

Cisco Hybrid Mesh Firewall Suite with Cisco ACI and Cisco Secure Workload



What if you could implement consistent policies across your hybrid enterprise, including Cisco ACI fabrics, making it easy for your organization to reduce your attack surface, prevent compromise, and stop the lateral movement?

The tangible benefits of integration

This next-generation integration offers significant advantages for organizations leveraging Cisco ACI, providing a smarter, streamlined approach to network security.

- **Deep application visibility:** Understand application behavior and dependencies inside your ACI environment, and simplify the creation of segmentation policies.
- **Automated policy lifecycle management:** Enable AI-driven discovery and automation, thereby eliminating manual processes, saving time, and reducing errors.
- **Agentless enforcement:** Enforce micro- and macro-segmentation policies seamlessly without requiring intrusive agent deployments.
- **Enhanced ACI fabric health monitoring:** Gain actionable insights into ACI fabric resources, including the health of switch memory (Ternary Content Addressable Memory [TCAM]).
- **Leverage existing investments:** Extend the value of your current ACI infrastructure while tapping into Cisco's broader Hybrid Mesh Firewall ecosystem.

A comprehensive solution for smarter security

The integration of Cisco® Application Centric Infrastructure (Cisco ACI) with Cisco Secure Workload as part of Cisco's Hybrid Mesh Firewall fabric is transforming how organizations secure their data centers. This powerful integration leverages AI-driven insights, automation, and agentless enforcement to streamline security operations while protecting application environments.

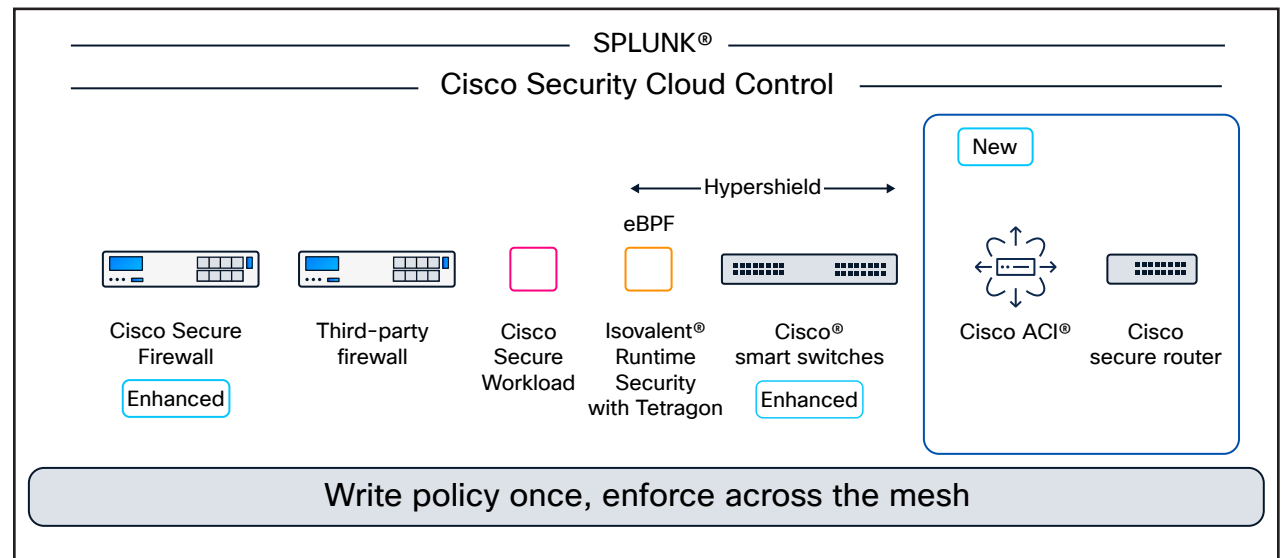


Figure 1. Cisco Hybrid Mesh Firewall Suite: better together with Cisco ACI and Cisco Secure Workload

Addressing today's challenges in data-center networking environments

Managing security in application-centric environments is no easy task. Many organizations find it challenging to transition from network-centric segmentation to application-centric approaches without disruption. Traditional tools often require deploying multiple agents, increasing complexity and slowing down operations. Manually managing segmentation policies further drains resources and leaves gaps in security.

These challenges compromise visibility into application behavior, delay policy implementation, and allow potential vulnerabilities to persist in critical business environments.

How it works

Key features of the integration

- **Agent-based visibility:** AI-driven visibility into application behavior and dependencies through agent-based approaches is coupled with agentless policy enforcement.
- **Agentless visibility (coming soon):** Upcoming enhancements will eliminate the need for agents altogether, further simplifying deployment and reducing operational overhead.
- **Seamless integration:** Cisco Secure Workload integrates directly with ACI's application policy infrastructure controller (APIC) through an ACI connector, enabling effortless policy discovery, validation, and enforcement within the ACI fabric.
- **Part of Cisco's Hybrid Mesh Firewall fabric:** Cisco Secure Workload is a critical component of Hybrid Mesh Firewall, extending its advanced security capabilities into the ACI architecture with centralized monitoring through Cisco Security Cloud Control.

Use cases where integration shines

Table 1 shows how customers can harness the power of Cisco Secure Workload and ACI integration for real-world challenges.

Table 1. Use cases

Use case	Description
Visibility	Allows a detailed understanding of application dependencies and insights into ACI fabric resource status.
Agentless policy enforcement	Allows customers to apply microsegmentation controls across the ACI environment without deploying agents.
Policy automation	Automates the discovery, validation, and management of segmentation policies to accelerate security.

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)

Customer outcomes achieved

By adopting this integration, customers can reduce their attack surface, automate policy management, and increase operational efficiency without compromising business continuity.

They can migrate to an application-centric model effortlessly.

And they can protect critical resources with confidence through validated, AI-generated policies.

Learn more

Whether you're an existing Cisco ACI or Cisco Secure Workload user, or are just beginning your digital transformation, this scalable suite is designed to meet your needs in securing hybrid environments.

Learn more about [Cisco ACI](#) and [Hybrid Mesh Firewall](#). Visit [Cisco Cloud Protection Suite](#) to learn more and start securing your ACI environment today.

