Cisco Hypershield Release Notes

First Published: 2024-10-31

Last Modified: 2025-01-16

Hypershield Release Notes

This document lists system requirements, new features, and open and resolved bugs.

Requirements for Hypershield

Hypershield for Security Cloud Control

You need a Security Cloud Control tenant with Hypershield enabled. See https://manage.security.cisco.com/provision to request a tenant. Contact your Cisco representative to enable Hypershield for your tenant.

Tesseract Security Agent

An agent installed on Linux in a standalone or Kubernetes deployment.

Table 1: Supported Linux Distributions

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

Table 2: Supported Kubernetes Distributions

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

Network-Based Enforcer

- Virtual Machine installed on Amazon Web Services (AWS).

Licenses

A subscription for a quantity of "protection units" is required. Each agent and enforcer requires the following units:

Table 3: Protection Units per Asset

Asset	Protection Units
Tesseract Security Agent	• Standalone—12 • Kubernetes node—36
Network-Based Enforcer	36

New Features

New Features in Hypershield October 31, 2024

Feature	Minimum Network-Based Enforcer Version	Minimum Tesseract Security Agent Version	Description
Platform			
Hypershield for Security Cloud Control	—	—	The Hypershield control plane and management plane are accessed through Security Cloud Control.
Tesseract Security Agents for Linux	—	1.3.4	The agent provides workload visualization and mitigation of workload vulnerabilities at the kernel level using the extended Berkeley Packet Filter (eBPF). eBPF is open source and native to the Linux kernel.
Network-Based Enforcers for Amazon Web Services	1.1.0	—	The network-based enforcer is a transparent, stateful virtual firewall that provides network segmentation and network security policy.
Security Policy			

Feature	Minimum Network-Based Enforcer Version	Minimum Tesseract Security Agent Version	Description
Unified policies	1.1.0	—	Hypershield deploys policies to all enforcers. All policies are evaluated, and the order doesn't matter. A block policy will always take precedence over a permit policy. By default, enforcers block all traffic unless you deploy a policy to permit traffic.
Manual policies using 5-tuple (source IP address/port number, destination IP address/port number, and the protocol), VLAN, and SGT	1.1.0	—	You can manually create policies that will be deployed to the enforcers.
Verification			
Dual data plane	1.1.0	—	A shadow data plane, with a copy of your traffic from the primary data plane, lets you test policy changes or system updates to make sure you don't unintentionally cause a network outage, for example. Hypershield tests the policies or update against useful measures and suggests a confidence score for the deployment or update.
Visualization and Guidance			
Visualization for all workloads	—	1.3.4	The Tesseract Security Agent on each node or VM keeps track of one or more workloads (a process or application) and sends telemetry to Hypershield so you can see all of the workloads for your entire network. Using that information, you can create enforcer policies as needed.
Cisco AI Assistant	—	—	The AI Assistant intelligently guides and informs decision-making.

Open Bugs

Table 4: Open Bugs

SHIELD-715	When refreshing an empty list of policy-groups, it takes 8 seconds and we see different view
SHIELD-718	When in policy-group view and using the Hypershield drop down menu the view does not change
SHIELD-719	Policies don't populate createdBy field
SHIELD-720	Setting character limitations for naming policies and objects
SHIELD-817	[TSA] Graph did not appear after 15 minutes
SHIELD-822	[TSA onboarding] Update UI for K8s cluster installation
SHIELD-867	[TSA] Discard changes pop-up does not appear
SHIELD-882	[TSA] There is an ability to edit agent name to 'space' symbol
SHIELD-886	[TSA] Discard of TSA provisioning does not redirect to the initiated page
SHIELD-939	TSA installation on t2-micro sometimes fails
SHIELD-941	Process graph from OpenShift may sometimes cause browser hang
SHIELD-951	Cancel button does not work on Install Network-based Enforcer screen
SHIELD-994	Follow-up verification requests not hitting agent after previous fail
SHIELD-1008	Send CP Reset when Policy Group testing fails
SHIELD-1035	[TSA Graph] Right panel > Fix detail spacing and process collapse component font style
SHIELD-1053	Dual Data Plane: Latency difference is showing -100% for old netflows
SHIELD-1054	Dual Data Plane: Hits on primary data plane is showing 0 for running TCP session