

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

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

## Cisco Security Reference Architect Overview

Jamey Heary, Distinguished Security Architect

CCIE #7680

BRKSEC-1240



#CiscoLive

# Cisco Webex App

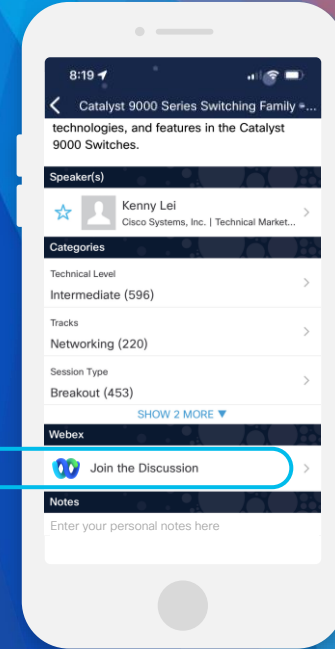
## Questions?

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 June 9, 2023.



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

# Agenda

- What is an architecture and why
- Cisco Security Reference Architecture
- Use cases with demos!
- Conclusion

# Objectives

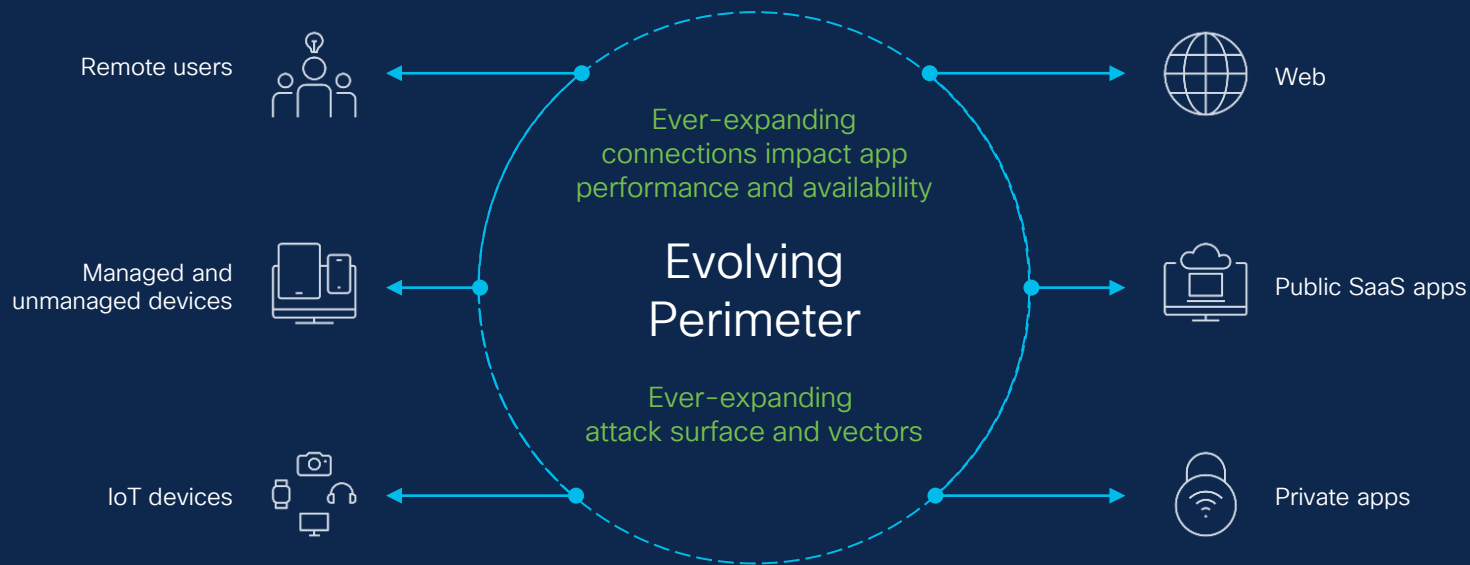
- Understand the overall value of having a security reference architecture
- Understand Cisco architecture alignment to industry frameworks
- Highlight use cases such as Zero Trust, application segmentation, XDR, and others
- See use case demonstrations in real-world environments

# Major Shifts in IT Landscape

Users, devices and apps are everywhere

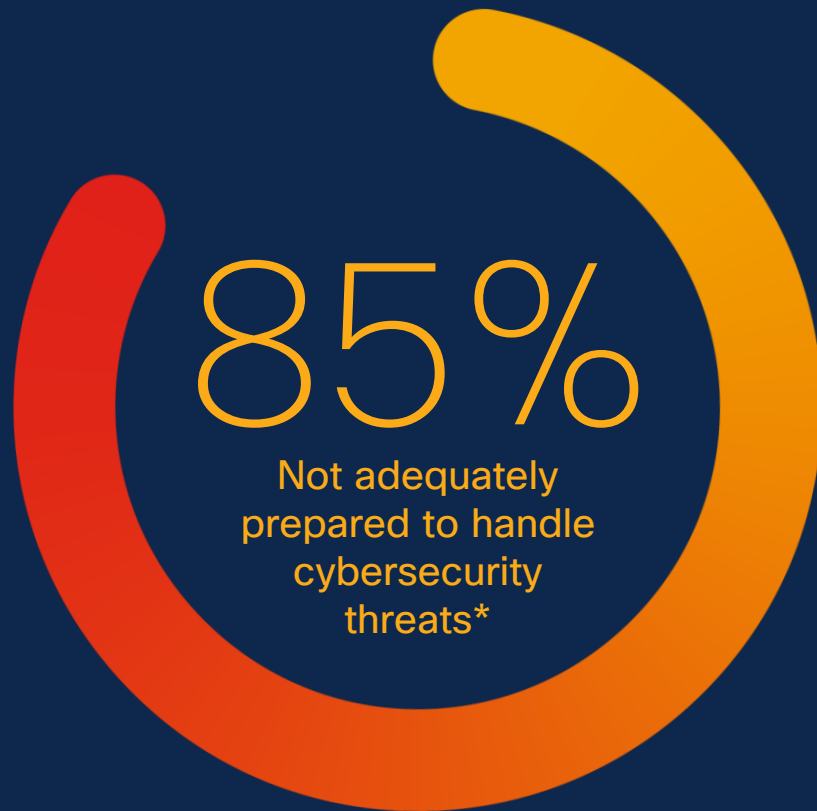
Hybrid work is the norm

Transition to multicloud and SaaS



# Hybrid work era creates unmanageable risk

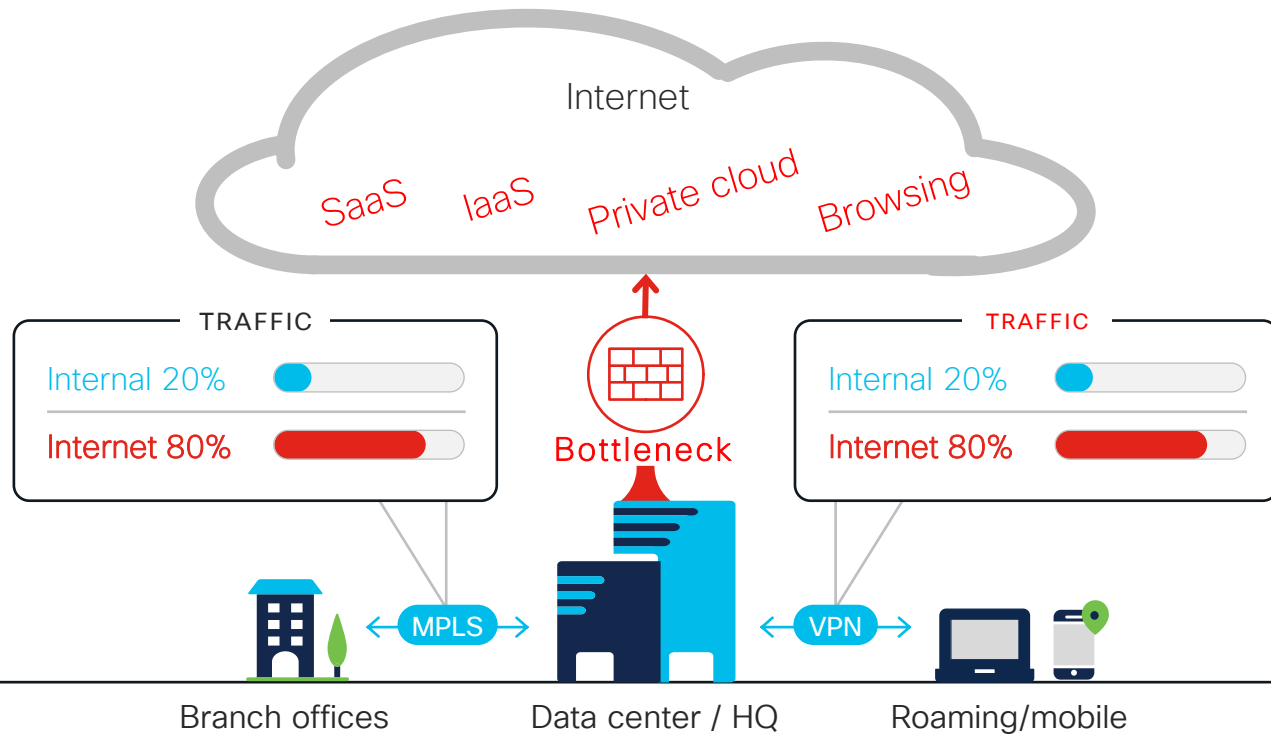
Your organization's security wasn't designed for a hyper-distributed model



\* Source: Cybersecurity Readiness Index – Cisco: March, 2023

# Inverted Traffic Model vs 5 years ago

## Changes in Types of Traffic, Origins and Destinations



### Problems:

- Experience
- Costs
- Performance
- Integrations
- Maintenance



# Current patchwork approach exacerbates the problem

More products leads to more complexity within your business and IT environment

Exfiltration  
Ransomware  
Lateral movement  
Web threats  
Stolen credentials  
Spam



76

Average number of security tools used per enterprise today\*

19%

Increase in last 2 years driven by cloud and remote work\*

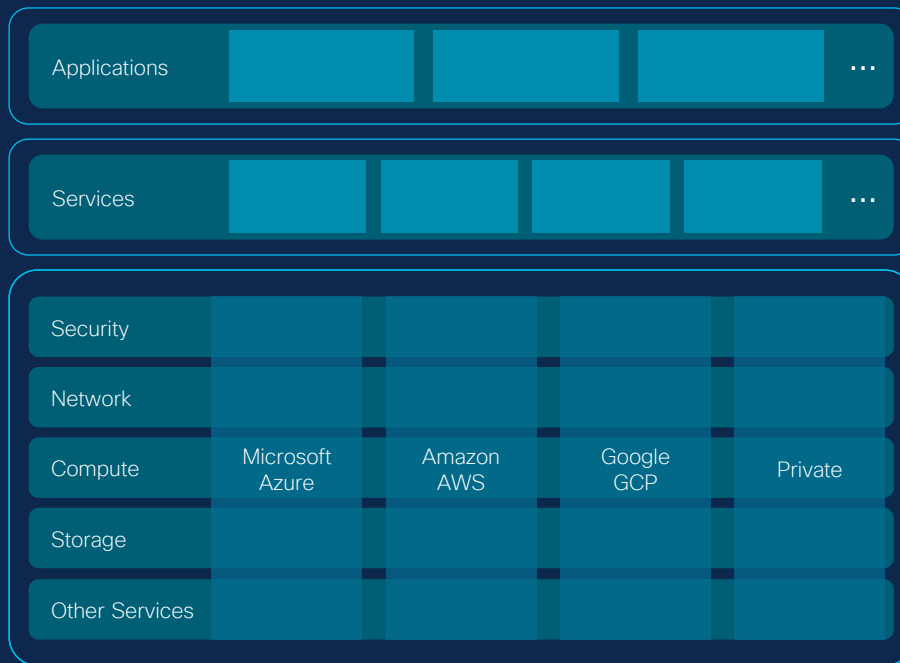
New threats spawn new vendors, putting the burden on customers

# Hybrid Multicloud Future

Software as a Service

Platform as a Service

Infrastructure as a Service



Expect a different patchwork of security tech in a multicloud world



# Cisco Security Cloud

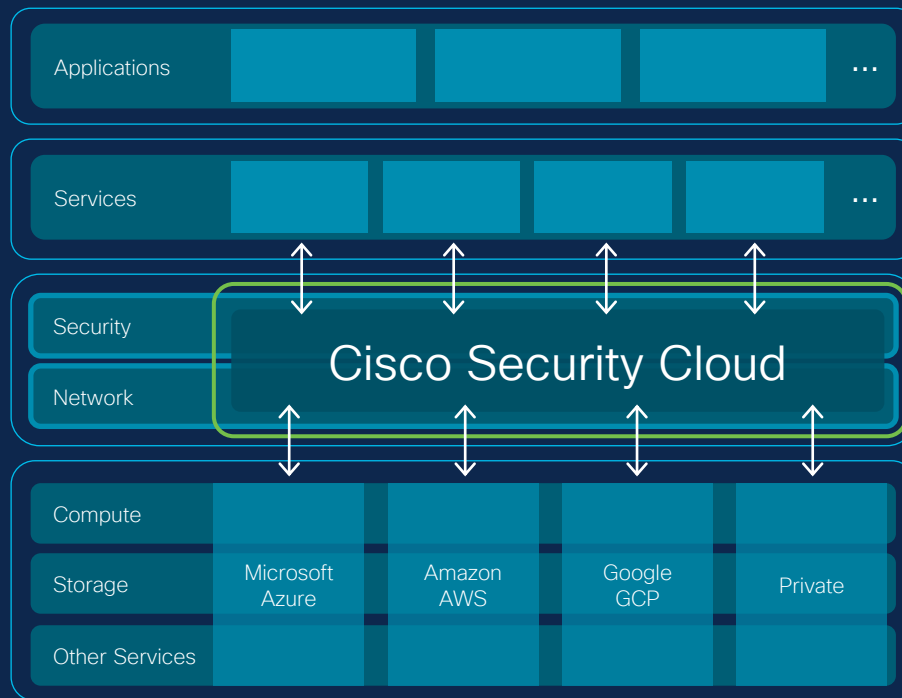
Software as a Service

Platform as a Service

Security & Networking as a Service

Optimizes performance & security of every connection

Infrastructure as a Service



# Security that only Cisco can deliver for you

Backed by unrivaled threat intelligence

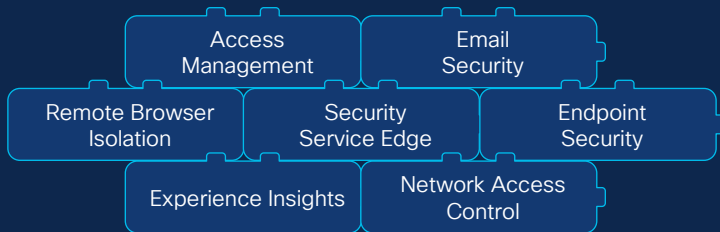
## Talos Threat Intelligence

### Breach Protection

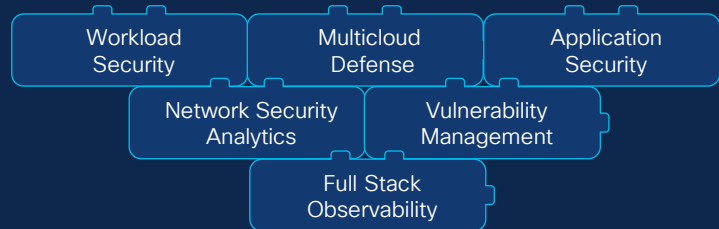
Powered by Talos, the world's most trusted commercial threat intelligence team

Extended Detection & Response

### User Protection



### Cloud Protection



## Firewall Protection

Cisco Security Cloud

# Cisco Talos: Best of Breed Threat Intel

## Leading Threat Intelligence

**625B** web requests per day  
**200+** vulnerabilities discovered per year  
**1.4M+** new malware samples per day  
**30B** endpoint events per day



## Founded in Fighting the Good fight

**Global Threat Hunting Team (500+)**  
**43** languages  
**60+** government and law enforcement partnerships  
**30K** critical infrastructure endpoints monitored in Ukraine

## Raising the Bar for Defensive Technology

**1.7M** networks protected  
**50M** mailboxes protected  
**87M** endpoints protected



It's segmentation



It's ZTNA



It's endpoint security



It's firewall



It's identity

Zero Trust  
means **different**  
**things** to different  
people

We believe Zero  
Trust is a  
METHODOLOGY  
not a product

## ZT Defined





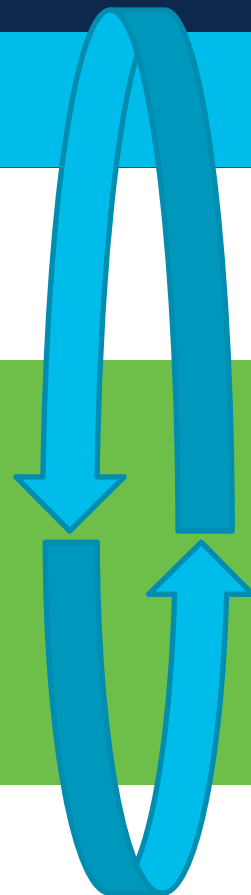
## Threat Detection and Intelligence

Visibility, Analytics, Automation & Response

User & Device

Network & Cloud Edge Environment

Workload, Application, and Data





**TALOS THREAT INTELLIGENCE**



Actionable threat intelligence



Collective responses



Comprehensive visibility



Signal identification



Threat research & analysis

**XDR SECURITY OPERATIONS TOOLSET**

**SERVICES**



Custom threat research on demand



Implement and manage



Incident response retainer



Managed detection & response



Strategy & assessment

Kenna | Secure Analytics | Cisco XDR  
Secure Client | Talos Incident Response

**CAPABILITIES**



Network detection & response



Device discovery & insights



Endpoint detection & response



Open API platform & 3rd party native integrations



Risk-based vulnerability management



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, Posture, Telemetry/Visibility, Endpoint detection & response, DNS-layer security, Secure Web, Anti-virus/Anti-malware, Query, Host FW, Mobile device management

Risk-based MFA, Passwordless, Device trust, Continuous trust

Email, Phishing, SPAM, BEC, DLP, content filtering, Digital experience monitoring

**Cloud Edge Network**

**SASE/Security Service Edge**

Duo | Secure Connect | Umbrella

Browser access control, Cloud access security broker, Cloud malware detection, Data loss prevention, DNS-layer security, Identity/posture, FWaaS, RAaaS, Remote browser isolation, Secure web gateway, Tenant restrictions, TLS decryption, Zero Trust Network Access

**On-Premises Network**

**SASE/SDWAN**

Meraki | Secure Firewall  
ThousandEyes | Viptela

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

**In the Office/Managed Location**

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

Application network gateway, Configuration orchestration, Content filtering, Encrypted visibility, 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

**HYBRID MULTI-CLOUD: Workload, Application, and Data Security**

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

**THREAT INTELLIGENCE**



Actionable threat intelligence



Collective responses



Comprehensive visibility



Signal identification



Threat research & analysis

**XDR SECURITY OPERATIONS TOOLSET**

**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



Security analytics



Security orchestration, automation & response



Threat visibility, incident response & threat hunting

**ZERO TRUST**

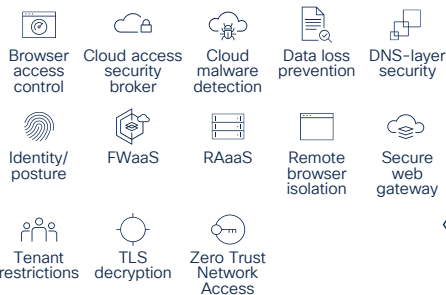
**SASE**

**User/Device Security  
SASE/REMOTE WORKER**



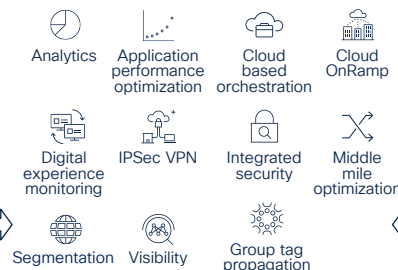
**Cloud Edge Network**

**SASE/Security Service Edge**



**On-Premises Network**

**SASE/SDWAN**



**In the Office/Managed Location**




**Industrial Threat Defense**



**Workload, Application, and Data Security  
HYBRID MULTI-CLOUD**



# WINNING

A man in a black suit and sunglasses strikes a confident pose in a hallway. He is standing with one leg bent and arms crossed, looking directly at the camera. The hallway is long and brightly lit, with a large doorway at the end. The word "WINNING" is written in large, bold, white letters at the top of the image.

- Live!



# Industry Alignment



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



# SABSA

## Sherwood Applied Business Security Architecture (2009)

- Focused on theory and process, not controls or tech
- Everything must be derived from an analysis of the business requirements for security and risk management, especially those in which security has an enabling function through which new business opportunities can be developed
- Being a successful security architect means thinking in business terms at all times

Table 1: Layered Architecture Views

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

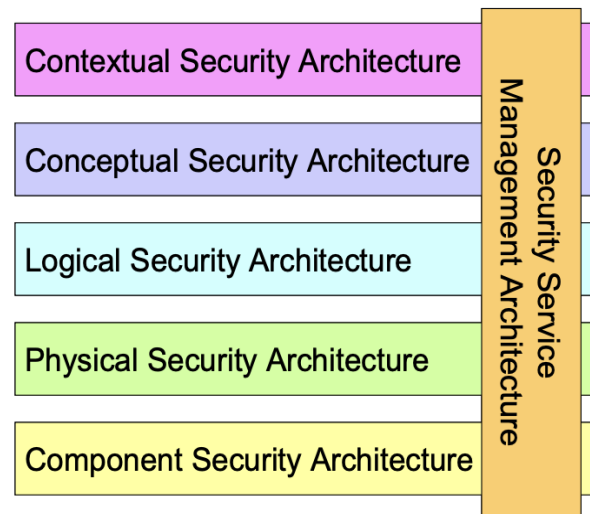


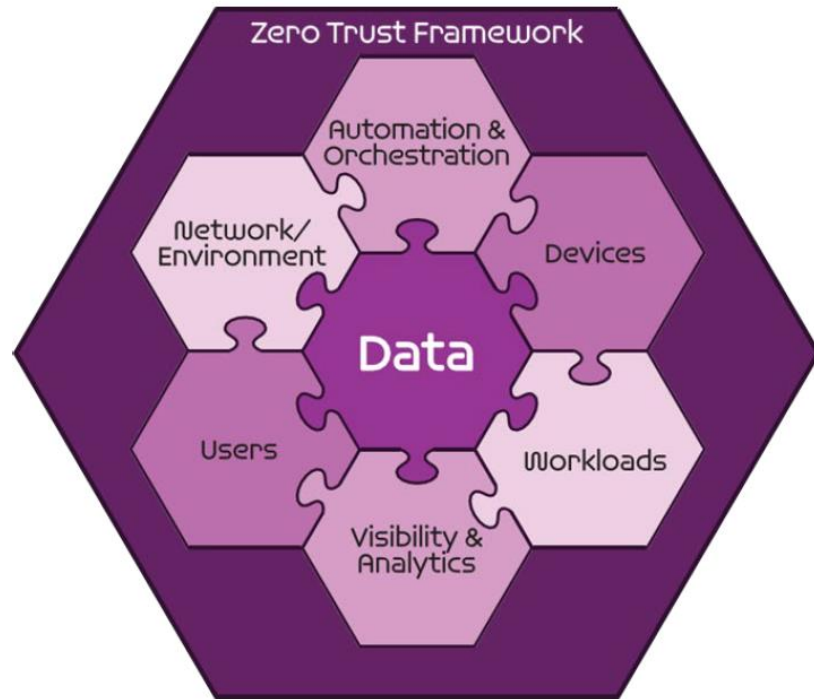
Figure 1: The SABSA Model for Security Architecture

# DISA Zero Trust Framework

Defense Information Systems Agency



- 7 pillars of DoD ZT Architecture
- Prepared by DISA and NSA, 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)

# CISA, Zero Trust Maturity Model 2.0

Based on NIST SP 800-207

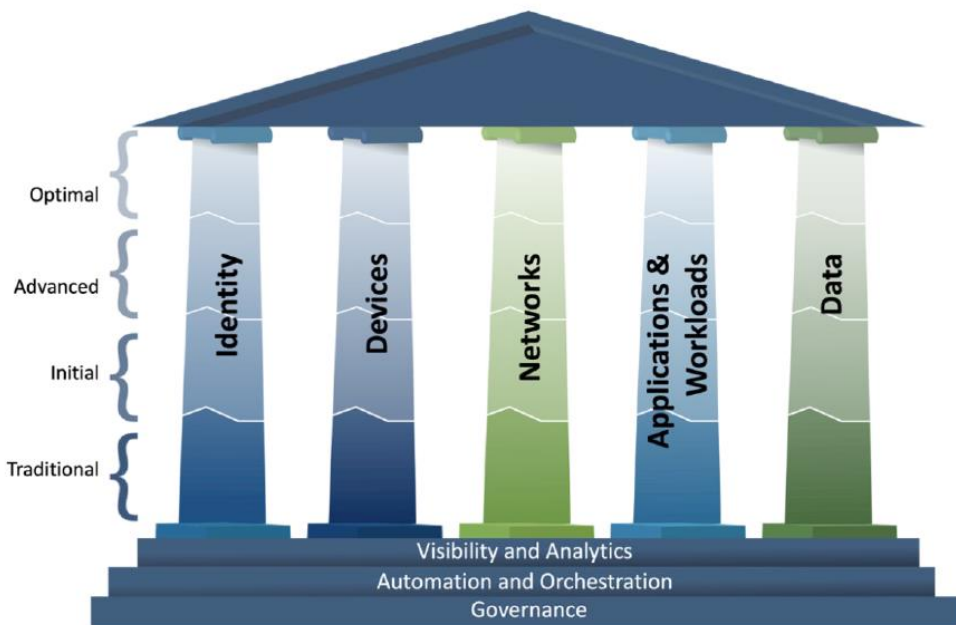
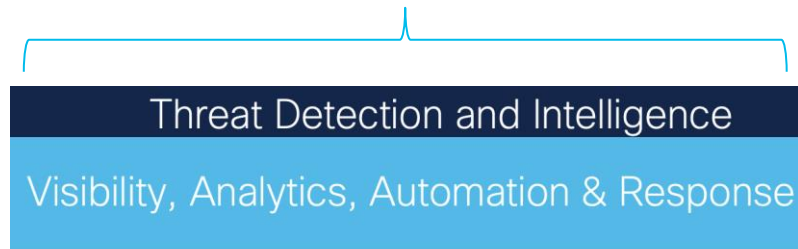


Figure 3: Zero Trust Maturity Evolution

U.S. Cybersecurity & Infrastructure Security Agency  
CISA framework is widely adopted

[https://www.cisa.gov/sites/default/files/2023-04/zero\\_trust\\_maturity\\_model\\_v2\\_508.pdf](https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf)

## Cisco SRA



User & Device



Workload, Application, and Data

# Security Architecture Frameworks

Cisco	NIST 800-207 Zero Trust Architecture	CISA Zero Trust Maturity Model	DISA Zero Trust Framework
User and Device Security	Users and/or Devices	Identity	Users
		Devices	Devices
Network and Cloud Security	Policy Decision and Enforcement Points	Networks	Network/Environment
Application and Data Security	Enterprise Resources	Applications and Workloads	Workloads
		Data	Data
Commons: Visibility & Analytics, Automation & Orchestration, Governance, Threat Intel			





## TALOS THREAT INTELLIGENCE

Actionable threat intelligence   Collective responses   Comprehensive visibility   Signal identification   Threat research & analysis

## XDR SECURITY OPERATIONS TOOLSET

### SERVICES

Custom threat research on demand   Implement and manage   Incident response retainer   Managed detection & response   Strategy & assessment

Kenna | Secure Analytics | Cisco XDR  
Secure Client | Talos Incident Response

### CAPABILITIES

Network detection & response   Device discovery & insights   Endpoint detection & response   Open API platform & 3rd party native integrations   Risk-based vulnerability management   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   Posture   Telemetry/Visibility   Endpoint detection & response   DNS-layer security   Secure Web   Anti-virus/Anti-malware   Query   Host FW   Mobile device management   Risk-based MFA   Passwordless   Device trust   Continuous trust   Email, Phishing, SPAM, BEC, DLP, content filtering   Digital experience monitoring

### Cloud Edge Network

#### SASE/Security Service Edge

Duo | Secure Connect | Umbrella

Browser access control   Cloud access security broker   Cloud malware detection   Data loss prevention   DNS-layer security   Identity/posture   FWaaS   RAaaS   Remote browser isolation   Secure web gateway   Tenant restrictions   TLS decryption   Zero Trust Network Access

### On-Premises Network

#### SASE/SDWAN

Meraki | Secure Firewall  
ThousandEyes | Viptela

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

#### In the Office/Managed Location

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

Application network gateway   Configuration orchestration   Content filtering   Encrypted visibility   Group tag classification   Identity/pxGrid Cloud   Network access control   Network security analytics   NGFW   NGIPS   Security analytics & logging   Segmentation   Threat mitigation   Profiling

#### Industrial Threat Defense

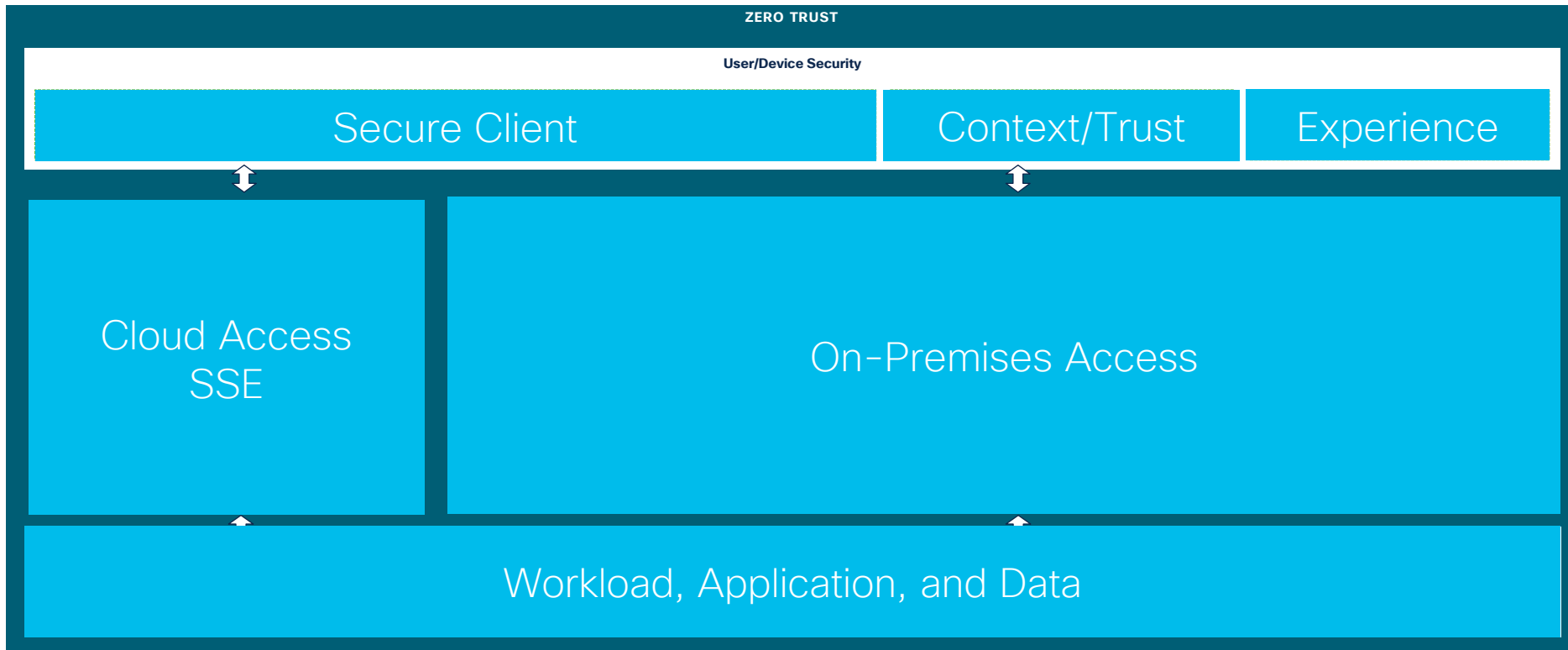
DNAC | CyberVision | Industrial Networking  
ISE | Secure Firewall | Secure Network Analytics

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

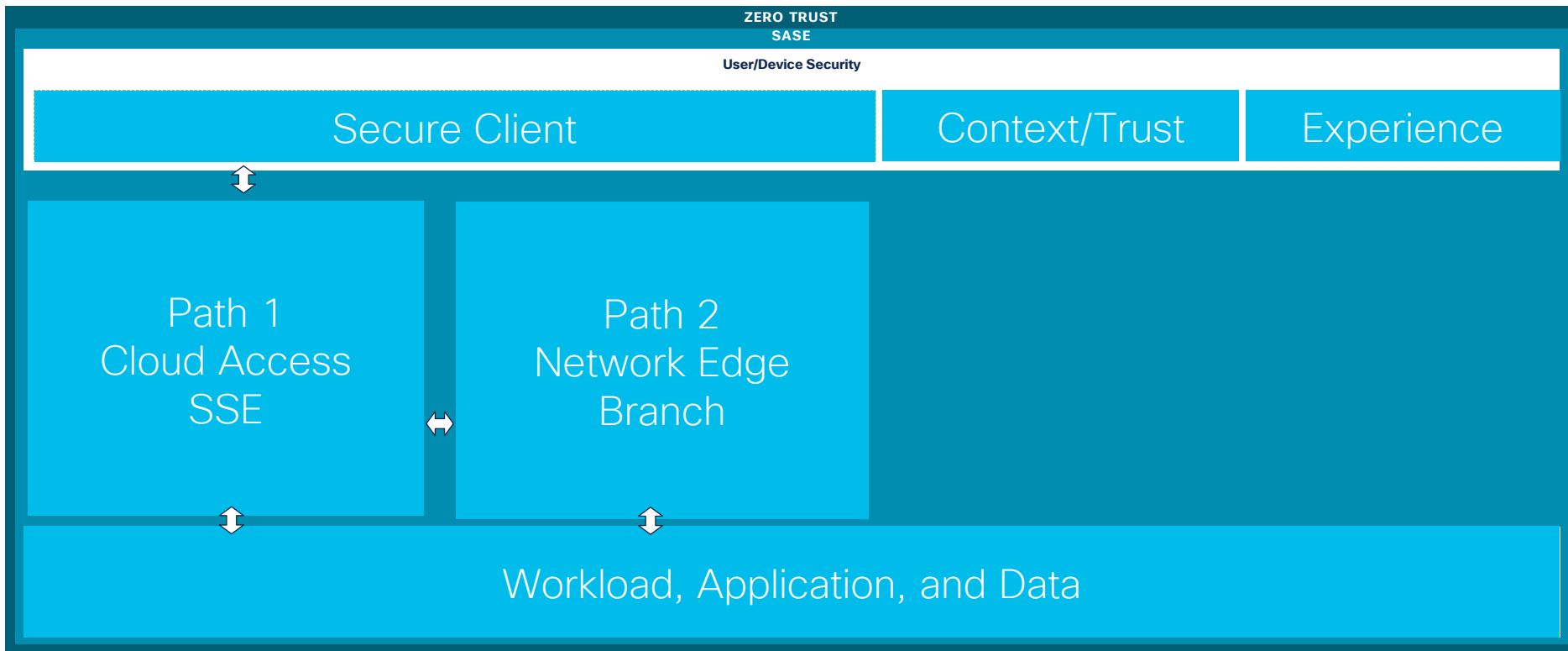
## HYBRID MULTI-CLOUD: Workload, Application, and Data Security

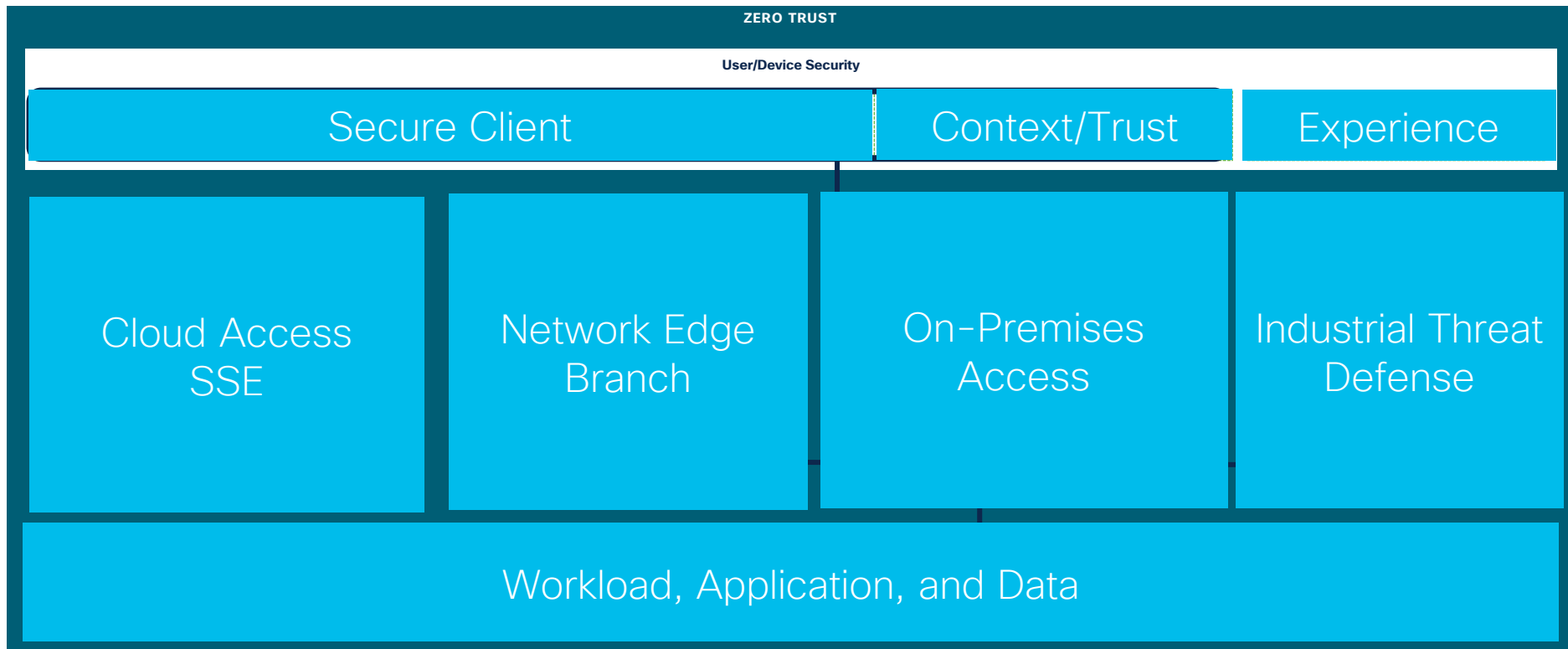
Anti-virus/Anti-malware   API security   App discovery   Cloud analytics   Cloud Native Security   Cloud Posture Management   DDoS, WAF/Bot   Identity/pxGrid   Micro/Macro Segmentation   Run-time Protection   Telemetry   Threat mitigation   Visibility   Data access & Integrity

# Security Reference Architecture – Zero Trust



# Security Reference Architecture – SASE





# Security Reference Architecture – Security Operations with XDR

## TALOS THREAT INTELLIGENCE



Actionable threat intelligence



Collective responses



Comprehensive visibility



Signal identification



Threat research &amp; analysis

## XDR SECURITY OPERATIONS TOOLSET

### SERVICES



Custom threat research on demand



Implement and manage



Incident response retainer



Managed detection &amp; response



Strategy &amp; assessment

Kenna | Secure Analytics | SecureX  
Secure Client | Talos Incident Response

### CAPABILITIES



Network detection &amp; response



Device discovery &amp; insights



Endpoint detection &amp; response



Open API platform &amp; 3rd party native integrations



Risk-based vulnerability management



Security analytics



Security orchestration, automation &amp; response



Threat visibility, incident response &amp; threat hunting

Secure Client

Context/Trust

Experience

Cloud Access  
SSESASE  
Network Edge  
BranchOn-Premises  
Managed LocationIndustrial  
Security

Workload, Applications, and Data

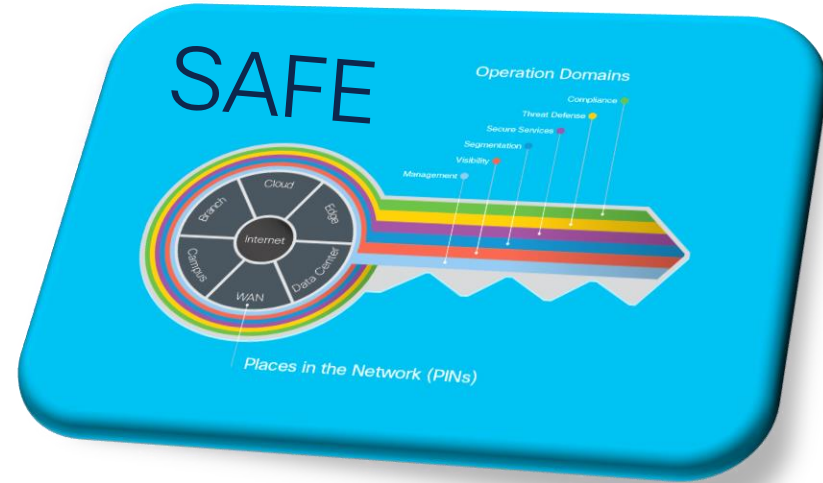
Designing a reference  
architecture

Cisco SAFE



# The Cisco SAFE Method

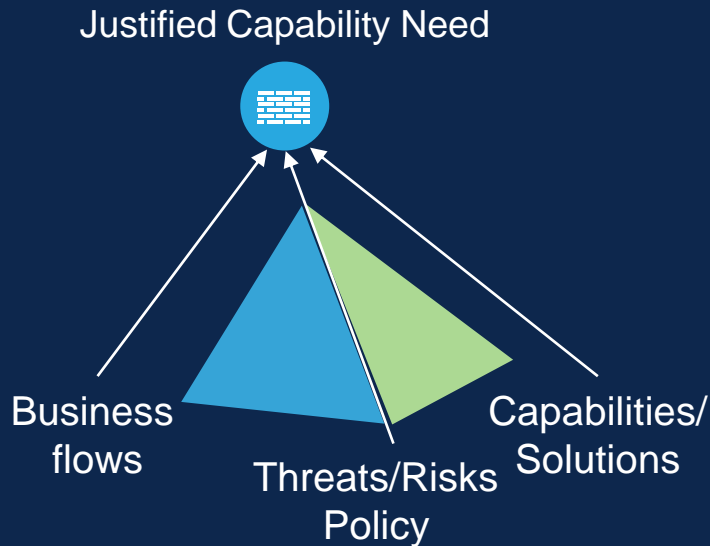
- Conceived specifically to improve security architecture design
- Security-Centric not Network-Centric
- Shows precisely how your business processes are secured from risks and threats
- Takes a security capabilities first based approach



# How Does SAFE Work?

A **Security-Centric** methodology for designing an effective Security Architecture

- Vendor agnostic process
- Focuses on protecting critical **business flows**
- Map risks, threats and policy needs to mitigating **capabilities**
- Map capabilities to **solutions**
- Backed by Cisco SAFE **Validated Design** guides and collateral.





# Security resilience is about securing the Business

- Too often, we don't relate security design to the business processes
- Investigate Business Processes and risk; not products and placement



**Use case:** Protect payment application

**Flow:** Clerk processing credit card transaction



**Use case:** Secure Remote Workers

**Flow:** Remote employee accessing public SaaS  
Application

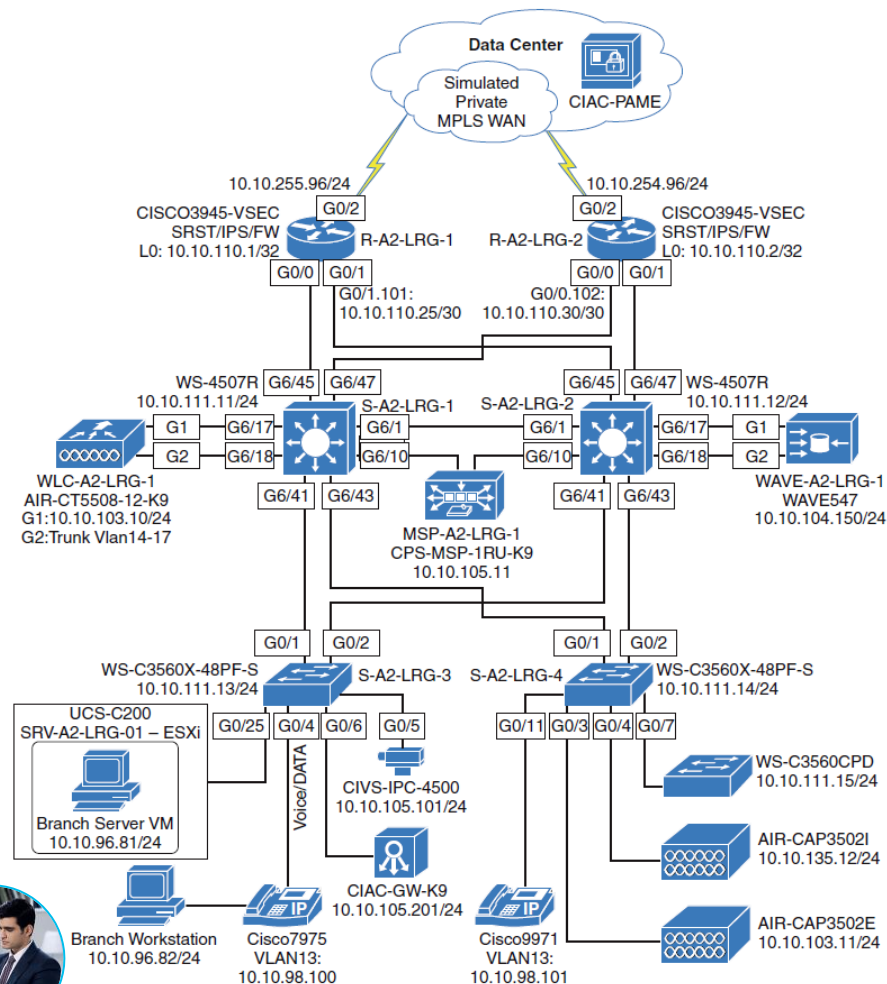
The standard “network centric” approach to design is not wrong, it’s just **not security-centric**

Where is the Security?

What are the critical business processes?

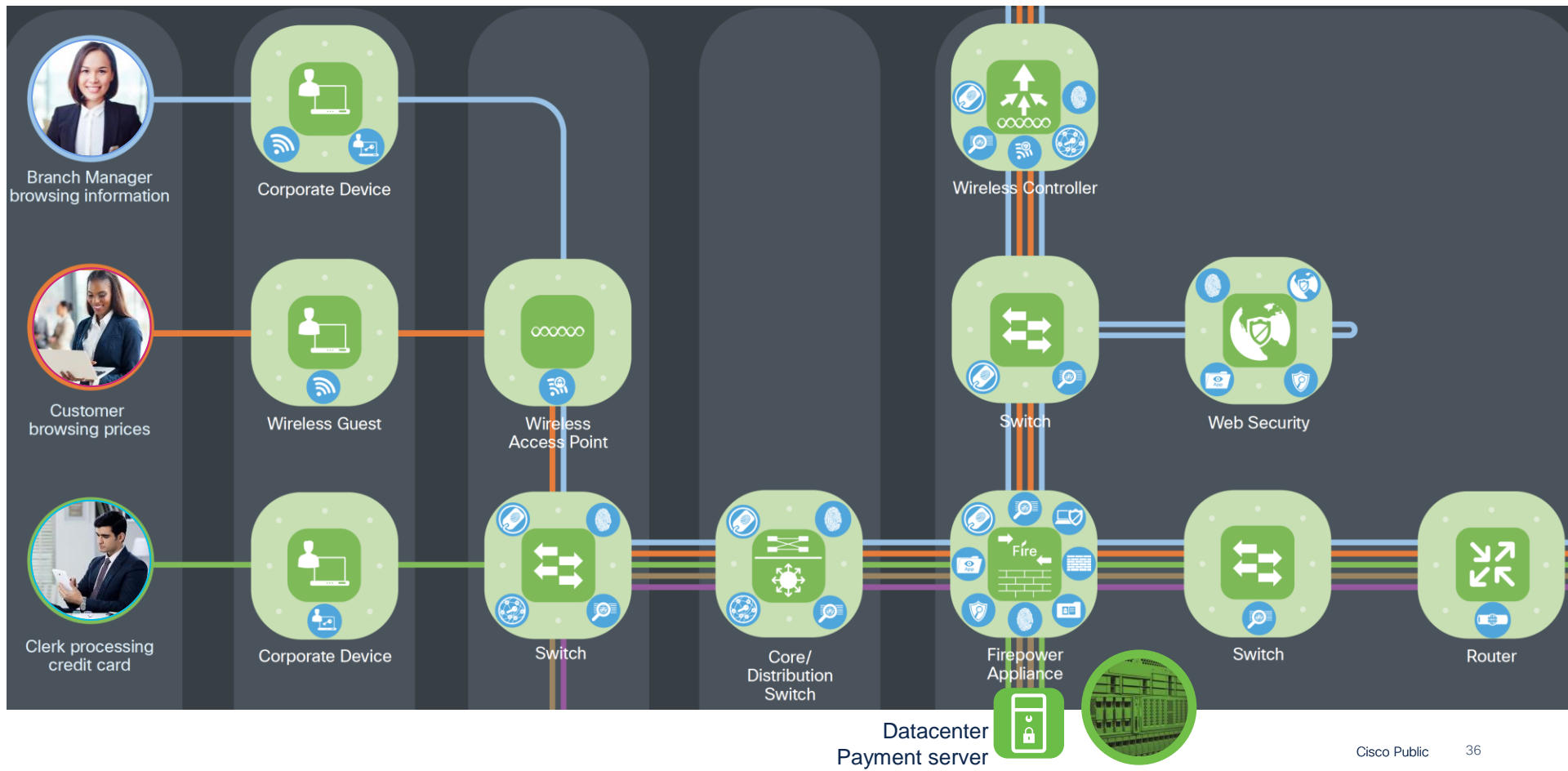
How are they secured?

Clerk processing credit cards

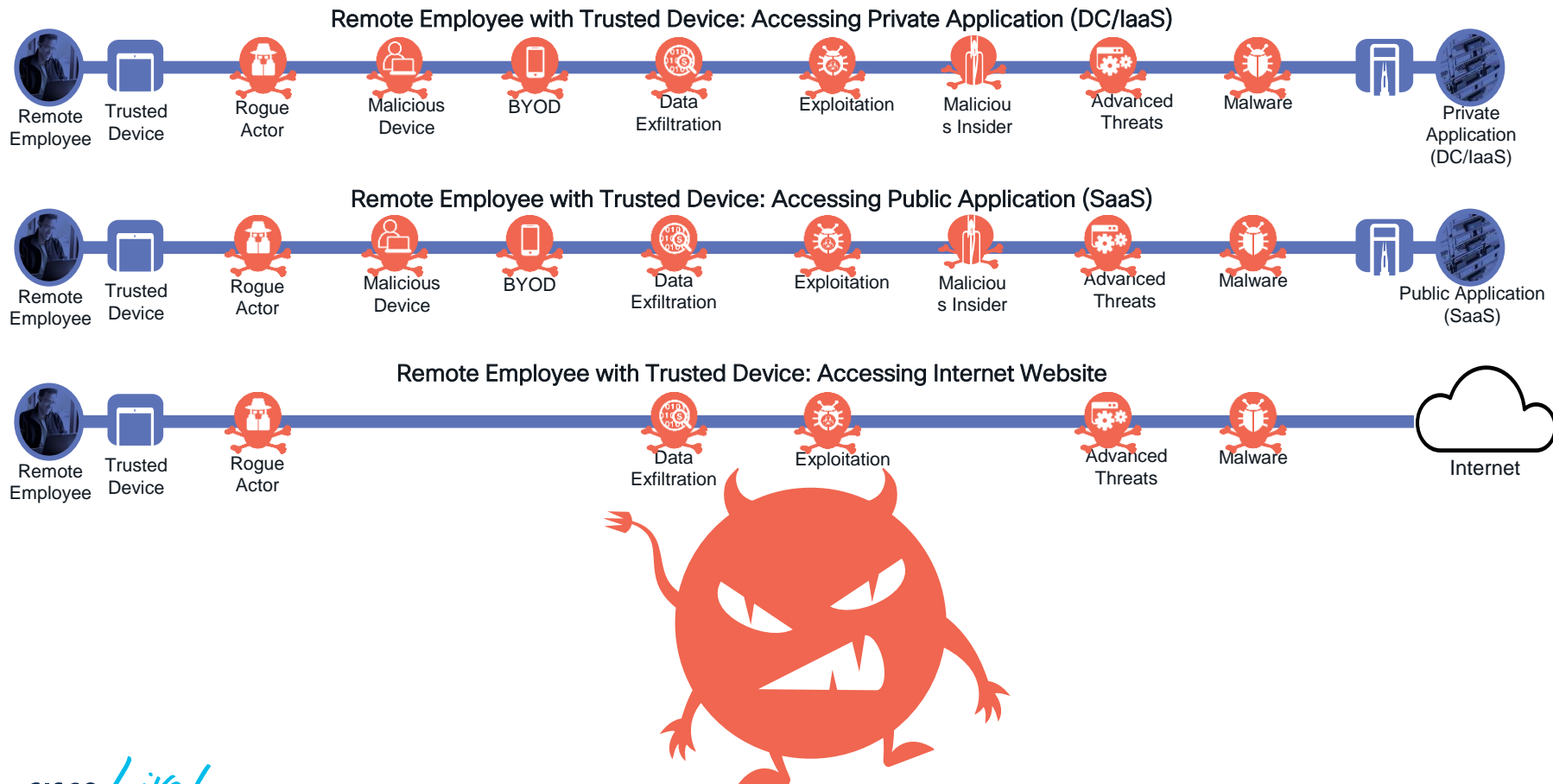


# Cisco SAFE Architecture Phase

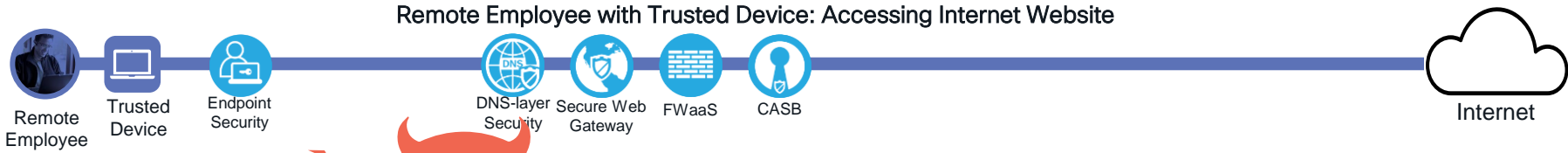
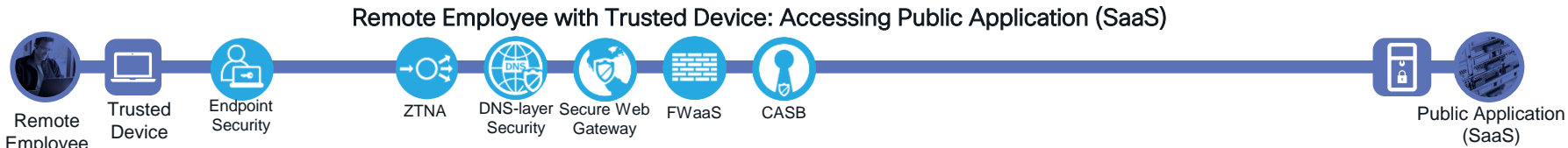
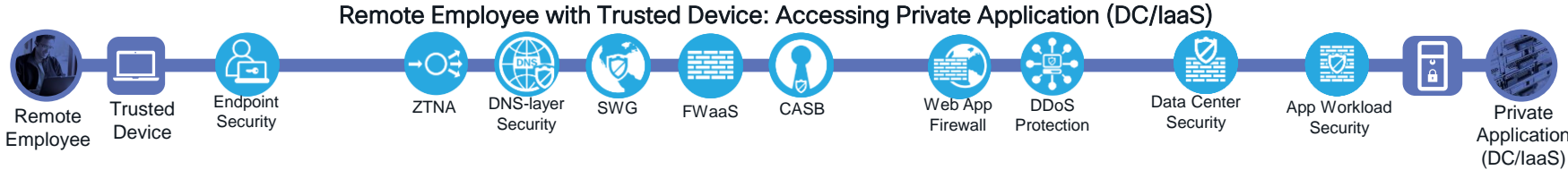
Security design relevant to the business



# SASE/SSE Remote Employee Business Flows with Threats



# SASE/SSE Remote Employee Business Flows with Security Capabilities



**Common Flow Capabilities**

Digital Experience Monitoring    Flow Analytics    Anomaly Detection    Threat Intelligence    SOAR

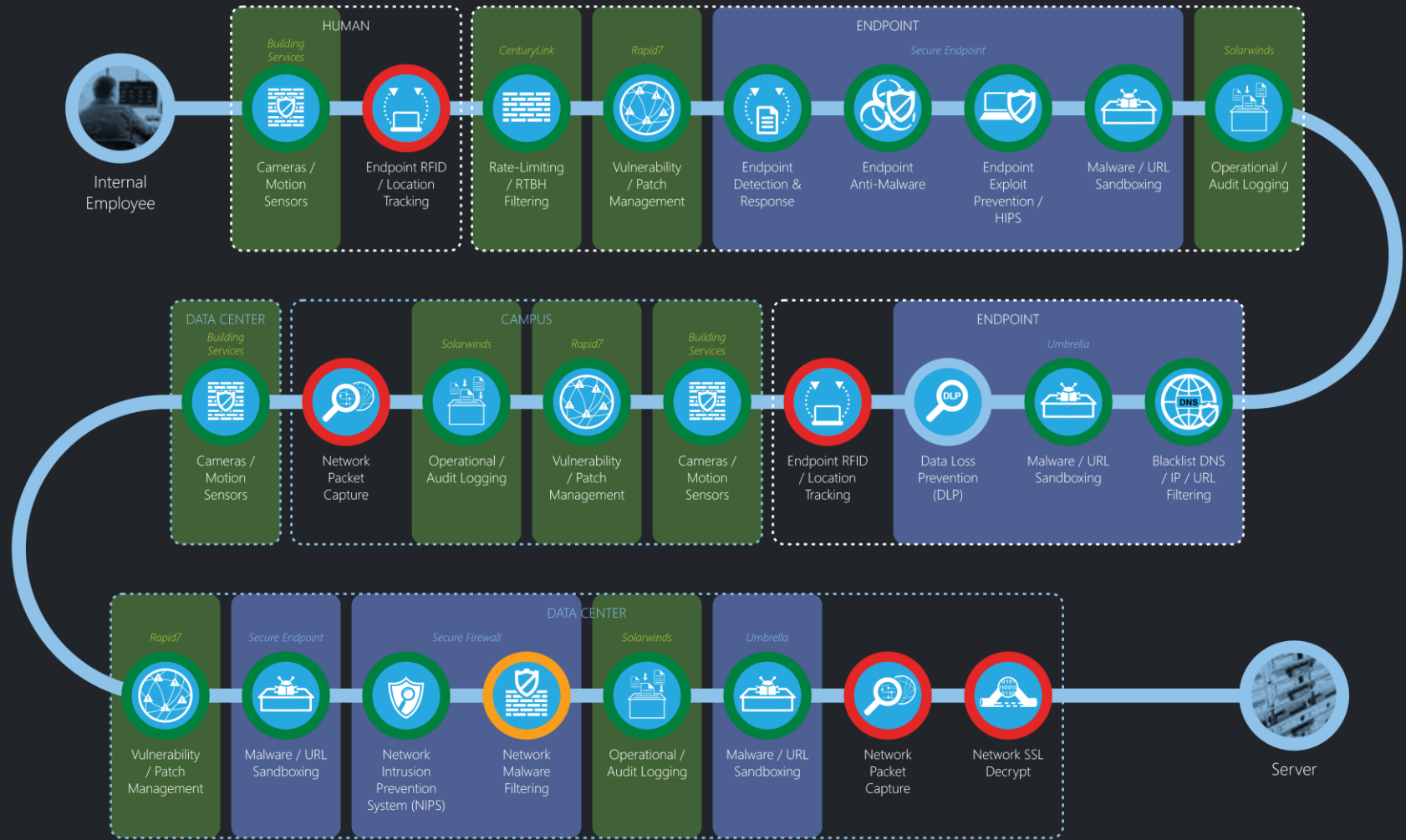
Hack the stack, have FUN with it!

**cisco** *Live!*

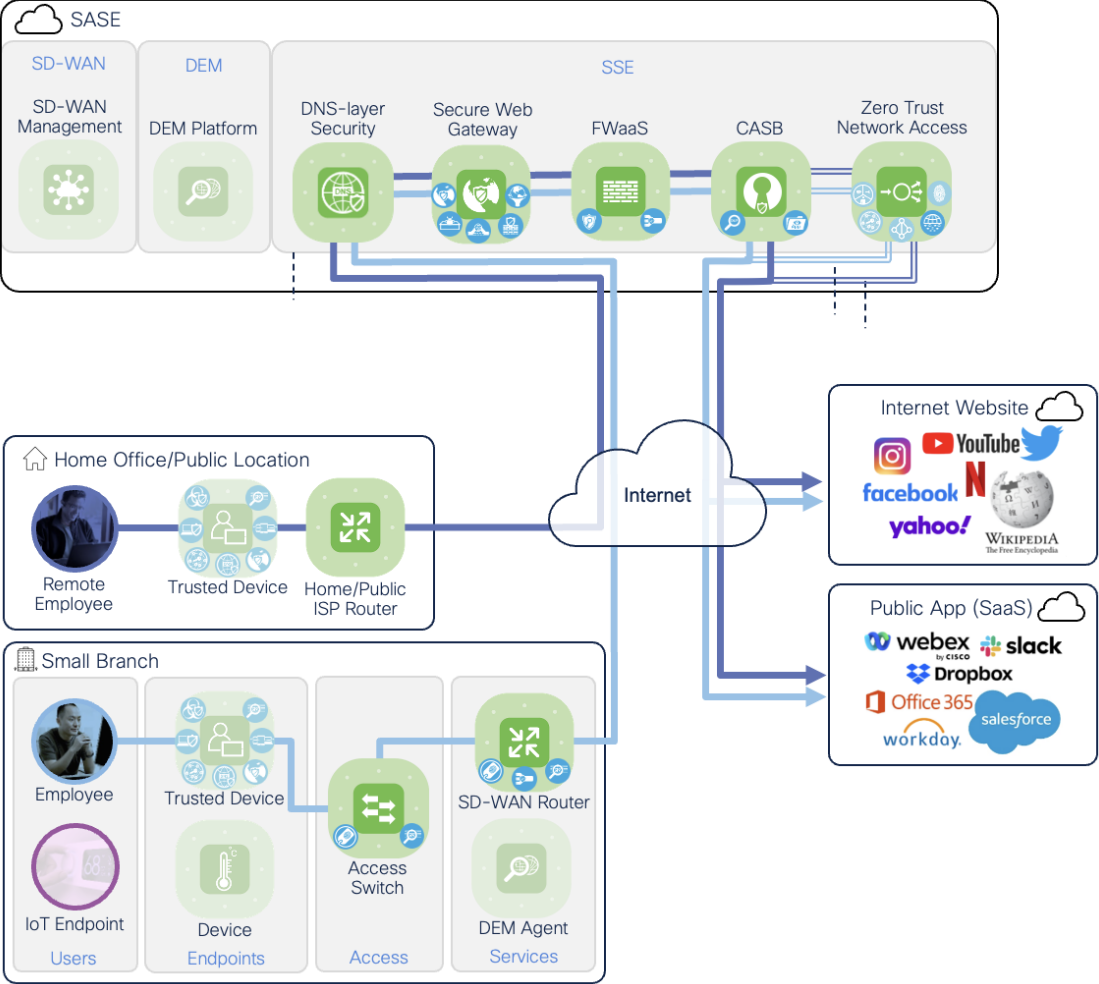
# Gap Analysis

Example  
Zero Trust  
Detection:  
Internal  
Employee  
to Critical  
Server

-  Solution Success
-  Challenges / Deficiencies
-  Not deployed or successful



# Remote Employee /Trusted Device: Accessing Public Application (SaaS)



# Risk & Compliance Tool Demo

The screenshot shows a web browser window displaying the 'Risk and Compliance Tool' interface. The browser's address bar shows 'frameworktool.cisco.com'. The page has a dark blue header with navigation links: 'Risk and Compliance Tool', 'SAFE Architect', 'SAFE Risk', 'Product', 'Framework', and 'Business Need'. The main content area features a large graphic with the text 'Risk and Compliance Tool' and 'Increase consultative value add with risk based security design'. To the right of this text is a complex flowchart with multiple interconnected nodes and arrows, representing a risk-based security design process. Below the main content area, there are two distinct sections. The left section is titled 'SAFE Workshops' and includes a sub-section 'SAFE Architect' with the text 'Gap Analysis Based on Cisco SAFE Reference Architectures'. The right section is titled 'Framework Mapping' and includes a sub-section 'Product' with the text 'Guide organizations in achieving their compliance goals with Cisco solutions'.



# Cisco Recommendations Based on Workshop

## Stop-Gap Summary

Priority / Cost	Capabilities	Recommend Solution/Product
-----------------	--------------	----------------------------

1 / Free

En

2 / Free-Low

Est

AC

3 / Free

Est

of

4 / Free

Ful

5 / Free

Us

sys

## SAFE: Short Term Recommendations

Priority / Cost	Capabilities
-----------------	--------------

1 / Low

Centrally collect both netw

2 / Medium

Further Deploy Duo to prot  
Applications

3 / High

Hire or establish dedicated  
personnel

4 / Med-High

DDoS Mitigation Service

5 / Med-Low

Consider additional Umbre  
Proxy) for critical remote e

6 / Low

Enable Endpoint Visibility f

## SAFE: Long Term Recommendations

Priority / Cost	Capabilities	Solution/Product
-----------------	--------------	------------------

1 / Medium

SSL Decrypt + Network Anti-malware protecting  
devices without endpoint security

Cisco Secure [SSLi](#), Umbrella

2 / Low

Deploy Separate AD structure for OT Network

Microsoft AD

3 / Low

Fully Segment BES/PCS Networks and SSIDs

Cisco ISE, Firewall/Switch ACLs, SGT, Wireless

4 / Med-High

Data Center Application Dependency Mapping /  
Whitelisting

Cisco Tetration

5 / Medium

Additional Door Access Controls

Physical Security Vendor

6 / Med-Low

Establish Endpoint Posture Assessment and/or  
Machine Certificate Based Authentication for OT  
Network Access

Cisco [Anyconnect](#) / ISE

7 / Medium-Low

Establish PKI for Wired Network, User/Machine  
Auth

Microsoft CA / Cisco ISE

8 / Medium

Cloud Network Analytics

Cisco Secure Analytics (Cloud or Network)

7 / Medium

Cloud Access Security Broker (CASB)

Cisco Cloudlock

Introduction to Cisco SAFE - BRKSEC-1027

Albra Welch, Solutions Architect, Cisco Systems, Inc.

Schedule

Monday, Jun 5 | 1:00 PM - 2:00 PM PDT | Level 2, Breakers DJ

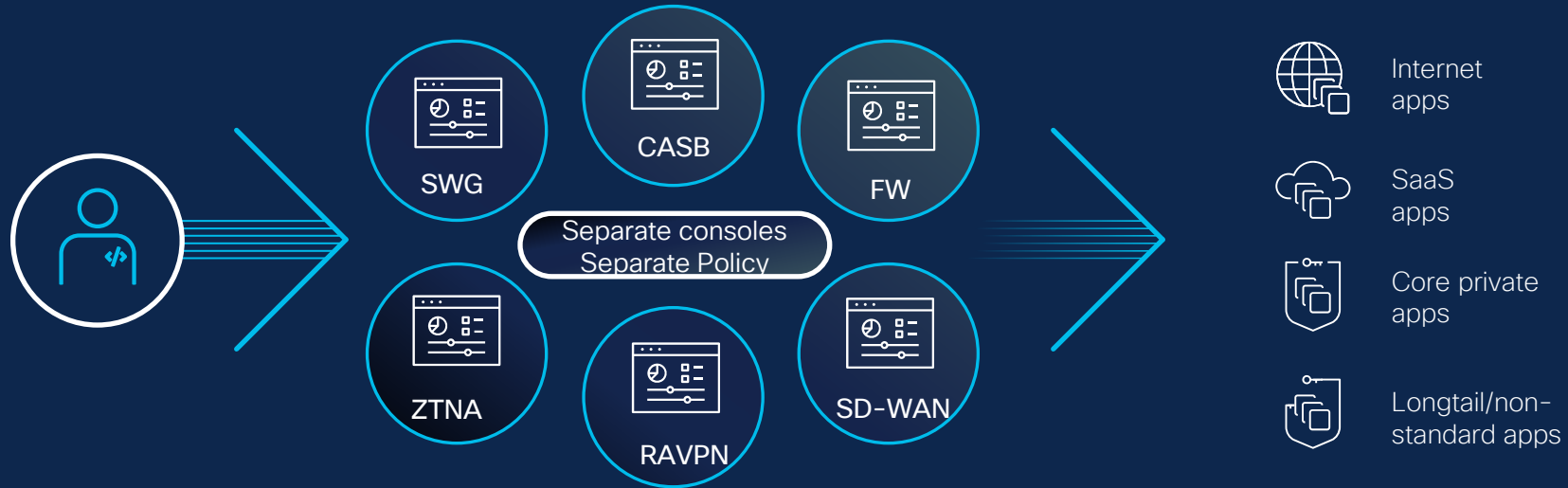
- 2-6hr Free Workshop
- Involves multiple stakeholders
- Contact your Cisco Account team

# Use Cases

# Security Service Edge Cisco Secure Access

# The multi-vendor approach is problematic

On-prem architecture never designed for hybrid work



## Cost and task inefficiencies across multiple products

- Licenses/hardware
- Policy management
- Client management
- Reporting
- Elevated staffing levels

**65%** of enterprises plan on consolidating vendors for better risk posture

# SASE approach to Security Architecture

Fundamental to your security strategy for a hyper-distributed world



# Cisco Secure Access

Go beyond core Secure Service Edge (SSE) to better connect and protect your business

## Core SSE



Secure Web  
Gateway (SWG)



Cloud Access Security  
Broker (CASB) and  
DLP



Zero Trust  
Network  
Access (ZTNA)



Firewall as a  
Service (FWaaS)  
and IPS



Cisco delivers the core and more in a single subscription...



DNS  
Security



Multimode  
DLP



Advanced  
Malware  
protection



Sandbox



Talos  
Threat  
Intelligence



VPN as a  
Service



Digital  
Experience  
Monitoring\*



Remote  
Browser  
Isolation\*

\* Included in the unified experience / separate license (optional)

## Add-on solutions



SD-WAN



XDR



DUO MFA/  
SSO



CSPM

Users

# Transparently secures the connections you need

Unified Agent or Clientless



Step 1. User Authentication and Device Trust  
Step 2. Transport method is auto selected



Internet

Redirected transparently to SSE cloud



SaaS apps

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



Private modern apps

ZTNA gives controlled access to selected applications

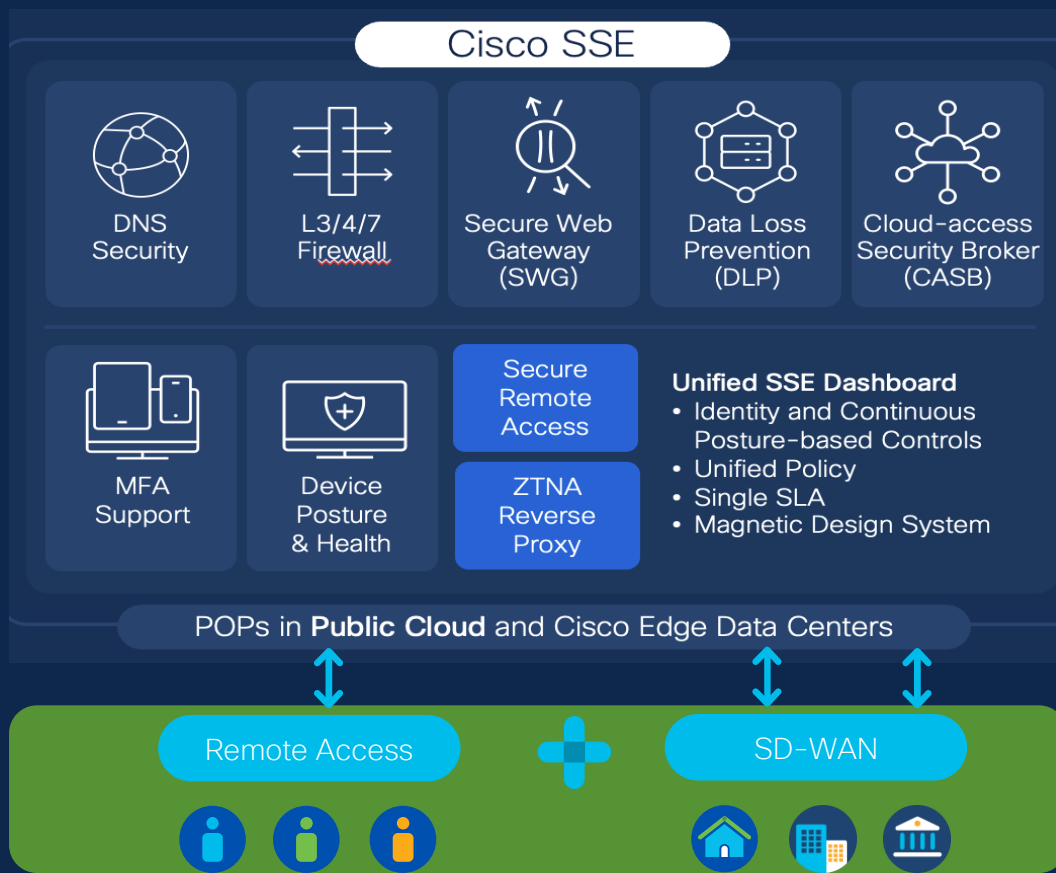


Private Traditional apps

RA-VPN gives full network access for existing applications

## Security Stack for the cloud edge

# Secure access and protection from risks/threats





# Efficiently route traffic to applications anywhere

Cisco SSE



Step 1. Simple, Automated deployment

Step 2. Perform intelligent, resilient routing



Internet apps

Scalable and Distributed PoPs. Direct Peering for superior SaaS experience



Application Connectors

Lightweight, easy to deploy containers to connect to apps anywhere without regard private IP space.



SD-WAN Fabric Private apps

Secure optimized cloud-scale transport to connect data centers, branches, clouds, and colocation facilities



Traditional IPSEC Tunnels

Standards based connectivity provides choice in backhaul devices including our firewalls and 3<sup>rd</sup> party

*Who better than Cisco to route packets to your apps!*

# Common Integrated Policy Table

Overview

Connect

Resources

Secure

Monitor

Admin

Workflows

Policy

Search

Filter

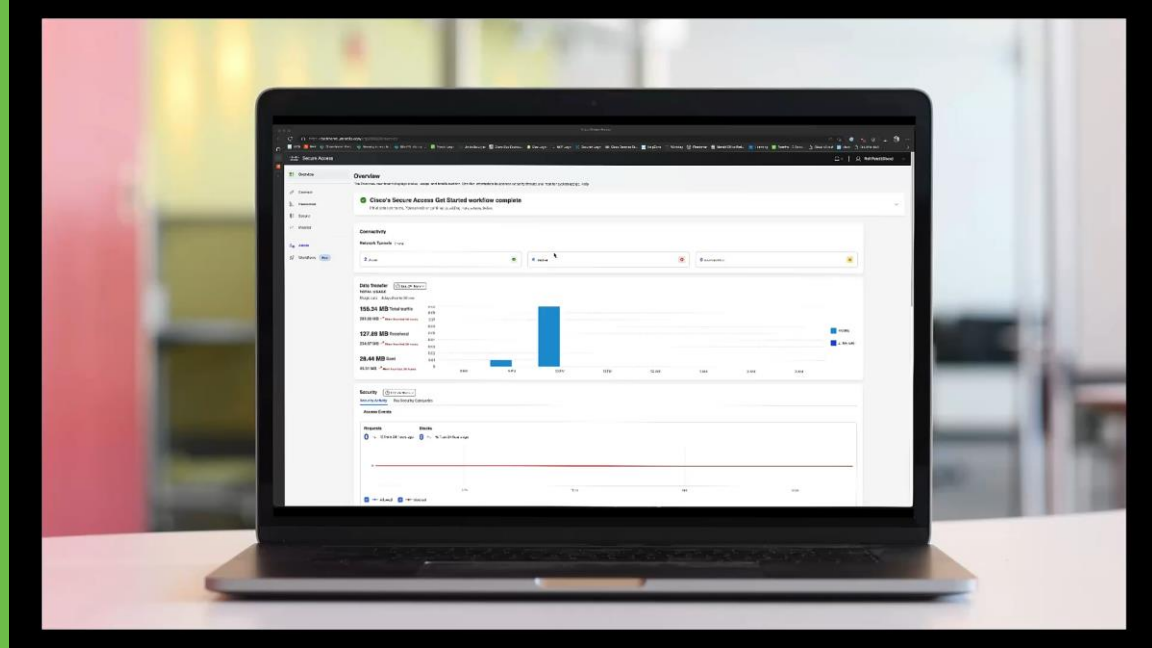
Global Settings

Add rule

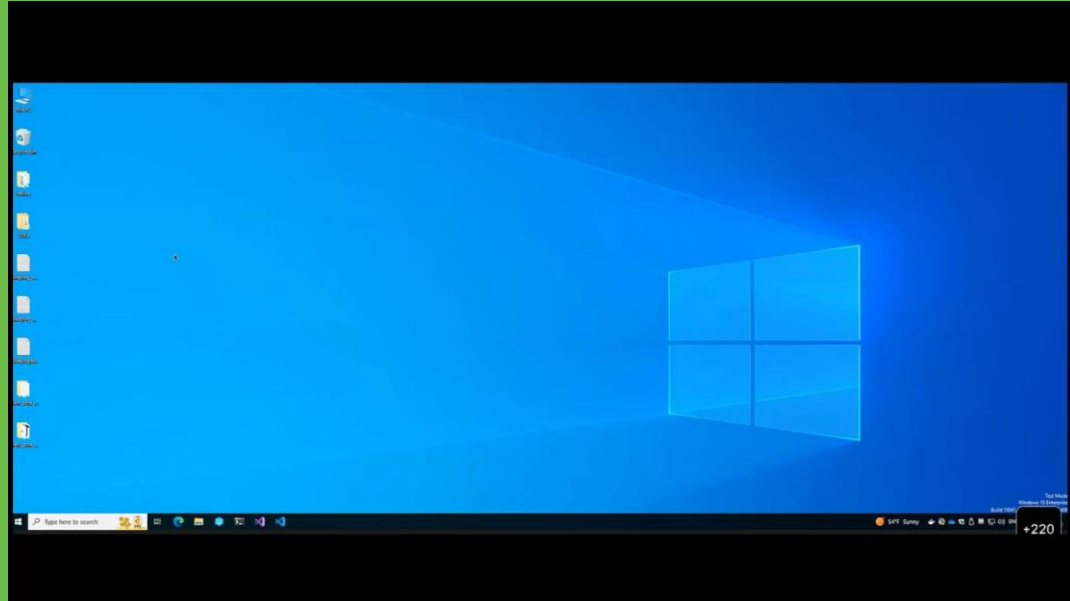
121 Rules

		#	Rule name	Rule type	Actions	Sources	Destinations	Security Control	Posture	Hit Counts	Status	
	<input type="checkbox"/>	1	Contrac...	Private Access	Allow	Contractors	Jira	IPS	Contractors	22K	Enabled	...
	<input type="checkbox"/>	2	Employ...	Private Access	Allow	All Employees	Miro +3	IPS	Default	14K	Enabled	...
	<input type="checkbox"/>	3	Contrac...	Private Access	Allow	Contractors	Comm App 1	IPS	Default	38K	Disabled	...
	<input type="checkbox"/>	4	Contrac...	Private Access	Allow	Contractors	Comm App 2	IPS	Default	24K	Disabled	...
	<input type="checkbox"/>	5	Contrac...	Private Access	Allow	Cont... +2	Comm A... +5	IPS	Contractors	21K	Disabled	...
	<input type="checkbox"/>	6	Develo...	Internet Access	Warn	All E... +4	Dev Tool	IPS	-	13K	Disabled	...
	<input type="checkbox"/>	7	IP phon...	Internet Access	Allow	IP Phone	Servers	IPS	-	27K	Disabled	...
	<input type="checkbox"/>	8	Restric...	Internet Access	Block	Marketing	FTP 21	-	-	45K	Enabled	...
	<input type="checkbox"/>	9	Employ...	Internet Access	Isolate	Employees	Comm App 1	Web Profile	-	16K	Disabled	...

# Cisco Secure Access Admin Demo



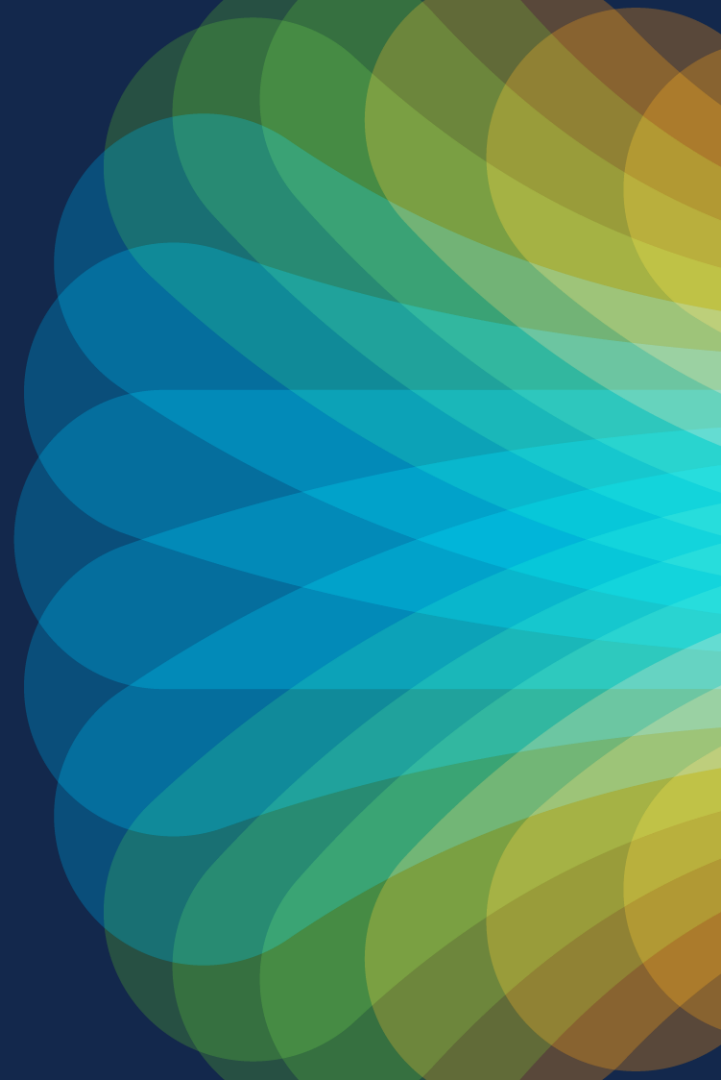
# Cisco Secure Access User Demo



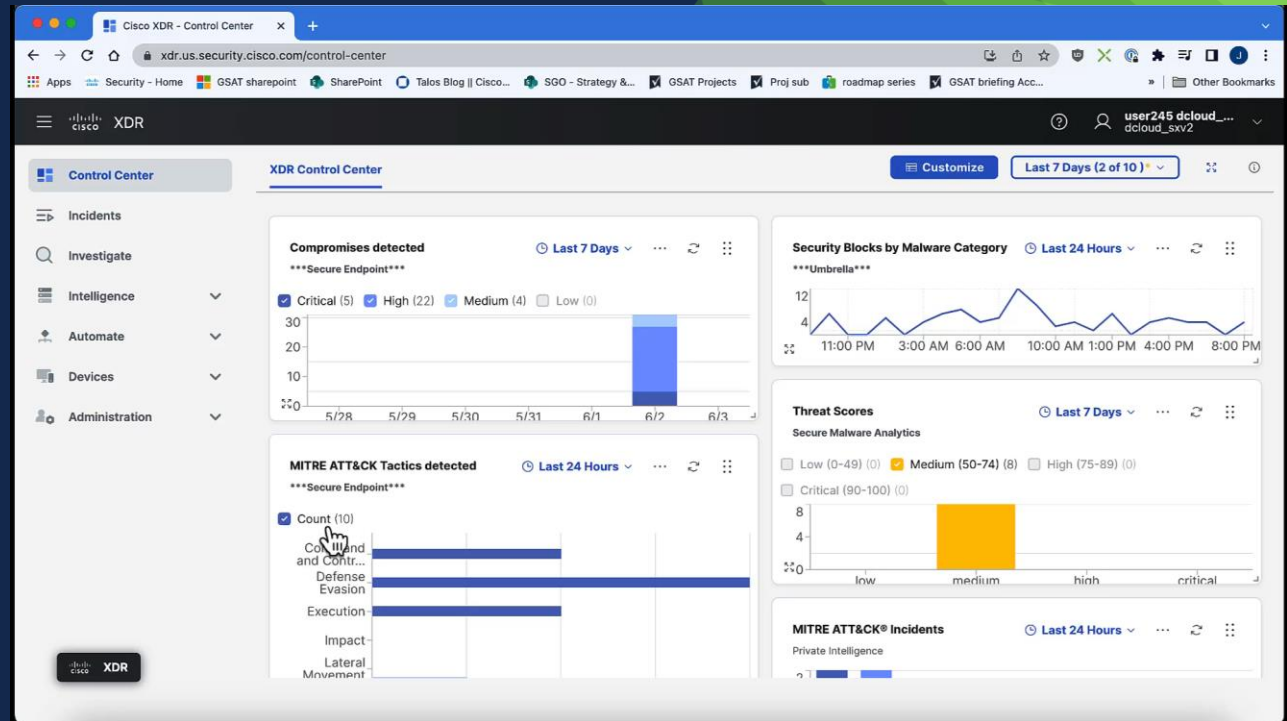
# Integrated Architecture

Automation, Orchestration and response

Cisco XDR

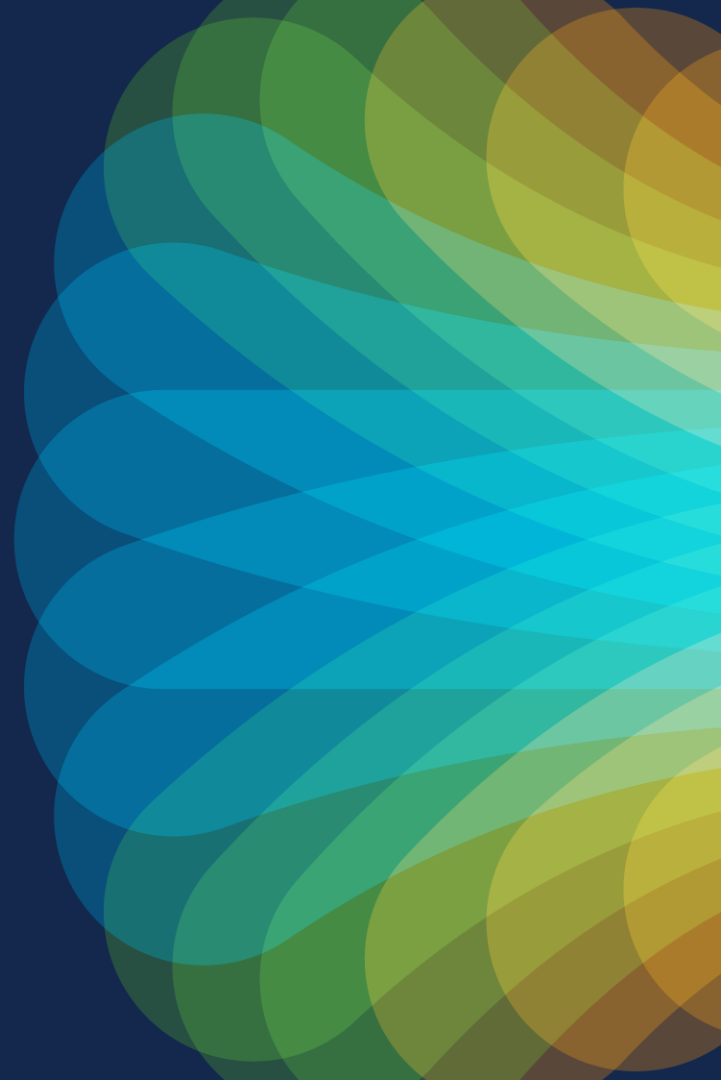


# XDR Demo



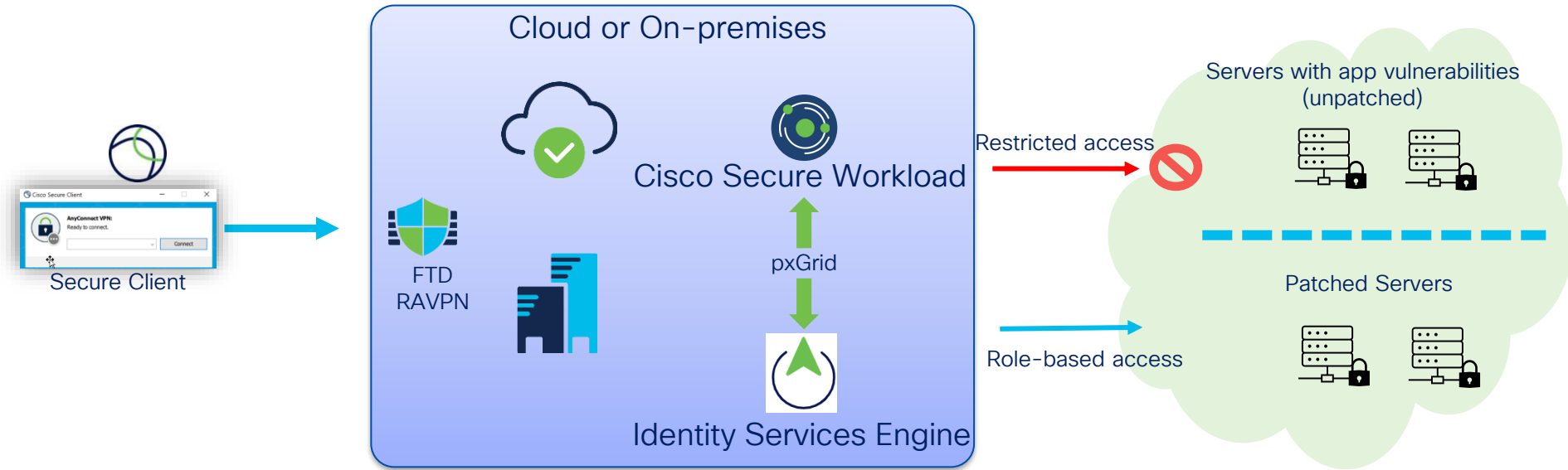
# Application Security Architecture

Integrated, Zero Trust, context-  
aware policy



# Zero Trust policy at scale

## Application vulnerability-aware policy enforcement



### Example Policy Outcomes

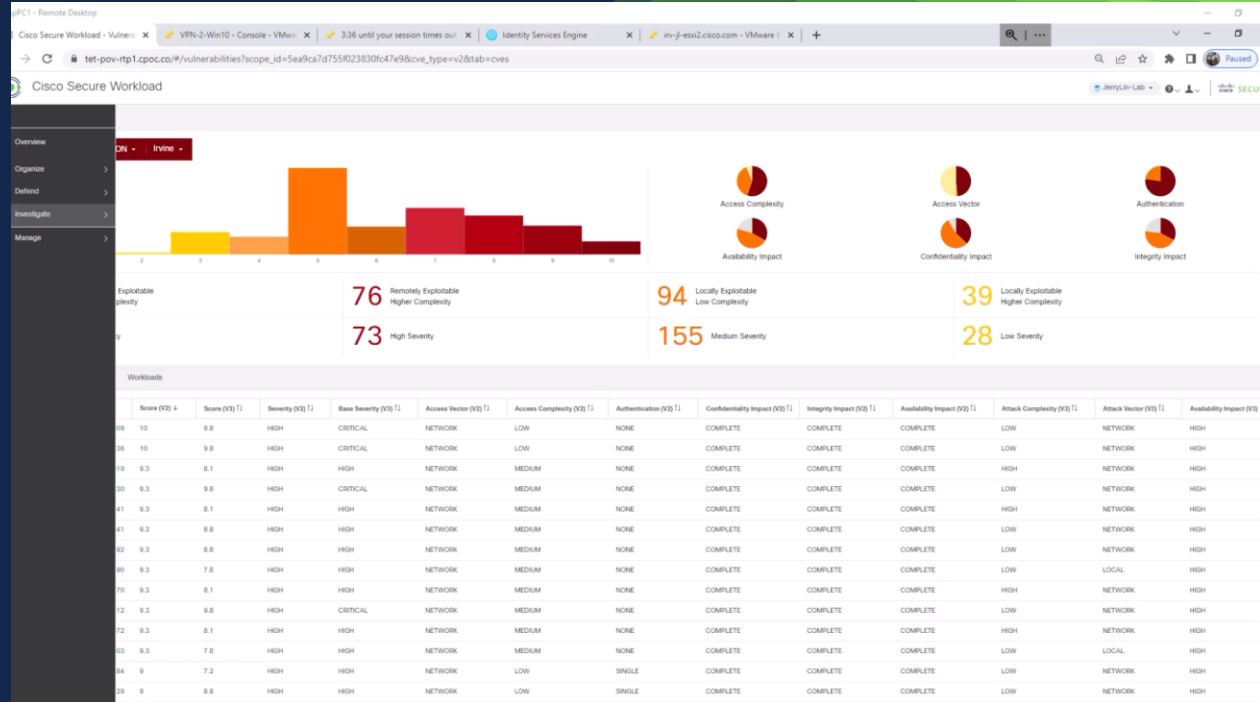
Role-based least-privilege application access

Eliminate risk of Contractors accessing critically vulnerable systems

Selectively reduce access for employees to critically vulnerable systems but maintain productivity



# Workload Demo



# Self-defending Security Architecture

Digital Patching



# Prioritize Incident Response with Kenna.VM and Digital Patching (Snort)



Prioritized host & app vulnerabilities

Ticket opened with CVE data enrichment



SOC Analyst

Analyst approval requested

NGFW CVE compared

Policy updated for CVE patching



Firewall Management Center

Digital Patching (Snort)



On-premises DC

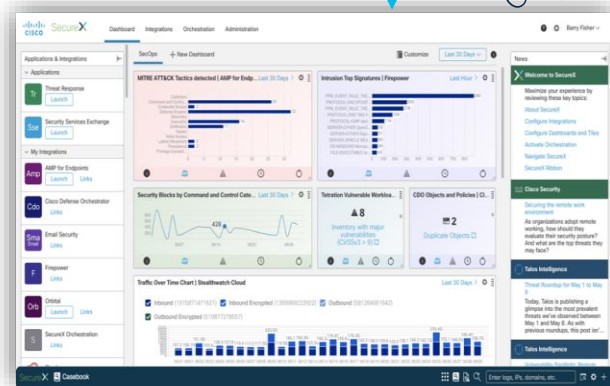


Unpatched Servers with log4j CVEs

Secure Workload (SaaS)



Host CVE export

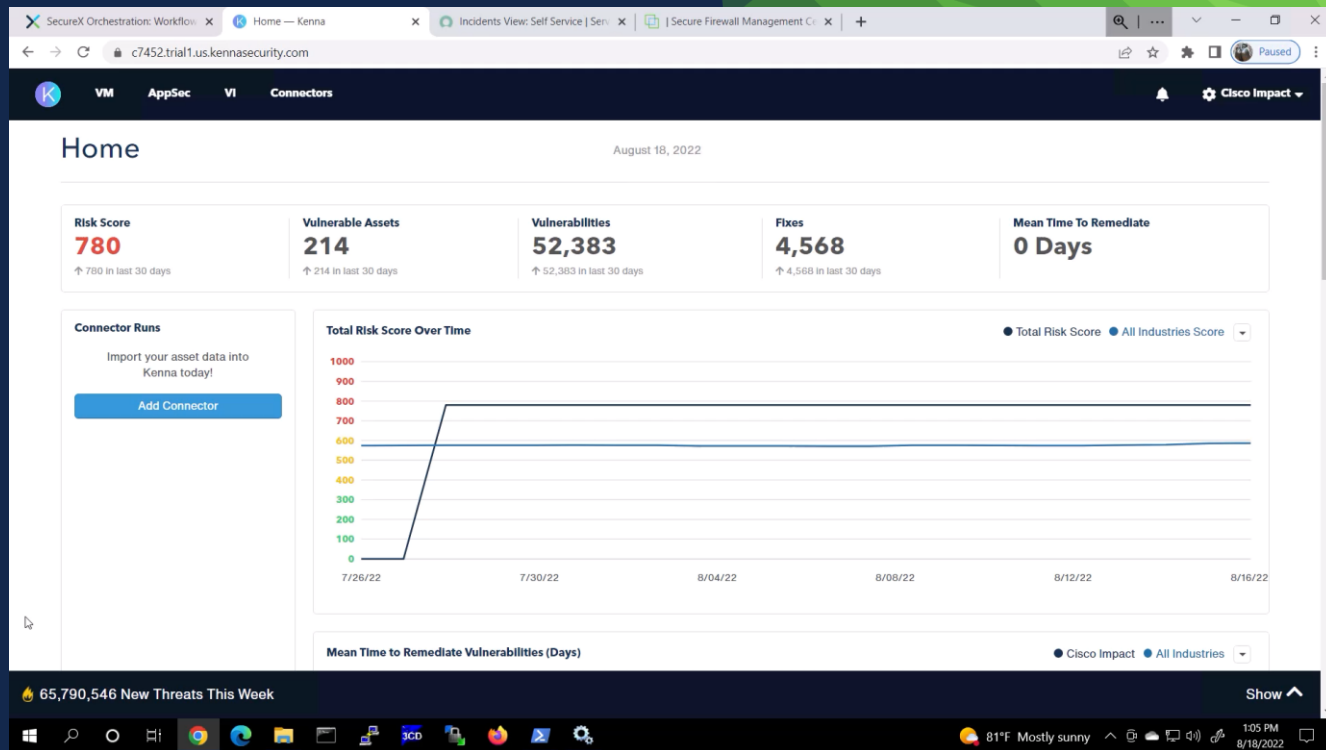


SecureX Orchestration

Remember log4j vulnerability back in December 2021?

**CISCO** *Live!*

# Digital Patching Demo



# Summary

# Value of a Security architecture

Here's what we're seeing:

## Relationships and Dependencies



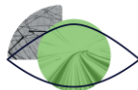
$$1 + 1 > 3$$

## Drivers



Security Controls for risk management

## Operations and Monitoring



Faster Time to detect

## Benefits



**Standardization** for cost effectiveness



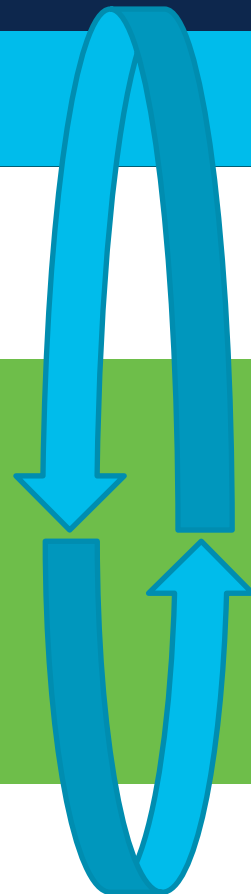
## Threat Detection and Intelligence

Visibility, Analytics, Automation & Response

User & Device

Network & Cloud Edge Environment

Workload, Application, and Data





## TALOS THREAT INTELLIGENCE

Actionable threat intelligence Collective responses Comprehensive visibility Signal identification Threat research & analysis

## XDR SECURITY OPERATIONS TOOLSET

### SERVICES

Custom threat research on demand Implement and manage Incident response retainer Managed detection & response Strategy & assessment

Kenna | Secure Analytics | Cisco XDR  
Secure Client | Talos Incident Response

### CAPABILITIES

Network detection & response Device discovery & insights Endpoint detection & response Open API platform & 3rd party native integrations Risk-based vulnerability management 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 Posture Telemetry/Visibility Endpoint detection & response DNS-layer security Secure Web Anti-virus/Anti-malware Query Host FW Mobile device management Risk-based MFA Passwordless Device trust Continuous trust Email, Phishing, SPAM, BEC, DLP, content filtering Digital experience monitoring

### Cloud Edge Network

#### SASE/Security Service Edge

Duo | Secure Connect | Umbrella

Browser access control Cloud access security broker Cloud malware detection Data loss prevention DNS-layer security Identity/posture FWaaS RAaaS Remote browser isolation Secure web gateway Tenant restrictions TLS decryption Zero Trust Network Access

### On-Premises Network

#### SASE/SDWAN

Meraki | Secure Firewall  
ThousandEyes | Viptela

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

#### In the Office/Managed Location

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

Application network gateway Configuration orchestration Content filtering Encrypted visibility 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

HYBRID MULTI-CLOUD: ACI | Cloud Insights | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Attack Surface Management | Secure Workload

Anti-virus/Anti-malware API security App discovery Cloud analytics Cloud Native Security Cloud Posture Management DDoS, WAF/Bot Identity/pxGrid Micro/Macro Segmentation Run-time Protection Telemetry Threat mitigation Visibility Data access & Integrity



# Security that only Cisco can deliver for you

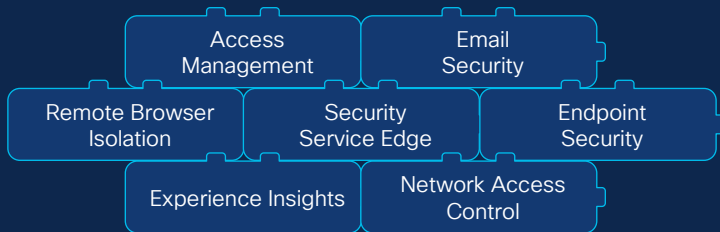
Talos Threat Intelligence

## Breach Protection

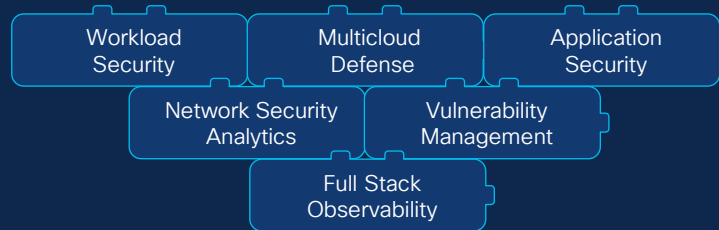
Powered by Talos, the world's most trusted commercial threat intelligence team

Extended Detection & Response

## User Protection



## Cloud Protection



Firewall Protection

Cisco Security Cloud

# Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

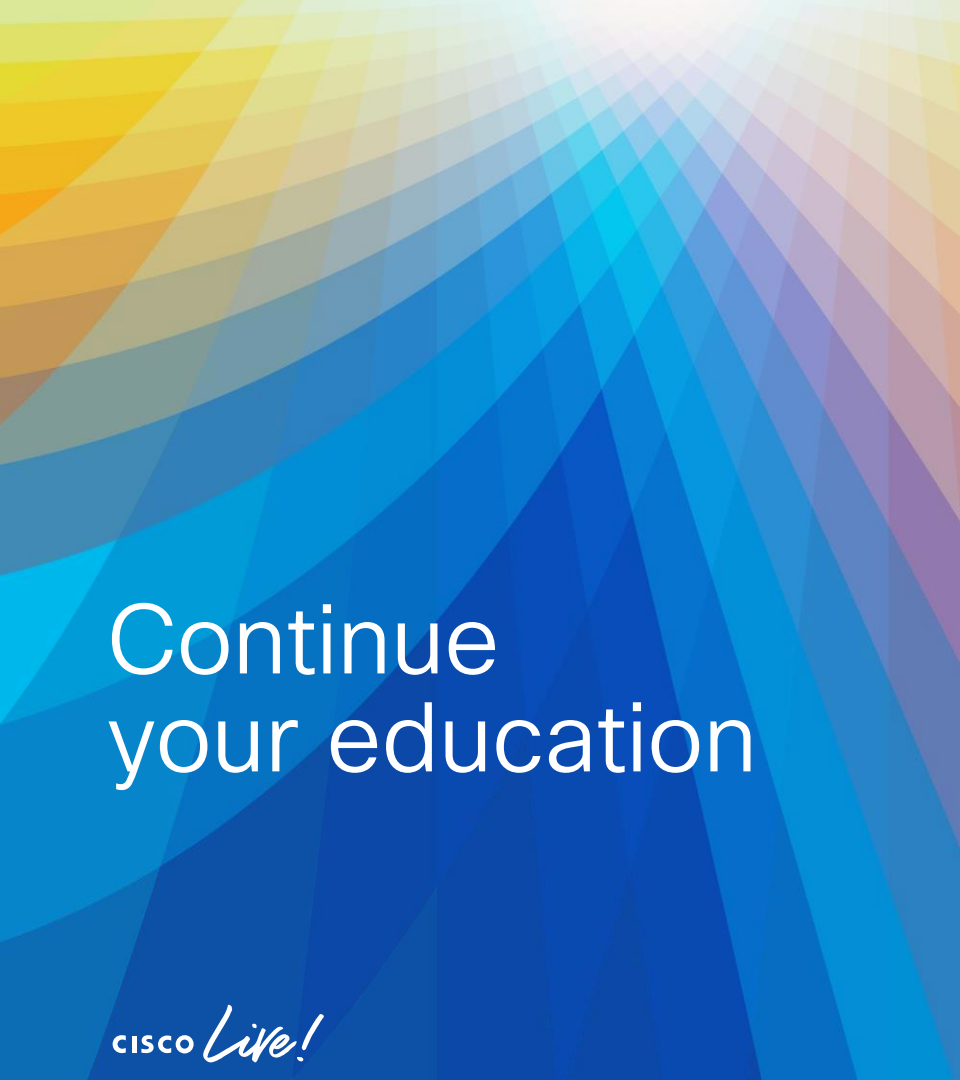
---



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



**These points** help you get on the leaderboard and increase your chances of winning daily and grand prizes



# Continue your education

**CISCO** *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

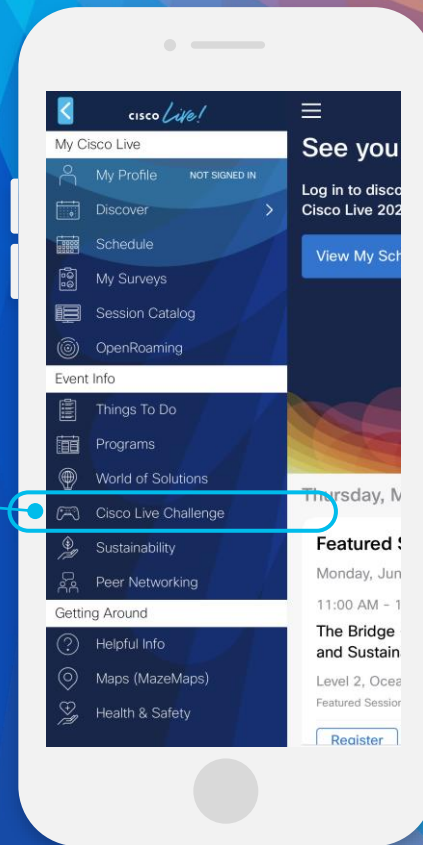
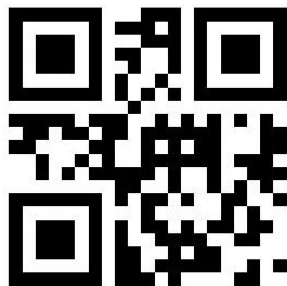
#CiscoLive

# Cisco Live Challenge

Gamify your Cisco Live experience!  
Get points for attending this session!

## How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive