CISCO Connect

Segmentation Untangled: Streamlining Hybrid Data Center Security

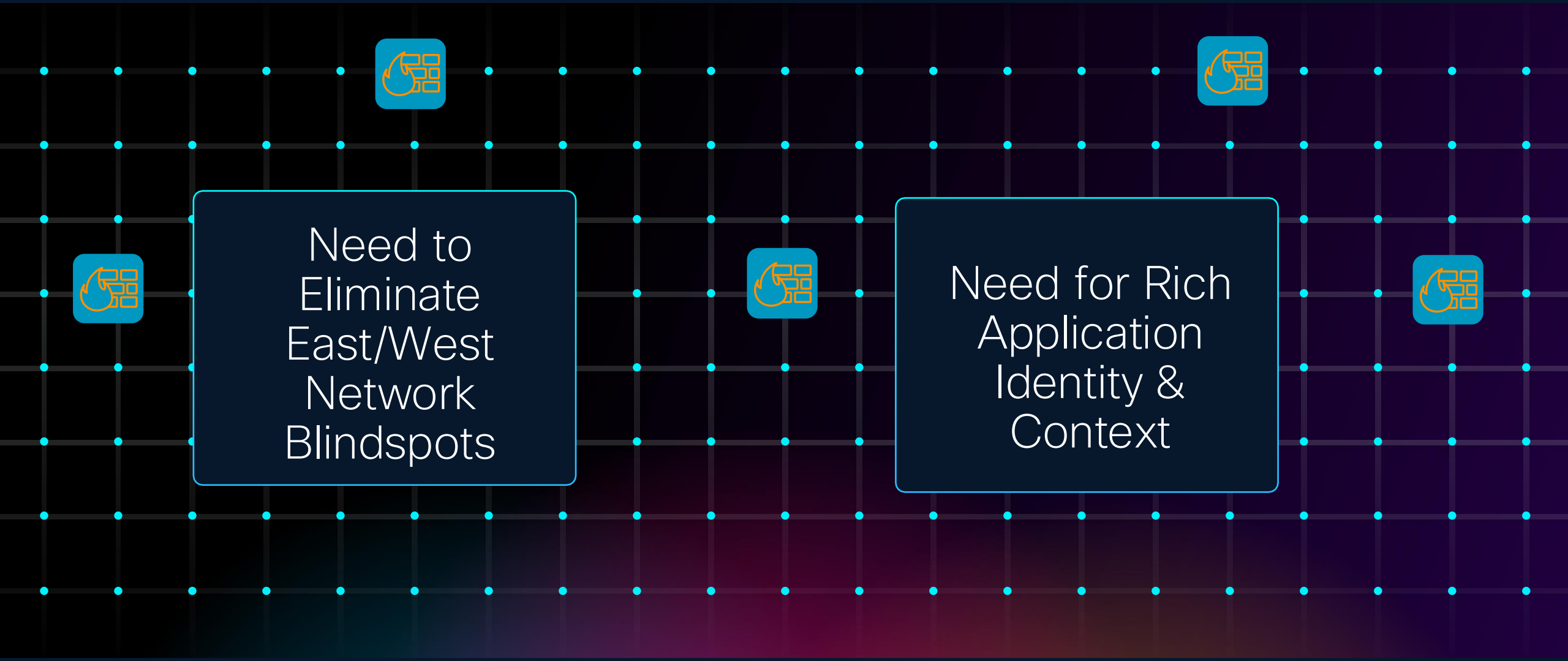
Jeff Fanelli – Distinguished Solutions Engineer

October 30, 2025

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

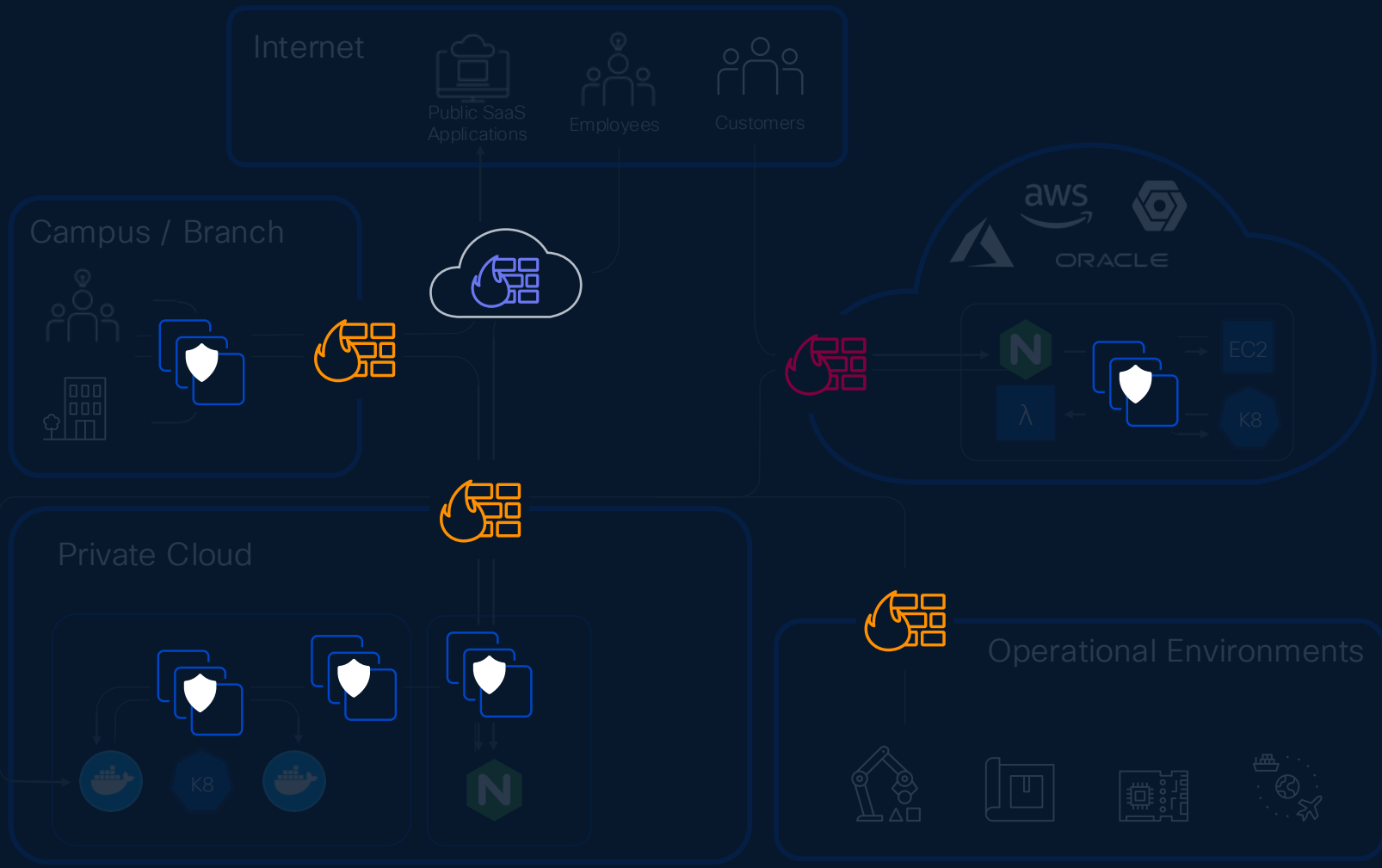
The Future of Network Security is **DISTRIBUTED**



Inserting security controls at every juncture

of user, device and applications interaction

Policy gaps
Manual & siloed policy management



Delayed threat detection & response
Disjointed telemetry

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

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

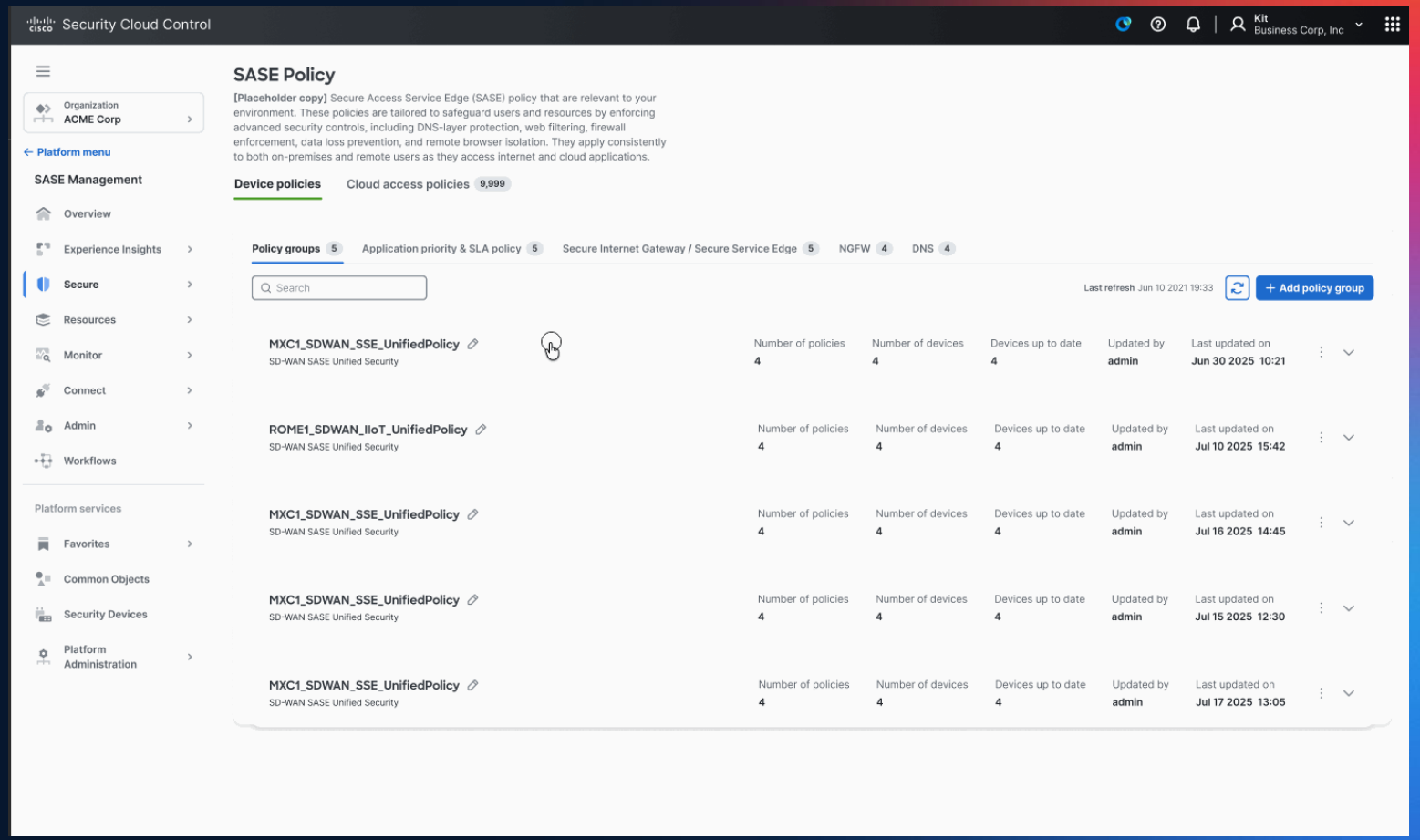
Centralized Policy and Objects

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



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

Security Cloud Control

Cisco Firewalls

Physical | Virtual | Cloud | FWaaS

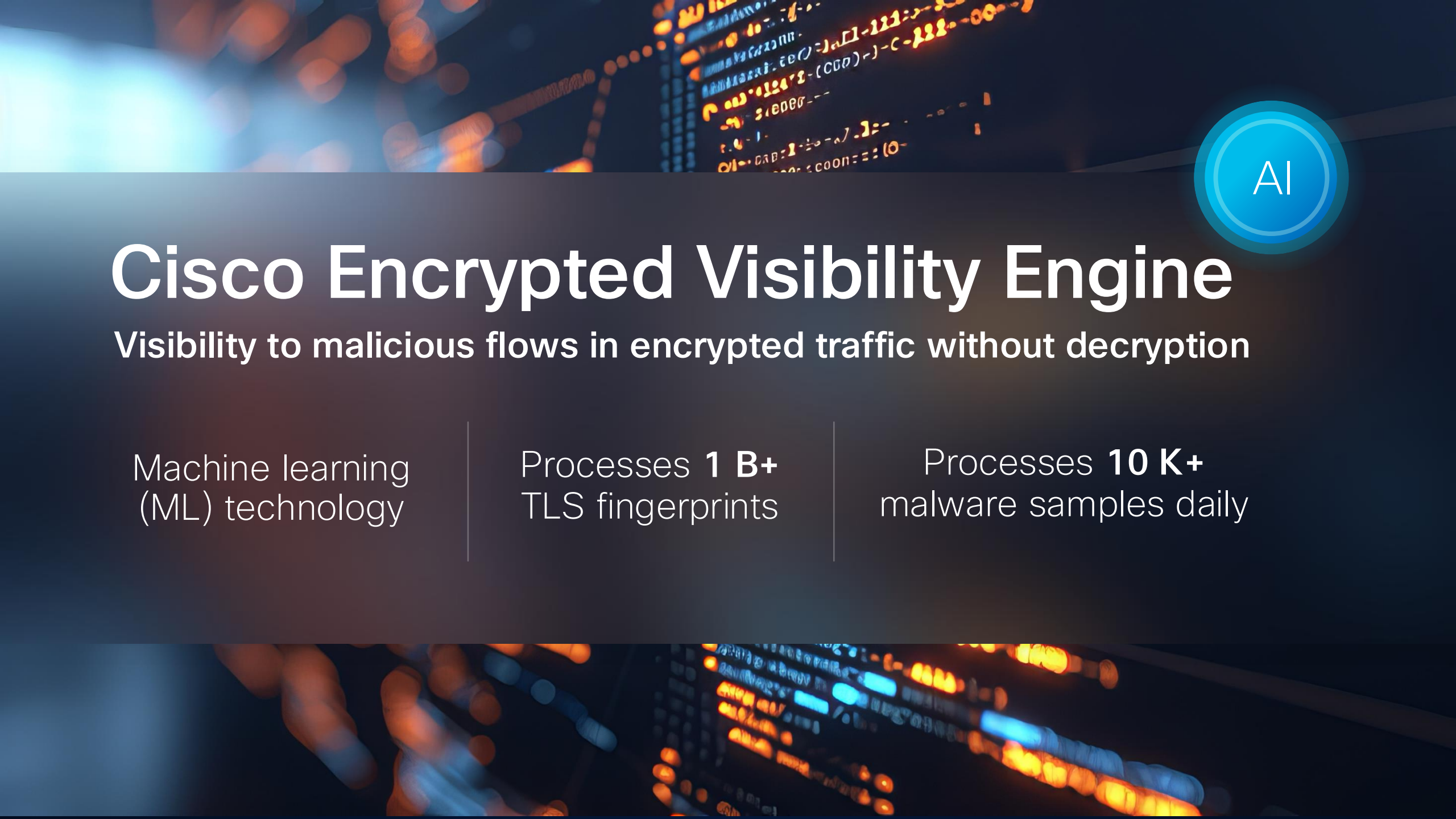
3rd Party Firewalls

Smart Switches

Workload agents

Macro — Segmentation → Micro

Define policy once, enforce everywhere



Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

Machine learning (ML) technology

Processes **1 B+** TLS fingerprints

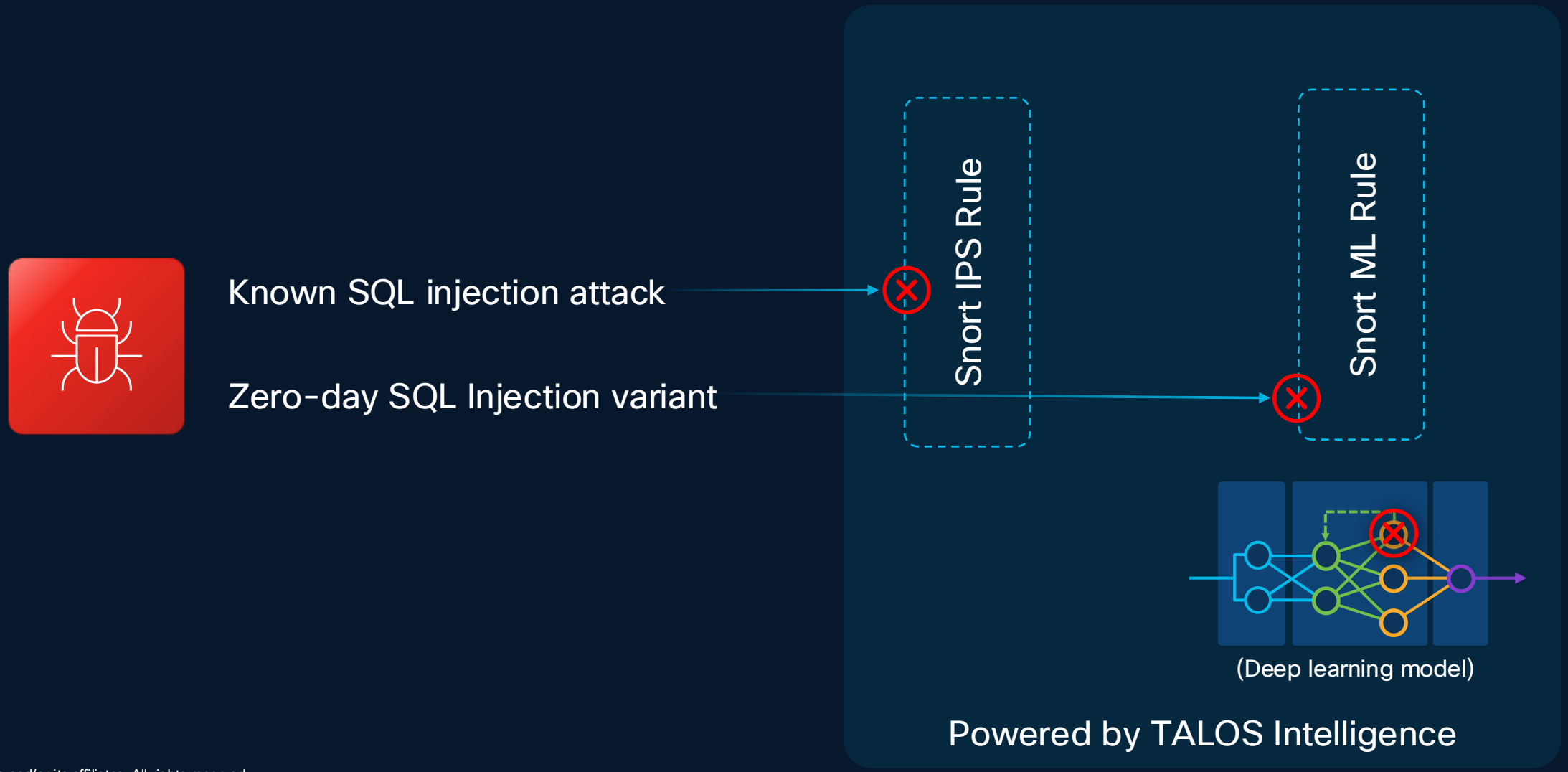
Processes **10 K+** malware samples daily

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



Home
Overview
Analysis
Policies
Devices
Objects
Integration

Create Report

Summary Dashboard (switch dashboard)

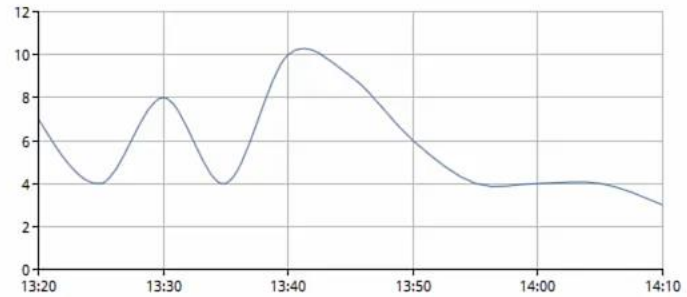
Provides a summary of activity on the appliance

Network | Threats | Intrusion Events | Status | Geolocation | QoS | Zero Trust | Encrypted Visibility Engine

Show the Last: 1 hour

Add Widgets

Unique Applications over Time



Last updated 3 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

Traffic by Business Relevance

Business Relevance	Total Bytes (KB)
Medium	69,454.96

Top Web Applications Seen

Application	Total Bytes (KB)
Ubuntu Update Manager	34,112.77
Ubuntu	405.35
Mozilla	18.15
Docker	11.03

Last updated 1 minute ago

Top Server Applications Seen

No Data

Top Client Applications Seen

Application	Total Bytes (KB)
Advanced Packaging Tool	34,478.07
SSL client	34.12
Firefox	9.33

Last updated 4 minutes ago

Top Operating Systems Seen

No Data

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

Policy is placed intelligently across Cisco and non-Cisco Firewalls

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

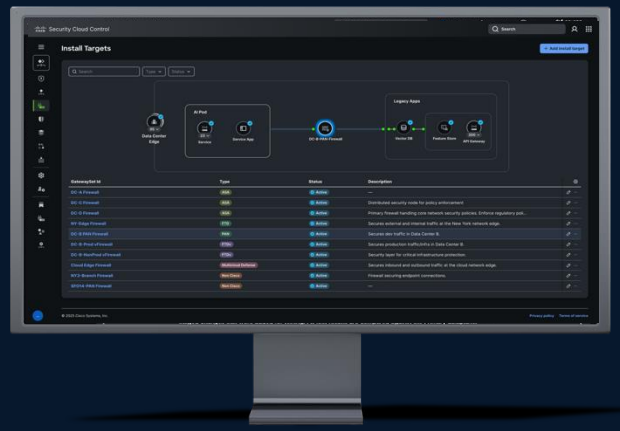
Orderable

N9348Y2C6D-SE1U

48-port 1G/10G/25G, 6-port 400G, 2-port 100G

800G Services Throughput

Security Cloud Control



Use Cases

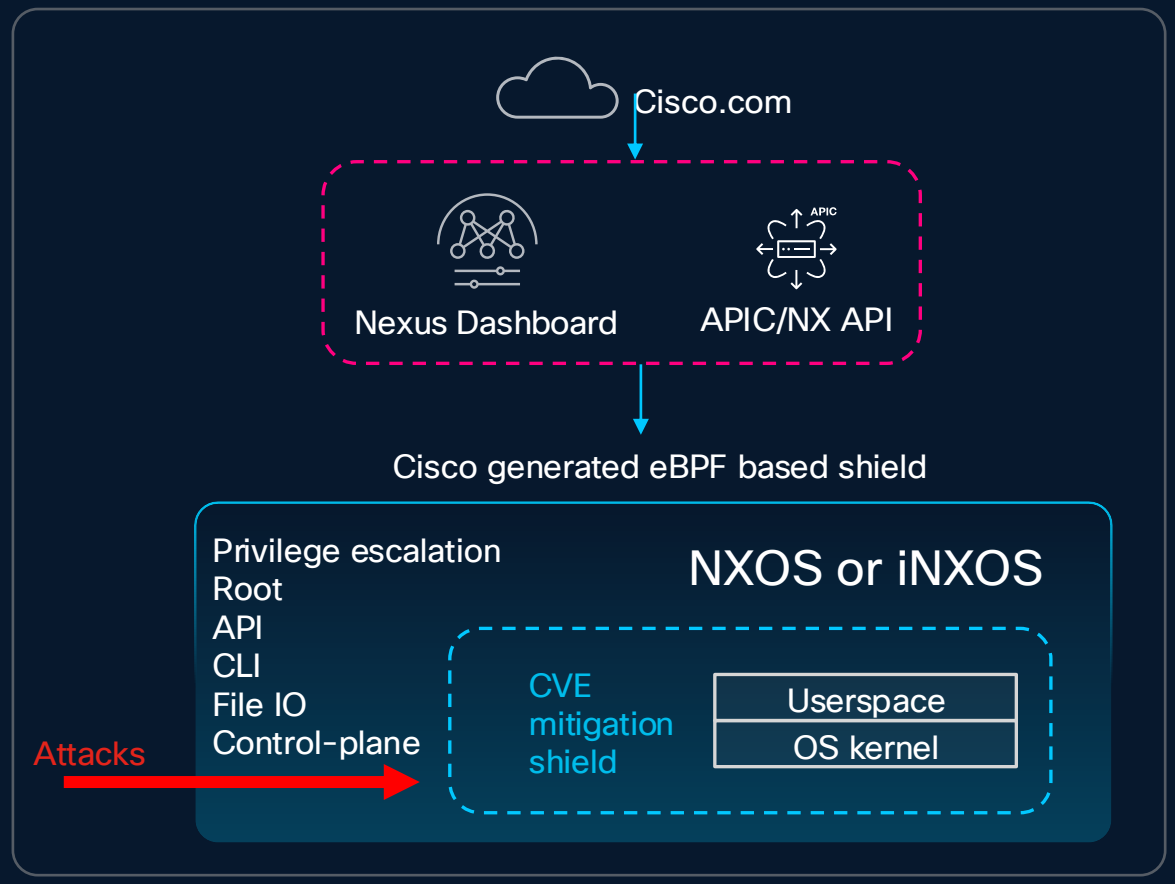
- Top of Rack segmentation and enforcement
- Cloud Edge*
- Zone-based segmentation*
- Data Center Interconnect*

*Limited scenarios

cisco

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

Live Protect Roadmap

Shipping NXOS 10.6(1)	Nov 2025 NXOS 10.6(2)	March 2025 NXOS 10.6(3)	July 2026 NXOS 10.7(1)	July 2026 ACI 6.2(3)
Observability policy CloudScale	Privilege escalation CloudScale & S1	Privilege escalation enhancements CloudScale & S1	Network control CloudScale & S1 (Planning)	Live Protect (Planning)

Security becomes consistent, everywhere

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

Full roadmap: Firewall (physical, virtual, cloud, container) | Multicloud agentless microsegmentation | AI security
Global threat intelligence | SSE | SD-WAN | SASE | Infrastructure Detection & Response | MFA | Email security | Endpoint security

Agentic Ops

AIOps

for Firewall

Simplifying Operations and Enhancing Security

AgenticOps capabilities in Security Cloud Control

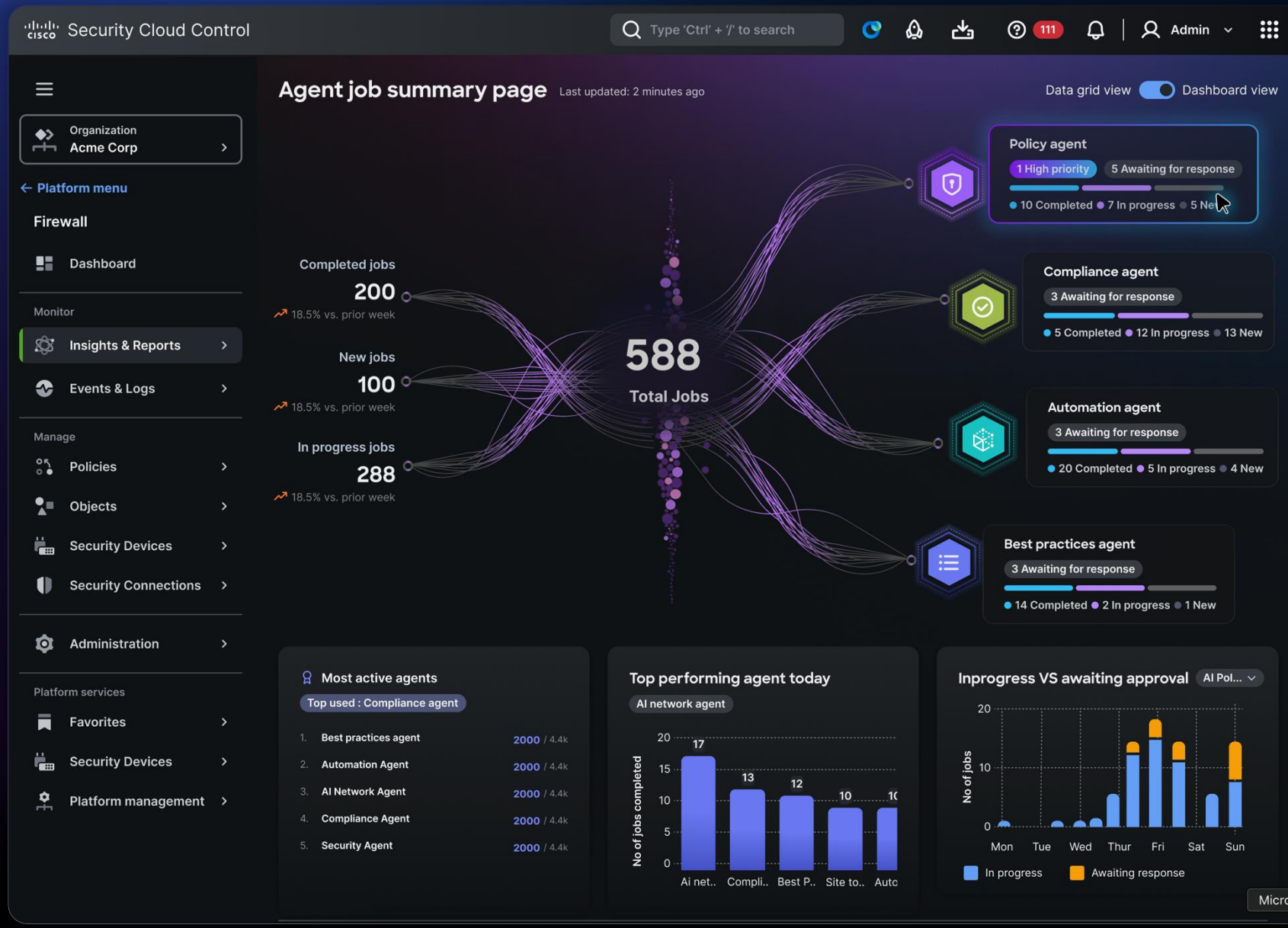
Zero Trust Access Policy Creation

VPN Capacity Planning

Elephant Flow Remediation

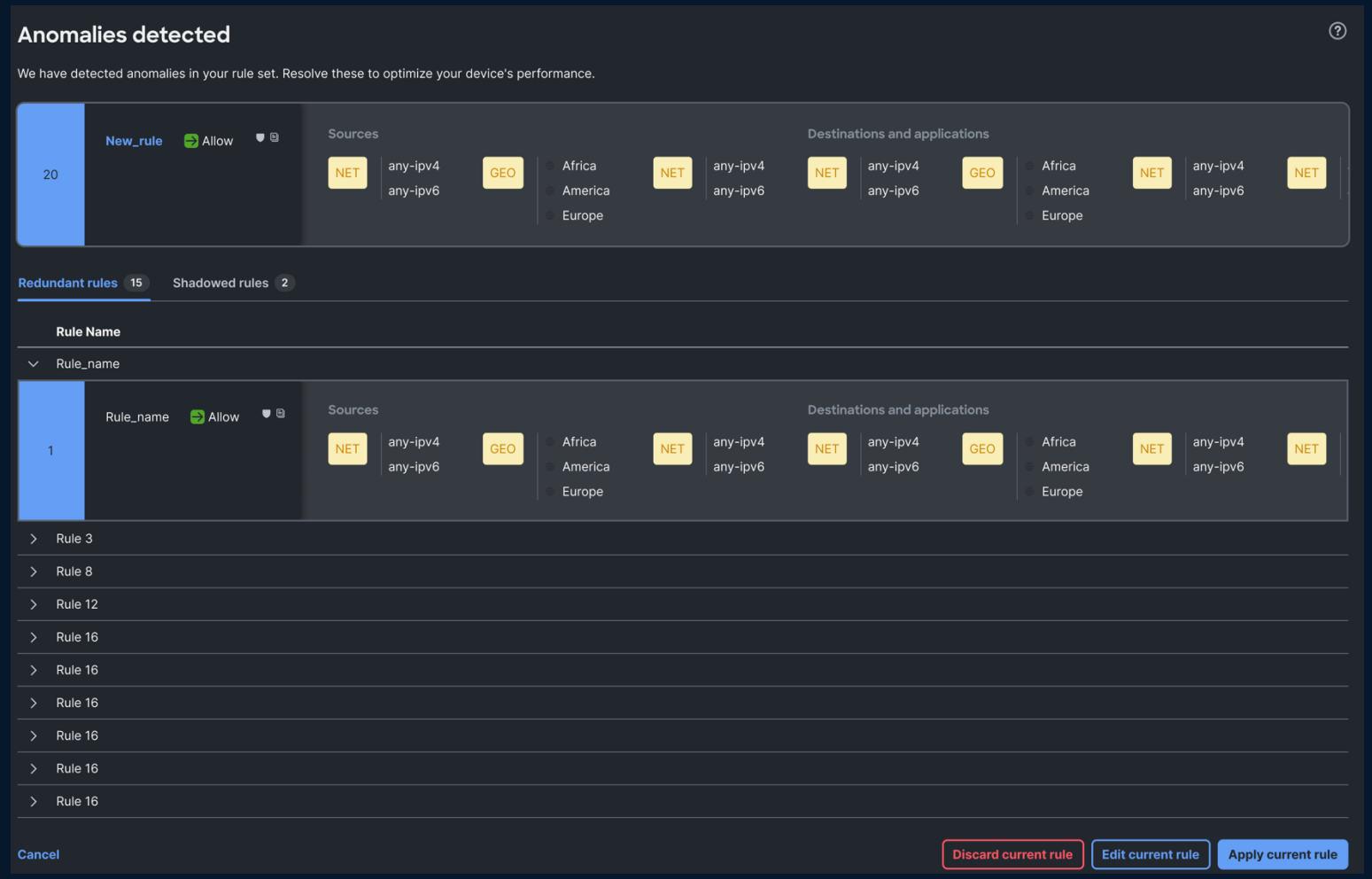
PCI-DSS Compliance

Firewall Policy Optimization



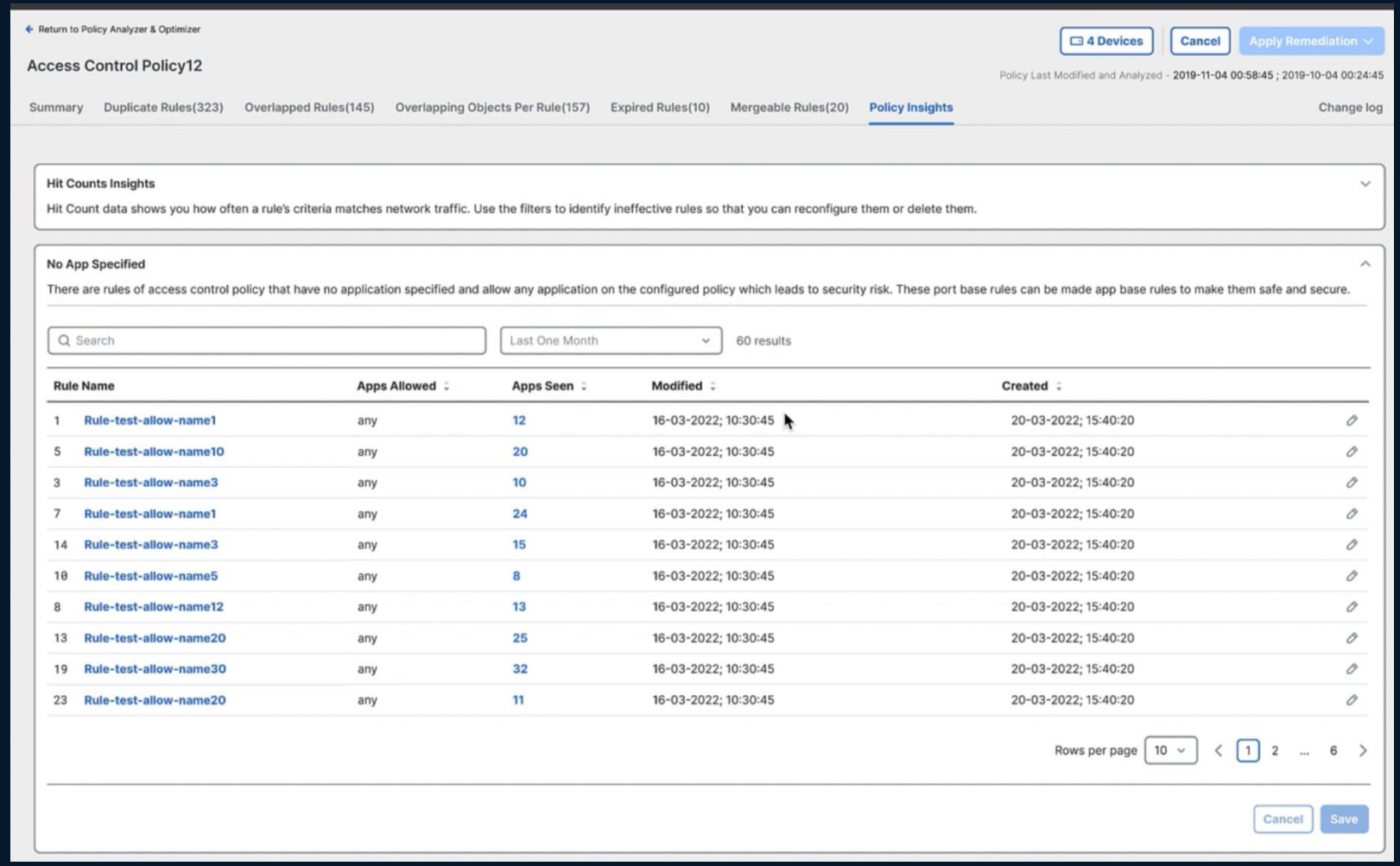
Targeted availability: May 2026

Inline Policy Analyzer & Optimizer



- 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



Problem:

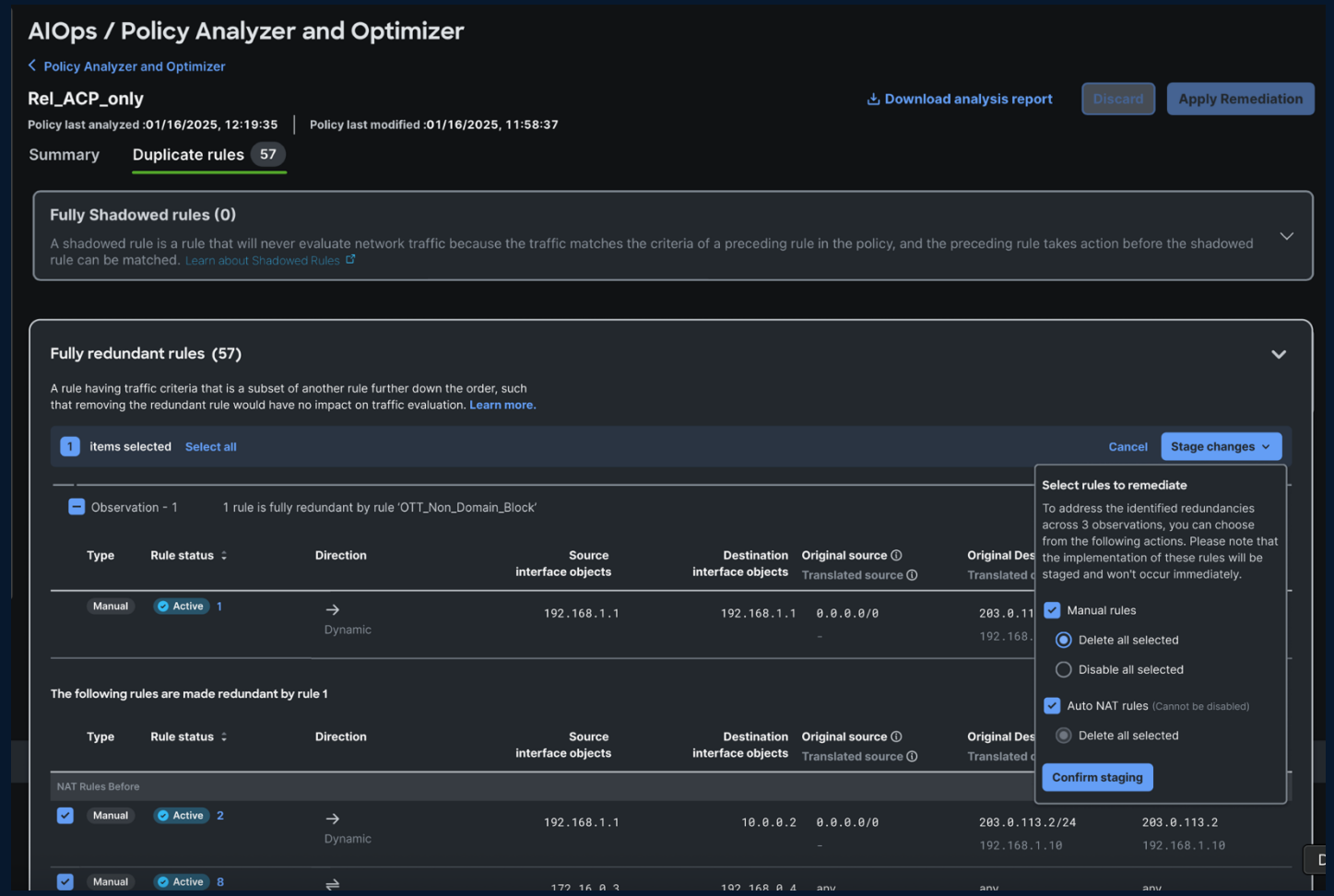
- Many firewall rules are created without specifying applications (only ports).
- These broad rules increase exposure because *any application* can pass through.
- Admins often lack visibility into which apps are using those rules.

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.

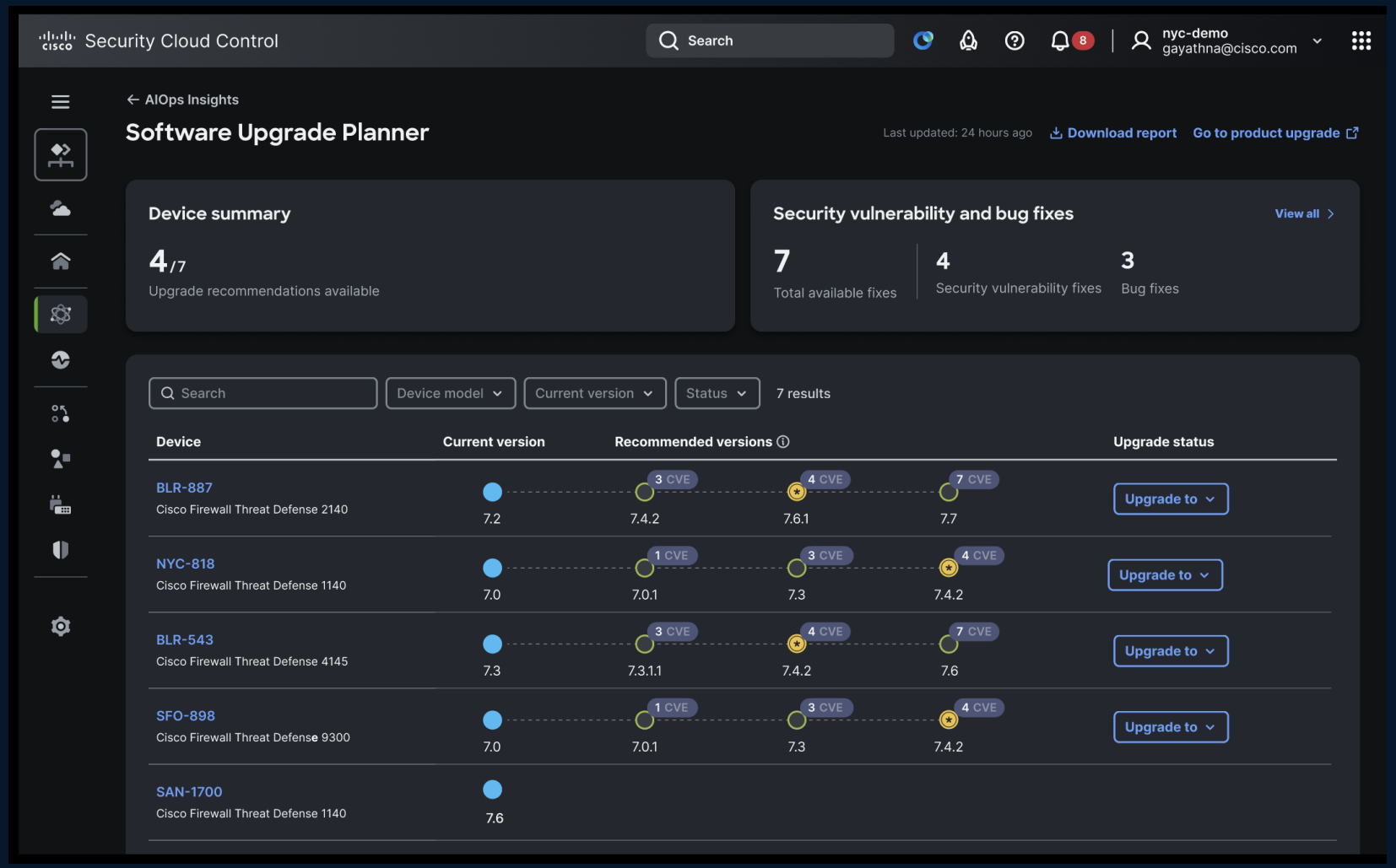
"Make every rule app-aware and stop blind spots."

NAT Policy Analyzer & Optimizer



- 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

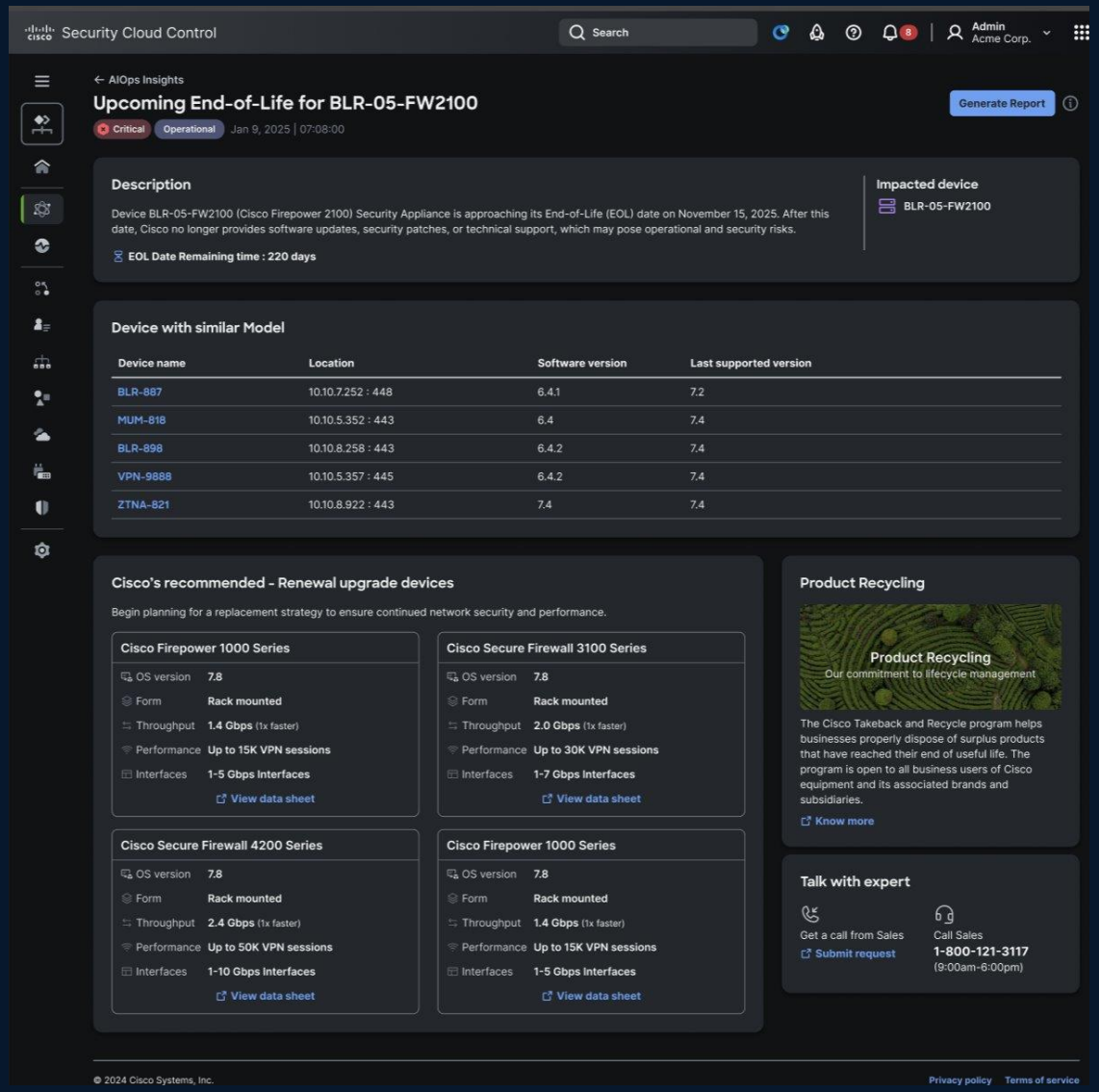


- Custom analysis of PSIRTs and bugs based on current customer versions.
Identify and mitigate relevant risks before upgrading.

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

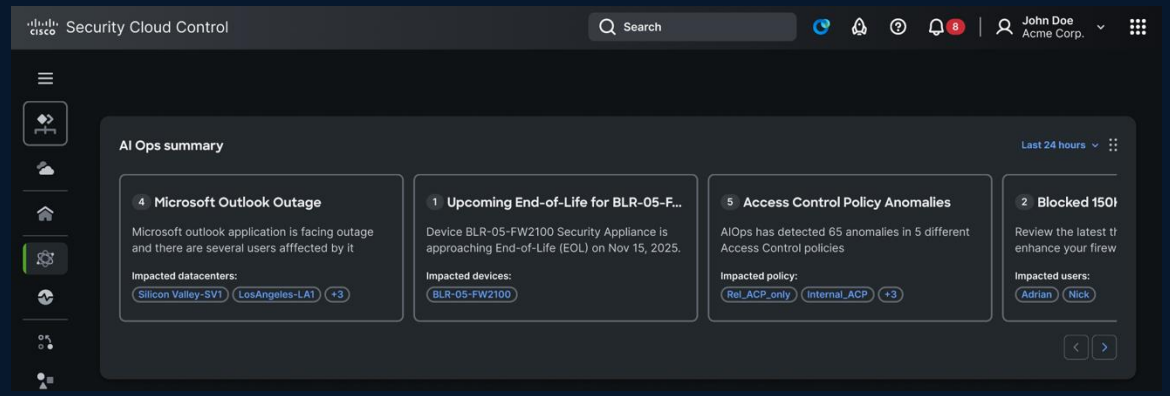
- No more manual research to determine upgrade paths.
Get upgrade version recommendations instantly tailored to your environment.

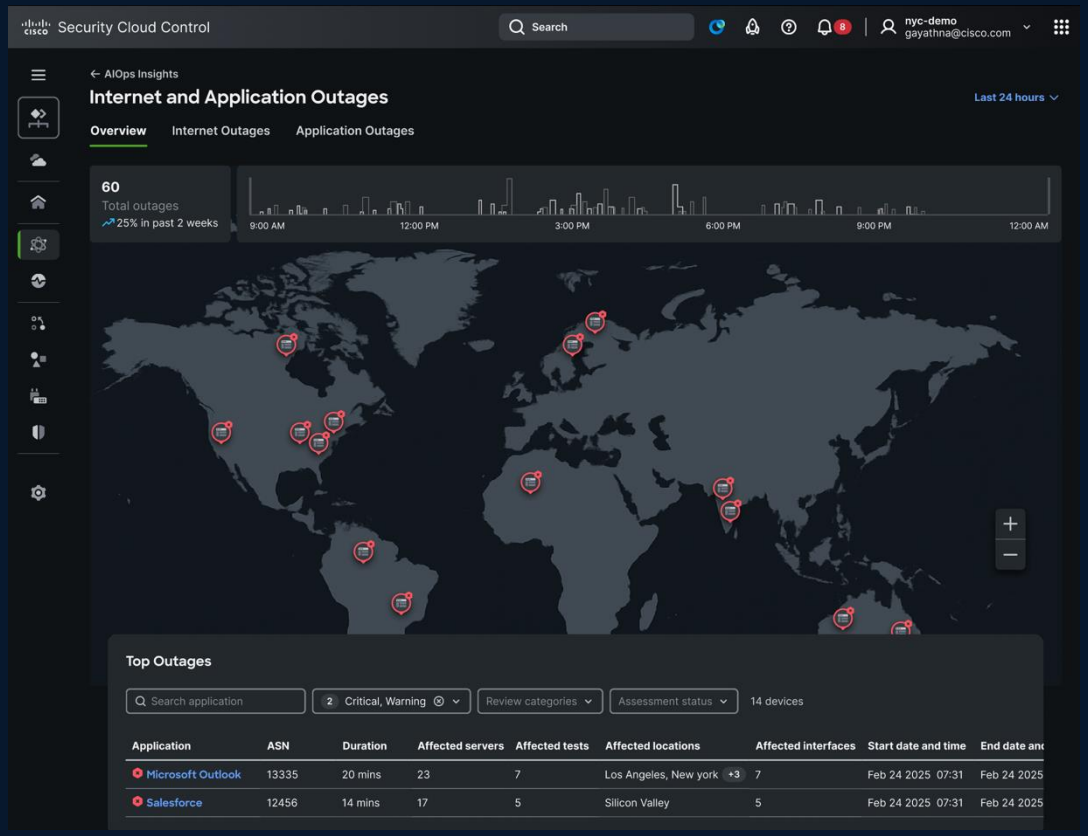
Renewal Upgrade Planner



- 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:

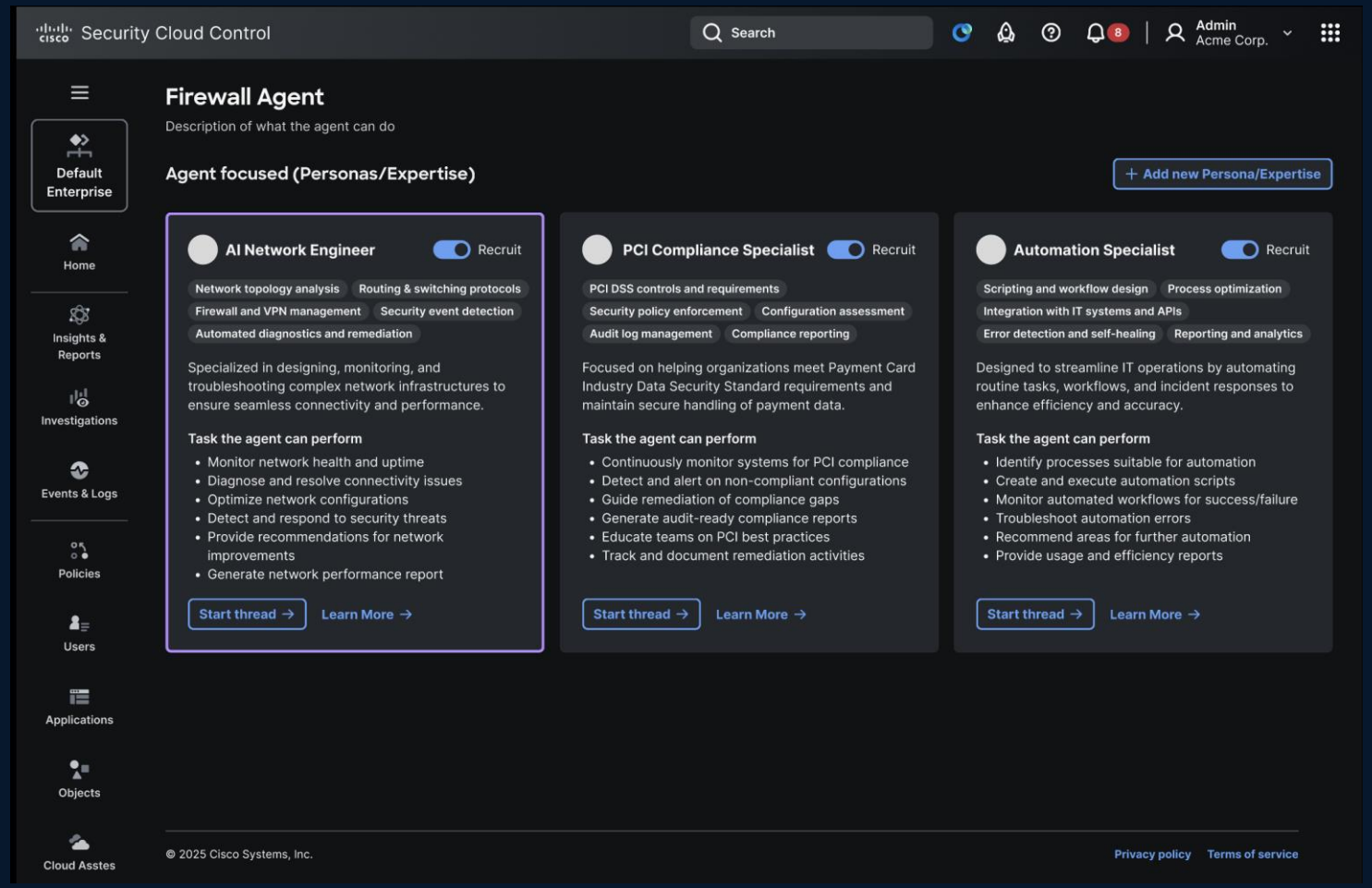
- When apps or internet services go down (e.g. Microsoft 365, Salesforce), IT teams often struggle to know:
  - Is it the network, the application provider, or our firewall?
  - How widespread is the issue (global vs local)?
  - Which users or sites are impacted?
- This lack of visibility slows root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

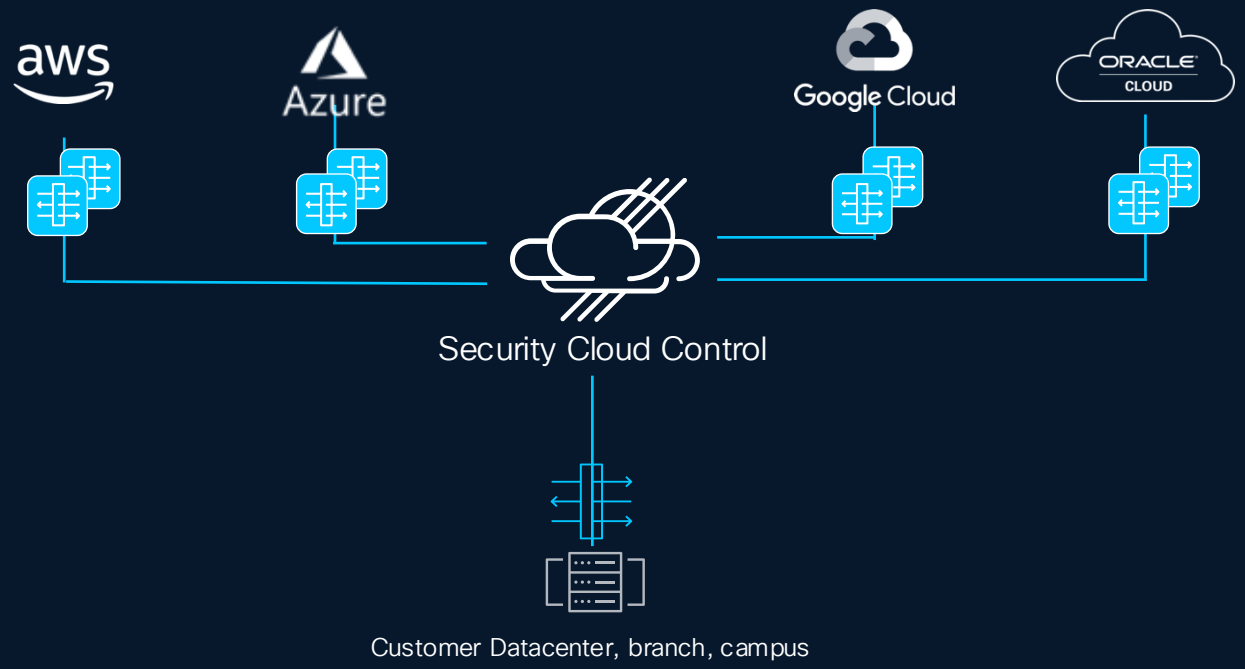


Design for representation purpose only

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.

Extending Secure Firewall to the cloud, *natively*

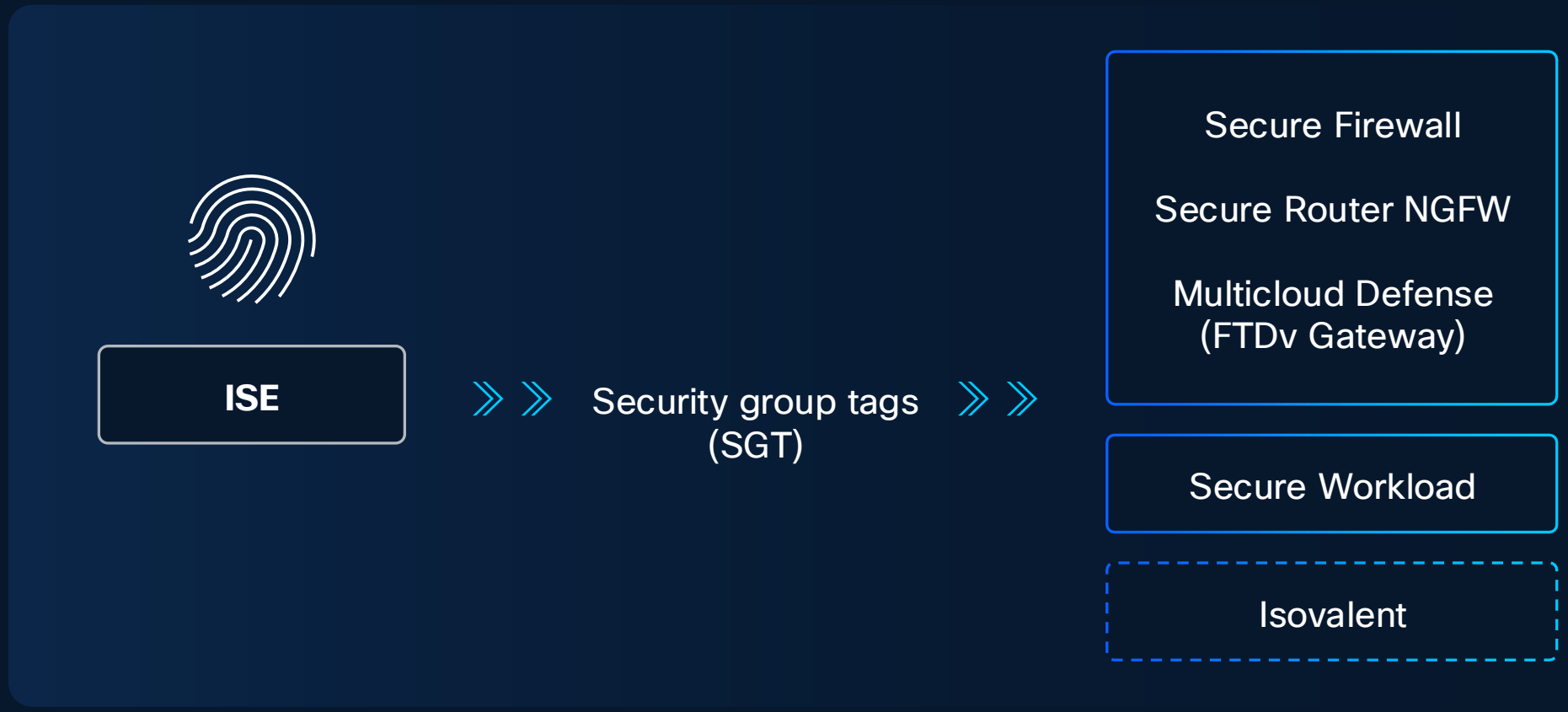
NEW



- 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

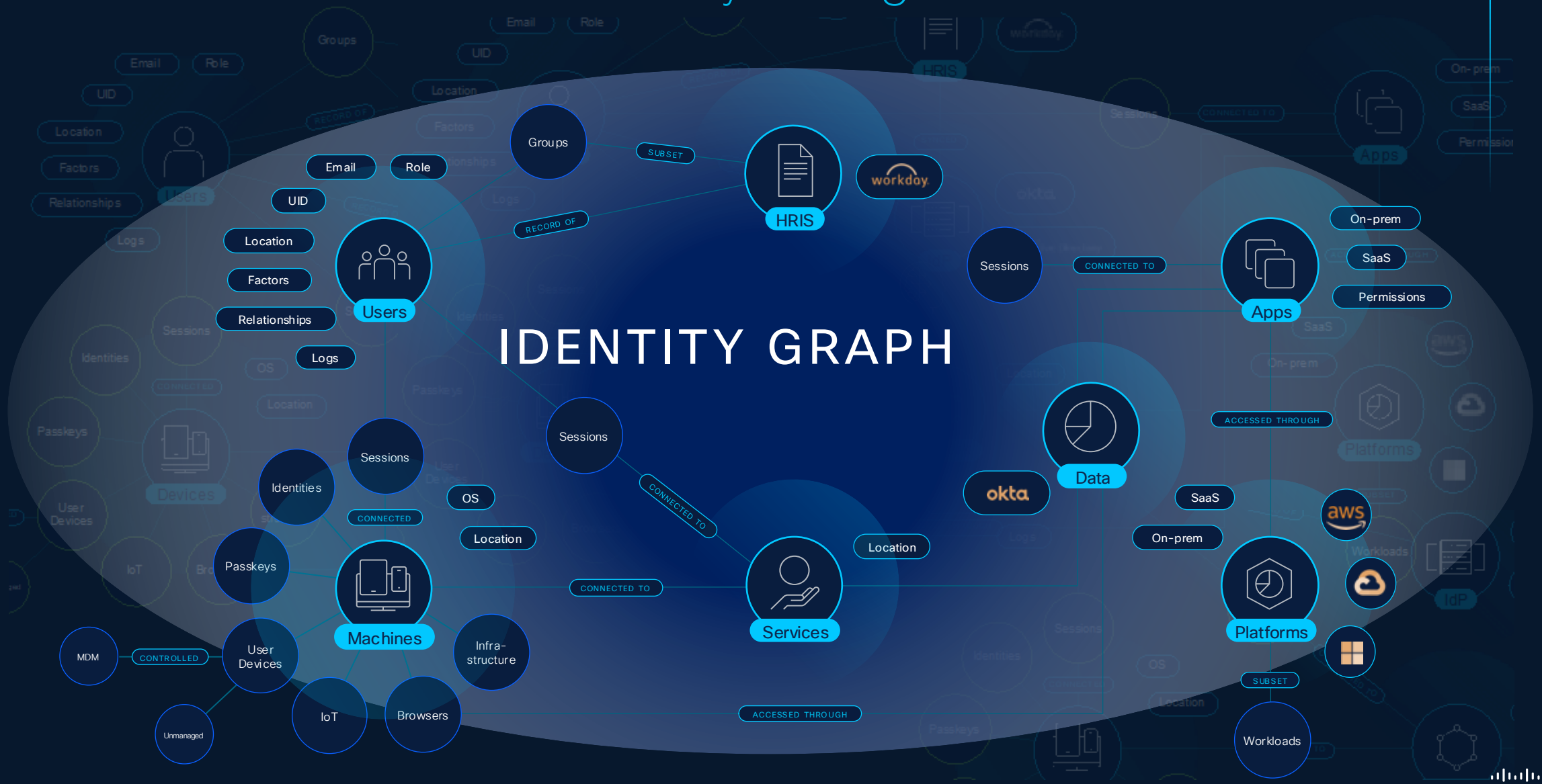
Our unique differentiator: Common classification across all Network and Security enforcement points



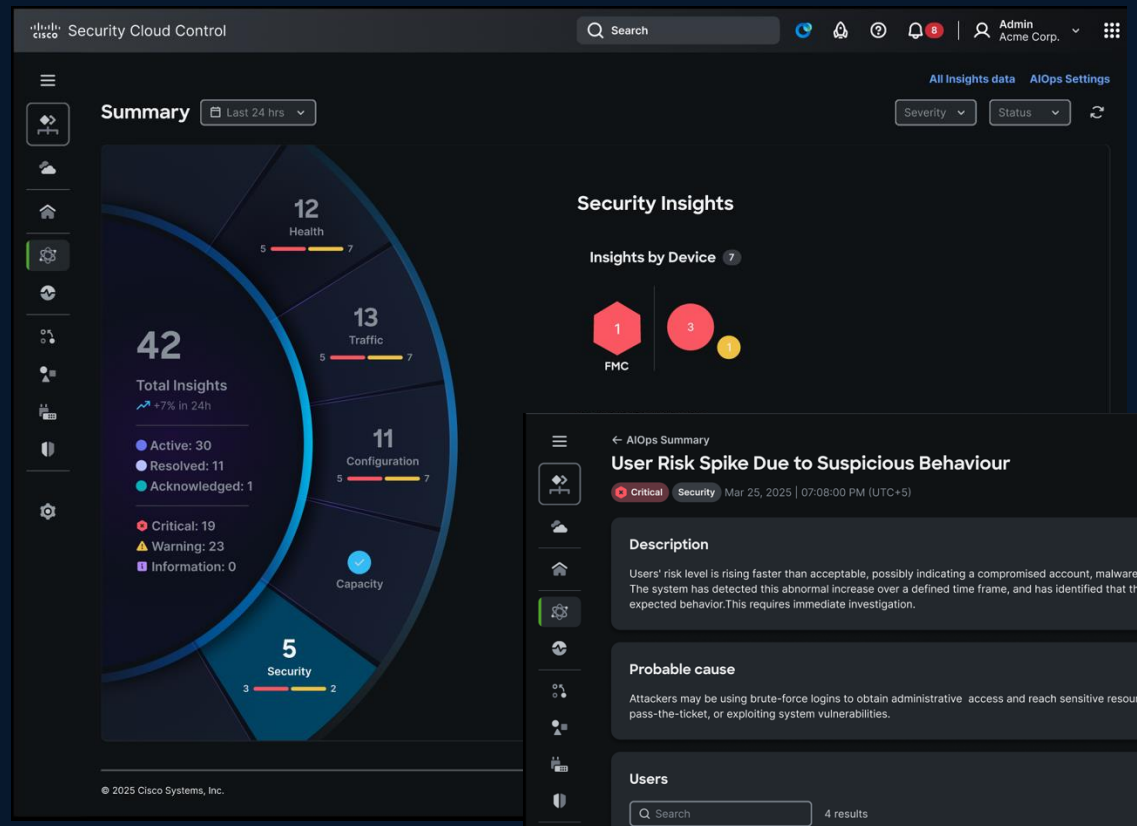
Cisco Identity Intelligence

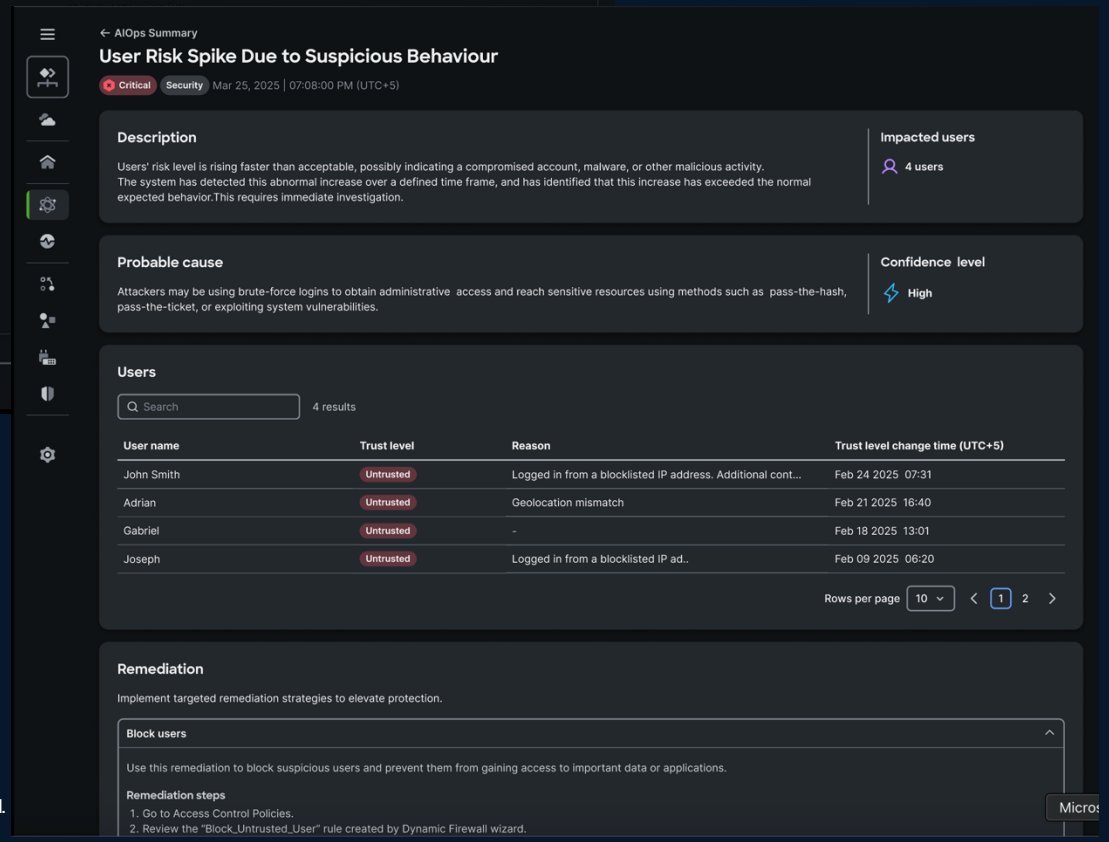
SailPoint
Dragos
CrowdStrike
Salesforce
PingIdentity
Okta
Microsoft
Zscaler
CyberArk
Google
Amazon

Cisco Identity Intelligence

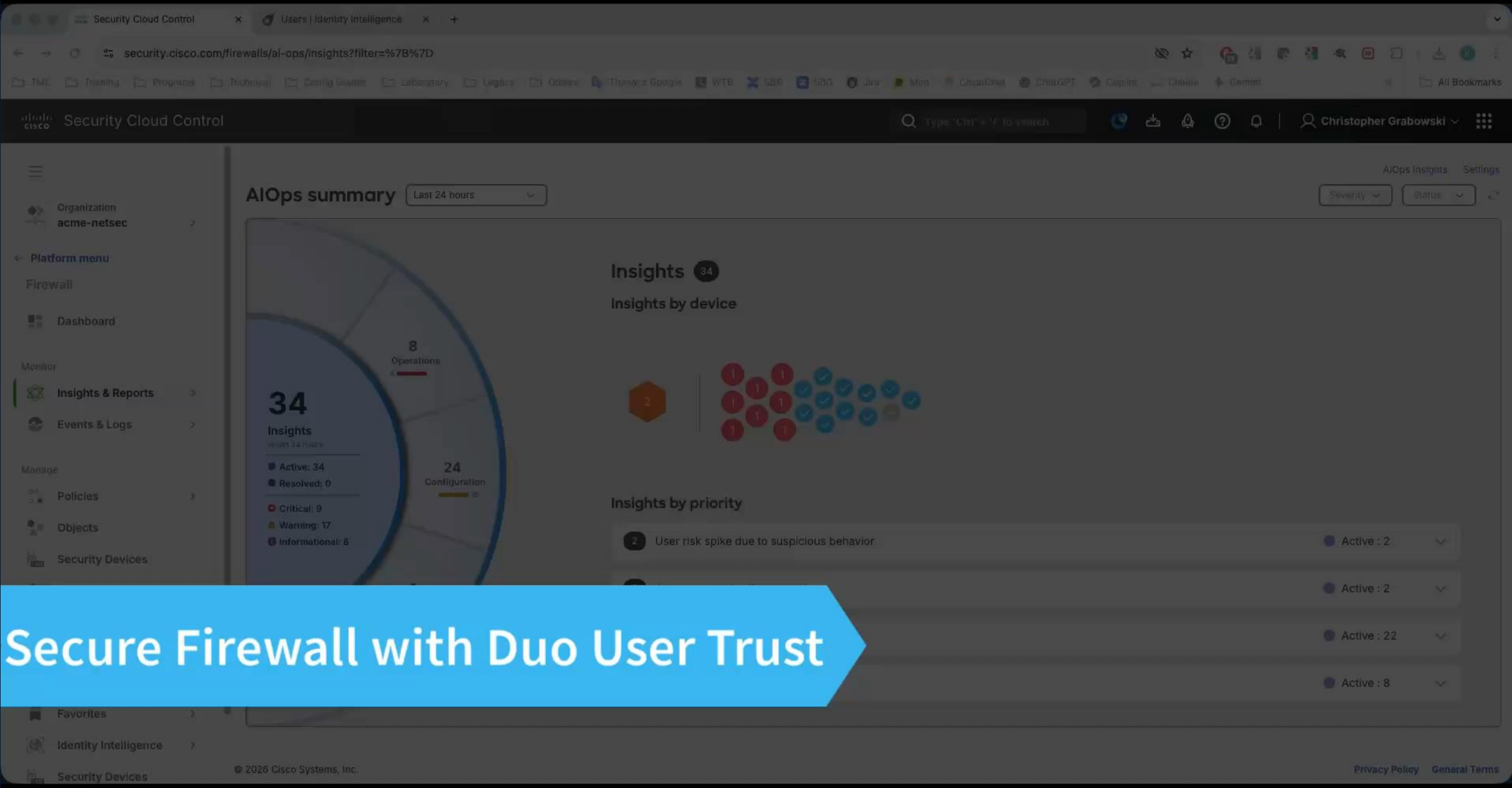


Risky user visibility with Cisco Identity Intelligence Integration





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



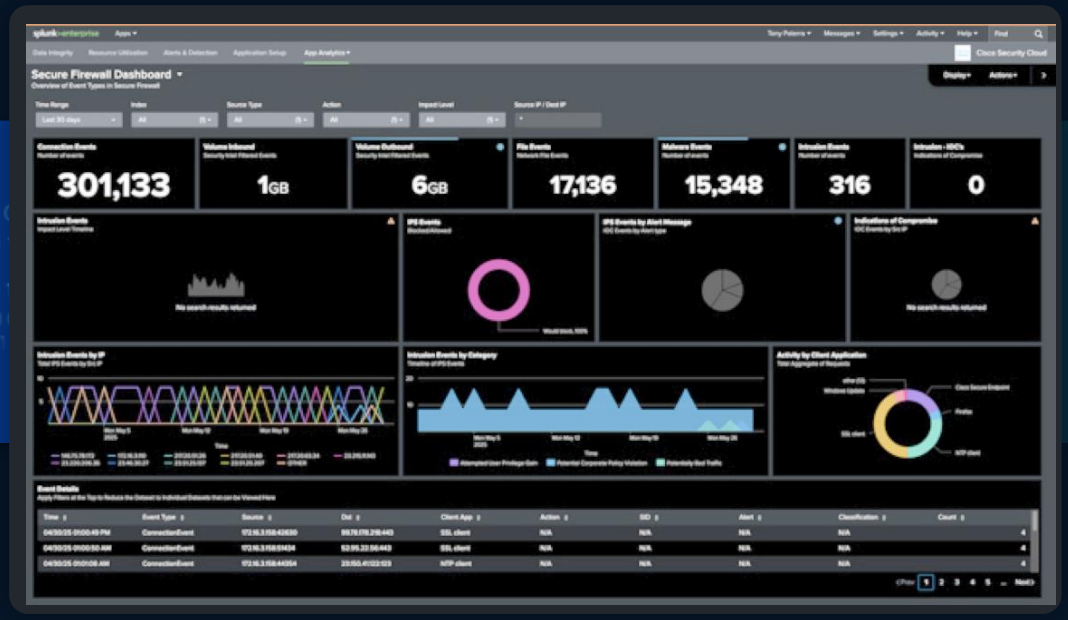
Secure Firewall with Duo User Trust

Hybrid Mesh Firewall (Segmentation as a Platform)

Write policy once, enforce across the mesh

Security Insight, on Us

Free Cisco firewall logs to Splunk*



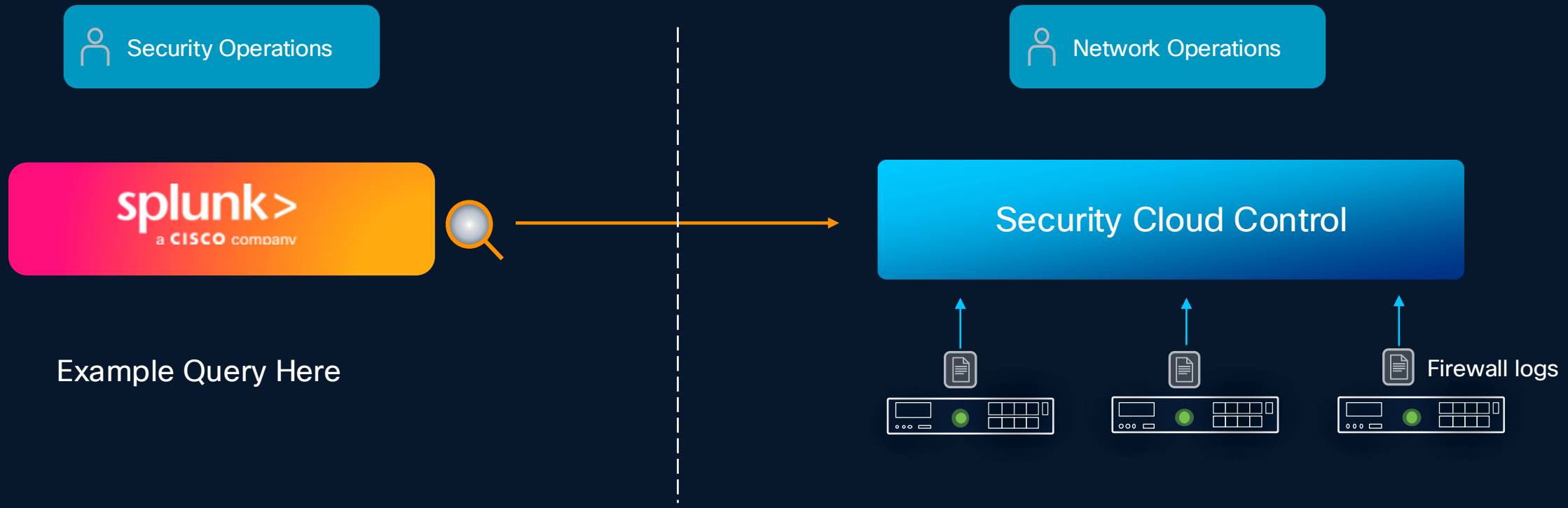
New detections | Automated response

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

Faster threat detection at lower cost

Roadmap

Federated Search with Cisco Secure Firewall and Splunk



Faster Threat Hunting | 60% cost savings | Operational simplicity

Customer and Industry Recognition

NetSecOPEN

iol 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 Vender 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

A Leader

cisco

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


CISCO