

Keeping Up with Zero Trust

cisco Live !

Zero Trust is running a marathon

Jerry Lin
Principal Solutions Engineer

Session ID: BRKSEC-2176

About Jerry Lin

- 25+ years at Cisco; Security CCIE#6469
- Distinguished Speaker Hall of Fame at Cisco Live
- Coauthor; “NAC Appliance: Enforcing Host Security with CleanAccess”, Cisco Press
- Cisco Security Reference Architecture
- Favorite sport; marathons!



RSAC



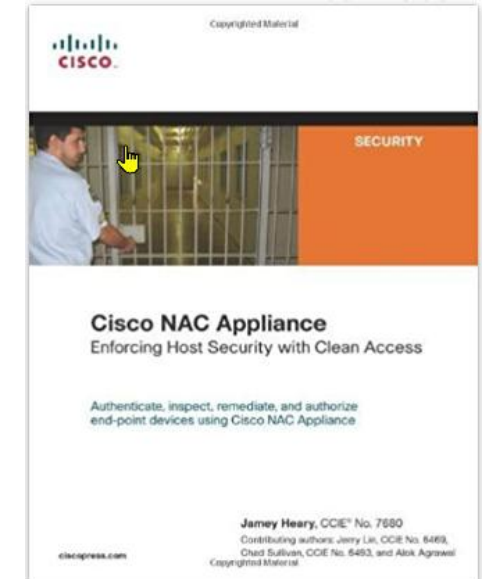
Boston



CL Hall of Fame



Coauthor



Cisco Webex App

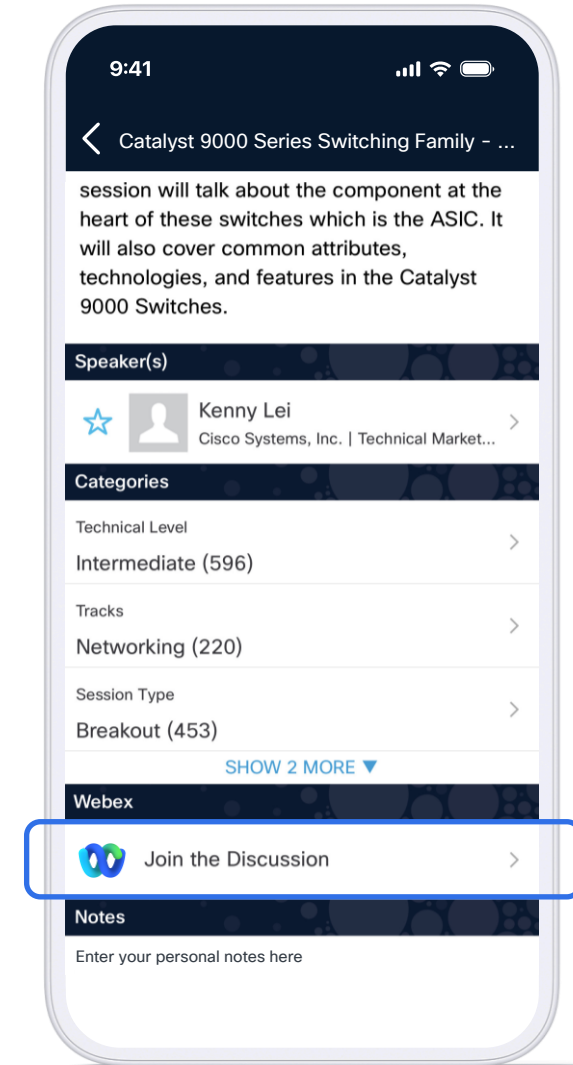
Questions?

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-2176>

Agenda

- 01 Introduction
- 02 Threat Landscape
- 03 Zero Trust Plan
- 04 Admin Access
- 05 Segmentation
- 06 Conclusion



Marathon
26.2 miles / 42.16 km

01	Introduction	→	2k
02	Threat Landscape	→	5k
03	Zero Trust Plan	→	10k
04	Admin Access	→	21k
05	Segmentation	→	32k
06	Conclusion	→	42k

Optimistic

Celebrating/Joy

Smiling

Focused - Silent

Pain Cave - self eval

Tears of JOY & PAIN



Talos 2024 Review

<https://blog.talosintelligence.com/category/year-in-review/>

60% 44%

More than half
of
Talos IR cases
had
an identity
attack
component

44% of
identity
attacks
targeted
Active
Directory

2026 RSA ID IQ Report

<https://www.rsa.com/wp-content/uploads/2026-rsa-id-iq-report.pdf>

69% 70%

of
organizations
reported ID
related breach
in the past 3
years.
Increase of
27% from
2025

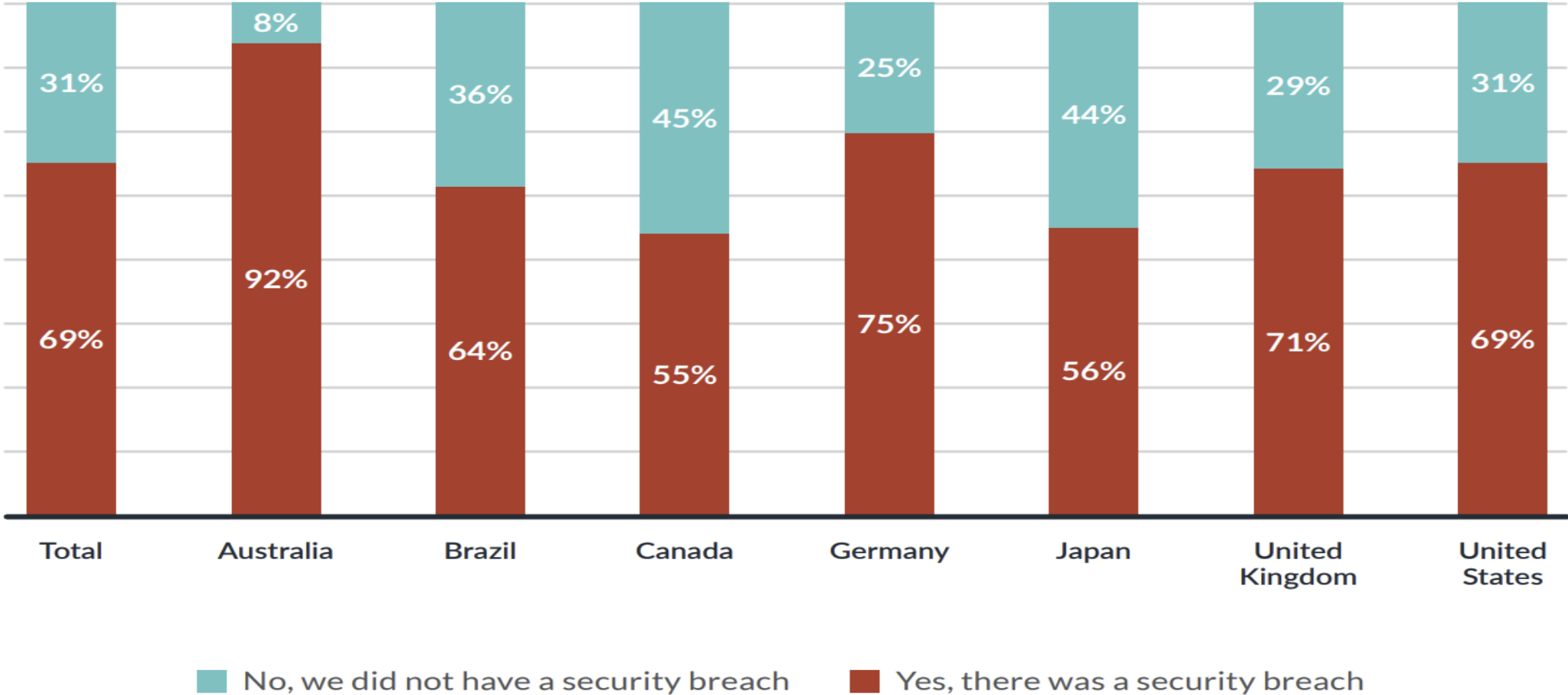
of
organizations
reported
breach caused
significant
harm

We have seen a strong shift toward identity-based attacks in Talos IR incidents

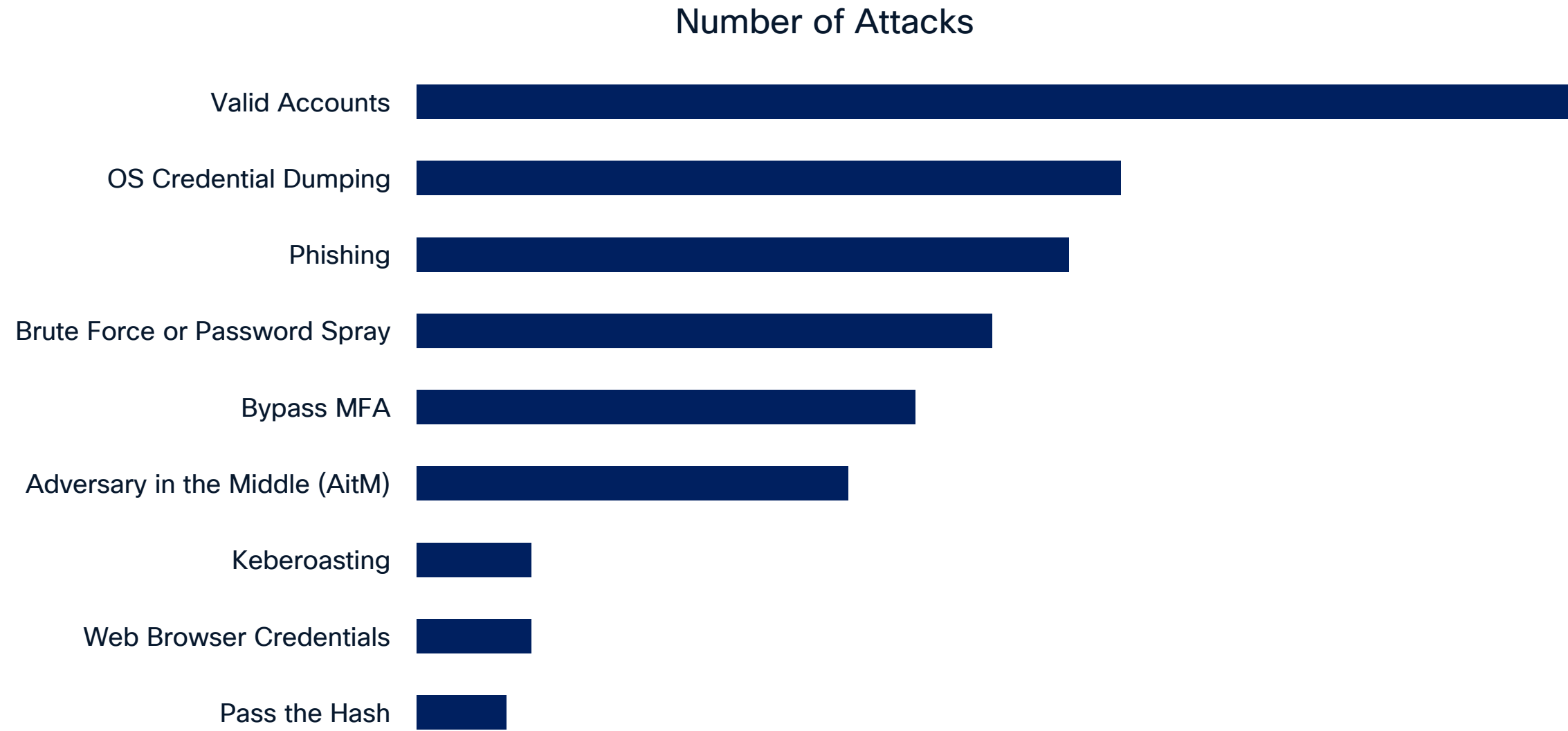
Security Breaches By Country

<https://www.rsa.com/wp-content/uploads/2026-rsa-id-iq-report.pdf>

By country: Did your organization experience an identity-related breach in the last three years?



The Many Flavors of Identity Attacks

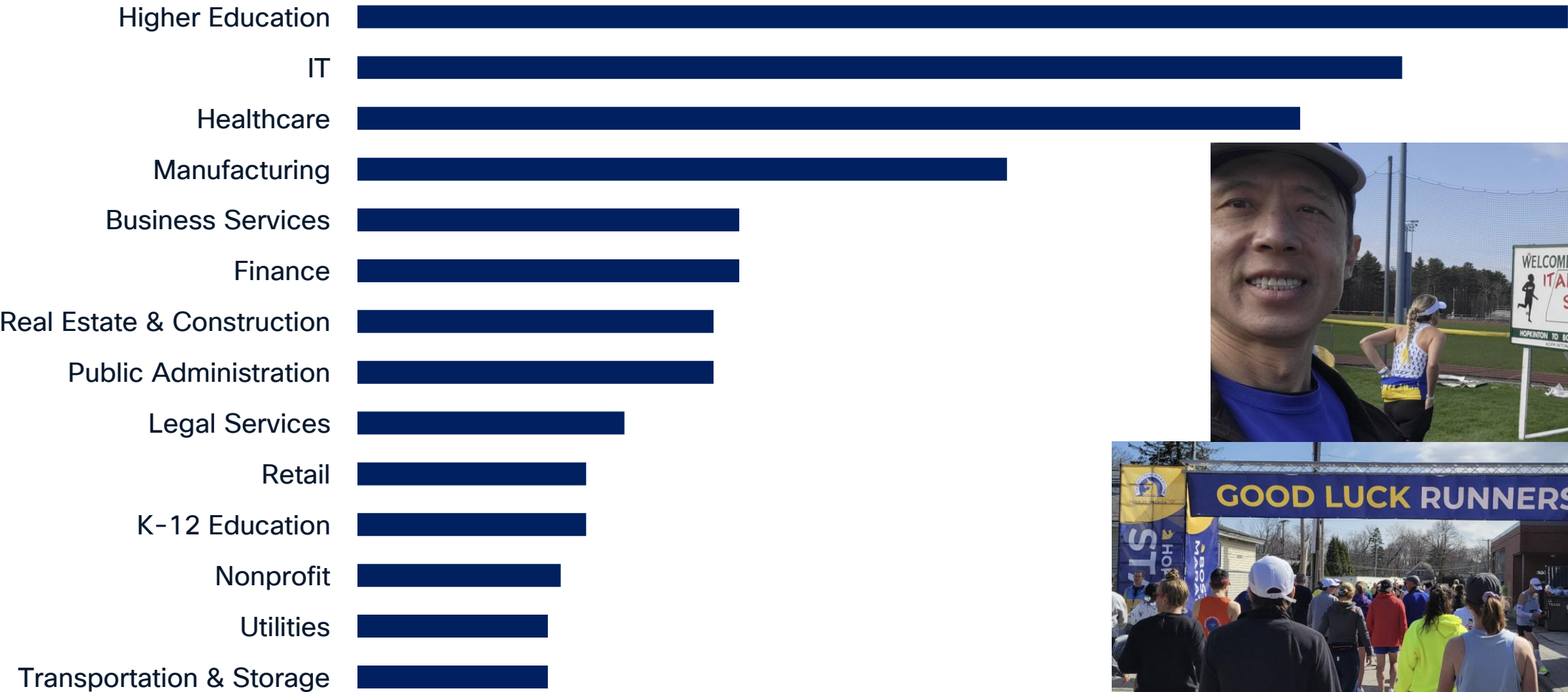


MFA is also an attack vector

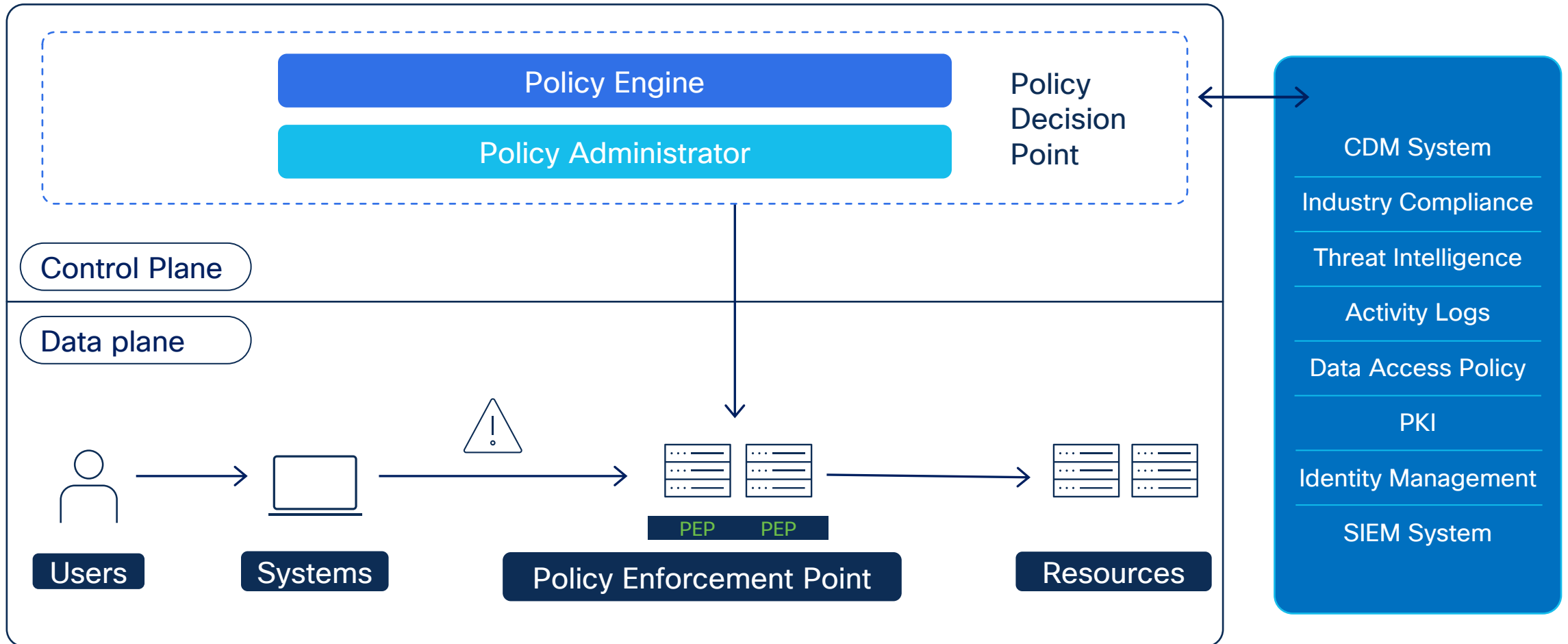


Marathon
2 km

Top-targeted industries in MFA Attacks



NIST 800-207 – Zero Trust Architecture



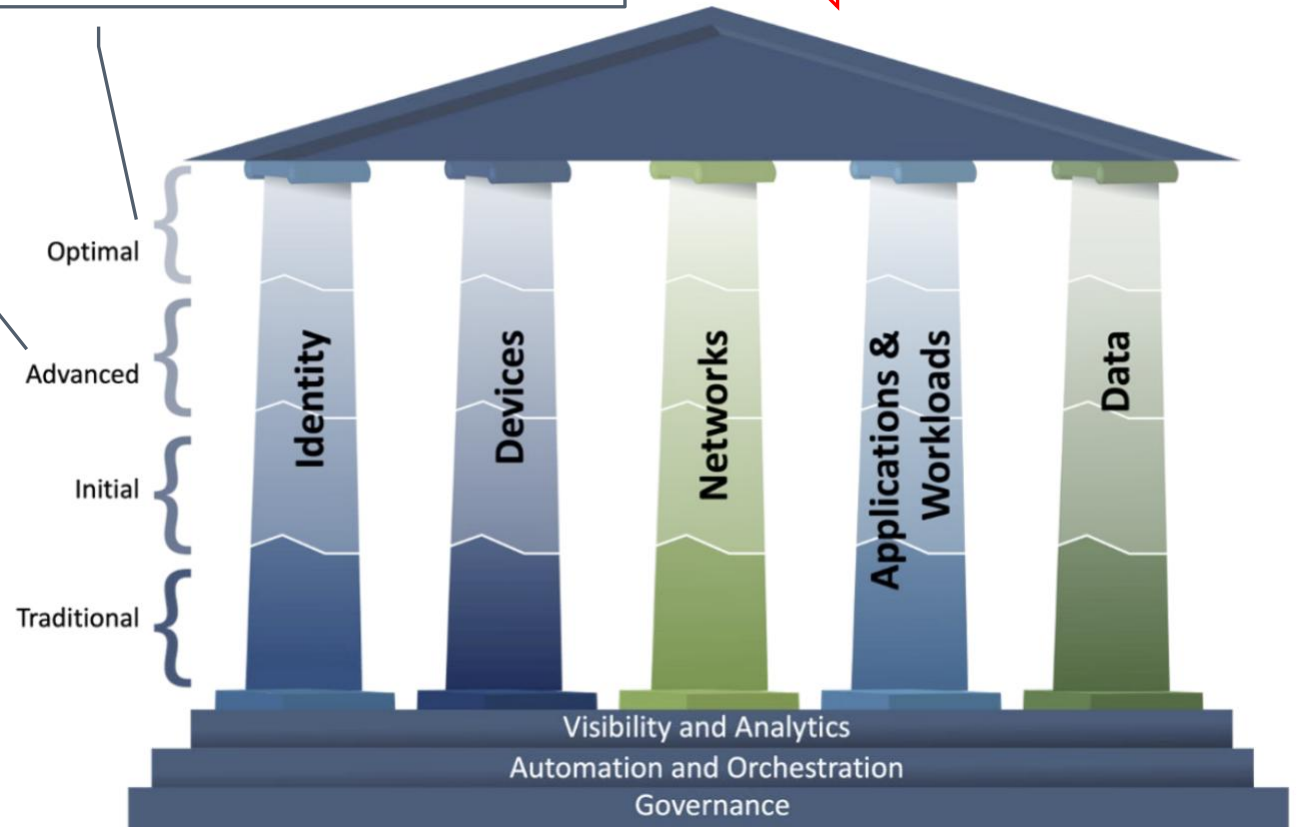
Zero Trust “progress”: Where are you today?

