

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Keeping Up With Zero Trust

Jerry Lin, Principal Solutions Engineer, GSSO

BRKSEC-2176



#CiscoLiveAPJC

Cisco Webex App

Questions?

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

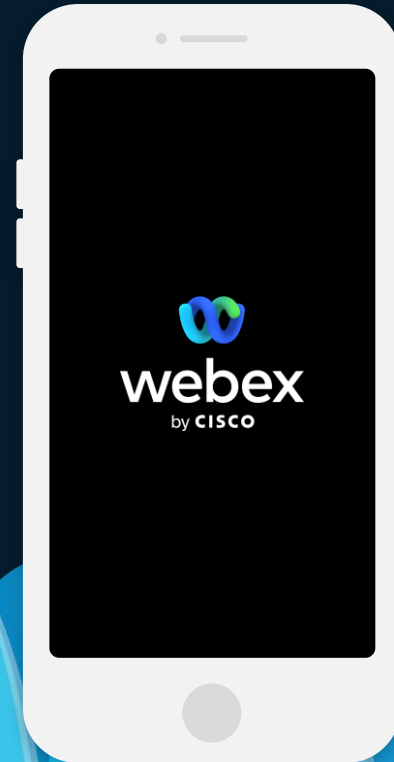
How

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

Webex spaces will be moderated by the speaker until November 15, 2024.



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





Agenda

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

What Zero Trust Means to Us



Never assume trust.
Always verify.
Enforce risk-based
least privilege.

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

The state of zero trust maturity



Identity



Network



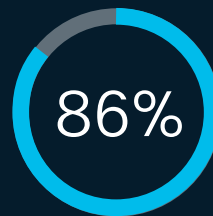
Devices



Apps/Workload

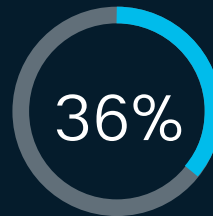


Data



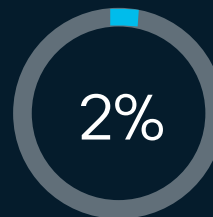
Nearly all organisations have started on some aspect of zero trust (at least one pillar)

"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



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

📅 Nov 01, 2024 👤 Ravi Lakshmanan

Vulnerability / Cloud Security

Microsoft Warns of Chinese Botnet Exploiting Router Flaws for Credential Theft

📅 Nov 01, 2024 👤 Ravi Lakshmanan

Threat Intelligence / Network Security

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

📅 Oct 28, 2024 👤 Ravi Lakshmanan

Cloud Security / Cyber Attack

“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.”

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

Zak Doffman Contributor ①

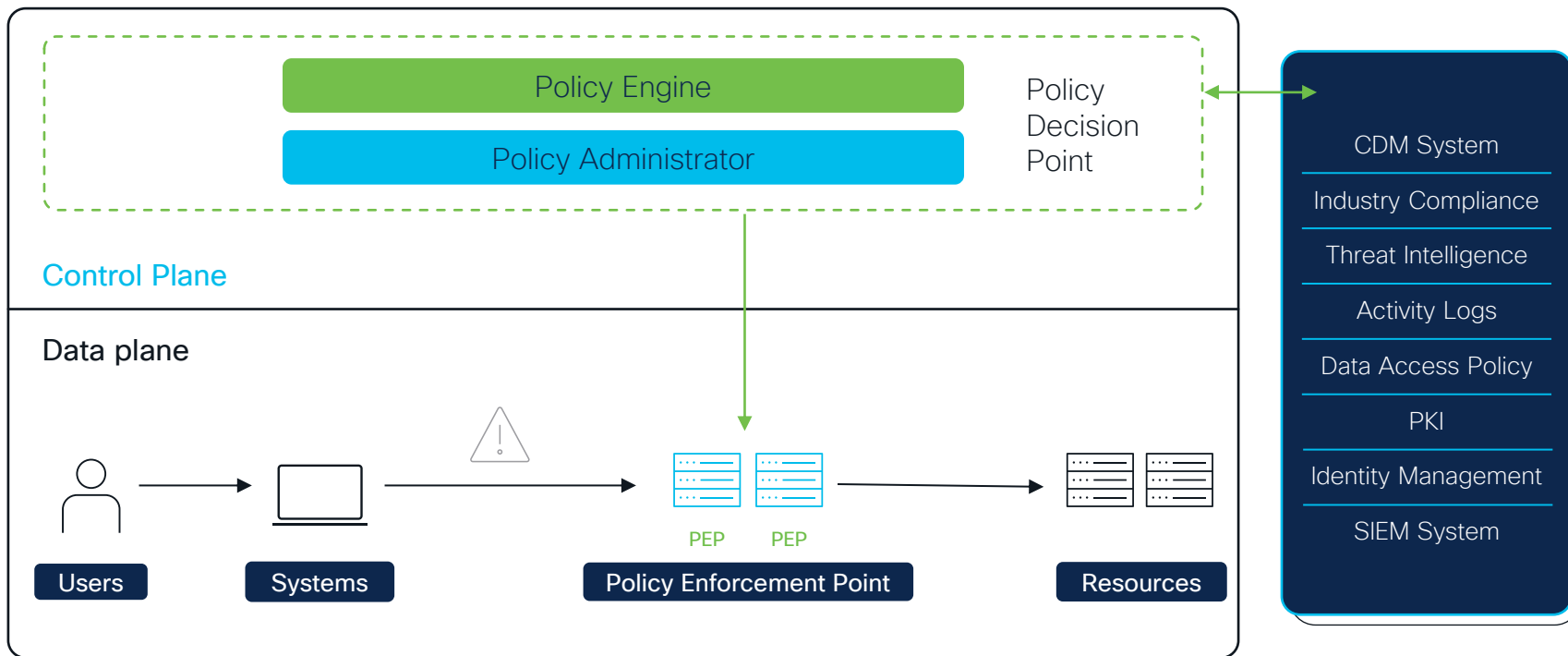
Zak Doffman writes about security, surveillance and privacy.

Follow



Nov 3, 2024, 05:38am EST

NIST 800-207 – Zero Trust Architecture

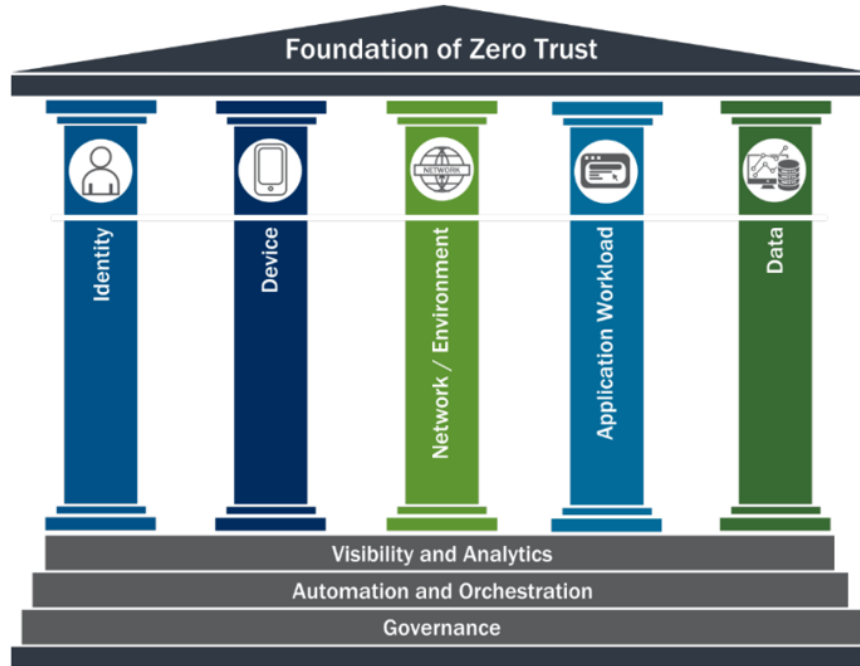


CISA - zero trust pillars - ZT maturity model

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

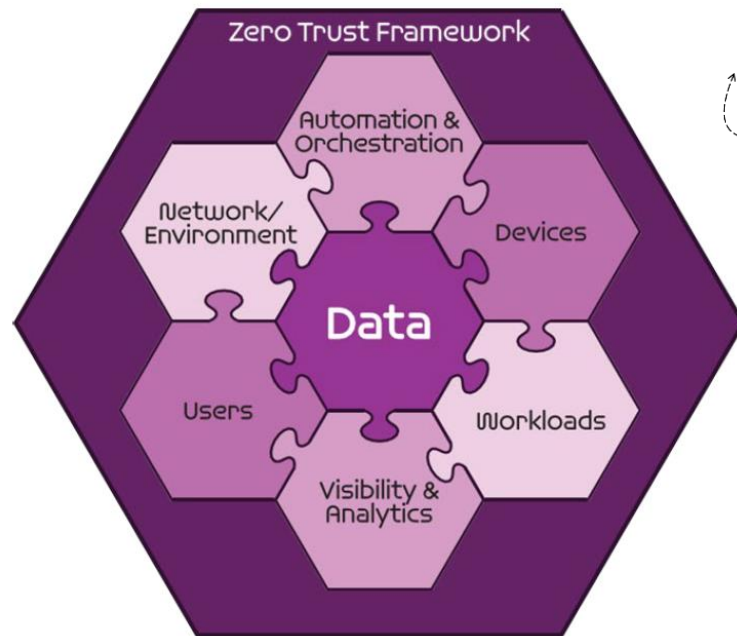
Dynamic – Continuous – Integrated – Optimised – Automated

Behaviour and posture analytics – suspicious and malicious behaviours

DISA zero trust framework

Defense Information Systems Agency

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



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

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



XDR SECURITY
OPERATIONS TOOLSETCisco Vulnerability Management | Secure Analytics
XDR | Secure Client | Splunk
Talos Incident Response

SERVICES

Custom threat
research on demandImplement
and manageIncident response
retainer

CAPABILITIES

Network detection
& responseDevice discovery
& insightsEndpoint detection
& response

Zero Trust

Identity
Threat
Detection &
Response

SOAR

SIEM

Threat visibility, incident
response & threat hunting

ZERO TRUST

SASE

User / Device Security

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

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

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

Browser access control | RAaaS | Cloud access security broker | Remote browser isolation | Cloud malware detection | Secure web gateway | Data loss prevention | TLS decryption | DNS-layer security | Zero Trust Network Access | FWaaS | Identity / posture | 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 tag propagation | IPSecVPN | 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 tag classification | Identity/pxGrid Cloud | Network access control | Network security analytics | NGFW | NGIPS | Security analytics & logging | Segmentation | Threat mitigation | Profiling

Industrial Threat Defense

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

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

Workload, Application, and Data Security

ACI | Attack Surface Management | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Multicloud Defense | Secure Workload | Hypershield

Hybrid Multicloud Infrastructure

DDoS WAF/Bot | Identity pxGrid | Macro segmentation | Flow analytics | Threat mitigation | Deployment automation | Firewall NGIPS | Defense gateway

Cloud Native Application Platform

External Attack SM | CSPM/CAASM | Micro segmentation | API security | App discovery & observability | Code+CI/CD security | Container security | DSPM | Run-time protection

Zero Trust
-Optimise
-Accelerate



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](#)

Attackers adapting: session hijacking is on the rise

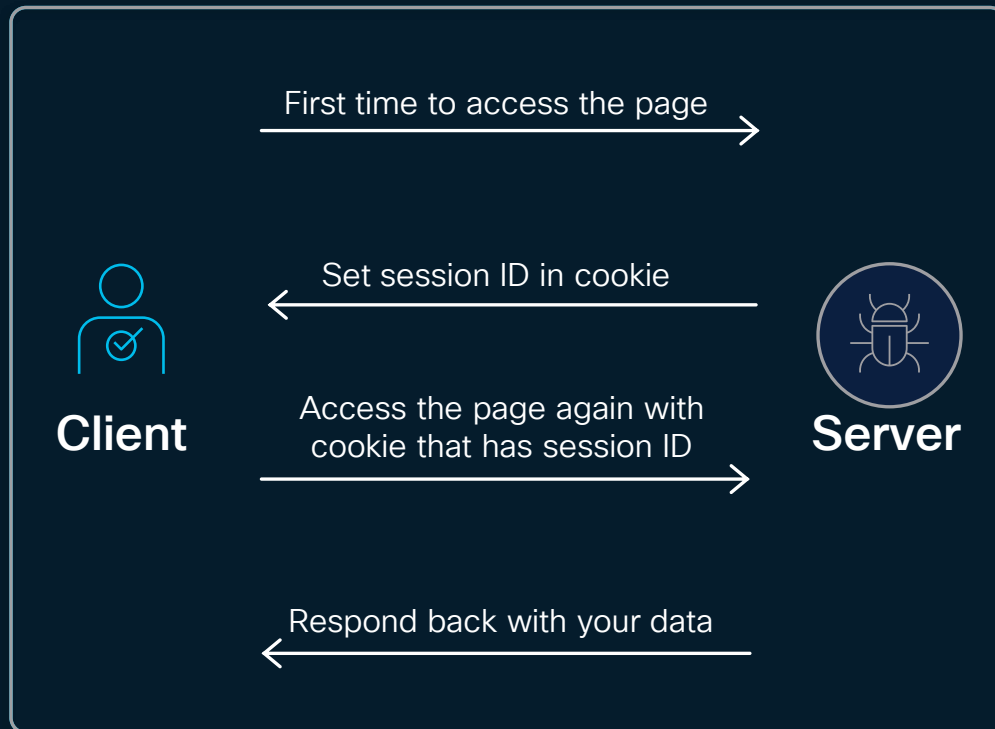
How does it work?

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

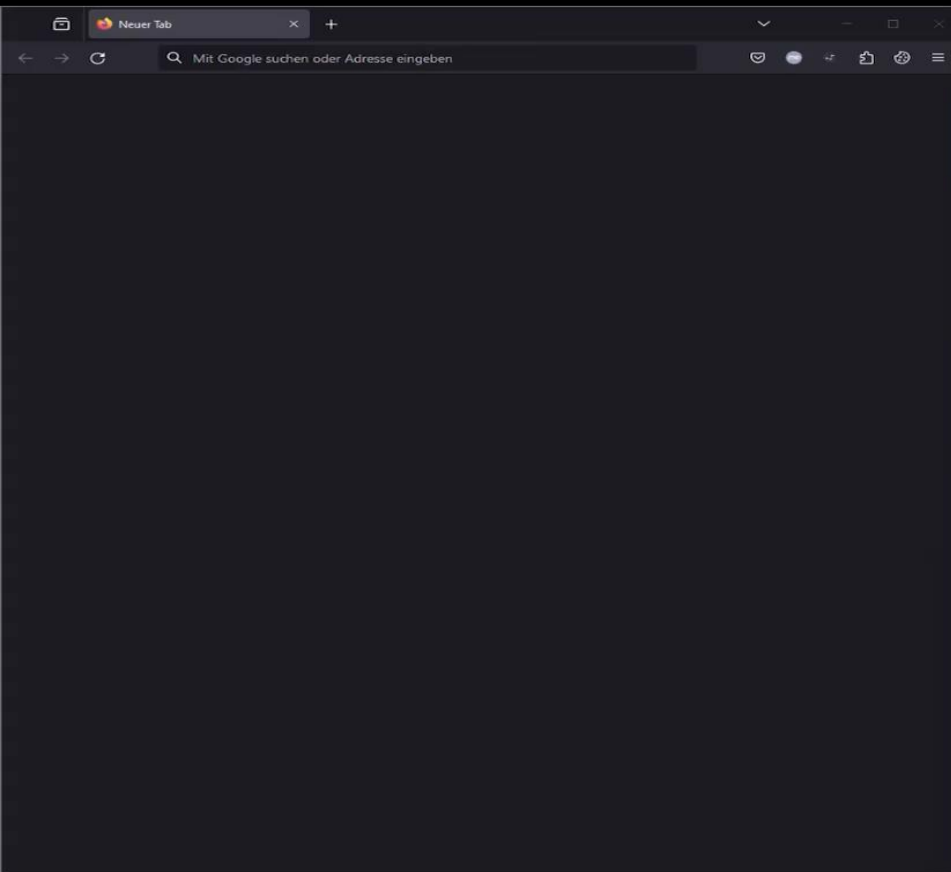
Huge, recent breaches

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



Session Hijack Demo





```
cisco@pi:~$ sudo evilginx
cisco@pi:~$ sudo evilginx

  _____
 /  _  _  _  \
|  _ \| | | | | | |
| |_) | |_| | |
|  _< |  _  | |
|_| \_|_|_|_|_|

  -- Gone Phishing --
by Ruba Gretzky (@margretzky) version 2.4.2

[17:05:16] [info] loading phishlets from: /usr/share/evilginx/phishlets/
[17:05:16] [info] loading configuration from: /root/.evilginx
[17:05:17] [info] blacklist: loaded 29 ip addresses or ip masks
[17:05:17] [info] setting up certificates for phishlet 'o365'...
[17:05:17] [info] successfully set up SSL/TLS certificates for domains: [login.sduernberger.de www.sduernberger.de log
in.sduernberger.de]

  phishlet      | author      | active | status | hostname
  -----
  facebook      | @charlesbel | disabled | available |
  instagram     | @charlesbel | disabled | available |
  linkedin      | @margretzky | disabled | available |
  o365          | @Jamesculum | enabled  | available |
  coinbase     | @AnOnud4y   | disabled | available |
  outlook       | @margretzky | disabled | available |
  paypal        | @AnOnud4y   | disabled | available |
  twitter       | @white_fl   | disabled | available |
  tiktok        | @AnOnUD4Y   | disabled | available |
  amazon        | @customsync | disabled | available |
  booking       | @Anonymous  | disabled | available |
  citrix        | @424f424f   | disabled | available |
  github        | @audibleblink | disabled | available |
  onelogin      | @perfectlylog... | disabled | available |
  protonmail    | @Jamesculum | disabled | available |
  reddit        | @customsync | disabled | available |
  wordpress.org | @seitar     | disabled | available |
  airbnb        | @ANONUD4Y   | disabled | available |
  okta          | @mikesiegel | disabled | available |
  twitter-mobile | @white_fl   | disabled | available |

  I
  :
```

