Security for the AI Era

The AI revolution is already changing what modern enterprises and their data centers look like. As applications become AI-enabled, agentic AI gains traction, and modern environments grow more complex and distributed, the task of protecting them becomes increasingly difficult. Additionally, AI-driven threats mean more vulnerabilities will be exploited, and faster than ever. A fundamentally different approach is needed now.

Cisco Hybrid Mesh Firewall

Security for tomorrow, ready today

Radical change requires radical thinking. That's why we're introducing an AI-native security architecture that's more fabric than fence. It fuses security directly into the network to create enforcement points all over your network, all centrally managed. This is security designed to work for every environment, at hyperscale, but ready to meet you where you are now and scale with you as you grow.

Today's enterprise security challenges

200+

AI-security and safety categories

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

AI Model Protection

Network-level, real-time protection of AI applications, built specially for this new era.

Learn

40+

days to segment an application

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

End-to-End Segmentation

Identity-driven macro and microsegmentation stops unauthorized lateral movement–from network to the workload, as deep as the process level.

Learn

95%+

of data center traffic is encrypted

Most attacks occur through encrypted data and generative AI is adding to the number of unknown threats. Decryption degrades performance and often isn't practical or even possible.

Advanced Threat Protection

Leading price-performance threat protection for data center, cloud, campus, branch, and IoT environments that sees through encrypted traffic and stops zero-day exploits.

Learn

600

CVEs reported each week on average

Patching is difficult and mitigation is slow, leaving you and your teams vulnerable and overwhelmed.

Distributed Threat Protection

Prioritizes vulnerabilities to quickly deploy vulnerability shields.

Learn

86%

of organizations identify shortage of skilled cyber-security professionals as a major challenge

Risk increases when teams are stretched thin, causing early warnings to be missed, issues to escalate resulting in otherwise avoidable downtime.

Unified, Agentic Operations

An agent-first model proactively analyzes traffic, health, and configuration data across environments and proposes one-click remediations to reduce human error and streamline operations.

Learn

Challenge

AI transformation is generating new risk vectors traditional security tools are not equipped to combat.

Critical safeguards for the development and use of AI applications.

New risks require new security capabilities. Cisco's AI model protection detects and defends against 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 self-configure to suit the vulnerabilities of each AI model.

Discover AI assets

Identify the AI workloads, applications, models, data, and users across your distributed environments.

Detect Risks

Spot the misconfigurations, security vulnerabilities, and adversarial attacks that threaten AI applications.

Protect in real time

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

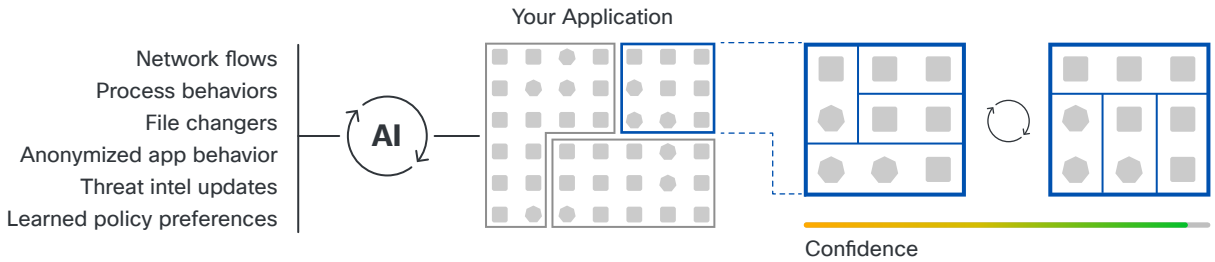
Challenge

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

Identity-driven macro and microsegmentation

Cisco Hybrid Mesh Firewall unifies firewalling, identity context, smart switches, and agents to enforce granular, identity-aware segmentation across campus, data center, cloud, and workload environments. Policies follow users, devices, applications, and services down to the process level. With Cisco Hybrid Mesh Firewall organizations are able to:

- Extend segmentation to every port on a smart switch—enforcing policy on internal traffic at scale
- Leverage agentless segmentation, through a deep integration with firewall enforcement points, to reduce friction and increase time to value
- Gain deep visibility into traditional and modern Kubernetes workloads and apply consistent microsegmentation policies at the process and kernel level using agents with eBPF technology.
- Flag and block risky devices, user behavior, and things with granular, dynamic security policies that incorporate identity sources and user trust scores



Comprehensive inputs for segmentation policy creation

AI efficiently correlates and analyzes all workload actions ranging from network, process, protocol, port, and file inspection as well as their interactions with devices, other applications, and systems of record to generate a high-fidelity application dependency map.

