

# Segmentation Untangled: Streamlining Hybrid Data Center Security



Jeff Fanelli – Distinguished Solutions Engineer

# Streamlining Hybrid Data Center Security

1. Distributed Security
2. Modern Secure Access
3. Evolution of Firewalling
4. Agentic Ops
5. Identity in the AI world

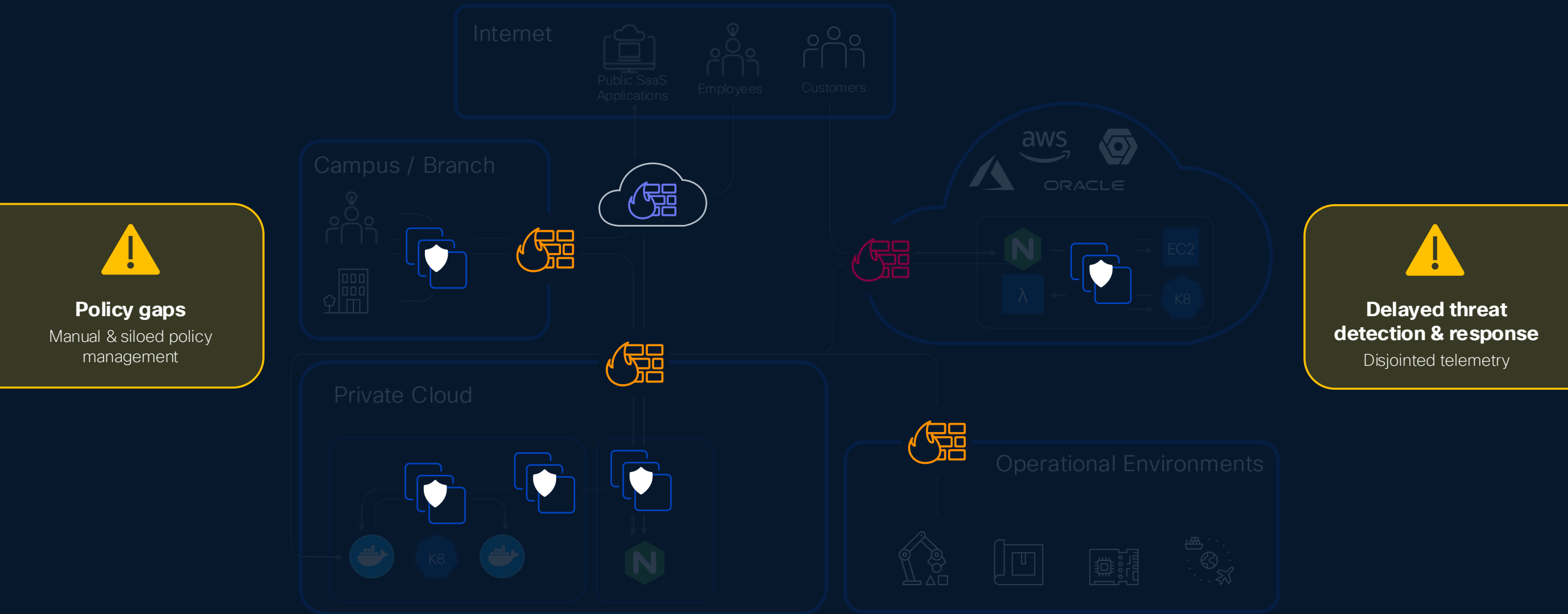
# The Future of Network Security is **DISTRIBUTED**



Need to Eliminate East/West Network Blindspots

Need for Rich Application Identity & Context

# Inserting security controls at every juncture of user, device and applications interaction



# Focus on outcomes, not management

Start with the customer's security requirements

Drive product adoption faster with new capabilities

Accelerate innovation while reducing operational overhead

The screenshot displays the Cisco Security Cloud Control interface for 'ACME Corp'. The dashboard is organized into several key sections:

- Home:** Features a navigation sidebar on the left with categories like Organization, Services, Products, Favorites, and Common Objects. The main content area is titled 'Home' and includes a search bar and user profile (Kit Johnson, Acme Corp).
- Top insights & alerts:** A grid of six alert cards. Three cards are labeled 'Elephant flow spike observed' with a 'Critical' status, and two are labeled 'Some other concern' with a 'Warning' status. Each card provides a brief description of the issue and a 'View details' link.
- Connectivity status:** A central section featuring a donut chart showing that 15% of assets are disconnected (up 8% since yesterday). A table to the right details the sources of disconnected assets, including Firewall devices (250, up 11%), Universal ZTNA Firewall devices (45, up 5%), Network tunnel groups (36), Resource connectors (8), Cloud accounts (1), Tesseract security agents (12,942, up 4%), and Workload agents (19).
- Workload attack framework:** A horizontal bar chart showing the status of various attack framework components: Initial Access (1), Execution (0), Persistence (0), Privilege Escalation (2), Defense Evasion (0), Credential Access (0), Discovery (0), Lateral Movement (1), Command and Control (0), and Exfiltration (0).
- Right-hand sidebar:** Contains sections for 'Talos Intelligence' (with an 'Under attack?' indicator), 'Latest bulletins' (highlighting a 'Critical SMBV3 remote code execution vulnerability'), and 'Latest blogs' (featuring articles like 'THE NEED TO KNOW' and 'Cybersecurity on a budget: Strategies for an economic downturn').

# Modern Secure Access Services Edge

# Cisco SASE

**Secure SD-WAN**

Commercial and Enterprise



**Secure Services Edge**

Cisco Secure Access



**Identity First**

ISE + Identity Intelligence

## Recent Developments

### Unified Cloud Management

Single dashboard for Meraki, Catalyst, all next-gen devices

### 8000 Series Secure Router

Next-gen firewall, SASE-ready

### FTD-200 Secure Firewall

Specific to primarily security buying motion

### Unifying Secure Access for Cisco SASE

Integration with Catalyst, Meraki and Firewall SD-WAN

### Market Access

Expanding Points of Presence (PoPs), Secure Access for Government

### Duo IAM

Runs standalone as primary IdP, directory and SSO, or integrates with existing IAM as an identity broker

### Identity Intelligence

Create one converged view of identity across an organization

# Centralized Policy and Objects

Admins will have one place to manage Network and Security SASE policies

Common Objects Service:  
Admins have one place to manage objects via a cloud service. Network objects will be the first to be unified

## Value and Delighters

- Manage Network and Security Policy from a single place, removing the need for separate dashboards
- Define objects (network objects) once to use in both Network and Security policies for better ease of use, extensibility, and management

The screenshot displays the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo, the text "Security Cloud Control", and user information for "Kit Business Corp, Inc.". The left sidebar contains a "Platform menu" with categories like "SASE Management", "Experience Insights", "Secure", "Resources", "Monitor", "Connect", "Admin", and "Workflows". The main content area is titled "SASE Policy" and includes a descriptive placeholder text. Below this, there are tabs for "Device policies" (5) and "Cloud access policies" (9,999). A table lists several policy groups, each with a search bar, a refresh button, and a "+ Add policy group" button. The table columns are: Policy groups, Application priority & SLA policy, Secure Internet Gateway / Secure Service Edge, NGFW, and DNS. The table rows show details for "MXC1\_SDWAN\_SSE\_UnifiedPolicy" and "ROME1\_SDWAN\_IIoT\_UnifiedPolicy", including the number of policies, devices, and update dates.

Policy groups	Application priority & SLA policy	Secure Internet Gateway / Secure Service Edge	NGFW	DNS
MXC1_SDWAN_SSE_UnifiedPolicy SD-WAN SASE Unified Security	4	4	4	4
ROME1_SDWAN_IIoT_UnifiedPolicy SD-WAN SASE Unified Security	4	4	4	4
MXC1_SDWAN_SSE_UnifiedPolicy SD-WAN SASE Unified Security	4	4	4	4
MXC1_SDWAN_SSE_UnifiedPolicy SD-WAN SASE Unified Security	4	4	4	4
MXC1_SDWAN_SSE_UnifiedPolicy SD-WAN SASE Unified Security	4	4	4	4

NEW

# Hybrid private access

Same optimized experience

Sensitive data stays private

Fail-over to on-prem firewall

REMOTE



CAMPUS



Capabilities are planned but not yet available or guaranteed.



# Evolution of Firewalling

# 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

# Security platform with enforcement points everywhere



Define policy once, enforce everywhere

A blue circular logo with the letters 'AI' in white, positioned in the top right corner of the slide.

AI

# Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

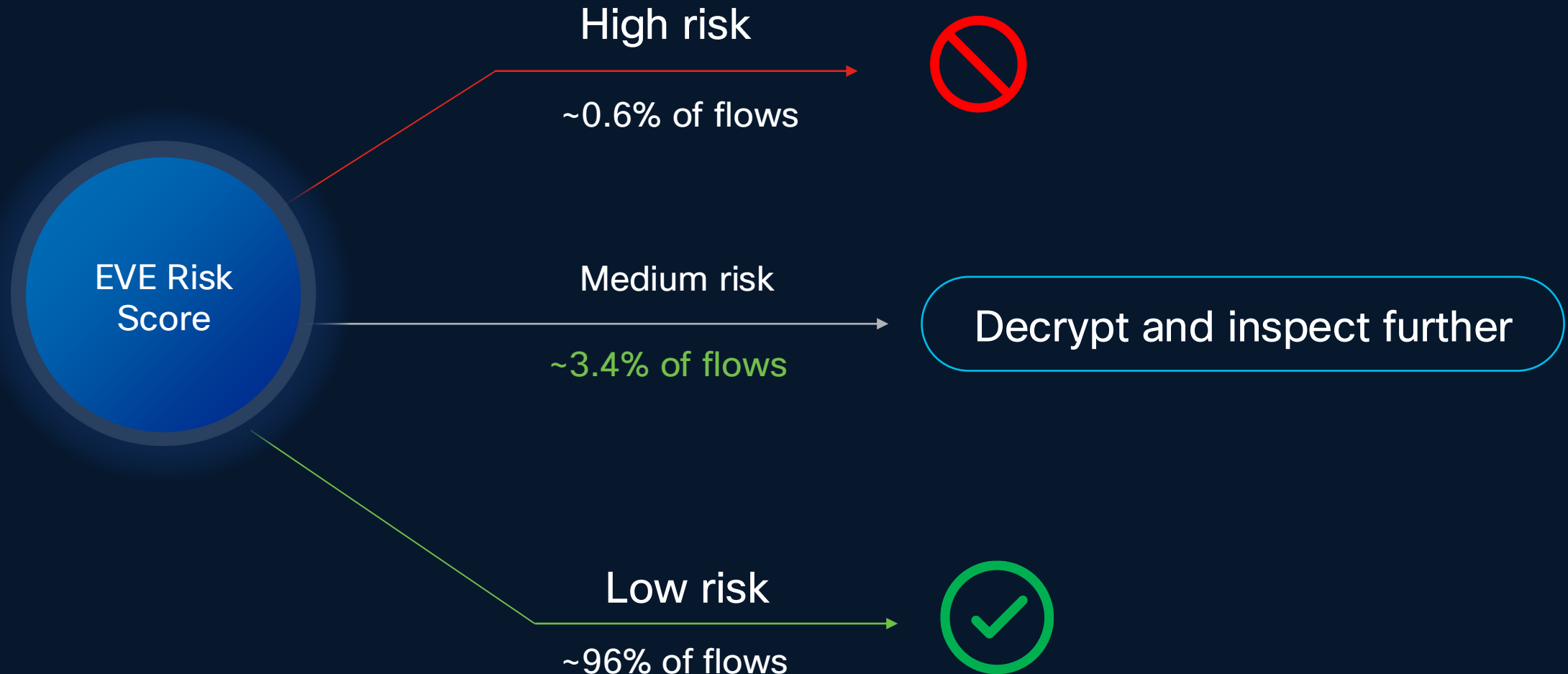
Machine learning  
(ML) technology

Processes **1 B+**  
TLS fingerprints

Processes **10 K+**  
malware samples daily

# Eve changes the game on decryption

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



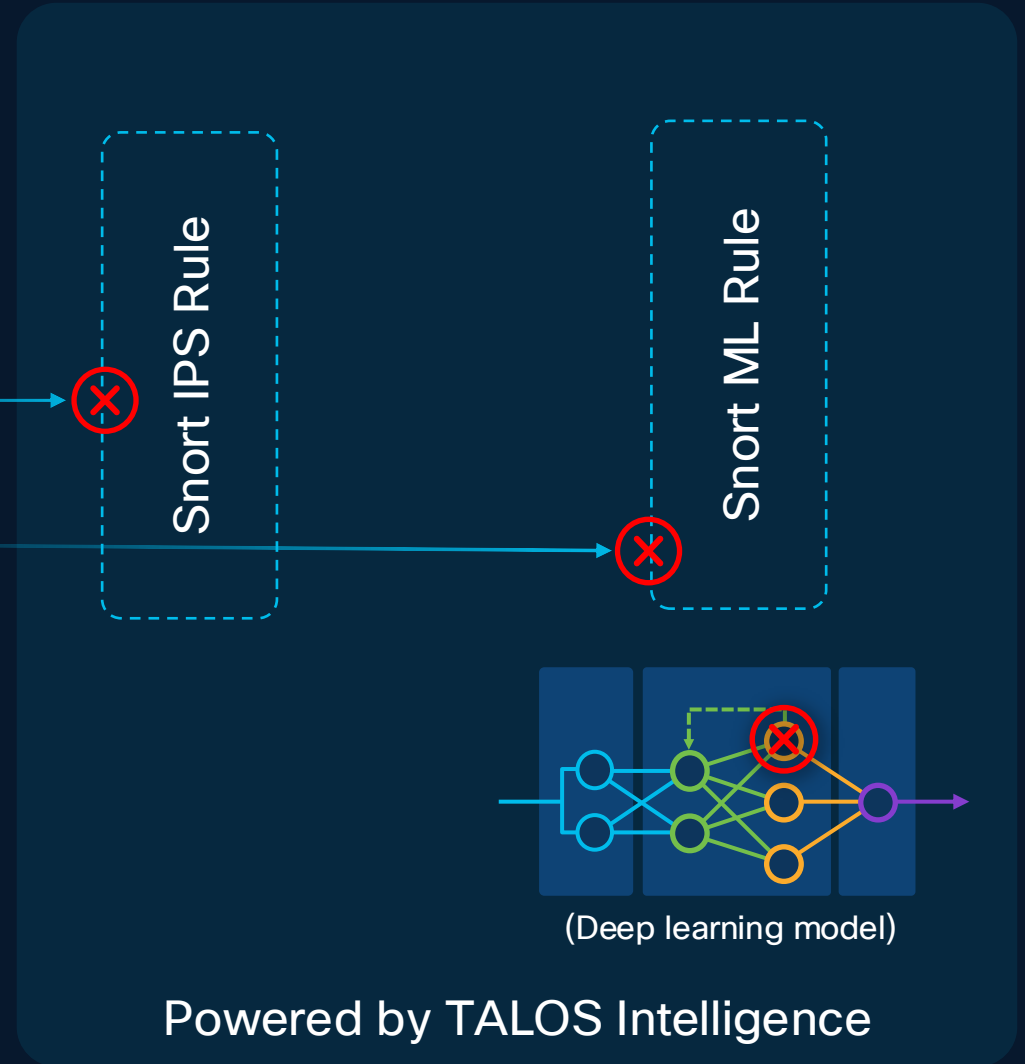
# The leading IDPS, now with zero-day protection

Snort ML extends IDPS protection to unknown variants of common attacks



Known SQL injection attack

Zero-day SQL Injection variant



- Home
- Overview
- Analysis
- Policies
- Devices
- Objects
- Integration

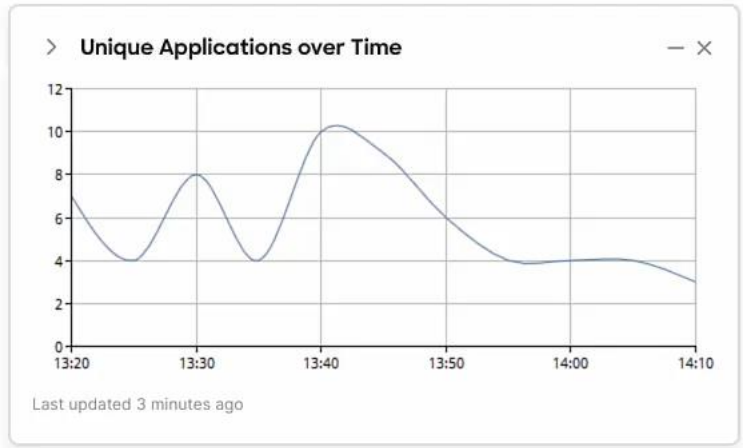
Create Report

# Summary Dashboard [\(switch dashboard\)](#)

Provides a summary of activity on the appliance

- Network
  - Threats
  - Intrusion Events
  - Status
  - Geolocation
  - QoS
  - Zero Trust
  - Encrypted Visibility Engine
  - +
- Show the Last

Add Widgets



### Top Web Applications Seen

Application	Total Bytes (KB)
<input type="checkbox"/> Ubuntu Update Manager	34,112.77
<input type="checkbox"/> Ubuntu	405.35
<input type="checkbox"/> Mozilla	18.15
<input type="checkbox"/> Docker	11.03

Last updated 1 minute ago

### Top Client Applications Seen

Application	Total Bytes (KB)
<input type="checkbox"/> Advanced Packaging Tool	34,478.07
<input type="checkbox"/> SSL client	34.12
<input type="checkbox"/> Firefox	9.33

Last updated 4 minutes ago

### Traffic by Application Risk

Risk	Total Bytes (KB)
Very Low	69,406.34
Medium	34,200.88
High	11.03

Last updated less than a minute ago

### Top Server Applications Seen

No Data

### Top Operating Systems Seen

No Data

### Traffic by Business Relevance

Business Relevance	Total Bytes (KB)
Medium	69,454.96
Low	34,112.77

# Security Cloud Control

## Introducing multi-vendor intent-based policy



Absorb and optimize  
existing rules

Change enforcement  
points, not policy

No rip and  
replace

# Policy management using Security Cloud Control



# Market-leading segmentation: Secure Workload SaaS

Zero trust segmentation across any workload, any environment

## Market Leadership



### Enterprise Scale

Single deployment supporting thousands of workloads



### Flexibility

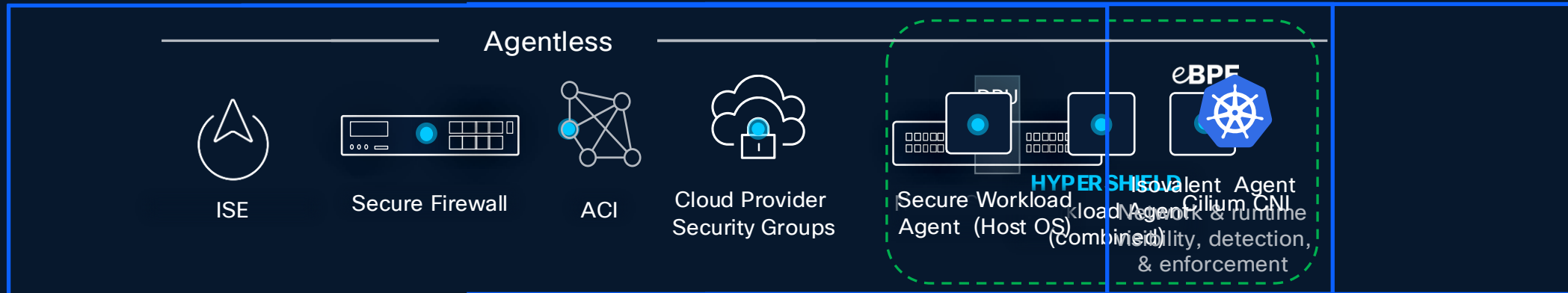
Agentless (firewall, cloud, ACI) and agent-based enforcement for any environment



### Trusted

10+ years in production, trusted by customers and recognized by analysts

# Enhancing Secure Workload with NEW enforcement points



# Security infused into the data center fabric

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\*

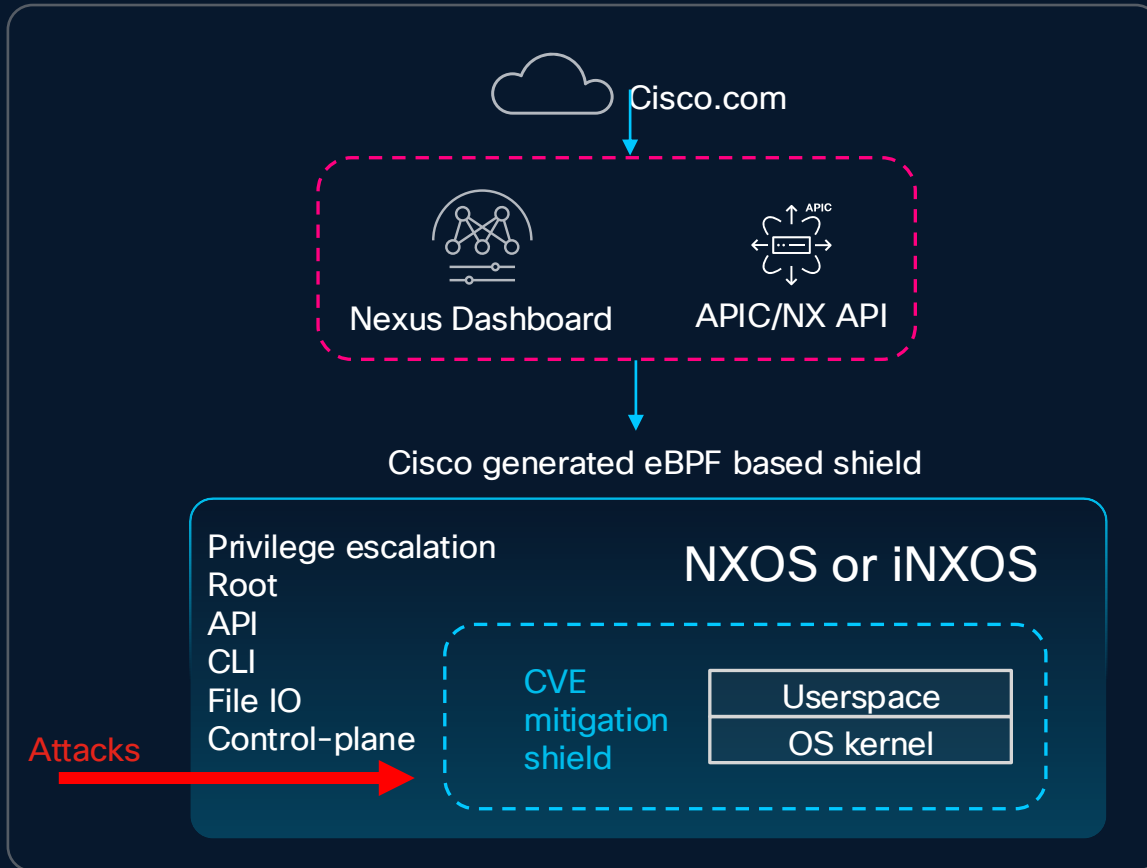
Zone-based segmentation\*

Data Center Interconnect\*

\*Limited scenarios

# Live Protect – CVE Mitigation for Nexus NXOS Switches

No Downtime or Immediate PSIRT Software Upgrades



## Data Center is critical infrastructure:

- PSIRTs require large switch fleet upgrades (100s-1000s)
- Require testing, planning, multiple maintenance windows
- High cumulative downtime - high MTTR

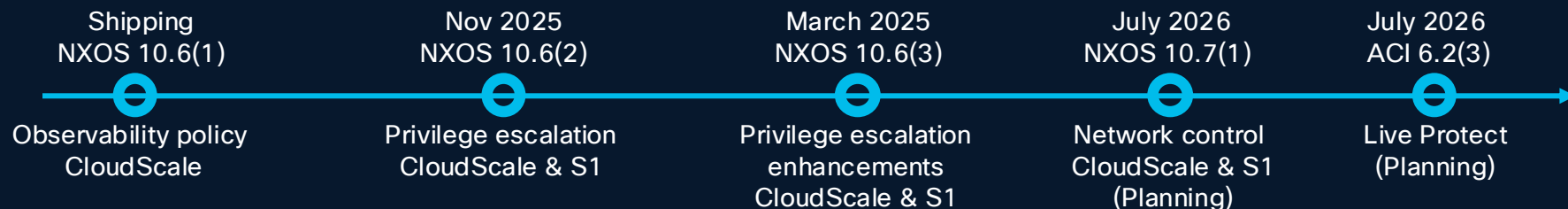
## Live Protect workflow:

- Support on **Nexus CloudScale** and **Silicon 1 switches**
- Download compensating controls from cisco.com
- Tetragon agent applies eBPF policy CVE shields
  - Monitor mode
  - Enforce mode

## Benefits:

- Nexus is 1<sup>st</sup> to market
- Arista, Juniper, Aruba, etc ... don't have it
- CVE mitigation with no downtime
- Upgrades during regular maintenance window

## Live Protect Roadmap



# Security becomes consistent, everywhere

The screenshot displays the Cisco Security Cloud Control interface. On the left is a navigation sidebar with sections: Organization (Acme Corp.), Home, Monitor (Insights, Investigations, Events & Logs, Reports & Analytics), and Manage (AI Agents, Policies, Users & Objects Inventory, Topology, Tools, Secure Connections, Platform Management, Product navigation). The main content area features a '10 new insights' section with three critical alerts: 'Elephant flow spike observed'. Below this is a 'Warning' section with 'Some other concern'. A large donut chart shows '15% Disconnected assets' with an 8% increase since yesterday. To the right of the chart is a table of asset sources:

Source	Count	24hr Δ
Firewall devices	250	↗ 11%
FTD   ASA   cdfMC		
Universal ZTNA Firewall devices	45	↗ 5%
Network tunnel groups	36	—
Resource connectors	8	—
Cloud accounts	1	—
Tesseract security agents	12,942	↗ 4%
Workload agents	19	—

At the bottom, a 'Secure Workload' section shows various security capabilities with counts: Persistence (0), Privilege Escalation (2), Defense Evasion (0), Credential Access (0), Discovery (0), Lateral Movement (1), Command and Control (0), and Exfiltration (0).

Available today

Cross-product policy experience with Mesh Policy Engine

Protect AI apps using AI Defense integration with Secure Access and Secure Firewall

Secure Workload policy into Secure Firewall

Secure Firewall virtual fully orchestrated in the cloud

# Agentic Ops



# AIOps

for Firewall

Simplifying Operations and Enhancing Security



# AgenticOps capabilities in Security Cloud Control

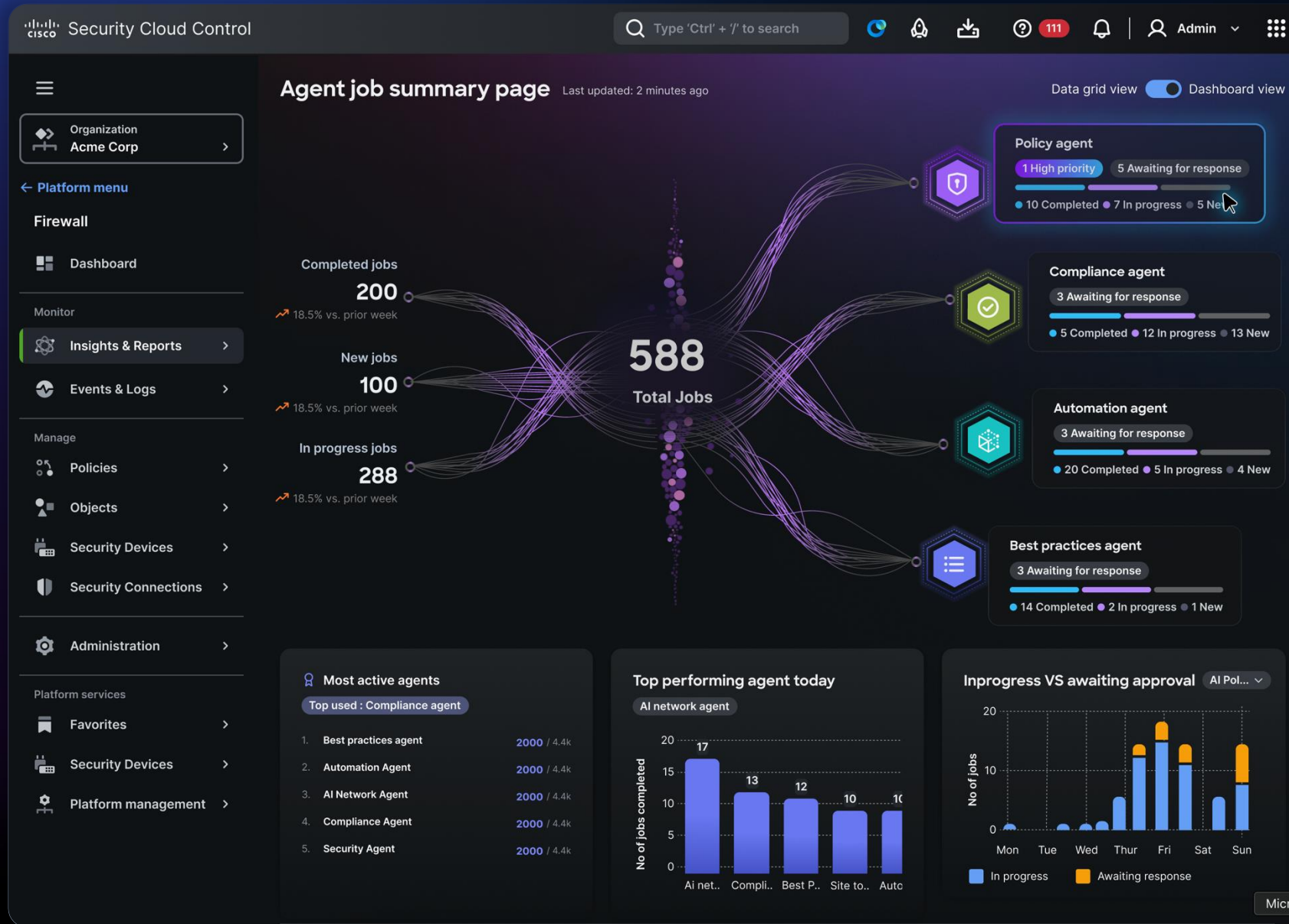
Zero Trust Access Policy Creation

VPN Capacity Planning

Elephant Flow Remediation

PCI-DSS Compliance

Firewall Policy Optimization



Targeted availability: May 2026

# Inline Policy Analyzer & Optimizer

**Anomalies detected** ?

We have detected anomalies in your rule set. Resolve these to optimize your device's performance.

**20** New\_rule Allow 🔖

**Sources** NET any-ipv4 any-ipv6 GEO Africa America Europe NET any-ipv4 any-ipv6

**Destinations and applications** NET any-ipv4 any-ipv6 GEO Africa America Europe NET any-ipv4 any-ipv6 NET

**Redundant rules** 15 **Shadowed rules** 2

**Rule Name**

Rule\_name Allow 🔖

**1** Rule\_name Allow 🔖

**Sources** NET any-ipv4 any-ipv6 GEO Africa America Europe NET any-ipv4 any-ipv6

**Destinations and applications** NET any-ipv4 any-ipv6 GEO Africa America Europe NET any-ipv4 any-ipv6 NET

> Rule 3

> Rule 8

> Rule 12

> Rule 16

> Rule 16

> Rule 16

> Rule 16

> Rule 16

> Rule 16

> Rule 16

**Cancel** Discard current rule Edit current rule Apply current rule

- Detects and shows anomalies proactively while making rule changes in a policy and saving it.
- Detects Redundant & shadowed rules.
- Requires AIOps onboarding to be complete to have inline optimizer enabled in Access control policy page.

# Adaptive Policy Insights – From Port-Based to App-Aware Security

The screenshot shows the 'Access Control Policy12' interface with the 'Policy Insights' tab selected. The main content area is titled 'No App Specified' and contains a table of rules. The table has columns for Rule Name, Apps Allowed, Apps Seen, Modified, and Created. The rules listed are all 'any' for Apps Allowed and have various 'Apps Seen' counts. The interface also includes a search bar, a filter for 'Last One Month', and a '60 results' indicator. At the bottom, there are 'Cancel' and 'Save' buttons.

Rule Name	Apps Allowed	Apps Seen	Modified	Created
1 Rule-test-allow-name1	any	12	16-03-2022; 10:30:45	20-03-2022; 15:40:20
5 Rule-test-allow-name10	any	20	16-03-2022; 10:30:45	20-03-2022; 15:40:20
3 Rule-test-allow-name3	any	10	16-03-2022; 10:30:45	20-03-2022; 15:40:20
7 Rule-test-allow-name1	any	24	16-03-2022; 10:30:45	20-03-2022; 15:40:20
14 Rule-test-allow-name3	any	15	16-03-2022; 10:30:45	20-03-2022; 15:40:20
10 Rule-test-allow-name5	any	8	16-03-2022; 10:30:45	20-03-2022; 15:40:20
8 Rule-test-allow-name12	any	13	16-03-2022; 10:30:45	20-03-2022; 15:40:20
13 Rule-test-allow-name20	any	25	16-03-2022; 10:30:45	20-03-2022; 15:40:20
19 Rule-test-allow-name30	any	32	16-03-2022; 10:30:45	20-03-2022; 15:40:20
23 Rule-test-allow-name20	any	11	16-03-2022; 10:30:45	20-03-2022; 15:40:20

## Problem:

- Many firewall rules are created without specifying applications (only ports).
- These broad rules increase exposure because *any application* can pass through.
- Admins often lack visibility into which apps are using those rules.

## Solution:

- Highlights all rules without app context.
- Shows the actual applications flowing through those rules, along with their security risk.
- Allows admins to update rules with application context, reducing attack surface and improving security posture.

"Make every rule app-aware and stop blind spots."

# NAT Policy Analyzer & Optimizer

**AIOps / Policy Analyzer and Optimizer**

< Policy Analyzer and Optimizer

**Rel\_ACP\_only** Download analysis report Discard Apply Remediation

Policy last analyzed :01/16/2025, 12:19:35 | Policy last modified :01/16/2025, 11:58:37

Summary Duplicate rules 57

**Fully Shadowed rules (0)**

A shadowed rule is a rule that will never evaluate network traffic because the traffic matches the criteria of a preceding rule in the policy, and the preceding rule takes action before the shadowed rule can be matched. [Learn about Shadowed Rules](#)

**Fully redundant rules (57)**

A rule having traffic criteria that is a subset of another rule further down the order, such that removing the redundant rule would have no impact on traffic evaluation. [Learn more](#)

1 items selected Select all Cancel Stage changes

Observation - 1 1 rule is fully redundant by rule 'OTT\_Non\_Domain\_Block'

Type	Rule status	Direction	Source interface objects	Destination interface objects	Original source Translated source	Original Destination Translated destination
Manual	Active 1	→ Dynamic	192.168.1.1	192.168.1.1	0.0.0.0/0 -	203.0.113.2/24 192.168.1.10

The following rules are made redundant by rule 1

Type	Rule status	Direction	Source interface objects	Destination interface objects	Original source Translated source	Original Destination Translated destination
Manual	Active 2	→ Dynamic	192.168.1.1	10.0.0.2	0.0.0.0/0 -	203.0.113.2/24 192.168.1.10
Manual	Active 8	⇒	172.16.0.3	192.168.0.4	any	any

**Select rules to remediate**

To address the identified redundancies across 3 observations, you can choose from the following actions. Please note that the implementation of these rules will be staged and won't occur immediately.

Manual rules

Delete all selected

Disable all selected

Auto NAT rules (Cannot be disabled)

Delete all selected

Confirm staging

- Detects rule anomalies across Network Address Translation Policy available in the cdFMC tenant
- Reports about Shadowed rules and redundant rules and provides remediation suggestions
- Option to download analysis report
- Flexibility for user to select specific anomalies & remediate.
- Ability to apply the changes in the policy

# 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](#)

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

# Renewal Upgrade Planner

The screenshot shows the Cisco Security Cloud Control interface for the 'Renewal Upgrade Planner'. The main heading is 'Upcoming End-of-Life for BLR-05-FW2100', with a 'Generate Report' button. The status is 'Critical' and 'Operational', dated 'Jan 9, 2025 | 07:08:00'. The description states that the device is approaching its End-of-Life (EOL) date on November 15, 2025, and that Cisco no longer provides software updates, security patches, or technical support. The impacted device is 'BLR-05-FW2100' with an EOL date remaining of 220 days.

Below the description is a table titled 'Device with similar Model' with the following data:

Device name	Location	Software version	Last supported version
BLR-887	10.10.7.252 : 448	6.4.1	7.2
MUM-818	10.10.5.352 : 443	6.4	7.4
BLR-898	10.10.8.258 : 443	6.4.2	7.4
VPN-9888	10.10.5.357 : 445	6.4.2	7.4
ZTNA-821	10.10.8.922 : 443	7.4	7.4

Further down, there are sections for 'Cisco's recommended - Renewal upgrade devices' and 'Product Recycling'. The recommended devices include:

- Cisco Firepower 1000 Series:** OS version 7.8, Rack mounted, 1.4 Gbps (1x faster), Performance Up to 15K VPN sessions, 1-5 Gbps Interfaces. [View data sheet](#)
- Cisco Secure Firewall 3100 Series:** OS version 7.8, Rack mounted, 2.0 Gbps (1x faster), Performance Up to 30K VPN sessions, 1-7 Gbps Interfaces. [View data sheet](#)
- Cisco Secure Firewall 4200 Series:** OS version 7.8, Rack mounted, 2.4 Gbps (1x faster), Performance Up to 50K VPN sessions, 1-10 Gbps Interfaces. [View data sheet](#)
- Cisco Firepower 1000 Series:** OS version 7.8, Rack mounted, 1.4 Gbps (1x faster), Performance Up to 15K VPN sessions, 1-5 Gbps Interfaces. [View data sheet](#)

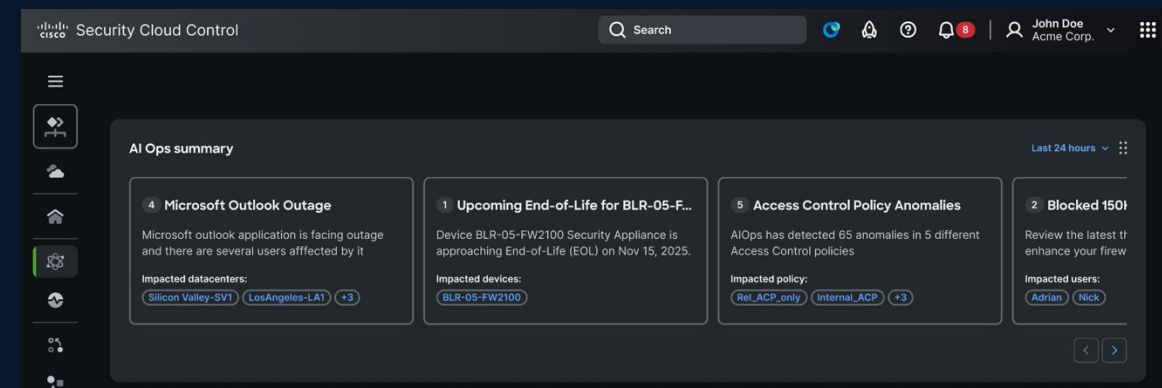
The 'Product Recycling' section highlights the Cisco Takeback and Recycle program, which helps businesses properly dispose of surplus products. It includes a 'Know more' link.

At the bottom, there is a 'Talk with expert' section with options to 'Get a call from Sales' (Submit request) and 'Call Sales' (1-800-121-3117, 9:00am-6:00pm).

© 2024 Cisco Systems, Inc. Privacy policy Terms of service

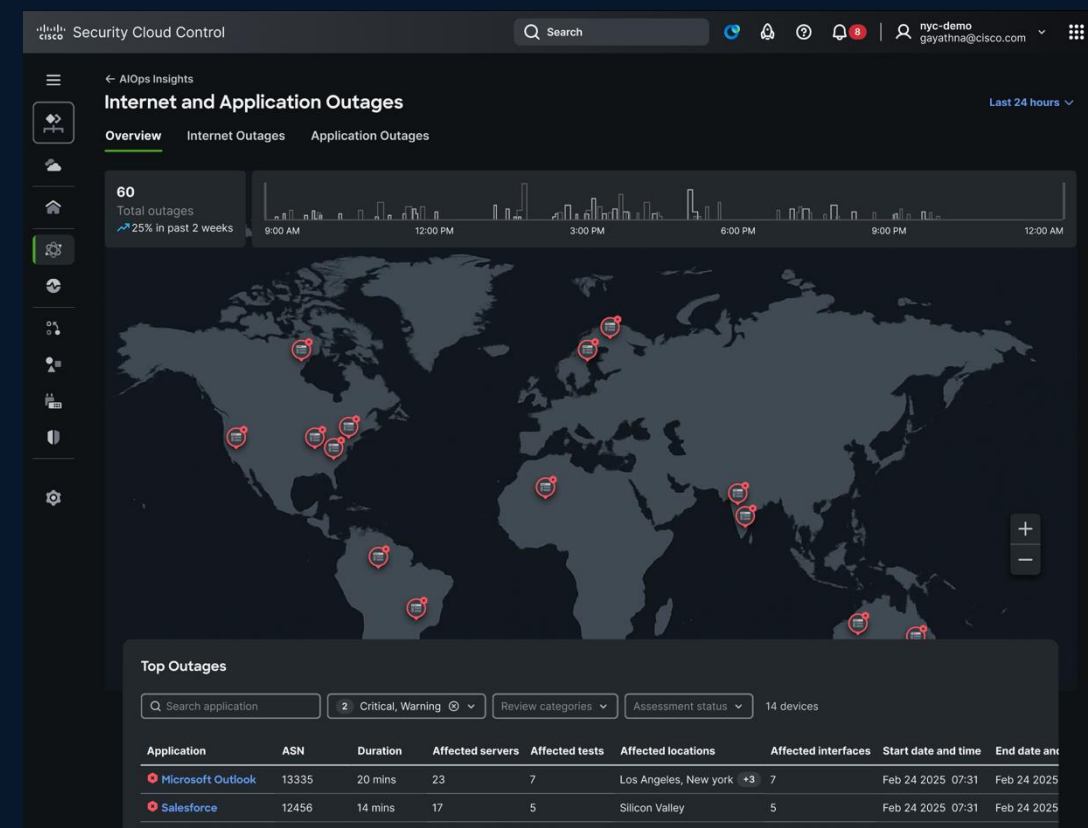
- List ASAs and FTDs reaching End of Life (EOL) in the tenant.
- Recommends FTD models to renew/refresh with based on newer models released.
- Provides quick access to data sheets & release notes for further details on the specification.
- In product notifications and reports about EOL available for customers

# Internet & Network Outages visibility with Thousand Eyes Integration



## Problem:

- When apps or internet services go down (e.g. Microsoft 365, Salesforce), IT teams often struggle to know:
  - Is it the network, the application provider, or our firewall?
  - How widespread is the issue (global vs local)?
  - Which users or sites are impacted?
- This lack of visibility slows root cause analysis and leads to wasted time troubleshooting problems outside your control.



## Solution:

- ThousandEyes Internet Insights integration into AIOps for firewall provides real-time visibility into internet and application outages.
  - What is broken?
  - Where is the impact and the duration of impact?
  - Shows outages which are relevant or applicable to the customer based on their configuration & event data.

# Agent Squad

## Workforce as a Service

The screenshot shows the Cisco Security Cloud Control interface for the Firewall Agent. The page is titled "Firewall Agent" and includes a search bar, user profile (Admin, Acme Corp.), and navigation icons. The main content area is titled "Agent focused (Personas/Expertise)" and features a "+ Add new Persona/Expertise" button. Three agent personas are listed:

- AI Network Engineer** (Recruit toggle on):
  - Network topology analysis
  - Routing & switching protocols
  - Firewall and VPN management
  - Security event detection
  - Automated diagnostics and remediation
  - Specialized in designing, monitoring, and troubleshooting complex network infrastructures to ensure seamless connectivity and performance.
  - Task the agent can perform:
    - Monitor network health and uptime
    - Diagnose and resolve connectivity issues
    - Optimize network configurations
    - Detect and respond to security threats
    - Provide recommendations for network improvements
    - Generate network performance report
- PCI Compliance Specialist** (Recruit toggle on):
  - PCI DSS controls and requirements
  - Security policy enforcement
  - Configuration assessment
  - Audit log management
  - Compliance reporting
  - Focused on helping organizations meet Payment Card Industry Data Security Standard requirements and maintain secure handling of payment data.
  - Task the agent can perform:
    - Continuously monitor systems for PCI compliance
    - Detect and alert on non-compliant configurations
    - Guide remediation of compliance gaps
    - Generate audit-ready compliance reports
    - Educate teams on PCI best practices
    - Track and document remediation activities
- Automation Specialist** (Recruit toggle on):
  - Scripting and workflow design
  - Process optimization
  - Integration with IT systems and APIs
  - Error detection and self-healing
  - Reporting and analytics
  - Designed to streamline IT operations by automating routine tasks, workflows, and incident responses to enhance efficiency and accuracy.
  - Task the agent can perform:
    - Identify processes suitable for automation
    - Create and execute automation scripts
    - Monitor automated workflows for success/failure
    - Troubleshoot automation errors
    - Recommend areas for further automation
    - Provide usage and efficiency reports

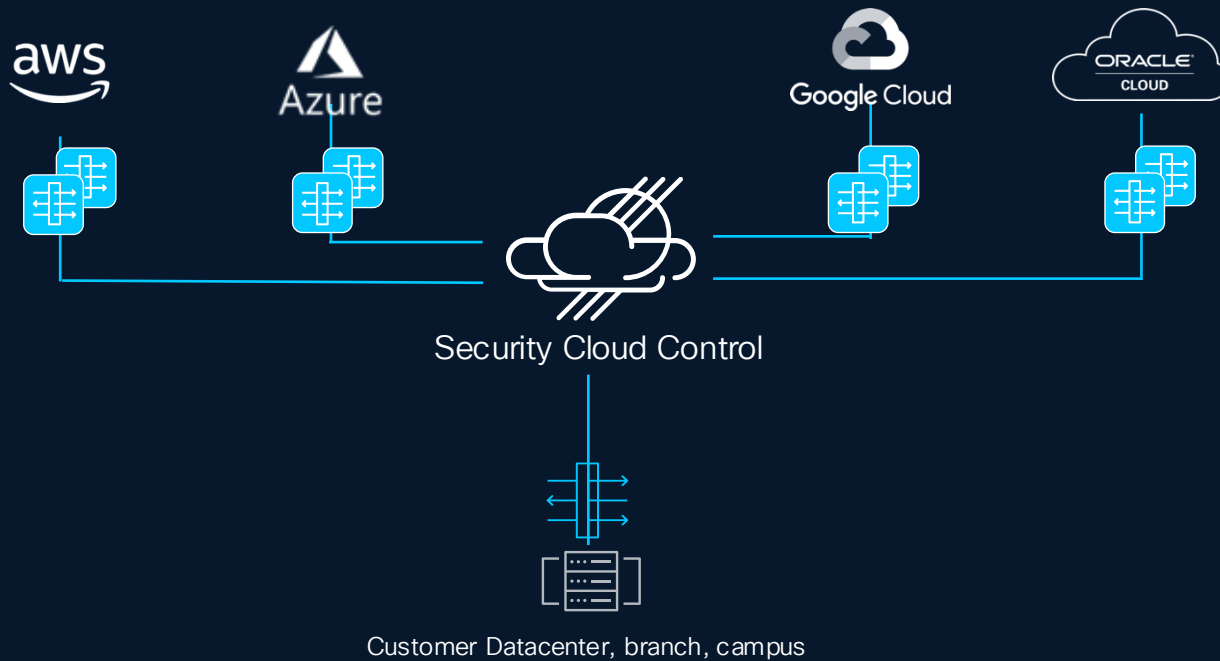
Each persona card includes "Start thread" and "Learn More" buttons. The footer contains copyright information (© 2025 Cisco Systems, Inc.) and links to Privacy policy and Terms of service.

Introduces autonomous AI agents as a new operational layer – not just to assist humans, but to become an integral part of the workforce fabric, enabling organizations to onboard AI agents like employees.

Design for representation purpose only

# Extending Secure Firewall to the cloud, *natively*

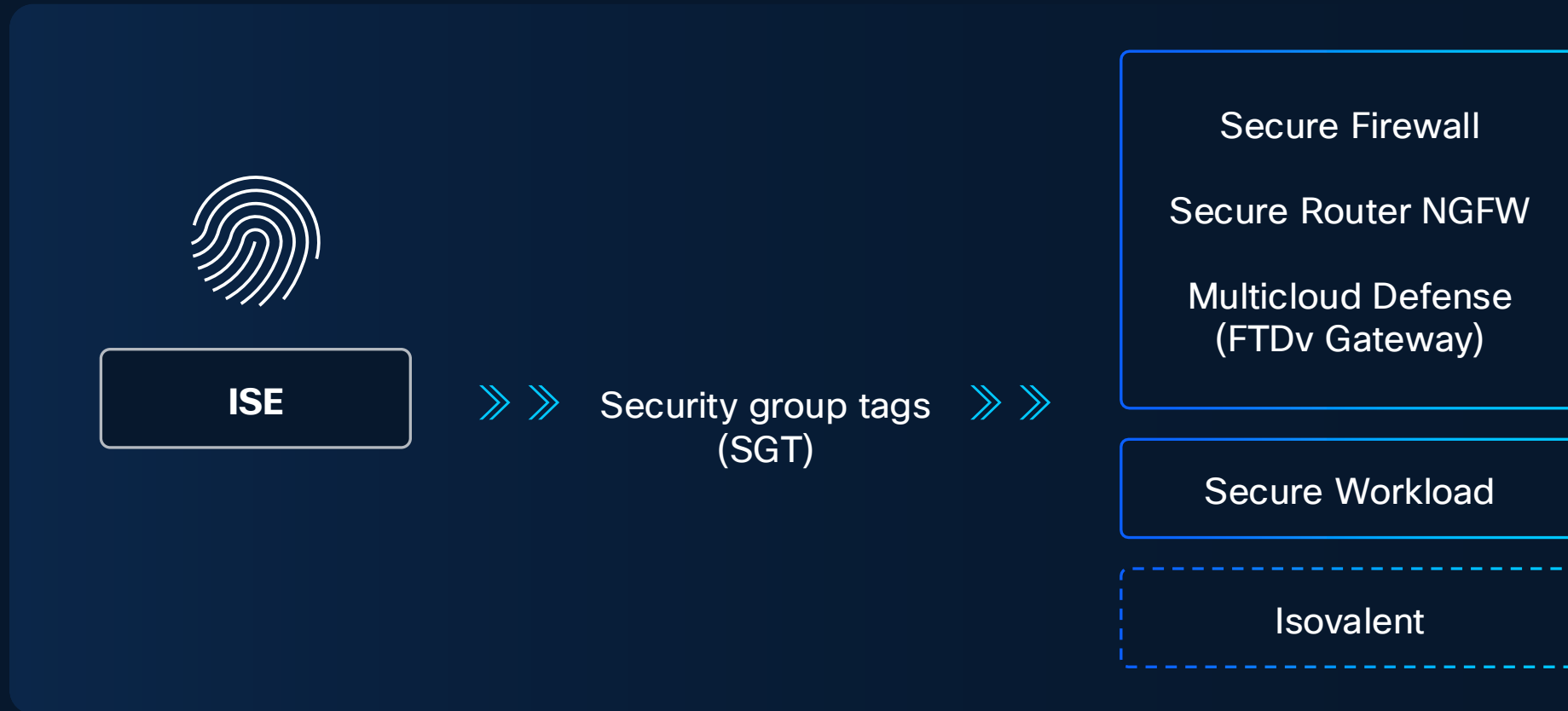
NEW



- Cloud-agnostic automation and orchestration
- Comprehensive visibility of clouds, assets, and their risks
- Automatically deploy, scale, and heal, from Security Cloud Control
- Hourly price; unlike other offers based on size and bandwidth

# Identity in the AI world

# Our unique differentiator: Common classification across all Network and Security enforcement points



# Cisco Identity Intelligence



Users



Machines



Services



Apps



Data



Behaviors

SailPoint

Dragos

Okta

CrowdStrike

PingIdentity

Salesforce

Microsoft



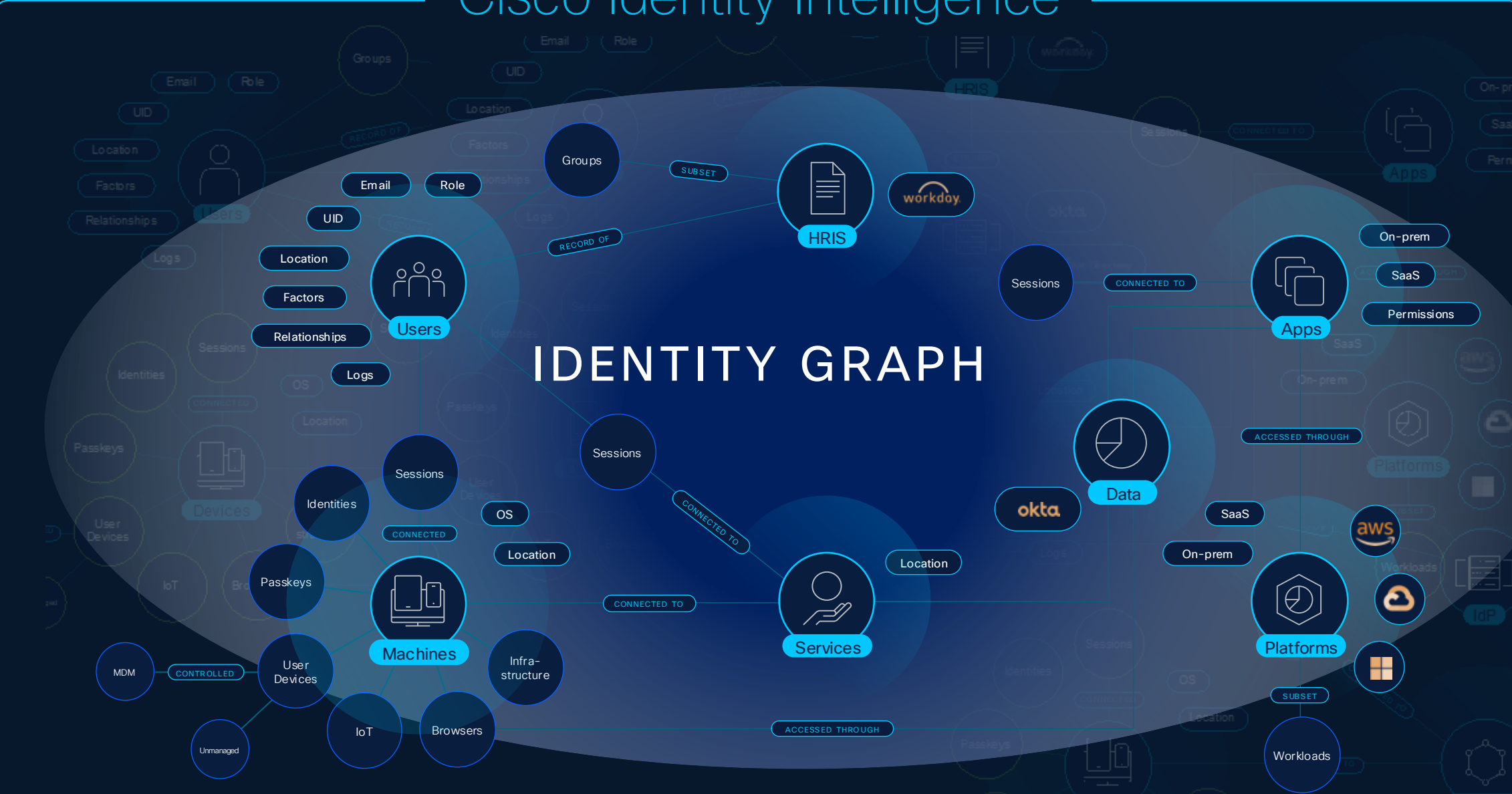
Google

Zscaler

Amazon

CyberArk

# Cisco Identity Intelligence



# Risky user visibility with Cisco Identity Intelligence Integration

- Cisco Secure Firewall integrates with Cisco Identity Intelligence as part of AI Ops
- Use Cisco Identity Intelligence to identify risky users and behavior



### AI Ops Summary

#### User Risk Spike Due to Suspicious Behaviour

Critical Security Mar 25, 2025 | 07:08:00 PM (UTC+5)

**Description**  
Users' risk level is rising faster than acceptable, possibly indicating a compromised account, malware, or other malicious activity. The system has detected this abnormal increase over a defined time frame, and has identified that this increase has exceeded the normal expected behavior. This requires immediate investigation.

**Impacted users**  
4 users

**Probable cause**  
Attackers may be using brute-force logins to obtain administrative access and reach sensitive resources using methods such as pass-the-hash, pass-the-ticket, or exploiting system vulnerabilities.

**Confidence level**  
High

**Users**  
4 results

User name	Trust level	Reason	Trust level change time (UTC+5)
John Smith	Untrusted	Logged in from a blocklisted IP address. Additional cont...	Feb 24 2025 07:31
Adrian	Untrusted	Geolocation mismatch	Feb 21 2025 16:40
Gabriel	Untrusted	-	Feb 18 2025 13:01
Joseph	Untrusted	Logged in from a blocklisted IP ad..	Feb 09 2025 06:20

Rows per page: 10 < 1 2 >

**Remediation**  
Implement targeted remediation strategies to elevate protection.

**Block users**  
Use this remediation to block suspicious users and prevent them from gaining access to important data or applications.

**Remediation steps**  
1. Go to Access Control Policies.  
2. Review the "Block\_Untrusted\_User" rule created by Dynamic Firewall wizard.

# Secure Firewall with Duo User Trust

The screenshot displays the Cisco Security Cloud Control AIOps Insights dashboard. The interface includes a navigation sidebar on the left with sections like Organization (acme-netsec), Platform menu (Firewall, Dashboard), Monitor (Insights & Reports, Events & Logs), and Manage (Policies, Objects, Security Devices). The main content area features an 'AIOps summary' for the 'Last 24 hours' period, showing 34 insights (8 Active, 0 Resolved, 9 Critical, 17 Warning, 8 Informational) and 24 configurations. A donut chart visualizes insights by device. Below this, there are sections for 'Insights by device' and 'Insights by priority', with a list of active insights such as 'User risk spike due to suspicious behavior'.

# Hybrid Mesh Firewall (Segmentation as a Platform)

## CUSTOMER SECURITY OUTCOMES

Network Segmentation

Macro & Micro Segmentation

Threat Detection & Exploit Protection

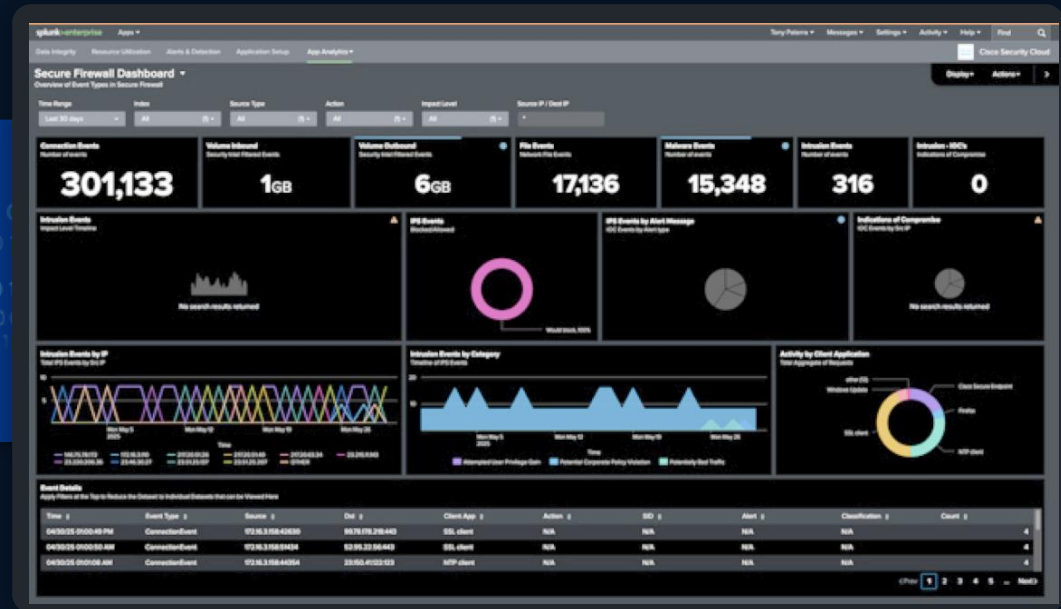
AI Security



Write policy once, enforce across the mesh

# Security Insight, on Us

## Free Cisco firewall logs to Splunk\*

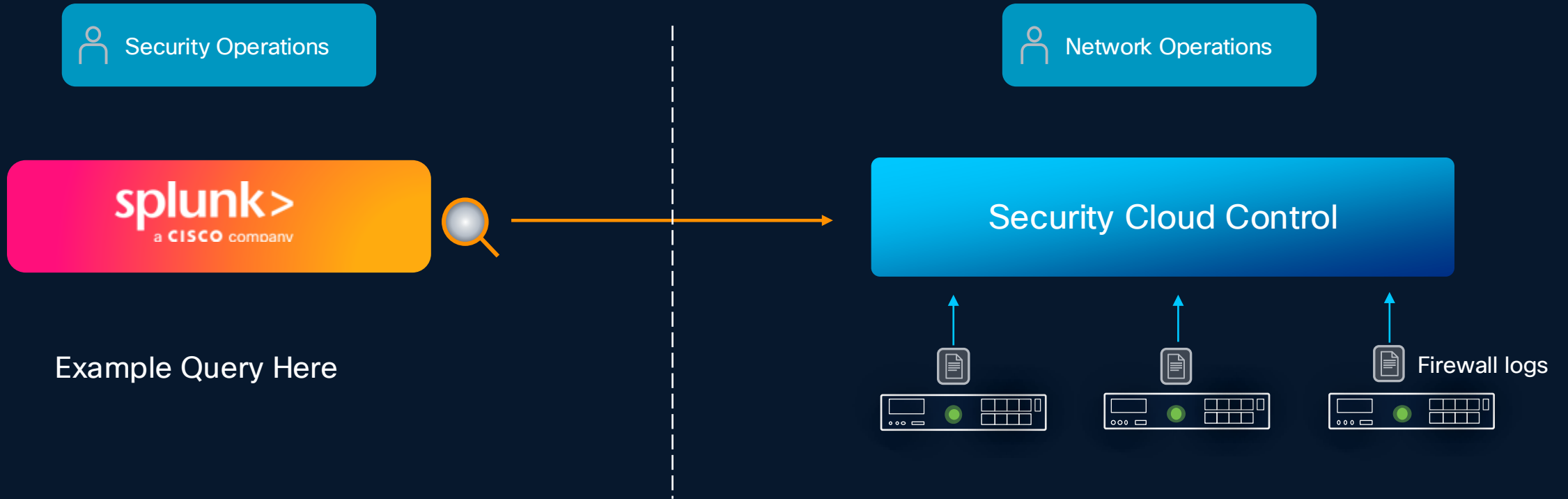


New detections | Automated response

\*Ingest up to 5GB/device/day requires Firewall Threat Defense subscription and Splunk license

# Faster threat detection at lower cost

Federated Search with Cisco Secure Firewall and Splunk



Faster Threat Hunting

60% cost savings

Operational simplicity

# Customer and Industry Recognition

NetSec **OPEN**

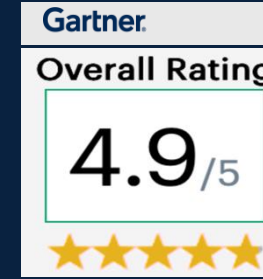


30% faster than other firewalls



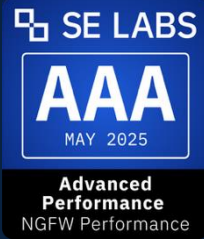
Positioned as the only Visionary

Magic Quadrant for Hybrid Mesh Firewall, 2025



Recognized in Peer Insights™

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



Industry's first to earn AAA rating in advanced performance



A Leader

MarketScape Worldwide Enterprise Hybrid Firewall 2025 Vendor Assessment

FORRESTER

A Leader

The Forrester Wave™: Enterprise Firewall Solutions, Q4 2024



100% accuracy in advanced security and NDR protection



A Winner

FORRESTER

A Leader

The Forrester Wave™: Microsegmentation Solutions Q3 2024

# AI powered Cisco security cloud: Cisco shines where security meets the network

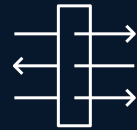
## Future-proof workplaces



Accelerate Universal  
Zero Trust Access

User Protection Suite

## AI-ready data centers



Accelerate Hybrid  
Mesh Firewall

Cloud Protection Suite

## Digital resilience



Power security  
operations

Breach Protection Suite  
Splunk Security

**CISCO** Connect

**Thank you**