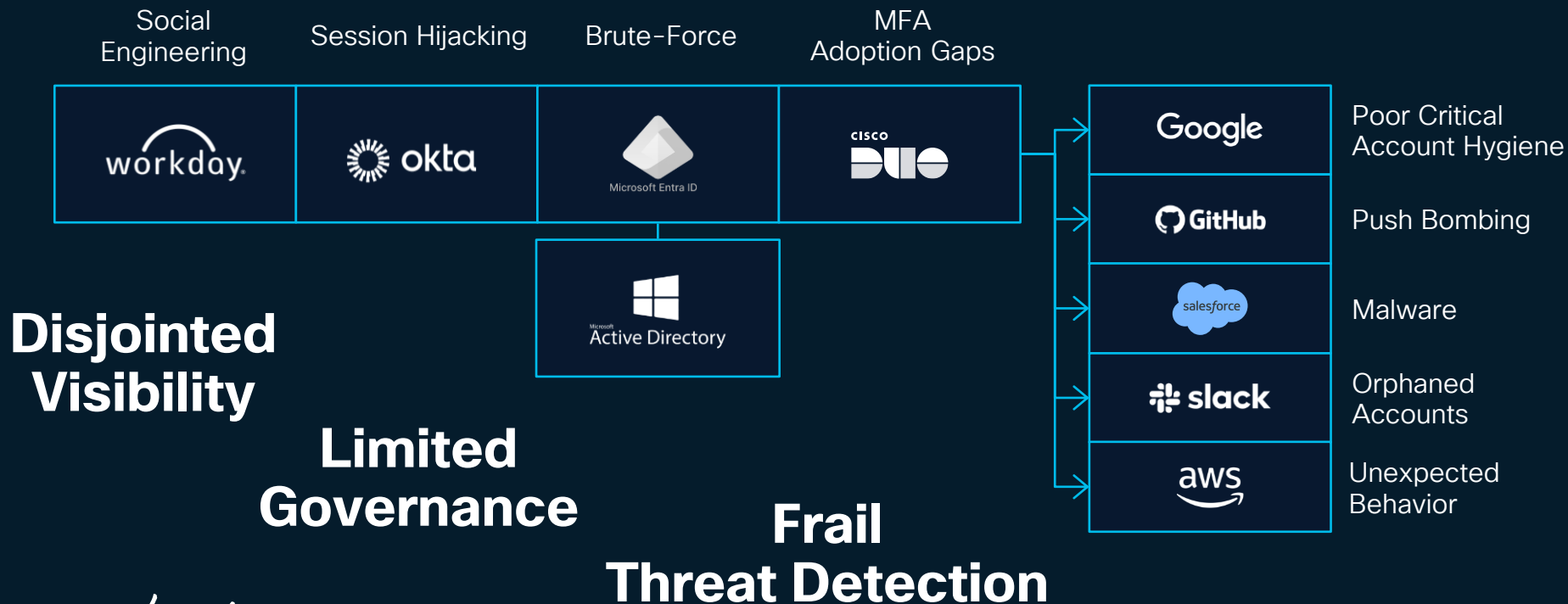
Why **hack** in...



...when you can **login**?

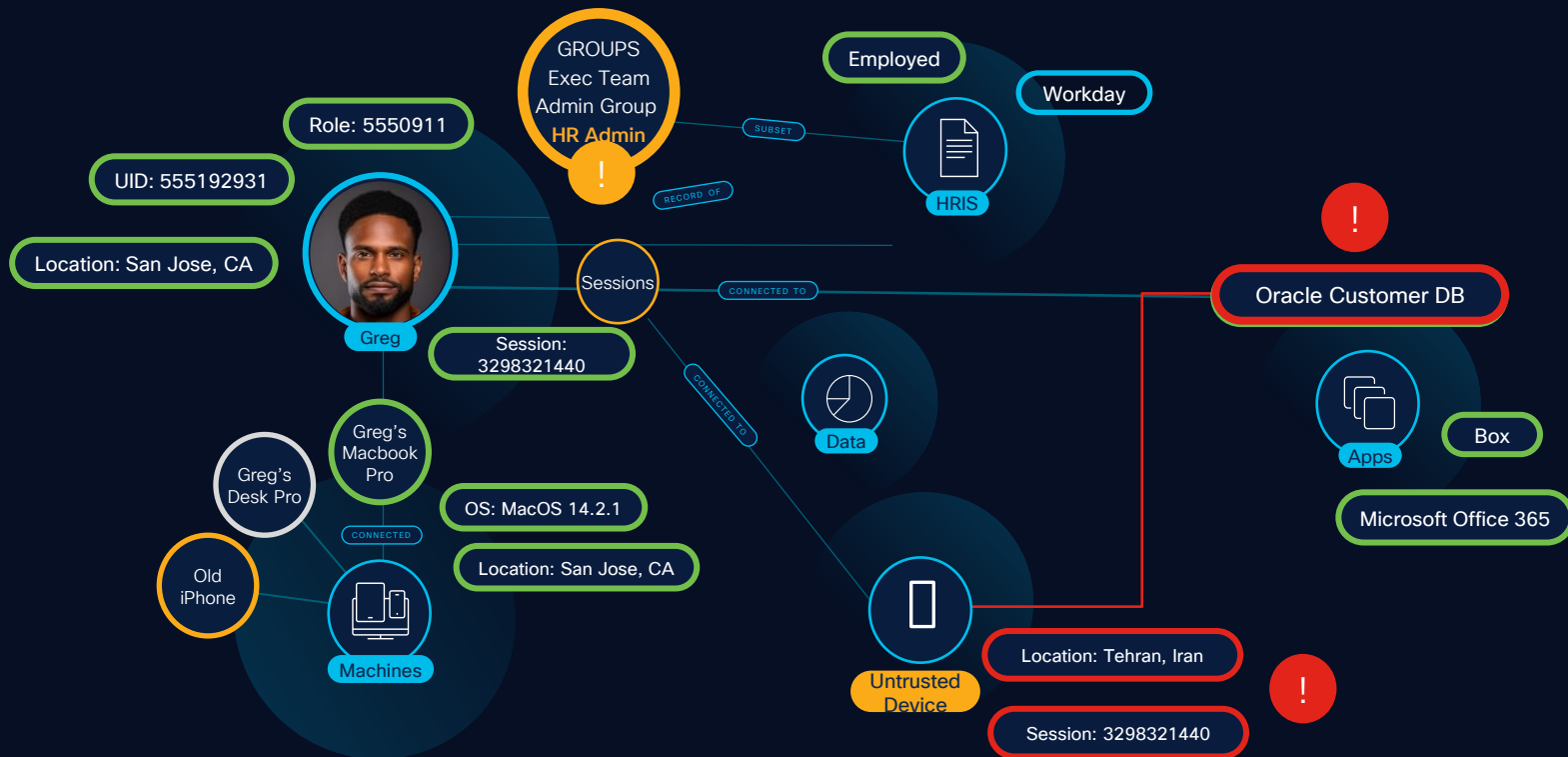
The modern identity stack is complex...

Identity security is a top 3 CISO Concern

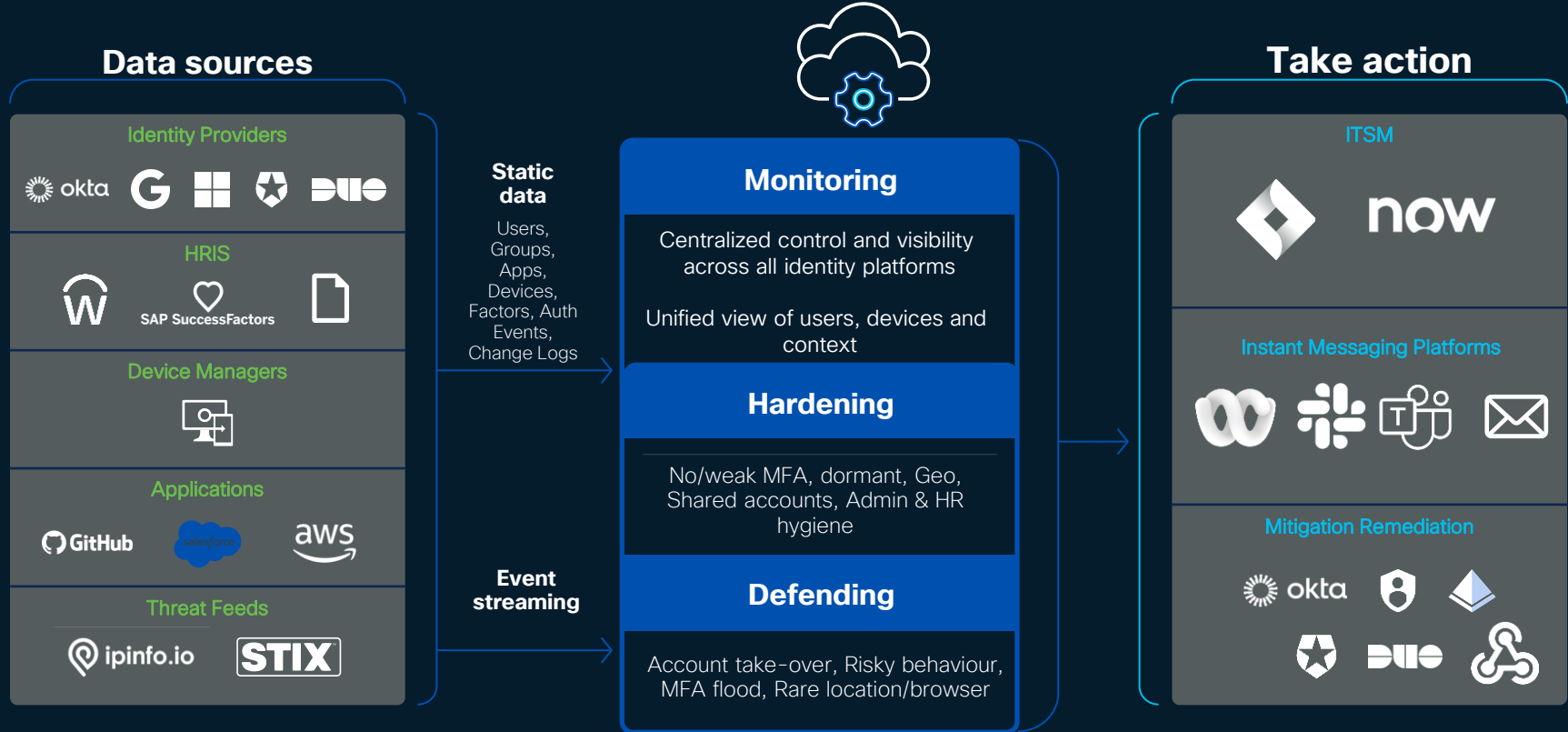


Identity Graph Analytics

Contextual Visibility | Advanced Defense



How Cisco Identity Intelligence works



CLI Demo



genie

Integration Status

10 Providers Synced

[Last data collection](#)

Providers

 **Demo AWS**
Success
Average Traffic: 26 records **Demo Azure AD**
Success
Average Traffic: 25 records **Demo GSuite**
Success
Average Traffic: 65 records **Demo Okta**
Success
Average Traffic: 133 records **Demo Workday**
Success
Average Traffic: 43 records **Demo Auth0**
Success
Average Traffic: 45 records **Demo Duo**
Success
Average Traffic: 59 records **Demo GitHub**
Success
Average Traffic: 19 records **Demo Salesforce**
Success
Average Traffic: 44 records **Slack - oort-teamdata-testing**
Success
Average Traffic: 10 records

Ticketing

 **Cisco Jira** **ServiceNow Instance**

Notification Targets

 **Okta Workflow**
Configured for 1 check **oort-demo**
Configured for 1 check

Identities

235

Total

235

In Protected Population

6

Inconsistent Users

4

Never Logged In

1

Inactive Guest Users

2

Inactive Account Probing

MFA Status

157

No MFA Configured

22

No Strong MFA Configured

22

Weak MFA Was Used To
Successfully Sign In

1

MFA Flood

1

Telecom MFA Limit Reached

4

Admins with Weak MFA

Cisco Identity Intelligence

Identity Posture Score ⓘ

Last Update: Aug 23, 2024

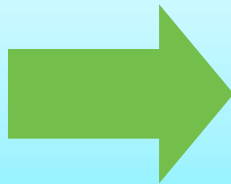
Identity Posture Trend

30d Jul 24, 2024 21:51 - Aug 23, 2024 21:51 UTC ▾

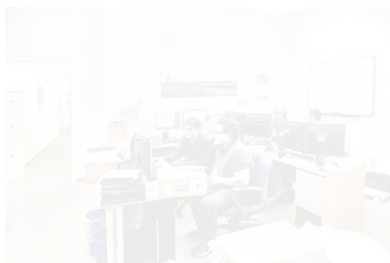
Zero trust use cases



Hybrid
Worker



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



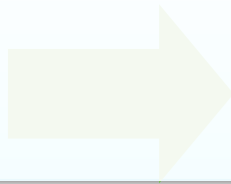
On-
Premises
User &
IOT



- 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

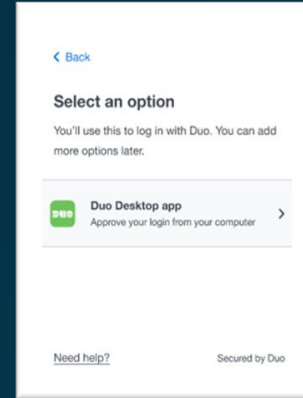
Accelerate Zero Trust Access

Duo Passport

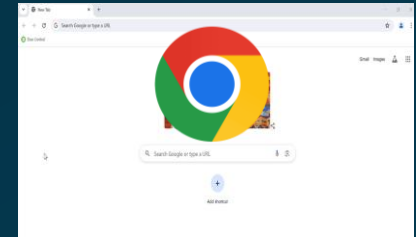


Log in **once** on a trusted device and access all web and client applications without requiring additional authentication by the user.

Desktop Authenticator



Device Trust Connector (Chrome)



* Private preview (Windows OS)

Duo Demos

- Passport
- Desktop Authenticator
- Chrome DTC





Lee

Sign in



Lee



Duo Desktop Authenticator



Cisco Umbrella

To log in, please enter your Umbrella email below.
You will be routed to your SSO identity provider
for login verification.

