CISCO Connect

Breakout T3S2 : Dépasser les limites du firewall traditionnel

Christophe Sarrazin
Technical solution Architect Cybersecurity
CCIE security #15 104

May 2026

China-nexus cyber threat groups rapidly exploit React2Shell vulnerability (CVE-2025-55182)

by CJ Moses | on 04 DEC 2025 | in Best Practices, Security, Identity, & Compliance, Thought Leadership | Permalink | Comments | Share

December 12, 2025: The blog post was updated to clarify when customers need to update their ReactJS version.

Within hours of the public disclosure of CVE-2025-55182 (React2Shell) on December 3, 2025, Amazon threat intelligence teams observed active exploitation attempts by multiple China state-nexus threat groups, including Earth Lamia and Jackpot Panda. This critical vulnerability in React Server Components has a maximum Common Vulnerability Scoring System (CVSS) score of 10.0 and affects React versions 19.x and Next.js versions 15.x and 16.x when using App Router. While this vulnerability doesn't affect AWS services, we are sharing this threat intelligence to help customers running React or Next.js applications in their own environments take immediate action.

https://aws.amazon.com/blogs/security/china-nexus-cyber-threat-groups-rapidly-exploit-react2shell-vulnerability-cve-2025-55182/

Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications

CRS PRODUCT (LIBRARY OF CONGRESS) Hide Overview ✕

CRS Product Type:	In Focus
CRS Product Number:	IF12798
Topics:	Commerce & Small Business; Defense & Intelligence; Foreign Affairs; H… Science & Technology
Publication Date:	01/23/2025
Author:	Jaikaran, Chris

www.congress.gov/crs-product/IF12798

Infosecurity Magazine source: https://www.infosecurity-magazine.com/news/ai-supercharges-attacks-cybercrime/

www.securityweek.com/two-years-on-log4shell-vulnerability-still-being-exploited-to-deploy-malware/

© 2026 Cisco and/or its affiliates. All rights reserved.

Firewalling needs to evolve to meet today's challenges

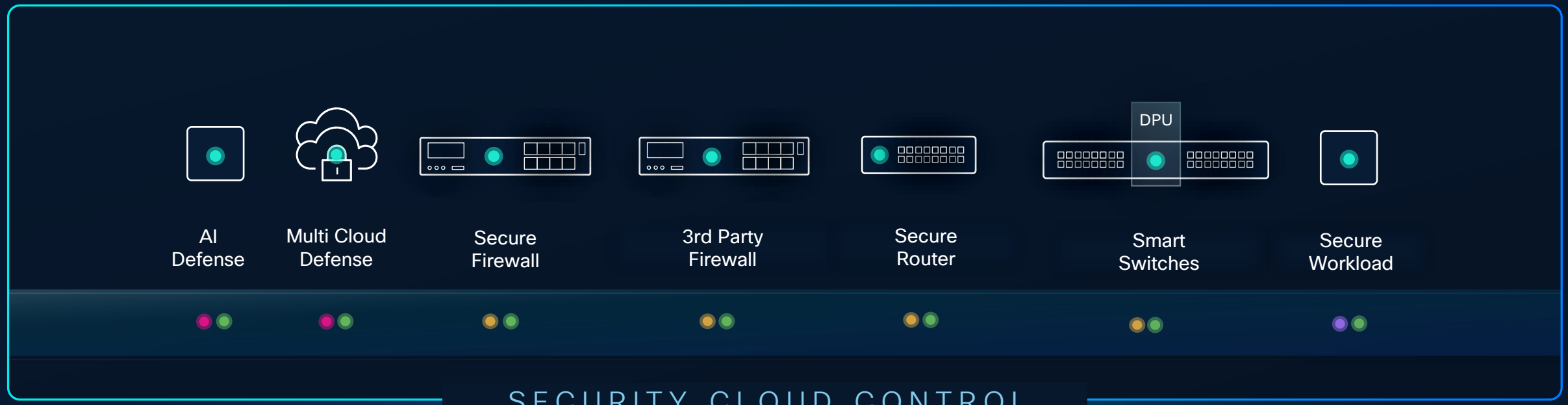
	Stateful Firewall 1990-2007	Next Generation Firewall 2008-2024	Hybrid Mesh Firewall 2025-
Drivers	Growing internet access Basic attacks Need perimeter control	Rise of SaaS/cloud apps Mobile users App layer threats	Increasingly distributed apps Rise of AI Zero trust imperative
Needs	Tracks connection state Filters by IP/port Basic traffic control	App & user aware Integrated threat prevention SSL/TLS decrypt	Hyper-distribution Integrated AI protection AI-powered management

© 2026 Cisco and/or its affiliates. All rights reserved.

Security close to every workload: Hybrid Mesh Firewalling

SECURITY OUTCOMES

Network Segmentation | Macro & Micro Segmentation | Threat Detection & Exploit Protection | AI Security



SECURITY CLOUD CONTROL

Write policy once, enforce across the mesh

Firewall price-performance leader

Top to bottom

Branch — Campus — Data center — Cloud

NEW

200 Series

1 Model

Firewalling + IPS

Up to 1.5 Gbps

1200 Series

6 Models

Firewalling + IPS

Up to 18 Gbps

3100 Series

5 Models

Firewalling + IPS

Up to 45 Gbps

4200 Series

3 Models

Firewalling + IPS

Up to 140 Gbps

NEW

6100 Series

2 Models

Firewalling + IPS

Up to 600 Gbps

Public/Private

20+ cloud variants

HyperFlex

NUTANIX

KVM

openstack

vmware ESXi

aws

Microsoft Azure

Google Cloud Platform

alkira

rackspace technology.

EQUINIX

Alibaba Cloud

ORACLE CLOUD INFRASTRUCTURE

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Advanced FPGA for PQC ready Crypto Engine

Traffic accelerator at the heart of 3100, 4200 and 6100 systems

Security

- Inline Crypto (DTLS, IPsec)
- PQC ready crypto engine
- Cisco Secure Firewall acceleration
- Full stateful processing for traffic being offloaded

Networking

- IPv4 and IPv6 traffic processing
- 2-16M of flows that can be statefully offload from software processing
- Market leading for Watt per Gbps of protected traffic
- Programmable µCode

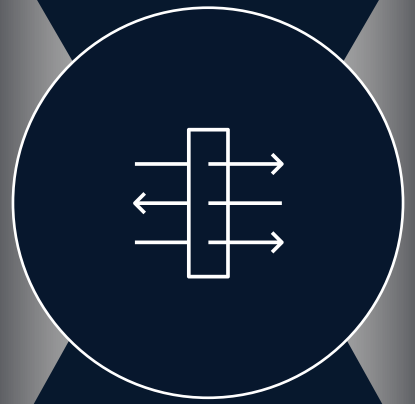
© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco NGFW New Features!

Encrypted Visibility Engine
Simplified configuration of AI/ML-driven detection of apps and malware in encrypted traffic, without decrypting

Splunk Integration for Syslog
Seamless integration empowers administrators to effectively monitor and respond to potential threats in the network.

SnortML
Deep neural network engine to detect exploits, trained on malicious and benign traffic



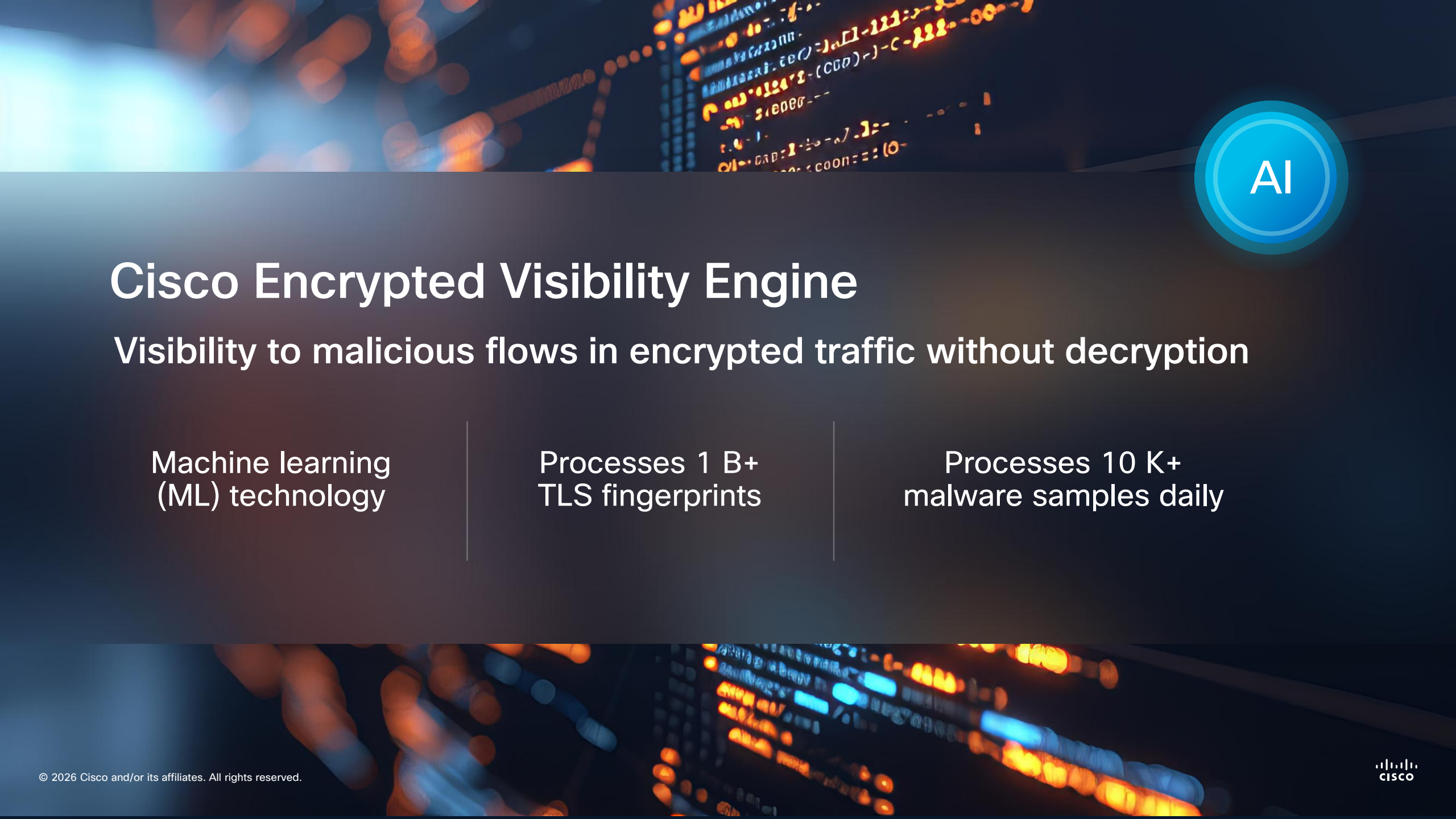
Firewall

Simplified Decryption Policy Creation
Ease of use with the focus on **what** the policy should do, while less focus **how** to generate the policy.

Firewall Upgrade Hardening
Simple, swift, & error-free upgrades with less than 10-clicks from anywhere in the UI to a fully upgraded environment.

Cisco Security Intelligence
Associate an identity source with identity intelligence like Cisco Identity Intelligence (CII)

© 2025 Cisco and/or its affiliates. All rights reserved.



Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

Machine learning (ML) technology

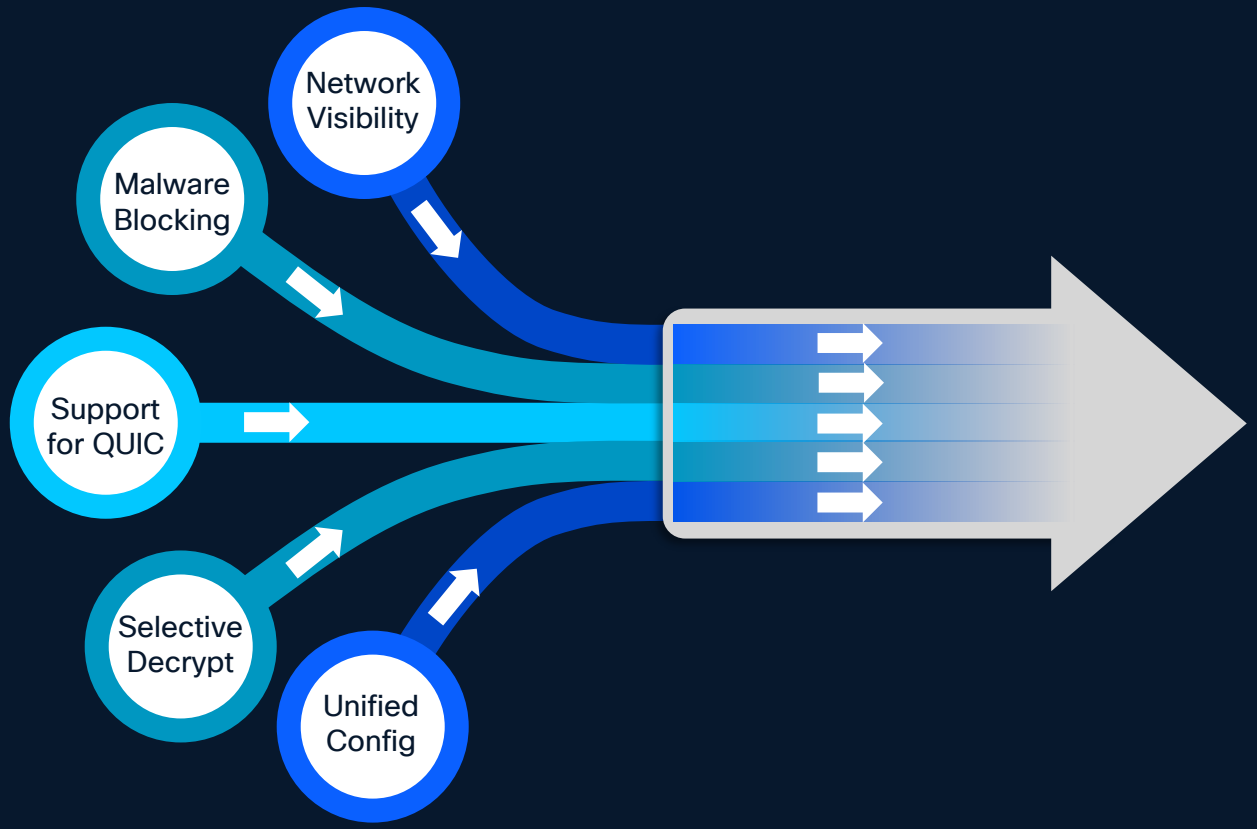
Processes 1 B+ TLS fingerprints

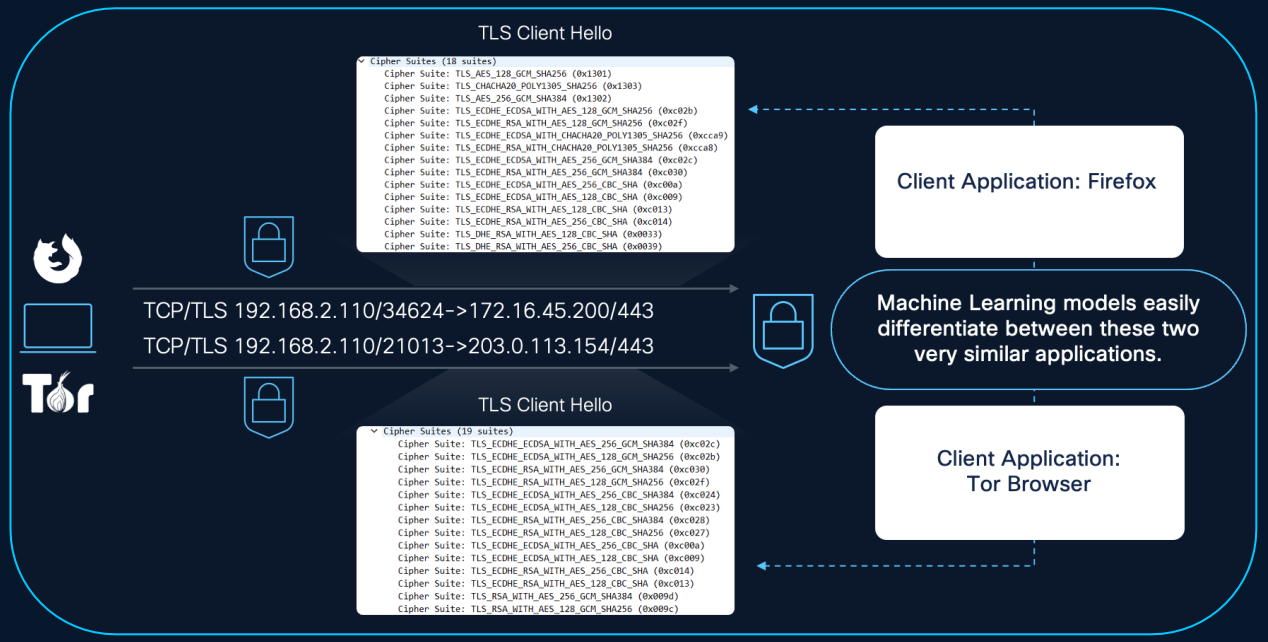
Processes 10 K+ malware samples daily

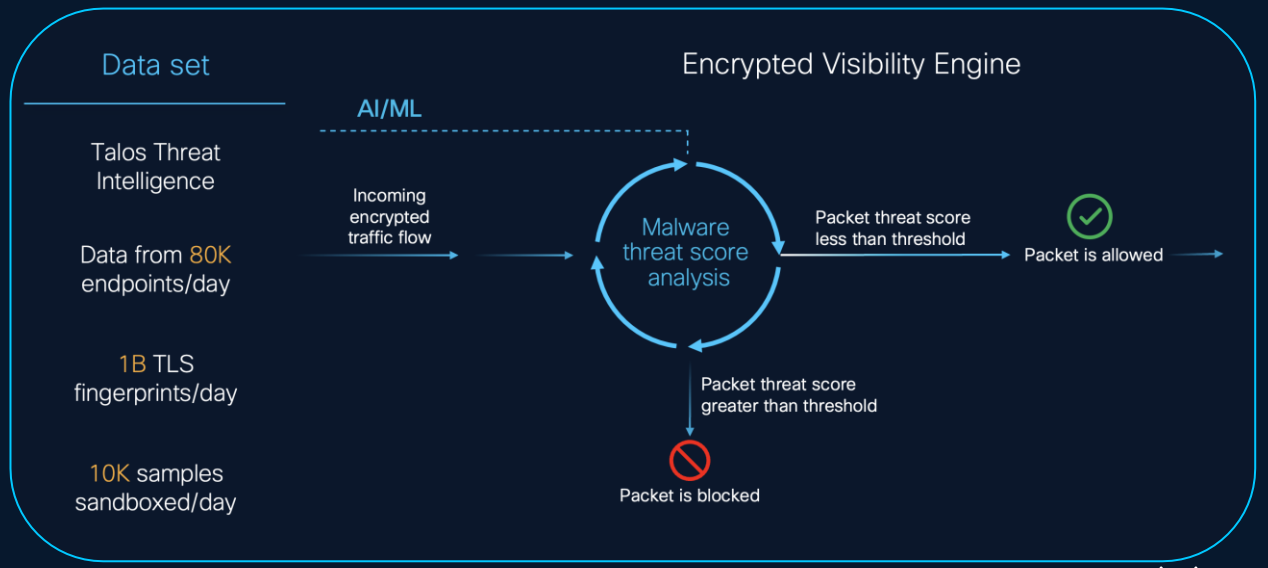
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

