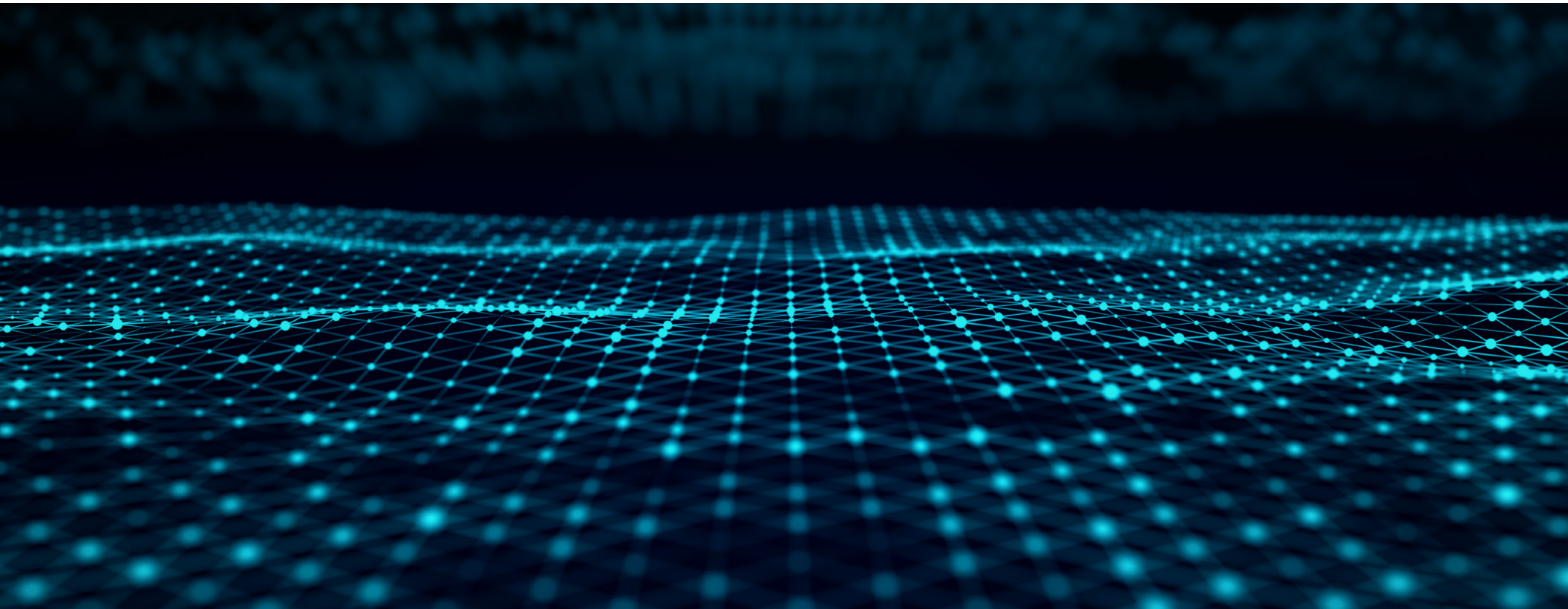
Cisco Hybrid Mesh Firewall At-a-Glance

Security architected for tomorrow, ready today



The distributive nature of today's enterprise IT environment is massively complex.

The proliferation of applications, the rise of AI technologies, and an increasingly mobile workforce continues to expand the attack surface. Organizations must be able to secure major traffic boundaries, protect business and AI-enabled applications, and ensure that users and devices can only access specifically permitted resources.

Radical change requires radical thinking, so we've reimagined security to work for every environment, at hyperscale. Firewalls have been the foundation of enterprise security and are as important as ever—at Cisco we've taken the power of firewalling to a whole new level.

Cisco's Hybrid Mesh Firewall solution is a highly distributed security fabric optimized to stop advanced threats, protect application vulnerabilities, and implement zero trust segmentation across environments. With unified cloud management that streamlines workflows and enhances security, Cisco gives you the ability to scale your security fabric without having to rip and replace existing infrastructure. Bolstering productivity, you can now leverage AI-native capabilities to simplify troubleshooting and optimize performance across your enforcement tools.

Our Hybrid Mesh Firewall simplifies adoption and protects your investment with flexible licensing through the Cisco Cloud Protection Suite, enabling you to easily access different capabilities and new innovations as your business needs evolve.

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 the 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.

Cisco's Hybrid Mesh Firewall Components

Hypershield:
AI-native distributed security architecture for AI-scale

Secure Firewall:
Industry-leading firewalls that see through encryption, at scale

Secure Workload:
Gain visibility and apply segmentation policies to applications across hybrid environments with or without agents

Multicloud Defense:
Cloud-native orchestration and automation simplifies deploying, networking, and scaling firewalls in the public cloud

AI Defense:
Safeguards for the development and deployment of AI applications

Isovalent Enterprise Platform:
Discover microservice interactions and enforce policies in Kubernetes environments

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

Why Cisco's Hybrid Mesh Firewall?

Highly distributed security fabric with unified management from a single vendor

Cisco goes beyond 'firewalling in a box' to fuse security into the network, cloud, container, and workload for a highly distributed fabric. It puts security where you need it, incorporates your existing firewalls, scales with your business, and handles policy management that goes beyond human-scale. Available in a flexible license that evolves with your needs and as Cisco innovates.

Five capabilities that sets Cisco's Hybrid Mesh Firewall solution apart:

1. Intelligent Centralized Management: Automatically configures, deploys, and autoscales firewalls across multi-cloud environments without scripting. Plus, the AI assistant reduces management overhead and frees up resources and expertise.
2. Advanced Threat Protection: Sees through encryption to detect threats in encrypted traffic without sacrificing performance using industry's first, ML-based encrypted visibility engine. Where decryption is essential, high-performance hardware offload architecture delivers price-performance leadership and deep visibility. Protect against known and unknown threats with Cisco Talos Threat Intelligence, industry leading Snort 3 IPS, and Snort ML.
3. Segmentation: Prevent unauthorized lateral movement and safeguard applications across data center and clouds with topology-aware security that understands app dependencies and applies zero trust segmentation policies across the Cisco security fabric.
4. AI Model Protection: Fuses AI guardrails into the fabric of the network to safeguard in real-time against the dynamic threats introduced through the development and deployment of AI applications.
5. Exploit Protection: Mitigates vulnerabilities by applying a surgical mitigation shield that is optimally placed in the path of the application to block the exploit—all while ensuring application uptime.

Cisco Hybrid Mesh Firewall Capabilities

Security that moves as fast and as agile as the business

- Security fabric consisting of firewalls (physical, virtual and cloud), agents (traditional and Kubernetes workloads), and smart switches that fuse security into the fabric of the network
- Puts security everywhere it's needed by fusing it into the fabric of physical, virtual, cloud, container, and IoT environments
- Cloud-native firewalling enables easy networking, autoscaling, and self-healing of enforcement points within public cloud environments
- Identify and block malicious threats hidden within encrypted traffic with Encrypted Visibility Engine
- Stop known and zero-day threats by leveraging Snort 3 IPS, Snort ML, and continuous threat intelligence updates from Cisco Talos
- Segment any application in any environment using consistent zero-trust policies with a security architecture designed to defend modern, AI-scale data centers
- AI model protection in real-time to safeguard AI-driven applications from misuse, data breaches, denial of service and sophisticated attacks such as prompt injections
- Protect against exploits with an AI-native rule engine that prioritizes vulnerabilities and automatically recommends a surgical mitigating control
- Native integration with Cisco Identity Services Engine (ISE) enables easy segmentation of IoT devices through consumption of security group tags
- Integrates with Cisco Universal ZTNA to provide a holistic Zero Trust platform across the hybrid enterprise

Cut through complexity at scale with intelligent centralized management

- Cloud-delivered management across multiple domains, including management of all enforcement points from a single interface, object sharing across the fabric, role-based access control (RBAC), license management, AI Ops, and policy lifecycle management
- Cloud policy management across Cisco infrastructure and third-party firewalls, and enforcement of Cisco Universal ZTNA policies anywhere for any user access, on-premises or remote
- Native configuration, deployment, and autoscaling of cloud firewalls across multicloud environments
- AI Assistant provides unified insights across the security mesh for policy configuration, troubleshooting, and optimization
- AI Assistant is capable of writing, deploying, and optimizing firewall rules within the environment and offers recommendations for common tasks

Protects your business

Increase resilience and avoid downtime with the right security controls and the optimal enforcement points.

Protects your team

Dramatically increase your team's efficiency to free up resources with centralized management of security tools across the fabric an autonomous, self-learning system that earns your trust.

Protects your investment

The Cloud Protection Suite is your path to Hybrid Mesh Firewall. It marries simplicity and flexibility to more easily achieve your outcomes and leverage solution innovations at your own pace as your business scales.

Learn More

To find out more about Cisco Hybrid Mesh Firewall products and services, visit www.cisco.com/go/hybridmeshfirewall.

To view buying options and speak with a Cisco sales representative, visit www.cisco.com/site/us/en/buy/index.html.