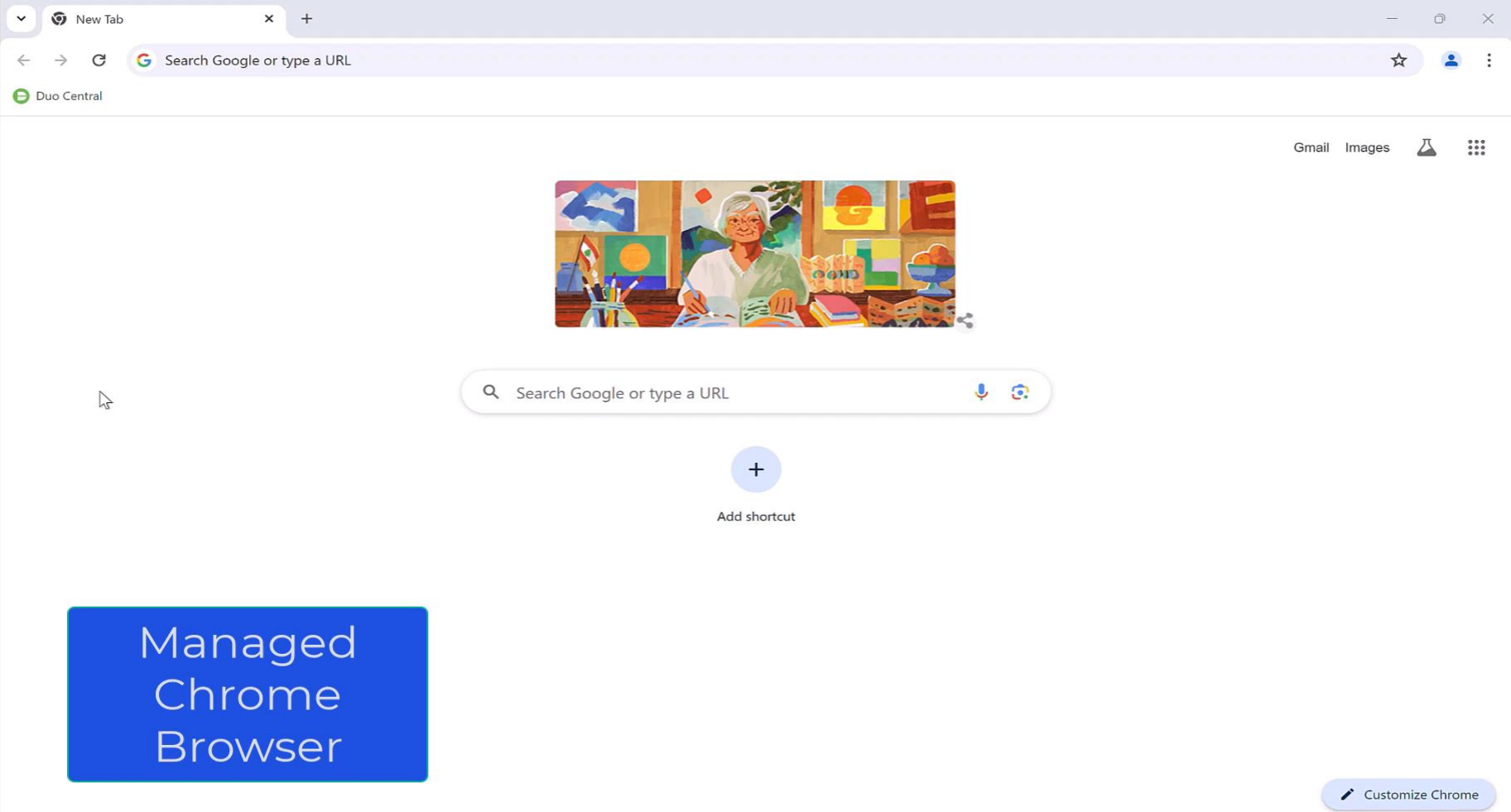
Email

☐ Remember me

[Regular sign in](#)

LOG IN

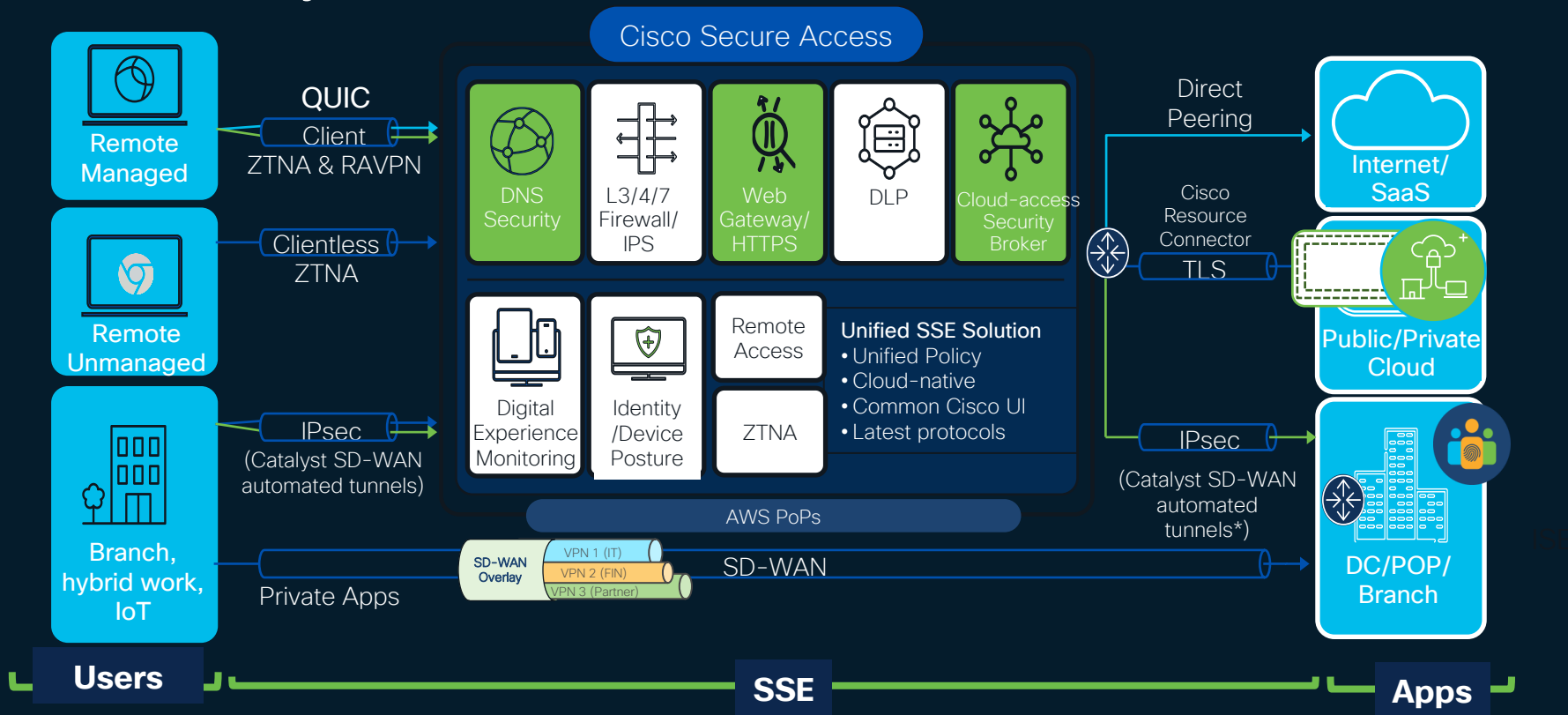
[Sign Up for a Free Trial](#)



Managed
Chrome
Browser

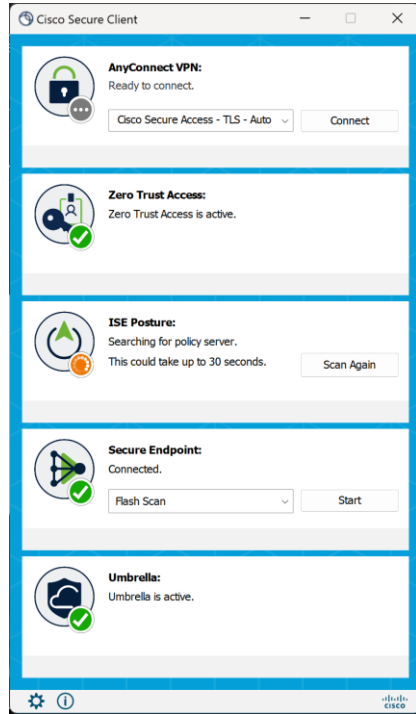
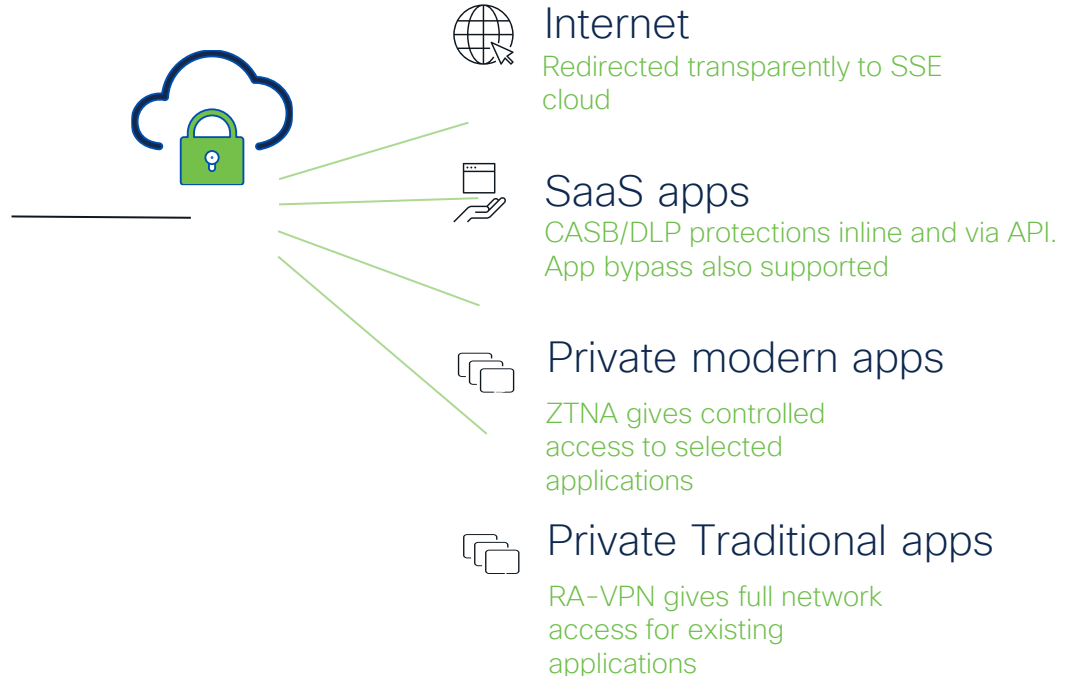
Secure Hybrid Worker

Secure hybrid worker

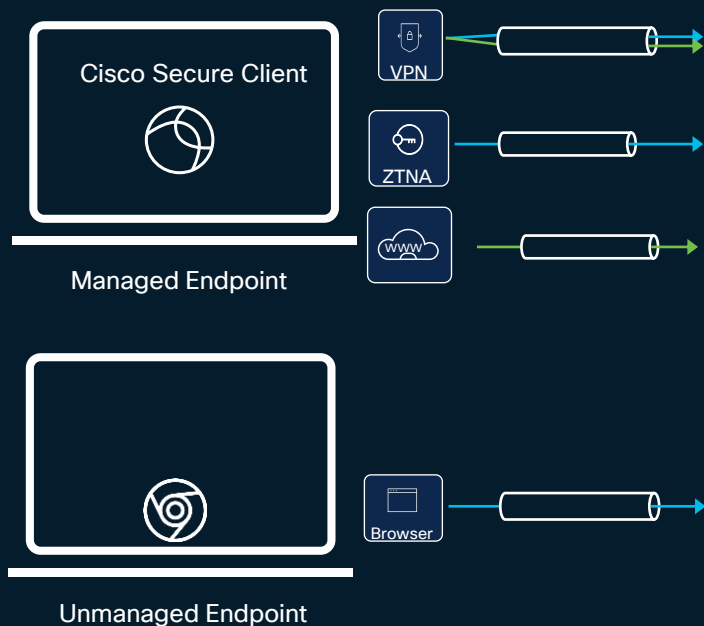


Unified ZTNA client

Transparently secures the connections needed



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

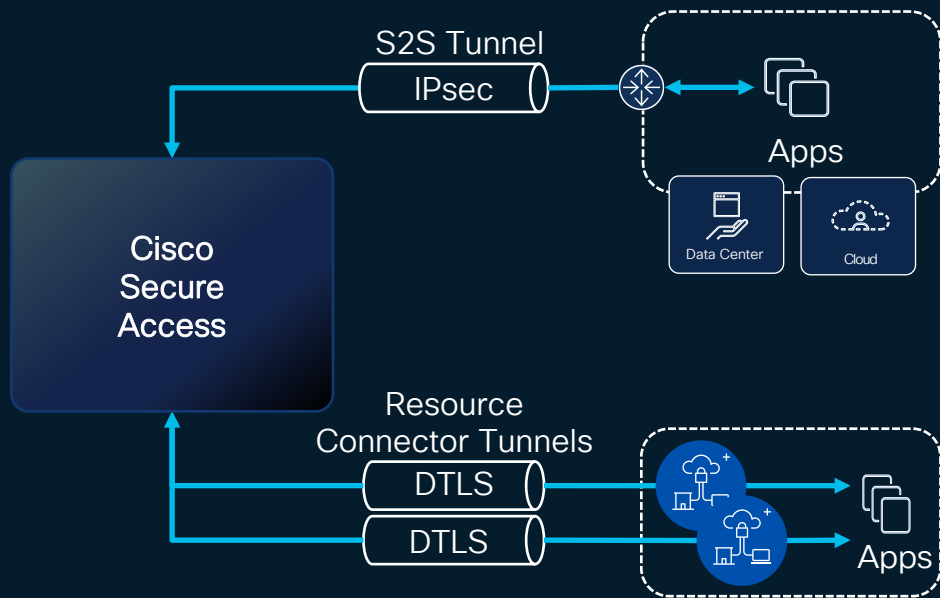
Web Roaming Module

- 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

Apps: private applications



Site-to-site tunnels with IPsec

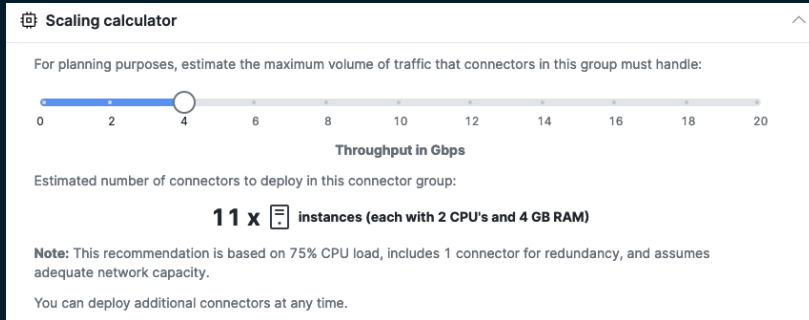
- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Fallback for resource connectors

Resource connectors

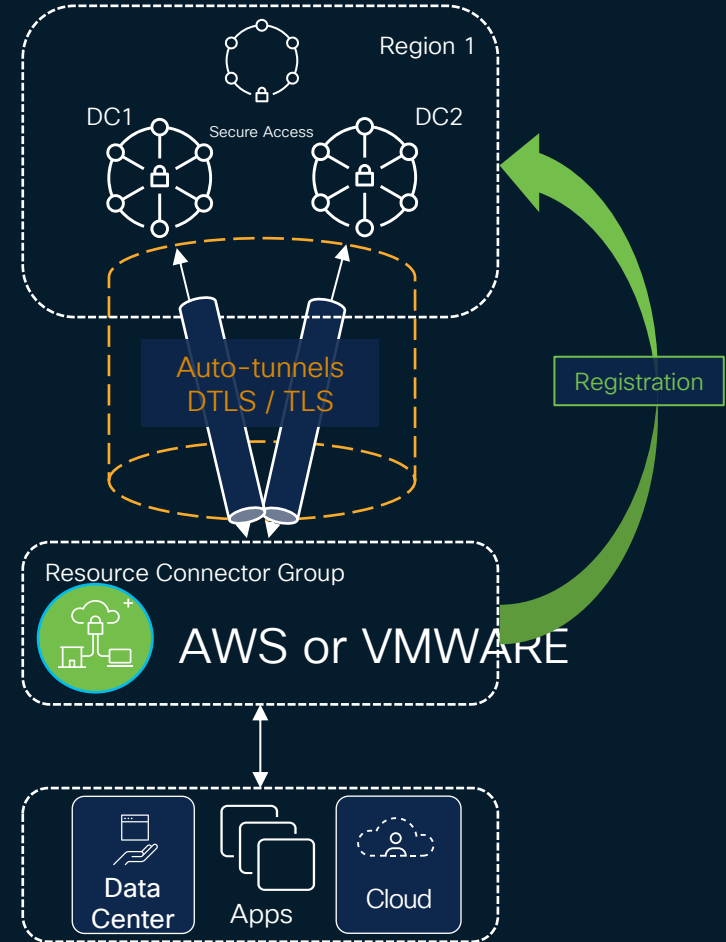
- Lightweight VM for AWS and ESXi
- All traffic egresses from Resource Connector IP
- Access applications with overlapping IPs
- Outbound connection / no firewall holes required
- No routing configuration required
- Auto failover / load balancing

Resource connector

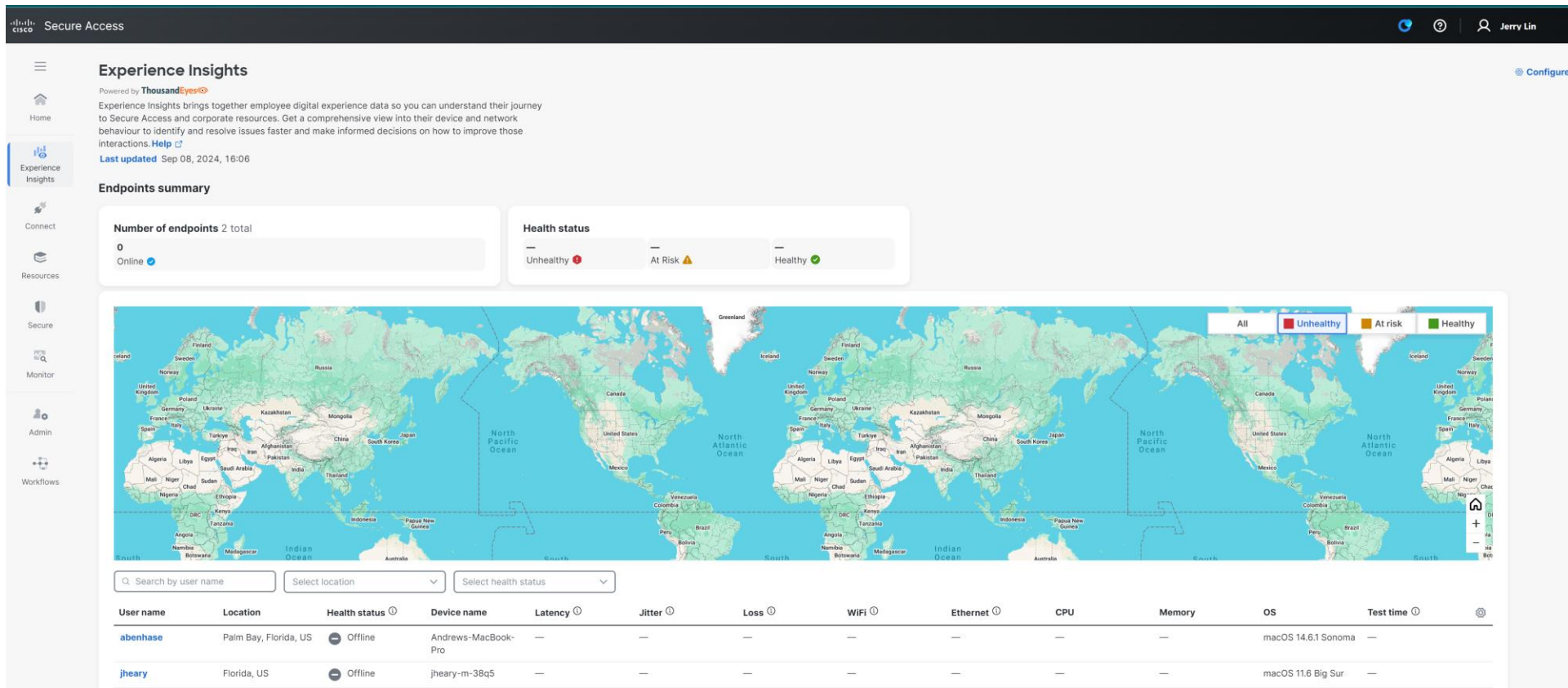
- Scaling and Redundancy
 - Dashboard provides calculator
 - Based on 70% CPU and DTLS
 - 500 Mb/s at full capacity
 - 400 Mb/s at 70% load



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



Digital Experience Monitoring



ZTNA Demo Secure Access



Cisco Zero Trust Network Access Demo



Cisco Secure Client - AnyConnect VPN Agent

[Start the service](#)

Description:

Cisco Secure Client AnyConnect VPN Agent for Windows

Name	Description	Status	Startup Type	Log On As
AVCTP service	This is Audio...	Running	Manual (Trigg...	Local Serv
Background Intelligent Transfer Service	Transfers file...	Running	Manual	Local Syst
Background Tasks Infrastructure Service	Windows inf...	Running	Automatic	Local Syst
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Serv
BitLocker Drive Encryption Service	BDESVC hos...	Running	Manual (Trigg...	Local Syst
Block Level Backup Engine Service	The WBENGL...	Running	Manual	Local Syst
Bluetooth Audio Gateway Service	Service supp...	Running	Manual (Trigg...	Local Serv
Bluetooth Support Service	The Blueto...	Running	Manual (Trigg...	Local Serv
Bluetooth User Support Service_1595f3	The Blueto...	Running	Manual (Trigg...	Local Syst
BranchCache	This service ...	Running	Manual	Network S
BrYNSvc		Running	Manual	Local Syst
Capability Access Manager Service	Provides faci...	Running	Manual (Trigg...	Local Syst
CaptureService_1595f3	Enables opti...	Running	Manual	Local Syst
Cellular Time	This service ...	Running	Manual (Trigg...	Local Serv
Certificate Propagation	Copies user ...	Running	Manual (Trigg...	Local Syst
Cisco AMP Orbital	Cisco AMP O...	Running	Automatic	Local Syst
Cisco Secure Client - AnyConnect VPN Agent	Cisco Secure...	Running	Automatic	Local Syst
Cisco Secure Client - Cloud Management	Cisco Cloud ...	Running	Automatic	Local Syst
Cisco Secure Client - ISE Posture Agent	Cisco Secure...	Running	Manual	Local Syst
Cisco Secure Client - Network Visibility Agent	Cisco Secure...	Running	Manual	Local Syst
Cisco Secure Client - Umbrella Agent	Cisco Secure...	Running	Manual	Local Syst
Cisco Secure Client - Umbrella SWG Agent	Cisco Secure...	Running	Manual	Local Syst
Cisco Secure Client - Zero Trust Access Agent	Cisco Secure...	Running	Manual	Local Syst
Cisco Secure Endpoint 8.2.3	Cisco Secure...	Running	Automatic	Local Syst
Cisco Security Connector Monitoring 8.2.3	Cisco Securit...	Running	Automatic	Local Syst
Client License Service (ClipSVC)	Provides infr...	Running	Manual (Trigg...	Local Syst
Clipboard User Service_1595f3	This user ser...	Running	Automatic (De...	Local Syst
Cloud Backup and Restore Service_1595f3	Monitors th...	Running	Manual	Local Syst
CNG Key Isolation	The CNG ke...	Running	Manual (Trigg...	Local Syst

Extended / Standard

VPN:
Service was stopped.
Cisco Secure Client - TLS - Auto
Connect

Access:
Access error. Contact your IT administrator.
Details

Scan:
Scan failed. No system administrator.
Scan Again

Endpoint:
Endpoint is inactive.
Start

Secure Access and CLI Demo



Overview

Connect

Resources

Secure

Experience Insights

Monitor

Admin

Workflows

Overview

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

Connectivity

Last 24 Hours

Network tunnels

283 total

8 Active

36 Inactive

161 Unestablished

Identity Intelligence

Last 24 Hours

Untrusted Users

Line chart showing untrusted users over time (Jun 27 to Jun 31). The y-axis ranges from 200 to 1.2k.

User Trust Levels

Horizontal bar chart showing user trust levels: Untrusted, Questionable, Neutral, Favorable, and Trusted. The x-axis ranges from 0 to 2.4k.

Usage monitoring

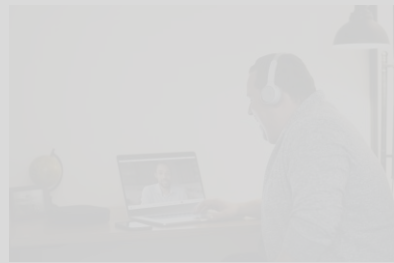
Last 24 Hours

Total usage

Usage data - delayed up to 30 min.

Secure Access Dashboard

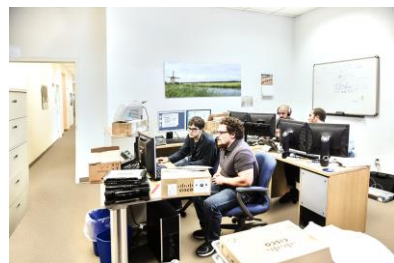
Zero trust use cases



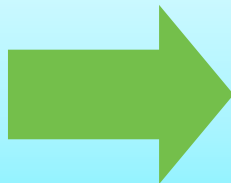
Remote
User



- 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

On-Premises Access

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

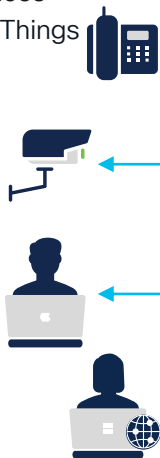
ISE provides zero trust for on-premises

Enterprise

Security

Endpoints

- Users
- Devices
- IOT Things



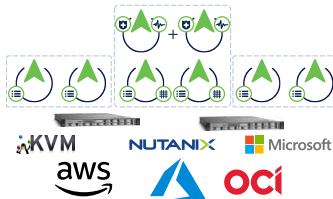
Network Devices

- Switches
- WLCs / APs
- VPN



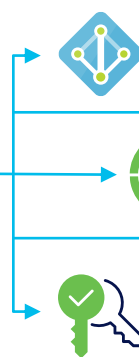
Cisco ISE

- 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

CISCO *Live!*

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)

			Results		
+	Status	Rule Name	Conditions	Profiles	Security Groups
+	✓	Employee BYOD	Context	PermitAccess	Employees

Context

BYOD_is_Registered

EAP-TLS

CERTIFICATE-Subject Alternative Name EQUALS Radius-Calling-Station-ID

ise-cream-ExternalGroups EQUALS ise-cream.inc/Users/Domain Users

Security Group

Employees

Search
Security Groups
Auditors
BYOD
Contractors
Developers

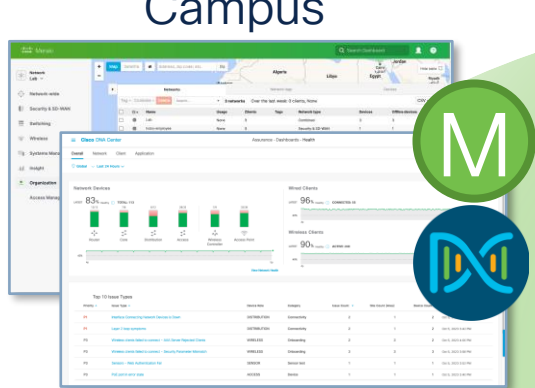
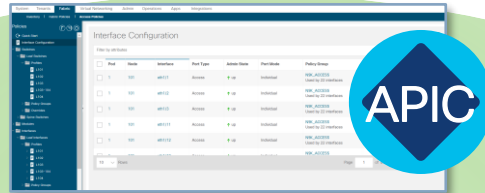
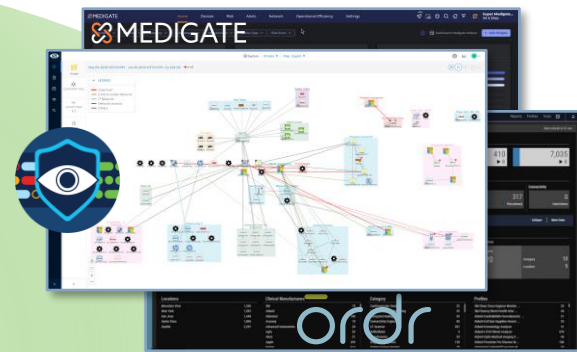
cisco Live!

ISE is the core of Cisco's common policy

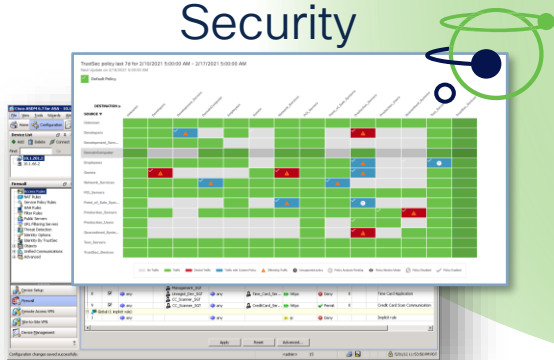
Data Center

Campus

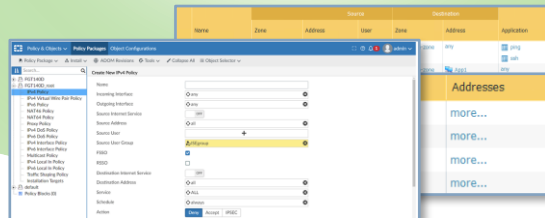
IoT



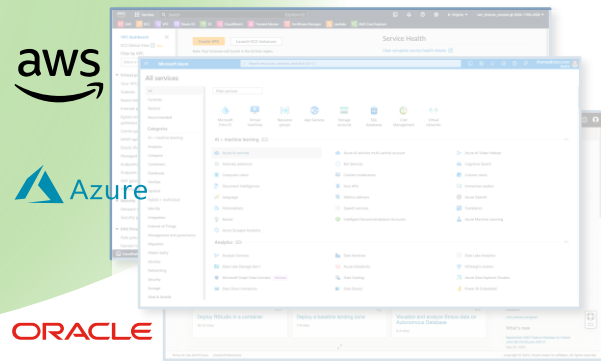
Security



Competitors



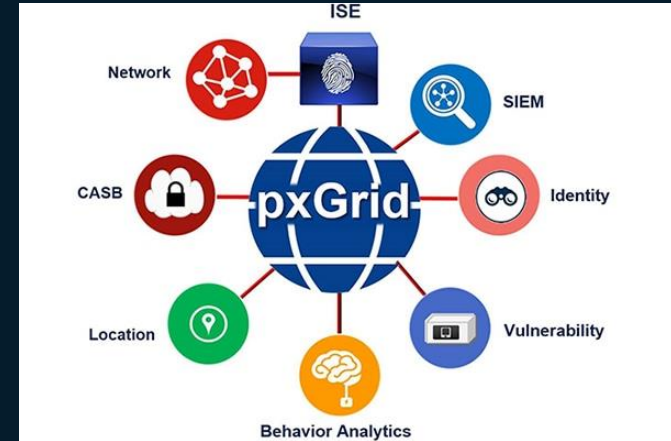
Cloud Providers



cisco Live!

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...

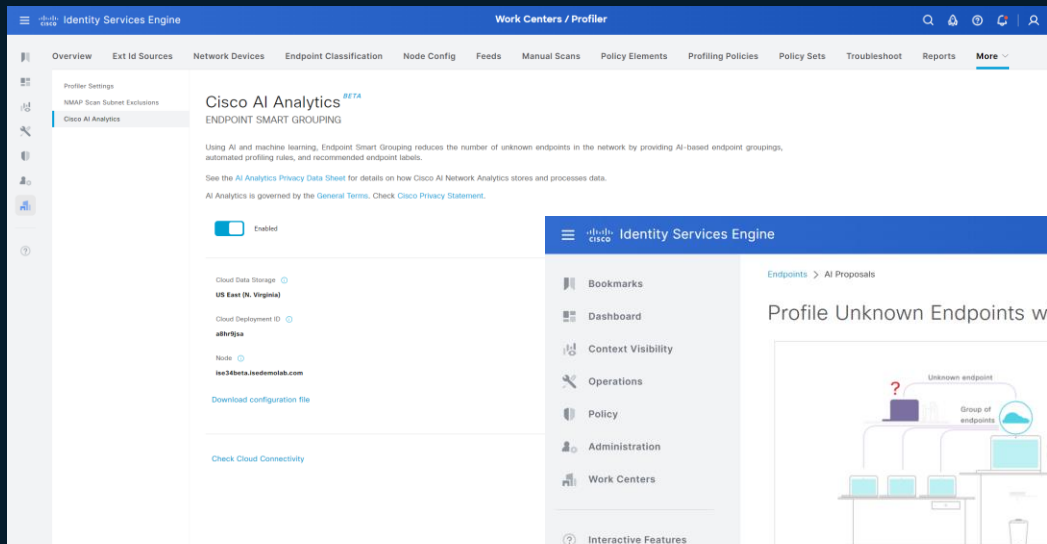
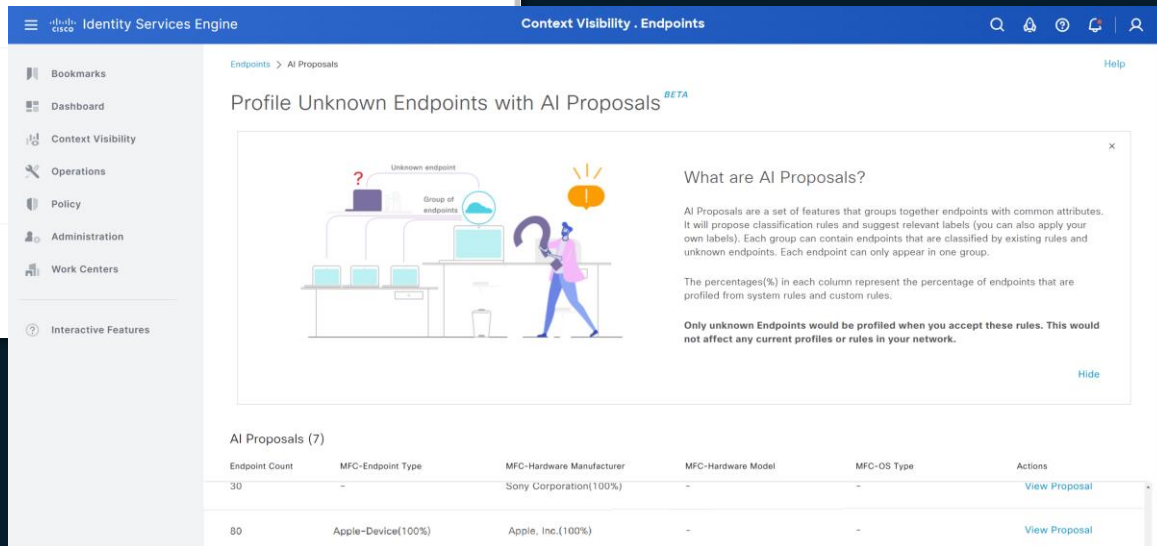


Cisco Rapid Threat Containment

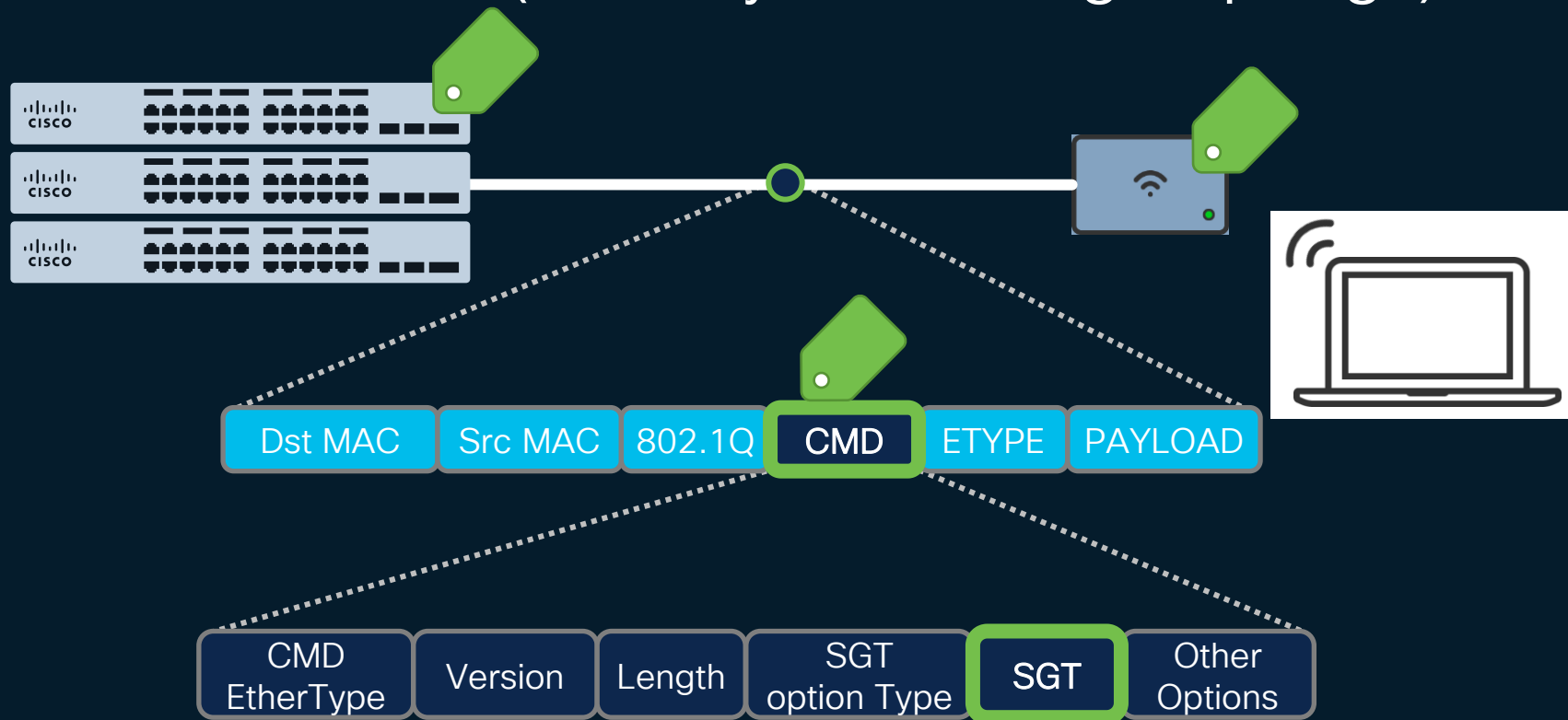
ISE 3.3 (AI profiling)

AI Analytics simplifies the profiling process

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



What are SGTs (security/scalable group tags)?



Scalable group tag (SGT)

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

Destination	1120asaVPNUser 18/0012	Auditors 9/0009	BYOD 15/000F	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Employees 4/0004
Source							
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

ISE Policy Matrix (SGACL)

Centralized policy for switches, routers, WLCs and APs

Production Matrix

Populated cells: 62

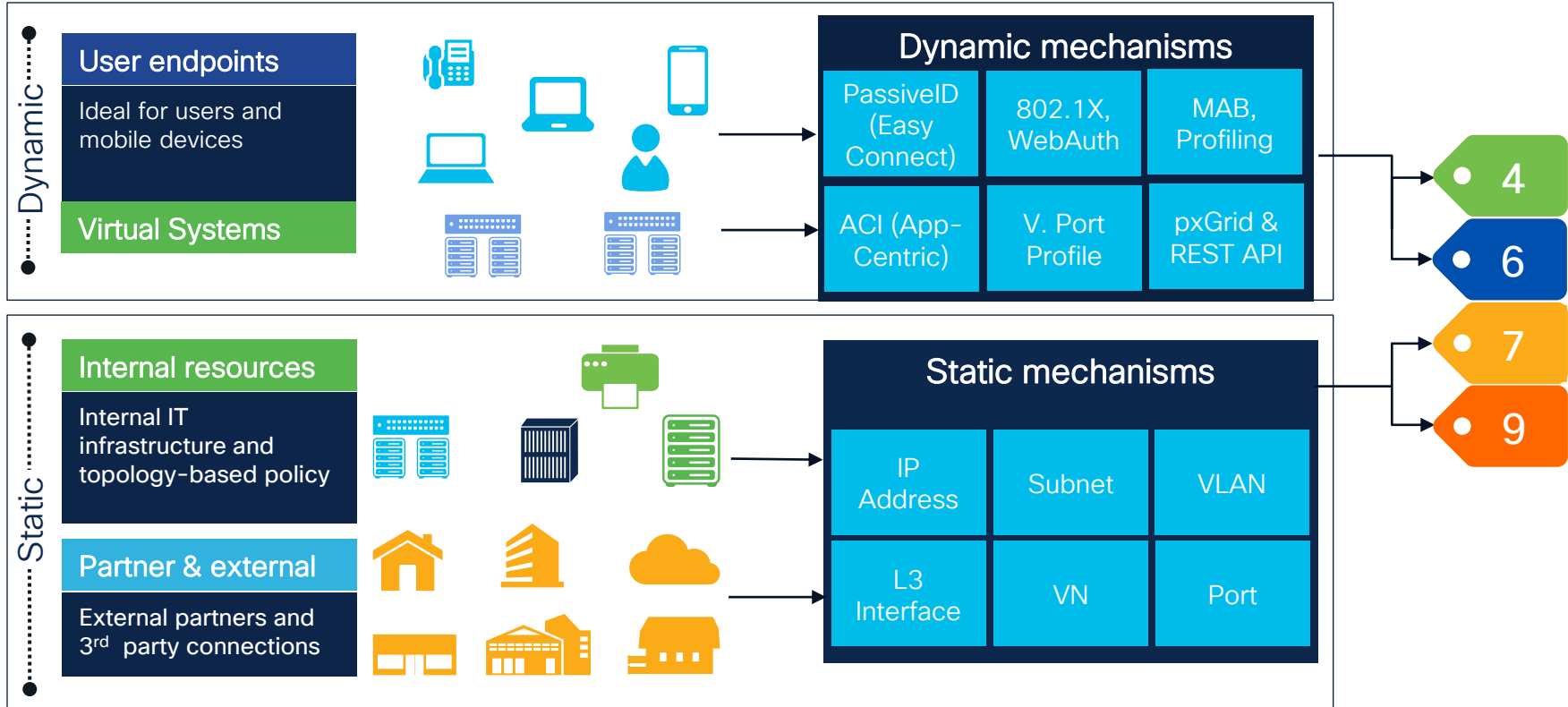
Tools: Edit, Add, Clear, Deploy, Monitor All - Off, Import, Export, View, Show All

Source	Billing_Systems 29/001D	Bldg_Mgmt_Sys 30/001E	CUCM_Servers 26/001A	Contractors 5/0005	Corp_Portal 8/0008	Dev_Sys 12/000C	Developers 15/000F	Doctors 9/0009	Edu_Adm 19/0013	Employees 4/0004	Net_Svcs 10/000A	PCL_Servers 7/0007	POS_Systems 23/0017	Prod_Sys 11/000B	Quarantined 255/00FF	Remediation_Svr 32/0020	Test_Servers 13/0000	Unknown ?
Auditors 3/0003	Anti_Malwar	Deny IP			Web_SGACL					Deny IP		Web_SGACL						
Developers 15/000F					Permit IP						Deny IP							
Employees 4/0004		Deny IP	Jabber_Sig_	Intra_Ja						Jabber	Permit IP	Deny IP		Permit IP	Deny IP		Deny IP	
IoT_Devices 6/0006		Permit IP								IP		Deny IP						
POS_Systems 23/0017	Deny IP	Deny IP	Deny IP	Deny IP						IP	Deny IP	Permit IP	Deny IP	Deny IP	Deny IP		Deny IP	
Quarantined 255/00FF	Deny IP	Deny IP	Deny IP	Deny IP						IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Permit IP	Deny IP	Deny IP

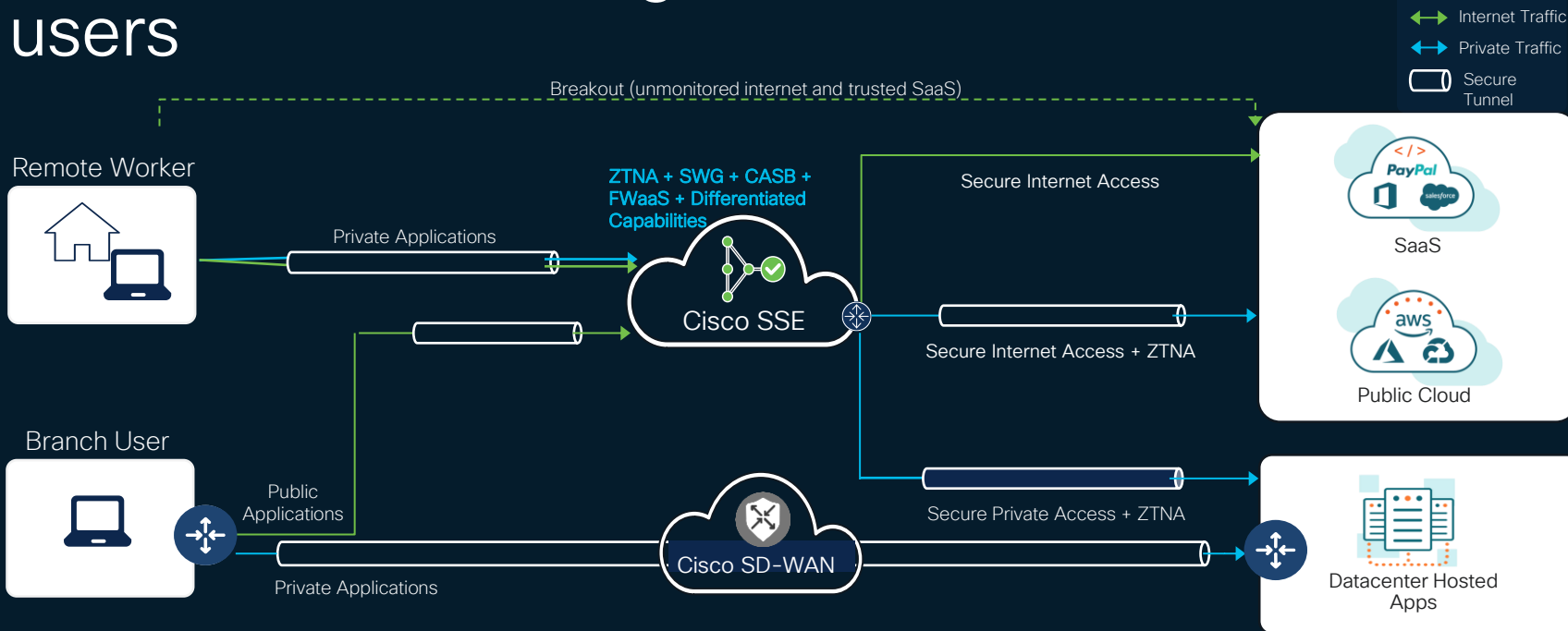
```
permit tcp dst eq 6970 log
permit tcp dst eq 6972 log
permit tcp dst eq 3804 log
permit tcp dst eq 8443 log
permit tcp dst eq 8191 log
permit tcp dst eq 5222 log
permit tcp dst eq 37200 log
permit tcp dst eq 443 log
permit tcp dst eq 2748 log
permit tcp dst eq 5060 log
permit tcp dst eq 5061 log
permit tcp dst range 30000 39999 log
permit udp dst range 5070 6070 log
deny ip log
```

Default ☒ Enabled SGACLs : Permit IP

Classification Methods



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 without having to hairpin

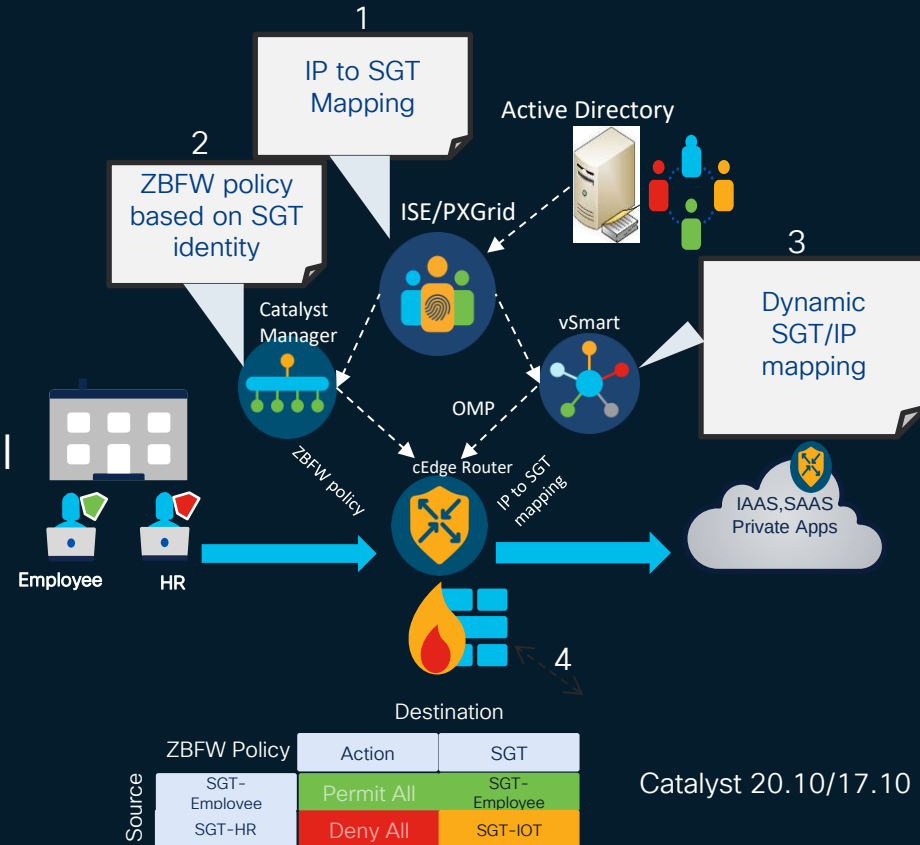
Connect remote workers securely to Internet / cloud / private applications

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



SGT Demo



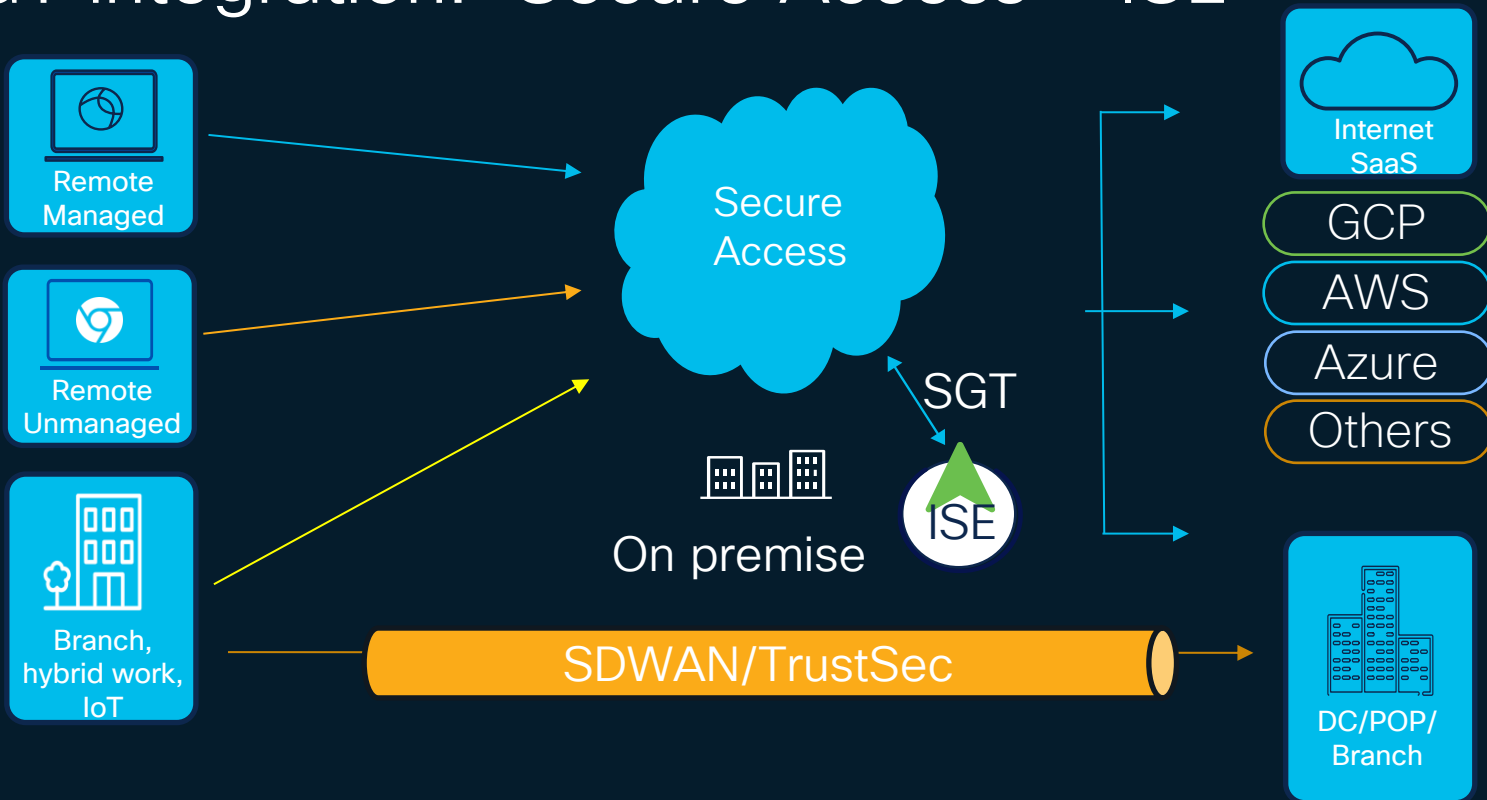
Zero Trust Demo Campus Segmentation

Identity Services Engine + Catalyst Switch demo

August 2024

Demo Lab provided by Keith Simmons, GES TSA

SGT integration: Secure Access + ISE

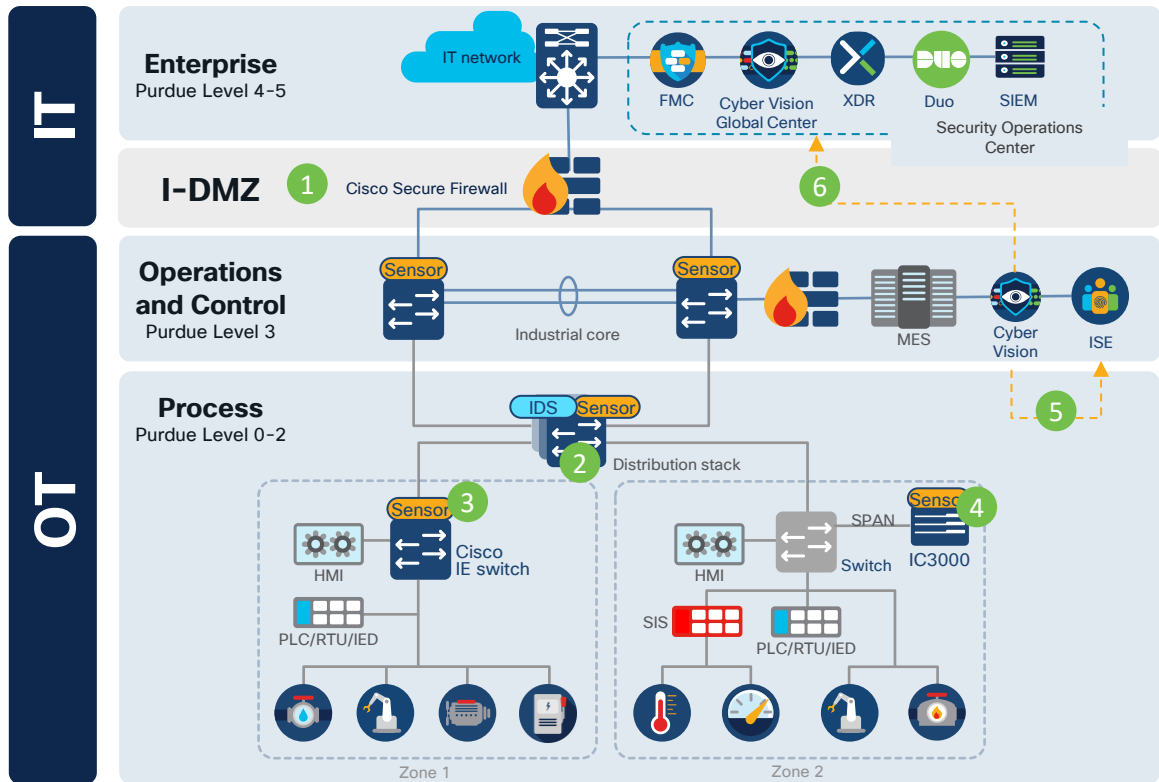


On-premises Access

- OT to Private Apps



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

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
- ✓ Short Threat Detection
- ✓ Talos Threat Intelligence
- ✓ On-prem & Cloud offers

CISCO *Live!*

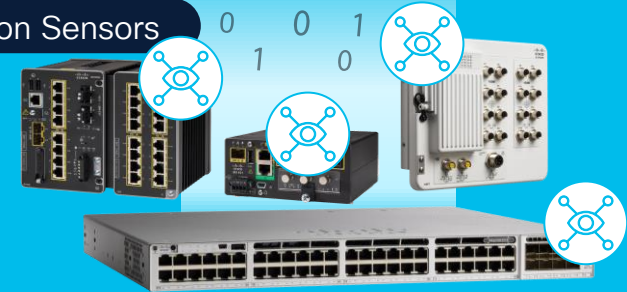
Cyber Vision Center



Metadata

1 0 0 1
0 0 1

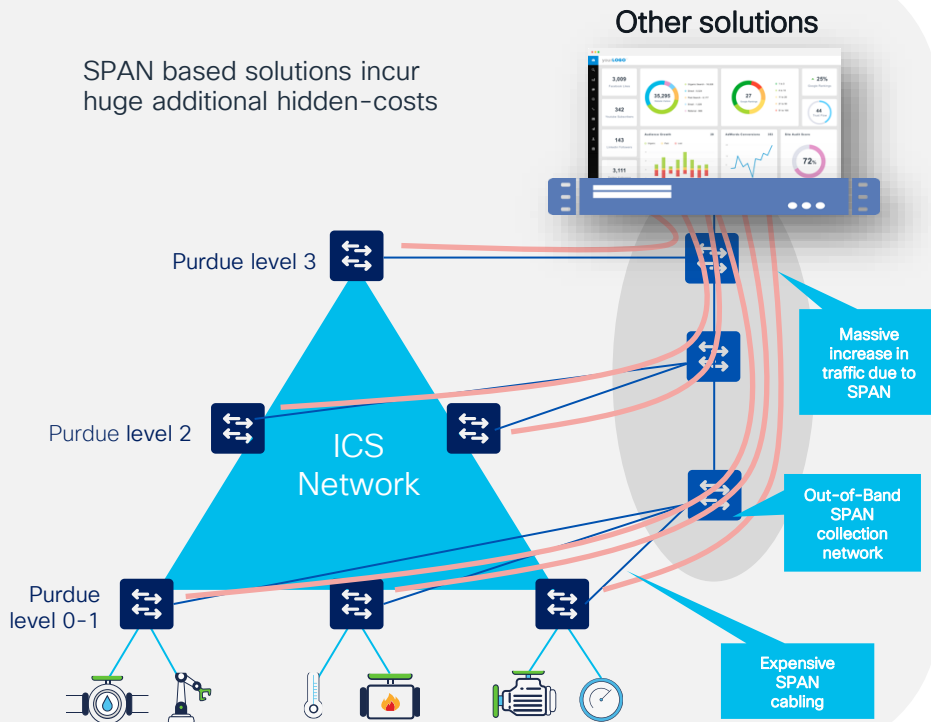
Cyber Vision Sensors



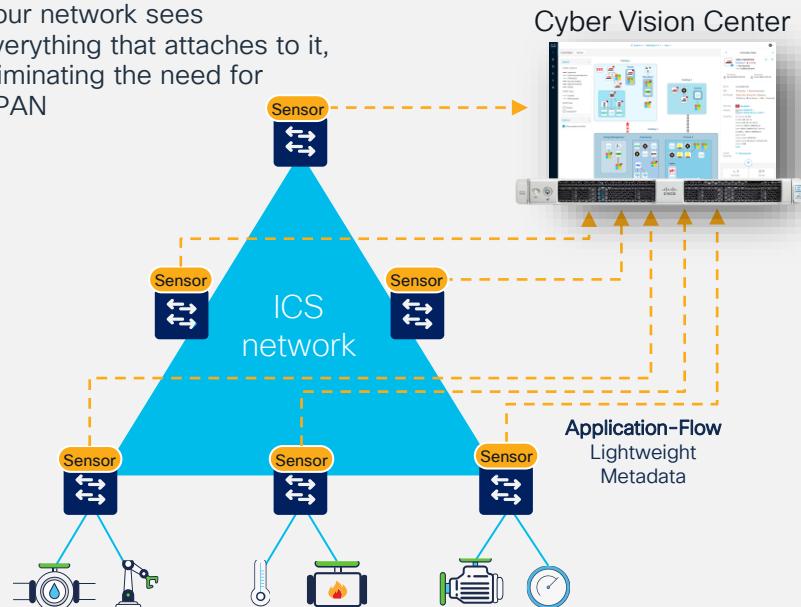
Deep Packet Inspection & Active Discovery
built into your network infrastructure

Old vs new scalable architecture

SPAN based solutions incur huge additional hidden-costs



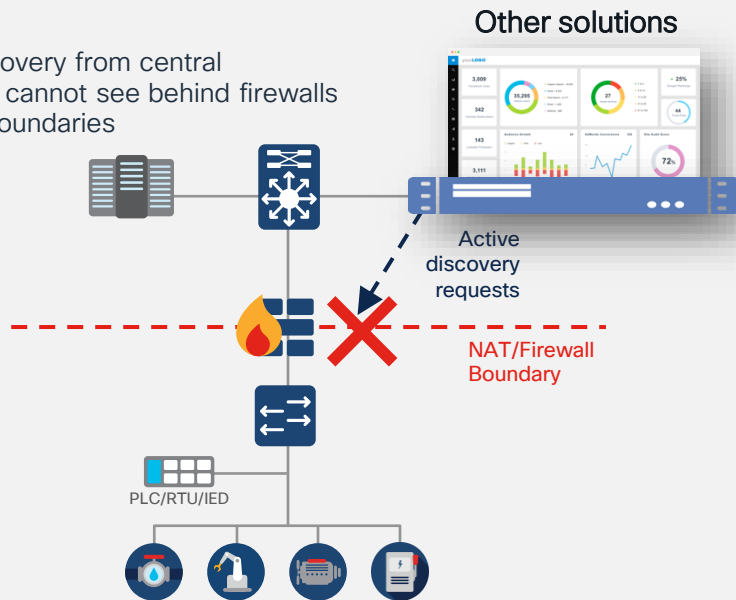
Your network sees everything that attaches to it, eliminating the need for SPAN



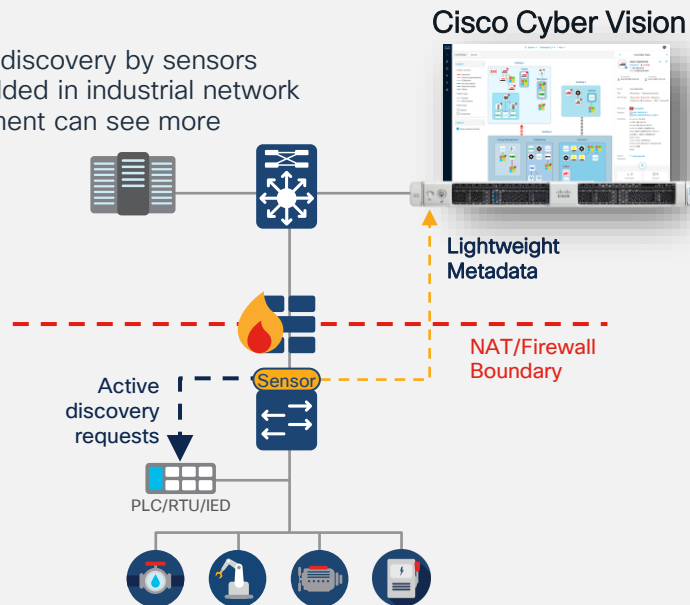
Why is a network-sensor important?

Distributed edge active discovery gives you 100% visibility

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



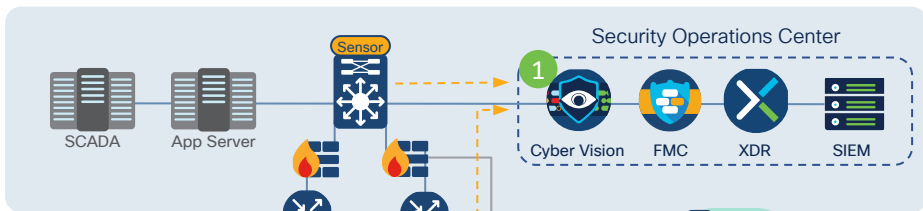
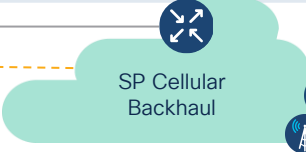
Active discovery by sensors embedded in industrial network equipment can see more



Sensors embedded in the network can see more

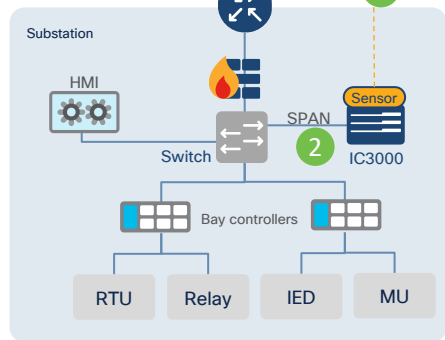
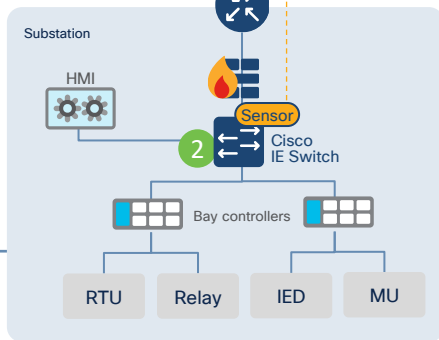
Cisco Cyber Vision in electric utilities

Data Center / Control Center

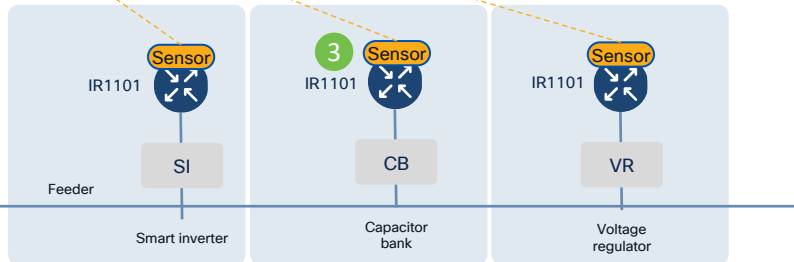


- 1 Cyber Vision Center deployed at control center
- 2 Cyber Vision Sensor embedded in IE3400 switches or deployed via one-hop SPAN on IC3000 in transmission substations
- 3 Cyber Vision Sensor embedded in IR1101 gateways in the distribution grid
- 4 Application-flow streamed from sensors to center over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

Transmission Grid

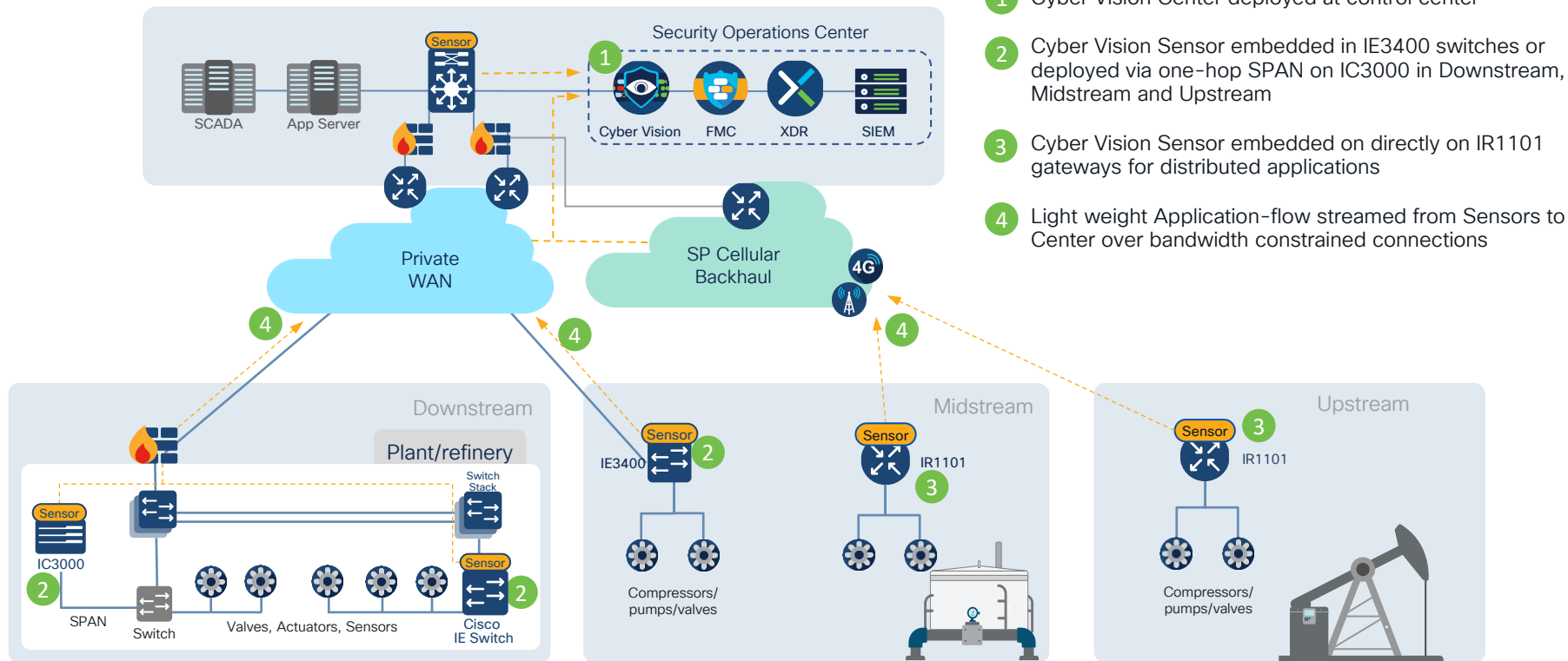


Distribution Grid



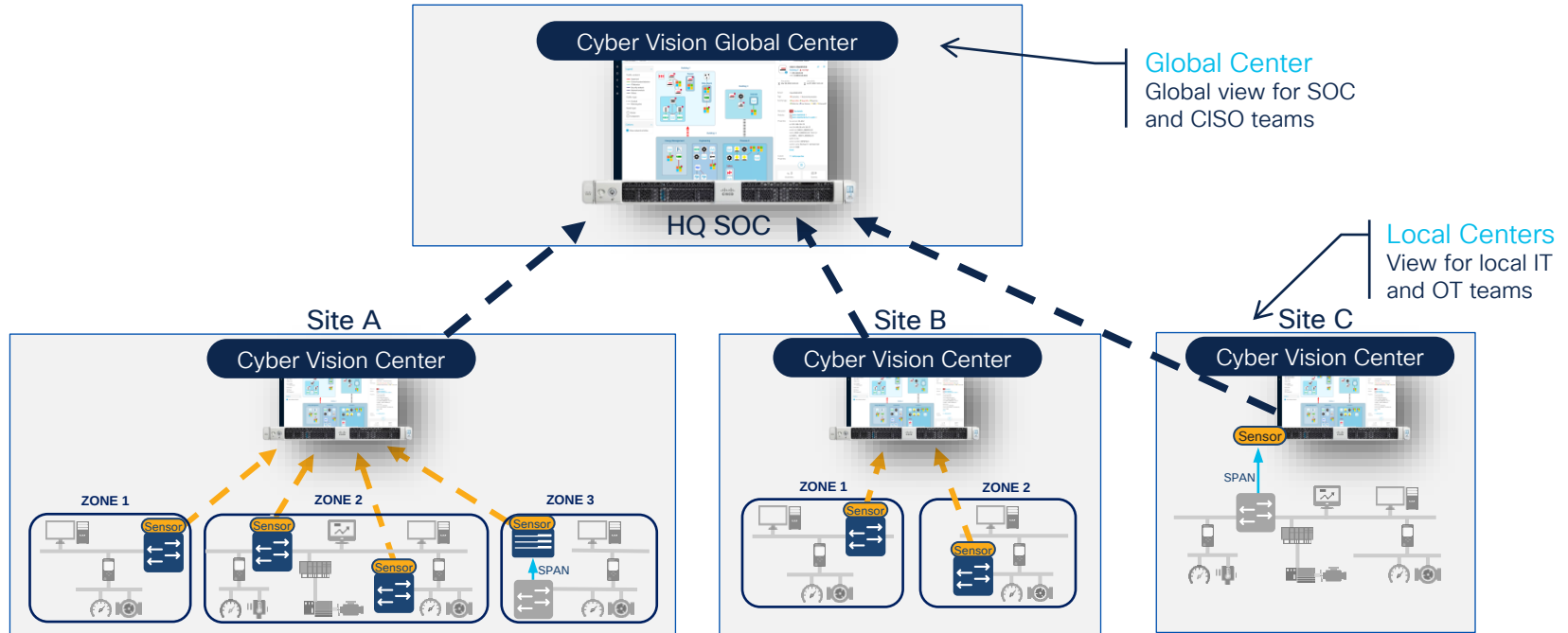
Cisco Cyber Vision in oil and gas

Data Center / Control Center

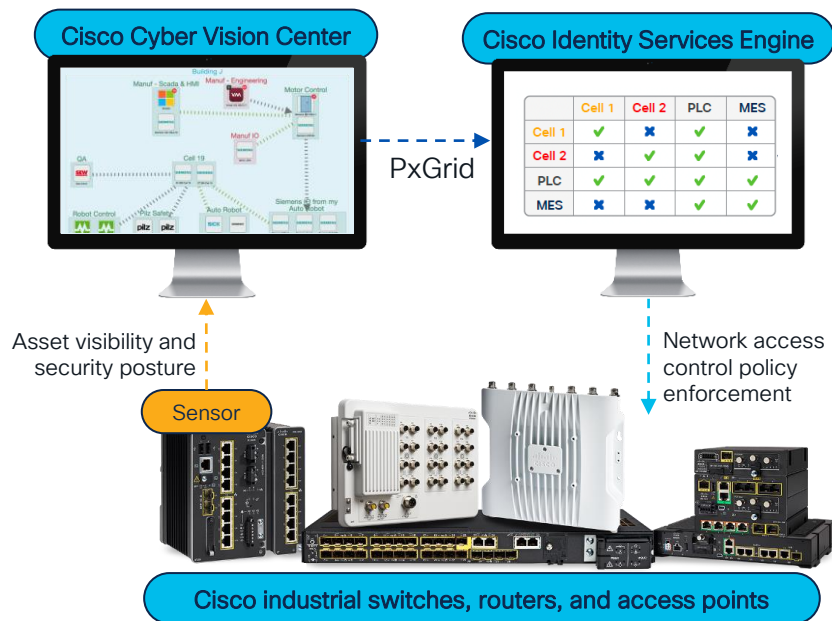


Cisco Cyber Vision Global Center

Global visibility on all sites from a central console



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

Integration with Cisco Identity Services Engine (ISE)

E4:90:69:9E:EF:7D

MAC Address: E4:90:69:9E:EF:7D
Username: E4:90:69:9E:EF:7D
Endpoint Profile: Austin_Plant_Profiler
Current IP Address: 192.168.119.39
Location: Location → All Locations

Applications | **Attributes** | Authentication | Threats | Vulnerabilities

General Attributes

Description

Static Assignment: false
Endpoint Policy: Austin_Plant_Profiler
Static Group Assignment: false
Identity Group Assignment: Austin_Plant_Profiler

Custom Attributes

Attribute Name	Attribute Value
assetGroup	Root > Austin_Plant
assetDeviceType	Controller
assetId	101
assetIpAddress	192.168.119.39
assetMacAddress	e4:90:69:9e:ef:7d
assetName	192.168.119.39
assetProductId	1769-L36RMA-LOGIXS336ERM
assetProtocol	CIP
assetSerialNumber	0x604052C7
assetSwRevision	28.011
assetVendor	Rockwell Automation/Allen-Bradley
ip	192.168.119.39

Devices in ISE get attributes from Cyber Vision

Production Matrix

Populated cells: 36

Destination	Plant 10/0/0	Cell 17/0/01	Cell 17/0/02	Cell 17/0/03
Plant 10/0/0	Deny IP	Deny IP	Deny IP	Deny IP
Cell 17/0/01	Deny IP	Deny IP	Deny IP	Deny IP
Cell 17/0/02	Deny IP	Deny IP	Deny IP	Deny IP
Cell 17/0/03	Deny IP	Deny IP	Deny IP	Deny IP

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

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

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

cisco Live!

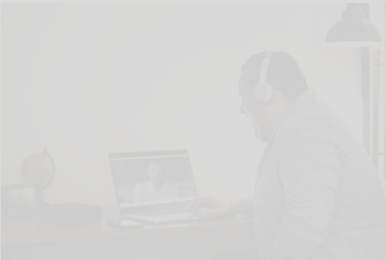


Helping industries with generic and specific designs,
as well as addressing regulatory requirements.

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

Zero trust use cases



Remote
User



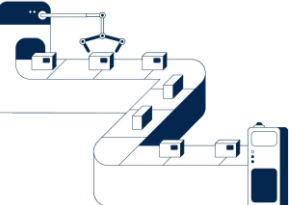
- ZT access to public SaaS
- ZTNA to private apps
- Client-based VPN private app access
- Secure Connect (VPNaaS)
- *Unified ZTNA client (roadmap)



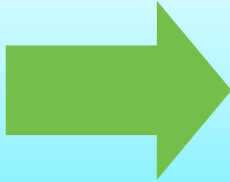
On-
Premises
User &
IOT



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



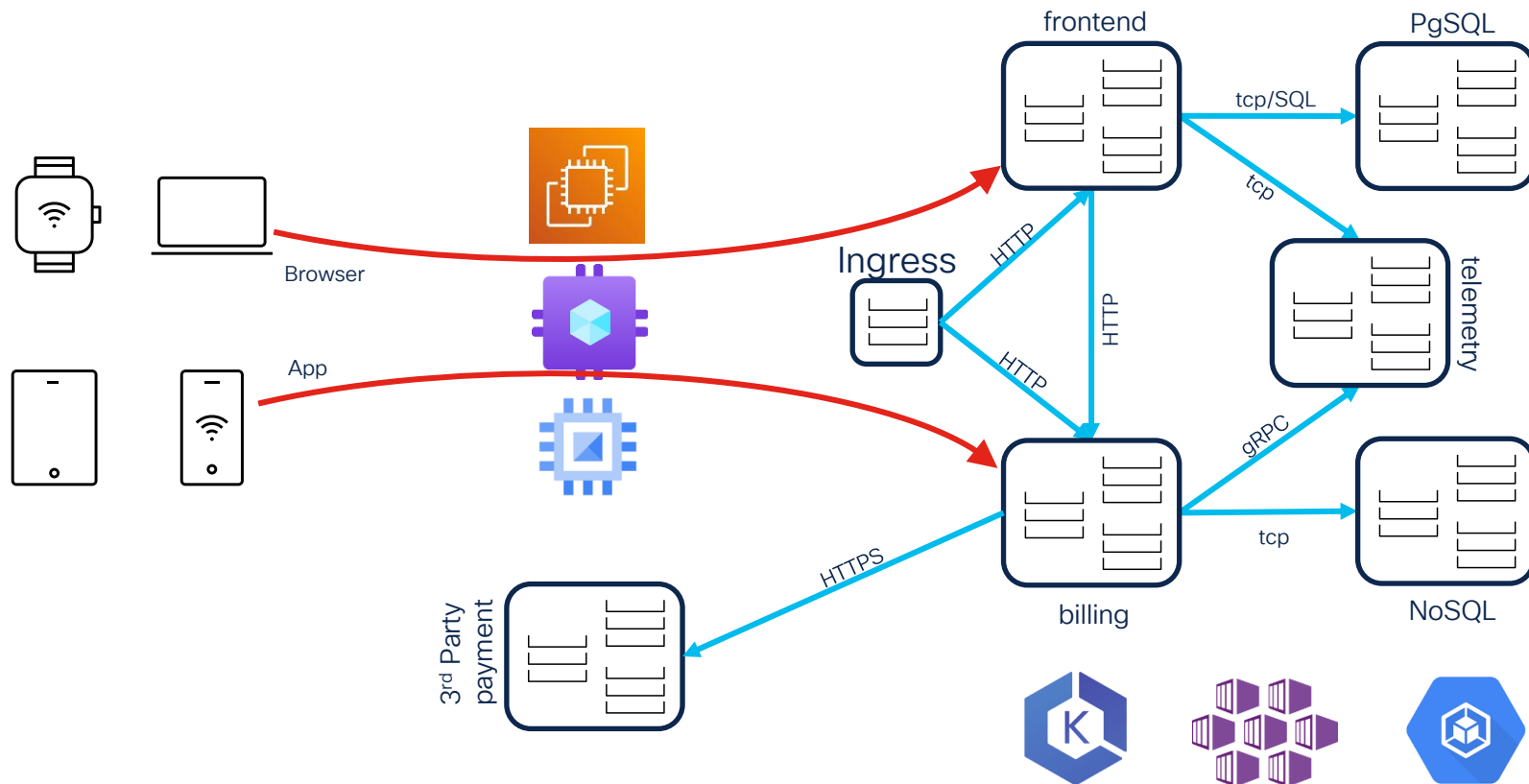
App-to-App



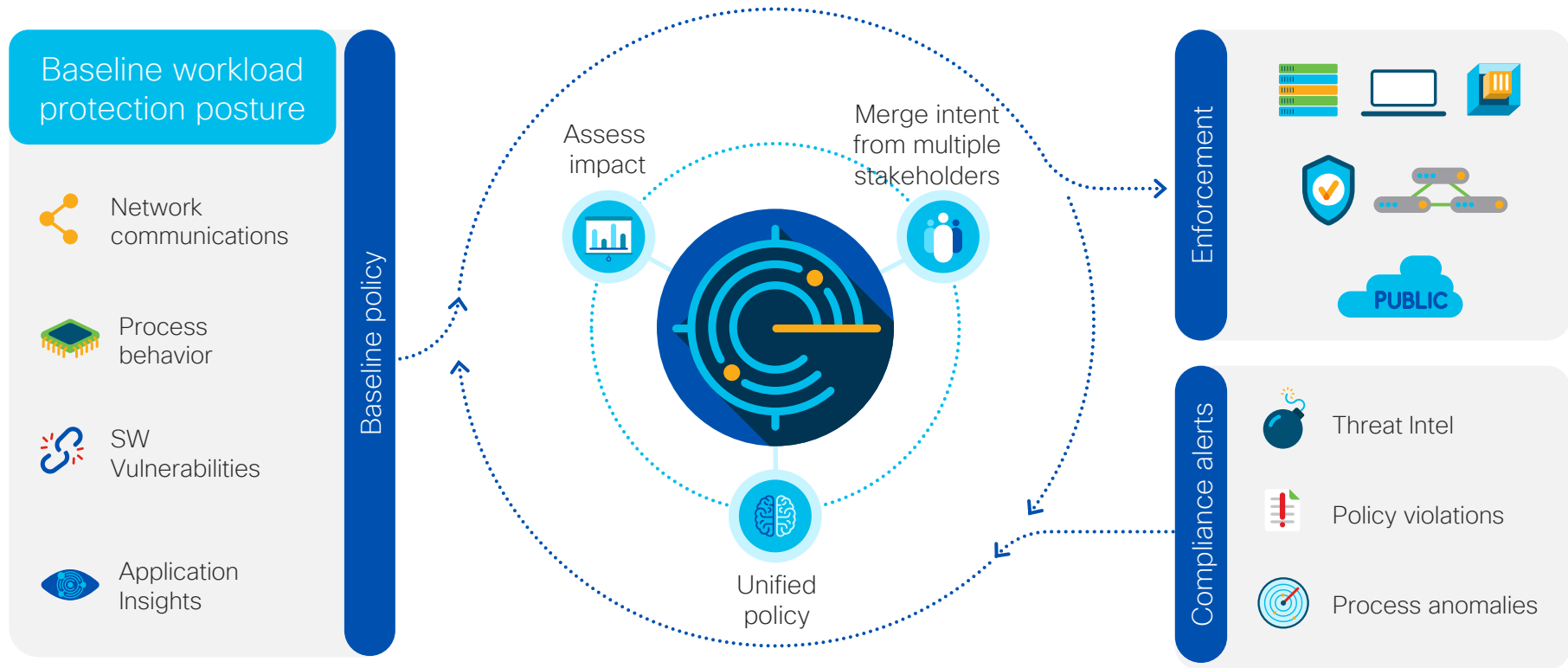
- App-to-App across multi-cloud

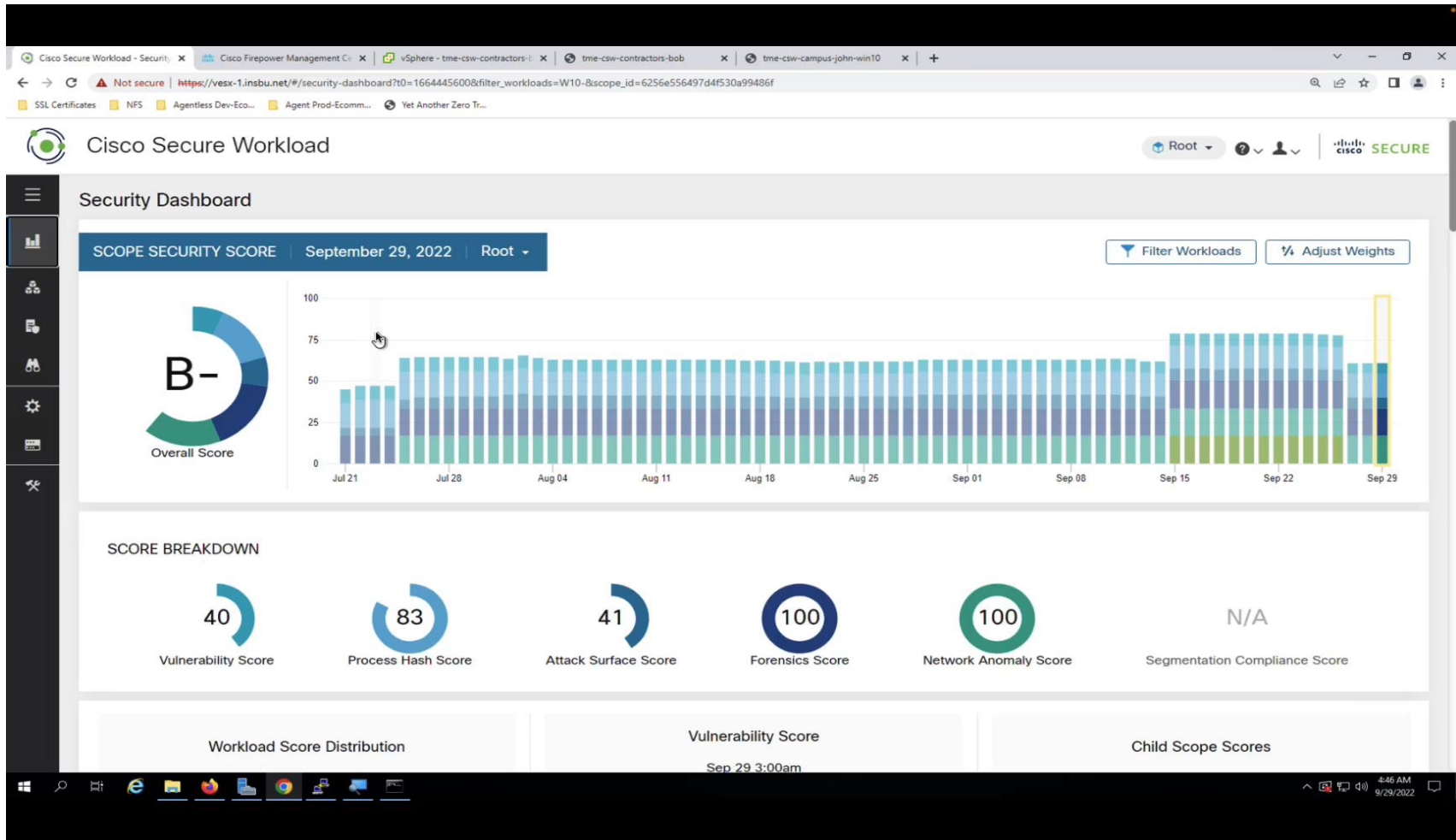
Securing Private Application Across Multi-cloud

Application architectures have evolved



Achieving ZT framework with Cisco Secure Workload





Cisco Secure Workload - Scopes
Cisco Firepower Management C...
vSphere - tme-csw-contractors-...
tme-csw-contractors-bob
tme-csw-campus-john-win10

Not secure
https://vesx-1.insbu.net/#/app_scopes?id=626f89be755f02063806b41b&chips=W10-
SSL Certificates
NFS
Agentless Dev-Eco...
Agent Prod-Ecomm...
Yet Another Zero Tr...

Cisco Secure Workload

Root
?
User
Cisco SECURE

Scopes and Inventory

Scopes
No Draft Changes
Filter Scopes...
47 Scopes and 29 Inventory Filters

Cloud
4 / 30 Children
Inventory: 23

Datacenter
6 / 34 Children
Inventory: 258
Uncategorized: 6

Development
4 / 13 Children
Inventory: ...
Uncategorized: ...
Overlaps 1 S...

InvoiceApp-Dev
0 Children
Inven...

Sock Shop Calico CRIO D
0 Children

Wiki
2 / 2 Children
Inventory: ...
Uncategorize...

eCommerce-Dev
7 / 7 Children
Unc...

Back-End
Inventory: ...

Root : CSW-SBG-Internal Datacenter

Query
* Location = Datacenter or
* orchestrator_system/cluster_name = Sock Shop Calico CRIO or
* orchestrator_system/cluster_name = Sock Shop Panoptica Flannel or
* orchestrator_system/cluster_name = Sock Shop Weaver Containerd or
* orchestrator_system/orch_type = f5

Delete
Edit
Add

All Inventory 259
Uncategorized Inventory 7
Overlapping Scopes 0
Suggested Child Scopes
Usages

Enter attributes...
Search Inventory

Services 43
Pods 104
Workloads 64
IP Addresses 48

48 of 48 inventory

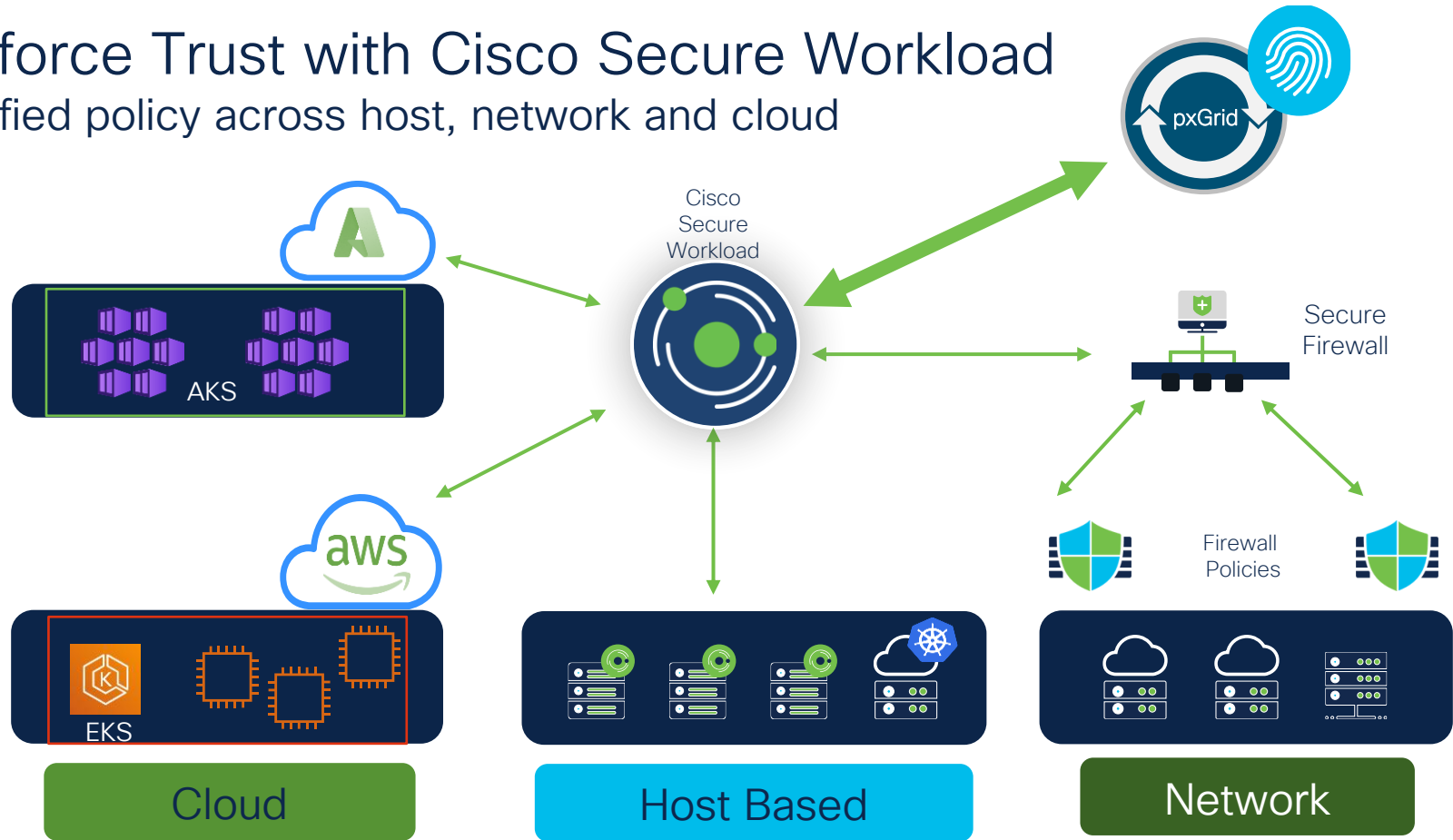
Address ↑	* Application ↑	* Cloud ↑	* Environment ↑	* Location ↑	* OCI-Region ↑	* Organization ↑
10.8.6.3	Retail		Production	Datacenter		SecureBusinessGroup
172.20.0.51	Insbu AD1		Shared Services	Datacenter		SecureBusinessGroup
172.20.0.52	Insbu AD2		Shared Services	Datacenter		SecureBusinessGroup
172.20.0.70				Datacenter		SecureBusinessGroup
172.20.0.71				Datacenter		SecureBusinessGroup
172.20.0.128				Datacenter		SecureBusinessGroup

cisco *Live!*

#CiscoLiveAPJC BRKSEC-2176 © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public 78

Enforce Trust with Cisco Secure Workload

Unified policy across host, network and cloud



- Overview
- Organize
- Defend
- Segmentation
- Enforcement Status
- Policy Templates
- Forensic Rules
- Investigate

Workspaces

DC-Access-PCI Compliance (NEW)
DC-Access-PCI Compliance - NEW

PRIMARY

Version 1

View Version History

Matching Inventories 42

Policies 6

Filters 0

Conversations

Provided Services

Policy Analysis

Enforcement Status

Enforcement

Filter Policies ...

Run Quick Analysis

Add Policy

Absolute and Default Policies 5

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	50	DENY	Kill_Switch	Finance Servers	Any
Default	90	DENY	CVE-2021-34480	PCI	Any
Default	90	DENY	Irvine : JerryLin-Lab	CVE 2022-30190	ICMP ...1 more
Default	92	ALLOW	JumpPC1-non-PCI	non-PCI server	ICMP

Filter

CVE 2022-30190

Filter Actions

Query

Package CVE = 2022-30190

Scope

Irvine:JerryLin-Lab

Restricted

No

Provides Service

No

View Filter Details

servers identified with CVE 2022-30190

Workloads 4

Address	Hostname	OS
10.3.3.111	Win2016-VM4	MSServer2016Standard
192.168.1.241	TomHomeLabDC	MSServer2019Standard
10.2.2.110	W2016-AuthProxy	MSServer2016Standard
10.3.3.110	Win2016-VM3	MSServer2016Standard

IP Addresses 0

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

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)



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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC