

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



AIOPS for Cisco Firewall

Enhancing Operational Efficiency & Improve Security Posture with

Gayathri Nagarajan, Engineering Product Manager
BRKSEC-2151

Your speaker throughout this journey



Also, an Indian classical dancer & home farmer

Gayathri Nagarajan
Engineering Product Manager
Cloud + Network Security
Management Portfolio
gayathna@cisco.com



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 November 15, 2024.



How many of you like Tesla ?

Evolution of Tesla

Advanced Driver-Assistance Systems



“Everything On”

2000



“Feet Off”

2013



“Hands Off”

2018



“Eyes Off”

2024



“Mind Off”

2027-30

Autonomous driving

Agenda

Navigating complexities of Firewall management
Simplifying Operations with AIOps: The How and Why
Charting the Future : Vision & Roadmap
Real-world Use cases & Outcomes
Advantage of implementing AIOps
Analyst perspective on AIOps
Easing the journey : Onboarding & Compliance
AIOps Architecture: Sneak-peek
Celebration time : Bonus Offering

Navigating complexities of Firewall management

Voice of a firewall admin – Real reddit Rants (vendor agnostic)

“You’ve been tasked with firewall rule cleanup for an entire year, how do you respond

As a bright-eyed firewall engineer, your employer breaks the news that you’ll be doing nothing but firewall rule cleanup for an entire year. All while your other colleagues get to focus on career building work. How do you respond?

- A. Embrace the mind-numbing work accepting the fact your career will be stagnant while you cleanup a mess you did not make.
- B. Grab a shovel while looking for another job
- C. Invoke 8th amendment rights against cruel and unusual punishment.
- D. Pretend like you're doing analysis and just block everything hoping for the best.
- E. Wildcard response

“There has to be a better way to identify and manage these long-lived flows. The firewall needs smarter tools.”

I'm setting up my firewall and I was wondering if there are some "best practice" Rule Sets for the firewall out there? Or maybe some basic configs

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?

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?

“I need a way to automate this! Manually troubleshooting these spikes is taking way too much time.”

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 :)

Voice of a firewall admin – Real reddit Rants (vendor agnostic)

"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?"

"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 :)"

Complexity breeds security blind spots

Complex
Rules

010110
110010
001011

Misconfigurations



Skill set
demand



Compromised Security Posture

Outages/Down time

Reactive process

«« The average cost of network downtime is \$300,000 per hour »»

Complexity breeds security blind spots



COMPLEX
RULES

Compromised Security Posture



Outages / Down Time



Reactive Process

《《《 The average cost of network downtime is \$300,000 per hour 》》》

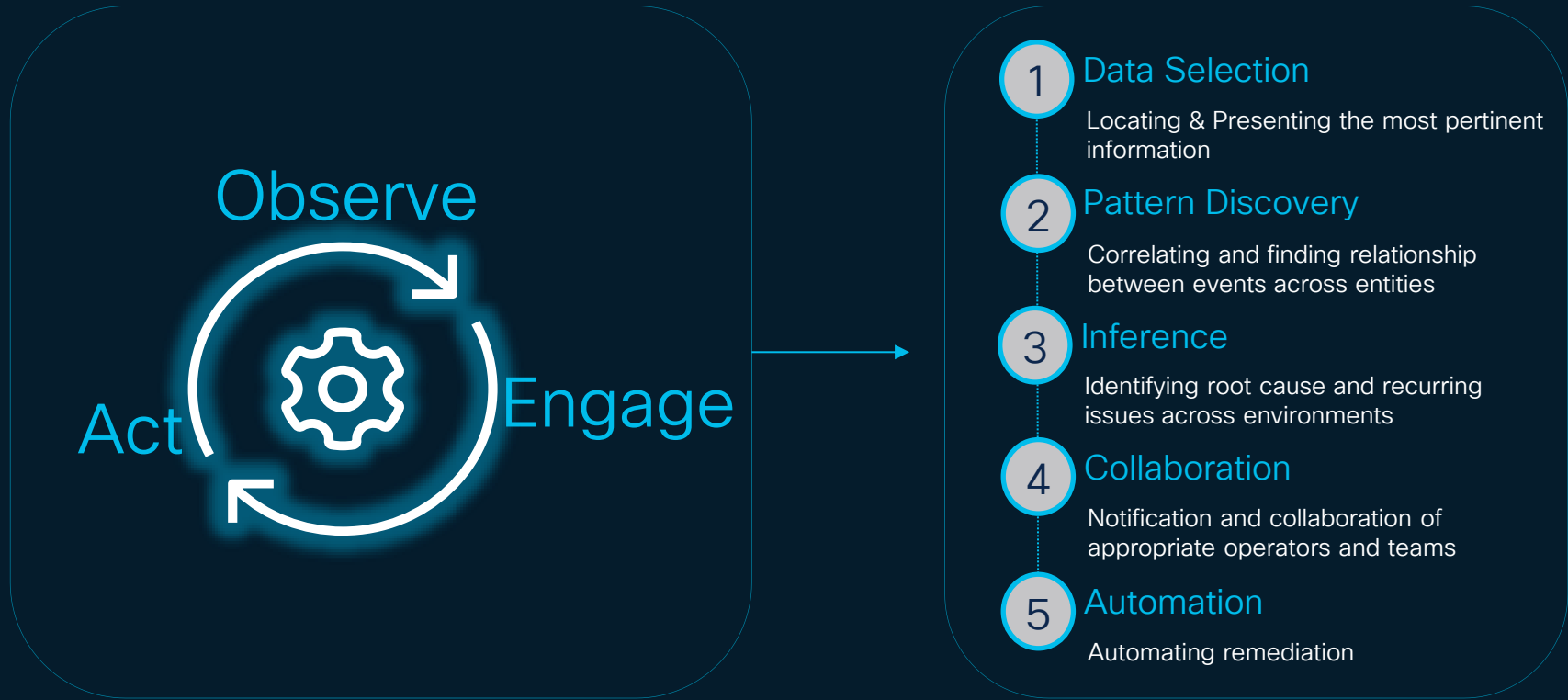
TOO MUCH DATA TO MAKE A DECISION



Simplifying Operations with AIOps: The How and Why

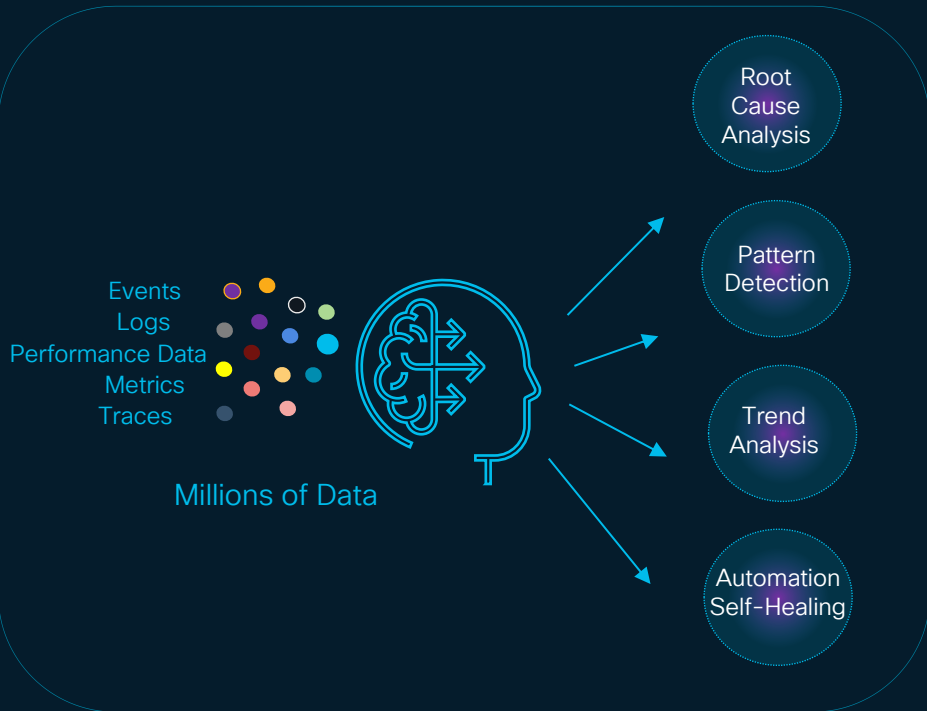


How does AIOps generally work ?