EVE Through the Years

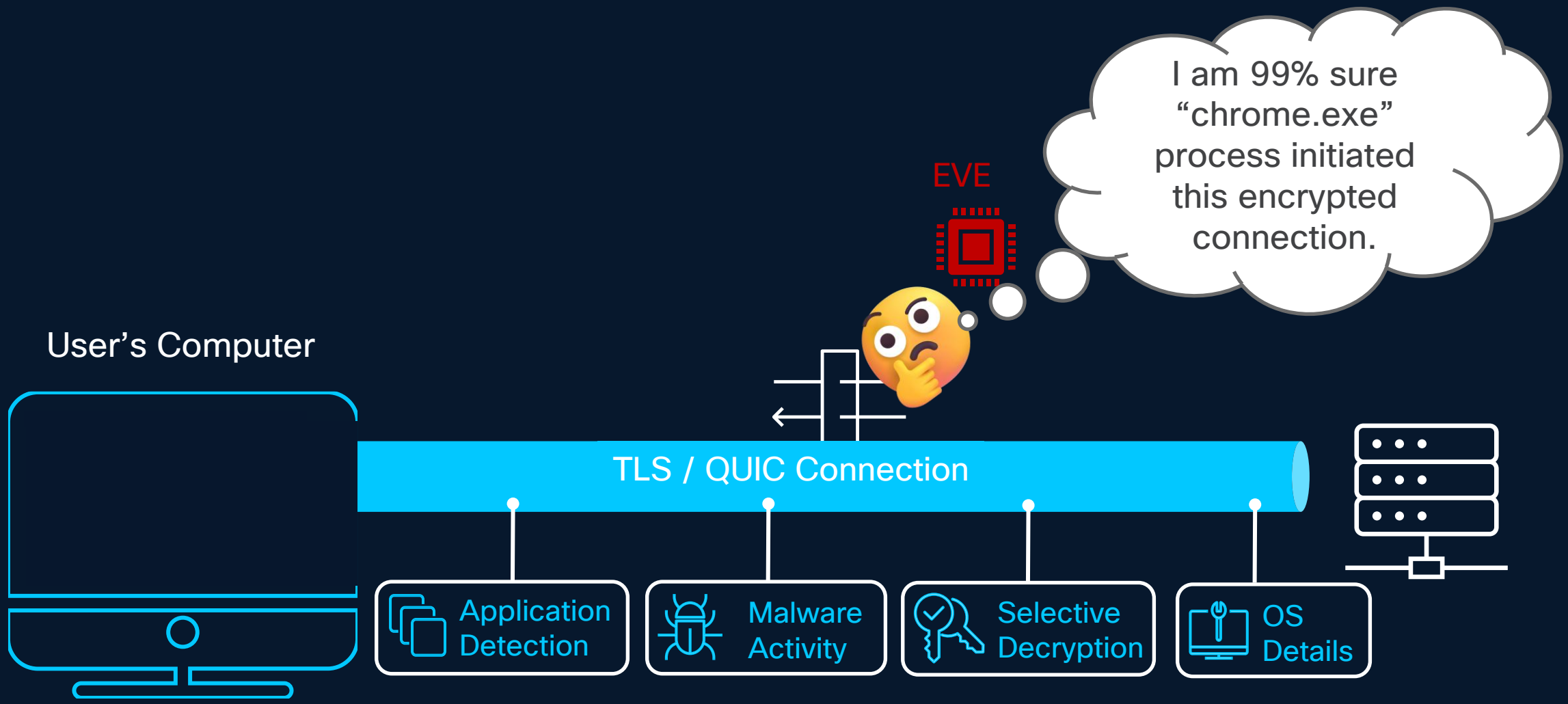






© 2026 Cisco and/or its affiliates. All rights reserved.

What Does Encrypted Visibility Engine Provide?



© 2025 Cisco and/or its affiliates. All rights reserved.

EVE in action: **Malicious flow**

Source / Destination

EVE fingerprint

Threat Level

192.168.10.13	85.214.228.140	443 (https) / tcp		tls/1/(0303)(0a0a1301	98%	malware-ransomware-...	Very High	98%	URL Block, Encrypt
10.67.0.50	13.85.23.86	443 (https) / tcp	Windows Update	tls/1/(0303)(13021301	99%	microsoft networking	Very Low	0%	
10.67.0.50	13.85.23.206	443 (https) / tcp	Windows Update	tls/1/(0303)(13021301	99%	microsoft networking	Very Low	0%	
192.168.25.13	52.185.211.133	443 (https) / tcp	Microsoft	tls/1/(0303)(c02cc02b	99%	microsoft networking	Very Low	0%	
192.168.12.15	54.149.101.221	443 (https) / tcp	Cisco	tls/1/(0303)(c02bc02f	48%	docker	Very Low	0%	
192.168.12.15	54.149.101.221	443 (https) / tcp	Cisco	tls/1/(0303)(c02bc02f	48%	docker	Very Low	0%	
192.168.25.33	99.83.250.143	443 (https) / tcp	Thousand Eyes	tls/1/(0303)(c02cc02b	99%	thousandeyes endpoint ...	Very Low	0%	
10.67.0.154	217.20.49.36	80 (http) / tcp	Microsoft Update	http/(474554)(48545	75%	cisco secure endpoint	Very Low	0%	
192.168.10.13	188.114.97.3	443 (https) / tcp		tls/1/(0303)(c02cc02b	98%	malware-cve-2017-11882	Very High	99%	Encrypted Visibility

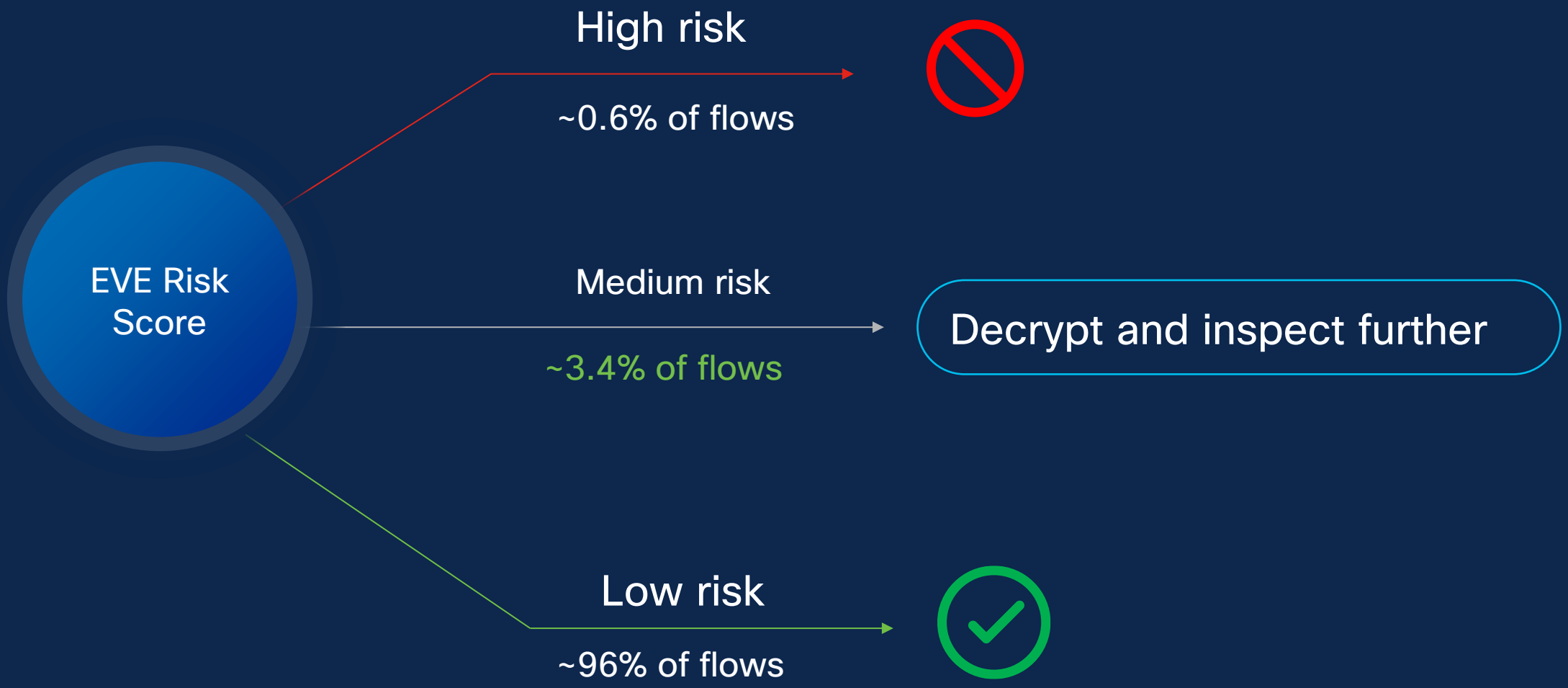
Protocol

Process

© 2025 Cisco and/or its affiliates. All rights reserved.

EVE changes the game on decryption

Risk-based intelligent decryption, powered by Cisco Encrypted Visibility Engine (EVE)



© 2025 Cisco and/or its affiliates. All rights reserved.

Vulnerability Classes

SQL Injection

MySQL, MariaDB, PostgreSQL, Oracle, MS SQL Injection:

CVE-2021-20028 (SonicWall)
CVE-2021-27101 (Accellion)
CVE-2021-30117 (Kaseya)
CVE-2022-21661 (WordPress)
CVE-2022-29383 (Netgear)

Command Injection

Unix/Linux/Windows Shell Injection:

CVE-2020-4006 (VMware)
CVE-2020-4211 (IBM)
CVE-2021-3060 (Palo Alto Networks)
CVE-2021-22123 (Fortinet)
CVE-2021-25296 (Nagios)
CVE-2022-28572 (Tenda)
CVE-2022-28573 (D-Link)
CVE-2022-27947 (Netgear)

Cross-Site Scripting

Reflected XSS:

CVE-2025-0133 (Palo Alto Networks)
CVE-2022-27926 (Zimbra)
CVE-2022-28818 (Adobe ColdFusion)

Code Injection

PHP Code Injection:

CVE-2020-5847 (Unraid)

Template Interpolation:

CVE-2021-44228 (Log4j)
CVE-2022-22954 (VMware Workspace)

Expression Language Evaluation (EL, OGNL, etc.):

CVE-2020-3956 (VMware Cloud Director)
CVE-2021-31805 (Apache Struts)

© 2026 Cisco and/or its affiliates. All rights reserved.

zero-day protection with Snort ML

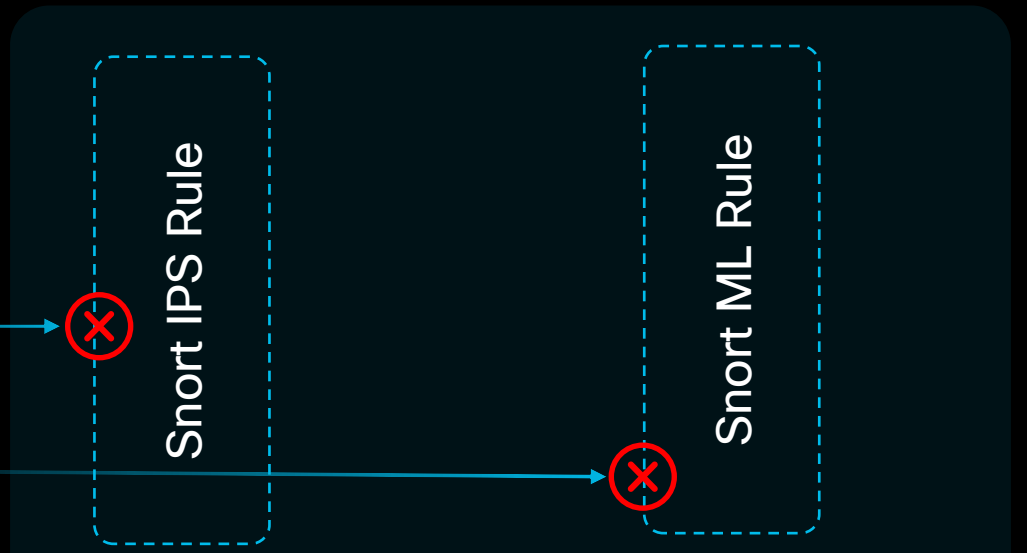
Snort ML extends IDPS protection to unknown variants of common attacks

SnortML uses Machine Learning to expand IPS capabilities

- Trained on all known embodiments for a given vulnerability type
- Detects new patterns for the vulnerability without a static signature
- TLS or QUIC decryption is still required
- Supports Command and SQL Injection attacks today
- Enabled by default in **Maximum Detection** IPS policy

Known SQL injection attack

Zero-day SQL Injection variant



	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
	411:1	(snort_ml) potential threat fo...	Block	Rule Override	Builtins

alert (gid:411; sid:1; rev:2; msg:"(snort_ml) potential threat found in HTTP parameters via Neural Network Based Exploit Detection"; metadata: policy max-detect-ips alert, rule-type preproc; reference:url,blog.snort.org/2024/03/talos-launching-new-machine-learning.html; classtype:unknown;)

(Deep learning model)

Snort Rule

```
alert ( gid:411; sid:1; rev:1; msg:"(snort_ml)
potential threat found in HTTP parameters via Neural
Network Based Exploit Detection"; metadata: policy
max-detect-ips alert, rule-type preproc;
classtype:unknown;)
```

Powered by TALOS Intelligence

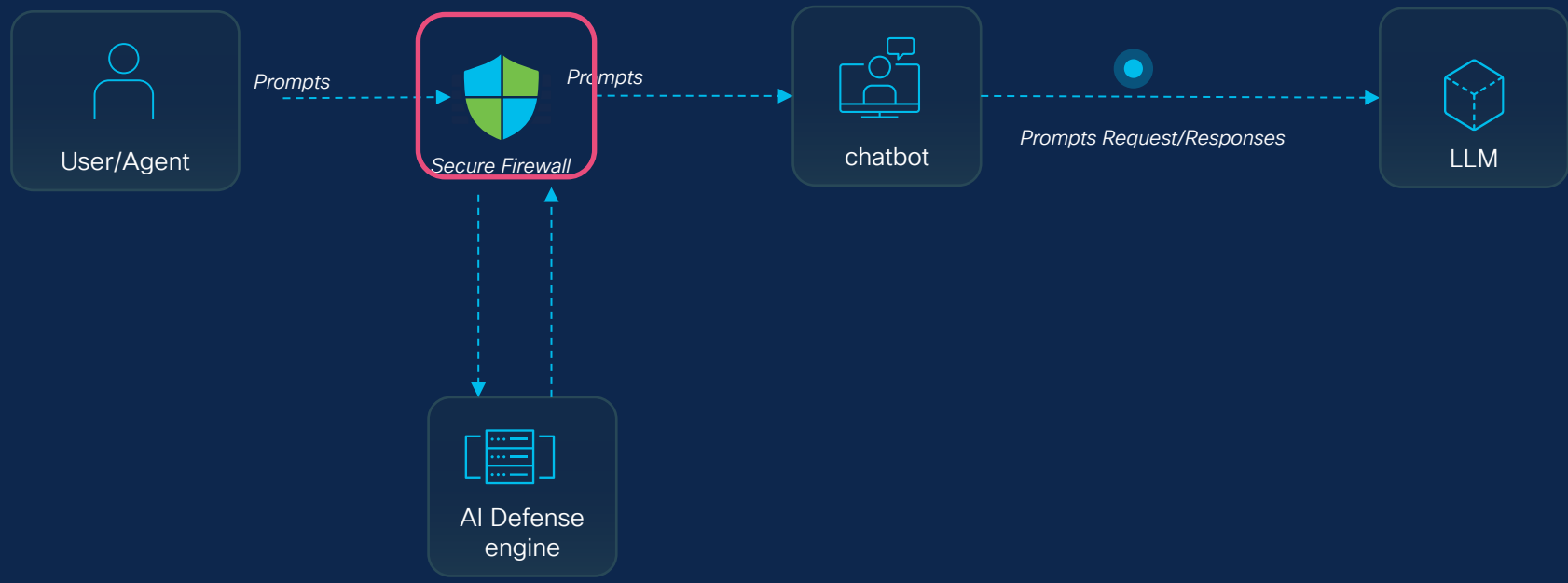
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Future Firewall Integration with AI Defense

Gen AI Protection

- Intercept and Evaluate prompts between enterprise applications to 3rd party AI Services
- Initially managed from Security Cloud Control
- Phase 2 will bring AI Defense Integration to FMC.
- Recruiting motivated customers for feedback and testing now!



© 2024 Cisco and/or its affiliates. All rights reserved.

Cisco roadmap

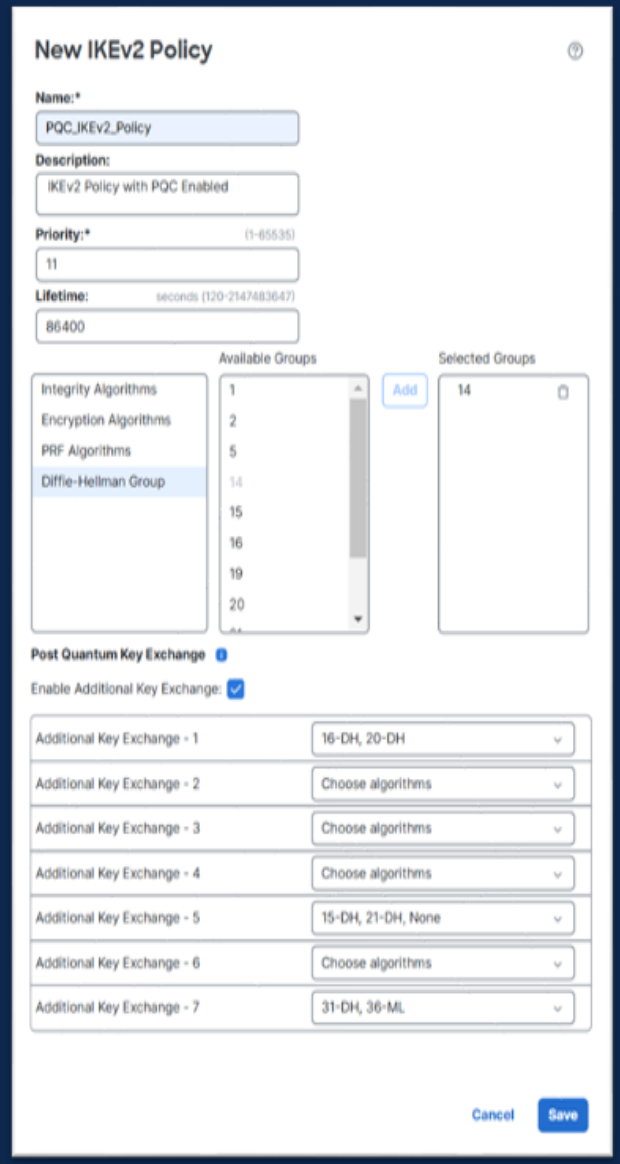
Quantum-Safe VPN and SSH – Future Proofing Encryption

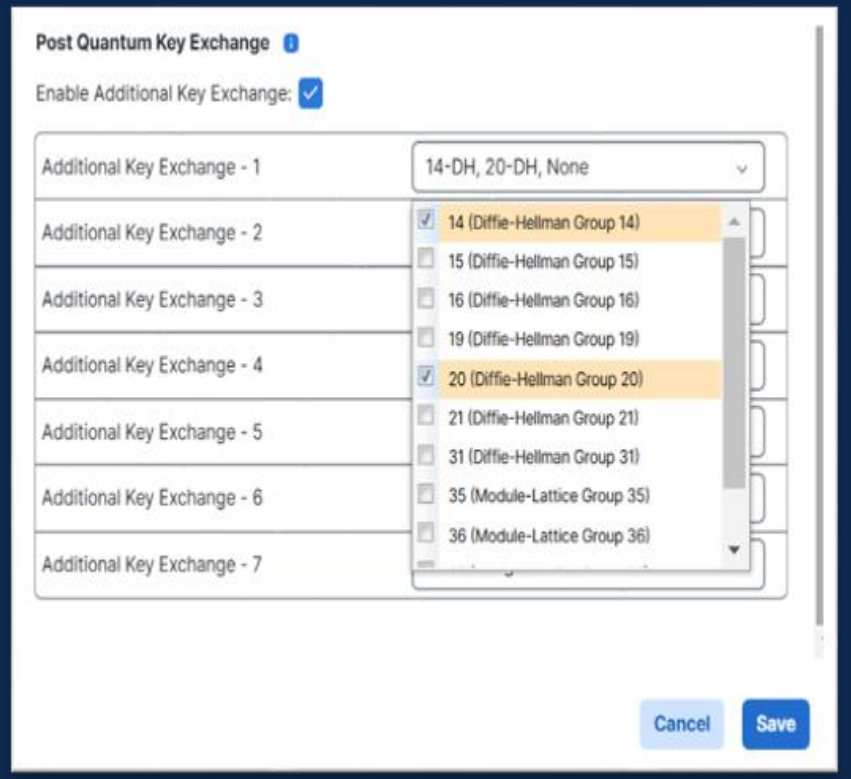
Problem:

Classical ciphers are vulnerable to quantum computers. Sensitive VPN and SSH traffic can be captured today and decrypted later.

Solution:

- **Post-Quantum IKEv2/IPsec** – Support for RFC-9242/9370 hybrid and ML-KEM key exchanges.
- **Quantum-Safe SSH** – ML-KEM available as a configurable SSH cipher.
- **Secure Management Links** – (FMC – FTD) sftunnel traffic protected with ML-KEM.





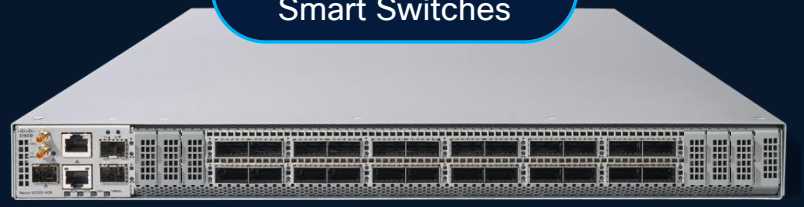
© 2024 Cisco and/or its affiliates. All rights reserved.

Fusing Security Into the Network

Nexus Smart Switch

Unmatched Flexibility, Performance, and Efficiency

Cisco
Smart Switches



Cisco Nexus 9300 Services Accelerated Switch

Networking

Cisco Silicon One

- Rich NX-OS Features and Services
- High-speed connectivity and scalable performance
- Optimized for latency and power efficiency

Routing Switching

EVPN/MPLS/ VXLAN/SR

Rich Telemetry

Line-rate Encryption

Power Efficiency

Hypershield

AMD PENSANDO

- Software-defined Stateful Services
- Programmable at all layers: add new services without HW change
- Scale-out services with wire-rate performance
- Power down DPU complex when not used

Distributed Security

IPSEC Encryption

Large-Scale NAT

Event-Based Telemetry

DoS Protection

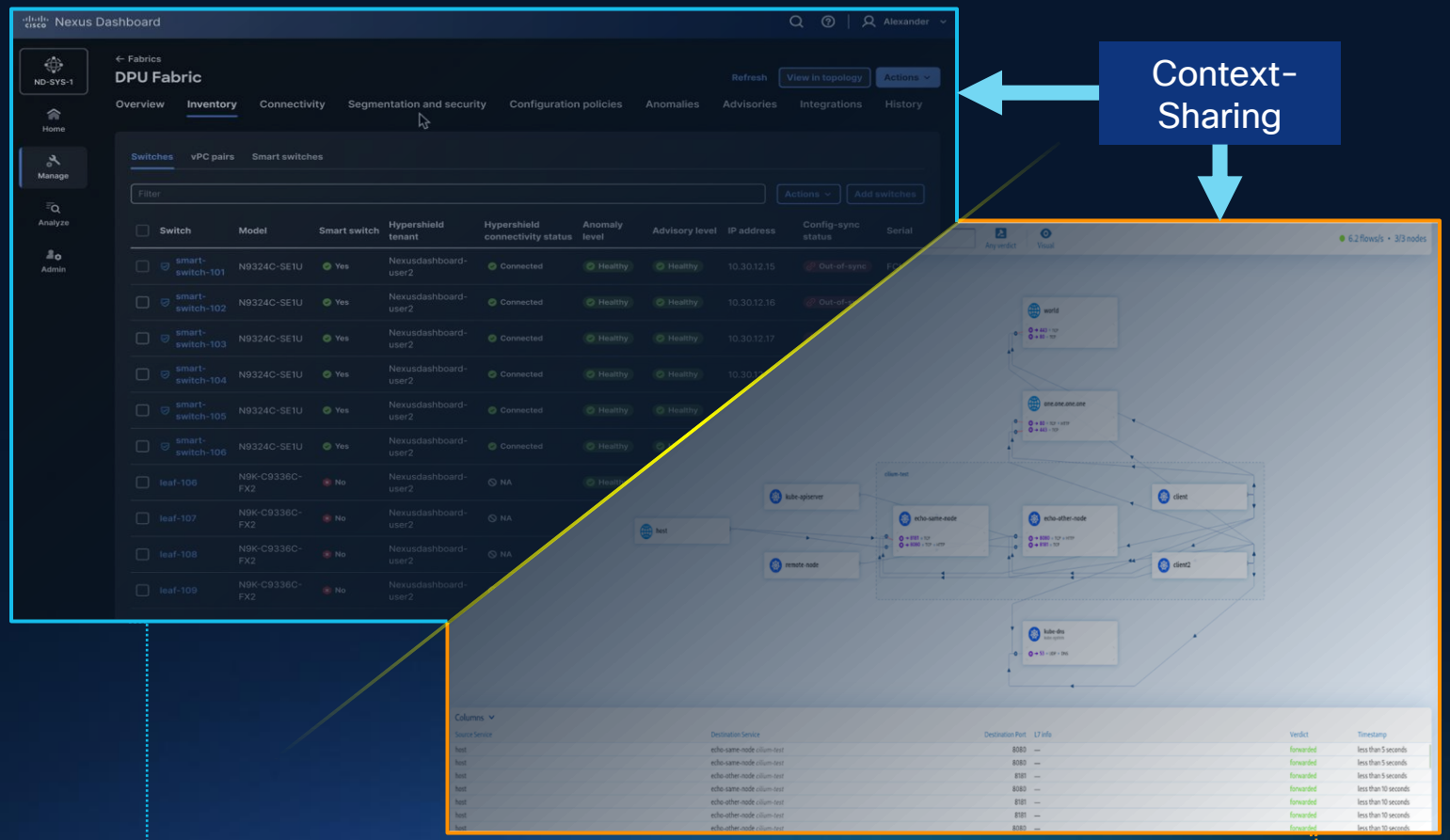
Future Use Cases

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Separate Workflows for NetOps and NetSecOps

Nexus Dashboard
NX-API, NX-CLI



Context-Sharing

Security Cloud Control

NETOPS

NETSECOPS

Nexus Smart Switch

© 2026 Cisco and/or its affiliates. All rights reserved.

Extending controls into the workload and applications

eBPF: Extending network controls into cloud-native workloads

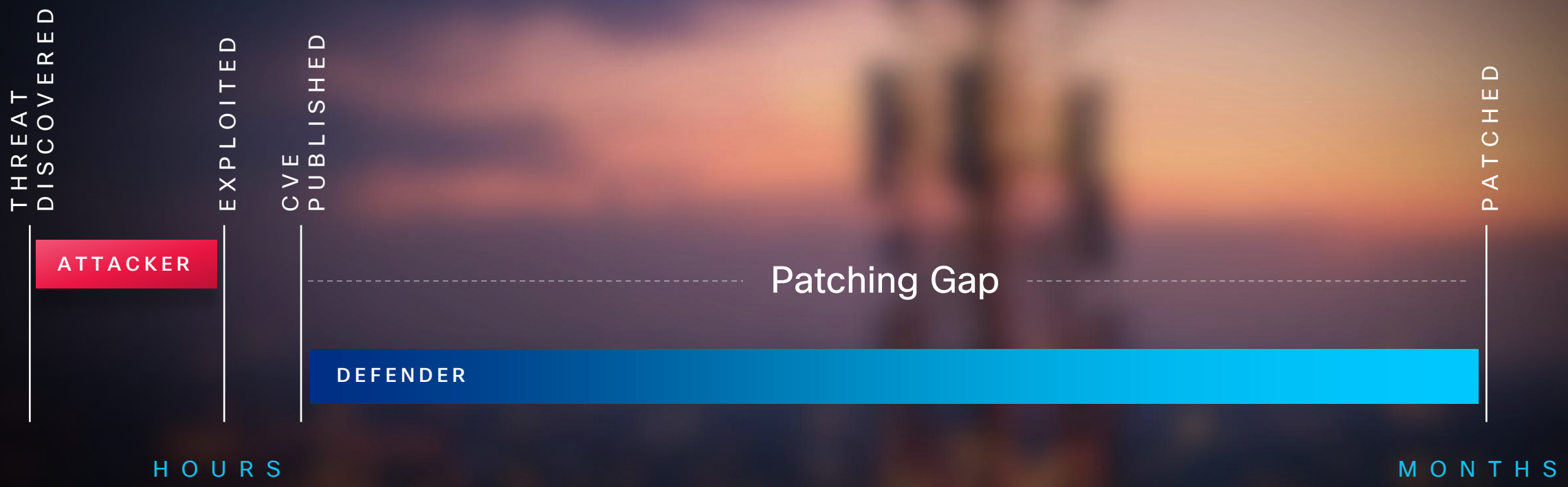
Extends security and observability into cloud-native architectures

Process-level container and workload visibility without risks of kernel modules

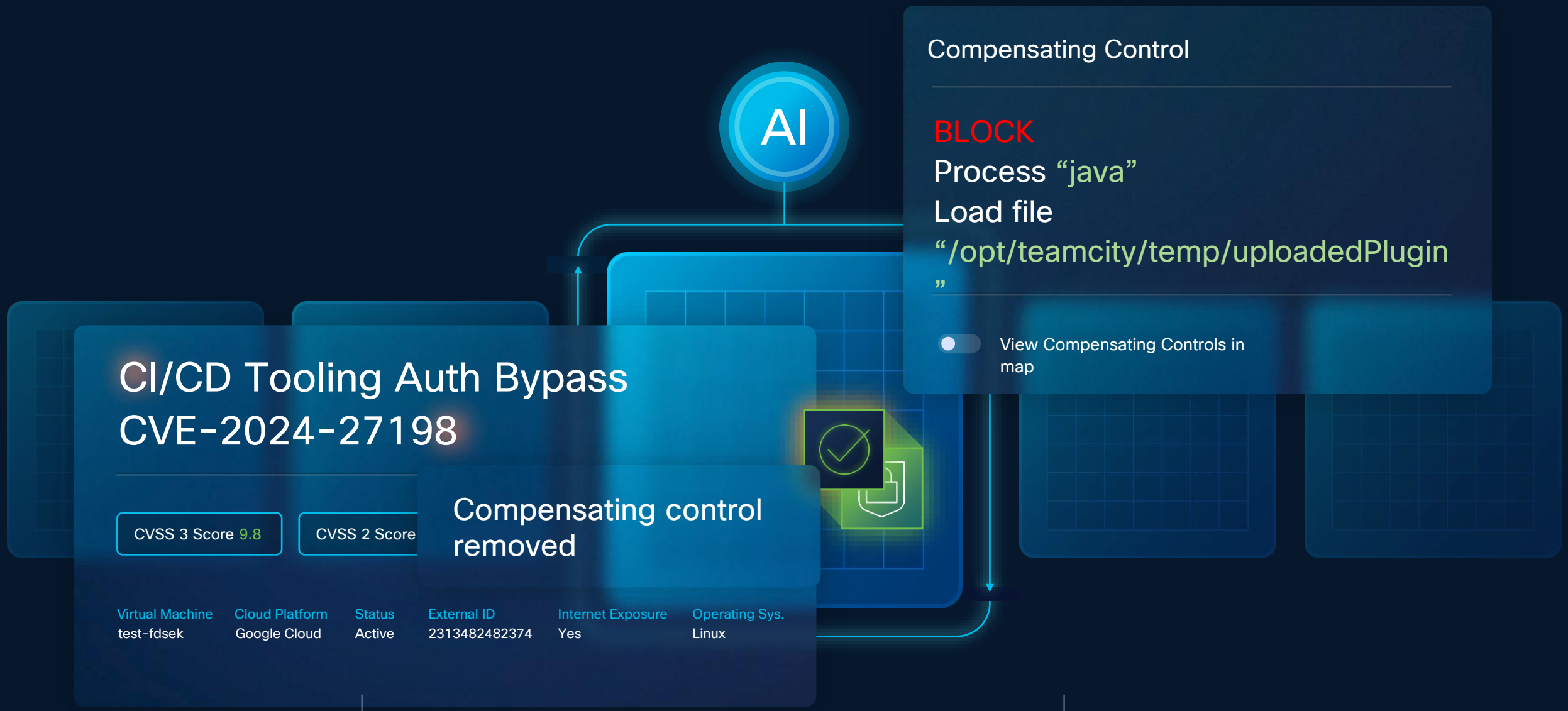
Based on open-source Cilium and Tetragon, which Cisco shepherds

© 2026 Cisco and/or its affiliates. All rights reserved.

Patching is hard



© 2026 Cisco and/or its affiliates. All rights reserved.



Perfect fit | Tested against real world traffic | Optimal placement

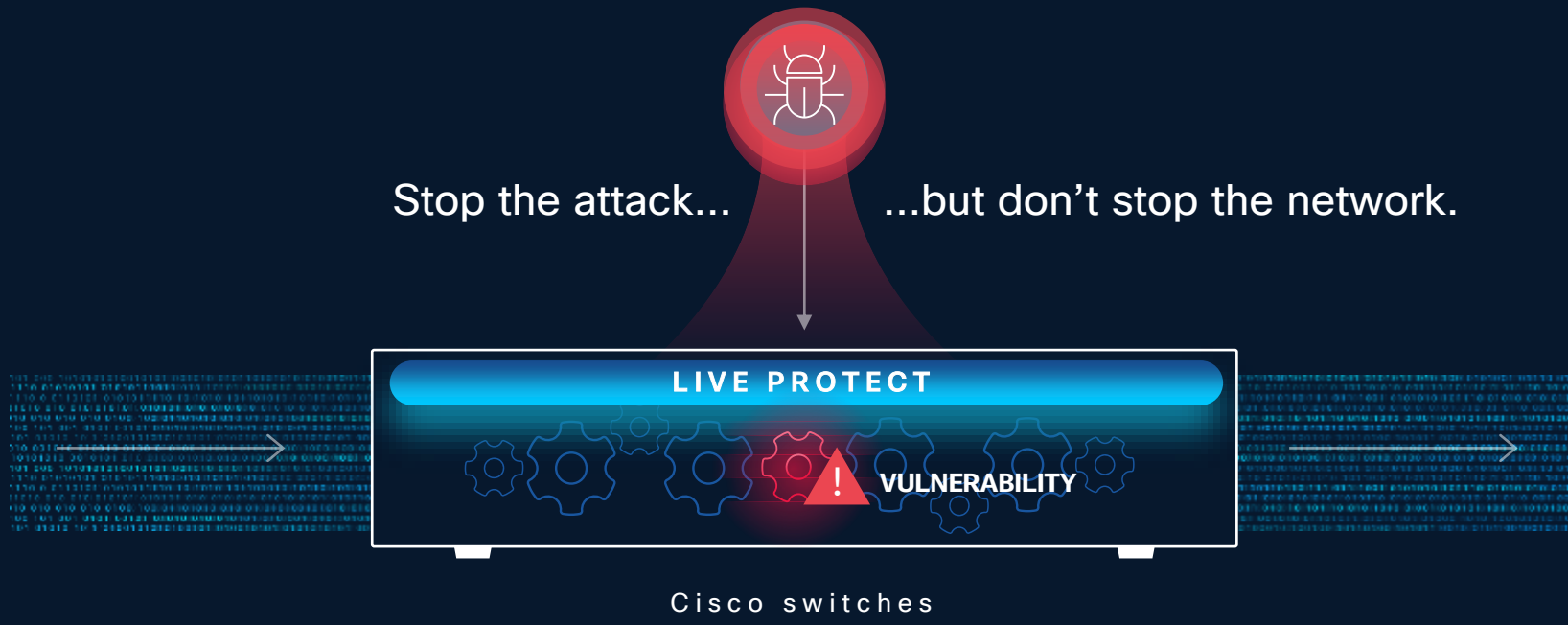
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Live Protect

Vulnerability shielding for Cisco networking devices

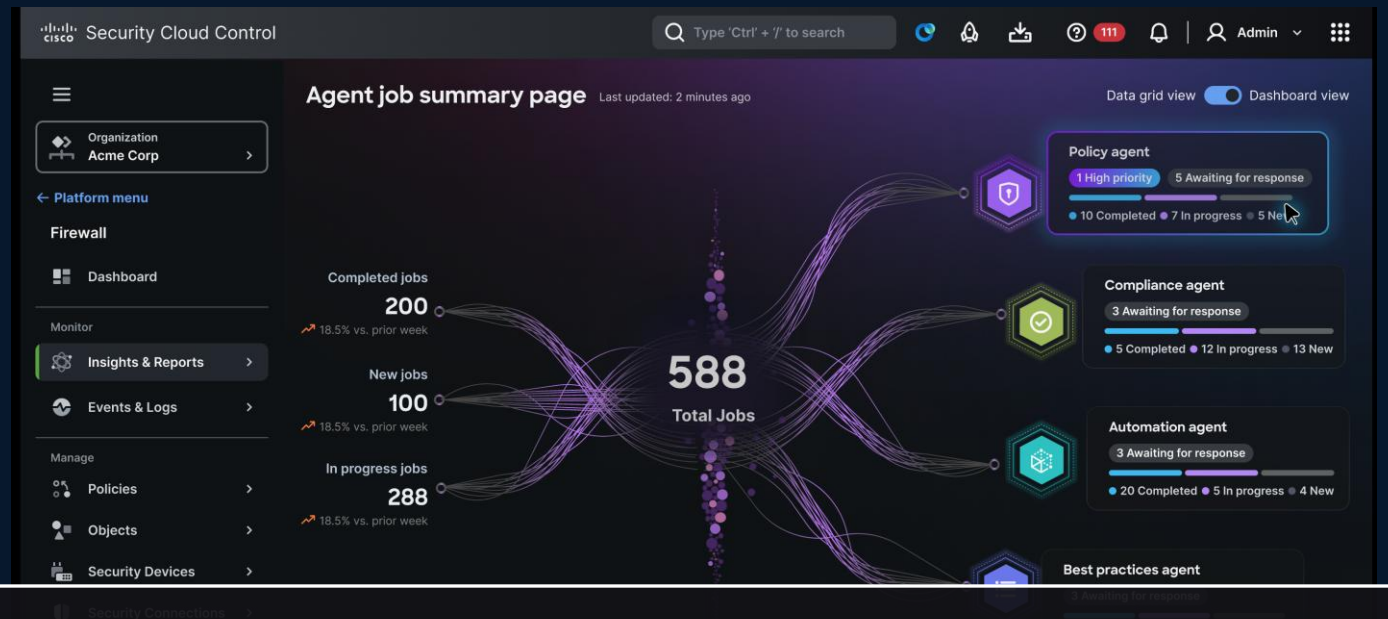
- Generates score and report
- Recommends guardrails
- Continuous re-validation



© 2026 Cisco and/or its affiliates. All rights reserved.

NEW

AgenticOps experience in Security Cloud Control



New AgenticOps Capabilities

Zero Trust Access Policy Creation

VPN Capacity Planning

Elephant Flow Remediation

PCI-DSS Compliance

Firewall Policy Optimization

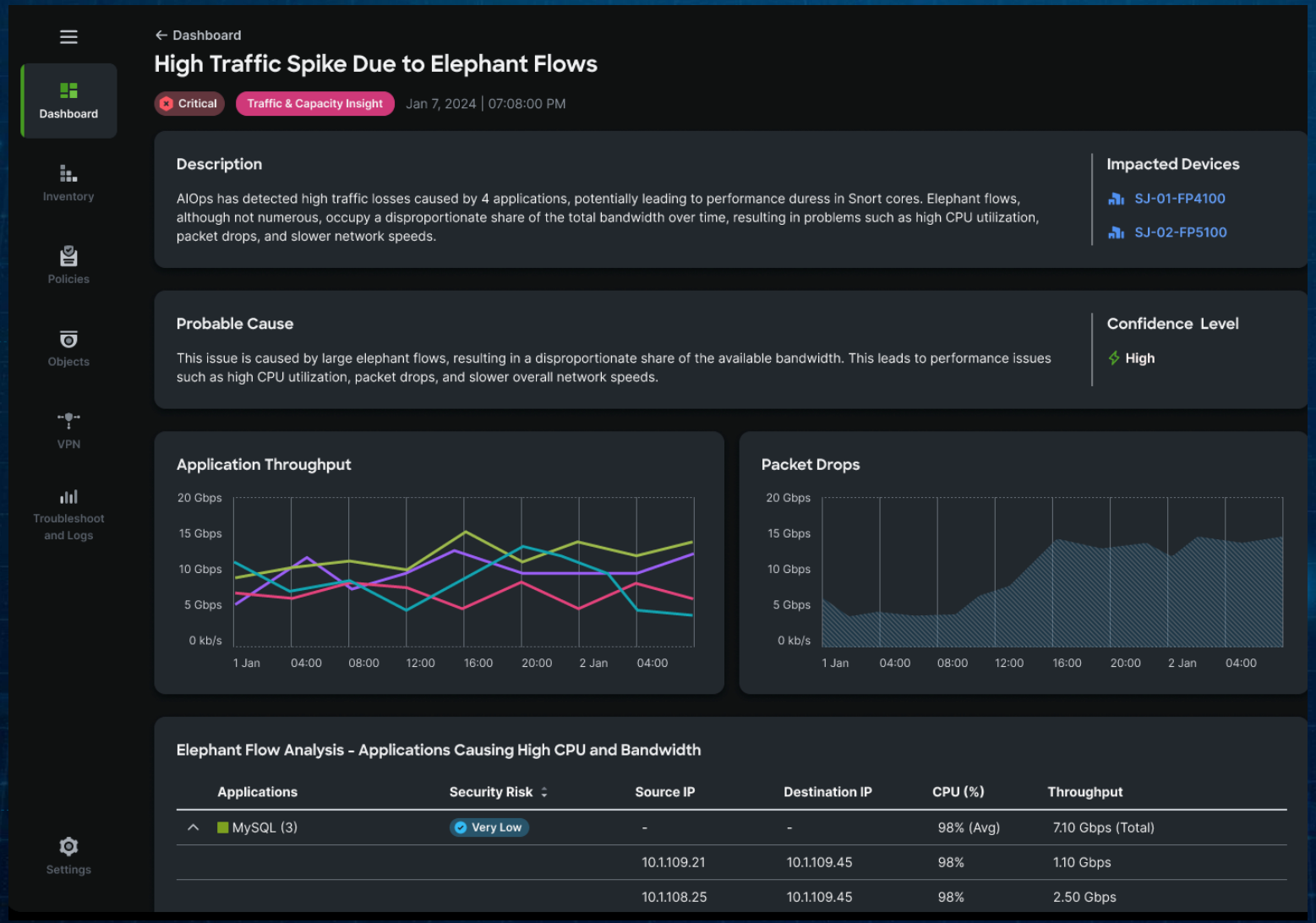
GA: May 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

Enhance security

Correlate and show performance overload due to specific applications that can lead to traffic drop and compromised security

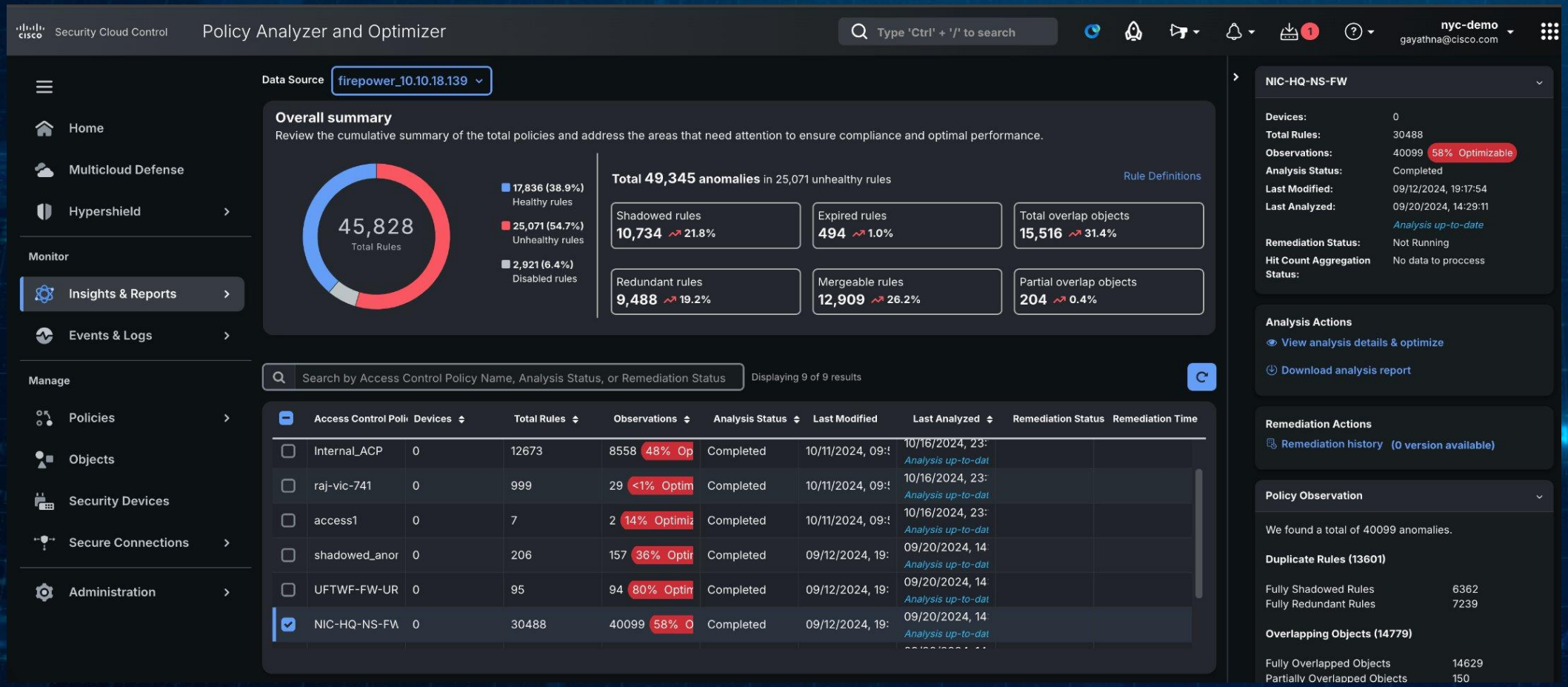
Recommendation to inspect high risk applications and bypass low risky apps



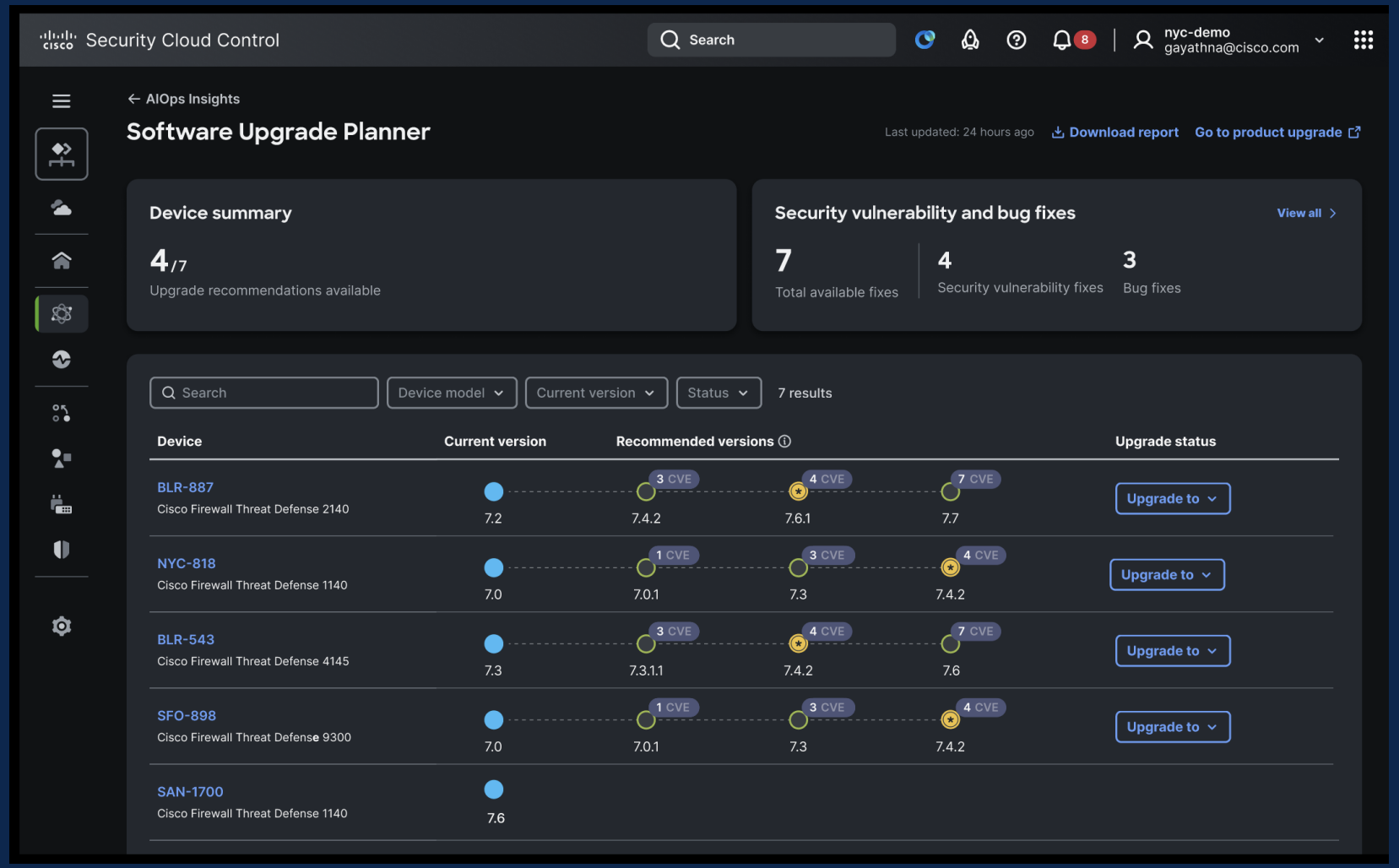
Policy Analyzer & Optimizer (FMC & Cloud control)

Simplify operations

Surface anomalies in rules to guide users to attend to stale rules and other policy hygiene issues that might be oversights



Software Upgrade Planner



- Custom analysis of PSIRTs and bugs based on current customer versions.
Identify and mitigate relevant risks before upgrading.

- Suggests best major and Minor versions which aligns with your stability and innovation preferences.

- No more manual research to determine upgrade paths.
Get upgrade version recommendations instantly tailored to your environment.

© 2025 Cisco and/or its affiliates. All rights reserved.

CVE per release and recommendations

Security Vulnerability and Bug Fixes

Last updated: 43 minutes ago

Security vulnerability fixes | Bug fixes

Summary

22	0	22
Total	Critical	High

Search | 2 Severity | 22 results

CVE ID	Title	Impact	Description	Impacted devices	CVSS score	Available fixe
CVE-2025-20217	Cisco Secure Firewall Threat Defense Softwar...	High	A vulnerability in the packet inspection functionality ...	FTD-VPN	8.6	7.2.10, 7.4.2
CVE-2024-20426	Cisco Adaptive Security Appliance and Firepo...	High	A vulnerability in the Internet Key Exchange version ...	FTD-VPN	8.6	7.2.9, 7.2.10
CVE-2024-20494	Cisco Adaptive Security Appliance and Firepo...	High	A vulnerability in the TLS cryptography functionality ...	FTD-VPN	8.6	7.4.2, 7.4.2.1
CVE-2025-20133	Cisco Secure Firewall Adaptive Security Applia...	High	Multiple vulnerabilities in the management and VPN ...	FTD-VPN	8.6	7.0.6.3, 7.0.7
CVE-2025-20243	Cisco Secure Firewall Adaptive Security Applia...	High	Multiple vulnerabilities in the management and VPN ...	FTD-VPN	8.6	7.0.6.3, 7.0.7
CVE-2025-20224	Cisco IOS, IOS XE, Secure Firewall Adaptive S...	High	Multiple vulnerabilities in the Internet Key Exchange ...	FTD-VPN	8.6	7.0.8, 7.2.10
CVE-2025-20225	Cisco IOS, IOS XE, Secure Firewall Adaptive S...	High	Multiple vulnerabilities in the Internet Key Exchange ...	FTD-VPN	8.6	7.0.8, 7.2.10
CVE-2025-20239	Cisco IOS, IOS XE, Secure Firewall Adaptive S...	High	Multiple vulnerabilities in the Internet Key Exchange ...	FTD-VPN	8.6	7.0.8, 7.2.10
CVE-2025-20252	Cisco IOS, IOS XE, Secure Firewall Adaptive S...	High	Multiple vulnerabilities in the Internet Key Exchange ...	FTD-VPN	8.6	7.0.8, 7.2.10
CVE-2025-20253	Cisco IOS, IOS XE, Secure Firewall Adaptive S...	High	Multiple vulnerabilities in the Internet Key Exchange ...	FTD-VPN	8.6	7.0.8, 7.2.10
CVE-2025-20254	Cisco IOS, IOS XE, Secure Firewall Adaptive S...	High	Multiple vulnerabilities in the Internet Key Exchange ...	FTD-VPN	8.6	7.0.8, 7.2.10
CVE-2024-20268	Cisco Adaptive Security Appliance and Firepo...	High	A vulnerability in the Simple Network Management P...	FTD-VPN	7.7	7.0.6.2, 7.0.6

Customer and industry recognition

NetSecOPEN

University of New Hampshire InterOperability Laboratory

30% faster than other firewalls

Gartner

Magic Quadrant for Hybrid Mesh Firewall, 2025

Positioned as the only Visionary

Gartner Overall Rating 4.9/5

Recognized in Peer Insights™

* vs Palo Alto Networks 4.6, Fortinet 4.7. All scores for last 12 months as of Jan 21,2026

SE LABS AAA MAY 2025 Advanced Performance NGFW Performance

Industry's first to earn AAA rating in advanced performance

IDC

MarketScape Worldwide Enterprise Hybrid Firewall 2025 Vendor Assessment

A Leader

FORRESTER

The Forrester Wave™: Enterprise Firewall Solutions, Q4 2024

A Leader

SE LABS AAA FEBRUARY 2025 Advanced Security NDR Protection

100% accuracy in advanced security and NDR protection

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

A Winner

FORRESTER

The Forrester Wave™: Microsegmentation Solutions Q3 2024

Wave Leader

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

CISCO Connect

Thank you