

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco Hypershield

A new era of AI-native security for data centers and cloud

Aamer Akhter
Director, Product Management
BRKSEC-1501



#CiscoLiveAPJC

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1501>





Cybersecurity basics are tough

Cybersecurity fundamentals remain elusive in today's complex enterprise IT environment

Segmentation is challenging

- Explosive workload growth
- Inconsistent enforcement
- Environments keep changing

Patching is hard

- High vulnerability rate
- Mitigation is too slow
- Ensure app is available

Change is risky, expensive

- Firmware updates delayed
- Policy changes are behind
- Delayed security posture

Cisco Hypershield



Cisco Hypershield puts security where you need it

Public Cloud



C L O U D N A T I V E
S E R V I C E S

AWS | Azure | Google

Private Cloud



S W I T C H /
S E R V E R



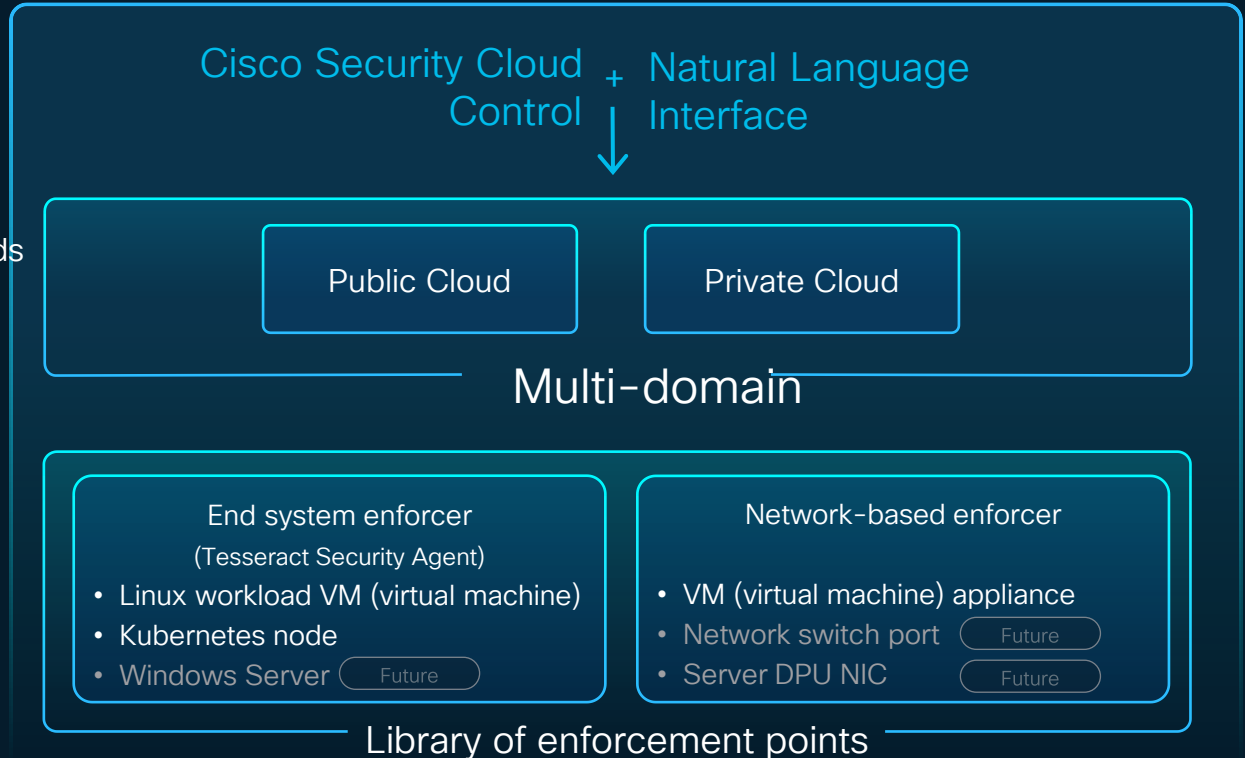
Manage globally, enforce locally

Includes

- Unified management
- Single global policy
- Intelligent placement of shields
- Integrations with cloud/app/infra metadata

Environments

- Kubernetes
- Cloud – Private/Public
- On-prem



Cisco Hypershield



Cisco Security Cloud Control

Simplify operations

Centralize control of devices and policies

Enhance security

Leverage AI to strengthen protection and prevent downtime

Increase efficiency

Reduce time spent on manual tasks up to 90%

cisco *Live!*

Security Cloud Control

Search

Admin PseudoCo

Dashboard

Top insights & alerts 10 new insights

Elephant flow spike observed

Data sources: FTD

Traffic has risen steadily over three weeks with some large flows consuming excessive bandwidth, necessitating intervention to avoid performance issues.

Last 24h [Details](#)

Risky users accessing privileged apps

Data sources: FTD, Secure Access

Implement ZTNA to limit access to only required user groups, and protect your applications from risky users.

