

INCREASING CISCO ACI ADOPTION WITH ALGOSEC

Better together: Cisco ACI and AlgoSec

Cisco ACI, an industry-leading software-defined networking solution, facilitates application agility and data center automation. ACI enables scalable multi-cloud networks with a consistent policy model and provides the flexibility to move applications seamlessly to any location or any cloud while maintaining security and high availability. But, using Cisco ACI alone, has limits.

AlgoSec Security Management for Cisco ACI delivers application-centric security policy change management, providing unified visibility across the entire network estate. It leverages policy-driven automation to manage security changes, assess risk, and maintain compliance.

Integrating AlgoSec with Cisco ACI, extends the capabilities of Cisco ACI, accelerating adoption and retention of ACI, by providing complete network security management for the entire multi-vendor and multi-cloud network.

Enterprise-wide ACI visibility

With Cisco ACI alone, users only have visibility within the Cisco ACI fabric. However, by integrating with AlgoSec, gain full visibility across your multi-vendor hybrid network, including your on-premises and multi-cloud network estate like firewalls and other security control.

With AlgoSec, users can search across multi-site Cisco ACI estates for tenants, endpoints, contracts, EPGs, and more. Visibility also extends beyond Cisco ACI, including items outside the ACI fabric so you can get visibility over your entire network estate. This provides a unified view of multiple environments including cloud, SDN, and on-premise deployments. Gain quick access to key findings via the AlgoSec App for the Cisco ACI App Center.

As a result of full visibility over the traffic flows across your entire network, troubleshooting is simplified. With traffic simulation queries, you can easily see what breaks, so you know exactly what needs to be fixed. Once the ACI fabric is in production, AlgoSec can even help troubleshoot applications and connectivity issues for connections that enter, exit, and traverse the fabric itself.



Why integrate AlgoSec with Cisco ACI?

-  Automate for scale – Extend ACI’s policy-based automation to all security devices across the enterprise, including multi-cloud and on-premises environments.
-  Reduce the attack surface – Enhance visibility into the security posture of the ACI fabric and across multiple on-premises, multi-cloud, and multi-vendor instances
-  Security and compliance – Get risk and compliance analysis for Cisco ACI contracts alongside firewall security policies
-  Application-centric security management – Map application connectivity to ACI contracts and EPGs, as well as in-fabric firewall policies
-  Troubleshoot data center connectivity challenges using advanced network traffic simulation

Application-centric connectivity mapping

AlgoSec natively provides visibility into Cisco ACI network topology, while tying the ACI fabric into the rest of the data center. This provides a complete network topology map for your entire hybrid network.

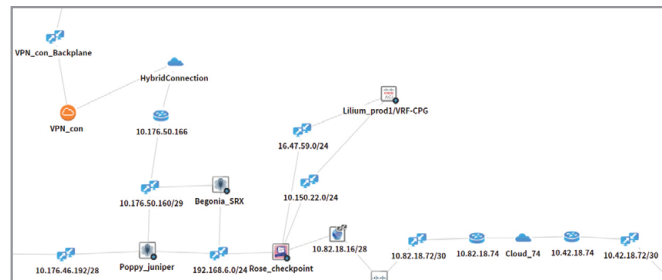
In addition, you can connect your network to the applications and their associated traffic flows. With Cisco ACI alone, applications are not connected to items outside of the ACI fabric or associated with all of the business applications on devices.

By integrating Cisco ACI with the AlgoSec Security Management Solution, your organization is also able to connect network and business applications for items within and also outside of the ACI fabric. As a result, you can map application connectivity to ACI contracts and EPGs, as well as in-fabric firewall policies.

Risk management

Integrating the AlgoSec Security Management Solution with Cisco ACI enables to manage risk both within Cisco ACI and over your entire network, including identifying already existing risky security policies and flagging risk when creating new policies.

AlgoSec helps identify risky rules for your entire network. In order to minimize outages, AlgoSec users can assess the impact of network changes on application availability. Risk and vulnerabilities can also be identified from the business application perspective. Potential changes can be recommended to the application policies in the ACI fabric. As a result, your application, security, and network teams are aligned.



Proactive regulatory compliance

By integrating Cisco ACI with AlgoSec, you can gain a complete picture of both items within the ACI fabric to meet compliance requirements, as well as items outside the fabric.

AlgoSec generates automatic audit-ready compliance reports on each Cisco ACI tenant for major regulations, flags issues upon changes, uncovers gaps, and even remediates problems throughout your entire network, ensuring a state of continuous compliance and even provides insights into your entire network's compliance state.

Intelligent automation

Cisco ACI provides automation for workflows and policies within the ACI fabric. But by integrating with AlgoSec, you can automate both inside and outside of the ACI fabric, including service graphs that control firewalls within the fabric.

AlgoSec's intelligent automation workflow enables automated deployment of contracts, EPGs, and filters on Cisco ACI. This allows clients to use a single process to deploy security policy across not only the Cisco ACI fabric, but rather across the entire hybrid, multi-vendor data center.