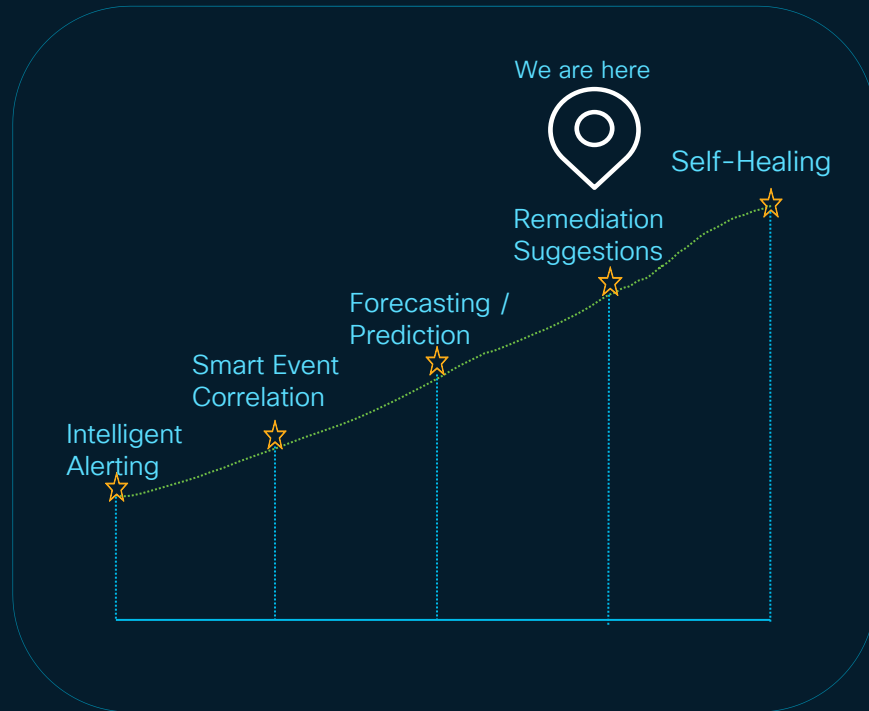


Our Approach

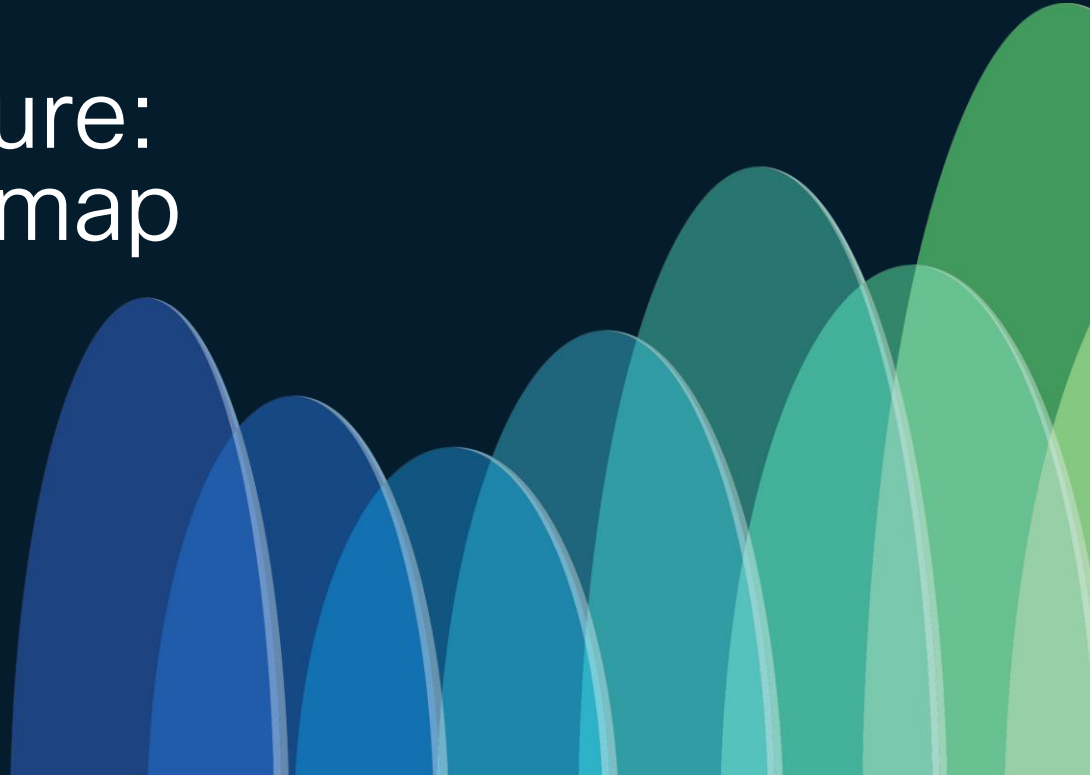
Inputs AIOps Engine Observations



AIOps Use cases: A maturity curve

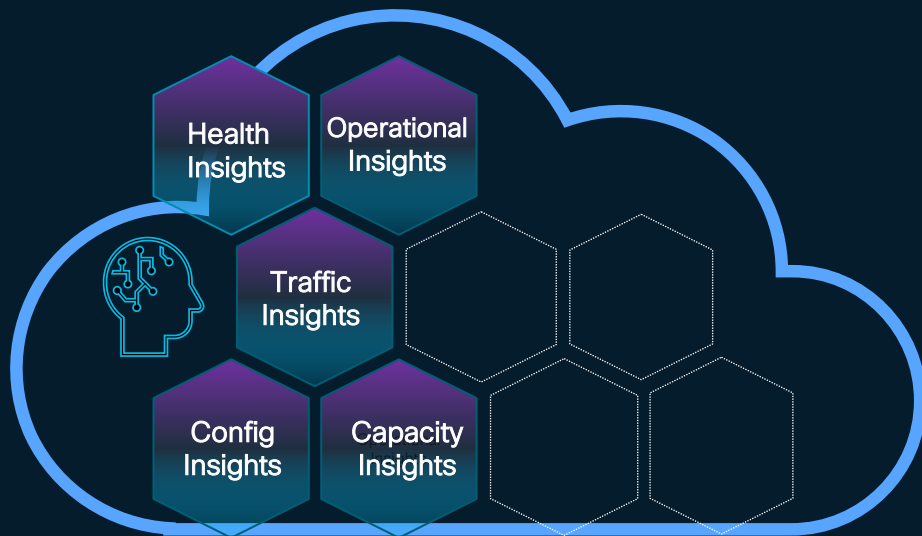


Charting the Future: Vision and Roadmap



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 prescriptive and guided remediations, **including integrations with change management systems like ServiceNow**
- Receive **Policy Optimization** suggestions and remediations tailored to your environment for easy Policy Management & optimal firewall performance
- Experience seamless interactions with **Cisco AI Assistant** to **assist** and **augment** human with their operations

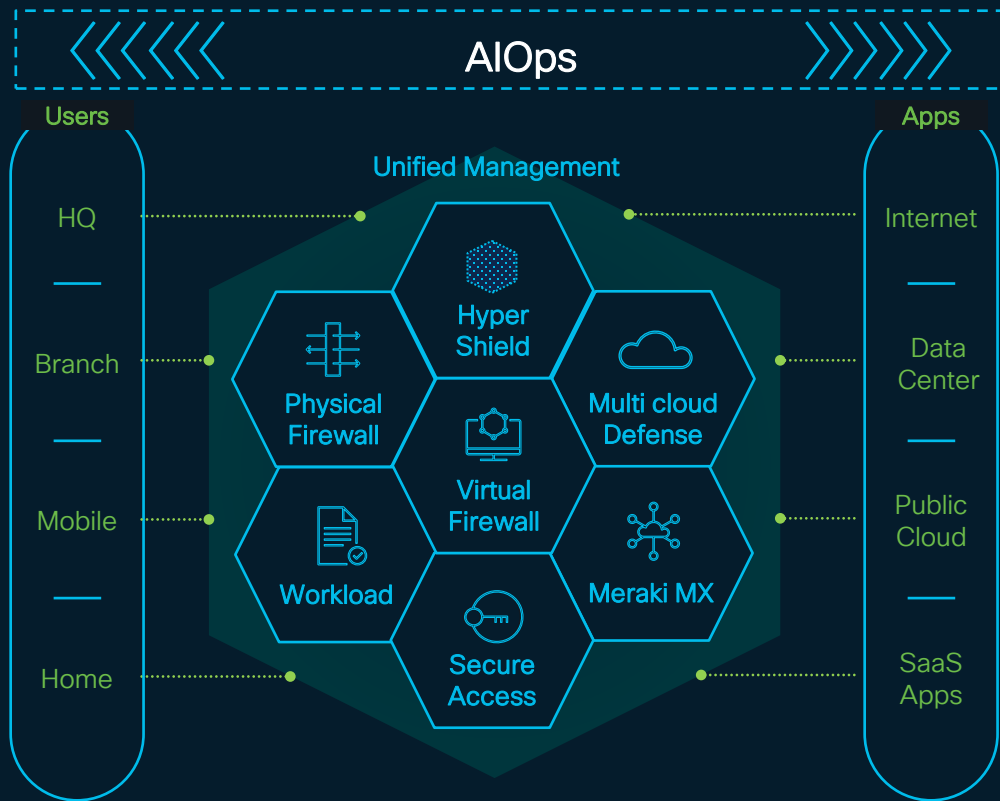
Derives insights from 3 Million metrics per day per device

Logs, Events, Metrics, Telemetry, Configuration, Database, Traces

Security Cloud Control Vision

For Hybrid Mesh Firewall

AIOps as a service harnesses the power of **artificial intelligence** and **machine learning**, leveraging operational insights to **enhance security posture**, and proactively strengthen the Hybrid Mesh Firewall Ecosystem



Gartner definition of [AIOps](#)

Product Roadmap

Strengthen Security Posture

Capacity Forecast with Predictive Analytics

Trends & Deviations

Best Practice Recommendations

Benefit the Ops team

Hardware Failure Prediction

Software Upgrade Planner Report

Policy Analyzer and Optimizer

Experience the future

Seamless AI Assistant interactions

Config Drift Analysis

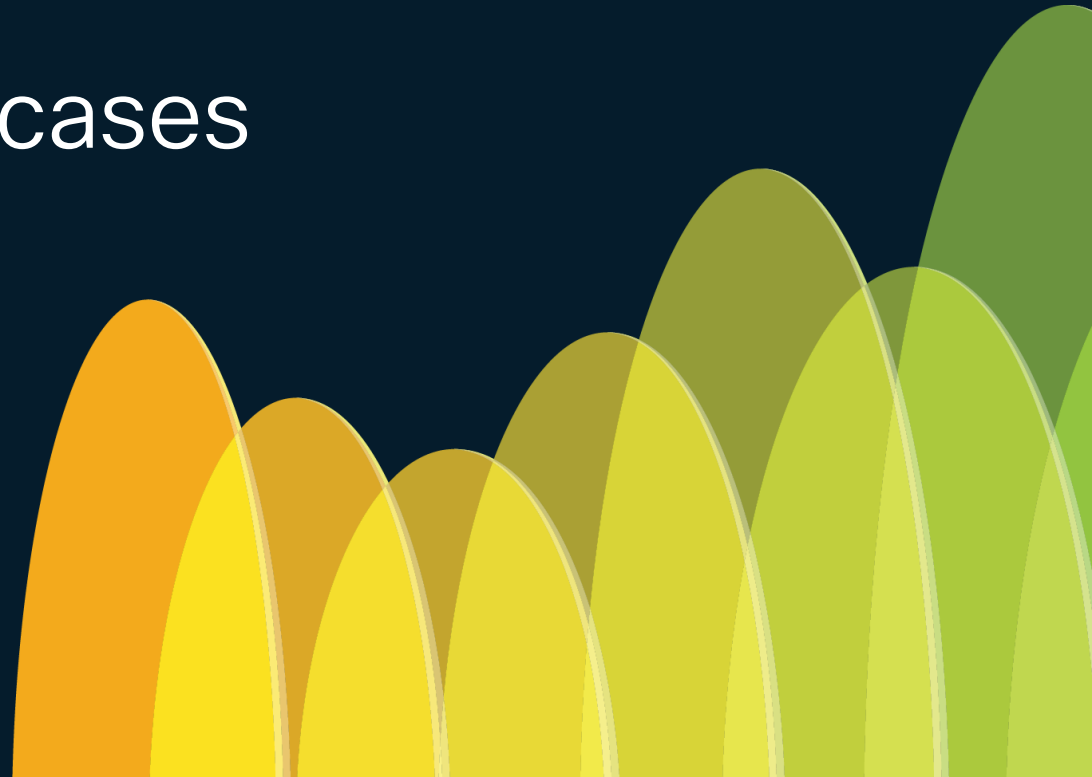
Assisted Intelligence for Troubleshoot

Pattern Discovery & Automated Remediations

Automatic ticket creation for change management

Logs, Metrics, Config, Telemetry, Traces, Perf Data

Real-world Use cases and Outcomes



Config Insights

- Policy Analyzer and Optimizer
- Best Practice Recommendations
- Feature Adoption



Policy Analyzer & Optimizer



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

Policy analysis and optimization, along with AI Assistant 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

