Enhancing Operational Efficiency and Improve Security Posture with AIOps for Cisco Firewall

Gayathri Nagarajan
Leader, Product Management, Cloud + Network Security, Cisco Speaker

BRKSEC-2883

Cisco Webex App

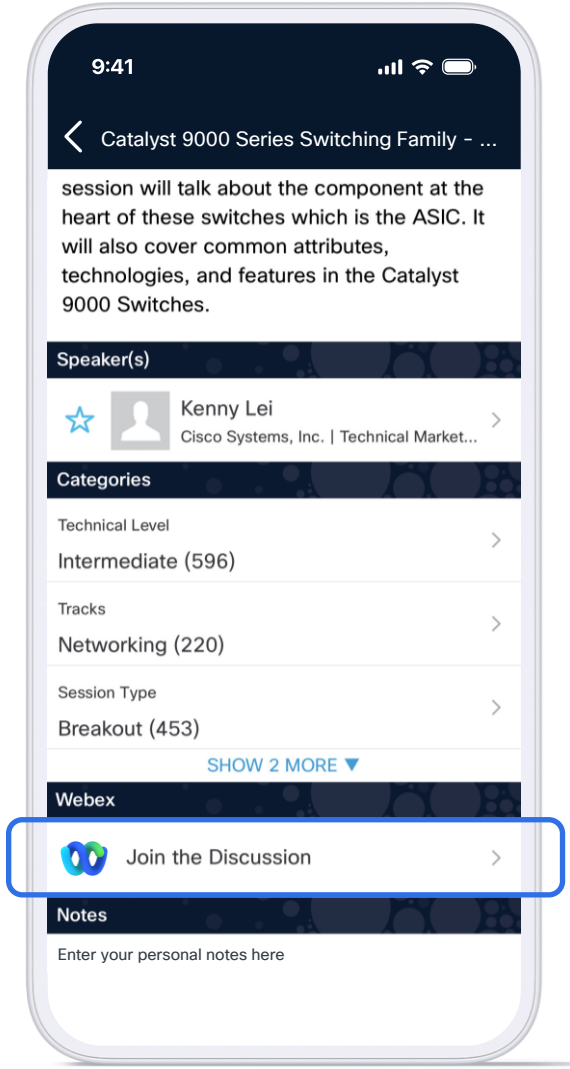
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

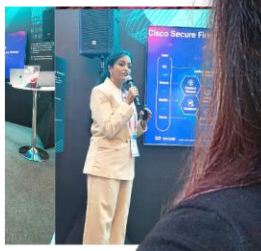
Webex spaces will be moderated by the speaker until 14 November 2025.

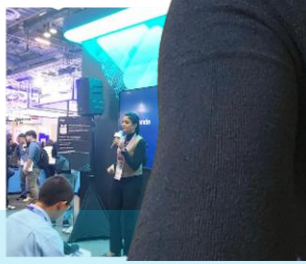


https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSEC-2883**

Your speaker throughout this journey....



Gayathri Nagarajan

Leader, Product Management

Cloud + Network Security Management Portfolio
Email : gayathna@cisco.com

Agenda

01 Navigating complexities of Firewall management

02 Simplifying Operations with AIOps: The How and Why

03 Charting the Future : Vision & Roadmap

04 Real-world Use cases & Outcomes

05 AgenticOps – The next evolution of AIOps

Navigating complexities of Firewall Management

Voice of a firewall admin

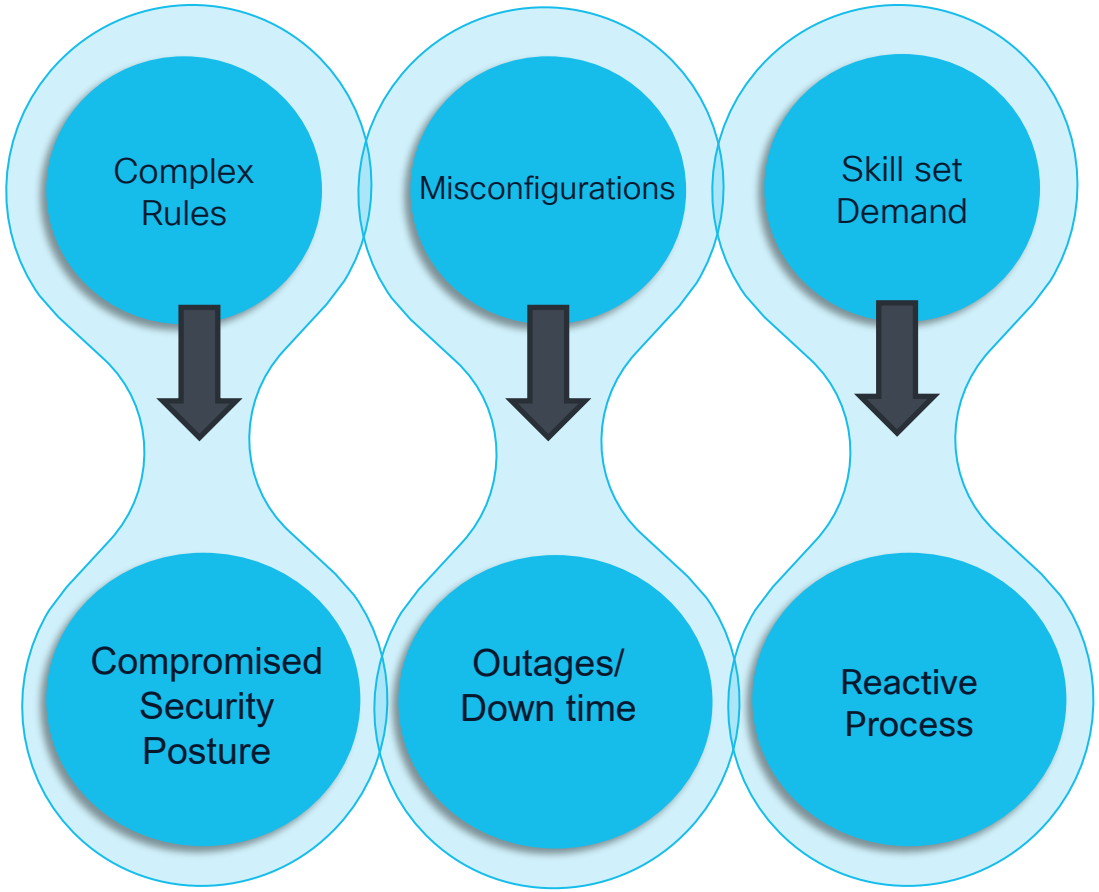
"You know, they say firewalls are essential for security, but with all the tech out there, it's hard to know if you're actually getting your money's worth. Like, is this fancy firewall gizmo really stopping attacks, or are we just throwing money at the problem?"

"Ugh, firewalls are giving me a headache again. You hear about these big breaches in the news, and half the time it's because some poor shmuck left a port open or forgot to tighten down a rule. One little mistake, that's all it takes! Here we are guarding the castle gates, and a single loose brick could let the whole thing crumble."

Managing Firewalls and keeping rules organized.
"Hi everyone, I need your opinion about managing firewalls. I am in a team which manages lots of customer firewalls and doing daily configuration. Customer creates a ticket to our system and they request for a permission and the team does the configuration. But after some time rule numbers increases dramatically and becomes really hard to manage. I'm in this team my role is not about doing daily configuration mostly architecture side. My manager asked me figure out a way to keep firewall rules organized and keeping the numbers low. If only 1 person does all configuration it will be easy like guiding him a few times but 8 people in that L1 team. I hope, i was clear. Looking for some help, thanks :)"

"Hey all, I've been tasked with finding unused, overlapping and outdated firewall rules. I'm 4 days new to this job and there are 900 rules on this main FW. Any ideas on how I can quickly find these rules?"

Complexity breeds security blind spots



The average cost of network downtime is

$300,000

per hour

Create Report

Summary Dashboard (switch dashboard)

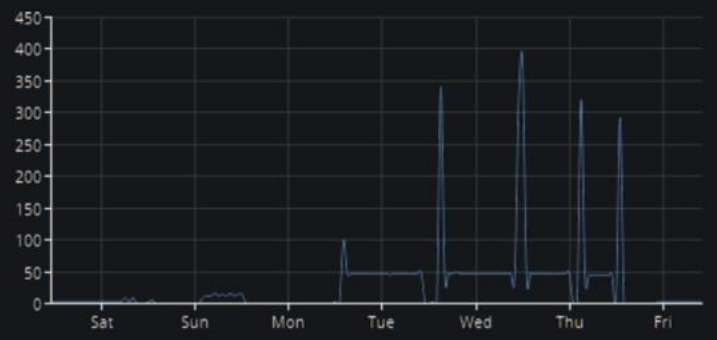
Provides a summary of activity on the appliance

Network | Threats | Intrusion Events | Status | Geolocation | QoS | Zero Trust | +

Show the Last 1 week

Add Widgets

Unique Applications over Time



Last updated 1 hour 53 minutes ago

Traffic by Application Risk

Risk	Total Bytes (KB)
Medium	1,798,478,979.1
Very Low	1,256,659,970.74
Low	161,189,216.21
Very High	5,538,746.92
High	344,415.75

Last updated 1 hour 53 minutes ago

Traffic by Business Relevance

Top Web Applications Seen

Application	Total Bytes (KB)
Microsoft Update	117,636,758.2
Microsoft Teams	114,939,281.95
Office 365	94,043,347.24
Microsoft Azure	57,776,054.61
Exchange Online	33,183,744.18
Sharepoint Online	27,668,340.53
FTP Active	6,321,509
Azure cloud portal	3,511,493.68
generic audio/video	3,004,062.8
BitTorrent	2,808,941.32
Office Mobile	2,448,127.88
OneDrive	1,865,205.63
Windows Live	1,800,741.51
Azure Authentication Service	1,335,639.25
Youdao Dictionary	819,434.97

Last updated 1 hour 52 minutes ago

Top Server Applications Seen

Risky Applications with Low Business Relevance

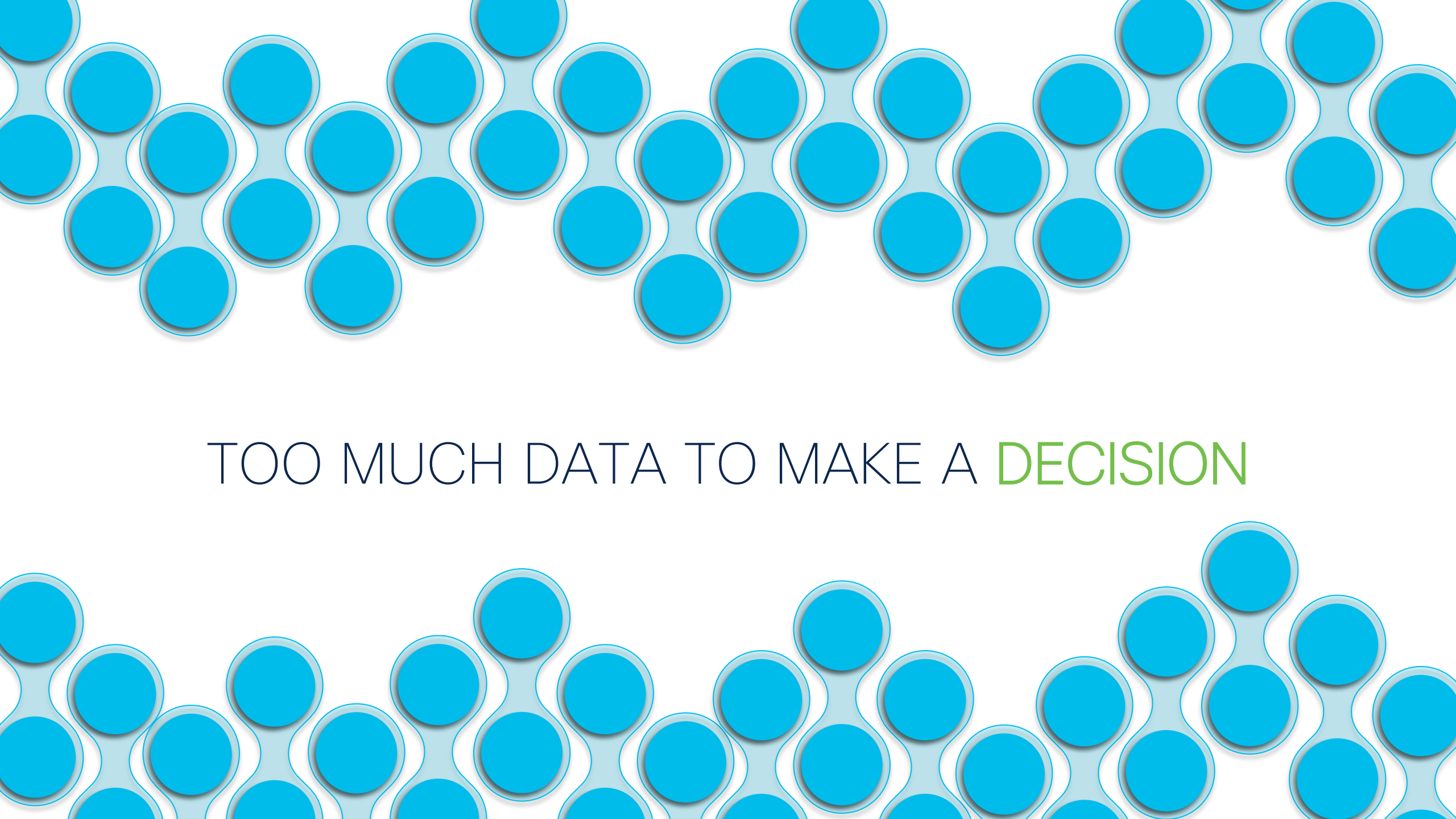
Application	Total Connections
eDonkey	148,771

Top Client Applications Seen

Application	Total Bytes (KB)
Internet Explorer	497,874,567.91
SSL client	480,675,423.55
BITS	59,429,748.62
DCE/RPC	58,616,506.69
Firefox	45,106,731.28
Chrome	39,681,638.02
BitTorrent	2,808,941.32
eDonkey	2,703,496
OneDrive	1,865,205.63
Windows Live	1,800,741.51
Microsoft Excel	898,705.38
Youdao Dictionary	819,434.97
RTP	611,582.94
Facebook	204,235.16
Discord	27,037.05

Last updated 1 hour 54 minutes ago

Top Operating Systems Seen


TOO MUCH DATA TO MAKE A DECISION

AIOps

for Firewall

Simplifying Operations and Enhancing Security

Simplify Operations with proactive insights & guided remediations

Before AIOps

Troubleshooting challenges

20+ clicks to navigate

2 hours to 3 weeks to detect issues

Expert-level knowledge for effective remediation

Significant Operational overhead

AIOps Impact

AIOps transformation for customers

Single-click issue identification

Near-zero Mean Time to Detect (MTTD)

Dramatically reduced Mean Time to Remediate (MTTR)

AI-guided remediation workflows

AIOps

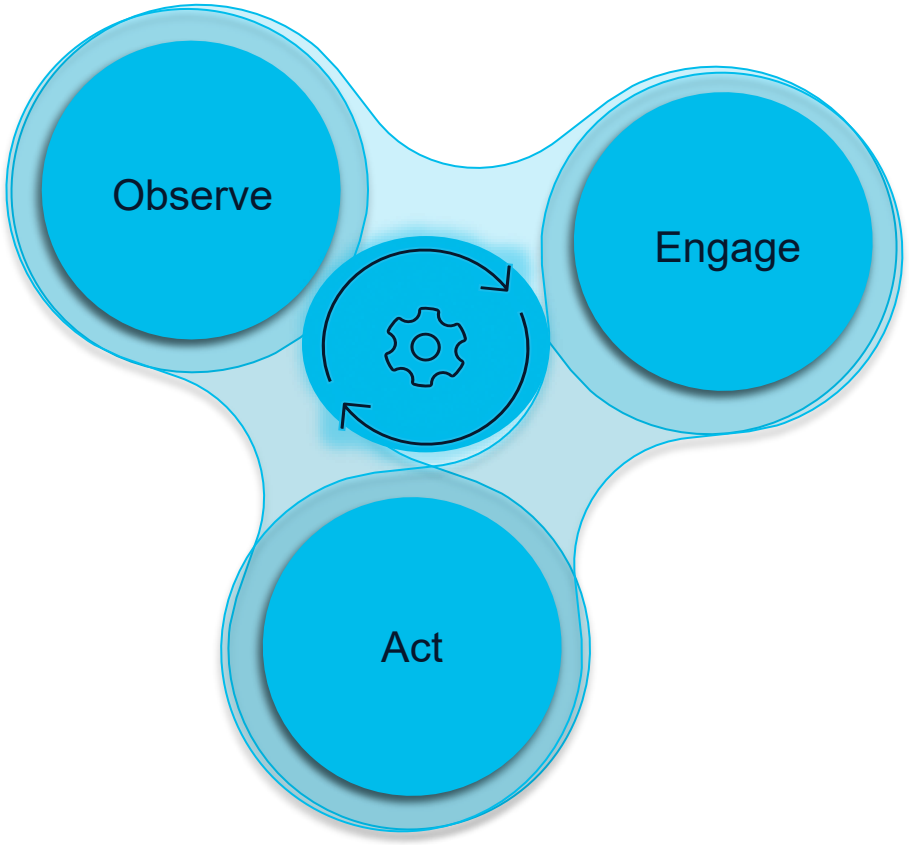
for Firewall

Simplifying Operations and Enhancing Security

- Predictive Insights
- Improved Operational Efficiency
- AI-guided remediations for Enhanced Decision Making

Simplifying Operations with AIOps: The How and Why

Our Approach



1 **Data Selection**

Locating & Presenting the most pertinent information

2 **Pattern Discovery**

Correlating and finding relationship between events across entities

3 **Inference**

Identifying root cause and recurring issues across environments

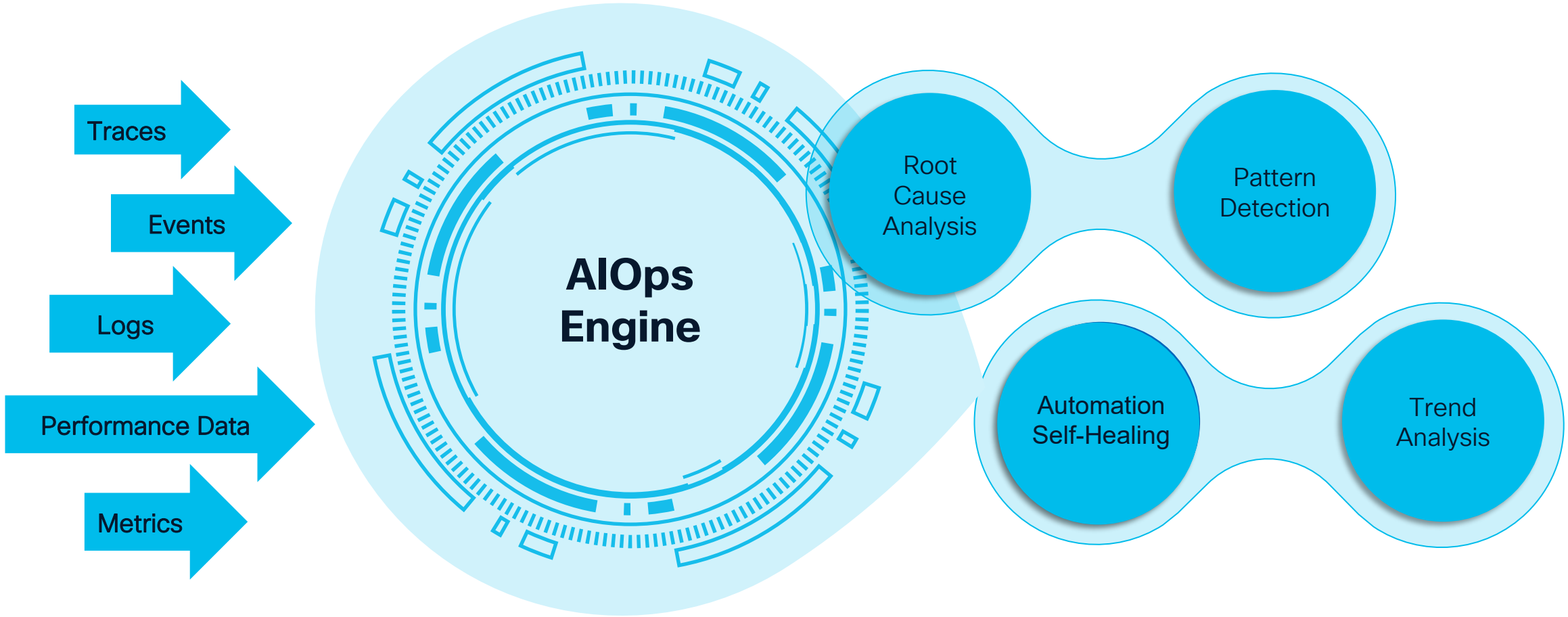
4 **Collaboration**

Notification and collaboration of appropriate operators and teams

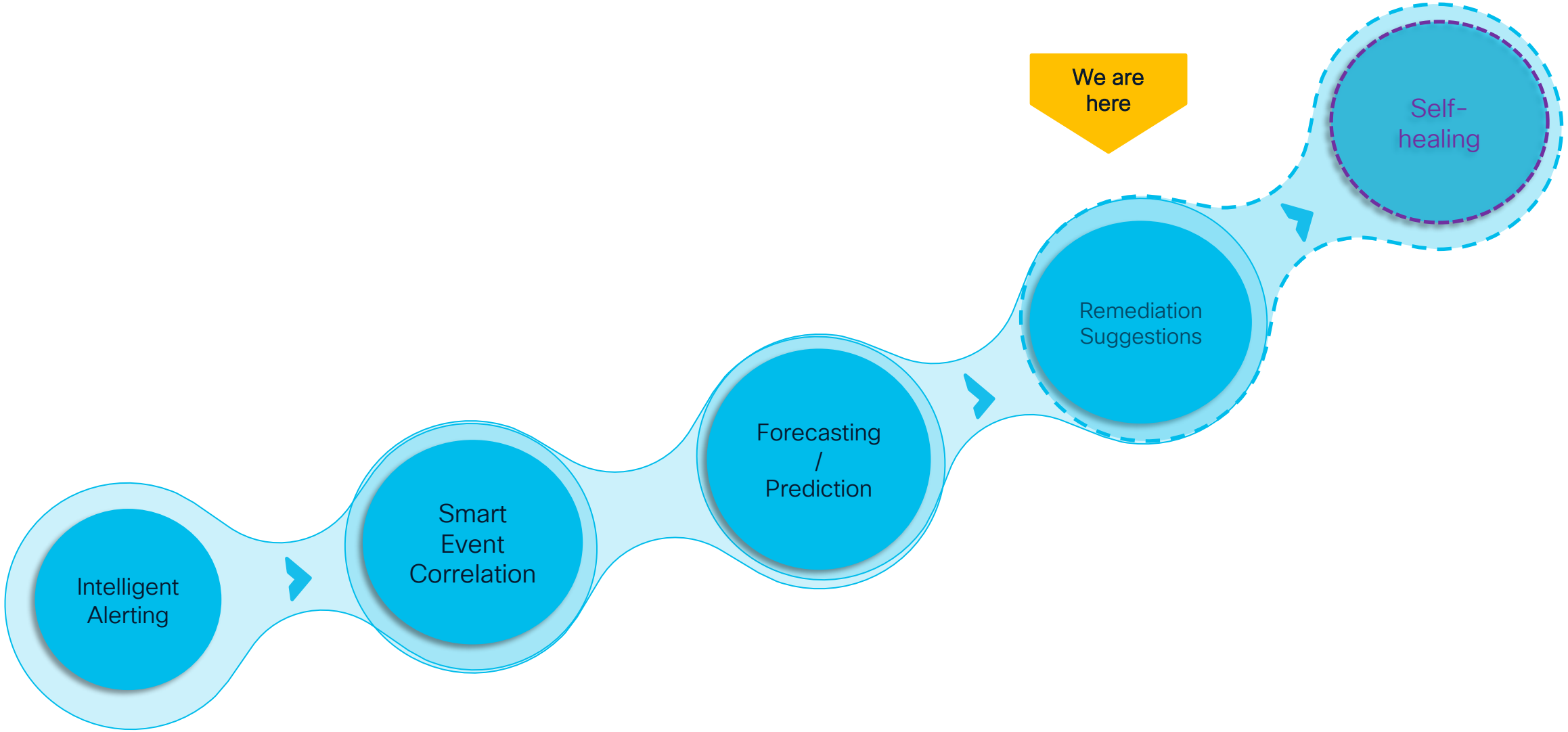
5 **Automation**

Automating remediation

Our Approach

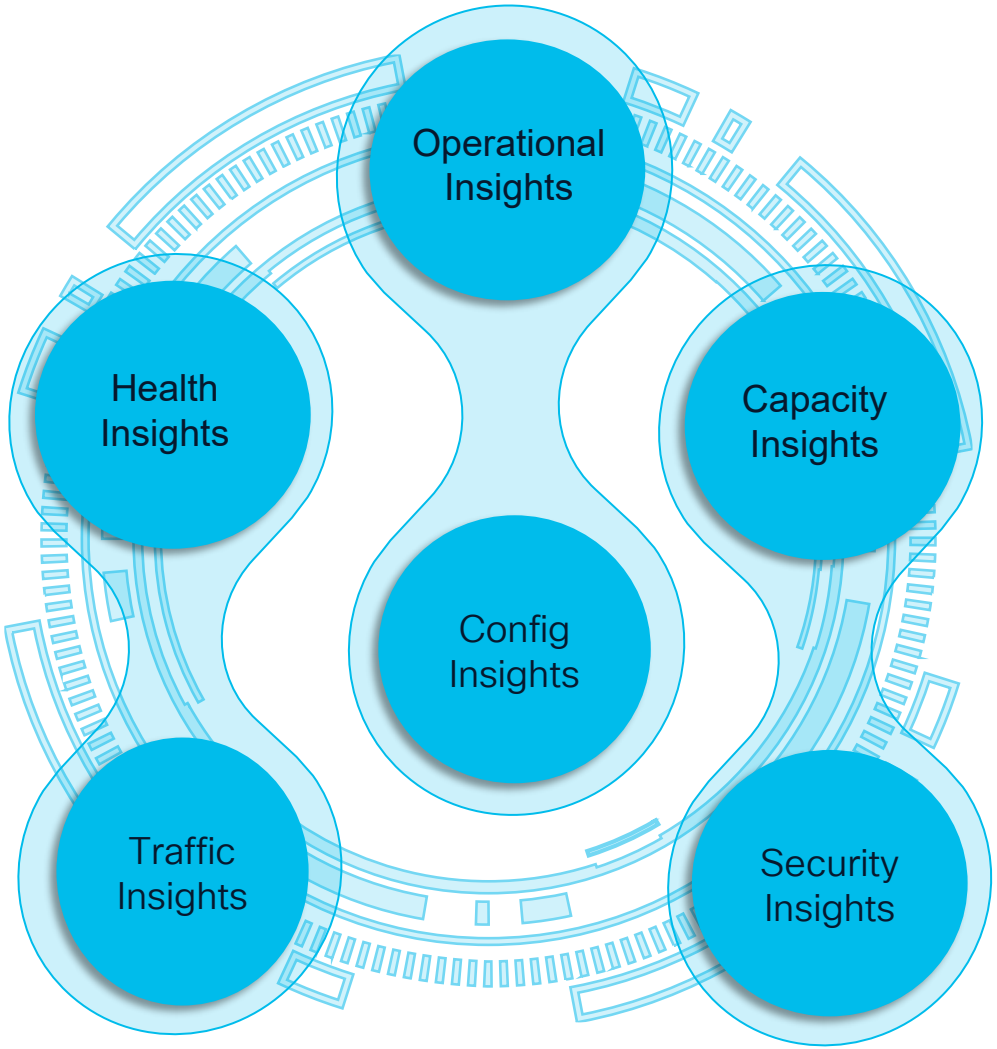


AIOps Use cases: A maturity curve



Charting the Future: Vision & Roadmap

AIOps Vision



Simplify Operations and Enhance Security Posture for Cisco Firewalls

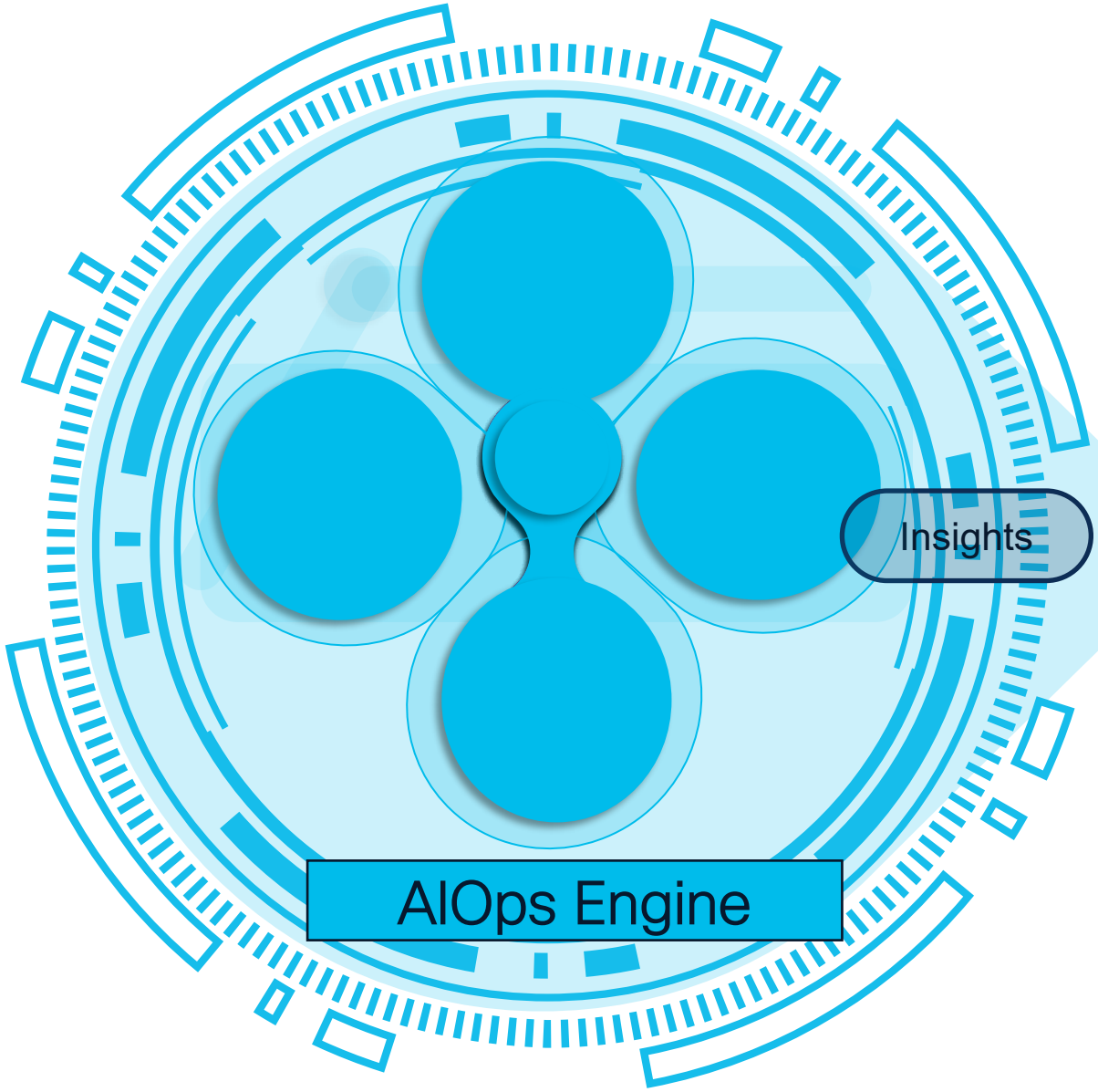
- Prevent misconfigurations and enhance security posture with best practice recommendations
- Provide Root cause analysis and forecast/predict patterns using predictive analytics and Dynamic Baseline
- Receive Policy Optimization suggestions and remediations tailored to your environment for easy Policy Management & optimal firewall performance
- Provide visibility into user risks and automated rules to step up authentication or block them based on risks.
- Application Insights to provide Internet and Application related outage details.

25TB -Troubleshoot

1 Million - Firewalls

52 Billion - Health Metrics

200 Billion - Threat Events



From investigating and correlating Millions of Metrics to few countable actionable Insights

Insights

Security Cloud Control

AIOps Insights

AIOps Engine

Anomaly Detection	Predictive Analytics	Curated Alerts	Policy Health & Compliance	Hardware Failure Prediction	Best Practice Recommendations	=====	Analytics Module N
Health Metrics	Health Metrics	Health Metrics	Policies & Configs	Telemetry	Lightweight TS		Metrics ...

Secure Firewall (Appliance)

Secure Firewall (Virtual)

Real-World Use cases & outcomes

Policy & Configuration Insights

- Policy Analyzer & Optimizer
- Port to App-Id based conversion of rules
- Inline Optimizer
- Best Practice Recommendation
- Feature Adoption
- NAT Policy Analyzer

Operational Insights

- Software Upgrade Planner
- Renewal Upgrade Planner
- Internet Insights

Security Insights

- Visibility into user risks

Traffic & Capacity Insights

- Elephant Flow Detection
- VPN Monitoring & Capacity Planner
- Capacity & Trend Analyzer

Inline Policy Analyser & Optimiser

The Problem

Customers often don’t fully use their security tools or use it ineffectively, leading to weak security practices and misconfigurations that raise the risk of a breach.

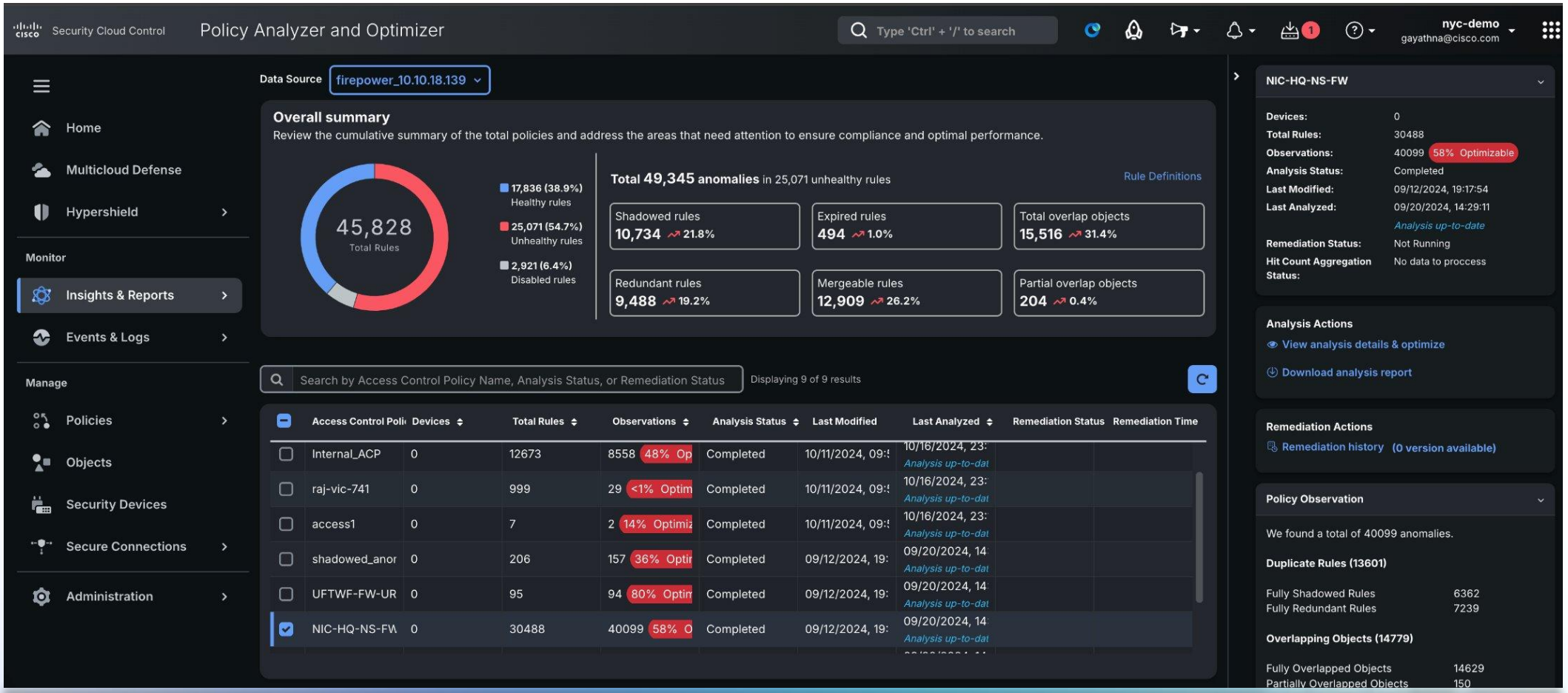
The Solution

Inline Policy analysis and optimization addresses issues like overlapping, hidden, or overly broad rules. For instance, if a customer has a rule that permits broad group of traffic above more specific rules that overlaps the same traffic, we will point out these malpractices and help reduce unnecessary rules.

- Optimize Policy Hygiene
- Detects Potential Security Gaps
- Reduction in Change Management Time

Policy Analyzer & Optimizer

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



Policy Analyzer & Optimizer

81%

Config anomalies detected in a real customer deployment

Monitor
Insights & Reports
Events & Logs
Manage
Policies
Objects
Firewall Devices
Secure Connections
Integrations
Troubleshooting
Administration

Security Cloud Control Integration

Integrate the management center with the Security Cloud Control to use a suite of cloud services. Use your Security Cloud Control Sign On account to authorize management center to register with Security Cloud Control. If you don't have a Security Cloud Control Sign On account, **create an account** and integrate management center with Security Cloud Control. If you were using Security Cloud Control services prior to version 7.6, you can continue to send events to Security Cloud Control. However, to use the new Security Cloud Control features, you must enable Security Cloud Control. **Learn more**

Integration

Security Cloud Control	Current Cloud Region	Tenant	Cloud Onboarding Status
Disabled	staging-sse.cisco.com (stagi...	None	Not Available

Learn more

Enable Security Cloud Control

Settings

To send **Events** to the Cisco cloud or to use the **Security Cloud Control Support** features, either register the management center with Smart License (System > Smart Licenses) or enable Security Cloud Control.

Event Configuration

- [x] Send events to the cloud
  - [ ] Intrusion events
  - [ ] File and malware events
  - [x] Connection events
    - ( ) Security
    - (•) All

View your **Events in Security Cloud Control**

Cisco AI Assistant for Security

Powered by generative AI and natural language processing, Cisco AI Assistant for Security enables you to create access control rules, query documentation and reference materials when required, and

Security Cloud Control Support

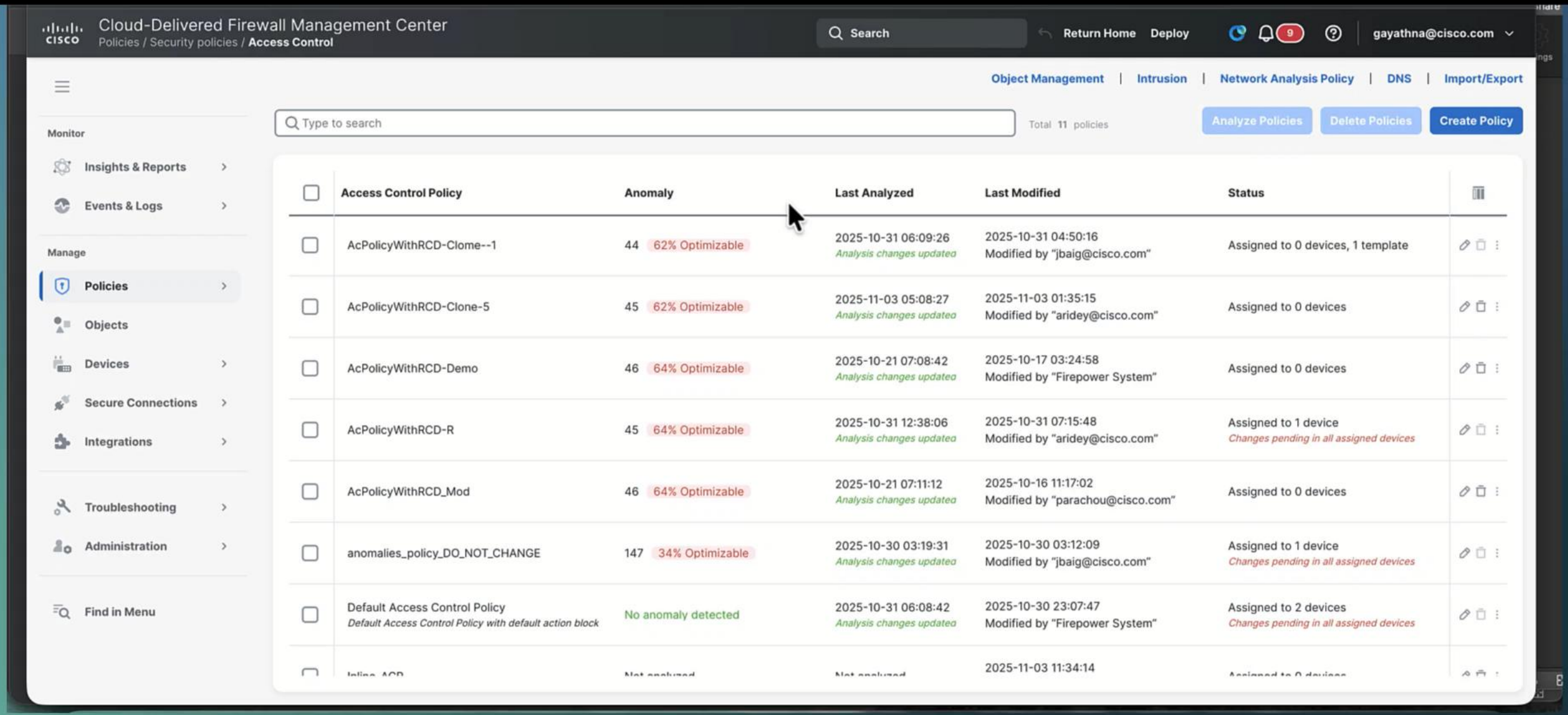
Cisco cloud support services provide an enhanced support experience and maximize the value of the Cisco products. The management center establishes and maintains a secure connection to Cisco cloud to participate in additional service offerings from Cisco.

- [ ] Enable Cisco Success Network
- [ ] Enable Cisco Support Diagnostics

Cisco XDR Automation

Enable Cisco XDR Automation to allow a Cisco XDR user to build automated workflows that interact with various resources in the Secure Firewall Management Center. **Learn more**

Save


Cloud-Delivered Firewall Management Center
Policies / Security policies / Access Control
Search
Return Home
Deploy
9
gayathna@cisco.com
Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export
Monitor
Insights & Reports
Events & Logs
Manage
Policies
Objects
Devices
Secure Connections
Integrations
Troubleshooting
Administration
Find in Menu
Type to search
Total 11 policies
Analyze Policies
Delete Policies
Create Policy
Access Control Policy
Anomaly
Last Analyzed
Last Modified
Status
AcPolicyWithRCD-Clome--1
44 62% Optimizable
2025-10-31 06:09:26
Analysis changes updated
2025-10-31 04:50:16
Modified by "jbaig@cisco.com"
Assigned to 0 devices, 1 template
AcPolicyWithRCD-Clone-5
45 62% Optimizable
2025-11-03 05:08:27
Analysis changes updated
2025-11-03 01:35:15
Modified by "aridey@cisco.com"
Assigned to 0 devices
AcPolicyWithRCD-Demo
46 64% Optimizable
2025-10-21 07:08:42
Analysis changes updated
2025-10-17 03:24:58
Modified by "Firepower System"
Assigned to 0 devices
AcPolicyWithRCD-R
45 64% Optimizable
2025-10-31 12:38:06
Analysis changes updated
2025-10-31 07:15:48
Modified by "aridey@cisco.com"
Assigned to 1 device
Changes pending in all assigned devices
AcPolicyWithRCD_Mod
46 64% Optimizable
2025-10-21 07:11:12
Analysis changes updated
2025-10-16 11:17:02
Modified by "parachou@cisco.com"
Assigned to 0 devices
anomalies_policy_DO_NOT_CHANGE
147 34% Optimizable
2025-10-30 03:19:31
Analysis changes updated
2025-10-30 03:12:09
Modified by "jbaig@cisco.com"
Assigned to 1 device
Changes pending in all assigned devices
Default Access Control Policy
Default Access Control Policy with default action block
No anomaly detected
2025-10-31 06:08:42
Analysis changes updated
2025-10-30 23:07:47
Modified by "Firepower System"
Assigned to 2 devices
Changes pending in all assigned devices
2025-11-03 11:34:14

Adaptive Policy Insights
Port based Rules to App-ID based Rules

The Problem

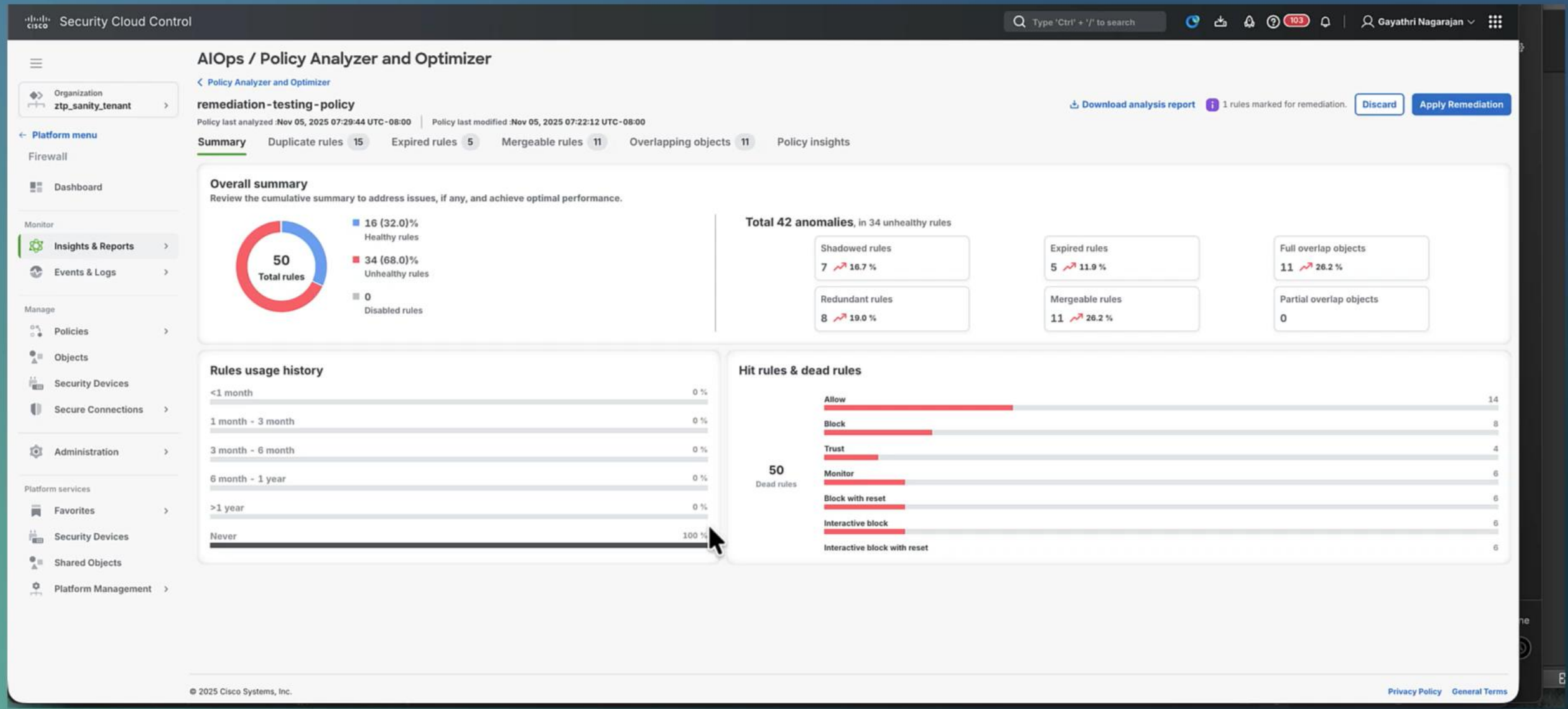
As customers transition from legacy firewalls to next-gen firewalls (NGFW), many legacy port-based rules are carried over without review. In addition, several port-based rules are often retained for convenience but they can significantly weaken your security posture.

The Solution

Leverage **application-based policy analysis and optimization tools** to identify and replace outdated port-based rules.

- Detect legacy and unused rules
- Suggest application-aware replacements
- Prioritize high-risk rules for cleanup

Reduced attack surface | Application aware policies | Improved security posture


Security Cloud Control
Type 'Ctrl' + '/' to search
103
Gayathri Nagarajan
AIOps / Policy Analyzer and Optimizer
Policy Analyzer and Optimizer
Organization
ztp_sanity_tenant
remediation-testing-policy
Policy last analyzed :Nov 05, 2025 07:29:44 UTC-08:00
Policy last modified :Nov 05, 2025 07:22:12 UTC-08:00
Download analysis report
1 rules marked for remediation.
Discard
Apply Remediation
Platform menu
Firewall
Dashboard
Monitor
Insights & Reports
Events & Logs
Manage
Policies
Objects
Security Devices
Secure Connections
Administration
Platform services
Favorites
Security Devices
Shared Objects
Platform Management
Summary
Duplicate rules 15
Expired rules 5
Mergeable rules 11
Overlapping objects 11
Policy insights
Overall summary
Review the cumulative summary to address issues, if any, and achieve optimal performance.
50
Total rules
16 (32.0)%
Healthy rules
34 (68.0)%
Unhealthy rules
0
Disabled rules
Total 42 anomalies, in 34 unhealthy rules
Shadowed rules
7 16.7 %
Expired rules
5 11.9 %
Full overlap objects
11 26.2 %
Redundant rules
8 19.0 %
Mergeable rules
11 26.2 %
Partial overlap objects
0
Rules usage history
<1 month 0 %
1 month - 3 month 0 %
3 month - 6 month 0 %
6 month - 1 year 0 %
>1 year 0 %
Never 100 %
Hit rules & dead rules
50
Dead rules
Allow 14
Block 8
Trust 4
Monitor 6
Block with reset 6
Interactive block 6
Interactive block with reset 6
© 2025 Cisco Systems, Inc.
Privacy Policy
General Terms

Maximize ROI with Feature Adoption

The Problem

Users often find themselves buried in day-to-day operation tasks. They have limited time to learn new features that can help to improve security and productivity. Licenses bought were also often time not fully utilized. Currently, this information is not surfaced. Users may not be aware of the untapped values.

The Solution

Aside from offering best practice recommendations, helping our users to identify and understand underutilized features allow us to bring awareness on how our customers can get the most values out of their security spending.

Dashboard
Multicloud Defense
Monitor
Insights & Reports
Events & Logs
Manage
Policies
Objects
Security Devices
Secure Connections
Administration

← AIOps Insights

Feature Adoption

Data sources: Cloud-Delivered Firewall Management Center

Last updated: 2 days ago Refresh page

Summary

37%
Adoption rate

Feature overview

8	5	0	3
Total features	Not adopted	Partially adopted	Adopted

Each feature is represented as a percentage, indicating the total number of products that have or have not adopted that feature.

Feature recommendations

Encrypted Visibility Engine Learn more

Encrypted Visibility Engine for Firewall Threat Defense devices

Cisco Secure Dynamic Attributes Connector Learn more

Dynamic Attributes Connector for Firewall Management Center

Licenses and associated features

Each of the following features is associated with a license. Enable or disable a feature to improve your adoption score without impacting feature functionality.

Essentials 66%

- Application Segmentation via ZTNA
- AI Assistant
- Policy Analyzer and Optimizer

IPS 0%

- Dismissed Features
- Intrusion Detection and Prevention
- Encrypted Visibility Engine
- IPS Event Logging
- Cisco Umbrella DNS Policy

Remote Access VPN Only 0%

Change management

Enables formal processes for configuration changes in Management Center, including audit tracking and official approval before changes are deployed.

0%
Adoption rate

Feature adoption rate at each enforcement point

Adoption:0%
Cloud-Delivered Firewall Management Center

1	1	0
Total	Not adopted	Adopted

Devices	Adoption status
Cloud-delivered FMC	Not adopted

Rows per page 10 1

Steps to improve your feature adoption rate efficiency:

Best practice recommendations

The Problem

Organizations struggle with misconfigurations, evolving threat landscape, and resource constraints. Customers follow best practices to improve their security postures. However, today, these knowledge is not integrated into the product. Customers have to manually reference and keep track of their policy hygiene and making sure that their configurations are in aligning with best practices to defend against threats.

The Solution

We utilize machine learning algorithms to identify and rectify errors based on industry-defined and Cisco best practices. For instance, should a user inadvertently permit access to high-risk URL categories such as Phishing and Hacking, our system will detect and bring attention to this oversight, proposing corrective actions. These insights are also conveniently displayed on the integrated dashboard for easy access.

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

← AIOps Insights

Best Practices and Recommendations

Assessment summary | Total: 2 device reports

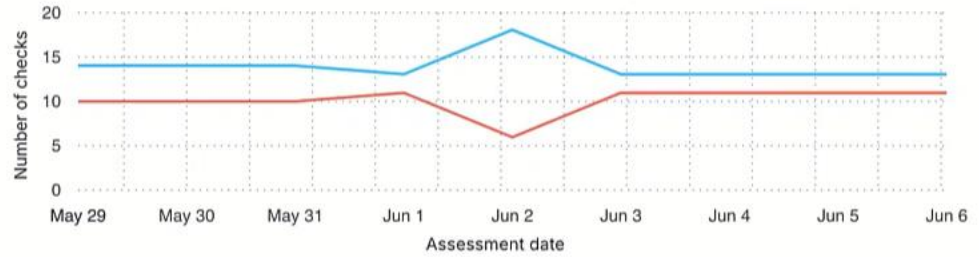
Checks summary

11/24

Checks requiring review

We recommend that you assess the checks that require review and set right any deviations from Firewall best practices. This is necessary for optimal performance of your device.

Best practices assessment trend



Device reports

Search | Device status | Review categories | Assessment status | 2 device reports

Device name	Device status	Checks requiring review	Review categories	Assessment status
FTD-7.6	Warning	11 50% improvement potential	Improve access control, Manage access and control pane +1	Updated 4 days ago
FMC	Passed	0	-	Updated 18 hours ago

Elephant Flow detection and Remediation

The Problem

Large long lived flows called Elephant flows can overload the firewall device leading to traffic drops, compromised security posture, and sub-optimal firewall performance

The Solution

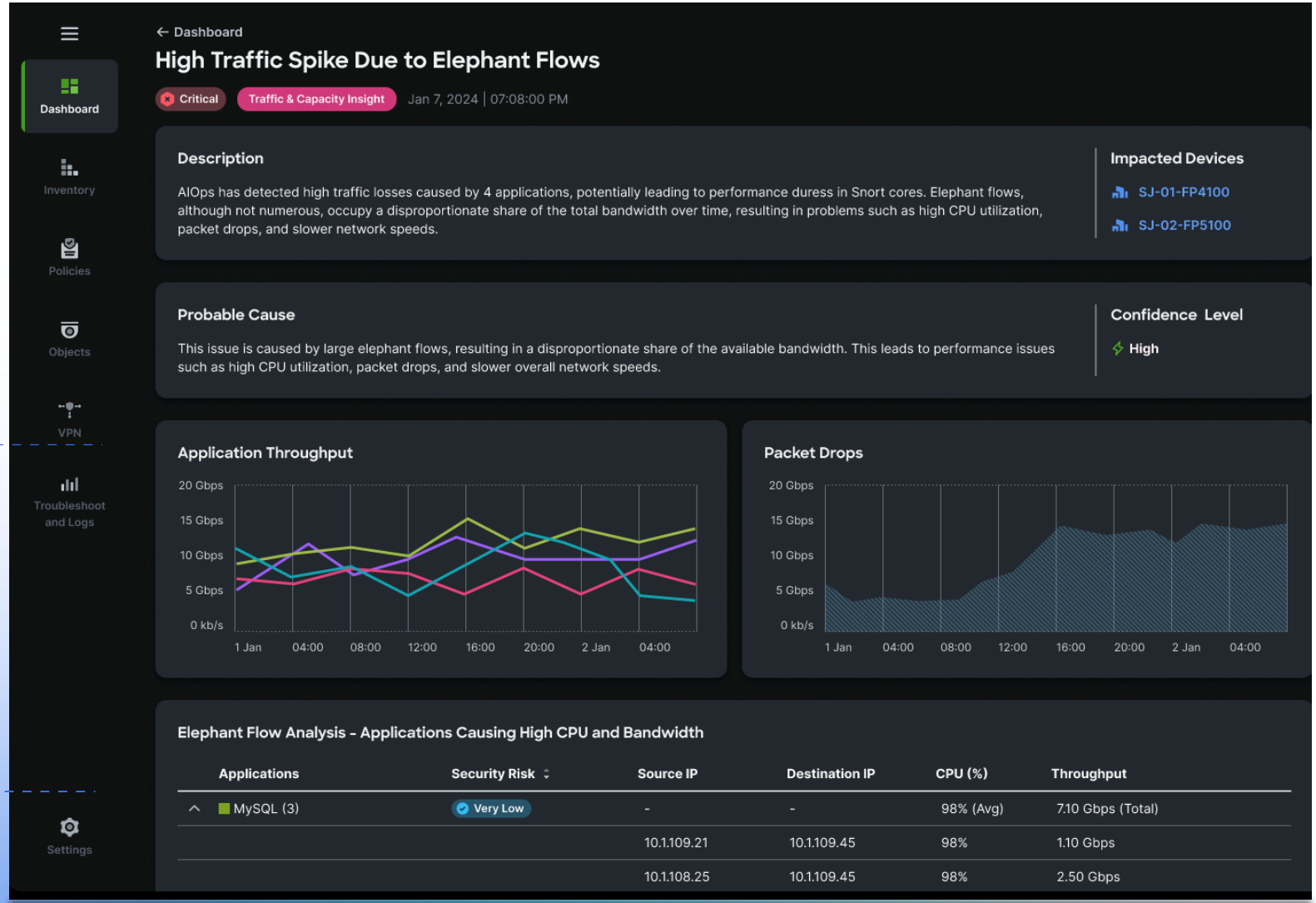
When a Firewall is managing a large network flow, we can forecast how large long-lived flows may impact CPU and memory. With AIOps insight, we can suggest to bypass low risky applications and throttle high risky apps and optimize the flows.

- Faster Troubleshooting
- Reduced Mean Time to Resolution
- Risk-based prioritization

Elephant Flow detection and remediation

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

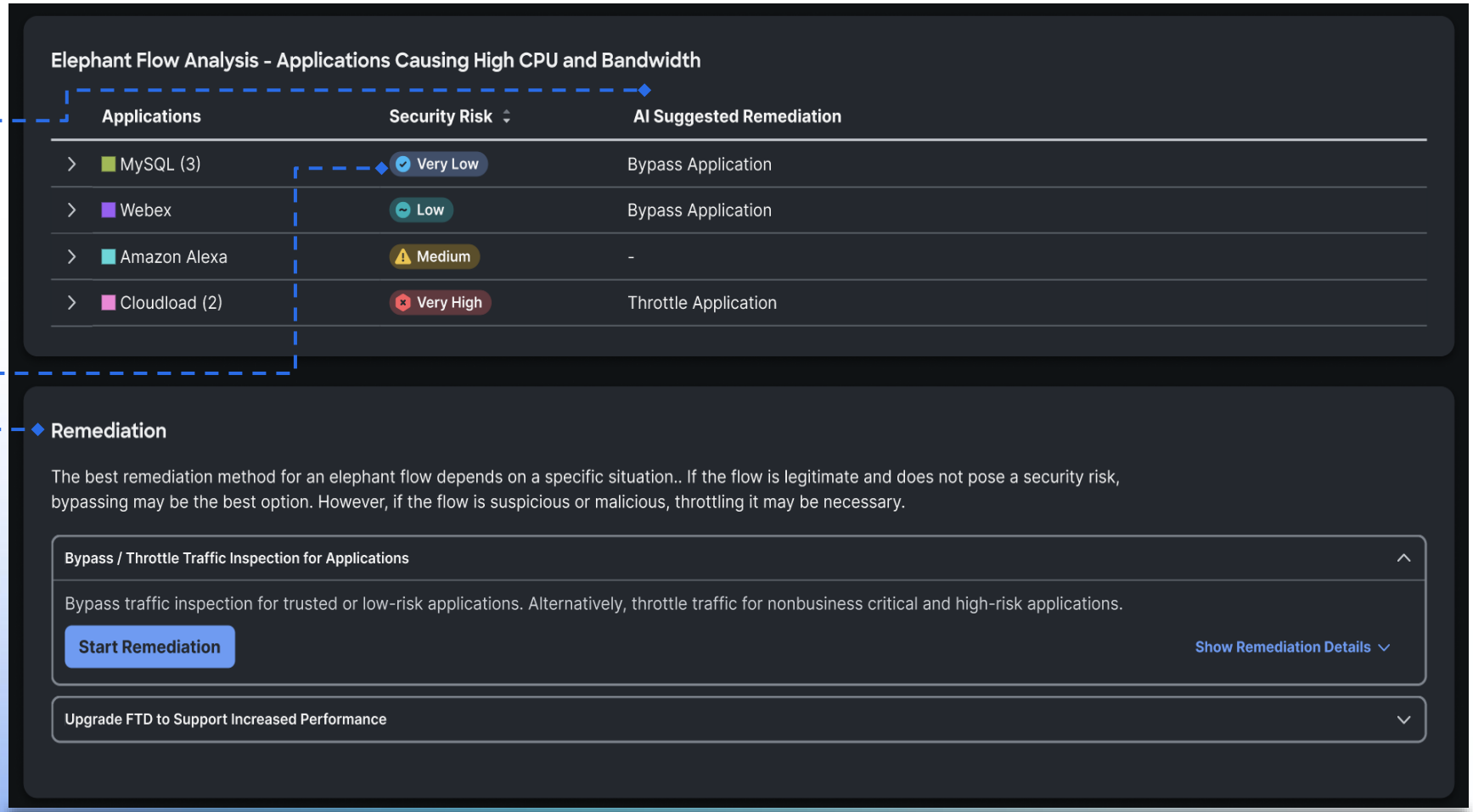


Elephant Flow detection and remediation

AI suggested remediations to bypass or throttle traffic

List of applications where elephant flows are observed contributing to traffic spike & CPU spike

Automated remediation suggestion workflow



VPN Monitoring and Capacity Planning

The Problem

Imbalance in VPN headend loads such as multiple users connect to a single VPN headend, while others remain underutilized or sessions that stay open for extended periods without actual usage can cause dropped connections and compromised performance.

The Solution

Using predictive analytics, we can identify these disparities and offer actionable solutions.

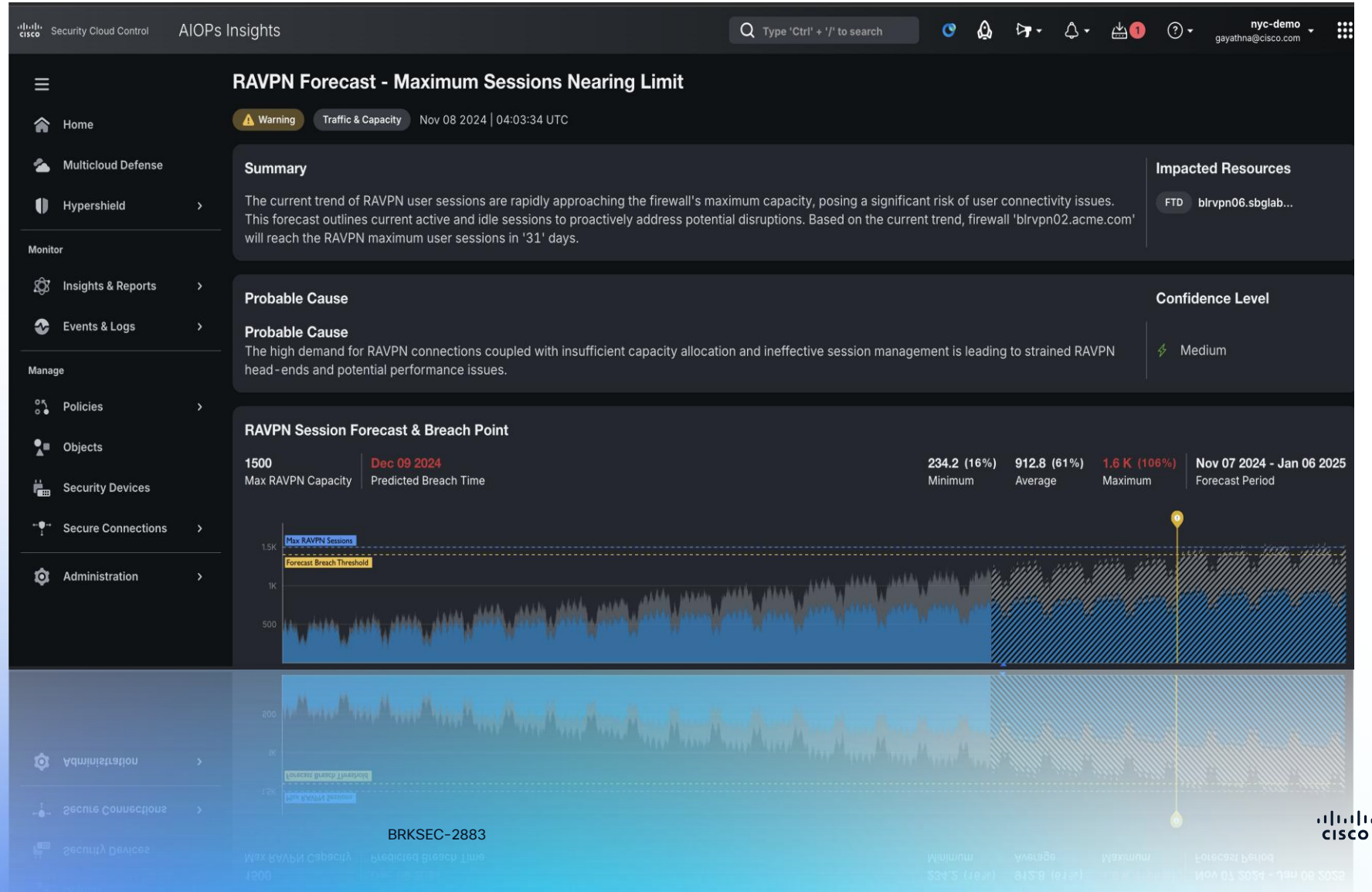
- Faster troubleshooting
- Reduced Mean Time to Resolution
- Risk-based prioritization

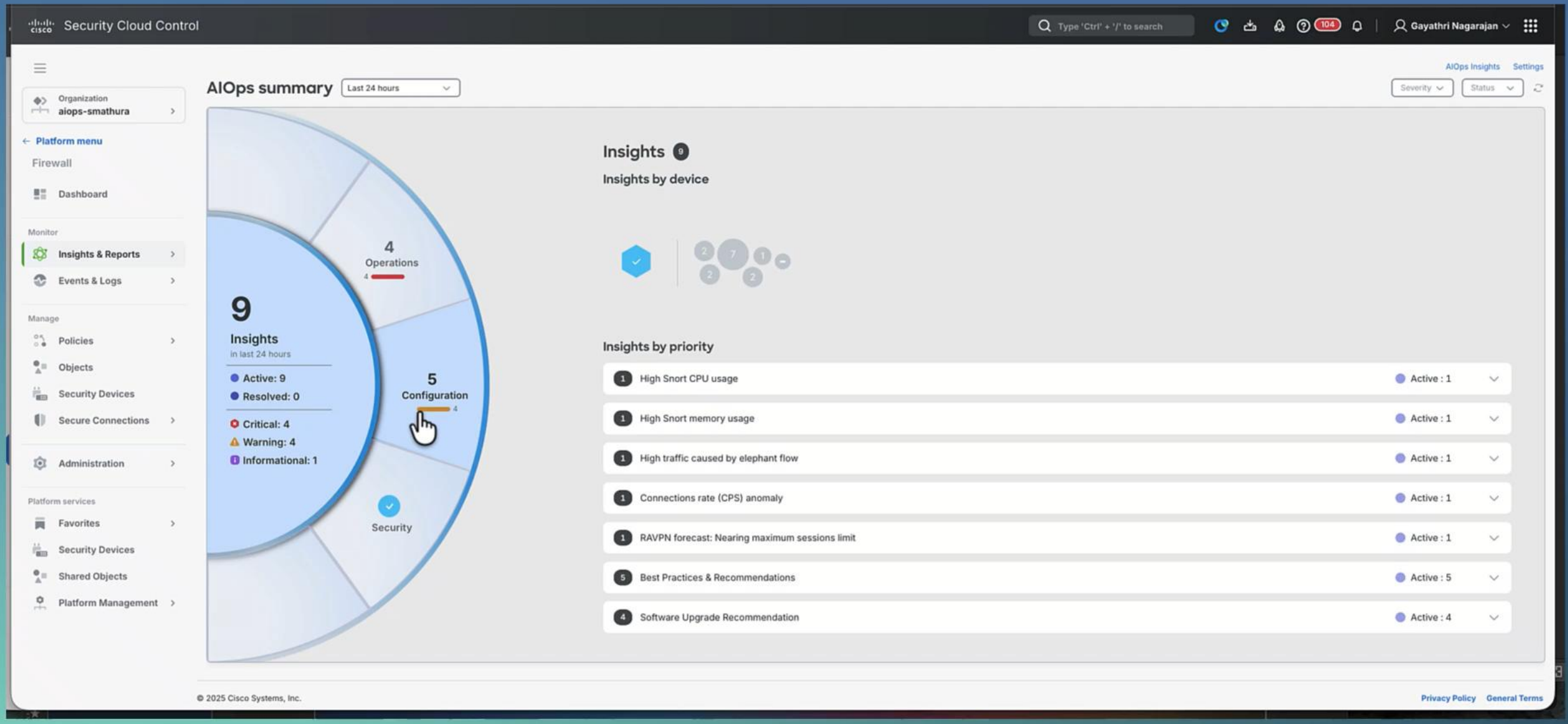
Traffic Insights: VPN Monitoring and Capacity Planning

Description of the anomaly and impacted devices

Probable cause & confidence level

Root cause analysis of the problem




Security Cloud Control
Type 'Ctrl' + '/' to search
104
Gayathri Nagarajan
Organization
aiops-smathura
Platform menu
Firewall
Dashboard
Monitor
Insights & Reports
Events & Logs
Manage
Policies
Objects
Security Devices
Secure Connections
Administration
Platform services
Favorites
Security Devices
Shared Objects
Platform Management
AIOps summary
Last 24 hours
AIOps Insights
Settings
Severity
Status
9
Insights
in last 24 hours
Active: 9
Resolved: 0
Critical: 4
Warning: 4
Informational: 1
4
Operations
5
Configuration
Security
Insights 9
Insights by device
Insights by priority
1 High Snort CPU usage
Active : 1
1 High Snort memory usage
Active : 1
1 High traffic caused by elephant flow
Active : 1
1 Connections rate (CPS) anomaly
Active : 1
1 RAVPN forecast: Nearing maximum sessions limit
Active : 1
5 Best Practices & Recommendations
Active : 5
4 Software Upgrade Recommendation
Active : 4
© 2025 Cisco Systems, Inc.
Privacy Policy
General Terms

Capacity and Trend Analyzer

Forecast problems before they occur

Helps with anomaly detection and proactive forecasting of problems along with root cause analysis

Ability to look into past, present & future

Ability to look through insights in real-time along with investigation capabilities to look through past and forecast options for future

Add your custom KPI to track

Provided with flexibility to choose KPI's and monitor those which matter to you.

Security Insights: Risky user visibility

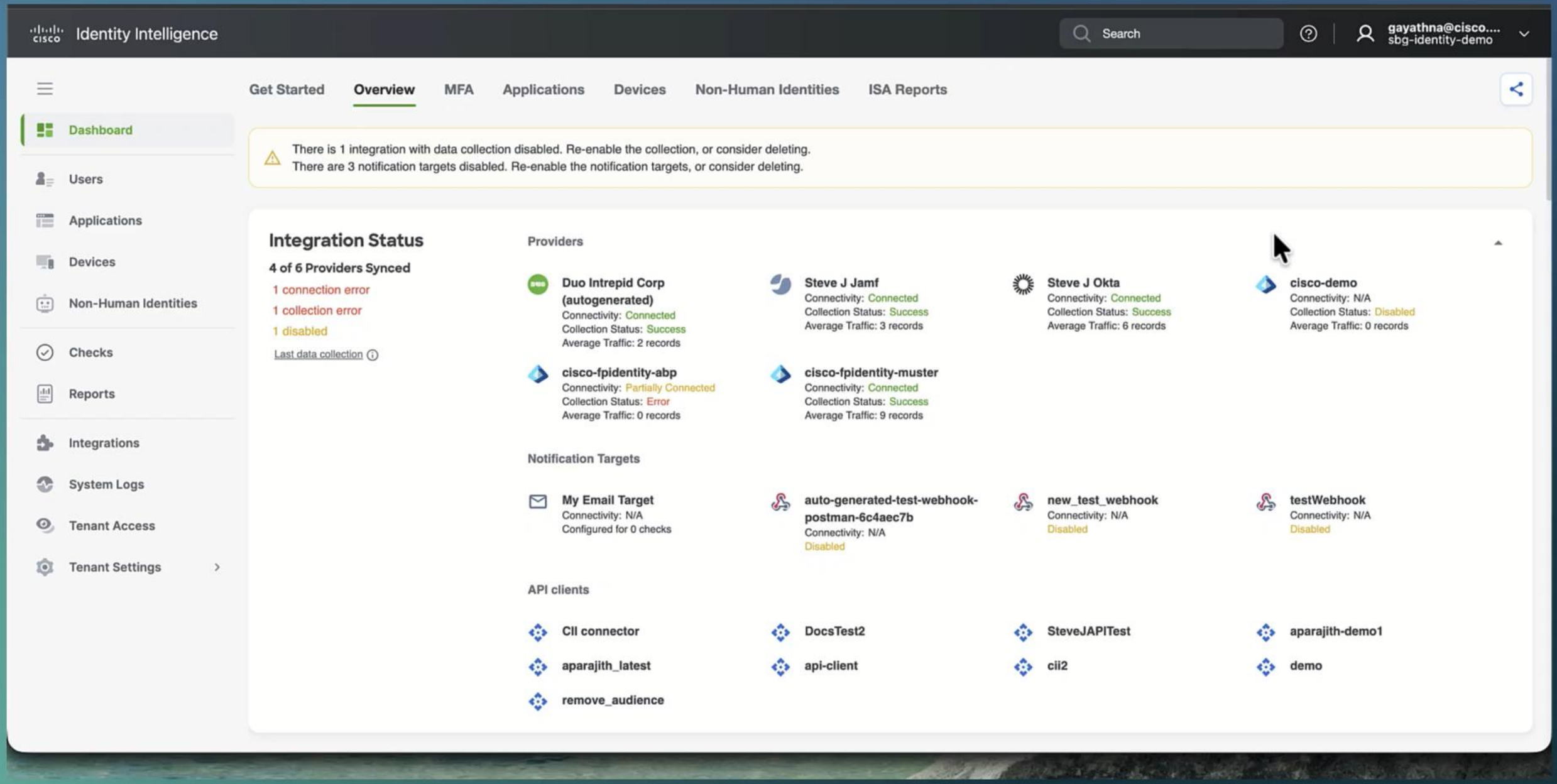
The Problem

Credential theft and identity-based attacks dominate cybersecurity incidents by exploiting the fundamental trust in digital identities. Traditional firewalls lack the architecture to detect or block malicious activities involving compromised credentials, leaving organizations exposed to persistent, stealthy attacks that leverage legitimate access to escalate privileges, move laterally, and deploy ransomware

The Solution

AIOps surfaces real-time insights into risky users and anomalous behavior and highlights risks such as privilege escalation, MFA fatigue, impossible travel, or sudden privilege spikes. These risks are surfaced through an intuitive dashboard, categorized by severity, and accompanied by root cause analysis and guided remediation steps.

- Risky user detection
- Automated remediation
- Identity aware firewall


Identity Intelligence
Search
gayathna@cisco....
sbg-identity-demo
Get Started
Overview
MFA
Applications
Devices
Non-Human Identities
ISA Reports
Dashboard
Users
Applications
Devices
Non-Human Identities
Checks
Reports
Integrations
System Logs
Tenant Access
Tenant Settings
There is 1 integration with data collection disabled. Re-enable the collection, or consider deleting.
There are 3 notification targets disabled. Re-enable the notification targets, or consider deleting.
Integration Status
4 of 6 Providers Synced
1 connection error
1 collection error
1 disabled
Last data collection
Providers
Duo Intrepid Corp (autogenerated)
Connectivity: Connected
Collection Status: Success
Average Traffic: 2 records
Steve J Jamf
Connectivity: Connected
Collection Status: Success
Average Traffic: 3 records
Steve J Okta
Connectivity: Connected
Collection Status: Success
Average Traffic: 6 records
cisco-demo
Connectivity: N/A
Collection Status: Disabled
Average Traffic: 0 records
cisco-fpidentity-abp
Connectivity: Partially Connected
Collection Status: Error
Average Traffic: 0 records
cisco-fpidentity-muster
Connectivity: Connected
Collection Status: Success
Average Traffic: 9 records
Notification Targets
My Email Target
Connectivity: N/A
Configured for 0 checks
auto-generated-test-webhook-postman-6c4aec7b
Connectivity: N/A
Disabled
new_test_webhook
Connectivity: N/A
Disabled
testWebhook
Connectivity: N/A
Disabled
API clients
CII connector
DocsTest2
SteveJAPITest
aparajith-demo1
aparajith_latest
api-client
cii2
demo
remove_audience

Software Upgrade Planner

The Problem

Today, planning for an upgrade involves extensive bug scrub & psirt identification triage process to understand whats the best version customers can upgrade too.

The Solution

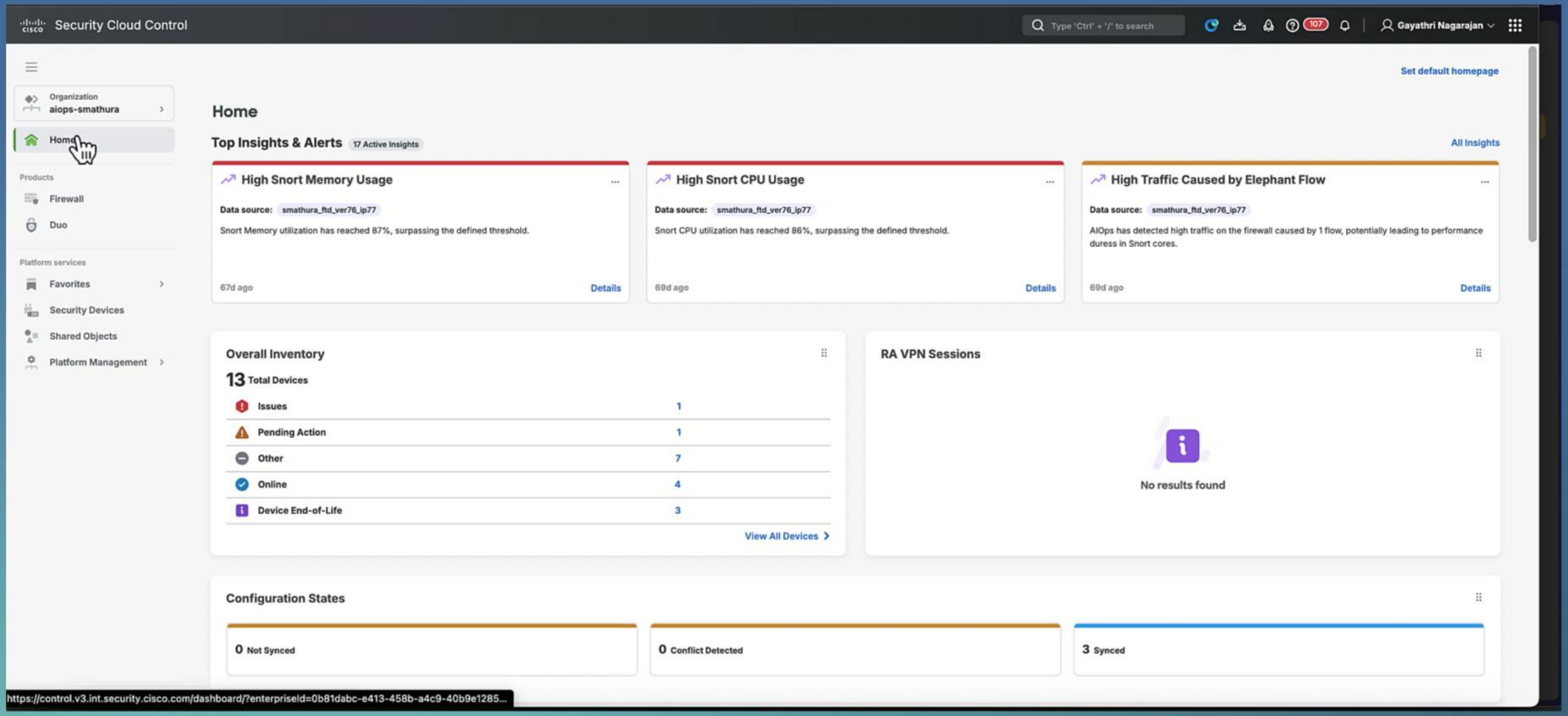
Analysis & report of PSIRTs and bugs based on current customer versions.

Identify and mitigate relevant risks before upgrading.

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

Eliminates manual research with environment-specific guidance

- Simplifies planning process
- Reduced mean time to resolution
- Major or minor upgrade versions


Security Cloud Control
Type 'Ctrl' + '/' to search
107
Gayathri Nagarajan
Organization
aiops-smathura
Home
Products
Firewall
Duo
Platform services
Favorites
Security Devices
Shared Objects
Platform Management
Set default homepage
Home
Top Insights & Alerts
17 Active Insights
All Insights
High Snort Memory Usage
Data source: smathura_ftd_ver76_ip77
Snort Memory utilization has reached 87%, surpassing the defined threshold.
67d ago
Details
High Snort CPU Usage
Data source: smathura_ftd_ver76_ip77
Snort CPU utilization has reached 86%, surpassing the defined threshold.
69d ago
Details
High Traffic Caused by Elephant Flow
Data source: smathura_ftd_ver76_ip77
AIOps has detected high traffic on the firewall caused by 1 flow, potentially leading to performance duress in Snort cores.
69d ago
Details
Overall Inventory
13 Total Devices
Issues 1
Pending Action 1
Other 7
Online 4
Device End-of-Life 3
View All Devices
RA VPN Sessions
No results found
Configuration States
0 Not Synced
0 Conflict Detected
3 Synced
https://control.v3.int.security.cisco.com/dashboard/?enterpriseId=0b81dabc-e413-458b-a4c9-40b9e1285...

Renewal Upgrade Planner

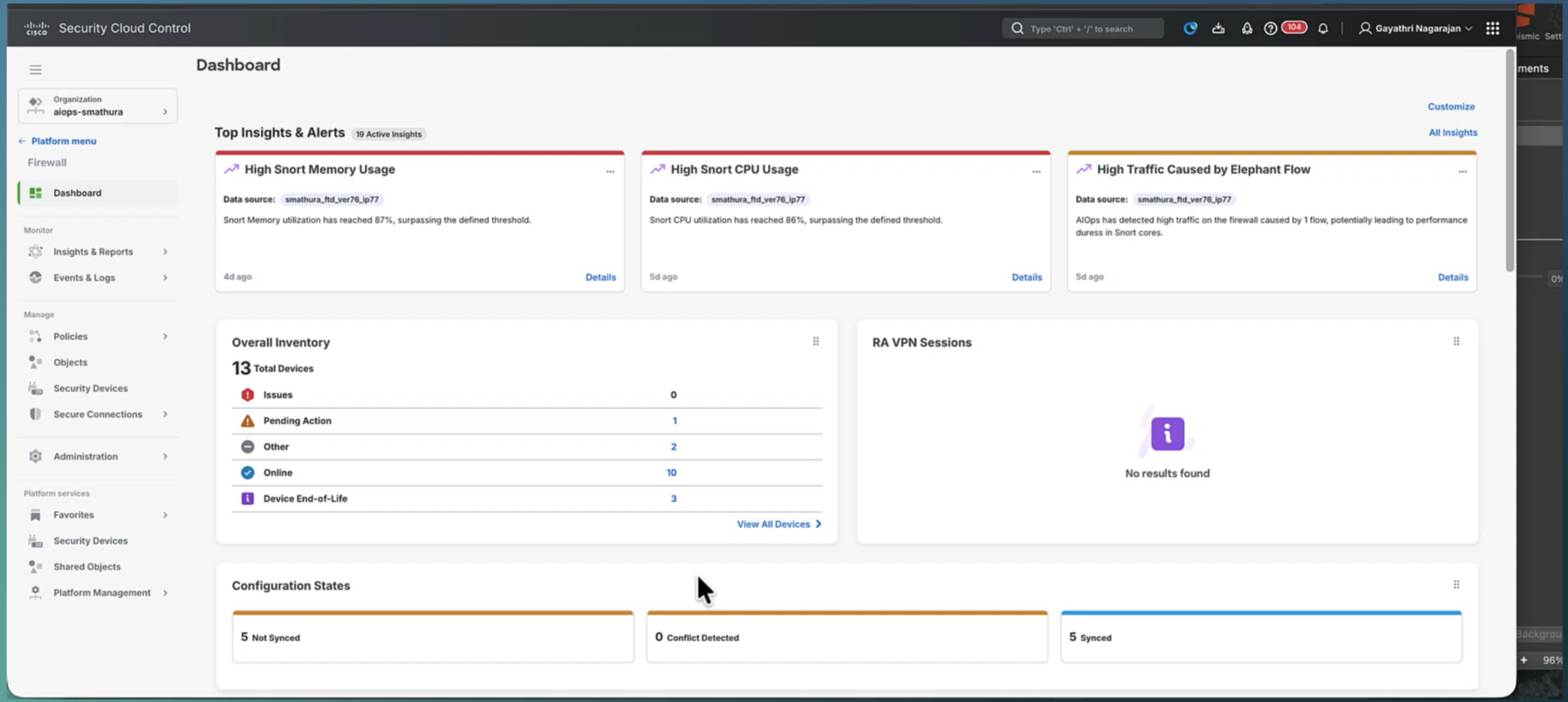
The Problem

Today, planning for renewal of new firewall model is a very manual process. It involves understanding of firewall models newly released by Cisco and migration paths

The Solution

Provides automated report of devices reaching End of Life along with various other dates. This also provides insights into new models released by Cisco along with links to data sheet.

- Simplifies planning process
- Reduced mean time to resolution
- Renew to latest & greatest


Security Cloud Control
Type 'Ctrl' + '/' to search
104
Gayathri Nagarajan
Dashboard
Organization
aiops-smathura
Platform menu
Firewall
Dashboard
Monitor
Insights & Reports
Events & Logs
Manage
Policies
Objects
Security Devices
Secure Connections
Administration
Platform services
Favorites
Security Devices
Shared Objects
Platform Management
Customize
Top Insights & Alerts
19 Active Insights
All Insights
High Snort Memory Usage
Data source: smathura_ftd_ver76_ip77
Snort Memory utilization has reached 87%, surpassing the defined threshold.
4d ago
Details
High Snort CPU Usage
Data source: smathura_ftd_ver76_ip77
Snort CPU utilization has reached 86%, surpassing the defined threshold.
5d ago
Details
High Traffic Caused by Elephant Flow
Data source: smathura_ftd_ver76_ip77
AIOps has detected high traffic on the firewall caused by 1 flow, potentially leading to performance duress in Snort cores.
5d ago
Details
Overall Inventory
13 Total Devices
Issues 0
Pending Action 1
Other 2
Online 10
Device End-of-Life 3
View All Devices
RA VPN Sessions
No results found
Configuration States
5 Not Synced
0 Conflict Detected
5 Synced

Internet & Network Outages visibility with Thousand Eyes Integration

The 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.

The Solution

ThousandEyes Internet Insights integration into AIOps for firewall provides real-time visibility into **internet and application outages.**

What is broken?

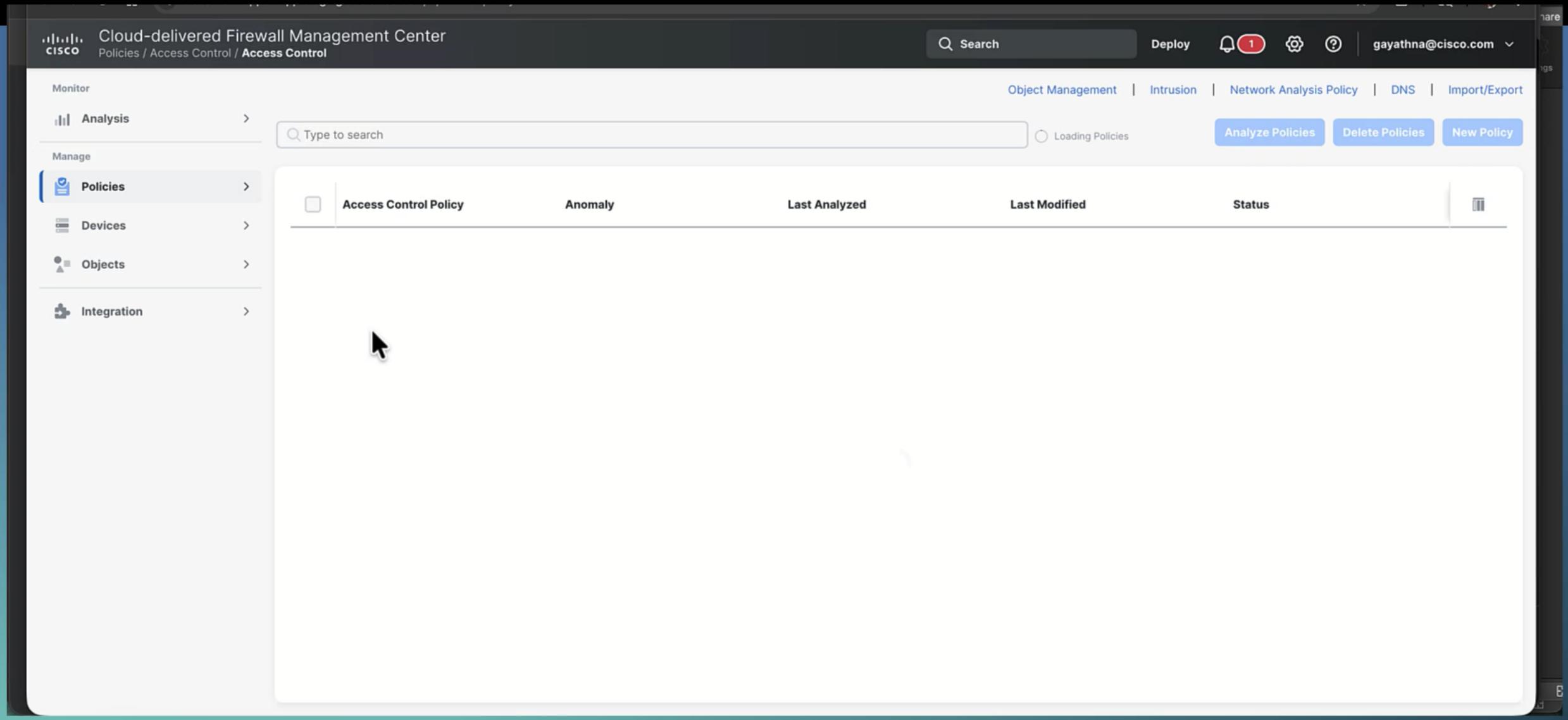
Where is the impact and the duration of impact?

Shows outages which are relevant or applicable to the customer based on their configuration & event data.

Reduce Mean Time to Detect

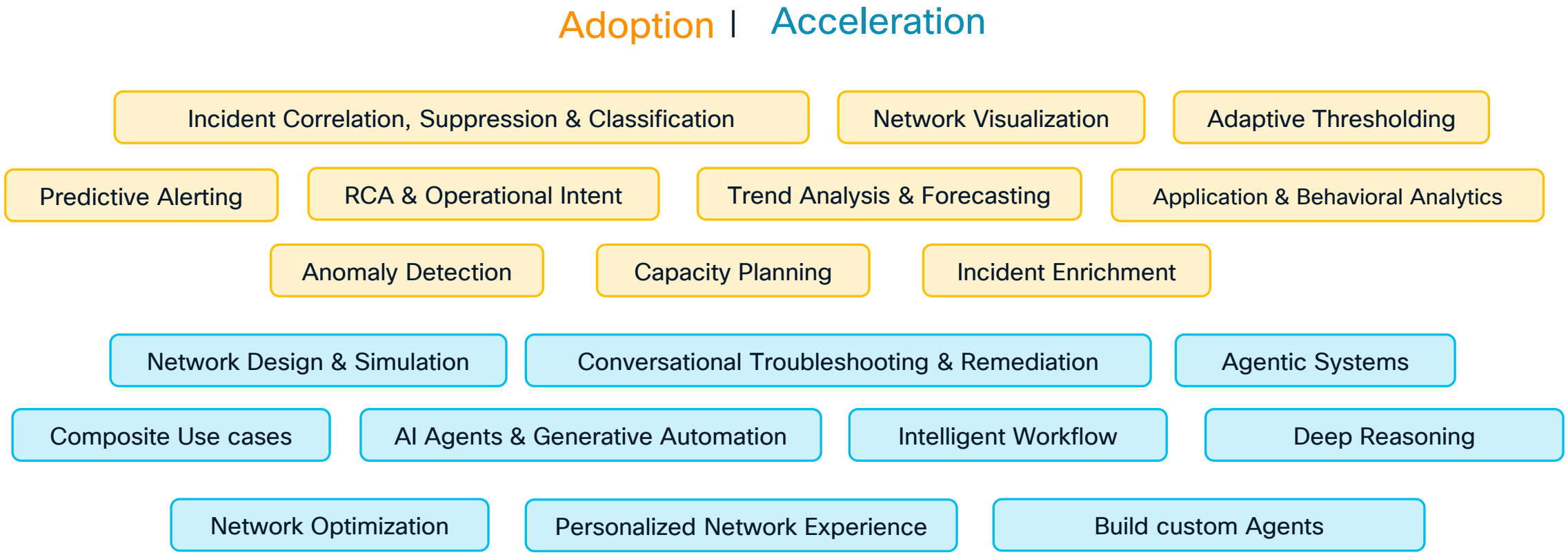
Visibility into application outages

Thousand Eyes Integration


Cloud-delivered Firewall Management Center
Policies / Access Control / Access Control
Search
Deploy
1
gayathna@cisco.com
Monitor
Analysis
Manage
Policies
Devices
Objects
Integration
Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export
Type to search
Loading Policies
Analyze Policies
Delete Policies
New Policy
Access Control Policy
Anomaly
Last Analyzed
Last Modified
Status

AI Capabilities Journey

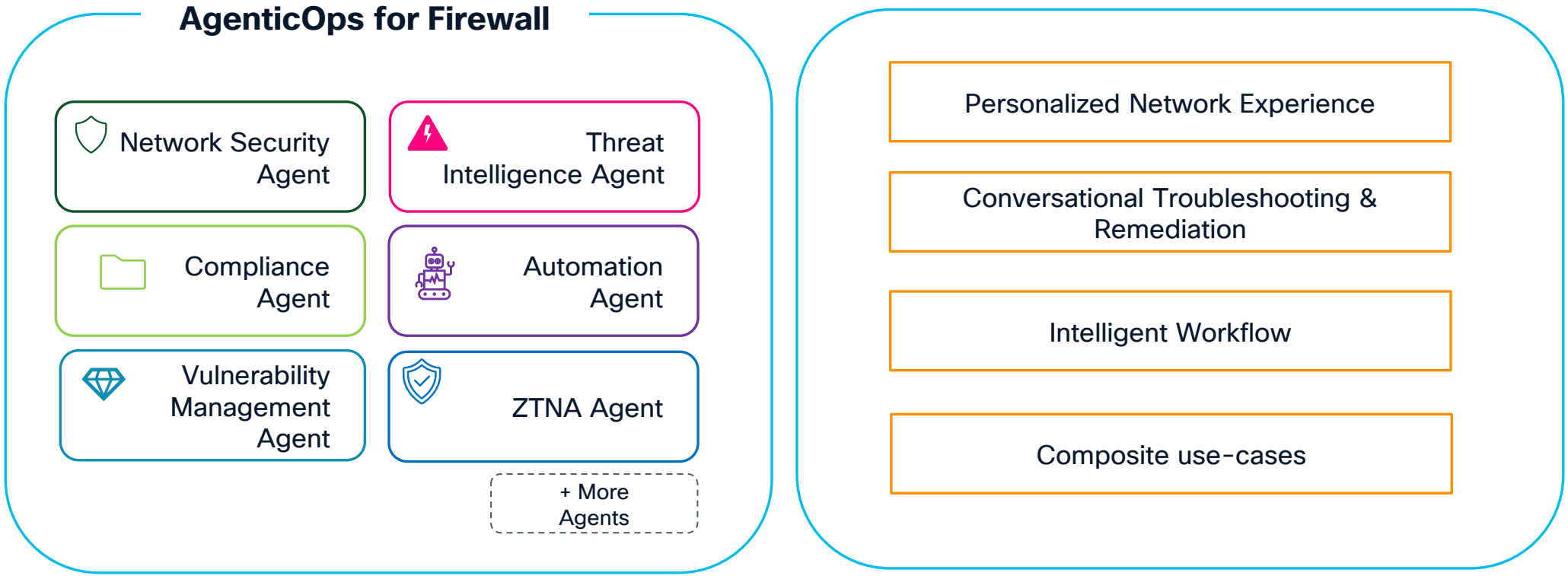
From Augmenting to a journey toward autonomy



AgenticOps: The next evolution of AIOps

Beyond Insights: Transitioning from AIOps to AgenticOps

Vision



Human-in-the loop approvals & Guardrails

AgenticOps for Firewall

Jan 2026
Beta

Security Cloud Control

Network Security Agent

Simplify complex product interactions and day-to-day network operations

- Configuration Management
- Troubleshooting
- Proactive Monitoring

Compliance agent

Simplify the overall compliance & audit process such as PCI DSS

- PCI DSS
- Audit Automation
- Autonomous Remediation

Operations agent

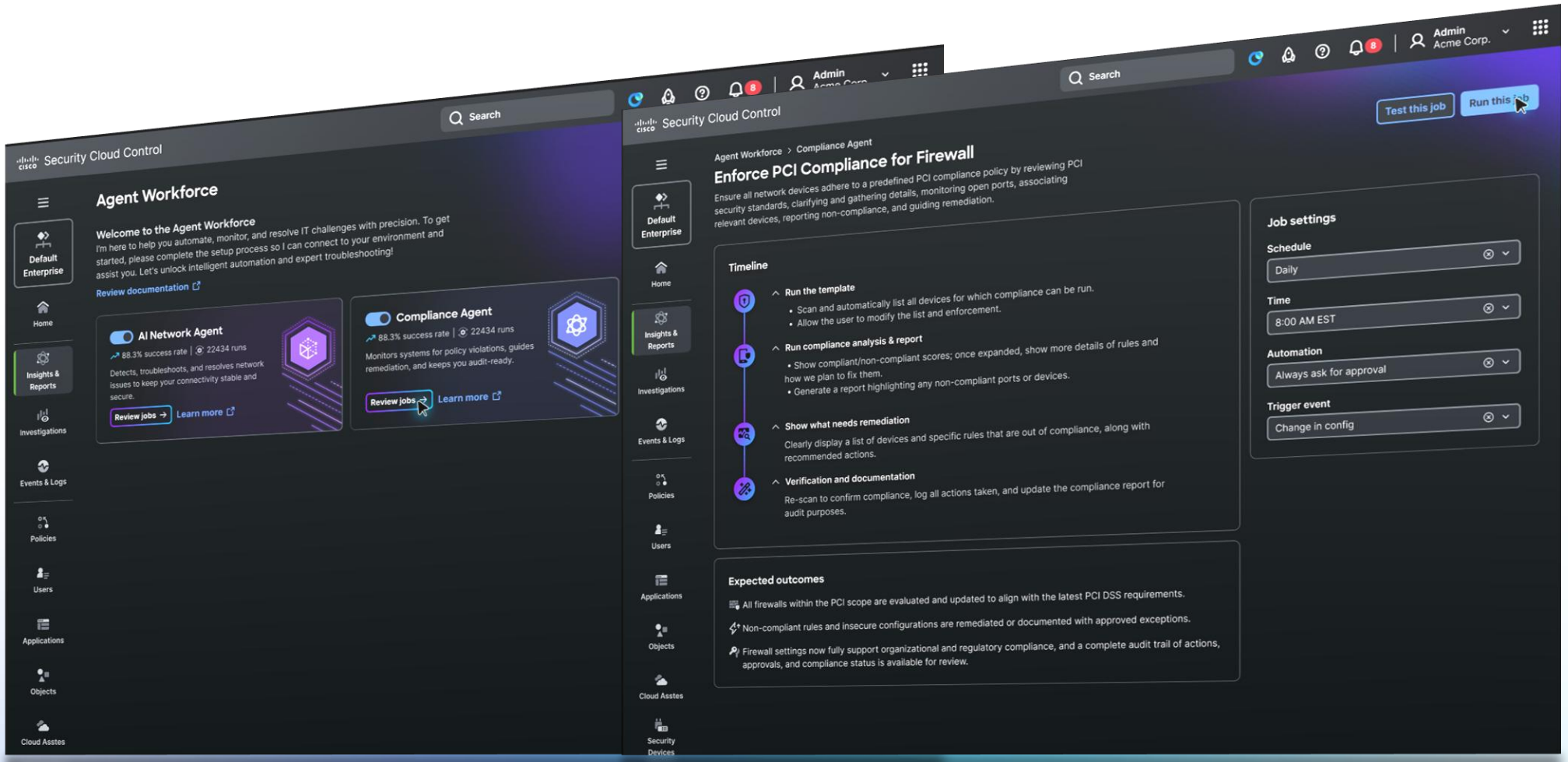
Accelerate troubleshooting, resolve support tickets

- Ticket Resolution
- Auto-Remediation
- Root Cause Analysis

Beta Sign up

AgenticOps for Firewall

The vision: networks that self-monitor, self-heal, and act, enabling proactive operations while keeping engineers in control (human in-the-loop).



AgenticOps for Cisco Firewall from Security Cloud Control

- Minimize misconfigurations and downtime
- Simplified Operations and Improved Security posture
- Autonomous troubleshooting and self-healing
- Enhance collaboration and approvals with Human-in-loop mechanism
- Productivity gains

Complete your session evaluations

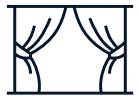
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

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

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

Thank you