

# Hypershield in a Nutshell – What It Is and How It Works

**CISCO** Live !

Errol Roberts – Distinguished Architect

Dave Zacks – Distinguished Engineer

**#HighBitRate**



# Cisco Webex App

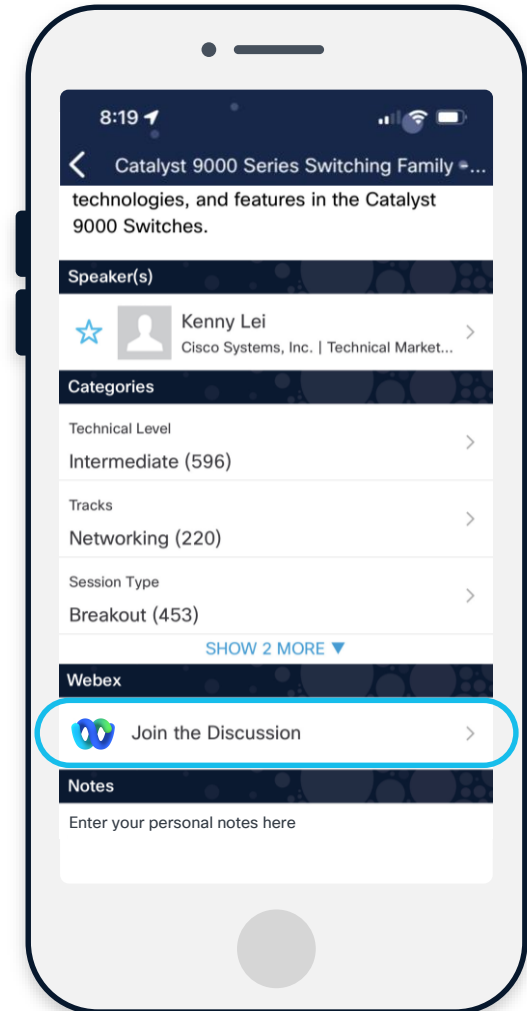
## Questions?

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 June 13, 2025.**



# By Way of Introduction ...

I am a **Distinguished Engineer** in the Cisco Security Innovation CTO team, and have been with Cisco for 25 years.

I work primarily with large, high-performance Enterprise network architectures, designs, and systems. I have over 30 years of experience with designing, implementing, and supporting solutions with many diverse network technologies.

I have a strong background in, and focus on, customer requirements, and integrating these into the products and solutions Cisco builds. I have a special interest in **Flexible Hardware, Fabrics, Assurance and ML/AI**.

**Dave Zacks**  
Distinguished Engineer  
dzacks@cisco.com



# By Way of Introduction ...

**James Earl Jones**  
RIP Sept. 9, 2024



**The Voice of Darth Vader ...  
and Errol Roberts? 😊**

I am a **Distinguished Architect** in the Cisco Security Innovation CTO team, and have been with Cisco for 25 years.

My journey into networking was fueled by a desire to explore the synergy between different tech domains. At Cisco, I've had the opportunity to solve complex problems for customers and gain a deep understanding of Cisco's stack and its integration with our vendors' tech platforms.

What excites me most is the impact technology can have on **operations and efficiency**. Every day, I am driven by the opportunity to leverage technology to create solutions that make a difference.



**Errol Roberts**  
**Distinguished Architect**  
eroberts@cisco.com

# eBPF and Hypershield – Overview

# Cisco acquires Isovalent

## Cisco Completes Acquisition of Isovalent to Define the Future of Multicloud Networking and Security

April 12, 2024

### News Summary:

- Cisco has completed the acquisition of Isovalent, Inc., a leader in open source cloud native networking and security
- Together, Cisco and Isovalent will build leading edge protection for every workload on every cloud
- Cisco is committed to nurturing and supporting eBPF, Cilium, Tetragon, and cloud native open source communities

SAN JOSE, Calif., April 12, 2024 /PRNewswire/ -- Cisco (NASDAQ: CSCO) today announced the completion of the acquisition of Isovalent, a leader in open source cloud native networking and security. This marks a significant step forward in Cisco's commitment to define the future of secure, multicloud networking.

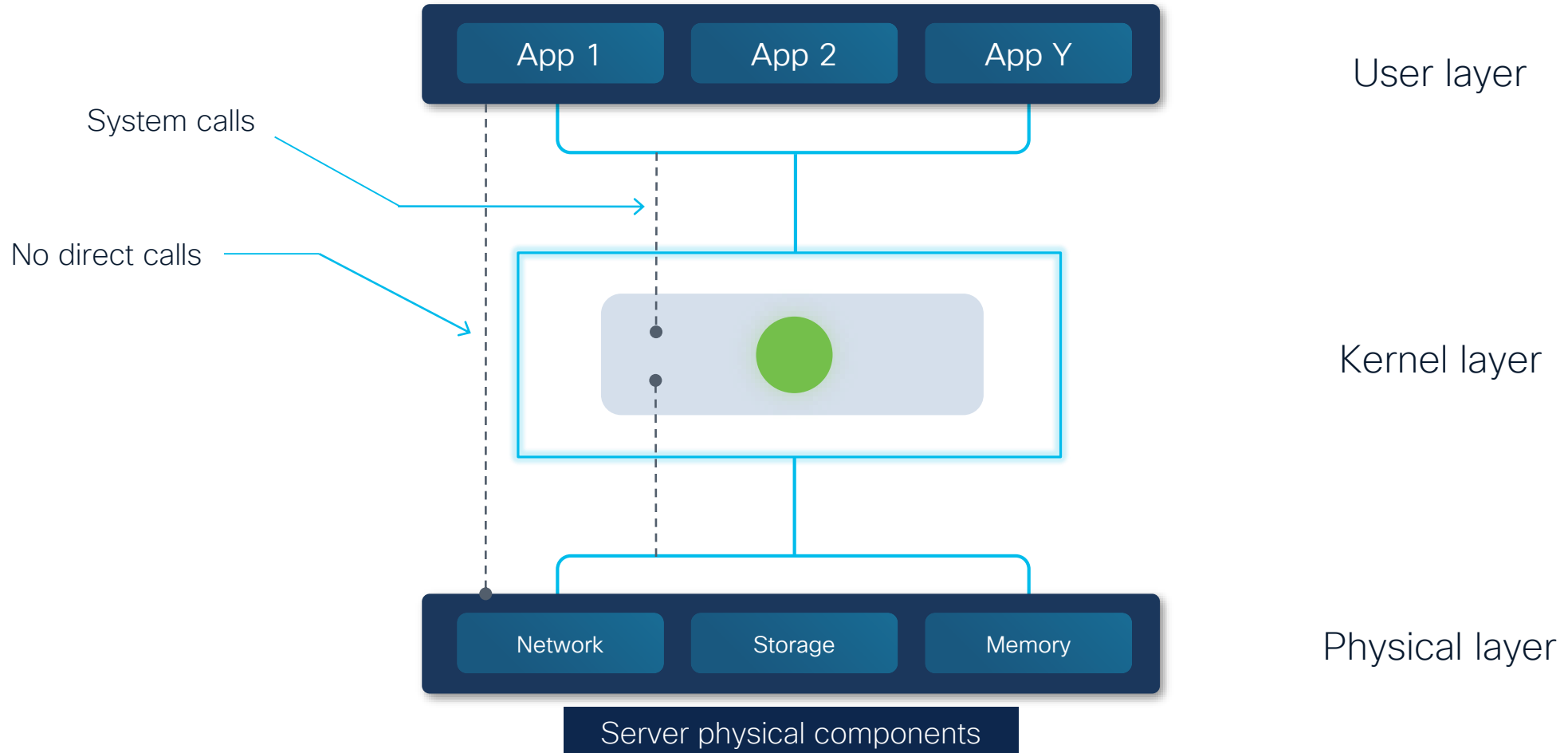


**ISOVALENT**  
now part of **CISCO**

# What is eBPF ?

- Makes the **kernel programmable**
- Allows bespoke, **dynamic** changes to kernel behavior
- Enables **high performance, low overhead** infrastructure tools

