Cisco **Security**

Reimagining Security for the AI Era

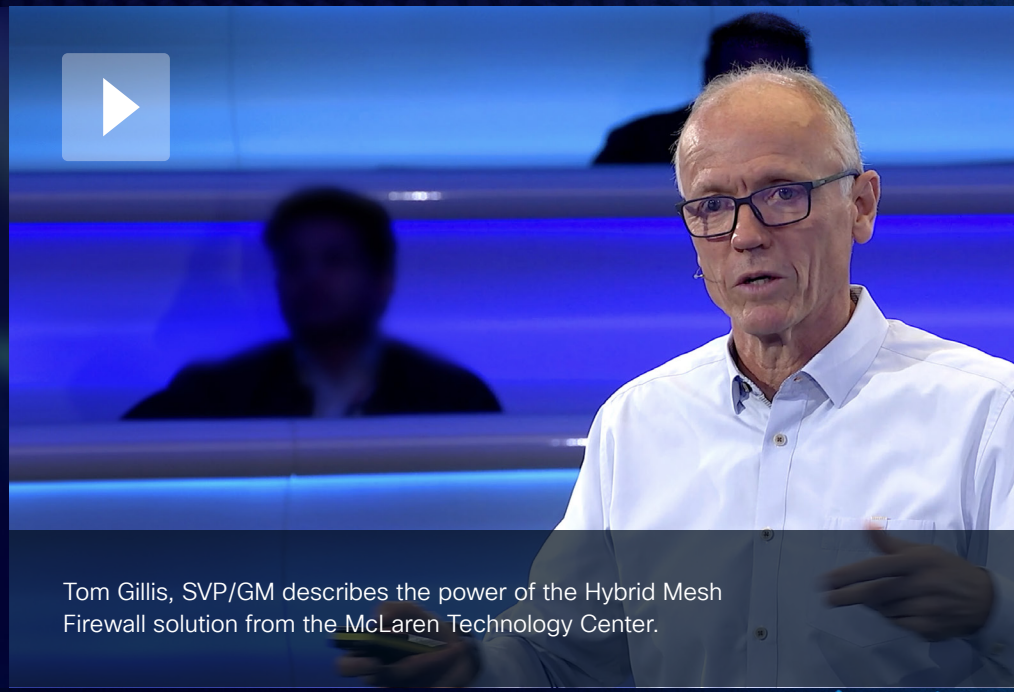
The AI revolution is gaining speed and is already changing what modern enterprises and their data centers look like. As applications become AI-enabled and increasingly complex, running on modern, highly distributed infrastructure, the task of protecting them is impossibly hard. AI-driven threats mean more vulnerabilities are being exploited smarter and faster. A fundamentally different approach is needed to protect applications now.

Cisco's Hybrid Mesh Firewall Solution

Security architected for tomorrow, ready today

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. We've taken the power of firewalling to a whole new level with an approach that fuses security into the network to create an army of enforcement points, all centrally managed. We're introducing an AI-native security architecture that's more fabric than fence at the heart of a game-changing solution that meets you where you are and scales with you.

Watch



Tom Gillis, SVP/GM describes the power of the Hybrid Mesh Firewall solution from the McLaren Technology Center.

Solving today's big enterprise security challenges

40+

days to segment an application

Explosive workload growth, changing environments, and inconsistent enforcement prevent successful segmentation.

Autonomous Segmentation

An extended network that segments itself and continuously adapts.

Learn

600

CVEs reported each week on average

Patching is hard and mitigation is slow, leaving you vulnerable and your teams overwhelmed for far too long.

Distributed Exploit Protection

Prioritizes vulnerabilities and deploys surgical mitigating controls.

Learn

95%+

of data center traffic is encrypted

Most attacks occur through encrypted data and generative AI is accelerating the number of threats.

Advanced Threat Protection

See through encrypted threats and stops zero day exploits.

Learn

1

annual security update on average

Upgrades and updates of a mushrooming number of assets and policies is risky and can lead to disruption.

Intelligent Centralized Management

All enforcement points centrally managed across the security fabric.

Learn

200+

AI-security and safety categories

The AI-transformation is generating a host of new risk vectors that traditional security tools are not equipped to combat.

AI Model Protection

Network-level, real-time protection for AI applications.

Learn

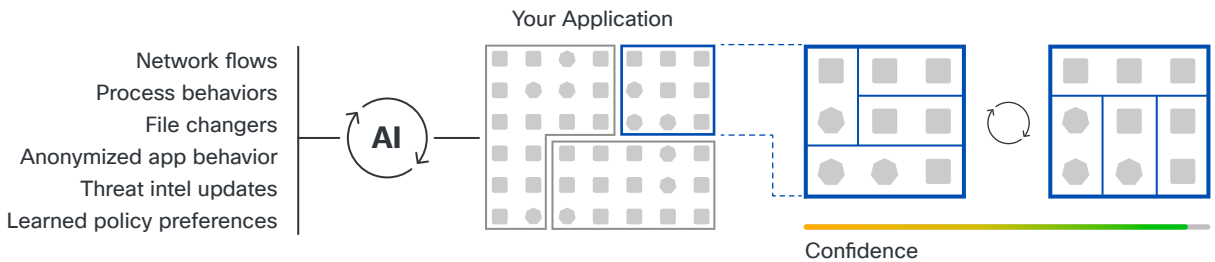
Challenge

Explosive workload growth, changing environments, and inconsistent enforcement prevent successful segmentation.

Autonomous segmentation that continuously adapts and learns.

Cisco's AI-native solution looks beyond network flows to what is happening within the workload - process behaviors, file changes, and learned policy preferences - for a very deep understanding of the application and what's happening across all the environments it's protecting. This includes and expands to:

- What assets are exposed to vulnerabilities
- What existing policies are deployed within the business
- What the system has learned based on best practices that model how the customer modifies recommended policies
- What threat intelligence teaches it about the latest attacks



Comprehensive inputs for segmentation policy creation

AI augments human ability by efficiently correlating and analyzing the details of all the workload actions ranging from network, process, protocol, port, file inspection, and application behavior – using it to further hone the application dependency map.

Automatically tighten, adjust, tighten, repeat

As the application changes, policies automatically adjust with it, increasing security admin's confidence in security controls, while keeping applications running.

Challenge

Patching is hard and mitigation is slow, leaving you vulnerable and your teams overwhelmed for far too long.

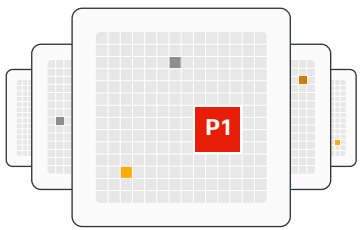
Close the exploit gap with Distributed Exploit Protection

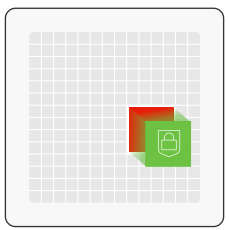
Mitigate vulnerabilities in minutes by applying a surgical mitigation shield that is optimally placed in the path of the application to block the exploit – all while ensuring the app keeps running. It starts by mapping vulnerable assets across your entire environment and prioritizes them based on three questions:

Q: Is the vulnerability reachable on the asset?

Q: Is it being exploited in the wild?

Q: Is it affecting a high-value asset?

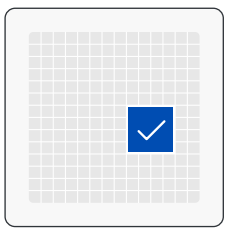




Perfect fit

Tested against real world traffic

Optimal placement



Patched

1: Prioritize vulnerability

Our AI capabilities and deep understanding of the application help prioritize the most critical vulnerabilities.

2: Apply mitigating shield

While the application team qualifies the patch, the solution applies a surgical mitigation shield directly in the application path to block the exploit.

3: Remove shield when patched

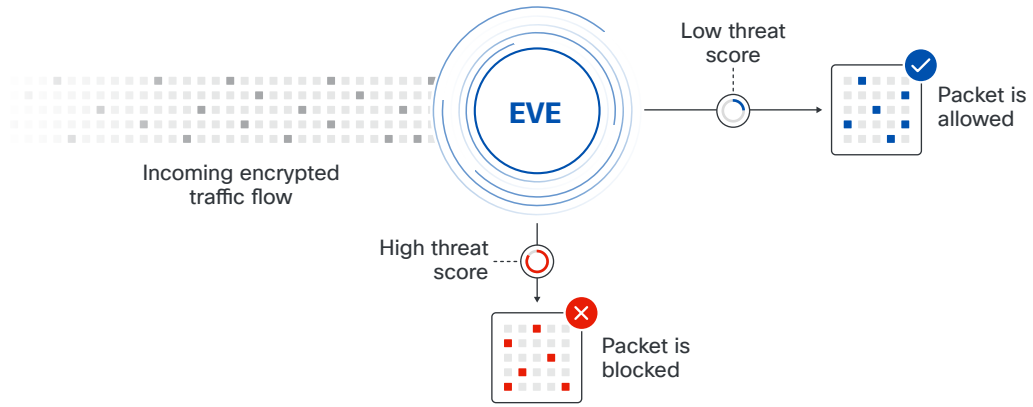
Once the patch is applied, the mitigation shield is automatically removed as the policy is no longer needed.

Challenge

Most attacks occur through encrypted data and generative AI is accelerating the number of threats.

See through encrypted traffic for strong price-performance threat prevention

Cisco Encrypted Visibility Engine (EVE) allows you to find malicious flows without having to decrypt it. The EVE risk score enables you to block, allow or intelligently examine traffic. The Cisco Secure Firewall is built with encryption in mind and so its architecture allows for efficient encryption visibility of traffic, and industry-leading Snort helps to detect known and unknown threats, now enhanced with Machine Learning (ML) for next-level performance.



1: Fingerprint

Process over one billion TLS fingerprints and over 10,000 malware samples daily.

2: Prioritize

Use the EVE Risk Score to take optimal action based on risk level, maintaining maximum operational performance.

3: Identify

Utilize Snort, enhanced with ML, to identify and mitigate known and unknown threats in real-time.

Challenge

Staying on top of every asset and security tool is becoming impossibly complicated and time consuming. Slow upgrade cycles can't keep up with threats.

AI-native design that lets you manage globally, enforce locally, update autonomously

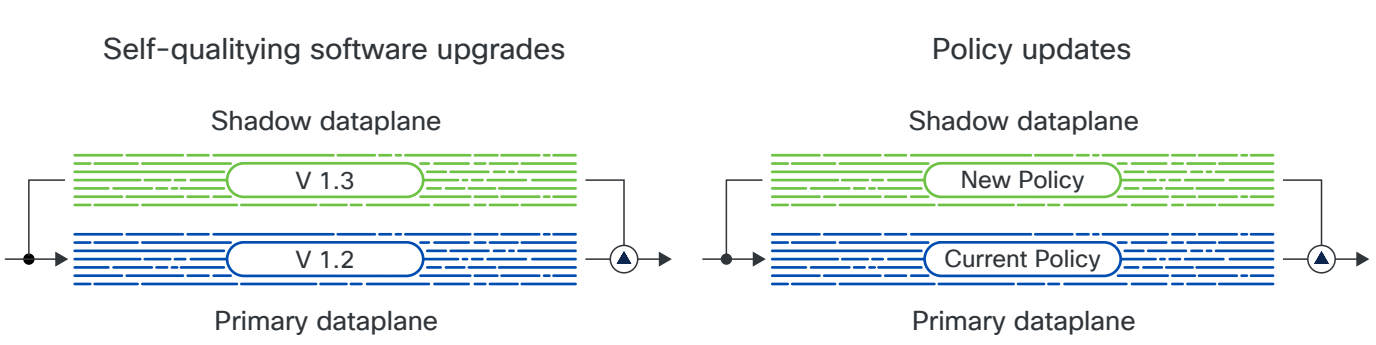
Protecting the entire enterprise from ground to cloud in an AI-era brings new levels of complexity. A strong security posture comes from always being connected and Cisco's cloud management ensures access from anywhere, anytime, without disruption. The Cisco Hybrid Mesh Firewall utilizes native AI capabilities for around-the-clock protection and productivity. Security management has never had this level of efficacy.

A dual data plane architecture removes the risk of automated software and policy updates by testing changes on live traffic before deployment. Live network traffic is replicated in a shadow path to test an update before switching to the primary path for a go-live.

A unified management platform overcomes security silos to provide a unified, outcome-centric picture, driving real-time insights, automation and policy enforcement.

An AI-assistant ties everything together, tells you where to prioritize your attention and answers all your queries. Benefit from up to 70% simpler policy administration for efficient, zero-downtime, zero-trust operations.

Going a step further, Cisco is also bringing management of all your Cisco and third-party firewalls under one platform, increasing productivity and enhancing efficacy.



Challenge

The AI-transformation is generating a host of new risk vectors that traditional security tools are not equipped to combat.

Enforce critical safeguards for the development and use of AI applications.

As applications become AI-enabled and teams look for performance uplifts, the AI transformation of the enterprise is also generating new safety and security risks that traditional security tools are not equipped to defend against. Cisco's AI model protection enables you to detect and defend against the dynamic threats introduced through the development and deployment of AI applications.

Cisco fuses AI guardrails into the fabric of the network to safeguard your production applications from attacks and undesired responses in real-time. The guardrails are automatically identified and configured to the vulnerabilities of each AI model.

Discover AI assets

Identify the AI workloads, applications, models, data, and users across your distributed on-premises and cloud environments.

Detect Risks

Spot the misconfigurations, security vulnerabilities, and adversarial attacks that put AI applications at risk.

Protect in real time

Safeguard AI applications against rapidly evolving threats, including prompt injections, denial of service, and data leakage.

The first hybrid mesh firewall for the AI-era

Delivering the hyperscaler model to the enterprise

A breakthrough solution built for the AI-era. Cisco is uniquely positioned to melt security into the network for a hyper-distributed fabric with hundreds or even millions of enforcement points, while leveraging your existing security and infrastructure investment. Protect every app, process, switch, server and device for data center security like never before.

Distributed Architecture

A distributed architecture that puts security wherever it needs to be.

Learn

Building Blocks

A radically different solution utilizing an army of optimized enforcement points.

Learn

Unified Management

A central platform that manages existing and new infrastructure.

Learn

Simplified Adoption

Simplicity and flexibility in one package that evolves with your needs.

Learn

A distributed architecture that puts security wherever it needs to be.

Tom Gillis, SVP/GM Cisco Security, illustrates the transformative effect of a distributed approach

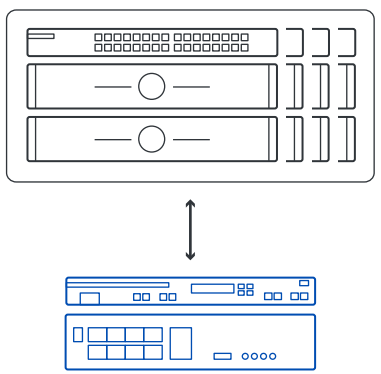
Watch Clip (1:48)

A security approach that moves as fast and is as agile as the business.

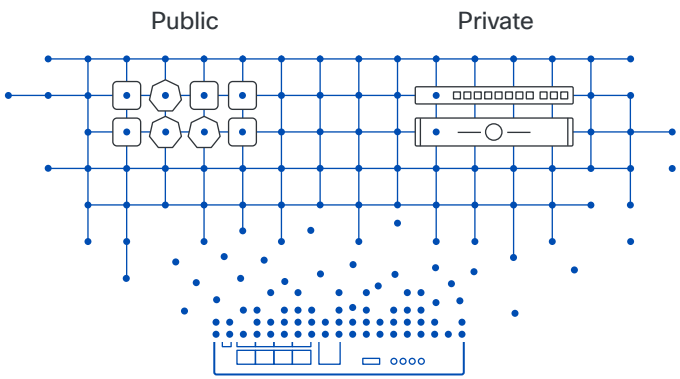
The first truly distributed, AI-native security architecture puts security everywhere it needs to be: in every software component of every application running on the network, on every server, and in public or private clouds.

Cisco gives you the ability to scale your security fabric without having to rip and replace your existing infrastructure. Our breakthrough security architecture is designed to meet you where you are today for seamless, extended protection and evolve with your organization.

What used to be a single box in the data center connecting to many...



...has been exploded into software and distributed into a fabric that lives everywhere.



A holistic, integrated approach that infuses security into each layer of the network and cloud fabric.

An army of optimized enforcement points

An ever-growing security fabric with thousands of different enforcement points, each with its own capabilities by design, optimized for its task. These enforcement points are the building blocks of this breakthrough security architecture and come in different forms, including traditional and eBPF agents, smart switches, physical and virtual appliances, all centrally managed with our cloud-native platform.

Physical, virtual & cloud firewalls

Utilize advanced threat inspection at key boundaries and protection against encrypted threats, zero-day exploits, AI runtime protection and full perimeter firewalling.

Smart switches

Fuse security into the fabric of the network to provide segmentation deeper inside the data center to prevent lateral movement.

Workload agents

Utilize Snort, enhanced with ML, to identify and mitigate known and unknown threats in real-time.

Every insight, asset and policy centrally managed. New and old infrastructure working together.

Craig Connors, CTO Cisco Security, describes AI-era uni ied management

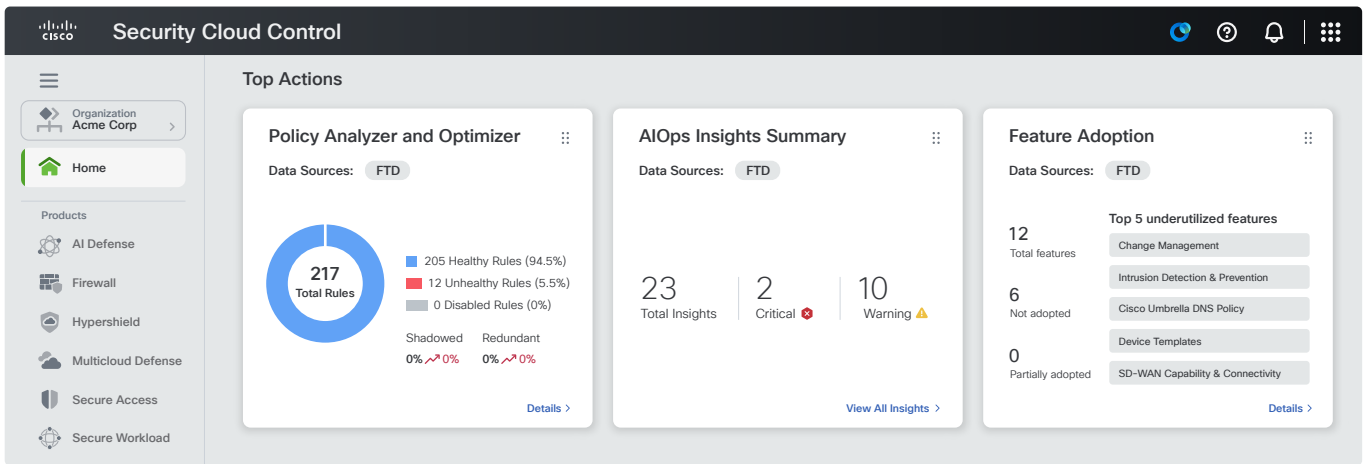
Watch Clip (2:23)

AI-native control to cut through the complexity of hyperscale operations

Multiple environments and a vast array of security tools already make management difficult, sucking in valuable team resources and expertise to make it work. This is unsustainable as we move to a hyperscaler model. However, Cisco Security Cloud Control tackles this complexity head on.

At scale, a policy update is like playing a game of Jenga - one wrong move can bring everything down. Security Cloud Control provides intelligent insights across your products to make sense of all your data center security rules for policy configurations and rule optimization over the lifetime of an asset. Its AI Assistant is also designed to answer questions and make recommendations for common tasks.

By simplifying rule creation, policy administration and orchestration, and everyday security operations, this AI-native console will change the way you think of security management.



Adoption and consumption of our Hybrid Mesh Firewall solution is easy with the Cisco Cloud Protection Suite.

A simpler, more flexible way to achieve your security resilience

A new era of security needs a new approach that doesn't stop at the technology. When Cisco talks about security that scales with you, we mean that in every sense. We're bringing a refresh to the way you buy security to make it easier, with simple choices and flexible licensing that protects your existing investment. The game has changed with an end to the traditional 'rip and replace' approach with the Cisco Cloud Protection Suite for Hybrid Mesh Firewall.

A smart solution made simple

A simple pricing model that comes with investment protection.

Security on your terms

Flexibility to utilize and migrate licenses as your deployment needs evolve.

Always future-ready

Leverage Cisco solution innovations at your own pace as your business scales.

A solution with the smarts to protect you on multiple levels

The security platform that keeps getting stronger

Cisco gives you the means to protect all your applications, anywhere, in a way not possible before. A single platform to see, secure, and simplify your security operations in the AI era. Cisco's Hybrid Mesh Firewall redefines security for modern environments.

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 an autonomous, self-learning system that earns your trust.

Protects your investment

No need to rip and replace your existing infrastructure. Add to it with class-leading products and services as your business evolves.

A new security era starts today

The Cisco Hybrid Mesh Firewall solution

Brings together brand new and familiar products, all sharing a common foundation and services. It's a flexible solution that leverages AI and identity intelligence and is designed to work with your existing infrastructure. Ready to safeguard your enterprise in the AI era.

Hypershield
AI-native distributed security architecture for AI-scale

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

Secure Workload
Application visibility & microsegmentation for traditional workloads

AI Defense
Safeguards for the development and deployment of AI applications

Isovalent Enterprise Platform
Visibility and segmentation for Kubernetes workloads

Security Cloud Control
Intelligent centralized management

*AI Defense Secure Access are add-ons to Cloud Protection Suite


cisco
To learn more, please visit cisco.com