Cisco **Security**

Securing today's AI-scale data centers.

In today's environment, managing security surpasses human capacity alone. Workloads are commonly distributed across multiple data centers and clouds, leading to fragmented policies that open security gaps and delay remediation of issues and incidents. At the same time, adversaries are exploiting vulnerabilities faster than ever – a trend that will only accelerate as AI continues to evolve and is fully adopted.

Cisco Hypershield

AI-native security for data centers and the cloud

Cisco Hypershield fundamentally reimagines how enterprises secure today's AI-scale data centers – both on-premises and in the cloud – empowering organizations to protect modern applications more effectively. We've taken the network security functions that used to come in a box and melted them into the network as hundreds of thousands or even millions of enforcement points. More a fabric than a fence, Hypershield allows security to be placed everywhere it needs to be.

Watch

Tom Gillis, SVP/GM and Craig Connors, CTO, Cisco Security, discuss the power of Hypershield from the McLaren Technology Center.

Solving three of the biggest security challenges enterprises face today.

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 continuously, placing macro-guardrails on workloads that become tighter and tighter through learned behavior.

Learn

600 **CVEs reported each week**

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

Distributed Exploit Protection

In minutes vs. months, an AI-native rule engine prioritizes vulnerabilities and deploys surgical mitigating controls that are tested against live production traffic with optimal placement.

Learn

1 **annual security update on average**

Upgrades and policy updates are risky and can lead to disruption. Relying on only one change window a year leaves you vulnerable.

Self-qualifying Updates

Powerful automation that allows you to validate upgrades and policy changes against live production traffic with our innovative dual data plane approach.

Learn

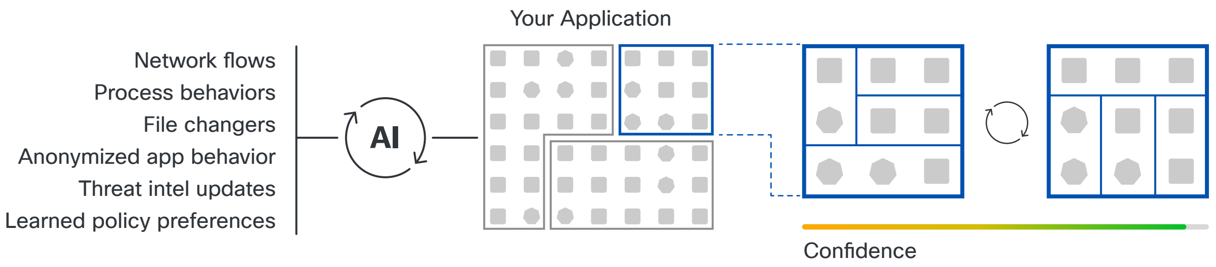
Challenge

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

Autonomous Segmentation that continuously adapts and learns.

The AI-native Hypershield looks beyond network flows to what is happening within the workload—including pre-production app behavior—for a very deep understanding of app identity across the entire app lifecycle, and what is happening across all the environments it is protecting. This includes and expands to:

- ✓ The assets that 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 latest attacks



Your Application

Network flows
Process behaviors
File changers
Anonymized app behavior
Threat intel updates
Learned policy preferences

AI

Confidence

Comprehenisve 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 Hypershield's 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.

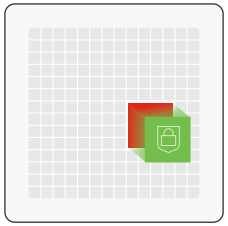
Close the exploit gap with Distributed Exploit Protection.

Hypershield mitigates vulnerabilities in minutes by applying a surgical mitigation shield that is optimally placed in the path of the process 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 running in memory?

Q: Is it being exploited in the wild?

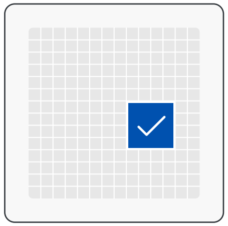
Q: Is it affecting a high-value asset?



Perfect fit

Tested against real world traffic

Optimal placement



Patched

1: Prioritize vulnerabilities

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

2: Apply mitigating shield

While the application team qualifies the patch, Hypershield 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

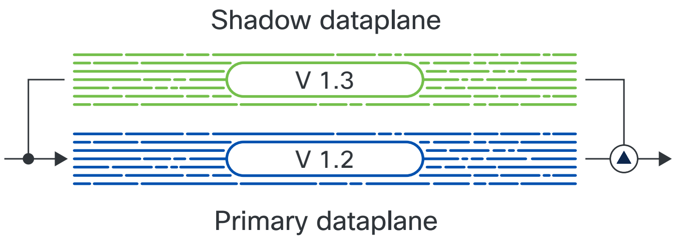
Upgrades and policy updates are risky and can lead to disruption. Relying on only one change window a year leaves you vulnerable.

Self-qualifying updates: Test in shadow, deploy with confidence.

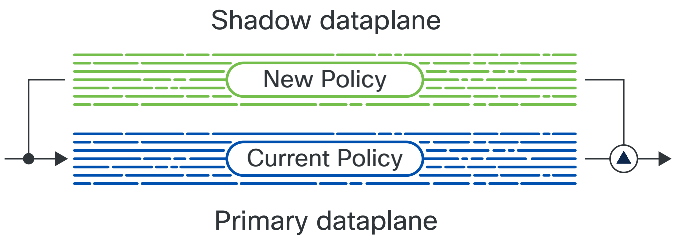
Hypershield enables safe, automated software and policy updates by testing changes on live traffic before deployment. The network-based enforcer uses a dual data plane architecture, where traffic is replicated between a primary path and a shadow path.

Updates are first tested in the shadow data plane, and after validation through a deployment confidence score, can be seamlessly activated by switching the shadow to primary. This approach allows admins to confidently approve updates without risking business disruption, ensuring systems stay current and secure.

Self-qualitying software upgrades



Policy updates



An approach that’s not the next-gen of anything. It’s the first-gen of something entirely new.

Delivering the hyperscaler model to the enterprise

Hypershield deeply combines security and networking in a way that only Cisco can by taking the network security functions that used to come in a box and melting them into the network into hundreds of thousands or even millions of enforcement points.

Distributed Architecture

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

Learn

Building Blocks

A radically different solution built on three unique building blocks.

Learn

Extended Connectivity

Control lateral movement with end-to-end visibility from user device to the application.

Learn

Security Fabric

A new security architecture that’s more fabric than fence.

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

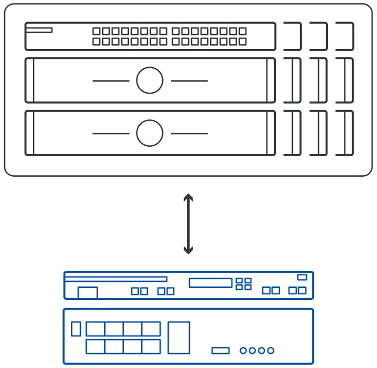
Watch Clip (1:48)

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

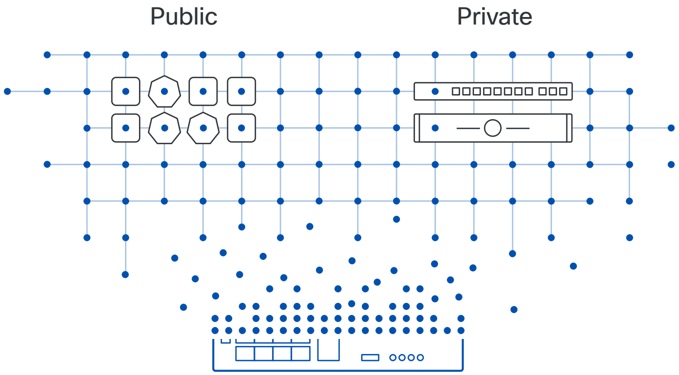
Cisco Hypershield is the first truly distributed, AI-native security architecture that puts security everywhere it needs to be: in every software component of every application running on the network, on every server, and in public or private cloud deployments.

The solution's unique architecture allows policy enforcement across multiple domains through a centralized, cloud-based management plane. Policy enforcement can be applied on the end system directly in the OS kernel or through the network on a virtual machine appliance. Our vision is to extend Hypershield to hardware accelerators running on networking devices such as switches.

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 radically different solution built on three unique building blocks.

A new approach to secure the modern enterprise.

Hypershield was built from the ground up to radically rethink how enterprises secure today's dynamic infrastructures across on-premises and cloud environments. It starts with kernel-level visibility and enforcement and uses powerful insights from AI, that is continuously learning, to simplify and harden modern application environments.

Artificial Intelligence

Hypershield was designed with artificial intelligence at its core rather than adding AI as a bolt-on. It can automatically analyze large amounts of security data, provide intelligent recommendations, and generate insights from the moment it starts observing your environment. The system helps security teams work more efficiently by automating complex analysis and decision-making processes while maintaining human oversight.

Extended Berkeley Packet Filter (eBPF)

Hypershield provides kernel-level visibility and enforcement on the workload using an open-source technology called eBPF. Co-created by Isovalent that was recently acquired by Cisco, eBPF is a software framework on modern operating systems that enables programs in user space to safely carry enforcement and monitoring actions via the kernel.

Hardware acceleration

Hypershield can deploy security in a variety of form factors to meet today's dynamic application environments. It lets you embed security on Kubernetes and Linux-based systems, VMs in public and private clouds – and in the future, insert security in high-performance server DPUs and hardware accelerators running on networking devices such as switches.

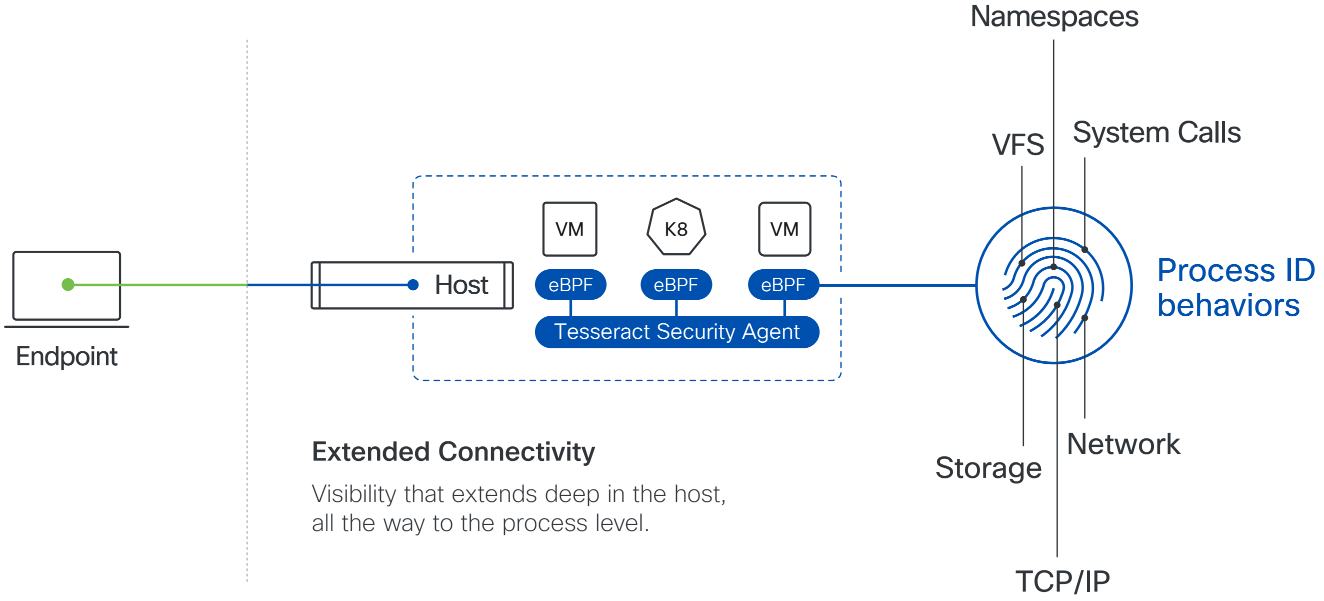
End-to-end visibility from the user device to the application in order to control lateral movement.

Craig Connors, CTO Cisco Security, describes the power of extended connectivity

Watch Clip (2:42)

Identify and respond to threats no matter where they are.

Cisco has presence on the user device and, now with Hypershield, close to the application, to detect any malicious behavior and control lateral movement in case of an attack. Hypershield uses deep workload visibility and enforcement to create an application fingerprint to gain an intimate understanding of application behavior. And, as the app changes, Hypershield dynamically modifies and shifts its policies as well. This understanding at the application level gives Hypershield and security teams the awareness to identify truly abnormal behavior.



Extended Connectivity

Visibility that extends deep in the host, all the way to the process level.

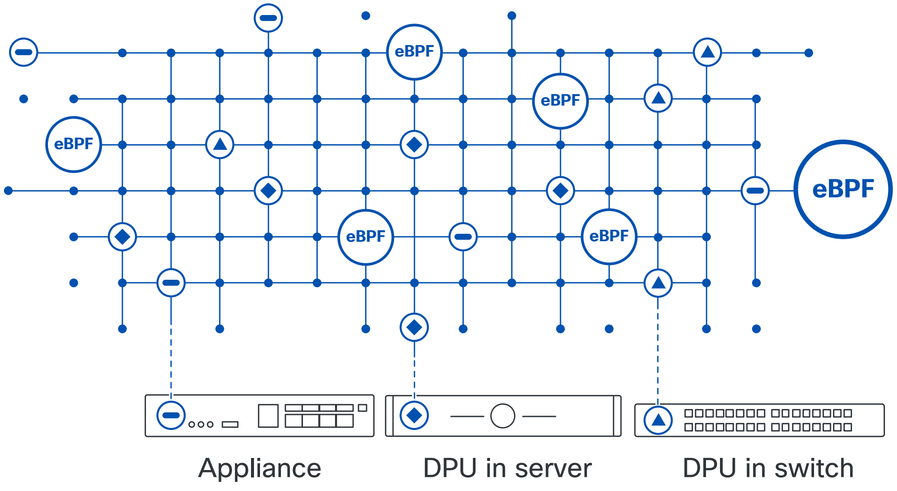
A new security architecture that’s more fabric than fence.

Craig Connors, CTO Cisco Security, describes how the security fabric meets you where you are and grows over time.

Watch Clip (1:24)

A security fabric that grows over time.

Hypershield helps scale security everywhere in your environment, without having to rip-and-replace your existing infrastructure. Hypershield is a software-based solution that can be deployed in different form factors. The light-weight Hypershield agent can be deployed close to the workload. In addition to that, network-based enforcement is offered in the form of virtual machines (VMs). It's also planned to be extended to DPU servers and switches. Hypershield meets you where you are today and grows with the organization for seamless, extended protection.

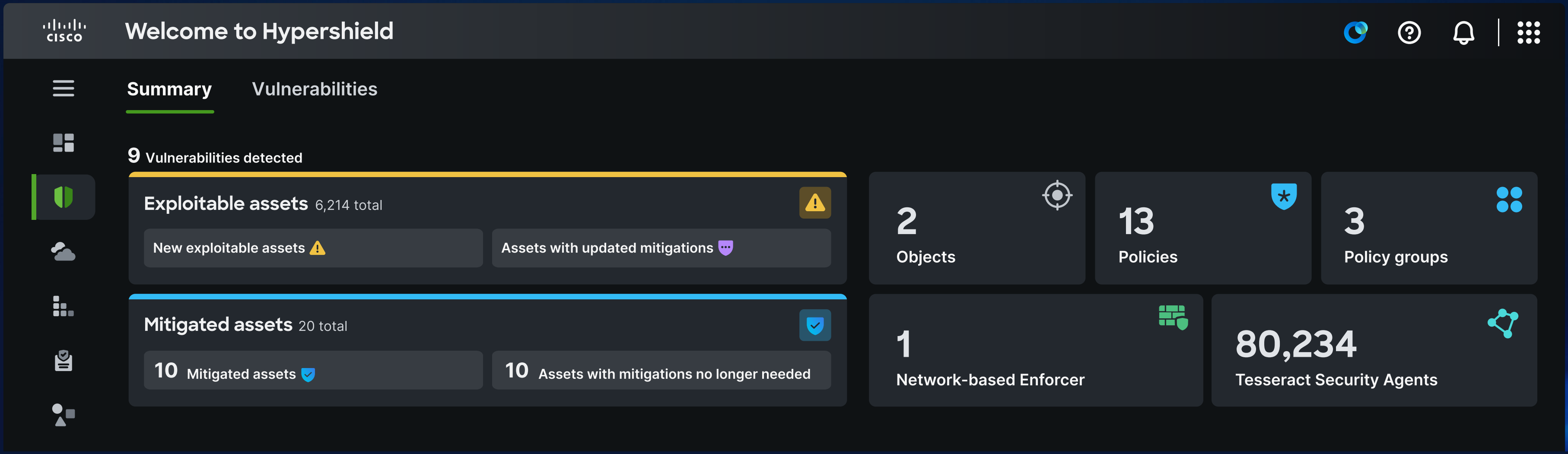


Hypershield provides kernel-level visibility and enforcement on the workload using an open-source technology called eBPF.

A centralized platform for managing and distributing policies across enforcement points.

Many environments, one screen

Hypershield is AI-powered and uniquely architected to implement a truly intent-based policy model that is centralized and easy to manage. No matter the form factor or location of the enforcement point, the policy is managed by Hypershield's central management console. When a new policy is created or an old one is updated, it is "compiled" and intelligently placed on the appropriate enforcement points. Security administrators always have an overview of the deployed policies, no matter the degree of distribution in the enforcement points. Policies follow workloads as they move – from on-premises to the public cloud and back again.



Welcome to Hypershield

Summary | Vulnerabilities

9 Vulnerabilities detected

Exploitable assets 6,214 total

New exploitable assets ⚠

Assets with updated mitigations

Mitigated assets 20 total

10 Mitigated assets

10 Assets with mitigations no longer needed

2 Objects

13 Policies

3 Policy groups

1 Network-based Enforcer

80,234 Tesseract Security Agents

To learn more, please visit **cisco.com/go/hypershield**