Last 24h [Details](#)

1% Decrypted traffic towards internet

Data sources: FTD

Failure to decrypt a significant portion of traffic poses a severe security risk, potentially concealing malicious activities, leaving your network vulnerable to threats.

Last 24h [Details](#)

Top actions

Policy optimizer

Data sources: FTD

18263 Rules with anomalies 5723 Shadowed

30524 Total rules

- 18263 Rules with anomalies (60%)
- 515 Disabled rules (17%)
- 79 Expired rules (10%)
- 11667 Healthy rules (38%)

[Details](#)

Top information

Workload protection status

Data sources: Hypershield

Last 90 days

400k Total assets

20k Vulnerable

320k Protected

60k Improvements recommended

8 Vulnerabilities
60k Exploitable assets

8 Shields verified
Ready to deploy

12 Recent protections
Auto-deployed

Change Log Management

Data sources: All, FTD, ASA, Multicloud, Hypershield

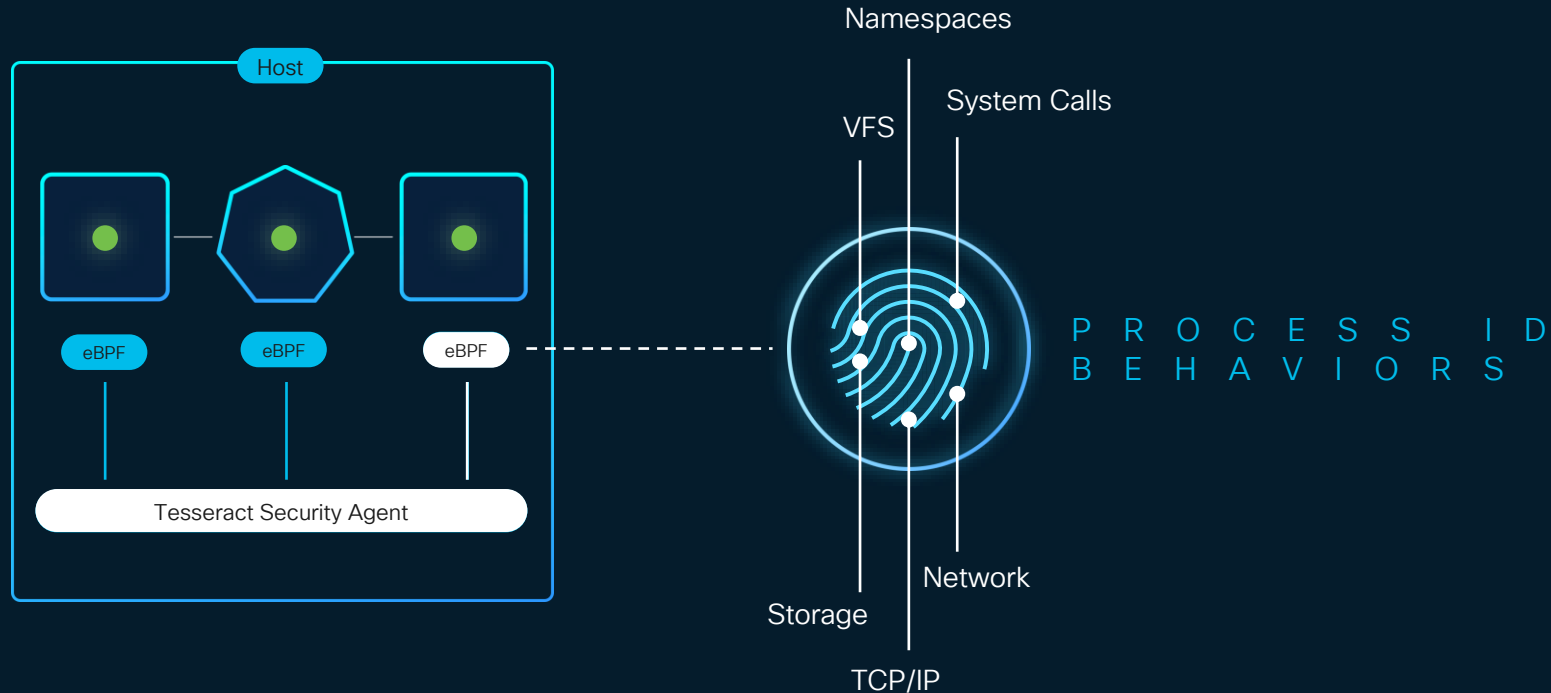
Last 90 days

Changes by all users | My changes

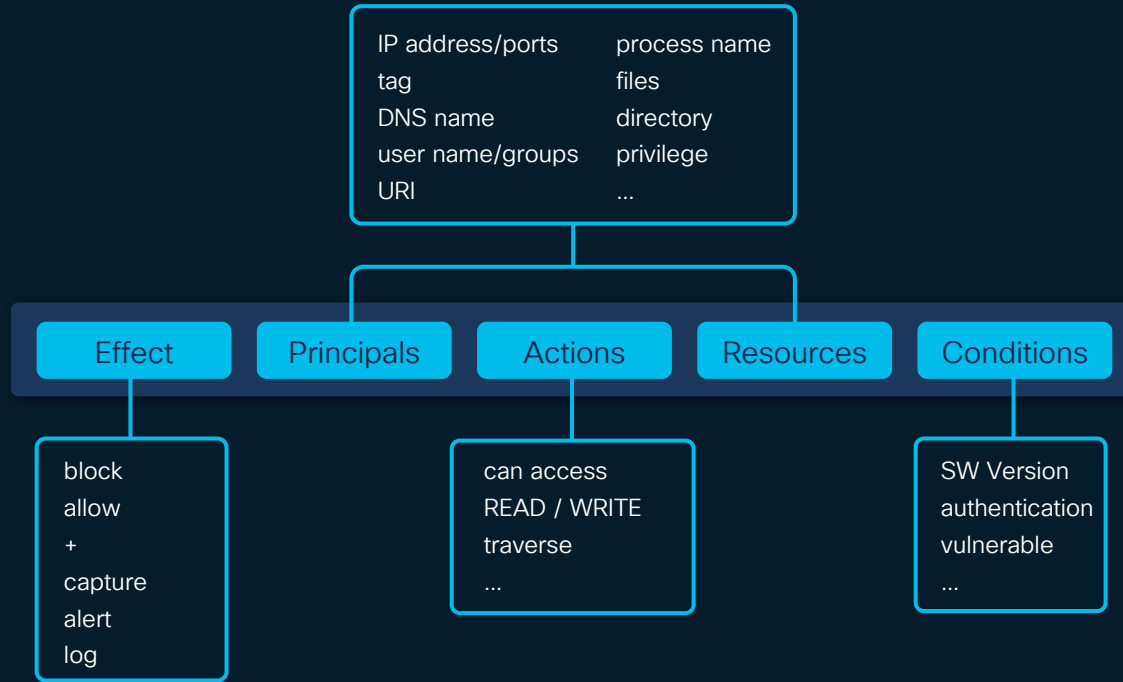
Device name	Last description	Last user
connected_fmc	—	System user
Corporate Duo	Successfully imported out-of...	System user
