
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Delivering Security Resilience For Governments

Steve Vetter, Global Government Strategist

PSOIND-1015

cisco Live!

Cisco webex app

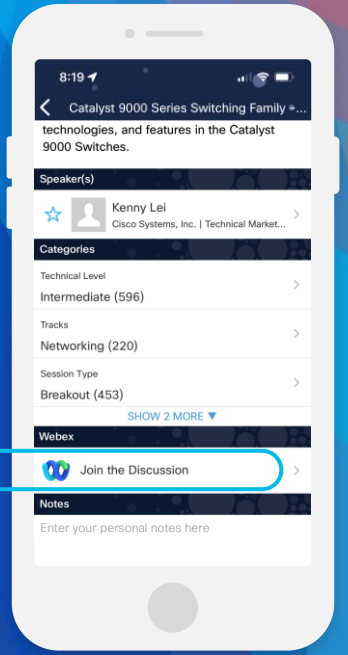
Questions?

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/#PSOIND-1015

Agenda

- Zero Trust is foundational
- Network (r)evolution
- Key cybersecurity guidance
- Zero trust models
- Core zero trust logical components
- IT / OT alignment criticality
- Security resilience differentiators

Getting zero trust right is essential for security resilience for governments

The ability to protect the availability and integrity of the critical aspects of the organization's mission to withstand unpredictable threats or changes...

...and emerge stronger

New U.S. cybersecurity strategy emphasis:

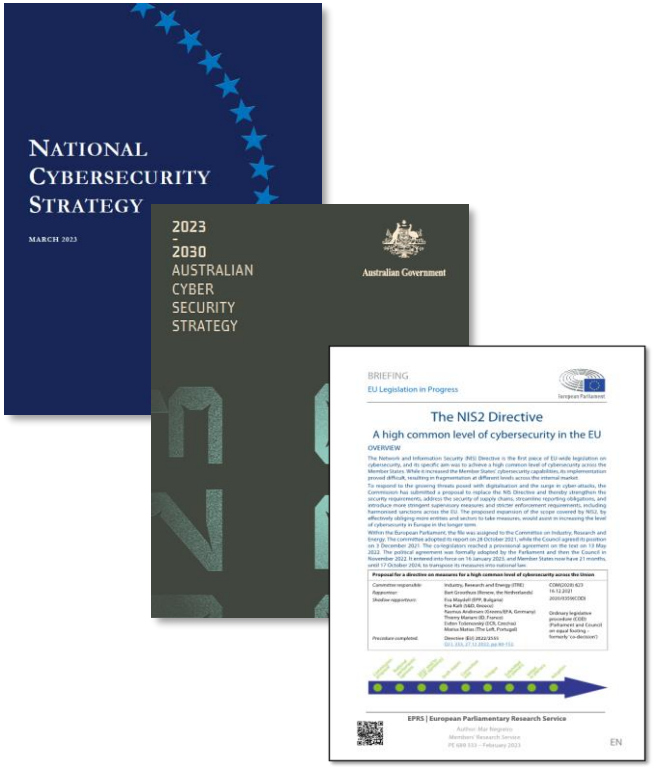
"re-architect digital ecosystem for resiliency"

– *White House*

Evolving global cybersecurity strategies

Key components:

