AlgoSec Network Security FAQs

What is AlgoSec?

AlgoSec is a network security management solution that provides organizations with a comprehensive and centralized platform to manage their network security policies, optimize firewall rules, and automate security workflows. It helps businesses gain visibility and control over their network infrastructure, ensuring security and compliance.

What are AlgoSec's key features?

AlgoSec offers several key features to enhance network security management. These include:

- Firewall Policy Management: AlgoSec allows organizations to efficiently manage firewall policies across heterogeneous networks, simplifying rule management, optimizing configurations, and ensuring policy compliance.
- Application Connectivity Management: AlgoSec provides visibility into application connectivity requirements and automates the process of configuring and deploying necessary network security changes, ensuring uninterrupted application availability.
- Risk and Compliance Management: AlgoSec helps businesses identify and mitigate risks by continuously monitoring network security policies, providing compliance reports, and automating compliance workflows.
- Change Automation and Orchestration: AlgoSec automates security change management processes, enabling organizations to implement changes quickly and accurately while reducing the risk of misconfigurations.
- Security Policy Optimization: AlgoSec analyzes firewall policies to identify redundant, unused, or risky rules, allowing organizations to optimize their security policies for better performance and reduced attack surface.

Which network infrastructure vendors does AlgoSec support?

AlgoSec supports a wide range of network infrastructure vendors, including but not limited to:

- Firewall and Security Devices: AlgoSec integrates with leading firewall vendors such as Cisco, Check Point, Palo Alto Networks, Fortinet, Juniper Networks, and many others, providing centralized management capabilities.
- Cloud Platforms: AlgoSec supports cloud platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), enabling organizations to manage their network security policies in both on-premises and cloud environments.
- Network Devices: AlgoSec integrates with various network devices, switches, routers, and load balancers from vendors like Cisco, Juniper Networks, F5 Networks, and others, facilitating comprehensive **network security management**.

How does AlgoSec help with compliance management?

AlgoSec assists organizations in compliance management by automating the auditing and reporting processes, ensuring network security policies align with regulatory and industry standards.

It provides predefined compliance frameworks such as PCI DSS, HIPAA, NIST, and GDPR, along with continuous monitoring and reporting capabilities. AlgoSec's Compliance and Risk Analyzer helps identify compliance gaps and recommends necessary actions to maintain a compliant security posture.

Can AlgoSec automate security policy workflows?

Yes, AlgoSec offers robust automation capabilities for security policy changes. It enables organizations to define predefined workflows and approval processes for security policy modifications.

AlgoSec's automated security policy change workflows help organizations respond to emerging threats and vulnerabilities, improving their cybersecurity posture against hackers leveraging the latest malware.

Our Change Manager application automates the change implementation process, ensuring that security policy changes are accurate, auditable, and compliant. This helps reduce the manual effort involved in change management, accelerates the change implementation time, and minimizes the risk of misconfigurations.

What are the requirements for using AlgoSec?

The **AlgoSec Security Management Suite** (ASMS) requires the following hardware and software configurations to run properly:

1: Hardware deployment devices must meet or exceed the following:

- 4-core CPU
- 16 GB of memory
- 300 GB of storage

2: Additional hardware requirements depend on the environment configuration and type. Here are some of the requirements associated with popular environments:

- **NAS Storage.** If you store reports on a remote NAS server, you will need to configure your ASMS deployment to use the **appropriate protocol for NAS connections.**
- **HA/DR Clusters.** Every node in a HA/DR cluster should be identical. That means every AlgoSec deployment instance should either be through hardware or through a VM appliance, with the same amount of disk space on every node.
- **Distributed Architecture.** Distributed architecture environments may include additional requirements from the central manager, geographically distributed remote agents, and load-distributing slave assets. Remote agents and slave assets do not store reports.

- **AWS Deployments.** Ensure your AWS environment is compatible with CentOS6. Machines from the Amazon EC2 General Purpose M4 family are recommended. Make sure your AWS instance uses high performance storage – solid-state drive disks are recommended.

3: Software requirements are only necessary on virtual appliances. AlgoSec hardware appliances come pre-installed with all necessary software. Virtual machines must use VMWare ESC Version 5.5 or higher.

What is the deployment process for AlgoSec?

A typical full ASMS deployment with out-of-the-box functionality involves the following steps:

- **Getting ready**. Work with AlgoSec to identify your environment's needs and provision the appropriate components.
- **Deploy infrastructure.** Deploy standalone or cloud-based appliances, set up your environment with high-availability and disaster recovery clusters. Configure and manage clusters for secure operation.
- **Deploy AlgoSec Firewall Analyzer.** License, authenticate, and configure the application. Define user roles and integrate mail, storage, and infrastructure components.
- **Deploy AlgoSecFlow.** Complete initial setup using fully configurable FireFlow templates and workflows. Create a sample change request and push it through the workflow to test each step.
- **Build ASMS Network Topology.** Verify network maps, run end-to-end traffic simulation queries, and adjust data visualization templates.
- **Deploy AlgoSecAppViz.** Complete initial setup. Define users, permissions, and roles. Identify security zones and manage vulnerability assessment scanners. Install AutoDiscovery so AppViz can automatically detect flows and applications.

What is the pricing model for AlgoSec?

Every organization is unique. We can't provide a one-size-fits-all pricing model for simplifying complex policy changes across such a varied landscape of information security policies and requirements.

AlgoSec's extensive and highly customizable information security policy management solutions are priced according to multiple factors. We take the organization's network environment into consideration, as well as the volume of confidential information protected by its security policies.

Although we can't offer complete pricing information on our Frequently Asked Questions page, we are happy to help your organization calculate the ROI it stands to gain from leveraging our IT security platform. Please refer to our **ROI calculator** to find out how much you can save with AlgoSec.

How is AlgoSec different from Tufin and FireMon?

AlgoSec is a comprehensive security policy management platform with capabilities that Tufin and FireMon do not have (or only partially implement). This makes it better-suited to meeting strict security compliance needs and reliably protecting organizations against cyber attacks, malicious software, and ransomware.

1. AlgoSec integrates fully with SIEM systems and allows for unified, consolidated management of different cloud security groups. It supports risk analysis for Infrastructure-as-Code deployments for DevSecOps as well.

2. Compared to **Tufin**, AlgoSec:

- Comprehensively discovers applications and services automatically.
- Connects applications to security policy rules.
- Automates policy change management workflows without additional add-ons.

3. Compared to **FireMon**, AlgoSec:

- Fully supports vulnerability management on the business application level
- Automatically associates firewall rules to relevant business applications
- Supports custom policy rule documentation

What is a firewall analyzer?

AlgoSec's Firewall Analyzer enables you to visualize your entire computer network and its topology from a single point of view. This lets you see where security threats may come from, and gives the opportunity to distribute resources more efficiently between firewall assets.

Firewall Analyzer users can run simulated "what-if" queries to find out how cybercriminals may interact with anti-virus solutions on endpoint mobile devices or known vulnerabilities in operating systems. You can use it to see how data breaches and denial of service attacks may impact your organization.

This gives you the opportunity to run highly targeted penetration testing initiatives. You can then update your data security policies in response to the insights you gain.

How does AlgoSec help with firewall management?

AlgoSec automates the process of managing firewall policies and rules in response to emerging cyber threats. This allows organizations to protect sensitive data and block unauthorized access without relying on painstaking manual processes.

Firewall management is a vital part of every organization's security posture. AlgoSec helps organizations develop and maintain valuable policies from a single dashboard.

It generates notifications when firewall policies need updating to include new threat signatures, and automates the process of introducing those new signatures into the organization's firewall policies.

This allows organizations to respond to rapidly-developing threats quickly. Organizations can protect themselves against phishing attacks, spyware, trojans, and computer viruses more effectively when their firewalls are consistently configured.

What is network security policy management?

Network security policy management is the process of optimizing the security rules information systems follow when handling network traffic.

This may include protections against using company devices for unauthorized purposes – like accessing social media – as well as strict rules for protecting personal data and fighting cybercrime. Network security policies are highly dependent on the solutions and technologies that make up the organization's tech stack.

Strong passwords, multi-factor authentication, and SSL certification are examples of elements common to many policies. However, these policies must also include specific rules for handling complex technologies like firewalls, intrusion detection solutions, and intrusion prevention systems.

Manually managing network security policies is a **time-consuming, error-prone process.** Many organizations deploy automated platforms to address these problems and provide better outcomes to security event mitigation processes.

How does AlgoSec help with network security management?

AlgoSec automates many of the processes that go into network security management. This allows security teams to address emerging threats more effectively while reducing the overall cost of managing complex network security deployments.

AlgoSec's automated network security management platform updates many different aspects of your organization's security policy framework. This ensures your organization's anti-virus software knows what to look for, while giving security personnel the ability to establish robust firewall rules, VPN policies, and endpoint security rules for employee smartphones.

Automated network security management helps trigger alerts when IP addresses associated with malicious servers attempt to connect with your assets, or when cybercriminals send malicious HTML links to your employees.

How does Algosec help with network segmentation?

Proper **network segmentation** helps protect organizations from costly cyberattacks. AlgoSec enables security teams to proactively identify segmentation opportunities that can improve the organization's overall security posture.

This may include suggestions to group certain types of devices together based on the security policies and rules they follow. It may also include heightened protections for network segments

that deal with sensitive personal data or credit card information. AlgoSec automates the process of identifying these opportunities and putting them into practice.

Can AlgoSec help with compliance management?

AlgoSec automatically identifies compliance gaps so that security teams can remediate them proactively instead of waiting for the next audit.

Preparing firewalls for audits is difficult and time-consuming. Most regulations require organizations to demonstrate continuous compliance by undertaking audits regularly. This puts a great deal of strain on organizations with thousands of rules and access control lists that must be updated with the latest changes before the next audit.

With AlgoSec, you can generate audit-ready reports for all major regulations, including SOX, HIPAA, NERC, and PCI. You can generate custom reports for internal compliance initiatives and create a comprehensive audit trail of firewall changes as well.

How does AlgoSec automate security policy management?

AlgoSec provides an end-to-end security policy management framework that integrates with multiple solutions throughout the network. It grants visibility into business applications and security policies, proactively identifies application dependencies, and accelerates policy changes with a zero-touch interface.

Organizations rely on AlgoSec to avoid costly misconfigurations and gain deep visibility into connectivity and security policy changes. AlgoSec's automated security policy management platform allows security teams to manage technical debt and address shadow IT risks more effectively than with manual, error-prone processes.

How does AlgoSec integrate with other security tools?

AlgoSec integrates with a broad variety of external security tools. It fully supports SIEM integration, allowing analysts to include extensive log data on firewall policies and configurations into their investigations. AlgoSec allows SIEM users to manage security policies and augment them with business context directly through the SIEM interface.

Some examples of external security tools that AlgoSec integrates with include **Splunk and IBM QRadar**.

You can also integrate AlgoSec FireFlow directly into third-party security tools using a **CMS web service**.

How does AlgoSec help with risk assessment and analysis?

AlgoSec allows security professionals to preview the effects of security policy changes before enacting them. This allows organizations to carefully assess the risks associated with new policy changes and identify rules that require remediation.

AlgoSec can also generate audit-ready reports designed to meet the requirements of major **compliance regulations**. This allows organizations to quickly assess policy changes for compliance violations before implementing new policies.

Security professionals can also use AlgoSec to discover risky traffic flows, providing early warning of potential risks. The platform can then update the appropriate firewall rules and security policies to address and remediate the risk associated with those flows.

Can AlgoSec be used to manage cloud security policies?

AlgoSec provides organizations with an industry-leading platform for managing cloud security policies effectively. Security teams can gain in-depth visibility into their cloud security posture and automatically manage connectivity between cloud-hosted infrastructure, virtual and hardware firewalls, and software-defined network assets.

With centralized management and comprehensive solutions for detecting and mitigating risk, AlgoSec enables automated cloud security policy management for organizations of all sizes.

How does AlgoSec ensure the security of its own platform?

All customer data stored or processed by AlgoSec enjoys state-of-the-art security in compliance with multiple regulatory frameworks.

AlgoSec is ISO/IEC 27001:2013 and ISO/IEC 27017:2015 certified, and operates rigorous ongoing technical security controls to maintain the confidentiality, integrity, and availability of customer data.

AlgoSec uses stateless services to isolate its software-as-a-service (SaaS) products. This protects against data leaks and ensures data remains isolated between tenants. When at rest, data is isolated in separate databases for each customer, secured with unique access credentials that are not directly available to users.

Does AlgoSec support multi-vendor environments?

Yes, AlgoSec supports multi-vendor environments, allowing organizations with complex infrastructure to manage security policies without trapping individual components in their own silos. AlgoSec unifies and consolidates multi-vendor environments so that security teams have a single point of reference for addressing security policy changes.

This allows organizations with multi-vendor environments to get a full and comprehensive picture of their network applications and traffic flows. It grants security teams full visibility into the **hybrid network estate**, allowing for better, more accurate risk assessment and policy management.

How does AlgoSec help with change management?

AlgoSec improves the accuracy of policy changes while reducing the amount of time and effort that goes into network policy **change management**. This helps organizations maintain regulatory compliance while proactively addressing vulnerabilities and blind spots in their overall security posture.

By automating the most time-consuming and error-prone parts of the change management process, AlgoSec enables organizations to reduce the risk associated with complex policy changes while automating the most complicated steps in that process.

What are the reporting and analytics capabilities of AlgoSec?

The AlgoSec Reporting Tool (ART) includes multiple templates and data visualization capabilities designed to help decision-makers understand their security posture. It includes a variety of ready-made compliance templates designed to address the needs of common regulatory frameworks, like HIPAA, SOX, and more.

AlgoSec also supports custom dashboards and data visualization tools so that security leaders can communicate their findings more fluently with non-technical executives and leaders. Users can explore data visualizations and create brand-new analytics queries directly through the ART interface.

Can AlgoSec be used for continuous compliance monitoring?

Yes, AlgoSec supports continuous compliance monitoring. As organizations adapt their security policies to meet emerging threats and address new vulnerabilities, they must constantly verify these changes against the compliance frameworks they subscribe to.

AlgoSec can generate risk assessment reports and conduct internal audits on-demand, allowing compliance officers to monitor compliance performance in real-time.

Security professionals can also use AlgoSec to preview and simulate proposed changes to the organization's security policies. This gives compliance officers a valuable degree of lead-time before planned changes impact regulatory guidelines and allows for continuous real-time monitoring.