Secure application connectivity.
Anywhere.

AlgoSec Cloud
Cloud security configuration and policy management

AlgoSec Cloud provides application-based risk identification and security policy management across the hybrid multi-cloud estate.

As organizations adopt cloud strategies and migrate applications to take advantage of cloud economies of scale, they face increased complexity and risk. Security controls and network architectures from leading cloud vendors are distinct and do not provide unified central cloud management.

Cloud security main challenges

IT and Security staff find it difficult to create and maintain security in the cloud due to:

Complexity of multiple layers of security controls including:

- Cloud providers' built-in security controls, such as security groups and network ACLs, impacts security posture. There is a need to protect cloud assets such as virtual machines, DBaaS, and serverless functions. Misconfigurations can introduce security risks across various assets, including IaaS and PaaS.
- Cloud and traditional firewall providers also offer advanced network security products (such as Azure Firewall, Palo Alto VM-Series, Check Point CloudGuard).

Multiple public clouds from AWS, Azure and GCP. Security professionals are challenged by the need to understand their differences while managing them separately using multiple consoles and diverse tools.

Multiple stakeholders: Unlike on-premise networks, managing deployment is especially challenging in the cloud where changes to configurations and security rules are often made by application developers, DevOps, and cloud teams.

What makes AlgoSec Cloud different?

- Minimize the attack surface by identifying network risks and the underlying applications affected by these risks
- Unified view of the hybrid multi-cloud estate from a single console
- Manage multiple layers of cloud security controls and proactively detect misconfigurations
- Identify unused security rules and have the confidence to remove them
- Adaptive guardrail risk policy

Key business benefits

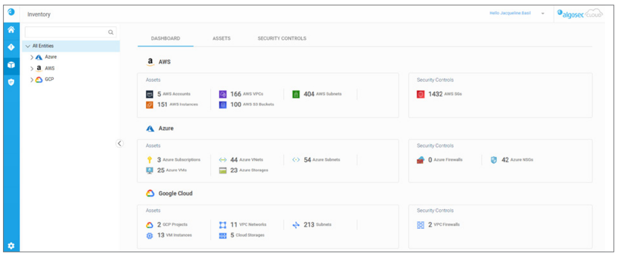
- Enhance visibility across the hybrid multi-cloud estate with central management
- Prioritize risks according to business applications and severity
- Reduce manual labor, errors, and their associated risks and costs
- Cleanup unused network security rules to reduce attack vector and better utilize resources

Manage the multi-cloud security environment

AlgoSec Cloud is an agentless SaaS solution and is easy to on-board in minutes. It offers immediate ROI and significant improvements to help you solve the hybrid multi-cloud application risk identification and security challenges. AlgoSec Cloud enables effective security management of the various security control layers across the hybrid multi-cloud estate.

AlgoSec Cloud offers instant visibility, risk assessment, and central policy management, enabling a unified and secure security control posture, proactively detecting misconfigurations.

Continuous visibility. AlgoSec Cloud provides holistic visibility for cloud accounts assets and security controls.



AWS

Assets: 5 AWS Accounts; 151 AWS Instances; 166 AWS VPCs; 100 AWS S3 Buckets; 404 AWS Subnets

Security Controls: 1432 AWS SGs

Azure

Assets: 3 Azure Subscriptions; 25 Azure VMs; 44 Azure VNets; 23 Azure Storages; 54 Azure Subnets

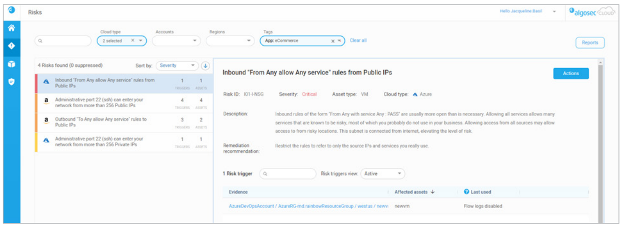
Security Controls: 0 Azure Firewalls; 42 Azure NSGs

Google Cloud

Assets: 2 GCP Projects; 13 VM Instances; 11 VPC Networks; 5 Cloud Storages; 213 Subnets

Security Controls: 2 VPC Firewalls

Risk management. Proactively detect misconfigurations to protect cloud assets. Identify risky rules as well as their last usage date and confidently remove them. Tighten overall network security by mapping network risks to applications affected by these risks.



Cloud type: 2 selected

Tags: App: eCommerce

Sort by: Severity

4 Risks found (0 suppressed)

Risk	Triggers	Assets
Inbound "From Any allow Any service" rules from Public IPs	1	1
Administrative port 22 (ssh) can enter your network from more than 256 Public IPs	4	4
Outbound "To Any allow Any service" rules to Public IPs	3	2
Administrative port 22 (ssh) can enter your network from more than 256 Private IPs	1	1

Inbound "From Any allow Any service" rules from Public IPs

Risk ID: I01-I-NSG Severity: Critical Asset type: VM Cloud type: Azure

Description: Inbound rules of the form "From Any with service Any : PASS" are usually more open than is necessary. Allowing all services allows many services that are known to be risky, most of which you probably do not use in your business. Allowing access from all sources may allow access to from risky locations. This subnet is connected from internet, elevating the level of risk.

Remediation recommendation: Restrict the rules to refer to only the source IPs and services you really use.

1 Risk trigger Risk triggers view: Active

Evidence	Affected assets	Last used
AzureDevOpsAccount / AzureRG-rnd.rainbowResourceGroup / westus / newv	newvm	Flow logs disabled

Central management of security policies. Manage network security controls, such as security groups and Azure Firewalls, in one system across multiple clouds, accounts, regions and VPC/VNETs. Manage similar security controls in a single security policy so you can save time and prevent misconfigurations.

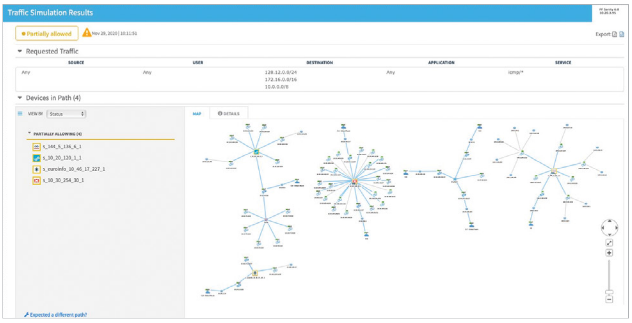
Policy cleanup. As cloud security groups are constantly adjusted, they can rapidly bloat. This makes it difficult to maintain, increasing potential risk. With AlgoSec Cloud's advanced rule cleanup capabilities, you can easily identify unused rules and remove them with confidence.

Put guardrails in place to protect your cloud network security

Speed up application delivery without compromising security. AlgoSec's infrastructure as code (IaC) connectivity risk analysis helps DevOps teams accelerate application delivery and optimize security. Developers can proactively check for vulnerabilities using this powerful capability before pushing code to a repository.

Check connectivity for the hybrid network

For Azure NSG policies, the connectivity check in AlgoSec Cloud allows you to observe how traffic is routed and whether it's allowed across your entire hybrid network (that is, across NSGs, firewalls routers etc. deployed on cloud and/or on-prem).



Partially allowed Nov 29, 2020 | 10:11:51

Requested Traffic

SOURCE	USER	DESTINATION	APPLICATION	SERVICE
Any	Any	128.12.0.0/24 172.16.0.0/16 10.0.0.0/8	Any	icmp/*

Devices in Path (4)

VIEW BY Status

PARTIALLY ALLOWING (4)

- s_144_5_136_6_1
- s_10_20_120_1_1
- s_euroinfo_10_46_17_227_1
- s_10_30_254_30_1

Active change

Process security changes in a fraction of the time by automating the security policy change process. Create custom workflows to change policies on supported Firewall and add or remove SG and NSG rules in AWS and Azure cloud environments.

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.com