Automate the policy lifecycle

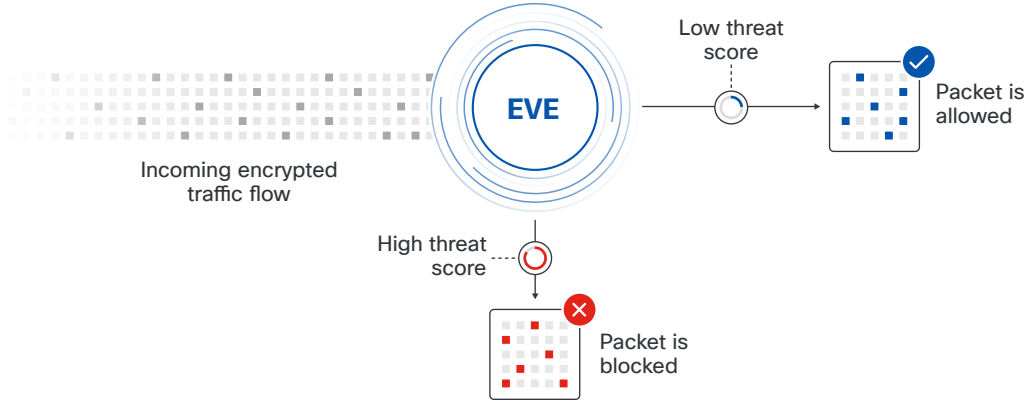
AI-powered automation discovers and recommends segmentation policies tailored to your unique environment, test and validate the policy without impacting the application.

Challenge

Most threats are hidden within encrypted traffic, and bad actors are using AI to automate and accelerate their attacks. Decryption degrades performance and often isn't practical or even possible.

Industry leading price-performance and zero-day threat protection for data center, campus, branch, and IoT environments

Hardware crypto offload, Encrypted Visibility Engine (EVE), and Snort ML help security teams easily inspect encrypted traffic, maintain performance, and stop known and zero-day threats at scale.



1: Fingerprint

Classify encrypted flows with rich telemetry and application finger-printing to expose malicious activity without decrypting.

2: Prioritize

Leverage EVE risk scores and selective decryption to take the right action while preserving privacy and performance.

3: Identify

Use Cisco Firewall, EVE, and Snort ML to detect and stop known, unknown, and zero-day threats in real time.

Challenge

In the AI era, the number of vulnerabilities is growing exponentially, patching is difficult, and mitigation is slow leaving you and your teams overwhelmed and environments at risk.

Protect infrastructure and applications in the AI era.

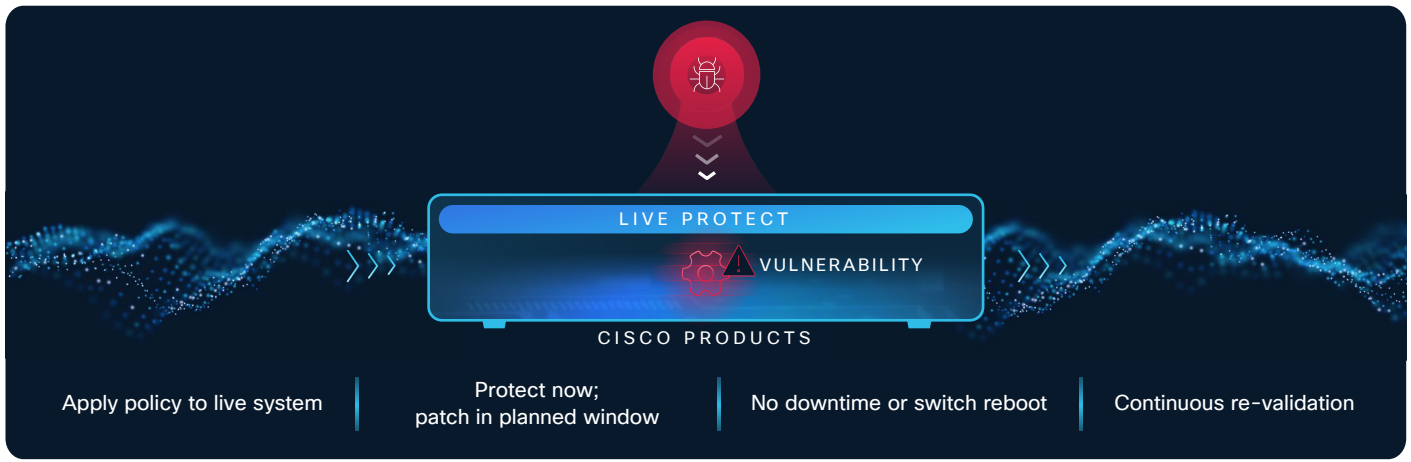
Block exploits in minutes by applying compensating controls in the path of the application. Further, Cisco Live Protect extends security to infrastructure including Cisco supported firewalls, routers, and switches.