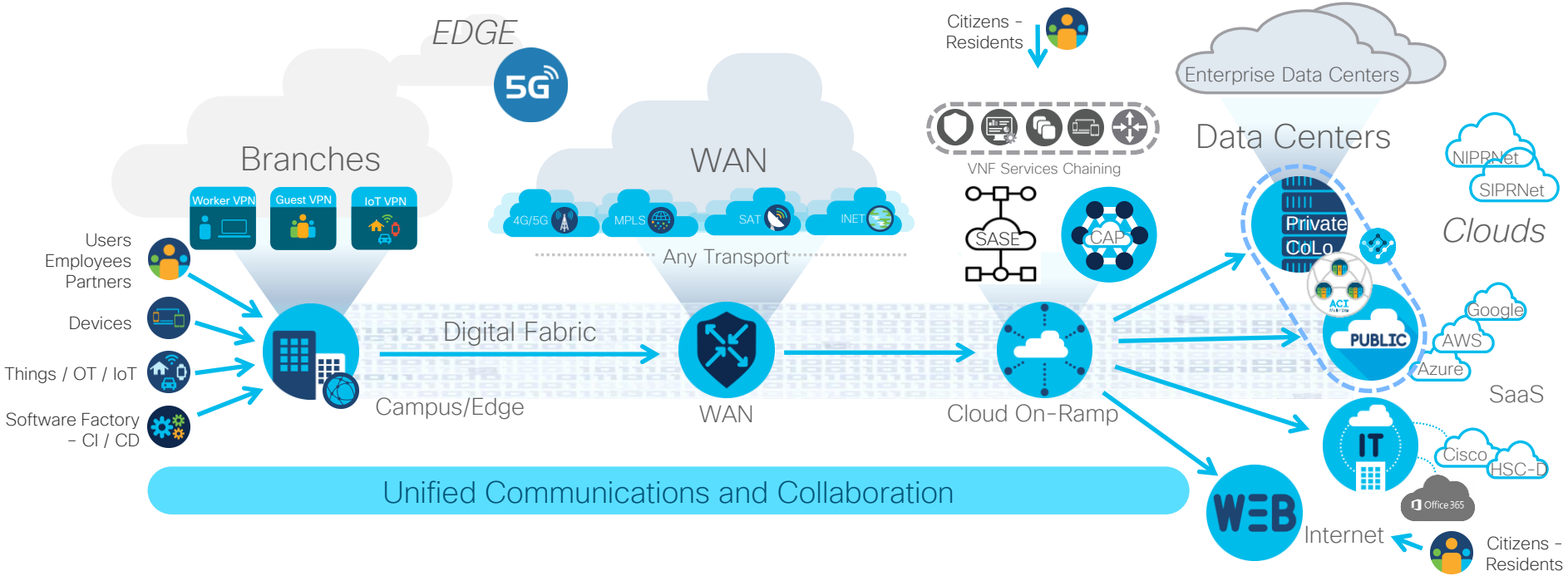
- Defend critical infrastructure and data
- Use existing security frameworks (NIST)
  - Cybersecurity Framework (CSF 2.0)
- Counter threat actors – esp. malware
- Drive security and resilience for digital ecosystem
  - Supporting economy / citizens



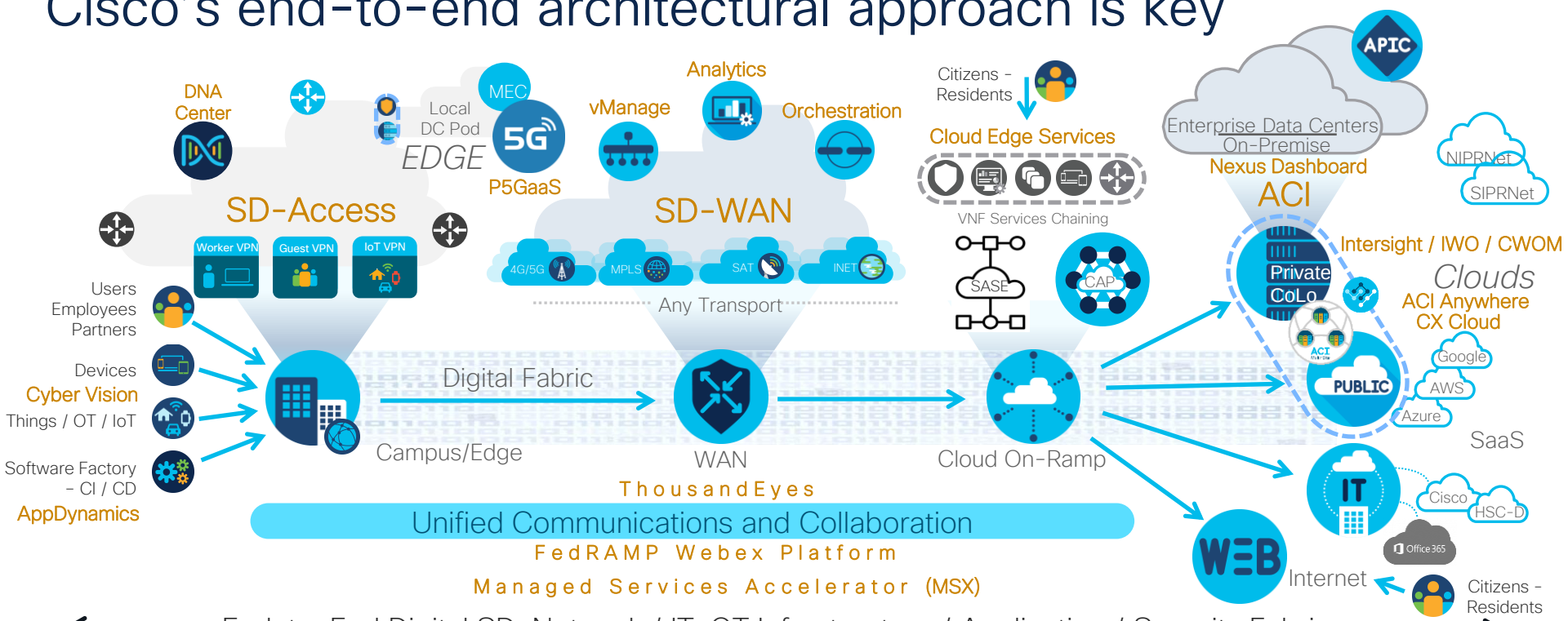
Zero trust serves as the foundation for security resiliency

Zero trust – bottom line

The challenge: end-to-end security resiliency



Cisco's end-to-end architectural approach is key



End-to-End Digital SD-Network / IT-OT Infrastructure / Application / Security Fabric

Telemetry, Visibility and Analytics | Automation and Orchestration, Assurance, Policy | Security, Compliance and Segmentation

Enterprise Multi-Domain Orchestration

Automate / orchestrate / optimize / secure across all domains is key to security and operational resiliency

The network (r)evolution

...and infrastructure and security

Key networking factors

- Performance
- Scale
- Security
- Performance at scale with security

The means: Automation / Machine Learning (AI) = Intent-based networking

- Facilitated by software-defined networking and infrastructure
- Switches as network sensors / policy enforcers and scale enablers (see every packet)

Key cybersecurity guidance

Improving the nation's cybersecurity

EO 14028 – 5/12/21

Zero trust architecture embeds:

- comprehensive security monitoring;
- granular risk-based access controls; and
- system security automation
- coordinated manner throughout all aspects of the infrastructure
- In order to focus on protecting data in real-time within a dynamic threat environment

Moving the US Government toward ZT cybersecurity principles

OMB-M-22-09 – 1/26/22

- Enterprise-wide architecture and isolation strategy (references NIST SP 800-207)
  - The goal is to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible
- Automation of security responses / detection of anomalous behavior requires rich data
- Early warning or detection of anomalous behavior in as close to real time as possible throughout their enterprise

Improving Asset Visibility & Vulnerability Detection on Federal Networks

BOD-23-01 – 10/3/22

- Perform automated asset discovery every 7 days
- Initiate vulnerability enumeration across all discovered assets every 14 days
- Be able to initiate on-demand asset discovery within 72 hours of CISA request

Scope is ALL IP-addressable network assets (IT and OT!)

DHS CISA zero trust guidance

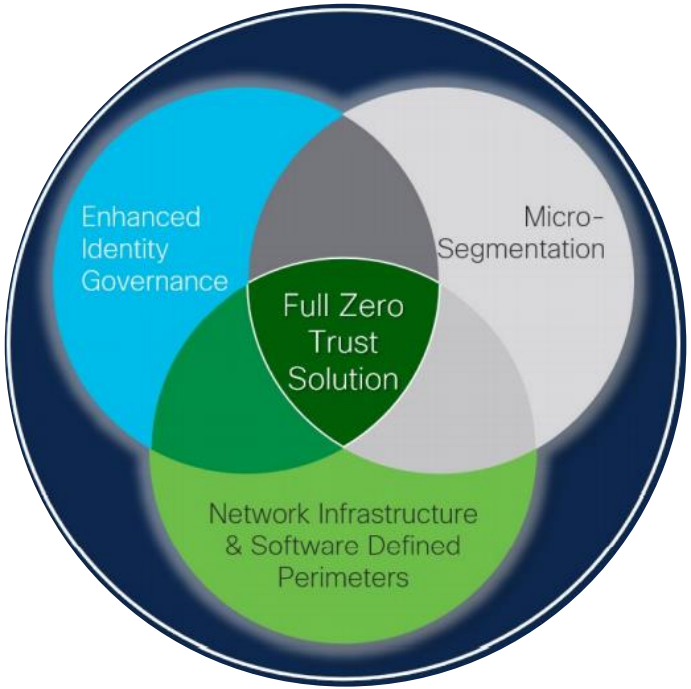
Where to start?

Five steps

1. Focus on the protect surface.
2. Map the transaction flows.
3. Architect the zero trust environment.
4. Create policy.
5. Monitor and maintain.

NIST zero trust architecture (SP 800-207)

Approach variations



"An enterprise may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources."

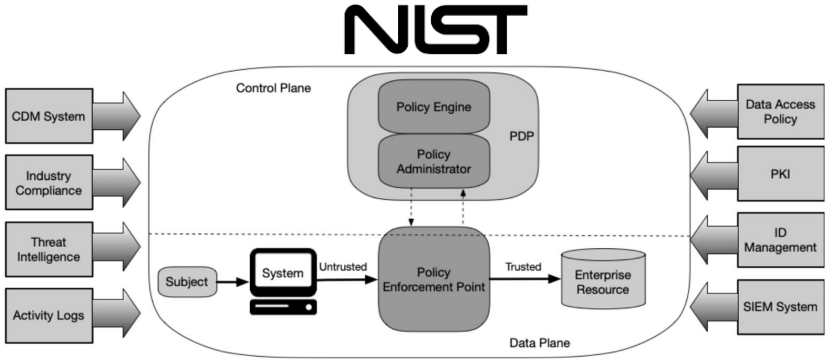
NIST SP 800-207

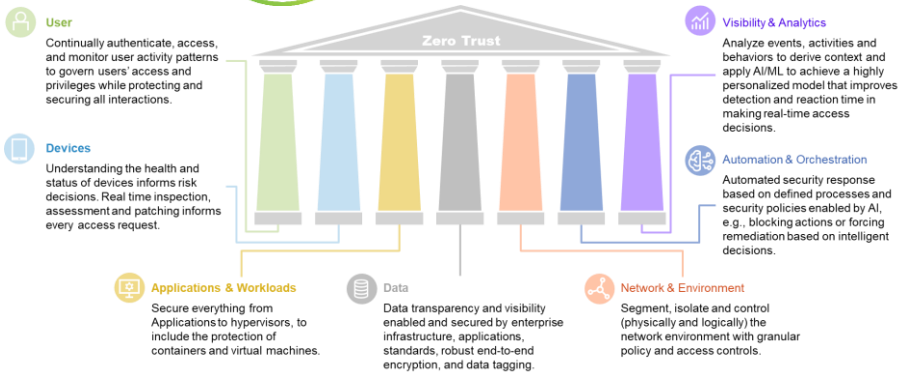
Key to granular security resilience:

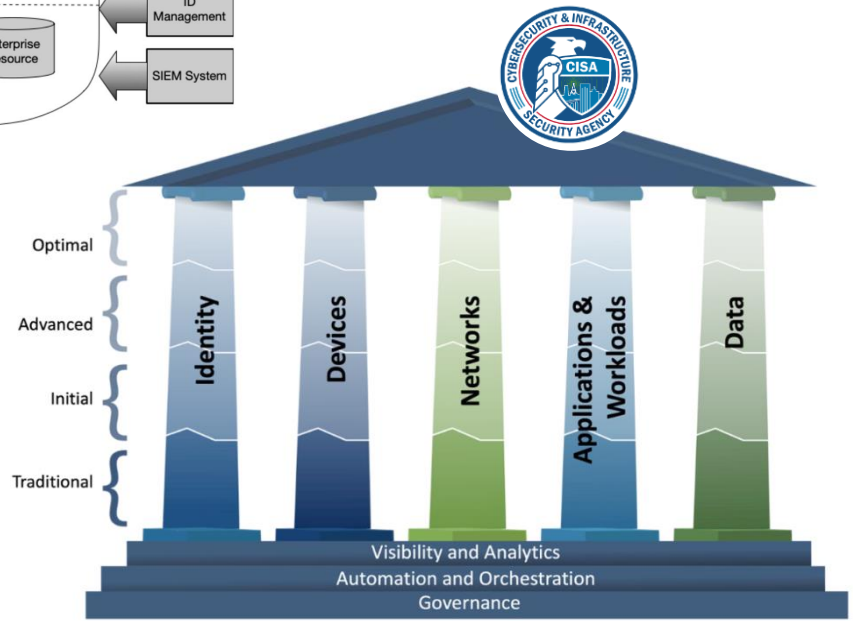
-Granular access control enforcement at OSI Model Layer 2
-Policy Enforcement at individual devices/users/applications

Zero trust models

Three zero trust models for government







DISA zero trust model view

Defense Information Systems Agency
Department of Defense

Zero Trust Pillars and Capabilities

User (Identity)	Device	Infrastructure and Network	Application & Workload	Data	Visibility & Analytics	Automation & Orchestration
Authentication	Authentication	Software Defined Data Center	Application Development	Data Tagging	Accounting and Analysis	API Standards
Authorization	Authorization	Application Delivery		Data Loss Prevention (DLP)	Discovery and Baselining	Incident Response
Privilege Access Management (PAM)	Compliance	Macro Segmentation	Supply Chain	Data Rights Management (DRM)	Security Information and Event Management (SIEM)	Security Orchestration, Automation and Response (SOAR)
		Micro Segmentation		Machine Learning	Artificial Intelligence	

Feeds and Supports Visibility & Analytics

Feeds and Supports Automation & Orchestration

These Cisco solutions support the NIST NCCoE *ZTA / OT / 5G* Projects

Secure Network Analytics (Stealthwatch)
Cyber Vision
Identity Services Engine
Cisco Secure WorkLoad (Tetration)

Zero trust operational approach for resiliency

www.cisco.com/go/securegovernment

Establish Trust

- User / device / service identity
- Posture + context
- Risk-based authentication

Enforce Trust-Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Continuously Verify Trust

- Re-assessment of trust
- Indicators of compromise
- Collect and analyze telemetry
- Behavior monitoring - threat and non-threat activity
- Vulnerability management

Respond to Changes in Trust

- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows

User & Device Security

Network & Cloud Security

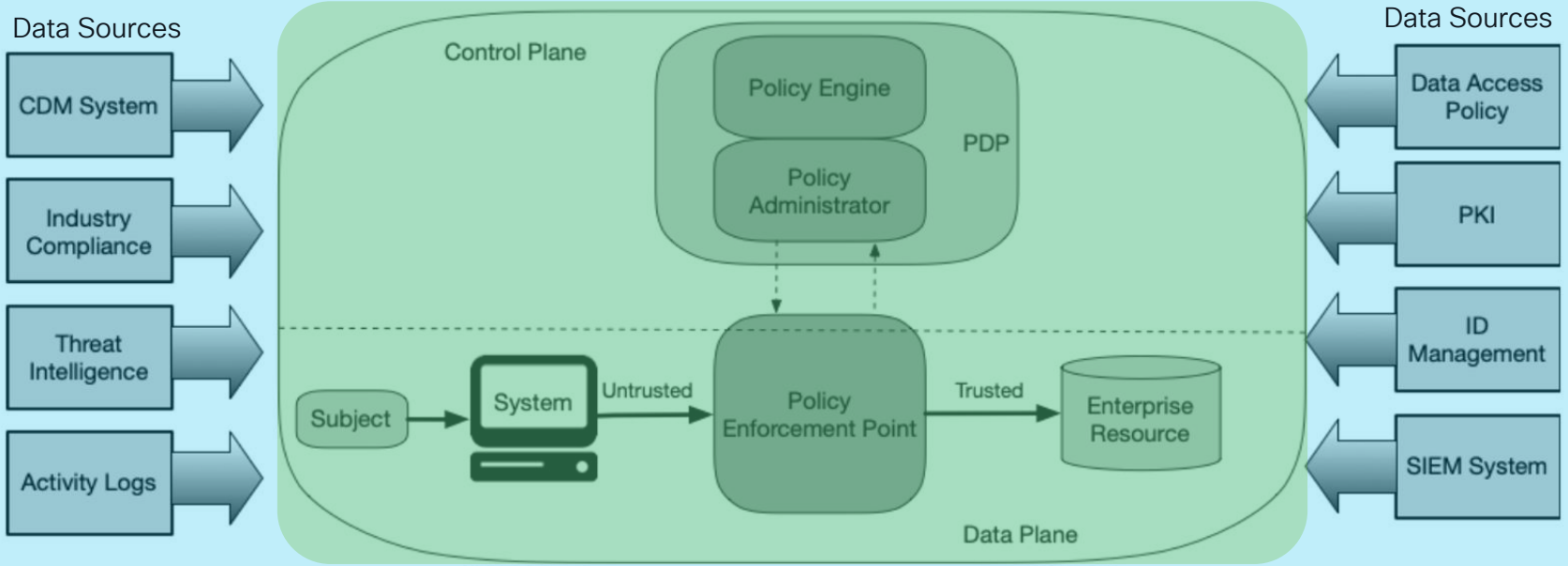
Application & Data Security

Visibility and Analytics

Automation and Orchestration

Zero trust – the core logical components

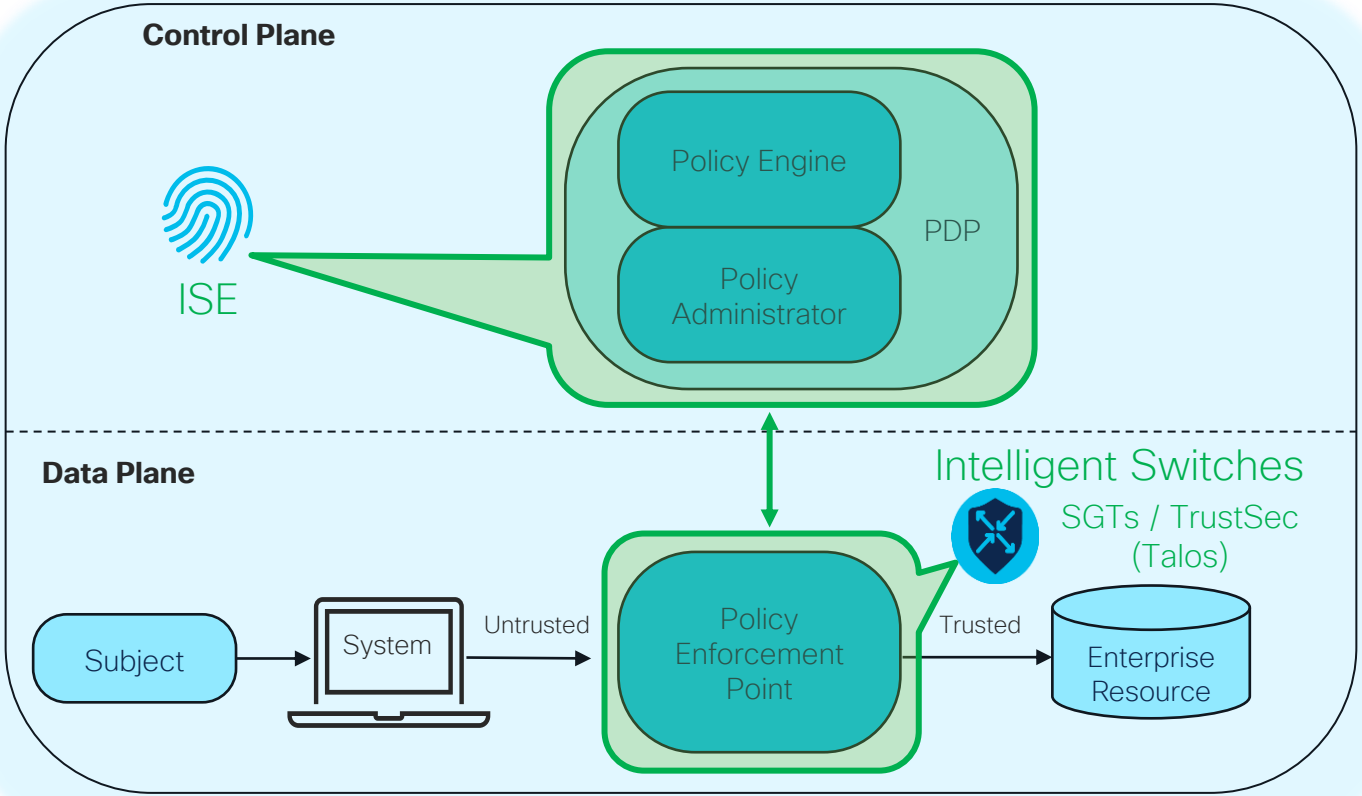
NIST Zero trust architecture – SP 800-207



NIST 800-207: Core Zero Trust Logical Components

The key to a successful Zero Trust journey is taking the first steps, often by leveraging existing enterprise tool investments

NIST zero trust architecture – SP 800-207



NIST 800-207: Core Zero Trust Logical Components

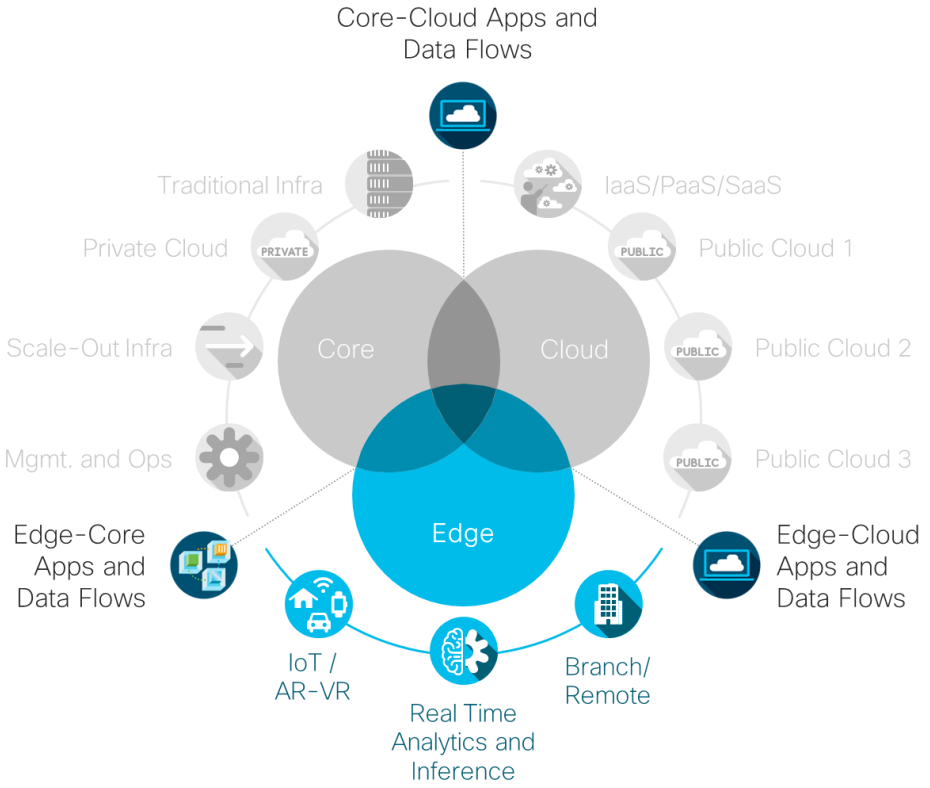
Criticality of IT / OT alignment

What does the future look like?

"By 2025, more than 50% of enterprise-generated data will be created and processed outside [of] the data center or cloud"

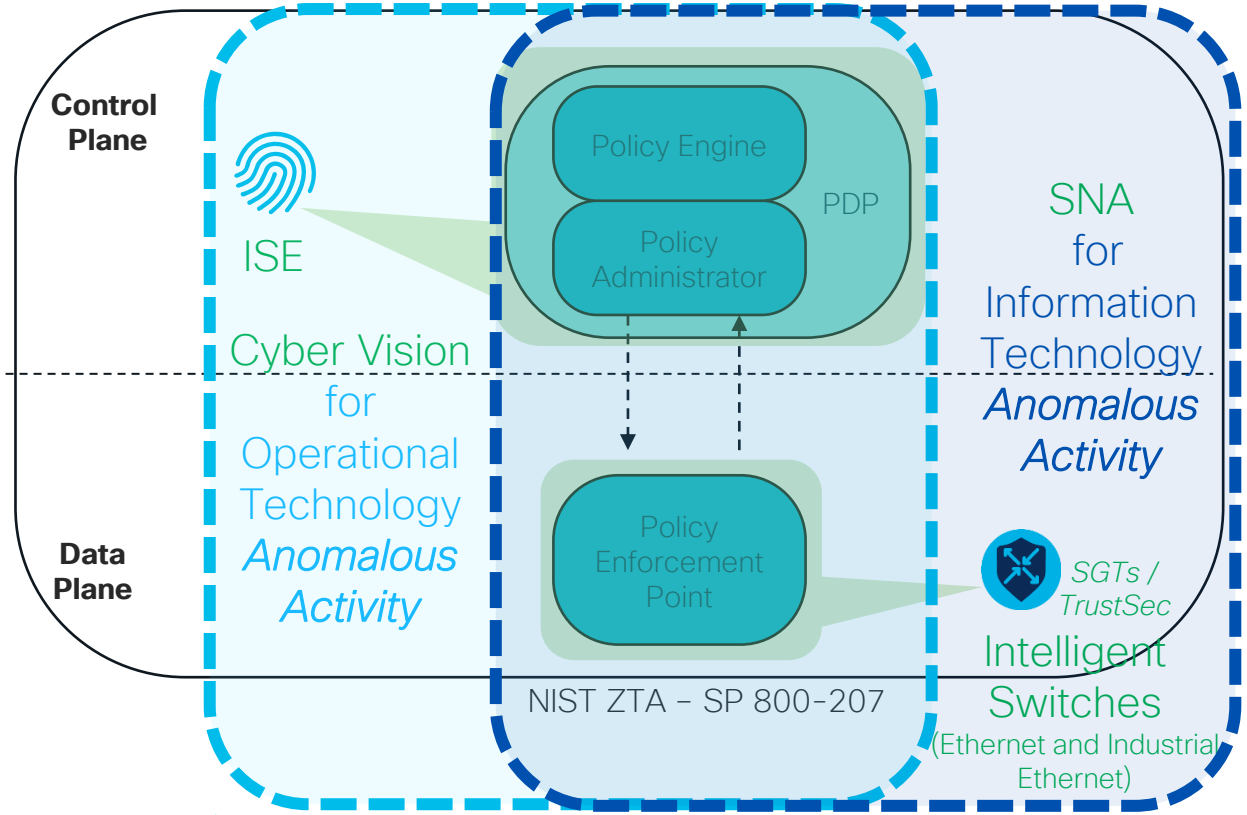
"By 2025, 25% of edge networks will be breached (up from less than 1% in 2021)"

10/21 Gartner,
Gartner Predicts 2022: The Distributed Enterprise Drives Computing to the Edge



IT/OT cybersecurity alignment

Aligned to NIST zero trust architecture



- Dynamic asset visibility
- Real-time, automated and continuous monitoring
  - Detect / alert / act upon
- Integrated, dynamic threat intelligence
- A cross-architecture, multi-domain security focus is key to effective security resiliency

Key security resilience differentiators

Security Resilience (and operational resilience) depend on enterprise visibility and orchestration

KNOW every host

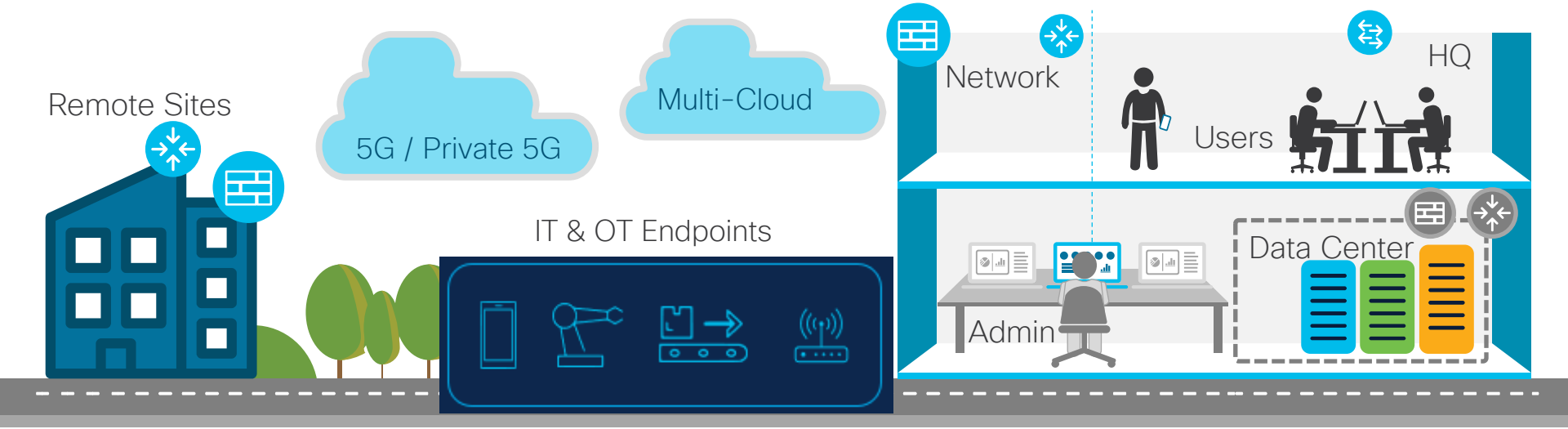
SEE every packet

MAP application flows

Understand what is NORMAL

Analyze ABNORMAL

Respond to THREATS dynamically



Integrated end-to-end network and security

Key to delivering both security and operational resilience

1

Integrated, software-defined networking capabilities that enable dynamic network access control and infrastructure reconfiguration in response to real-time threats and anomalous activity

2

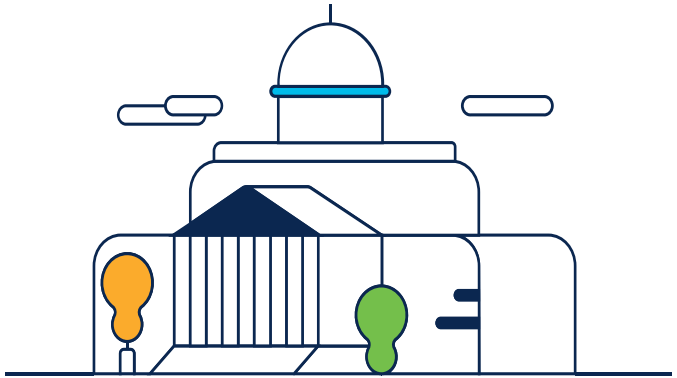
Dynamic, AI/ML-driven application-centric infrastructure and security automation and orchestration trained on massive global data sets

3

The most granular access control and advanced micro-segmentation capabilities that constrain threats at the individual application, device and user level

cisco.com/go/securegovernment

Resources



- Cisco Government website
- Government Portfolio Explorer
- Government blogs

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

- 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

The bridge to possible

Thank you

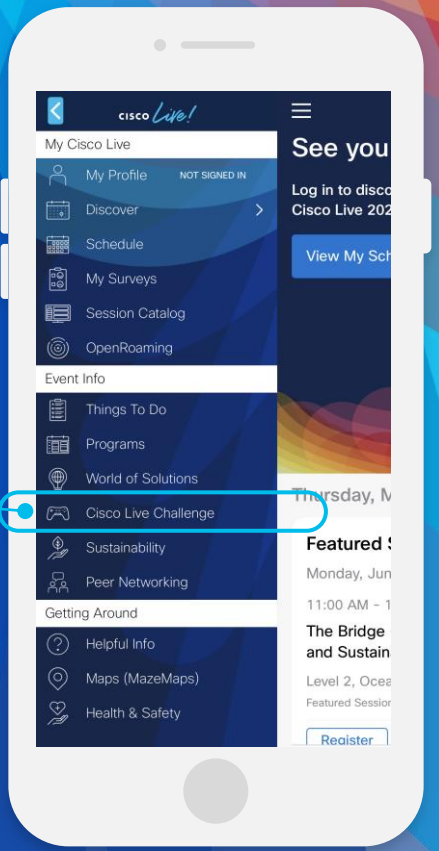
Cisco Live
Challenge

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:



cisco Live!


cisco Live!
Let's go
#CiscoLive