57% of organizations have reached CISA “Advanced” maturity

7% of organizations have reached CISA optimal Zero Trust maturity

Contradicts the 69% and 70%

- **Optimal** – fully automated, just-in-time identity lifecycle management
- **Advanced** – some automated controls of identity lifecycle management
- **Initial** – starting automation of identity lifecycle management
- **Traditional** – manual identity lifecycle management and configuration



https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf



Security Reference Architecture

cisco.com/go/sra



Cloud Platform

Security Cloud Control

CLOUD-BASED

Identity Intelligence

MULTICLOUD

UNIFIED MANAGEMENT & Risk Assessment

AI / ML DRIVEN

OPEN & EXTENSIBLE

TALOS THREAT INTELLIGENCE

Actionable threat intelligence

Collective responses

Comprehensive visibility

Signal identification

Threat research & analysis

SECURITY OPERATIONS CENTER

Cisco Vulnerability Management | Secure Analytics XDR | Secure Client | Splunk | Security Cloud Control Talos Incident Response

SERVICES

Custom threat research on demand | Implement and manage | Incident response retainer

CAPABILITIES

Network detection & response | Asset discovery & insights | User Behavior | Endpoint detection & response

Zero Trust

ZERO TRUST

SASE

User / Device Security

Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | Email Threat Defense | ThousandEyes

Cloud managed | VPN | Telemetry Visibility | Endpoint detection & response | DNS-layer security | Secure web | Posture | Anti-virus Anti-malware | Query | Host FW | Mobile device management | ZTNA | Risk-based MFA | Password-less | User trust | Identity Intelligence | Email, Phishing, SPAM, BEC, DLP, content filtering | Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Secure Access | Umbrella | Secure Connect

Enterprise browser | Cloud access Security broker | Cloud malware detection | Data loss prevention | DNS-layer security | FWaaS | Identity/Posture | Group tagging | AI Access | RAaaS | Remote browser isolation | Secure web gateway | TLS decryption | Zero Trust Network Access | Tenant restrictions

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Catalyst

Analytics | Application performance optimization | Cloud based orchestration | Cloud OnRamp | Digital experience monitoring | Group tagging | IPSec VPN | Integrated security | Middle mile optimization | Segmentation | Visibility

In the Office/Managed Location

Catalyst Center | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance

Application network gateway | Configuration orchestration | Content filtering | Encrypted visibility | Zero Trust Network Access | Group tagging | Identity/pxGrid Cloud | Network access control | Network security analytics | NGFW | NGIPS | Security analytics & logging | Segmentation | Threat mitigation | Profiling/Posture

Industrial Threat Defense

DNAC | SEA | CyberVision | Industrial Networking | ISE | Secure Firewall | Secure Network Analytics

Anomaly detection | Compliance | Group tagging | Identity pxGrid | Zero Trust Network Access | Ruggedized | Segmentation | Threat mitigation | Visibility

Workload, Application, and Data Security

ACI | Radware | Secure Application | Secure Endpoint | Secure Firewall | Multicloud Defense | Secure Workload | Hypershield | AI Defense

Identity pxGrid | Macro segmentation | Flow analytics | Threat mitigation | Firewall NGIPS | Defense gateway | AI Defense | Deployment automation | Micro segmentation | App discovery & observability | Container security | Run-time protection | DDoS WAF/Bot

Zero Trust use cases

Admin
Access

Remote
Worker

On-
Premises

Application
to
Application

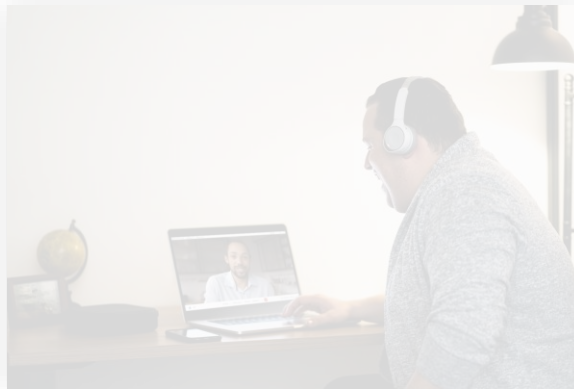


Zero Trust Use Cases

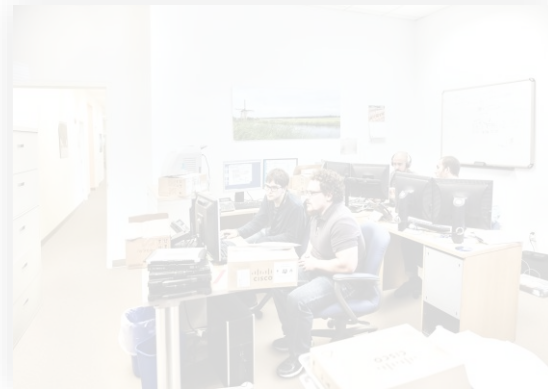
Admin
Access



Remote
Worker



On-
Premises



Application
to
Application



Why Admin Access?

What's considered Admin Access Accounts?

Typically high access privilege

- Administrator accounts
- Service accounts (Domain Controller accounts, software systems integrations, software process accounts, etc)
 - Weak shared credentials
 - Weak passwords
 - Lack of password rotation
 - Excessive privilege
 - Lack of monitoring/auditing

Salt Typhoon Review



Marathon
10 km



Big Hill!

Salt Typhoon

[Article](#) [Talk](#)

[Read](#) [Edit](#) [View history](#) [Tools](#)

From Wikipedia, the free encyclopedia

Salt Typhoon is an [advanced persistent threat](#) actor operated by [China's Ministry of State Security](#) (MSS) which has conducted high profile [cyber espionage](#) campaigns, particularly against the United States. The group's operations place an emphasis on [counterintelligence](#) targets in the United States and [data theft](#) of key corporate [intellectual property](#). The group has infiltrated targets in dozens of other countries on nearly every continent.^[1] Former [NSA](#) analyst Terry Dunlap has described the group as a "component of China's [100-Year Strategy](#)."^[2]

Salt Typhoon	
Formation	2020; 5 years ago
Type	Advanced persistent threat
Purpose	Cyber espionage , counterintelligence , data exfiltration
Location	China
Affiliations	Ministry of State Security

- Recently attacking as many as 8 major telecommunications providers using “living off the land” tactics to stay under the radar
- Leveraging PowerShell, WMIC, and exploiting network device vulnerabilities

Salt Typhoon... described to Cisco



Attacker infiltrated the network and accessed a device shell



Attacker able to make lateral movements and see **device access credentials**



Potential **service accounts** compromised



“Network infrastructure was compromised”..... Per customer

“Cisco, YOU need to fix this!” ... customer quote

Talos Blog: Salt Typhoon

Feb 20, 2025, <https://blog.talosintelligence.com/salt-typhoon-analysis/>



Talos blog: Salt Typhoon CVEs disclosed

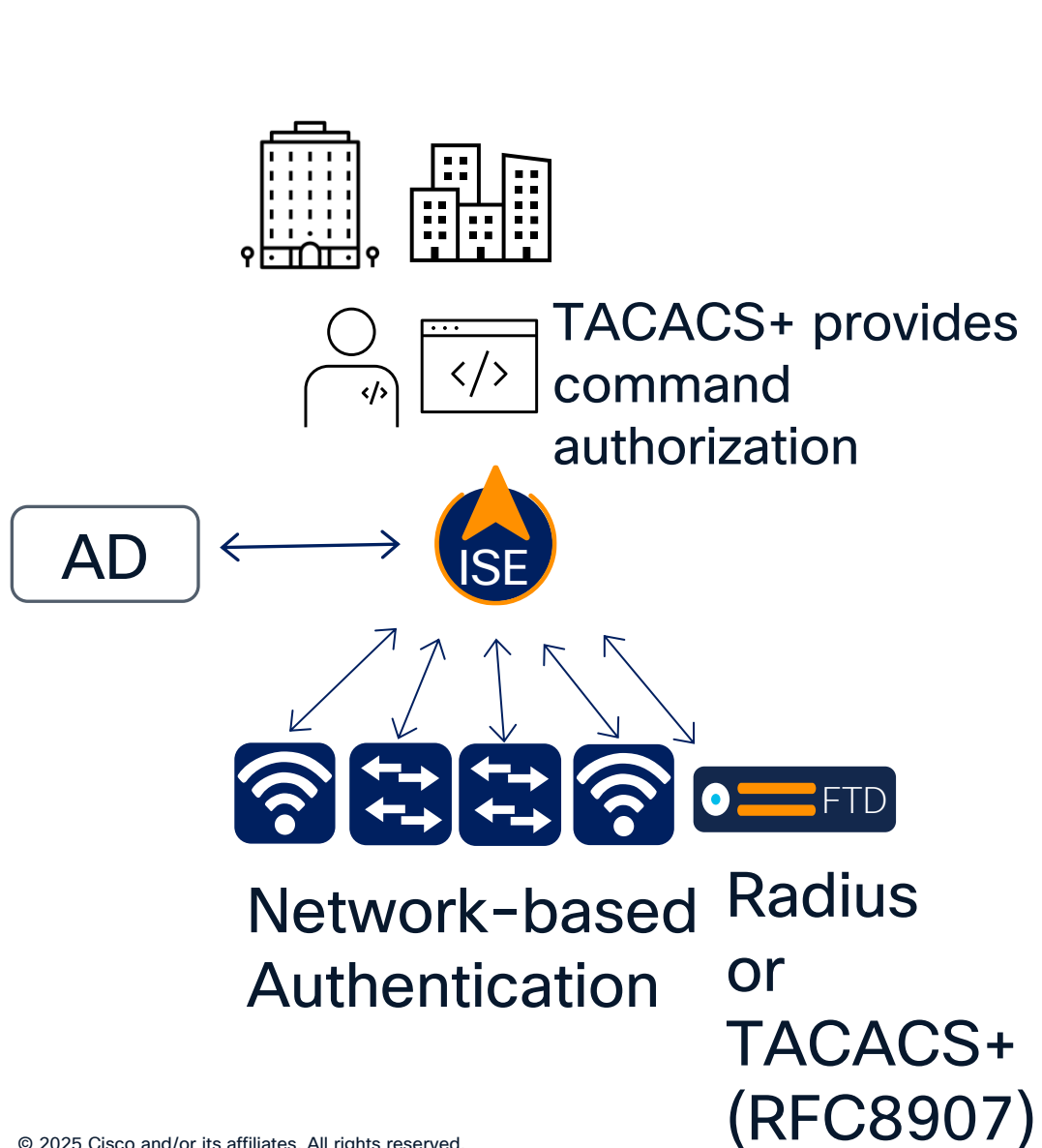
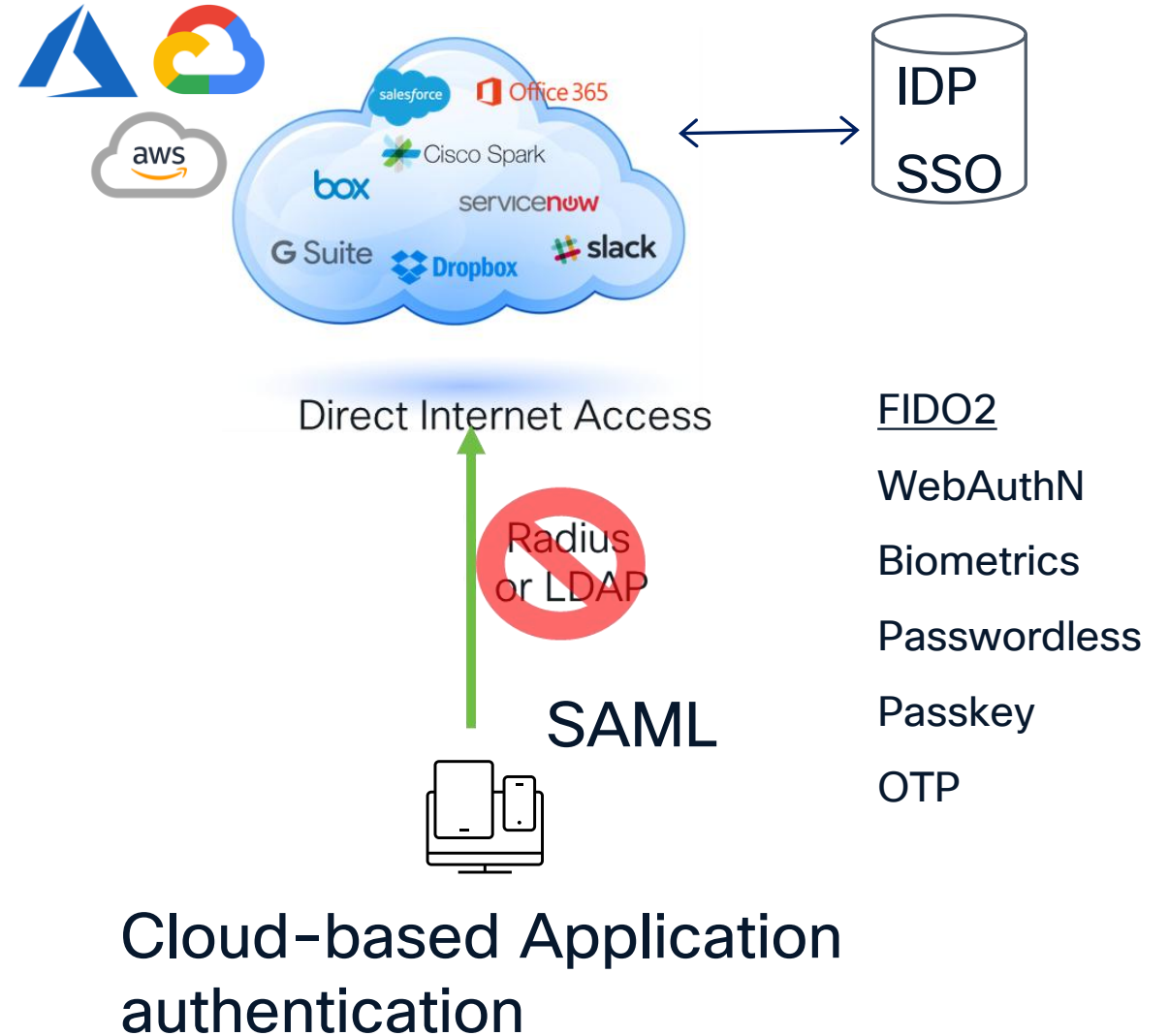
All three CVEs have patches available.
Patching HIGHLY Recommended

CVE-2018-0171 - Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability (Last Updated: Dec 15, 2022)

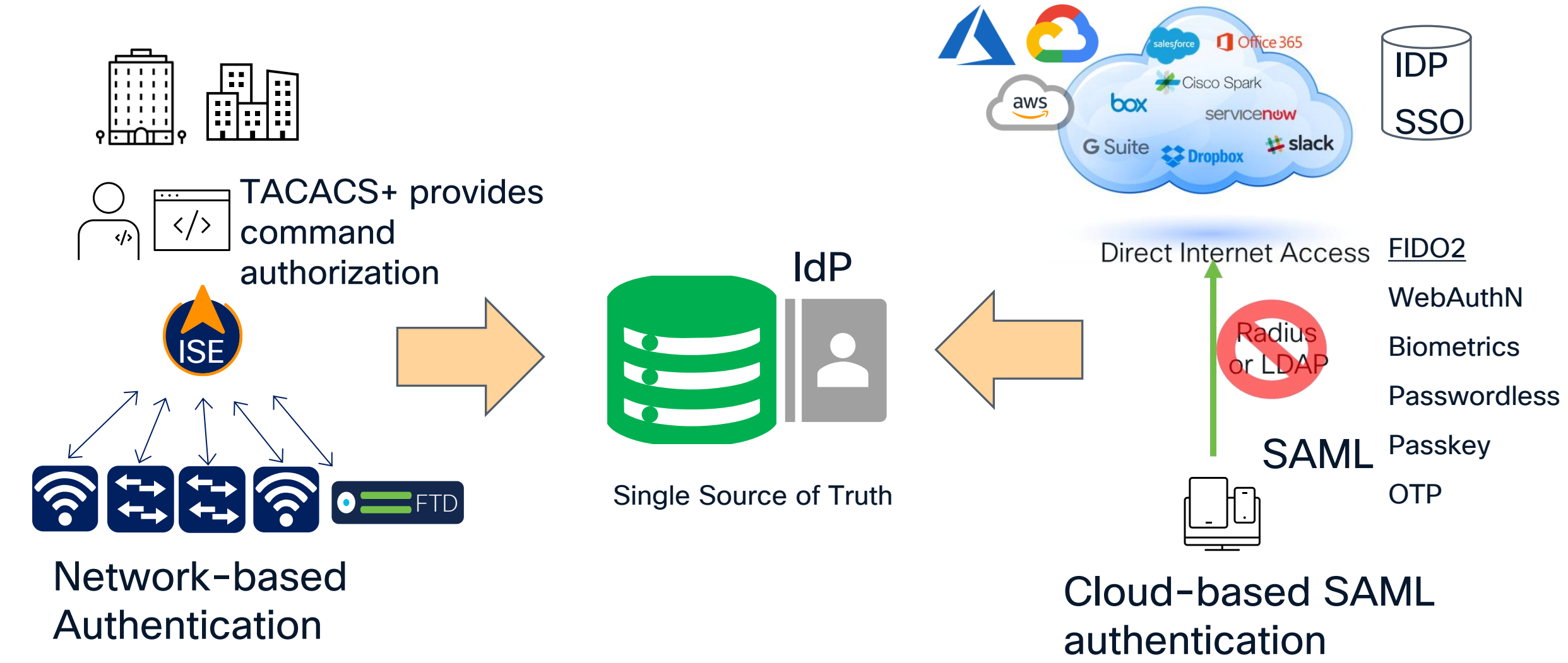
CVE-2024-20399 - Cisco NX-OS Software CLI Command Injection Vulnerability (Last Updated: Sept 17, 2024)

CVE-2023-20198, CVE-2023-20273 - Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature (Last Updated: Nov 1, 2023)

Network-based vs Cloud Apps Authentication



Can we unified traditional network-based authentication with current cloud-based authentication?



Potential considerations to address Salt Typhoon

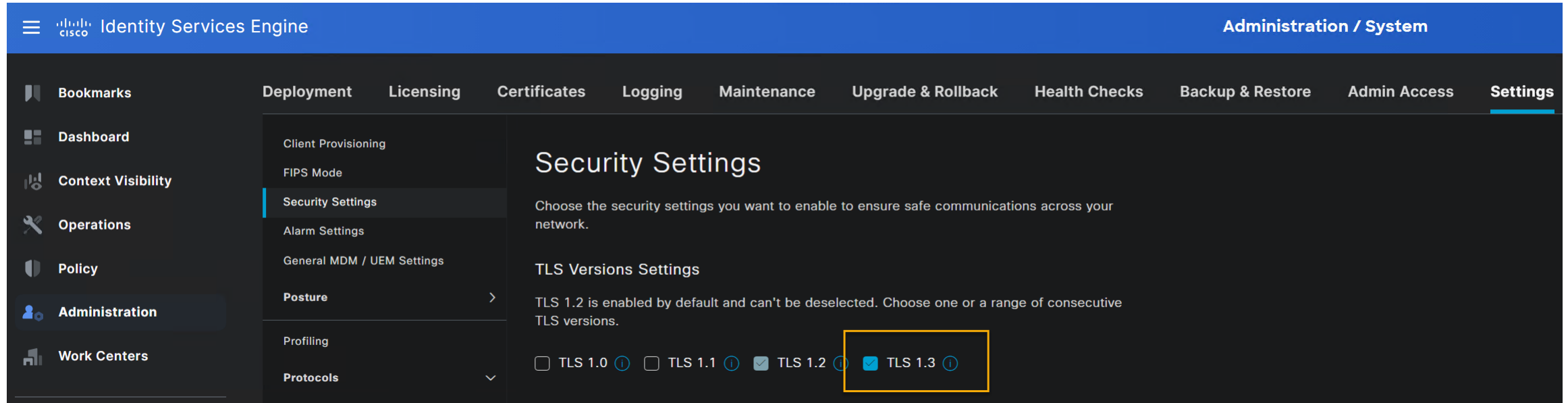
Can we improve Network Security ?

- Modify TACACS+ standard to rotate share secrets
- Modify TACACS+ RFC 8907 to support FIDO2
- RadSec
- Radius over IPSec(ISE support today)
- TACACS+ over TLS 1.3 (In ISE 3.4 P2 or 3.5)

If Identity security related,

- Likely stolen credentials. Eliminate passwords. Use FIDO2
- Lockdown access to corporate infrastructure

TACACS+ over TLS 1.3



The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows the navigation menu with 'Administration' selected. The main content area is titled 'Security Settings' and includes a sub-section for 'TLS Versions Settings'. Below this, there are four checkboxes for TLS versions: TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. The 'TLS 1.3' checkbox is checked and highlighted with a yellow box. The text indicates that TLS 1.2 is enabled by default and cannot be deselected, and that one or a range of consecutive TLS versions can be chosen.

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/224882-configure-tacacs-over-tls-1-3-on-a.html#:~:text=TACACS%2B%20over%20TLS%201.3%20%5BRFC8446,between%20TACACS%2B%20clients%20and%20servers.>

 Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

More 

Network Devices

Default Device

Device Security Settings

Device Type Cat9300 Switch [Set To Default](#)☐  RADIUS Authentication Settings☒  TACACS Authentication Settings

Shared Secret

[Show](#)[Retire](#)☐ Enable Single Connect Mode☒ Legacy Cisco Device☐ TACACS Draft Compliance Single Connect Support☒  TACACS over TLS Authentication Settings

To enable TACACS over TLS authentication, ensure that:

- TACACS over TLS option is enabled in [Device Administration Deployment](#) page

Subject Alternative Name (SAN)

Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (iPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.

☐ IP Address

The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details [Show](#)

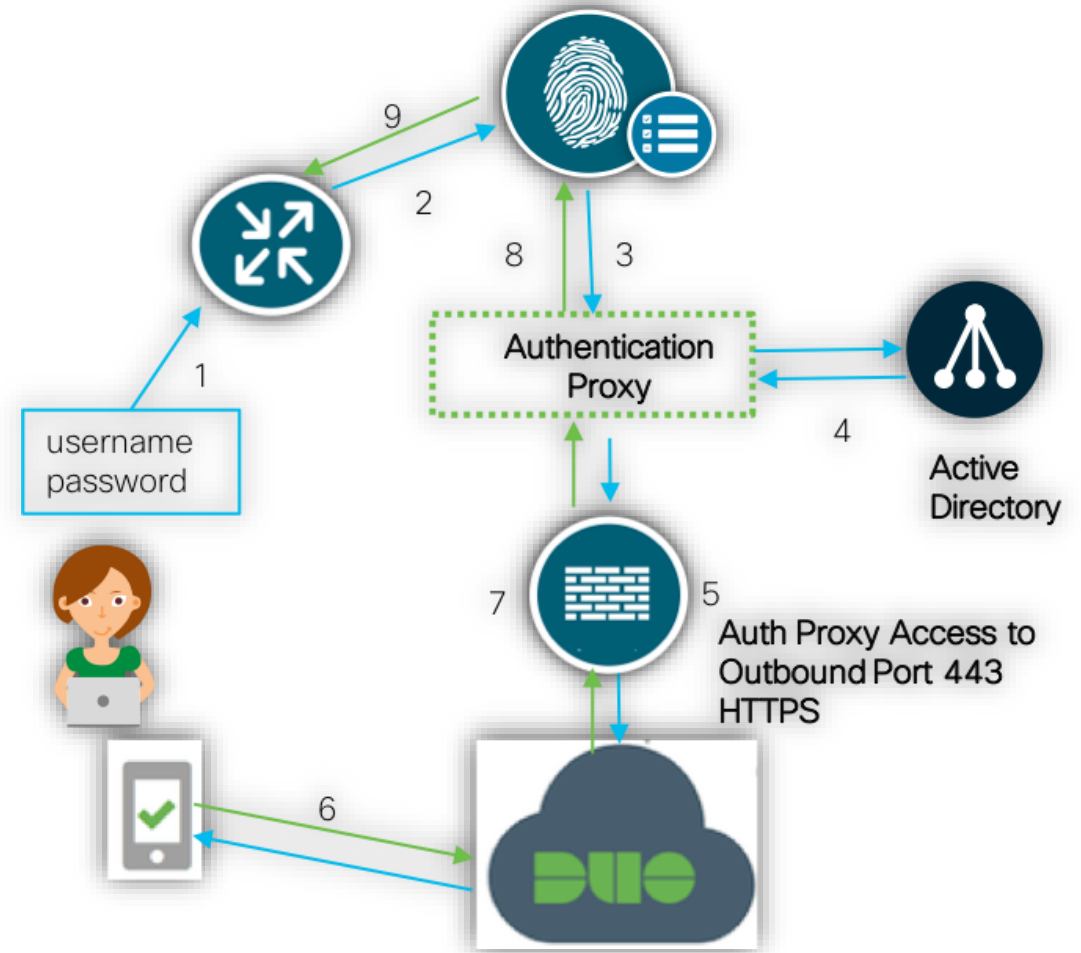
Additional SAN Attributes

☒ Enable Single Connect Mode

Allow a network device to use one TCP connection for all TACACS+ requests, reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

Protecting Access to Network AuthC with ISE TACACS+ and DUO MFA

- <https://community.cisco.com/t5/security-knowledge-base/protecting-access-to-network-devices-with-ise-tacacs-and-duo-mfa/tap/3783600>
- Cisco TACACS+ to the rescue
- TACACS+ is based on a shared secret or password
- Some customers are still using Microsoft NPS for MFA!!!



IOS-XE with “Guest Shell”

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/173/b_173_programmability_cg/guest_shell.html

- Guestshell is a virtualized Linux-based environment, designed to run custom Linux applications, including Python for automated control and management of Cisco devices.
- Guest Shell lacks typical AAA functionality
- Bad actor’s playground?
- Customer wants it disabled/removed

In Cisco IOS XE Amsterdam 17.3.1 and Later Releases

The following example shows how to enable Guest Shell. In Cisco IOS XE Amsterdam 17.3.1 and later releases, only Python V3.6 is supported.

```
Device> enable
Device# guestshell enable
```

```
Management Interface will be selected if configured
Please wait for completion
Guestshell enabled successfully
```

```
Device# guestshell run python3
```

```
Python 3.6.8 (default, Nov 21 2019, 22:10:21)
[GCC 8.3.1 20190507 (Red Hat 8.3.1-4)] on linux
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>>>
```

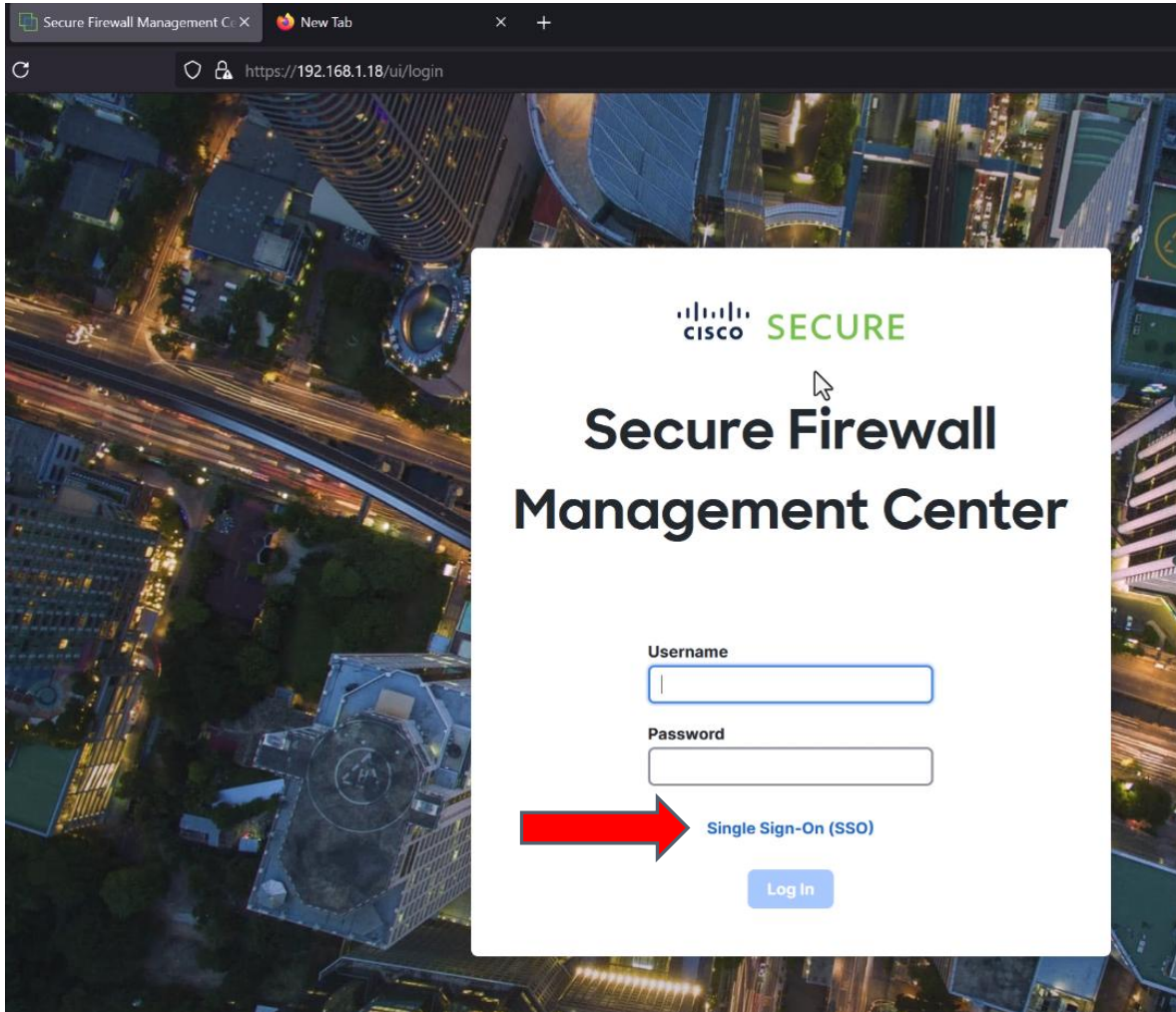
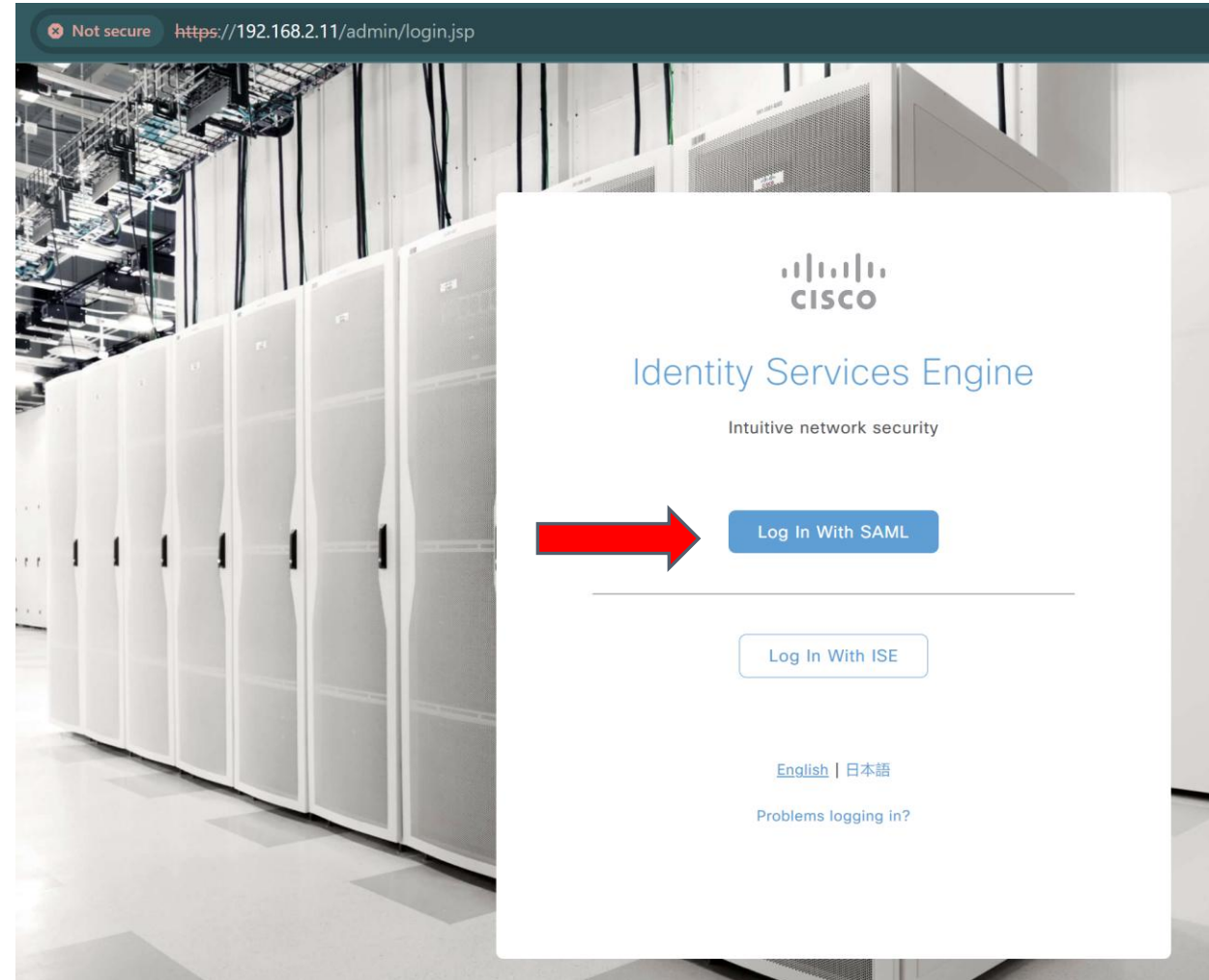
```
Device# guestshell run bash
```

```
[guestshell@guestshell ~]$
```

```
Device# guestshell disable
```

SAML/SSO for ISE and FMC admin login

Enable IdP of your choice! Or use Duo Directory.



Salt Typhoon... RESPONSE by Cisco



Marathon
15 km



Attacker infiltrated the network and accessed a device shell



Attacker able to make lateral movements and see **device access credentials**



Potential **service accounts** compromised

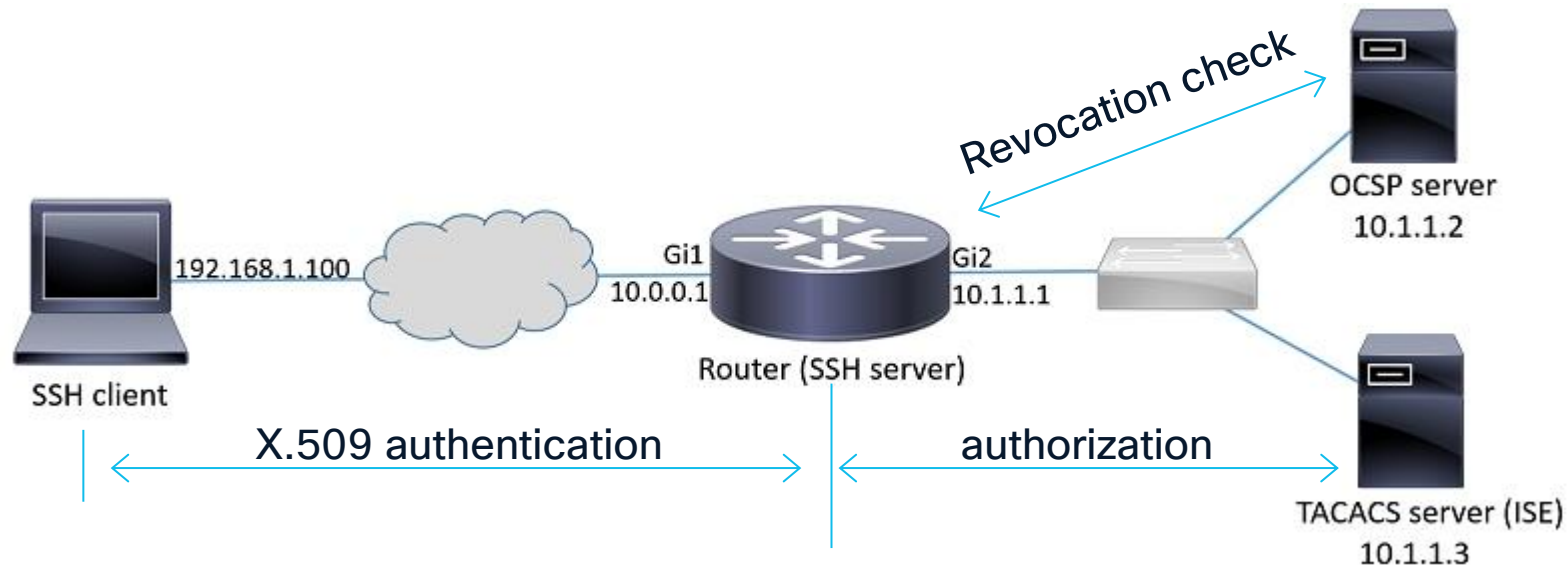


“Network infrastructure was compromised”..... Per customer

Secure your Infrastructure & Monitor Identities

SSH with X.509 Certificate Authentication for IOS devices

<https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/212178-Configuring-SSH-with-x509-authentication.html>



Requires a mature PKI Infrastructure and skilled operations staff to maintain

Zero Trust Use Cases



Admin Access

Remote Worker
(Edge)

On-Premises
(Campus)

Application to Application
(Data Centers)



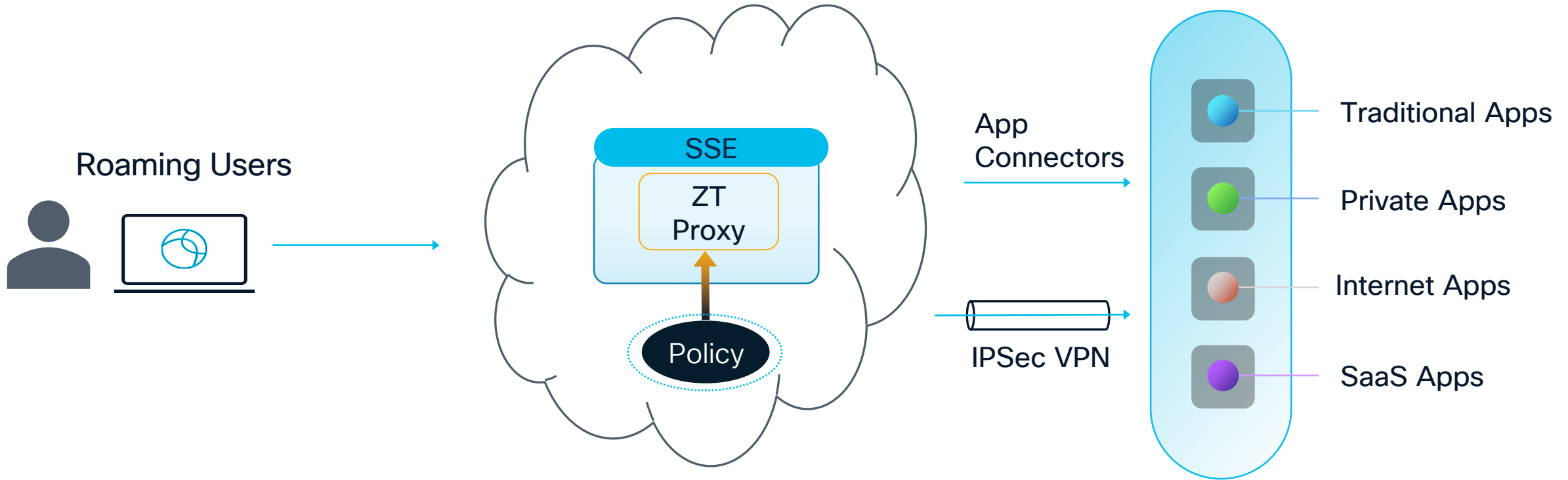
Zero Trust Network Access (ZTNA)



Zero trust network access (ZTNA) is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities.

Gartner

ZTNA Application Access



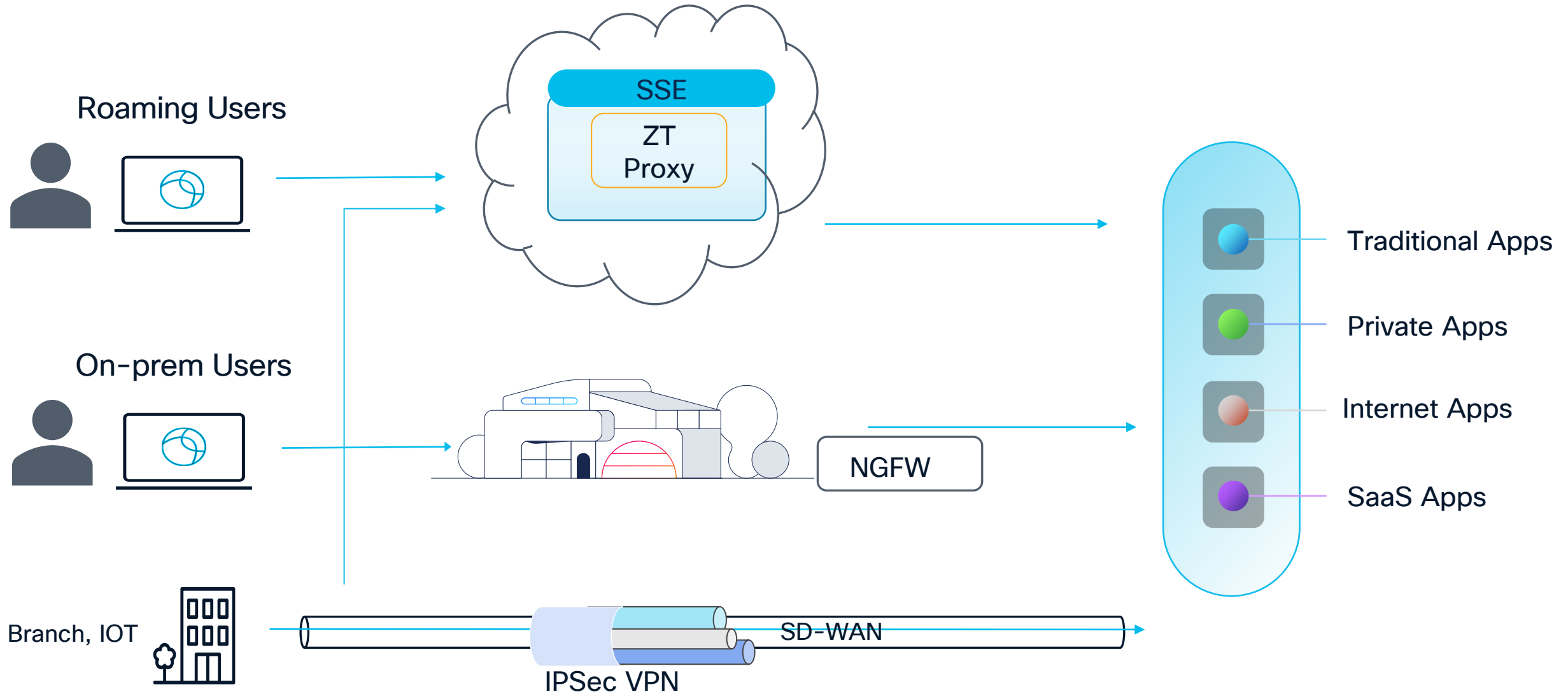
Universal Zero Trust Network Access (UZTNA)



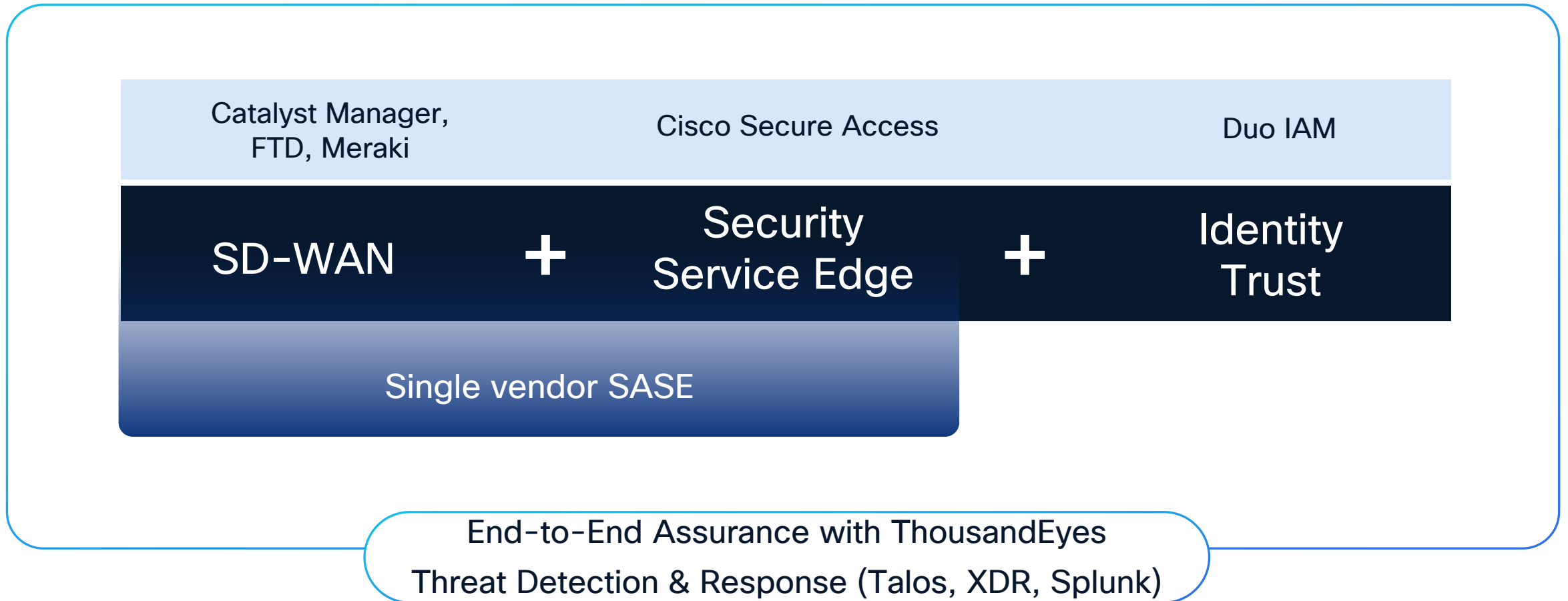
Application of Zero Trust Network Access (ZTNA) principles to both remote and on-campus networks, ensuring a single security policy, consistent user experience, simpler troubleshooting, and improved efficiency. It extends beyond ZTNA, which often focused primarily on remote access, to encompass all users regardless of their location

Gartner

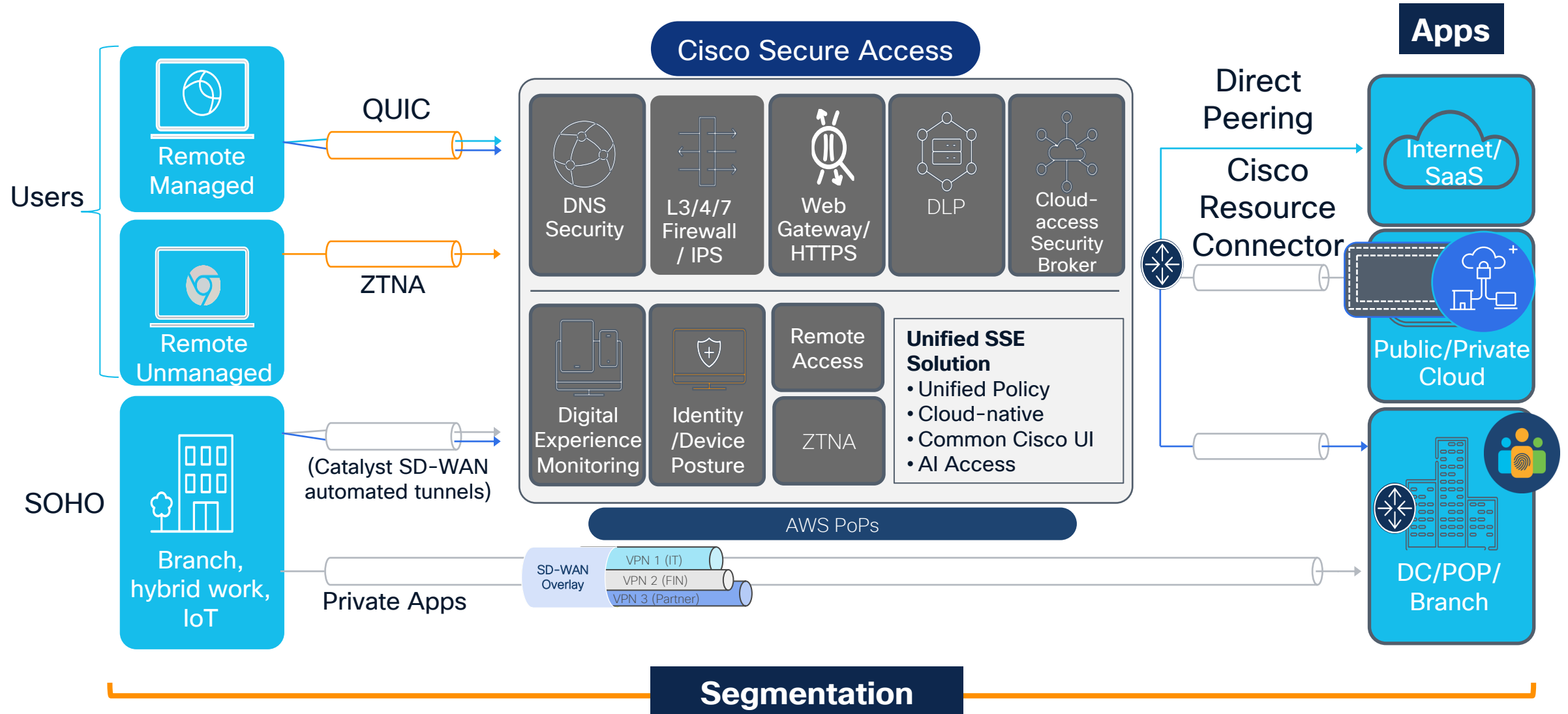
UZTNA Application Access



Cisco Universal ZTNA

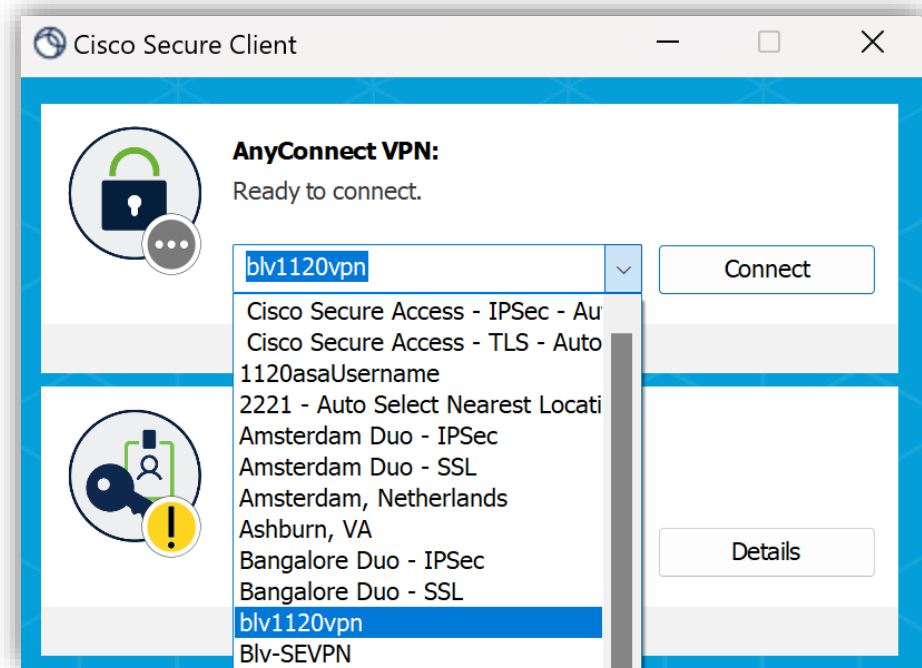
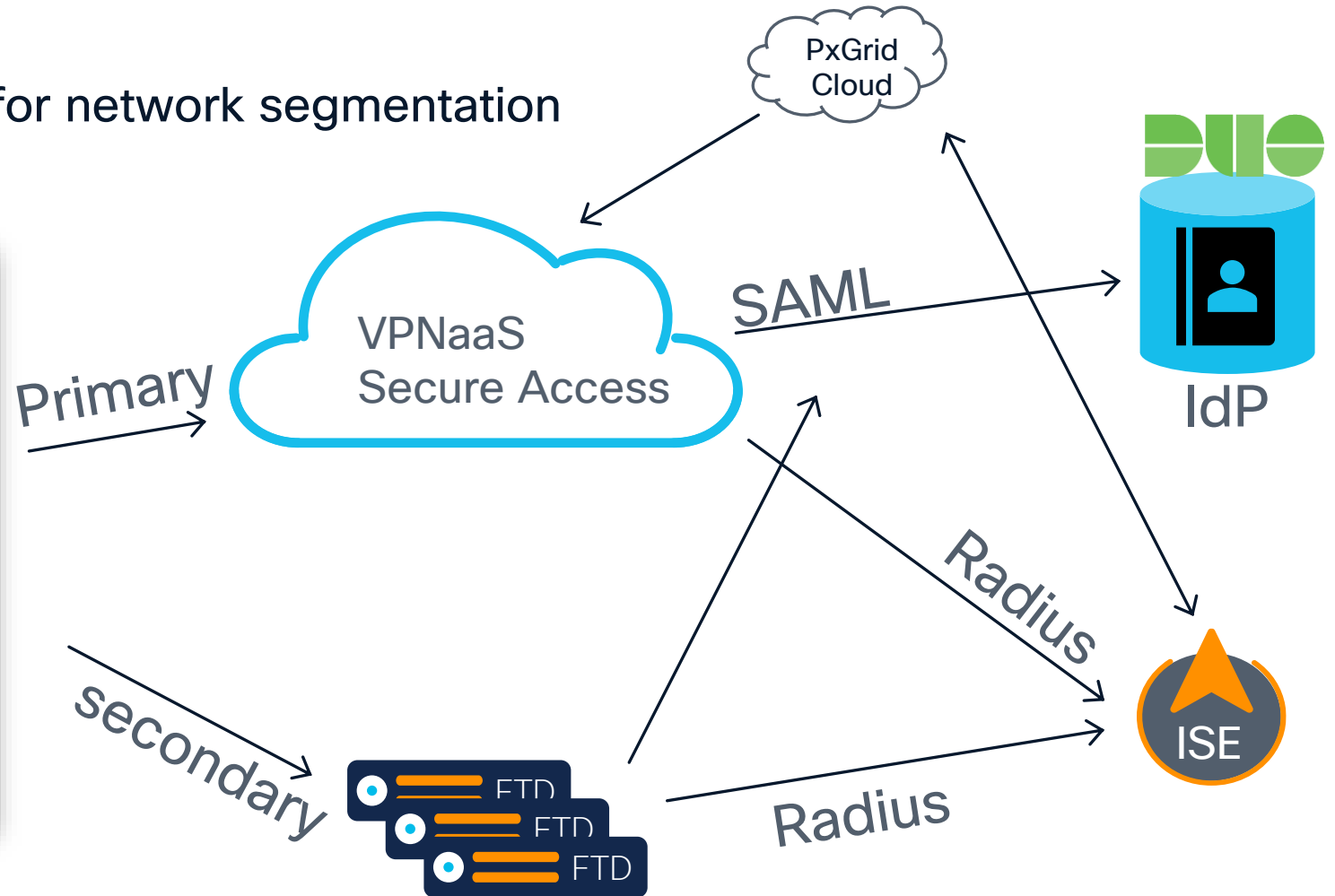


Start of segmentation



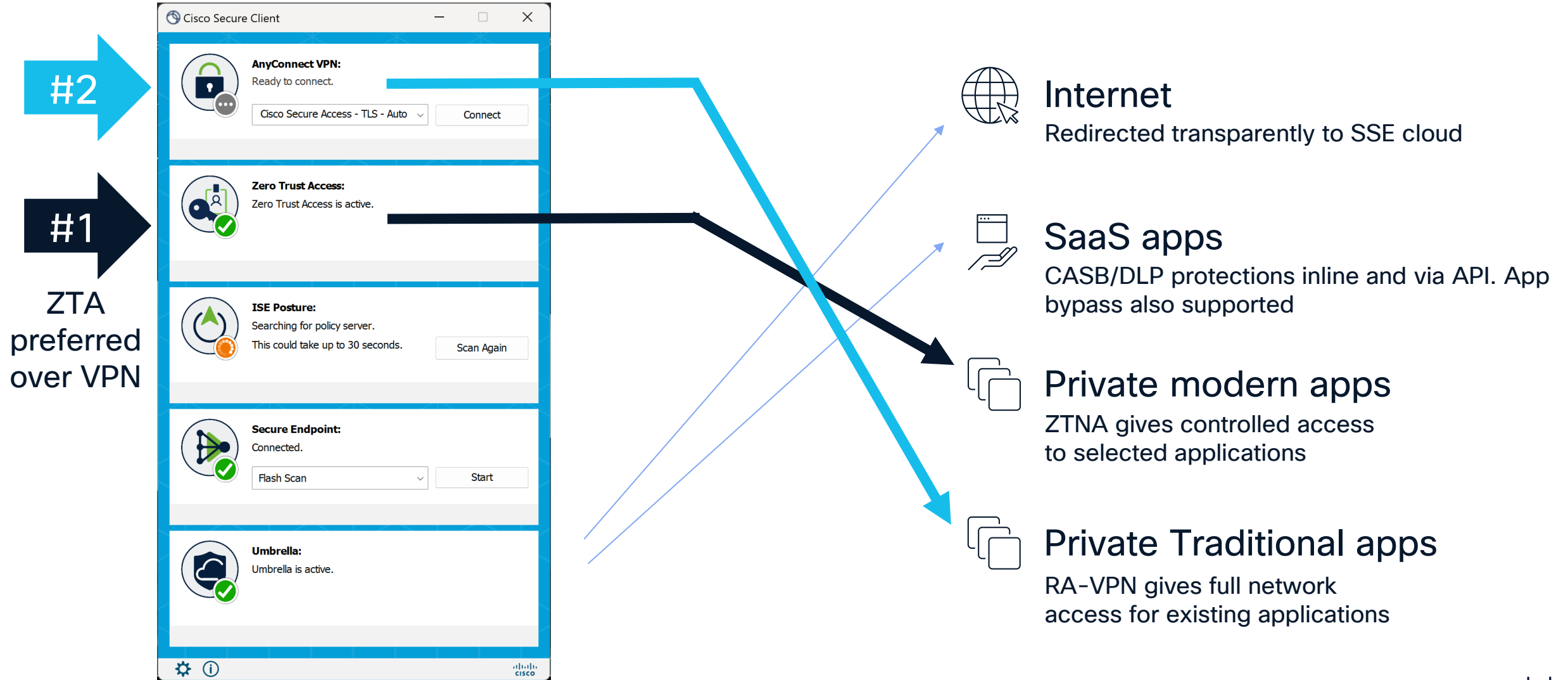
VPNaaS for segmentation, scalability and ease of deployment

ISE/TrustSec/SGT is the foundation for network segmentation



Unified ZTNA Client

Zero Trust Access starts the segmentation journey!



Segmentation by application access method

Secure Access

Home

Experience Insights

Connect

Resources

Secure

Monitor

Resources

Sources and destinations

Internal Networks

Registered Networks

Roaming Devices

Security Group Tags

SDWAN Service VPN IDs

Destinations

Internet and SaaS Resources

Private Resources

Settings

AAA Servers

Browser-based

ZTA

Private Resources

Add a Private Resource

Private Resources are applications, networks, or subnets that your organization controls access to. You must configure private resources before you can create policies that allow access to them.

General

Private Resource Name

FMC-jelin-BlvIFT

Description (optional)

Belleuve DMZ SE Lab, FMC for IFT testing

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will use these addresses to connect to the resource.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR)

192.168.1.17

Protocol

TCP - (HTTP/HT...

Port / Ranges

443

+ IP Address or FQDN

☒ Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

☐ Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoints. [Help](#)

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address)

192.168.1.17

+ FQDN or IP Address

☐ Browser-based connection

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when device checks are possible. [Help](#)

Public URL for this resource

https:// fmc-jelin-blvift -8239439.ztna.sse.cisco.io

Protocol

HTTPS

Custom host header (optional)

Server Name Indication (SNI) (optional)

☐ Validate Application Certificate

☒ VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN. [Help](#)

Full VPN

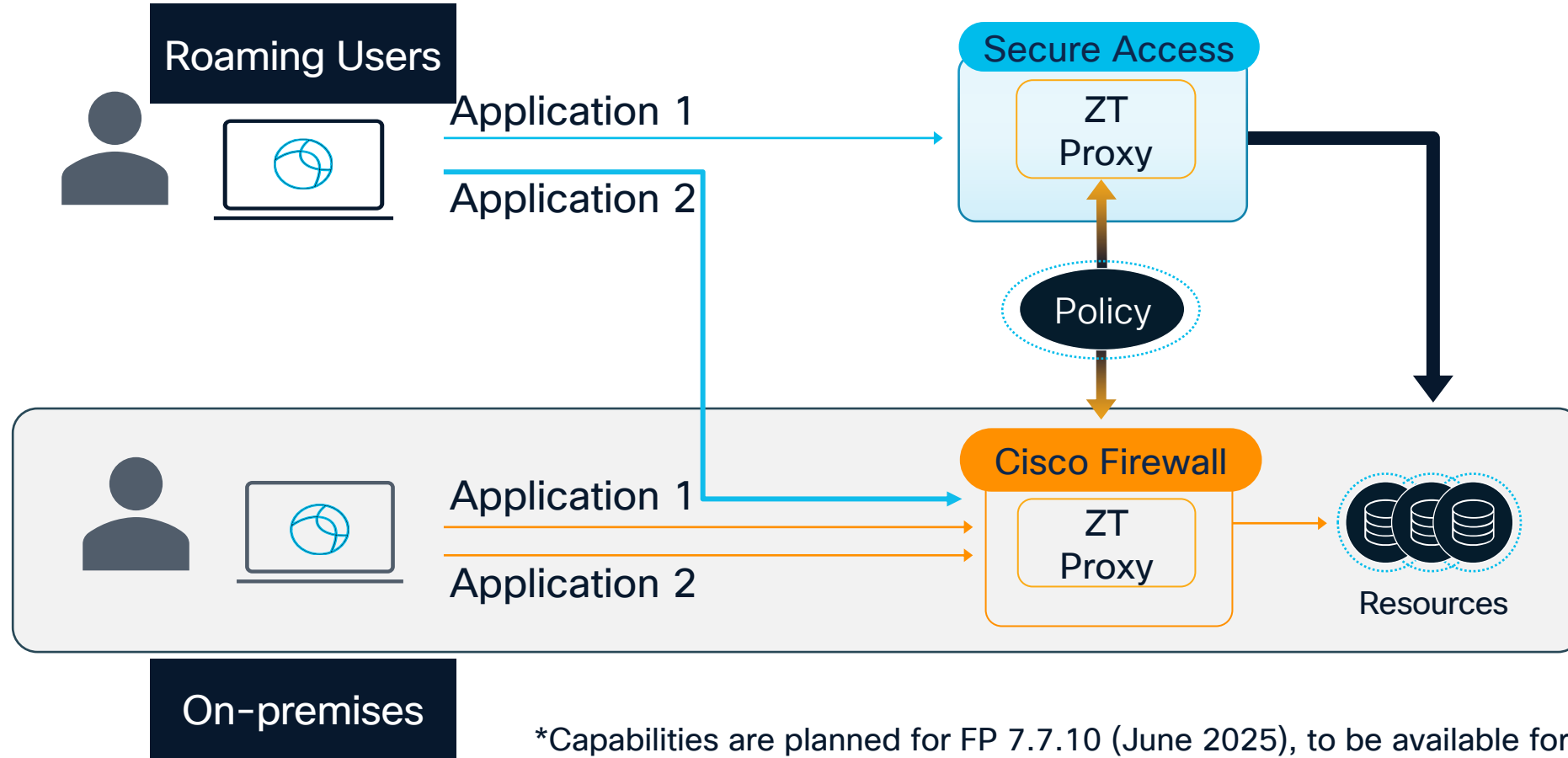
© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2176

Universal ZTNA Private Application Design

Single set of ZTNA policies used in cloud and on-premise

NEW*



*Capabilities are planned for FP 7.7.10 (June 2025), to be available for FMC and cdFMC. TND on Secure Access comes out in May 2025.

UZTNA Demo

Secure Access + NGFW

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#)

Connector Groups Network Tunnel Groups FTDs

Next steps

Resource connectors deployed in a connector group will connect user traffic to all private resources assigned to the group. After one or more connector groups is configured, take the following steps to deploy connectors in the connector groups and assign private resources to groups. [Help](#)

1 Deploy your Connectors

Create connectors using the image provided by Cisco.

[Connector Image for AWS](#)

- Each connector in a group must be able to connect to all of the resources assigned to the group.
- All connectors in a group must use the same deployment environment, for example AWS or VMware.
- Deploy at least two connectors in each connector group for redundancy during connector upgrades.
- An image can be used for any connector group that uses the same environment.
- When you create each connector, you will associate it with a connector group using the connector group's provisioning key from the table below.

Connector Group	Environment	Provisioning Key
jelin-aws-GSAT-VPC	AWS	...

2 Confirm Connectors

3 Assign Private Resources to Connector Group

Hybrid Private Access
(with Secure Firewall)

Role of Identity in UZTNA

Attackers Adapting: Session Hijacking is on the rise

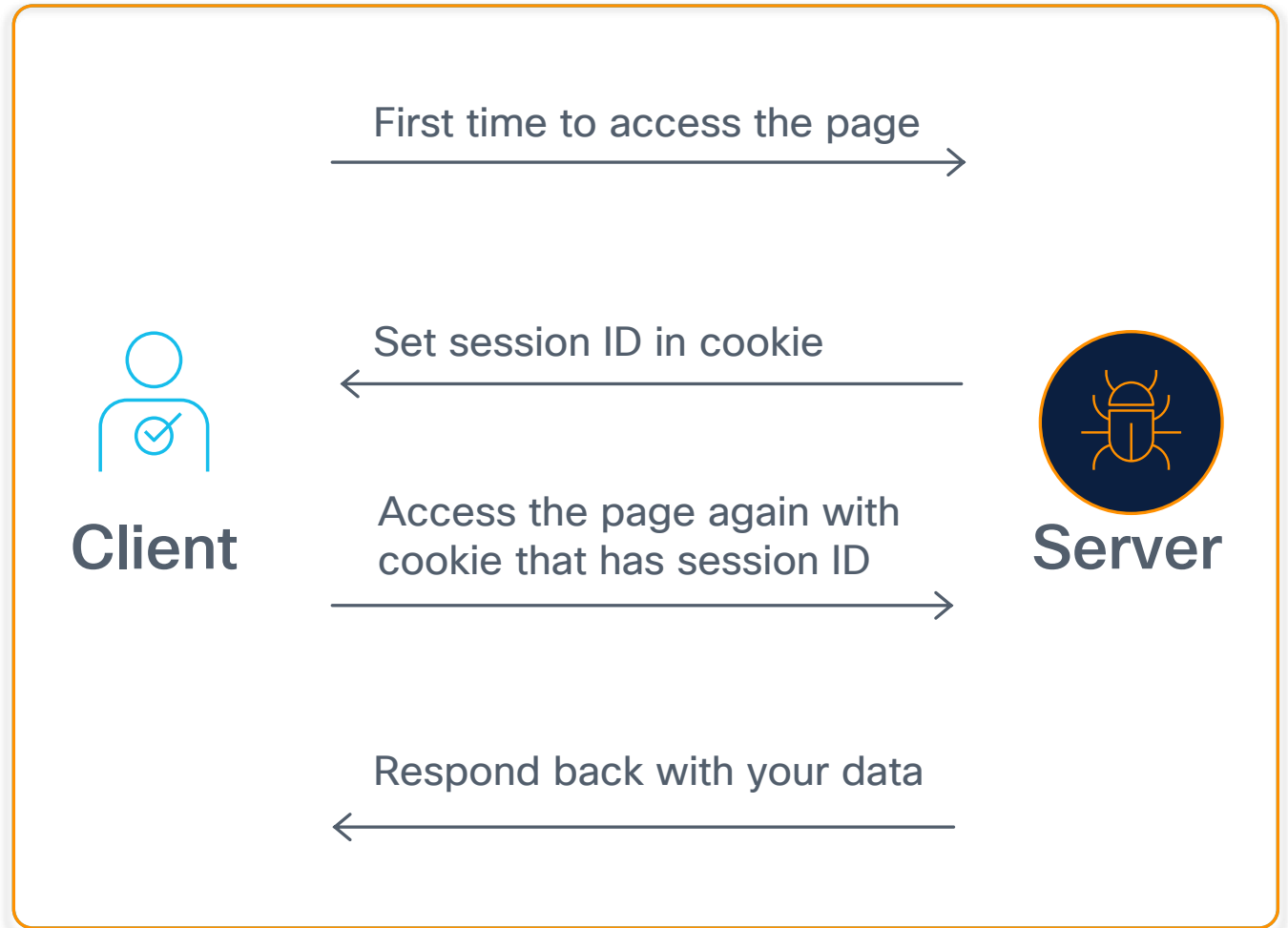
- How does it work?

What happens if an attacker steals a session cookie?

- Bypass multi-factor authentication and act as the user.
- They can log in anywhere SSO is allowed.
- Can establish permanent access and enroll new MFA devices

Huge, recent breaches

- CitrixBleed VDI Breach
- Okta Breach
- Google Cloud Breach
- Slack-Github Data Breach



How are you tracking identities?

genie

Integration Status

No Providers Synced

10 waiting for collection

[Last data collection](#)

Providers

 **Demo AWS**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 26 records

 **Demo Azure AD**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 25 records

 **Demo GSuite**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 65 records

 **Demo Okta**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 133 records

 **Demo Workday**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 43 records

 **Demo Auth0**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 45 records

 **Demo Duo**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 59 records

 **Demo GitHub**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 19 records

 **Demo Salesforce**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 44 records

 **Slack - oort-teamdata-testing**
Connectivity: N/A
Collection Status: Unknown
Average Traffic: 10 records

Ticketing

 **Cisco Jira**
Connectivity: N/A

 **ServiceNow Instance**
Connectivity: N/A

Notification Targets

 **Okta Workflow**
Connectivity: N/A
Configured for 0 checks

 **oort-demo**
Connectivity: N/A
Configured for 0 checks

© 2025 Cisco and/or its affiliates. All rights reserved.

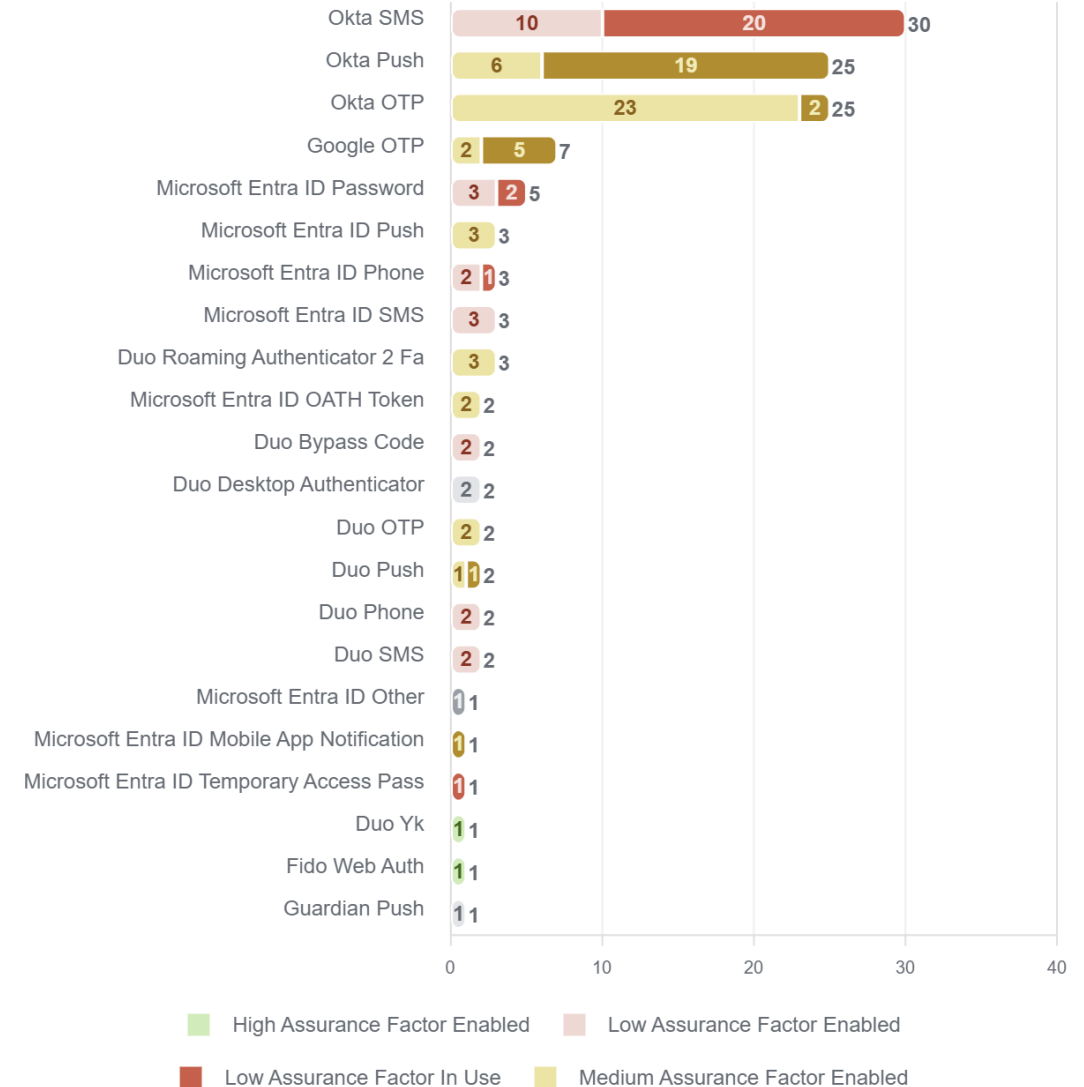
BRKSEC-2176



MFA Prevalence

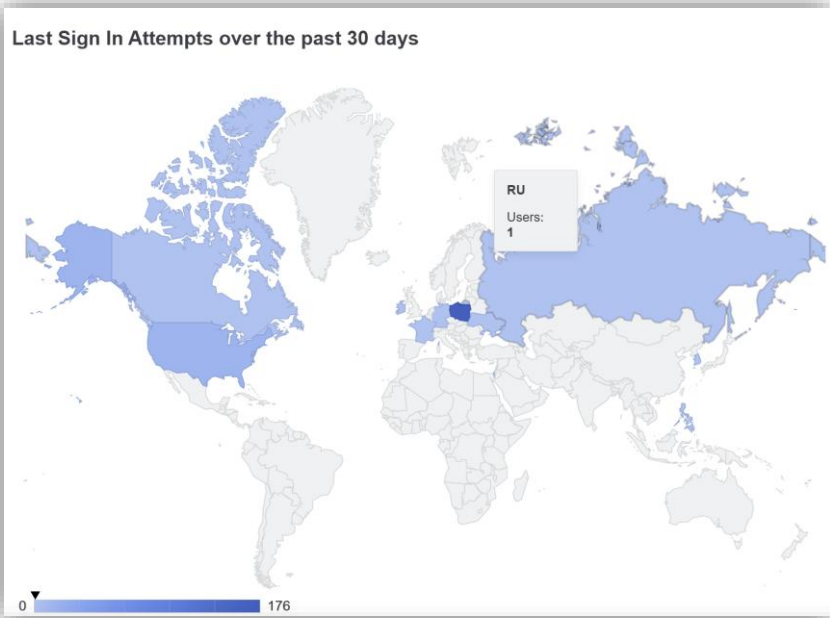
- I call this the compliance check
- Did the bad actor breach your network via password reset?
- Are the users connecting as corporate policy dictates?

MFA Prevalence by User Count



Unsanctioned Access

- Where did the bad actor originate?
- Access from unusual locations?



Dashboard > Users

<> Advanced ×

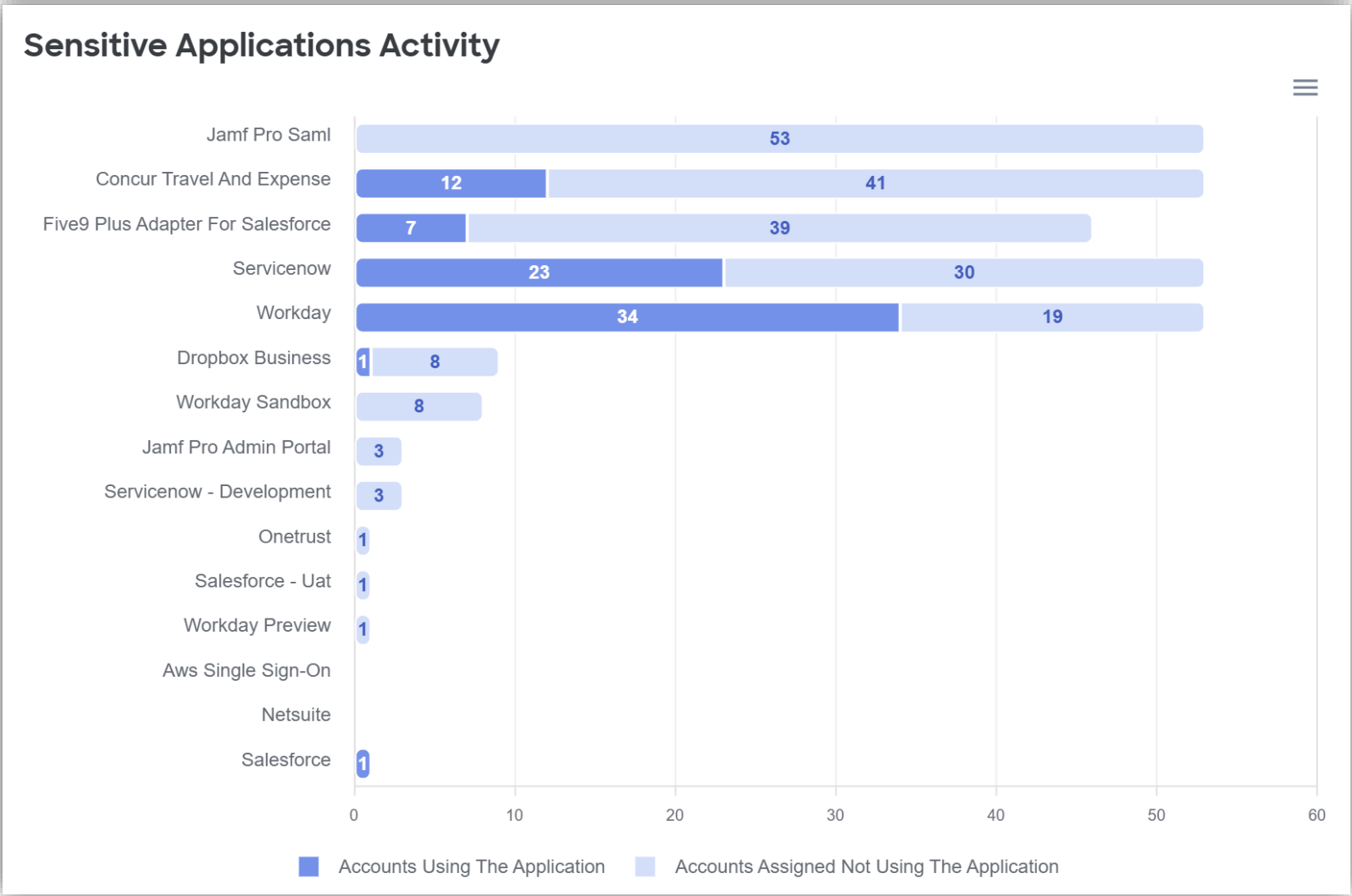
1 user found

Columns

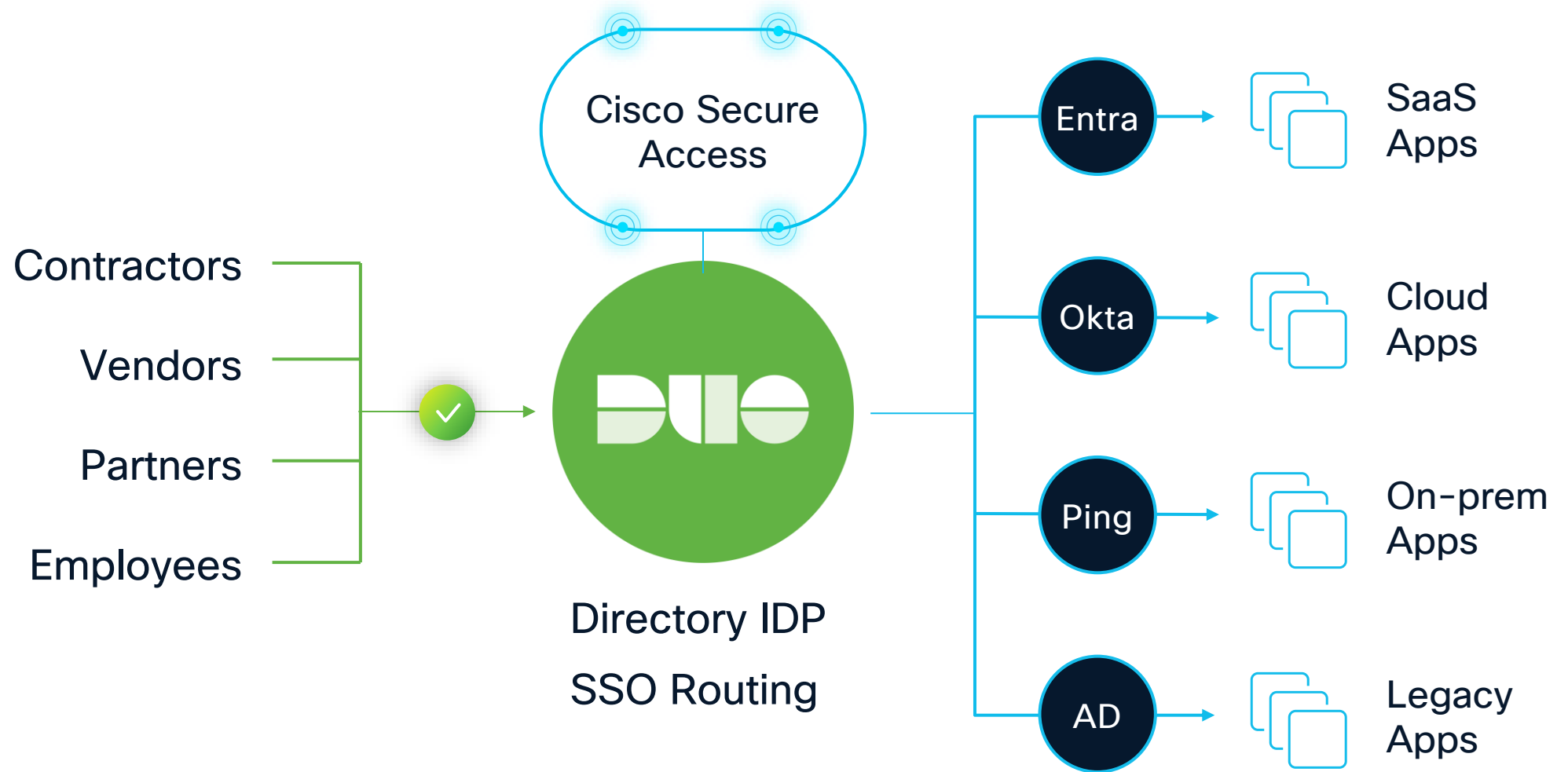
User	Trust Level	Checks	# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Prov
Kolluri Hofferber kolluri.hofferber@simubiz.com	Neutral	7	6	38	A Day Ago Nov 26, 2024 23:59:59	46.3.27.137	Perm, Perm Krai, RU		

Who's using your critical applications?

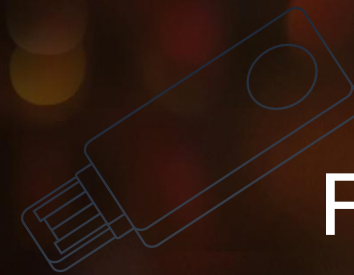
- Which applications seem abnormal?



Identity Broker for IAM



End-to-end phishing resistance



FIDO2, Hardware
Tokens

≡ Collapse

🏠 Home

👤 Users

💻 Devices

🛡️ Policies

📄 Applications

📊 Reports

🔍 Monitoring

📄 Billing

⚙️ Settings

← Users

jheary

Logs | Verify with government ID | Send Duo Push | 🗑️ Send to Trash

Password

Password set by user

Password last set on August 2, 2025 at 5:07 PM.

[Reset password](#)

[Learn more about Duo IdP and other password reset options](#)

Device enrollment

🟢 Enrolled

Username

jheary

[+ Add a username alias](#)

Username aliases

Users can have up to 8 aliases.

[Click here for a specific alias](#)

Zero Imposters: Verify Digital Identity

Display Name

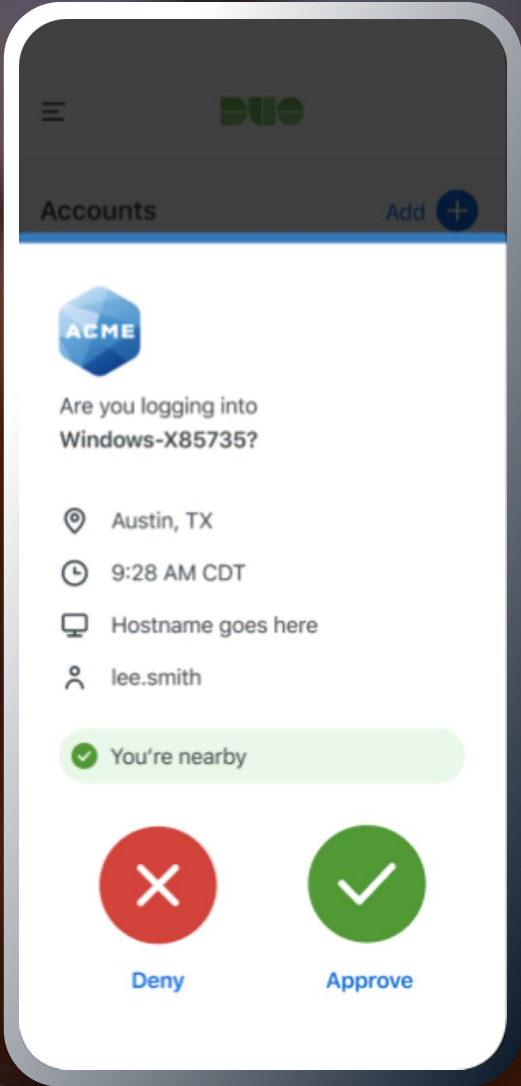
Jamey Heary

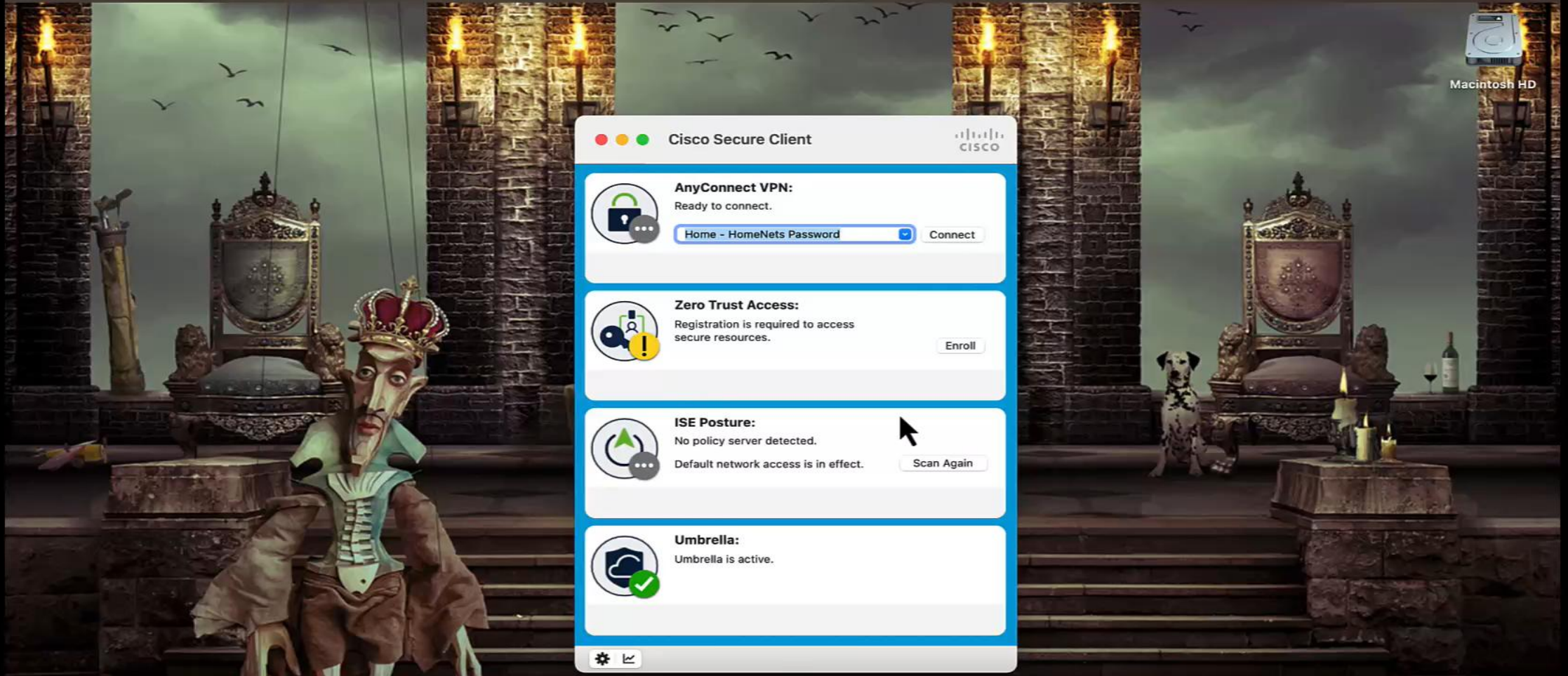
End-to-end phishing resistance

Proximity
Verification



Bluetooth Low
Energy (BLE)



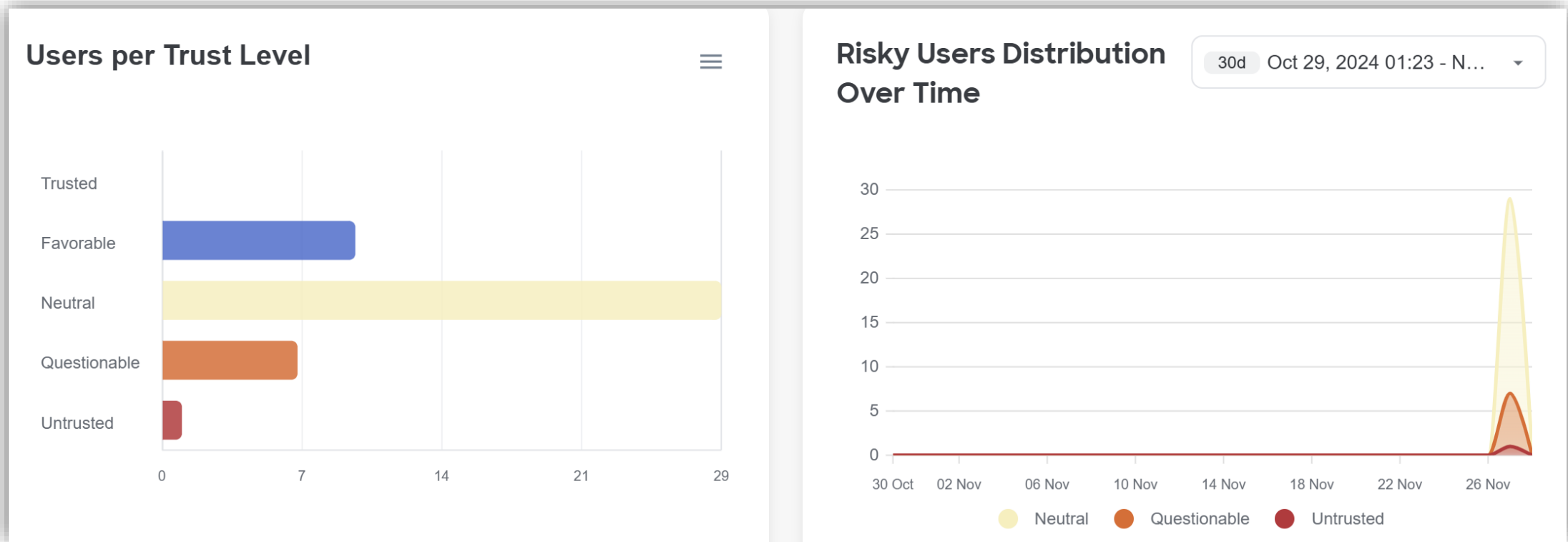


ZTA Enrollment with Duo Proximity

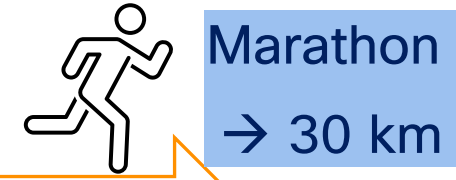


Cisco Identity Intelligence User Trust Levels

- Monitoring user behavior over time
- Can you enforce User Trust Levels across all enforcement points in the network?



Zero Trust in 4 use cases



Admin Access

Remote Worker
(Edge)

On-Premises
(Campus)

Application to Application
(Data Centers)



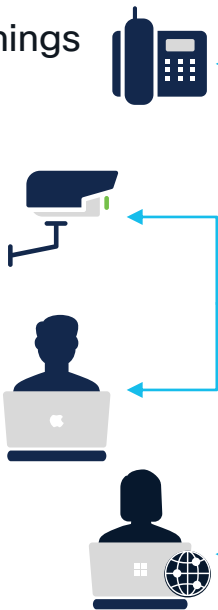
ISE Provides Zero Trust for On-Premises

Enterprise

Security

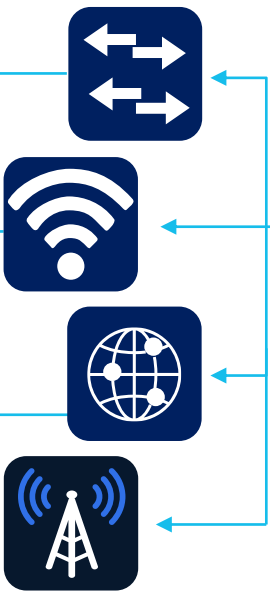
Endpoints

- Users
- Devices
- IOT Things



Network Devices

- Switches
- WLCs / APs
- VPN



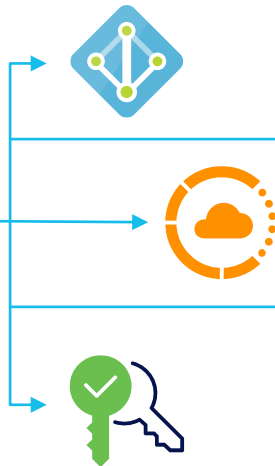
Cisco ISE

- Shared or Distributed
- VM/Appliance/Cloud
- Up to 2M Endpoints
- RADIUS and TACACS
- pxGrid



Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA



Security Services

- Cloud Analytics
- Secure Firewall
- Partners



See It

Secure It

Share It

Dynamic Classification and SGT Assignment via ISE

Cisco ISE

Policy • Policy Sets

🔍 ? 📄 ⚙️

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
🟢	Default	Default policy set		Default Network Access	0
> Authentication Policy (3)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
✓ Authorization Policy (15)					

+

Status

Rule Name

Conditions

Profiles

Security Groups

Hits

Actions

🔍 Search

🟢	Employee BYOD	AND AND BYOD_is_Registered EAP-TLS CERTIFICATE:Subject Alternative Name EQUALS Radius-Calling-Station-ID ise-cream-ExternalGroups EQUALS ise-cream.inc/Users/Domain Users	PermitAccess x	Employees	0
---	---------------	--	----------------	-----------	---

Context

Security Group

🔍

Security Groups

Auditors

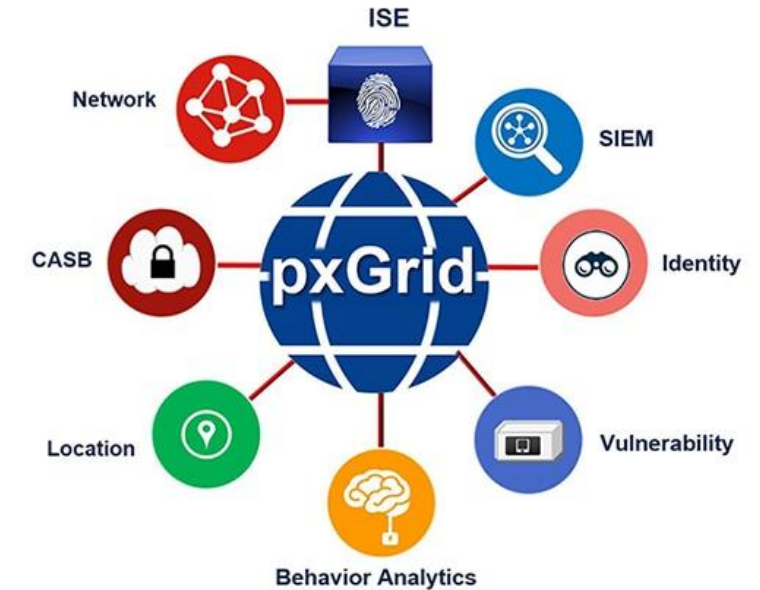
BYOD

Contractors

Developers

Cisco Platform Exchange Grid(pxGrid)

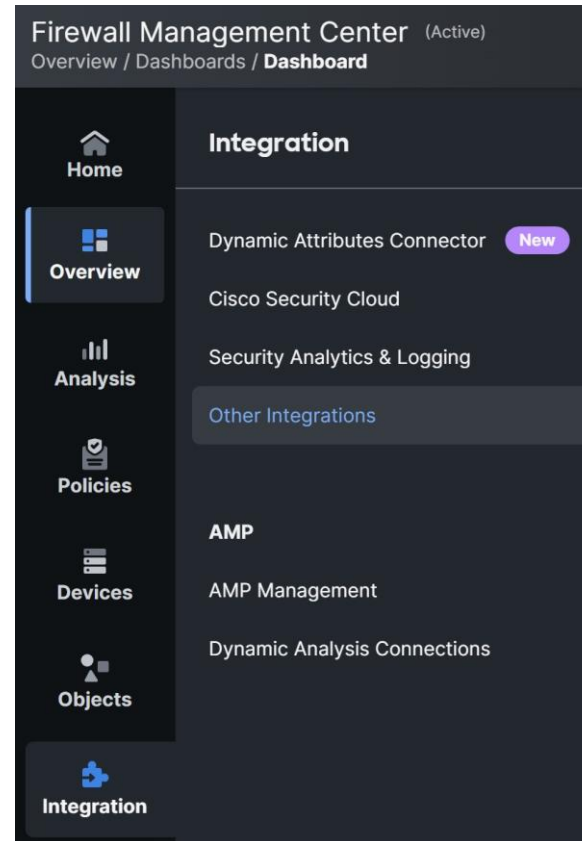
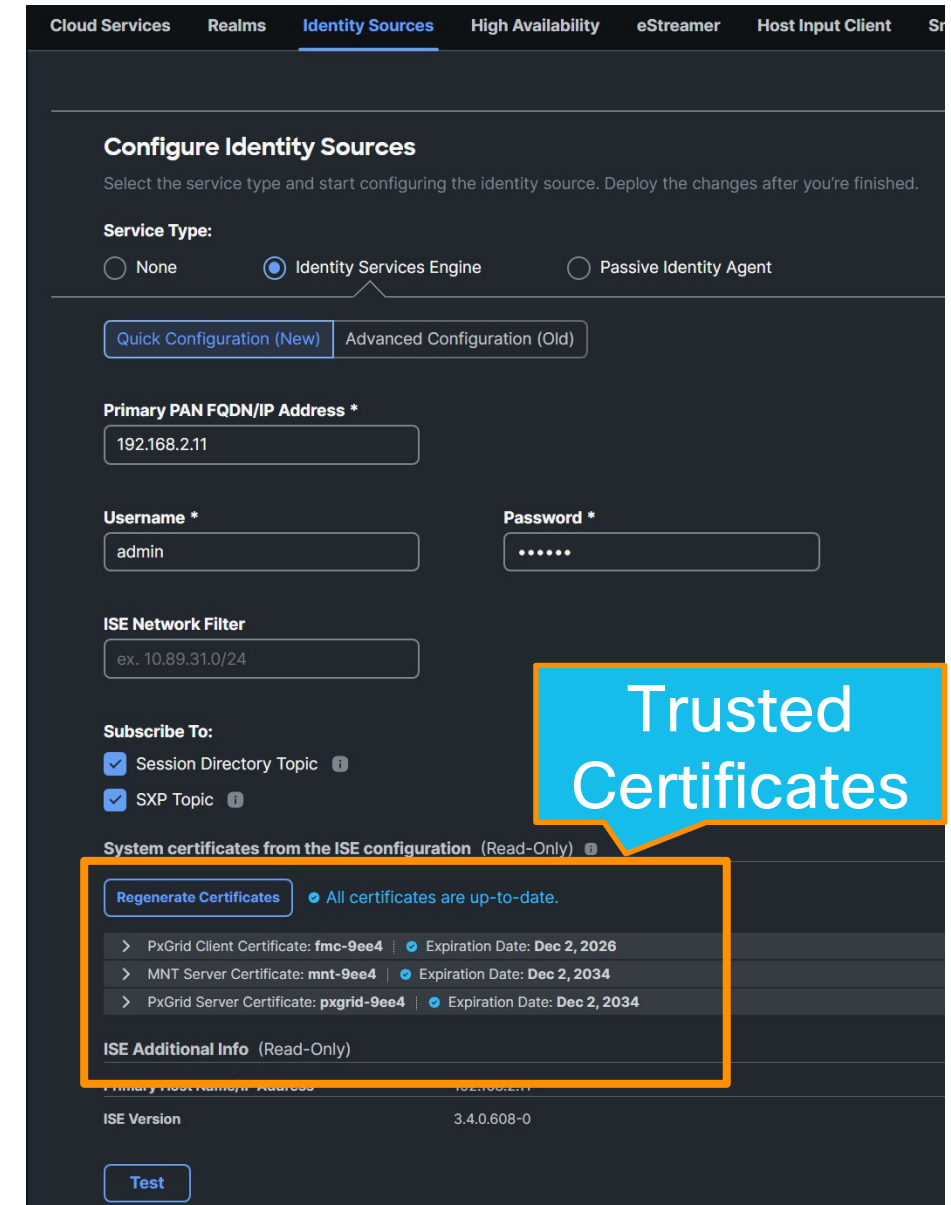
- Open, scalable, IETF standards-driven; IETF RFC8600 XMPP (Extensible Messaging and Presence Protocol) for Security Information Exchange
- Data broker and consumer relationship
- pxGrid Cloud (May 2022) available between on-prem applications and cloud-based solutions
- <https://developer.cisco.com/pxgrid-cloud/> to learn more
- ISE ecosystem partners
 - Google, Microsoft, Ixia, SAP, and more...



Cisco Rapid Threat Containment

Firepower & ISE Integration

- Quick Configuration (New) starting in 7.6
- Auto import of ISE trusted certificate
- Minimizes human error on certificates



SGT in FTD Dynamic Attributes

Firewall Management Center (Active)
Policies / Access Control / Policy Editor

SearchDeploy4SettingsHelpJerry

1

Editing Rule Inspect_All

Mandatory

NameInspect_All

↕

ActionAllow

LoggingON

Time RangeNone

Rule Enabled

Intrusion PolicyIPS-policy

Default-Set

File PolicyNone

Search

Zones

Networks

Ports

Applications

Users

URLs

Dynamic Attributes (2)

VLAN Tags

Search Dynamic Attribute Objects

Total 20

Selected Sources: 2

Selected Destinations and Applications: 0

Filter by type

Device Type

ISE Security Group T...

Dynamic Objects

Location IP

Dynamic Attributes

Production_Users (ISE Security Gr...

Quarantined_Systems (ISE Securit

Test_Servers (ISE Security Group ...

TrustSec_Devices (ISE Security Gr...

Unknown (ISE Security Group Tag)

VPN_Employee (ISE Security Grou...

7

255

13

2

0

16

+ Create External Attributes

Collapse All

Remove All

DYN

2 Objects

Quarantined_Systems

VPN_Employee

Any

Add Source Dynamic Attribute

Add Destination Dynamic Attribute

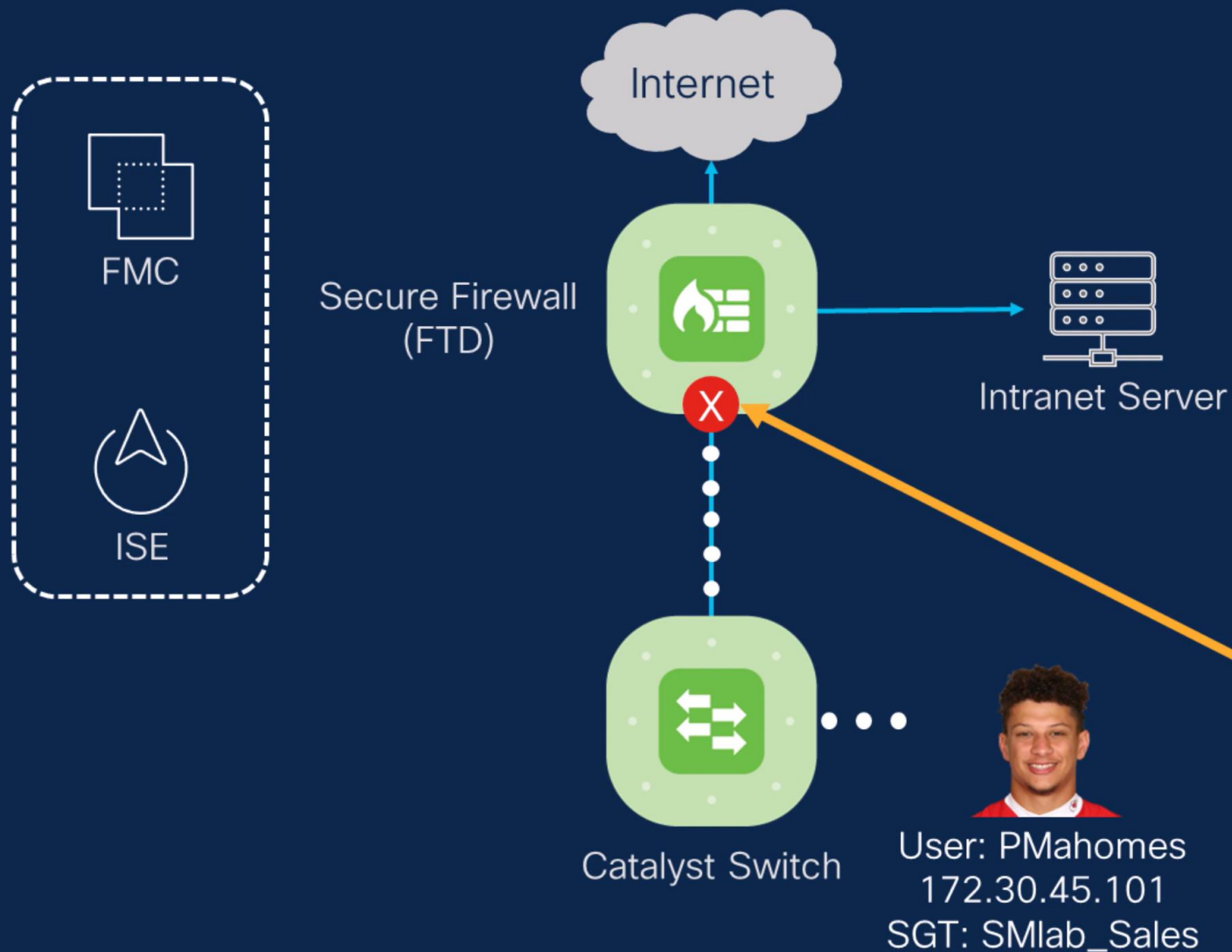
Comments (1)

Cancel

Apply

SGT Demo

Rapid Threat Containment – Firewall Enforcement



- 1) IPS rule triggers on malicious traffic from PMahomes to the Intranet Server
- 2) Secure Firewall and FMC send notification to ISE of this event
- 3) ISE assigns the Quarantined_Systems Security Group TAG
- 4) Subsequent traffic is blocked at the firewall based on the TAG

Add jelin-testpolicy

Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

☒ Rule is enabled

Logging is enabled [Edit](#)

Summary

Sources

Any

Allow

Security Controls

Destinations

Any private destination

Rule name

jelin-testpolicy

1 Specify Access

Specify which users and e

Action

Allow

Allow specified traffic i
met.

✓ **Allow**
Allow specified traffic if security requirements are met.

✗ **Block**
Block specified traffic.

From
Specify one or more **sources**.

Any

Select sources

Add a source

Users14 >

Groups1 >

Endpoint Devices11 >

Security Group Tags0 >

Network Tunnel Groups15 >

Network Objects and Network Object Groups0 >

To
Specify one or more **destinations**.

Any

Zero Trust Browser-based Posture Profile

Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

Profile: **None** | Requirements: **None**

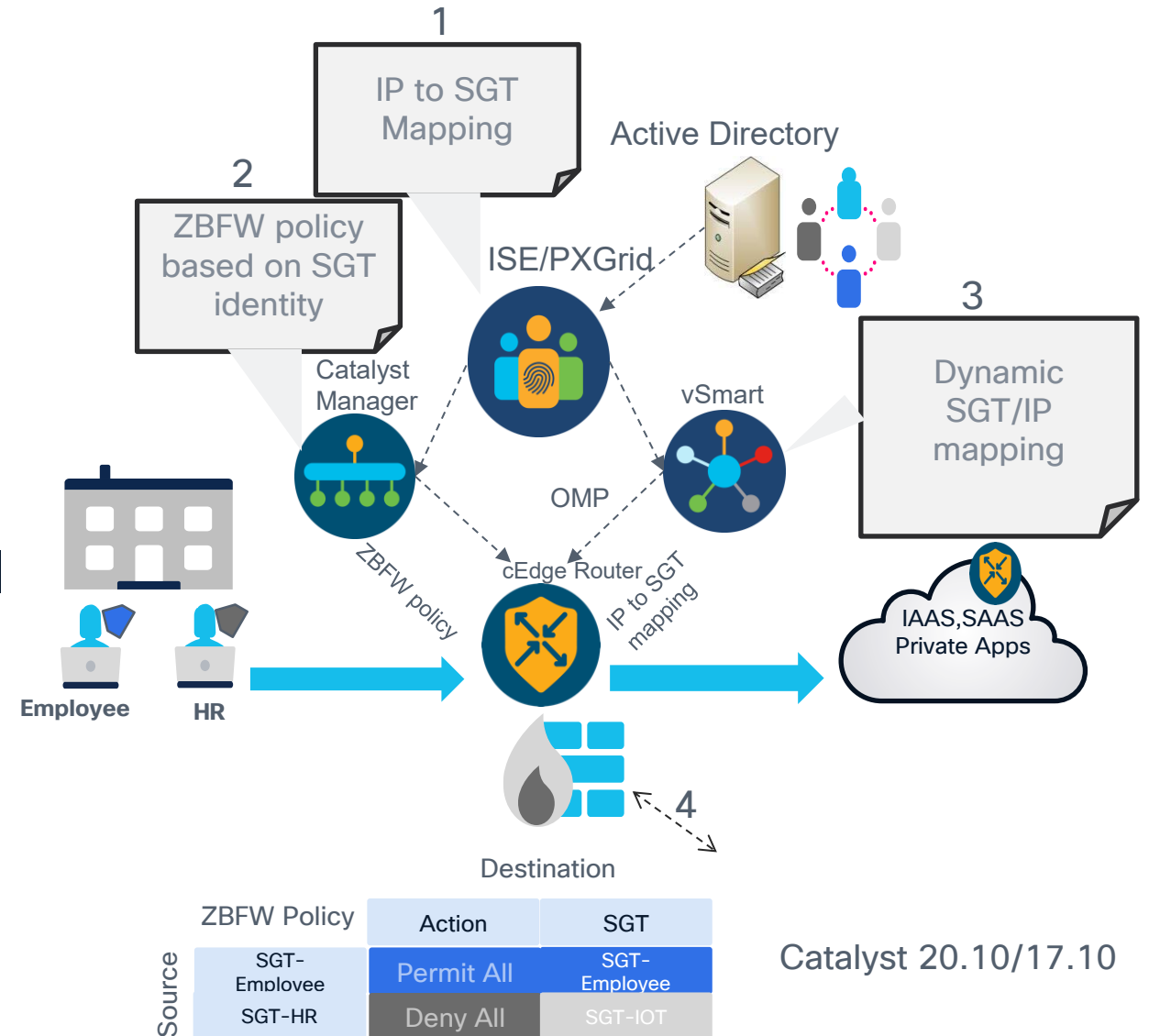
BRKSEC-2176

Catalyst SDWAN integration with ISE/TrustSec

Problem: SDWAN customers require segmentation and to meet compliance/regulations such as PCI

Solution: Catalyst SDWAN integrates with ISE via pxGrid for IP/SGT binding sharing. SDWAN can use SGACL(stateless FW) or ZBFW(stateful ACL) for identity enforcement

Outcome: Seamless segmentation policy from campus to SDWAN for security policy compliance



Catalyst SD-WAN Manager Example

Catalyst SD-WAN

Monitor

Configuration

Configuration Groups

Policy Groups

Network Hierarchy

Topology

Policy Groups

Policy Group 10Application Priority & SLA 8NGFW 5Secure Internet Gateway / Secure Service Edge 7DNS Security 0

NGFW Policy 5

Search Table

As of: Jan 26, 2025 01:19 PM

Name	Description	Device Solution	Policy Group	References	Updated By	Last Updated
SecPolicy-npitaev		sdwan	DC2-Policy-Group,Secure-Edge-SSE-NGFW-App	2	ashtwill	Dec 10, 2024, 2:47:
sdwandemo-ID-NGFW		sdwan		0	ashtwill	Jan 10, 2025, 9:14:1
SMB_NGFW		sdwan	SMB_Policy BRKSEC-2176	1		

Group of Interest

Catalyst SDWAN Manager: SGT Policy



Monitor



configuration



Analytics

Tools


[Reports](#)

Additional Settings

Default Action: Drop

Source		Destination	
SGT	IOT_Sensors	SGT	IOT_Management-Cor

- ☰
- Organization
GSSO-GSAT
- Home
- Products
- AI Defense
- Firewall
- Hypershield
- Multicloud Defense
- Secure Access
- Secure Workload
- Platform services
- Favorites
- Identity Intelligence
- Security Devices
- Shared Objects
- Platform Management

Home

Set default homepage

All Insights

Top Insights & Alerts 12 Active Insights

📈 Access Control Policy Anomalies ...

Data source: Test-abc Cloud-delivered FMC

AIOps has detected 32 anomalies in Access Control policy 'Test-abc'.

25d ago [Details](#)

📈 Best practices and recommendations ...

Data source: ftdv-test6

AIOps has detected 6 needs review checks.

21d ago [Details](#)

📈 Best practices and recommendations ...

Data source: ftdv-test5

AIOps has detected 6 needs review checks.

21d ago [Details](#)

Multicloud Defense

Multicloud Defense ::

Account Resources

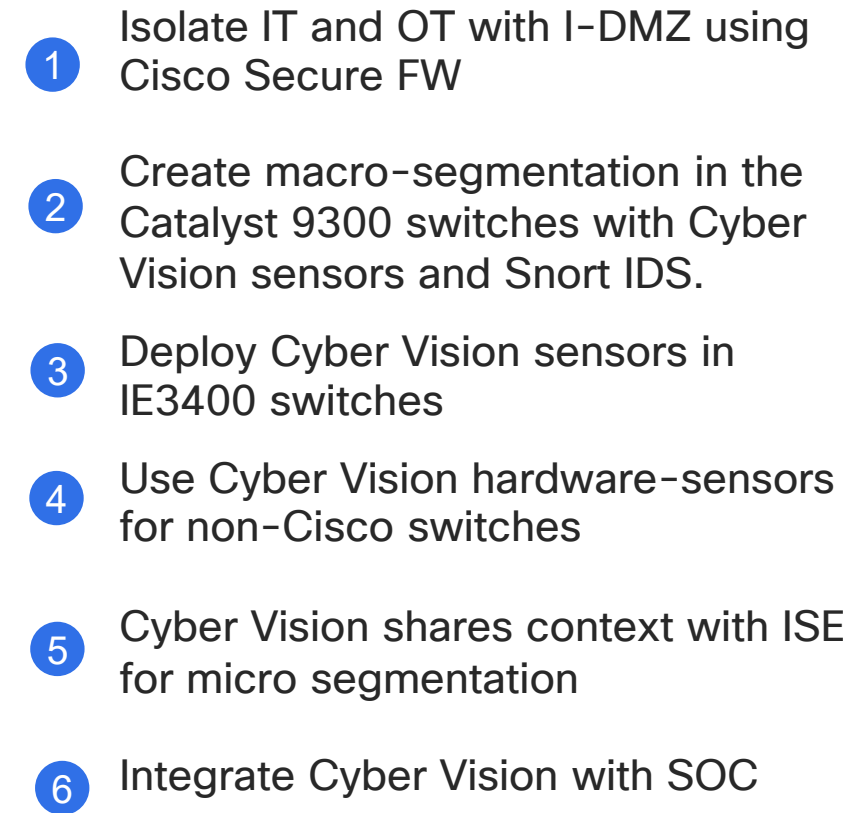
21 VPCS/ VNets	35 Security Groups	31 Route Tables	69 Subnets
8 Instances	1 Load Balancers	0 Tags	1 Applications

Security Considerations

VPCs/VNets not protected

0 Service VPC/VNets without Gateways

Catalyst SASE Use cases



TrustSec/SGT Success & Failure Tips

- Don't try boil the ocean
- Have Executive Sponsorship
- ISE/TrustSec/SGT won't solve ALL problems
- Zero Trust / Segmentation is an ongoing process

Zero Trust Use Cases

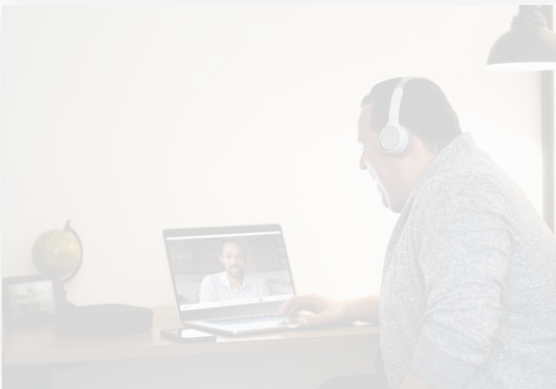
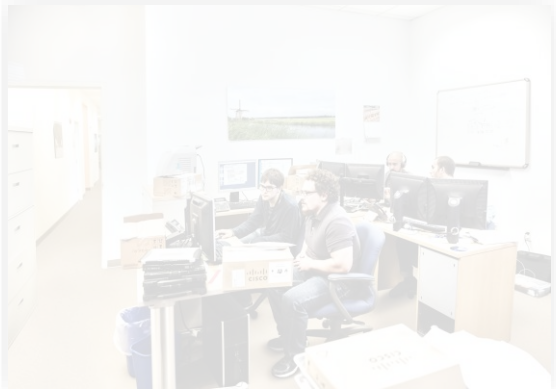


Admin Access

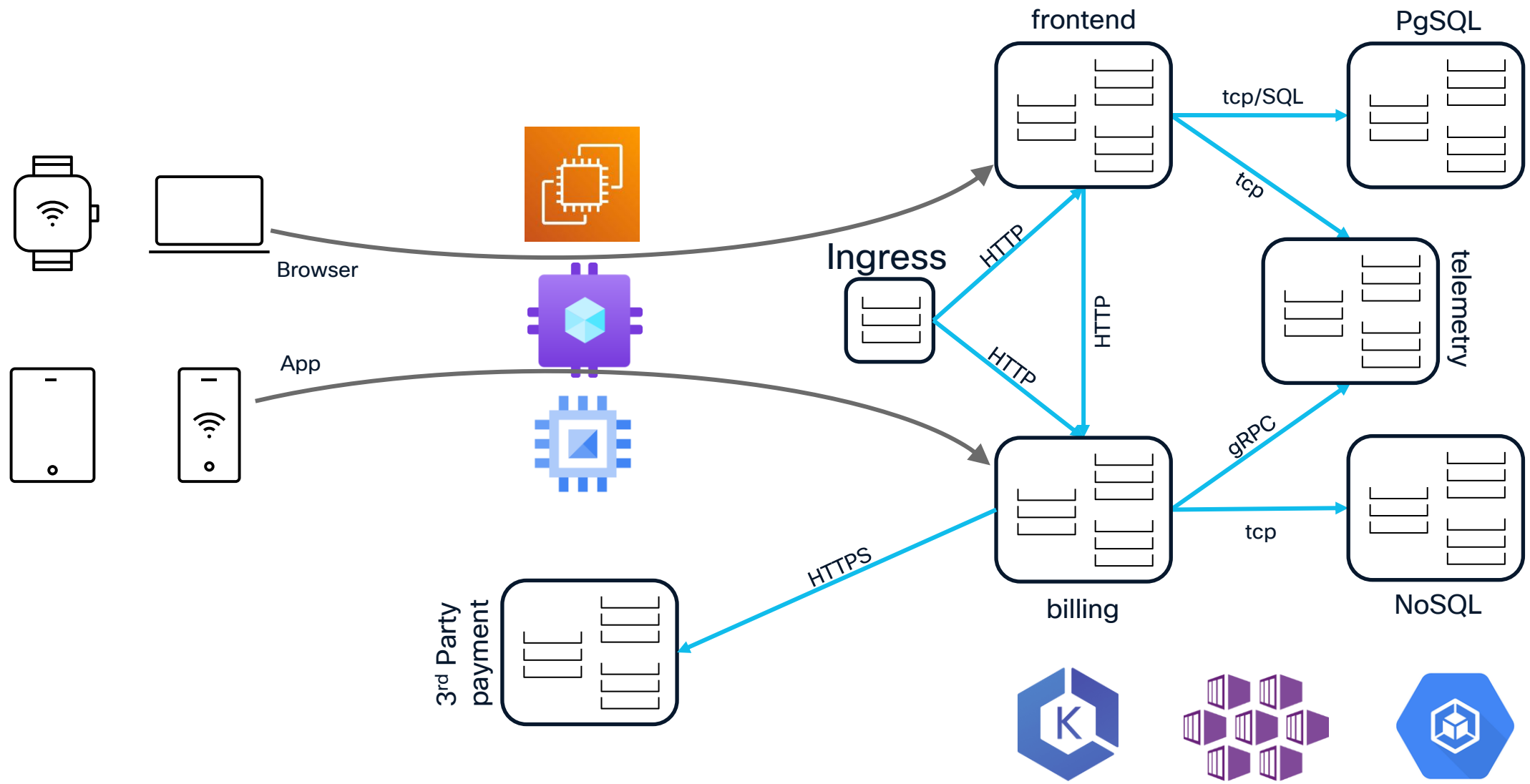
Remote Worker (Edge)

On-Premises (Campus)

Application to Application (Data Centers)



Application Architectures have evolved

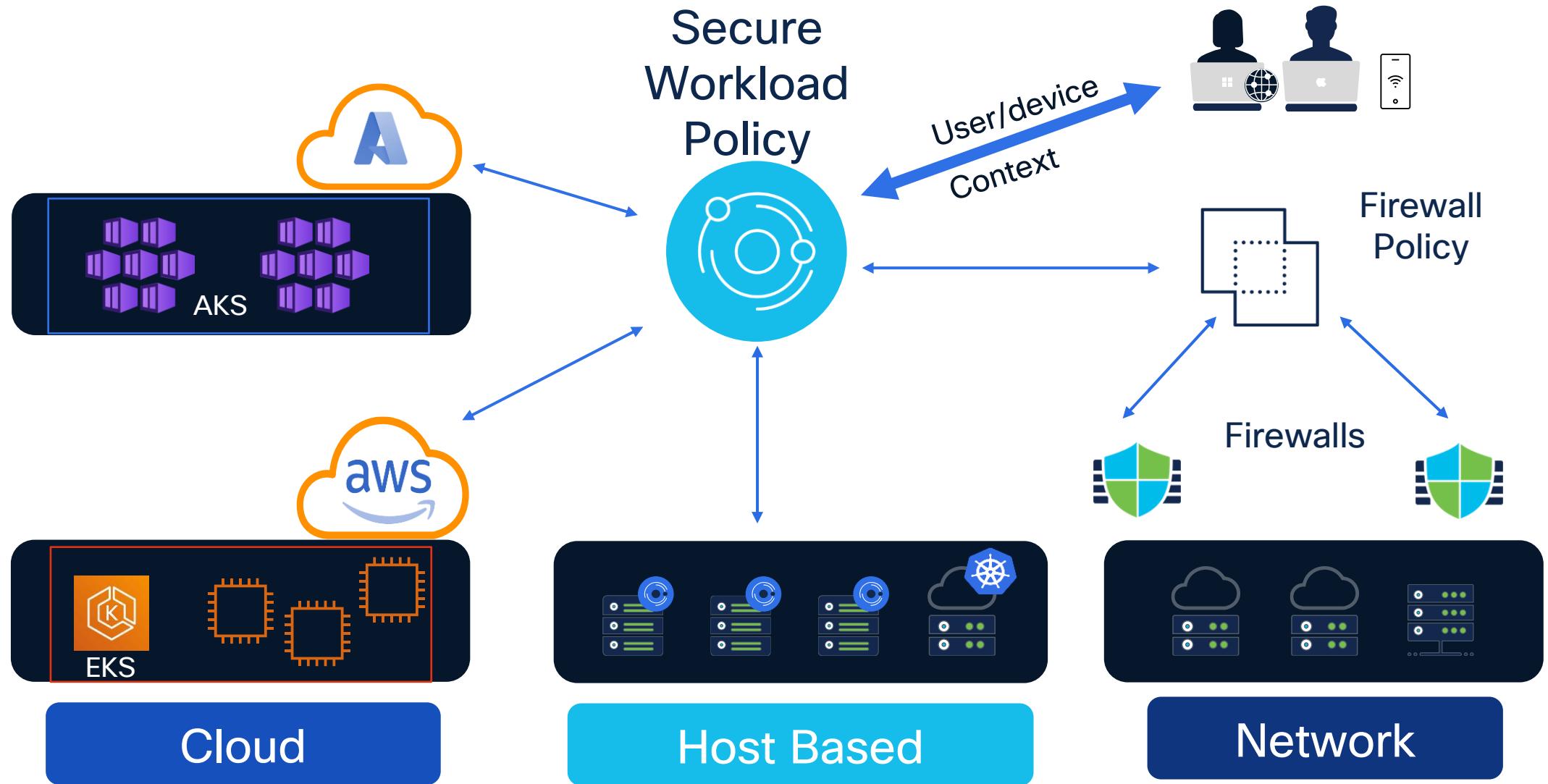


Customer Challenges: Application Visibility & Control

- How do I get visibility of my cloud apps?
- How do I extend segmentation into cloud since it's been mainly on-premises?
- What is the best policy to deploy for my environment?



Cisco Secure Workload across Hosts, Network, and Cloud



DC Unified Policy



Workload admin
makes policy
change



Secure
Firewall
Management
Center

Firewall
Policies



Cisco Secure Workload

Workspaces DC-Access-PCI Compliance (NEW) PRIMARY Version 1 View Version History

Matching Inventories 20 Policies 8 Filters 0 Conversations Provided Services Policy Analysis Enforcement Status Enforcement

Filter Policies ...

Absolute and Default Policies 7 Catch All ALLOW Grouped 1 Ungrouped

DENY and policies for ANY protocol have different behavior in Windows firewalls when compared to Linux. See User Guide for more details.

Rank ↑↓ Priority ↑↓ Action ↑↓ Consumer ↑↓ Provider ↑↓ Protocols and Ports ↑↓

Default 90 DENY Kill_Switch Finance Servers Any

Firewall Management Center Policies / Access Control / Policy Editor Overview Analysis Policies Devices Objects Integration Deploy

Return to Access Control Policy Management

FTDV-AWS-policy

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More

No Identity policy selected Total 13 rules

	Name	Action	Zones	Networks	Ports	Dynamic Attributes
▼	Mandatory (1 - 6)					
	1 Workload_golden_1	➔ Allow	Any	Any	TCP (6):5640	WorkloadObj_collector
	2 Workload_golden_2	➔ Allow	Any	Any	Any	Any
	3 Workload_golden_3	➔ Allow	Any	Any	TCP (6):5660	WorkloadObj_collector
	4 Workload_golden_4	➔ Allow	Any	Any	Any	Any
	5 Workload_golden_5	➔ Allow	Any	Any	TCP (6):443	WorkloadObj_wss
	6 Workload_golden_6	➔ Allow	Any	Any	Any	Any
▼	Default (7 - 13)					
	7 Workload_7	⊖ Block	Any	Any	Any	WorkloadObj_JumpPC1_non_PCI
	8 Workload_8	⊖ Block	Any	Any	Any	WorkloadObj_VPN1120_contractor
	9 Workload_9	⊖ Block	Any	Any	Any	WorkloadObj_Kill_Switch
	10 Workload_10	⊖ Block	Any	Any	Any	WorkloadObj_JumpPC1_non_PCI
	11 Workload_11	⊖ Block	Any	Any	Any	WorkloadObj_JumpPC1_non_PCI

Secure Workload + AWS Security Groups

Security Groups (1/2) Info

Filter security groups

Actions

Export security groups to CSV

Create security group

< 1 >

	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules co
☐	-	sg-00e837e70e5780e33	default	vpc-04ae4072760e59d34	default VPC security gr...	998494316702	2 Permission entries	2 Permission entries
☒	-	sg-0d5de67ce7f8d1c03	csw_a042ddfb_15803...	vpc-04ae4072760e59d34	Cisco Secure Workload...	998494316702	5 Permission entries	0 Permission entries

sg-0d5de67ce7f8d1c03 - csw_a042ddfb_1580330995_000_1658016423

Details

Inbound rules

Outbound rules

Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (5)

Filter security group rules

Manage tags

Edit inbound rules

< 1 >

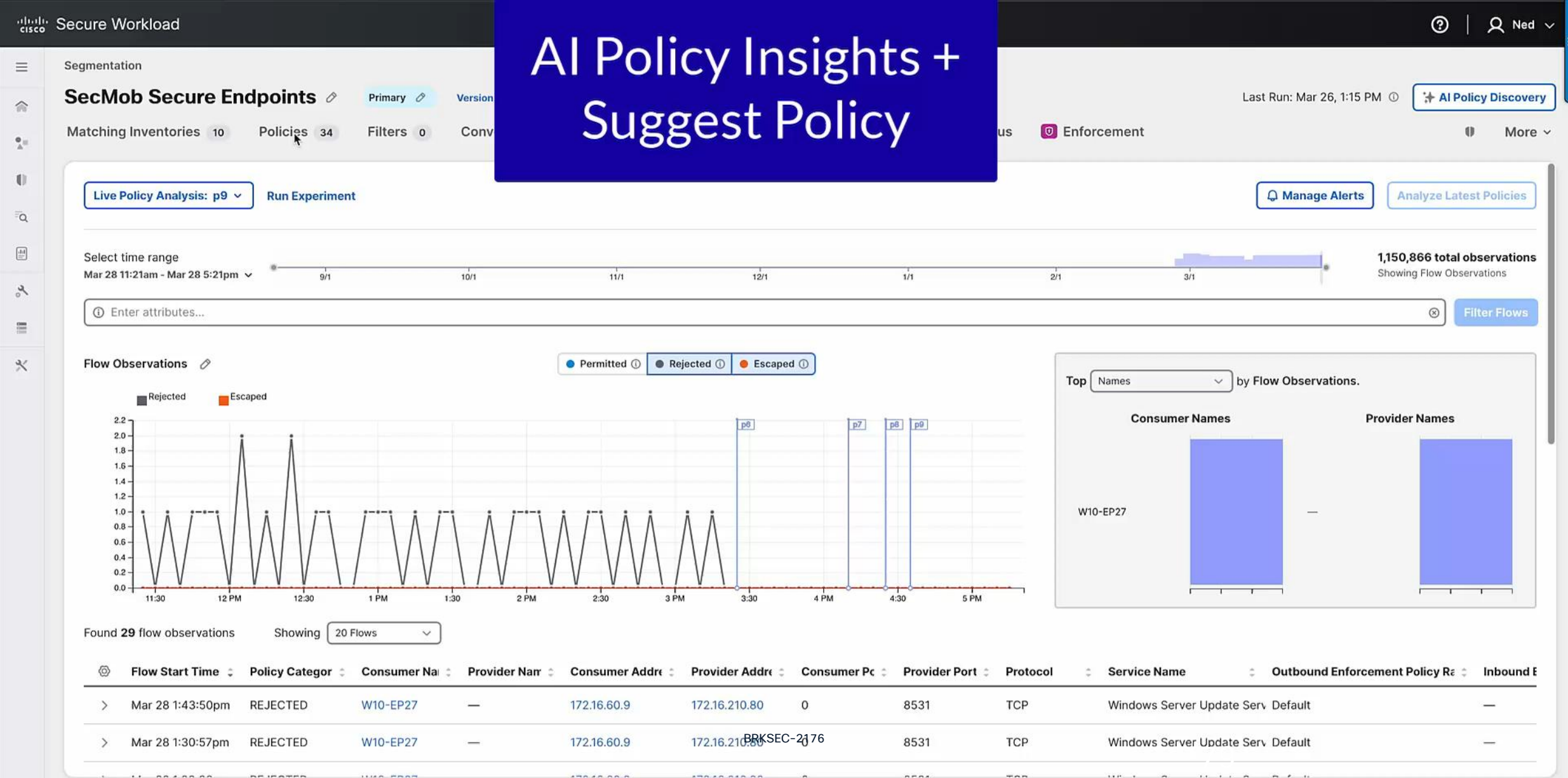
	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☐	-	sgr-0b5d8151025e45...	IPv4	All ICMP - IPv4	ICMP	All	10.2.2.40/32	PolicyId=DEFAULT:10...
☐	-	sgr-074b79bec5c6d6c4e	IPv4	SSH	TCP	22	10.11.11.11/32	PolicyId=DEFAULT:95...
☐	-	sgr-05b25baa33e6b81...	IPv4	All ICMP - IPv4	ICMP	All	10.11.11.10/32	PolicyId=DEFAULT:90...
☐	-	sgr-07d472ff135d12542	IPv4	Custom TCP	TCP	80 - 443	10.11.11.11/32	PolicyId=DEFAULT:95...
☐	-	sgr-093010afe37dd9ed3	IPv4	All ICMP - IPv4	ICMP	All	10.11.11.11/32	PolicyId=DEFAULT:95...

Dynamic Push

Automated Policy Lifecycle Management

AI Policy Insights / Suggested Policy v1

Available Now -3.10.1



Extending Policy Enforcement into Cloud

Secure Workload

Workload - AWS Enforcement

Scopes and Inventory

CSW-TME

Filter scopes...

89 scopes and 17 matching inventory filters

csw-tme-account

2 / 10 Children

Inventory: 94

us-east-1

2 / 2 Children

Inventory: 51

us-west-2

4 / 6 Children

Inventory: 43

Security-Services-DEV

0 Children

Inventory: 0

Security-Services-PROD

0 Children

Inventory: 0

acme-saas-dev-vpc-aws

1 / 1 Children

Inventory: 1

estore dev

0 Children

Inventory: 11

acme-saas-prod-vpc-aws

1 / 1 Children

Inventory: 1

sbg-tme-account

0 Children

Inventory: 0

Azure

2 / 14 Children

Inventory: 93

CSW-TME : AcmeEnterprise

estore dev

All Inventory 11

Overlapping Scopes 0

Usages

Enter attributes...

Search Inventory

Services 0

Pods 0

Workloads 11

IP Addresses 0

11 of 11 Workloads

Orchestrator Type	Hostname	Address	OS
aws	—	10.130.3.10	—
aws	—	10.130.3.18	—
aws	—	10.130.3.77	—
aws	—	10.130.3.17	—
aws	—	10.130.3.14	—
aws	—	10.130.3.16	—
aws	—	10.130.5.10	—
aws	—	10.130.3.11	—
aws	—	10.130.3.13	—

BRKSEC-2T76

Workspace

Query

*orchestrator_application = estore dev and

*orchestrator_owner = jorgquin

There's more...in ISE/SGT

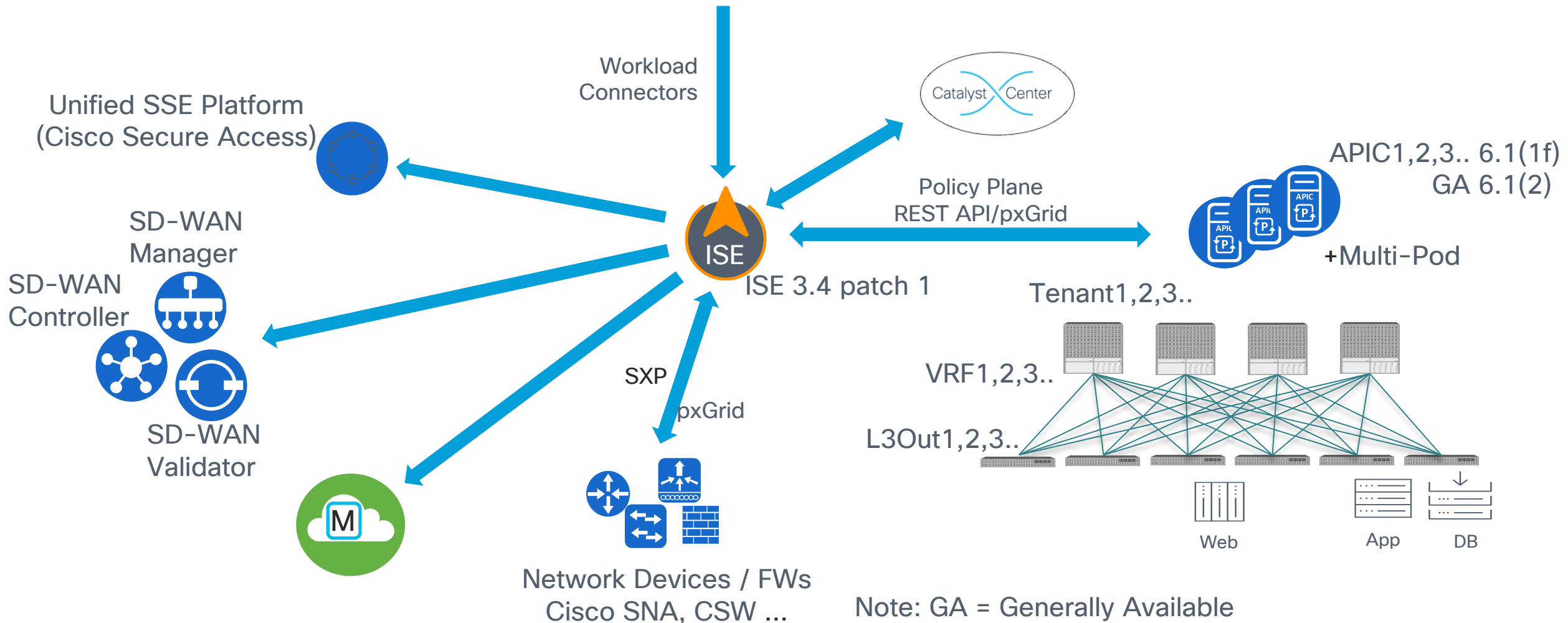
ISE Common Policy Context Sharing



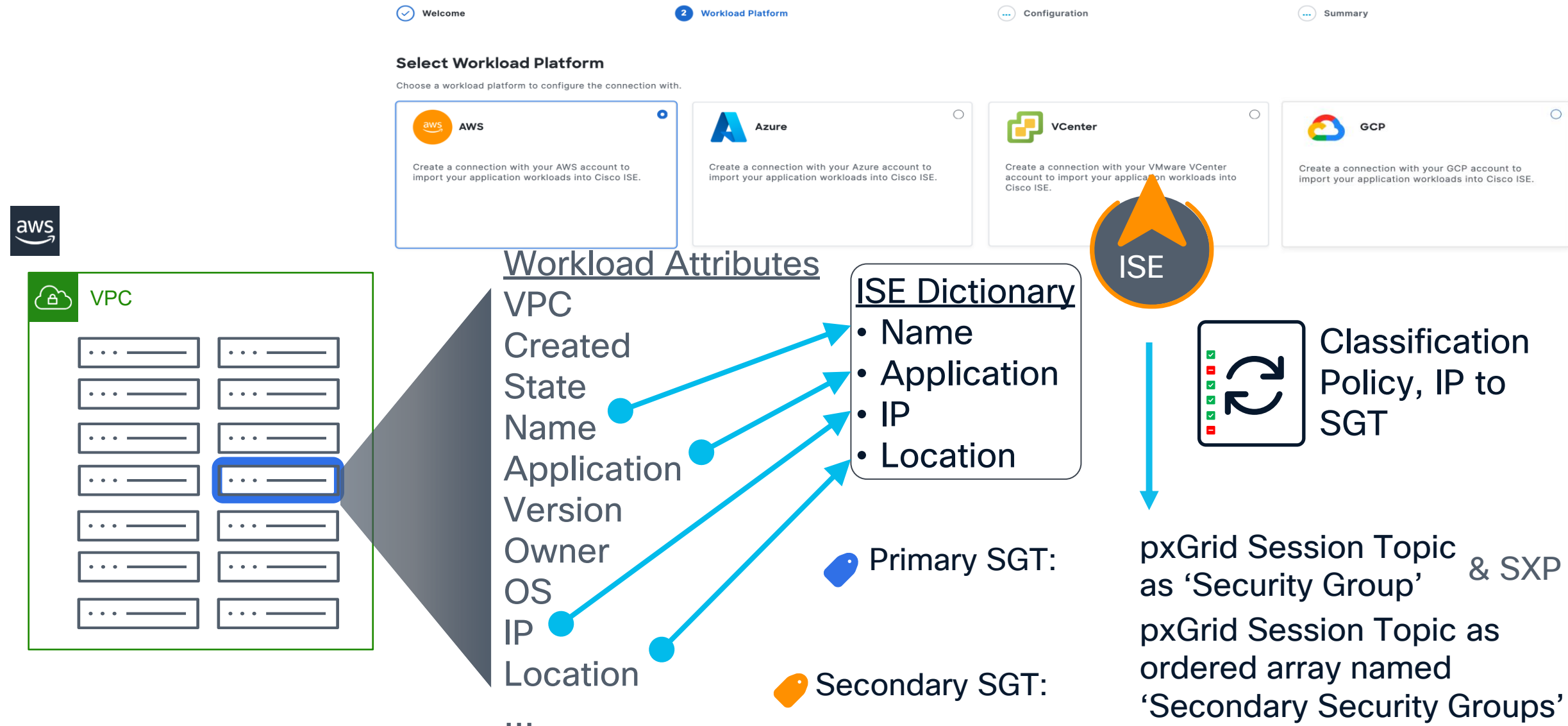
Azure

Google Cloud

vmware
by Broadcom



ISE + AWS Workload Integration



Identity Services Engine

Dashboard | EC2 | us-east-1

APIC (10.53.227.3)

Home - Cisco Catalyst Cente

Dashboard | Secure Firewall

Overview - Meraki Dashboard

Cisco Secure Access

Not Securehttps://10.53.227.37/admin/#workcenters/workcenter_trustsec/workcenter_trustsec_policy_sets_new

PersonalWork generalLabTrustSecISESDAMagellanDCSMatt/Jeff TeamCL EMEA 25CDPDNACSwitchingSecurityCL EMEA 24CL US 24

Identity Services EngineWork Centers / TrustSecEvaluation Mode 44 Days

OverviewComponentsTrustSec PolicyPolicy SetsSXPIntegrationsTroubleshootReportsSettings

Authorization Policy(30)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
+	Search						
✔	Wireless Block List Default	AND <div>Wireless_Access</div> <div>IdentityGroup-Name EQUALS Endpoint Identity Groups:Blocked List</div>	Block_Wireless_Access	Select from list	0		
✔	Profiled Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones	Select from list	29740		
✔	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones	Select from list	0		
✔	Energy Control in BldgMgmt	Kernow-AD-ExternalGroups EQUALS kernow.com/Users/Energy	1stdVLAN-BldgMgmt	Energy_Control	0		
✔	Wireless HVAC	AND <div>Radius-NAS-Port-Type EQUALS Wireless - IEEE 802.11</div> <div>Radius-User-Name EQUALS hvac</div>	Profile4Wireless	HVAC	0		
✔	Scanners in BldgMgmt	Radius-Calling-Station-ID EQUALS 00-50-56-A0-C8-67	1stdVLAN-BldgMgmt	Scanners	0		
✔	Employees in BldgMgmt	Kernow-AD-ExternalGroups EQUALS kernow.com/Users/Employees	1stdVLAN-BldgMgmt	Employees	0		
✔	Doctors in BldgMgmt	Kernow-AD-ExternalGroups EQUALS kernow.com/Users/Doctors	1stdVLAN-BldgMgmt	NHS	5		
✔	Lighting in BldgMgmt	Kernow-AD-ExternalGroups EQUALS kernow.com/Users/Lighting	1stdVLAN-BldgMgmt	Lighting	0		
✔	PACS from profiling	EndPoints-EndPointPolicy EQUALS Abatron-Device	1stdVLAN-BldgMgmt	Storage	0		
✔	PACS from MAC	Radius-Calling-Station-ID EQUALS 00-50-56-A0-D7-3F	1stdVLAN-BldgMgmt	Storage	0		

https://10.53.227.37/admin/#workcenters/workcenter_trustsec/workcenter_trustsec_integrations



Marathon
42.16 km

Summary



Zero Trust in 4 use cases



Marathon
→ 42.16 km

Segmentation

Admin
Access

Remote
Worker

On-
Premises

Application
to
Application



Review and Take Aways



Marathon Completed!

1

Have a Zero Trust Plan

- Deliver excellent user experience
- Address the Identity problem

2

Develop Segmentation Plan

- UZTNA, ISE+TrustSec
- Unify IT/OT if practical

3

Zero Trust policy should be end-to-end

- Include workload and application security

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

Contact me at: jelin@cisco.com

Thank you

CISCO Live !

