



Secure application connectivity.
Anywhere.



Part of the AlgoSec Horizon Platform.

Horizon ACE.

Cloud connectivity without compromise

Cloud growth should not create connectivity blind spots

Applications increasingly span public cloud, private cloud, containers, and on-premises networks. When teams lack a shared view of application dependencies, exposure, and policy changes, security work becomes slower, more manual, and harder to govern.

Horizon ACE brings cloud resources, connectivity, risk findings, and security policy changes into the AlgoSec Horizon Platform's shared application context. Security, network, and application teams can see how business services communicate, focus on risky exposure, and move changes forward with greater confidence.

START WITH THE APPLICATION

1

What is connected?

2

What is exposed?

3

What needs to change?

Connect technical findings to the applications they affect.

Map dependencies

Surface exposure

Prioritize change

Application-centric cloud network security across hybrid and multi-cloud environments

See application connectivity

Prioritize exposure

Accelerate secure changes

Stay audit-ready

Application-centric view of cloud resources, connectivity, and risk

Accounts VPCs / VNETs Virtual Machines Inventory Assets Security Controls													
Q Search Cloud Type Accounts Address Type Risk Triggers Severity Application Risky Findings Open Ports Clear all													
VM Name	VM ID	Cloud Type	Account Name	VPC/VNet Name	Status	Public Address	Private Address	Policy Directly Protecting	Network Risk Triggers	Application Graph	Application Risky Findings	Tags	
PaloAlto_Firew...		1	AWSsunflowerAcc...	DevOps	Not Running	10.176.1.252 +2		default +3	2 14	Application Graph	3	map-migrated.mig39358	+
Dev_demo_team			AWSsunflowerAcc...	DevOps	Not Running	10.176.57.233		DevOps_SG	4	Application Graph		map-migrated.mig39358	+
AZURE-AWS_S...			AWSsunflowerAcc...	Azure-AWS-vpc	Not Running	10.70.2.143		VM-Series Next-Gen Virtual I	1 1 4	Application Graph		map-migrated.mig39358	+
demo-logsec2-2			AWS Demo Account	APP-S-VPC	Not Running	10.1.10.205		APP-S-VPC-SG-2	1 1 4	Application Graph		map-migrated.mig39358	+
Palo-FW-VM			AWSsunflowerAcc...	RND_Department	Not Running	10.200.0.29		Palo Alto Networks VM-300	1 1 4	Application Graph		map-migrated.mig39358	+
Demo-PAN-Pan...			AWSsunflowerAcc...	DevOps	Not Running	18.190.128.140	10.176.1.69	PAN-MGT-SG	1 1 4	Application Graph		map-migrated.mig39358	+
PAN-2			AWSsunflowerAcc...	RND_Department	Not Running	10.200.0.33		Palo Alto Networks Panoran	1 1 4	Application Graph		map-migrated.mig39358	+
Panorama-Dev...			AWSsunflowerAcc...	RND_Department	Not Running	10.200.2.37		Palo Alto Networks Panoran	1 1 4	Application Graph		map-migrated.mig39358	+
AZURE-AWS_U...			AWSsunflowerAcc...	Azure-AWS-vpc_2	Not Running	10.9.1.139		launch-wizard-1	1 1 3	Application Graph		map-migrated.mig39358	+
demo-logsec2-1			AWS Demo Account	APP-S-VPC	Not Running	10.1.7.50		APP-S-VPC-SG-1	1 1 3	Application Graph		map-migrated.mig39358	+

1

Map cloud resources and dependencies to applications.

2

Identify connectivity and policy risks in application context.

3

Focus remediation and change decisions on the applications that matter.

Horizon ACE
Cloud network security

AlgoSec Horizon Platform
Shared application context across cloud and on-premises environments

Turn application connectivity insight into action

Horizon ACE helps teams understand what is connected, identify what is exposed, and determine which policy changes should be prioritized.



Core capabilities:

01. Application discovery and visualization

Discover cloud applications and resources, then map dependencies and connectivity flows to understand how business services communicate.

02. Hybrid connectivity visibility

Understand application connectivity across public cloud, private cloud, containers, and on-premises environments from a unified application view.

03. Segmentation and exposure analysis

Identify overly permissive access, segmentation gaps, and unintended connectivity that can increase application risk.

04. Cloud security policy management

Analyze and manage cloud-native security controls, including security groups and network access control lists, in application context.

05. Change visibility and troubleshooting

Maintain detailed visibility into supported policy changes to investigate issues, identify root causes, and support audits.

06. Compliance and audit readiness

Assess security policies against applicable regulatory and organizational requirements and simplify evidence collection.

What this means for your teams

Faster decisions

Connect cloud network findings to the applications affected so teams can focus on the most important exposure.

Less manual effort

Reduce time spent reconciling application dependencies, connectivity, and policy context across environments.

Stronger governance

Maintain change visibility and simplify evidence collection for troubleshooting, reviews, and audits.

Application connectivity across your hybrid environment



Trusted to help secure critical workloads

Across public cloud, private cloud, containers, and on-premises networks.

See Horizon ACE in action

Explore how Horizon ACE can help your organization map application connectivity, identify risky exposure, accelerate secure policy changes, and strengthen audit readiness. [Request a personalized demo](#)

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

The Horizon 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 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](https://www.algosec.com)