Start 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?



1: Prioritize vulnerabilities

Our AI capabilities and deep understanding of the application prioritize the most critical vulnerabilities based on the organization's specific environments.

2: Apply vulnerability shield

While the application team builds the patch, a vulnerability shield can be placed directly in the application path to protect against exploitation.

3: Remove control when patched

Once the patch is applied, the vulnerability shield can be removed.

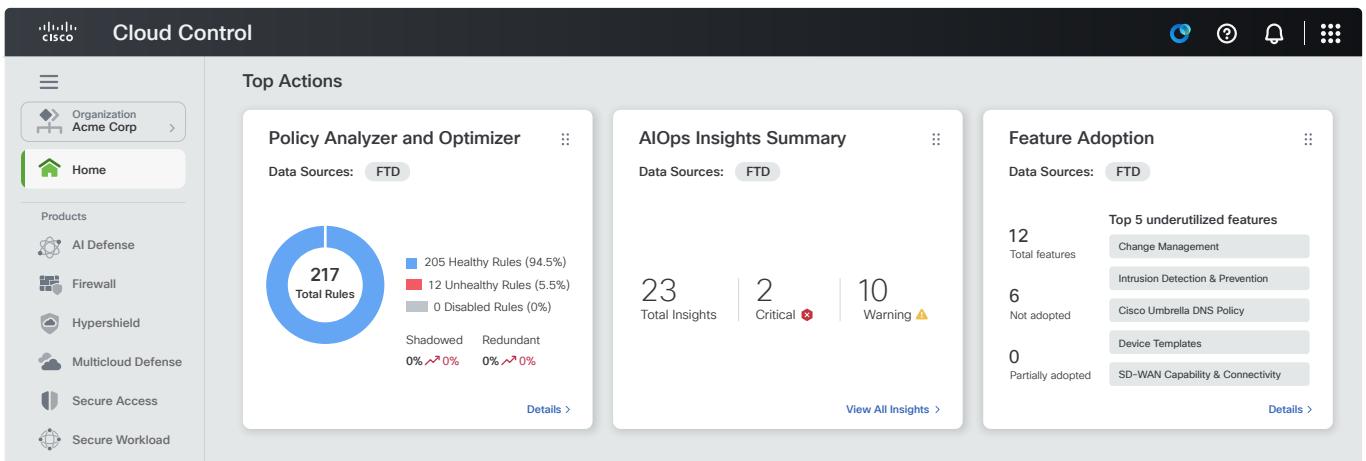
Fragmented tools and manual workflows make it hard to keep distributed security controls aligned, current, and resilient. This impedes real-time threat detection and response.

Reduce complexity, simplify operations

Managing security across data centers, clouds, campuses, and third-party firewalls is too complex and stretches security teams thin. That's why Cisco is bringing AgenticOps into security management. Combining unified management with an agent-first operating model enables teams to move faster and more intelligently with ready-to-execute configurations for monitoring data, identifying and troubleshooting issues, and enforcing compliance—all at machine speed. AgenticOps capabilities act like specialized experts, moving teams from reactive troubleshooting to proactive management.

Only Cisco lets you extend policy to non-Cisco firewalls

Define policy once and Cisco automatically translates it into tailored rules that can be deployed across Cisco and third-party enterprise firewalls, a Cisco exclusive capability.



The first hybrid mesh firewall for the AI-era

Delivering the hyperscaler model to enterprise security

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 different enforcement points, each with its own capabilities by design. Start by leveraging your existing security and infrastructure investment. Now you can protect every app, process, switch, server, and device in highly distributed environments for perhaps the first time ever.

Distributed Architecture

A distributed architecture that puts security where it needs to be: Everywhere.

Learn

Building Blocks

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

Learn

Unified, agentic operations

A central platform that unifies policy and automates operations across your infrastructure.

Learn

Simplified Adoption

Simplicity and flexibility in one package that evolves as you do.

Learn

A distributed architecture that puts security where it needs to be: Everywhere.

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

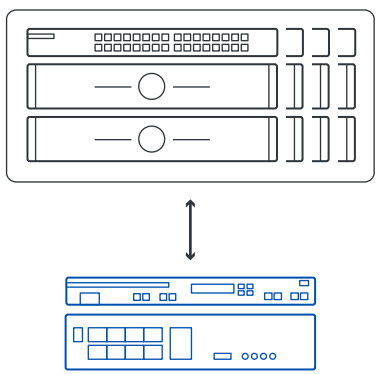
Watch Clip (1:48)

A security approach that moves with your business and just as quickly.

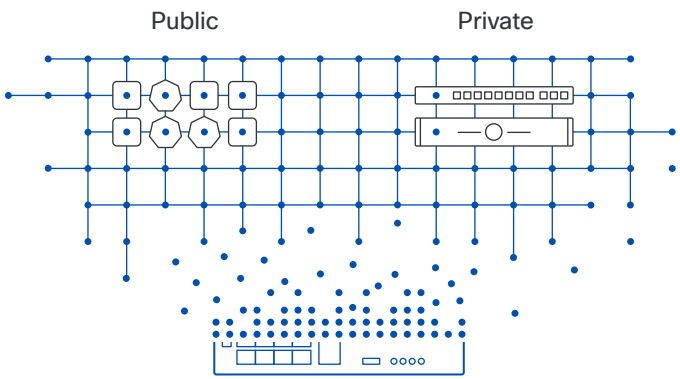
The first truly distributed, AI-native security architecture puts security where it needs to be: in every software component of every application running on the network, on every server, and in public or private clouds. In other words. Everywhere.

Cisco lets you scale your security fabric without “rip and replace.” Our security architecture meets you where you are today for seamless, extended protection and evolves when you do.

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.



Security that's infused into every layer of the network and cloud fabric.

An army of optimized enforcement points

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

Physical, virtual, cloud, and container firewalls

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

Data processing units (DPUs) in servers and smart switches

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

Workload agents

Traditional and eBPF agents place security controls closer to the application—enabling process and kernel-level visibility and control to reduce the attack surface and increase protection.

Unified control and agentic operations streamline protection for distributed IT environments

Managing policy across data centers, clouds, campuses, branches, and third-party firewalls with siloed tools is too complex. Cisco brings visibility, policy, and operations together in one AI-native platform purpose-built for hybrid environments.

Combining AgenticOps with unified security management enables users to define policy intent once, automatically translate that intent into tailored rules, and deploying them to Cisco and third-party firewalls.

AgenticOps changes the way teams run security at scale—for the better, simplifying rule creation, policy administration and optimization, and orchestration, giving operators the support to manage with confidence.

Adopt and consume Cisco Hybrid Mesh Firewall with ease

A simpler, more flexible way to achieve security resilience

When Cisco talks about security that scales with you, we mean that in every sense. We're changing the way you buy security to reflect a too-rapidly changing world, with simple choices and flexible licensing that protect your existing investment. And that means, you can say goodbye to 'rip and replace,' thanks to the future-ready Cisco Hybrid Mesh Firewall.

A smart solution made simple

A simple pricing model that comes with built-in investment protection.

Security on your terms

Flexibility to utilize and migrate licenses as your needs evolve.

Always future-ready

Take advantage of Cisco solution innovations at your own pace as your business scales.

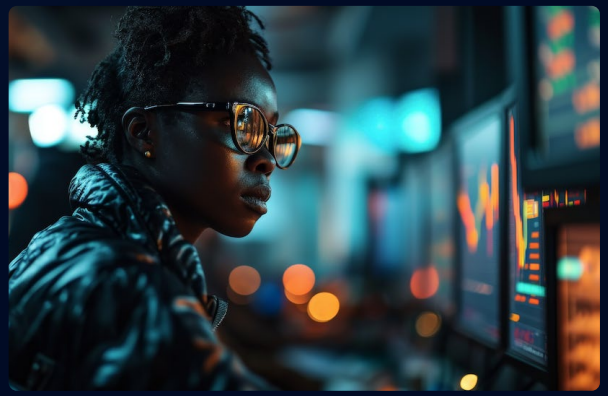
A security solution that protects your investment, too.

The solution that keeps growing with you

Cisco Hybrid Mesh Firewall protects all your applications, anywhere, in a way that was simply not possible before. It's a solution that sees, secures, and simplifies your security operations for the AI era.

Protects your business

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



Protects your team

Elevate your team's efficiency with AI-native security that earns your trust.

Protects your investment

No more 'rip and replace.' Add best-in-class products and services as your business evolves.

It's security for the one place you need it most. Everywhere.


cisco
To learn more, please visit cisco.com