

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; Health, Science & Technology

Publication Date: 01/23/2025

Author: Jaikaran, Chris

www.congress.gov/crs-product/IF12798

Infosecurity Magazine

News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

Infosecurity Magazine Home » News » AI Supercharges Attacks in Cybercrime's New 'Fifth Wave'

DEEPFAKE

NEWS 20 January 2026

AI Supercharges Attacks in Cybercrime's New 'Fifth Wave'

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

ADVERTISMENT

Infosecurity Magazine
Stay informed. Stay secure.
Get weekly updates on the latest threats, breaches & trends in cybersecurity
REGISTER NOW!

AI is powering a "fifth wave" in the evolution of cybercrime, offering inexpensive, ready-made malicious tools enabling sophisticated attacks, according to Group-IB.

In its latest report, published on January 20, the Singapore-based cybersecurity firm divided the history of cybercrime in four phases, from the opportunistic malware and viruses of the 1990s and early 2000s to "ecosystem and supply chain attacks" wave that marked the 2010s and 2020s.

Since 2022, the firm argued, cybercrime has entered a fifth wave, which it called "weaponized AI."

This new era is marked by the rapid adoption of AI and generative AI (GenAI) tools by attackers that "turn human skills into scalable services" and make cybercrime "cheaper, faster and more scalable," Dmitry Volkov, Group-IB's CEO, said in the report's foreword.

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Malware & Threats Security Operations Security Architecture Risk Management

iddataweb

Identity Under Attack:
Why Every Business Must Respond Now

February 11, 2026 at 1PM ET REGISTER NOW

LIVE WEBINAR

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

MALWARE & THREATS

Two Years On, Log4Shell Vulnerability Still Being Exploited to Deploy Malware

More than two years after the Log4j crisis, organizations are still being hit by crypto-currency miners and backdoor scripts.

By Ryan Naraine | August 22, 2024 (10:44 AM ET)

More than two years after the critical Log4j zero-day sparked chaos around the world, organizations are still being hit by exploits pushing crypto-currency miners and malicious backdoor scripts.

TRENDING

Crunchbase Confirms Data Hacking Claims

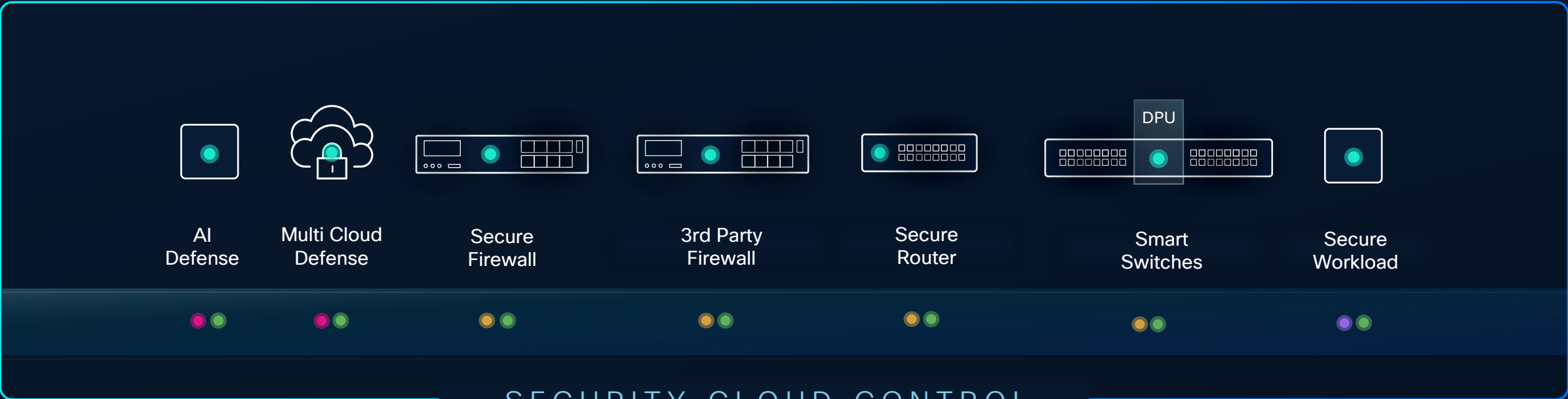
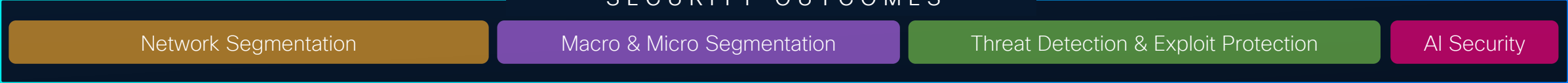
Infosecurity Magazine source:
<https://www.infosecurity-magazine.com/news/ai-supercharges-attacks-cybercrime/>

Firewalling needs to evolve to meet today's challenges



Security close to every workload: Hybrid Mesh Firewalling

SECURITY OUTCOMES



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



6100 Series

2 Models
Firewalling + IPS

Up to 600 Gbps



Public/Private

20+ cloud variants



NUTANIX

openstack



Google Cloud Platform

rackspace
Technology

Alibaba Cloud

HyperFlex



vmware
ESXi

Microsoft Azure

alkira





EQUINIX

ORACLE
CLOUD INFRASTRUCTURE

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 μ Code

Cisco NGFW New Features!

Encrypted Visibility Engine

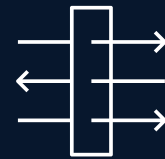
Simplified configuration of AI/ML-driven detection of apps and malware in encrypted traffic, without decrypting

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)



AI

Cisco Encrypted Visibility Engine

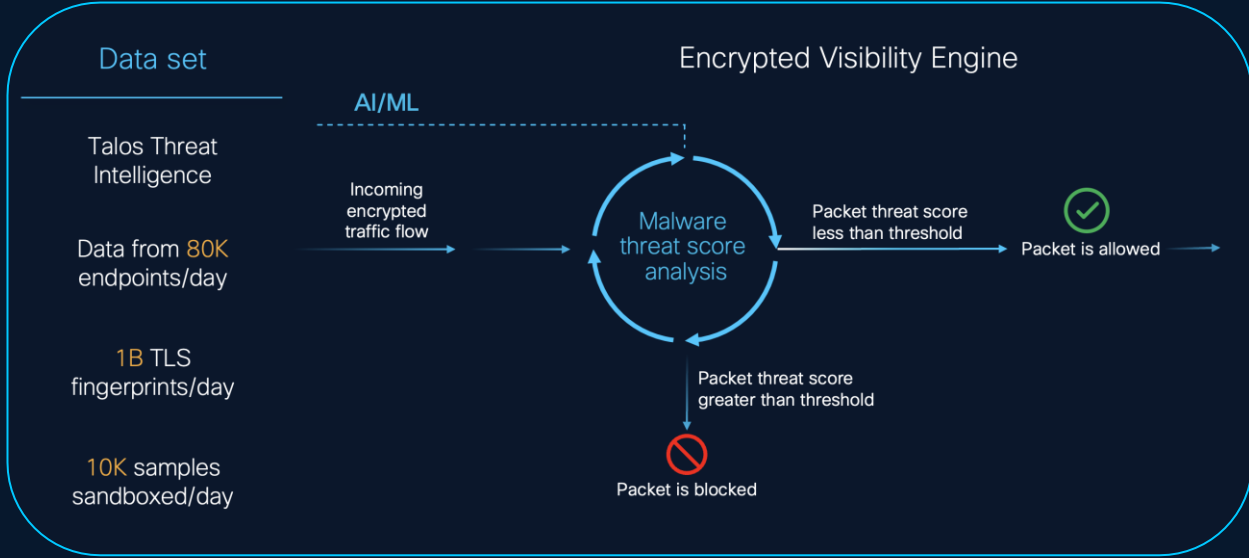
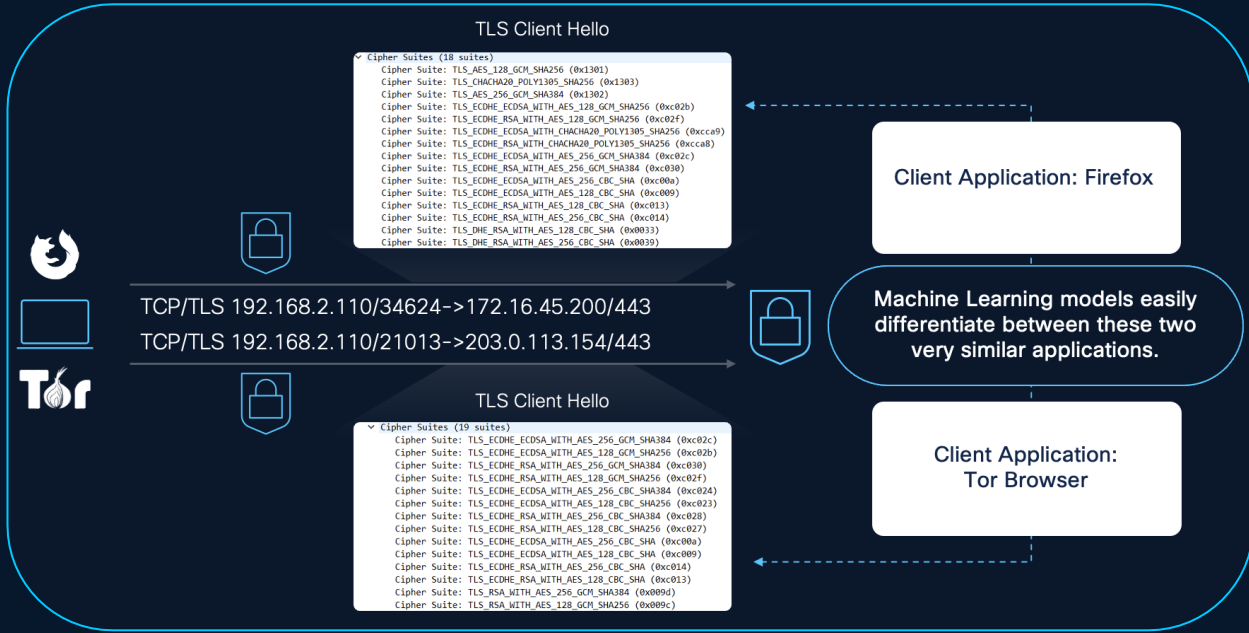
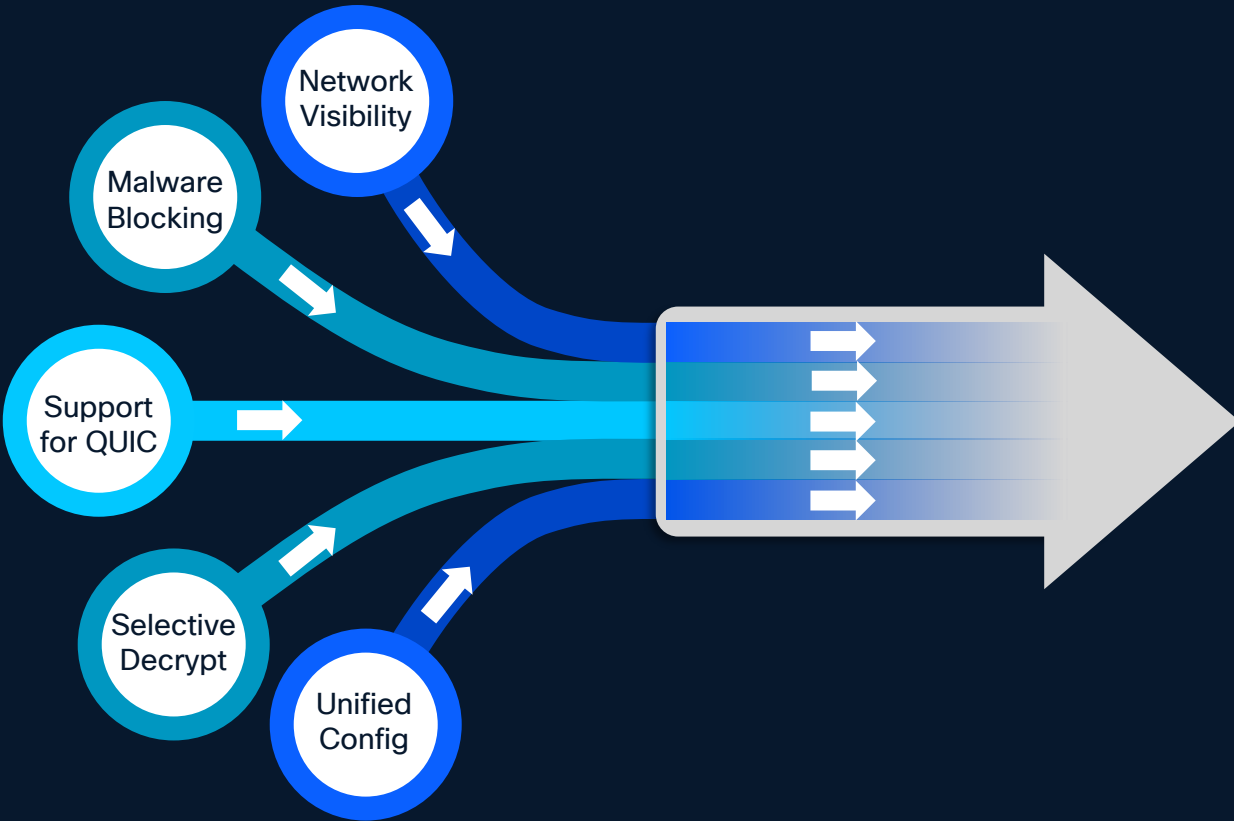
Visibility to malicious flows in encrypted traffic without decryption

Machine learning
(ML) technology

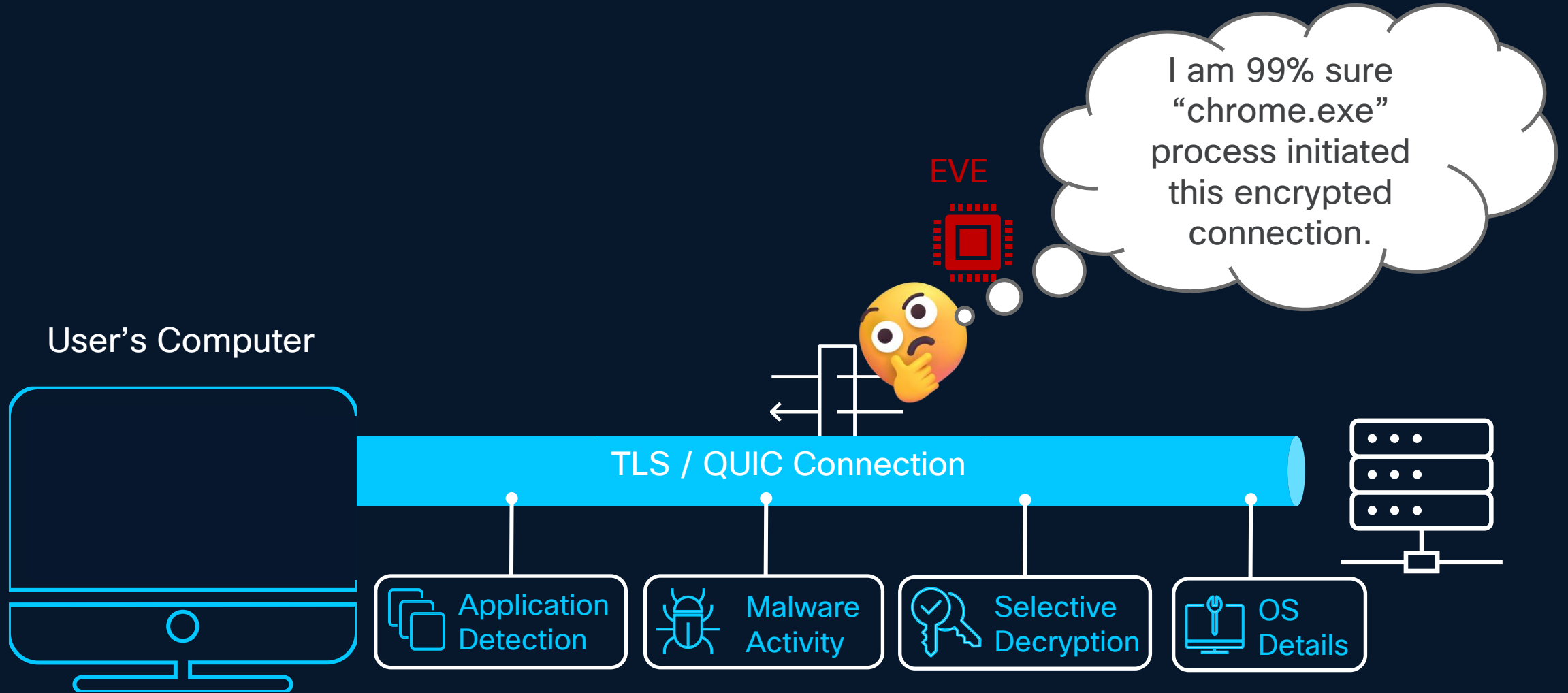
Processes 1 B+
TLS fingerprints

Processes 10 K+
malware samples daily

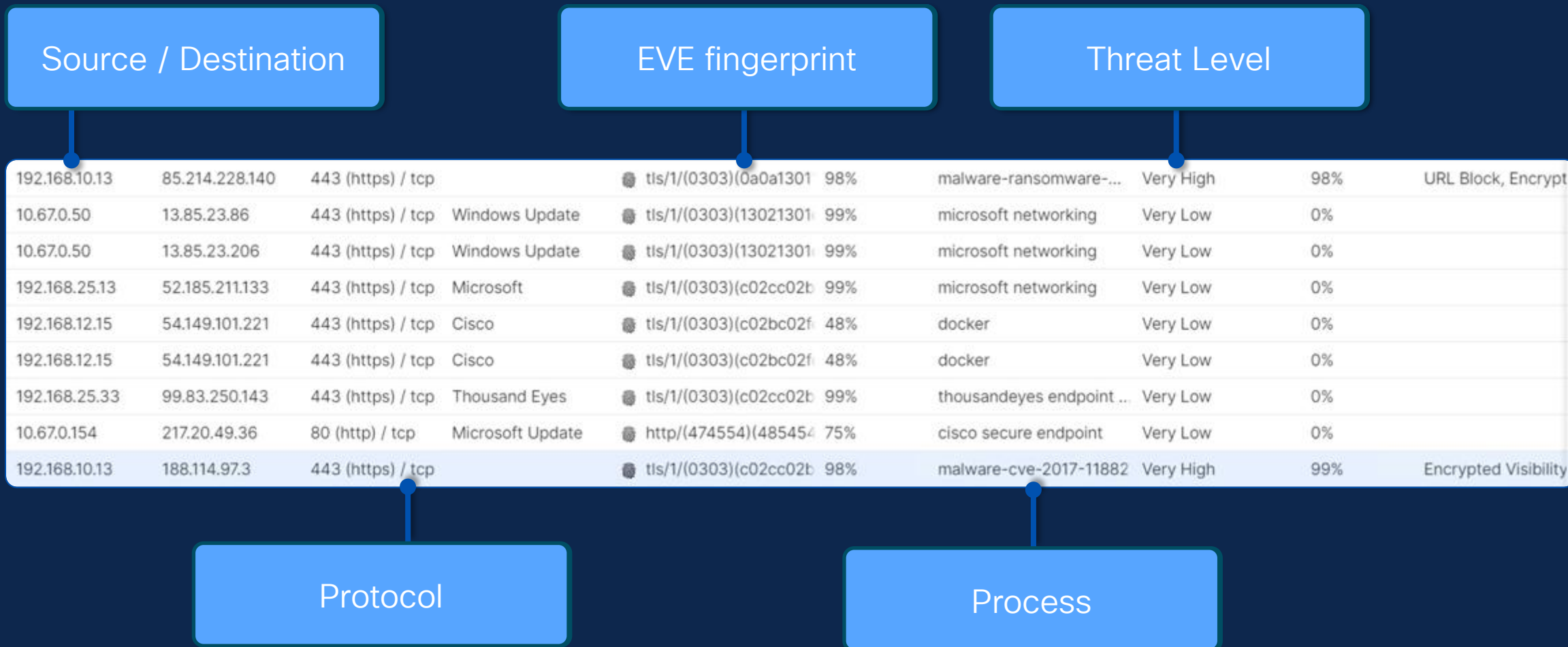
EVE Through the Years



What Does Encrypted Visibility Engine Provide?



EVE in action: Malicious flow



EVE changes the game on decryption

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



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)

zero-day protection with Snort ML

Snort ML extends IDPS protection to unknown variants of common attacks

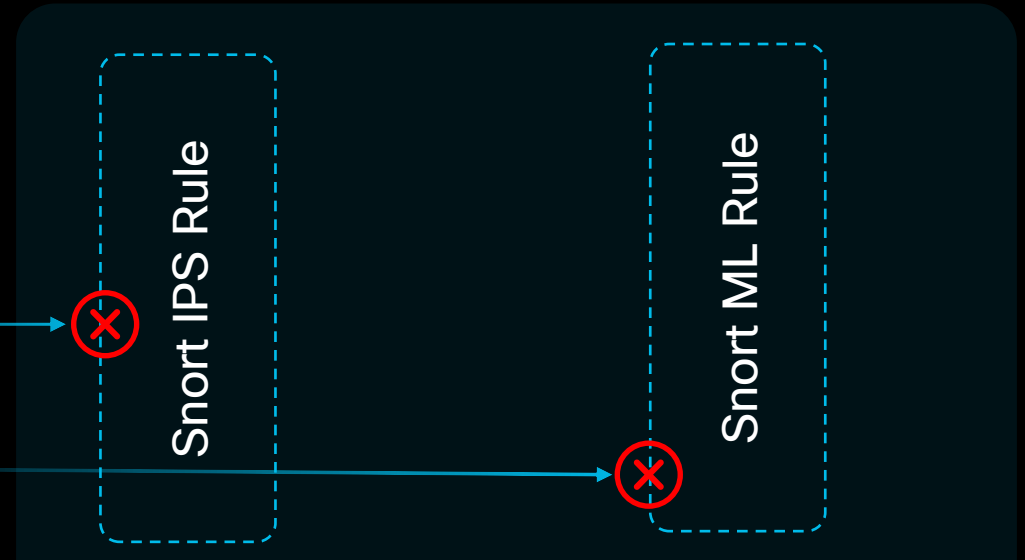
SnortML uses Machine Learning to expand IPS capabilities

- 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



| <input type="checkbox"/> GID:SID | Rule Details | Rule Action | Set By | Assigned Groups |
|---|-----------------------------------|--------------------|---------------|------------------------|
| <input type="checkbox"/> 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)

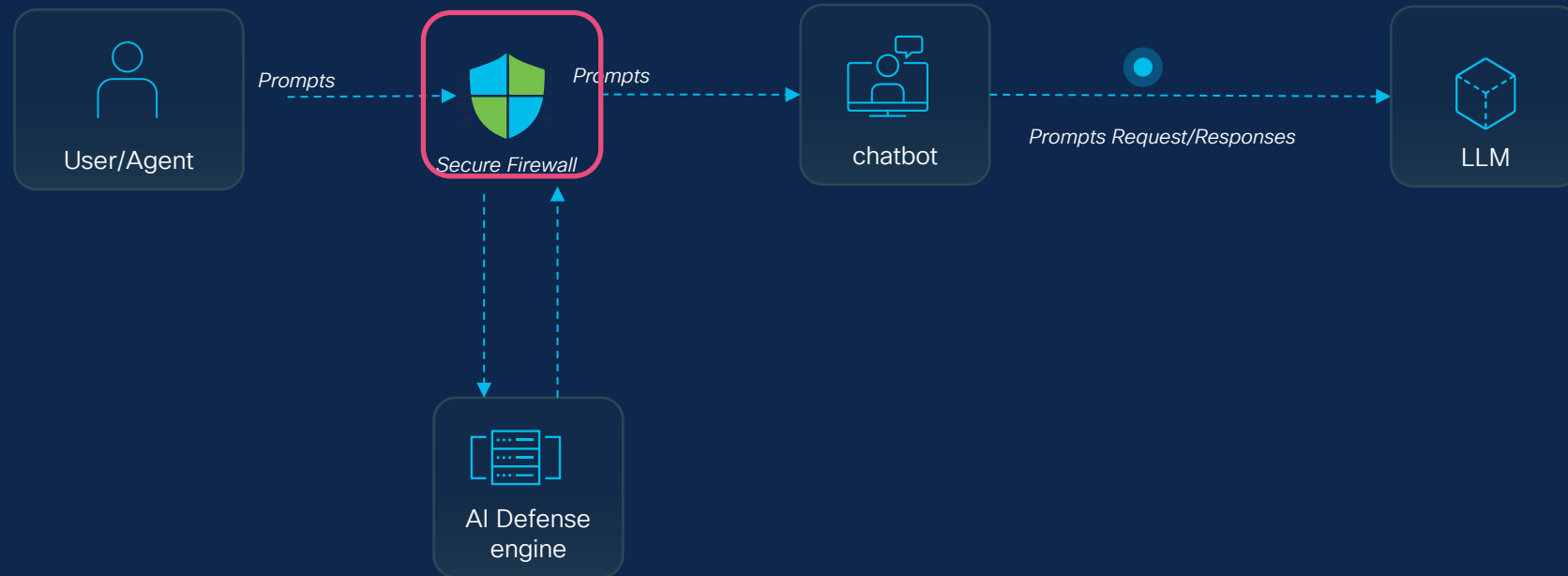
```
Snort Rule
alert ( gid:411; sid:1; rev:1; msg:"(snort_ml)
potential threat found in HTTP parameters via Neural
Network Based Exploit Detection"; metadata: policy
max-detect-ips alert, rule-type preproc;
classtype:unknown;)
```

Powered by TALOS Intelligence

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!



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.

New IKEv2 Policy

Name: PQC_IKEv2_Policy
Description: IKEv2 Policy with PQC Enabled
Priority: 11
Lifetime: 86400 seconds

Available Groups: Integrity Algorithms, Encryption Algorithms, PRF Algorithms, Diffie-Hellman Group (14, 15, 16, 19, 20)

Selected Groups: 14

Post Quantum Key Exchange: Enable Additional Key Exchange:

Additional Key Exchange - 1: 16-DH, 20-DH
Additional Key Exchange - 2: Choose algorithms
Additional Key Exchange - 3: Choose algorithms
Additional Key Exchange - 4: Choose algorithms
Additional Key Exchange - 5: 15-DH, 21-DH, None
Additional Key Exchange - 6: Choose algorithms
Additional Key Exchange - 7: 31-DH, 36-ML

Post Quantum Key Exchange

Enable Additional Key Exchange:

Additional Key Exchange - 1: 14-DH, 20-DH, None
Additional Key Exchange - 2: 14 (Diffie-Hellman Group 14), 15 (Diffie-Hellman Group 15), 16 (Diffie-Hellman Group 16), 19 (Diffie-Hellman Group 19), 20 (Diffie-Hellman Group 20), 21 (Diffie-Hellman Group 21), 31 (Diffie-Hellman Group 31), 35 (Module-Lattice Group 35), 36 (Module-Lattice Group 36)
Additional Key Exchange - 3
Additional Key Exchange - 4
Additional Key Exchange - 5
Additional Key Exchange - 6
Additional Key Exchange - 7

Cancel Save

Fusing Security Into the Network

Nexus Smart Switch

Unmatched Flexibility, Performance, and Efficiency

Cisco
Smart Switches

Networking



- 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

Cisco Nexus 9300 Services Accelerated Switch



Hypershield



- 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



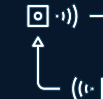
Distributed
Security



IPSEC
Encryption



Large-Scale
NAT



Event-Based
Telemetry



DoS
Protection

Future Use Cases

Separate Workflows for NetOps and NetSecOps

Nexus Dashboard
NX-API, NX-CLI

The screenshot shows the Nexus Dashboard interface. On the left, a table lists various switches with columns for Switch, Model, Smart switch, Hypershield tenant, Hypershield connectivity status, Anomaly level, Advisory level, IP address, Config-sync status, and Serial. The main area displays a network topology diagram with nodes like 'kube-apiserver', 'kube-scheduler', 'kube-controller', 'etcd', 'client', and 'client2' connected in a mesh. A blue box labeled 'Context-Sharing' has arrows pointing from the dashboard to the topology and from the topology to the dashboard.

| Switch | Model | Smart switch | Hypershield tenant | Hypershield connectivity status | Anomaly level | Advisory level | IP address | Config-sync status | Serial |
|------------------|----------------|--------------|----------------------|---------------------------------|---------------|----------------|-------------|--------------------|--------|
| smart-switch-101 | N9324C-SETU | Yes | Nexusdashboard-user2 | Connected | Healthy | Healthy | 10.30.12.15 | Out-of-sync | FX2 |
| smart-switch-102 | N9324C-SETU | Yes | Nexusdashboard-user2 | Connected | Healthy | Healthy | 10.30.12.16 | Out-of-sync | FX2 |
| smart-switch-103 | N9324C-SETU | Yes | Nexusdashboard-user2 | Connected | Healthy | Healthy | 10.30.12.17 | Out-of-sync | FX2 |
| smart-switch-104 | N9324C-SETU | Yes | Nexusdashboard-user2 | Connected | Healthy | Healthy | 10.30.12.18 | Out-of-sync | FX2 |
| smart-switch-105 | N9324C-SETU | Yes | Nexusdashboard-user2 | Connected | Healthy | Healthy | 10.30.12.19 | Out-of-sync | FX2 |
| smart-switch-106 | N9324C-SETU | Yes | Nexusdashboard-user2 | Connected | Healthy | Healthy | 10.30.12.20 | Out-of-sync | FX2 |
| leaf-106 | N9K-C9336C-FX2 | No | Nexusdashboard-user2 | NA | Healthy | Healthy | 10.30.12.21 | Out-of-sync | FX2 |
| leaf-107 | N9K-C9336C-FX2 | No | Nexusdashboard-user2 | NA | Healthy | Healthy | 10.30.12.22 | Out-of-sync | FX2 |
| leaf-108 | N9K-C9336C-FX2 | No | Nexusdashboard-user2 | NA | Healthy | Healthy | 10.30.12.23 | Out-of-sync | FX2 |
| leaf-109 | N9K-C9336C-FX2 | No | Nexusdashboard-user2 | NA | Healthy | Healthy | 10.30.12.24 | Out-of-sync | FX2 |

Security Cloud Control

NETOPS

NETSECOPS



Nexus Smart Switch

**Extending controls into the
workload and applications**

eBPF: Extending network controls into cloud-native workloads

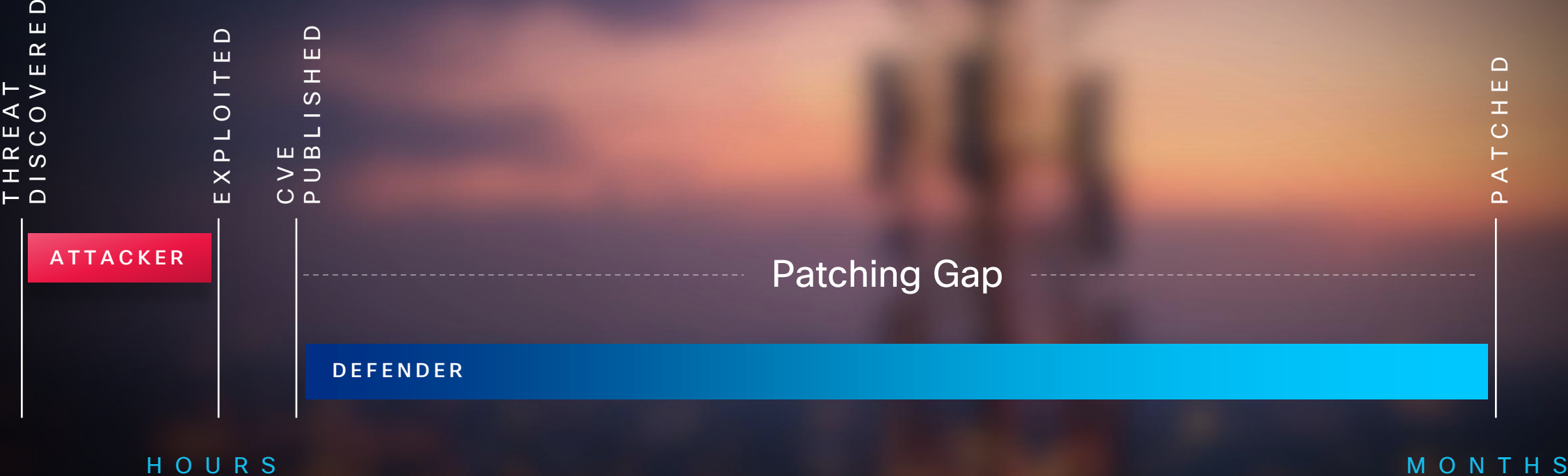


Extends security and observability into cloud-native architectures

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

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

Patching is hard





Compensating Control

BLOCK

Process "java"

Load file

"/opt/teamcity/temp/uploadedPlugin"



View Compensating Controls in map

CI/CD Tooling Auth Bypass CVE-2024-27198

CVSS 3 Score 9.8

CVSS 2 Score

Compensating control removed

| Virtual Machine | Cloud Platform | Status | External ID | Internet Exposure | Operating Sys. |
|-----------------|----------------|--------|---------------|-------------------|----------------|
| test-fdsek | Google Cloud | Active | 2313482482374 | Yes | Linux |

Perfect fit

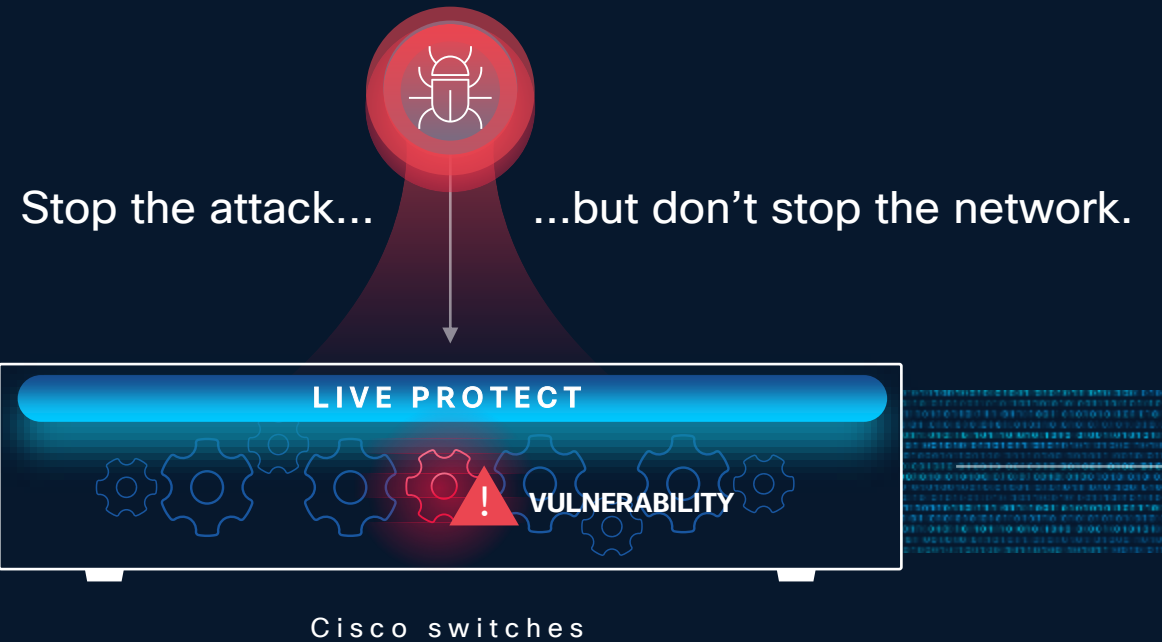
Tested against real world traffic

Optimal placement

Live Protect

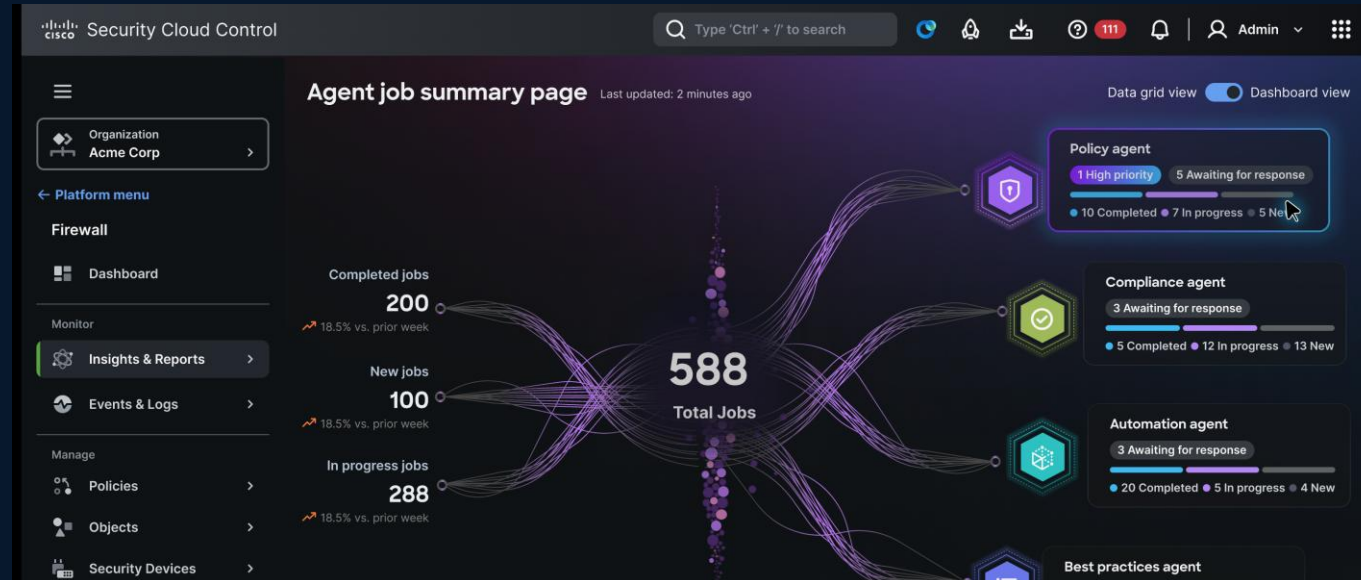
Vulnerability shielding for Cisco networking devices

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



NEW

AgenticOps experience in Security Cloud Control



New AgenticOps Capabilities

Zero Trust
Access Policy
Creation

VPN Capacity
Planning

Elephant Flow
Remediation

PCI-DSS
Compliance

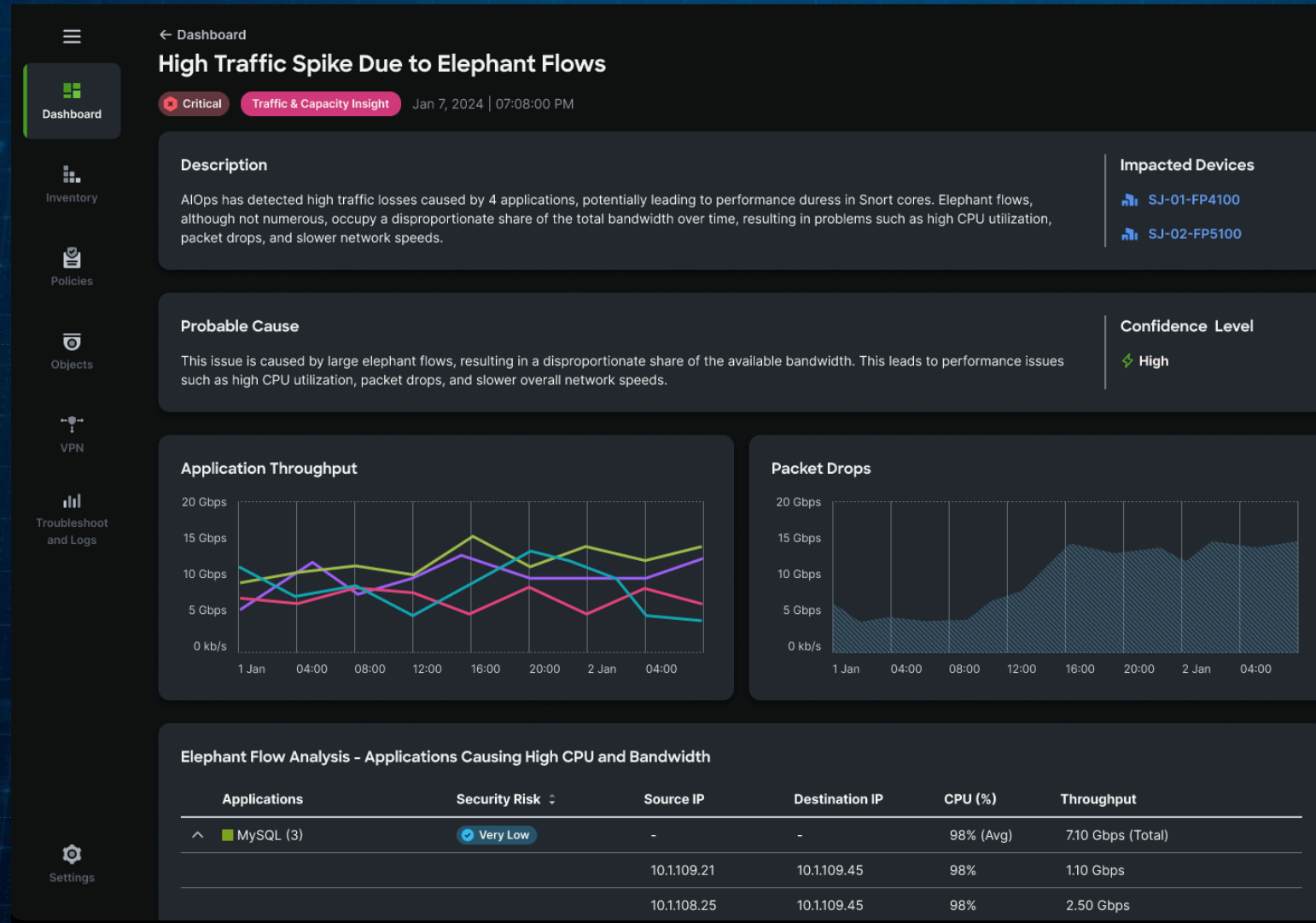
Firewall Policy
Optimization

GA: May 2026

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

Overall summary
Review the cumulative summary of the total policies and address the areas that need attention to ensure compliance and optimal performance.

Total 49,345 anomalies in 25,071 unhealthy rules

45,828 Total Rules

- 17,836 (38.9%) Healthy rules
- 25,071 (54.7%) Unhealthy rules
- 2,921 (6.4%) Disabled rules

Shadowed rules: 10,734 ↗ 21.8%

Expired rules: 494 ↗ 1.0%

Total overlap objects: 15,516 ↗ 31.4%

Redundant rules: 9,488 ↗ 19.2%

Mergeable rules: 12,909 ↗ 26.2%

Partial overlap objects: 204 ↗ 0.4%

Table of Results:

| Access Control Poli | Devices | Total Rules | Observations | Analysis Status | Last Modified | Last Analyzed | Remediation Status | Remediation Time |
|---------------------|---------|-------------|---------------|-----------------|-------------------|-------------------|--------------------|------------------|
| Interna_LACP | 0 | 12673 | 8558 48% Op | Completed | 10/11/2024, 09:11 | 10/16/2024, 23:00 | | |
| raj-vic-741 | 0 | 999 | 29 <1% Optim | Completed | 10/11/2024, 09:11 | 10/16/2024, 23:00 | | |
| access1 | 0 | 7 | 2 14% Optimiz | Completed | 10/11/2024, 09:11 | 10/16/2024, 23:00 | | |
| shadowed_anor | 0 | 206 | 157 36% Optim | Completed | 09/12/2024, 19:19 | 09/20/2024, 14:00 | | |
| UFTWF-FW-UR | 0 | 95 | 94 80% Optim | Completed | 09/12/2024, 19:19 | 09/20/2024, 14:00 | | |
| NIC-HQ-NS-FW | 0 | 30488 | 40099 58% O | Completed | 09/12/2024, 19:19 | 09/20/2024, 14:00 | | |

Policy Observation

We found a total of 40099 anomalies.

Duplicate Rules (13601)

- Fully Shadowed Rules: 6362
- Fully Redundant Rules: 7239

Overlapping Objects (14779)

- Fully Overlapped Objects: 14629
- Partially Overlapped Objects: 150

Software Upgrade Planner

Security Cloud Control

Search

← AIOps Insights

Software Upgrade Planner

Last updated: 24 hours ago [Download report](#) [Go to product upgrade](#)

Device summary

4/7
Upgrade recommendations available

Security vulnerability and bug fixes

7 Total available fixes | 4 Security vulnerability fixes | 3 Bug fixes [View all](#)

Search Device model Current version Status 7 results

| Device | Current version | Recommended versions | Upgrade status |
|---|-----------------|---|----------------------------|
| BLR-887 Cisco Firewall Threat Defense 2140 | 7.2 | 7.4.2 (3 CVE), 7.6.1 (4 CVE), 7.7 (7 CVE) | Upgrade to |
| NYC-818 Cisco Firewall Threat Defense 1140 | 7.0 | 7.0.1 (1 CVE), 7.3 (3 CVE), 7.4.2 (4 CVE) | Upgrade to |
| BLR-543 Cisco Firewall Threat Defense 4145 | 7.3 | 7.3.1.1 (3 CVE), 7.4.2 (4 CVE), 7.6 (7 CVE) | Upgrade to |
| SFO-898 Cisco Firewall Threat Defense 9300 | 7.0 | 7.0.1 (1 CVE), 7.3 (3 CVE), 7.4.2 (4 CVE) | Upgrade to |
| SAN-1700 Cisco Firewall Threat Defense 1140 | 7.6 | | |

- 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.

CVE per release and recommendations

Security Vulnerability and Bug Fixes

Last updated: 43 minutes ago

Security vulnerability fixes Bug fixes

Summary

22

Total

0

Critical ✖

22

High ⚠

Search

2

Severity



22 results

| CVE ID | Title | Impact | Description | Impacted devices | CVSS score ⓘ | Available fixes |
|----------------|---|--------|--|------------------|--------------|-----------------|
| 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

NetSec **OPEN**



30% faster than other firewalls

Gartner

Magic Quadrant for Hybrid Mesh Firewall, 2025

Positioned as the only Visionary



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

Recognized in Peer Insights™

SE LABS



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



Advanced Security
NDR Protection

100% accuracy in advanced security and NDR protection



A Winner

FORRESTER

The Forrester Wave™: Microsegmentation Solutions Q3 2024

Wave Leader

Thank you

