



SHIELD vzw

# Jarviss Heartbeat and Optimize services fueled by Palo Alto Networks Strata Cloud Manager

by Kevin Thys, Tomas Van Beek & Jo Vander Schueren



Cybersecurity

Networking

Cloud

Managed services

# About us

## Who are we?

+30 passionate trusted advisors in Cybersecurity, networking and managed services.

## What do we solve?

Problem of insufficient resources & knowledge in Cybersecurity & Networking.

## What is our vision?

Intelligent use of AI/ML technology & automation can reduce workloads & optimize resources.

## Where are we active?

- Belgium with offices in Ghent & Antwerp
- Netherlands with offices in Amsterdam

## Who are our customers?

Public and private midsize organizations in the Benelux with extensive experience in healthcare.

# Build resilience to manage incidents and avoid breaches

## Cybersecurity

Implementing 3 layers of defense to answer OT & IT cybersecurity challenges

## Networking

Building self-managed & end-user driven networks to create optimal experiences.

## Cloud Security

Extending your security posture in the cloud for applications & infrastructure.



**Managed Services**

JUNIPER  
NETWORKS

SentinelOne

VECTRA

infoblox

AVANAN  
A Check Point Company

paloalto  
NETWORKS

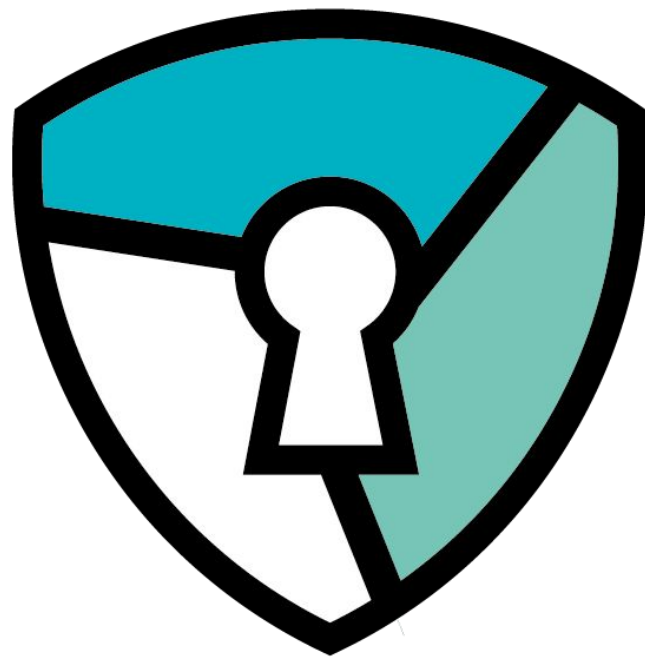
SILVERFORT

ATTACKIQ

ARMIS

f5

Blyott



**SHIELD** vzw

Framework agreement for  
**NEXTGEN/NETWORK FIREWALLS**



**JARVISS**®  
When Your OT & IT Security Get Personal



**paloalto**®  
NETWORKS



# Scope

## 1. Nextgen firewall platform based on Palo Alto Networks

- I. **Flexible platform:** branch, datacenter, segmentation, cloud, ...
- II. **Cloud delivered security services:** URL security, DNS security, Threat prevention, Saas, DLP, IOT, SDWAN, ...
- III. **Central (cloud) management**

## 2. Consultancy services

- I. Design & architecture
- II. Implementation & onboarding
- III. Security Control Baseline Testing (SCBT)
- IV. Certification training
- V. Project management

## 3. Support & managed services

- i. Basic
- ii. Advanced
- iii. Managed

# Support services for NGFW

## 1. Basic

- I. Builds upon the vendor support
- II. Includes a pay as you go 8x5 Jarvis helpdesk
- III. Only recommended if extensive Palo Alto Networks knowledge is present

## 2. Advanced

- I. Direct Jarvis support with fix price
- II. Different SLA's possible (NBD, 8x5, 24x7)
- III. Different scope's possible (support, best practice checks, changes, ...)

## 3. Managed


- I. Full managed by Jarvis in a fix price model
- II. Jarvis takes full responsibility
- III. Different SLA's possible (NBD, 8x5, 24x7)

# Get in touch!

 <https://www.shield-vzw.be>

 <https://www.jarviss.be>

 [info@jarviss.be](mailto:info@jarviss.be)

 +32 (0)9 394 99 11

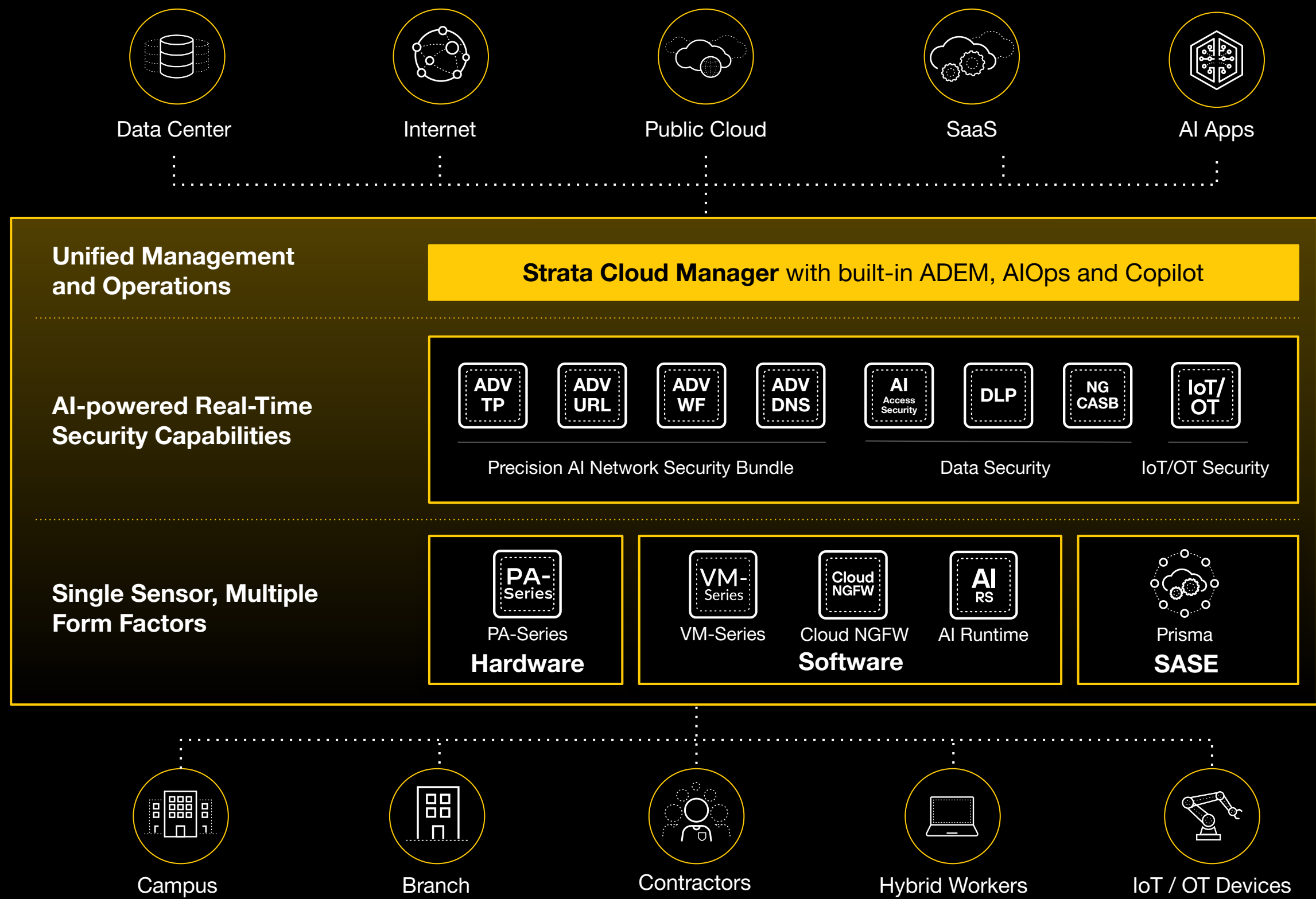
 <https://www.linkedin.com/company/jarviss/>



**LOOKING FORWARD TO MEET YOU!**

# Strata Network Security Platform

Simple & unified. Prevents threats in real time everywhere.



## Unified Management and Operations

Write policy once and enforce everywhere. Proactively strengthen security and prevent outages using Generative AI.

## AI-powered Real-Time Security

Prevent threats in real time using ML and Deep Learning applied to rich data from 70,000+ customers.

## Single Sensor, Multiple Form Factors

Simplify security with consistent operating system. Protect every location with a fitting form factor.



# The Industry's First AI-powered Unified Management and Operations Solution



# Demo

# Jarviss Services

## Heartbeat

Analyse use of investment made. Recommendations regards to your environment.

## Optimize

Pre planned days to perform tasks from Heartbeat.

## Credits

On demand request for consultancy.

# Heartbeat

- Best Practice check
- New feature mapping
- Recommendations for upgrades
- Q&A about a topic
- Strata Cloud Manager
  - Feature adoption
  - Policy analyzer
  - Device alerts



# Optimize

- Pre-scheduled days every x time
- Jarviss plans topics to address
- Next Heartbeat => improved outcome.

