

CISCO Live !

Live Protect on IOS-XE

Ninad Diwakar
Technical Marketing Engineer

Aishwarya Sudeep
Product Manager

With special thanks to
Ama Owusu-Hammond
Technical Marketing Engineer

BRKENS-2615

Cisco Webex App

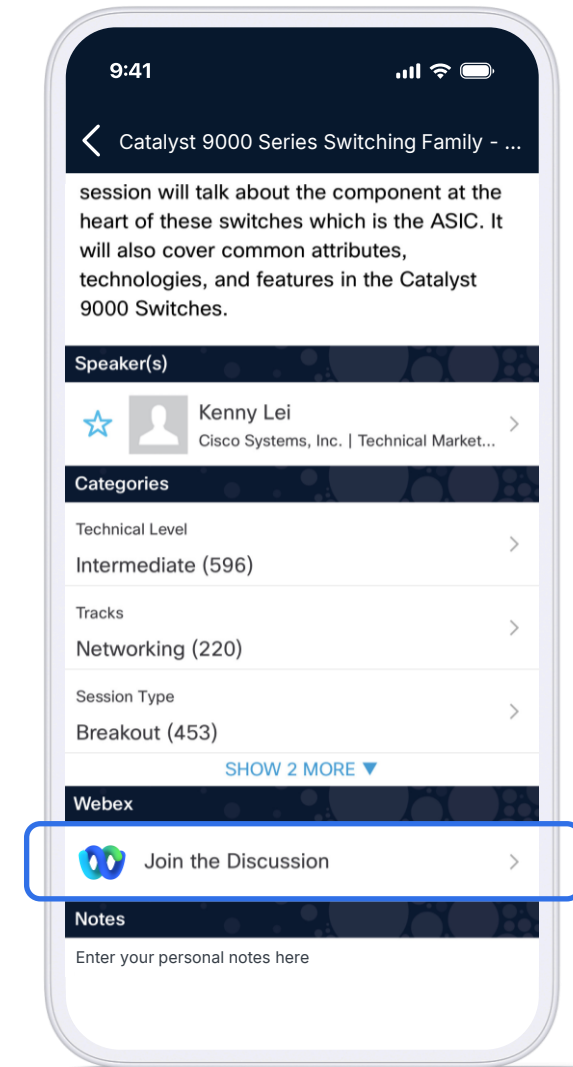
Questions?

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, 2026.



<https://ciscolive.ciscoevents.com/clamer26/BRKENS-2615>

Agenda

- 01 Introduction**
- 02 Vulnerabilities Overview**
- 03 Live Protect**
- 04 eBPF and Tetragon Ecosystem**
- 05 Tetragon on IOS-XE**
- 06 Supported Operations & Platforms**

Existing methods of fixing vulnerabilities

Cisco already offers methods to deal with PSIRTs and keep your network secure.

Software Maintenance Update (SMU)

- Software patch for IOS XE
- **Sometimes** requires reboot
- Fixes existing/running code version
- Released weeks or months

Integrated into a release

- Bug fix integrated into new software release
- Provides complete remediation
- Operational burden to plan maintenance and testing windows to new software version

Attack isolation

SELinux

- Security-Enhanced Linux
- Defines mandatory access controls for applications, processes, and files
- Generated at build time, cannot be changed
- Not granular (allow/deny only)

Friction with Upgrading Software Versions

To prevent **downtime**, we open ourselves to **downtime**

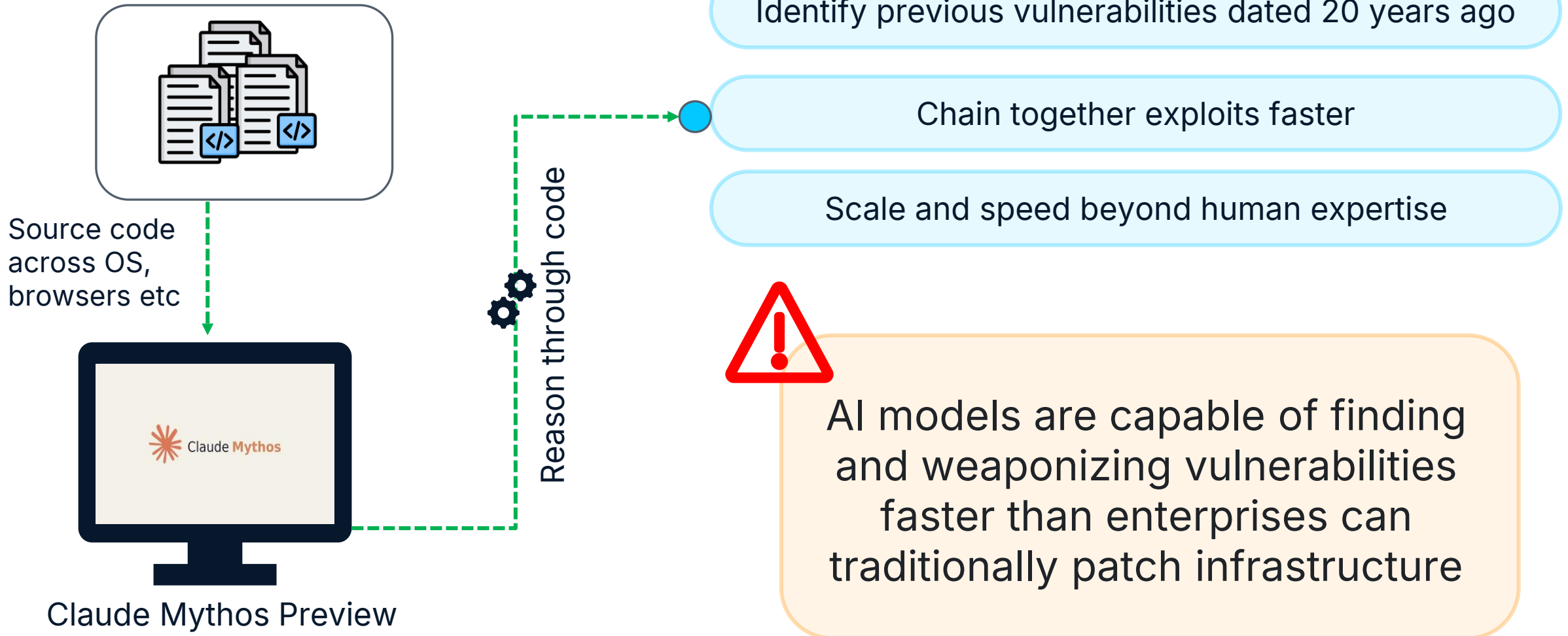
- Customers don't update network devices to avoid reboots and downtime
- This means they are open to critical CVEs
- This opens the network up to downtime

- Once a CVE becomes public, attackers can reverse engineer the vulnerability quickly
- That gap between CVE disclosure and safe deployment of upgrades creates a dangerous exposure window

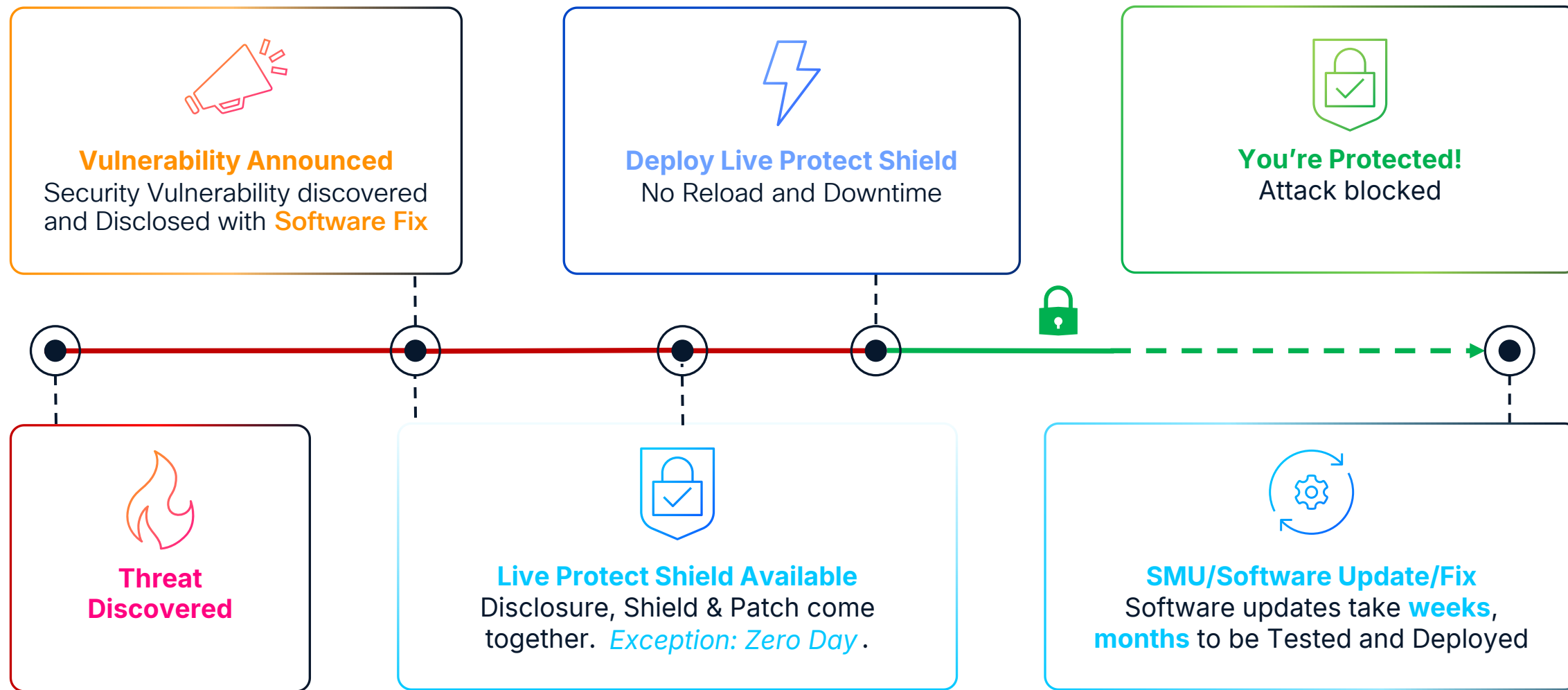
Name	Type	Up Time	SKUs
ADW-UMS-B-5-5006-SWX-02		18y 7m 16d 0h 52m	WS-C3560G-24TS-S

Project Mythos

Vulnerabilities in era of AI



How **Live Protect** Works



Protect now, Patch in Planned Window

Live Protect



Live Protect Shields *compensate* for a vulnerability until it can be *fixed*.



Vulnerable



Live Protect Shield



Fixed

eBPF and Tetragon Ecosystem



eBPF

eBPF is a Linux kernel technology that lets you run safe, sandboxed programs directly inside the kernel and modify kernel behavior at runtime—without changing kernel code



Cilium

Cilium is an open-source project that leverages eBPF to deliver high-performance networking, security, and observability functionality for containers and microservices.



tetragon

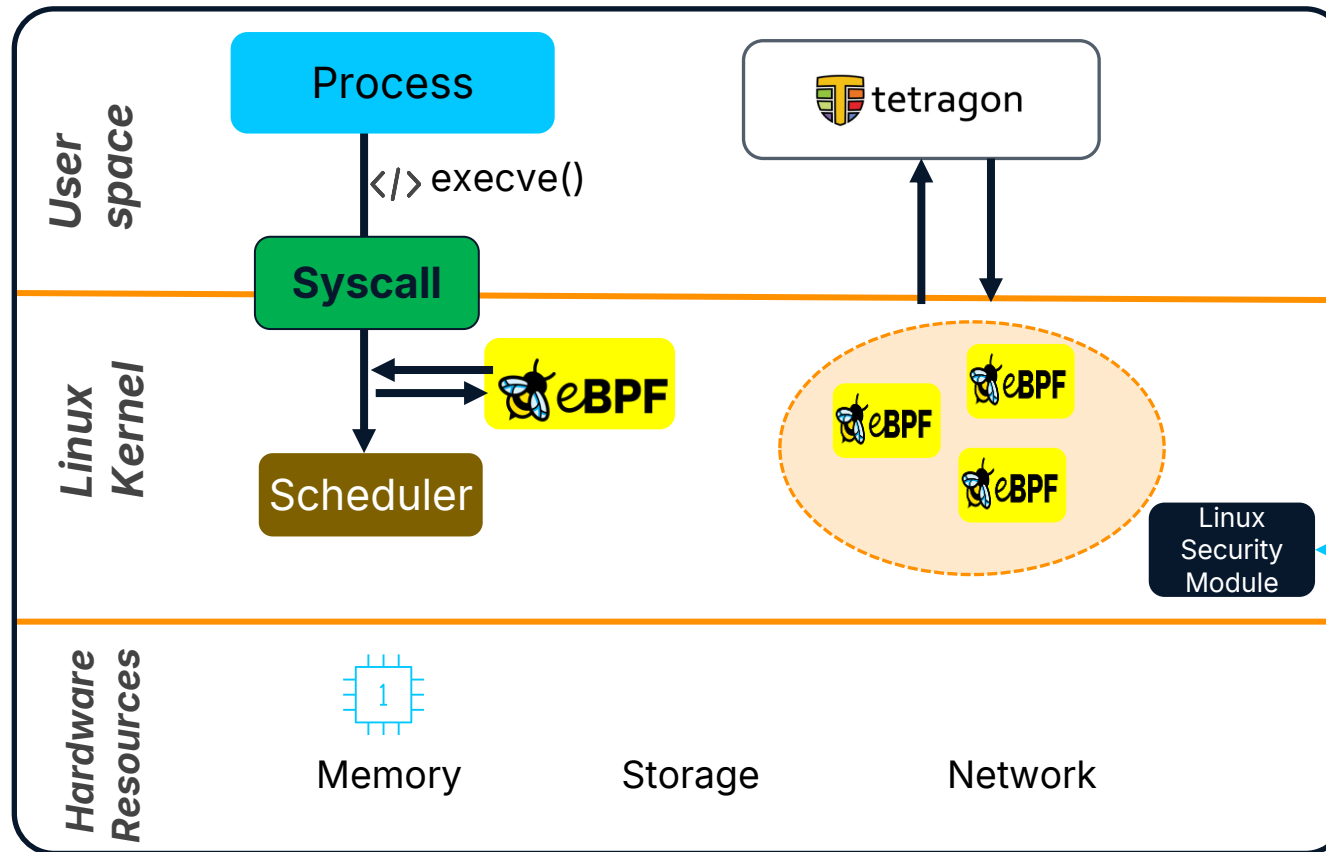
Tetragon is an open source security and observability tool leveraging eBPF to provide deep insights into system behavior and enforce security policies directly within the Linux kernel.

