

Cisco Hypershield

Distributed Workload Security across Hosts and Smart Switches

Aamer Akhter
Sr. Director, Product Management, Cisco

cisco Live !

Session ID: BRKSEC-1501

Cisco Webex App

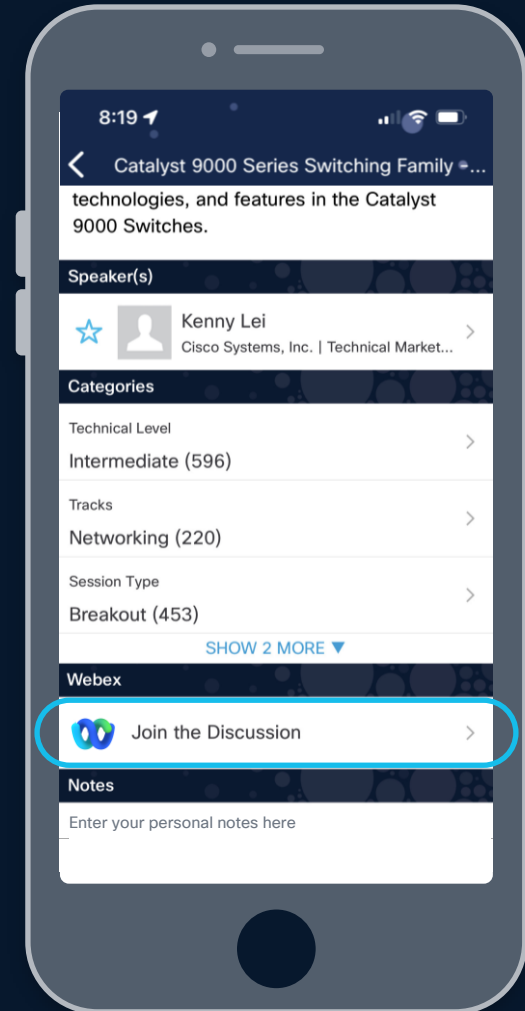
Questions?

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 14 November 2025.



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

Agenda

- 01 Market Trends & Challenges
- 02 Issues with Today's Implementation
- 03 Cisco Hypershield
- 04 Differentiations
- 05 Q&A

The perfect storm

130 vulnerabilities/day
+16% YoY

30% weaponized within 24h
Before you can respond

70% use lateral movement

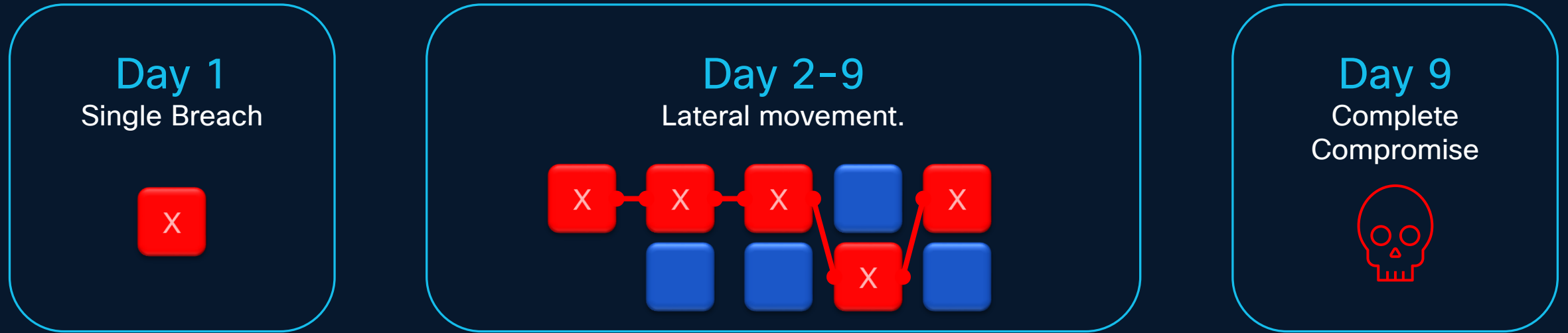
\$4.88M avg breach
Board-level reputational risk, regulatory exposure

Defense gap

- Centralized architecture → blind spots
- 60-day patch cycle → persistent exposure



Feb 2024: The most expensive health care breach in history



Stolen from

100M people

- Personal data
- Health records
- Financial information

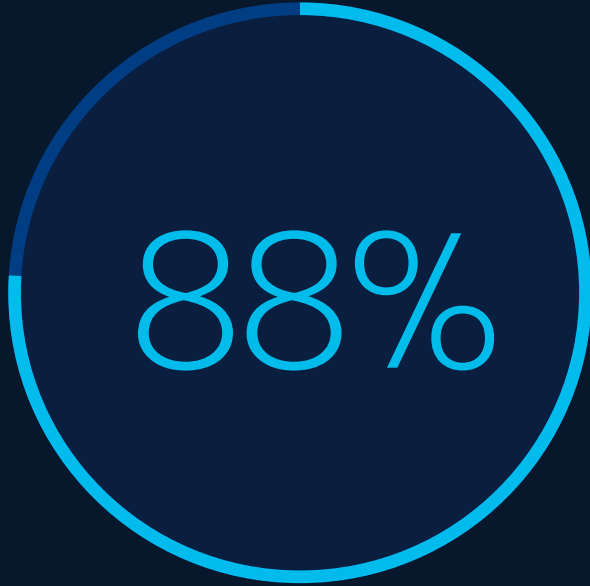


\$22M
ransom paid

\$2.5B
total cost

The gap: No segmentation → No containment

Security's visibility crisis

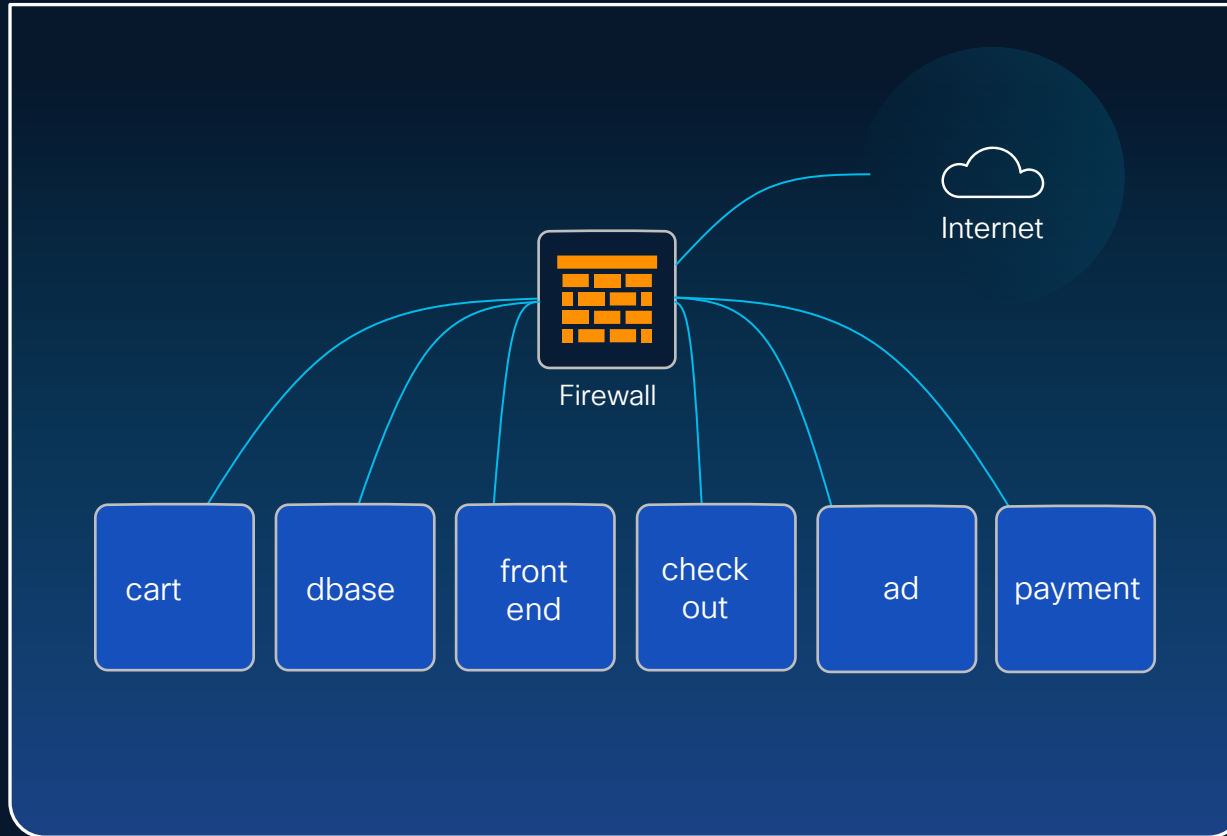


lack critical visibility to make
informed security decisions

Resulting in critical blind spots

- Undetected lateral movements
- Policy enforcement gap
- Unpatched and noncompliant workloads

The segmentation gap

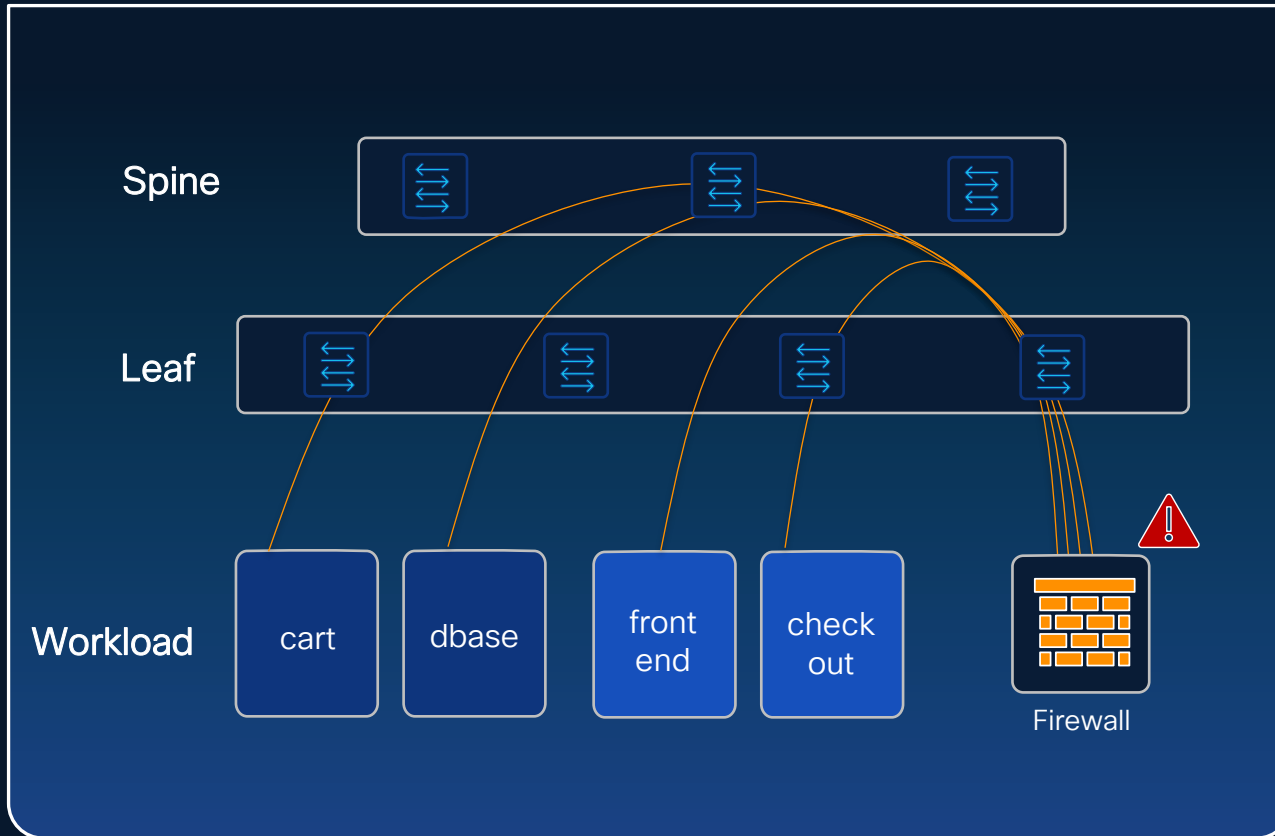


Firewalls are essential for north-south traffic...

... but stopping lateral movement requires more

- Policies can't scale with dynamic infrastructure
- Visibility ends at the perimeter
- Lateral movement goes undetected

Traditional architecture creates east-west bottlenecks



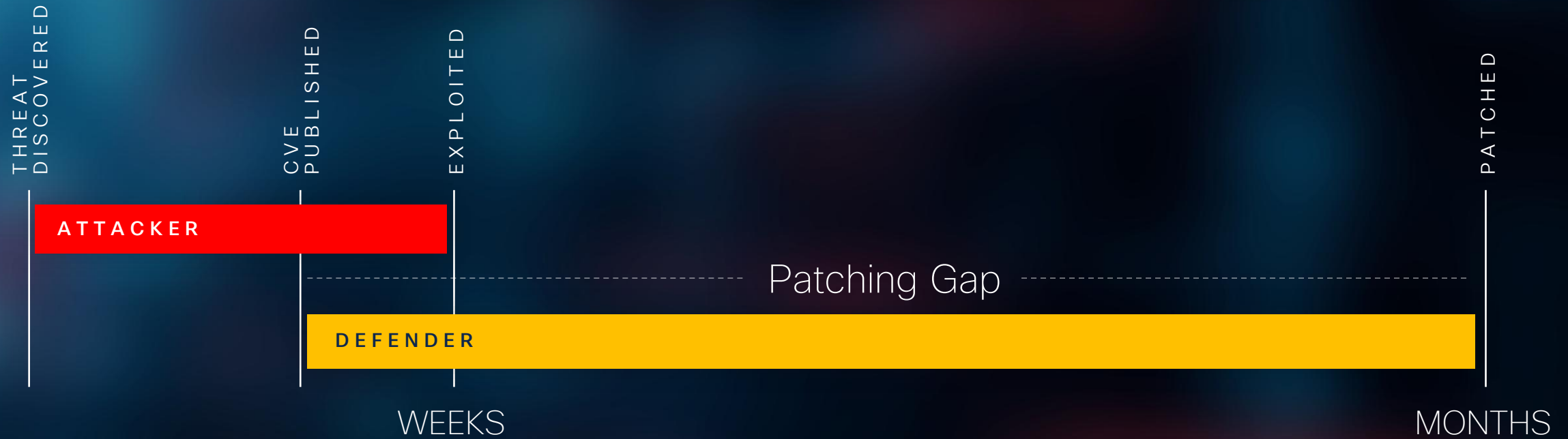
Firewalls excel at perimeter defense and compliance

- IPS/IDS
- URL Filtering
- NAT, Identity, others.

But **lateral traffic defense** needs a different approach

- Hair pinning adds latency
- Architectural limits create visibility gaps
- Scaling east-west security is costly

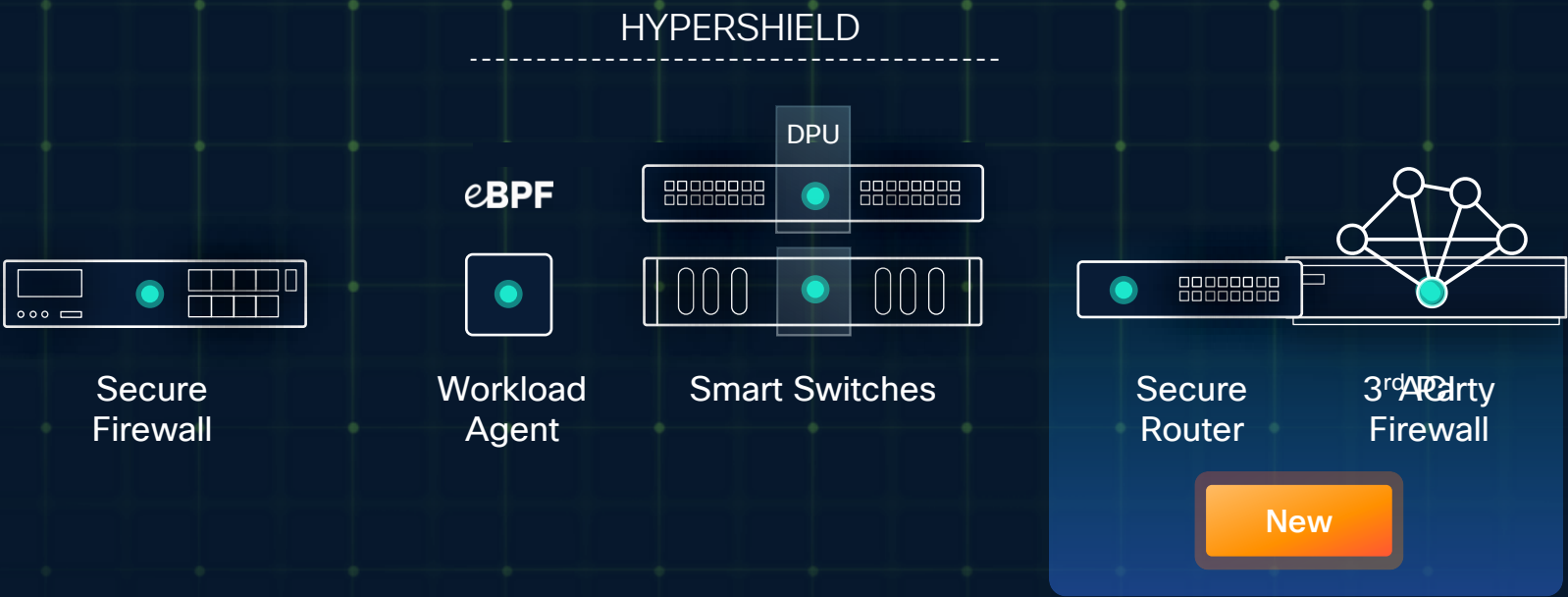
Patching is hard



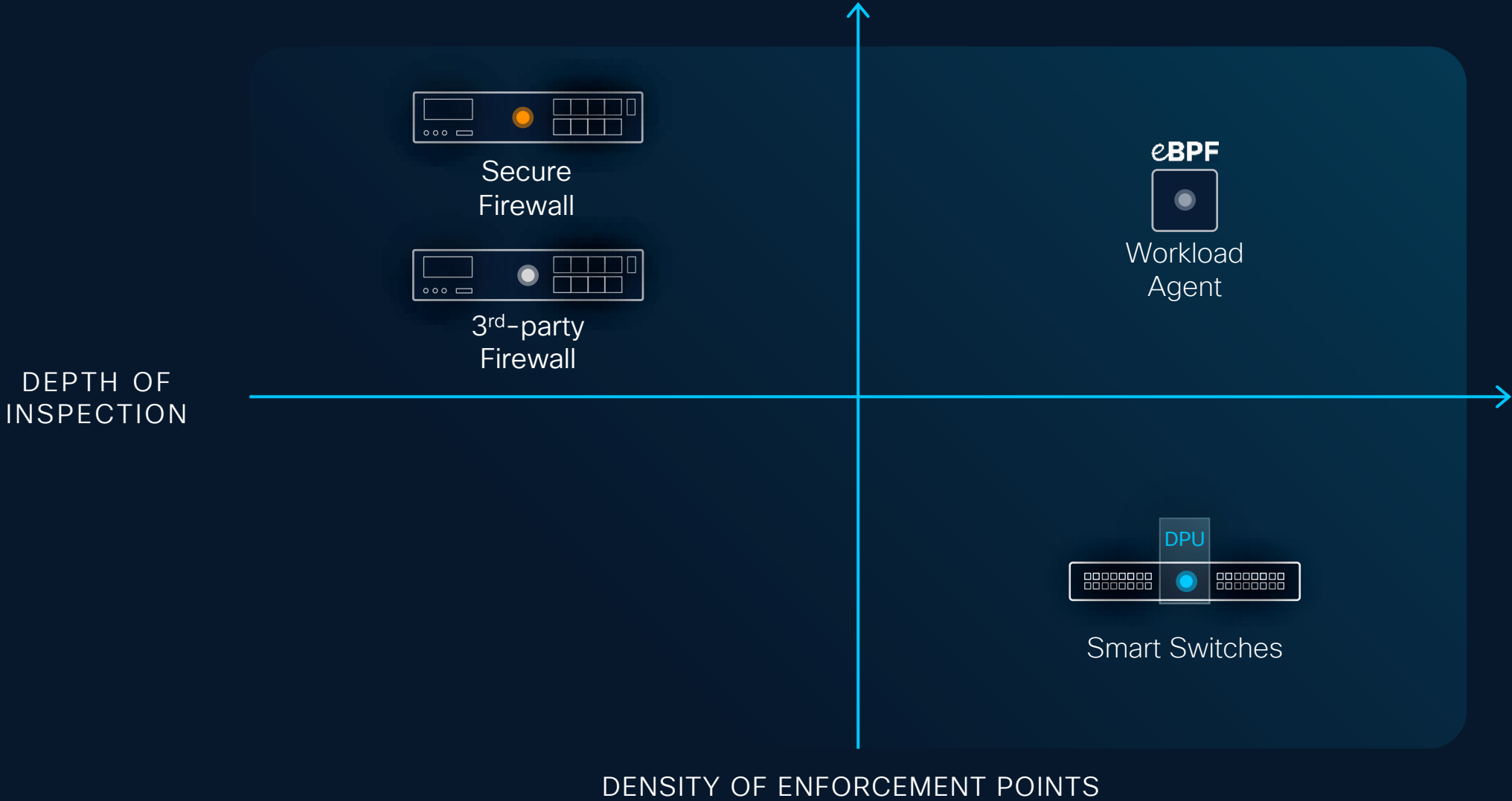
Solution – Hypershield

Cisco Hybrid Mesh Firewall

SECURITY CLOUD CONTROL



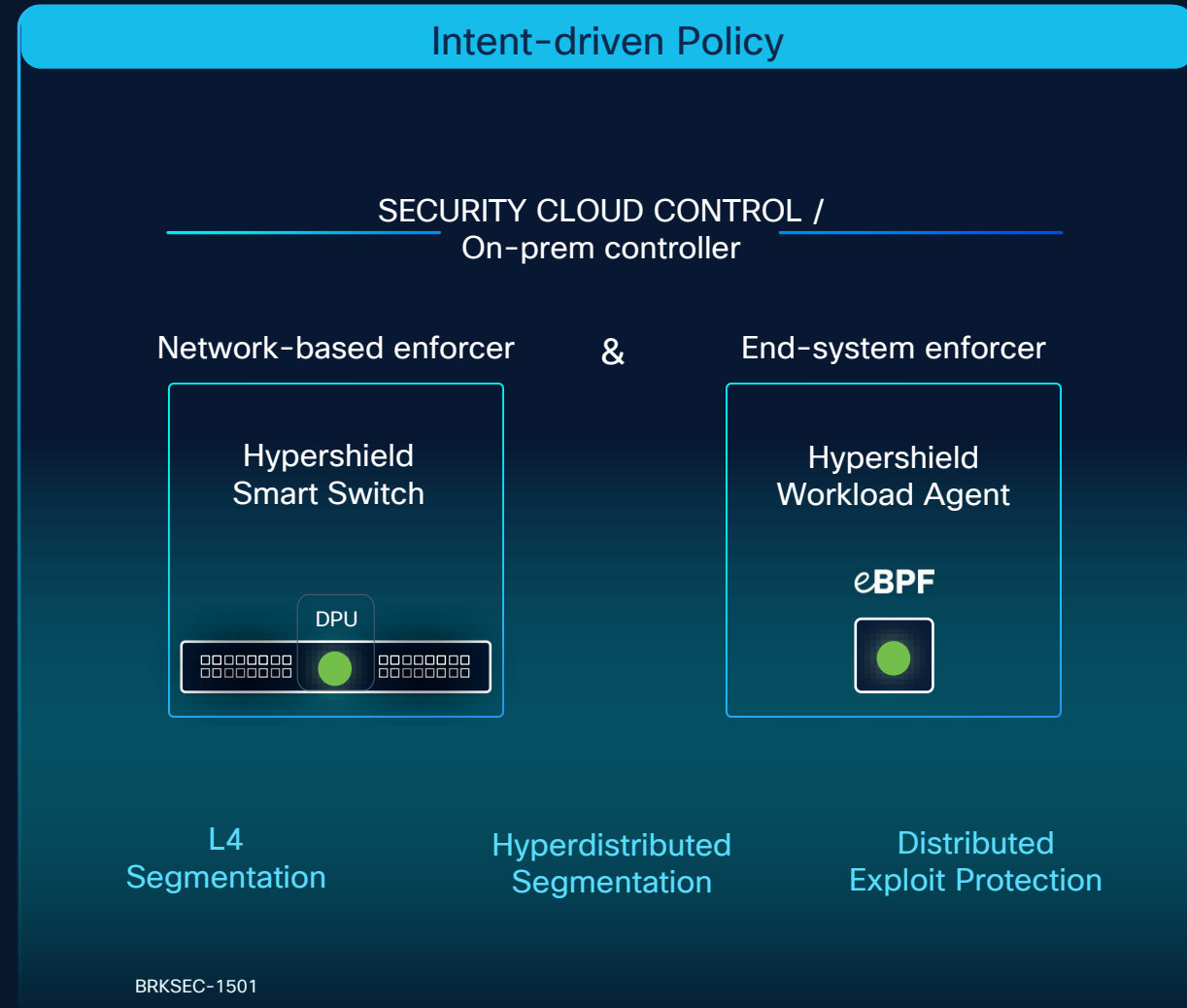
Hybrid Mesh Firewall: One Policy, Multiple Enforcement Points



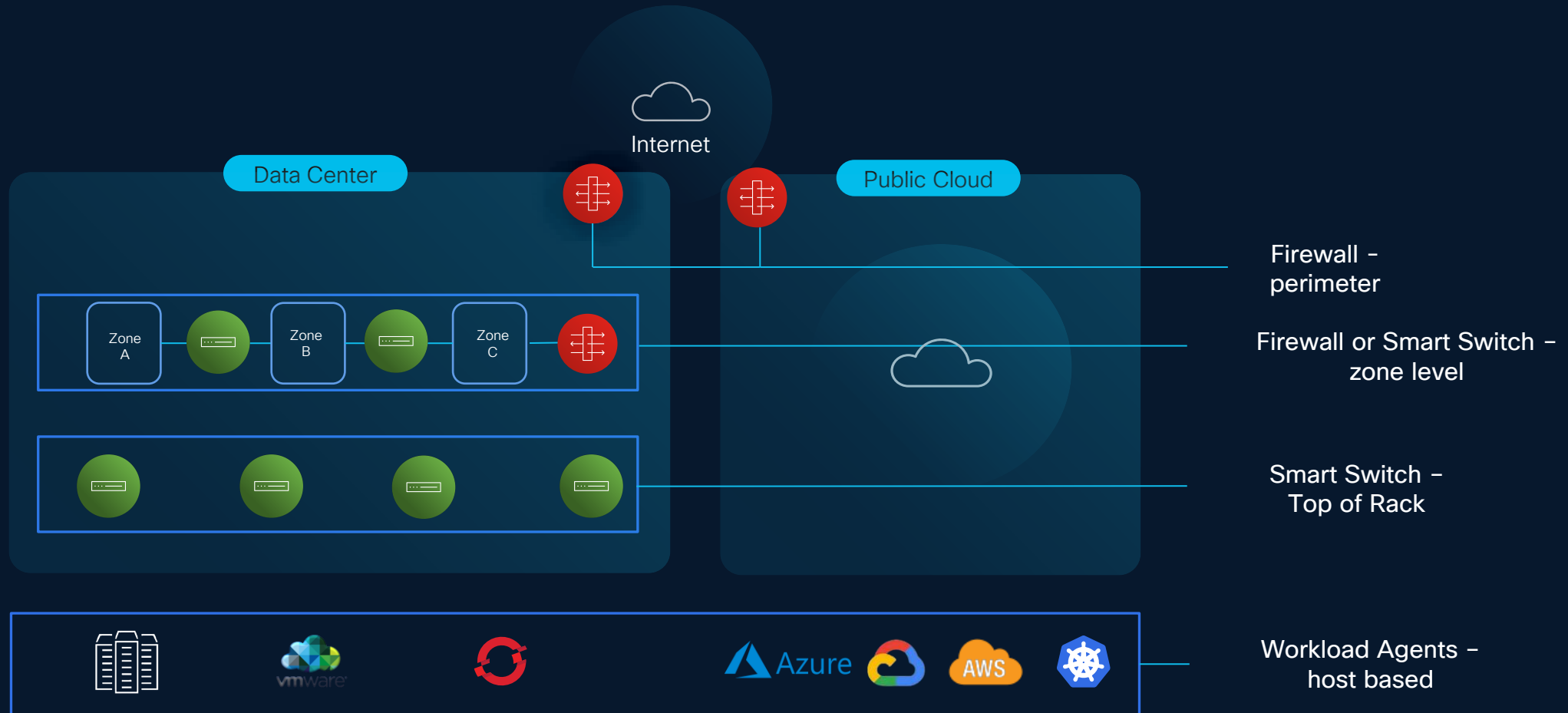
Hypershield: high-performance distributed enforcement

Part of Cisco Hybrid Mesh Firewall

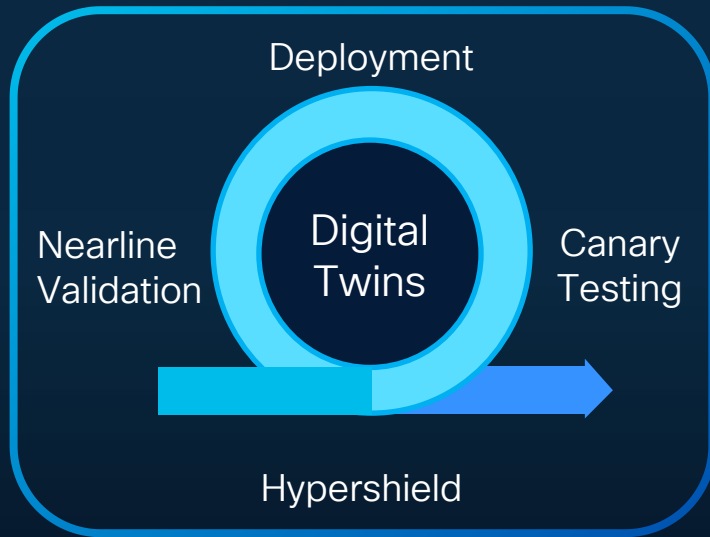
- Wire-speed segmentation at any scale
- Inline inspection, zero traffic redirection
- Infrastructure-embedded, minimal attack surface



Enforcement points for every environment



Improve security posture with self-qualifying policy updates



Test

Nearline policy validation using digital twin, staged canary deployment

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

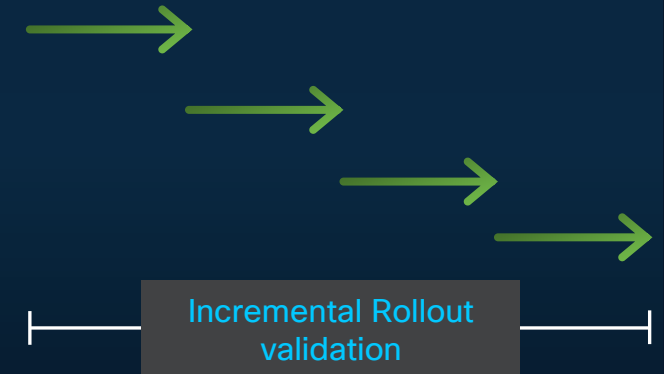
The application affected by these changes is the **Finance app**.
The app owner's approval is needed due to the high risk of the affected application.

Drew has been identified as the app owner of Finance app.

Review

AI system evaluates change.
Admin controls promotion

New Policy



Deploy

Canary roll-out to gain trust,
enabling teams to move fast
with confidence

Fusing Security into Smart Switches

Security infused into the data center fabric

with Cisco Nexus Smart Switches

Cisco N9300 Series Smart Switches

Shipping



N9324C-SE1U

24-port 100G
800G Services Throughput

Shipping



N9348Y2C6D-SE1U

48-port 1G/10G/25G, 6-port 400G, 2-port 100G
800G Services Throughput

Use Cases

Top of Rack segmentation
and enforcement

Cloud Edge*

Zone-based segmentation*

Data Center Interconnect*

*Limited scenarios

Security infused into the data center fabric

with Cisco Nexus Smart Switches

Ultra Ethernet
Consortium

Cisco N9300 Series Smart Switches

Shipping



N9324C-SE1U

24-port 100G

800G Services Throughput

Orderable

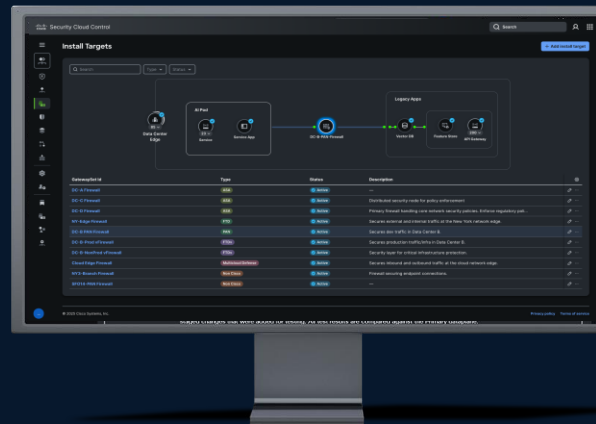


N9348Y2C6D-SE1U

48-port 1G/10G/25G, 6-port 400G, 2-port 100G

800G Services Throughput

Security Cloud Control



Use Cases

Top of Rack segmentation
and enforcement

Cloud Edge*

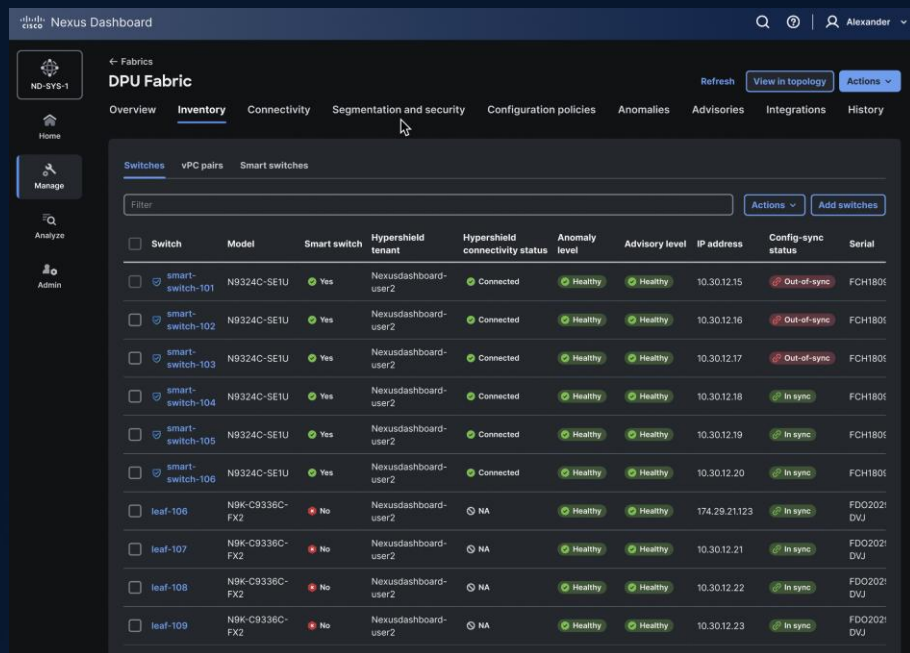
Zone-based segmentation*

Data Center Interconnect*

*Limited scenarios

Separate Workflows for NetOps and NetSecOps

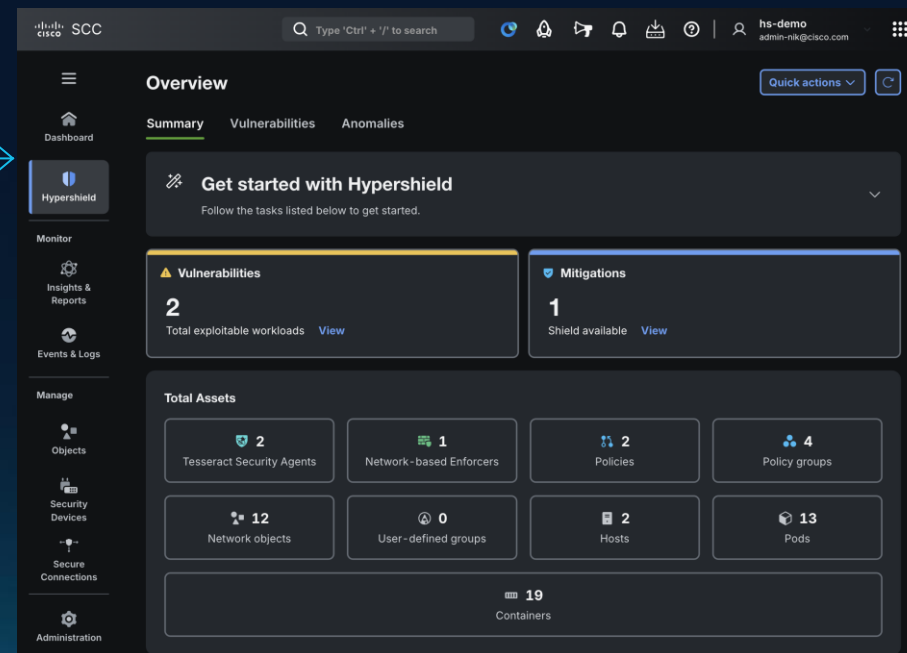
Nexus Dashboard, NX-API, NX-CLI



Switch	Model	Smart switch	Hypershield tenant	Hypershield connectivity status	Anomaly level	Advisory level	IP address	Config-sync status	Serial
smart-switch-101	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.15	Out-of-sync	FCH180f
smart-switch-102	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.16	Out-of-sync	FCH180f
smart-switch-103	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.17	Out-of-sync	FCH180f
smart-switch-104	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.18	In sync	FCH180f
smart-switch-105	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.19	In sync	FCH180f
smart-switch-106	N9324C-SE1U	Yes	Nexusdashboard-user2	Connected	Healthy	Healthy	10.30.12.20	In sync	FCH180f
leaf-106	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	174.29.21.123	In sync	FDO202i DVJ
leaf-107	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	10.30.12.21	In sync	FDO202i DVJ
leaf-108	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	10.30.12.22	In sync	FDO202i DVJ
leaf-109	N9K-C9336C-FX2	No	Nexusdashboard-user2	NA	Healthy	Healthy	10.30.12.23	In sync	FDO202i DVJ

Context sharing for troubleshooting

Hypershield On-Prem Controller



Nexus Smart Switch

BRKSEC-1501

Network-level enforcement

Turn every switch port into an enforcement point

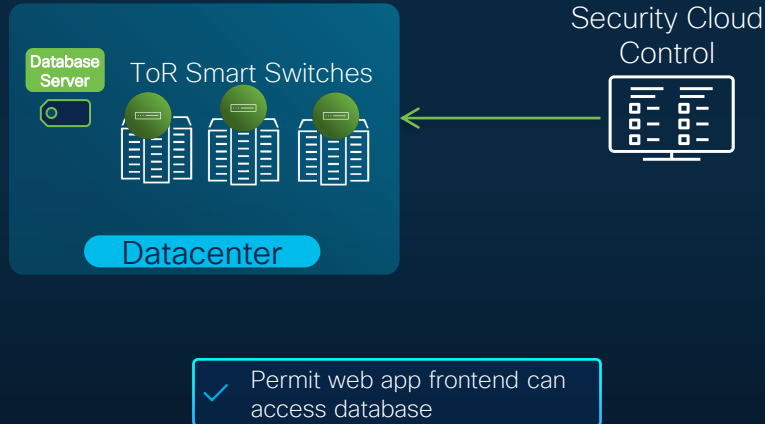
FW Cluster +
ToR switches



Security built into
Cisco ToR Smart
Switches



Eliminate blind spots by bringing
security close to every application and
securing every port

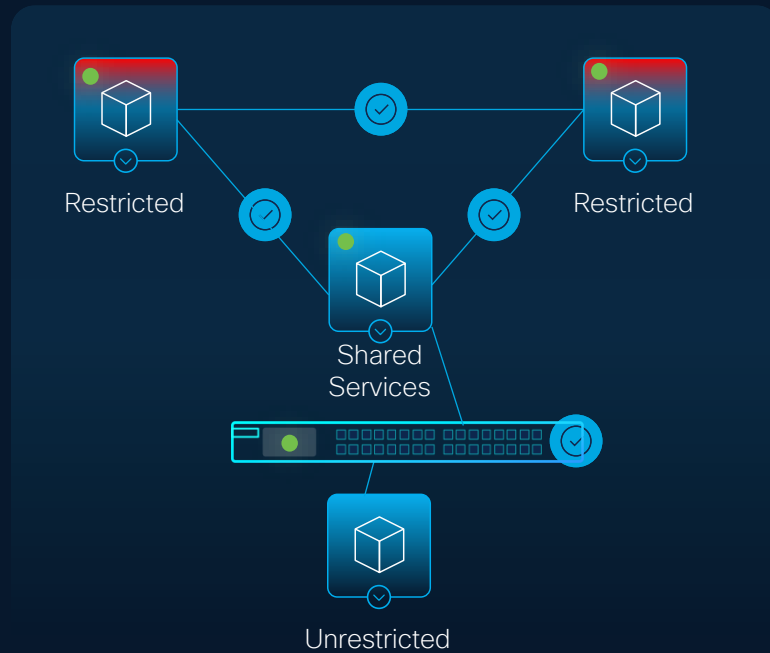


Consistent & intelligently placed policies
across all enforcement points, from
data centers to public cloud workloads

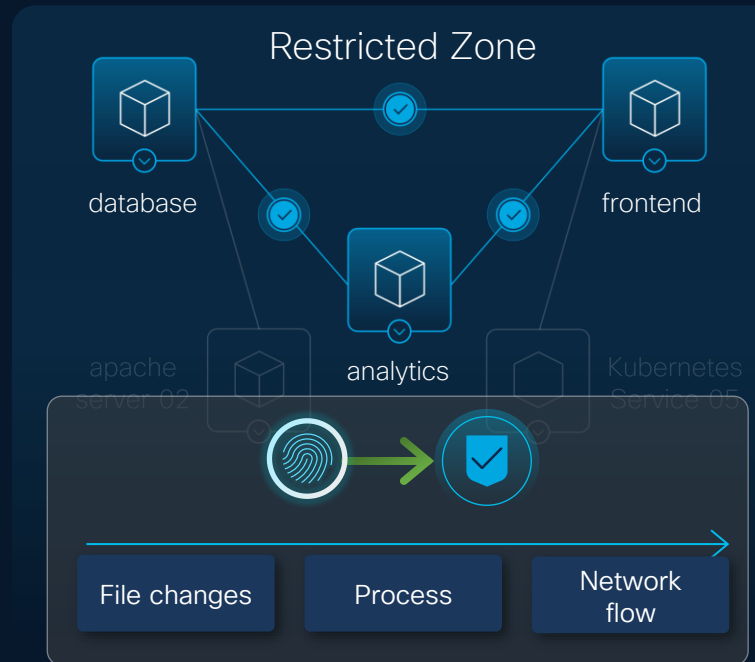


Changes tested against live
production traffic to earn
trust, deploy with confidence

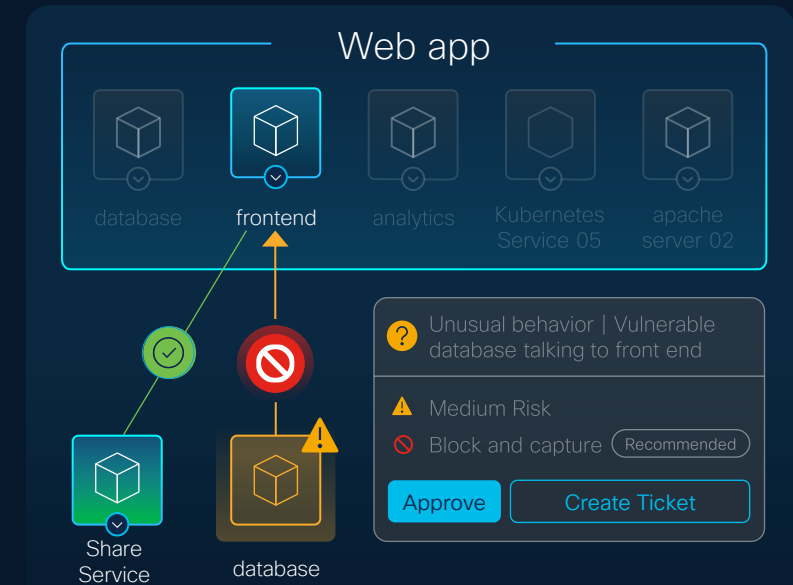
Segmentation that keeps up with changing applications



Set business guardrail and compliance policies
Enforce at the workload and in the network



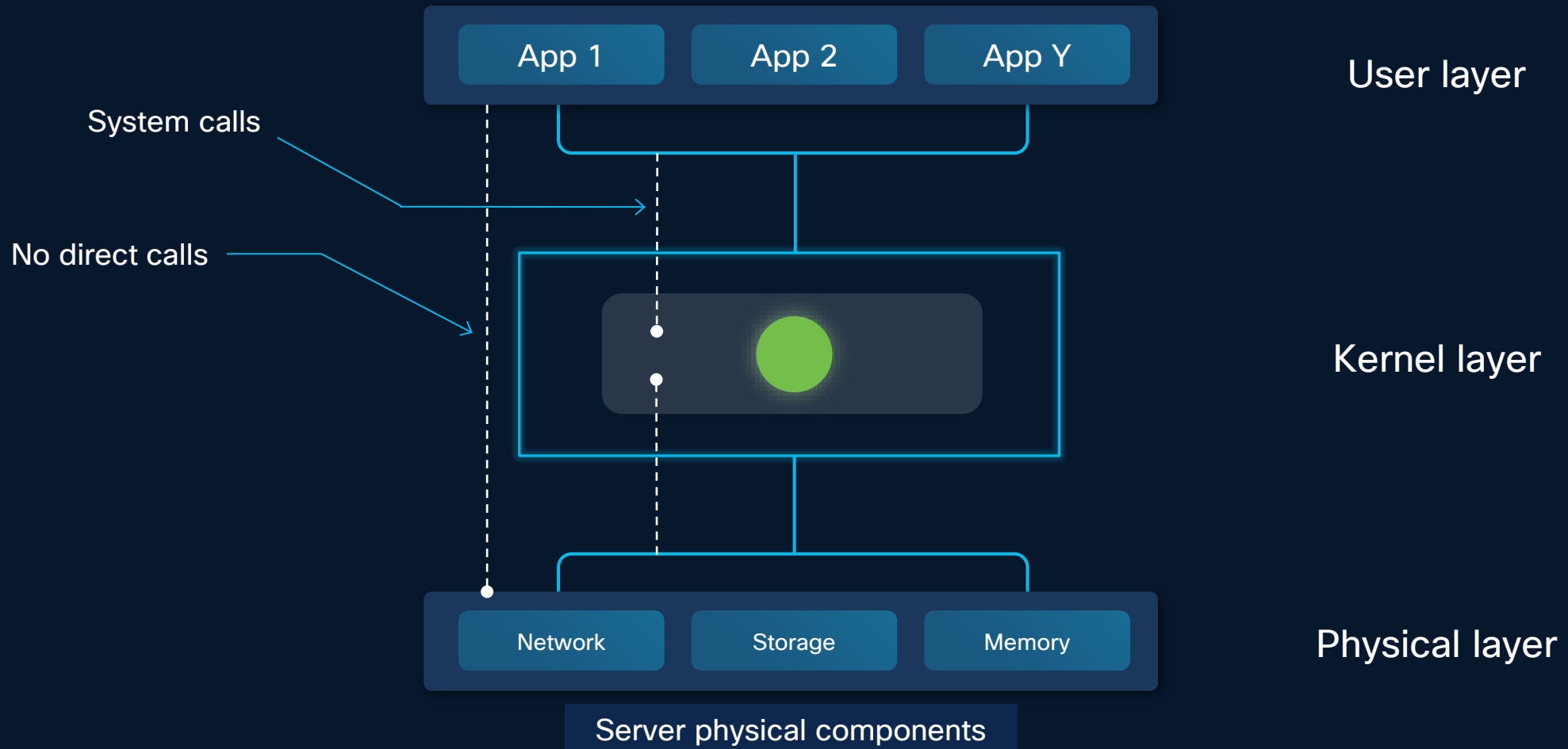
Continuous trust assessment



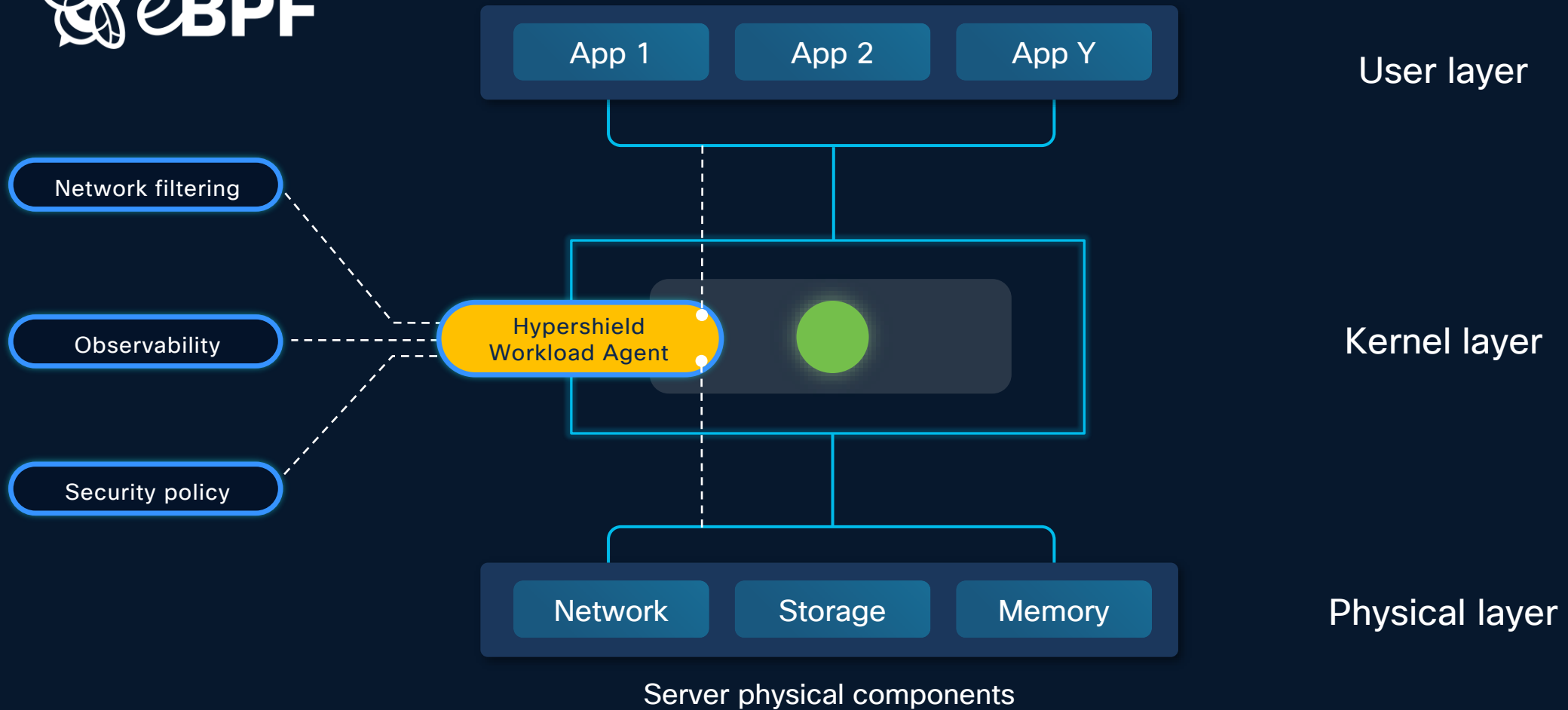
Assess trust to allow normal app
behavior and surface risks

Visibility and Enforcement with Hypershield Workload Agent

How do operating systems work?



eBPF – Foundation of Hypershield



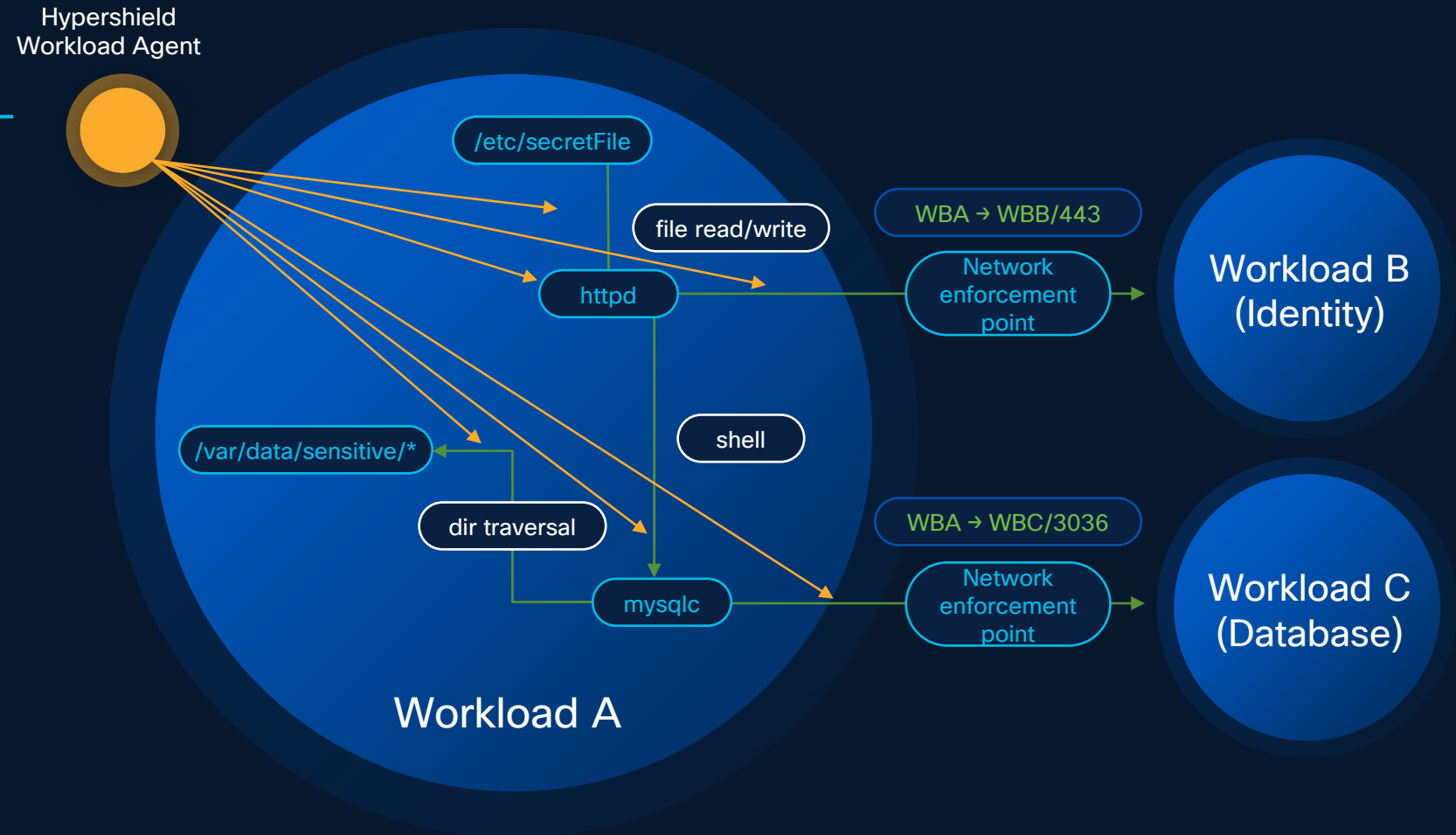
Workload enforcement with Hypershield Workload Agent

Hypershield Workload Agent provides deep **visibility** and **enforcement** within workloads

- Network
- File read/write
- Directory traversals
- Privilege escalations

End Systems

- Kubernetes
- Linux
- Windows server (CY26H2)



Distributed Exploit Protection

Exploit Protection: Prioritize. Shield. Keep the lights on.

Prioritize vulnerabilities intelligently

60,234 vulnerable assets

65% | 20,123 Assets

High risk assets Severe risk assets Medium risk assets

CVE-2024-21626

High Priority

runc. 1.1.11 vulnerability

16,234 vulnerable assets

Cisco Security Risk Score 91 High CVSS 3 9.3

3 Affected zones

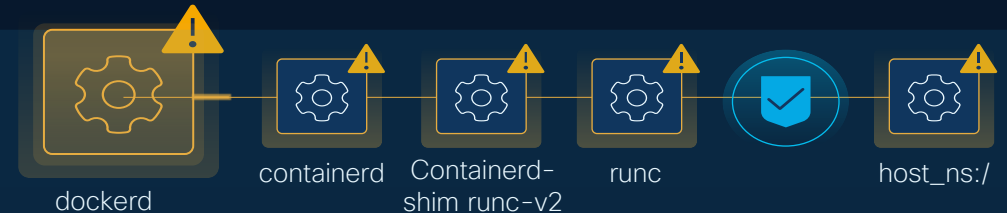
Production - External

Critical

Production - Internal

Dev

Protect-now
Patch later



Distributed
Exploit Shield
recommended
to deploy



The Distributed Exploit Shield blocks new container processes with a current directory of "/" in the host name space.



Block and alert

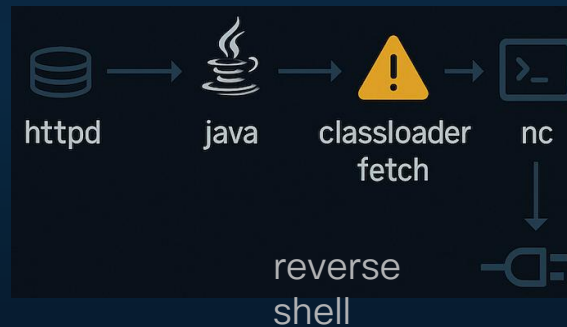
Proactive defense that buys you time and reduces risks

Not every attack maps to a CVE



Well known bad runtime behaviors
Block and alert as it happens

Block today's threats
Anticipate tomorrow's behaviors



Automatically blocks dangerous
combinations if they score too high.
Limit can be lowered during an attack.

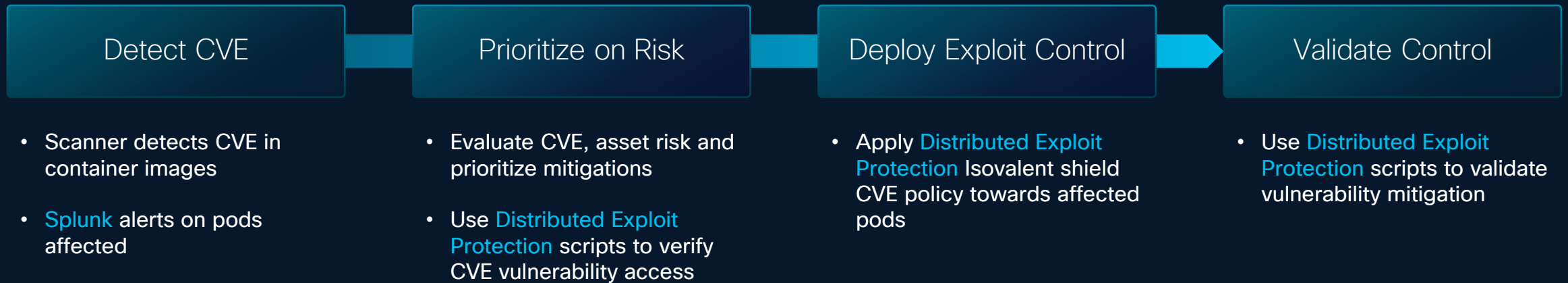
Dynamic Shields tighten when
risk increases



Adaptive shields stop what static rules
miss
Less risk. Free up time for SecOps

Distributed Exploit Protection via Splunk

- Assets and capabilities are also available in Security Cloud Control and Splunk
- Security Cloud Control automates detection to validation within a single workflow



Visibility

Runtime security visibility

Threat Detection & Incident Investigation

Examples:

- Privilege escalation and shells
- DNS queries and file access
- Data exfiltration attempts

Compliance Monitoring

Examples:

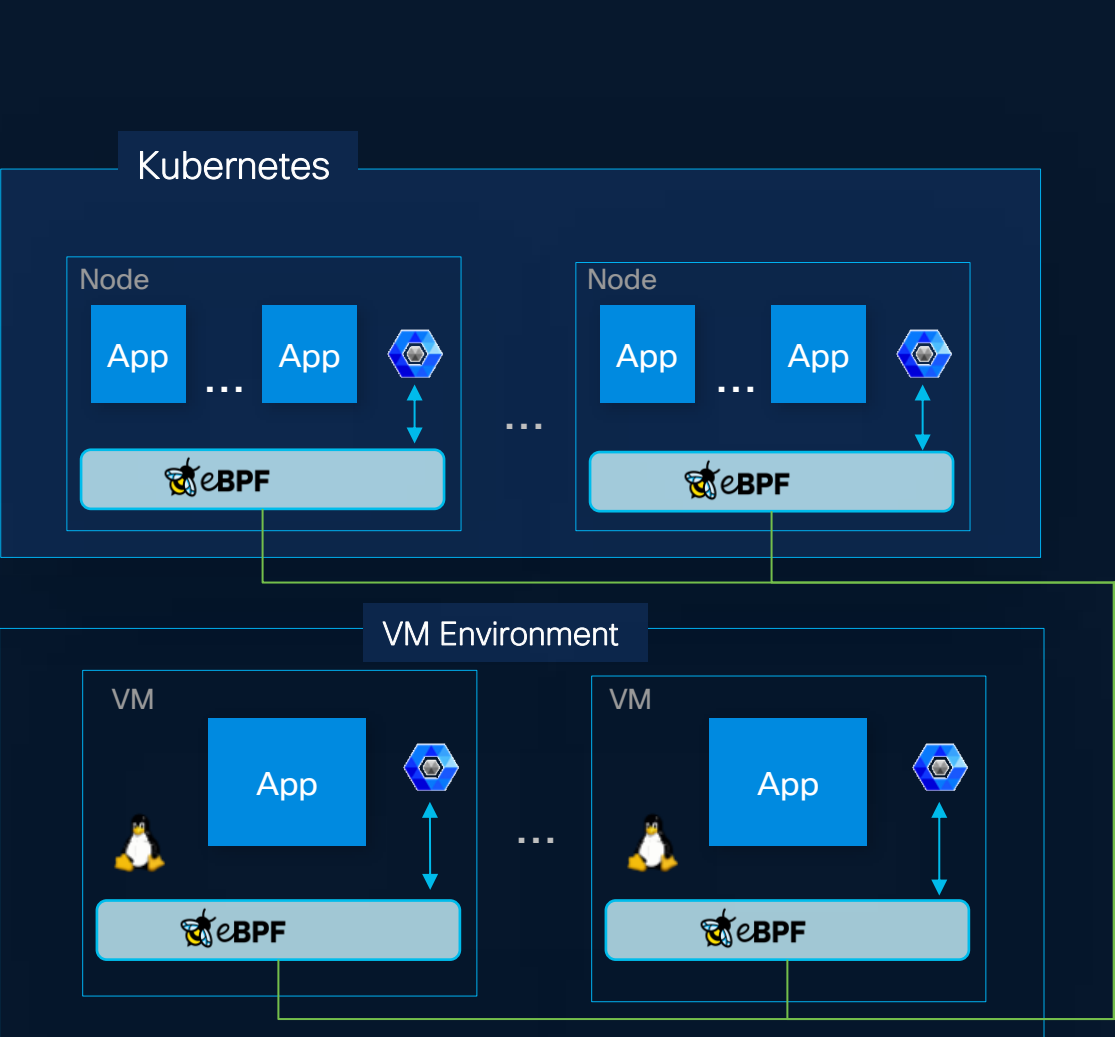
- Linux privilege violations
- Weak encryption protocols
- Unauthorized remote access

Continuous Exposure Monitoring

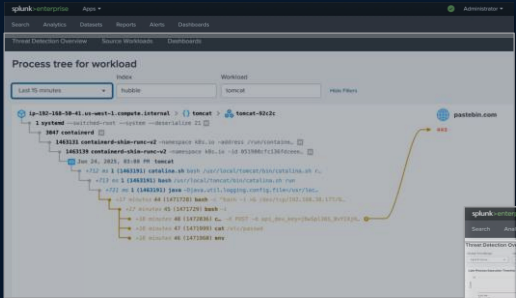
Examples:

- Identify Internet-facing systems
- Detect unprotected services
- Find open ports and services

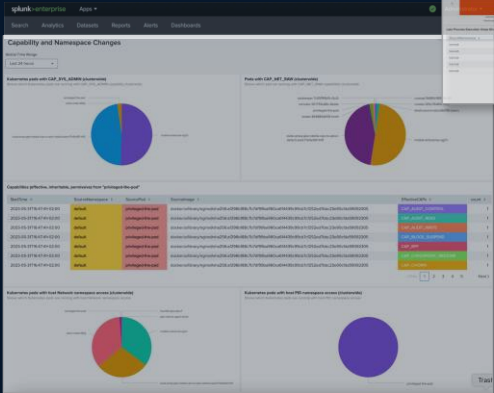
Runtime security with Splunk SIEM



Security Operations



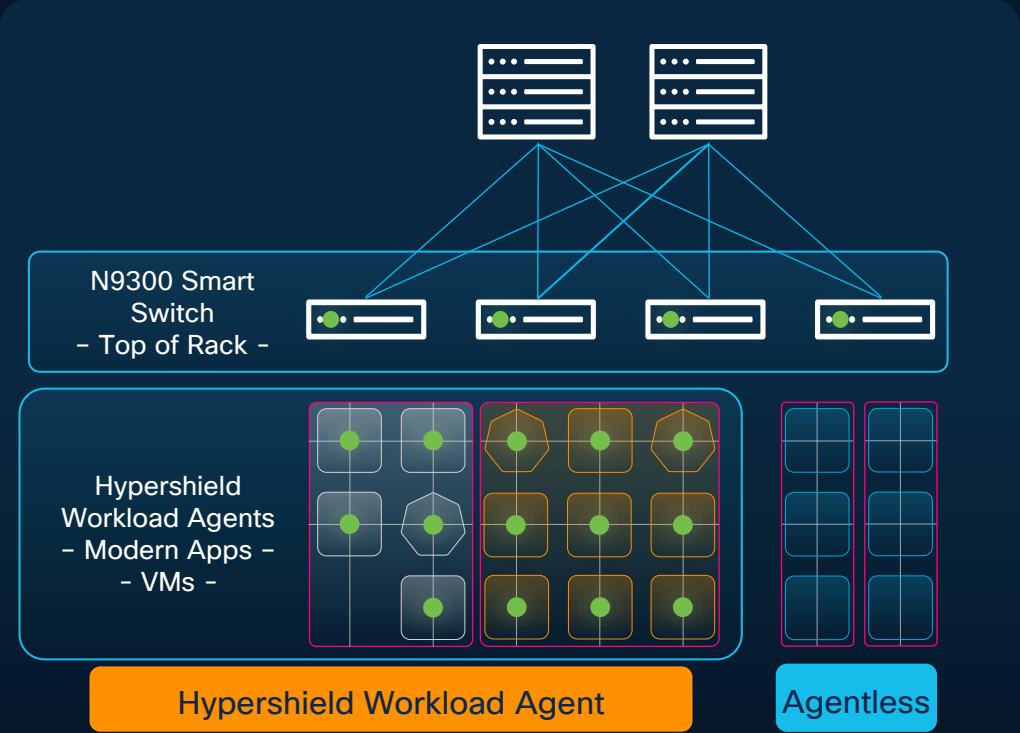
- Runtime Security Visibility
- Efficient threat detection
 - Incident response
 - Continuous compliance monitoring



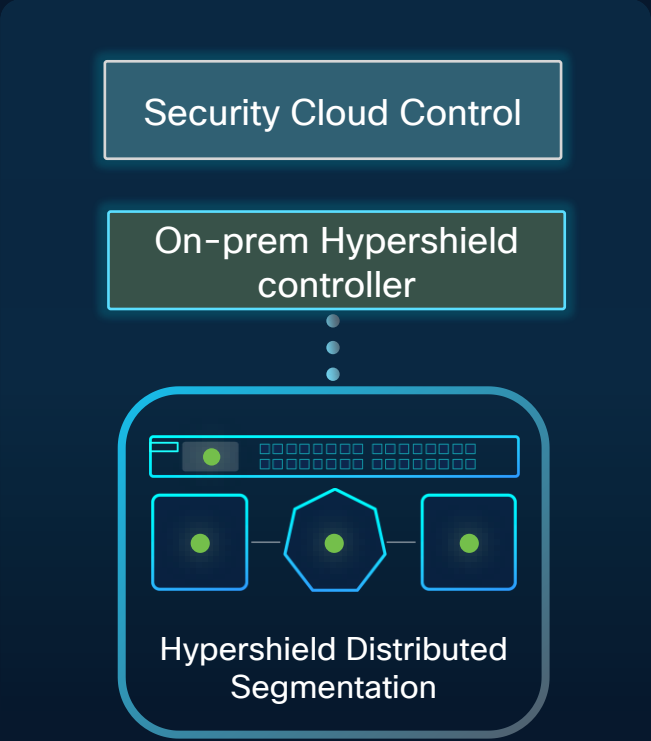
- Runtime Security Shields
- General purpose & CVE-specific “shields”
 - Shield deployment workflows

Hypershield provides distributed defense for every workload

Distributed



Global Control



Workload Protection

The screenshot displays the details of a vulnerability, CVE-2024-21626, which is a runc. 1.1.11 vulnerability affecting 16,234 vulnerable assets. The vulnerability is marked as High Priority. The Cisco Security Risk Score is 91 (High), and the CVSS 3 score is 9.3. The affected zones are Production - External (Critical), Production - Internal, and Dev.

CVE-2024-21626 High Priority

runc. 1.1.11 vulnerability 16,234 vulnerable assets

Cisco Security Risk Score 91 High CVSS 3 9.3

3 Affected zones

Production - External Critical Production - Internal Dev

Proactive defense that buys you time and reduces risks

Hypershield helps deliver business outcomes

Accelerated
security
protection

Higher
security
efficacy

Reduced
outage
downtime

Lower
barrier to
expertise

Let's get started

Check out this session

**BRKDCN-2643 Cisco Nexus
Smart Switches with DPUs**

Wed Nov 12,
10:30 – 11:30a, Room 216

Cisco Hypershield resources:



- <https://cisco.com/go/hypershield>
- Keep up-to-date on product news, demos and more [here](#)

Engage with your Cisco team today!

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer 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

Contact me at: Insert preferred comms method

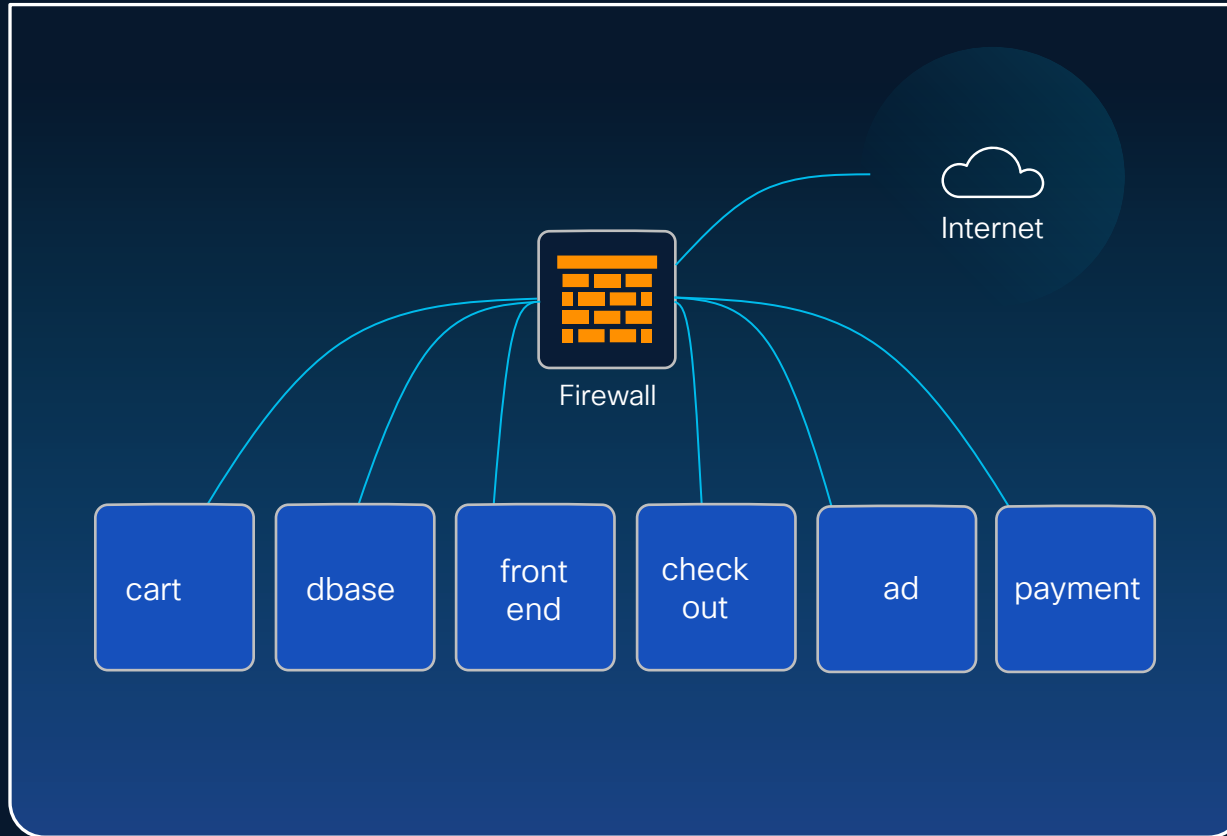
Thank you

CISCO Live !



Issues with today's implementation

Why traditional segmentation falls short



Too Complex and Rigid

- Manual and static, can't match dynamic networks
- Limited visibility into devices and flows
- Inconsistent enforcement weakens security