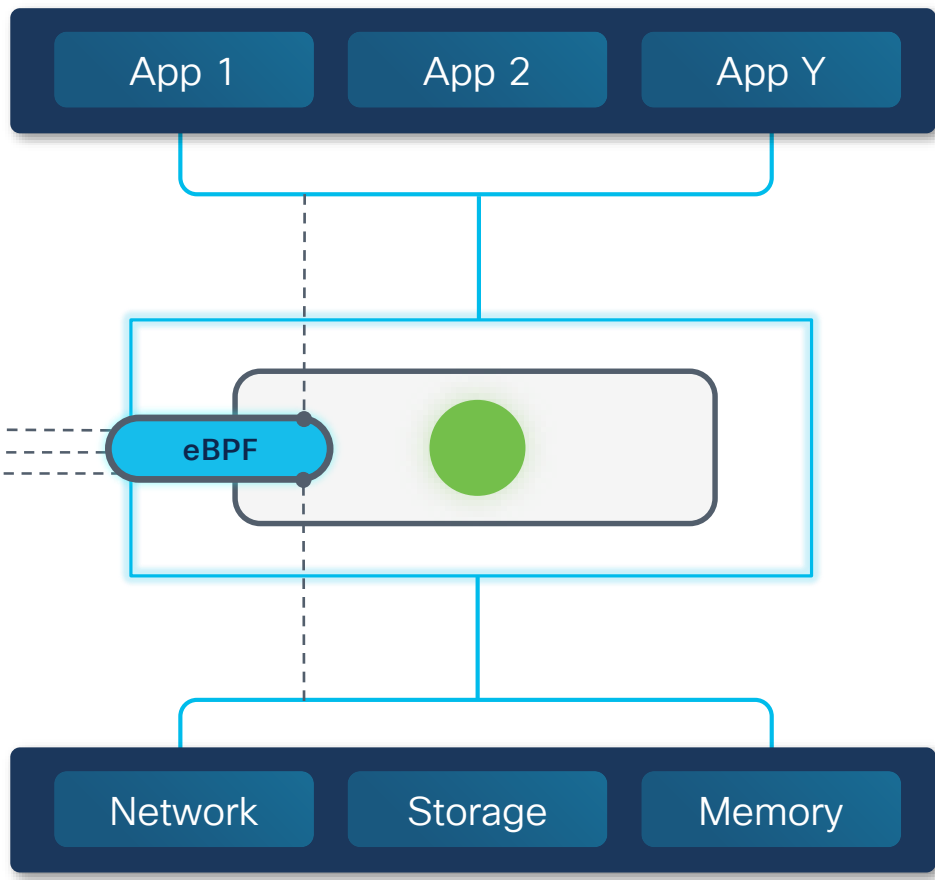
# How do operating systems work?



# eBPF – Foundation of Hypershield



- Network filtering
- Observability
- Security policy



User layer

Kernel layer

Physical layer

What Javascript is to the browser, eBPF is to the kernel.

# eBPF – Foundation of Hypershield

- Kubernetes networking
- Load balancing
- Kubernetes services
- Identity-based security
- L7 policies

- Dependencies map (service and flows)
- Monitoring and alerting
- App monitoring

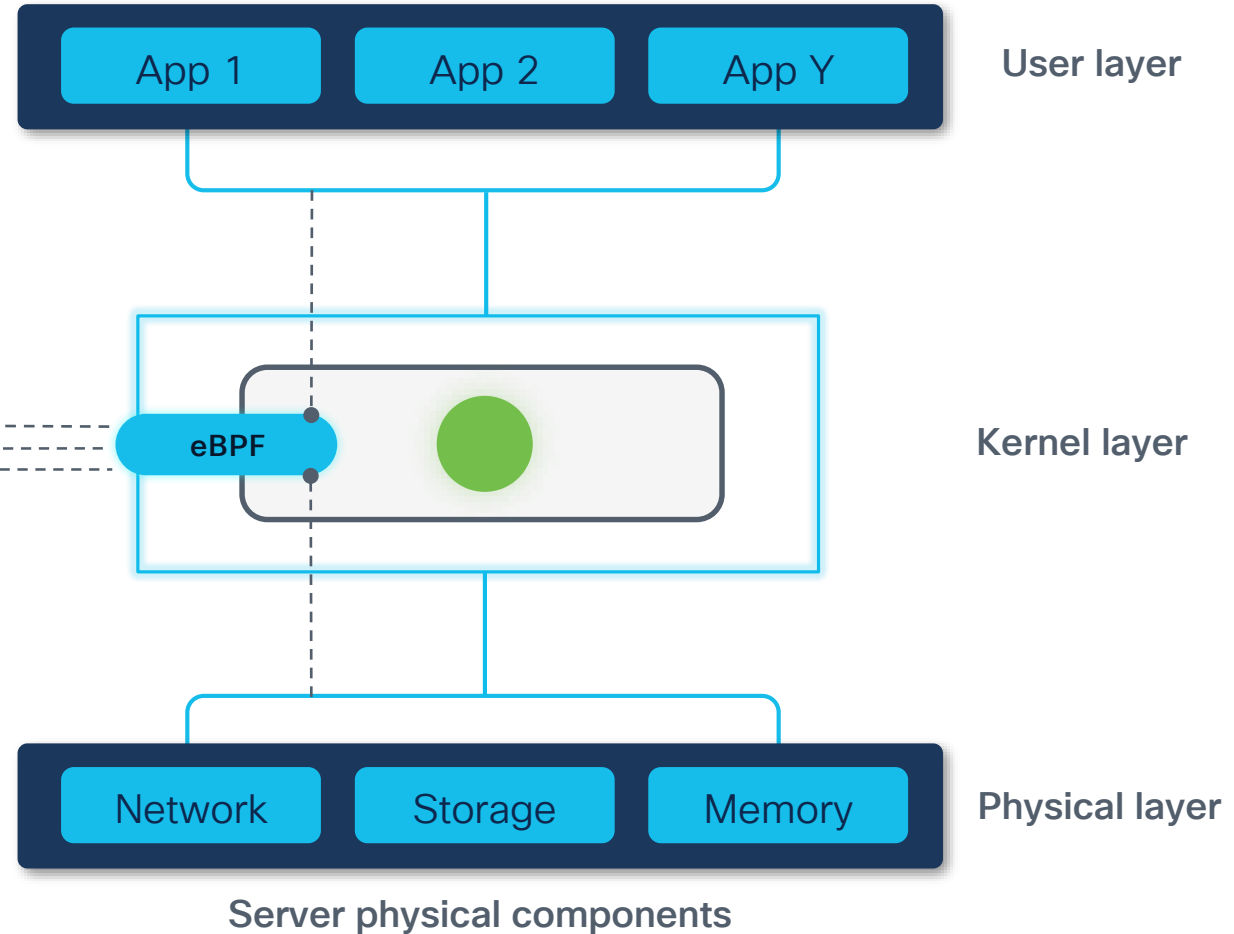
- Monitor process execution
- Runtime security policies
- Real time enforcement



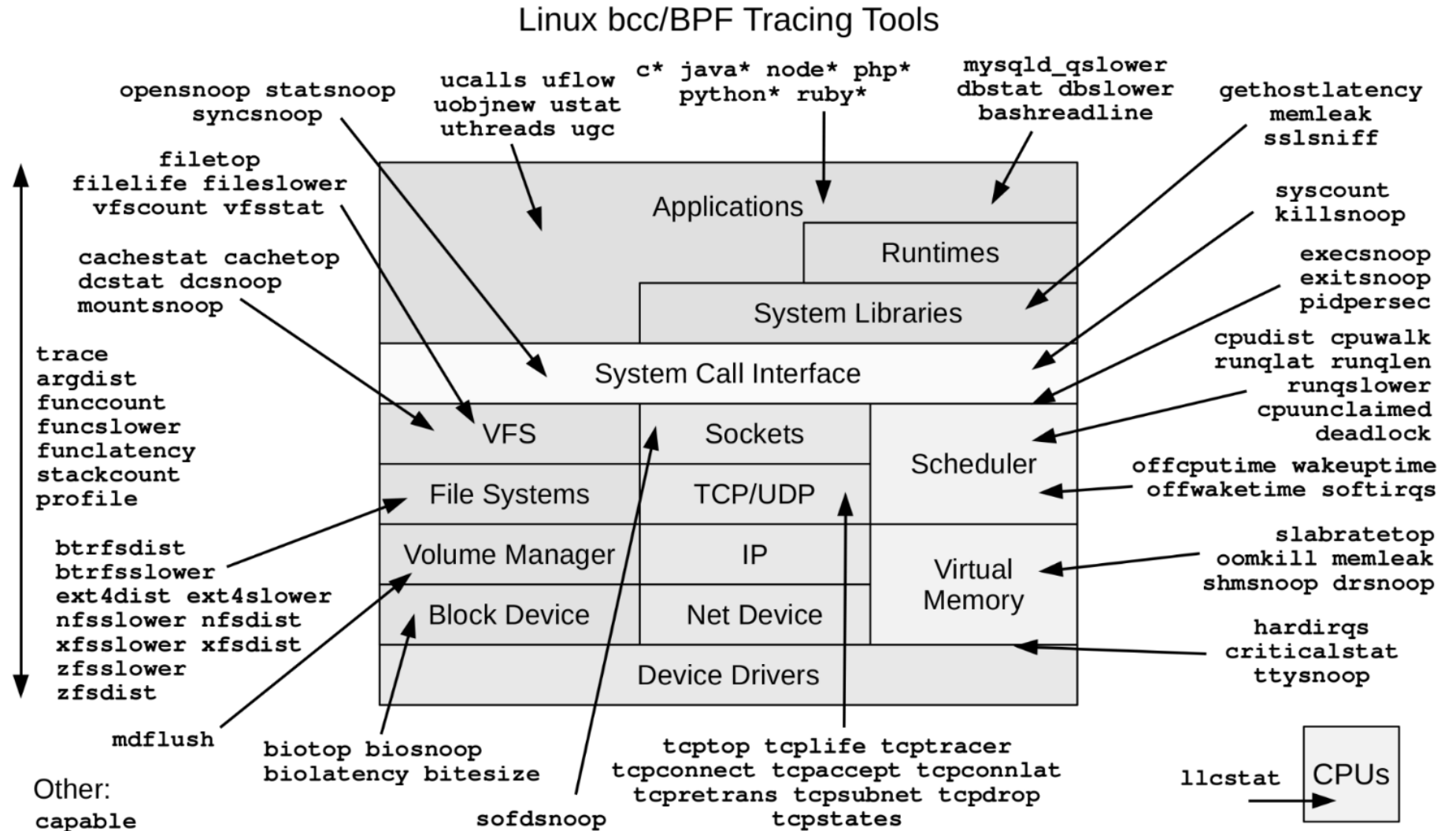
Network filtering

Observability

Security policy



# What can eBPF see?



<https://github.com/iovisor/bcc#tools> 2019

# Cisco HYPERSHIELD

Network flows  
Process behaviors  
File changes



Anonymized app behavior  
Threat intel updates  
Learned policy preferences  
...

- WHAT IF ...

We could build on the strong foundation of eBPF to create a dynamic, distributed, and high-performance security solution ... running on both the host as well as within the network?

# 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



# Scalable hyper-distributed architecture

## AI- Native

Built-in AI from inception.

Earns your trust, analysis-backed recommendations and interactions



## Cloud- Native

Built on open source eBPF

eBPF powers default network for cloud-native workloads in hyperscalers

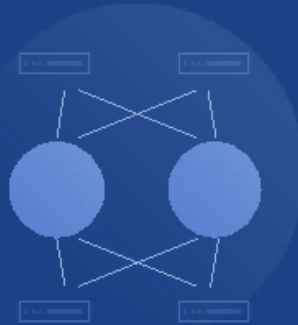
## Hyper- Distributed

Distributed enforcement points across appliances, in the network, and the workload.

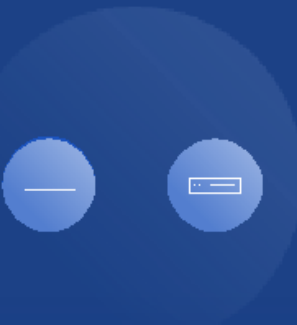
Managed as one system.

# Secure the data center

## with a simplified, easy to scale architecture

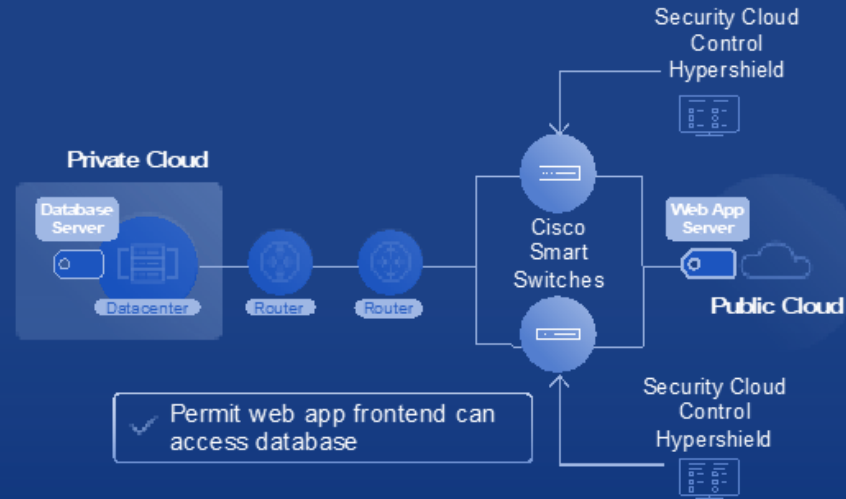


2x firewalls  
+4x switches



  
Just 2x  
N9324C

Simplified architecture, high-performance stateful segmentation, lower costs, & scalable security



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



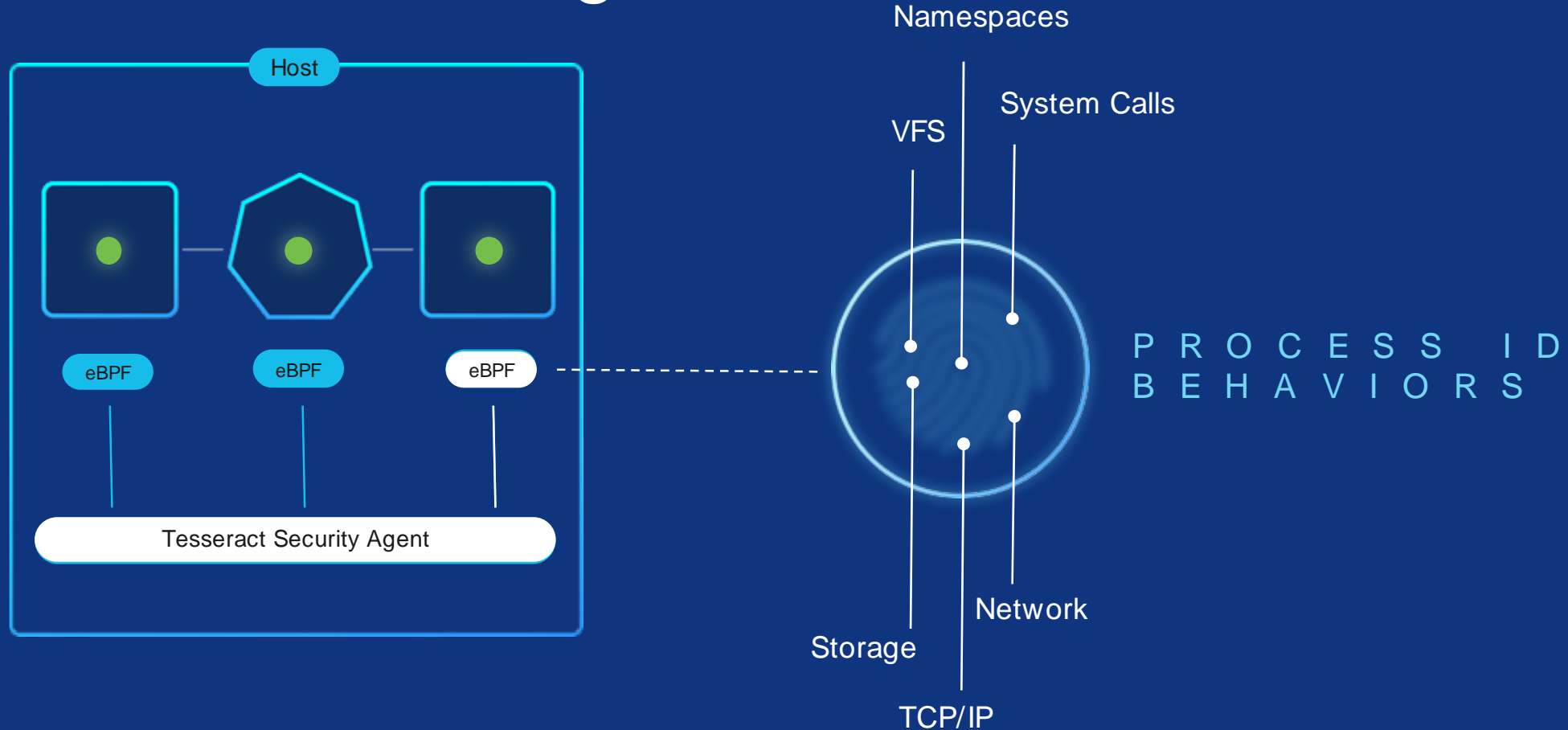
Tested against live production traffic to earn trust and deploy with confidence

# Hypershield – Deeper Dive

Errol

# Deep visibility and enforcement in the workload

## built on Isovalent Tetragon



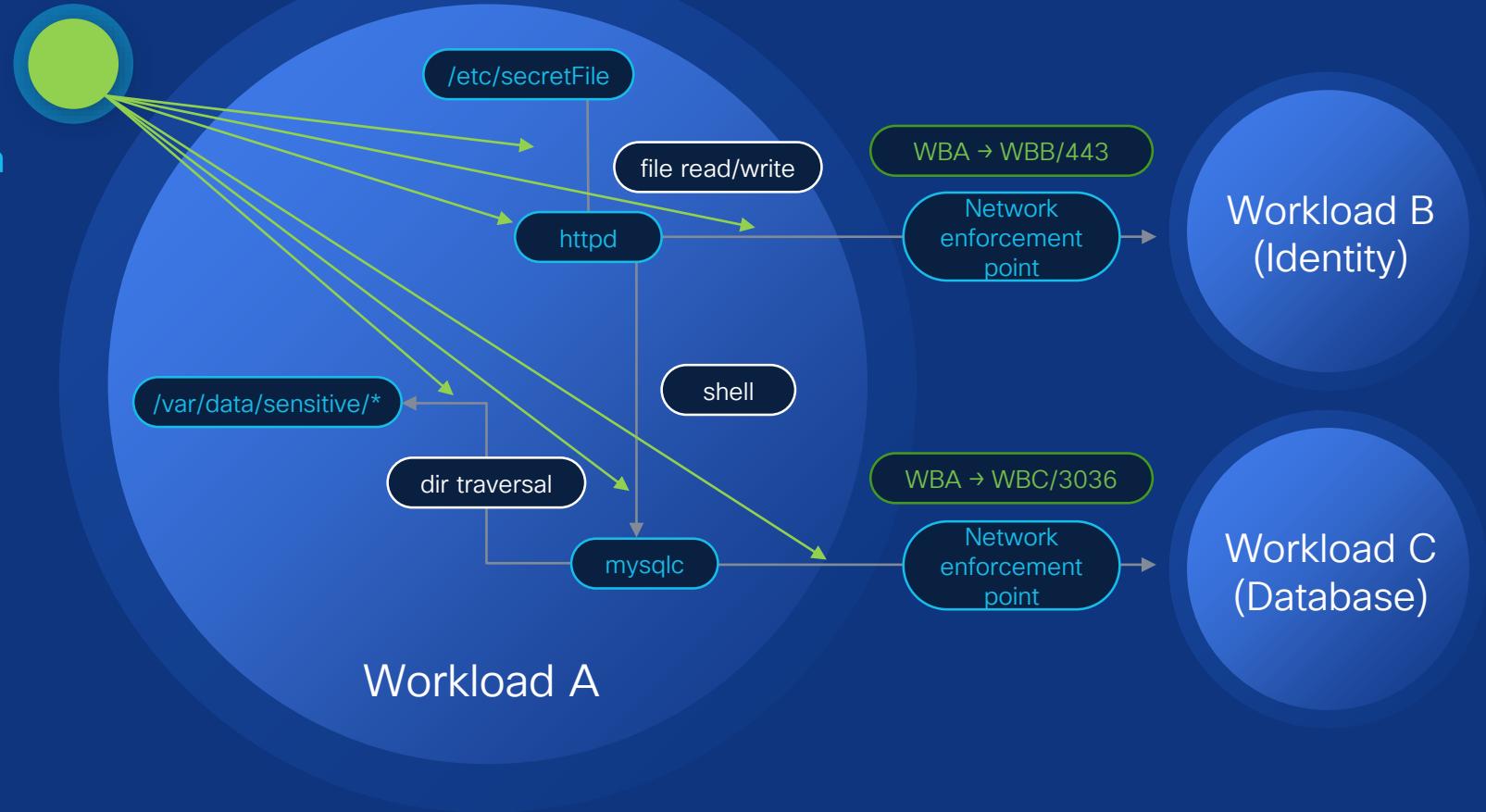
# Visibility and controls in network and workload

Tesseract Security Agent provides deep **visibility** and **security controls** within workload

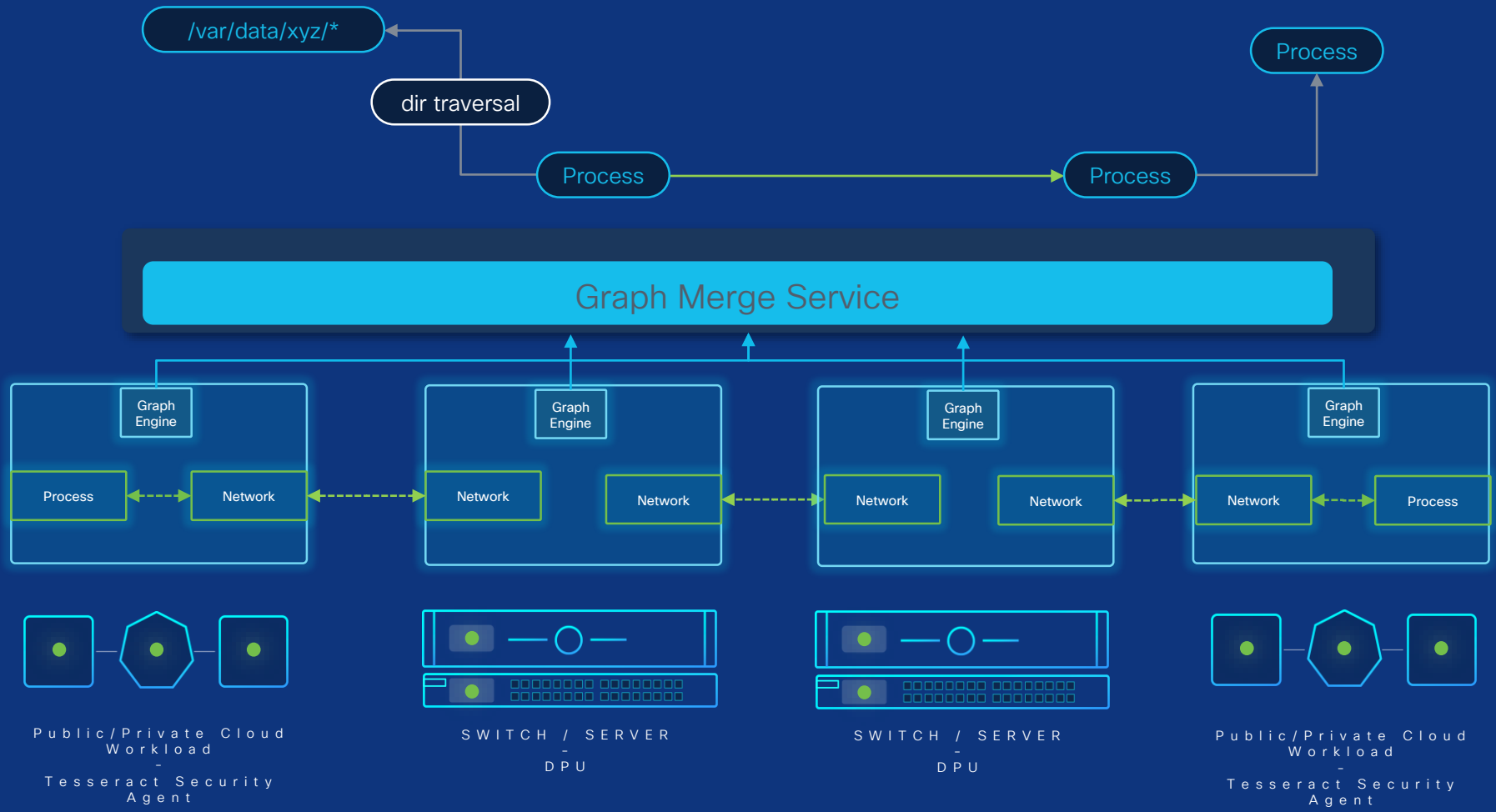


- Network
- File read/write
- Directory traversals
- Privilege escalations

Tesseract Security Agent

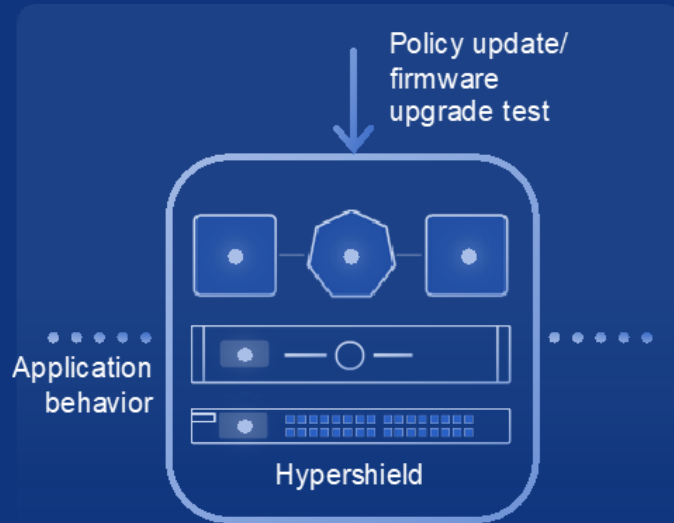


# AI & Graph Engine



# Improve security posture with

# self-qualifying firmware and policy updates



## Test

Using a digital twin, firmware and policy changes are 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



95%

Passed

Confidence Score

## Deploy

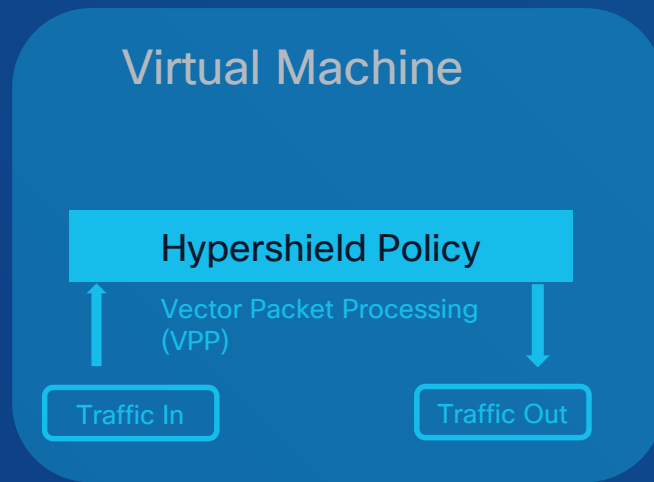
Hitless deployment with single click, enabling teams to move fast with confidence

**Note:** Images are not an exact product UI representation

# Network Enforcer VM

A platform to enable stateful services

## Network



## Security

### Cisco Hypershield



Integrated security (license add-on)

- Intelligent security policy placement
- Self-qualifying policy updates
- Policy unified with workload/network enforcement, public and private clouds

# Network Enforcer: N9300 Smart Switch

A platform to enable stateful services

## Network

### N9300 Series Smart Switches



Converge stateful services and network

- 800G stateful services throughput and scale
- 24-port 100G
- 4.8T Silicon One + 4 AMD DPU
- 1 RU

## Security

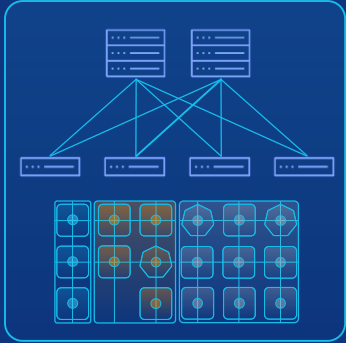
### Cisco Hypershield



Integrated security (license add-on)

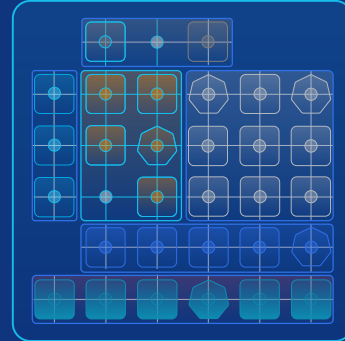
- Intelligent security policy placement
- Self-qualifying policy updates
- Policy unified with workload/network enforcement, public and private clouds

# Cisco Hypershield use cases



## L4 Zone-Based Segmentation

- Within and across data centers, cloud edge and top-of-rack
- Consistent policy enforcement
- Simplified architecture and lower costs



## Autonomous Segmentation

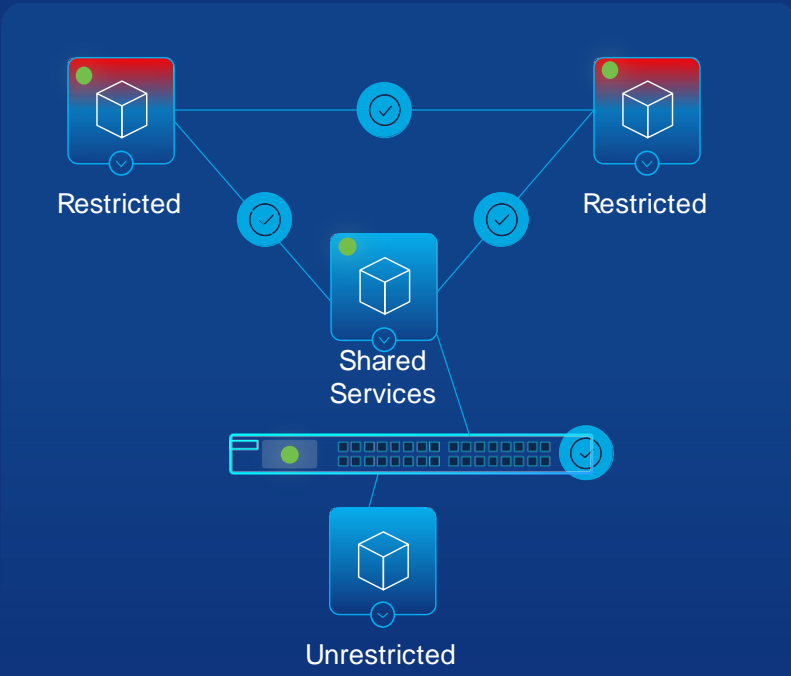
- Deep understanding of app behavior
- Comprehensive inputs for policy creation
- Constantly adapting to changing apps



## Distributed Exploit Protection

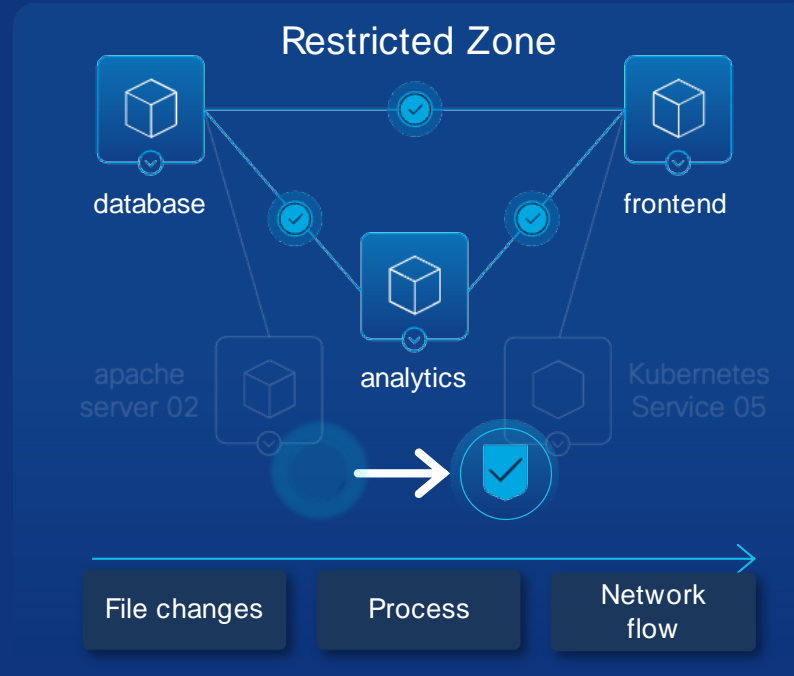
- Mitigate known and unknown vulnerabilities
- Surgical mitigating controls
- Protection within minutes, while app keeps running

# Segmentation that is effective and keeps up with changing apps

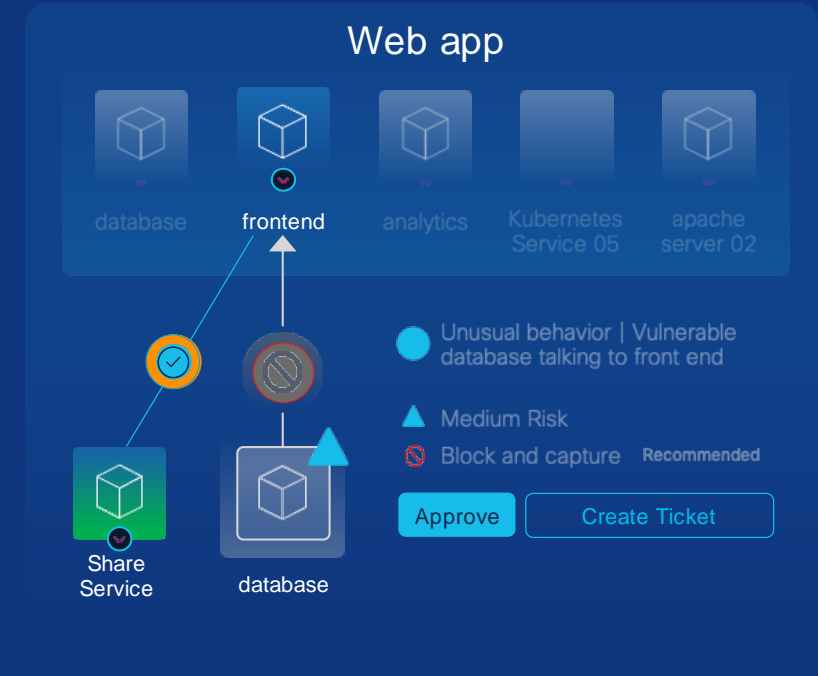


Set business guardrail and compliance policies

Enforce at the workload and in the network



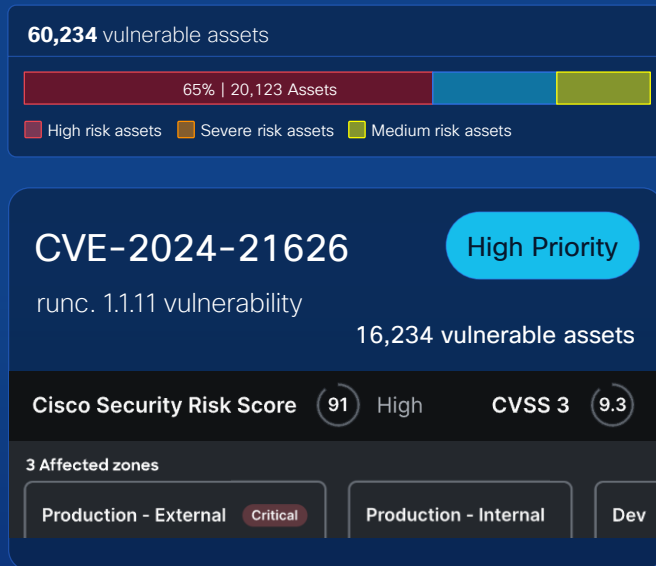
Codify application fingerprints into micro trust boundaries



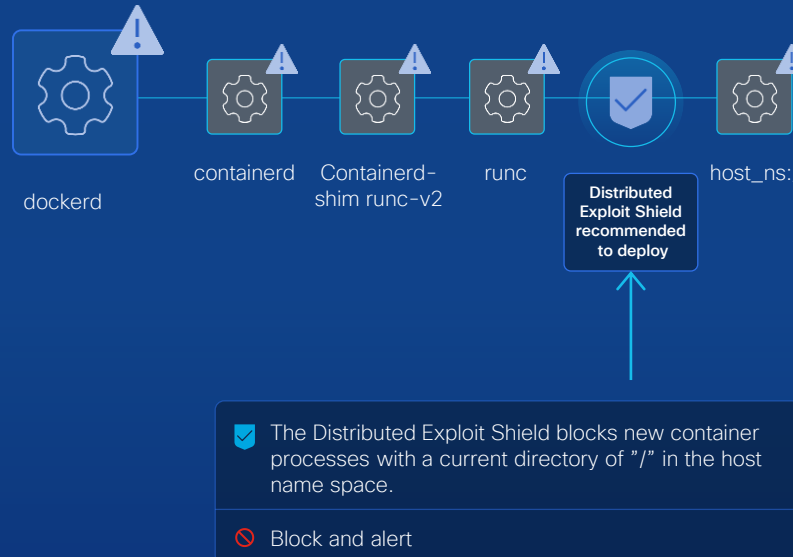
Assess trust to allow normal app behavior and surface anomalies

# Close the exploit gap

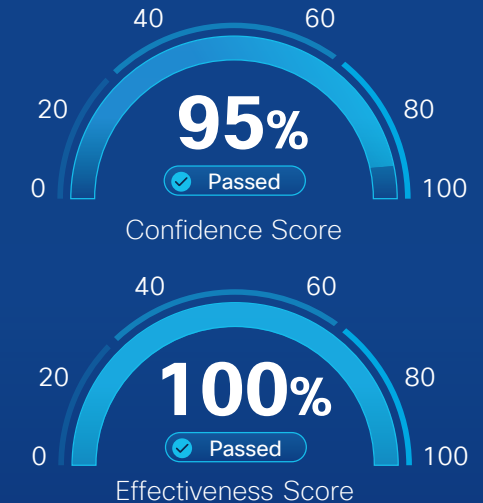
## against growing vulnerabilities with automated workflows



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

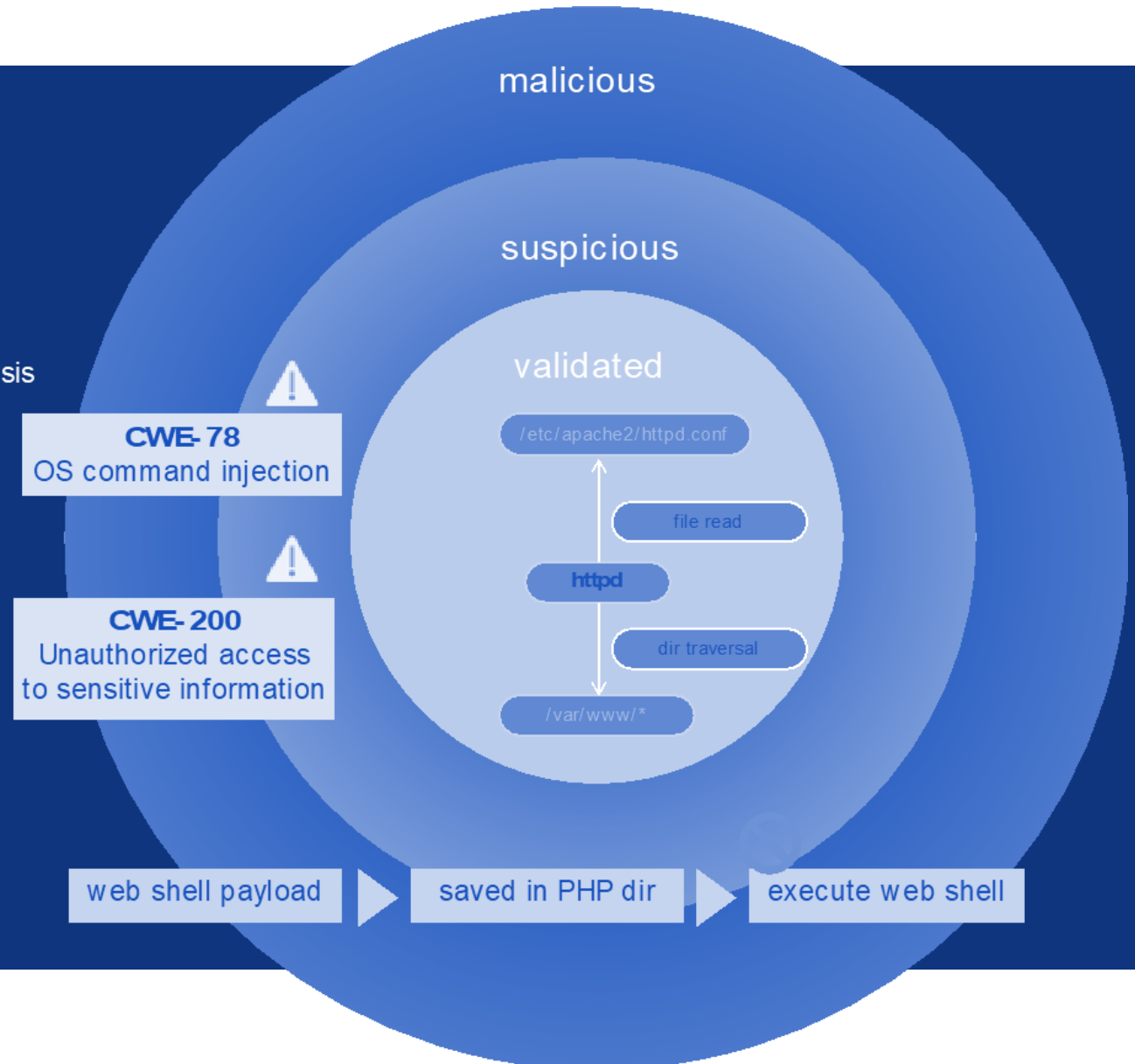
# Unknown vulnerability protection

## Runtime protection against unknown exploits

Security efficacy and efficiency with multi-stage AI analysis  
Unique application process behavior graph  
Common Weakness Enumeration (CWE) analysis  
Application-specific behavior classifications

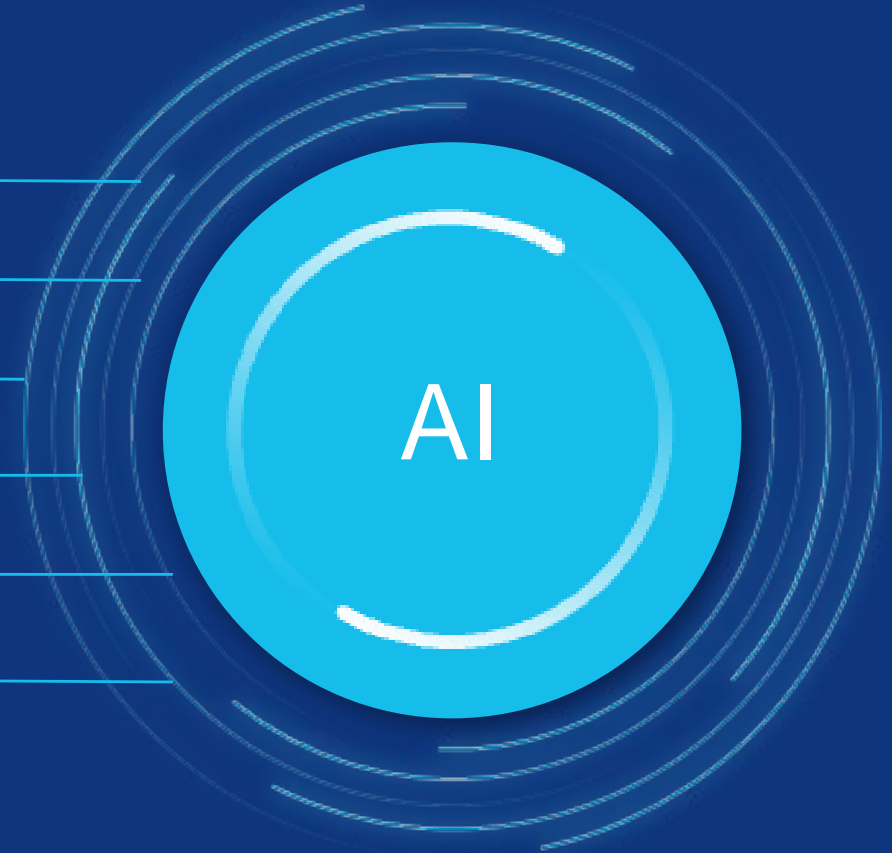
## Detect, block, isolate

Asset-specific AI-guided graduated responses



# Comprehensive inputs for policy creation

Network flows  
Process behaviors  
File changes  
Anonymized app behavior  
Threat intel updates (Talos)  
Learned policy preferences  
...



# Cisco Hypershield Policy Model

## "PARC" Policy Model

Principal

Action

Resource

Conditions

Effect

Priority

Guardrails/Governance Policies

Zone- Based Guardrails

Block Well- Known Bad

Universal Known Malicious

Compensating Controls

Distributed Shielding

App Team

Declare Policy

Well-defined common services/Connectivity requests

App Intent

Permit Belief

Auto- Generated Policies

Review / Block New

Risk evaluate new and suspicious

# AI in Hypershield

AI-Native – AI modules as building blocks to deliver capabilities in Hypershield

## Use Cases

ML: Self qualifying updates

Autonomous Segmentation

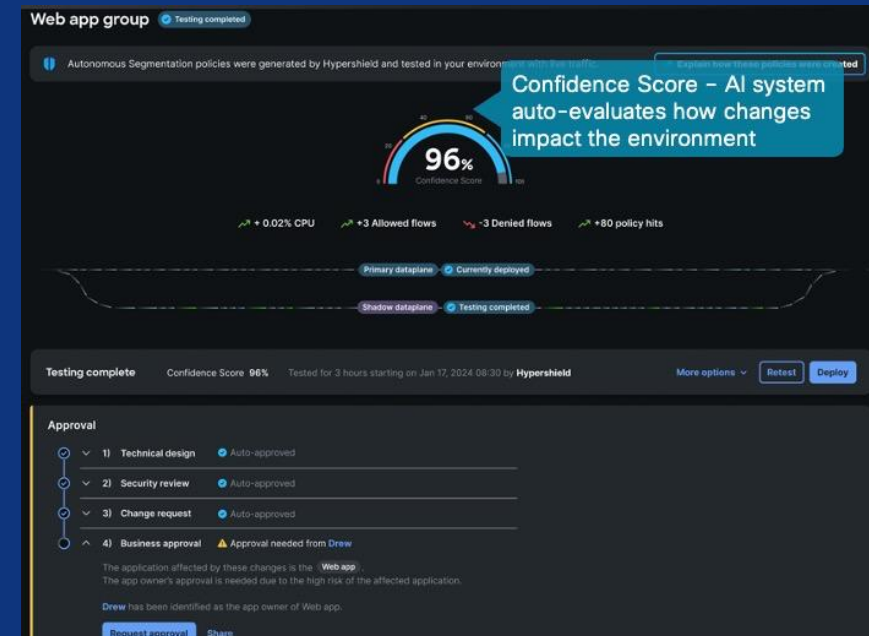
Gen AI: Distributed Exploit Protection

AI Assistant

...



## Digital Twin : Verify AI recommendation



# Summary – HyperShield Innovations

**OUTCOMES THAT MATTER**  
for customer network and app deployments



**LEVERAGING AI**  
for enhanced visibility and control



**SECURITY**

**O11Y**  
(OBSERVABILITY)

Network & App Infra

# 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 2026.



**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 mobile 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](https://www.CiscoLive.com/on-demand)

**Thank you**

**CISCO** Live !

