You make **possible**

Foundational Trust

For Foundational Infrastructure

Matt Carling, Security Architect, Trust Transformation Office

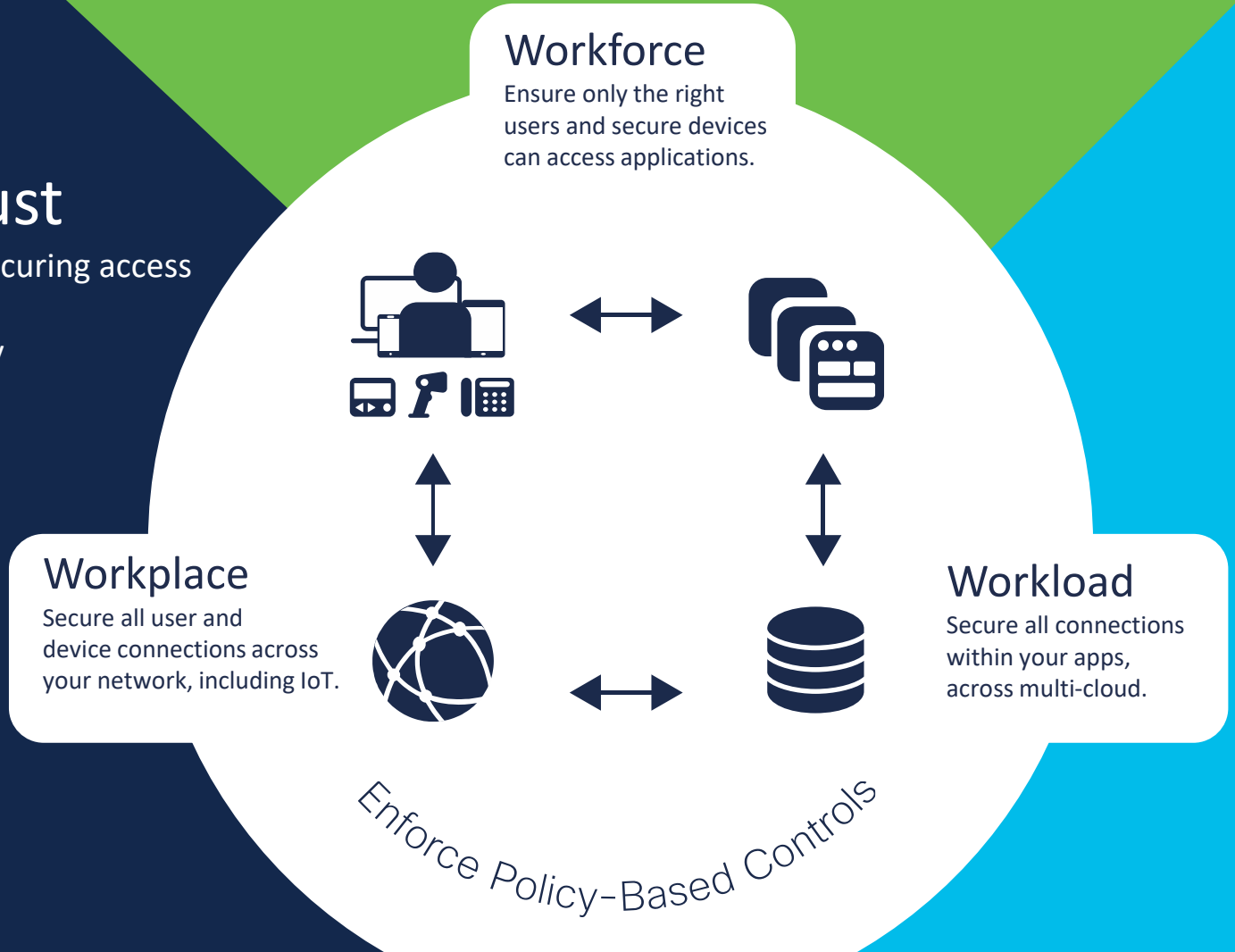
BRKSEC-2634

Agenda

- Zero Trust and Trustworthiness
- Security Culture
- Platform Integrity
- ZTP
- Trust Visibility
- Call to action

Cisco Zero Trust

A zero-trust approach to securing access across your applications and environment, from any user, device and location.



Workforce

Zero-Trust Security

Verify user & device trust with multi-factor authentication (MFA)

Enforce access policies for every app with adaptive & role-based access controls

Continuously monitor risky devices with endpoint health & management status

Workloads

Zero-Trust Security

Gain visibility into what's running & critical by identifying workloads & enforcing policies

Contain breaches & minimise lateral movement with application micro-segmentation

Alert or block communications by continuously monitoring & responding to indicators of compromise

Workplace

Zero-Trust Security

Discover & classify devices with IoT device profiling, BYOD & user device posture.

Network access control policies for users & devices with network segmentation.

Continuous monitoring with vulnerability assessments & identifying indicators of compromise.

Trust Requires a Trustworthy Foundation

Workforce Workplace Workload

Cisco Zero Trust

Network Integrity

Device Level Attack Protection

- DHCP Snooping
- Port Security
- uRPF
- Intrusion Detection
- IP Source Guard
- ACLs

Solution Level Attack Protection

- TrustSec
- ISE
- Stealthwatch
- FnF

Platform Integrity

- Secure Boot
- Image Signing
- Counterfeit Protections
- Hardware Trust Anchor
- Runtime Defences
- OS Validation
- Modern Crypto
- Secure Device Onboarding

Security Culture

- Value Chain Security
- Open Source Registration
- Security Training
- Threat Modeling
- Product Security Baseline
- PSIRT Advisories

Cisco Secure Development Lifecycle

Security Culture

Increased Resilience in Solutions, Infrastructure

Trusted Partners of Genuine Solutions

Uncompromised integrity throughout solutions lifecycle – cradle to grave

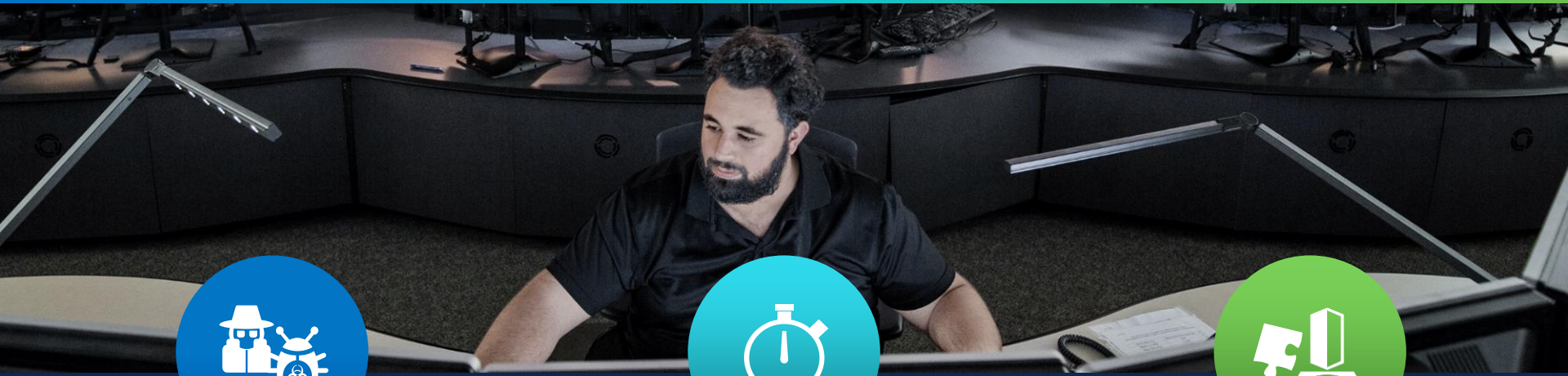
Design | Plan | Source | Make | Quality | Deliver | Sustain | End of Life

A Layered Approach

- Logical Security
- Security Technologies
- Physical Security Practices

Product Security Incident Response Team

Protect the Customer. Protect the Company.



Vulnerability Management

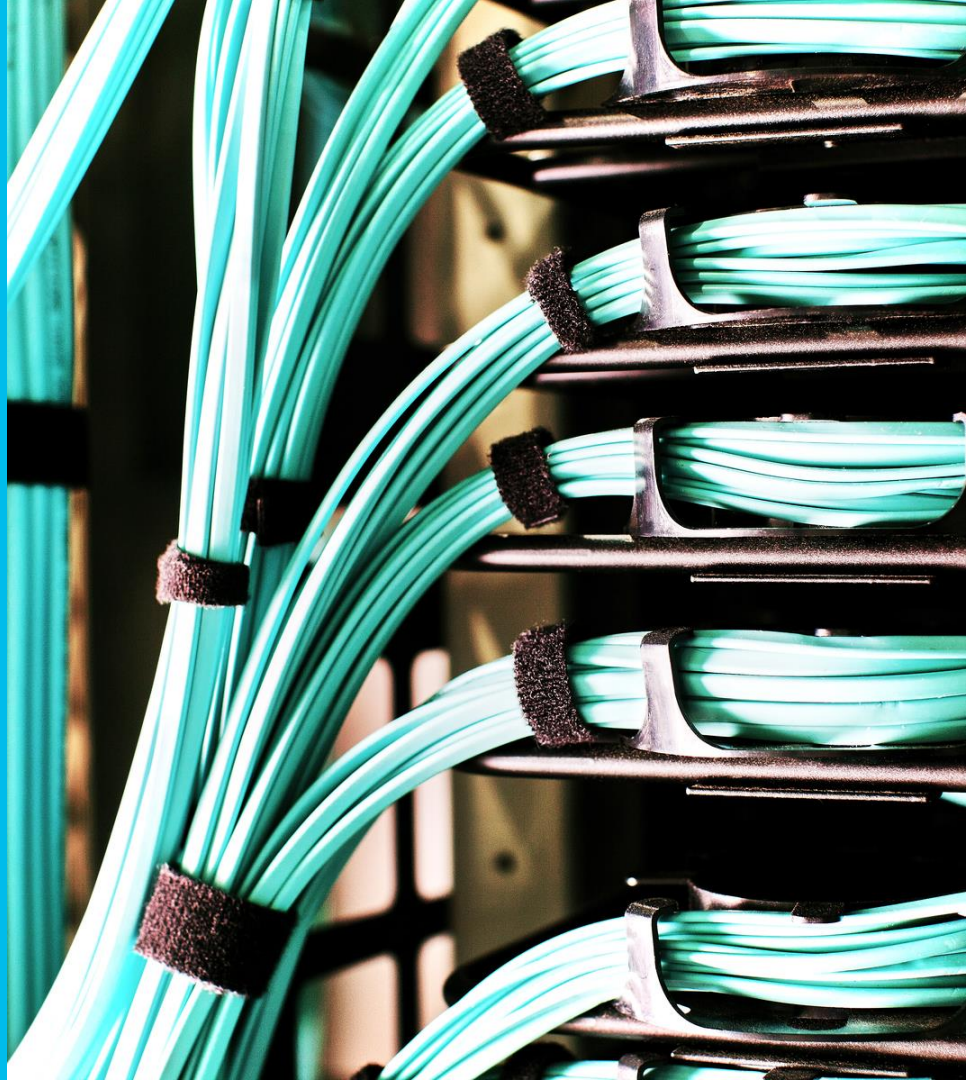
Incident Response

Proactive Engagement

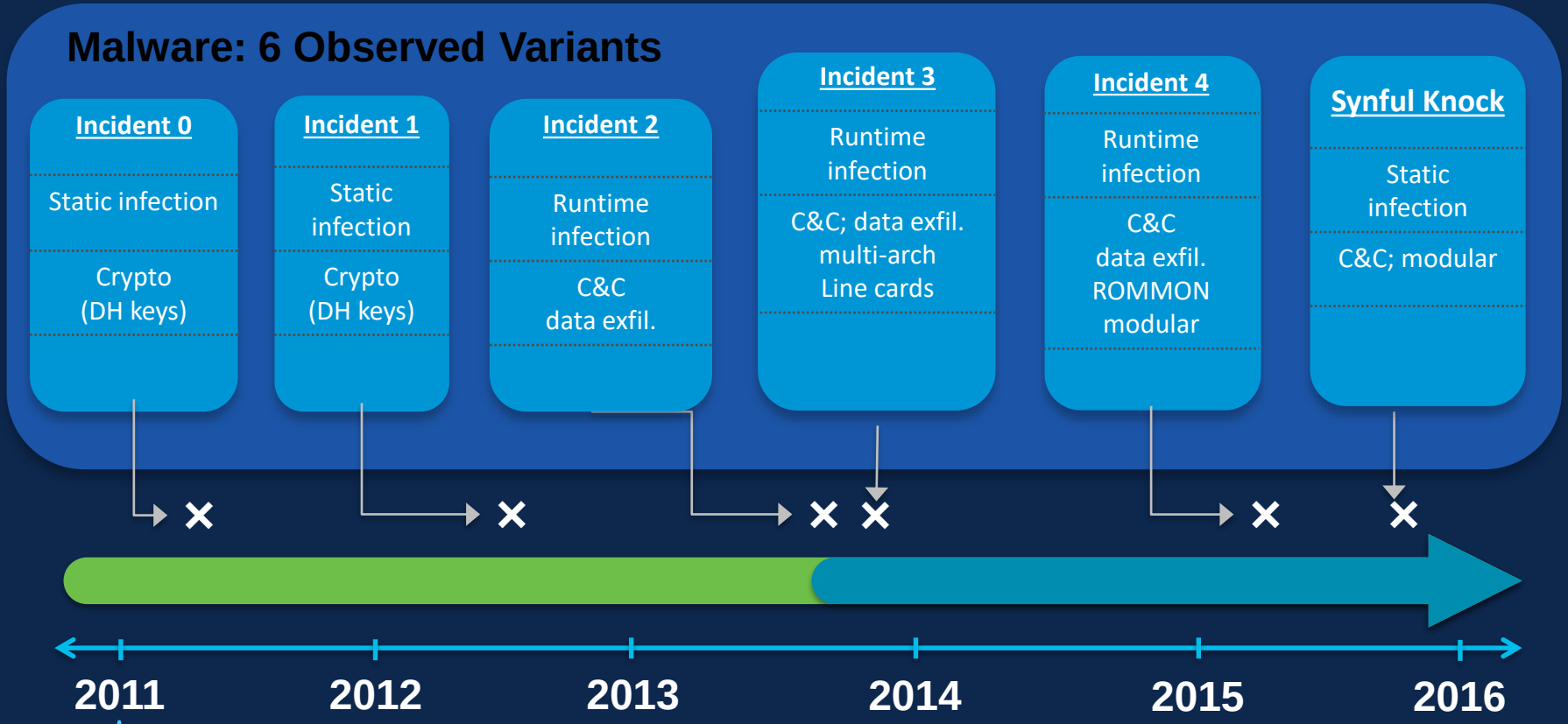
Cisco Secure Development Lifecycle

Platform Integrity

Direct attacks on network devices are a real threat

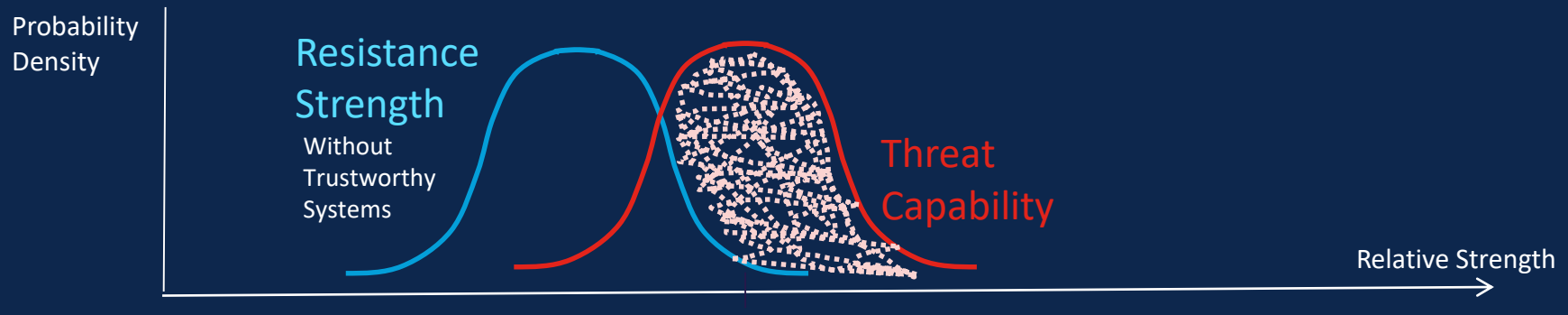


Malware in IOS is a Real Threat



Measuring Vulnerability

Probability that an attack results in a loss

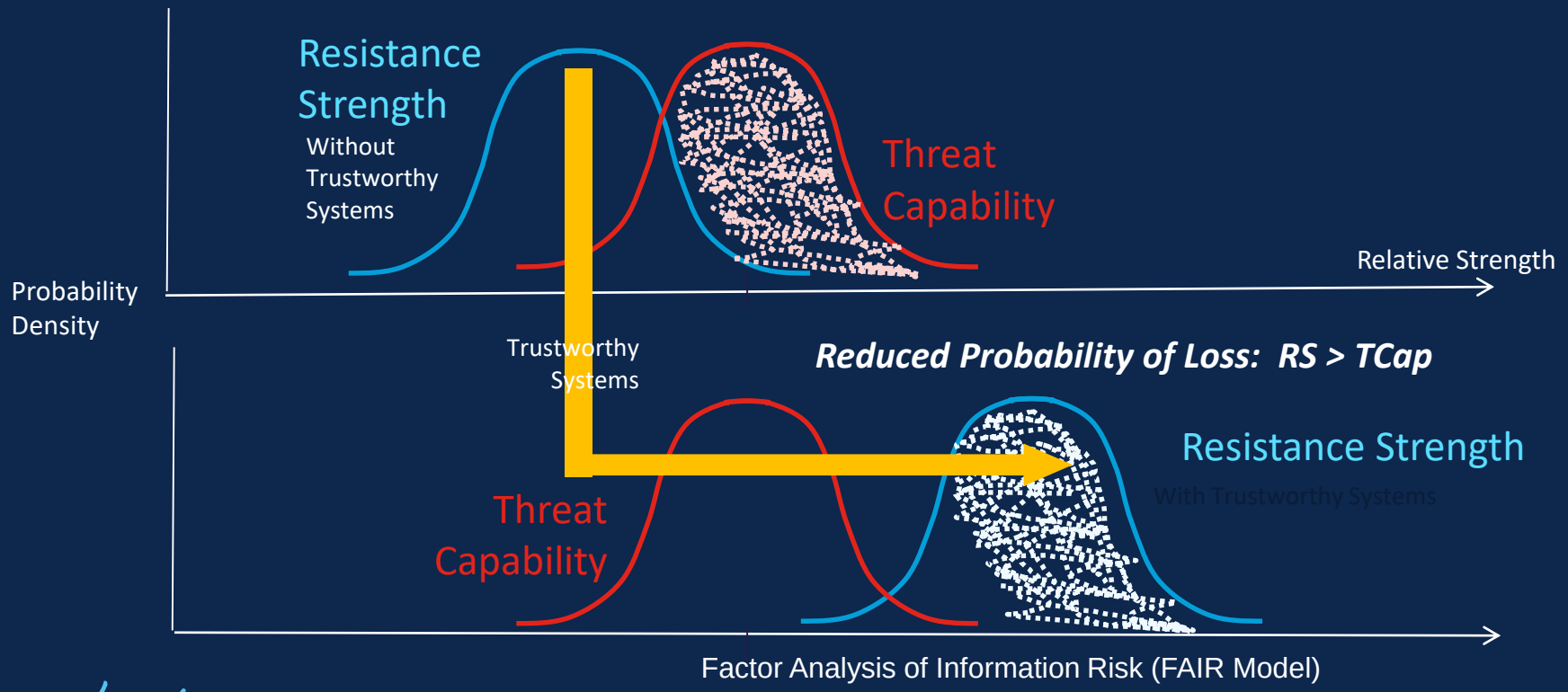


Threat Capability Exceeds Resistance Strength
Definite Probability of Loss

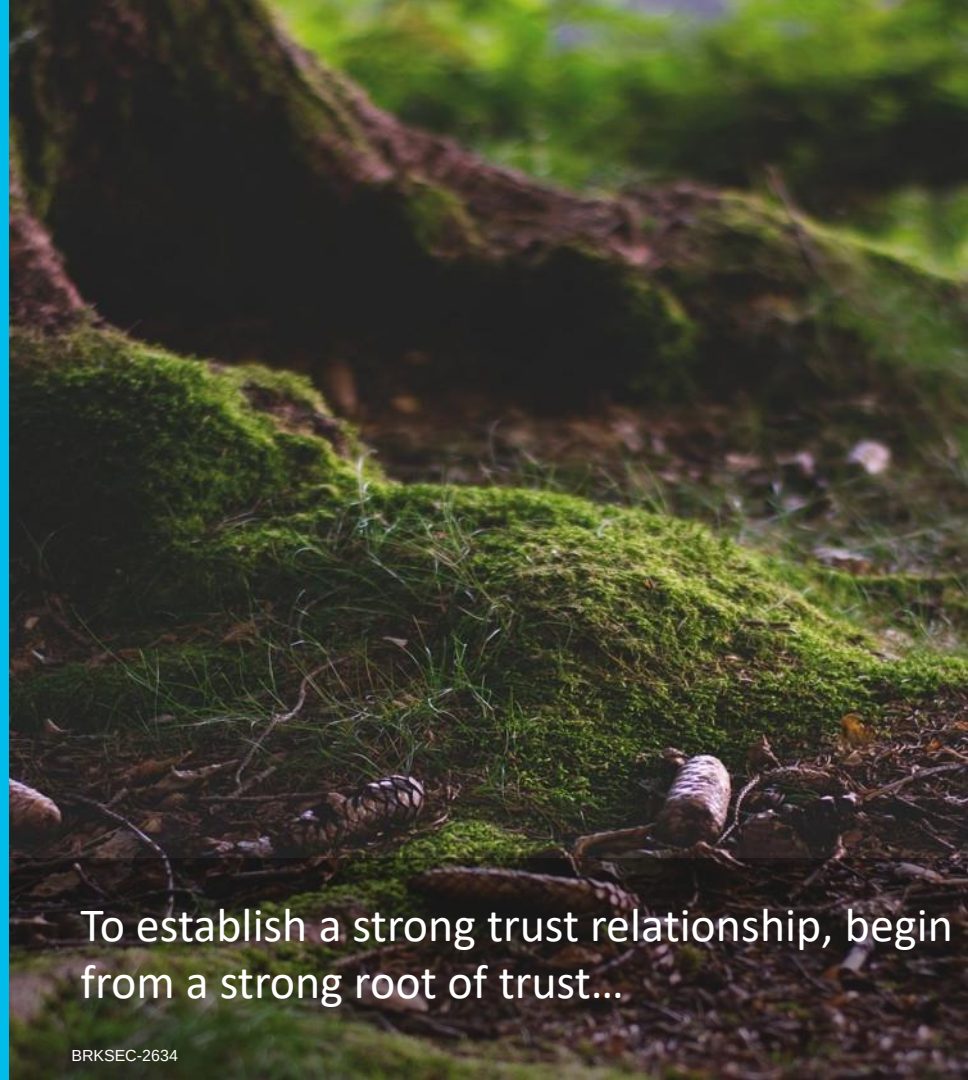
Factor Analysis of Information Risk (FAIR Model)

Trustworthy Technologies

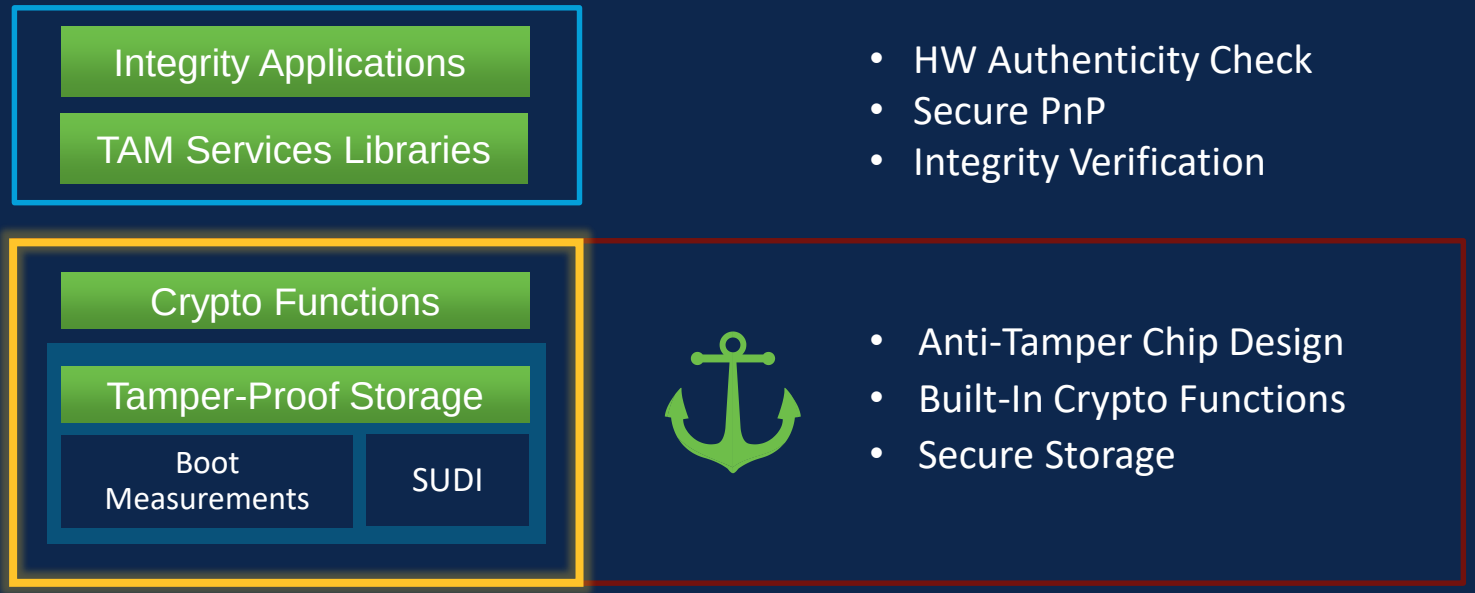
Increase Resistance Strength to Reduce Vulnerability



Cisco Trust Anchor



Cisco Trust Anchor Module (TAm)



- HW Authenticity Check
- Secure PnP
- Integrity Verification

- Anti-Tamper Chip Design
- Built-In Crypto Functions
- Secure Storage

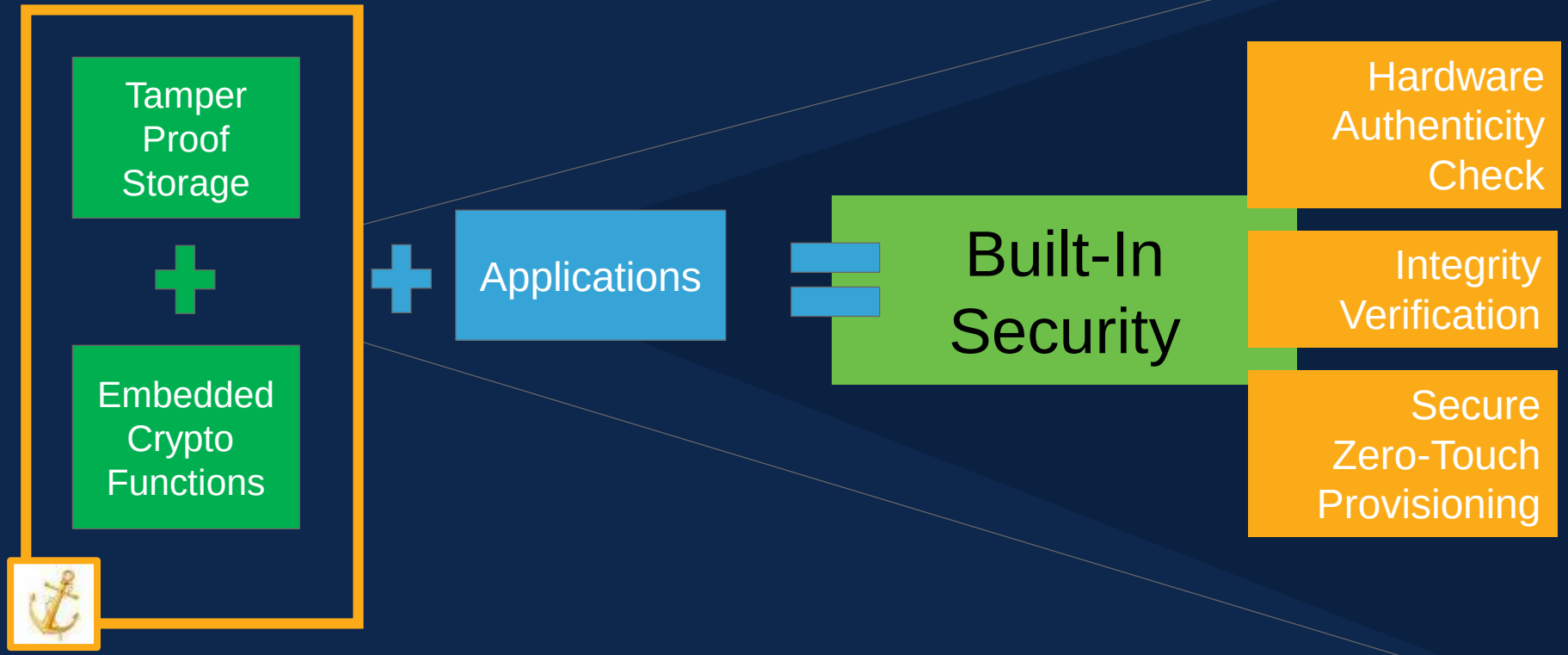
Secure Unique Device Identification (SUDI)

- Tamperproof ID for the device
- Binds the hardware identity to a key pair in a cryptographically secure X.509 certificate PID during manufacturing
- Connections with the device can be authenticated by the SUDI credential
- IEEE 802.1AR Compliant

Uses for SUDI

- Internal checks in the box
- Authentication Bootstrap Identity
- Remote Attestation

Cisco Trust Anchor Module



Modified Images & Secure Boot

CNN tech BUSINESS CULTURE GADGETS FUTURE STARTUPS

Security experts say 'Vault 7' leak describes common, public hacks

SYNful Knock router exploit isn't going away soon

By Tim Greene

Senior Editor, Network World | SEP 16, 2015 5:52 AM PT

NETWORKWORLD FROM IDG

CSO Mobile Security Data Protection Identity & Access CSOM CISO Leaders CSO Events Resources/Whitepapers Women in Security

Strategy for cyber crime: own the routers, own the Internet

By Rick McElroy, Carbon Black

Rick McElroy (CSO Online) on 10 April, 2017 05:18

Threat Scenario

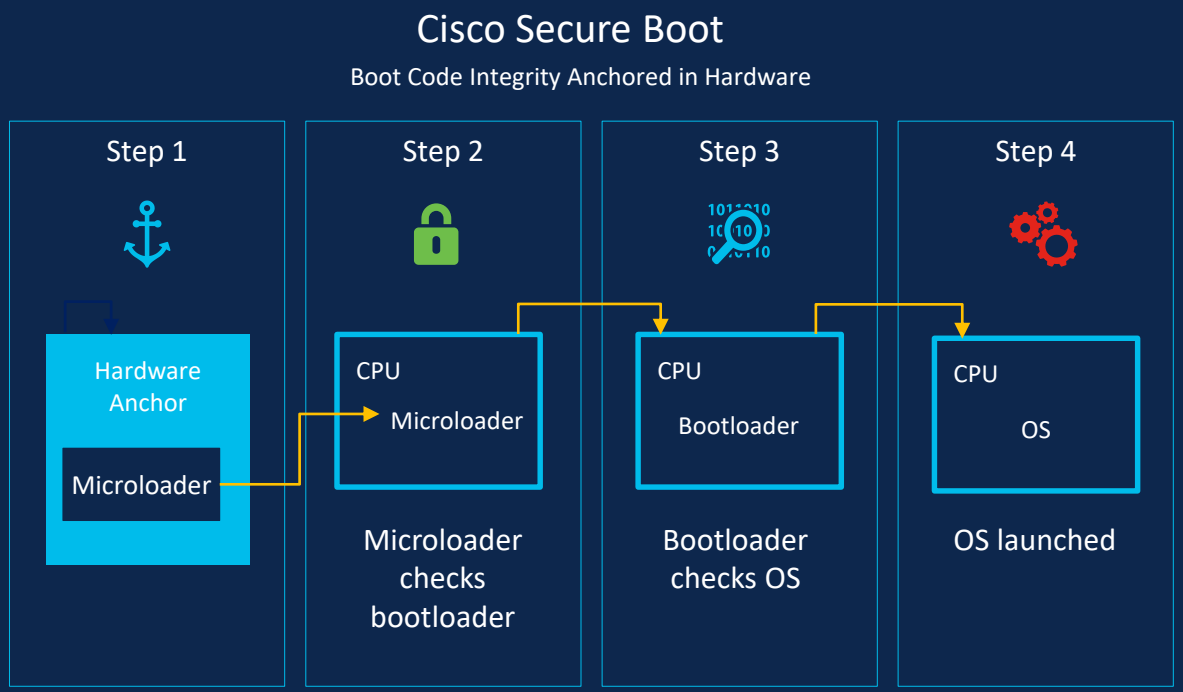
- Attacker causes modified software / firmware to be installed
- How?
  - Administrative access thru lost or stolen password
  - Infiltrating the network operations workflow
- The attackers goal:
  - Boot with modified SW
  - The system will be infected
  - Modified code can persist thru reboot

What can the attacker do?

- Target specific email addresses, MAC addresses, IP addresses
- Redirect targeted network traffic
- Redirect targeted browser connections
- Proxy VPN traffic
- Copy all network traffic
- Harvest email addresses, chat usernames, VOIP numbers

Cisco Secure Boot

Anchors Secure Boot in Hardware to Create a Chain of Trust



- Only authentic signed Cisco software boots up on a Cisco platform
- The boot process stops if any step fails to authenticate

ROMMON Protection

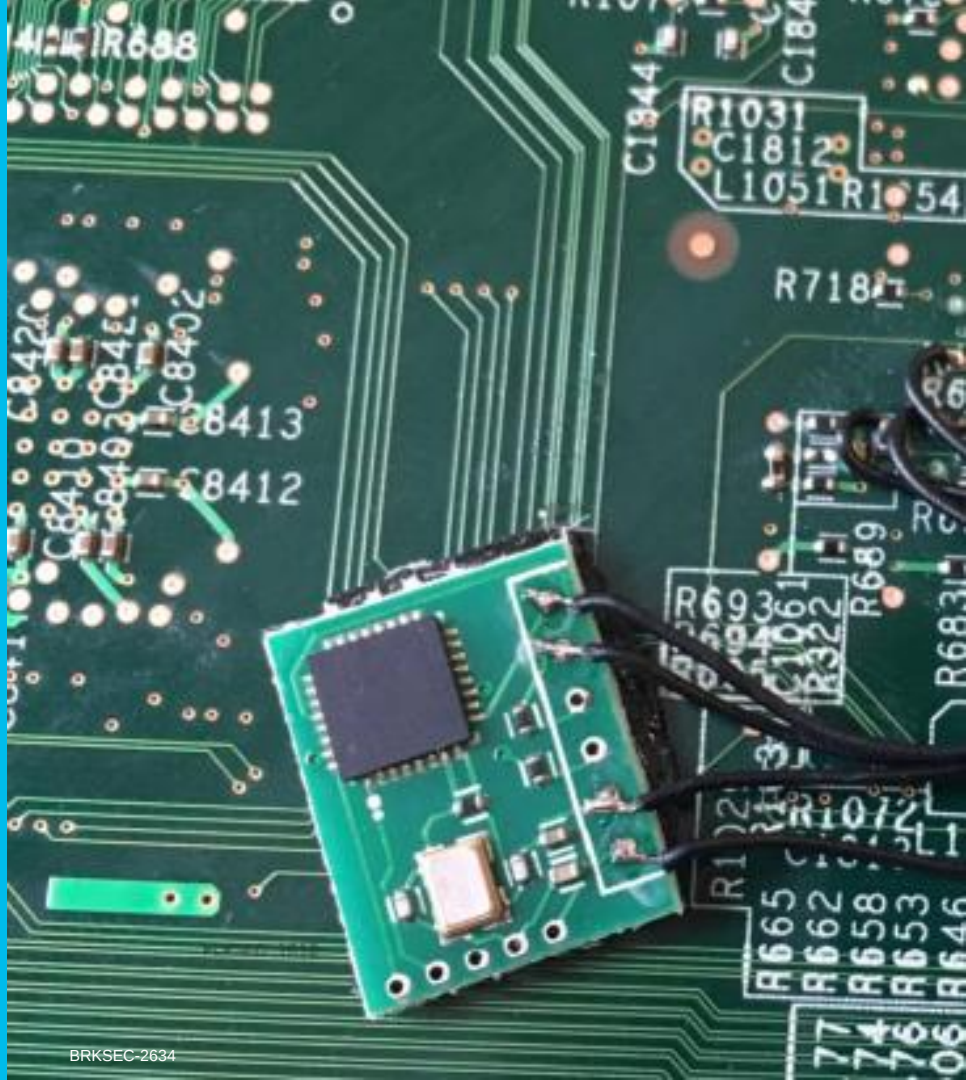
The Threat:

- Attacker attempts to install and boot with a modified ROMMON
- To permanently disable the device

The Defence:

- Built-in checks to assure that only authentic ROMMON can be installed.
- The old ROMMON verifies the new ROMMON prior to allowing it to run

Counterfeiting and HW Authenticity Check



Threat Scenario

- Fraudulent Supplier builds fake Cat 9500 2x40 Gig Network Modules…
- To:
  - Profit from Cisco brand and sell fraudulent hardware
  - Create backdoor for command & control, data theft, etc.

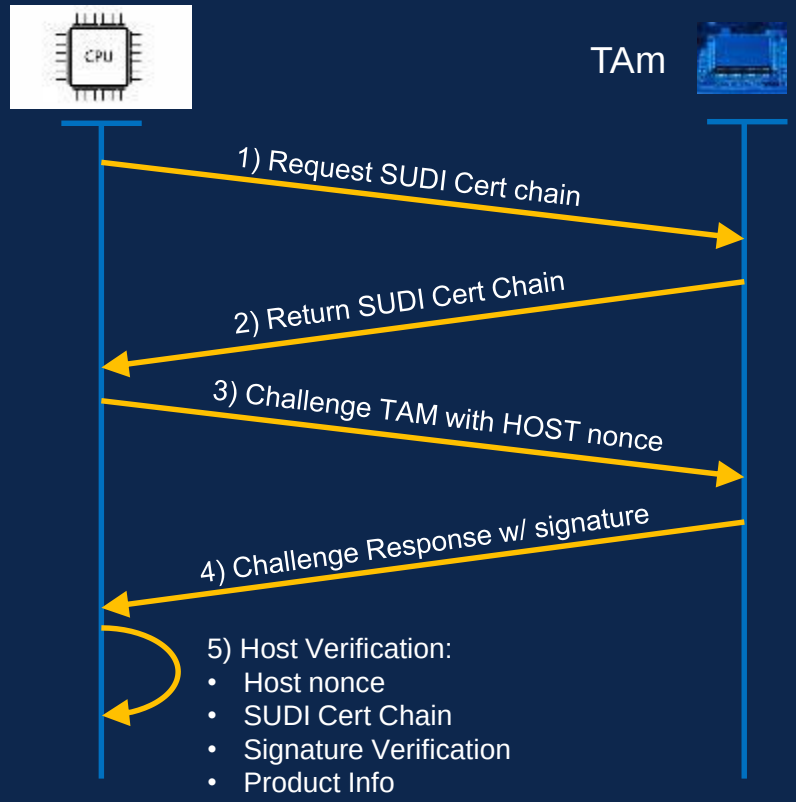
Threat Scenario

- Will the counterfeit card boot?

```
Switch#
*Jun  4 19:19:24.441: %PLATFORM_PM-6-FRULINK_INSERTED: 2x40G uplink module inserted in the switch 1 slot 1
Switch#show mod
Switch  Ports    Model                 Serial No.   MAC address     Hw Ver.       Sw Ver.
------  -----   ---------              -----------  --------------  -------       --------
 1       50     C9500-40X              FCW2133A4NB  00a3.d145.7800  V01           16.8.1a
Switch#show inventory
NAME: "c95xx Stack", DESCR: "c95xx Stack"
PID: C9500-40X          , VID: V01  , SN: FCW2133A4NB

NAME: "Switch 1", DESCR: "C9500-40X"
PID: C9500-40X          , VID: V01  , SN: FCW2133A4NB

NAME: "Switch 1 - Power Supply A", DESCR: "Switch 1 - Power Supply A"
PID: PWR-C4-950WAC-R    , VID: 000  , SN: APS2139000J

NAME: "Switch 1 - Power Supply B", DESCR: "Switch 1 - Power Supply B"
PID: PWR-C4-950WAC-R    , VID: 000  , SN: APS2139004B

NAME: "Switch 1 FRU Uplink Module 1", DESCR: "2x40G Uplink Module"
PID: C9500-NM-2Q        , VID: V00  , SN: FOC21172QCE


Switch#
```

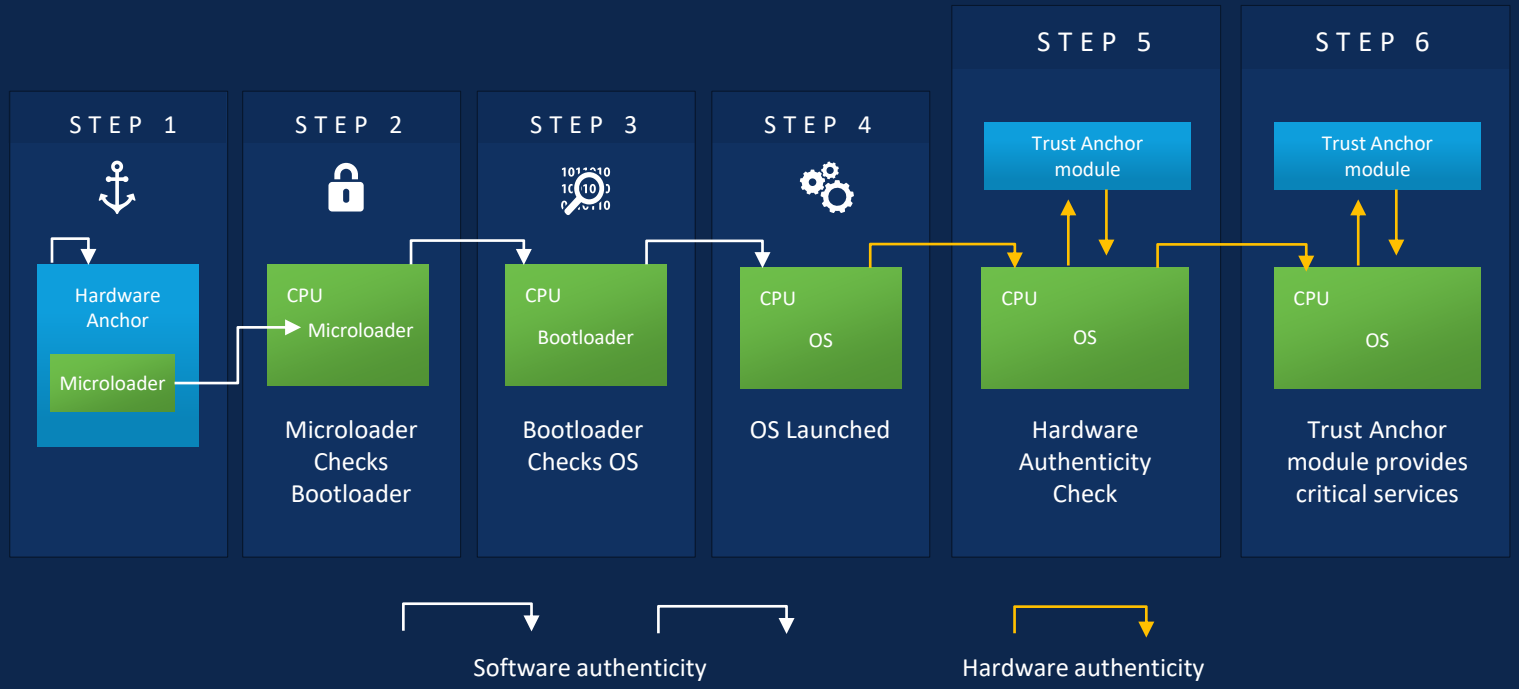
How it works

- Trust Anchor Module (TAm) securely stores HW Identity (SUDI)
- After the operating system is up and running…
- IOS-XE automatically verifies that the HW is genuine



How They Come Together:

Cisco Secure Boot and Trust Anchor Module Validating the Authenticity of Software Followed by Hardware



Code-Injection Attacks and Runtime Defences

Attack Scenario

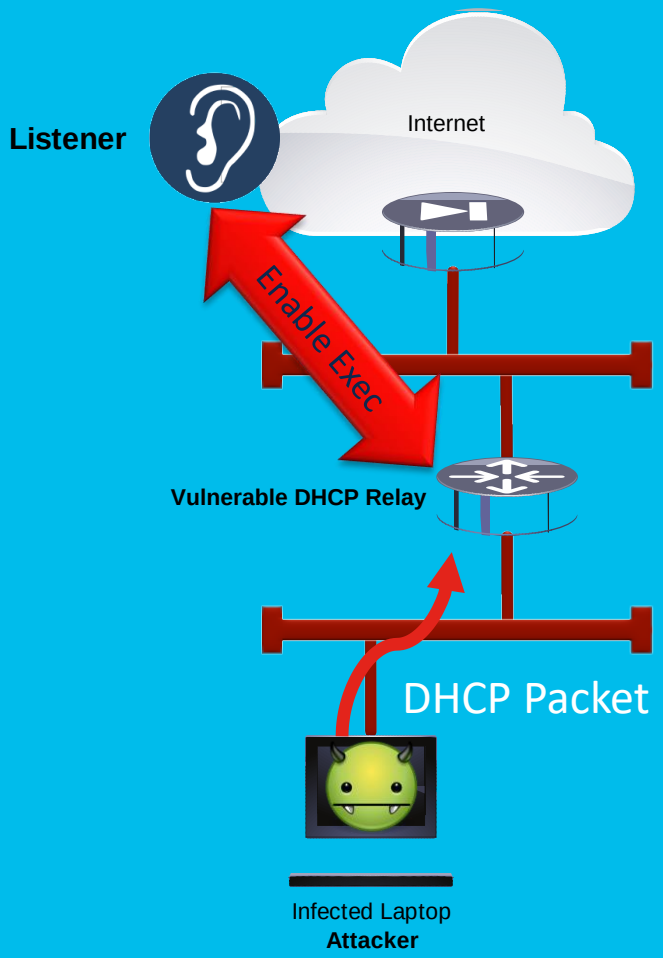
- Cyber criminal successfully breaches network perimeter
- Exploits 0-Day vulnerability with code injection
- Real-life PSIRT vulnerability in the DHCP relay - internally found

Critical

Advisory ID:	cisco-sa-20170927-dhcp	CVE-2017-12240
First Published:	2017 September 27 16:00 GMT	CWE-20
Last Updated:	2018 February 12 21:34 GMT	
Version 1.2:	Final	
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCsm45390	
	CSCuw77959	
CVSS Score:	Base 9.8, Temporal 9.1	

What *could* the attacker do?

- Take command and control
- With single-packet UDP exploit
- To create reverse shell



Using this foothold the Attacker can now…

- Monitor and redirect traffic at will
- Collect credentials sent in cleartext
- Set up ERSPAN sessions to exfiltrate packets outside a firewall
- Reroute DNS to an attacker-controlled server
- Infiltrate other hosts

Cisco Runtime Defences

Address Space Layout Randomisation (ASLR)

Object-Size Checking

X-Space

Hardware, Operating System, Compiler, and Development Best Practices

To protect against Buffer-Overflow and Return-Oriented Programming Attacks

Device Loss and Theft

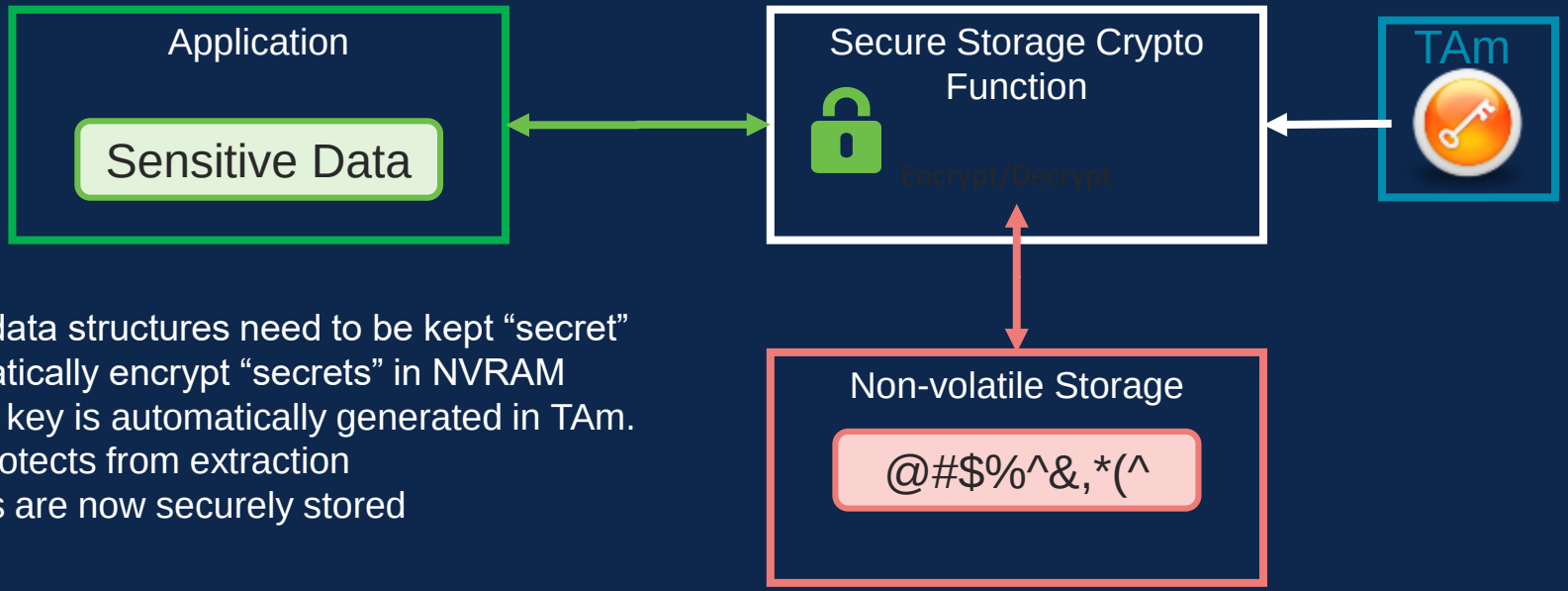
Threat Scenario

Attacker steals device

Uses forensic techniques to read secrets from non-volatile RAM

How can we protect the critical information from being compromised?

Secure Storage



Some data structures need to be kept “secret”
Automatically encrypt “secrets” in NVRAM
Unique key is automatically generated in TAm.
TAm protects from extraction
Secrets are now securely stored

Protected Data Includes:

- Asymmetric key-pairs for VPNs and IPSec
- Pre-shared secrets,
- Type 6 password encryption key, and
- Credentials for Lawful Intercept and TFTP

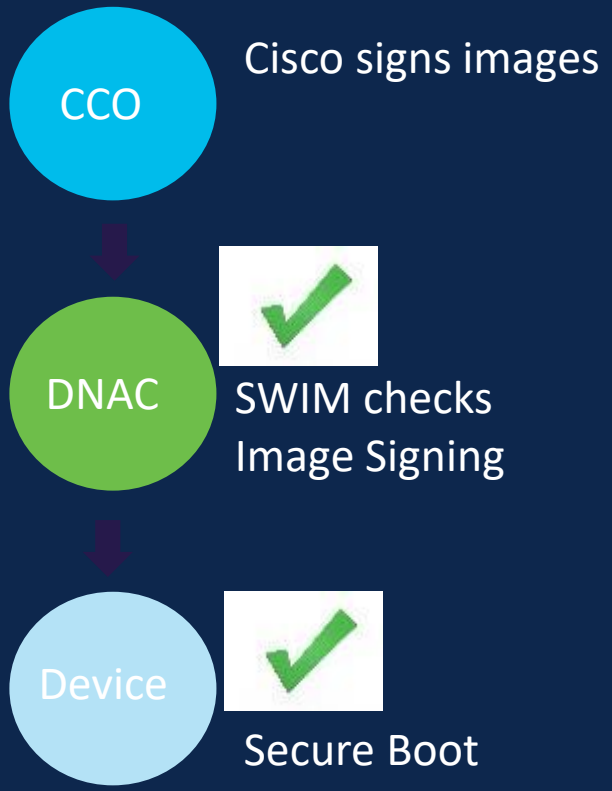
Can I trust the Image that I install?

Software Image Management with DNA Center

- Support for Software Deployment
  - Routing, Switching, NFV, WLC, and AP
- Patching support for Routing (ISR4K) and Switching (CAT9K)
- Distribution vs Activation of Software
- Pre-Check and Post-Check along with Rollback
- Integrity Verification (IV) checks that downloaded software images are genuine on DNA Center

Integrity Verification

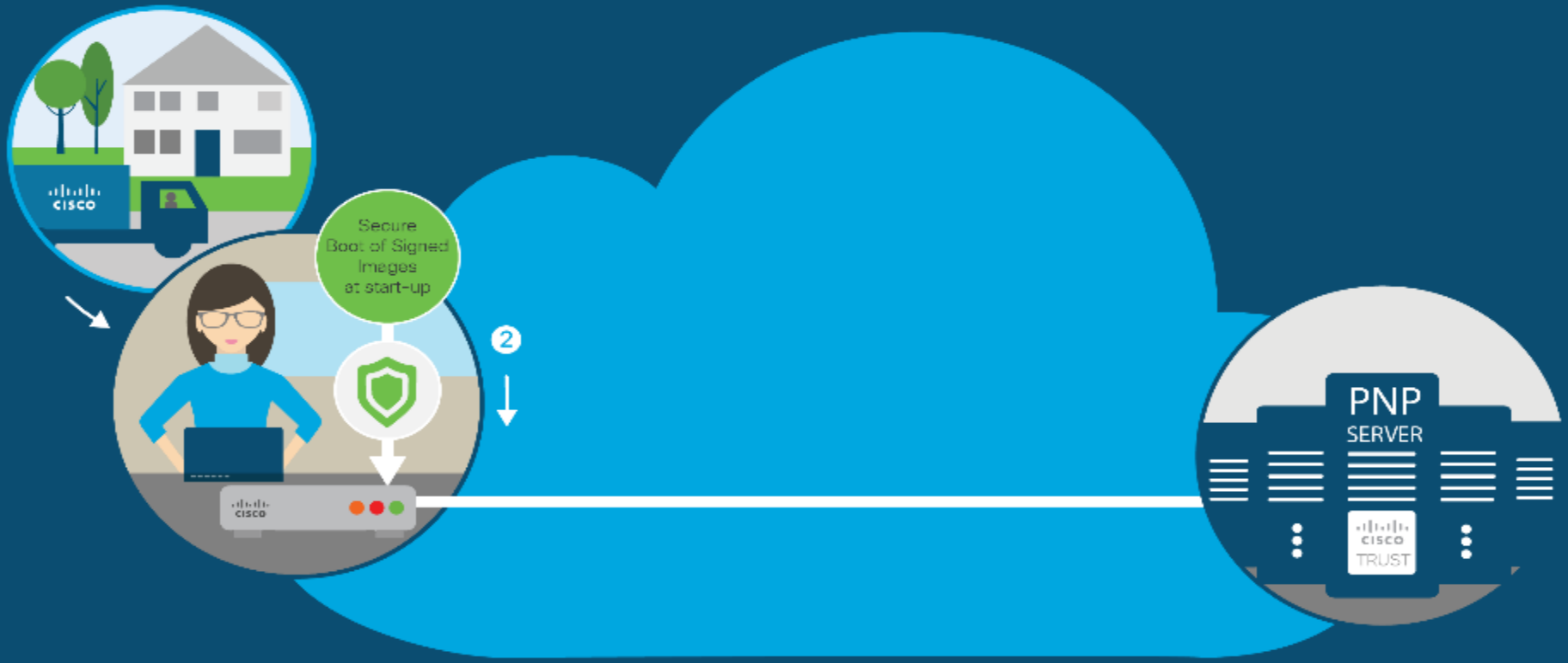
- The Cisco Integrity Verification (IV) application monitors your devices for unexpected or invalid changes indicating a risk that your devices are compromised.
- IV compares the device's software, hardware, platform and configuration settings against an authoritative set of Known Good Values (KGV).
- In DNA Center 1.1, SWIM automatically checks the images that it keeps on file against the KGV to verify that the image is genuine
- Secure Boot will then verify that the image has not been changed when it boots on the device
- Results of boot sequence securely stored for later validation. (Boot Integrity Visibility)



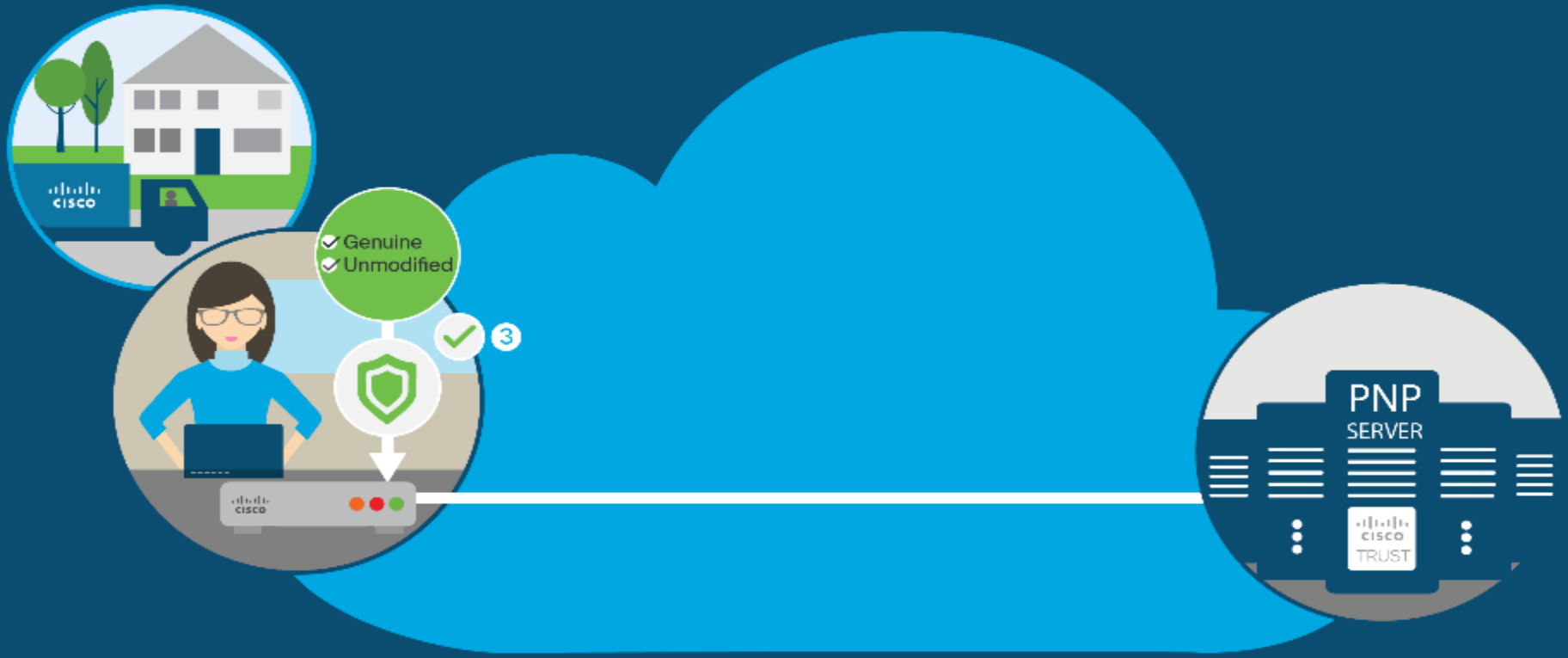
Zero Trust Provisioning

Step 1: SUDI unique device identifier and serial number installed at manufacturing

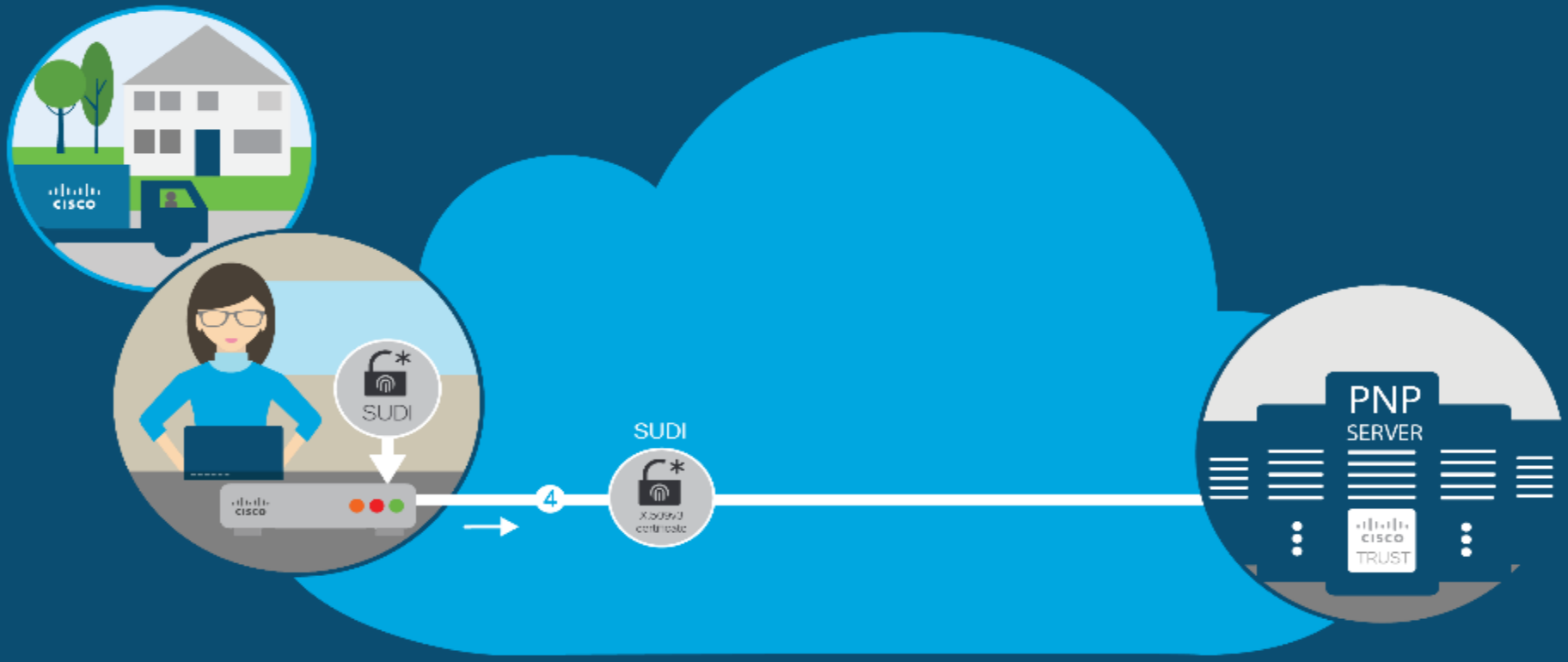
Step 2: Secure boot of signed images at start-up verifies platform integrity



Step 3: Verification of device authenticity and integrity



Step 4: Network device sends its credentials to the Plug and Play server



Step 5: Plug and Play server verifies the identity of the device to be provisioned

Step 6: Two-way trust and secure communications established

Step 7: Secure provisioning of Cisco network device

Plug and Play

1 Discovery

Configure device discovery mechanism

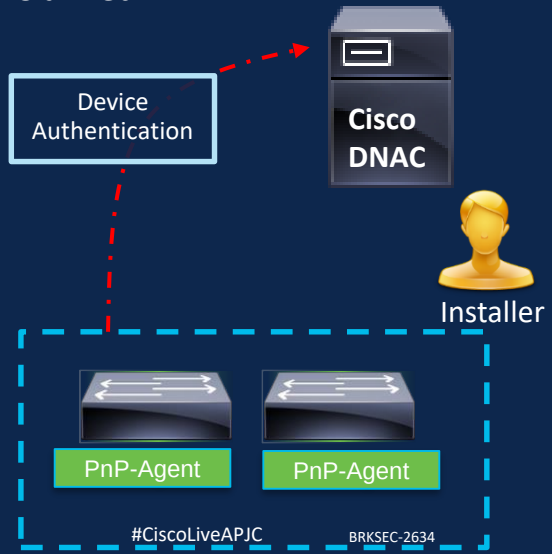
- DHCP Option-43
- DNS
- Cisco Cloud Redirect

DHCP Server OR DNS Server

PnP Cloud Redirection Service

2 Un-claimed Devices

- Installer powers-on devices
- Devices securely connects to Cisco DNA-C Server, waiting to be 'Claimed'



3 Secure Deployment

- Network admin claims devices based on device information
- Adds Device to Site for Provisioning

Network Integrity

Trust Visualisation and Reporting requires a Service

Introducing Crosswork Trust Insights

- Visualise Trustworthiness
- Track & Verify Inventory
- Utilise Trusted Data for Automation

A Cloud-based SaaS offer that reports on the trustworthiness of network devices and provides forensics for assured inventory

Use-case: Trustworthiness Reporting & Audit

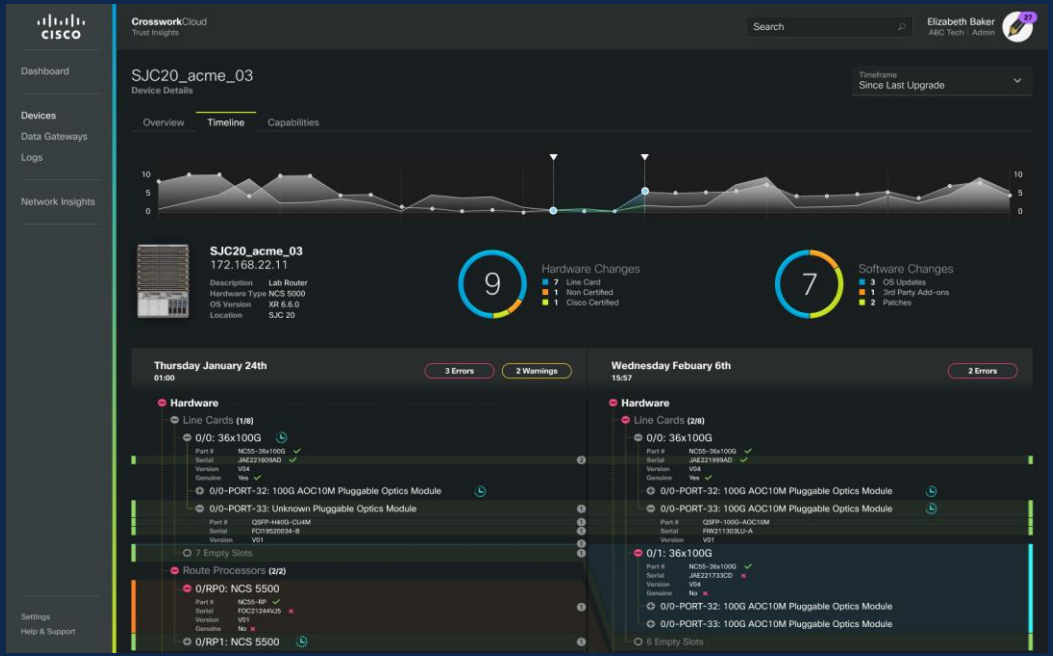
Goal: Visualise and report on the trustworthiness of network infrastructure

Challenges:

1. How do I examine the trust posture of IOS XR devices?
2. How do I prove system integrity through examining trust evidence in IOS XR devices?
3. How do I prove authenticity and integrity of hardware* on production IOS XR devices?

Outcome

Stay ahead of the curve by monitoring integrity of your network devices and maintaining trustworthy infrastructure



* Based on available device capabilities

Use-case: Software Update & Compliance Reporting

Goal: Apply critical patches to infrastructure and maintain compliance policy

Challenges:

1. How do I know what devices are running the affected software?
2. How do I identify whether patches are already applied?
3. How do I prove that patches are not only applied but are actually running, e.g. installed SMU but not active
4. How do you prove compliance to auditors that patches were applied at a specific time?

Outcome

Reduce the effort and time to identify where critical software updates are needed and maintain authoritative proof of compliance

Use-case: Forensics Analysis

Goal: Track changes in infrastructure over time. Prove historical status and inventory of systems

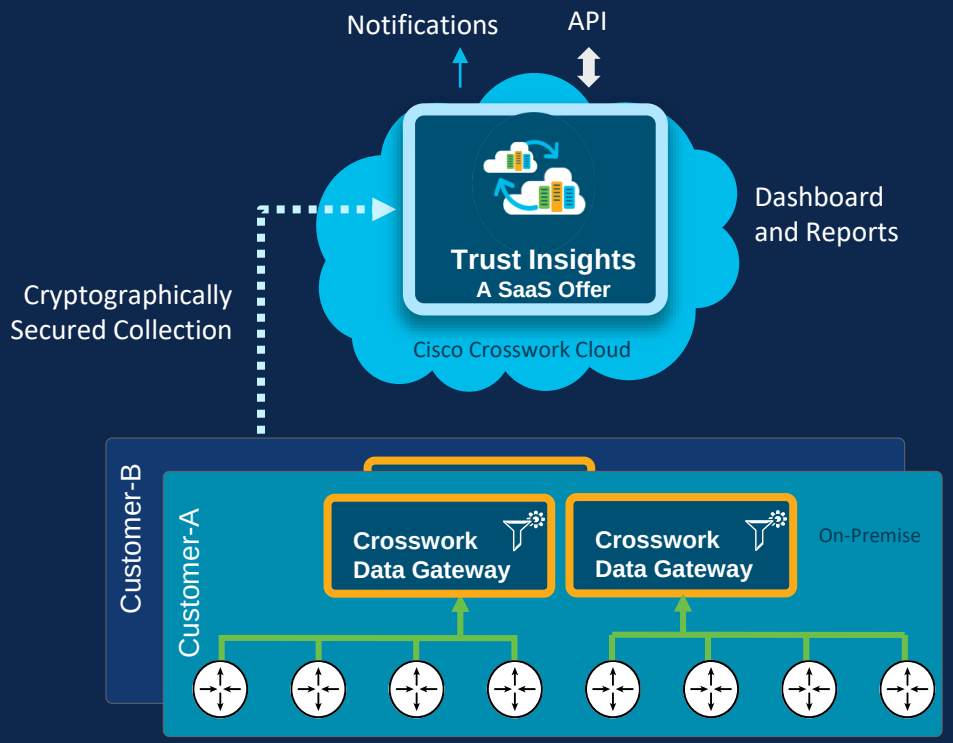
Challenges:

1. How do I know what hardware and software changes have occurred in production devices?
2. How do I prove what hardware and software inventory was present during past operational events?
3. How do I prove that current and previous inventory measurements are accurate?

Outcome

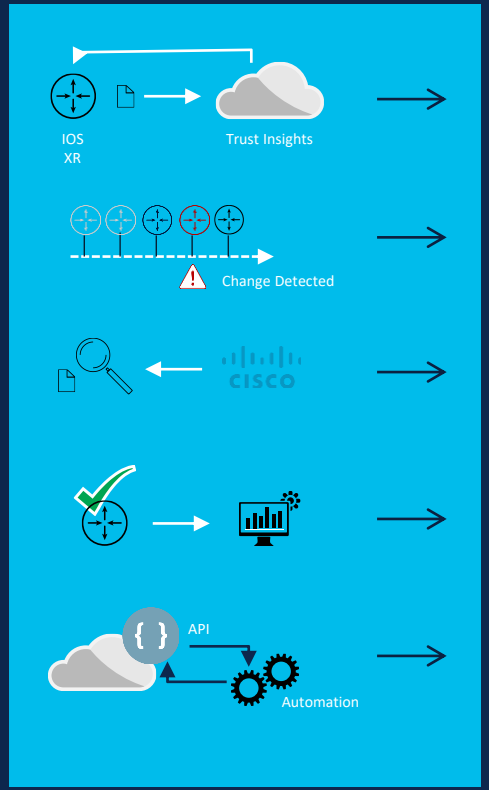
- Expedite investigation into operational events with reliable visibility into current and historical systems inventory
- Ensure readiness for regulatory audits with authoritative proof of hardware and software integrity

Crosswork Trust Insights Components



- Requires up-to-date feed of Known-Good-Values (KGV) from IOS XR Build and Regression
- Constantly evolving analytics of hardware and software fingerprints in Cloud Service
- On-Premises Data Gateway collects trust dossier from IOS XR Routers
- Dossier creation controlled via AAA, and is human-readable with digital signature

How Trust Insights Works



1. Trust Insights securely requests and collects signed evidence dossier from IOS XR devices
2. Dossier evidence verified and added to timeline of running hardware and software
3. Trust data verified against Known-Good-Values (KGV) for hardware and software from Cisco
4. Trust Insights delivers assured inventory reporting with history, and trust visibility for IOS XR systems
5. Trust and Assured Inventory data accessible via API to enable Closed-Loop Automation

Summary - Lifecycle of a Trustworthy Network OS

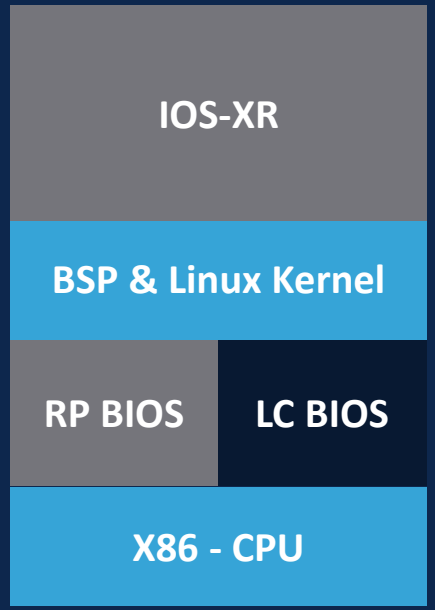
Integrity Visibility (Boot & Run-time)

- External Trust Posture Assessment
- Secure Quote for Integrity Measurements

Maintain Trust at Run-time

Establish Trustworthy NOS

Establish Trust in Hardware



- Run-time defence
- Integrity Management Arch.

- Address Space Layout Randomisation
- Security Enhanced Linux

- Hardware Integrity Measurement
- Secure Boot

- Trust Anchor Module (TAM)
- Secure UDI (Manufacturer Cert)

Call to action - Trustworthy Technologies to look for

Built-in security features that defend against today's threats

Image Signing

Creates a unique digital signature for a block of code. Signed images may be checked at runtime to verify that software has not been modified.

Hardware Anchored Secure Boot

Helps ensure that code is authentic and unmodified. Anchors the microloader in immutable hardware, establishing a root of trust and preventing Cisco devices from executing tainted software.

Trust Anchor Module (TAm)

A tamper-resistant chip featuring nonvolatile secure storage, SUDI, and crypto services including RNG, key store, and crypto engine.

Hardware Authenticity Check

Uses a X.509 SUDI certificate to verify hardware authenticity. Runs only after the secure boot process has completed and software has been verified to be trusted.

Boot Integrity Visibility

Allows platform identity and software integrity information to be visible and actionable. Admins can verify whether the platform has booted with trusted code.

Cisco Catalyst 9000 Series

Cisco ISR 4000 & 1100 Series

SUDI for Cisco Plug & Play

The Secure Unique Identifier (SUDI) is an X.509 certificate that provides factory-installed device identity. Prevents spoofing and MITM attacks. Enables remote on-boarding of devices.

Runtime Defences

Built-in operating system features that protect against malware being injected into running code.

Modern Cryptography

Provides secure, up-to-date encryption so that encrypted data communications in-transit and at-rest remains confidential.

Simplified Factory Reset

One command to reset the device to factory-original settings to protect sensitive corporate data when device is out of direct control.

Secure Development Lifecycle (SDL)

A repeatable, measurable process designed to reduce vulnerabilities and enhance the security and resilience of Cisco solutions.

Thank you

You make **possible**