Cisco Hypershield

AI Scale | Cloud Native | Highly Distributed

© 2024 Cisco and/or its affiliates. All rights reserved.

Contents

© 2024 Cisco and/or its affiliates. All rights reserved.

Product overview

Cisco® Hypershield is a distributed, AI-native security architecture. Our vision is to put security wherever it needs to be—in every software component of every application running on the network, server, and public or private cloud deployments.

Hypershield uniquely combines security and networking by taking the network security functions that used to come in dedicated boxes and "melting" them into the network. It provides AI-powered management that automates security policy lifecycles and security infrastructure upgrades. At the same time, the system lets customers choose their preferred level of autonomy, using testing and reporting capabilities to earn trust.

Hypershield allows you to embed security within workloads and the network from a single policy framework and management system.

Unique capabilities for overcoming today's security challenges

- **AI-native security:** Cisco Hypershield was designed with artificial intelligence at its core rather than adding AI as a bolt-on. For example, Hypershield 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.
- **Kernel-level enforcement:** Hypershield provides deep workload visibility and enforcement at the operating system level, which is native to the Linux kernel. This allows high-performance granular visibility into application process actions and the surgical control needed for security actions.
- **Self-qualifying updates:** Security requires high confidence and deliberate actions. Hypershield is designed to self-upgrade and update against changes. Administrators can reach targeted security postures faster with previews of policy updates and Hypershield software upgrades tested against the live production environment.

For more information, go to **cisco.com/go/hypershield**.

Use cases

Autonomous Segmentation

Modern security challenges demand more than traditional tools can offer. Current segmentation tools lack a deep understanding of the application (app) and try to baseline application behavior based on network flow observations across time—without considering app-specific events and how the app evolves with each new release. Traditional approaches can miss changes in application that result in higher application fragility. For this reason, organizations need a more effective segmentation approach to reduce their attack surface.

Hypershield's **Autonomous Segmentation module** transforms this process with a dynamic and intelligent segmentation model informed by a deep understanding of application behaviors and other critical inputs. This model continuously adapts based on observations and customer-defined policies, reducing the time and complexity traditionally associated with segmentation.

© 2024 Cisco and/or its affiliates. All rights reserved.

Distributed Exploit Protection

Security patches are a challenge for organizations today. Installing patches can disrupt business operations, leading companies to delay essential security updates for months to avoid downtime. Alternatively, mitigations require extensive manual effort for analysis, implementation, and testing while still carrying significant application uptime risks.

Hypershield addresses this by reducing the time it takes to protect against new vulnerabilities with its **Distributed Exploit Protection module**. This module automates the entire process—from detection, prioritization, and evaluation of controls to testing and deployment—ensuring applications continue running smoothly without interruption.

Product architecture

Tesseract Security Agent. This safe, high-performance enforcer sits in the workload, interfacing with processes and the operating system kernel through the extended Berkeley Packet Filter (eBPF). This end-system enforcer is optimized for easy deployment in Kubernetes environments and is also fully functional in non-Kubernetes settings. It offers deep visibility and enforcement within the workload, monitoring network connections, file and system calls, and kernel functions, and generates event-based telemetry.

Network-based enforcer. This enforcer is powered by a network-based appliance or virtual machine (VM). Moving away from traditional centralized enforcement approaches, the network-based enforcer is strategically placed close to the workload to protect specific assets more effectively. It offers network-based visibility, enforcement, and checks and self-qualifies updates using a digital twin of the data plane.

> **Dual data plane**. Traditional software upgrades to infrastructure or policy changes pose a high risk of disrupting business operations. These updates require significant time and resources to test, typically limiting them to a few times a year. This slow update cycle leaves organizations vulnerable to emerging threats with outdated defenses. Hypershield addresses this challenge with its dual data plane technology to check for and self-qualify updates using the network-based enforcer. This approach allows live production traffic to operate under current rules while simultaneously sending a copy of this traffic to a shadow data plane within the network-based enforcer. With this shadow plane, admins can test and validate new software upgrades or policy changes using live traffic and before deployment, all without impacting the production environment.
>
> With Hypershield's dual data plane, IT and security teams can deploy updates more frequently and with greater confidence, ensuring robust defenses against the latest threats without disrupting business processes.

Unified cloud management. Regardless of the enforcement point's form factor or location, Hypershield is architected to implement an intent-based policy model that is centralized and easy to manage. New or updated policies are "compiled" and intelligently distributed to enforcement points. Powered by Cisco Security Cloud Control (previously Cisco Defense Orchestrator) SaaS management, this system ensures administrators maintain a comprehensive overview of all deployed policies regardless of deployment in public or private clouds.

Unified control plane. Hypershield uses a secure control plane to link enforcers with the cloud management system, enabling smooth policy distribution across environments. Enforcers connect outward to Cisco's cloud service, simplifying deployment and firewall setup. Both sides verify each other's identity to prevent unauthorized access. The control plane allows two-way communication. Enforcers receive policies and updates while sending back security events and performance data. The control plane can manage thousands of enforcers across many locations, with resiliency via backups in case of network issues. This setup ties

© 2024 Cisco and/or its affiliates. All rights reserved.

Hypershield's components together from workloads to the cloud. It helps spread security policies and threat information quickly, maintaining consistent security everywhere.

AI-native security. Designed from the ground up with AI integration, Hypershield is built to earn trust through appropriate levels of autonomy, reporting, and control to deliver high efficacy, rapid response, and continuous protection. While the system can autonomously group workload objects like pods and containers, test, deploy, and manage its rules, the user has complete control and final authority. An AI assistant is also on hand to explain the analysis, observed behaviors, recommendations, and more.

Product features and benefits

Product Modules: Each module has been developed to solve a dedicated use case using the architecture components listed above.

Module	Feature/Benefit
Autonomous Segmentation	• **Application fingerprinting** - Workload classification and good data hygiene are the basis for successful segmentation and simplifying workload management. The system provides autonomous discovery, tagging, and grouping of workloads based on high-performance distributed analysis of all process and network actions. • **Simplified policy management** - Maintaining policy across data centers can be error-prone and time-consuming. Singular policy management allows segmenting across multiple enforcement points on public and private clouds. • **Deployment confidence score** - Deploy with confidence by knowing how policies, protections, and software updates would perform in real time. Before ever hitting "deploy," changes in CPU usage, memory usage, and latency against live production traffic can be compared.
Distributed Exploit Protection	• **Vulnerability detection** - Identify known security vulnerabilities in workloads by automatically scanning installed software against a database of Common Vulnerabilities and Exposures [CVEs]. • **Mitigation shields** - Protect applications against known vulnerabilities by automatically implementing precise mitigating security controls. This gives application teams time to properly test and deploy software patches without leaving systems exposed to attacks.

Product Architecture: The Cisco Hypershield architecture was built from the ground up with AI and offers both agent and agentless form factors all unified by a centralized cloud management platform.

Component	Feature/Benefit
Tesseract Security Agent	• **Kernel-level visibility and enforcement** - Get full visibility and control into the processes, network flows, and system I/O running inside of the workload all without breaking or modifying the application.
Network-based enforcer (Powered by Network Appliance/Virtual Machine)	• **Network-level enforcement** - Secure your east/west traffic using a Virtual Machine appliance with Layer 3 and Layer 4 network enforcement. • **Self-qualifying updates** (via Dual Data Plane) - Minimize time between update cycles by using the Dual Data plane to test and validate new firmware upgrades or policy changes using live traffic and before deployment; all without impacting the actual production environment.

© 2024 Cisco and/or its affiliates. All rights reserved.

Component	Feature/Benefit
Unified cloud management (Powered by Cisco Security Cloud Control)	• **Unified policy management and reporting** - Organize and manage all policies from a centralized place regardless of an enforcement point's form factor or location. • **Simplified, scalable policy** - Simplify and automate policy management by using an intent-based policy model that compiles and distributes policies at scale across enforcement points. • **Policy testing** - Increase confidence in recommended policies by self-qualifying those policies against live traffic before deployment.
AI-native security (Powered by Cisco Security Cloud Control)	• **AI-powered analysis** - Visualize relationships between workload actions ranging from network, process, protocol, port, file inspection, and application behavior, among others. • **Cisco AI Assistant** - Access the breadth and scale of Hypershield data to guide and inform faster decision-making more intelligently.

Subscription requirements

Cisco Hypershield's subscription price is based on the quantity of Protection Units purchased. A Protection Unit is a unit of allocation that entitles the deployment of Hypershield components in a network. A minimum of 100 Protection Units is required for an active subscription. Customers may re-assign their Protection Units at any time and purchase additional Protection Units during their active subscription term. The allocation of Protection Units can be monitored within the Hypershield module found in Cisco Security Cloud Control.

Depending on the use case, enforcement can happen at different places in the network, using a varying number of units:

Enforcer Type	Deployment	Protection Unit Cost
Tesseract Security Agent	Linux workload VM	12 units per deployment
	Kubernetes node (each 16 vCPU, 64 GB RAM)	36 units per deployment
Network-based enforcer	VM Appliance	36 units per deployment

Deployment models and scale

Hypershield can be deployed based on enforcement needs and flexibly scaled up/down. The product can be deployed in the below variants:

Enforcer Type	Deployment	Specification
Tesseract Security Agent	Linux workload VM	An agent deployed at the Linux workload VM
	Kubernetes node (each 16 vCPU, 64 GB RAM)	An agent deployed at the Kubernetes node
Network-based enforcer	VM Appliance	A virtual image of a network enforcement point

© 2024 Cisco and/or its affiliates. All rights reserved.

Software subscription model

Hypershield units allow for enforcement across the above enforcement points.

Feature	Essentials
Modules	
Autonomous Segmentation Module	
Application fingerprinting	✓
Simplified policy management	✓
Deployment confidence score	✓
Distributed Exploit Protection Module	
Vulnerability detection	✓
Mitigation shields	✓
Architecture	
Tesseract Security Agent	
Kernel-level visibility and enforcement	✓
Network-based enforcer	
Network-level enforcement	✓
Self-qualifying updates (via Dual Data Plane)	✓
Unified cloud management	
Unified policy management and reporting	✓
Simplified, scalable policy	✓
Policy testing	✓
AI-native security	
AI-powered analysis	✓
Cisco AI Assistant	✓

© 2024 Cisco and/or its affiliates. All rights reserved.

Support and compatibility

Below are the recommended Linux and Kubernetes distribution releases for Hypershield.

Linux Distribution	Minimum Kernel Version
Ubuntu 22.04 LTS	5.15
Ubuntu 20.04 LTS	5.4
Red Hat Enterprise Linux 9	5.14
Fedora 38	6.3
Debian 12	6.1
Debian 11	5.10
Arch Linux	6.4
CentOS Stream 9	5.14

Kubernetes Distribution	Minimum Kubernetes Version
Amazon Elastic Kubernetes Service (EKS)	1.23

AI and privacy

Responsible AI

At Cisco, we appreciate that Artificial Intelligence (AI) can be leveraged to power an inclusive future for all. We also recognize that by applying this technology, we have a responsibility to mitigate potential harm. That is why Cisco adheres to our Responsible AI Framework (the "Framework"), which is based on six principles of Transparency, Fairness, Accountability, Privacy, Security, and Reliability. Cisco translates these principles into product development requirements, which ultimately form part of the product development lifecycle alongside our Security by Design, Privacy by Design, and Human Rights by Design processes.

Accordingly, Cisco Hypershield as a AI-native solution was built with transparency, fairness, accountability, privacy, security, and reliability at its core. Every feature and module powered by AI is subject to an AI Impact (AII) Assessment –a best-in-class review of how the technical underpinnings of the functionality measure against the Framework principles.

To learn more, visit the Responsible AI webpage.

Data Privacy

Cisco Hypershield Privacy Data Sheet

Cisco Security Cloud Control (previously Cisco Defense Orchestrator) Privacy Data Sheet

© 2024 Cisco and/or its affiliates. All rights reserved.

Cisco environmental sustainability

Information about Cisco’s environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the “Environment Sustainability” section of Cisco’s Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the “Environment Sustainability” section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about Cisco Hypershield, please visit https://www.cisco.com/go/Hypershield or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C78-4789245-00 10/24