fmc-fulton-10.10.5.107	Read FMC records successfully	System user
connected_fmc	Read policy successfully	System user
fmc-fulton-10.10.7.110	Read policy successfully	System user

[View All Changes](#)

Deep visibility and enforcement in the workload built on Isovalent Tetrason



Single policy covering network and workload



Hypershield Policy Construct

- AWS Cedar inspired/adapted
- Intent based
- Order independent
- Auto-compiled to rule

Putting policy into practice with AI

AI generated rule blocking a vulnerable container process

The screenshot shows the 'Distributed Exploit Shield' interface. It includes a description of the shield's purpose, a table of statistics, and a detailed policy configuration. Blue arrows map specific fields to a structured policy representation on the right.

Field	Value
Time Hypershield created	1 hour from known exploit
Confidence Score	95%
Assets shielded	16,234
Created on	Jul 8 2024

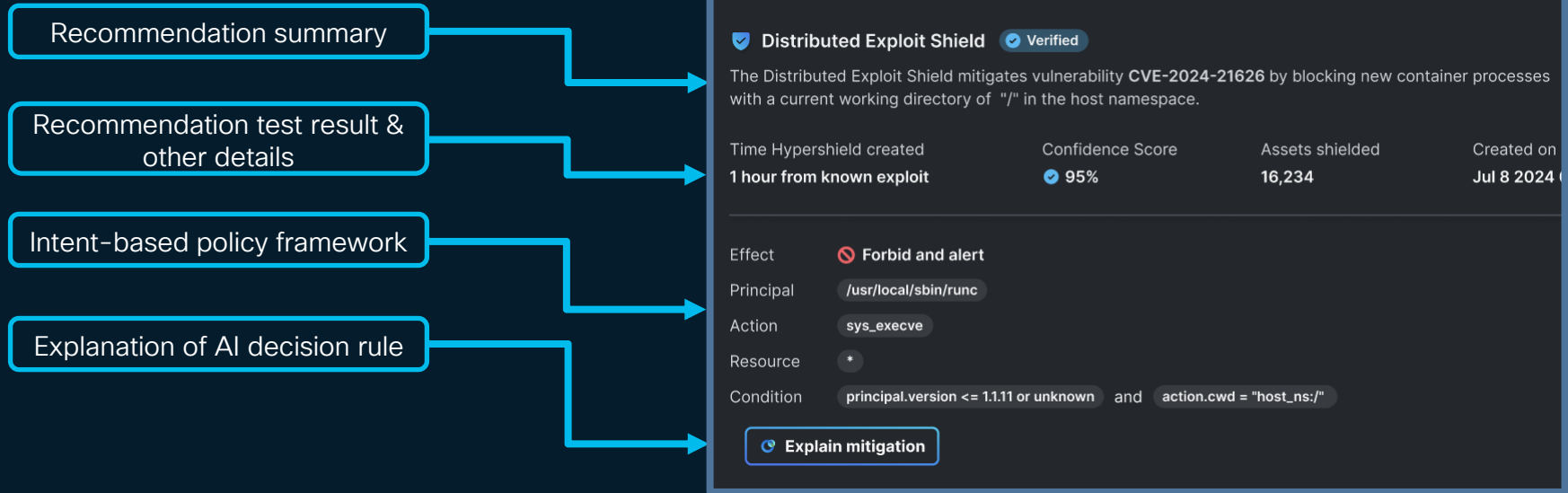
Field	Value
Effect	Forbid and alert
Principal	/usr/local/sbin/runc
Action	sys_execve
Resource	*
Condition	principal.version <= 1.11 or unknown and action.cwd = "host_ns:/"

[Explain mitigation](#)

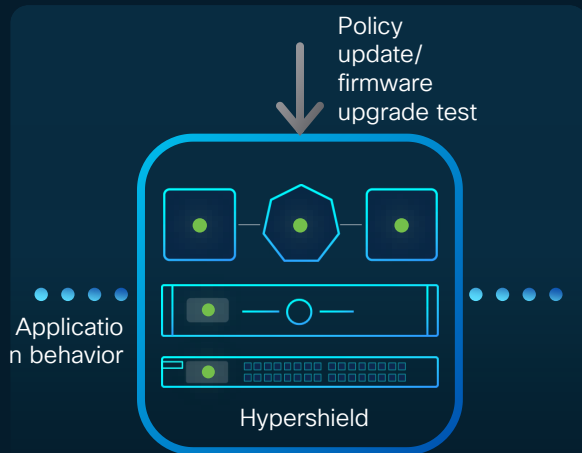
Policy Component	Value
Effect	Forbid & Alert
Principals	File path / executable
Actions	Execute Permit
Resources	* (act on any resource)
Conditions	Minimum version & namespace

Putting policy into practice with AI

Confidence & Trust



Improve security posture with self-qualifying firmware and policy upgrades



Test

Firmware and policy changes validated against customer environment

- 1) Technical design  AI-approved
- 2) Security review  AI-approved
- 3) Change request  AI-approved
- 4) Business approval  Approval needed

The application affected by these changes is the **Finance app**.
The app owner's approval is needed due to the high risk of the affected application.
Drew has been identified as the app owner of Finance app.

Review

AI system evaluates change.
Admin controls promotion



Deploy

Hitless deployment with single click, enabling teams to move fast with confidence

Note: Images are not an exact product UI representation

Changes can be validated on your live, production environment

Network-based enforcer's dual data plane: Earning your trust

Primary Data Plane

VERSION 2.0

VERSION 2.1

Shadow Data Plane

Self qualifying software updates

Primary Data Plane

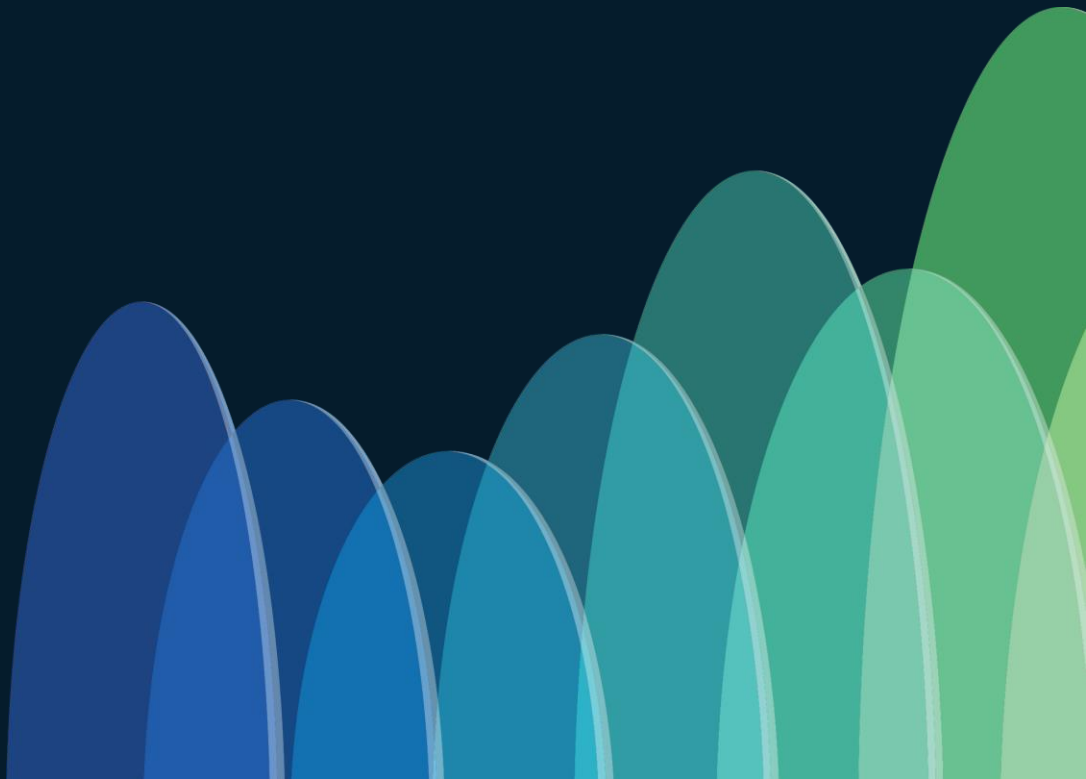
DEPLOYED POLICY

POLICY GROUP A

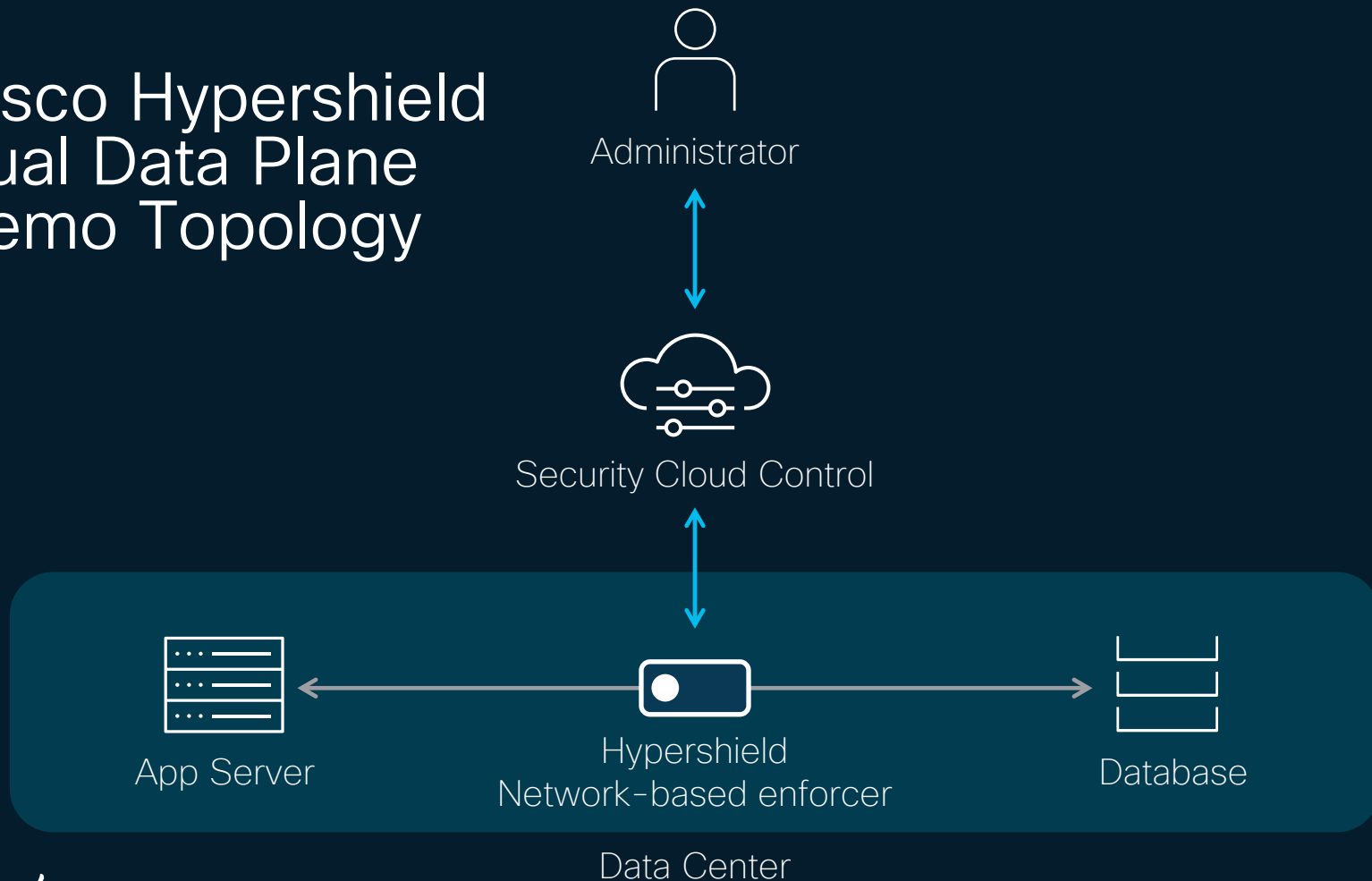
Shadow Data Plane

Policy verification, exploit protection test

Dual Data Plane Demo



Cisco Hypershield Dual Data Plane Demo Topology



- Hide Menu
- Dashboard
- Multicloud Defense
- Hypershield New
- Inventory
- Configuration
- Policies
- Objects
- VPN
- Events & Monitoring
- Analytics
- Change Log
- Jobs
- Tools & Services

Firewall Agents

Firewall Agents Update History

Status	Name	Version	Updated at	Updated by
 Active	Lab Firewall	11.0~g75e52ad7~t20240618185733	8/26/2024, 12:16:03 PM	hyperlab@CDO_cisco-daf-ea-demo

app-server

lab.cisco-daf-ea-demo.hypershield.cloud/console/#/client/YXBwLXNlcnZlcnBjAGRIZmF1bHQ

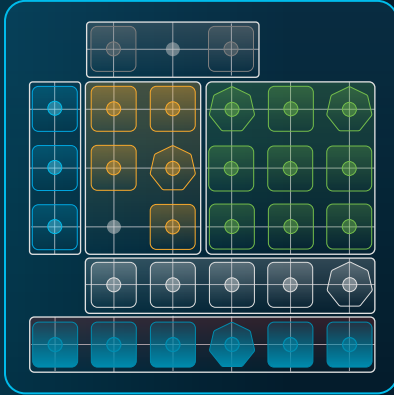
Expanded Security Maintenance for Applications is not enabled.

11 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at <https://ubuntu.com/esm>

Last login: Mon Aug 26 19:13:05 2024 from 10.0.10.10
hyperlab@app:~\$
hyperlab@app:~\$
hyperlab@app:~\$
hyperlab@app:~\$
hyperlab@app:~\$

Cisco Hypershield use cases



Autonomous Segmentation

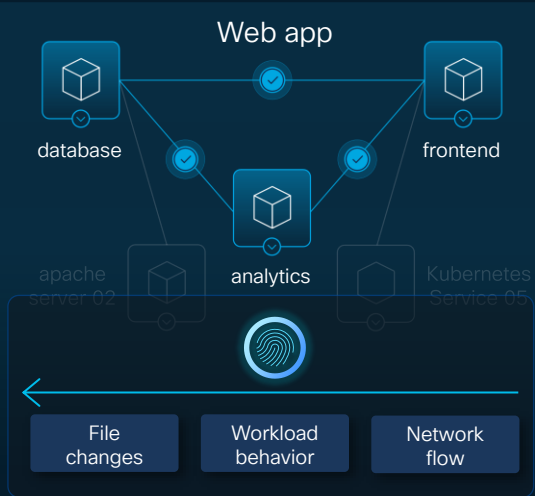
- Deep understanding of app behavior
- Comprehensive inputs for policy creation
- Constantly adapting to changing apps



Distributed Exploit Protection

- Mitigate known and unknown vulnerabilities
- Surgical mitigating controls
- Protection within minutes, while app keeps running

Segmentation that is effective and keeps up with changing applications

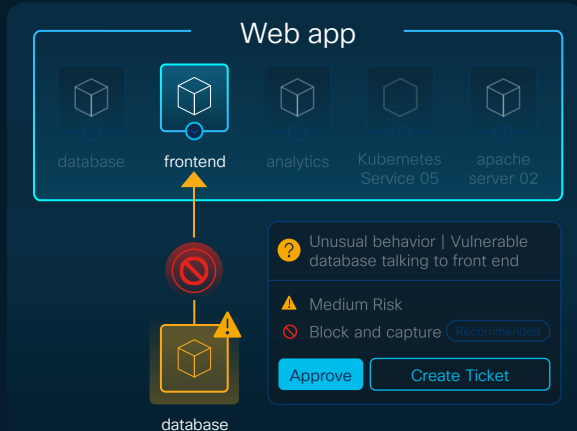


Complete understanding of changing app behavior from network to workload to pre-prod

Recommendations

- ✓ Permit web app frontend can access database ✓
- ✓ Permit web app frontend can access analytics ✓
- ✓ Permit web app analytics can access database ✓
- ✓ Default observe and permit web app policy group... ✓

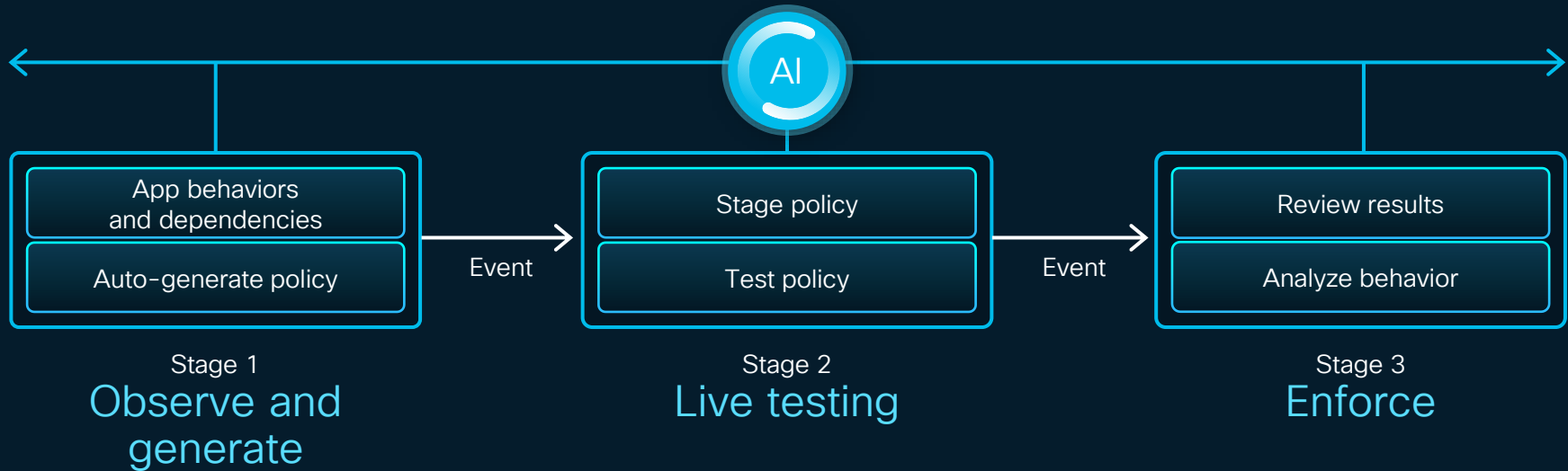
Flexible segmentation rules that help avoid app fragility



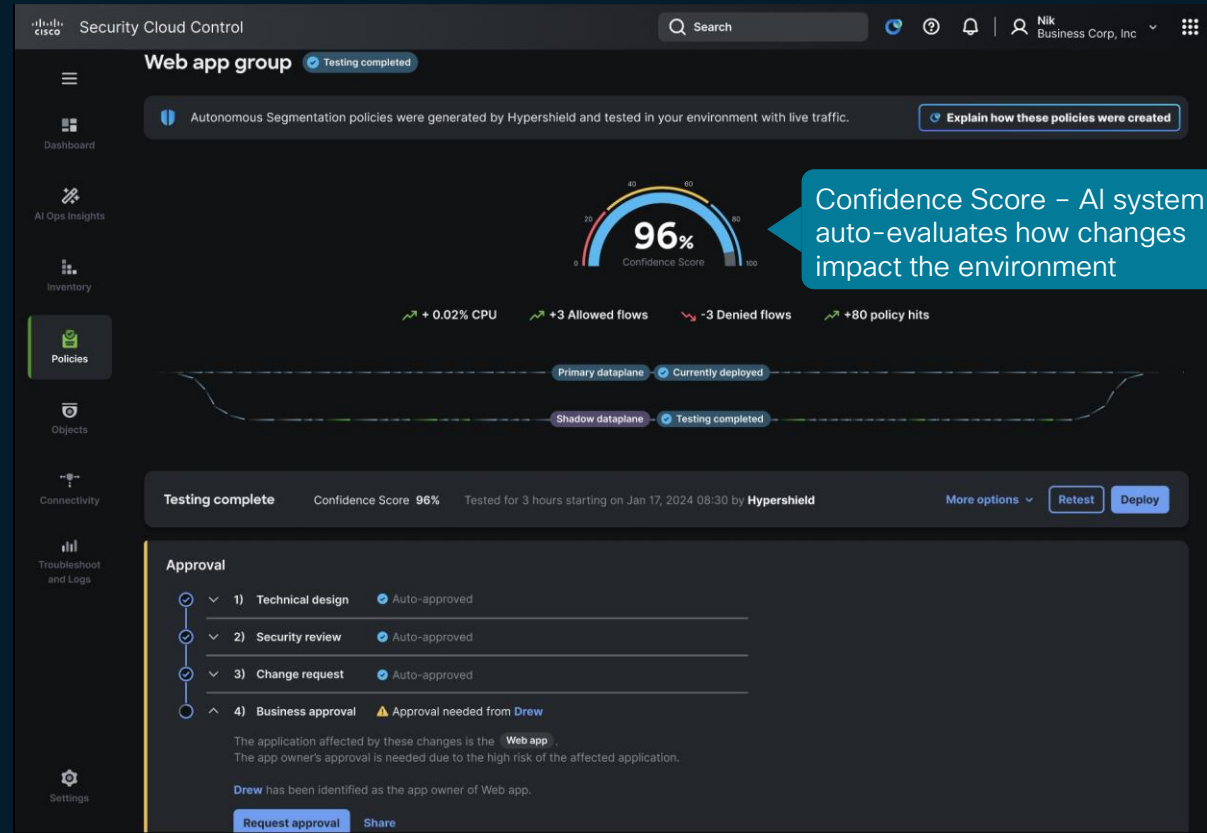
Policies updated to stricter rules in response to suspicious events

Note: Images are not an exact product UI representation

A policy lifecycle that earns your trust

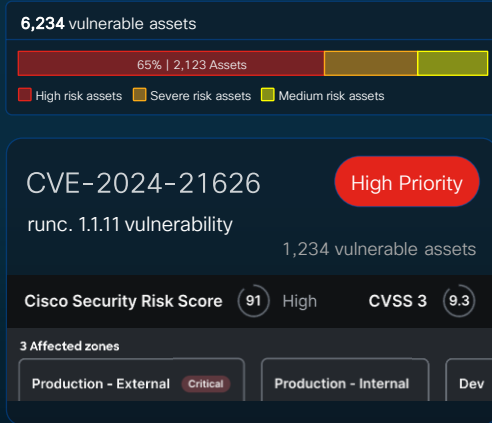


Autonomous segmentation policies generated and tested with live traffic

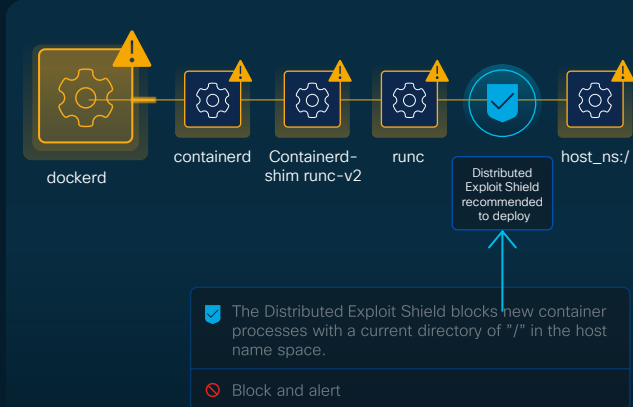


Confidence Score – AI system auto-evaluates how changes impact the environment

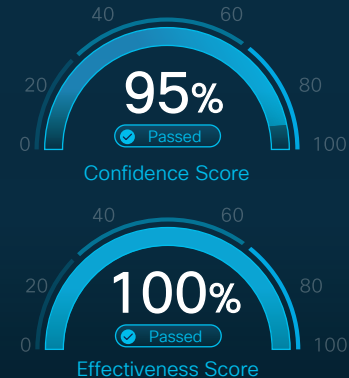
Close the exploit gap against growing vulnerabilities with automated workflows



Complete view of the vulnerabilities, prioritized by severity and critical business flows



Surgical mitigating control in the path of the process that keeps application running



The Distributed Exploit Shield was already tested in your environment

Tested against live production traffic to earn trust and increase confidence

Note: Images are not an exact product UI representation

Vulnerability detection

Identify known **software** vulnerabilities (CVEs)

Mitigation shields

Protect applications by automatically implementing precise mitigating security controls

Tesseract Security Agents + Install Tesseract Security Agents

Q Search

Agent status	Name	Asset security status	Number of vulnerabilities	
Connected	ip-172-31-17-204.ec2.internal	Exploitable	1	...
Connected	ip-172-31-17-210.ec2.internal	No vulnerabilities	0	...
Connected	ip-172-31-32-70.ec2.internal	No vulnerabilities	0	...

← Tesseract Security Agents

ip-172-31-17-204.ec2.internal Exploitable Delete Edit Refresh

Node

Data Vulnerabilities

Q Search Deploy

Status	Vulnerability	CVSS v3	Mitigation
Exploitable	CVE-HS-TEST	9.5 Critical	Ready to deploy

← Vulnerability

CVE-HS-TEST Mitigated Refresh

Description CVSS v3 9.5 Critical

Test vulnerable package for testing.

Remediation

Distributed Exploit Shield

Created on 10/17/2024, 5:51:05 PM Updated on 10/17/2024, 5:51:05 PM

Effect Forbid and warn

Principal package:hs-test

Action security_bpm_check

Resource book_string:undefined

Condition principal.version <= 1.0.0

Q Search

Security status	Name	Agent status
Shielded	CVE-HS-TEST	Connected

Hypershield helps deliver business outcomes

Accelerated
security
protection

Higher
security
efficacy

Reduced
outage
downtime

Lower
barrier to
expertise

Let's get started

Cisco Hypershield

Cisco Hypershield resources:

- Learn more at <https://cisco.com/go/hypershield>
- Read the [Solution Overview](#)
- To keep up-to-date on product news, demos and more, sign up [here](#)
- Engage with your Cisco team today!

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC