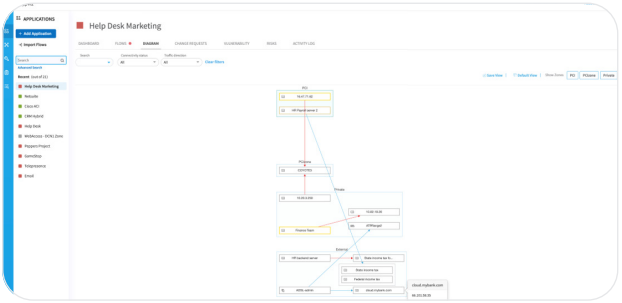
aws

Key value delivered

- **Visualize** application connectivity across supported AWS controls and hybrid networks.
- **Discover and map** applications, dependencies, workloads, and the policies supporting each flow.
- **Identify exposure** from overly permissive access, internet paths, risky policies, and misconfigurations.
- **Prioritize risk** using application context so teams focus remediation on the exposures that matter most.
- **Govern changes** with risk analysis, approvals, implementation guidance, validation, and an audit trail.
- **Maintain compliance** with continuous analysis, rule and connectivity recertification, and audit-ready evidence.
- **Accelerate delivery** by reducing manual investigation and coordination between application, cloud, network, and security teams.

Visualize application connectivity

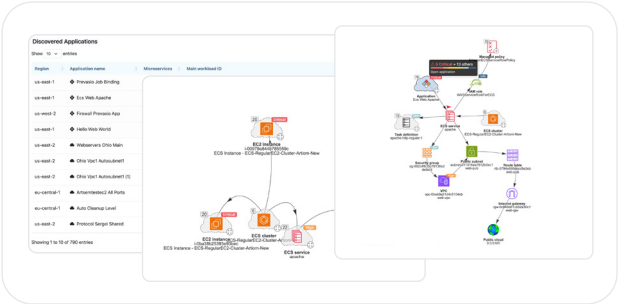
See how AWS VPCs, routes, security groups, cloud firewalls, and on-premises controls work together to permit or block an application flow. Trace the complete path, identify the devices and rules involved, and understand which policies support the connection.



Discover applications and connect them to AWS security controls

Discover cloud applications and dependencies from supported workload and flow data. Map applications to their workloads, connectivity, and supporting security controls so teams can review access in business context.

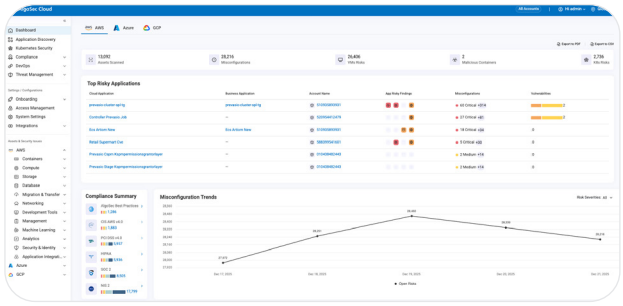
This application-centric view helps migration, cloud, network, and security teams understand why access exists before they change or remove a policy.



Identify, prioritize, and reduce risk

Find overly permissive policies, internet exposure, risky paths, and configuration gaps. Prioritize remediation using application context so teams focus on the exposures that matter most without disrupting critical services.

Use risk and application information together to decide which access should be tightened, recertified, or removed first.



Always be compliant

Continuously assess network and cloud security policy and maintain evidence for audits. Support recertification, change history, and reports for internal policies and common regulatory frameworks. Application context helps reviewers understand which business services are affected by each finding.

Govern secure changes

Analyze proposed access before implementation, route requests through approvals, and coordinate supported cloud and network changes. Validate the result after implementation and preserve the request, risk analysis, approvals, and change evidence in a complete audit trail.

available in aws marketplace

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 100 times faster by automating application connectivity and security policy across hybrid network environments. Trusted by over 2,300 organizations, AlgoSec brings two decades of expertise in securing complex hybrid networks. The AlgoSec Horizon platform uses advanced AI to automatically discover and identify business applications across multi-cloud environments, provide unified visibility into security and compliance issues, and remediate risks more effectively. With intelligent automation, AlgoSec streamlines security change processes, helping application, security, SecOps and cloud teams improve agility while maintaining security and compliance.

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.

AlgoSec.com