# Credits

- Customer initiated
- Project based approach: sales & planning process.
- SoW



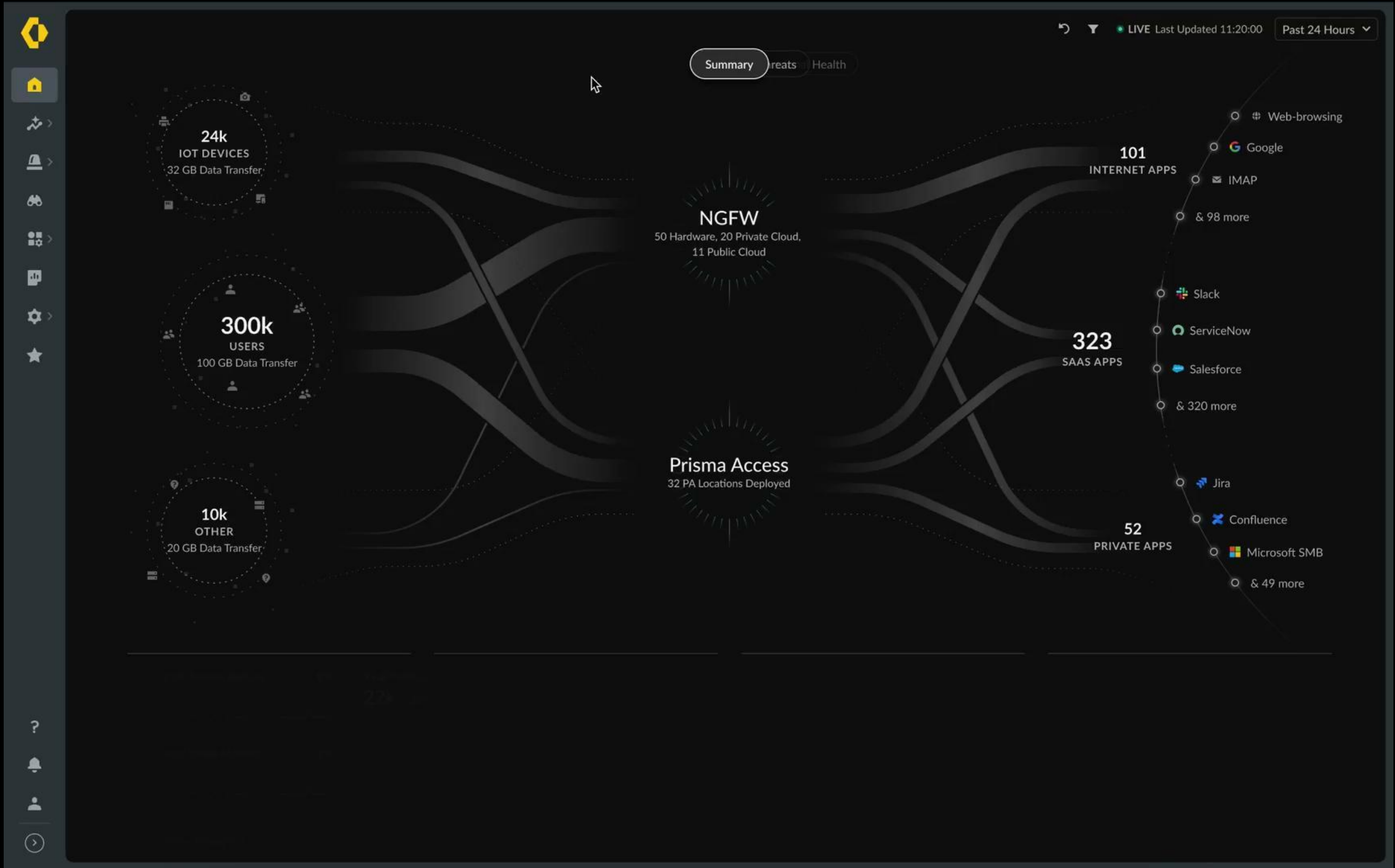
SHIELD vzw

# Thank you

by Kevin Thys, Tomas Van Beek & Jo Vander Schueren

# Strata Network Security Platform

## Strata Cloud Manager Command Center





# Unified management and operations for your entire network security estate



## STRATA™ CLOUD MANAGER

BY PALO ALTO NETWORKS

### AI-Powered Zero-Trust Management and Operations



Predict and Prevent  
Network Disruptions



Strengthen Security  
in Real-Time



Comprehensive Management for All  
Deployments in a Single UI

Cloud-Delivered  
Security Services



Hardware Firewalls

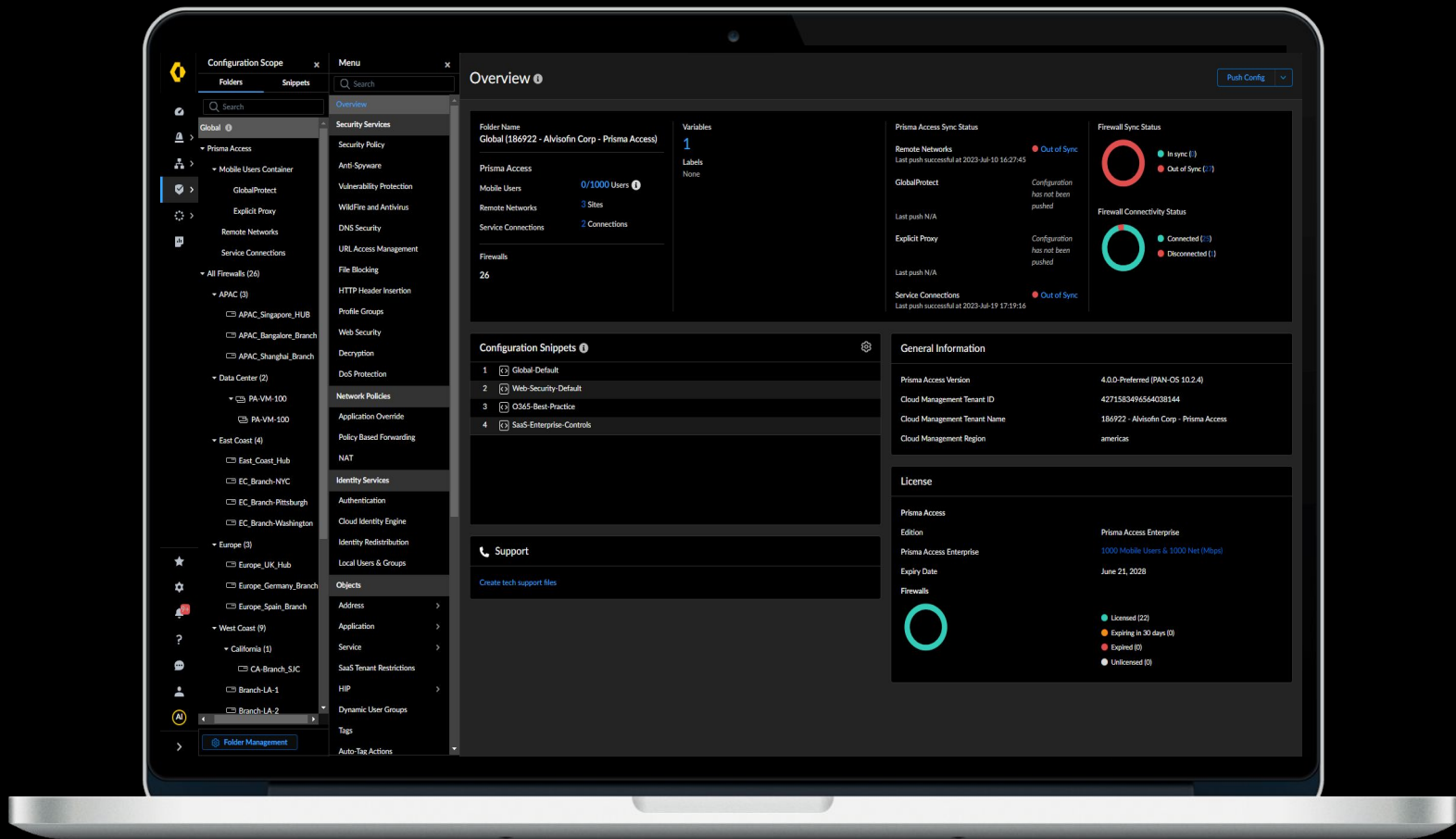


Software Firewalls  
Cloud NGFW



SASE

# Comprehensive Management for All Deployments in a Single UI

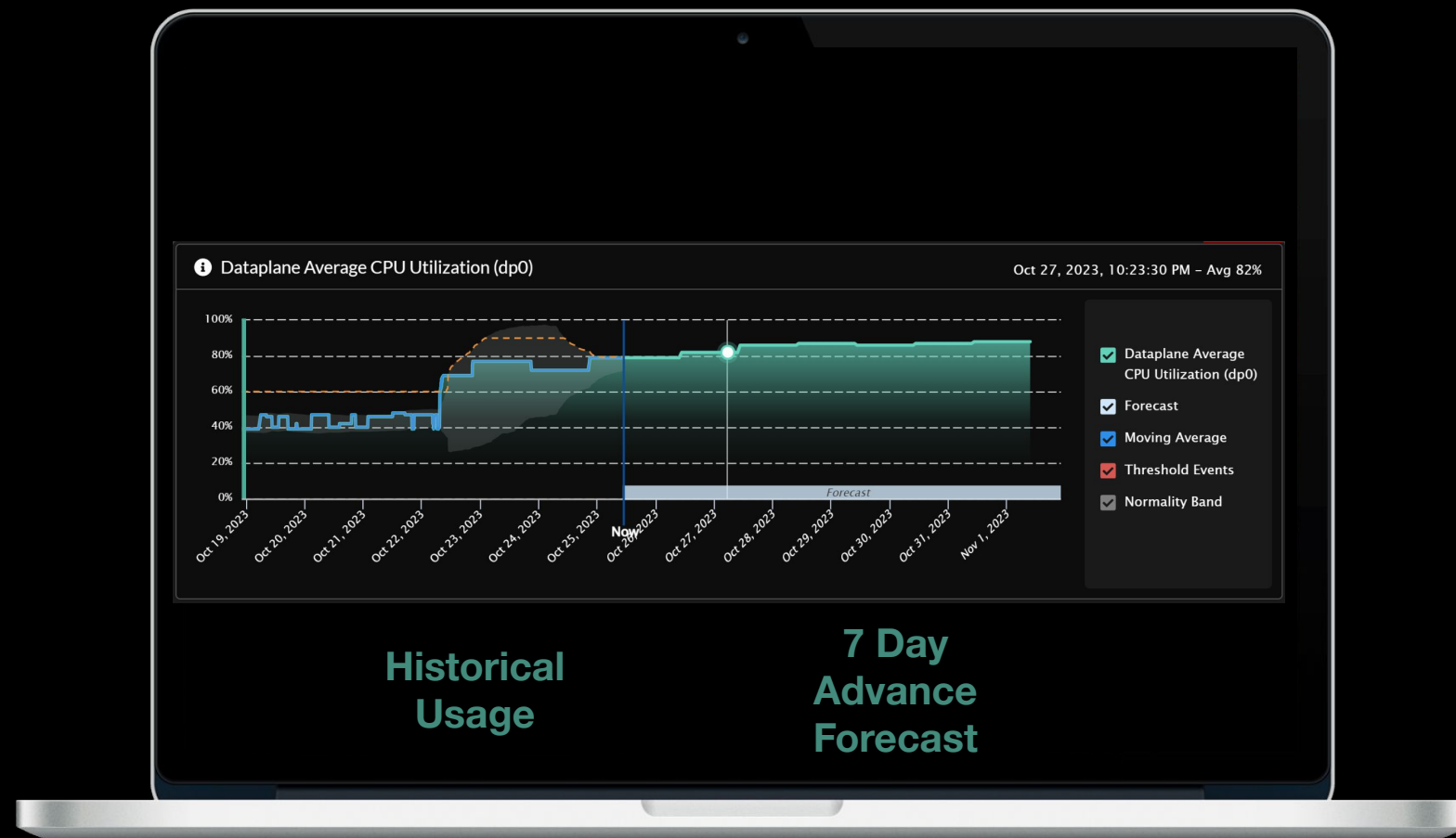


**1 Consistent Configuration**  
Ensure consistent security posture across all deployments with flexible configuration organization. Achieve a \$1.5M increase in ROI through a unified platform.

**2 Efficient Configuration Workflows**  
Improve productivity and reduce workload with streamlined use-case driven workflows

**3 Centralized Troubleshooting**  
Reduce operational burden by issuing one-click operational commands from a centralized troubleshooting UI

# Predict & Prevent Operational Disruptions



1

## Comprehensive Observability

Eliminate blind spots and identify problems with unified visibility into all users, apps, infrastructure and network connectivity

2

## Proactive Health

Prevent potential disruptions up to 7 days in advance with ML-powered actionable insights

3

## Automated Resolutions

Reduce resolution time with remediation playbooks and automatic support tickets. Each month, it processes 77B metrics, shares 715K+ misconfigurations and 17K+ firewall health issues for resolution

# Strengthen Security in Real-Time

1

## Maximize Security

Maximize the ROI from security investments by understanding unused or underutilized security capabilities and turn them on with best practices

2

## Optimize Configuration

Remediate misconfigurations with ML-powered analysis to optimize and secure existing firewall configurations. Strata Cloud Manager users witness a substantial improvement in their security posture within the first 90 days.

3

## Write Secure Configuration in Real-Time

Proactively improve security posture with best practices and Infosec policy enforcement at configuration time, without the need for review





# The Industry's First AI-powered Unified Management and Operations Solution



# Gain Complete Visibility Across Your Enterprise



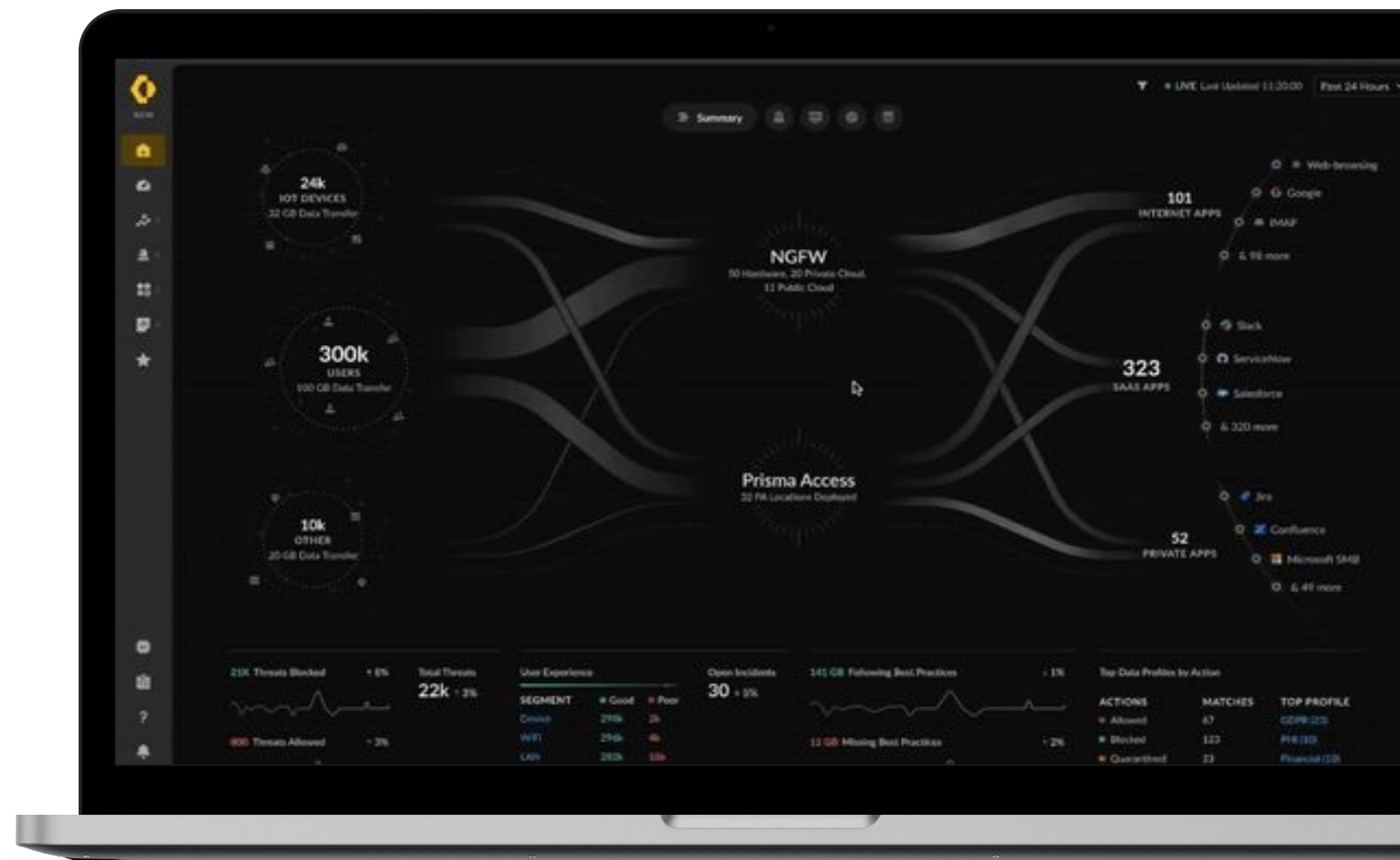
Get a **comprehensive view** of users, devices, applications, and threats to assess how everything is protected in your enterprise