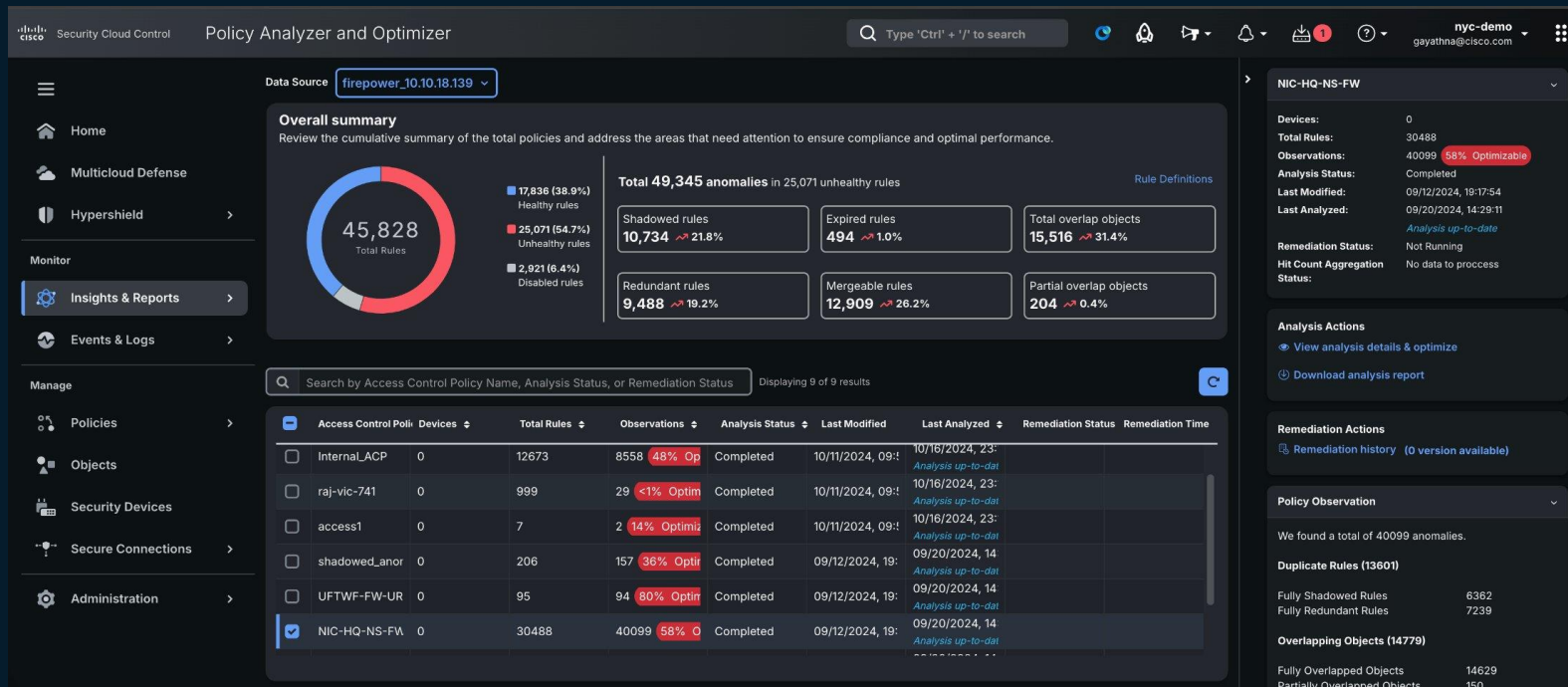
Detects Potential Security Gaps

Reduction in Change Management Time

Policy Analyzer & Optimizer

Simplify operations

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

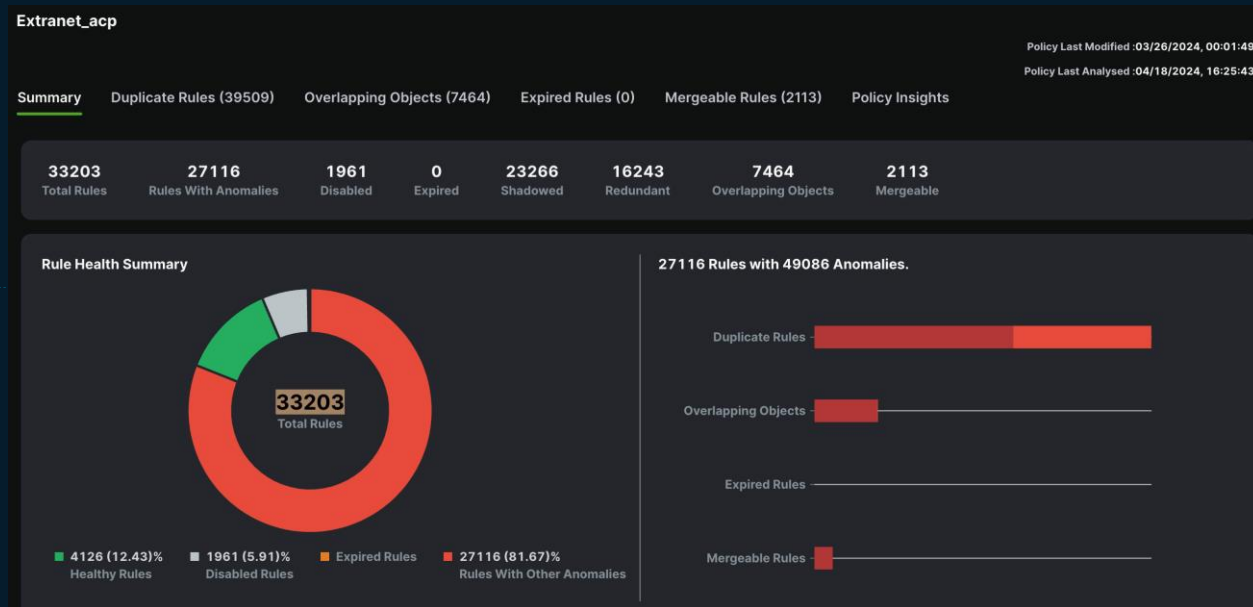


Policy Analyzer & Optimizer

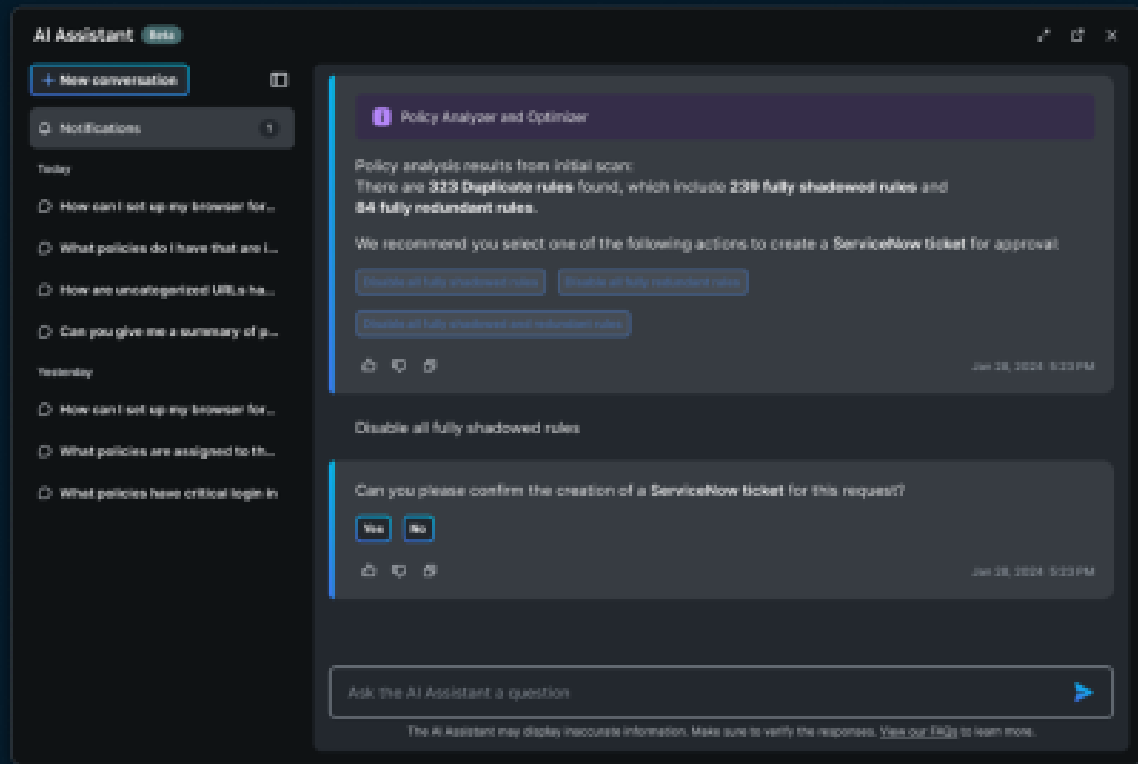
Simplify operations

81%

Config anomalies detected in
a real customer deployment

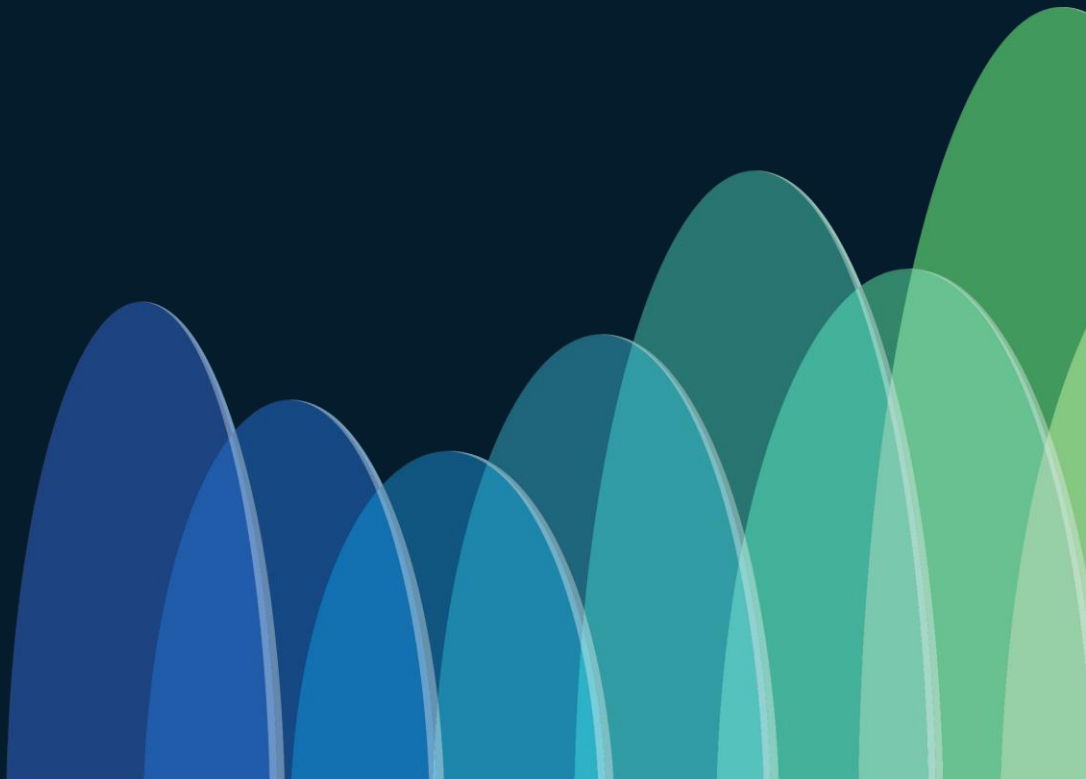


AI Assistant for Config Analysis & Optimization



Users will be notified through AI assistant and could kick off remediation workflow through the conversational interface.

Policy Analyzer & Optimizer Demo



Policy Insights

Firewall Policy Analyzer and Optimizer

Underutilized features to nudge customers to maximize the ROI



The problem

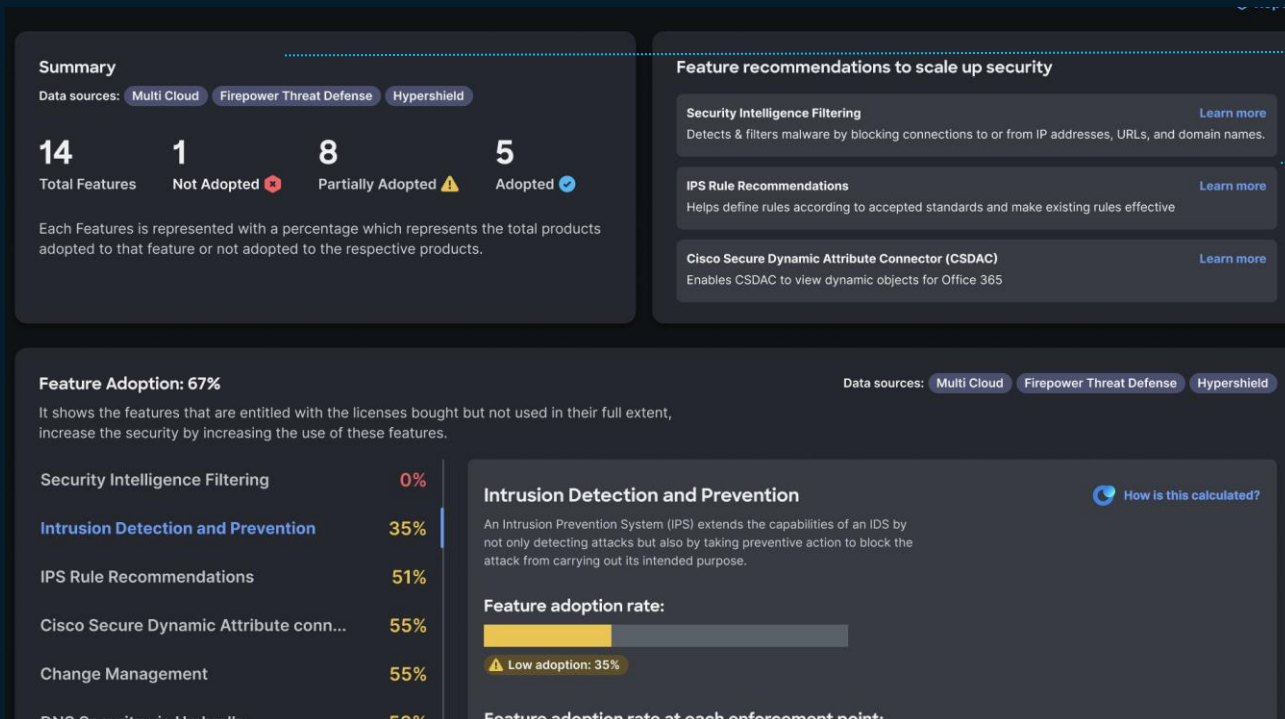
Users often find themselves buried in day-to-day operation tasks. They have limited time to learn new features that can help to improve security and productivity. Licenses bought were also often time not fully utilized. Currently, this information is not surfaced. Users may not be aware of the untapped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

Feature Adoption



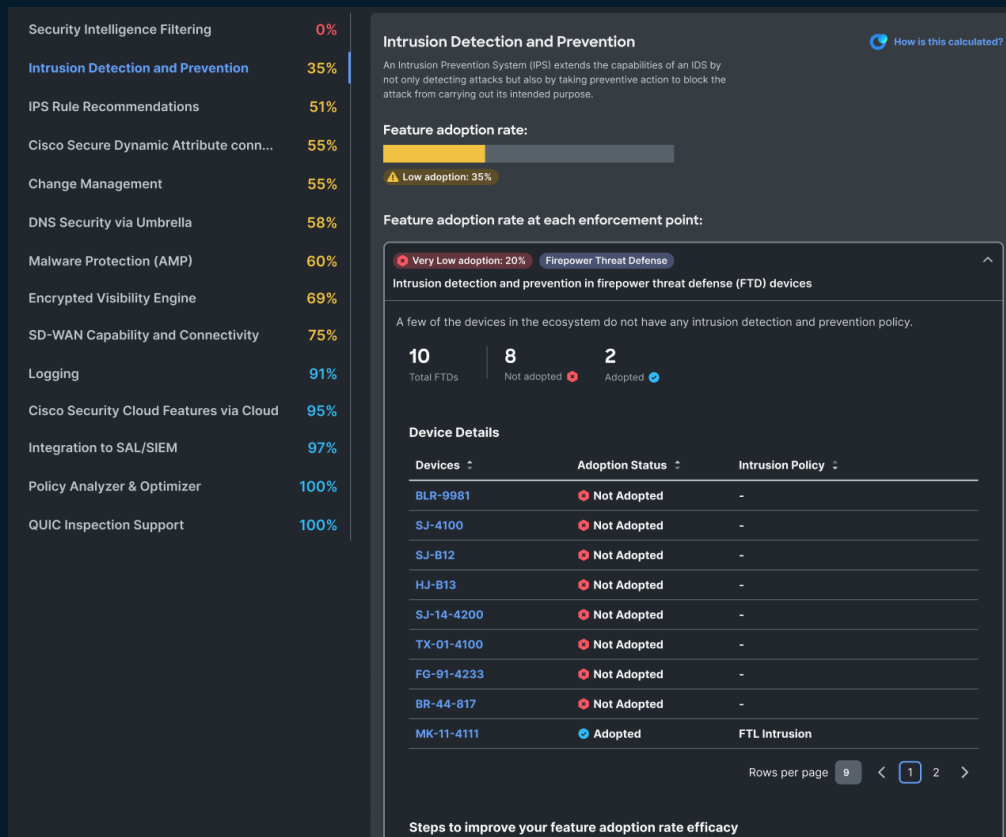
Summary view across the ecosystem

Feature recommendations & access to learn more about it

Guided workflows to remediate

Underutilized features

Surface underutilized features and provide information



Feature Adoption Demo



Feature Adoption

Last 24 hours

Summary

Data Sources: Firepower Threat Defense Multi Cloud Hypershield

13

Total Features

2

Not Adopted 🔴

3

Partially Adopted ⚠️

8

Adopted ✅

Each feature is represented with a percentage which shows the total number of products that have or have not adopted that feature.

Feature recommendations to scale up security

Encryption Visibility Engine

[Learn More](#)

Enables more visibility into the encrypted sessions without the need to decrypt them.

Intrusion Detection and Prevention

[Learn More](#)

Detects attacks and takes preventive actions to block the attack from carrying out its intended purpose.

Cisco Secure Dynamic Attribute Connector (CSDAC)

[Learn More](#)

Enables CSDAC to view dynamic objects for Office 365.

Feature Adoption: 72%

Data Sources: Firepower Threat Defense Multi Cloud Hypershield

It shows the features that are entitled with the licenses bought but not used in their full extent. Increase the overall security by increasing the use of these features.

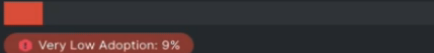
Encrypted Visibility Engine	9%
Intrusion Detection and Prevention	18%
Cisco Secure Dynamic Attribute Conn...	56%
SD-WAN Capability and Connectivity	74%
Change Management	76%
DNS Security via Umbrella	82%
Malware Protection (AMP)	82%

Encrypted Visibility Engine

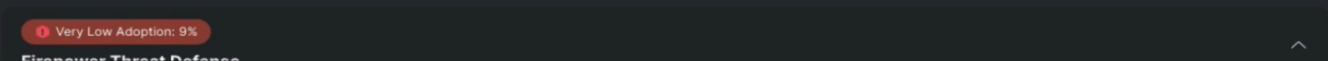
[How is this calculated?](#)

Encrypted Visibility Engine (EVE) is used to provide more visibility into the encrypted sessions without the need to decrypt them.

Feature adoption rate:



Feature adoption rate at each enforcement point:



No Active Jobs

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, this 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.



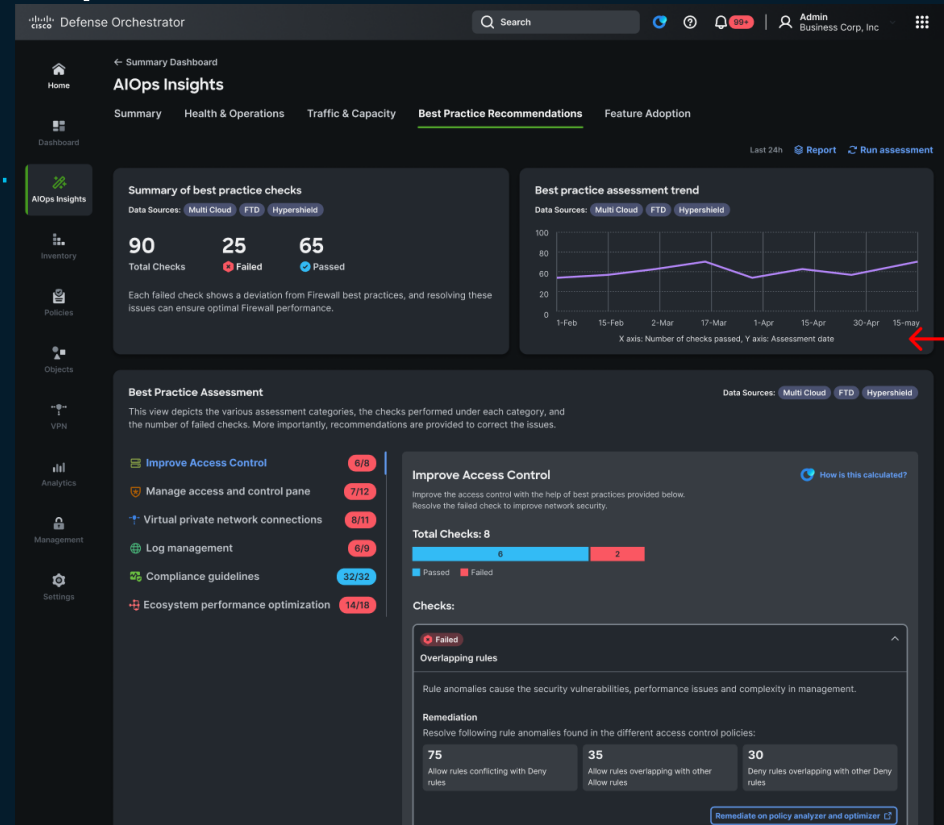
The solution

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.

Improved clarity with AIOps

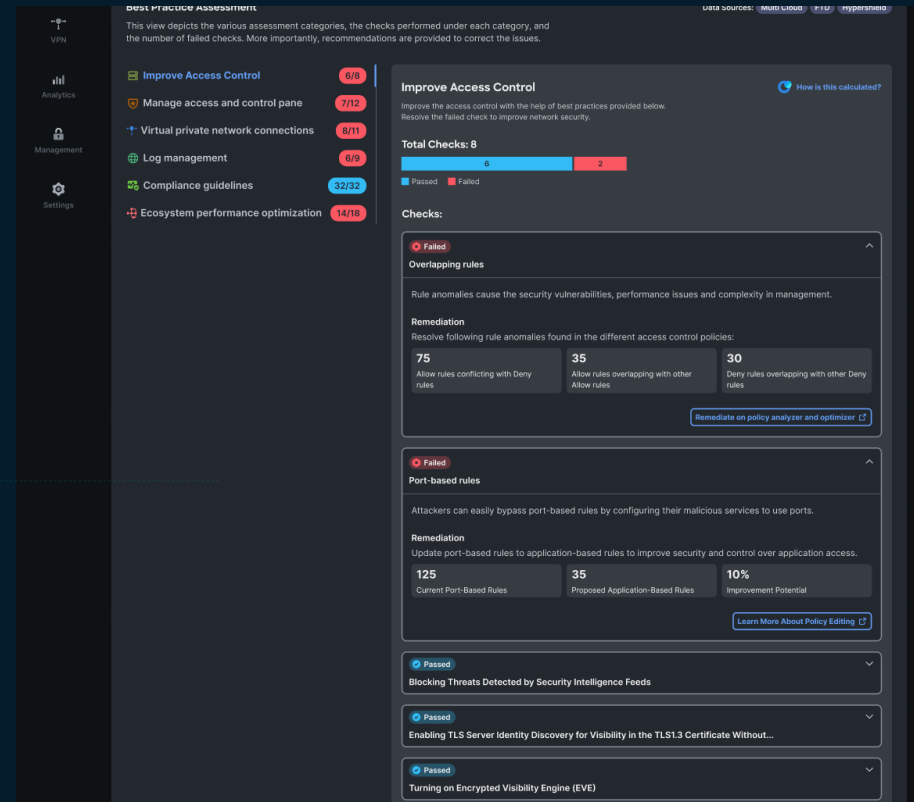
Users see their configurations benchmarked against best practice.

Track improvements over time.

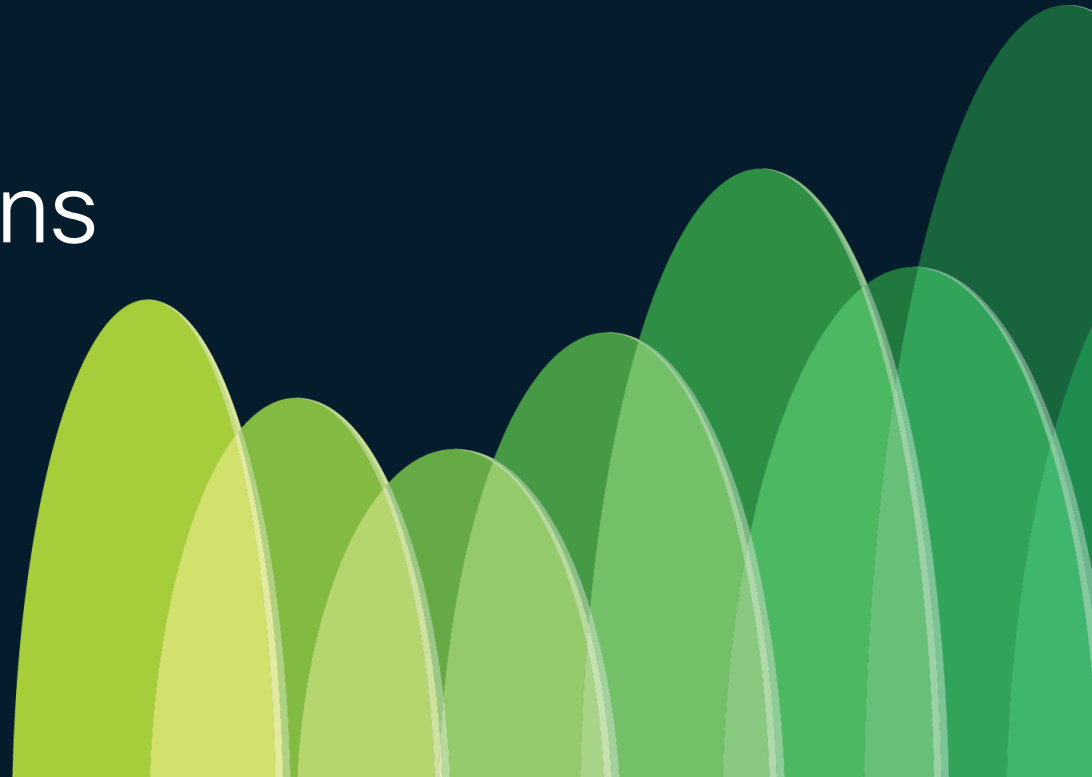


Improved clarity with AIOps

Suggestions to convert port based rules to application based rules for improved security postures



Best Practice Recommendations Demo





Dashboard



AIOps Insights >



Inventory



Policies >



Objects



VPN >



Analytics >



Change Log



Jobs



Tools & Services >

Best Practices and Recommendations

Last 24 hours [Run Assessment](#)

Summary

Data Sources:

Firepower Threat Defense

Multi Cloud

Hypershield

34

Total Checks

24

Failed 🔴

40

Passed 🟢

Each failed check shows a deviation from firewall best practices, and resolving these issues can ensure optimal firewall performance.

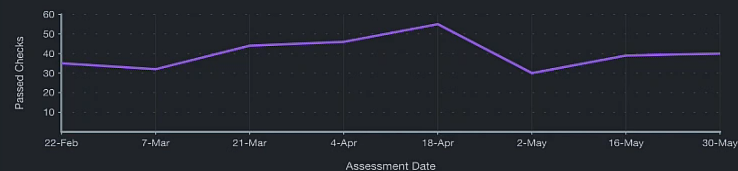
Best Practice Assessment Trend

Data Sources:

Firepower Threat Defense

Multi Cloud

Hypershield



Best Practice Assessment

This view depicts the various assessment categories, the checks performed under each category, and the number of failed checks. More importantly, recommendations are provided to correct the issues.

Data Sources:

Firepower Threat Defense

Multi Cloud

Hypershield

[🔒 Manage Access and Co...](#) 4 Failed/18[📋 Compliance Guidelines](#) 3 Failed/11[🔧 Improve Access Control](#) 2 Failed/5[🌐 Virtual Private Network ...](#) 15 Failed/16

Manage Access and Control Pane

[📖 How is this calculated?](#)

Improve the access control with the help of best practices provided below. Resolve the failed checks to improve network security.

Total Checks: 18

Failed Passed

Checks:

🔴 Failed

NAT Misconfiguration

Translation for an entire subnet to a single IP address, which could drop traffic.

NAT configuration is trying to translate an entire subnet to another address. The translated address is not a correct network address/subnet based on the source subnet specified in the object's definition. This can cause unexpected NAT behaviors and connectivity problems.

[Change Request](#) [+](#) [None](#) [▲](#)

No Active Jobs

Traffic Insights

- Elephant Flow Detection & Remediation
- RAVPN Monitoring & capacity planning

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

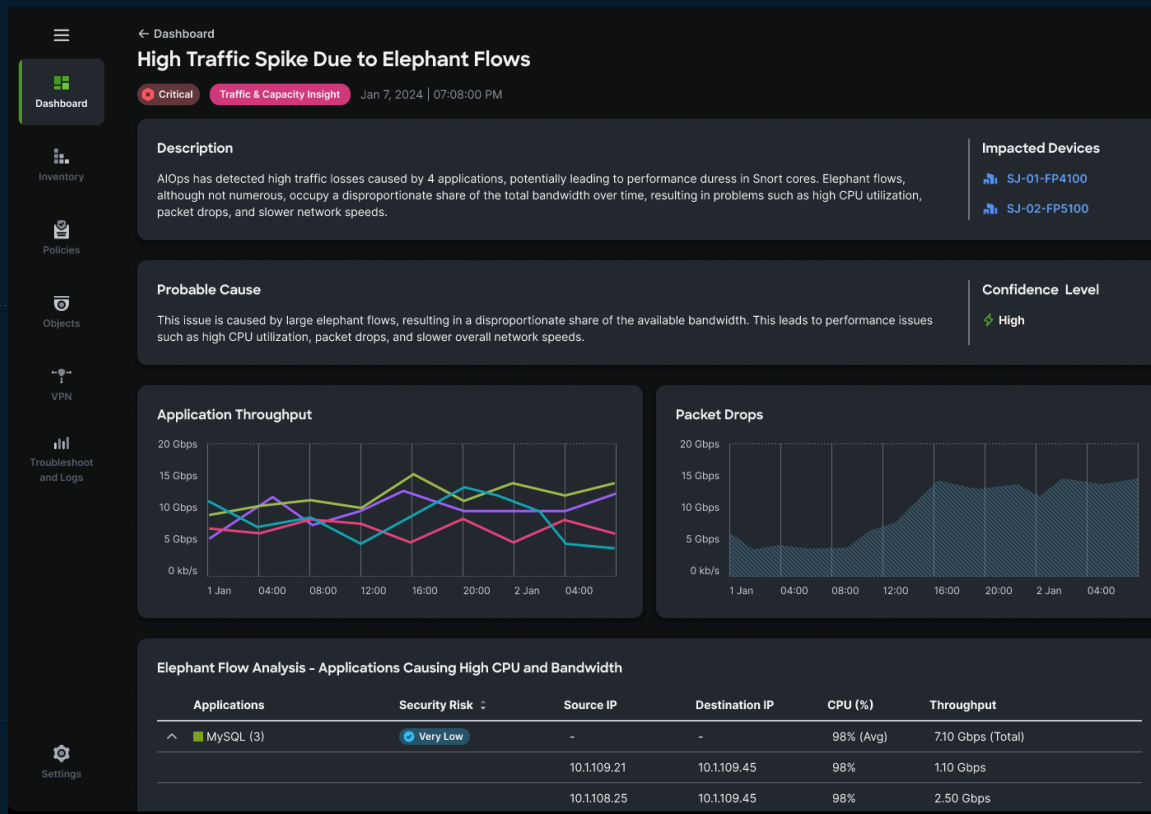
Reduced Mean Time to Resolution

Risk-based prioritization

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



Traffic Insights: Elephant flow detection & Remediation

Elephant Flow Analysis - Applications Causing High CPU and Bandwidth

Applications	Security Risk	AI Suggested Remediation
> MySQL (3)	Very Low	Bypass Application
> Webex	Low	Bypass Application
> Amazon Alexa	Medium	-
> Cloudload (2)	Very High	Throttle Application

AI suggested remediations to bypass or throttle traffic

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

Remediation

The best remediation method for an elephant flow depends on a specific situation. If the flow is legitimate and does not pose a security risk, bypassing may be the best option. However, if the flow is suspicious or malicious, throttling it may be necessary.

Bypass / Throttle Traffic Inspection for Applications

Bypass traffic inspection for trusted or low-risk applications. Alternatively, throttle traffic for nonbusiness critical and high-risk applications.

Start Remediation

Show Remediation Details

Automated remediation suggestion workflow

Upgrade FTD to Support Increased Performance

Traffic Insights: Elephant flow detection & Remediation

Bypass or Throttle Traffic Inspection for Applications

i AIOps automatically identified and bypassed/throttled the application that is causing the elephant flow, based on the application's risk profile. If required, you can override this action and assign appropriate actions to unassigned applications

Applications

Application Name	Security Risk
☒ Amazon Alexa	Medium

[Add to Bypass >](#)

[Add to Throttle >](#)

Bypass Applications

Application Name	Security Risk
MySQL	Very Low
Webex	Low

Throttle Applications

Application Name	Security Risk
Cloudload	Very High

*Unassigned applications may require your attention to be moved to the appropriate section

Impact

AIOps will apply the recommendations to the following policy and devices:

Corporate-Edge-Access

SJ-01-FP4100

Access Control Policy

[Cancel](#) [Save](#)

Automated workflow to bypass or throttle traffic

Based on user decision, policy changes are made

Shows the impacted devices & policy changes before user performs "save"

Traffic Insights Demo for Elephant Flow Detection & Remediation



Traffic Insights

Elephant Flow Detection & Remediation

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

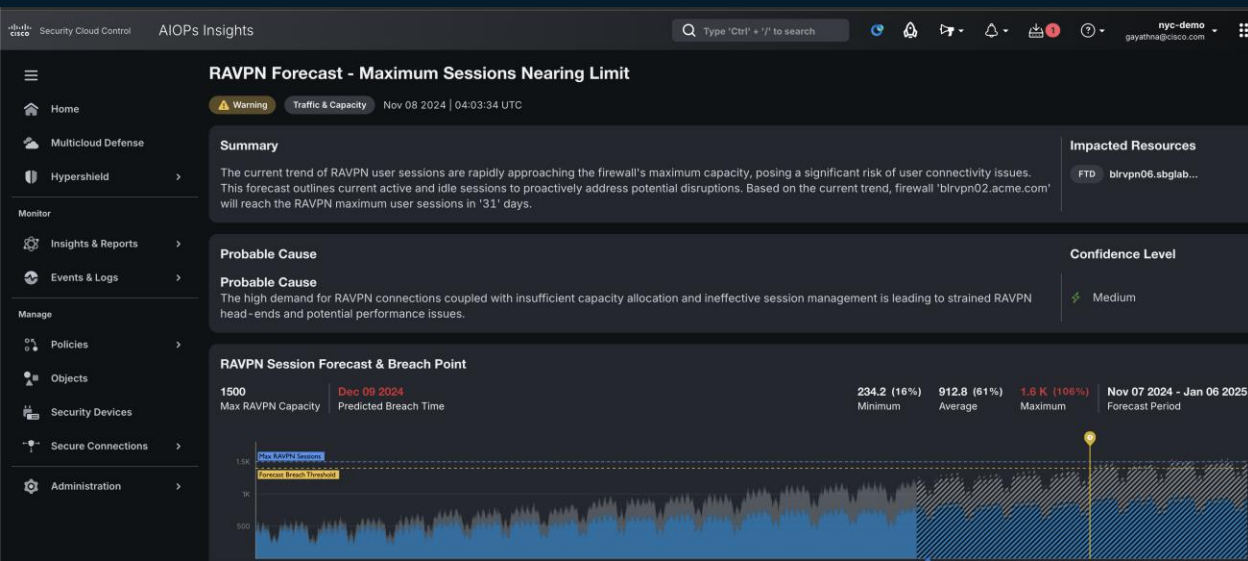
Using predictive analytics, we can identify these disparities and offer actionable solutions.

Faster troubleshooting

Reduced mean time to resolution

Risk-based prioritization

Traffic Insights: VPN Monitoring and Capacity Planning

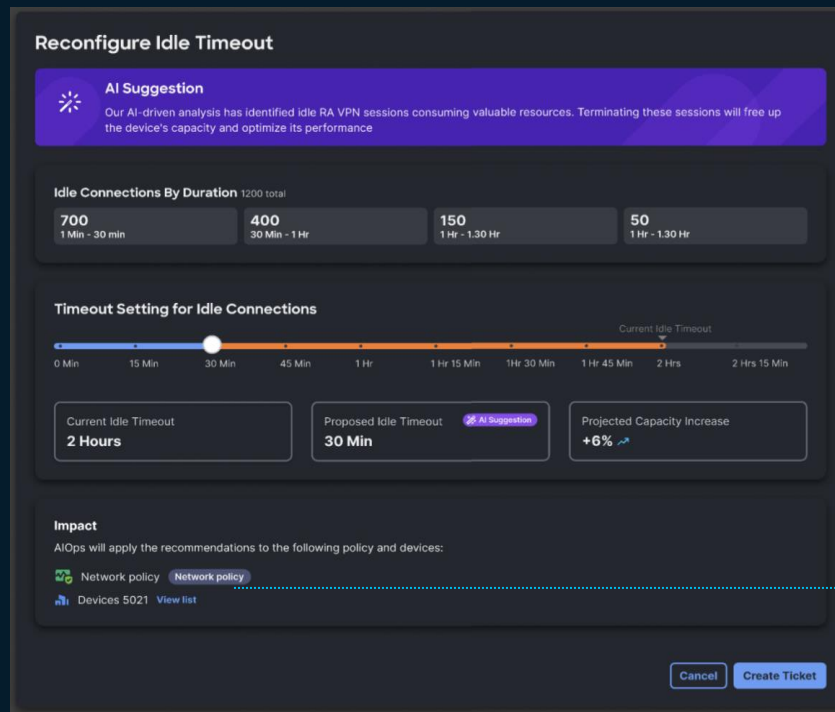


Description of the anomaly and impacted devices

Probable cause & confidence level

Root cause analysis of the problem

Traffic Insights: VPN Monitoring and Capacity Planning



AI identified idle RA VPN sessions consuming valuable resources. It recommends timeout setting and allow users to customize it to their needs.

Based on user decision, policy changes are made

Shows the impacted devices & policy changes before user performs "save"

Traffic Insights Demo for VPN Monitoring & Capacity Planning

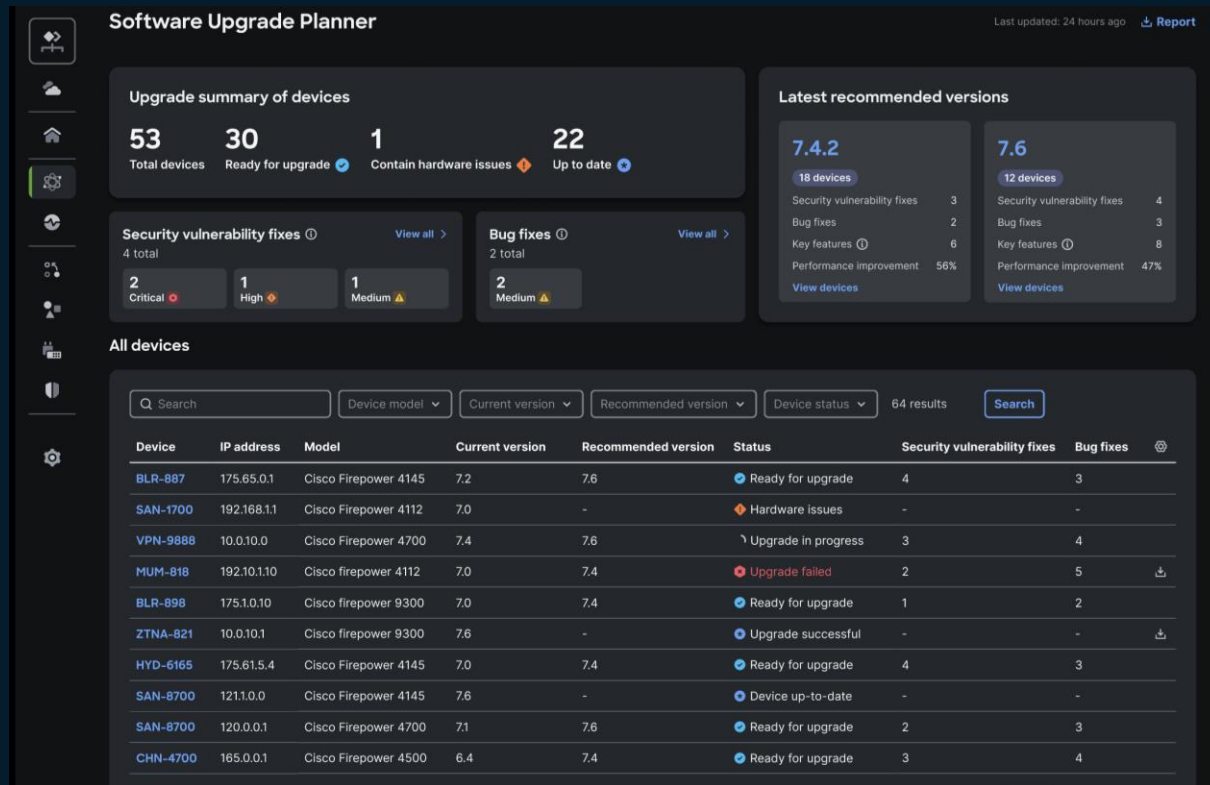


Capacity Insights

RAVPN Monitoring & Capacity Planning

Operational Insights Software Upgrade Planner

in roadmap



Summary



Unified Console

With AIOps, the administrator has access to a unified console that provides a centralized view of firewall operations, performance and health.



Trend identification

AIOps analyses network data and identifies trends, such as the emergence of "elephant flows" that are causing high CPU utilization.



Prescriptive Remediation

AIOps offers prescriptive recommendations to the administrator, guiding them on the steps to mitigate the issue and restore network performance.

..... Faster Troubleshooting>

..... Reduced Mean time to resolution>

An artistic illustration of a young man with brown hair and a surprised expression, holding a glowing, ornate box. From the box, a bright, golden light bursts forth, creating a large, radiant cone of light that fills the upper right portion of the frame. Several small, glowing icons float in the air around the man and the box. These icons include a cross, a plus sign, a gear, and a square with a cross. The background is dark and textured, suggesting a night sky or a cave. The overall style is painterly and dramatic, with a focus on the magical and transformative nature of the scene.

Advantage of implementing AIOps

Advantage of implementing AIOps



Key benefits of AIOps

AIOps for Cisco
Firewall from
Security Cloud
Control



Minimize misconfigurations
and downtime



Simplified Operations and
Improved Security posture



Enhance human judgements with
AI-enriched actionable information



Enhance customer experience
with guided remediation



Boost collaboration with integration
to chatOps and ITSM tools

Key benefits of AIOps

AIOps for Cisco
Firewall from
Security Cloud
Control



Minimize misconfigurations
and downtime



Simplified Operations and
Improved Security posture



Enhance human judgements
with AI-enriched actionable
information



Enhance customer experience
with guided remediation



Boost collaboration with integration
to chatOps and ITSM tools



How does our AIOps for Cisco Firewall help you?



Augment



Actionable



Autonomous

How does our AIOps for Cisco Firewall help you?



AUGMENT



ACTIONABLE



AUTONOMOUS

Analyst perspective on AIOps



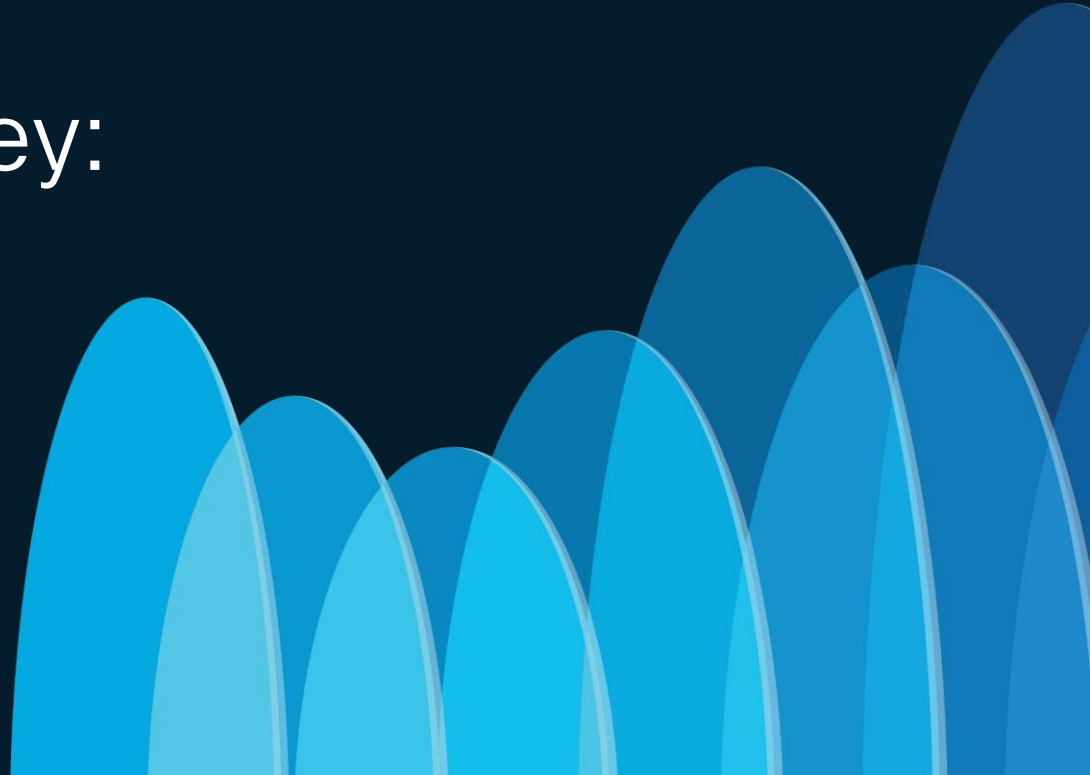
Analyst perspective on AIOps

“By 2023, 40% of DevOps teams will augment application and infrastructure monitoring tools with artificial intelligence for IT operations (AIOps) platform capabilities.” AIOps platforms are platforms that “utilize big data, modern machine learning and other advanced analytics technologies to directly and indirectly enhance IT operations functions with proactive, personal and dynamic insight” - Gartner

"Operational costs are too high and the velocity of business is too fast to continue running IT in a highly or mostly manual manner. Automation and data-driven remediation is no longer a luxury; it is a must. 40% of IT pros use AI for problem-solving. 75% of data leaders apply AI for automation and analytics"

- Forrester, State of AIOps

Easing the journey: Onboarding and Compliance



Onboarding

Onboarding Experience for cloud and on-prem customers

On-Prem customers:

- Customers can leverage the security cloud onboarding via Integration menu from on-prem FMC
- Alternatively, customers can on-board the on-prem FMC into CDO and start leveraging the cloud assist features.
- Customers need to accept and acknowledge the data collected before Starting to leverage the AI & cloud features.

Cloud customers:

- Before leveraging AI features, customers accept and ack is needed. Once done, customers can leverage AI features

Compliance : Handling Customer Data



Model Training

1. We do not utilize any Customer Data to train or finetune third party or Cisco-hosted models
2. We do not store any PII information or use it for model training
3. Where needed we use synthetic data for evaluating model behavior



Guardrails

1. We implement and update industry leading Guardrails to protect assistants against security attacks (Prompt Injections/poisoning)
2. We further protect Assistant requests from leaking any private Customer data to a model



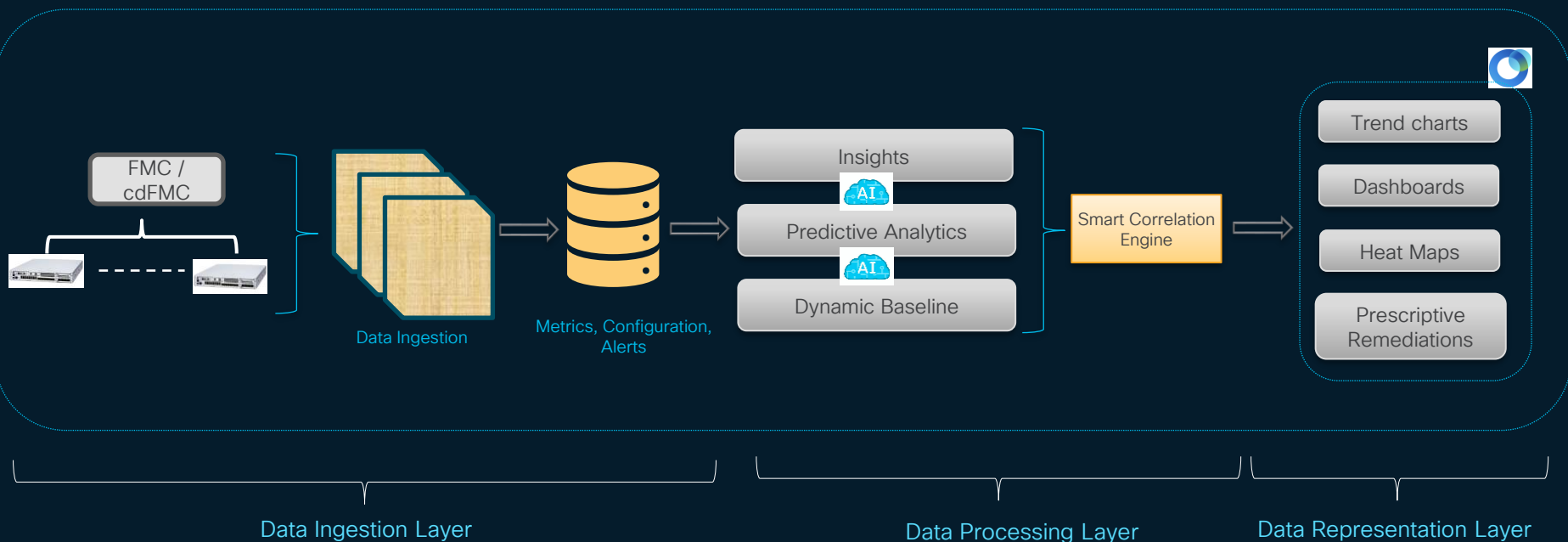
Data Privacy

1. We retain a Customer's conversations and feedback to responses in our systems only to improve the relevancy of future responses
2. Product data required for AI Assistants is colocated/hosted with the product's data

AI Ops Architecture: Sneak-peek



AIops - Data Flow Overview



Celebration time: Bonus Offering



Get Cisco Defense Orchestrator FREE for 1 year



Offer across Firewall (ASA& FTD) customer base includes:



Multicloud Defense
(max: 9,000 Gateway
Hours)



Security Analytics and
Logging
(Cloud logging 50Gb/day
with 90 days retention)



Cloud-delivered
Firewall Management
Center

Get Cisco Defense Orchestrator FREE for 1 year



Capabilities	Customer base		
	ASA Firewalls customer's using via CLI/CSM/ASDM	FTD Firewalls customer's using via FDM	FTD Firewalls customer's using via FMC
Multicloud Defense (max: 9,000 Gateway Hours)	■	■	■
Unified Event Viewer for easy monitoring & troubleshooting (50Gb/day with 90 days retention)	■	■	■
Manage firewalls of different form factors from the cloud	■	■	■
Migration path to FTD/cdFMC through CDO	■	■	■
Cisco managed upgrades, updates, and uptime	■	■	■
Share objects across hybrid and multi-cloud environments	■	■	■
Streamlines policy management across diverse security firewall offerings	■		
Auto-scales to any size environment		■	■
Cloud assist capabilities - AI Assistant, AI Ops, Policy optimizer & Analyzer (Future)		■	■
Early access to FMC features in cloud			■

For select customers with the following use cases (terms and conditions apply):

Offer available to first 500 customers



Boost efficiency, reduce
security risk – fill out the
form here to enroll

Cisco Defense Orchestrator



AI Ops for Secure Firewall Beta



Influence product design

Design research participants shape the look, feel, & functionality of new product features and offerings



Attention to Feedback

Beta customer bugs and enhancements receive high visibility & priority



Top notch communication

Private conference calls with product team



Training

Customers receive early training and experience with new features



Customer Support

Our feature experts will be on-hand and responsive to your issues

Sign-Up Now: <https://cs.co/aiops-beta-interest>

AI Ops for Secure Firewall dcloud Demo

Demos and Labs

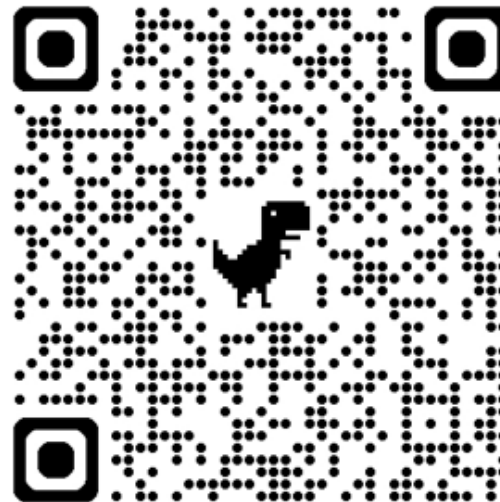


New!

AI Ops for Cisco Firewall

Minimize misconfigurations and downtime.
Simplify operations and Enhance security.
AI Ops enriches human judgments with *actionable* information, improves customer experience with *guided* remediation, and integrates with chatOps and ITSM tools to boost collaboration.

[Watch Video >](#)



https://dcloud-docs.cisco.com/c/r/dcloud-docs/sites/en_us/explore/ai.html#aiops-cisco-firewall/

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile 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 DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC