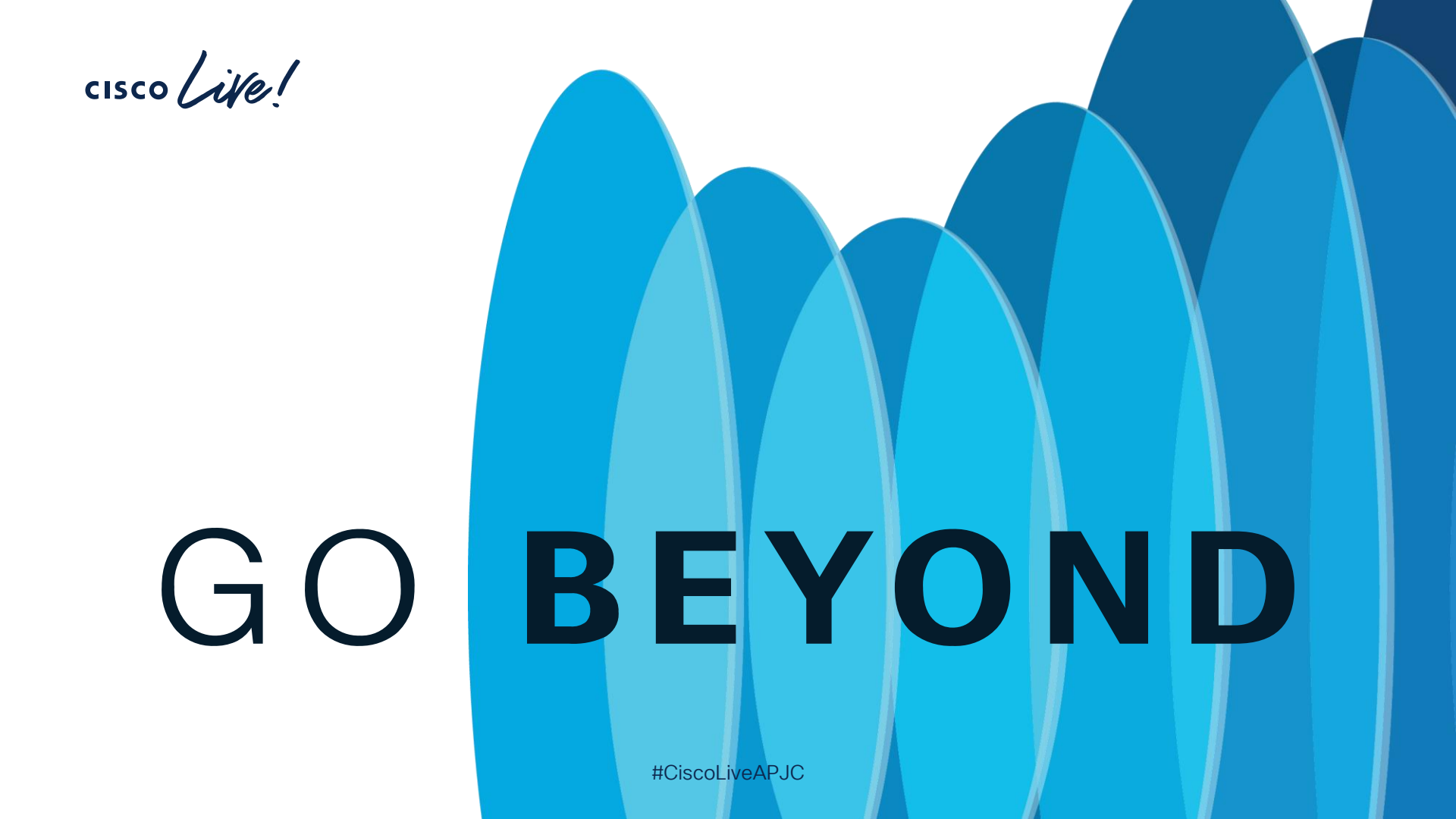

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Keeping Up With Zero Trust

Jerry Lin, Principal Solutions Engineer, GSSO

BRKSEC-2176

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2176

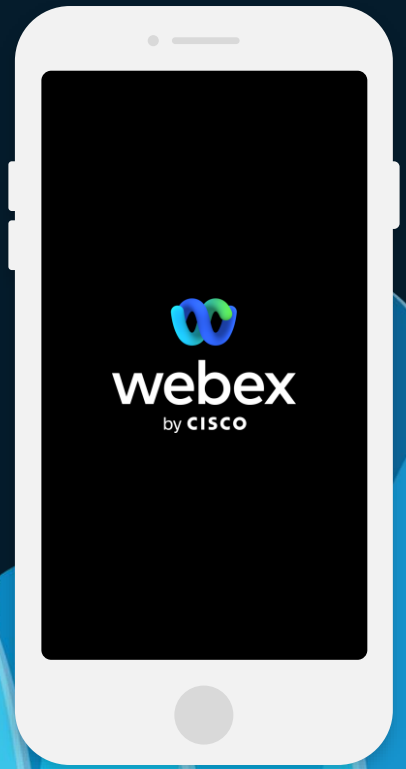
Questions?

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.



cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Zero trust maturity
- Zero trust use cases
- Conclusion

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What Zero Trust Means to Us

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero trust principles

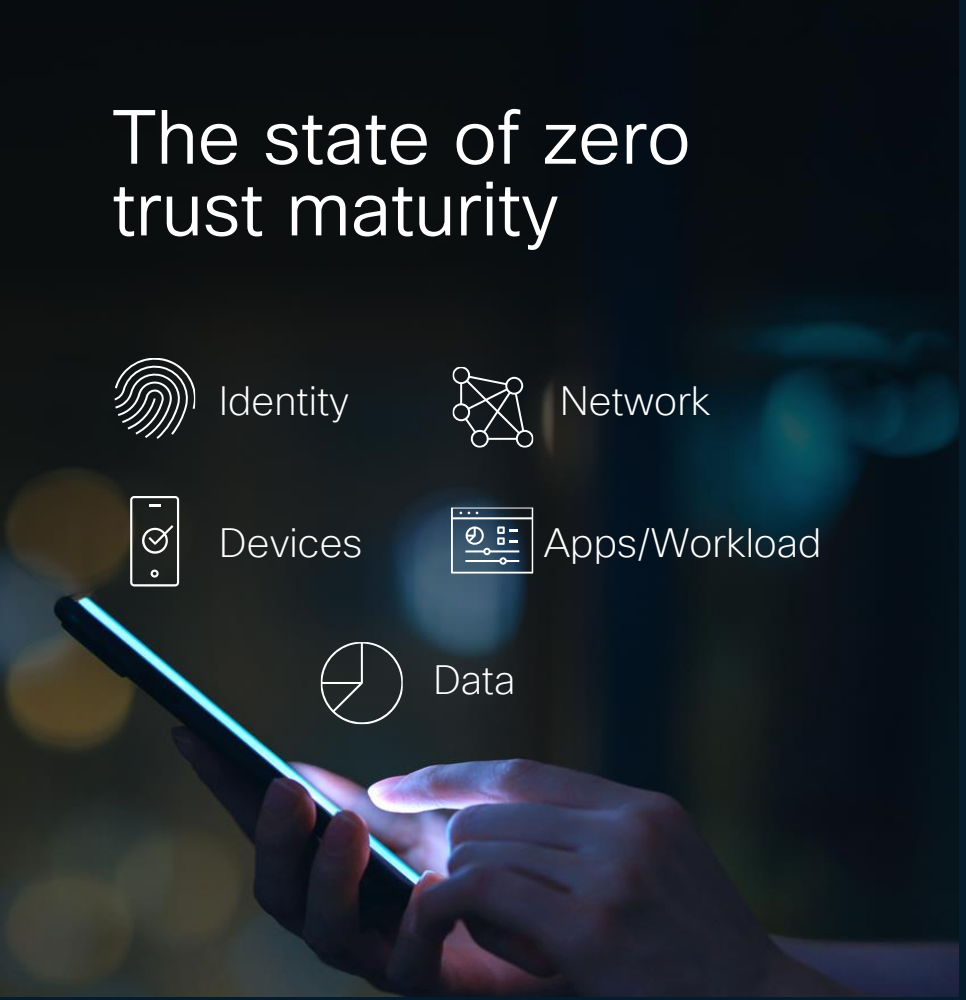
1. Never assume trust
2. Always verify
3. Enforce least privilege

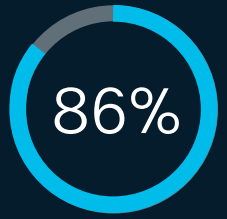
Zero trust success factors

1. Improved user experience
2. Adjust policy to risk
3. Compliance and governance across environments

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

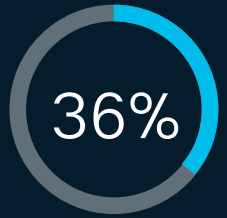
The state of zero trust maturity





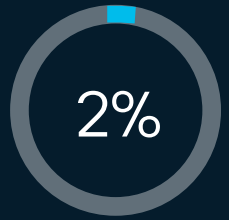
Nearly all organisations have started on some aspect of zero trust (at least one pillar)

"We know we need to do it"



Have reached maturity in at least one pillar

"Our focus is on XYZ pillar"



Have reached maturity across all pillars which means that 98% have not.

"We've still got a long way to go"

Source: Cisco's Security Outcomes for Zero Trust Report, January 2024

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Hacker News™
Security in a serious way

NEWS UPDATES

Massive Git Config Breach Exposes 15,000 Credentials; 10,000 Private Repos Cloned

Nov 01, 2024 Ravie Lakshmanan Vulnerability / Cloud Security

Microsoft Warns of Chinese Botnet Exploiting Router Flaws for Credential Theft

Nov 01, 2024 Ravie Lakshmanan Threat Intelligence / Network Security

Chinese Hackers Use CloudScout Toolset to Steal Session Cookies from Cloud Services

Oct 28, 2024 Ravie Lakshmanan Cloud Security / Cyber Attack

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Forbes

"Cybercriminals are gaining access to email accounts," the FBI warned this week, even when accounts are protected by multifactor authentication (MFA). Attacks begin when users are lured into "visiting suspicious websites or click on phishing links that download malicious software onto their computer."

FORBES > INNOVATION > CYBERSECURITY

FBI Warns Gmail, Outlook, AOL And Yahoo Users—Hackers Gain Access To Accounts

Zak Doffman Contributor

Zak Doffman writes about security, surveillance and privacy.

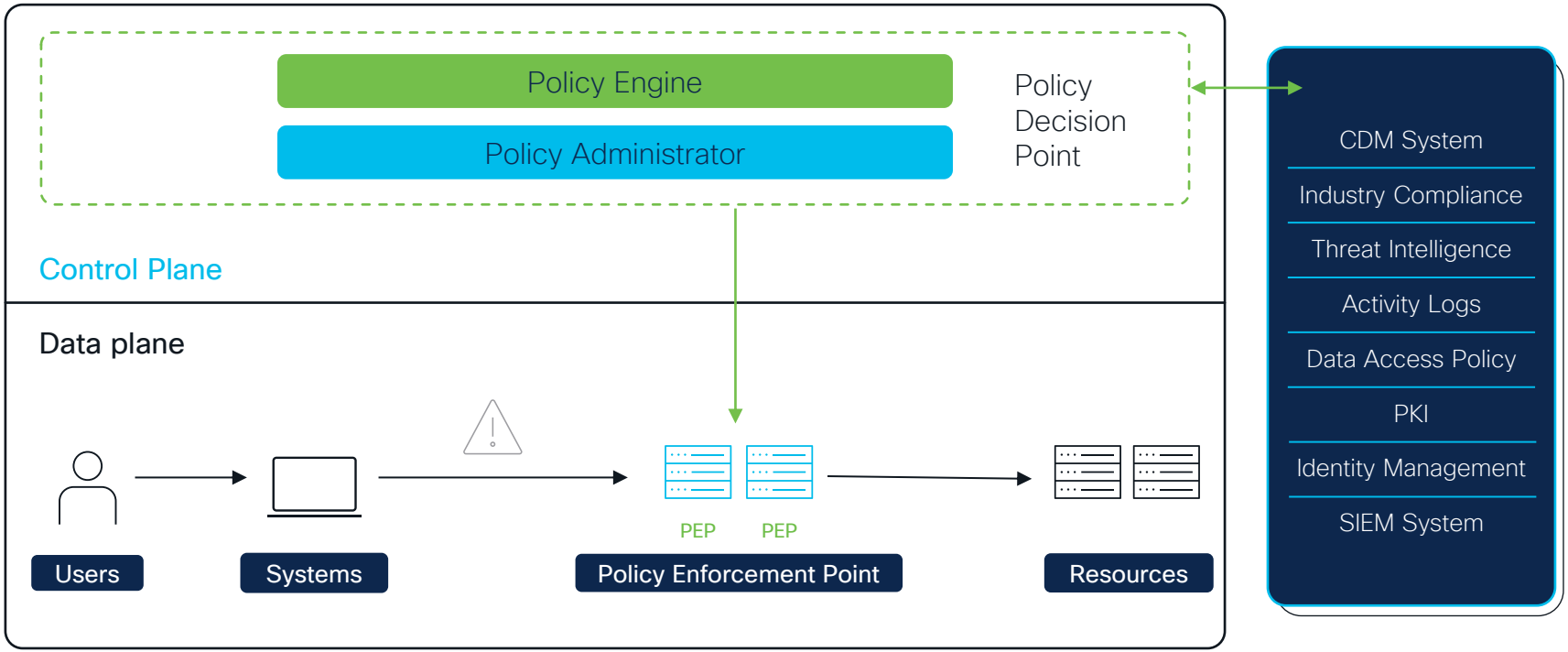
Follow

9

Nov 3, 2024, 05:38am EST

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

NIST 800-207 – Zero Trust Architecture



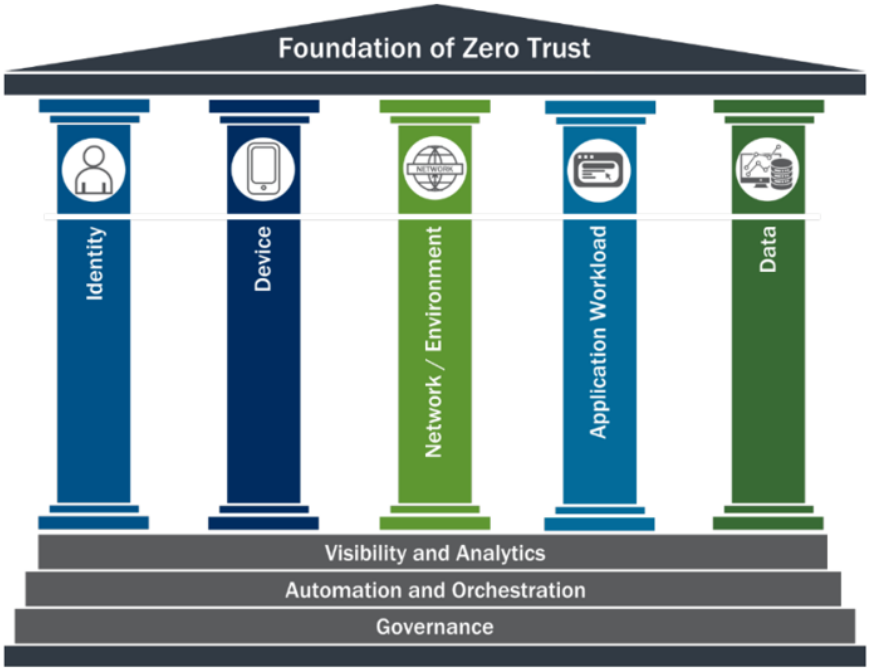
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

CISA – zero trust pillars – ZT maturity model

CISA = Cybersecurity Infrastructure and Security Agency

Maturity levels:

- Traditional
- Advanced
- Optimal



Source: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

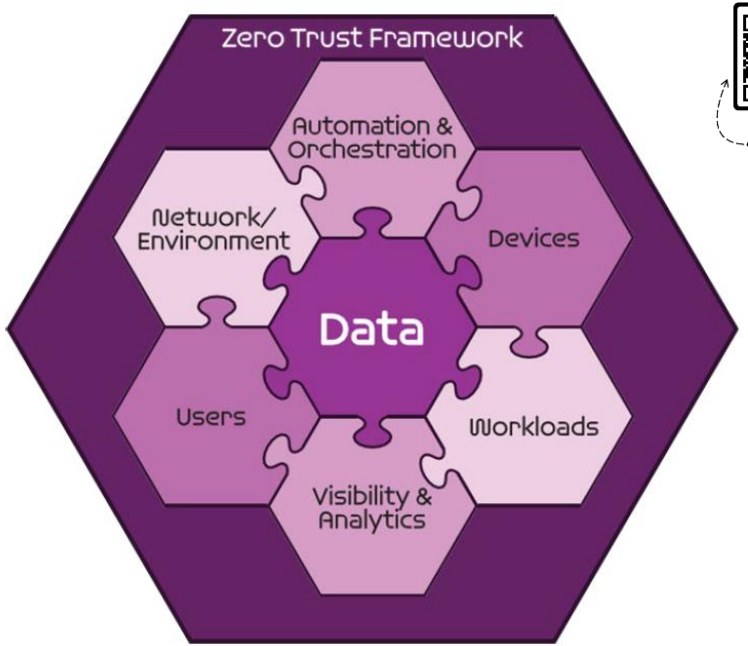
Dynamic – Continuous – Integrated – Optimised – Automated

Behaviour and posture analytics – suspicious and malicious behaviours

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DISA zero trust framework
Defense Information Systems Agency

- 7 pillars of DoD ZT Architecture
- Prepared by DISA and NSA(National Security Agency, July 2022



SCAN ME

Source: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Cisco enables zero trust

IDENTITY

- User / device / service identity
- Identity intelligence
- Posture and auth mgmt
- Risk-based authentication

ACCESS

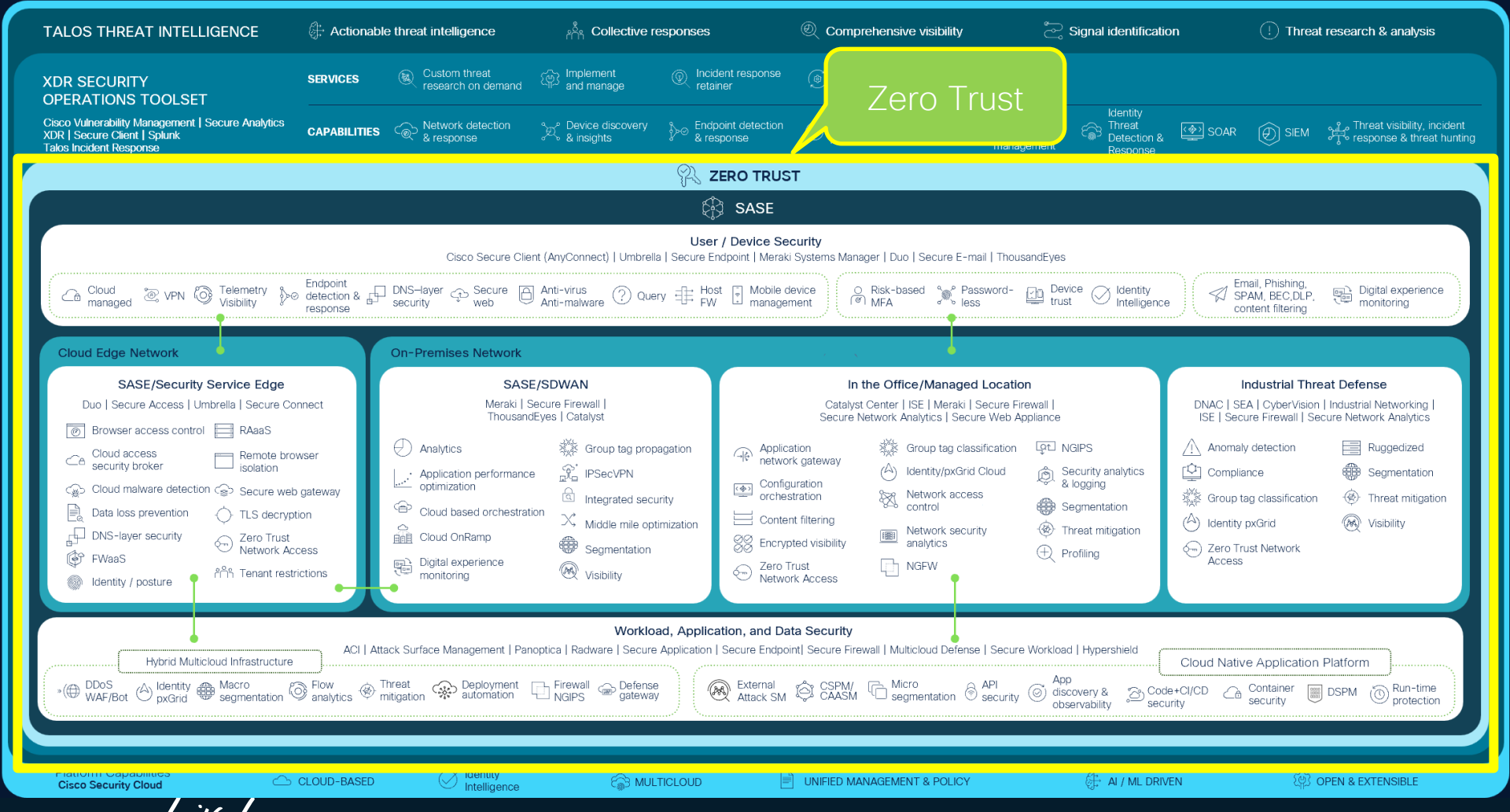
- Unified access control
- SSE: ZTNA, SWG, CASB, DLP, RBI
- Micro and macro-segmentation

RESPONSE

- AI-powered extended detection and response
- Orchestrated remediation
- Integrated threat intelligence

User & Device → Network & Cloud → Application & Data

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero Trust
-Optimise
-Accelerate

cisco Live!

Identity is the new perimeter

Identity is fundamental to **zero trust** and a **top 3 CISO concern**

Identity is critical infrastructure

Stolen credentials is the #1 attack technique, double the frequency of #2 Phishing

Verizon's Data Breach Investigation Report 2024

Strong authentication has low adoption

Across industry reports we see **less than ~5% of authentications** are phishing-resistant methods.

Duo's Trusted Access Report 2024

Attackers are doubling down

Domains associated with **Adversary-in-the-Middle (AitM) attacks quadrupled** from 2022 to 2023

Microsoft's Digital Defense Report 2023

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Attackers adapting: session hijacking is on the rise

How does it work?

What happens if an attacker steals a session cookie?

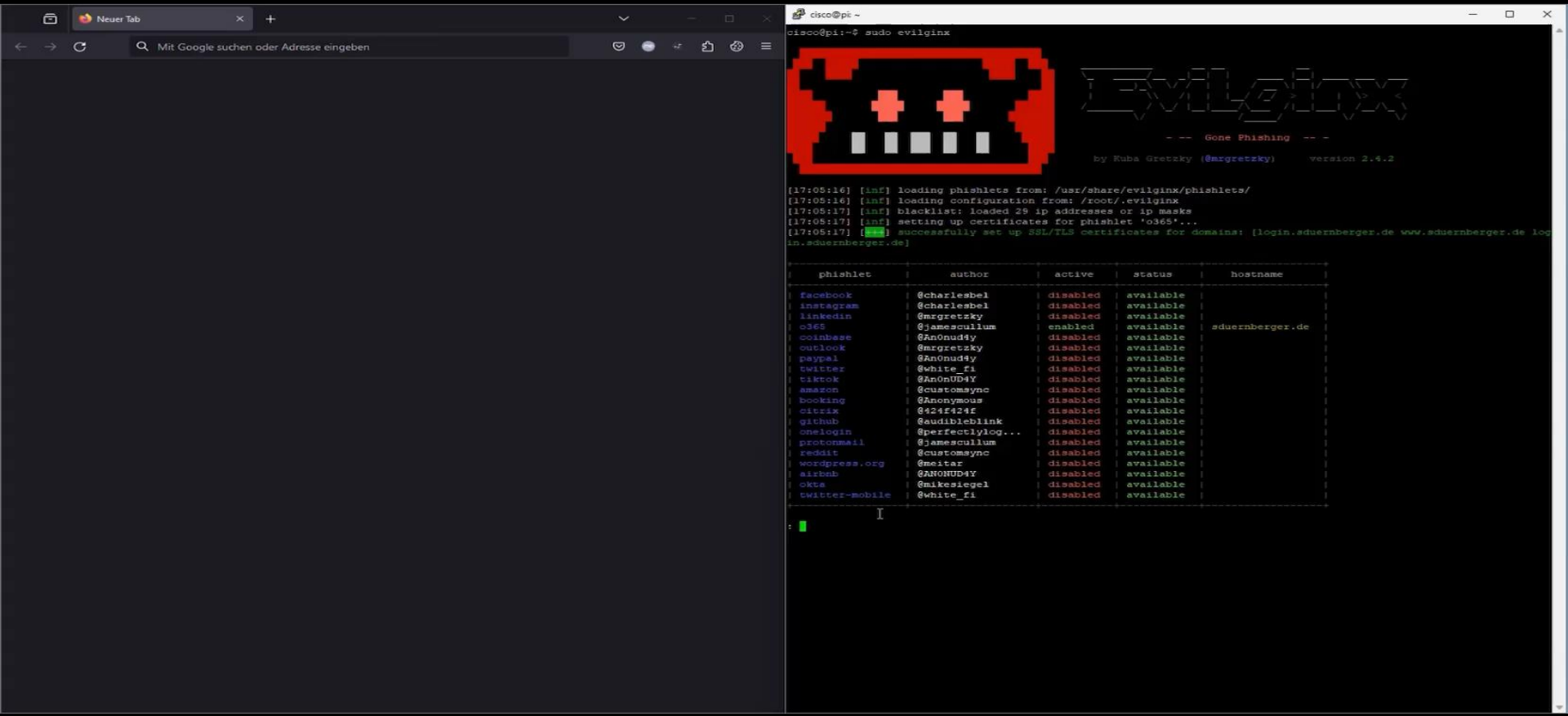
- Bypass multi-factor authentication and act as the user.
- They can log in anywhere SSO is allowed.
- Can establish permanent access and enroll new MFA devices

Huge, recent breaches

- CitrixBleed VDI breach
- Okta breach
- Google Cloud breach
- Slack-Github data breach

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Session Hijack Demo

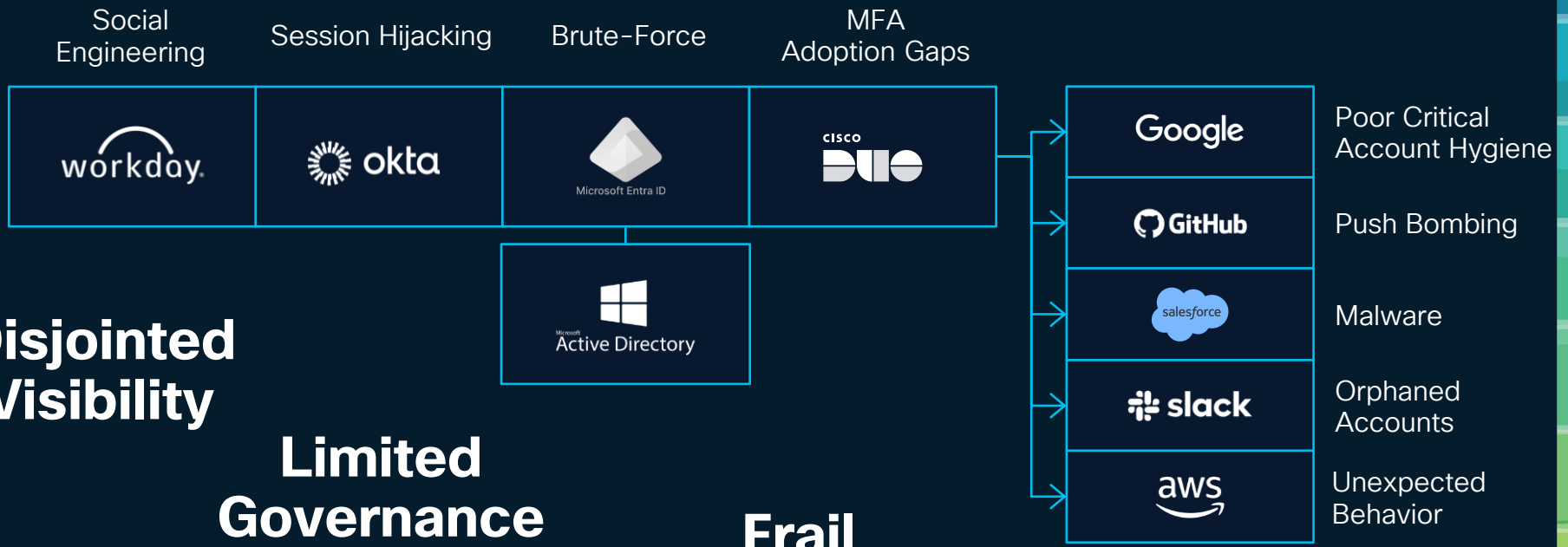


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The modern identity stack is complex...

Identity security is a top 3 CISO Concern



Disjointed Visibility

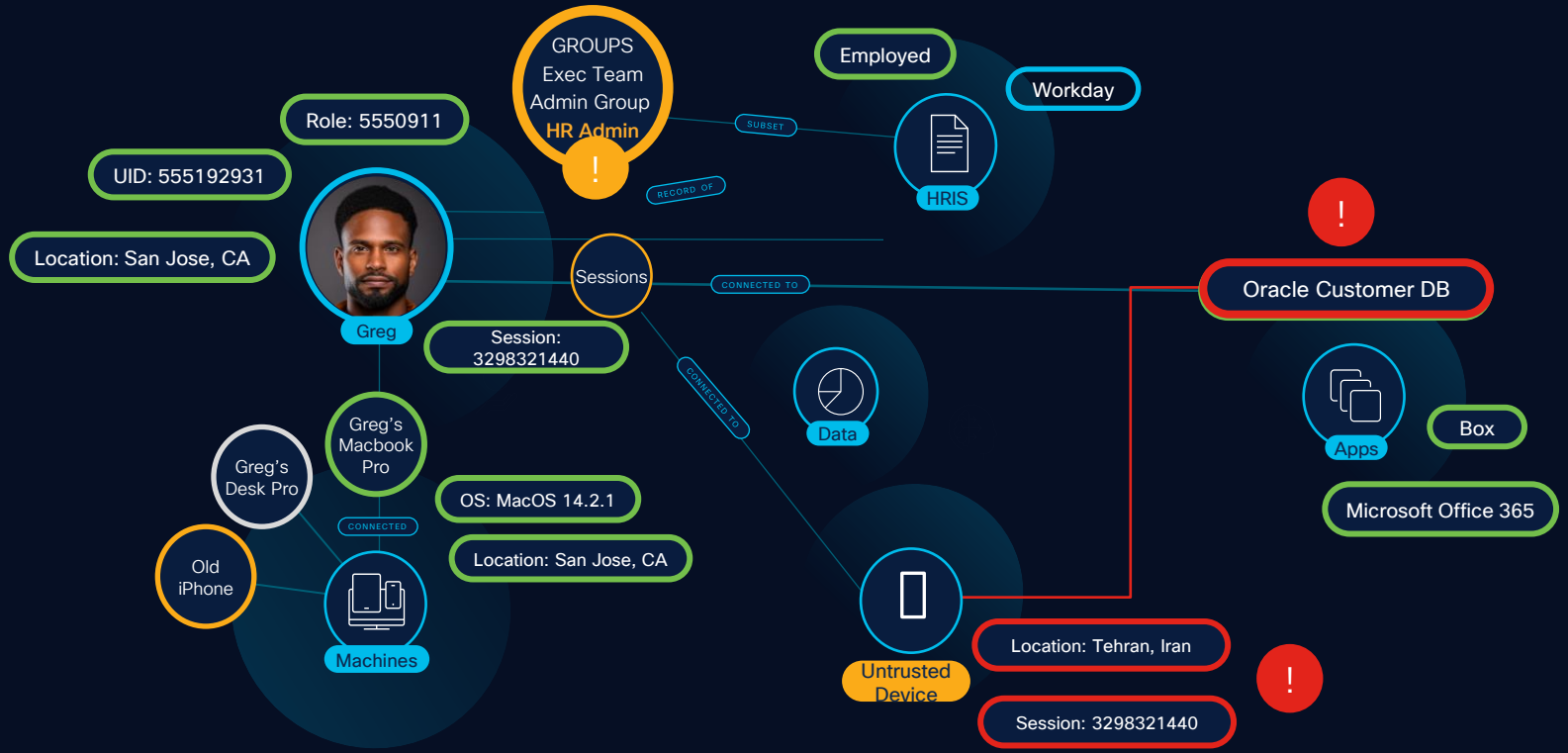
Limited Governance

Frail Threat Detection

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

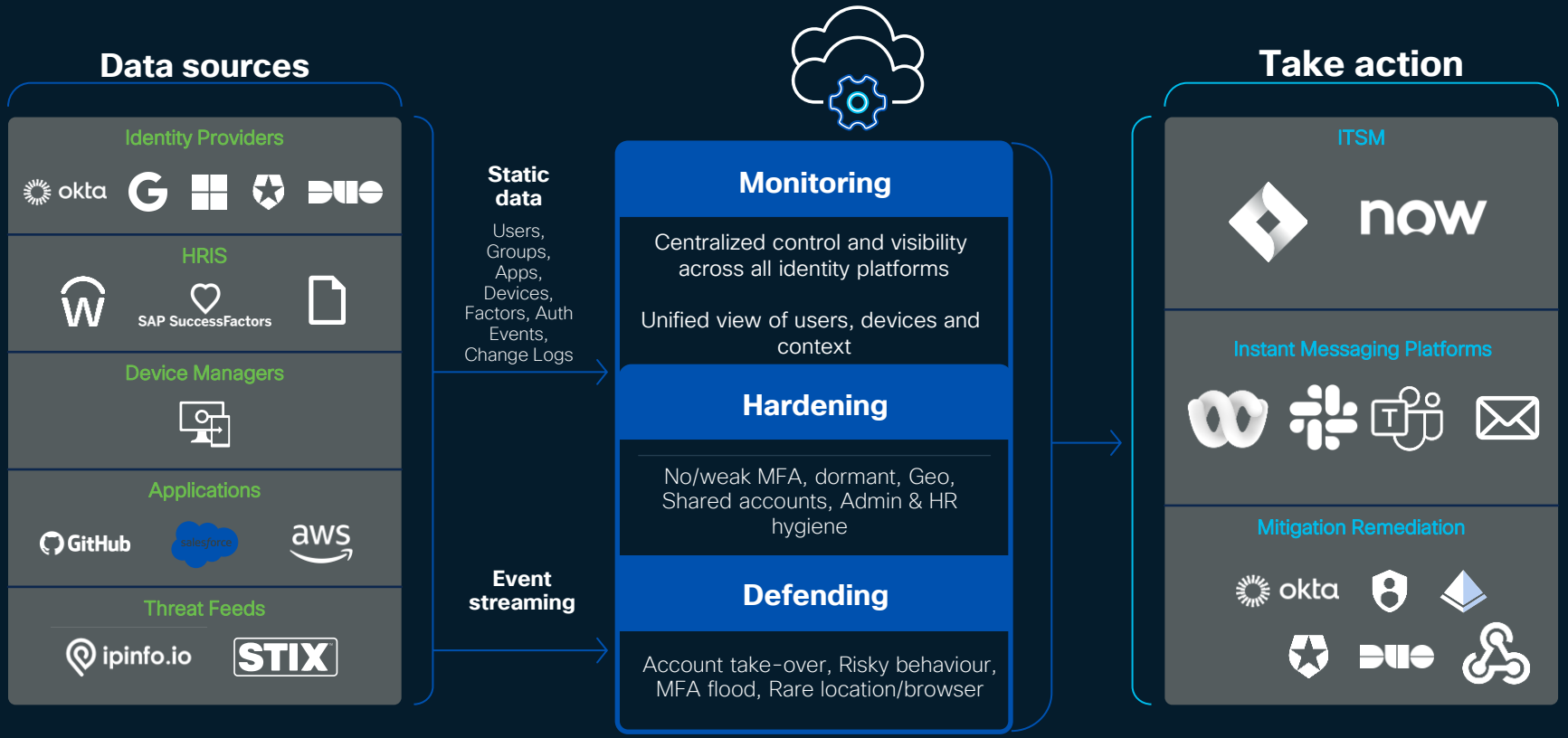
Identity Graph Analytics

Contextual Visibility | Advanced Defense



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

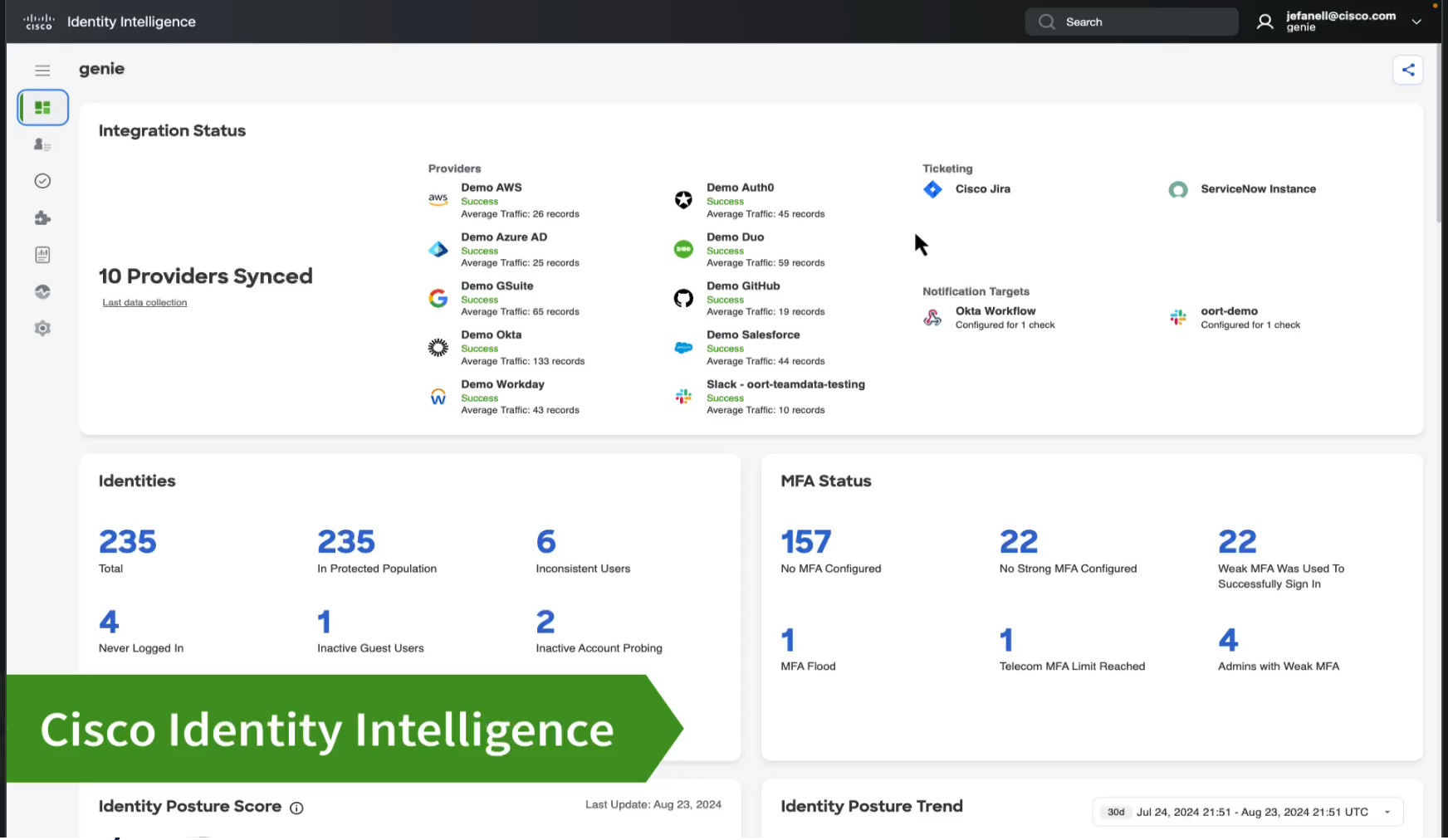
How Cisco Identity Intelligence works



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

CII Demo

cisco Live!



Cisco Identity Intelligence

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero trust use cases

Hybrid Worker

- ZT access to public SaaS
- ZTNA to private apps
- Client-based VPN private app access
- Secure Access / Connect (VPNaaS)

On-Premises User & IOT

- Campus .1x/MAB to public SaaS
- Campus .1x/MAB to private apps
- Branch .1x/MAB to public SaaS
- Branch .1x/MAB to private apps

App-to-App

- App-to-App across multi-cloud

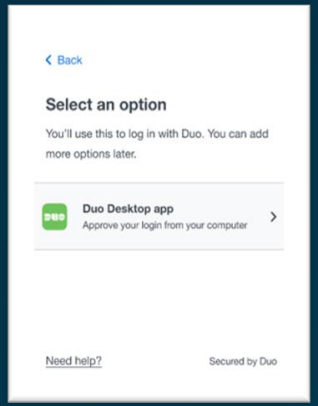
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Accelerate Zero Trust Access

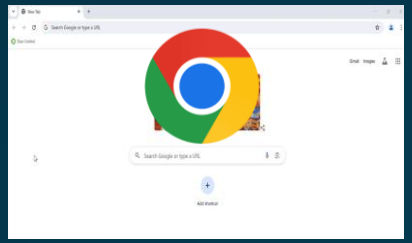
Duo Passport

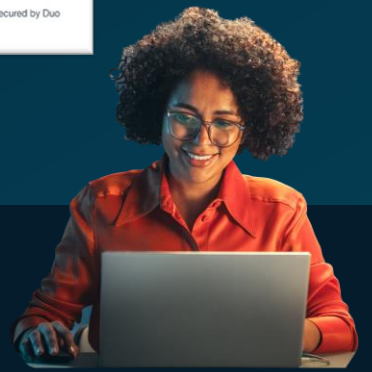
Log in once on a trusted device and access all web and client applications without requiring additional authentication by the user.

Desktop Authenticator



Device Trust Connector (Chrome)



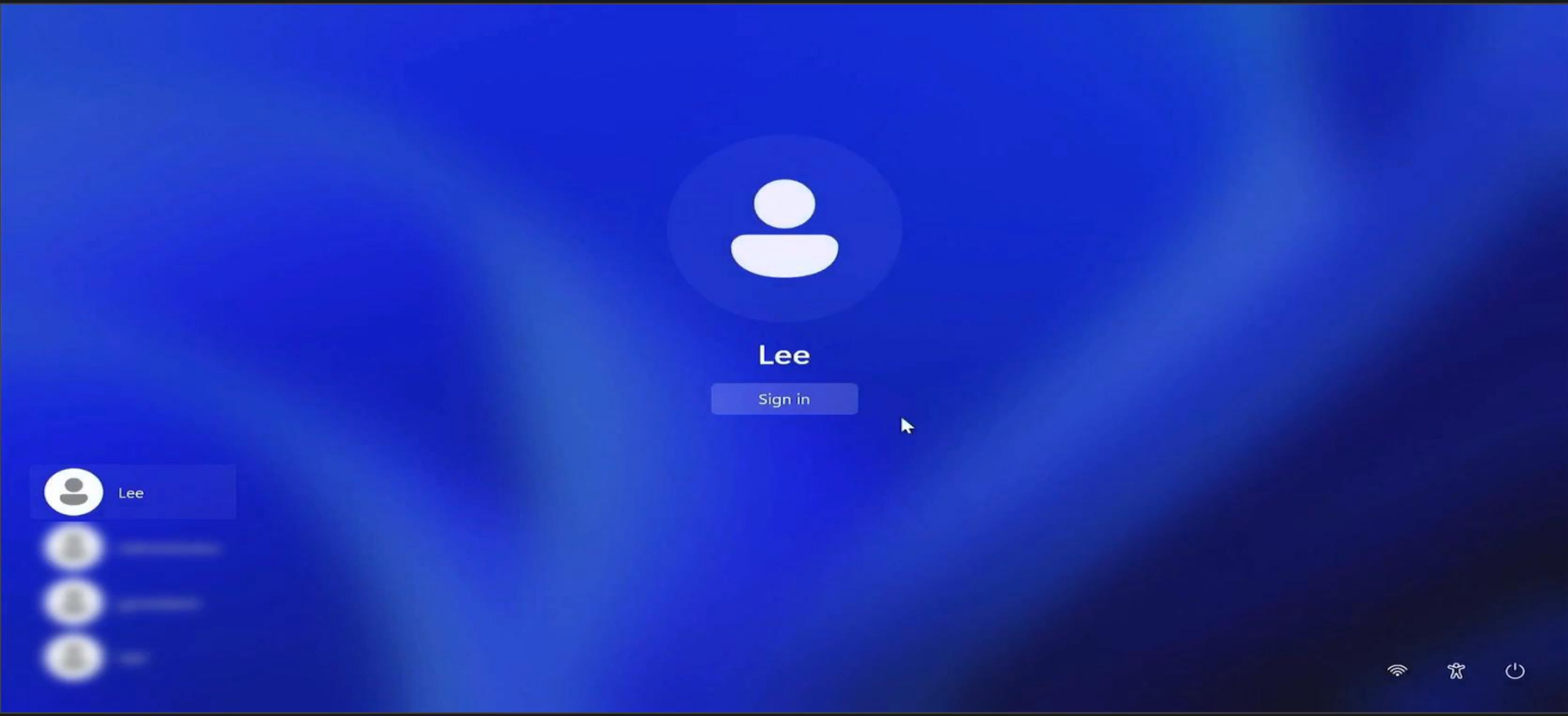


* Private preview (Windows OS)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

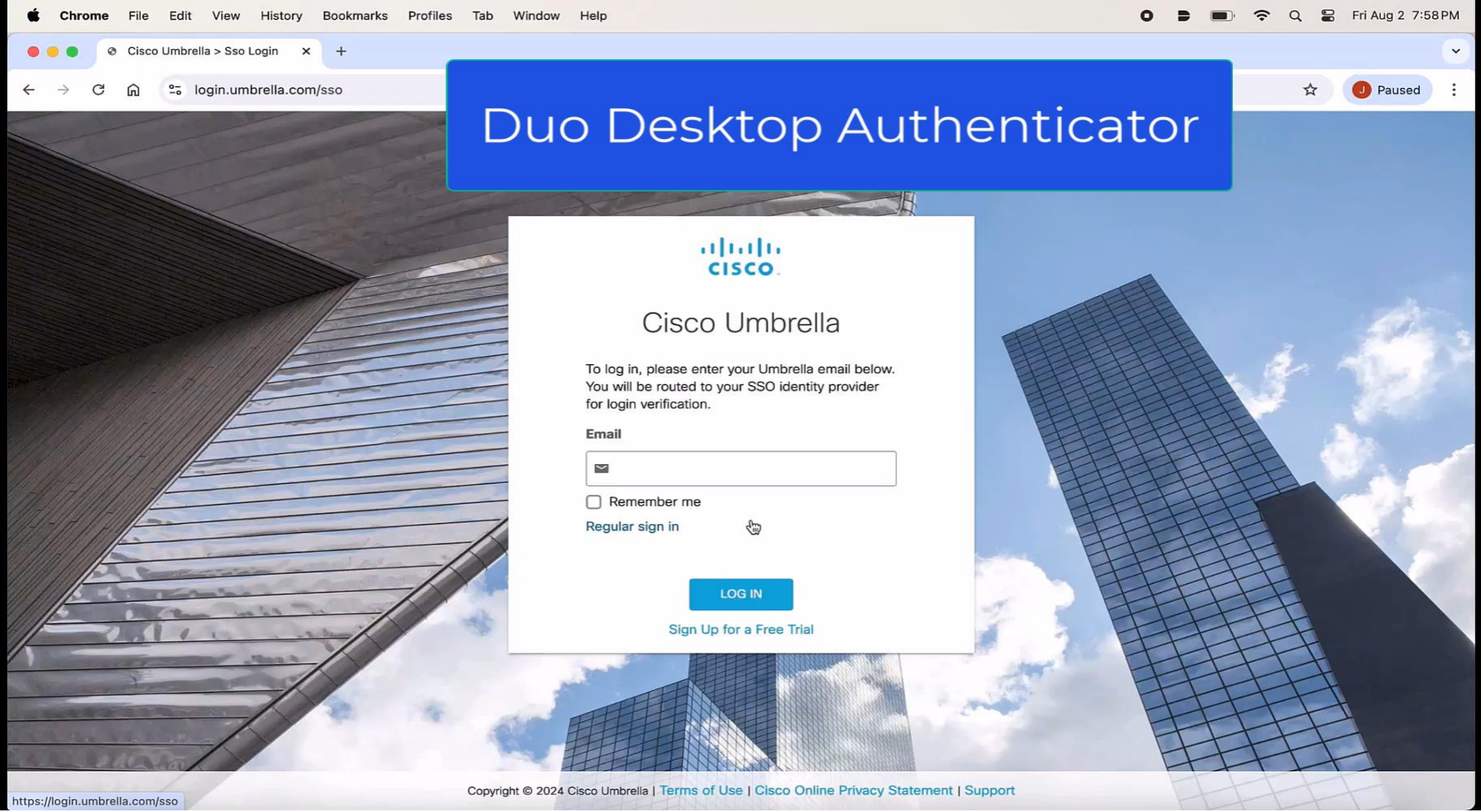
Duo Demos

- Passport
- Desktop Authenticator
- Chrome DTC

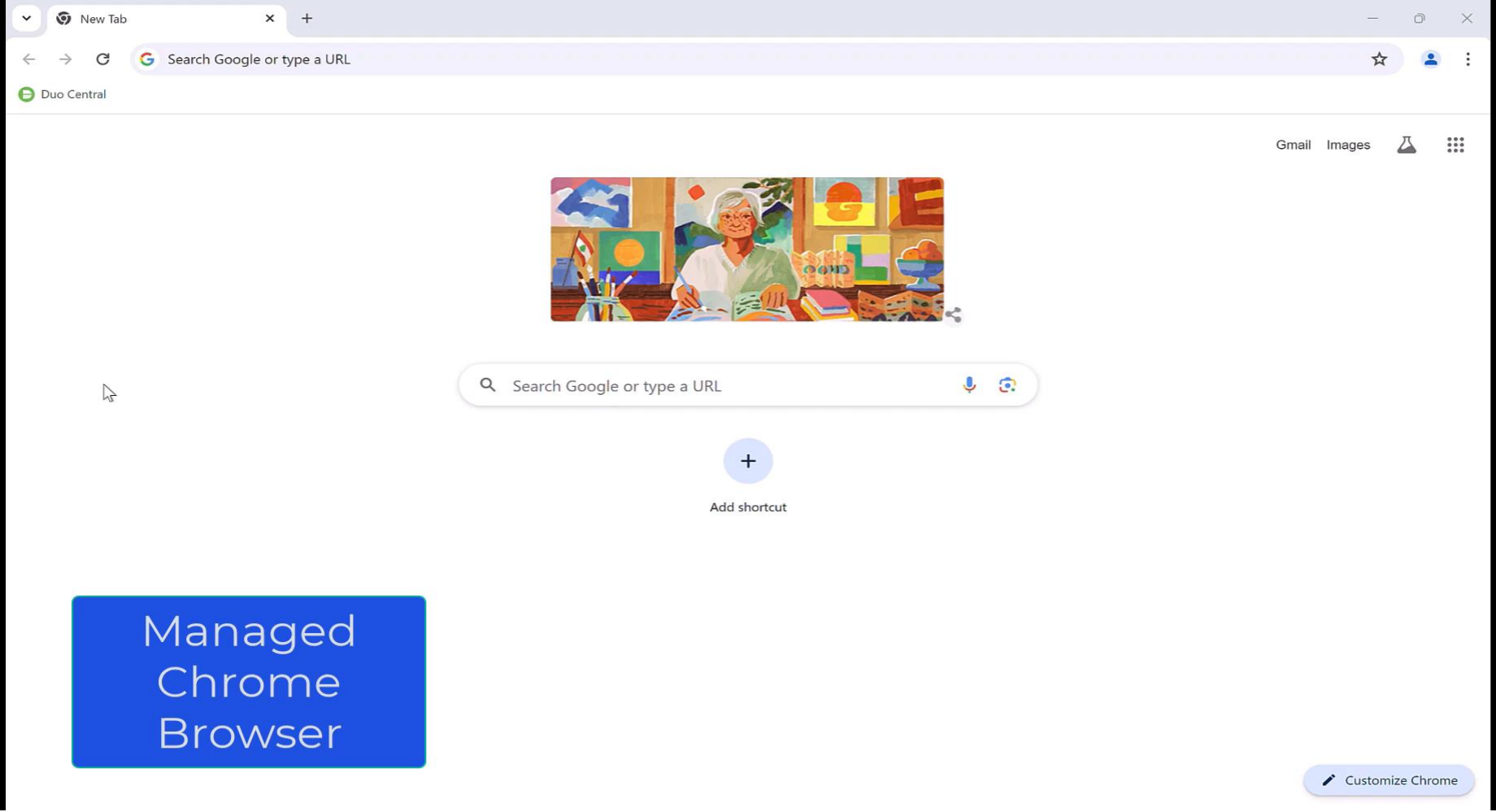


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Duo Desktop Authenticator



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

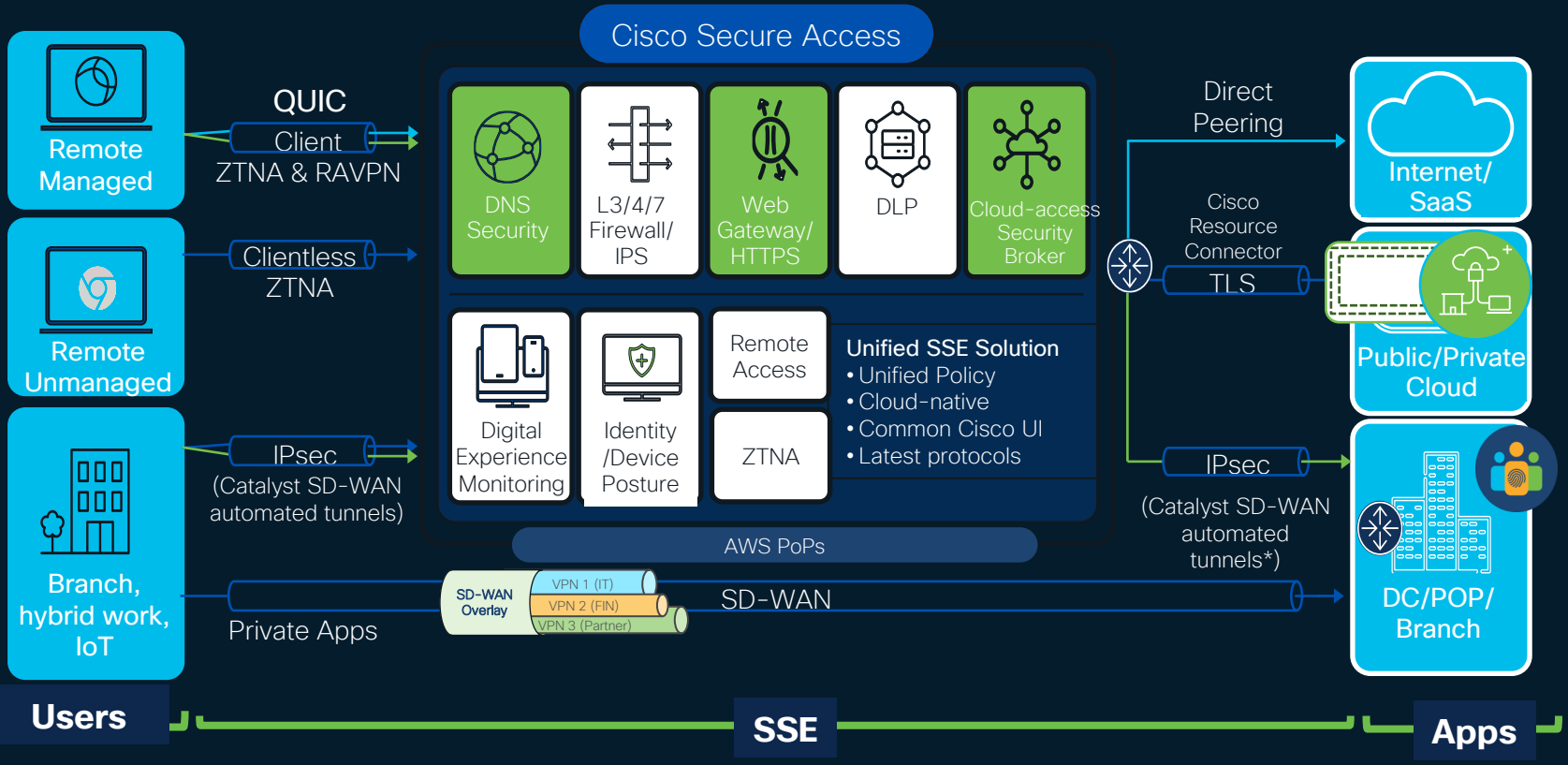


Managed Chrome Browser

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

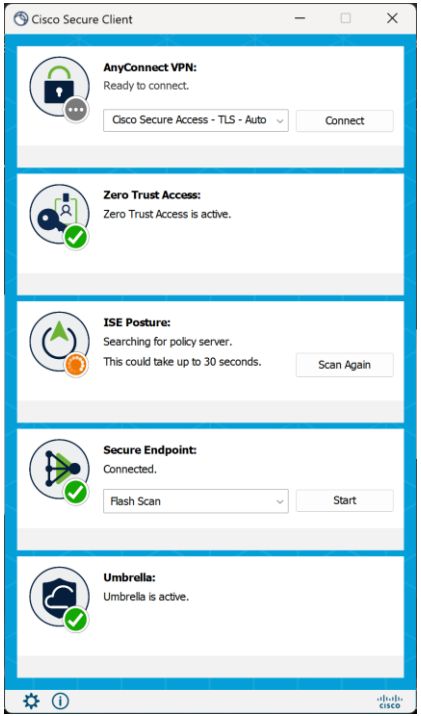
Secure Hybrid Worker

Secure hybrid worker



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unified ZTNA client
Transparently secures the connections needed



Internet
Redirected transparently to SSE cloud

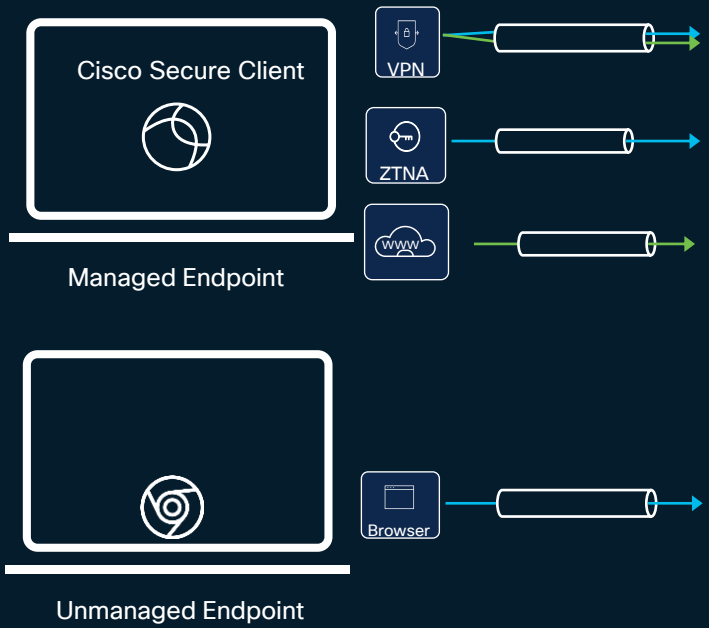
SaaS apps
CASB/DLP protections inline and via API.
App bypass also supported

Private modern apps
ZTNA gives controlled access to selected applications

Private Traditional apps
RA-VPN gives full network access for existing applications

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Users: remote connectivity



AnyConnect VPN
→ Authentication & Posture @ Connect time
→ DTLS Tunnel
→ Carry Internet & Private Traffic (All ports & protocols)
→ SAML, (+) Cert, & (+) Multi-Cert Authentication

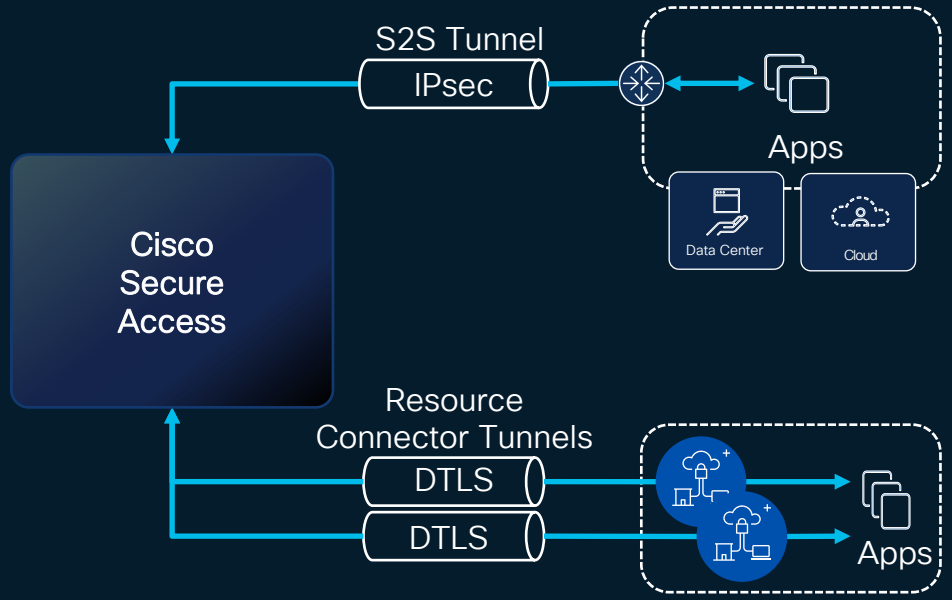
ZTNA Module
→ Authentication & Posture per session
→ QUIC tunnel (MASQUE proxy)
→ Carry Private Traffic (All ports & protocols)
→ SAML Auth + Auto re-new

Web Roaming Module
→ Device Enrollment (profile)
→ Carry Internet Web Traffic (80/443)

Clientless ZTNA
→ Accessible from any browser that supports SAML/Cookies
→ Request based posture (geolocation, browser version, OS)
→ Web Apps Only

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Apps: private applications



Site-to-site tunnels with IPsec

- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Fallback for resource connectors

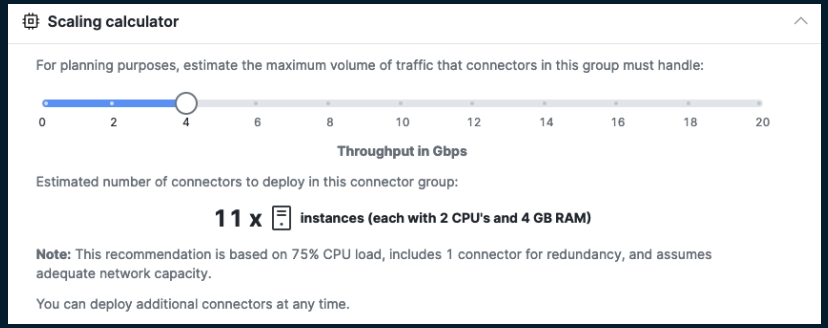
Resource connectors

- Lightweight VM for AWS and ESXi
- All traffic egresses from Resource Connector IP
- Access applications with overlapping IPs
- Outbound connection / no firewall holes required
- No routing configuration required
- Auto failover / load balancing

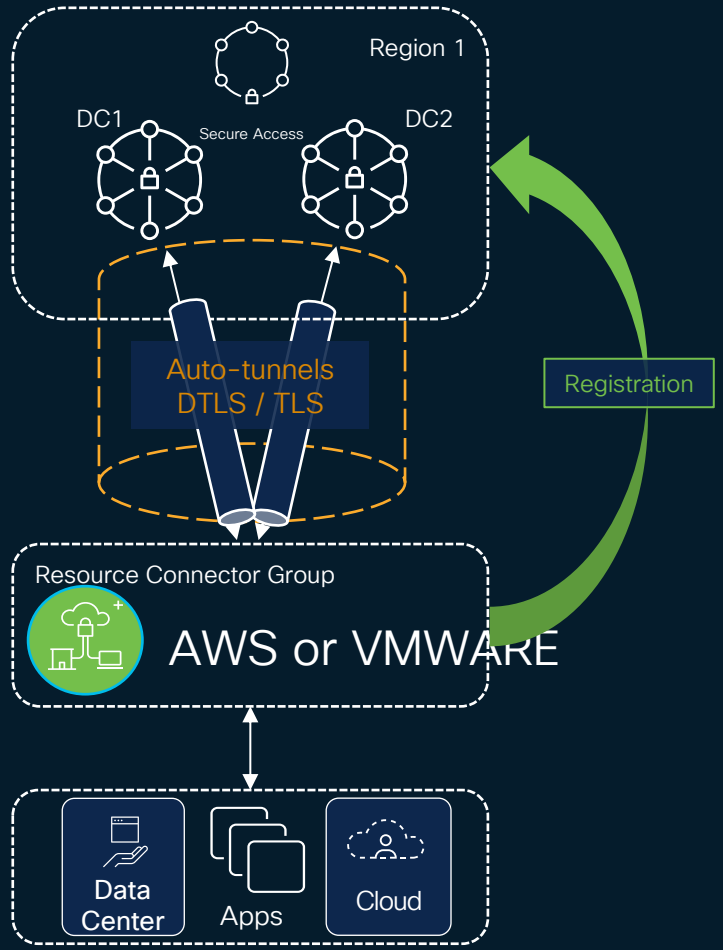
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resource connector

- Scaling and Redundancy
  - Dashboard provides calculator
  - Based on 70% CPU and DTLS
  - 500 Mb/s at full capacity
  - 400 Mb/s at 70% load

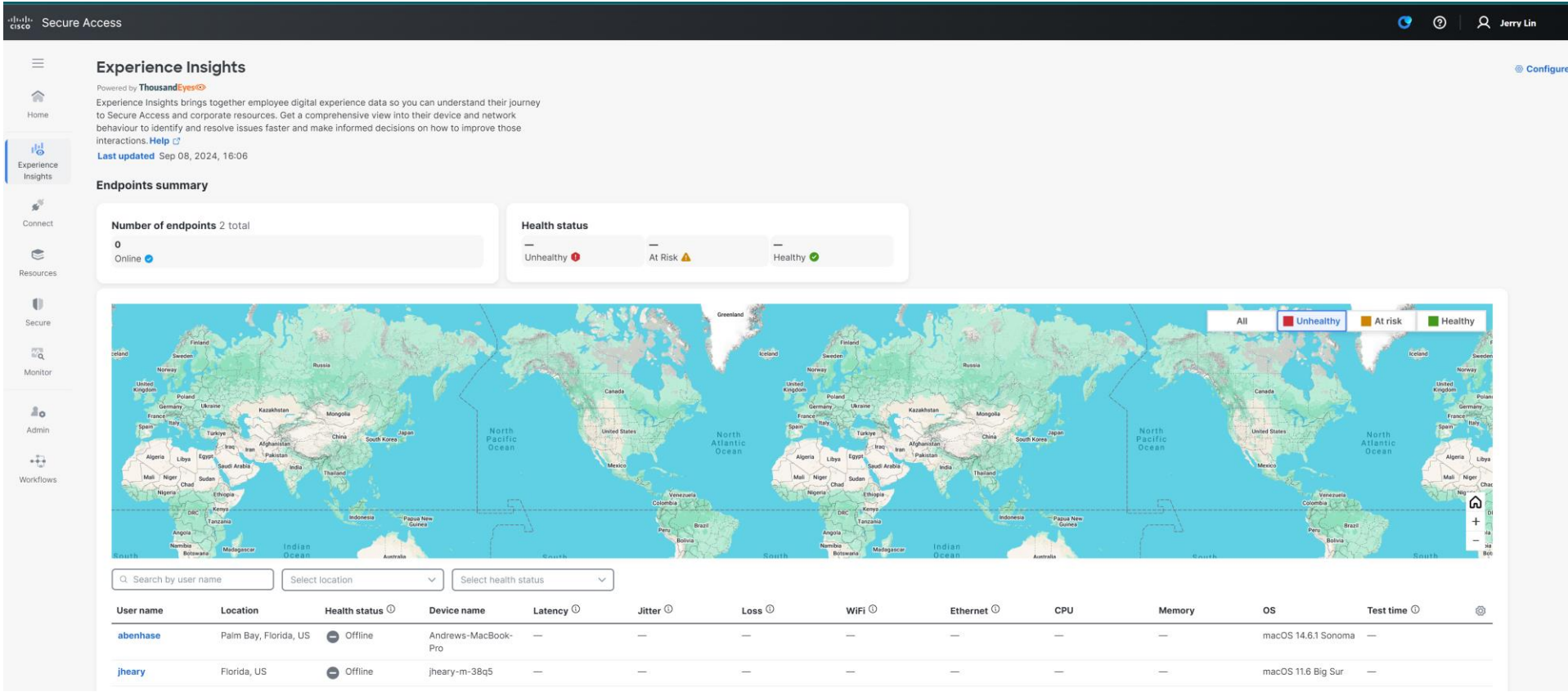


Source: https://docs.sse.cisco.com/sse-user-guide/docs/limitations-and-range-limits



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Digital Experience Monitoring

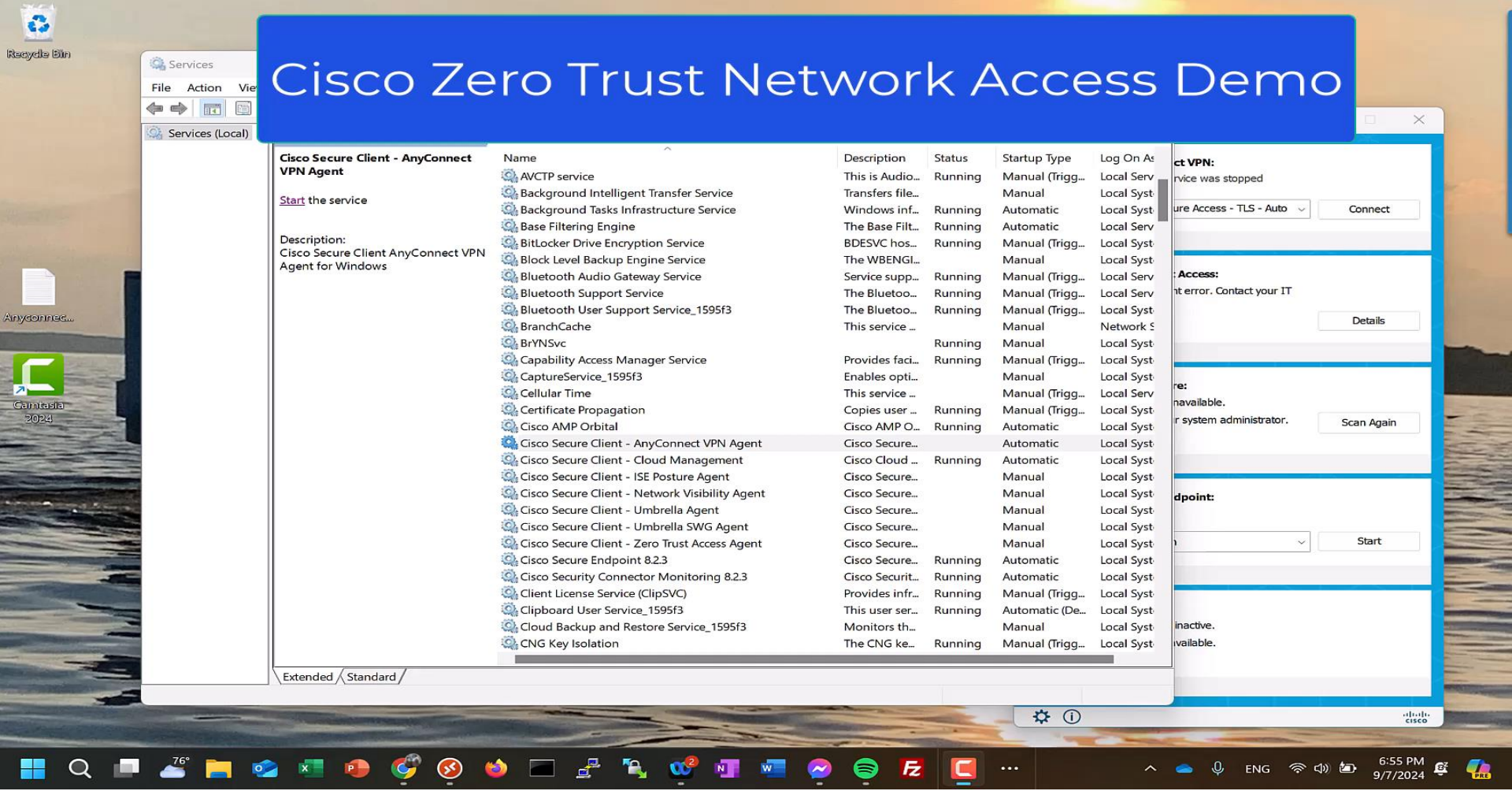


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ZTNA Demo
Secure Access

cisco Live!

Cisco Zero Trust Network Access Demo



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Access and CII Demo

cisco Live!

Cisco Secure Access

dashboard.sse.cisco.com/page-url

Secure Access

Kit
Business Corp, Inc

Secure Access Dashboad

Overview

The Overview dashboard displays status, usage, and health metrics. Use this information to address security threats and monitor system usage. Help.

- Overview
- Connect
- Resources
- Secure
- Experience Insights
- Monitor
- Admin
- Workflows

Connectivity

Last 24 Hours

Network tunnels 283 total

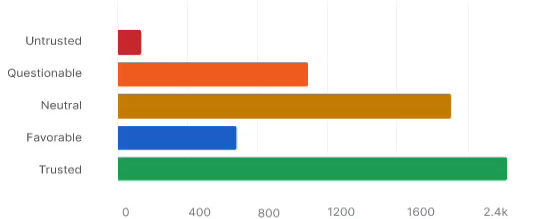
- 8 Active
- 36 Inactive
- 161 Unestablished

Identity Intelligence

Last 24 Hours

Untrusted Users

User Trust Levels



Usage monitoring

Last 24 Hours

Total usage

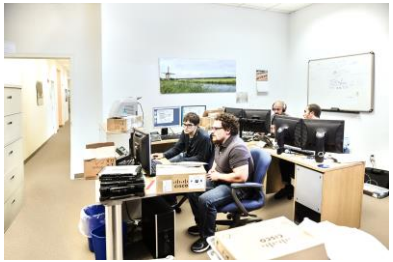
Usage data - delayed up to 30 min.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Zero trust use cases

Remote User

- ZT access to public SaaS
- ZTNA to private apps
- Client-based VPN private app access
- Secure Connect (VPNaaS)
- *Unified ZTNA client (roadmap)



On-Premises User & IOT

- Campus .1x/MAB to public SaaS
- Campus .1x/MAB to private apps
- Branch .1x/MAB to public SaaS
- Branch .1x/MAB to private apps

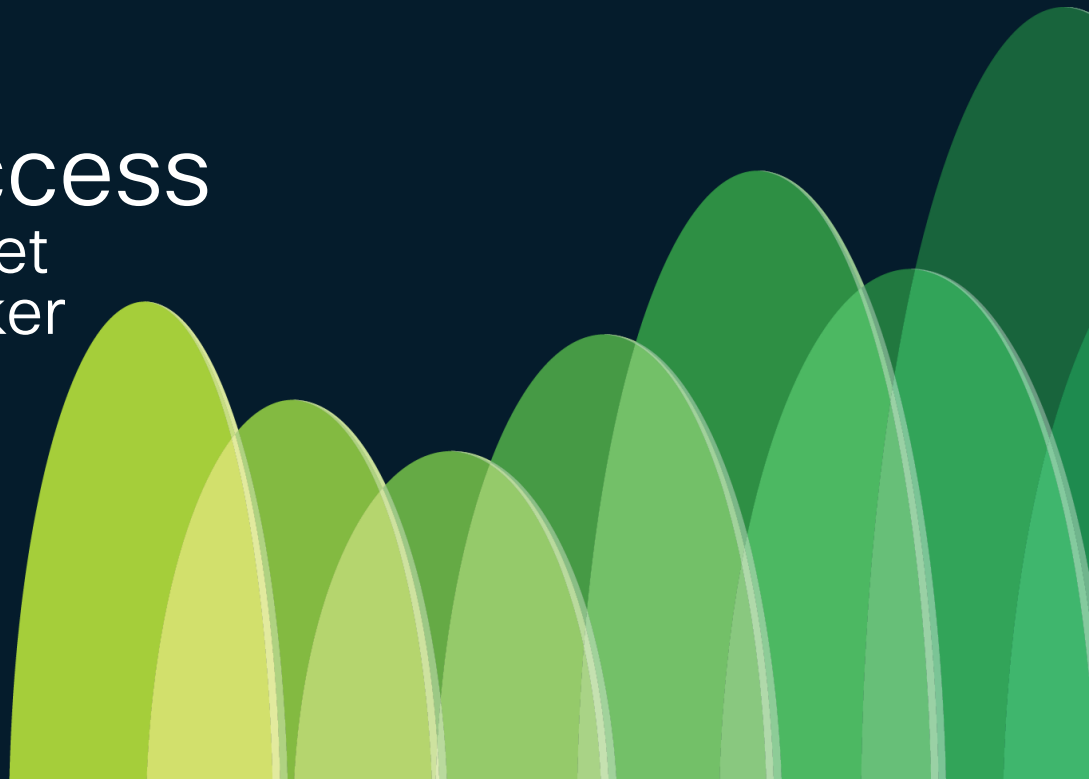
App-to-App

- App-to-App across multi-cloud

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

On-Premises Access

- Public SaaS and Internet
- On-Prem/Branch Worker



ISE provides zero trust for on-premises

Enterprise

Security

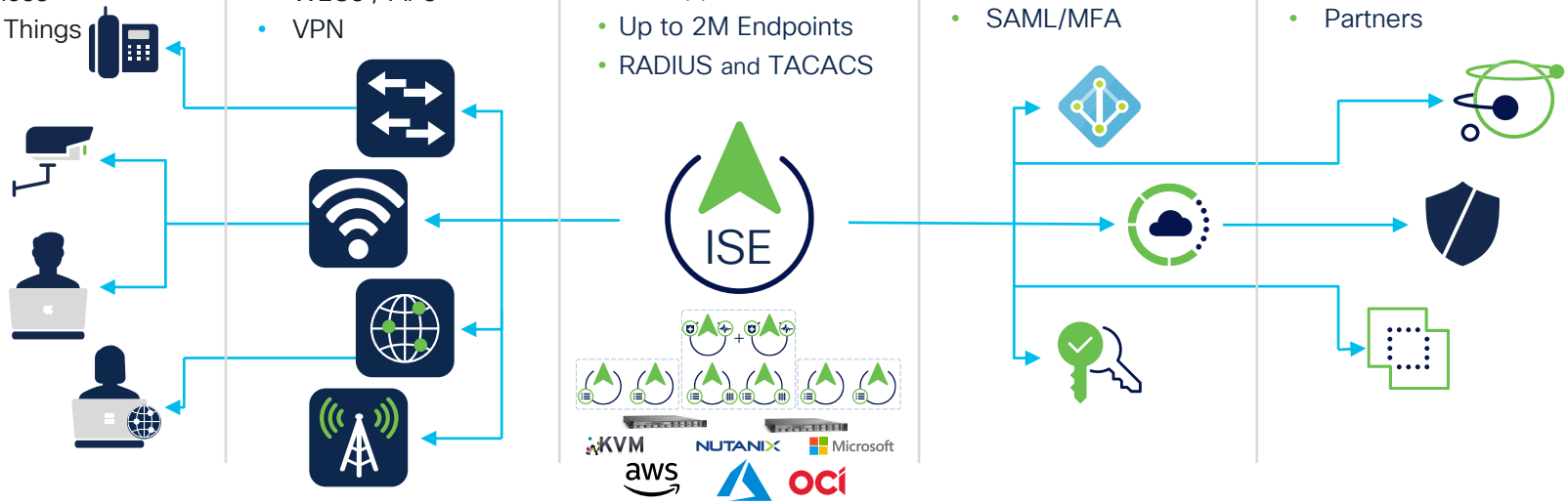
Endpoints
- Users
- Devices
- IOT Things

Network Devices
- Switches
- WLCs / APs
- VPN

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

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

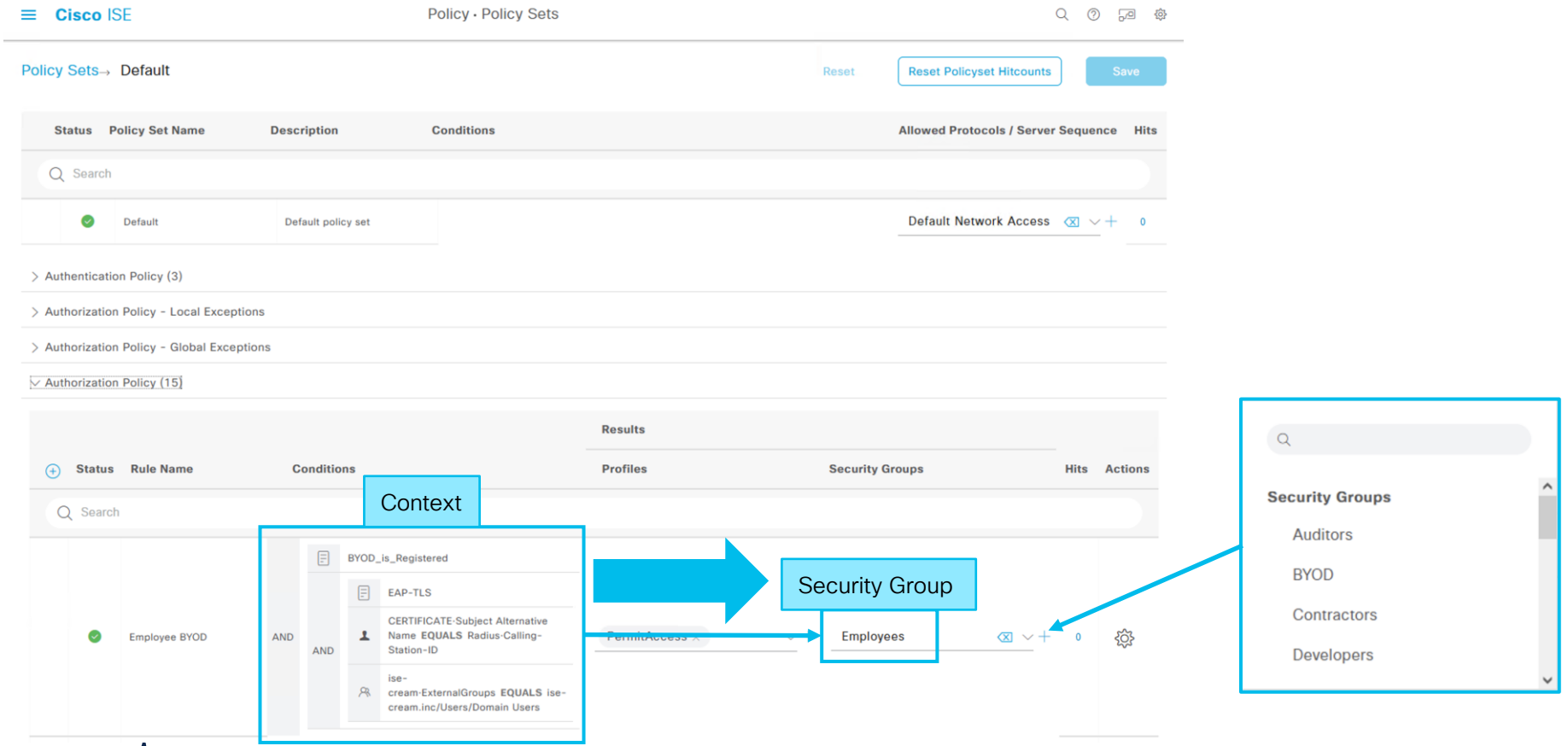
Security Services
- Cloud Analytics
- Secure Firewall
- Partners



See It | Secure It | Share It

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

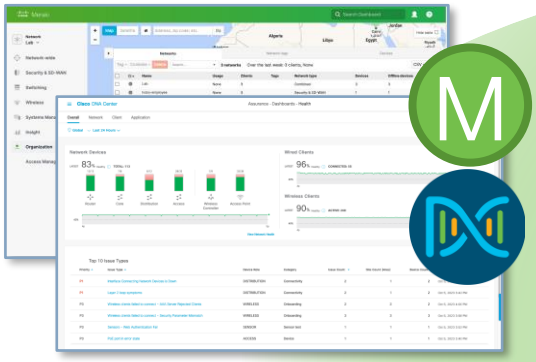
Dynamic classification and SGT assignment via ISE



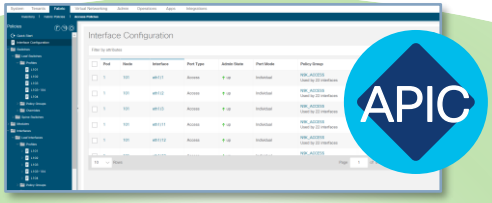
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE is the core of Cisco's common policy

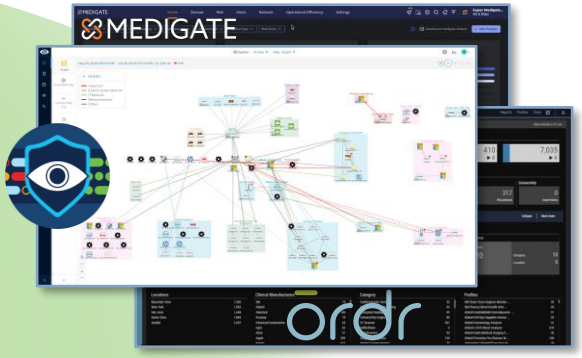
Campus



Data Center



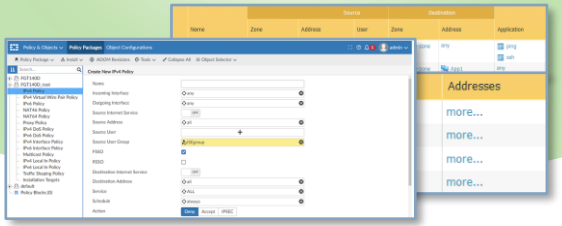
IoT



ISE

Security

Competitors

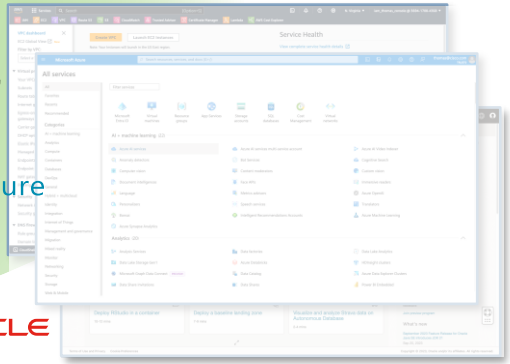


Cloud Providers

aws

Azure

ORACLE

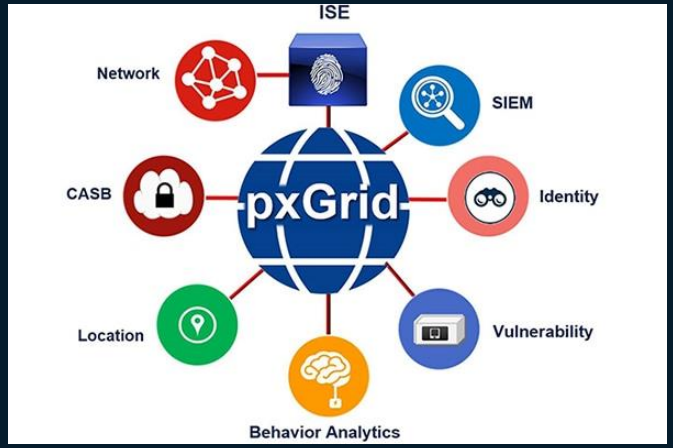


cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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…



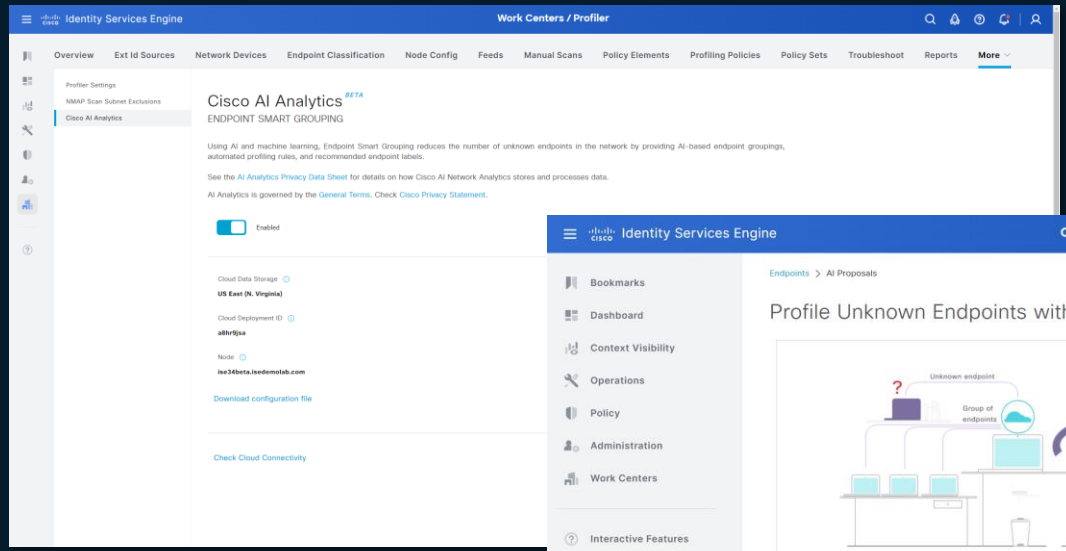
Cisco Rapid Threat Containment

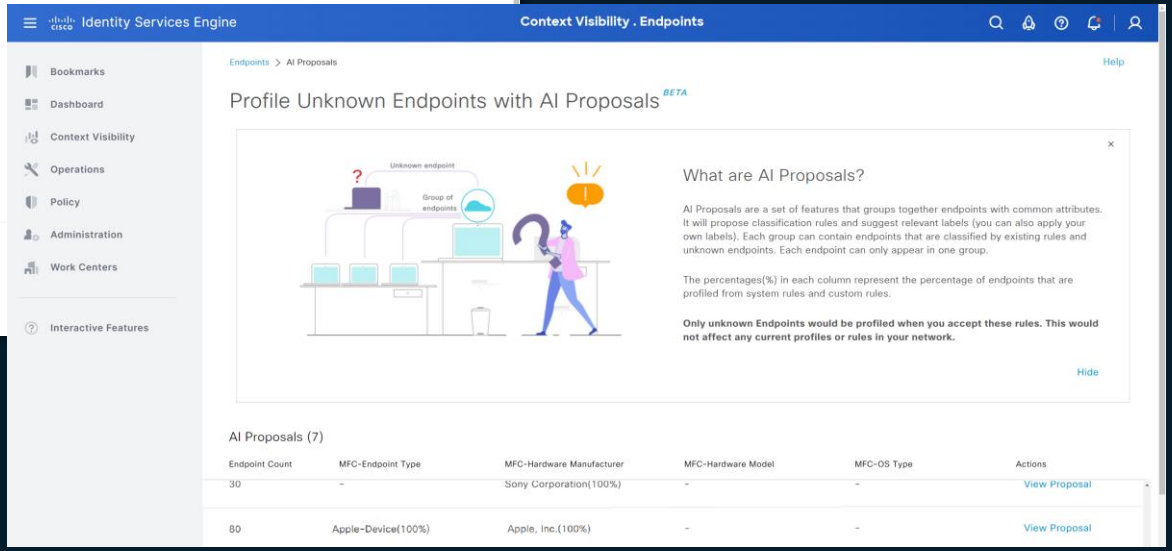
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE 3.3 (AI profiling)

AI Analytics simplifies the profiling process

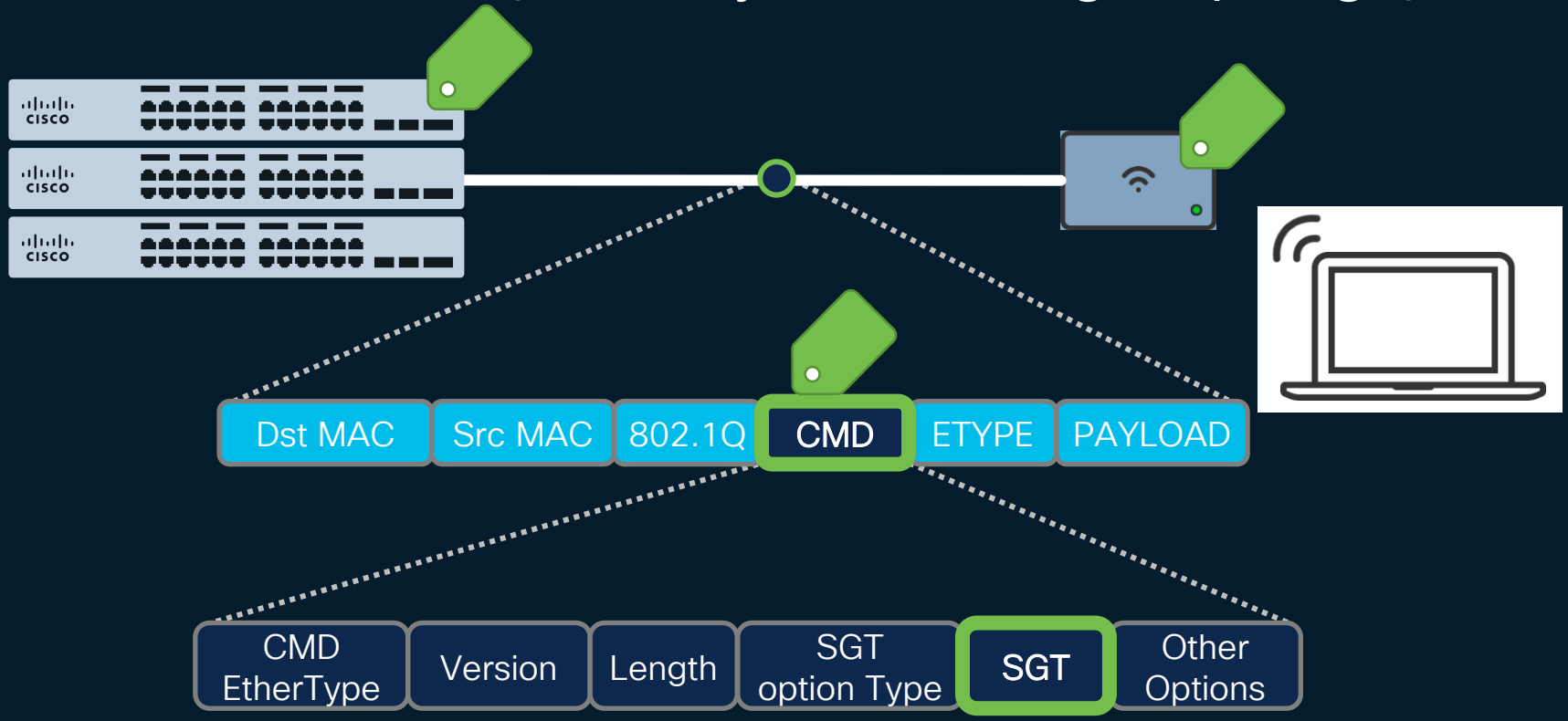
- Profiling probes discover unknown devices
- AI Proposals presented and enforced in authorisation policy





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What are SGTs (security/scalable group tags)?



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scalable group tag (SGT)

Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit | Add | Import | Export | Trash | Push | Verify Deploy

Icon	Name	SGT (Dec / Hex)	Description
	1120asaVPNuser	18/0012	FP1120asa VPN user
	Auditors	9/0009	Auditor Security Group
	BYOD	15/000F	BYOD Security Group
	Contractors	5/0005	Contractor Security Group
	Developers	8/0008	Developer Security Group
	Development_Servers	12/000C	Development Servers Security Group
	Employees	4/0004	Employee Security Group
	FP4120_VPNusers	20/0014	
	Guests	6/0006	Guest Security Group
	Network_Services	3/0003	Network Services Security Group

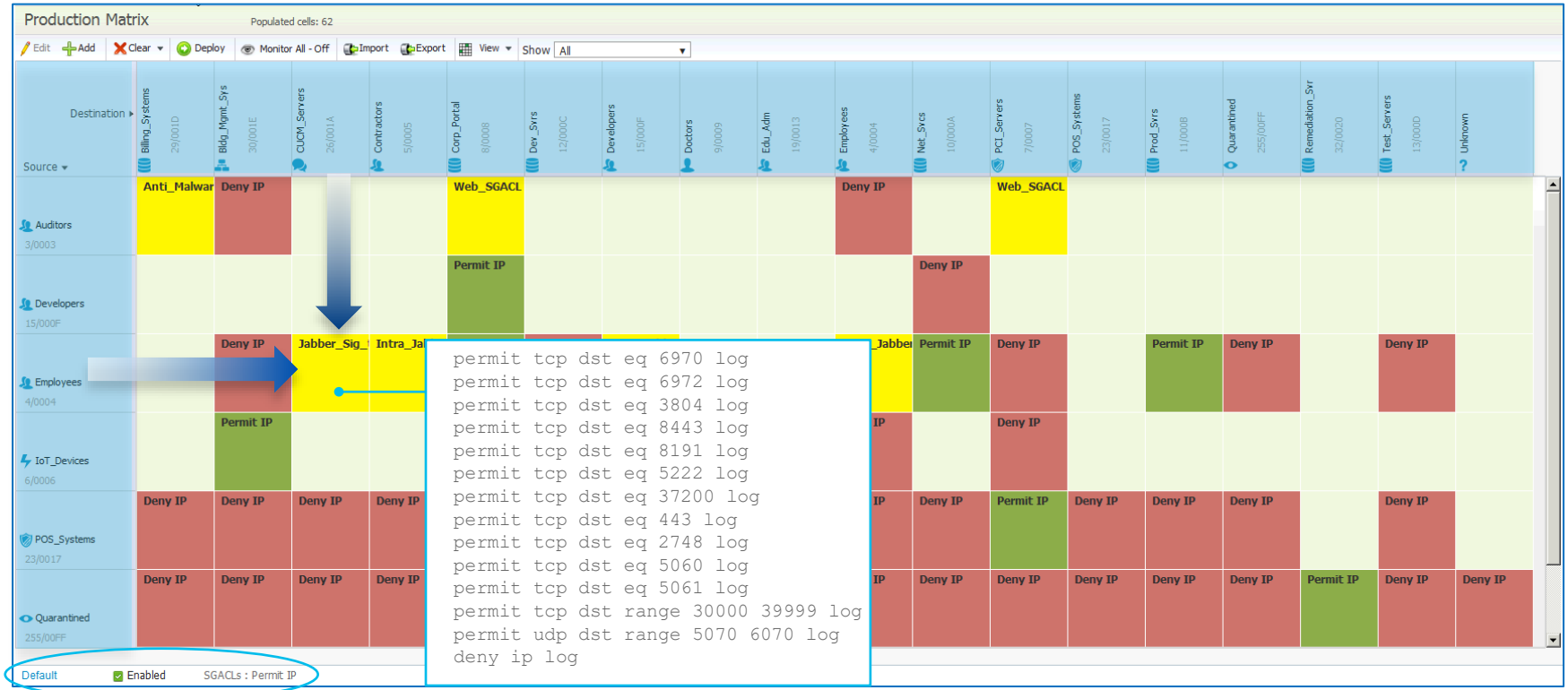
ISE TrustSec matrix

Source \ Destination	1120asaVPNuser 18/0012	Auditors 9/0009	BYOD 15/000F	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Employees 4/0004
1120asaVPNuser 18/0012	Permit IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Permit IP
Auditors 9/0009	Deny IP	Permit IP	Permit IP	Permit IP	Permit IP	Permit IP	Permit IP
BYOD 15/000F	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	VPN_ACL2	Deny IP
Contractors 5/0005	Deny IP	Permit IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Developers 8/0008	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

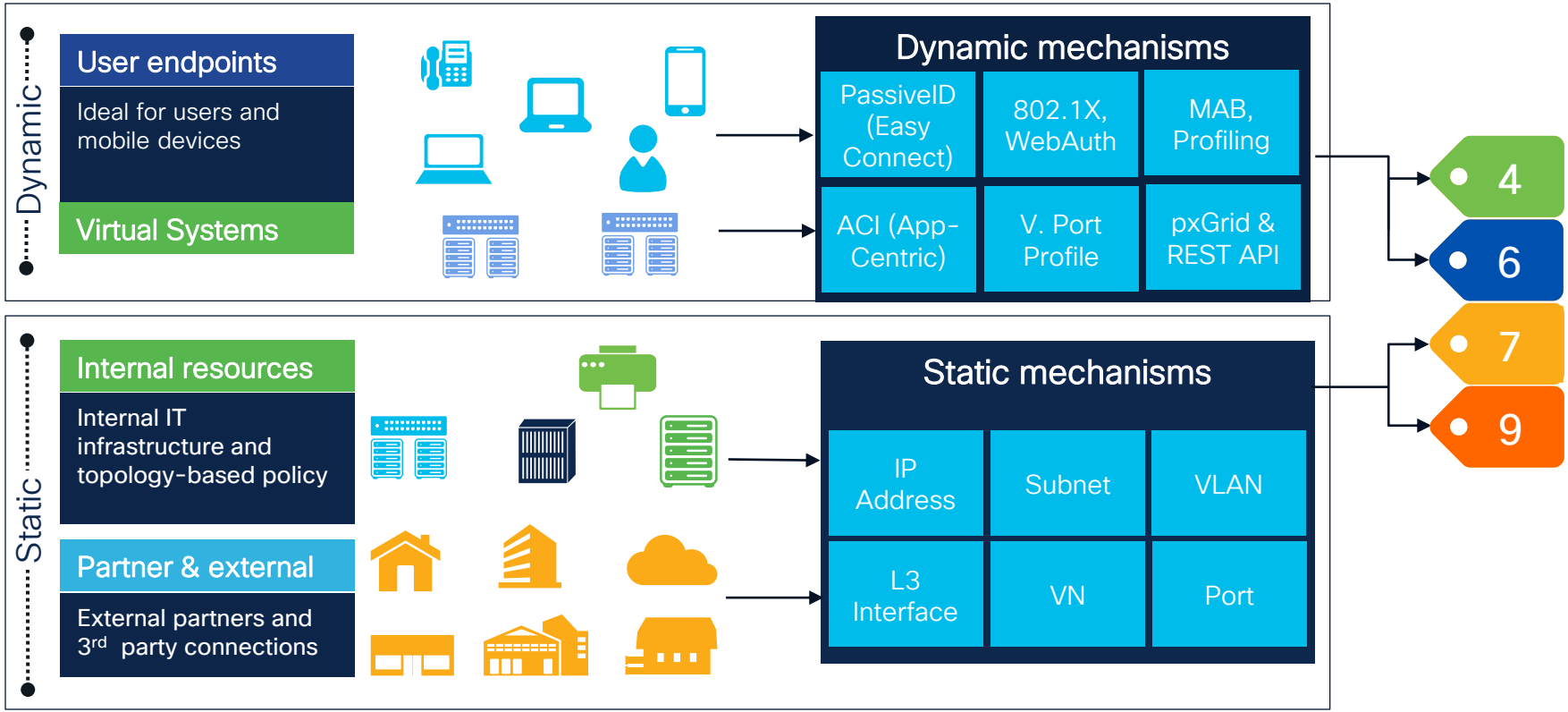
ISE Policy Matrix (SGACL)

Centralized policy for switches, routers, WLCs and APs



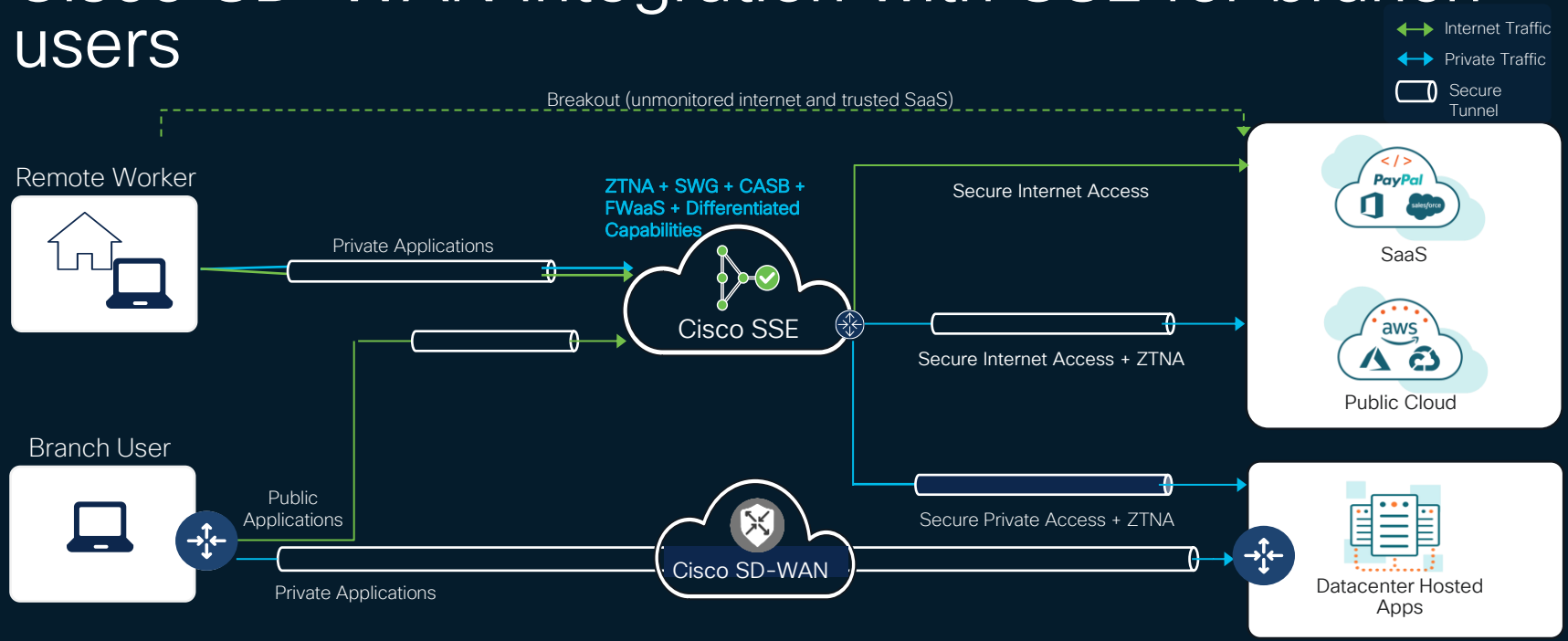
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Classification Methods



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-WAN integration with SSE for branch users



Combine SD-WAN along with powerful security architecture

Steer Branch traffic to private DC with SD-WAN with-out having to hairpin

Connect remote workers securely to Internet / cloud / private applications

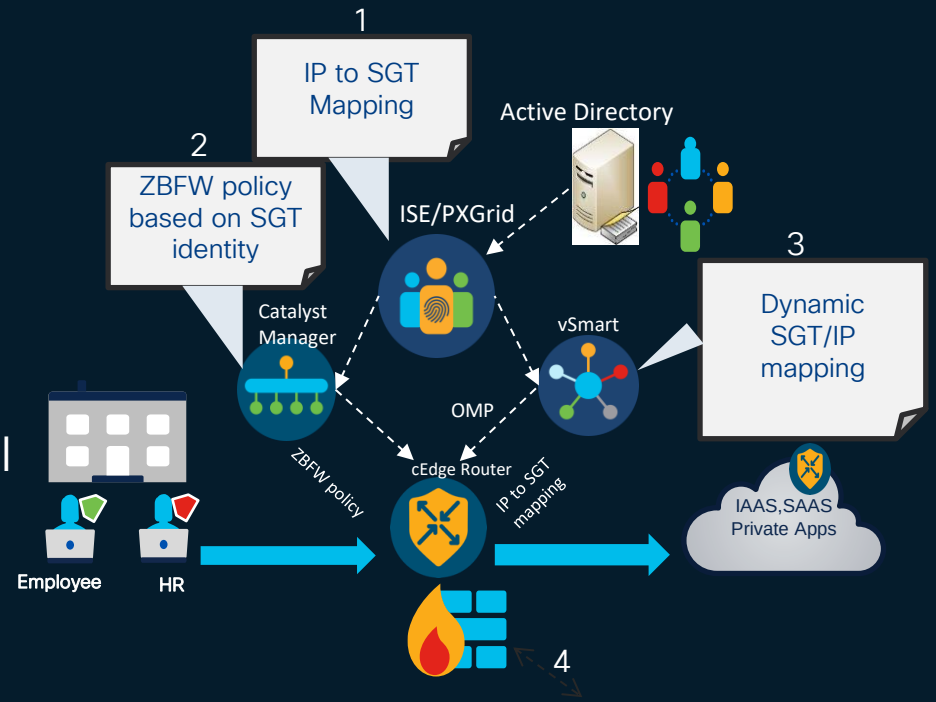
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 20.10/17.10

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SGT Demo

cisco SECURE

cisco The bridge to possible

Zero Trust Demo
Campus Segmentation

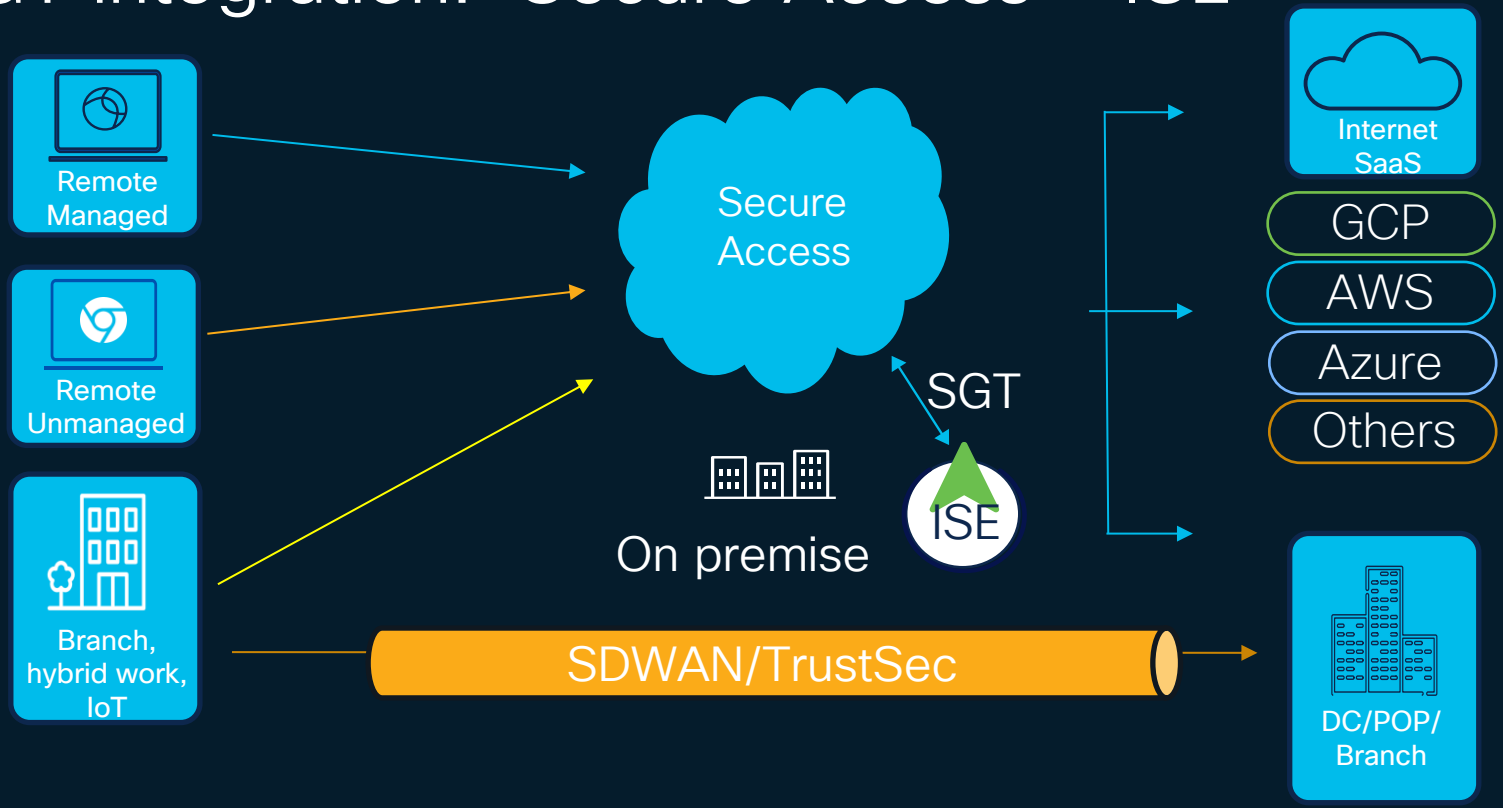
Identity Services Engine + Catalyst Switch demo

August 2024

Demo Lab provided by Keith Simmons, GES TSA

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SGT integration: Secure Access + ISE

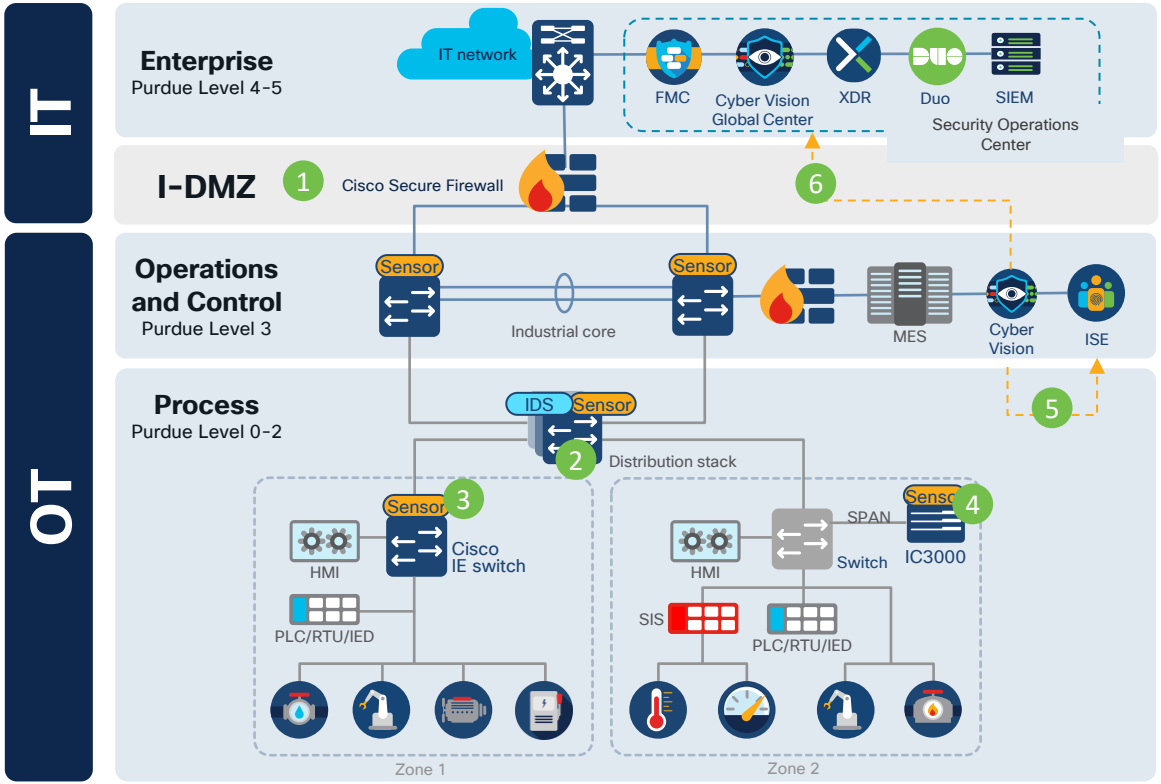


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

On-premises Access
- OT to Private Apps

cisco Live!

Cisco Cyber Vision in manufacturing



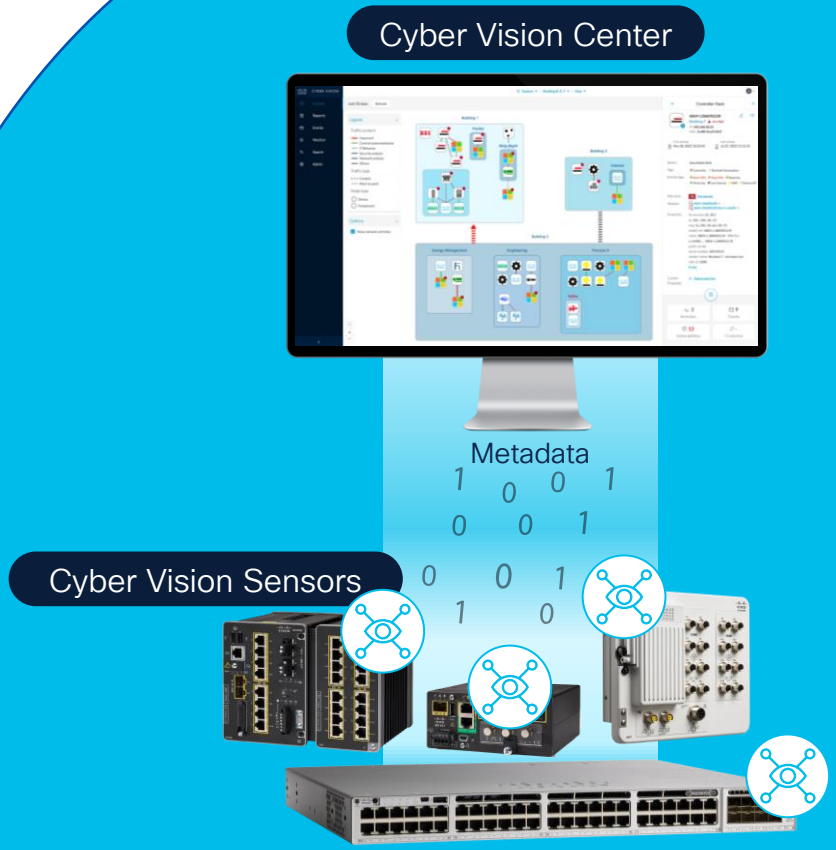
1. Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
2. Create macro-segmentation zones in the Catalyst 9300 switches and deploy Cyber Vision sensors with Snort IDS.
3. Cyber Vision sensors deployed within segments across IE3400 switches
4. Cyber Vision hardware-sensors deployed via one-hop SPAN to gain visibility on non-Cisco switches
5. Build zones and conduits in Cyber Vision and share with ISE for micro segmentation
6. Cyber Vision shares details on OT devices and events with SOC to build informed security policies and investigate threats across domains

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cyber Vision

Manage risks from OT assets with full visibility on your OT security posture

- Asset Inventory & Profiling
- Asset Communications
- Asset Vulnerabilities
- Asset Risk Scores
- Behavior Baselining
- Snort Threat Detection
- Talos Threat Intelligence
- On-prem & Cloud offers

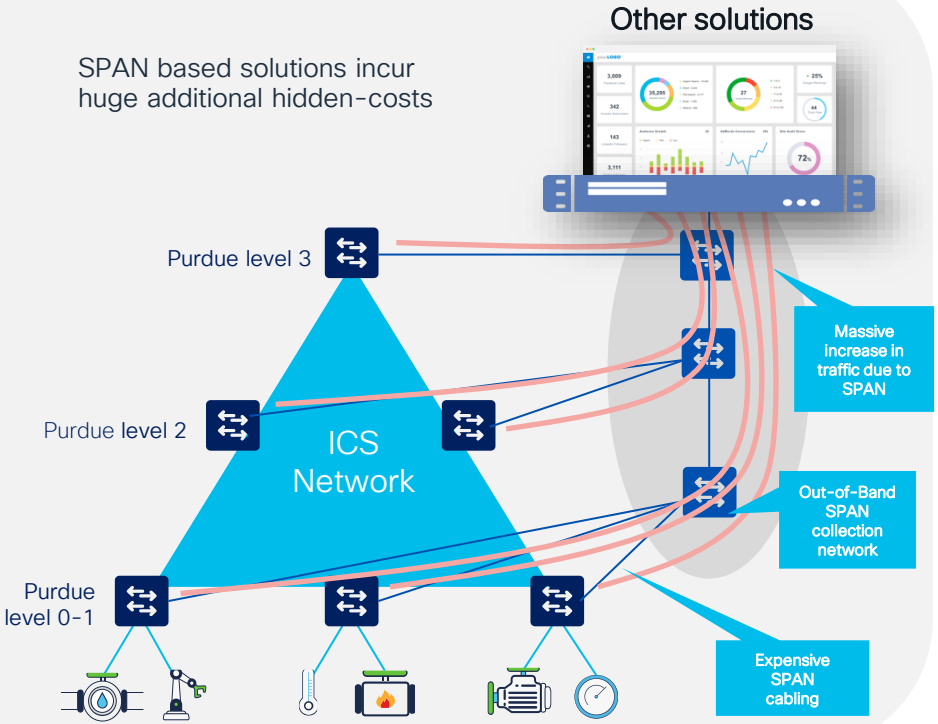


Deep Packet Inspection & Active Discovery
built into your network infrastructure

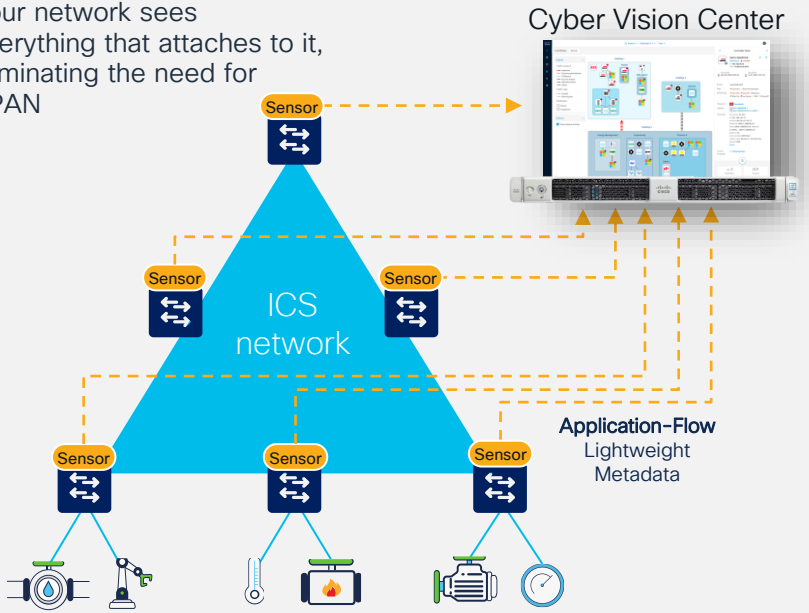
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Old vs new scalable architecture

SPAN based solutions incur huge additional hidden-costs



Your network sees everything that attaches to it, eliminating the need for SPAN

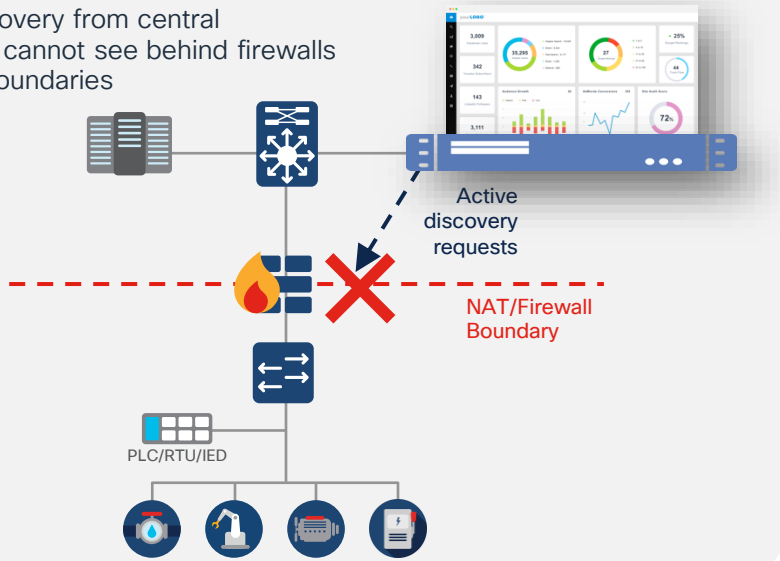


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why is a network-sensor important?
Distributed edge active discovery gives you 100% visibility

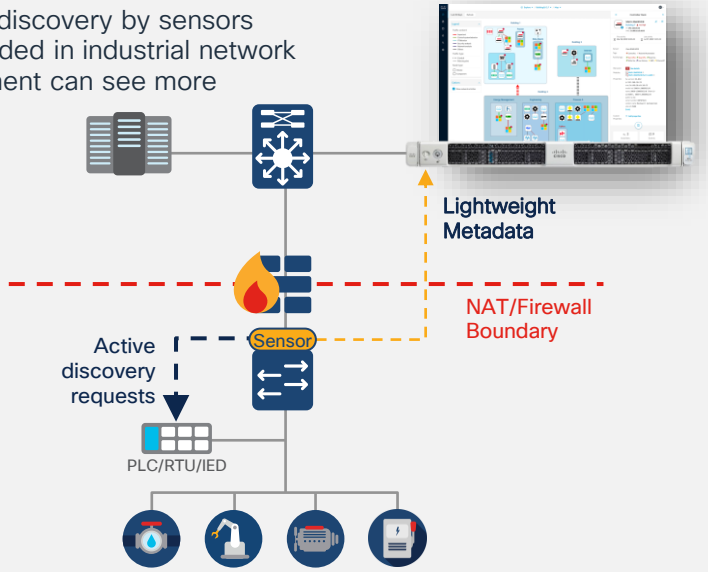
Other solutions

Active discovery from central appliances cannot see behind firewalls and NAT boundaries



Cisco Cyber Vision

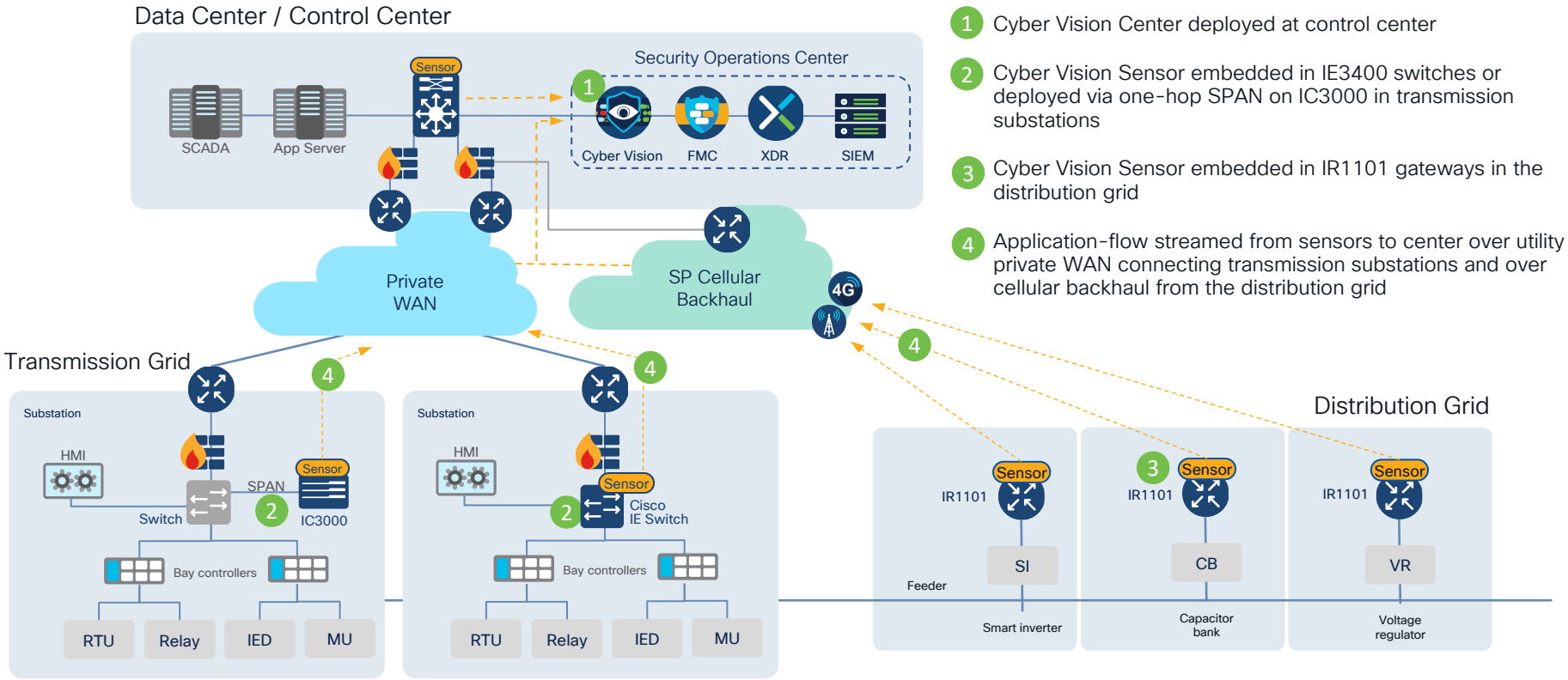
Active discovery by sensors embedded in industrial network equipment can see more



Sensors embedded in the network can see more

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

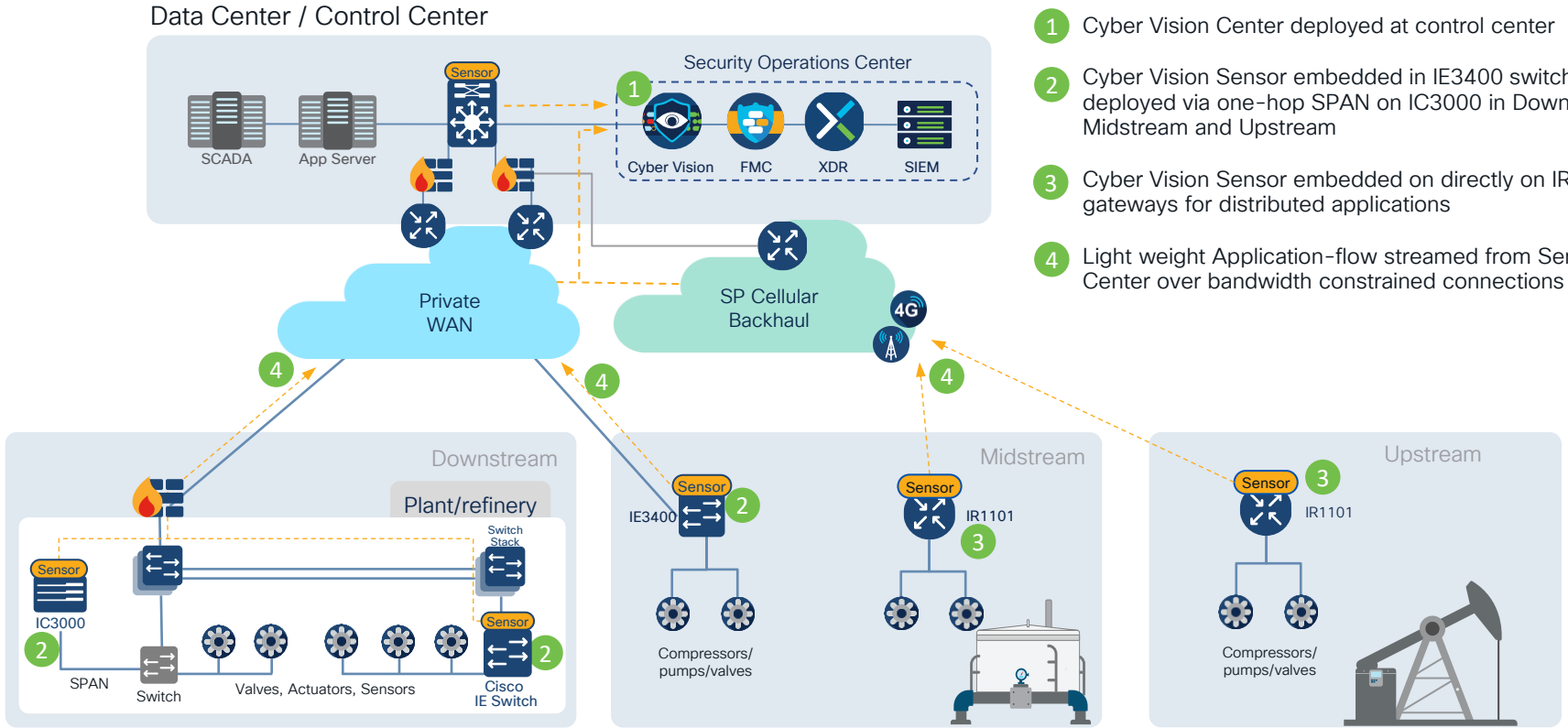
Cisco Cyber Vision in electric utilities



1. Cyber Vision Center deployed at control center
2. Cyber Vision Sensor embedded in IE3400 switches or deployed via one-hop SPAN on IC3000 in transmission substations
3. Cyber Vision Sensor embedded in IR1101 gateways in the distribution grid
4. Application-flow streamed from sensors to center over utility private WAN connecting transmission substations and over cellular backhaul from the distribution grid

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Cyber Vision in oil and gas

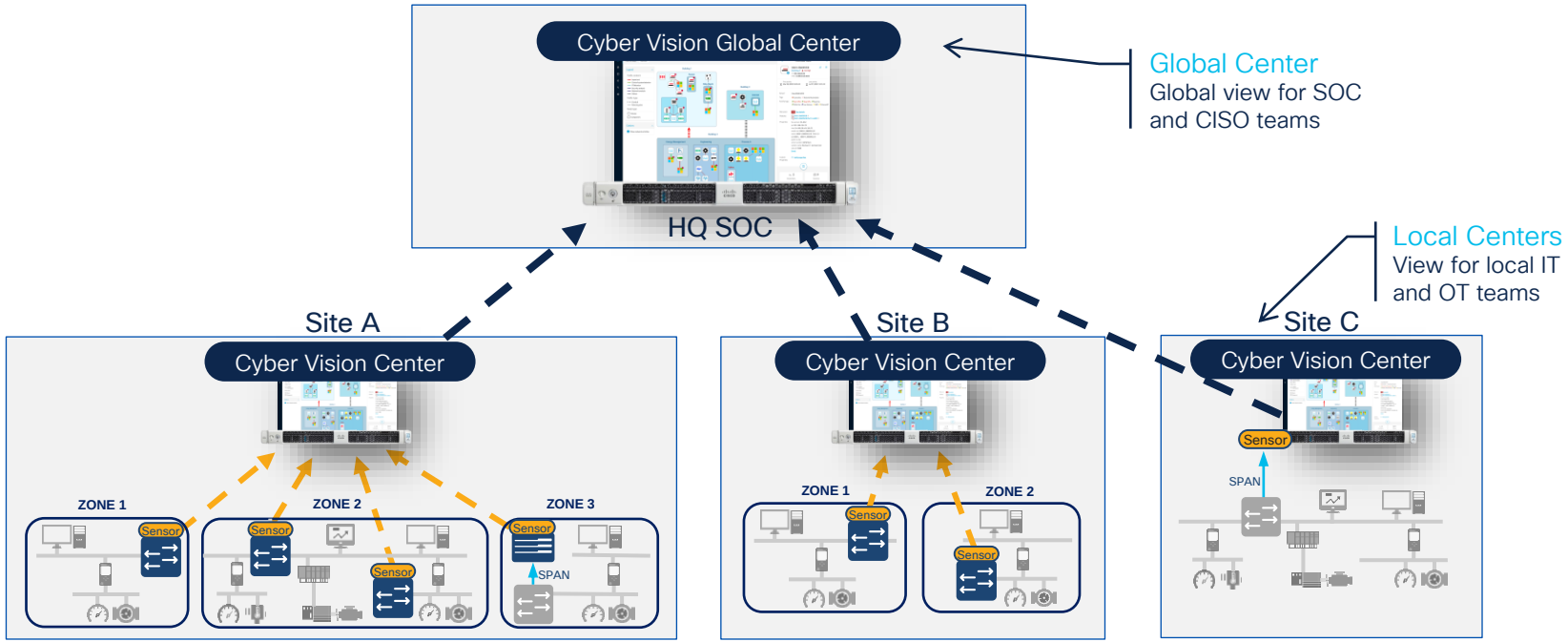


1. Cyber Vision Center deployed at control center
2. Cyber Vision Sensor embedded in IE3400 switches or deployed via one-hop SPAN on IC3000 in Downstream, Midstream and Upstream
3. Cyber Vision Sensor embedded on directly on IR1101 gateways for distributed applications
4. Light weight Application-flow streamed from Sensors to Center over bandwidth constrained connections

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

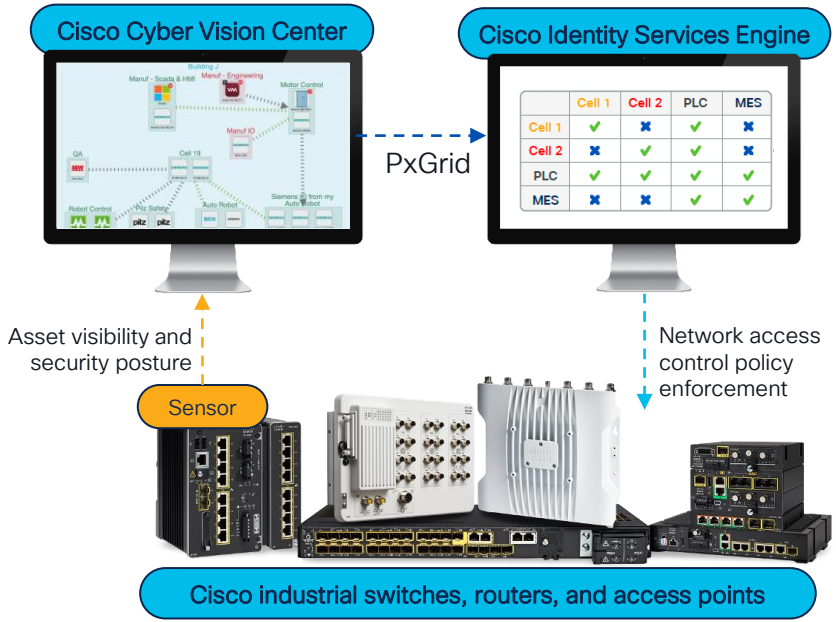
Cisco Cyber Vision Global Center

Global visibility on all sites from a central console



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Visibility drives micro-segmentation with Cisco ISE



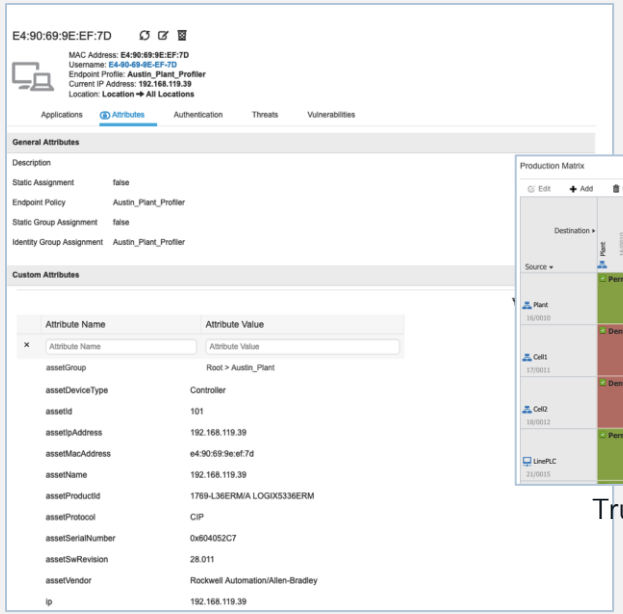
Cisco Cyber Vision
Gain full visibility into assets, and group them according to their role in the industrial process

Cisco Identity Services Engine
Automatically update access control policies for the network to enforce zero-trust segmentation based on Cyber Vision groups

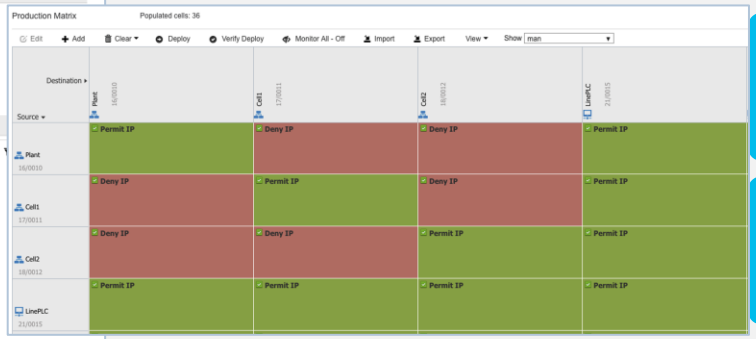
Enforcing network access policies for each device connected to the industrial networks

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Integration with Cisco Identity Services Engine (ISE)



Devices in ISE get attributes from Cyber Vision



TrustSec policy to enforce zone segmentation

Enrich endpoint attributes in ISE with rich context from Cyber Vision

Assign SGTs based on Cyber Vision grouping for dynamic policy assignment to endpoints

Enforce segmentation through dynamic assignment of VLAN, dACLs or TrustSec

Device information can be sent to ISE based on user selection and filtering of network.

Cyber Vision and ISE enable dynamic segmentation of industrial networks

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cyber Vision Demo on Cisco dCloud

Cisco Cyber Vision 4.3 Instant Demo v4

ID: cisco-cyber-vision-4-3-instant-demo-v4 Published Date: 08-Apr-2024 08:39 Instant Demo Internet of Things (IoT) Security Industrial security IoT Manufacturing English

Learn how Cisco Cyber Vision leverages deep packet inspection (DPI) with the ability to decode industrial protocols to identify assets, application flows, and compare against known baselines to identify anomalies or operational change.

★ Favorite Copy Related Documents View

Securing Industrial Networks with Cisco Cyber Vision Demo

ID: securing-industrial-networks-with-cisco-cyber-vision-demo Published Date: 25-Oct-2022 01:19 Guided Demo Enterprise Networks Internet of Things (IoT) Security English

This is a Guided demo based on the Scheduled demo: Securing Industrial Networks with Cisco Cyber Vision Demo v3.1.

Cisco's Securing Industrial Networks solution solves manufacturer challenges such as cyber attacks through Visibility and Analytics, Secure Remote Access, Segmentation, and Services. In this demo we focus on the former three security capabilities using Cisco Cyber Vision, Identity Services Engine (ISE), Firepower Threat Defense (FTD), Duo, Stealthwatch, and DNA Center (DNAC).

★ Favorite Copy View

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Validated Designs

Cisco Validated Design

Reference architectures validated for the specific needs of your industry

Faster deployments

Less risk

Predictability

End to end designs

Design, deploy, and extend networking and cybersecurity technologies successfully

Helping industries with generic and specific designs, as well as addressing regulatory requirements.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cyber Vision 5.0 – Attributes via pxGrid

ISE attribute	Cisco Cyber Vision property	Description
IOTASSET Library		
assetId	ID	Cyber Vision Component ID
assetName	Name	Component name
assetIpAddress	IP	Component IP address
assetMacAddress	Mac	Component MAC address
assetVendor	Vendor-name	Component manufacturer (IEEE OUI)
assetProductId	Model-ref	Manufacturer product ID
assetSerialNumber	Serial-number	Manufacturer serial number
assetSwRevision	Fw-version	Component firmware version
assetHwRevision	Hw-version	Component hardware version
assetProtocol	Protocols	All Protocols concatenated in one string
Custom Attributes		
assetModelName	Model-name	Manufacturer model name
assetOsName	OS-name	Operating system name
assetProjectName	Project-name	Project name (from PLC program)
assetProjectVersion	Project-version	Project version (from PLC program)
assetGroup	Group	Component group in Cyber Vision
assetGroupPath	Group Path	Component group path in Cyber Vision (Nested Groups)
assetCustomName	Custom Name	Custom Name assigned to component by user

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

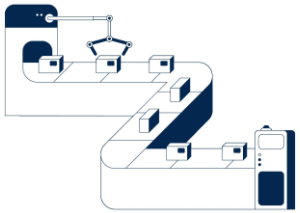
Zero trust use cases

Remote User

- ZT access to public SaaS
- ZTNA to private apps
- Client-based VPN private app access
- Secure Connect (VPNaaS)
- *Unified ZTNA client (roadmap)

On-Premises User & IOT

- Campus .1x/MAB to public SaaS
- Campus .1x/MAB to private apps
- Branch .1x/MAB to public SaaS
- Branch .1x/MAB to private apps



App-to-App

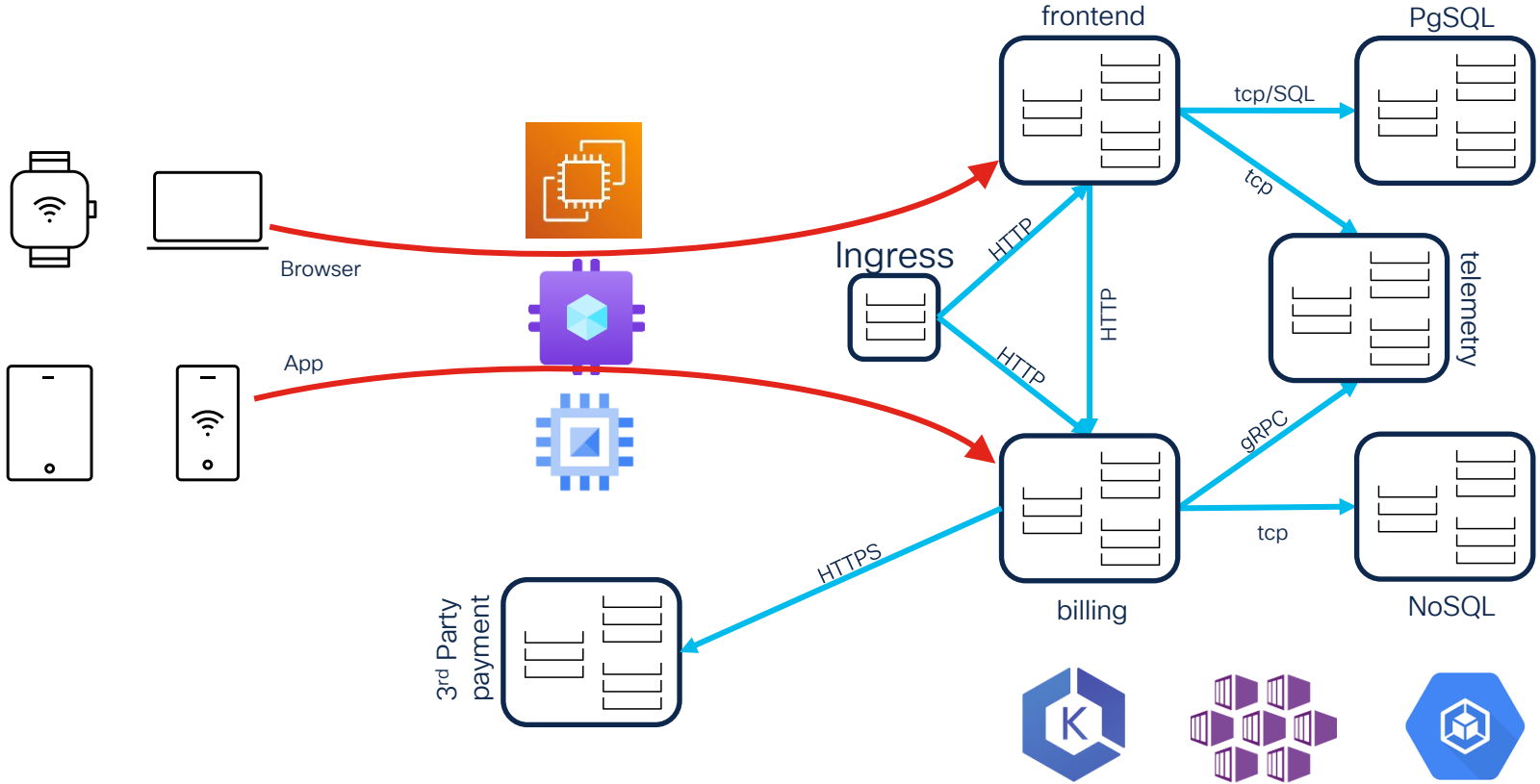
- App-to-App across multi-cloud

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing Private Application Across Multi-cloud

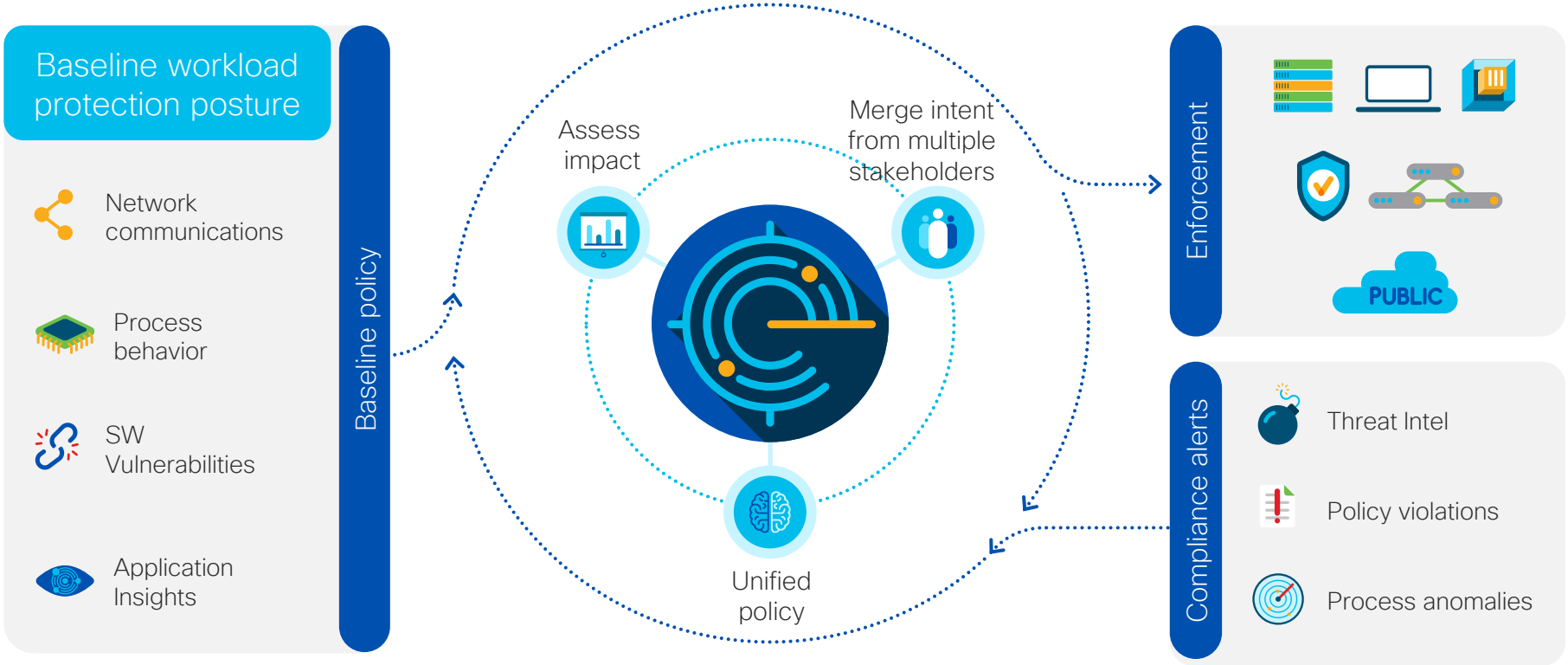
cisco Live!

Application architectures have evolved

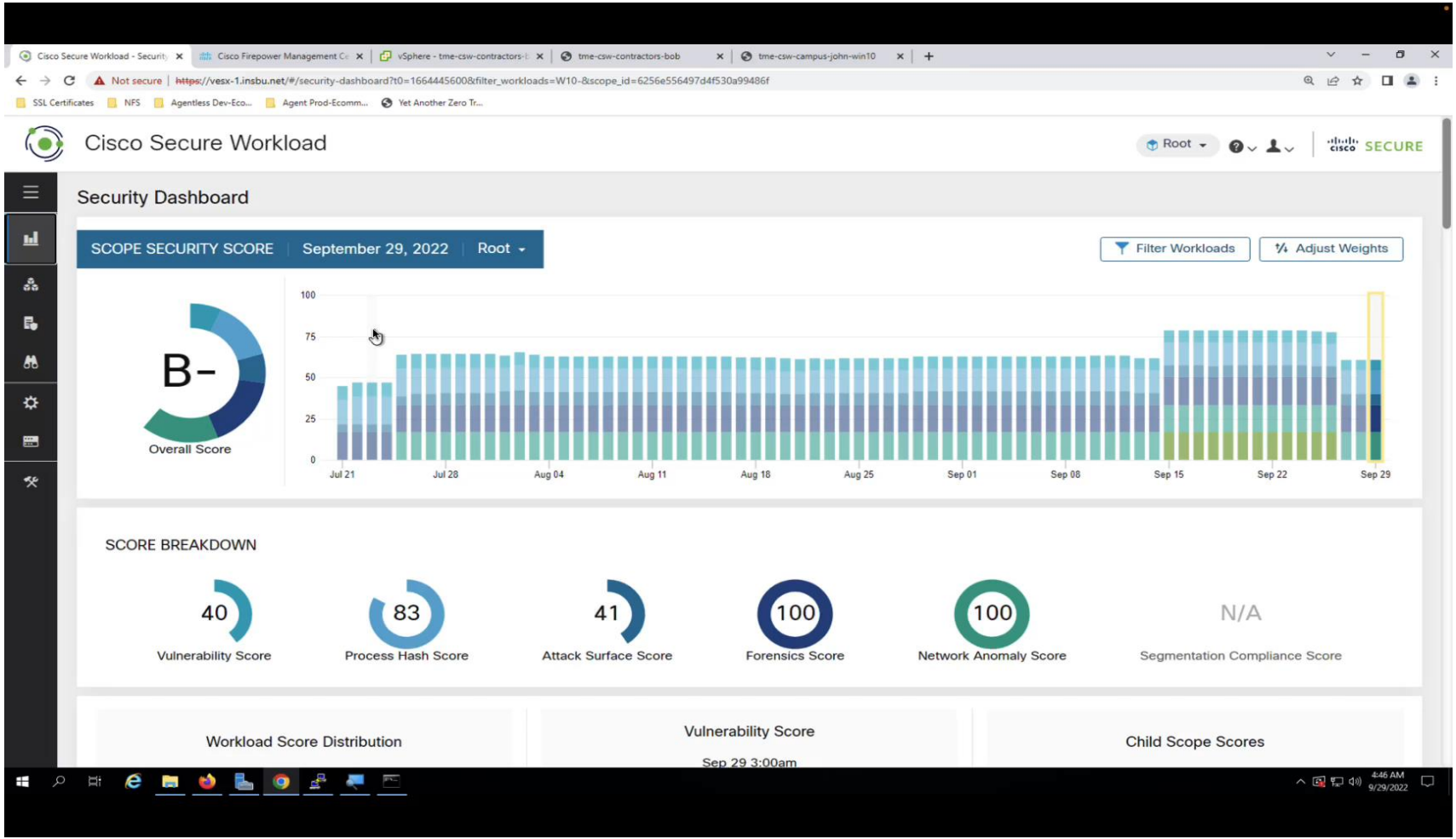


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

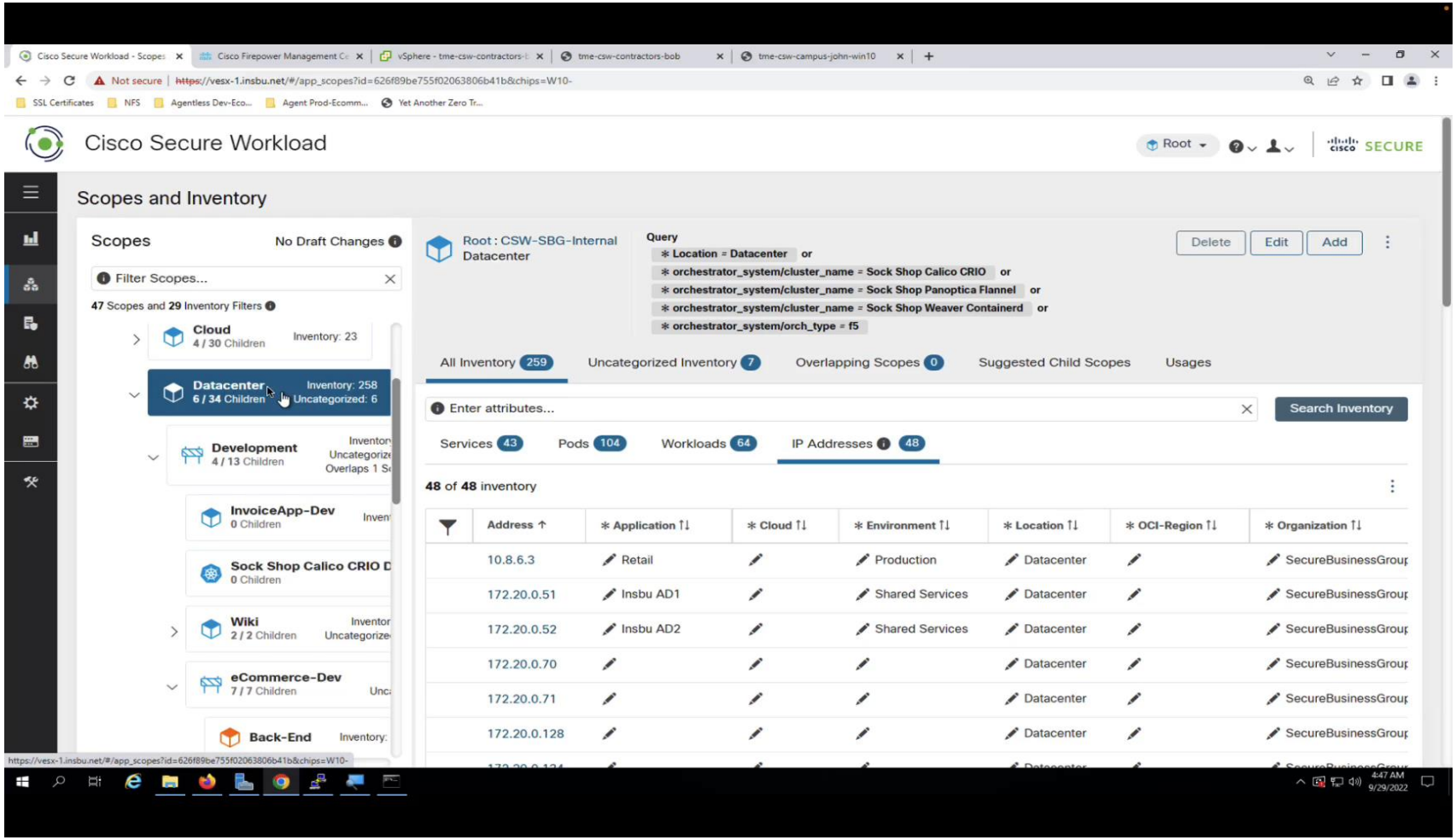
Achieving ZT framework with Cisco Secure Workload



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



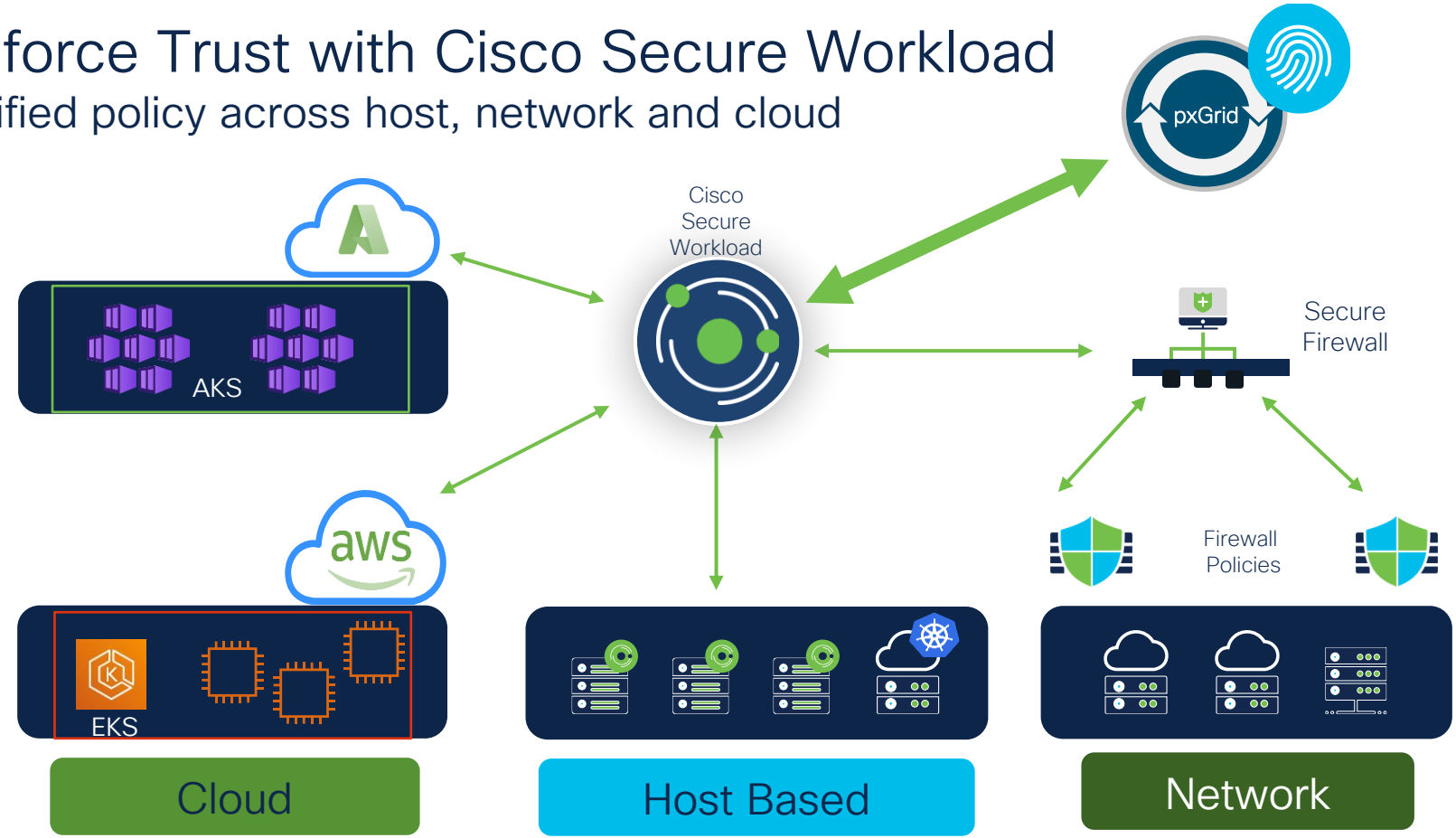
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



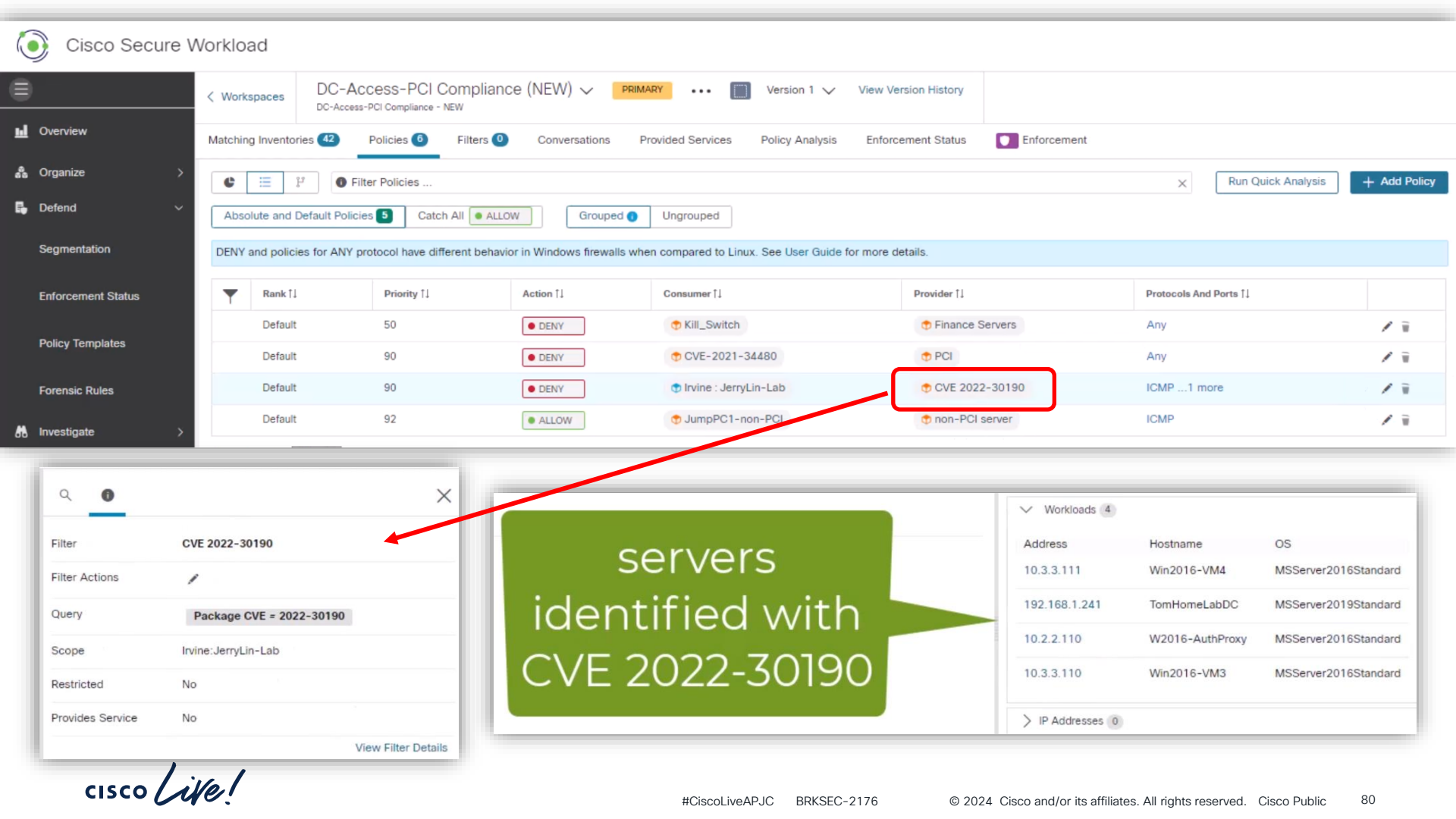
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enforce Trust with Cisco Secure Workload

Unified policy across host, network and cloud



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Summary

Your Take Aways

1

Accelerate Zero Trust
- ✓Deliver excellent user experience
- ✓FREE Identity Security Assessment

2

ISE+TrustSec for segmentation
- ✓Unify IT/OT if practical

3

Zero Trust policy should be end-to-end
- ✓ Include workload and application security

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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**.

Score = 5(excellent)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

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

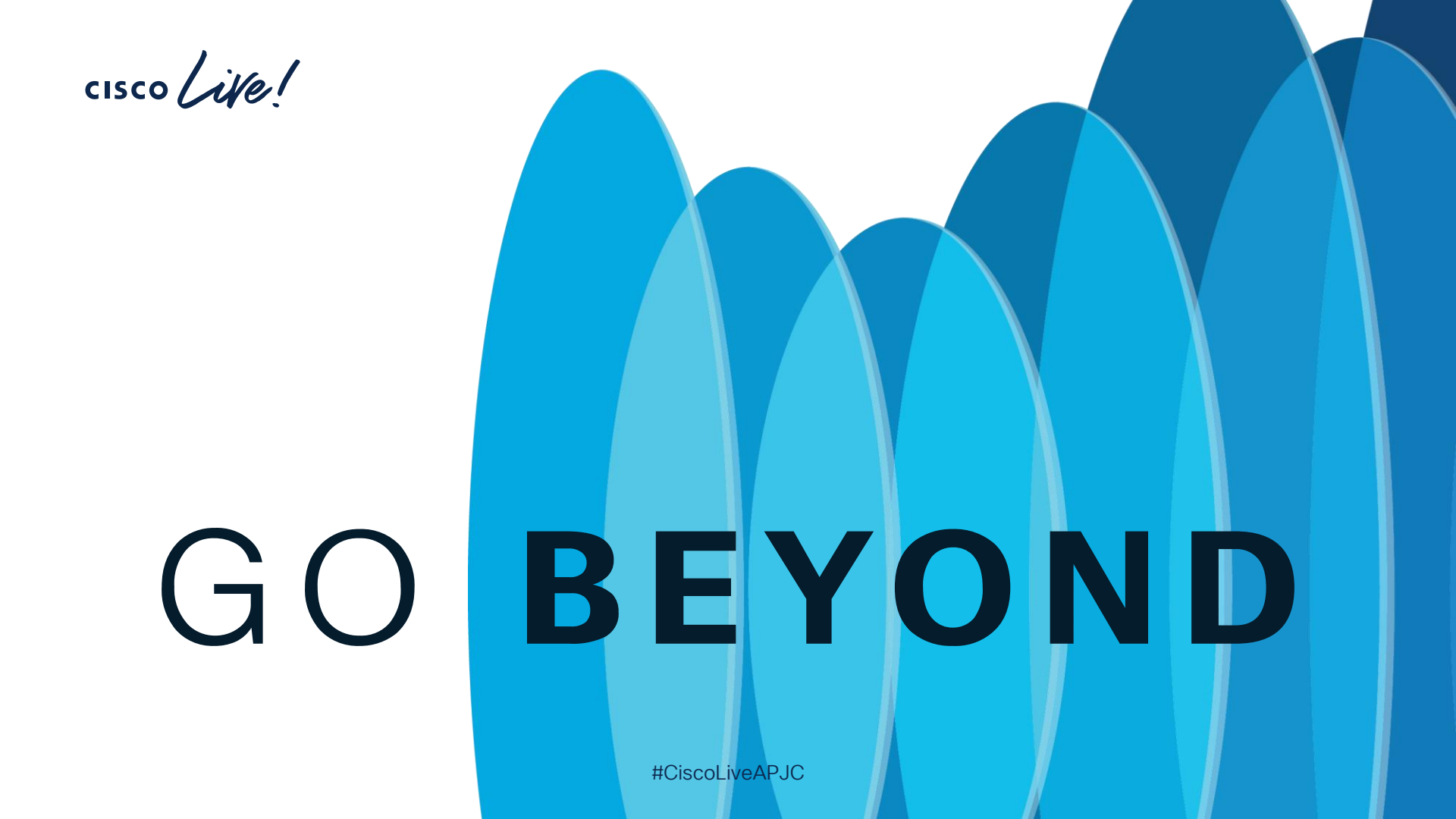
Continue your education

- 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

Contact me at: jelin@cisco.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC