

CISCO *Live!*



#CiscoLive



The bridge to possible

# How to Securely Build a Product

Peter Jones  
Distinguished Engineer  
@petergjones

Dave Zacks  
Distinguished Engineer  
@DaveZacks

BRKARC-2021



#CiscoLive

# Cisco Webex App

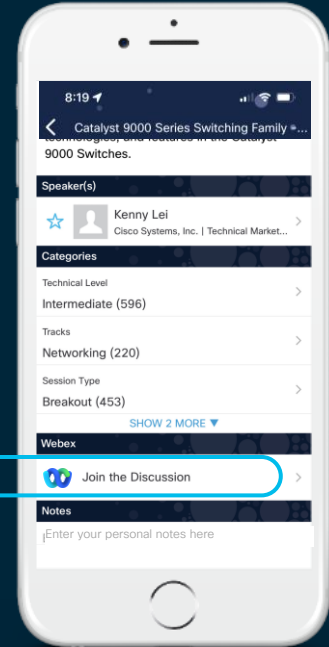
## Questions?

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 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKARC-2021>

# By Way of Introduction ...

I am a **Distinguished Engineer** in the DC/EN/IoT Hardware team, with Cisco since 2005.

I work on System Architecture for the switching, routing, wireless and IE platforms, especially Catalyst 3850/3650/9K and the UADP ASIC family.

I am heavily involved in Ethernet standardization in IEEE 802.3 (e.g., 802.3bz, 802.3cc, 802.3cg), as Ethernet Alliance chair, and former NBASE-T Alliance chair.

I am passionate about **Network Evolution** and **Adoptable Technology**.

**Peter Jones**  
Distinguished Engineer

[petejone@cisco.com](mailto:petejone@cisco.com)

[@petergjones](https://twitter.com/petergjones)



# By Way of Introduction ...

I am a **Distinguished Engineer** in the CX team, and have been with Cisco for 22 years.

I work primarily with large, high-performance Enterprise network architectures, designs, and systems. I have over 30 years of experience with designing, implementing, and supporting solutions with many diverse network technologies.

I have a strong background in, and focus on, customer requirements, and integrating these into the products and solutions Cisco builds. I have a special interest in **Flexible Hardware, Fabrics, Assurance and ML/AI**.

**Dave Zacks**  
Distinguished Engineer

[dzacks@cisco.com](mailto:dzacks@cisco.com)

[@DaveZacks](https://twitter.com/DaveZacks)





# Agenda

- Introduction
- Trustworthy Solutions & Technologies
  - Supply Chain
  - Hardware
  - Software
  - Decommissioning
- Capabilities of/with Platforms:
  - ISE device profiling
  - IPsec, MACSEC security improvements
  - PSIRT – what it is, what it provides, and why
  - TALOS – what it is, what it provides, and why
- Summary

# NSA Releases Network Infrastructure Security Guidance

Original release date: March 03, 2022

The National Security Agency (NSA) has released a new Cybersecurity Technical Report (CTR): [Network Infrastructure Security Guidance](#). The report captures best practices based on the depth and breadth of experience in supporting customers and responding to threats.

*“All networks are at risk of compromise, especially if devices are not properly configured and maintained. **An administrator’s role is critical** to securing the network against adversarial techniques and **requires dedicated people** to secure the devices, applications, and information on the network. “*

<https://www.cisa.gov/uscert/ncas/current-activity/2022/03/03/nsa-releases-network-infrastructure-security-guidance>

# Definitions



*No more! No less!*

## Trustworthy definition

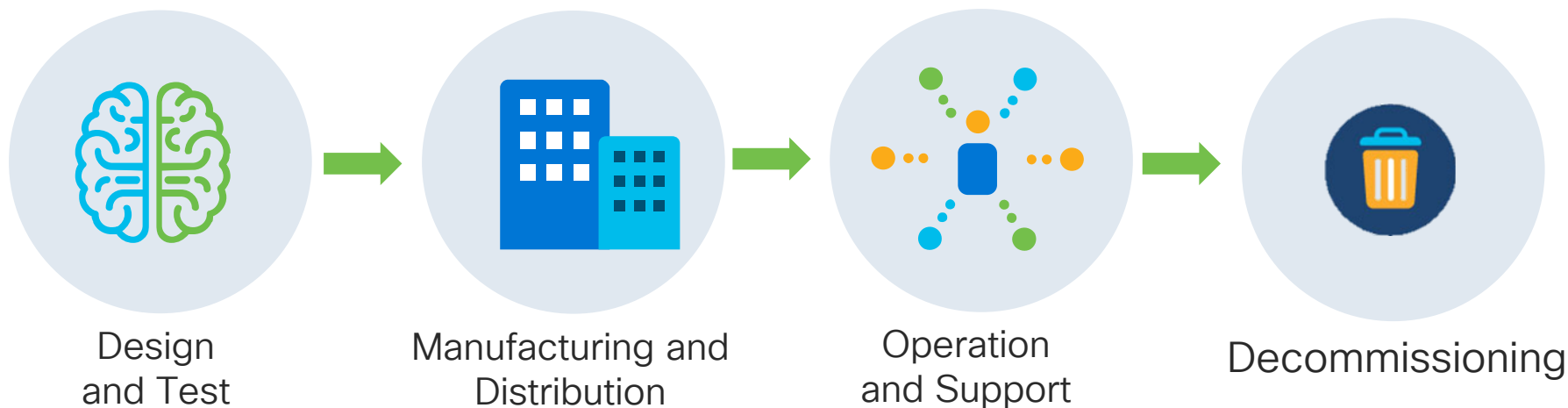
*“able to be relied on to do or provide what is needed or right\*”*

## A secure trustworthy system

- Provides required access to authorized users, *no more & no less*
- Performs functions requested by authorized users, *no more & no less*
- Permits network access defined by authorized users, *no more & no less*

\* <https://www.britannica.com/dictionary/trustworthy>

# A Trustworthy Solution Has: Security built into...



“Security embedded throughout the solution lifecycle,  
and across the Cisco product portfolios”

# What are key Trustworthy Technologies ?



Trust  
Anchor



Secure  
Boot



Image  
Signing



Runtime  
Defense

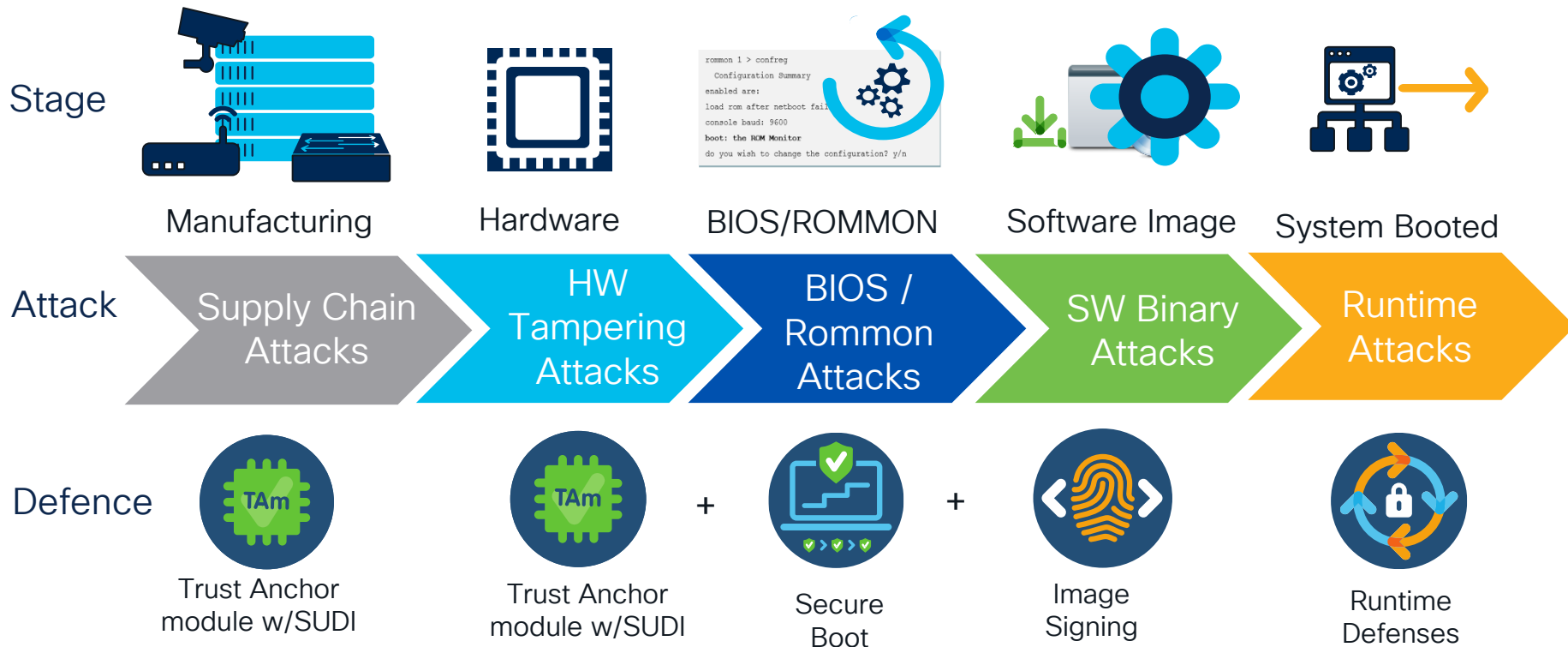


Modern  
Crypto

- Foundational security at the system infrastructure level
- Starting with HW to the SW, from boot time to runtime.
- Building blocks integrated into Cisco product.

Trust can be measured, verified, and audited.

# Trustworthy Technologies Protection Scope



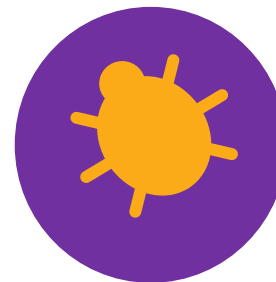
# Threat Manifestations in the Supply Chain



Denial of  
Service



Social  
Engineering



Malware



Account  
Privilege  
Misuse



Forgery or  
Copy



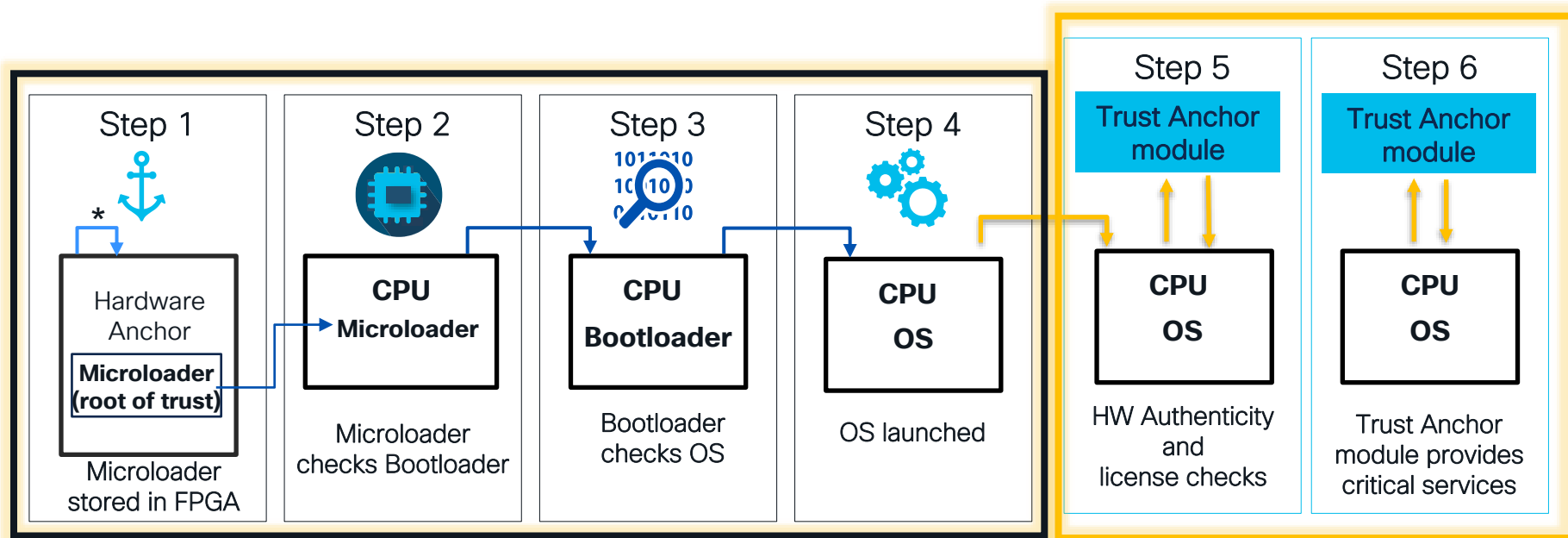
Tampering

# Supply Chain Defence

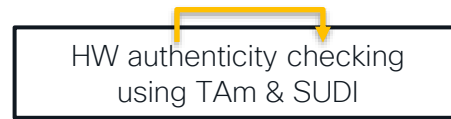
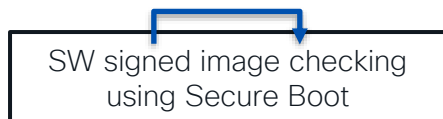
LOGICAL SECURITY	TECHNICAL SECURITY	PHYSICAL SECURITY	BEHAVIORAL SECURITY
Secure development lifecycle	Encryption	Camera monitoring	Increases awareness of insider threats
Scrap weight validation	Smart chips	Security checkpoints	Employs “human sensing”
Role-based access	Data extracting test beds	Electronic or biometric access control	Builds a security culture and behaviors

The **RIGHT SECURITY** in the **RIGHT PLACE** at the **RIGHT TIME**

# Secure Boot Process Reminder



\* The first instructions that run on a CPU are either stored in immutable hardware so that they cannot be tampered with or are validated by the hardware anchor



# Hardware Tampering Defenses

- **Chip Protection**: CPU, ASIC and SoC identities are fingerprinted during platform manufacture and compared during boot time to ensure chips are not replaced or compromised
- **Secure JTAG<sup>1</sup>**: Prevent unauthenticated access to JTAG port to probe or modify CPU memory contents
- **Host-TAm Bus Encryption**: Encrypt host to Trust Anchor messages to prevent modification/snooping of keys and other sensitive data

1: JTAG -Joint Test Action Group - <https://en.wikipedia.org/wiki/JTAG>

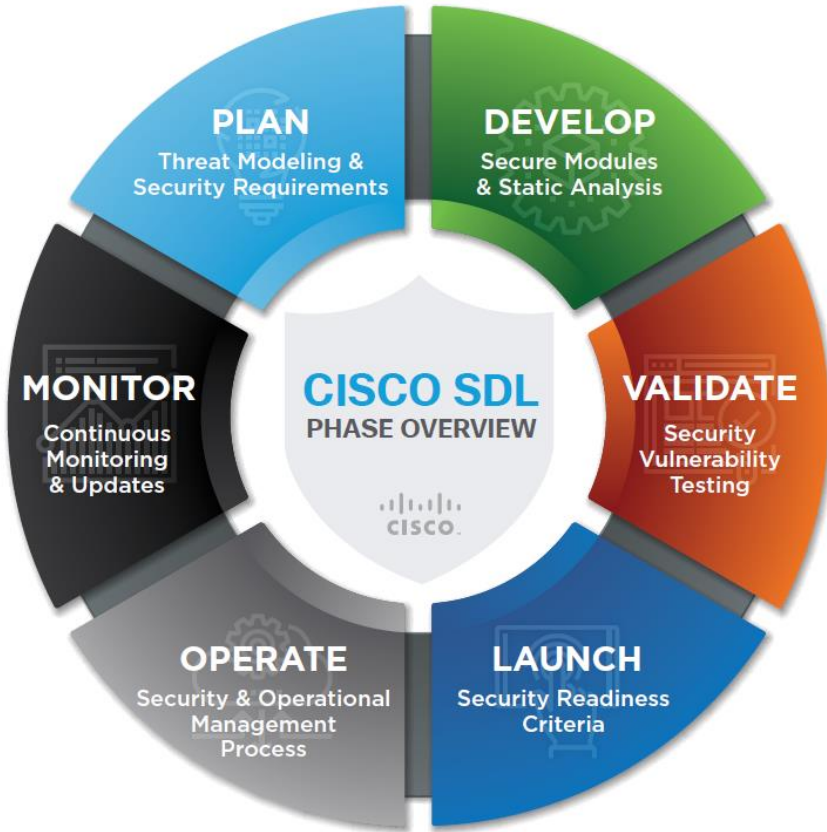
# Image Defenses

- **FPGA Bitstream Security:** Secure FPGA bitstream (config image) through image Authentication and/or Encryption
- **BIOS/Bootloader Protection:** BIOS/Bootloader resiliency with secure BIOS FW upgrade and BIOS Golden image auto recovery
- **Multistage BIOS:** Breaking down BIOS/Bootloader code from boot flash into multiple, smaller pieces so that they are loaded, validated, AND executed entirely in the RAM to protect it from external modification

# Integrity Verification

- **Boot Integrity Visibility (BIV)**: Boot code integrity measurements collection, storage, and data accessibility using Cisco proprietary format and workflow
- **Attestation**: TCG-TPM2.0 style Attestation support for boot code, config, keys measurements, chip components identities, IMA and SW integrity measurements storage and attestation

# Cisco Secure Development Lifecycle (CSDL)



- **Plan** – security & privacy controls, risk assessment
- **Develop** – secure modules and static analysis
- **Validate** – security vulnerability testing
- **Launch** – security and privacy readiness
- **Operate** – security and operational management
- **Monitor** – continuous monitoring and updating

# RunTime Defenses (RTD)

## WHAT?

- Safe C libraries and Object Size Checking protects against buffer overflow (e.g Heartbleed) attacks
- X-Space and ASLR protect against code injection attacks

## HOW?

- Safe C libraries bounds-checking of memory and all Copy functions.
- Object Size Checking detects many overflows at compile and runtime.
- X-Space disallows/mutually excluding execution from data area in memory
- ASLR randomize the locations in memory where different code or data is loaded

## Safe C Libraries

Check only the most secure coding libraries are used in code

## Object Size Checking

Mitigate buffer overflow attacks



## Address Space Layout Randomization (ASLR)

Mitigate code injection attacks

## X-Space

Mitigate code injection attacks

# Cisco Product Takeback & Reuse Program

Free removal and transport of equipment at customer end-of-use



## Simple

Cisco offers **various tools** to help you create a return request and schedule the free pickup of your used Cisco equipment.



## Secure

Returned equipment is stored in a secure location and non-volatile storage is cleared according to the **U.S. NIST 800-88 guidelines**.



## Sustainable

Cisco can help you reach your sustainability goals – we **reuse and recycle 99.9%** of what is returned to our facilities.

Learn more: <https://www.cisco.com/c/en/us/about/takeback-and-reuse.html>

# Secure disposal

## Cisco Product Takeback



All non-volatile storage (e.g., Flash, SSD) are wiped, and erasure process is verified by an independent personnel



If the data cannot be wiped, the hardware is securely destroyed



Our data wipe process meets requirements set by some of the most stringent data destruction standards in the world, including the U.S. NIST 800-88 guidelines.



# Want More?

About Cisco /

## The Trust Center

Cisco 2022 Data Privacy Benchmark Study

Discover why privacy is now mission critical.

[Learn more](#)



[Key Topics](#) [Featured Content](#) [Responsible Innovation](#) [Our Story](#) [Cyber Safety](#) [For Sellers](#) [Resources](#)

## Trustworthy. Transparent. Accountable.



### Data Management

Addressing your top priorities regarding the use and management of data.



### Trust Principles

Committed to maintaining strong protections for our customers, products and company.



### Transparency

Working to gain and keep your trust by sharing our reports, certifications and verification service.



### Trustworthy Solutions

Embedding security across processes and technology to provide a trustworthy network foundation.

<https://www.cisco.com/c/en/us/about/trust-center.html>

**CISCO** *Live!*

The Trust Center /

## Trust Portal

[Get documents](#)

Self-service access to security, data privacy and compliance documents



### Access Specific Trust Documents

[Audit Reports \(SOC, FedRAMP, ISO,C5\)](#)  
[Pen Tests and Security Assessments](#)  
[Security Questionnaires](#)  
[Privacy Data Sheets](#)

[Search all documents >](#)



### Get Trust Packages by Product

[Webex Meetings Trust Package](#)  
[Webex App Trust Package](#)  
[Duo Trust Package](#)  
[Corporate Trust Package](#)

[View all Trust Packages >](#)



## Build and share your own document collection

Use **My collection** to easily access and organize your important documents. Create custom folders where you can view, download and share content.

[Trust Portal Guide](#)

[Trust Portal FAQ >](#)

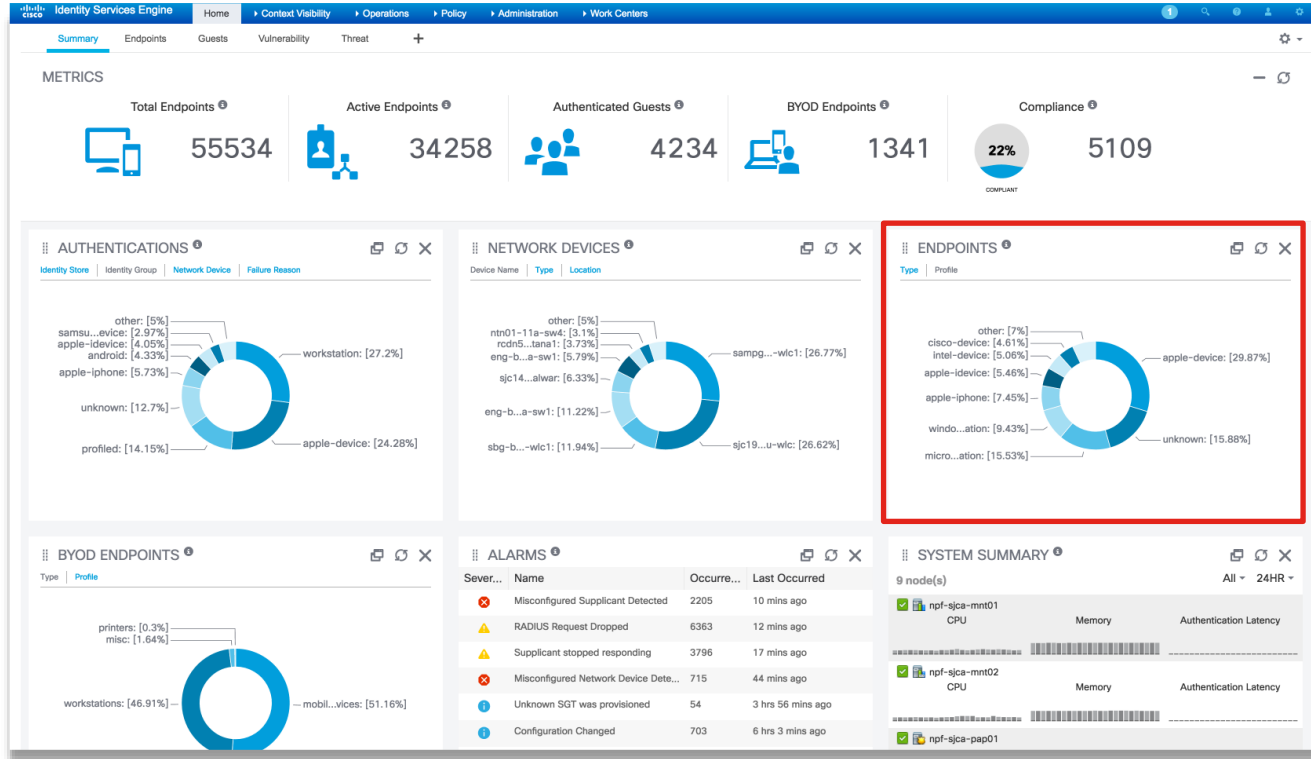
<https://trustportal.cisco.com/>

# ISE

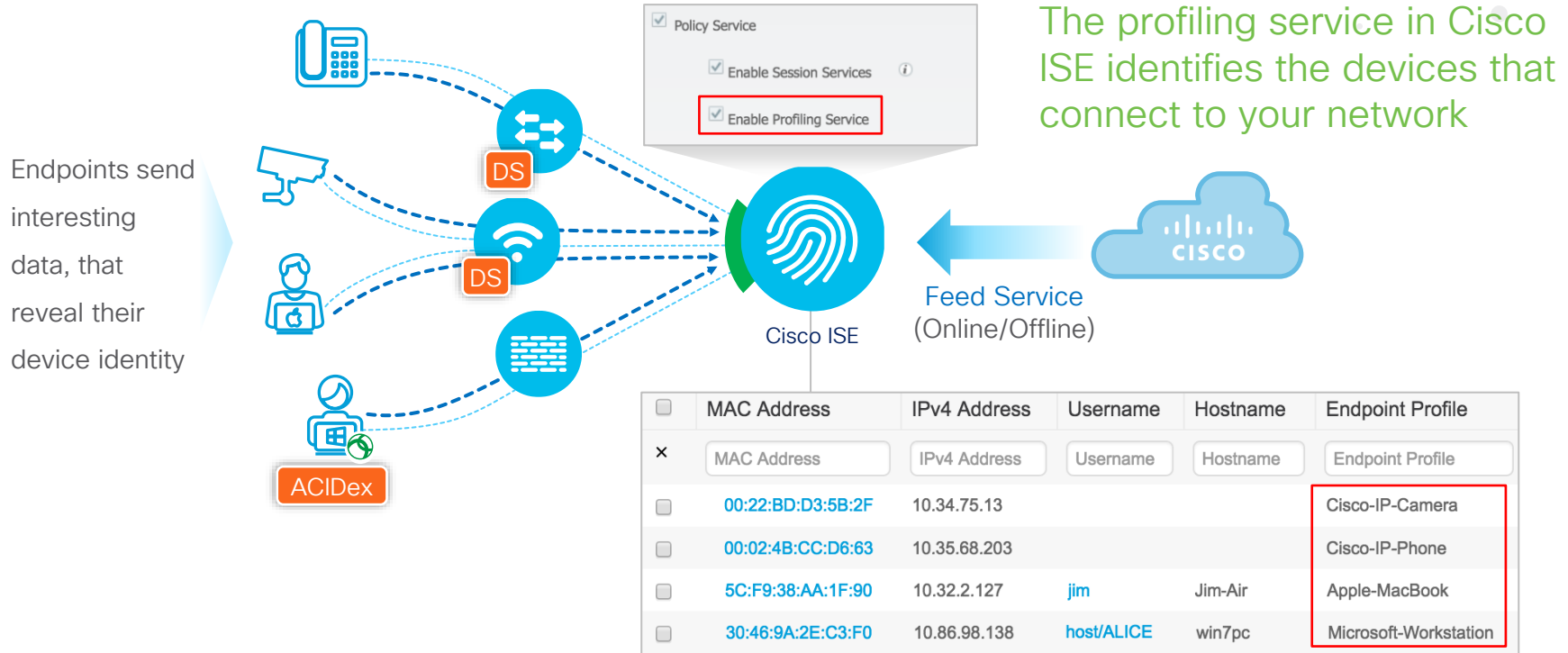
## Device Profiling



# ISE Device Profiling – What are we talking about?

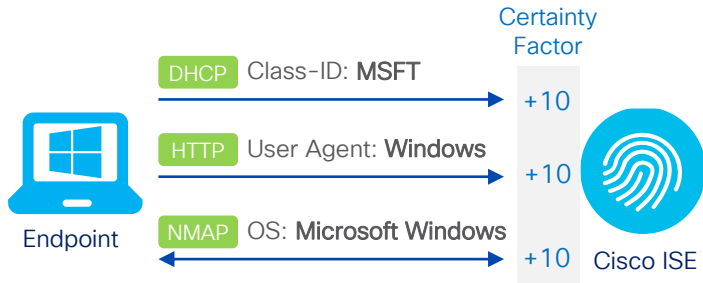


# ISE Device Profiling



# ISE Profiles based on 'profiling policies'

The minimum 'certainty metric' in the profiling policy evaluates the matching profile for an endpoint.



- DHCP:dhcp-class-identifier CONTAINS MSFT
- DHCP:dhcp-class-identifier CONTAINS MS-UC-Client
- IP:User-Agent CONTAINS Windows
- NMAP:operating-system CONTAINS Microsoft Windows

Profiler Policy List > Microsoft-Workstation

### Profiler Policy

\* Name: Microsoft-Workstation Description: Generic policy for Microsoft workstation

Policy Enabled ☒

\* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

\* Exception Action: NONE

\* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy ☐ Yes, create matching Identity Group ☒ No, use existing Identity Group hierarchy

Parent Policy: Workstation

\* Associated CoA Type: Global Settings

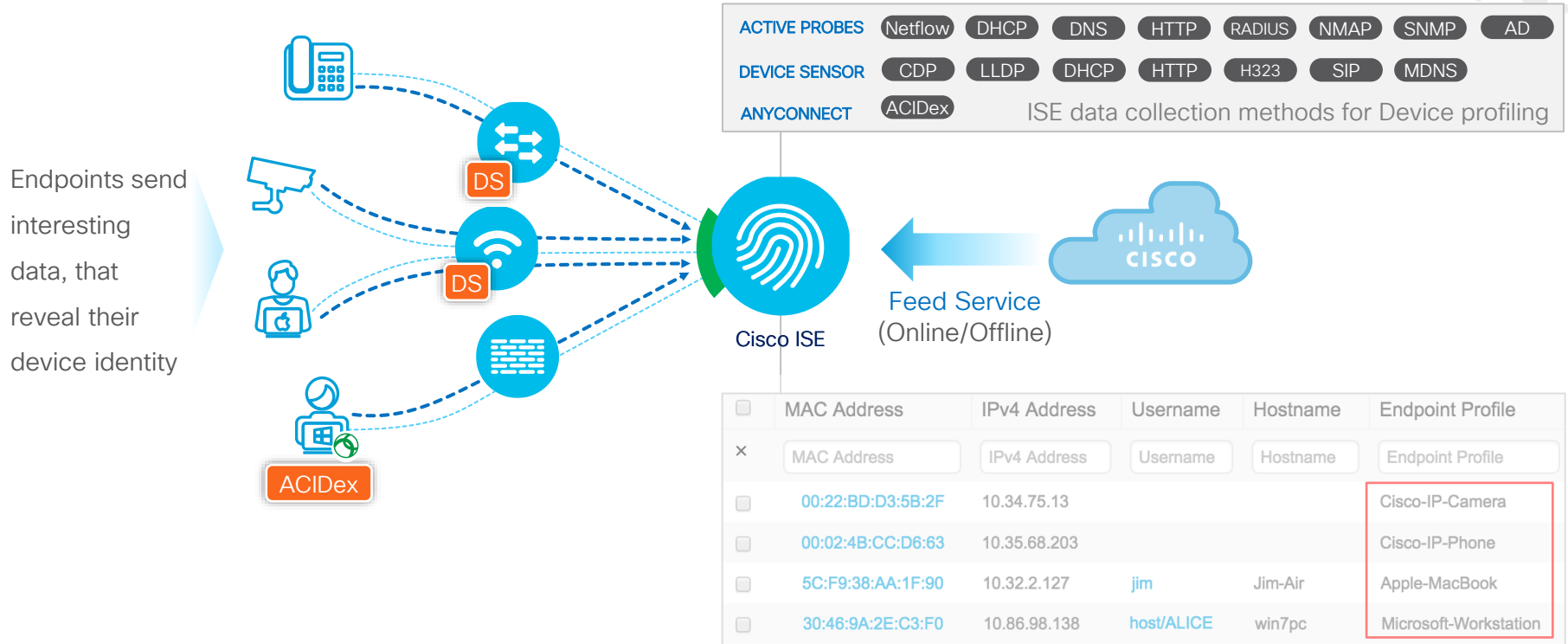
System Type: Cisco Provided

#### Rules

If Condition	Microsoft-WorkstationRule1Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-Workstation-Rule4-Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-WorkstationRule2Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-WorkstationRule3Check1	Then	Certainty Factor Increases	10

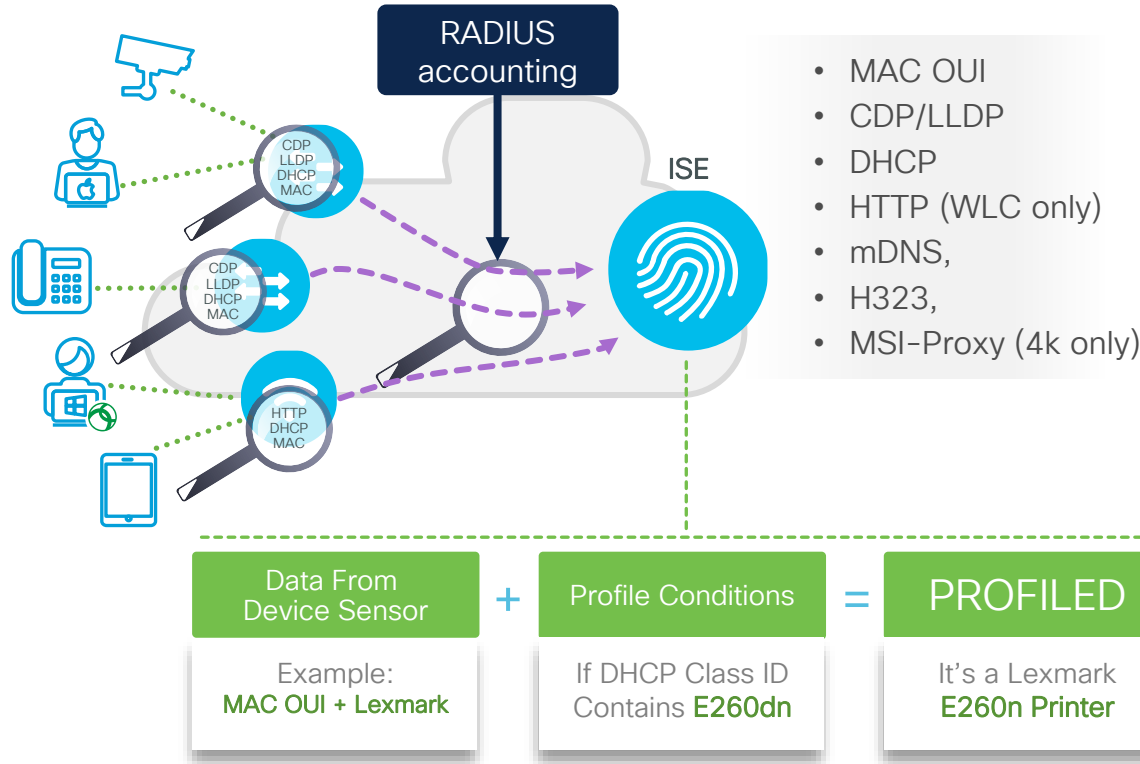
BRKARC-2021

# ISE Profiling – Data sources



AnyConnect Identity Extensions (ACIDex) | Device Sensor (DS)

# Device Sensor



## RADIUS

Description The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP, HTTP



From 15.0(2)SE

device-sensor accounting  
device-sensor notify all-changes



From AireOS 7.2

## Radius Client Profiling

DHCP Profiling ☒  
HTTP Profiling ☒

WLANs > (SSID) > Advanced

# Network access based on device profile

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Authentication Policy (3)

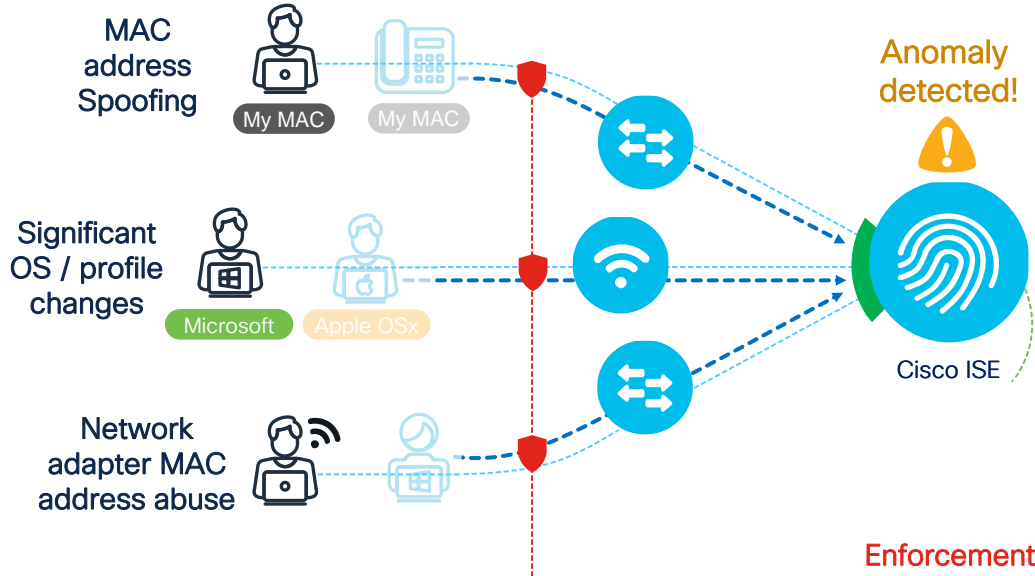
Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (12)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
+	✓	Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	* Cisco_IP_Phones +	IPPhones x +	0	⚙
+	✓	Printers	EndPoints-LogicalProfile EQUALS Printers	* PermitAccess +	Printers x +	0	⚙
+	✓	Basic_Authenticated_Access	Network_Access_Authentication_Passed	* PermitAccess +	Select from list +	0	⚙
+	✓	Default		* DenyAccess +	Select from list +	0	⚙

# Profiler: Anomaly detection



## Profiler Configuration

\* CoA Type: No CoA

Current custom SNMP community strings: .....

Change custom SNMP community strings:

Confirm changed custom SNMP community strings:

EndPoint Attribute Filter: ☐ Enabled

Enable Anomalous Behaviour Detection: ☒ Enabled

Enable Anomalous Behaviour Enforcement: ☒ Enabled

## Anomaly Detection and Enforcement

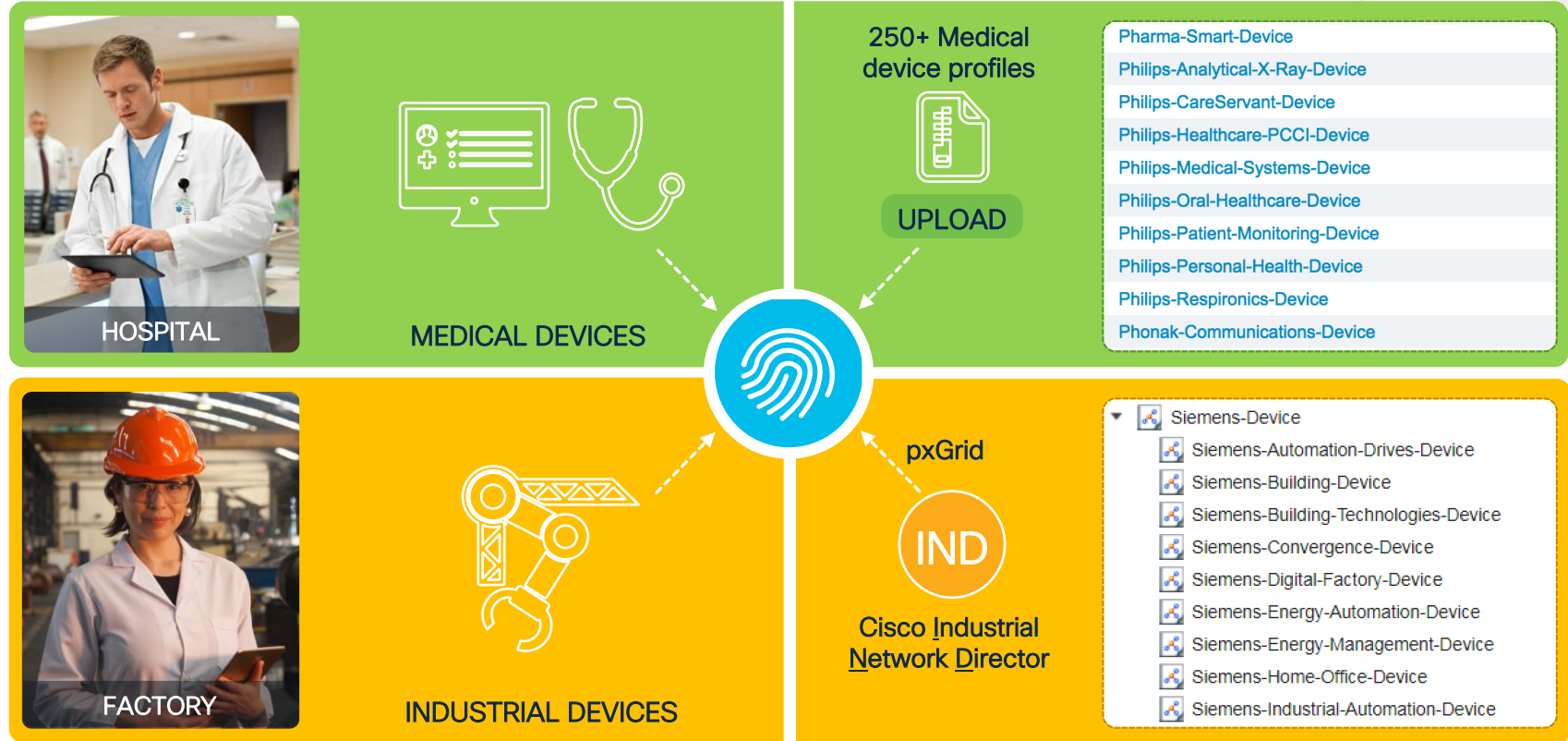
Upon change in any of the following:

- NAS-Port-Type
- DHCP Class ID
- Operating System
- Endpoint Policy

▼ Authorization Policy - Local Exceptions (1)

	Status	Rule Name	Conditions	Results	Security Groups
+				Profiles	
Search					
+	✓	Anomaly Action	EndPoints-AnomalousBehaviour EQUALS true	Limited Access	Quarantined_Systems

# Medical NAC and Internet of Things



IoT profiles ships with ISE 2.4. Profiling data collection via pxGrid

# IPsec, MACSEC, ... Security Improvements



# Catalyst 9300X

## Purpose Built for the New Edge



Cisco Catalyst 9300X

Encryption	Authentication
AES-128-CBC	HMAC/SHA1
AES-128/256-GCM	GMAC
Tunnel mode	
Encapsulation - ESP	
IKEv2	

Static virtual tunnel interface

IPv4/IPv6

OSPF/BGP

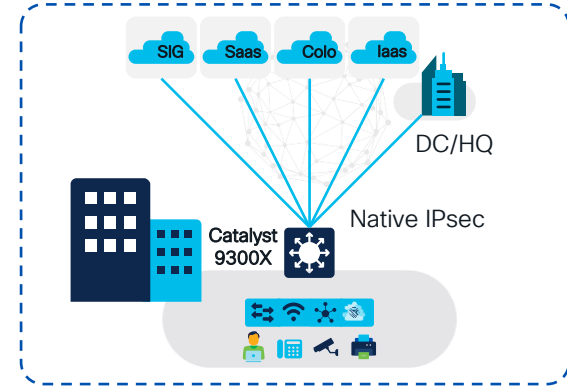
PBR + Set interface\*

NAT traversal\*

Multicast routing\*

Layer 3 segmentation over IPsec\*

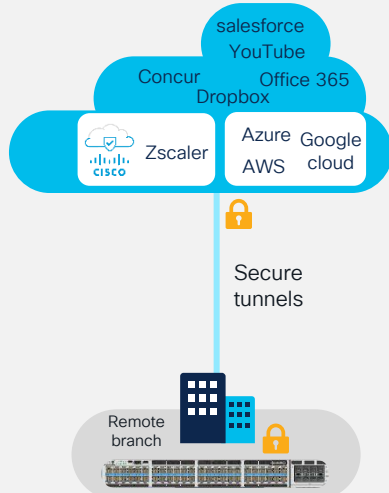
Layer 2 extension over IPsec\*



\* Roadmap.

# Catalyst 9300X

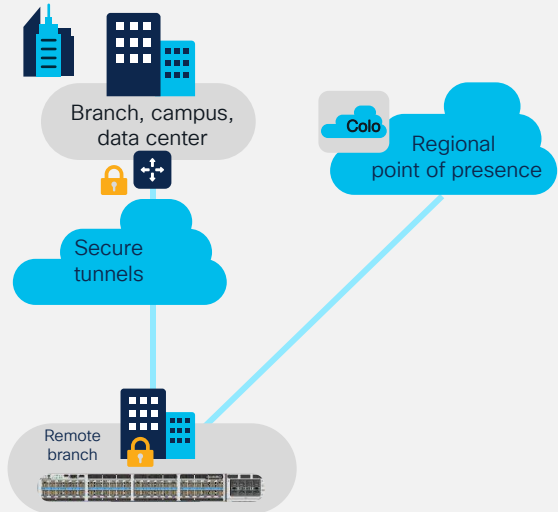
## Secure Connectivity to Anywhere



Cisco Catalyst 9300X

### Site to cloud

Standards-based IPsec for secure direct internet access and cloud-native workloads



Cisco Catalyst 9300X

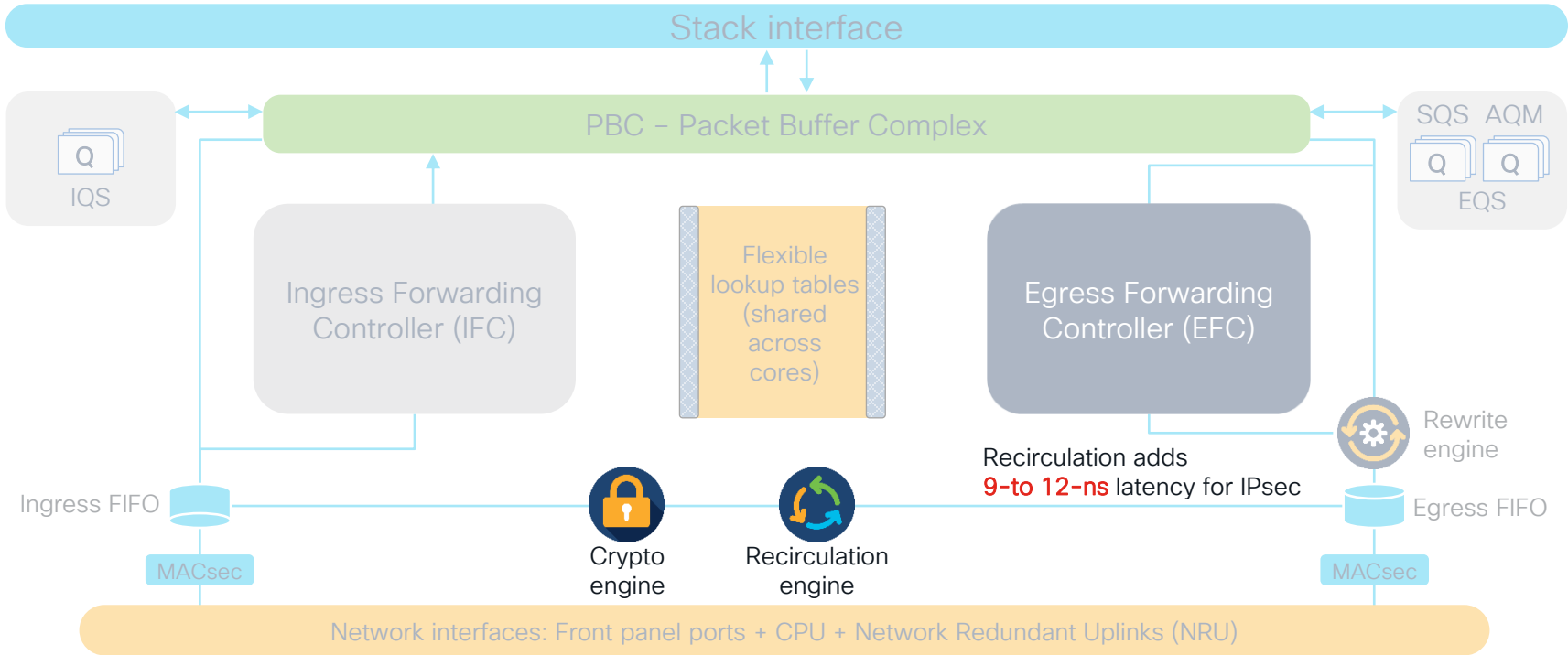
### Site to site

100G line-rate IPsec encryption with low-latency forwarding

\* Roadmap.

# UADP 2.0sec

## Crypto Engine

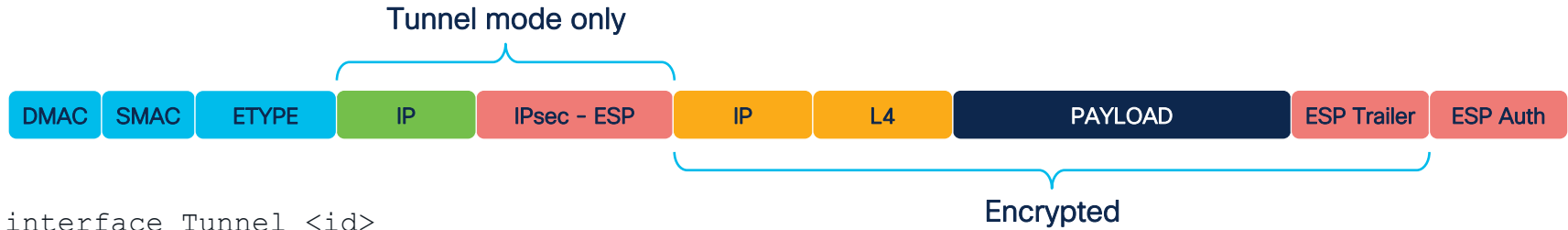


# IPsec Static Virtual Tunnel Interface (SVTI)



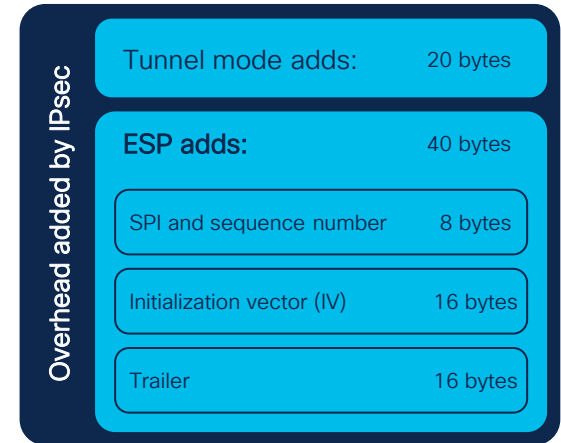
- SVTI provides a virtual routable interface using IP-in-IP encapsulation
- SVTI terminates IPsec tunnel and is used to assign protection parameters
- SVTI interface is UP when Secure Associations (SAs) are established
- SVTI interface has a single destination

# IPsec with SVTI



```
interface Tunnel <id>
  tunnel mode ipsec {ipv4 | ipv6}
  tunnel protection ipsec profile default
```

- IP in IP → Less overhead
- Mixed mode – IPv4 over IPv6 (tunnel mode ipsec ipv4 v6-overlay) or vice versa



# Supported IKEv2 proposal

IKEv2 (SW) proposal	Encryption	Integrity	Diffie-Hellman
Models supported	<ul style="list-style-type: none"><li>• des*</li><li>• 3des*</li><li>• aes-cbc-128</li><li>• aes-cbc-192</li><li>• aes-cbc-256</li><li>• aes-gcm-128</li><li>• aes-gcm-256</li></ul>	<ul style="list-style-type: none"><li>• md5*</li><li>• sha1*</li><li>• sha256</li><li>• sha384</li><li>• sha512</li></ul>	<ul style="list-style-type: none"><li>• 1 – 768 MODP*</li><li>• 2 – 1024 MODP*</li><li>• 5 – 1536 MODP*</li><li>• 14 – 2048 MODP</li><li>• 15 – 3072 MODP</li><li>• 16 – 4096 MODP</li><li>• 19 – 256 ECP</li><li>• 20 – 384 ECP</li><li>• 21 – 521 ECP</li><li>• 24 – 2048 (256 sub groups) MODP</li></ul>

\* CLI will show that these options are deprecated on Catalyst® 9300X.

# Supported transform sets (hardware)

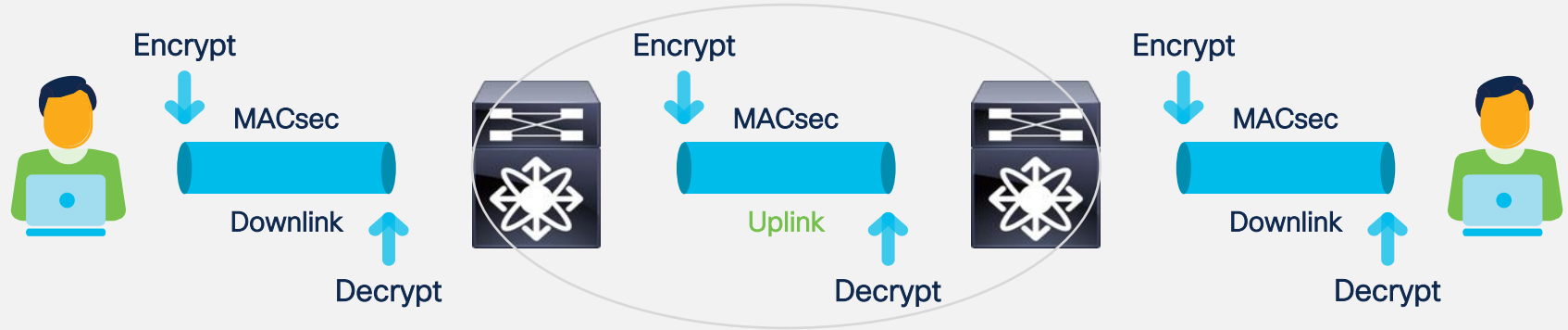
Transform set (HW) encryption	Bandwidth
esp-aes + esp-sha-hmac	Up to 15 Gbps
esp-gcm 128 (gmac is derived)	Up to 100 Gbps
esp-gcm 256 (gmac is derived)	Up to 100 Gbps

## Catalyst® 9300X IPsec performance

	Catalyst 9300X
IPsec throughput (for all tunnels total)	100 Gbps
Total number of tunnels at FCS	128 (2 SAs per 128 tunnels + 128 rekey = 384 SAs)
New established tunnels per second	25

# MACsec

## Hop-by-hop encryption via 802.1AE



- Packets are encrypted on egress, decrypted on ingress
- Offers line-rate encryption on all ports and speeds (1G, 2.5G, 5G, 10G, 25G, 40G, and 100G)
- Transparent to all upper-layer protocols
- Supports switch-to-switch and switch-to-host MACsec
- 256-bit MACsec-capable between switch to switch
- Manual or 802.1X modes supported

# MACsec-256 link encryption

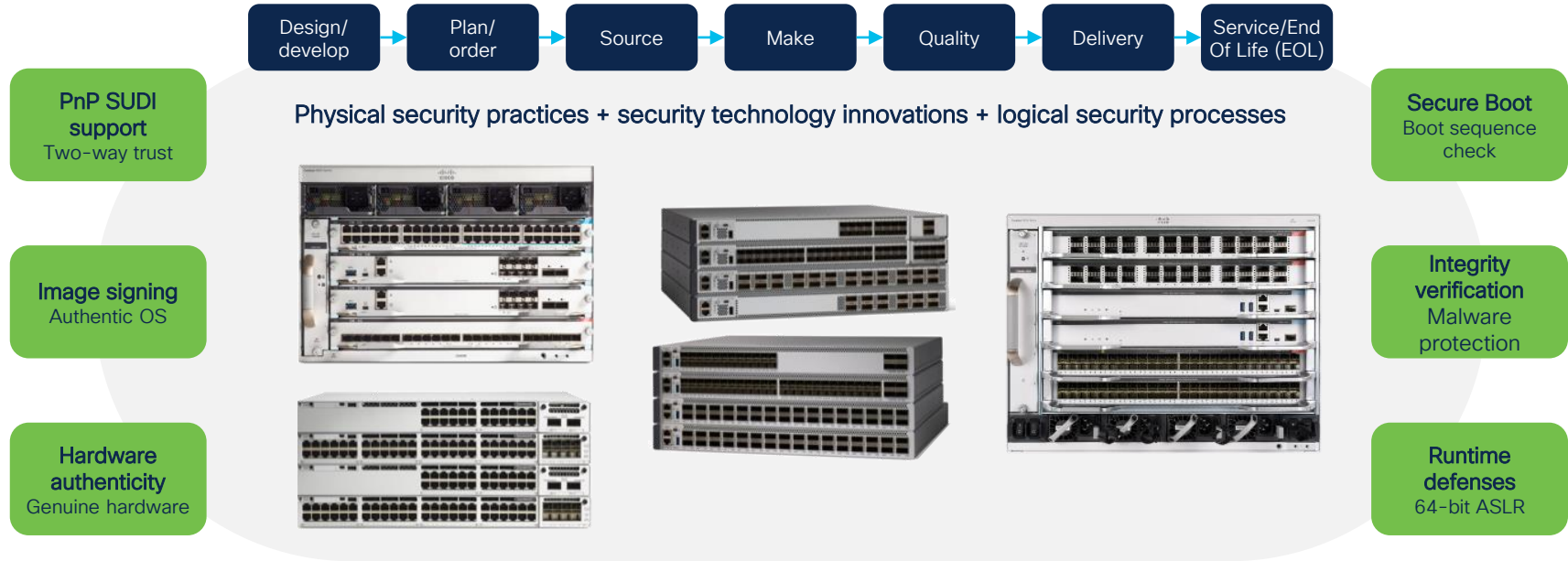
Hop-by-hop encryption via 802.1AE

MACsec	
Switch to switch	128 bits Security Association Protocol (SAP)
	128 bits MACsec Key Agreement (MKA)
	256 bits MKA
Host to switch	128 bits MKA
	256 bits MKA

- Supported on all models (modular and fixed SKUs)
- For C9300-48UXM and C9300-48UN switch models, MACsec is supported only on the first 16 downlink ports

# Cisco Catalyst 9000 platform

## Trustworthy solutions



Cisco Trustworthy Solutions use industry best practices to help ensure full development lifecycle integrity and end-to-end security

# PSIRT

What It Is, What It Provides,  
and Why



# What is PSIRT?

## Cisco Product Security Incident Response Team

Protection. Security. Transparency.

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.



# What is PSIRT?

## Cisco Product Security Incident Response Team

Protection. Security. Transparency.

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

**Over 20 years of experience helping to alert customers about vulnerabilities in Cisco products**



**The single entity authorized within Cisco to disclose vulnerability information to customers**



**Global team of incident managers providing 24/7 support**



**ISO 29147 compliant**



# How does PSIRT Operate?

Cisco Product Security  
Incident Response Team  
Protection. Security. Transparency.

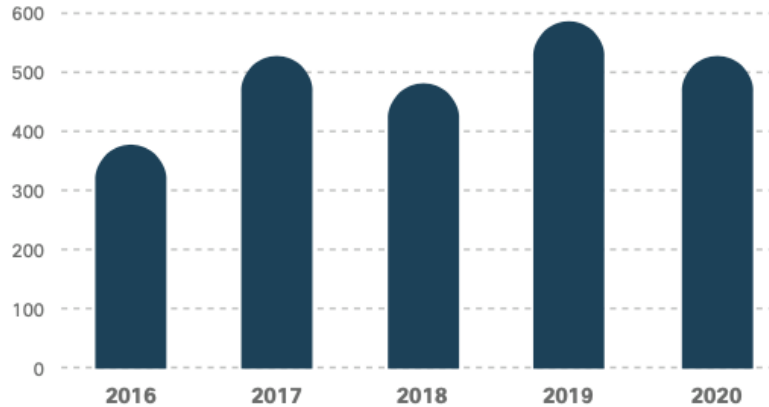
The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.



Incident  
Handling  
Process

# How does PSIRT Operate?

Cisco CVE Assignments



Assigning Common Vulnerabilities and Exposure (CVE) identifiers to internally and externally found vulnerabilities across hundreds of products reflects Cisco's commitment to transparency and helping customers mitigate risk.



Cisco  
proprietary code

+



Third-party software  
components

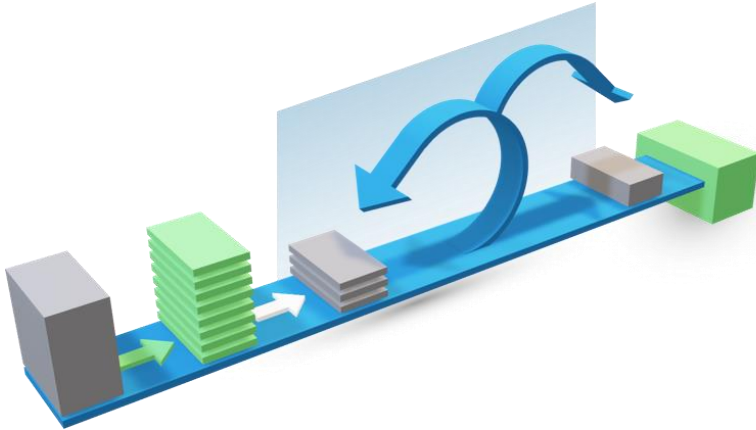
## COMPLETE PROTECTION:

PSIRT investigates vulnerabilities across the entire Cisco product portfolio.

# PSIRT – Policy

PSIRT investigates all reports, regardless of the Cisco software code version, through the last day of support for a given product.

Issues will be prioritized based on the potential severity of the vulnerability and other environmental factors. Ultimately, the resolution of a reported incident may require upgrades to products that are under active support from Cisco.



# PSIRT – Staying up to date

PSIRT investigates all reports, regardless of the Cisco software code version, through the last day of support for a given product.

## Receiving Security Vulnerability Information from Cisco

There are several ways to stay connected and receive the latest security vulnerability information from Cisco.

Cisco Security: [cisco.com/security](https://cisco.com/security)

Contact PSIRT: [psirt@cisco.com](mailto:psirt@cisco.com)

RSS feeds: <http://tools.cisco.com/security/center/rss.x?i=44>

My Notifications: <https://www.cisco.com/c/en/us/support/web/tools/cns/notifications.html>

Cisco PSIRT openVuln API: <https://developer.cisco.com/site/PSIRT/>

# PSIRT – Summary

**Industry Standards:** Follows standard rules, policies, and scoring systems



**Consistency:** Applies the same mature process across the Cisco portfolio, even as the product line grows



**Best-in-Class Service:** Provides dedicated support for product security and network protection



**Speed:** Quickly assigns CVEs for security vulnerabilities



**Collaboration:** Works with product teams across Cisco and third parties



**Transparency:** Publicly discloses both internally and externally reported vulnerabilities



# TALOS

What It Is, What It Provides,  
and Why



# TALOS – Cisco Security Research

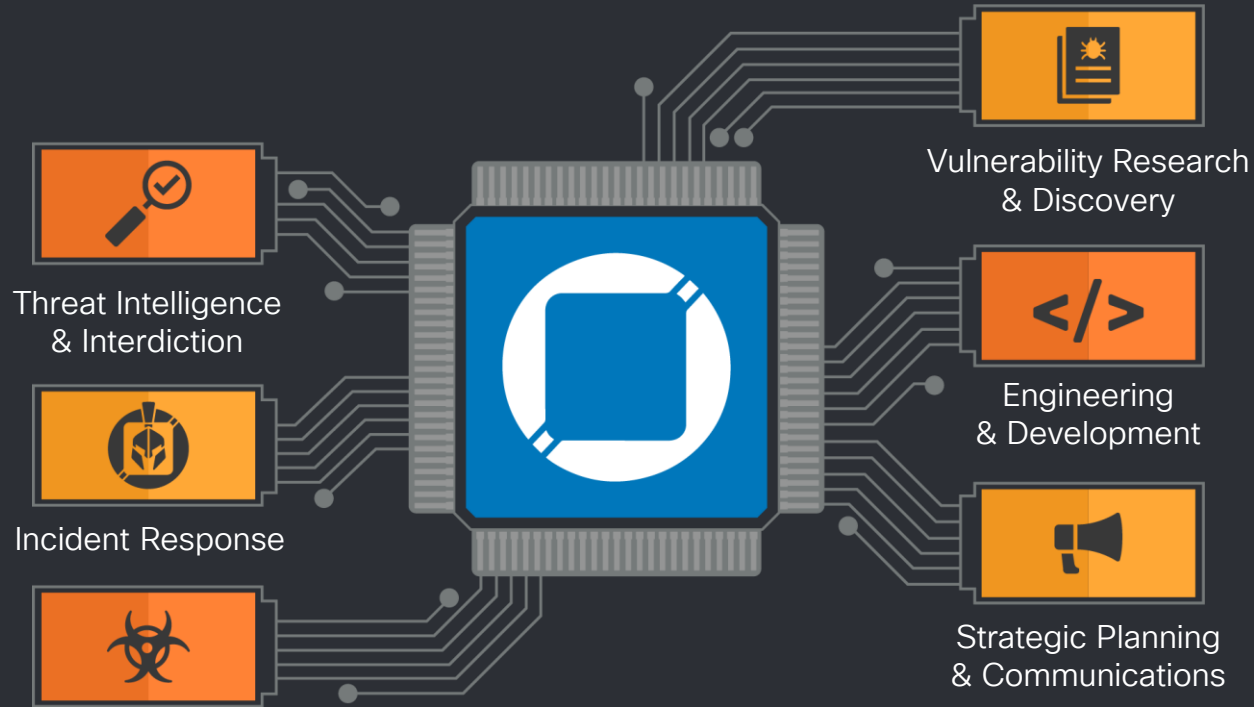


## Fighting the Good Fight

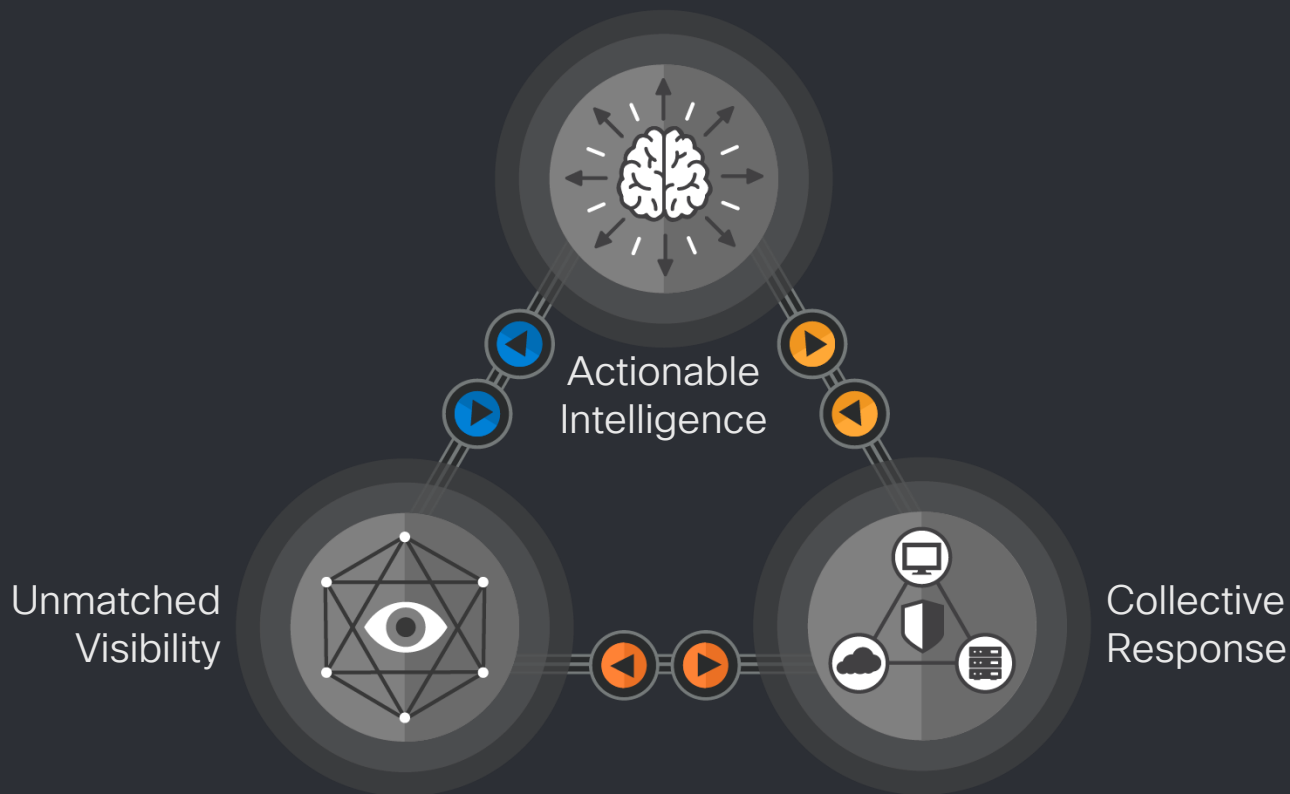
# Protecting Customers



# Our Job is Protecting Your Network



# Why Trust TALOS?



# Unmatched Visibility



To stop more, you have to see more.

- The most diverse data set
- Community partnerships
- Proactively finding problems

Unmatched visibility is built on relationships



# Actionable Intelligence



Security controls are best served by data that lets tools respond to immediate threats.

- Rapid coverage
- Distillation and analysis
- Threat Context

It's not detect and forget, it's detect and analyze.



# Collective Response



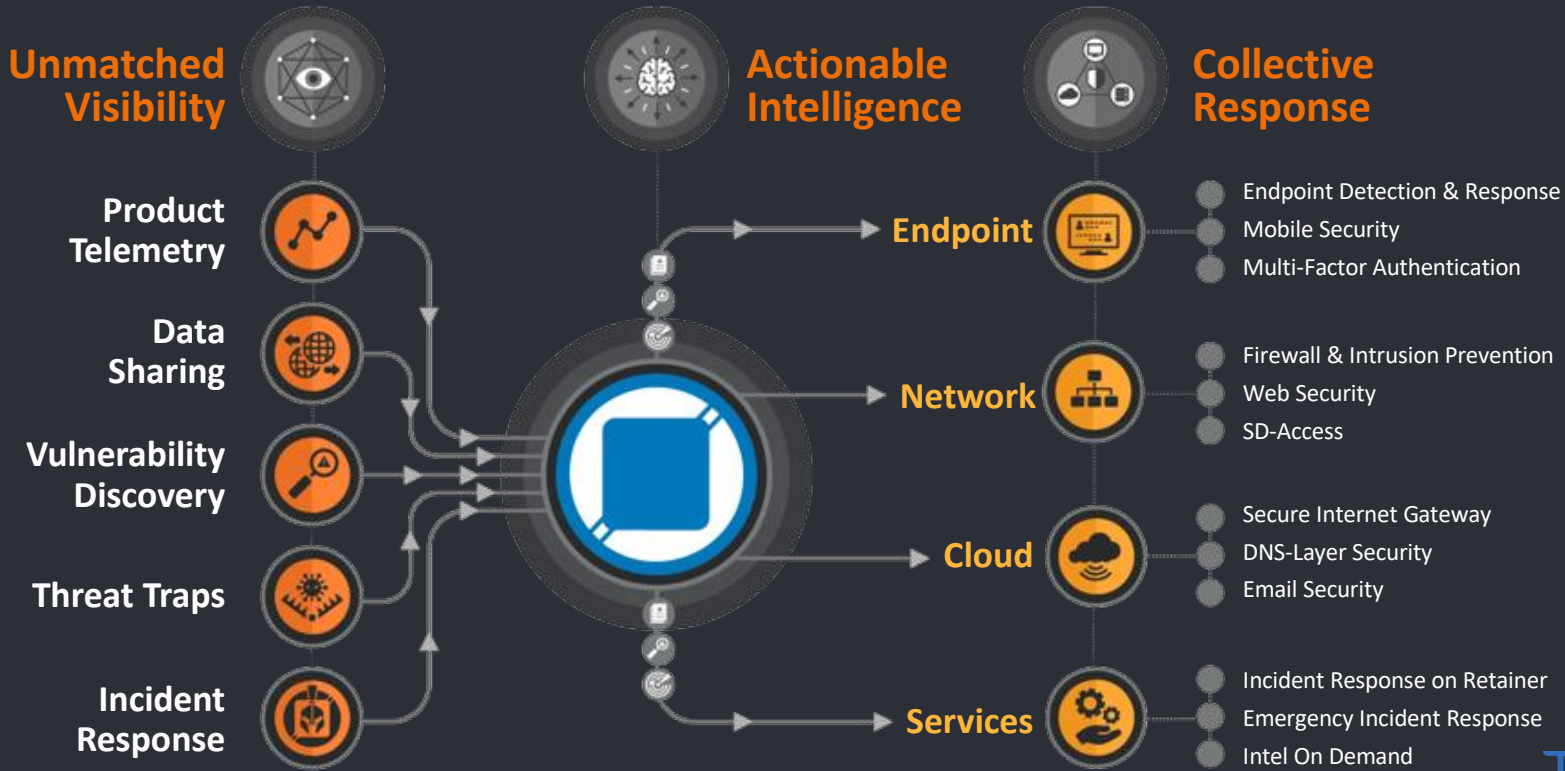
The ability to bring rapid protection to close off multiple attack vectors instantaneously is crucial

- **Breadth:** See once, protect everywhere
- **Depth:** Response and interdiction drives continuous research
- **Scale:** Delivering portfolio-wide protection, in real-time



**TALOS**  
Cisco Security Research

# From Unknown to Understood



# TALOS – Stay Connected and Up-to-Date



Talos publicly shares security information through numerous channels to help make the internet safer for everyone.

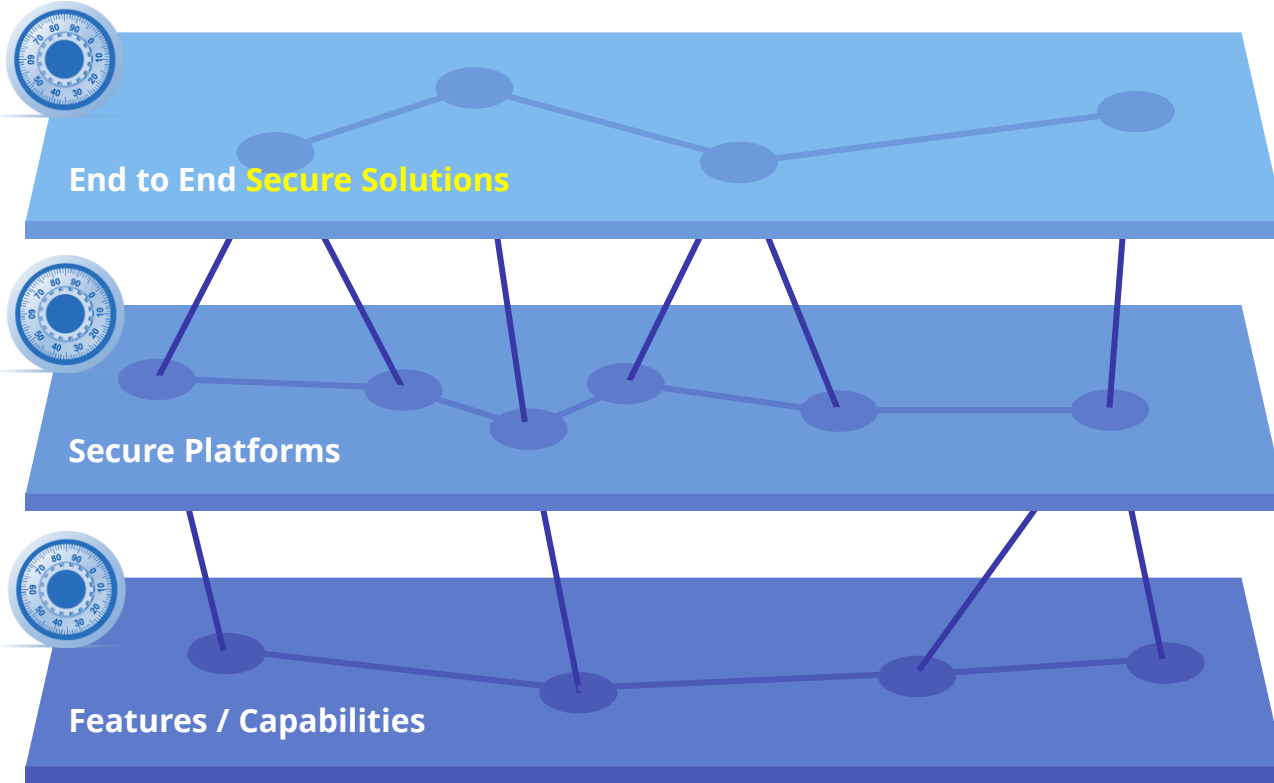
# Summary

*Solution*

Building a Secure Product



# Building Secure Solutions



Not just at initial deployment – but over the **ENTIRE LIFECYCLE** of your network and apps



# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](https://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

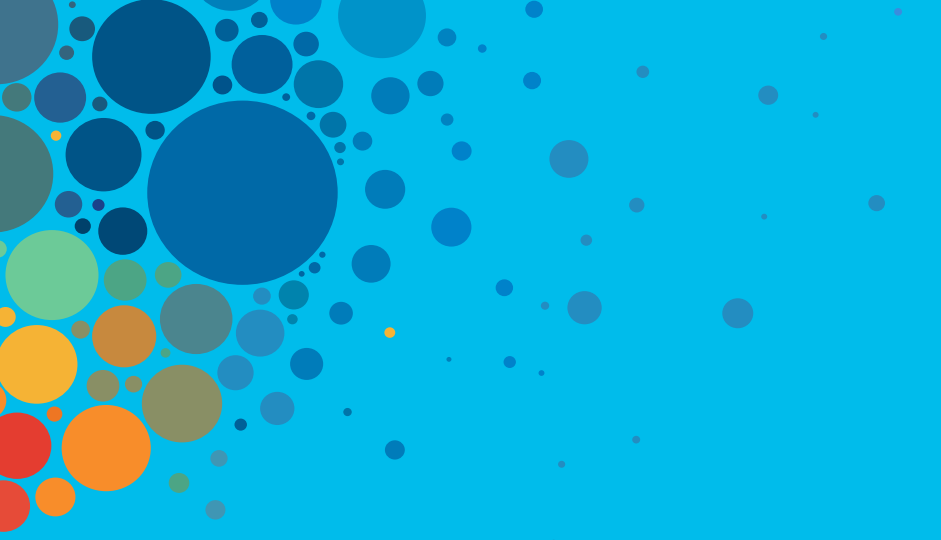
### Cisco Guided Study Groups

180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# 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](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*



#CiscoLive