Surface insights into how your apps and users are affected by **threats in real-time and take action**



Understand **end-to-end user experience** across branch sites, applications, and IT infrastructure, from a single dashboard

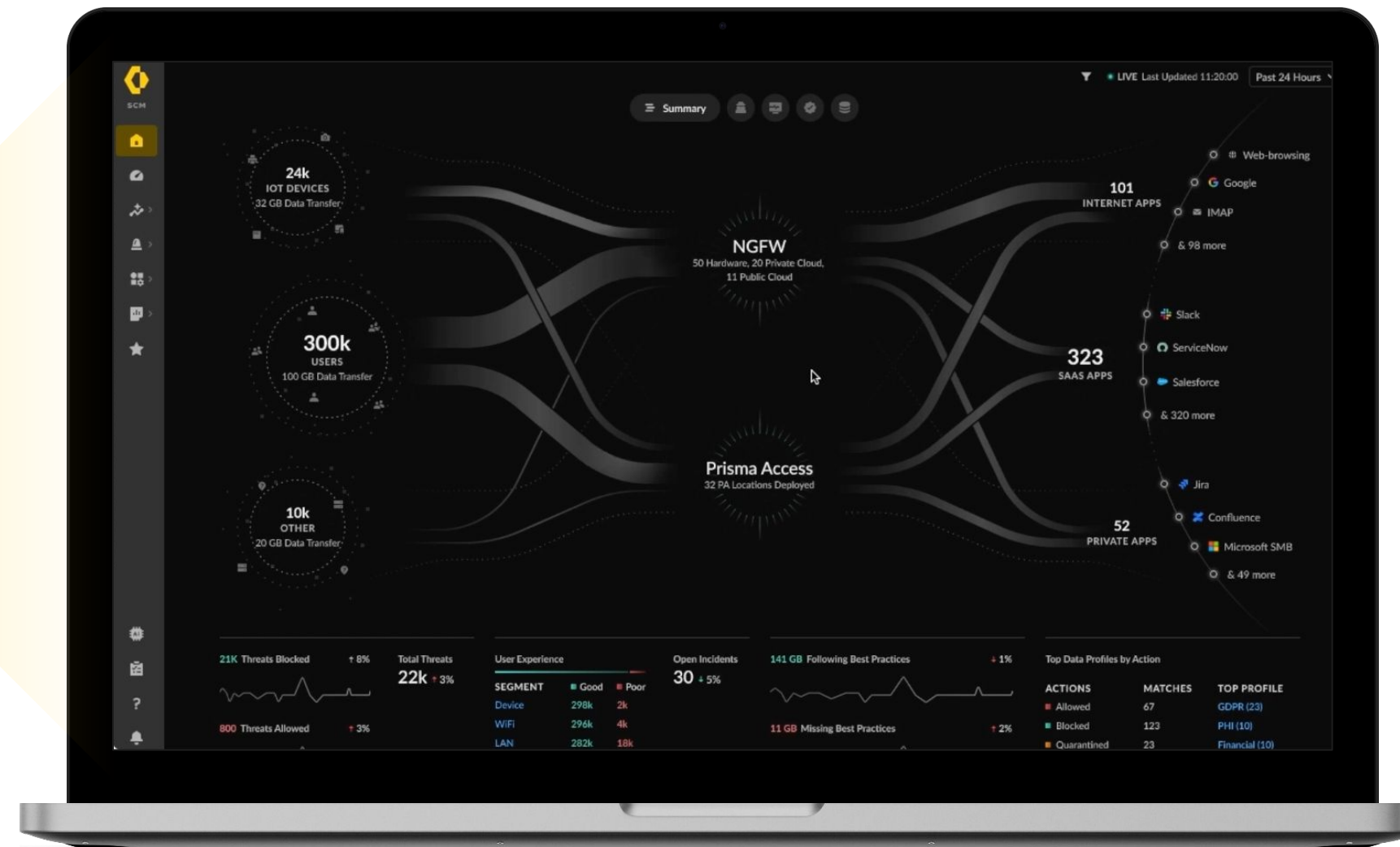
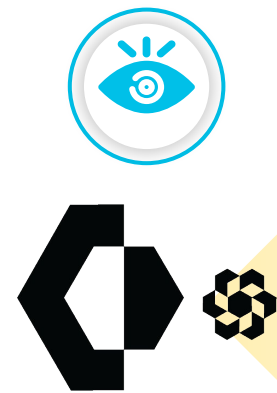


# Comprehensive View of Users, Devices, Applications, and Threats in Your Network

What are the top apps my users are using and are those apps approved?



**Emily**  
NetSec Admin



1

Emily has users and apps everywhere that are being protected by both NGFW and SASE

2

Emily wants to make sure all users are accessing approved apps only

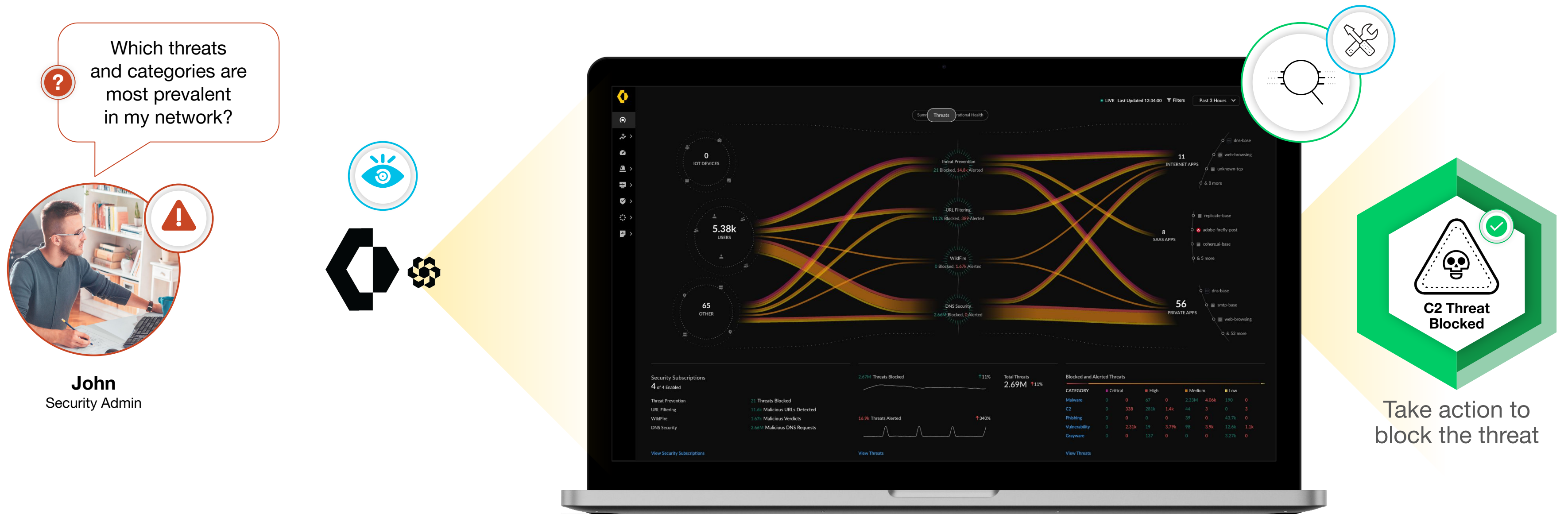
3

Drilling down to see the top accessed apps, Emily can quickly see how many are sanctioned and unsanctioned across her infrastructure

4

Emily takes action on the unsanctioned apps to further protect the enterprise from users who are accessing the apps

# Get Insights into Threats in Real-Time and Take Action



1

John wants to see which threats are most prevalent and which users are bringing the most threats in his network

2

John navigates to the "Command Center" threat view and sees a high number of C2 threats

3

John drills down to find the source of the threats and analyzes the guided suggestions on how to block those threats

4

Take action to block those threats



# Understand End-to-end User Experience from a Single Dashboard



1

Emily notices that a lot of remote users on her network are having internet issues

2

Emily navigates to the NOC view in Strata Cloud Manager to get visibility for all her users everywhere

3

Emily quickly sees that 159 remote and branch site users in California are having a degraded experience

4

Emily can further drill down to the segment that is causing the issue in the branch site, user, app, and IT infrastructure



# Enable Simple and Consistent Network Security Lifecycle Management



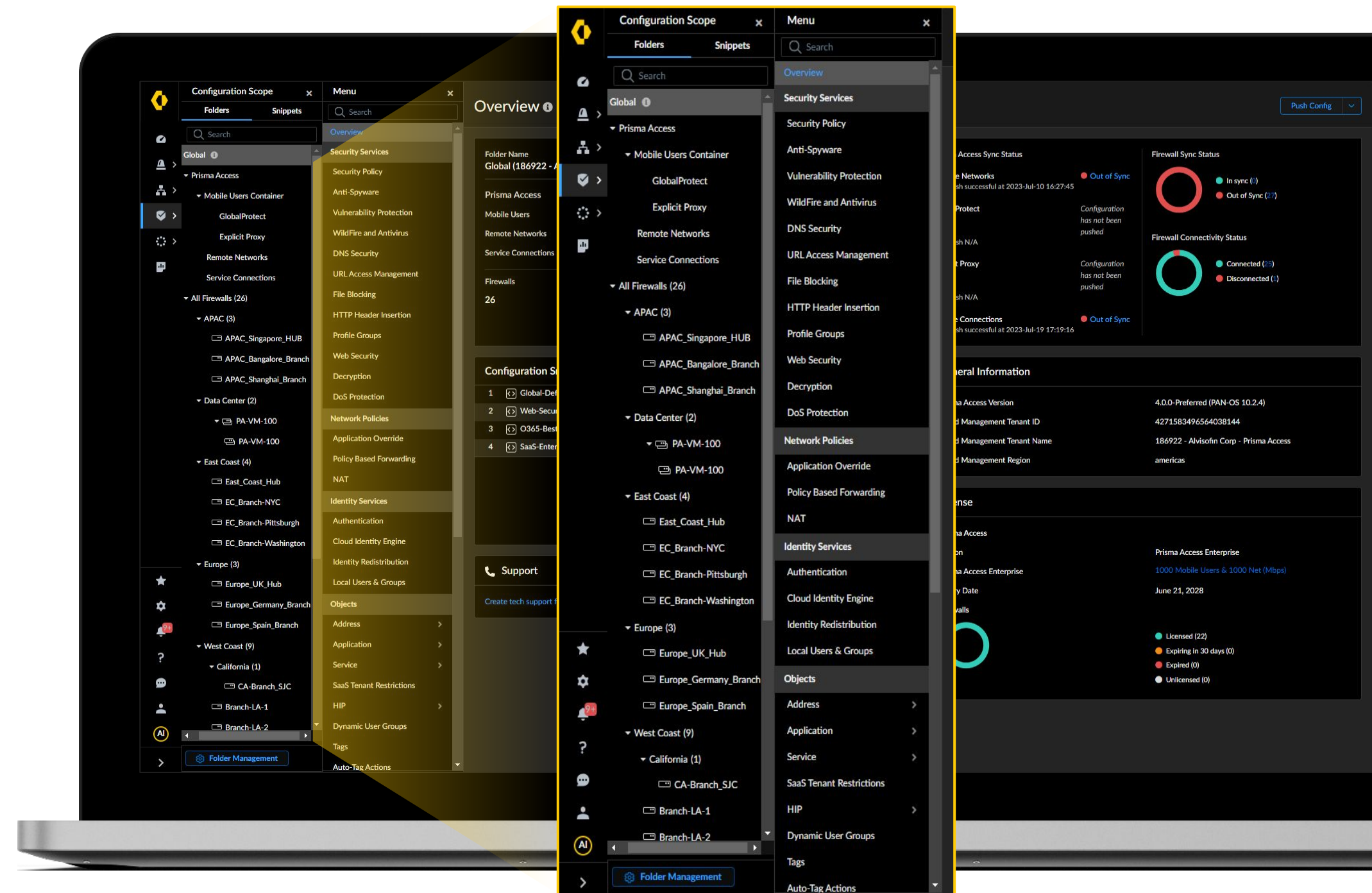
Simplify onboarding (**zero touch provisioning**), operations (software upgrade and config operations), and device refresh



**Achieve consistent security configuration** and policies throughout your network estate combined with Palo Alto Networks best practices



**Scale efficiently and reduce network configuration complexity** with predefined workflows (Auto VPN for hub-and-spoke connectivity), and integrations



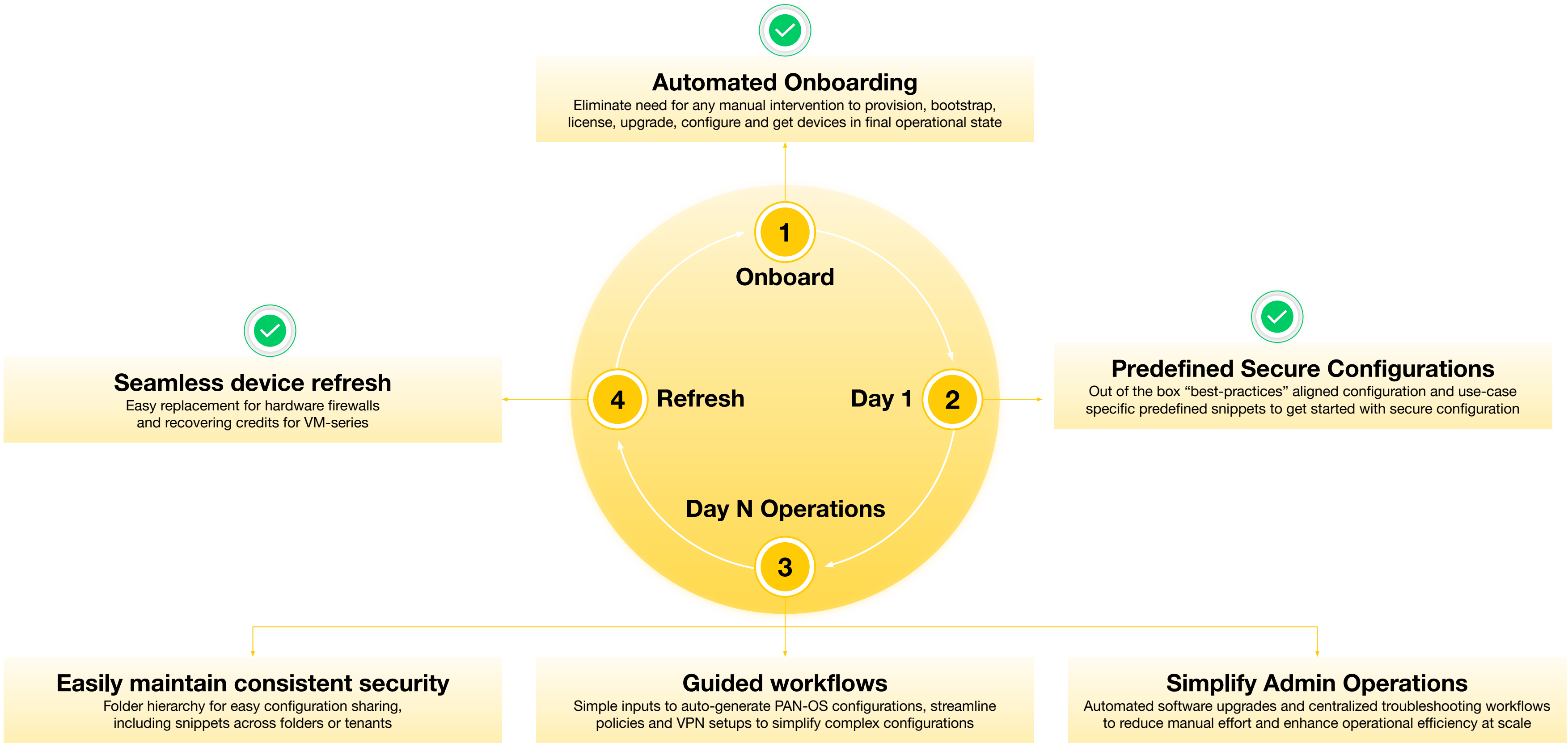
72%

**Reduced configuration and deployment time with automation**

(as per customer feedback)

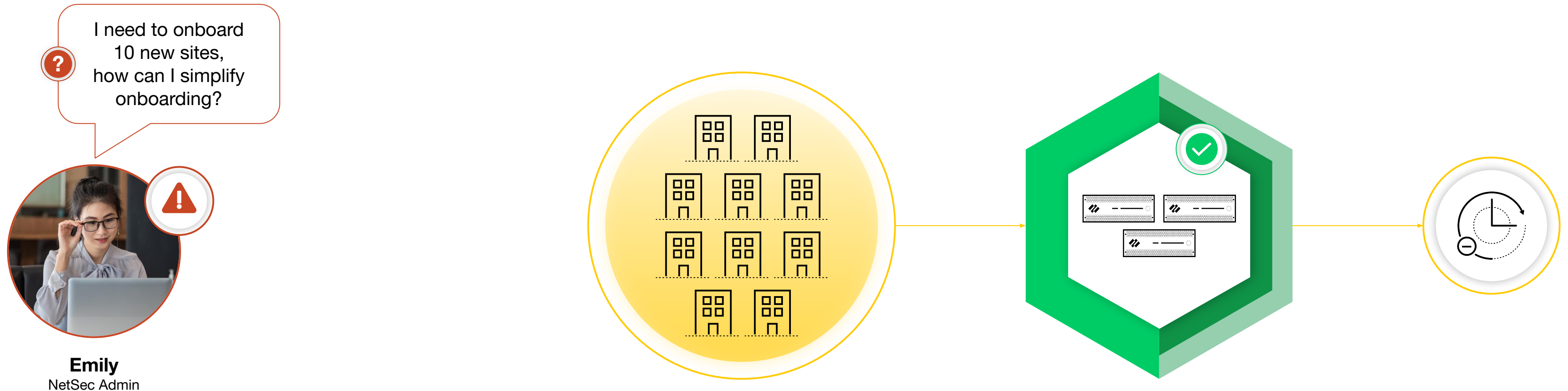
# Simplify Network Security Lifecycle Management

See detailed slide [here](#)



# Efficient Onboarding with Zero Touch Provisioning

Automate onboarding and day-0 workflows for increased productivity



1

10 new branch offices are opening and Emily needs to set up the new deployments

2

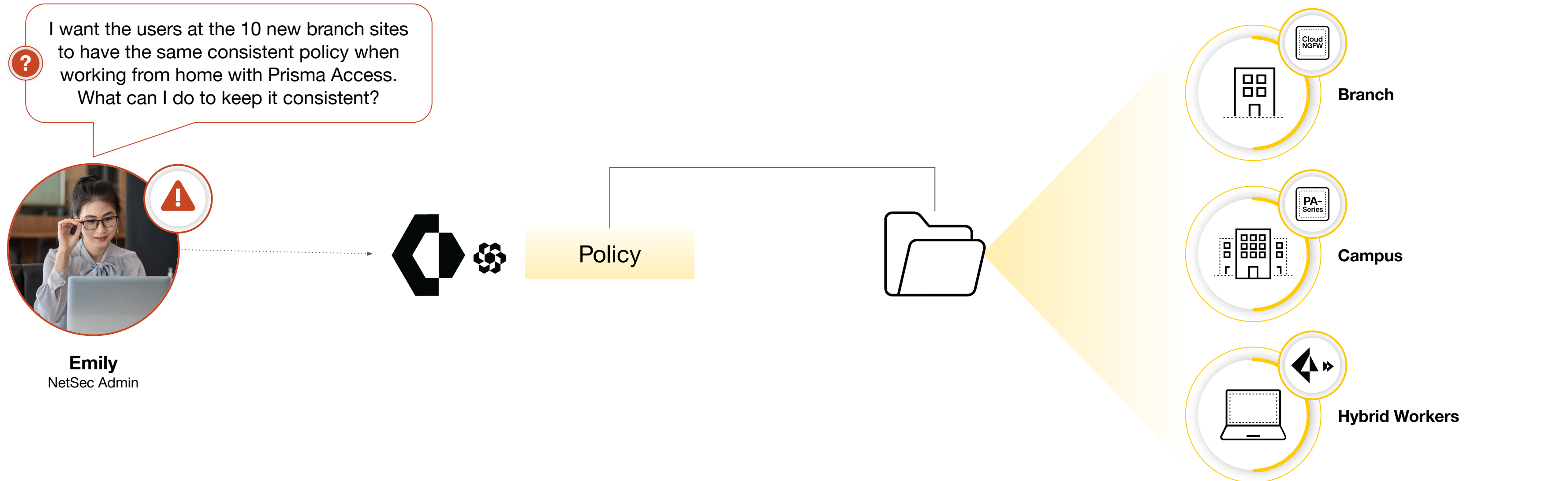
With Strata Cloud Manager, Emily uses zero touch provisioning to get the firewalls configured and automate onboarding and licensing

3

Emily remotely onboards the new sites without IT expertise in the branches while eliminating misconfigurations

# Achieve Consistent Security Configuration

Share configuration across your entire network estate



1

2

3

Emily needs to update a policy for users working from the office and working from home

With Strata Cloud Manager, Emily updates a common configuration and shares it across her entire network estate

Emily streamlines security by applying consistent policies across NGFW and SASE, **cutting operational costs by up to 50%** with an automated, unified management system

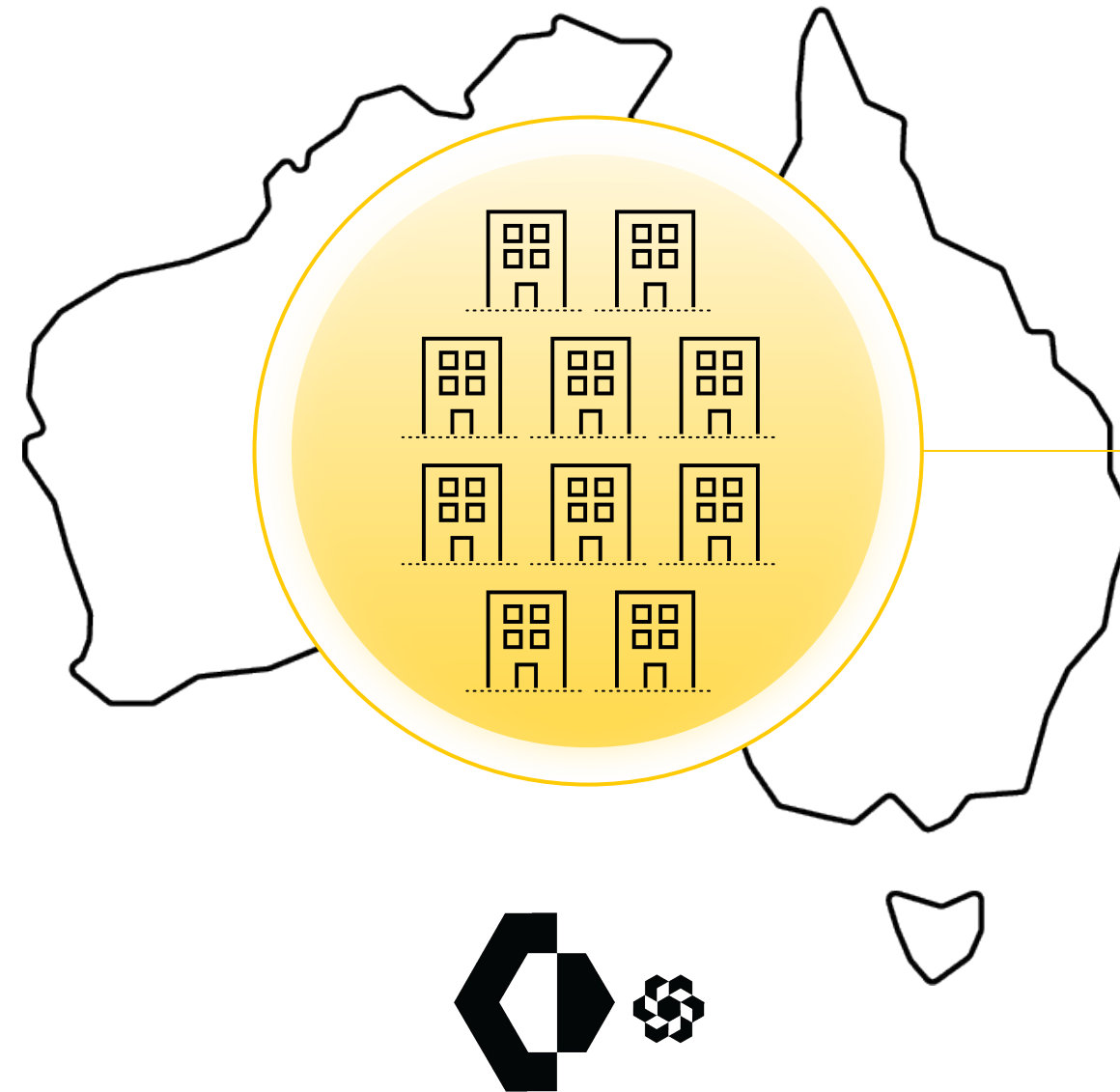


# Scale Efficiently and Reduce Network Configuration Complexity

? I need to securely connect 10 branch sites in a new region to my datacenter, where do I start?



**Emily**  
NetSec Admin



1

Emily needs to securely connect 10 branch sites in Australia to the HQ datacenter

2

Emily uses the guided workflow and provides simple inputs to generate all configuration workflows required to connect the 10 branch sites

3

Emily efficiently scales her organization and securely connects the branch sites in **72% less time** compared to traditional configurations methods with automation\*

\*Based on real customer use case data



# Simplify Network Security Lifecycle Management

Onboarding

## **Automated Onboarding**

Auto provisioning, bootstrap, license, upgrade, configure and get devices in final operational state

Day 1

## **Minimize Misconfigurations**

Out of the box “best-practices”, use-case specific predefined snippets

Day N

## **Easily Maintain Consistent Security**

Simple Folder hierarchy with snippets across folders or tenants, variable support for environment differences within a common config

Day N

## **Guided Workflows**

Simple inputs to auto-generate PAN-OS configurations, large-scale VPN deployments

Day N

## **Simplify Admin Operations**

Automated software upgrade orchestration, centralized troubleshooting workflows

Refresh

## **Seamless Device Refresh**

Easy replacement for hardware firewalls and recovering credits for VM-series

# Strengthen Security Posture in Real-Time



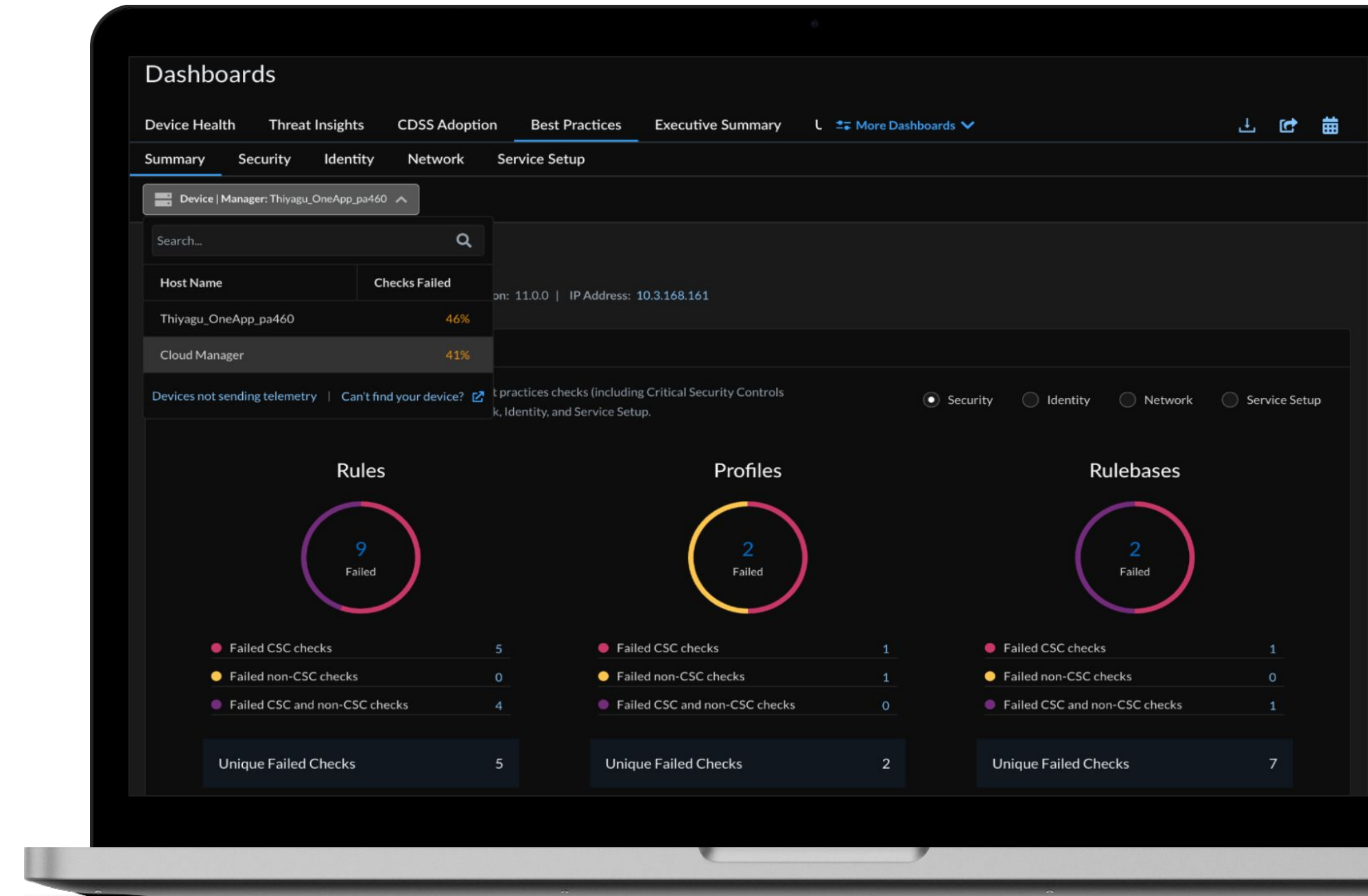
Write new and existing policies that align with enterprise **best practices in real-time**



Continuously **detect and remediate policy anomalies** ensuring zero trust posture



Ensure **continuous compliance** across standard industry frameworks



Every Month

1,924,143 Misconfigurations shared for resolution

# Write Secure Configuration in Real-Time

Implement security policies that comply with best practices at the time of configuration

How do I make sure I am writing policies without misconfigurations?



**Risky Security Policy**

1

Emily is writing a new policy without knowledge of best practices and her organization's frameworks

**Configuration Analysis**  
Last checked: 2023-Oct-13 16:41:12 EDT

6 out of 9 Security Checks Passed

Resolving all checks keeps your policy rules precise and effective.

**Required**

- Source Address must be in CIDR 10.10.10.0/24
- The 'Service' is not configured in a rule with the 'Allow' action
- The 'Source' and 'Destination' address and zone are set to 'Any'
- Server Response Inspection in the allow rule is disabled
- A Security policy rule with the Action set to Allow does not specify applications (App-IDs)
- URL Profile must be "best practice" for traffic destined to the Internet

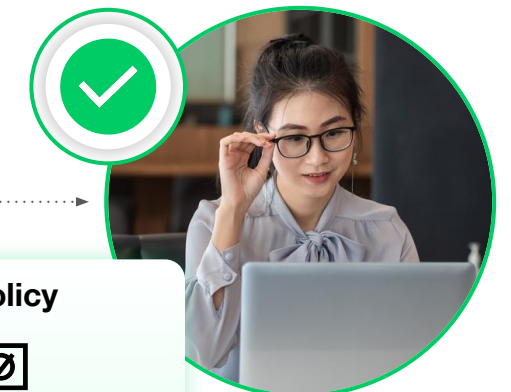
**Recommended**

- Logging is enabled at session start
- The rule Description is not populated
- Log Forwarding is not configured in the security rule

2

Strata Cloud Manager enables real-time policy enforcements utilizing best practices

Write a new security policy with best practice guardrails



**Secure Policy**

3

Emily can now ensure that the security policy committed to her deployment is free from misconfigurations and complies with best practices

# Detect and Remediate Shadow Policies in Your Environment

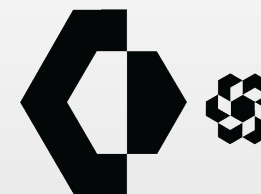
Get rid of risky security policies to reduce your attack surface



## Detect and Remediate Policy anomalies

- ✓ Shadow and redundant policies
- ✓ Overly permissive rules
- ✓ Unused rules and objects
- ✓ Unhit rules

Automatically detect gaps in configuration



Data Center



Legal Application

1

Emily gets an alert that Joe in Marketing has access to legal apps

2

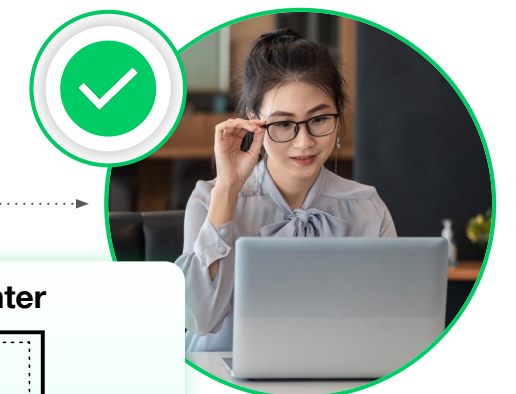
Emily can easily identify ineffective security policy within the configuration interface

3

Emily receives safe guaranteed recommendations to remove anomalies

4

Emily can now ensure that Joe in Marketing does not have access to legal apps



Data Center



Legal Application



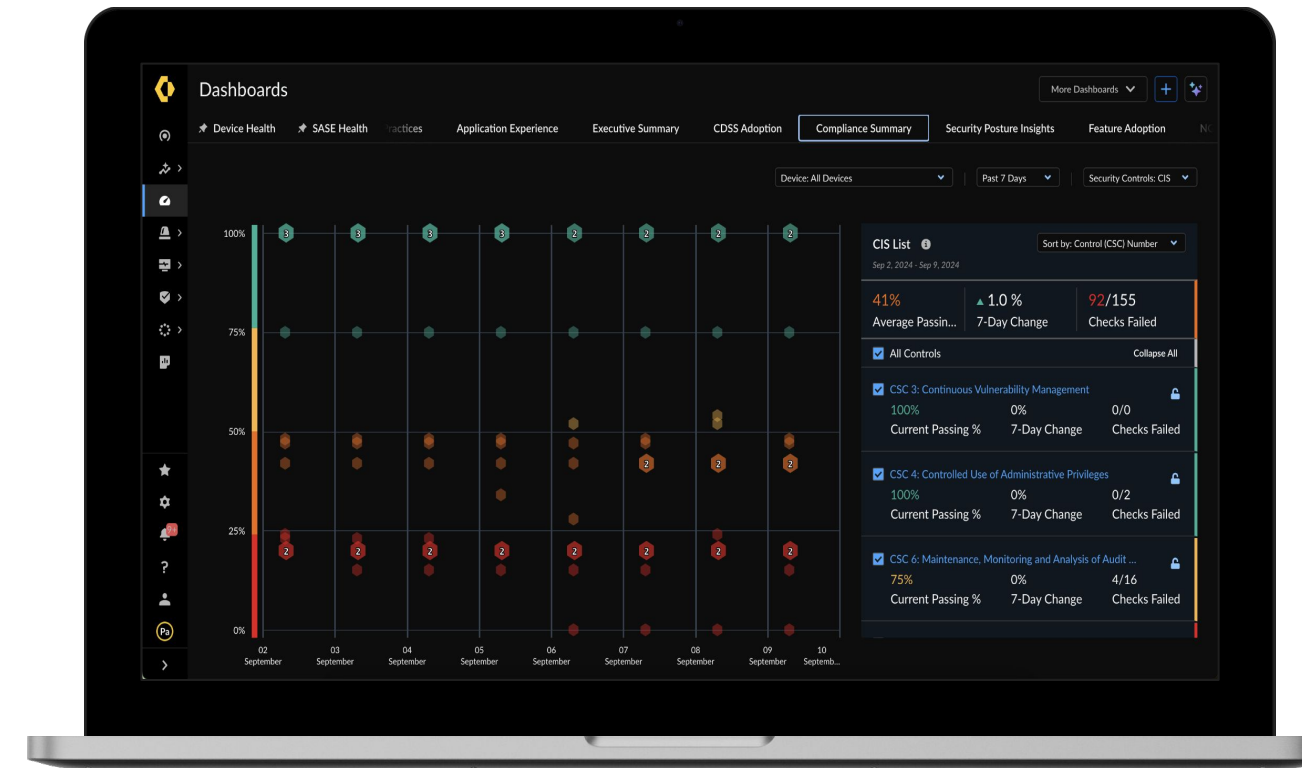
# Ensure Continuous Compliance with Industry Frameworks

Check against NIST, CIS, PCI-DSS\*

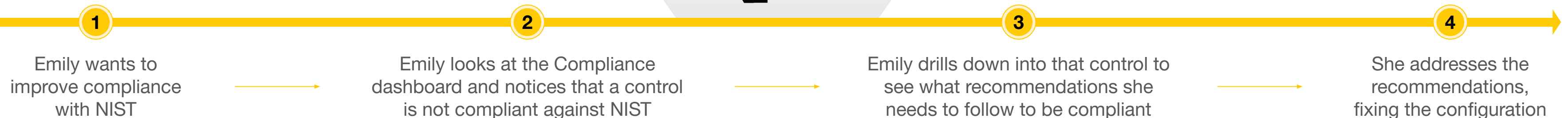
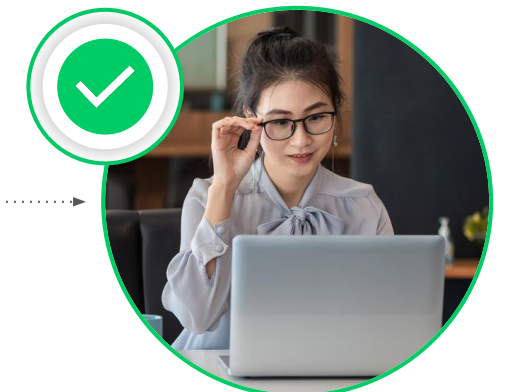
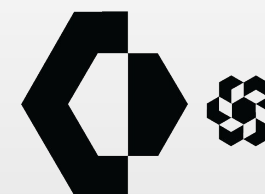
How do I ensure I am compliant against my industry best practice frameworks?



**Emily**  
NetSec Admin



Comprehensive view of your deployment compliance against regulatory compliance frameworks



\*PCI-DSS compliance framework coming soon



# Strengthen Security Posture

Key scenarios where alerts are generated

## Palo Alto Networks Defined Best Practices

Decryption, continuous app traffic inspection, authentication, etc

## Shadows & Redundancies

Prevent unintended allows exposing security risks and unintended denies causing business disruptions

## Intent-Based Policy Analysis

Clean up unused objects and security rules to strengthen security posture and firewall performance

## Zero Trust Policy

Optimize policies based on actual traffic logs to adhere to zero trust principles of least privileges

## Regulatory Compliance

Stay compliant with NIST, PCI DSS, CISv8, CRI, etc. frameworks and build organization specific Infosec compliance frameworks

# Optimize Network Operations and User Experience



**Proactively predict and prevent** network infrastructure health issues



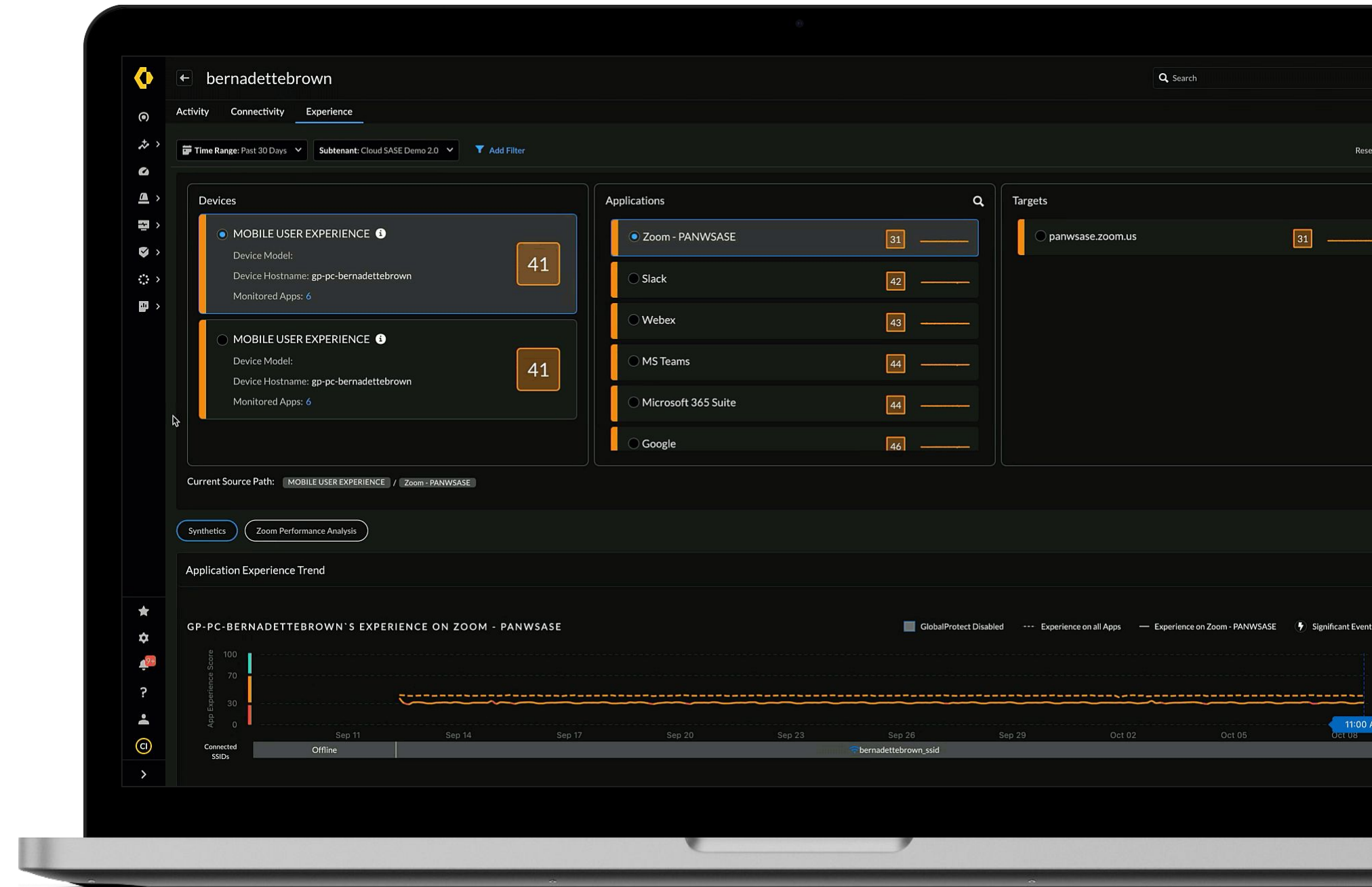
Detect, diagnose and remediate existing operational health issues (**authentication issues, CVE vulnerabilities**)



Ensure optimal **end-user application experience**



**One-click centralized troubleshooting** to reduce operational burden



**Every Month**

**635,000** Firewall health issues shared for resolution

# Proactively Prevent Disruptions and Quickly Remediate

Forecast disruptions up to 30 days in advance



### 3. Recommendations

Take recommended action to fix your issue.

#### Recommendations

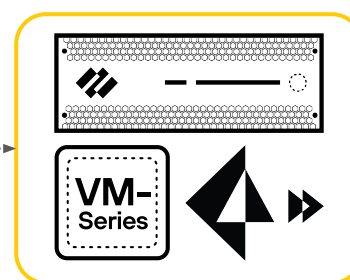
2 STEPS

Follow these steps

- 1 Your CPU is high because of SSL application. You can temporarily disable SSL decryption. Please click [Here](#) to learn more about how to temporarily disable SSL decryption.
  - 1.1 The SSL traffic, if not decrypted, is offloaded and thus shouldn't be the main contributor of the high usage of dataplane resources if the total number of sessions received on the firewall are within the limit of what the platform supports. In that case, it is recommended to investigate the other high usage applications.
  - 1.2 If SSL traffic is getting decrypted on the firewall during the time of high data plane CPU, check if the value in the output of:
 

```
> show session all filter ssl-decrypt yes count yes
```

 is at any point exceeding maximal concurrent decryption sessions of the platform. If so consider either changing your firewall config to reduce the amount of decrypted traffic by creating a decryption exclusion rule for the traffic exempt from decryption or plan to upgrade your firewall to a higher capacity platform
- 2 Your firewall data plane CPU is high because of some interfaces. Please refer to [How to mitigate High DP CPU issue due to an increase in an interface counter](#) for more details.



ML-Powered  
Predictions

Strata Cloud  
Manager



Forecasts high firewall  
computing in the next 7 days



Service connection will  
exceed capacity in 30 days

1

New users added due  
to company expansion

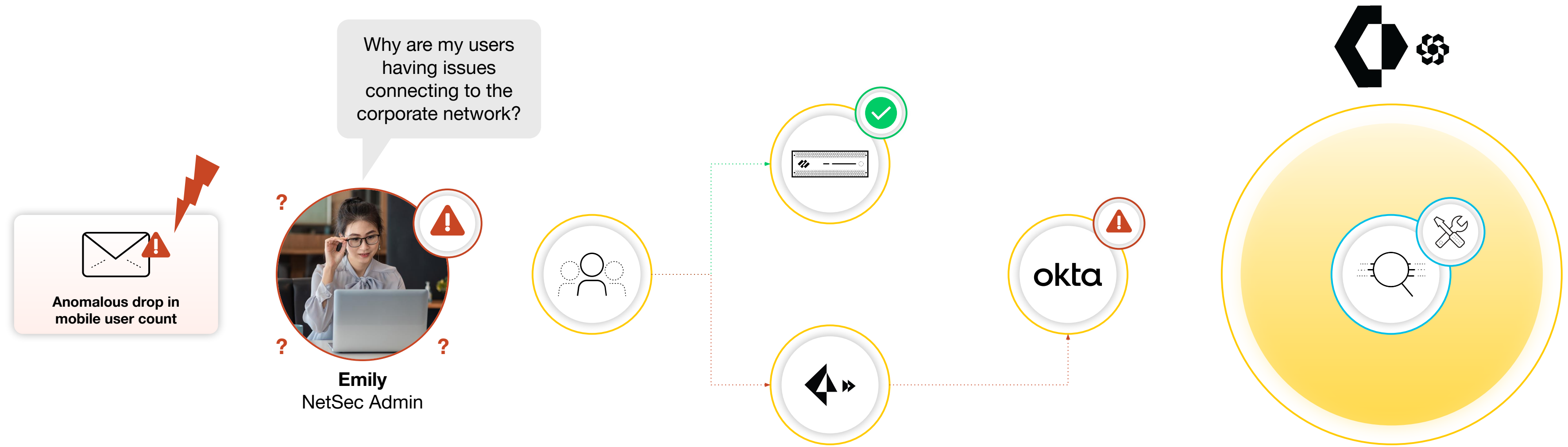
2

Emily gets an alert for projected high processing activity in the next 7  
days and for service connection exceeding capacity in the next 30 days.

3

Emily quickly identifies the root cause and  
takes the appropriate remediation steps

# Resolve Authentication Issues for All Users Anywhere within Minutes



1

2

3

4

Emily is alerted about a large drop in mobile users on her network

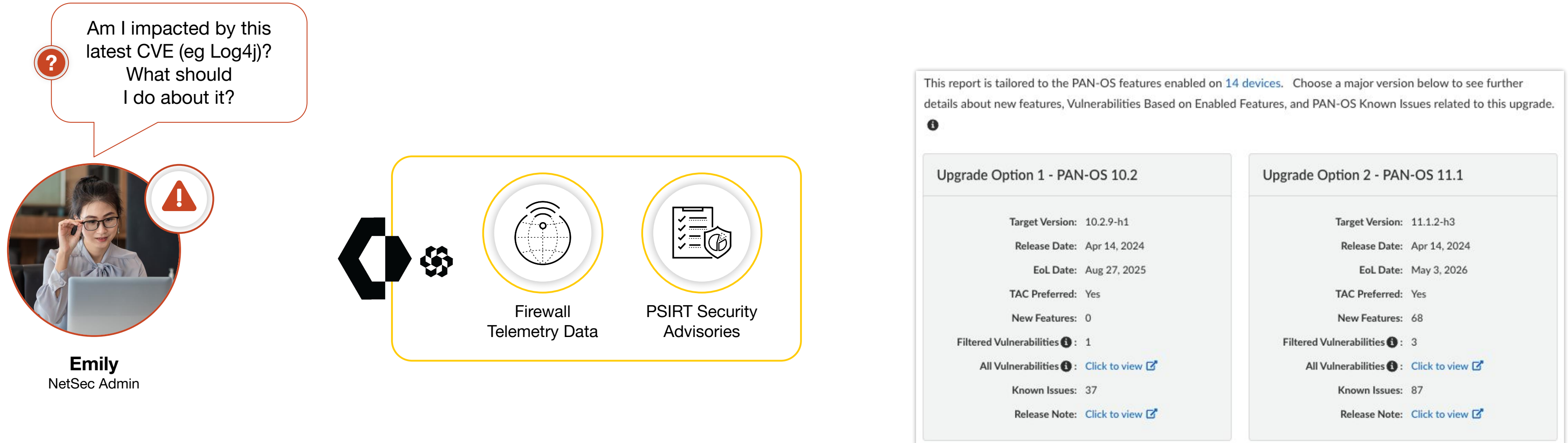
Emily clicks the alert and see that mobile users are not being able to connect to the corporate network due to authentication issues

Emily can quickly investigate the cause and impact of the issue along with actionable remediation

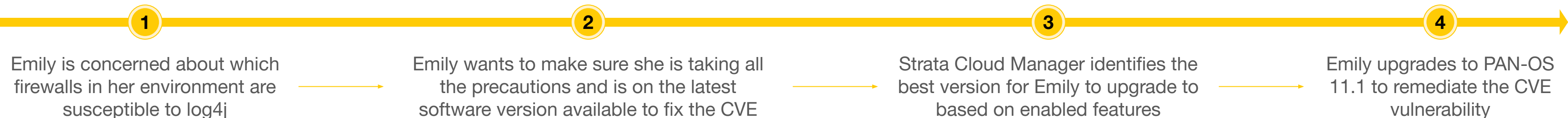
Emily is able to proactively resolve authentication failures before her users complain



# Software Upgrade Recommendations and Orchestration

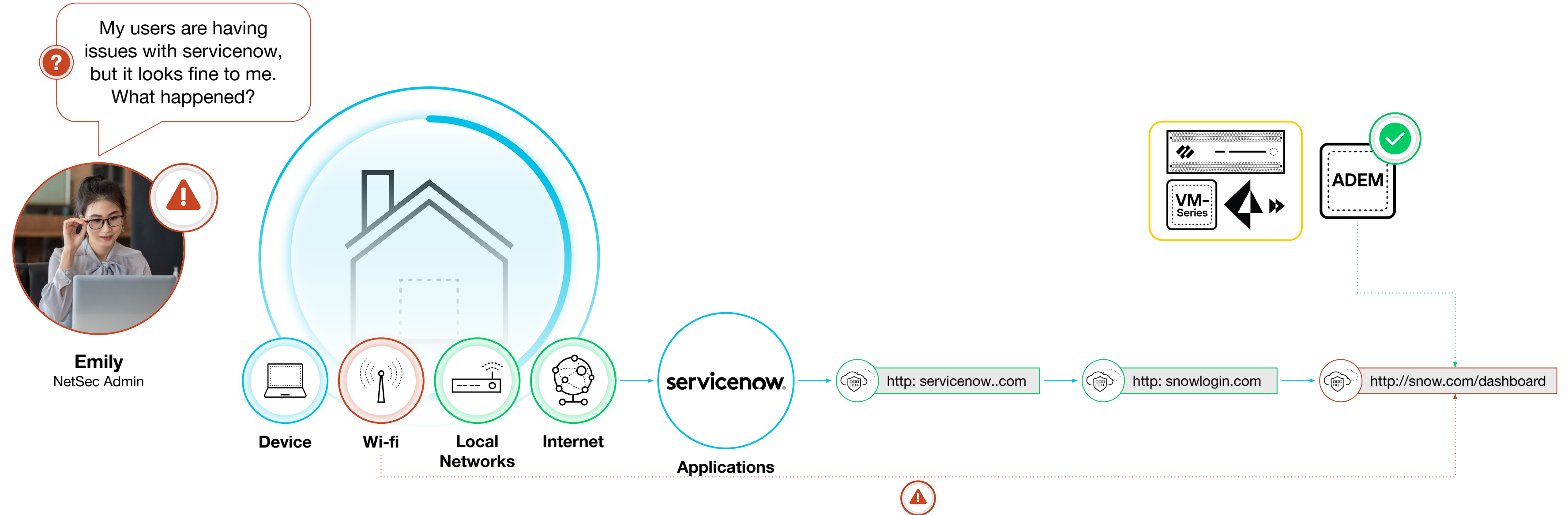


Upgrade to Software Version X to mitigate the CVE personalized to your configurations



# Ensure Optimal End-User Application Experience

## Across NGFW and SASE



1

Emily receives an IT ticket from a user experiencing issues while accessing servicenow from home

2

With ADEM in Strata Cloud Manager, Emily can pinpoint the exact app transaction causing the issue and identify poor WiFi as the root cause.

3

Emily resolves the user issue in **6 playbook steps** compared to an average of **26 steps**, reducing **MTTR by ~77%**

\*Availability on NGFW coming soon

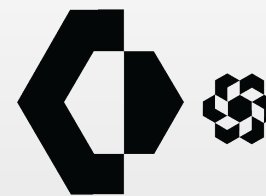
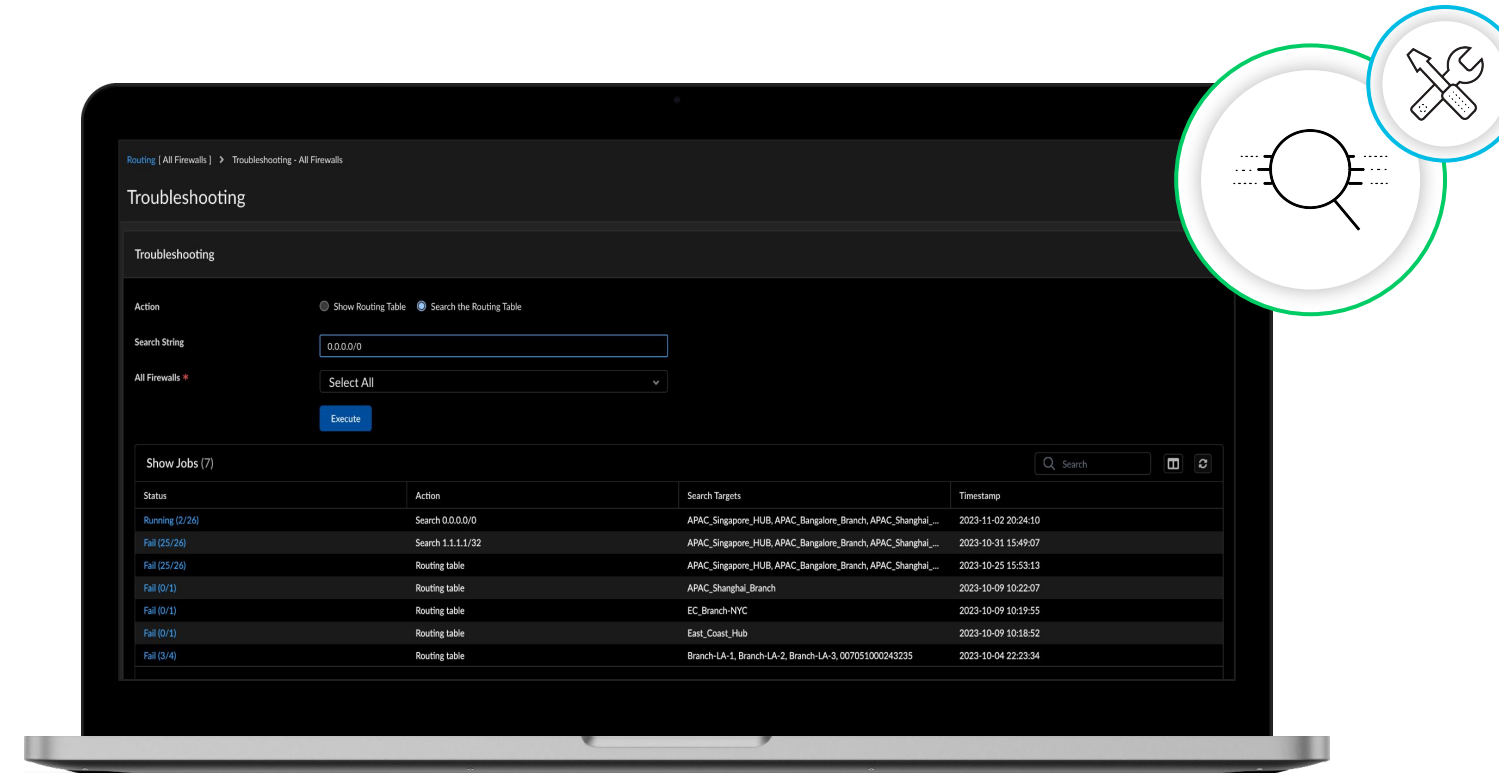
# One-click centralized troubleshooting to reduce operational burden



I just deployed a new service to the 10 branch sites, did my firewalls receive the new routing update?



**Emily**  
NetSec Admin



1

Emily just deployed a new service and wants to verify whether routing\* to that service is available on all branch sites

2

Using Strata Cloud Manager, Emily leverages the troubleshooting workflow to perform a one-click check on the routing tables across all firewalls

3

Emily saves time and effort troubleshooting in one single interface for the entire deployment

\*See [here](#) for all troubleshooting workflows

# Proactively Resolve Network Disruptions

Key categories where alerts are generated

## Device

System resources (CPU, memory, disk), hardware, management (license, certificates)

## Network & Traffic

IPSec VPN, Routing, tunnel/interface performance (latency), bandwidth utilization, ISP degradation

## Software Issues

End-of-life, end-of-sale, CVEs, known vulnerabilities

## Security & Cloud Services Health

Strata Logging Service, Cloud Identity Engine, Cloud Delivered Security Services

## Application

Poor application experience, layer-7 services

## Endpoint Agent

GlobalProtect client health, endpoint performance



# Instant Knowledge at Your Fingertips with Strata Copilot

The ultimate AI assistant for network security augmented with ML, workflows, and automation



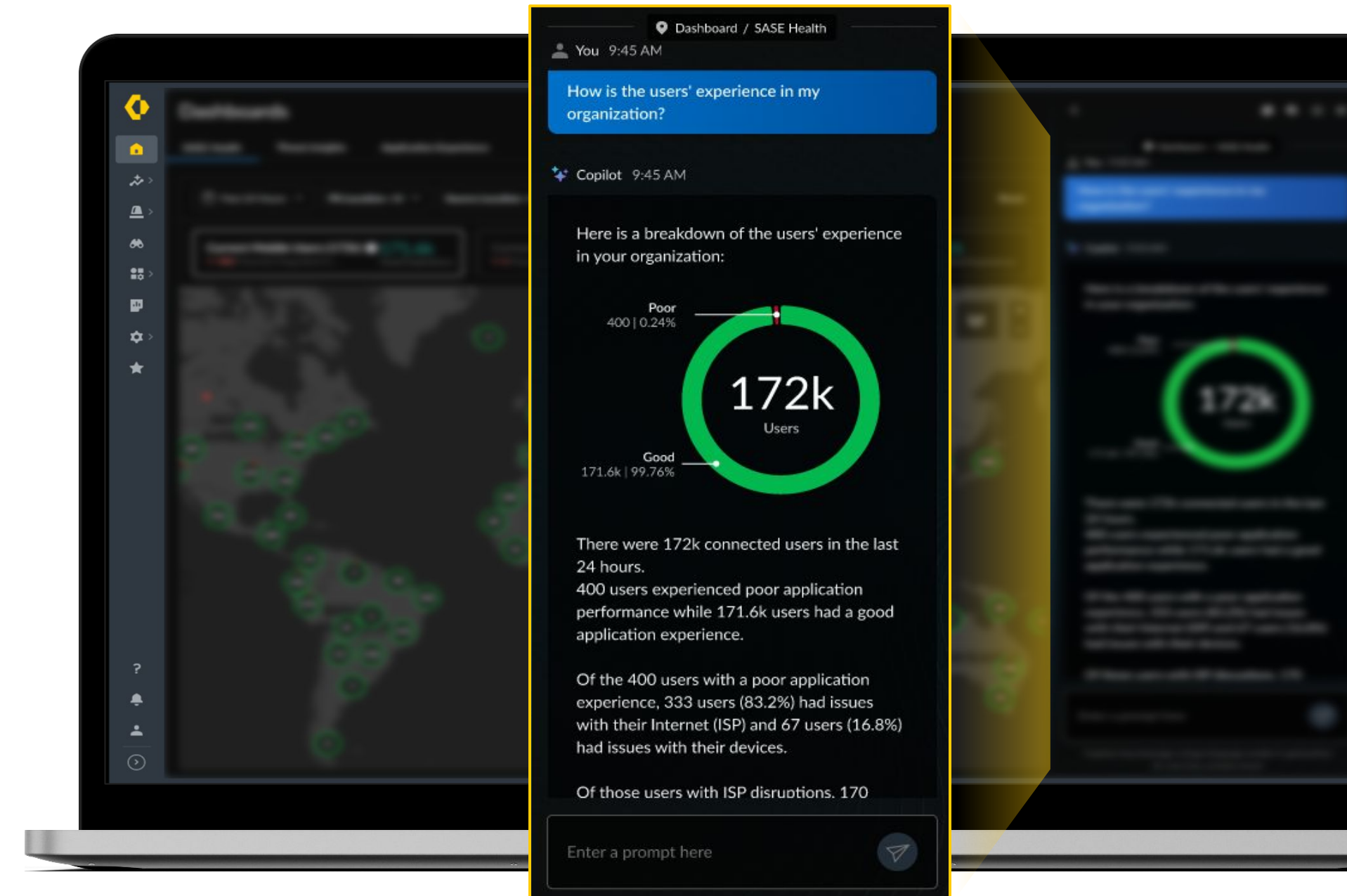
Gain broad and deep **product knowledge** with Copilot, a natural language AI assistant, trained on ~50,000+ sources from technical documentation to LIVEcommunity blogs