Isovalent Enterprise



1. ***This brings eBPF + Cilium into Cisco's portfolio***
2. ***Expands Cisco security portfolio by adding Tetragon to security offerings***
3. ***Kernel-Level Security & Zero Trust***

eBPF – The Infrastructure Technology Revolution



Traditionally, to change how kernel works or manages, you'd have to modify its source code, recompile it, and reboot.

eBPF Programs

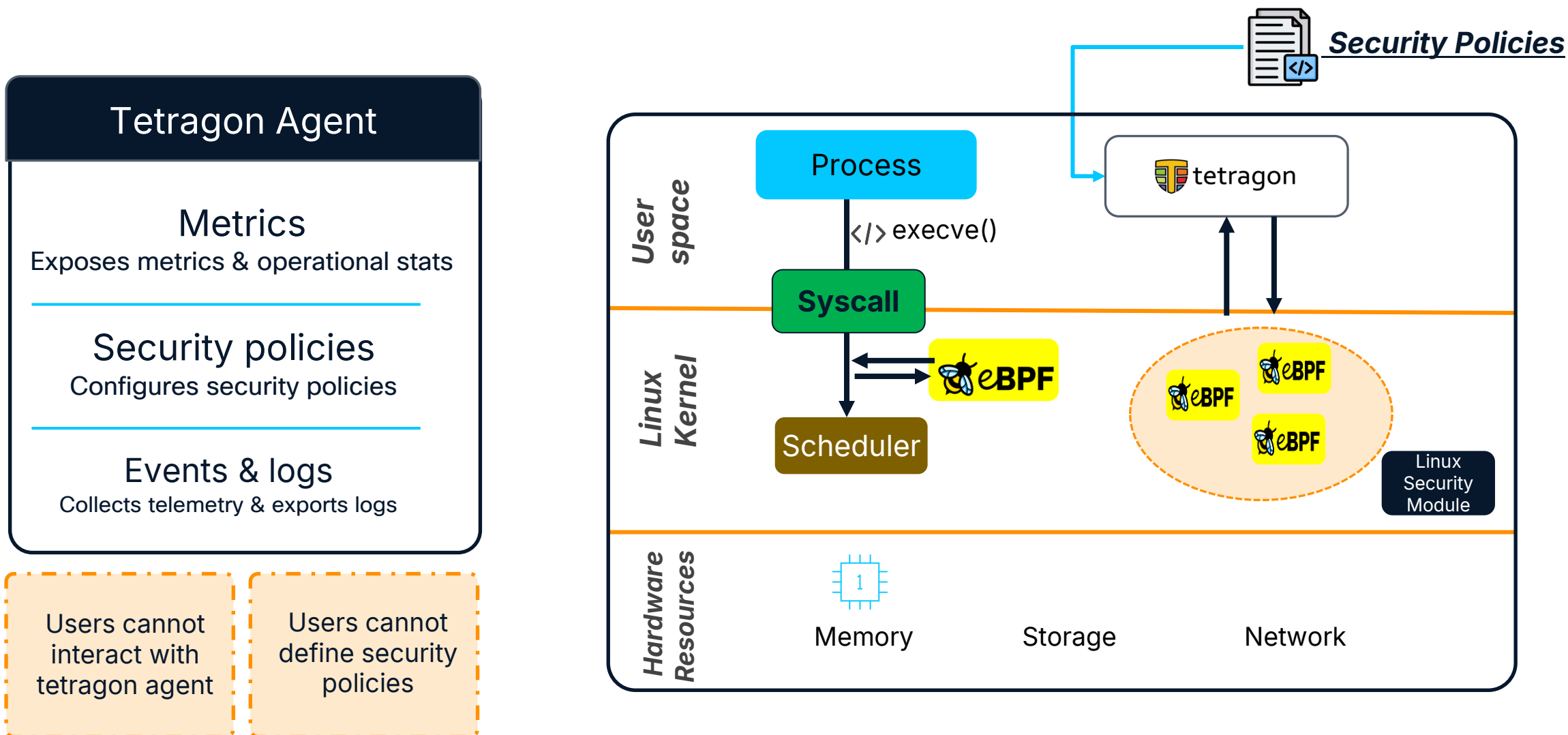
Attaches to syscalls, kprobes, networking hooks

Executes enforcement logic in real time

Sends events back to Tetragon agent

eBPF makes the Linux Kernel Programmable

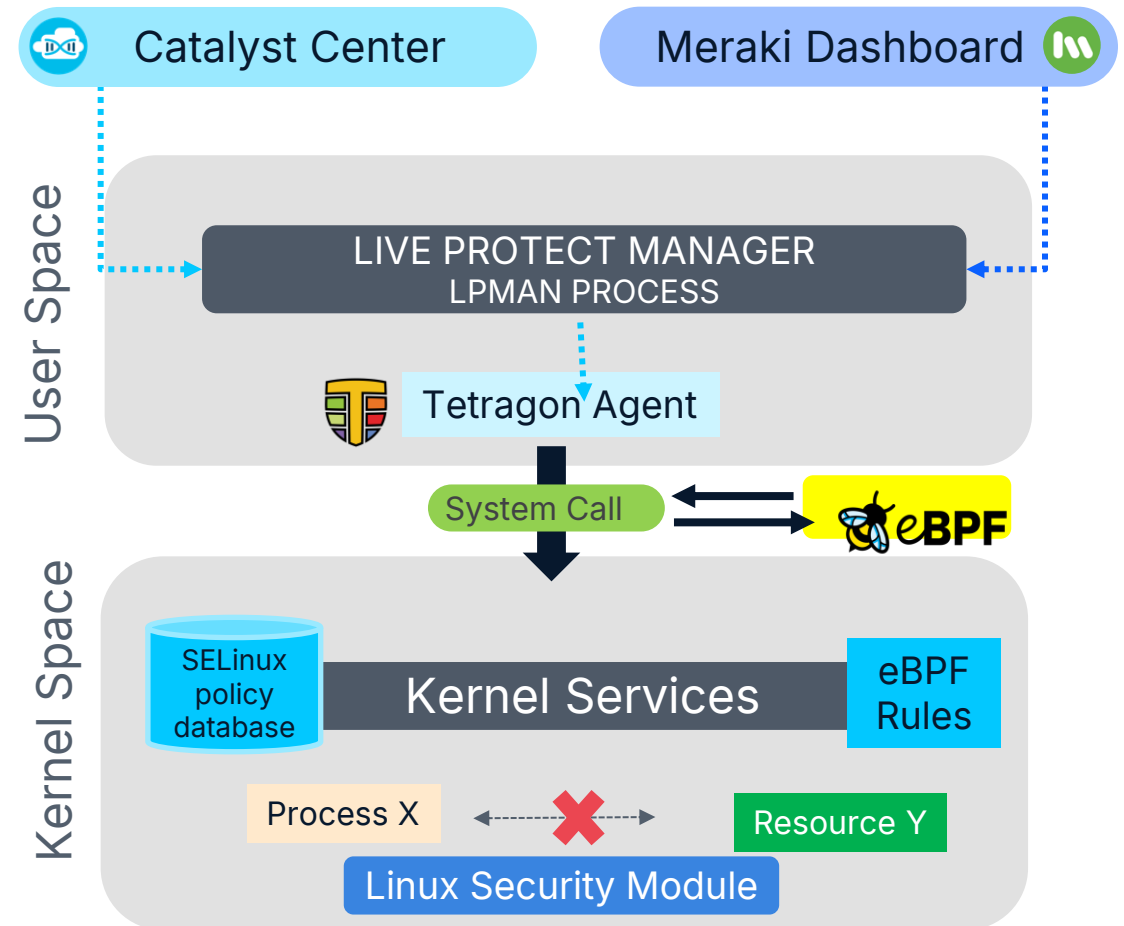
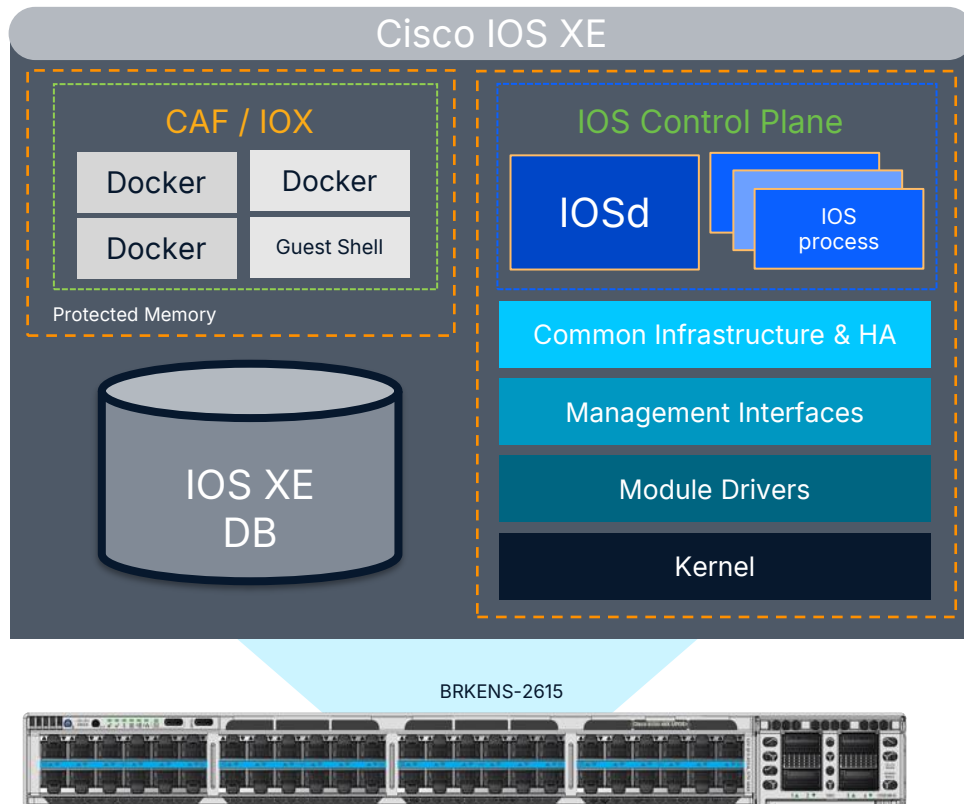
Tetragon : Security Observability and Runtime tool



Tetragon on Cisco IOS XE

Native eBPF & SELinux

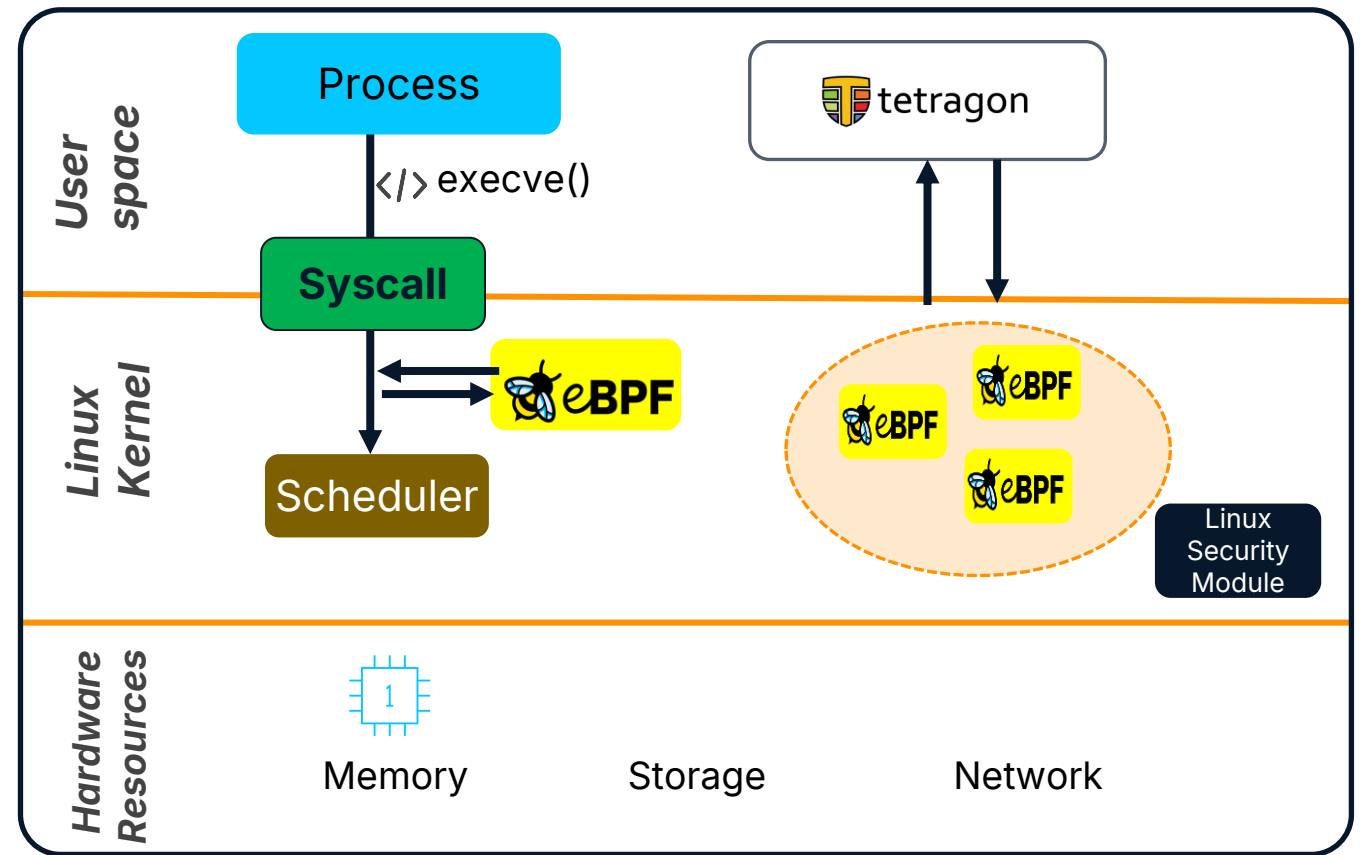
Leverage eBPF based control in Cisco IOS XE Linux Kernel to implement dynamic low-level system protection. Complements SELinux rules.



How a vulnerable packet is handled in network stack

Without live protect, vulnerable service/process is reached

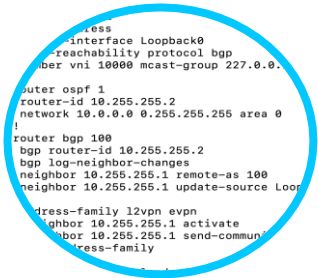
- 6 Vulnerable service or process never reached
- 5 eBPF policies evaluate packet contents and execute based on rule
- 4 Syscall for process is triggered and eBPF program is deployed
- 3 Packets enter linux kernel
- 2 Destination is to switch itself and punted to CPU (**forwarding packets never reach kernel**)
- 1 Malicious packet enters network interface



Security Policies for eBPF Programs

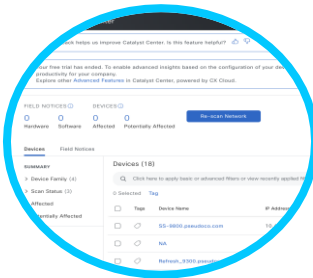
- Policies are delivered as shields in a .bin artifact
- Defines allowed processes, syscalls, network, and file operations
- Policies configured via Tetragon agent in user space
- Tetragon translates policies into eBPF-based enforcement
- eBPF programs are loaded into linux kernel
- Hooks execute automatically during runtime events

Mode of Operations



CLI

- Configure via command line
- YANG Models
- Provision compensating controls
- Monitor status
- Send alerts and logging off-box



Catalyst Center

- View CVEs
- Deploy controls
- Monitor status
- Logging of shield hits



Meraki Dashboard

- View CVEs
- Deploy controls
- Monitor status
- Logging of shield hits

Mode of Deployment



Observing

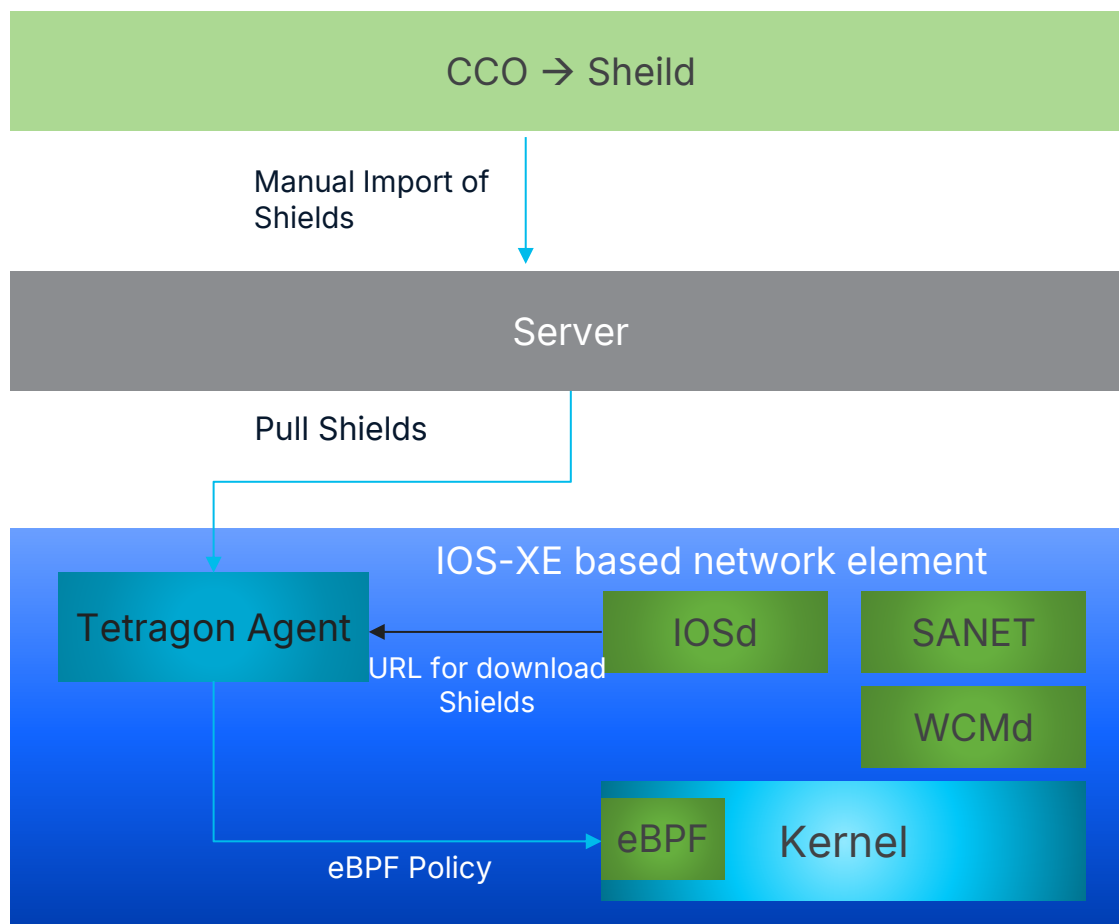
Detect and report on potential compromises



Protecting

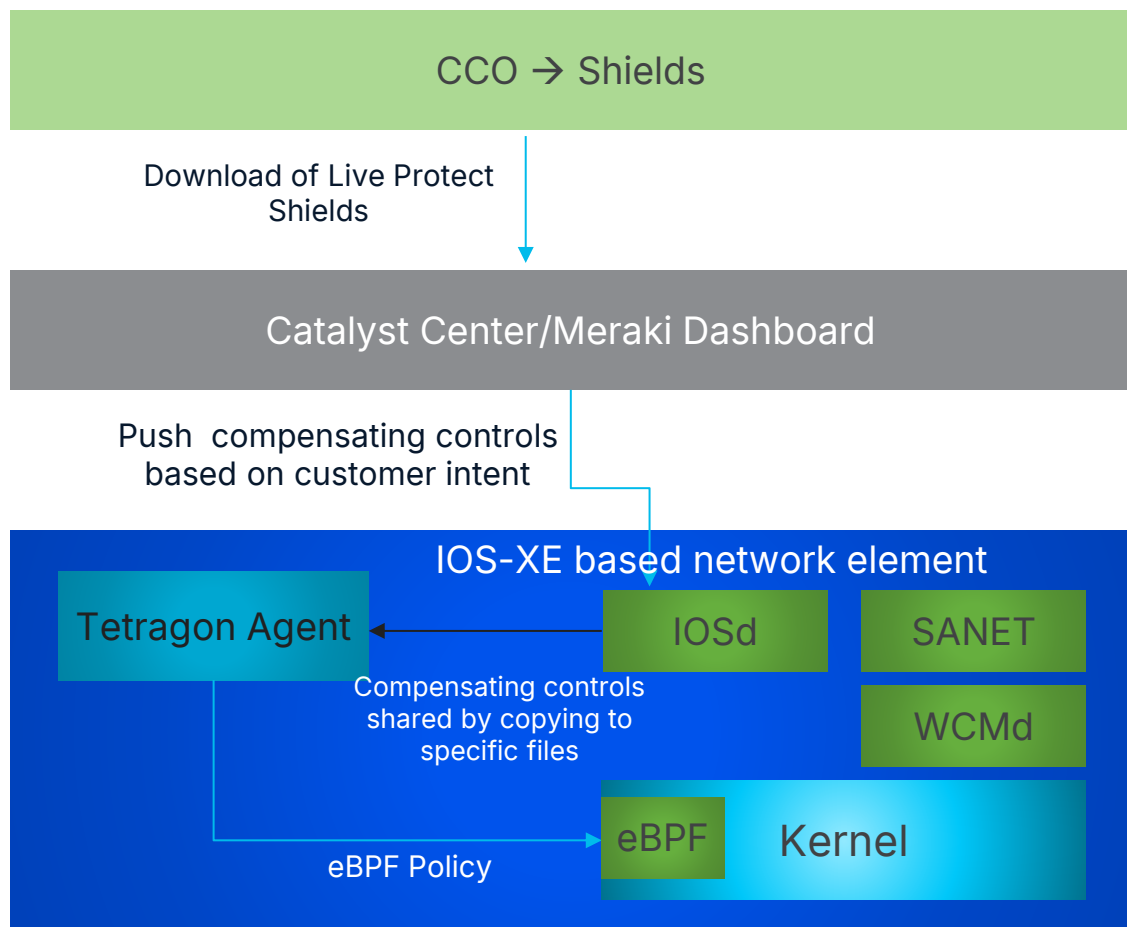
Block and report on potential compromises

Architecture for Non-Controller Based Deployments



- Tetragon agent integrated into IOS-XE as a binos process
- IOSd CLI deployment will be similar to what is done for SMU
- Customers have to manually download the required shields from CCO and store in server
- Tetragon agent will pull the shields periodically and deploy in the kernel
- The shields should have context about the CVEs that are addressed and the specific platform(s) affected (switches, routers, APs, wireless LAN controllers) – this will help in determining which CVEs are applicable for a specific device

Architecture for Controller Based Deployments



- Tetragon agent integrated into IOS-XE as a binos process
- Catalyst Center will pull shields from CCO – allows customers to know which PSIRTs have exploit protection capabilities.
- IOSd configuration triggered from controllers push the controls to specific files that will be monitored by the agent to then deploy in the kernel
- The shields should have context about the CVEs that are addressed and the specific platform(s) affected (switches, routers, APs, wireless LAN controllers) – this will help in determining which CVEs are applicable for a specific device

Demo Video

Two-factor Authentication is not currently enabled on your Meraki Dashboard account. For an extra layer of security, we recommend [enabling it](#) at your earliest convenience.

Meraki

- Network
- Security Advisory Switch Network
- Network-wide
- Assurance
- Switching
- Organization
- Security
- Automation

Find in Menu (⌘+K)

+

Map

Satellite

Address, zip code, etc.

Go

Hide table

Networks

Network tags

Devices

Search...

1 network

Name	Usage
Security Advisory Switch Network	None

1 total

Platform and License Support

Platform	Minimum IOS-XE version	License
C9350	26.2.1	Network Essentials
C9550	26.2.1	Network Essentials
C9610	26.2.1	Network Essentials

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 2027.



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



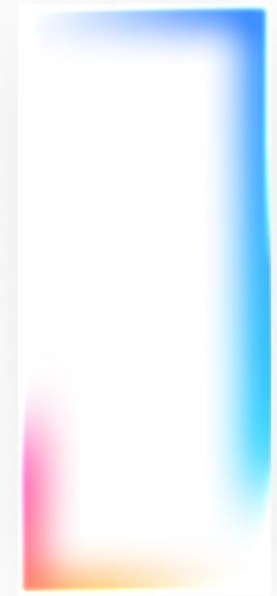
Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

CISCO Live !

Thank you





Deploying compensating controls via CLI/YANG

Step	Purpose	Suggested CLI Command
Add	Add the control from a URL, download, or file but does not activate.	<code>compensating-control add</code>
Activate	Run hw/sw compatibility checks, install and enable CC	<code>compensating-control activate <audit enforce></code>
Commit (optional)	Commits the comp. control to persist after reloads	<code>compensating-control commit</code>
Deactivate	Disables the comp. control while leaving it available	<code>compensating-control deactivate</code>
Remove	Removes control making it unavailable for future use	<code>compensating-control remove</code>

Note: This syntax flow is nearly identical to the SMU flow. "Rollback" has been removed as "Deactivate" should be adequate to achieve this.

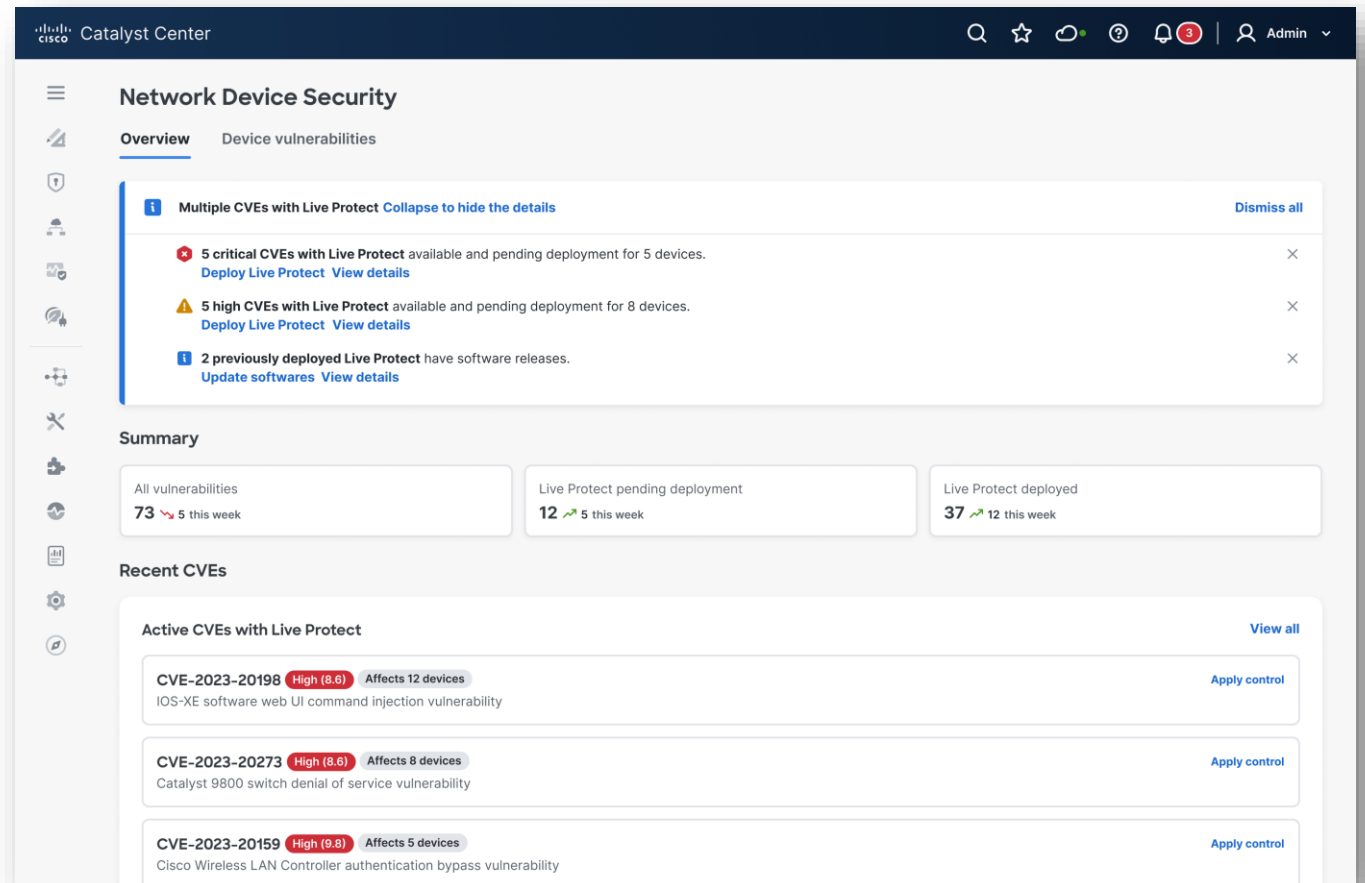
Monitoring compensating controls via CLI/YANG

Step	Purpose	Suggested CLI Command
Summary	View installed controls by name and ID and status (installed, active, etc.)	<code>show compensating-control summary</code>
Detail	Look at details for control, including description, relevant metadata, hits (if relevant)	<code>show compensating-control <ID> detail</code>
Logging	Syslog details from compensating control	<code>show log</code>

Note: YANG models should be available to provide equivalent functionality to all show commands.

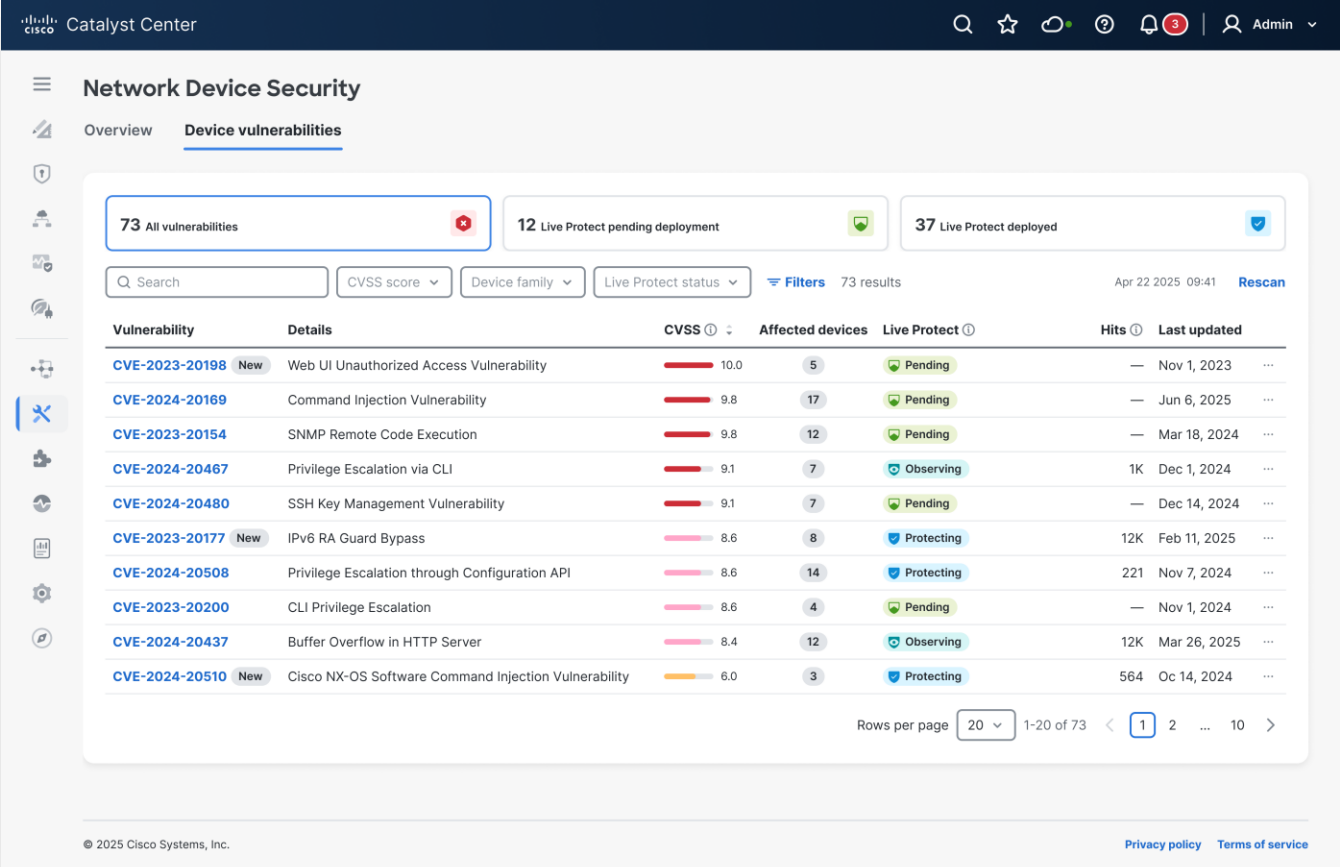
Overview Dashboard

- Overview of network devices' security status
- Highlights active vulnerabilities (CVEs) with available, but not yet applied fixes
- Visual trend shows how fixes reduce network security risks over time



Vulnerabilities Listing

- Prioritize critical issues (Severity, exploitable vulnerabilities, deployment status)
- Show Live Protect status badges (e.g. "Pending")
- Display triggered or blocked exploit attacks as "Hits"

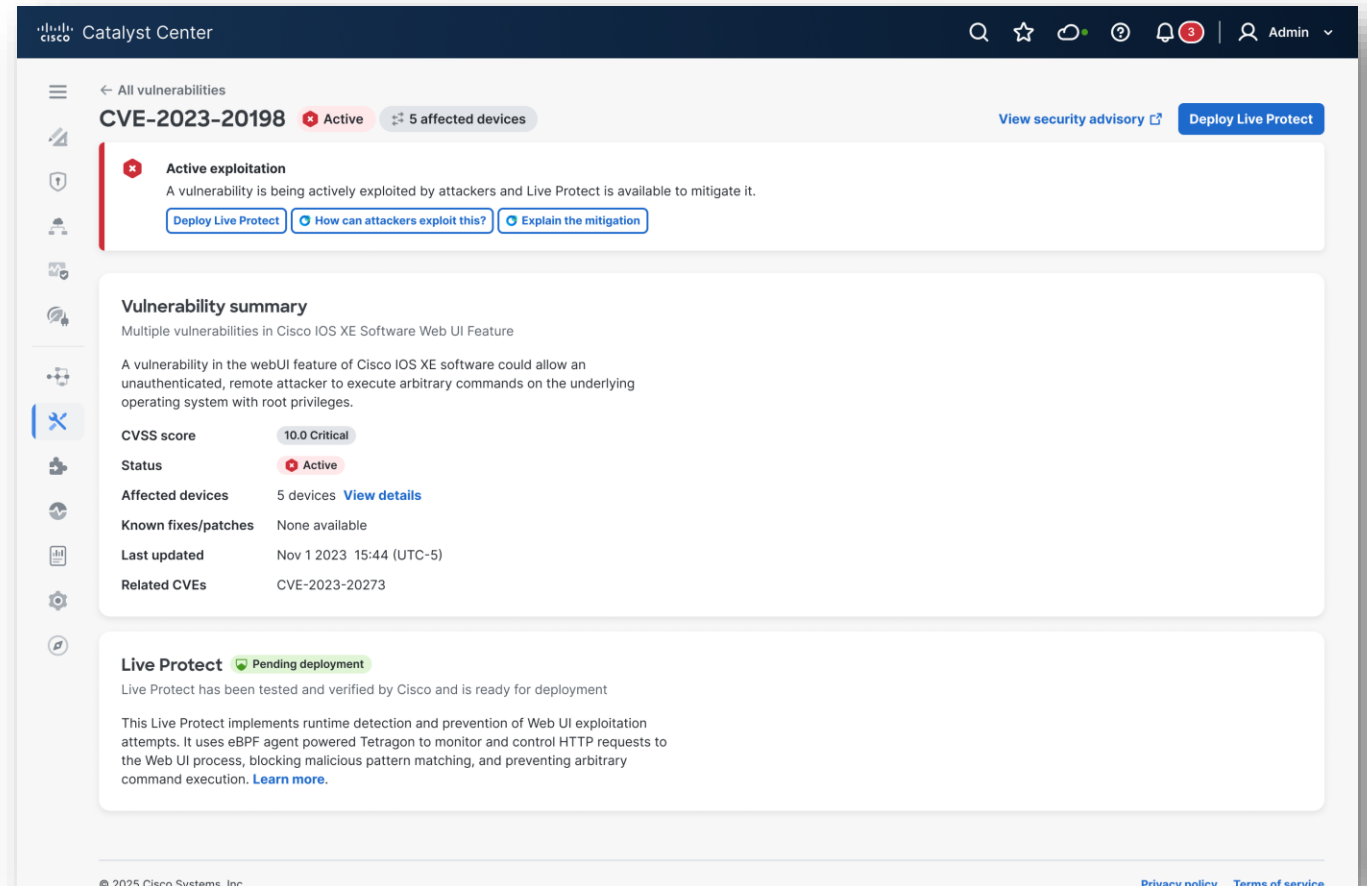


The screenshot displays the Cisco Catalyst Center interface for Network Device Security. The 'Device vulnerabilities' tab is active, showing a summary of 73 vulnerabilities, 12 pending Live Protect deployments, and 37 deployed Live Protect instances. A table lists individual vulnerabilities with columns for Vulnerability ID, Details, CVSS score, Affected devices, Live Protect status, Hits, and Last updated. The table includes entries for CVE-2023-20198, CVE-2024-20169, CVE-2023-20154, CVE-2024-20467, CVE-2024-20480, CVE-2023-20177, CVE-2024-20508, CVE-2023-20200, CVE-2024-20437, and CVE-2024-20510. The interface also features a search bar, filters for CVSS score, Device family, and Live Protect status, and a 'Rescan' button.

Vulnerability	Details	CVSS	Affected devices	Live Protect	Hits	Last updated
CVE-2023-20198 New	Web UI Unauthorized Access Vulnerability	10.0	5	Pending	—	Nov 1, 2023
CVE-2024-20169	Command Injection Vulnerability	9.8	17	Pending	—	Jun 6, 2025
CVE-2023-20154	SNMP Remote Code Execution	9.8	12	Pending	—	Mar 18, 2024
CVE-2024-20467	Privilege Escalation via CLI	9.1	7	Observing	1K	Dec 1, 2024
CVE-2024-20480	SSH Key Management Vulnerability	9.1	7	Pending	—	Dec 14, 2024
CVE-2023-20177 New	IPv6 RA Guard Bypass	8.6	8	Protecting	12K	Feb 11, 2025
CVE-2024-20508	Privilege Escalation through Configuration API	8.6	14	Protecting	221	Nov 7, 2024
CVE-2023-20200	CLI Privilege Escalation	8.6	4	Pending	—	Nov 1, 2024
CVE-2024-20437	Buffer Overflow in HTTP Server	8.4	12	Observing	12K	Mar 26, 2025
CVE-2024-20510 New	Cisco NX-OS Software Command Injection Vulnerability	6.0	3	Protecting	564	Oc 14, 2024

Vulnerability Detail View

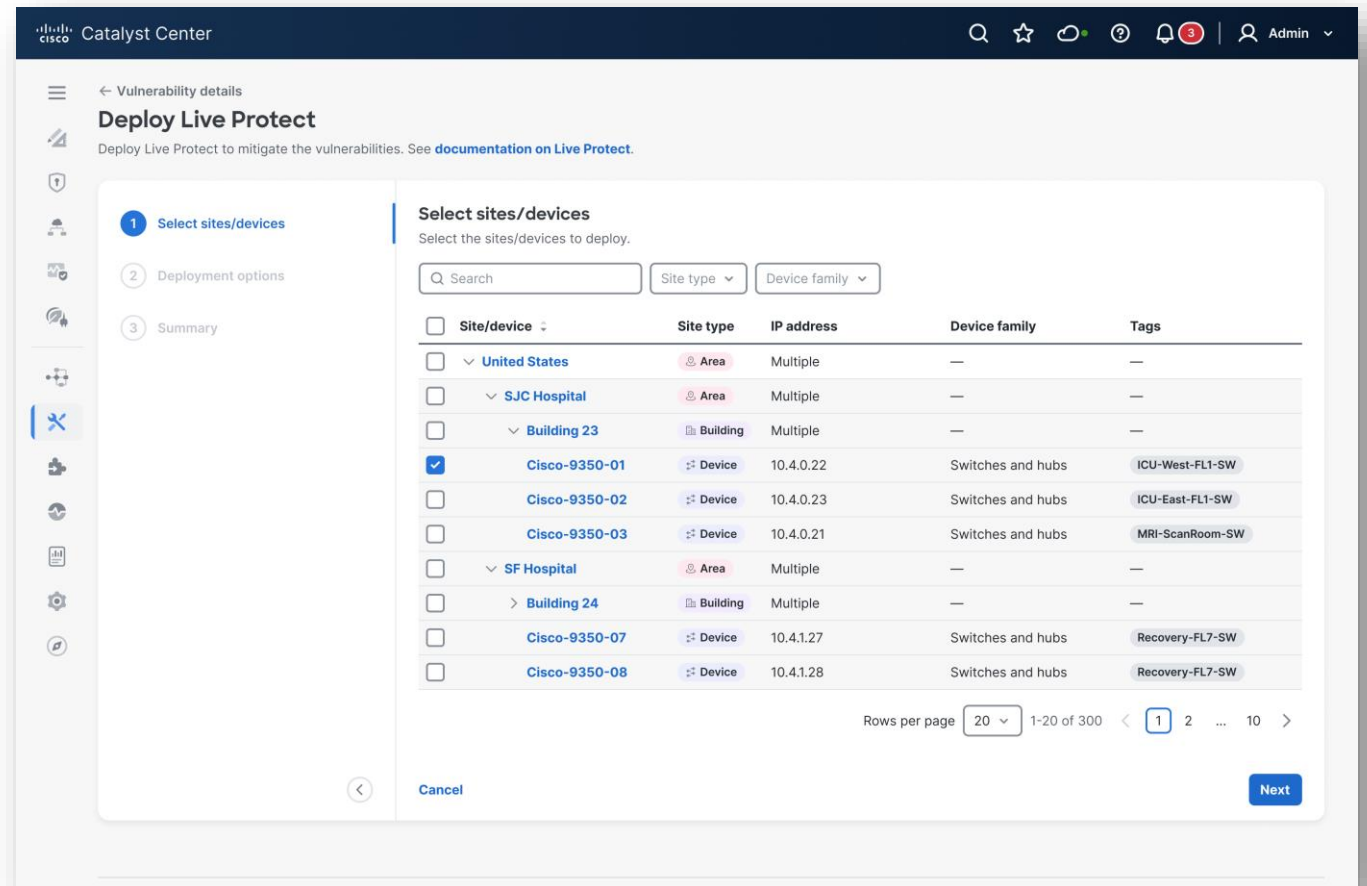
- Click CVE to view its detailed vulnerability page
- Network and security team can apply compensating control to block CVE
- AI Assistant explains the attack's impact and behavior
- "Deploy Compensating Control" button provide clear next steps



Deployment Workflow

- Deploying Live Protect is a simple three-steps process
- Easily select devices using a clear and hierarchical view
- Scalable to support thousands of devices
- Allows users to observe first, then protect their devices

UX prototype



SELinux and Tetragon-based Compensating Controls Coexistence

SMU	SE Linux	Compensating Controls
• 5-6 Week Turnaround • May require reload • Limited Coverage • Needs an available fix for CVE • Release specific	• SELinux policies are generated during the IOSXE build • Many SELinux policies are auto-generated based on the Polaris platform TDL and Lux DSL files • SELinux policies cannot be altered on IOSXE devices (except those controlled by SELinux boolean or by SMU) • SELinux Policies are binary, Allow or Deny, without additional control	• Comp controls provide dynamic policy changes without reload • Comp controls can alter the kernel space or user space functional behavior based on events and parameters • Tetragon offers high performance deep observability of events to trace unexpected system events and behavior • Turnaround in days for high priority • Never requires reload • Can cover ~25% non-SMUable • Blocks CVE even when fix unavailable

Operation



CVE Published to public database. CVE pulled down to Cisco by automated tooling. (Some will be published by us.)

Automation tools select highest risk CVEs based on applicability and CVSS score

Team evaluates which CVEs require immediate response via comp. control

Isovalent responds to CVEs within agreed SLA

Isovalent develops control and sends back to IOS XE teams for publishing

CVE: Common Vulnerabilities and Exposures

CVSS: Common Vulnerability Scoring System