Cisco Hypershield

Cisco Partner
https://cs.co/1page

Cisco Hypershield is a security architecture that makes hyperscaler technology accessible to enterprises and delivers AI-native security for modern data centers and cloud. Hypershield places control points (e.g. switch ports, DPU enabled servers etc.), to enforce different capabilities and policies not possible to configure manually.

Benefits:

Deep Visibility and surgical control at the workload level

Machine Learning and Analysis of the relationships between the application process, file, and network operations against Common Weakness Enumeration (CWE) database, which is a classification system for hardware and software security weaknesses

Analysis of the Application process graph and known application behaviors to classify suspicious or malicious activity

Block Application Exploits in Minutes. Employs compensating controls that are evaluated and tested against live production traffic for optimal effectiveness

Protects Everywhere. Implement a hyper-distributed security approach that reaches all areas of your network, tapping into a broad range of previously unreachable workload and network enforcement points

Achieve Effective Segmentation that continuously adapts and learns. Applied to highly specific controls, even down to regex filtering, ensuring tailored security

Unified Management across the network and workloads. Deploy software and policy updates with confidence using a dual data-plane approach, enabling safe testing on live traffic without risking your operations

FAQs:

Q: What platforms will Hypershield support at GA?
A: The Tesseract Security Agent (TSA) will be supported on Linux-based systems (kernel version 5.14+). This includes Kubernetes systems. In the case of Kubernetes, the TSA can be installed on the Kubernetes Nodes, and its capabilities made available to resident Kubernetes Pods on these Nodes. These Nodes could be VMs or bare-metal based.

Q: What does eBPF stand for?
A: extended Berkeley Packet Filter goes beyond just “packets” or “filtering”

Q: How will Hypershield help manage security in a unified way?
A: Hypershield will leverage Security Cloud Control (SCC).

Q: How does Hypershield impact existing solutions like Cisco Secure Workload?
A: See Secure Workload and Hypershield co-positioning

Key Components:

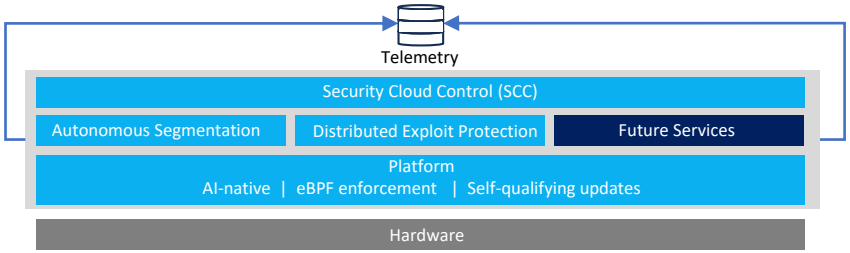
Workload agent (Tesseract Security Agent) provides deep visibility into the application forensics and workload behavior while reporting and enforcing the network, process, and file artifacts surrounding the app and workloads.

Network-based enforcer that provides an agentless means to visibility and enforcement in situations where an agent cannot be installed.

The **Unified control plane** is used to link enforcers with the cloud management system, enabling 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.

Dual Data Plane is used to deploy self-qualifying updates. The technology can be used to test and deploy software upgrades at the network-based enforcer or to do the same for policy updates across both workloads and the network enforcement points. Can be used to validate new software upgrades or policy changes using live traffic before deployment.

Hypershield's **AI-native security** 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 write, test, deploy, and manage its own rules, the user can have full control to achieve desired results and gather additional insights.



Resources:

SalesResources	Data Sheet	FAQ’s	Call Guide
Ordering Guide	Solution Overview	Security Cloud Control	Public page

Example SKU: ***HYPRSHLD-SEC-SUB*** | ***HYPRSHLD-ESS***