

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright, multi-colored sunburst graphic that radiates from the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

If you don't have a Security Reference Architecture, you must get one!

Jerry Lin, Principal Security Engineer
BRKSEC-1240

CISCO *Live!*

#CiscoLiveAPJC



“Reconciliation” – Dustin Koa Art



“Reconciliation” – Dustin Koa Art

About Jerry Lin

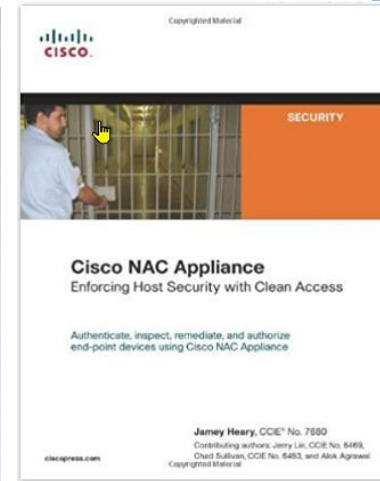
- 20+ years at Cisco; Security CCIE#6469
- Distinguished Speaker Hall of Fame at Cisco Live
- Coauthor; “NAC Appliance: Enforcing Host Security with CleanAccess”, Cisco Press
- Cisco Security Reference Architecture
- Favorite sport; marathons! Boston



CL Hall of Fame



Coauthor



www.cisco.com/go/sra

CISCO *Live!*

RSAC 2023

#CiscoLiveAPJC

BRKSEC-1240

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

6

Cisco Webex App

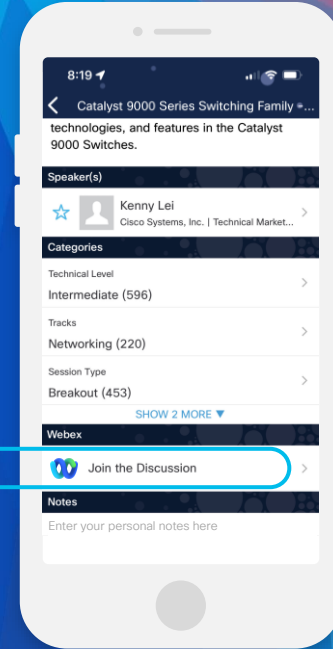
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1240>

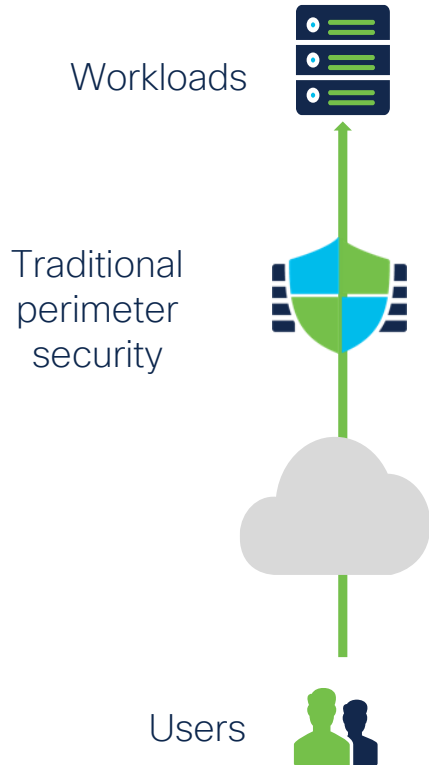
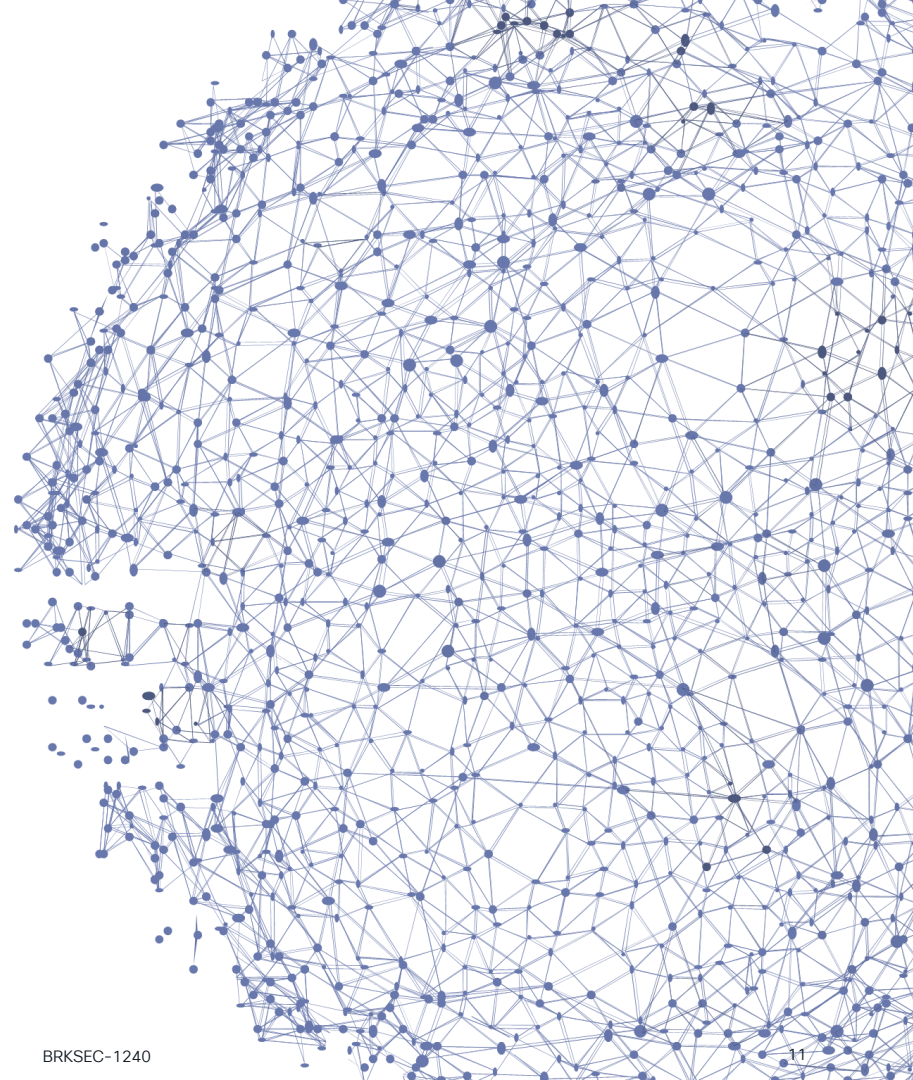
Agenda

- What is an architecture and why
- Cisco Security Reference Architecture compared
- Use cases and threat modeling
- Conclusion

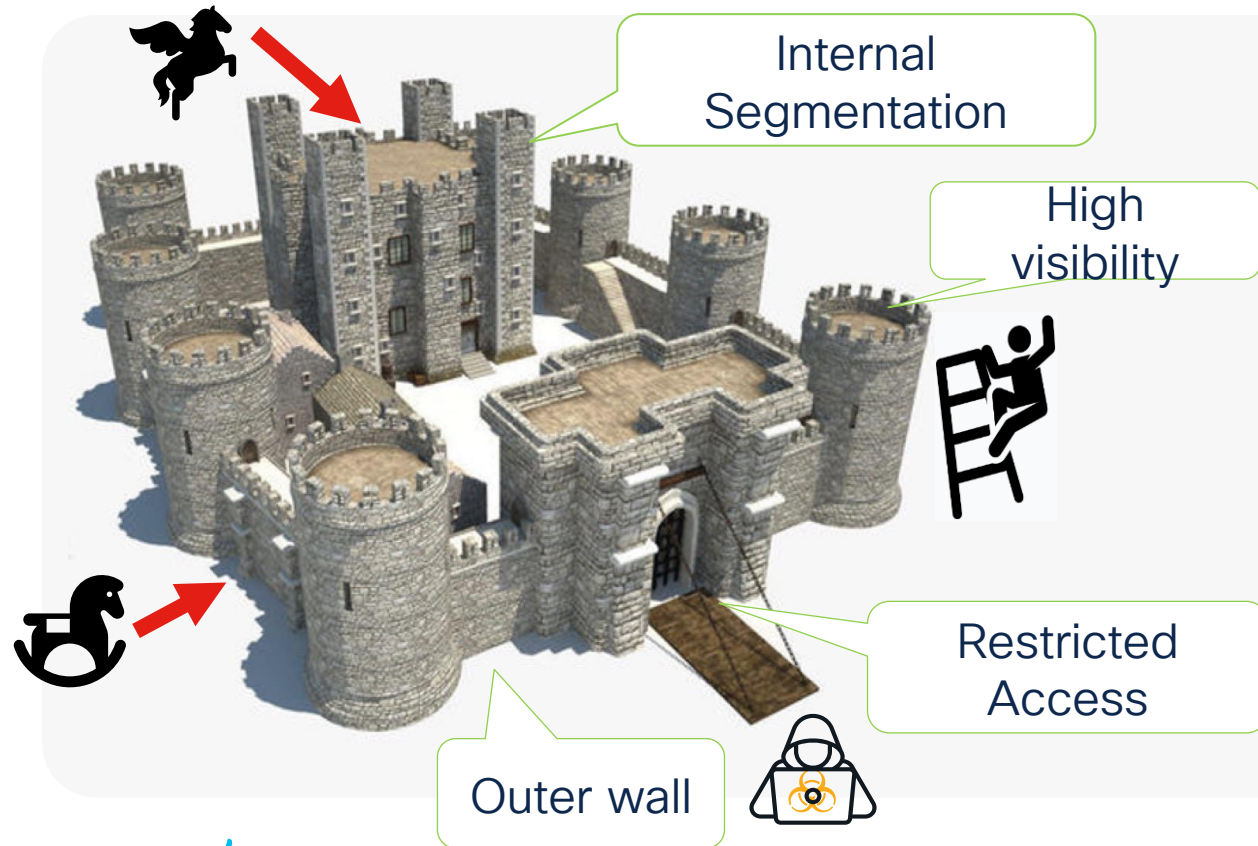
Objectives

- Understand the overall value and benefits of a security reference architecture
- Understand Cisco architecture alignment to industry frameworks
- SRA Use cases: Zero Trust, SASE, XDR, and others
- Threat Modeling of the SRA

Shift in IT Landscape



Defense in depth “Is this an architecture? Or a design?”



- Redundancy – Planning for failure with backups
- Segmentation – Reduce attack surface

The Industry architecture has you covered...

Infrastructure Security



Endpoint Security



Application Security



Messaging Security



Web Security



IOT Security



Security Ops & Incidence Response



Threat Intelligence



Mobile Security



Data Security



Transaction Security



Specialized Threat Analysis



Identity & Access Management



Cloud Security



Risk & Compliance



Requirements of a security architecture

Inputs from OpenAI and Cisco AI

Policy, Procedure, Standards

Identity Access Management

Physical Security

Network Security

Encryption

FW/IDS/VPN

Data Security

Endpoint Security

Security Incident Management

Security Awareness/Training

Disaster Recovery

Business Continuity Plan

Audits and Assessments

Scalability and Flexibility

Integration and Interoperability

Cloud Security

+ many more, likely

Desired business outcome

Strengthen Communications



Communicate between stakeholders, security, and users. Explain milestones and benefits

Business outcomes/risks



Mapping business outcomes to business risks. Identify gaps.

Confidence



YES, I know what I am doing!

Benefits

$$1 + 1 > 3$$



"An architecture is more than the sum of its parts"

Who uses the security reference architecture

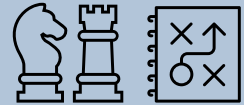
CxO, xVP, Leadership

Business
Transformation



Information Security/Risk Compliance

Security Strategy,
Compliance



Architects

Architecture and
Policy



Security and/or Network Operations

Configuration,
Deployment



Show me the
architecture!



TALOS THREAT INTELLIGENCE



Actionable threat intelligence



Collective responses



Comprehensive visibility



Signal identification



Threat research & analysis

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

SERVICES



Custom threat research on demand



Implement and manage



Incident response retainer



Managed detection & response



Strategy & assessment

CAPABILITIES



Network detection & response



Device discovery & insights



Endpoint detection & response



Open API platform & 3rd party native integrations



Risk-based vulnerability management



Identity & Security analytics



Security orchestration, automation & response



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



Continuous Trust



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 | Viptela



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



Anomaly detection



Compliance



Group tag classification



Identity pxGrid



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



Anti-virus Anti-malware



API security



App discovery



Cloud analytics



Cloud Native Security



CSPM/CAASM



DDoS, WAF/Bot



Identity pxGrid



Micro/Macro Segmentation



Run-time application



Telemetry



Threat mitigation



Visibility



Firewall



Data access & Integrity



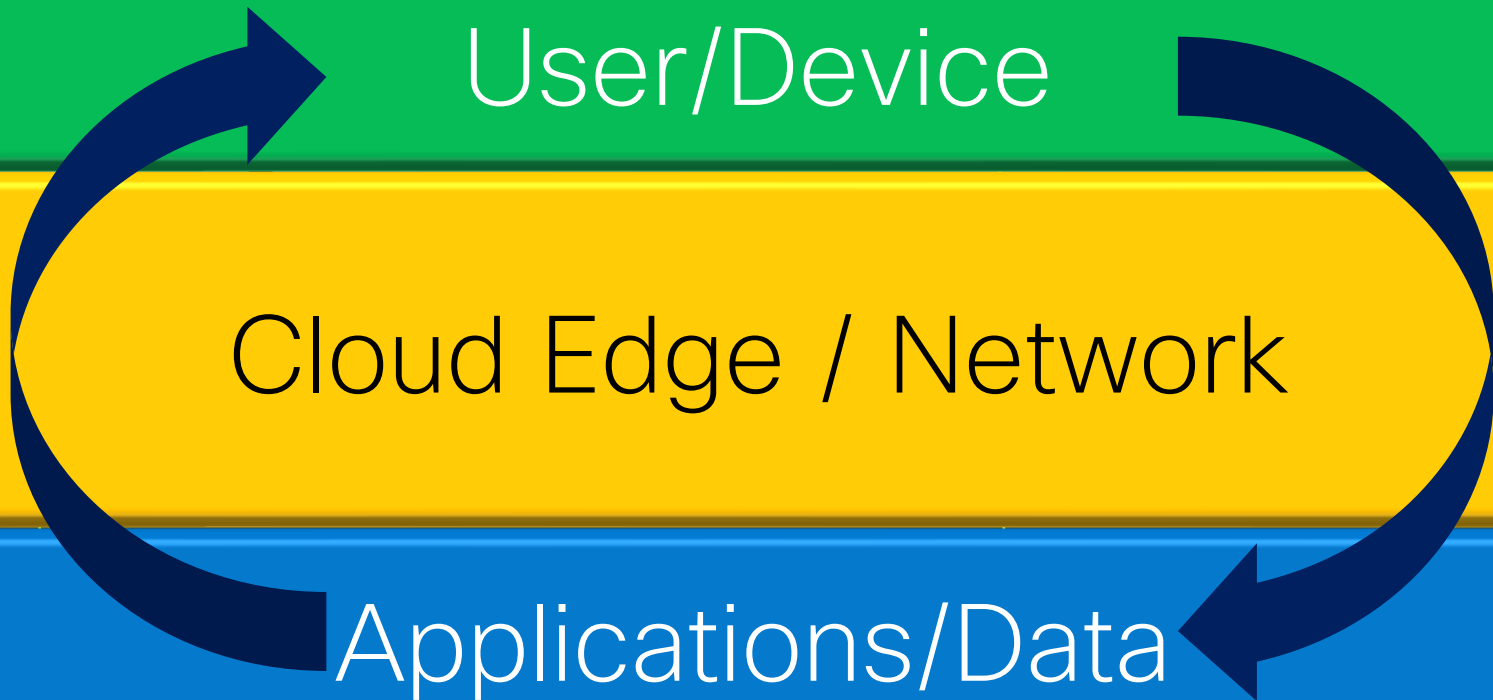
Defense Gateway

Extended Detection & Response

User/Device

Cloud Edge / Network

Applications/Data



CISCO *Live!*

- [illegible]

Cisco SRA ~~versus~~ and others...



Is Cisco SRA aligned to
other published security
architectures or
frameworks?



SRA compared to others

Existing frameworks

- SABSA and TOGAF
 - <https://sabsa.org/sabsa-executive-summary/>
- NIST
- CIS Controls
- NCSC
- And others...

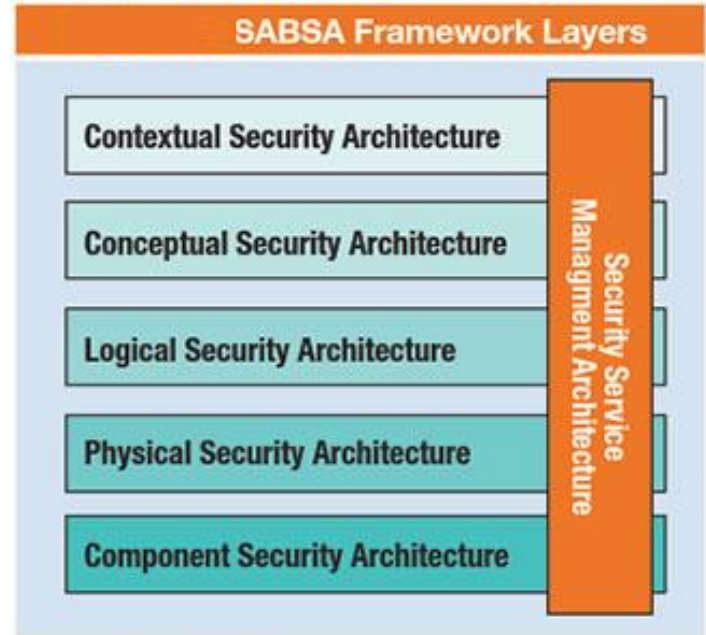
Provides detailed processes and guidelines + TIME



My goal is to focus on outcomes, not the process

SABSA

- Sherwood Applied Business Security Architecture
- Framework for developing risk-driven enterprise information security and information assurance architectures.
- SABSA does not offer any specific control and relies on others, such as the International Organization for Standardization (ISO) or COBIT processes

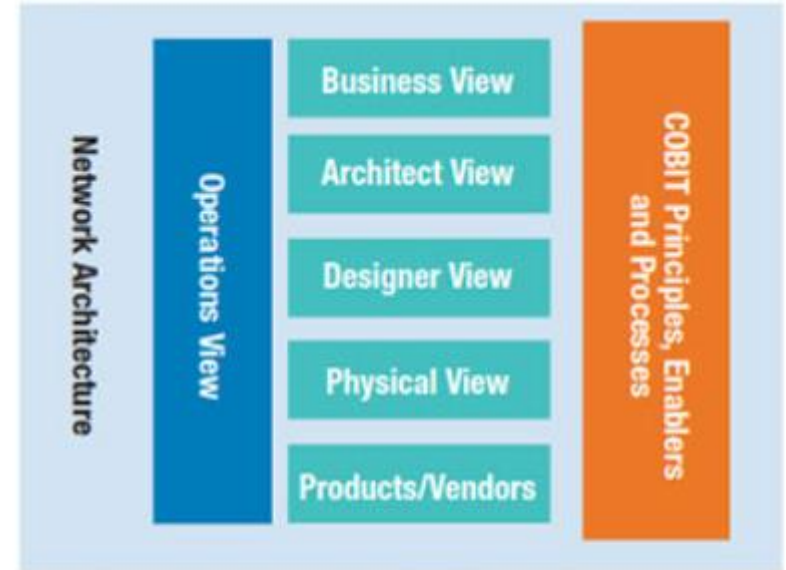


Source: SABSA, SABSA White Paper, 2009. www.sabsa.org/sabsa-white-paper. Reprinted with permission.

COBIT 5 Principles



Source: ISACA, COBIT® 5, USA, 2012. Reprinted with permission.



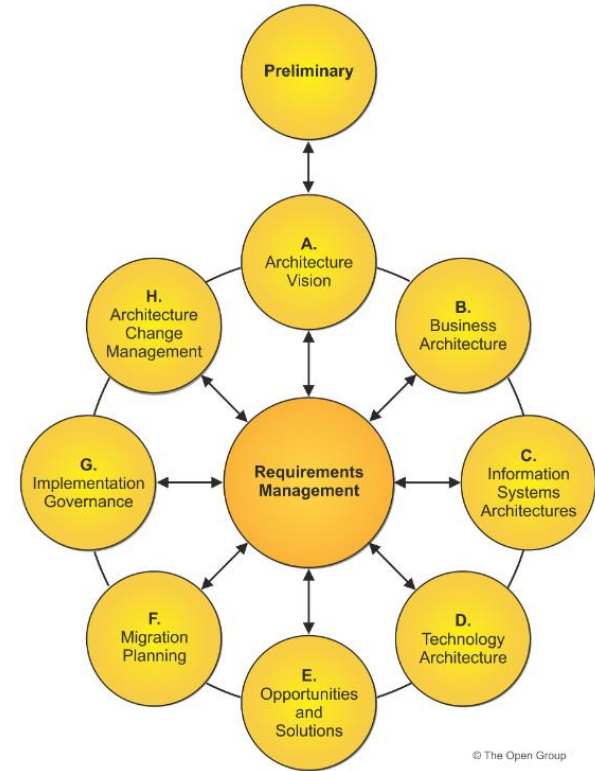
Source: R. Ghaznavi-Zadeh. Reprinted with permission.

Version 1 released in 1996 by ISACA

Control Objectives for Information and Related Technology

The Open Group Architecture Framework (TOGAF)

- Developed in 1995
- TOGAF is a framework and a set of supporting tools for developing an enterprise architecture
- TOGAF also starts at business vision and followed by technology
- TOGAF Series Guides – 10th edition
- Certifications available



CIS Controls Ecosystem

Center for Internet Security

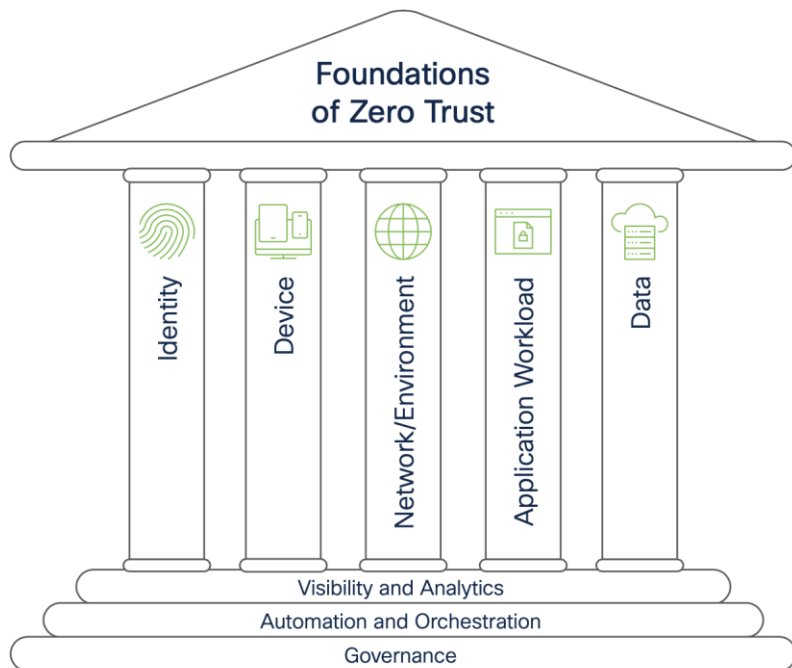
CIS Critical Security Controls

Control 01 Inventory and Control of Enterprise Assets	8
Why is this Control critical?	8
Procedures and tools	9
Safeguards	10
Control 02 Inventory and Control of Software Assets	11
Why is this Control critical?	11
Procedures and tools	12
Safeguards	12
Control 03 Data Protection	14
Why is this Control critical?	14
Procedures and tools	15
Safeguards	16
Control 17 Incident Response Management	54
Why is this Control critical?	54
Procedures and tools	55
Safeguards	55
Control 18 Penetration Testing	57
Why is this Control critical?	57
Procedures and tools	58
Safeguards	59

- It's not about the list
- Focus on stopping the threat, not “Nice to have”
- Feasible, Measurable
- Align to other frameworks, regulations, governance, etc

Zero Trust Market Alignment

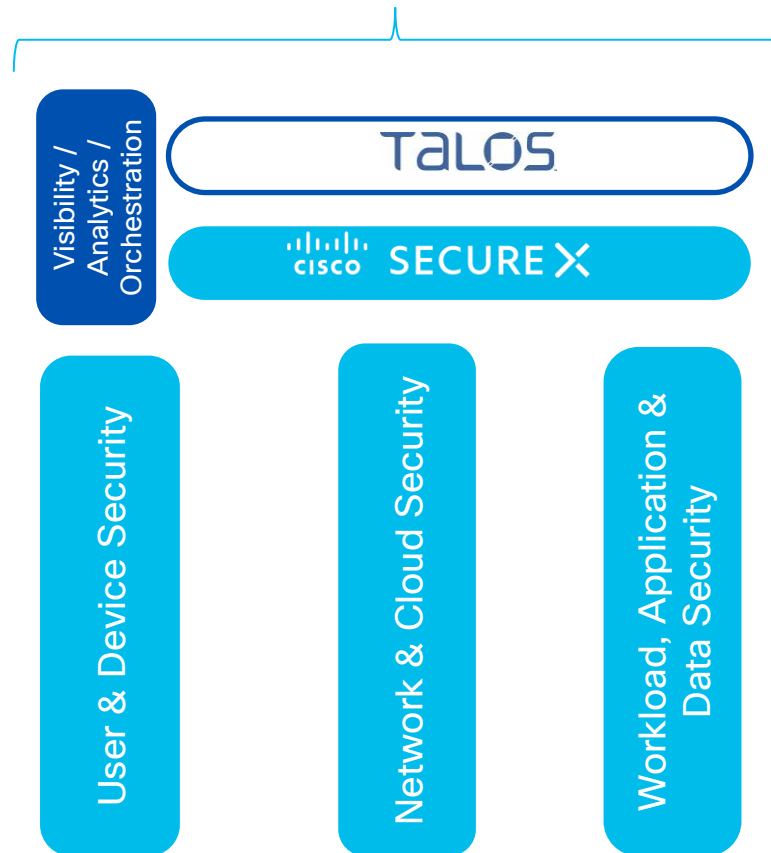
Based on NIST SP 800-207



US Cybersecurity Infrastructure and Security Agency, CISA Framework adopted by many industry analysts and experts

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

Cisco



NCSC Zero Trust

<https://www.ncsc.gov.uk/collection/zero-trust-architecture>

Introduction to Zero Trust

1. Know your architecture including users, devices, services and data

2. Know your user, service and device identities

3. Assess user behaviour, service and device health

4. Use policies to authorise requests

5. Authenticate and authorise everywhere

6. Focus your monitoring on users, devices and services

7. Don't trust any network, including your own

8. Choose services which have been designed for zero trust

Help implementing zero trust architecture +



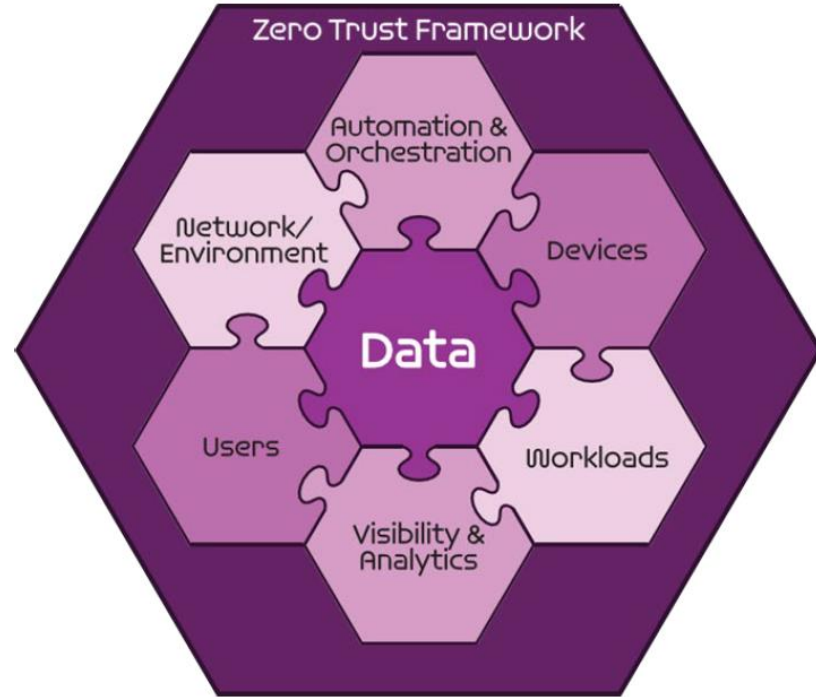
July 23, 2021

DISA Zero Trust Framework

Defense Information Systems Agency



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



[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)



Threat Intelligence



Extended Detection and Response



ZERO TRUST



SASE



User / Device Security



Cloud Edge Network



On Premises Network

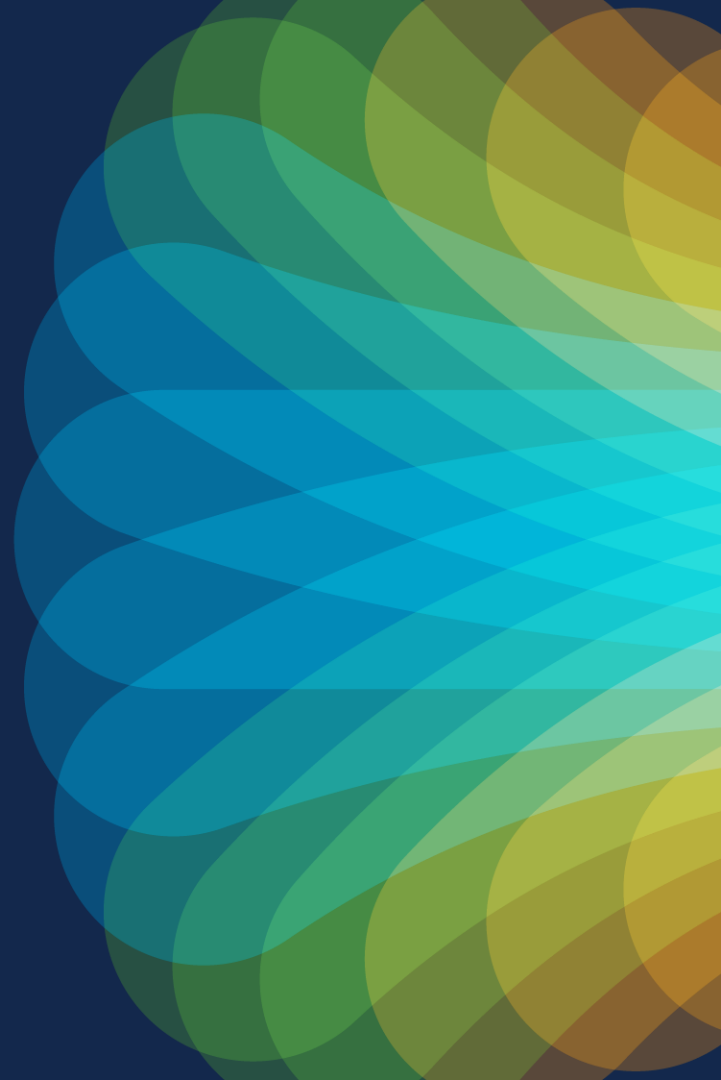


Workload, Application, and Data



Platform

How to use the SRA



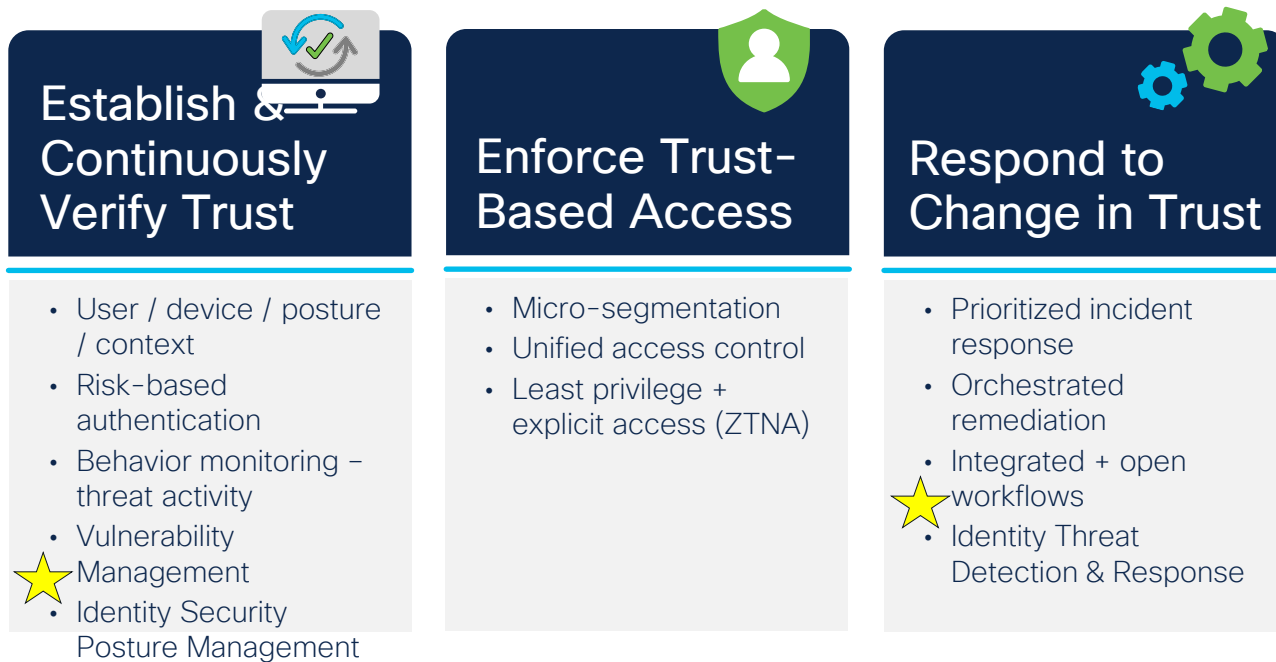
Zero Trust

What Zero Trust Means to Us



What it takes to get Zero Trust right

Zero Trust requirements





ZERO TRUST

SASE

User / Device Security

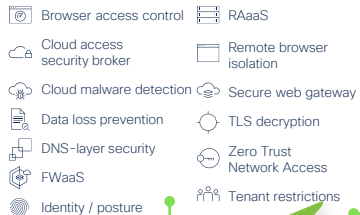
Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes



Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect



On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Viptela



In the Office/Managed Location

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



Industrial Threat Defense

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



Workload, Application, and Data Security

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



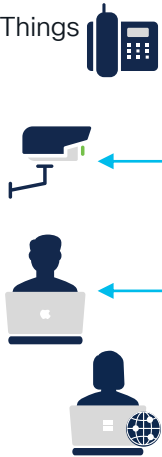
ISE Provides Zero Trust for On-Premises

Enterprise

Security

Endpoints

- Users
- Devices
- IOT Things



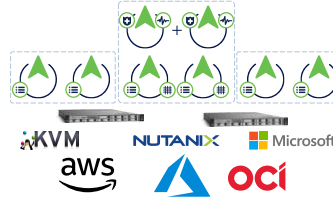
Network Devices

- Switches
- WLCs / APs
- VPN



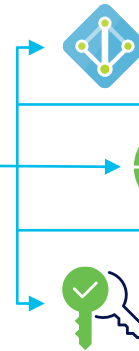
Cisco ISE

- 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

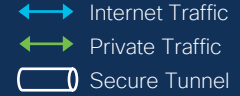
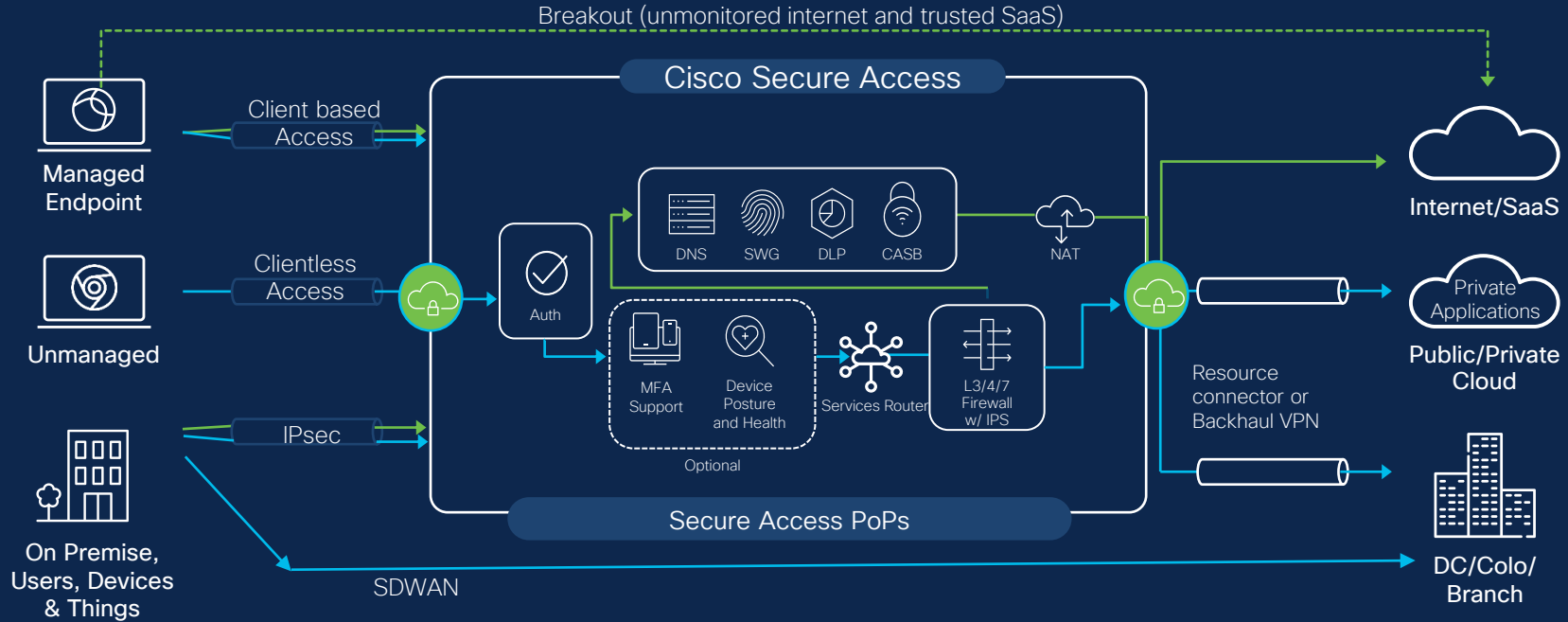


See It

Secure It

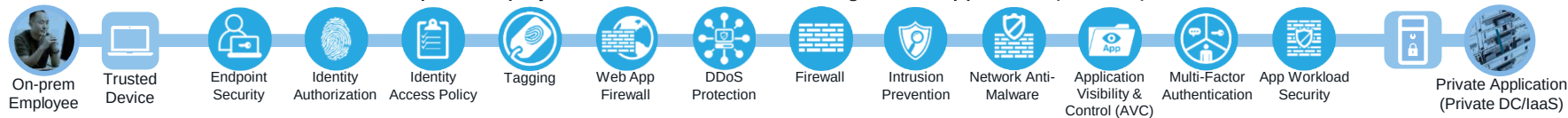
Share It

Secure Remote Worker + Branch

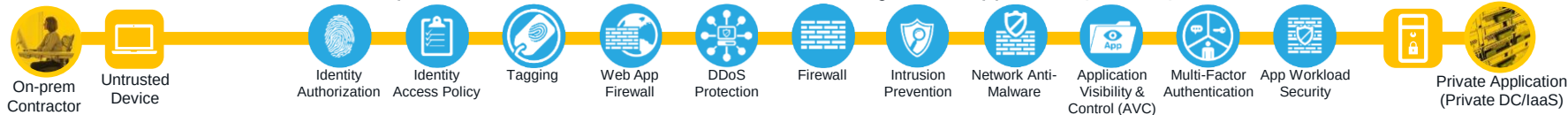


Zero Trust Business Flows with Security Capabilities

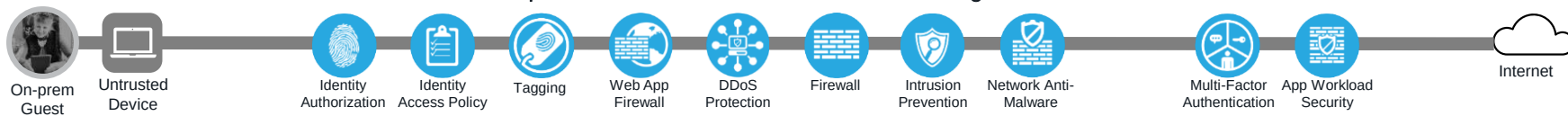
On-prem Employee with Trust Device: Accessing Private Application (DC/IaaS)



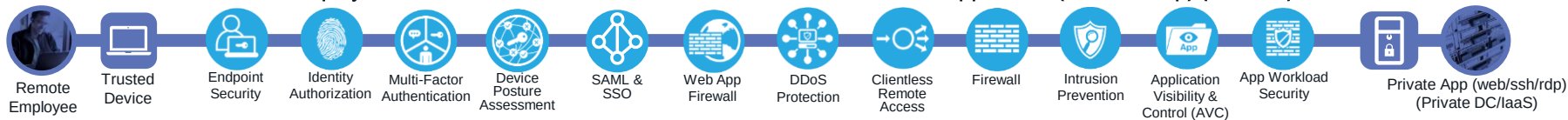
On-prem Contractor with Untrusted Device: Accessing Private Application (DC/IaaS)



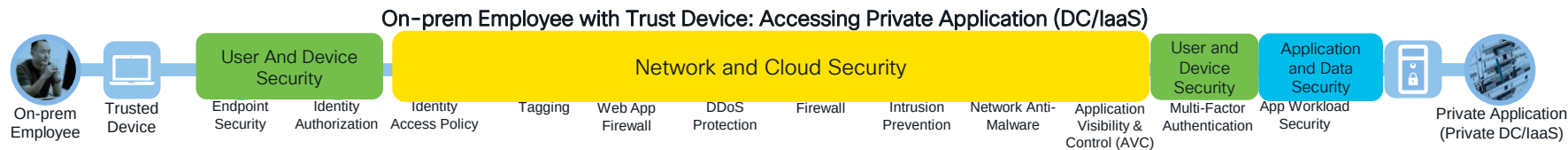
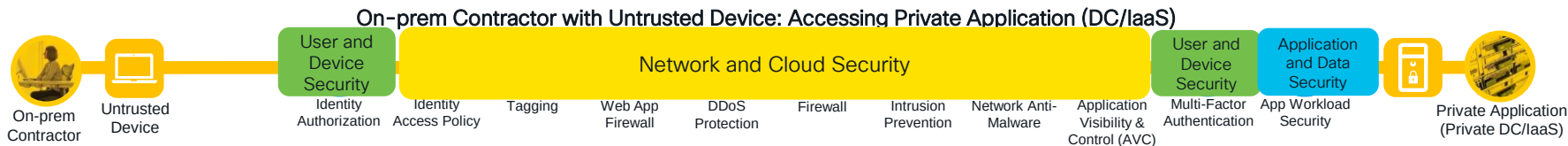
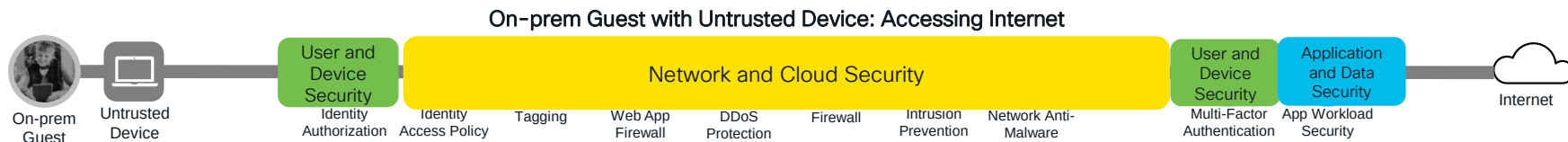
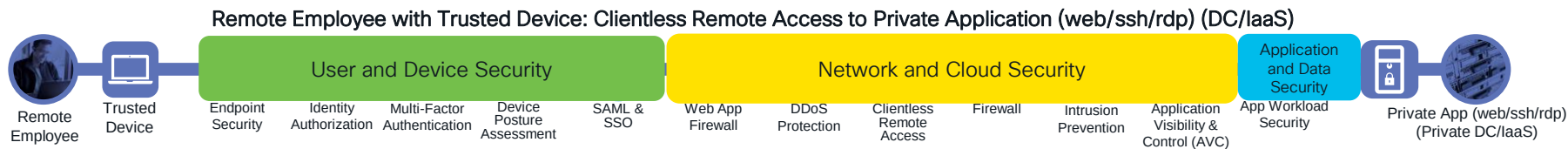
On-prem Guest with Untrusted Device: Accessing Internet



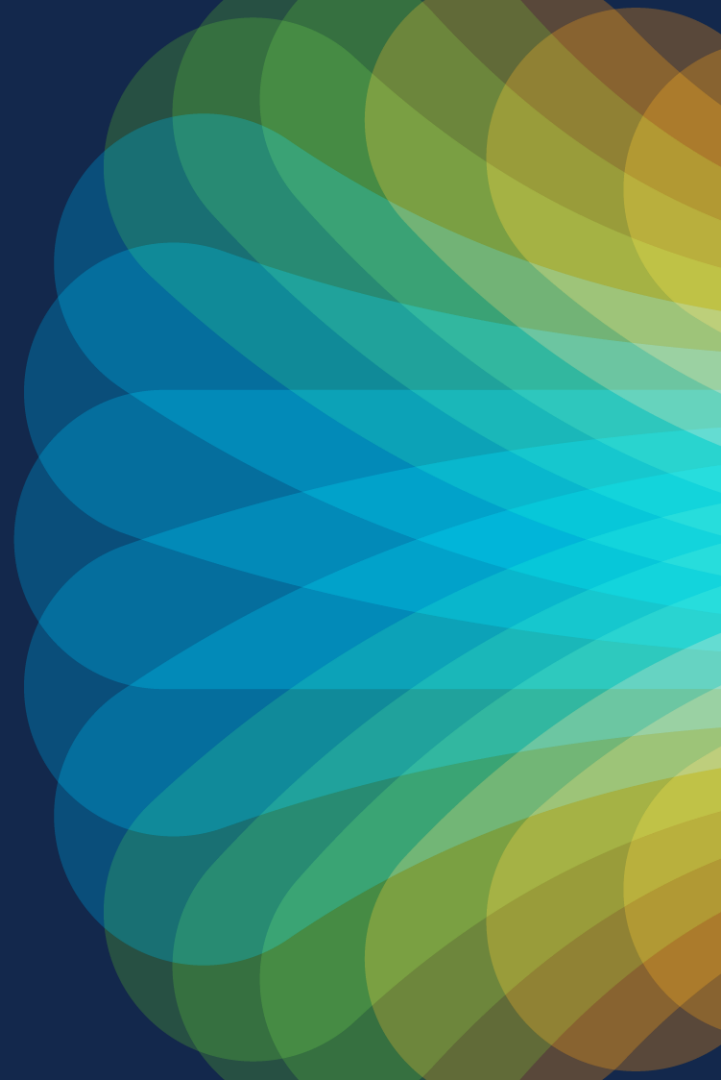
Remote Employee with Trusted Device: Clientless Remote Access to Private Application (web/ssh/rdp) (DC/IaaS)



Zero Trust Business Flows with Cisco Zero Trust Principles



Zero Trust - Identity



TALOS THREAT INTELLIGENCE

Actionable threat intelligence

Collective responses

Comprehensive visibility

Signal identification

Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics
XDR | Secure Client | Talos Incident Response

SERVICES

Custom threat research on demand

Implement and manage

Incident response retainer

Managed detection & response

Strategy & assessment

CAPABILITIES

Network detection & response

Device discovery & insights

Endpoint detection & response

Open API platform & 3rd party native integrations

Risk-based vulnerability management

Identity & Security analytics

Security orchestration, automation & response

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 | Continuous Trust | 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 | Viptela

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 | DNAC | Meraki | Secure Firewall | Secure Network | Secure Web Appliance

Application network gateway | Group tag classification | NGIPS | Segmentation | Threat mitigation | Profiling | Content filtering | Encrypted visibility | Zero Trust Network Access

Industrial Threat Defense

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

Anomaly detection | Ruggedized | Compliance | Segmentation | Group tag classification | Threat mitigation | Identity pxGrid | Visibility

Workload, Application, and Data Security

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

Anti-virus | Anti-malware | API security | App discovery | Cloud analytics | Cloud Native Security | CSPM/CAASM | DDoS, WAF/Bot | Identity pxGrid | Micro/Macro Segmentation | Run-time application | Telemetry | Threat mitigation | Visibility | Firewall | Data access & Integrity | Defense Gateway

Scalable Group Tag(SGT)

AKA Security Group Tags

Security Groups

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

[Edit](#) [+ Add](#) [Import](#) [Export](#) [Trash](#) [Push](#) [Verify Deploy](#)

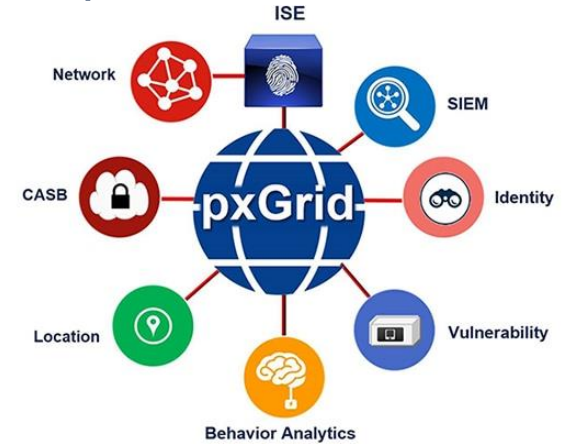
☐	Icon	Name	SGT (Dec / Hex)	Description
☐		1120asaVPNuser	18/0012	FP1120asa VPN user
☐		Auditors	9/0009	Auditor Security Group
☐		BYOD	15/000F	BYOD Security Group
☐		Contractors	5/0005	Contractor Security Group
☐		Developers	8/0008	Developer Security Group
☐		Development_Servers	12/000C	Development Servers 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

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

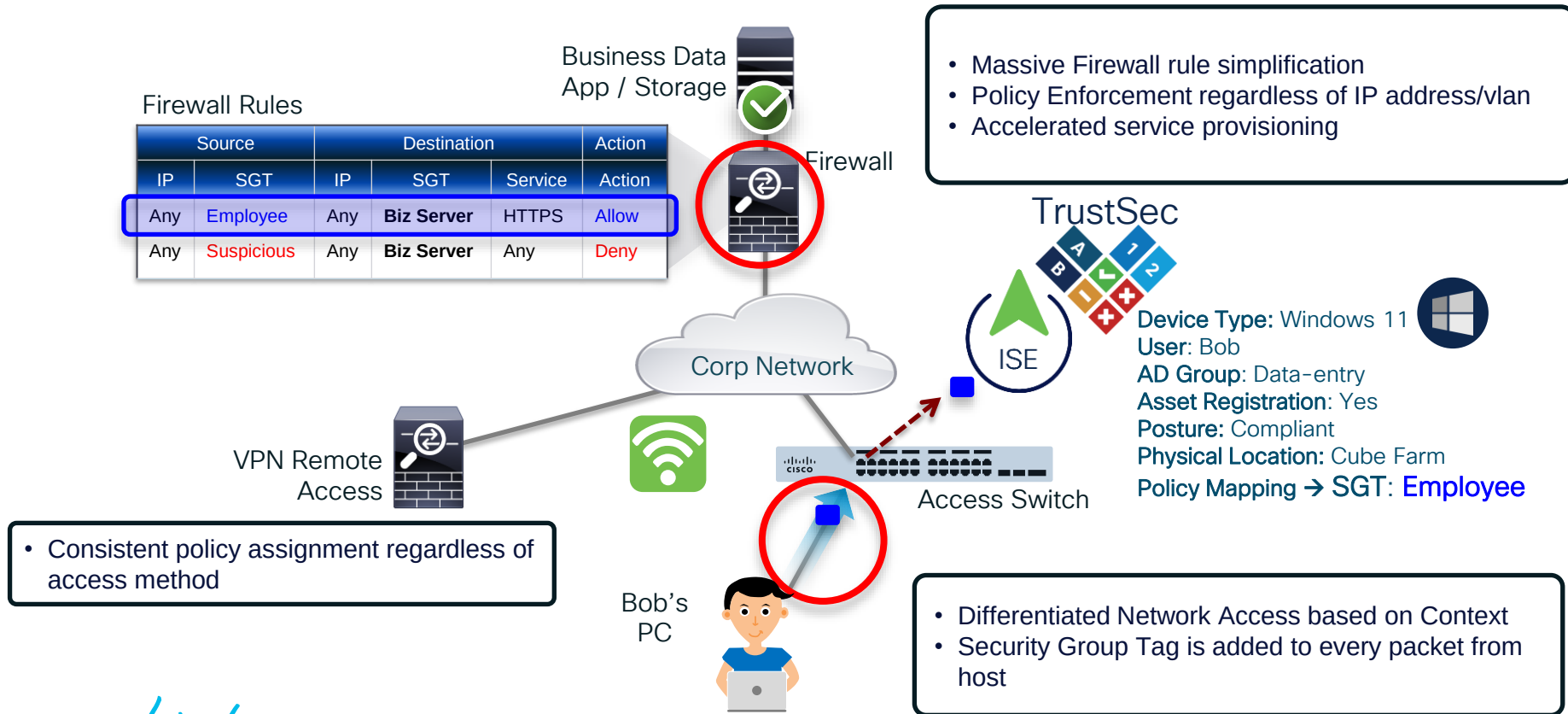
Cisco Platform Exchange Grid(pxGrid)

- 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...



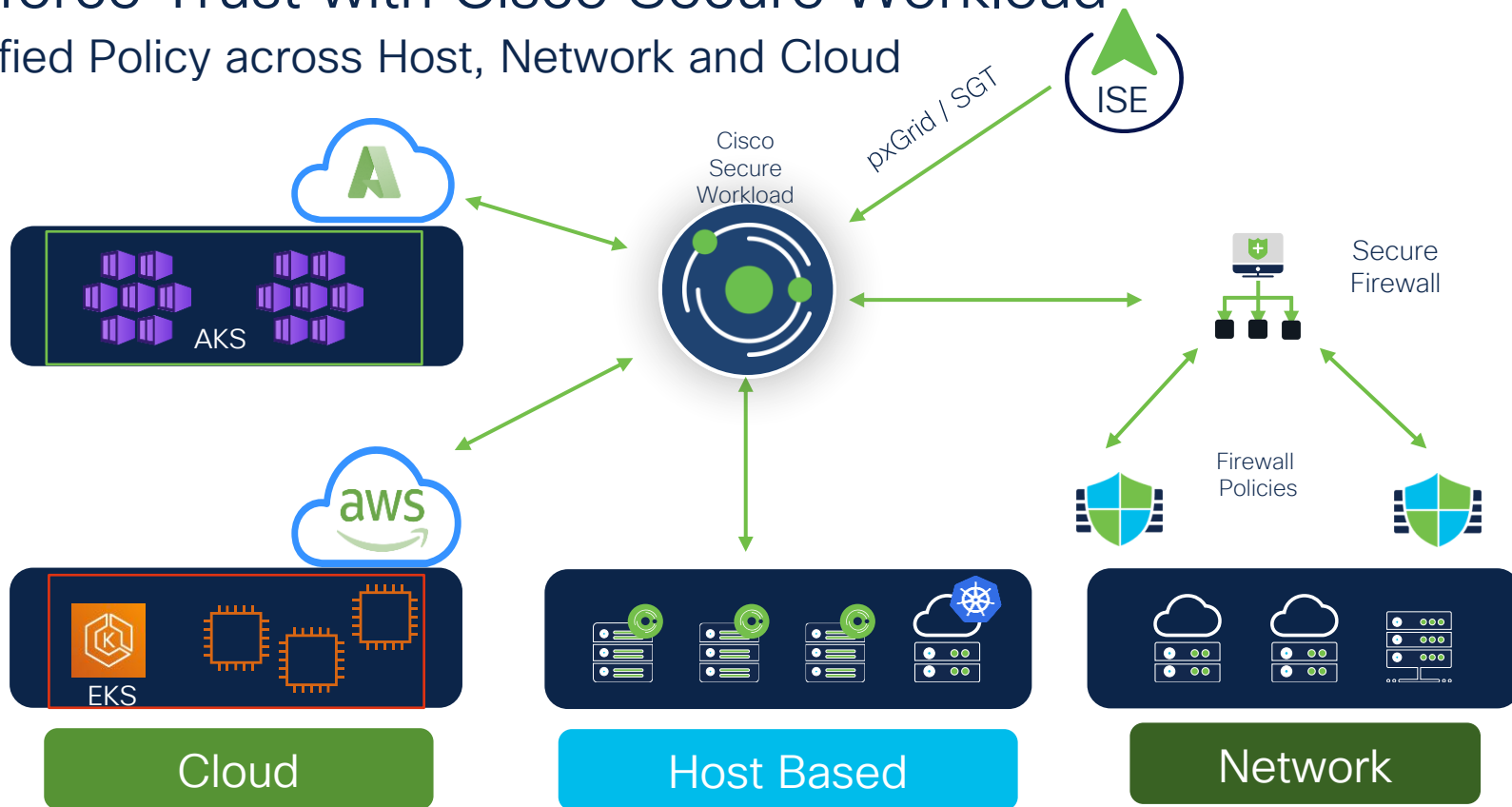
Dynamic Segmentation: Solving the age old problem

Cisco TrustSec

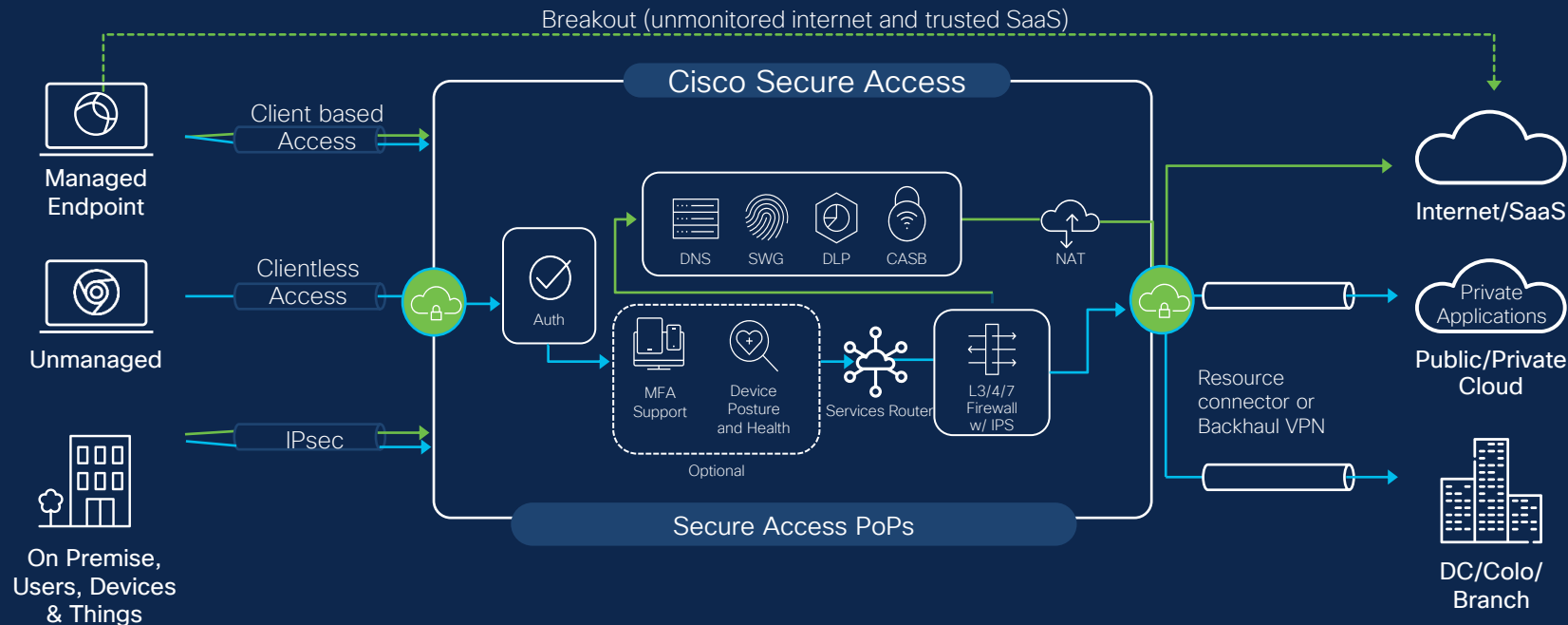


Enforce Trust with Cisco Secure Workload

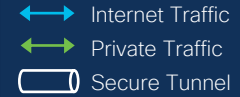
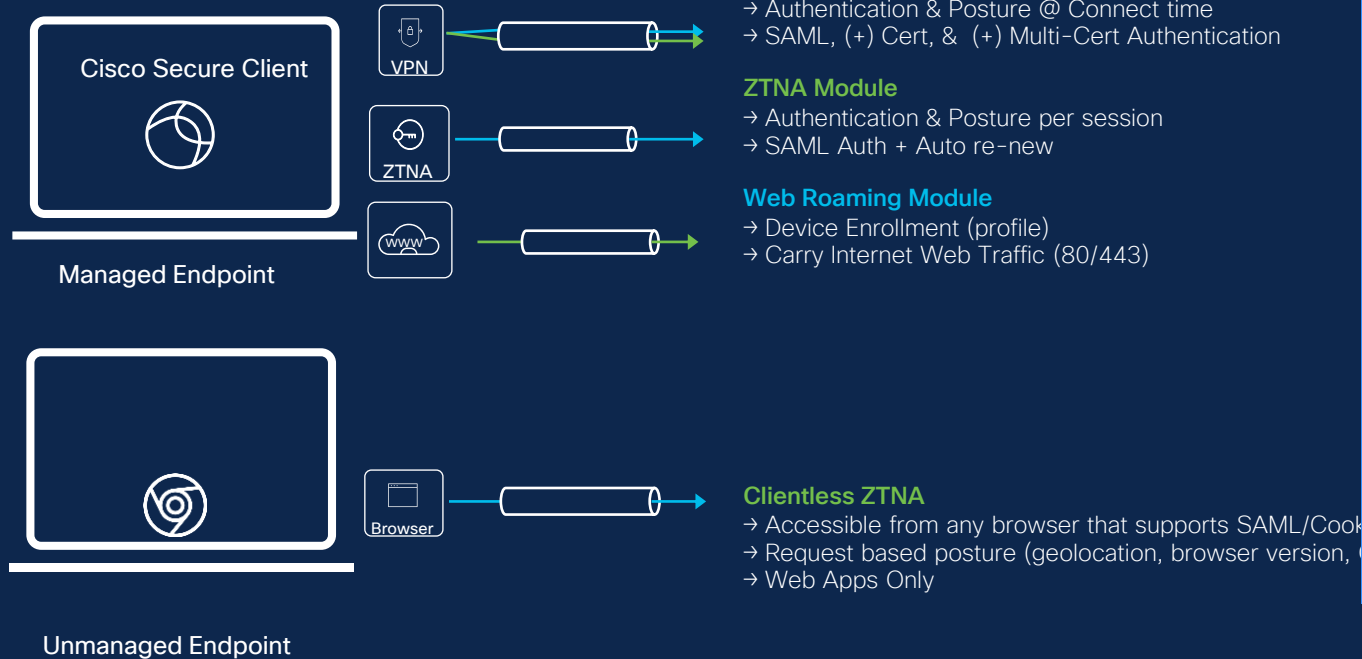
Unified Policy across Host, Network and Cloud



Identity: Secure Remote Worker + Branch



Risk-Based Authentications



Risk Factors

- Device Trust
- GeoIP
- Historical Auths
- WiFi-Fingerprint
- Push Harassment
- Push Spray
- Unrealistic travel
- Country code mismatch
- Novel ASN

Identity Sprawl



Azure Active Directory

okta



CISCO *Live!*

- jelin@cisco.com
- jerrylin@gmail.com
- jeremylin@gmail.com
- Jerry@ID.onmicrosoft.com
- jerrylin949@dropbox.com
- + more

Google



 PingIdentity[®]

 Dropbox

 slack

Identity Threat Detection and Response (ITDR)

“...a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools, and processes to protect identity systems.

It works by implementing detection mechanisms, investigating suspicious posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure...”

Gartner Analyst

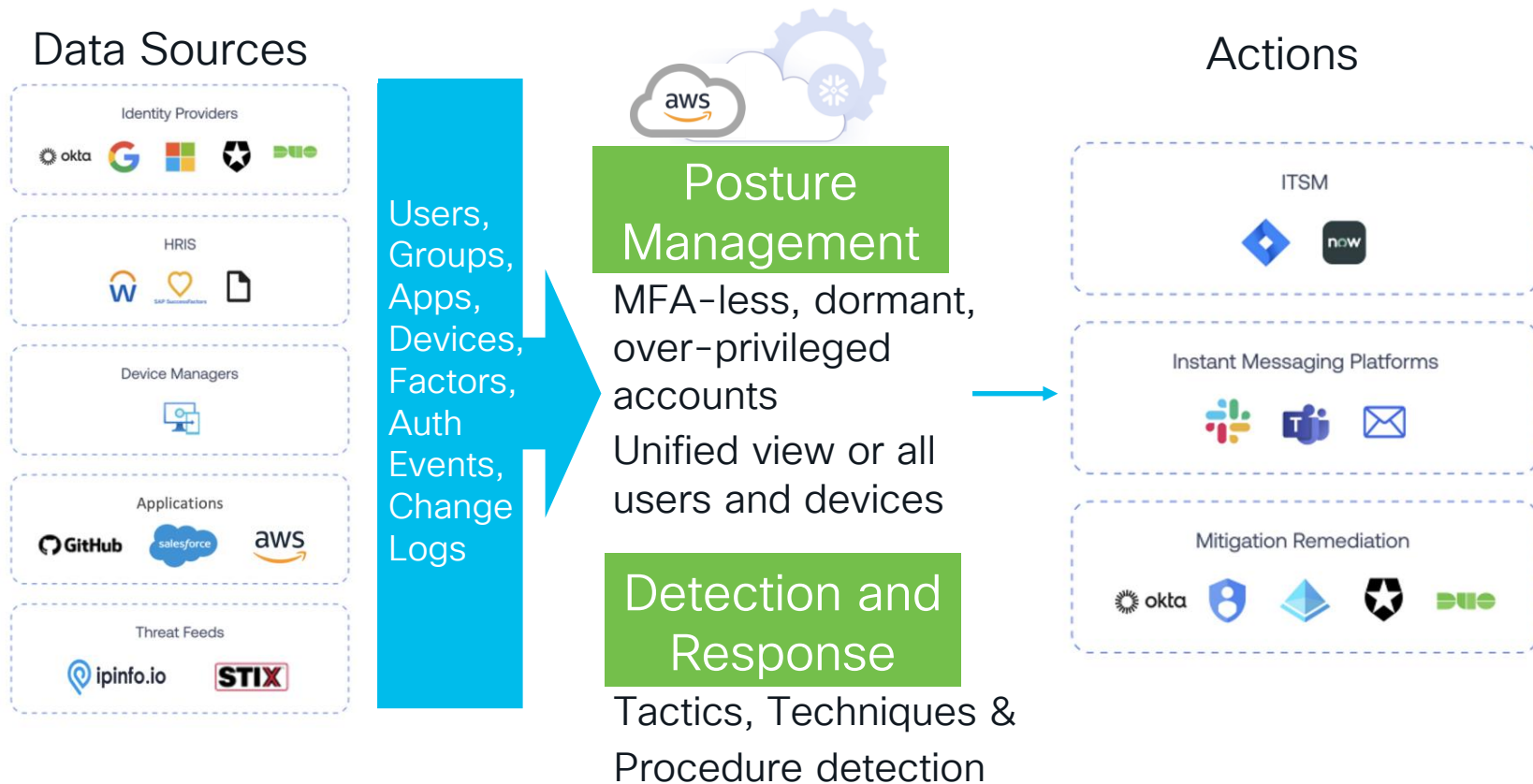
By 2026, 90% of organizations will be using some type of embedded identity threat detection and response function from access management tools as their primary way to mitigate identity attacks

Gartner: Magic Quadrant for Access Management, Nov 2022

Identity Security Posture Management (ISPM)

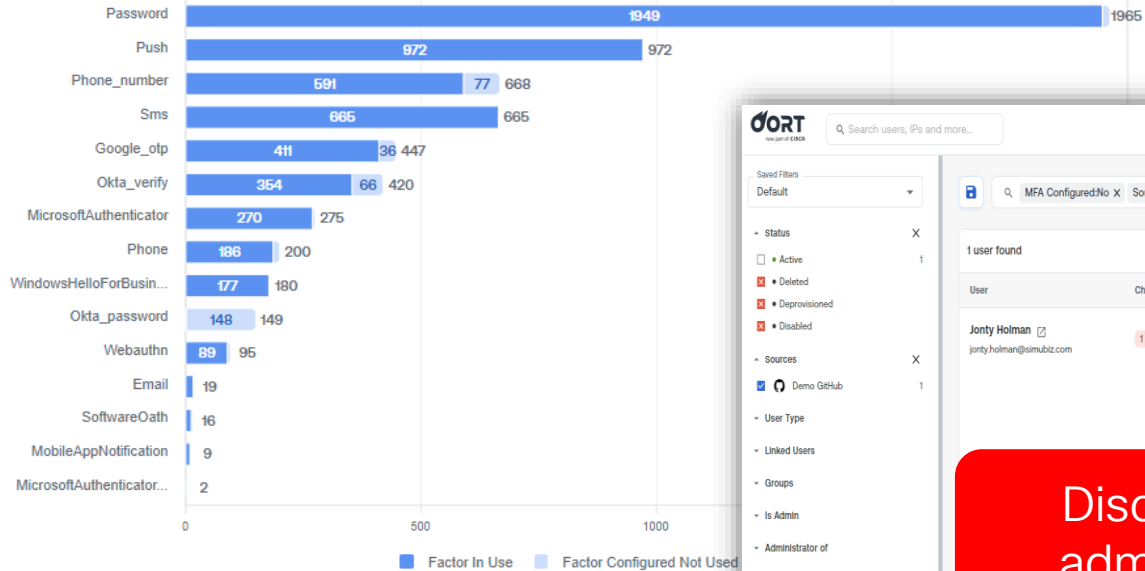
- Enables organizations to manage and protect identities proactively by monitoring and analyzing an organization's identity security posture to detect weaknesses and misconfigurations
 - No or weak MFA
 - Dormant accounts
 - Over-privileged users (especially partners, contractors, etc)
 - Administrative account overuse
 - SSO bypass
 - User inconsistencies

Cisco Identity Threat Detection & Response



Inconsistent Authentication policies

MFA Prevalence by User Count



MFA	Providers	Status
		Active

Search users, IPs and more...

Dashboard Users Checks Integrations

MFA Configured: No X Sources: Demo GitHub X NOT Status: (3 conditions) X Search users, names, groups, applications and IPs

1 user found

User	Checks	# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Providers	Status
Jonty Holman jonty.holman@simubtz.com		0	N/A	11 Hours Ago Nov 8, 2023 04:10:46	N/A	N/A			Active

Discover which Github user or administrator is not using MFA

Overall MFA compliance view

Inactive Guest Accounts

Remove inactive accounts to minimize attack surface

The screenshot shows the Cisco DuoORT interface. The top navigation bar includes the logo, a search bar, and links to Dashboard, Users, Checks, and Integrations. The user profile for Michael Marriott is visible. The main content area shows the user profile for Pantomima Visholdo, with tabs for Overview, Activity, Networks, Devices, Applications, Groups, and Checks. The 'Actions' menu is highlighted with a red box. A modal dialog is open for deleting the user from Microsoft Entra ID.

Checks / Inactive Guest Users / panto.visho@simubiz.com

Pantomima Visholdo • Active

Overview Activity Networks Devices Applications Groups Checks **Actions**

Failing Checks

Name	Result	Times Excluded	First Reported (UTC)
Inactive Guest Users	Failure	0	Nov 8, 2023 04:23:51
No MFA Configured	Failure	0	Nov 8, 2023 04:23:51

Delete user from Microsoft Entra ID (formerly Azure AD)

Are you sure you want to delete this user account from Microsoft Entra ID?

The account may be recovered before it is automatically deleted according to Microsoft Entra ID policies.

Cancel Confirm

Unified User Inventory

Problem: Identity Sprawl

Likely same user

Multiple IdPs

Linked Users

User		User Type	Last Seen (UTC)	Last Location	MFA	Providers
Aalto Helmig  aalto.h@simubiz.com	• Transient	Internal	5 Hours Ago Oct 25, 2023 11:46:11	N/A		
Aalto Helmig  aalto.helmig@simubiz.com	• Active	External	19 Hours Ago Oct 24, 2023 22:00:05	Fort Lauderdale, Florida, US		
Aalto Helmig  helmig@simubiz.com	• Active	Internal	13 Hours Ago Oct 25, 2023 04:11:07	N/A		  

Identity Hygiene

- Link multiple ID's as one user based UserID, email, UPN, etc
- Prevent unauthorized logins if employee leaves organization

Secure Access Service Edge (SASE)

SASE = SDWAN
+ SSE

ZERO TRUST

SASE

User / Device Security

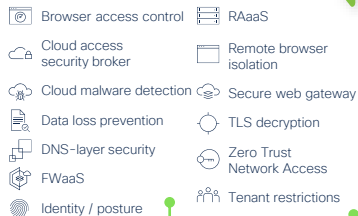
Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes



Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect



On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Viptela

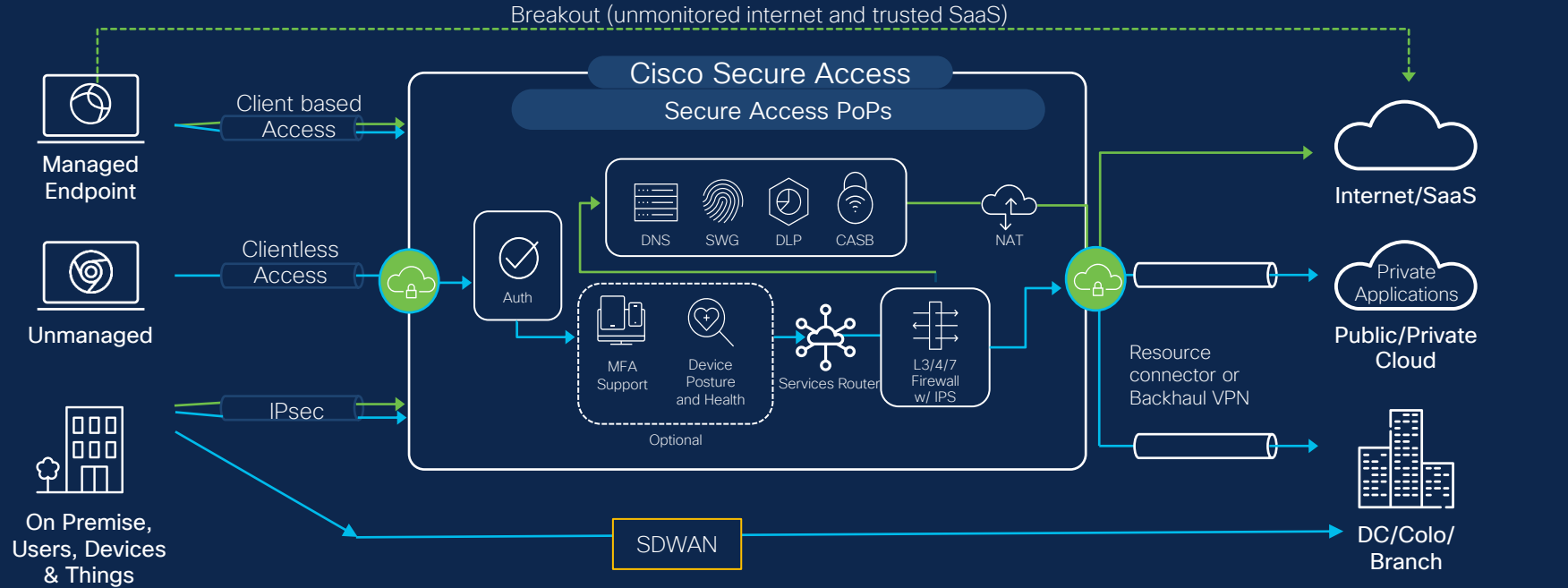


Workload, Application, and Data Security

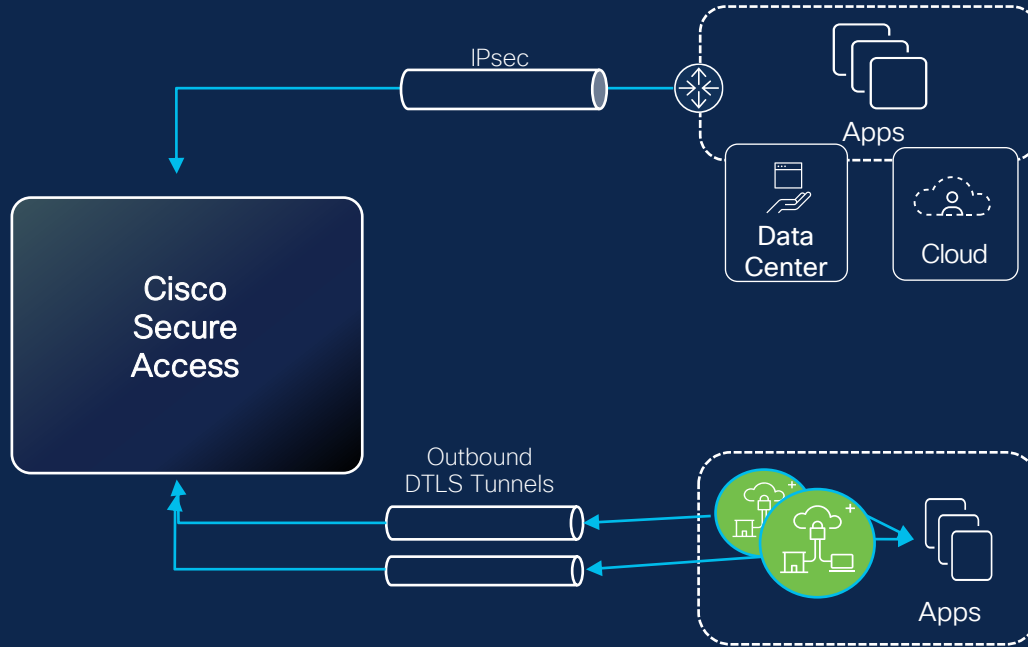
ACI | Attack Surface Management | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Multicloud Defense | Secure Workload



Architecture Overview



Apps: Private Applications



Network Tunnel

- IPsec Backhaul
- Static or BGP based routing
- Auto Failover/ Redundancy

Resource Connector (RC)

- Software deployment (VM or Cloud Instance)
- Deploy closest to application
- Outbound connectivity (no holes in firewall)
- Auto failover / load balancing

Apps: Internet/SaaS Applications

Trusted SaaS/Bypass

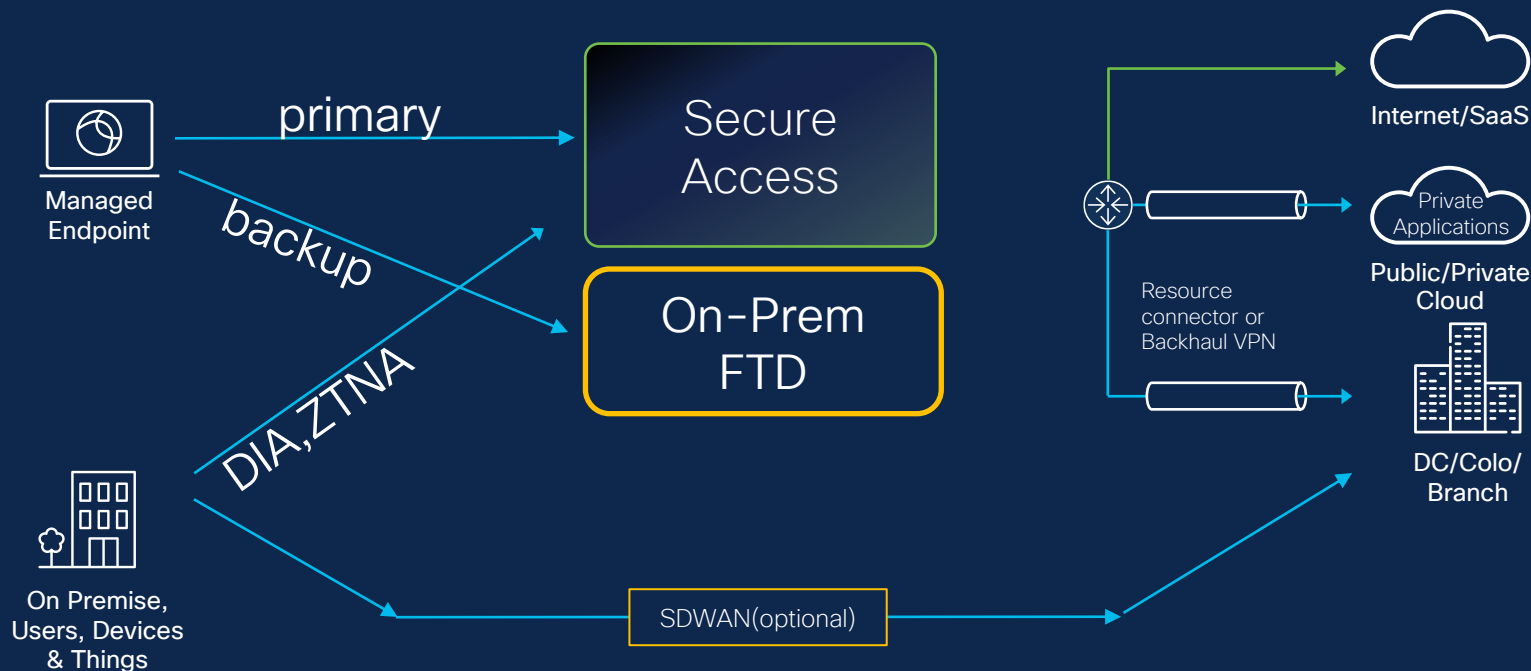
- Bypass inspection for trusted web apps
- route traffic directly from host to internet



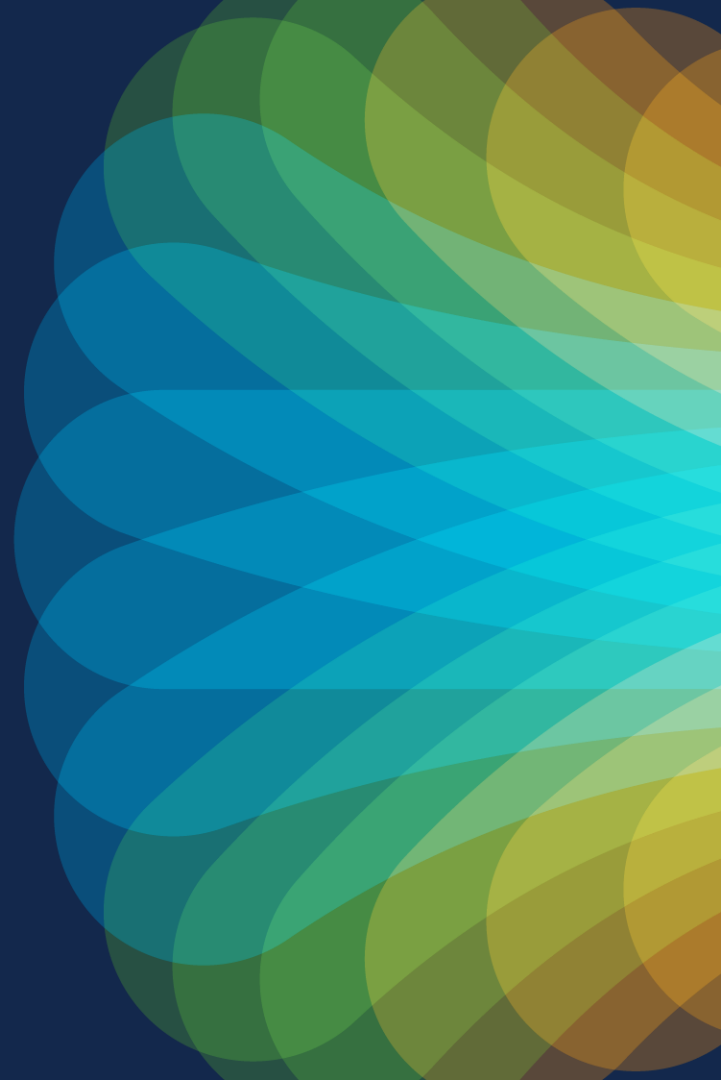
Secure Internet Access

- All traffic filtered through Secure Access
- Branch traffic routed via IPsec tunnel
- Remote user traffic acquired via Secure Client

High Availability Architecture (Planned Goal)



Converged Multicloud Policy



TALOS THREAT INTELLIGENCE

Actionable threat intelligence

Collective responses

Comprehensive visibility

Signal identification

Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics
XDR | Secure Client | Talos Incident Response

SERVICES

Custom threat research on demand

Implement and manage

Incident response retainer

Managed detection & response

Strategy & assessment

CAPABILITIES

Network detection & response

Device discovery & insights

Endpoint detection & response

Open API platform & 3rd party native integrations

Risk-based vulnerability management

Identity & Security analytics

Security orchestration, automation & response

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 | Continuous Trust | 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 | Viptela

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 | DNAC | Meraki | Secure Firewall | Secure Network | Secure Web Appliance

Application network gateway | Group tag classification | NGIPS | Application security | Content filtering | Encrypted visibility | Zero Trust Network Access | Segmentation | Threat mitigation | Profiling

Industrial Threat Defense

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

Anomaly detection | Compliance | Group tag classification | Identity pxGrid | 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

Anti-virus | Anti-malware | API security | App discovery | Cloud analytics | Cloud Native Security | CSPM/CAASM | DDoS, WAF/Bot | Identity pxGrid | Micro/Macro Segmentation | Run-time application | Telemetry | Threat mitigation | Visibility | Firewall | Data access & Integrity | Defense Gateway

Problem: Inconsistent access policies across data centers

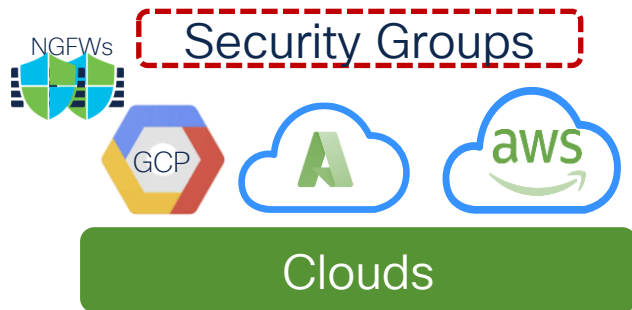
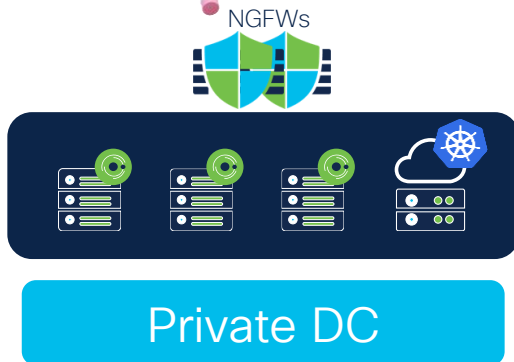
Access Policy



Access Policy

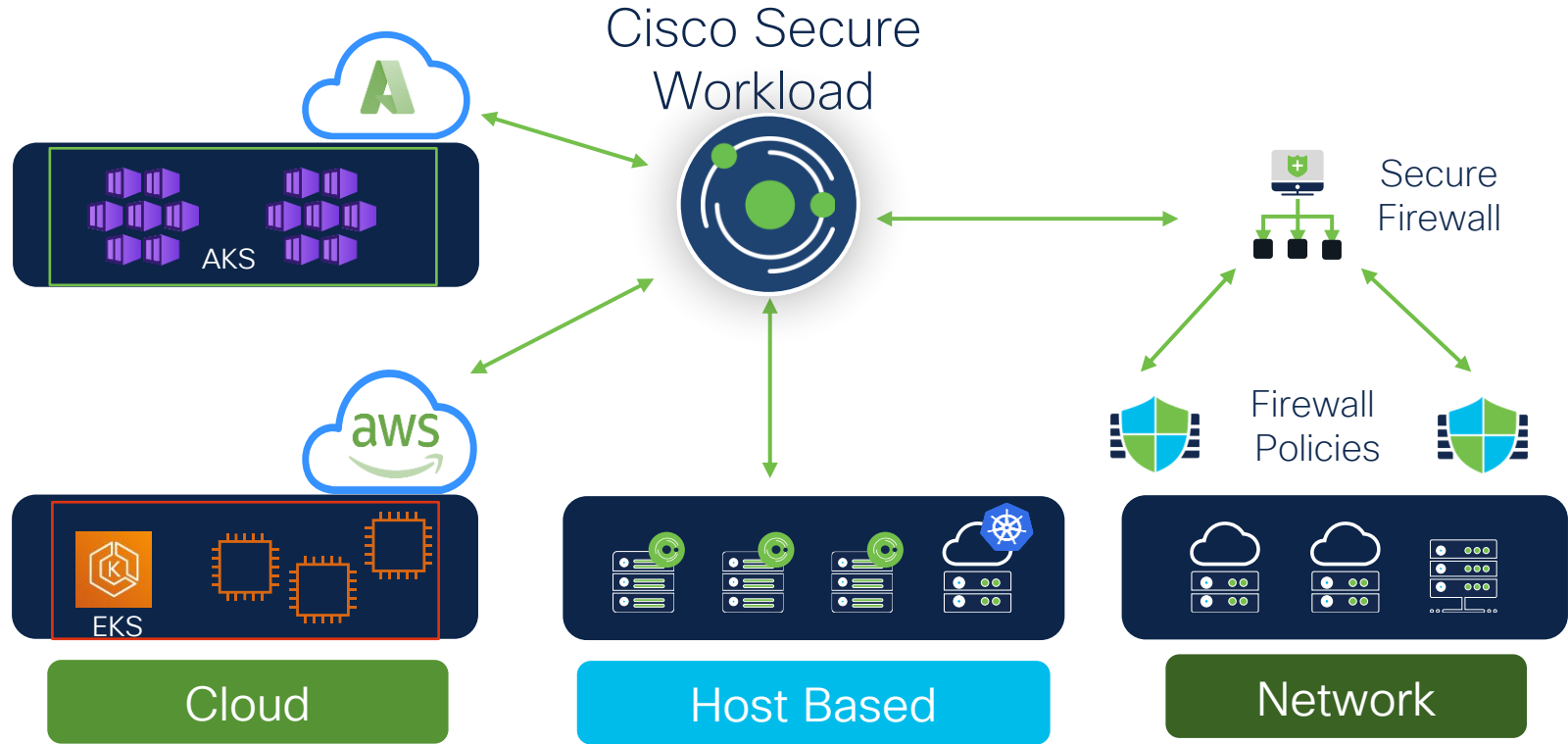


Access Policy



Enforce Trust with Cisco Secure Workload

Unified Policy across Host, Network and Cloud



DC Unified Policy



Workload admin
makes policy
change



dynamic



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: 1 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
Default	90	DENY	VPN1120_contractor	CVE 2022-30190	Any
Default	91	DENY	VPN1120_employees	CVE 2022-30190	ICMP

Firewall Management Center

Policies / Access Control / Policy Editor

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

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
-	sg-0d5de67ce7f8d1c03	csw_a042ddfb_15803...	vpc-04ae4072760e59d34	Cisco Secure Workload...	998494316702	5 Permission entries	0 Permission entries

sg-0d5de67ce7f8d1c03 - csw_a042ddfb_158030995_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

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

Extended Detection & Response

TALOS THREAT INTELLIGENCE

Actionable threat intelligence

Collective responses

Comprehensive visibility

Signal identification

Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics XDR | Secure Client | Talos Incident Response

SERVICES

Custom threat research on demand

Implement and manage

Incident response retainer

Managed detection & response

Strategy & assessment

CAPABILITIES

Network detection & response

Device discovery & insights

Endpoint detection & response

Open API platform & 3rd party native integrations

Risk-based vulnerability management

Identity & Security analytics

Security orchestration, automation & response

Threat visibility, incident response & threat hunting

ZERO TRUST

SASE

User / Device Security

Cisco Secure Client (Any Connect) | Umbrella | Secure Endpoint | Meraki System Manager | Duo | Secure E-mail | ThousandEyes

Cloud managed | VPN | Telemetry Visibility | Endpoint detection & response | DNS-layer security | Secure web | Antivirus | Query | Host FW | Mobile device management | Risk-based MFA | Password-less | Data loss prevention | Continuous Trust | Email, Phishing, SPAM, EBC, 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 | Viptela

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

Any Connect | DNAC | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance

Application network gate | Configuration orchestration | Content filter | 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 | CyberVision | Industrial Networking | ISE | Secure Firewall | Secure Network Analytics

Anomaly detection | Compliance | Group tag classification | Identity pxGrid | Ruggedized | Segmentation | Threat mitigation | Visibility

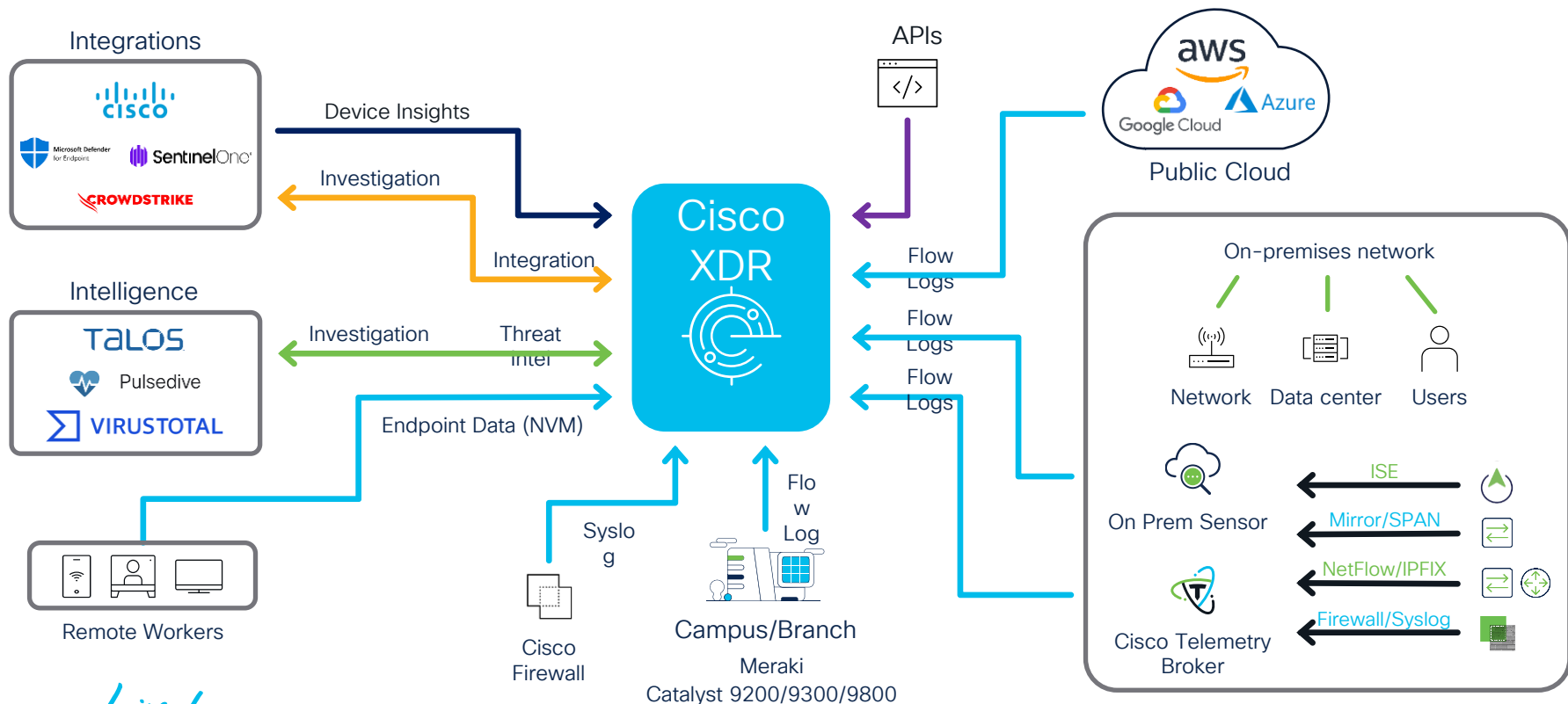
Workload, Application, and Data Security

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

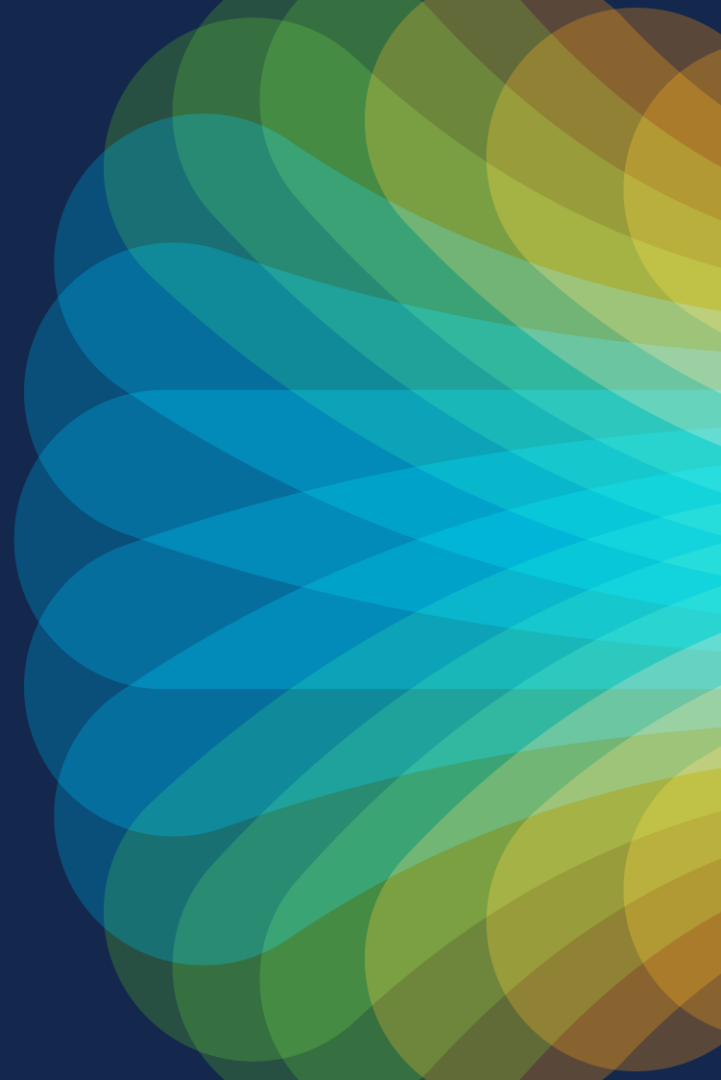
Anti-virus | Anti-malware | API security | App discovery | Cloud analytics | Cloud Native Security | CSPM/CAASM | DDoS, WAF/Bot | Identity pxGrid | Micro/Macro Segmentation | Run-time application | Telemetry | Threat mitigation | Visibility | Firewall | Data access & Integrity | Defense Gateway

Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



Threat Modeling



What is Threat Modeling? Per Cisco Enterprise AI



“Proactive approach for evaluating potential threats and vulnerabilities in a system. It involves identifying, understanding, and addressing the threats that could potentially harm a system.”



Identity your assets



Define the system



Identity and categorize threats



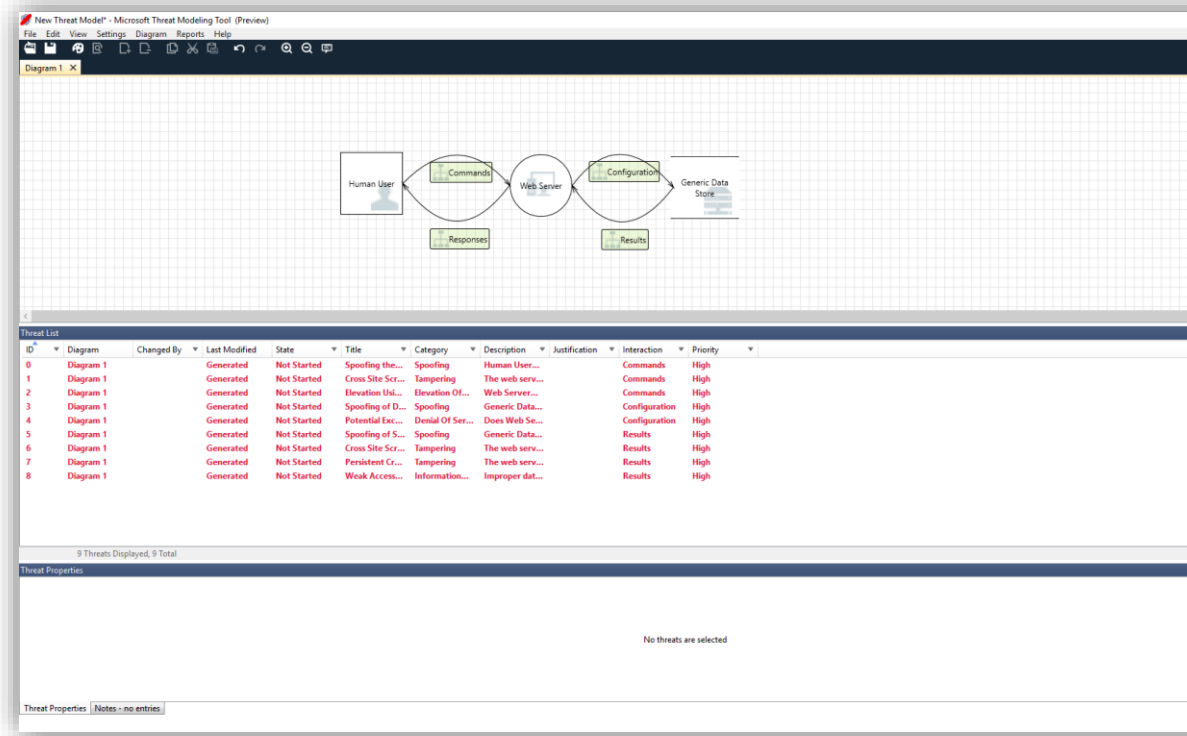
Prioritize threats



Define countermeasures

Threat Modeling Tools

- Microsoft Threat Modeling Tool (TMT) version 7.3.x
- MITRE ATT&CK
- STRIDE
 - Spoofing identity
 - Tampering with data
 - Redudiation
 - Information disclosure
 - Denial of service
 - Elevation of privilege
- Others



Example: Zero Trust Business Flows with Threats

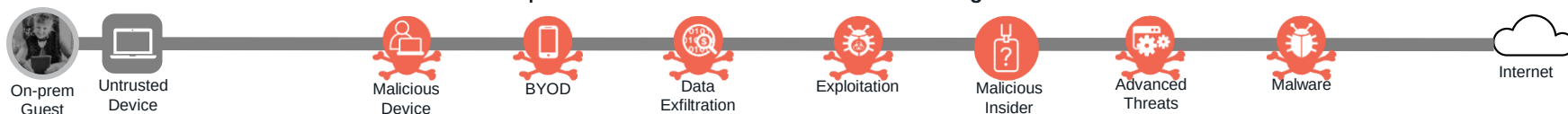
On-prem Employee with Trust Device: Accessing Private Application (DC/IaaS)



On-prem Contractor with Untrusted Device: Accessing Private Application (DC/IaaS)



On-prem Guest with Untrusted Device: Accessing Internet



Remote Employee with Trusted Device: Clientless Remote Access to Private Application (web/ssh/rdp) (DC/IaaS)



What is a MITRE? What is ATT&CK?

- Who is MITRE Corporation?
 - Not-for-profit, US company with multiple federally funded R&D centers (FFRDCs)
 - Public-private partnerships in many areas, including cybersecurity
 - Same folks who brought us CVE database/list
- What is ATT&CK
 - Adversarial Tactics, Techniques, and Common Knowledge
 - Born in 2013 to document tactics, techniques, and procedures (TTPs) that APTs use on Windows networks
 - Globally-accessible knowledge base
 - Used for the development of specific threat models & methodologies in the private sector, in government, and in the cybersecurity product and service community.

The MITRE logo consists of the word "MITRE" in a bold, blue, sans-serif font.The ATT&CK logo features the text "ATT&CK" in a large, bold, red, sans-serif font. Below it, the words "Adversarial Tactics, Techniques & Common Knowledge" are written in a smaller, black, sans-serif font. A small trademark symbol (TM) is located to the right of "ATT&CK".

ATT&CK Navigator a versatile tool for our needs



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (13)	Acquire Infrastructure (27)	Drive-by Compromise	Command and Scripting Interpreter (38)	Account Manipulation (19)	Abuse Elevation Control Mechanism (34)	Abuse Elevation Control Mechanism (34)	Adversary-in-the-Middle (33)	Account Discovery (24)	Exploitation of Remote Services	Adversary-in-the-Middle (33)	Application Layer Protocol (14)	Automated Exfiltration (23)	Account Access Removal
Gather Victim Host Information (14)	Compromise Accounts (21)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (30)	Access Token Manipulation (30)	Brute Force (14)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (24)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (23)	Compromise Infrastructure (17)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (114)	Access Token Manipulation (30)	Access Token Manipulation (30)	Credentials from Password Stores (14)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Obfuscation (12)	Exfiltration Over Alternative Protocol (21)	Data Encrypted for Impact
Gather Victim Network Information (14)	Develop Capabilities (14)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (30)	Boot or Logon Autostart Execution (114)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (14)	Automated Collection	Data Encoding (12)	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information (14)	Establish Accounts (23)	Phishing (21)	Inter-Process Communication (23)	Browser Extensions	Boot or Logon Initialization Scripts (30)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (18)	Browser Session Hijacking	Dynamic Resolution (20)	Exfiltration Over Other Network Medium (27)	Disk Wipe (10)
Phishing for Information (13)	Obtain Capabilities (24)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (114)	Create or Modify System Process (114)	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (22)	Exfiltration Over Physical Medium (14)	Endpoint Denial of Service (2)
Search Closed Sources (22)	Stage Capabilities (36)	Supply Chain Compromise (2)	Scheduled Task/Job	Create Account (17)	Domain Policy Modification (30)	Direct Volume Access	Input Capture (14)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Failback Channels	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Technical Databases (3)	Trusted Relationship	Valid Accounts (14)	Serverless Execution	Create or Modify System Process (114)	Domain Policy Modification (30)	Domain Policy Modification (30)	Multi-Factor Authentication Process (14)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (30)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Open Websites/Domains (2)	Valid Accounts (14)		Shared Modules	Event Triggered Execution (114)	Event Triggered Execution (114)	Execution Guardrails (30)	Multi-Factor Authentication Interception	Domain Trust Discovery	Use Alternate Authentication Material (24)	Data from Information Repositories (23)	Multi-Stage Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			System Services	Hijack Execution Flow (30)	Hijack Execution Flow (30)	File and Directory Permissions Modification (30)	Network Service Discovery	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
			User Execution (23)	Implant Internal Image	Process Injection (30)	Hide Artifacts (30)	Network Sniffing	Network Service Discovery		Data from Removable Media	Protocol Tunneling		System Shutdown/Reboot
			Windows Management Instrumentation	Modify Authentication Process (114)	Scheduled Task/Job (30)	Hijack Execution Flow (30)	OS Credential Dumping (14)	Network Share Discovery		Data Staged (22)	Proxy (22)		
				Office Application Startup (14)	Valid Accounts (14)	Indicator Removal (14)	Steal Application Access Token	Password Policy Discovery		Email Collection (20)	Remote Access Software		
				Pre-OS Boot (30)		Indirect Command Execution	Steal or Forge Authentication Certificates	Peripheral Device Discovery		Input Capture (14)	Traffic Signaling (27)		
				Scheduled Task/Job (17)		Masquerading (17)	Steal or Forge Kerberos Tickets	Permission Groups Discovery (13)		Screen Capture	Web Service (13)		
				Server Software Component (14)		Modify Authentication Process (114)	Steal Web Session Cookie	Process Discovery		Video Capture			
				Traffic Signaling (27)		Modify System Image (23)	Unsecured Credentials (27)	Query Registry					
				Valid Accounts (14)		Network Boundary Bridging (30)		Remote System Discovery					
						Obfuscated Files or Information (30)		Software Discovery (30)					
						Plist File Modification		System Information Discovery					
						Pre-OS Boot (30)		System Location Discovery (30)					
						Process Injection (30)		System Network Configuration Discovery					
						Reflective Code Loading		System Network Connections Discovery					
						Rogue Domain Controller		System Owner/User Discovery					
								System Service Discovery					
								System Time Discovery					
								Virtualization/Sandbox Evasion (30)					

- <https://mitre-attack.github.io/attack-navigator/>

Financial Service

Bank in South Africa increases visibility of key payment systems

Threat Modelling Assessment – Cisco mapped key payment applications using tools such as STRIDE, ATT&CK and CAPEC to model the Cyber Kill Chain to determine gaps in visibility, segmentation, remediation and threat protection.



South Africa Bank Engagement Outcome

- Solid Zero Trust workflow for key payment systems
 - Good segmentation for branches with ATM machines and terminals
 - Deployed Secure Workload for app/data protection
 - Traffic analysis for policy creation
- Futures
 - Run live data against updated policy
 - Leverage vulnerability management features to identify gaps

Transport Network

European airport wants to assess resilience of key safety and logistics systems

Threat Modelling Assessment – Cisco used threat modelling to identify scope and map likely cyber physical attack paths using ATT&CK allowing purple team assessment coverage to be planned, agreed and communicated with key SMEs in advance of impactful technical assessment activities.



Customer wanted to safely ask “what if?” based on real world scenarios

Complexity, safety and time concerns prevent full scope testing approach



Answer the question “is a given attack feasible and if so, how?”

Enabled prioritised testing of scenarios likely to result in a ransomware incident



European Airport Engagement Outcome

- One of the most mature customer architectures CX has seen
 - Proper segmentation
 - Least privileged access
 - Very capable SOC; detected keyboard mapping changes
- Gaps
 - Potential Application/Data vulnerabilities (out of scope)
 - Certain critical apps supported by 1 dedicated person
 - Lack App/Data Recovery plans

Summary

Value of a Security architecture

Here's what we're seeing:

Relationships and Dependencies



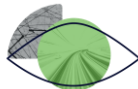
$$1 + 1 > 3$$

Drivers



Security Controls for risk management

Operations and Monitoring



Faster Time to detect

Benefits



Standardization for cost effectiveness

Objectives achieved



Understand the overall value and benefits of having a security reference architecture



Understand Cisco architecture alignment to industry frameworks



Apply use cases such as Zero Trust, SASE, XDR, and others



Threat Modeling of your security architecture

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session and the overall event surveys to claim a Cisco Live merchandise.

SCORE = EXCELLENT (5)



Continue your education



- Visit the Cisco Showcase 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background of the slide is a vibrant, abstract graphic. It features a large, stylized cloud shape on the left side, composed of overlapping, semi-transparent layers of orange, red, and yellow. To the right of the cloud, a bright, multi-colored sunburst or starburst pattern radiates outwards, transitioning through a spectrum of colors including yellow, green, blue, and purple. The overall effect is energetic and celebratory.

cisco *Live!*

Let's go

#CiscoLiveAPJC