algosec

Secure application connectivity.
Anywhere.

The AlgoSec technology partner ecosystem

The AlgoSec platform automates the application connectivity and security policy for your entire hybrid network, which includes public cloud, private cloud, and on-premises networks. By using AlgoSec, users can easily monitor and manage network security devices such as firewalls, load balancers, and routers to ensure compliance and reduce risk. The platform intelligently automates the change management process for these devices and provides deep, dynamic, and immediate insight and remediation options to improve security and ensure continuous compliance.

Additionally, AlgoSec can leverage traditional Netflow to fully characterize and dynamically understand your critical application relationships and tiers. AlgoSec can provide details on all the policies that currently exist for those applications and provide insight into how to reshape those policies to be precise to what the applications truly need to function.

Network and security devices

JUNIPER NETWORKS | zscaler | paloalto NETWORKS

FORTINET | CISCO Meraki | f5

CISCO Partner | CHECK POINT | VERSA NETWORKS

Cloud and SDN

Google Cloud | CISCO Partner ACI

Azure | aws | vmware

AlgoSec seamlessly integrates with your current orchestration systems, ITSM systems, SIEM/SOAR, vulnerability scanners, and more, making it a comprehensive and centralized solution for your network security needs. Additionally, AlgoSec provides an extensive list of APIs for risk and security compliance, change management, and DevOps for creating new applications and connectivity. Various actions that can be executed through our GUI can also be realized by leveraging our APIs.

IT Service Management systems (ITSM)

Intelligently automate change requests within your existing tools and processes. This enables you to seamlessly integrate AlgoSec's functionality with your current ITSM system and leverage its benefits without disrupting your established workflows.

servicenow | hp | bmc REMEDY

Micro-segmentation tools

Use existing micro-segmentation tools to build your application library and firewall rules by importing application connectivity from existing tool, turning thin flows to comprehensive flows and implement them as firewall/SDN network security policies.

Vulnerability scanners

Clearly see all host/server vulnerabilities and tie them to your critical application policies. Quickly identify which host/servers have security risks that need to be remediated. Reduce the risk for your critical business applications by making vulnerability information available as part of your network security risk assessment.

SIEM/SOAR

Tie incident response to business processes, automate and prioritize remediation within your existing SIEM/SOAR solutions. This integration saves valuable time in investigating and isolating an attack, enabling faster and more effective incident response.

DevOps

Integrate network security into your CI/CD pipeline to enable the DevOps team to securely make app connectivity change requests and implementation using their native tools. Drive efficient communication between the DevOps team and the network security team, for fast and effective resolution of security issues.

Chat solutions

Chatbots can be integrated with AlgoSec to verify application connectivity, initiate change requests, review application details, and many more options. This saves your team a tremendous amount of time from having to create change requests to verify the details that can be presented in seconds.

AlgoSec.com