Hybrid Mesh Firewall

https://cs.co/1page

A **Cisco Hybrid Mesh Firewall** is a distributed security fabric with centralized cloud management, designed to address challenges of securing modern, distributed applications and networks. This hybrid solution goes beyond traditional firewalls to provide intelligence and security across hybrid environments.

Benefits:

Simplify security management: Access and manage all your enforcement capabilities across your hybrid environment and gain AI-driven insights from one centralized interface.

Protect against modern threats: Safeguard environments at key boundaries while protecting against zero-days and threats hidden within encrypted traffic.

Stop unauthorized lateral movement: Reduce attack surface and contain the blast radius with coarse and fine-grained segmentation for both traditional and Kubernetes workloads.

Secure your AI transformation: Detect and defend against dynamic threats introduced through the development and deployment of AI applications.

Close the exploit gap: Protect against exploits in minutes with an AI-native rule engine that prioritizes vulnerabilities and automatically recommends a surgical mitigating control.

Use Cases:

1 **Distributed Security Enforcement:** Push security controls closer to where applications, users, and devices reside. This includes securing data centers, cloud environments, campuses, and IoT devices.

2 **Unified Management:** Centralized management through Cisco Security Cloud Control, an AI-native management system. This allows for management and configuration of all aspects of network security from a single interface.

3 4 **Zero Trust Segmentation and Application Protection:** Implementing zero trust principles to segment networks and protect applications by validating every flow between applications to prevent unauthorized lateral movement.

3 4 **SD-WAN:** Simplified onboarding and config using Zero Touch Provisioning and Device templates using centralized mgmt. Intelligent path selection across multiple paths using Direct Internet Access (DIA) and path monitoring along with simplified wizard that automates hub and branch communication.

5 **Integration with Network Fabric:** Cisco's approach involves fusing security into the network fabric with Hypershield, Secure Workload, and Multicloud Defense.

2 6 7 **AI-Native Capabilities:** Cisco integrates AI into its Hybrid Mesh Firewall solution to enhance security, productivity, and scalability. This includes AI-driven threat intelligence, autonomous segmentation, and AI assistance.

8 **Multi-Vendor Policy Enforcement:** Cisco's Mesh Policy Engine allows organizations to define a single intent-based policy that can be enforced across both Cisco and third-party firewalls to simplify policy management.

1	All Security Products
2	Security Cloud Control
3	Cisco Secure Access
4	Cisco Secure Firewall
5	Hypershield
6	AI Defense
7	Firewall Management
8	Mesh Policy Agent

Key Cisco Components:

Cisco Secure Firewall: Find malicious flows in encrypted traffic and intelligently decrypt without sacrificing performance with Cisco Encrypted Visibility Engine (EVE). Stop zero-days leveraging Snort ML and Talos Threat Intelligence.

Cisco Secure Workload: Gain visibility and security for applications across hybrid environments with or without agents. Auto-discover, validate, and enforce the right policies at the right enforcement points.

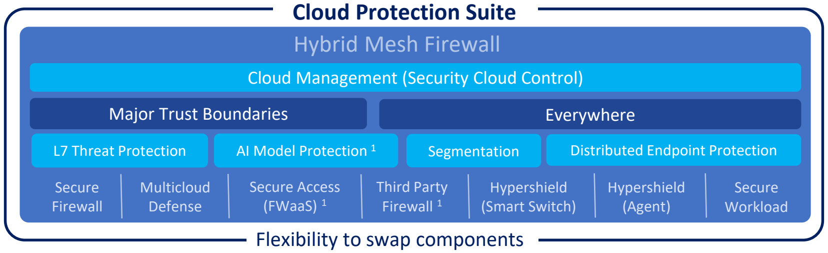
Cisco Multicloud Defense: Extend Layer-7 firewalling capabilities to the cloud, natively. Leverage cloud-agnostic automation and orchestration for deployment, scaling, and auto-healing of enforcement points.

Isovalent Enterprise for Cilium: Cloud-native forensics, compliance monitoring, and threat detection by harnessing eBPF, because Isovalent Enterprise for Cilium integrates network and run-time behavior with Kubernetes identity.

Cisco AI Defense: Build safeguards for the development and usage of AI applications so you can advance your AI initiatives with confidence.

Cisco Hypershield: Close exploit gaps, segment everywhere, and self-qualify updates and changes with security architecture designed to defend modern, AI-scale data centers.

Security Cloud Control: Centrally manage all enforcement points across the security fabric.



[1] AI Defense & Secure Access are add-ons to Cloud Protection Suite

Resources:

Sales Resources
At-a-Glance
Fact Sheet
Sales FAQ
Cloud Protection Suite
Blogs
E-Book
Public Page

Example SKU: *n/a*