Get **curated questions** that are **contextually relevant** to the content of the page in focus along with relevant suggestions



**Fast remediation** with intelligent guidance and support case creation

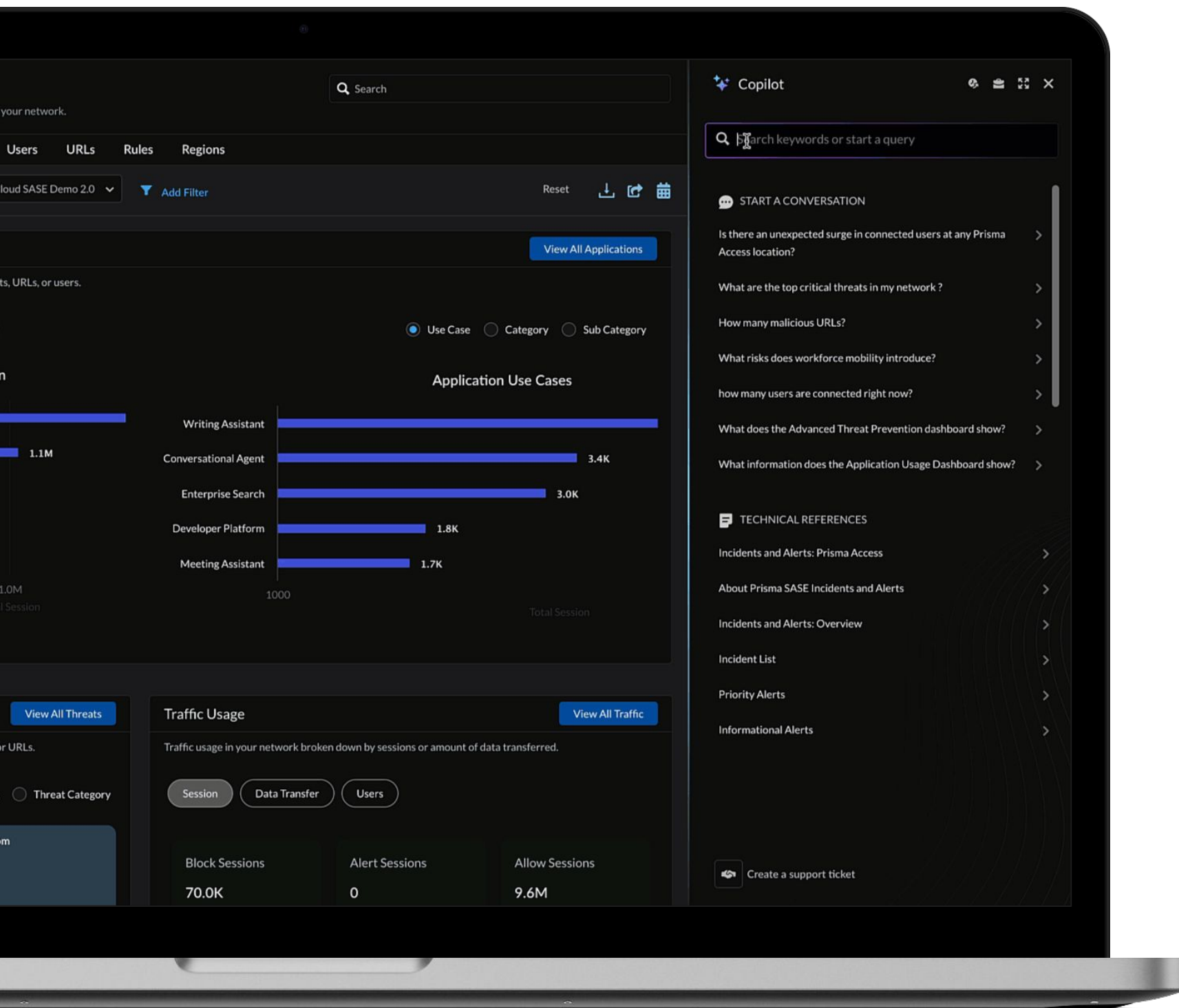


Beta results

500+ users engaged with Strata Copilot, submitting over 2,400 queries in the US, ranging from basic troubleshooting to advanced data analysis.

# Comprehensive Product Knowledge

Instantly access all Strata Network Security Platform documentation in one place



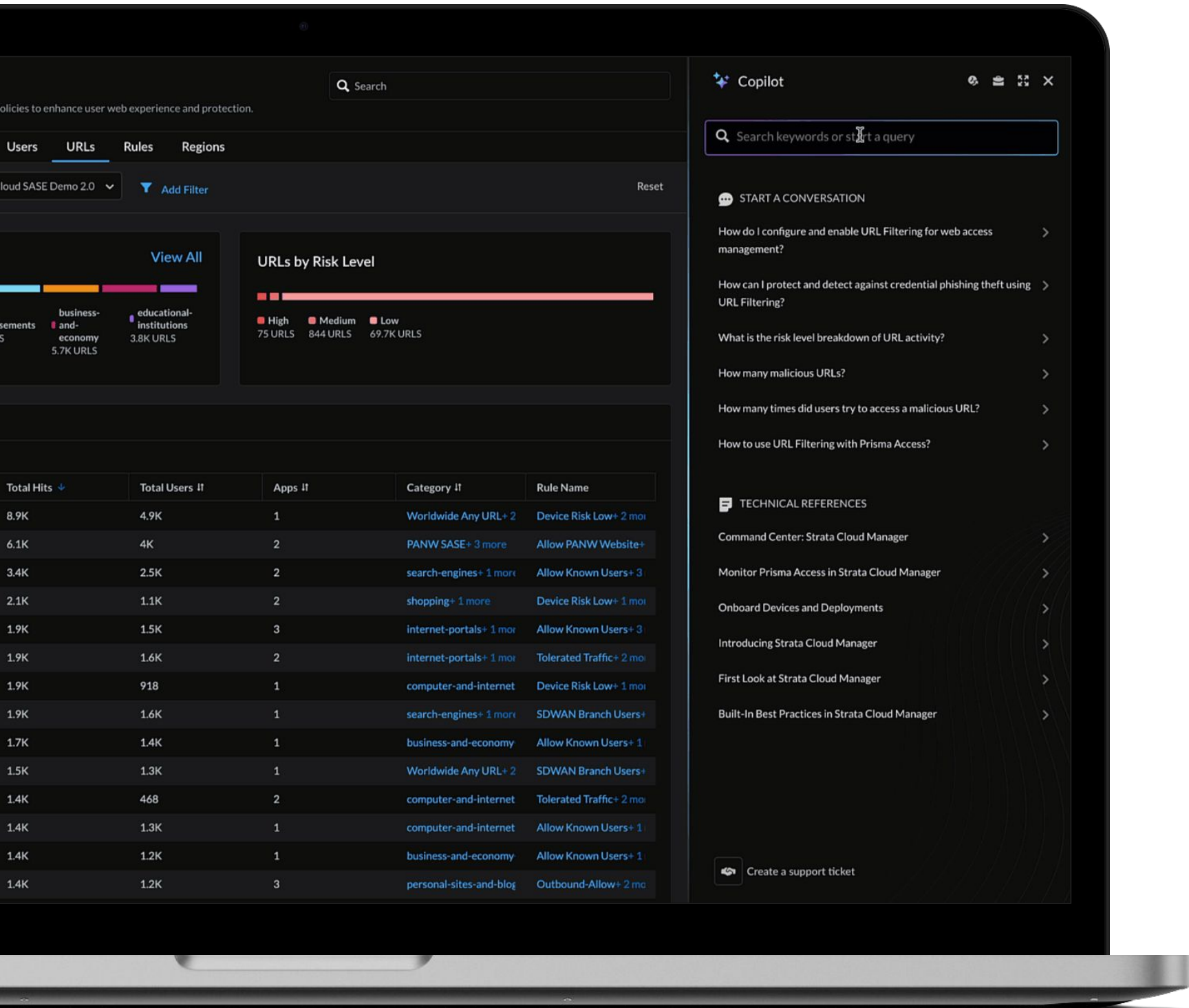
**How can I investigate activity on my network related to incidents and alerts?**

**How do I check FIPS Compliance?**

**How can I see if my users are having performance issues?**

# Intelligent and Relevant Suggestions

AI-Driven curated questions that are contextually relevant for securing and optimizing your network



Who are the 5 users exposed to the highest number of threats?

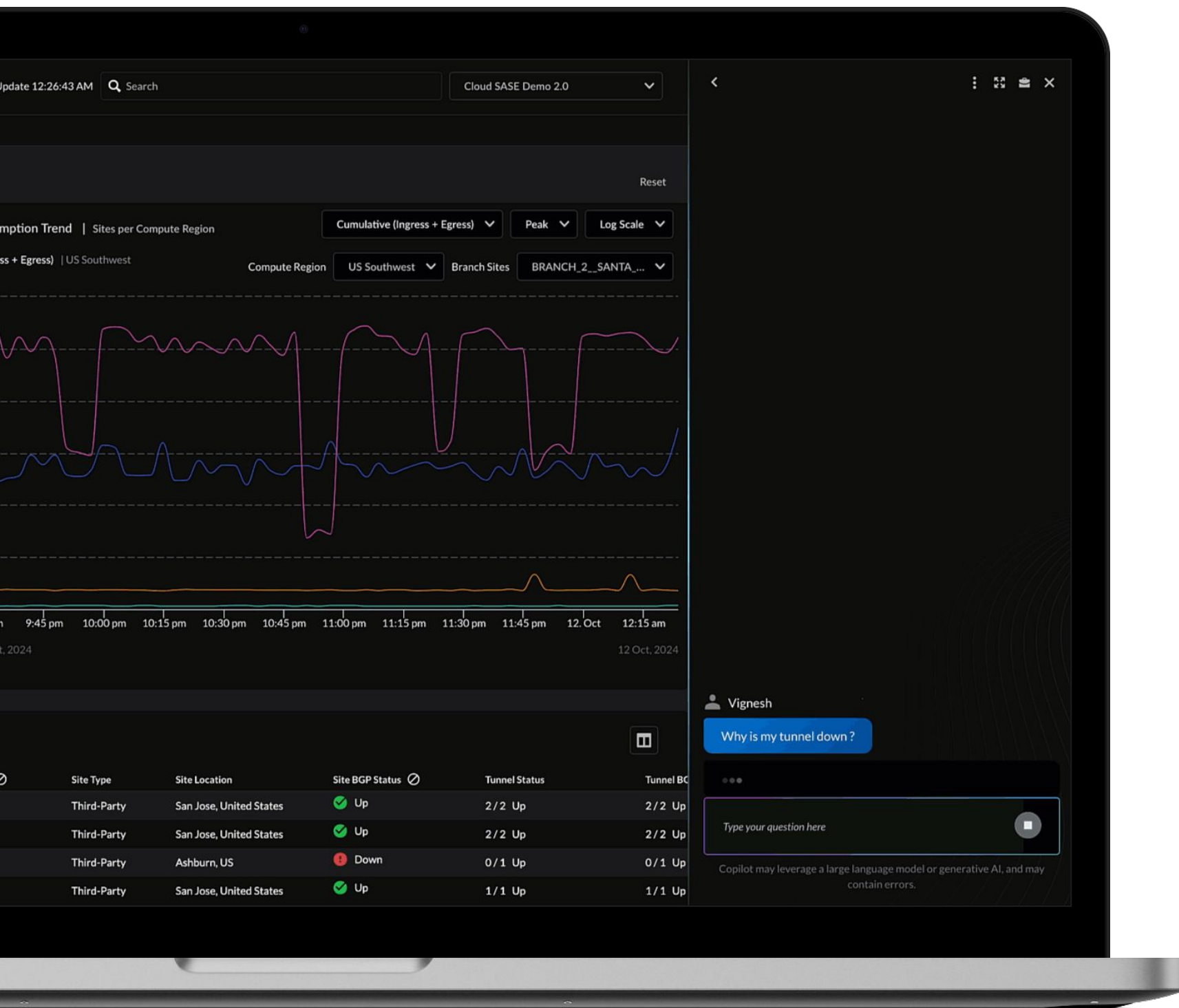
What are the most vulnerable devices on my network?

What is the total number of users browsing to a URL categorized as artificial-intelligence within the last 7 days, grouped by application name?



# Intelligent Guidance

Recommended next steps and intelligent support case creation for faster remediation



**Raise support tickets in a matter of seconds**

**Include historical information and evidence**

**Get suggested remediations to accelerate MTTR**