Building Trustworthy Infrastructure with IOS-XR Platforms

Rakesh Kandula
Technical Marketing Engineer

March 4th, 2021

Agenda

1. Service Provider Security Concerns
2. Trustworthy Platforms Overview
3. IOS-XR Security Features

Why Security is Mandatory for Service Providers?

Targeted attacks on Critical Infrastructure

Impact on Economy

Untrusted Locations

Complex to Manage

Growing Concerns for Service Providers

Trustworthy Platforms Overview

Foundations of Trustworthy Platforms

Process ..... Technology ..... Policy

Secure Process

Lifecycle / Security Baseline

CSDL

Trustworthy Systems Technology

Common Modules & Hardware

- Trust Anchor
- Secure Boot
- Entropy
- Immutable Identity
- Image Signing
- Common Crypto
- Secure Storage
- Run Time Integrity
- Trust Visibility

Secure Standards

Information Assurance (IA)

Common Criteria

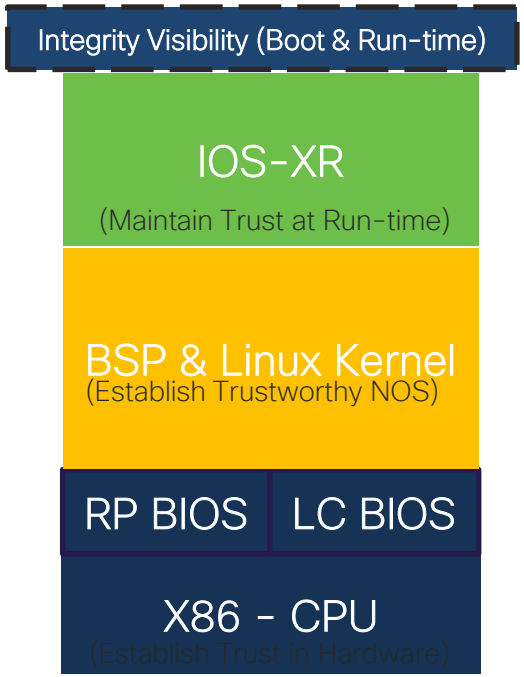
ISO 27034

FIPS / USGv6

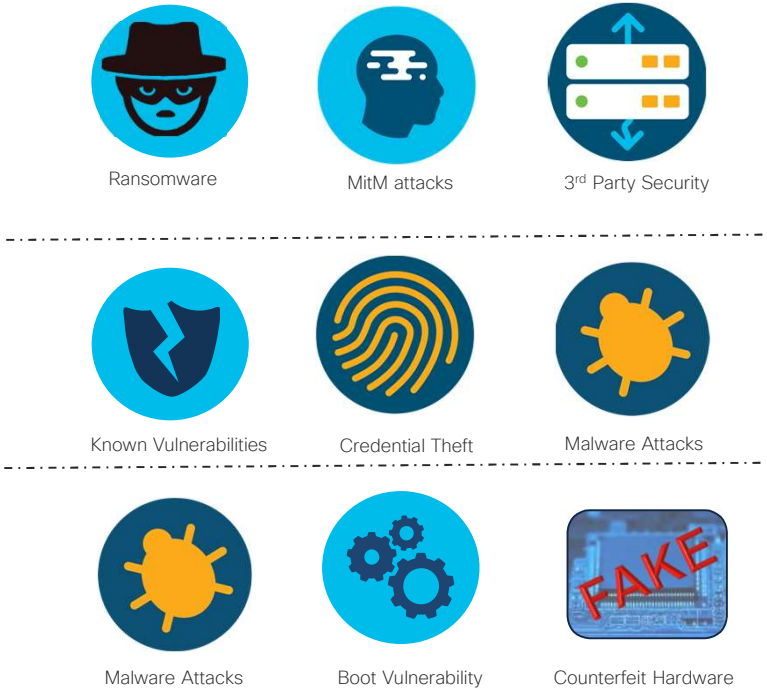
TCG

Trustworthy Platforms – Network OS View

NOS



Protection against



XR Protection

- Run-time defenses
- Integrity Measurement Arch.
- Disk Encryption
- Remote Attestation

- Measured Boot
- Security Enhanced Linux

- Trust Anchor Module
- SUDI
- Secure Boot
- Chipguard

Components of Trustworthy Platforms

Hardware Integrity

Provides counterfeit hardware protection and acts as a trust anchor

Boot Integrity

Ensures integrity of the boot process

Runtime Integrity

Ensures integrity of the IOS-XR runtime

Trust Visibility

Provides visualization of Trust

Components of Trustworthy Platforms

Hardware Integrity

Provides counterfeit hardware protection and acts as a trust anchor

Boot Integrity

Ensures integrity of the boot process

Runtime Integrity

Ensures integrity of the IOS-XR runtime

Trust Visibility

Provides visualization of Trust

Cisco TAm – Hardware-based Trust Anchor

Anti-Theft and Anti-Tamper Chip Design

Built-In Crypto Functions

Hardware Entropy for RNG*

Secure Storage

- Hardware designed to provide both end-user and supply chain protections
  - End-user protections include highly secure storage of user credentials, passwords.
  - Supply chain protections -- Cisco SUDI (**S**ecure **U**nique **D**evice **I**dentifier) inserted during manufacturing
- Secured at Manufacturing. No user intervention required
- Ideal for embedded computing like routers and Wi-Fi access points

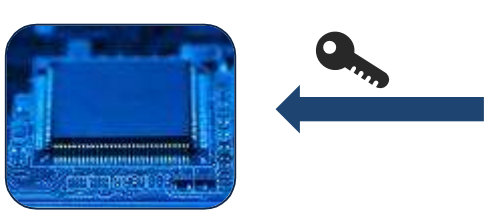
* NIST 800-90 certified

Unique hardware Identity (SUDI)

"How do I know this is really my router?"

- Unique cryptographic key embedded in hardware trust anchor module within every IOS XR Router
  - Secure Unique Device Identifier (SUDI)
  - Provides 802.1AR Secure Device Identity
  - Immutable key imbedded in Trust Anchor Module at time of manufacture
  - Signed by Cisco for proof of authenticity
  - Includes PID and Serial number of device
- Cryptographically strong identification of remote hardware
- Establishes unique, immutable hardware identity

Hybrid TAm Secure Storage
(Extending the on-chip storage)



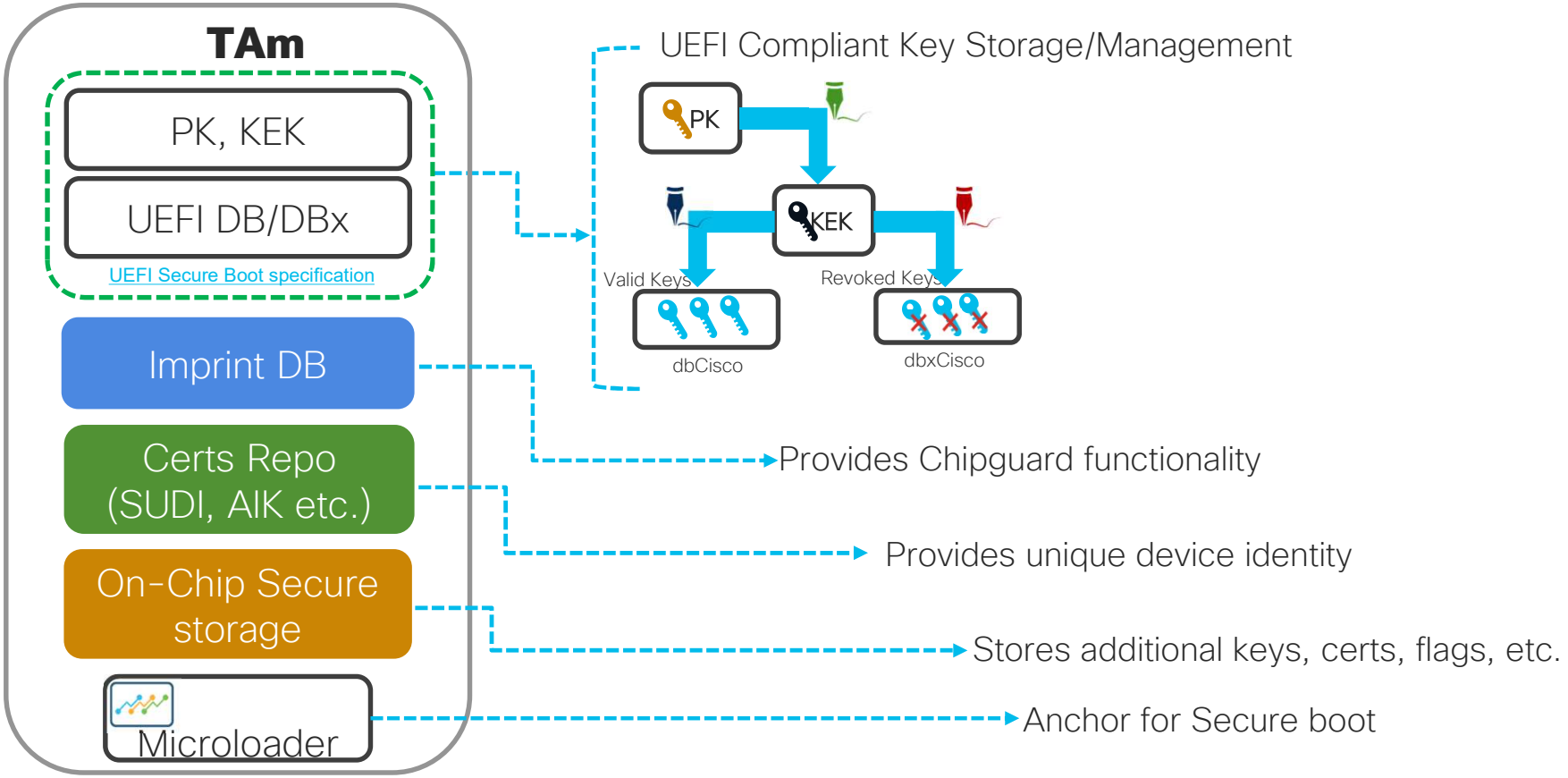
HW TAm Chip

Hybrid TAm
Secure Storage

- Encrypted filesystem on the disk to store protected secrets within IOS XR.
- Accessed via TAm services secure storage APIs (internal)

- Secure storage is protected by key inside TAm chip
- Secure storage extends the on-chip TAm storage on to the disk

TAm Chip Module Overview



Components of Trustworthy Platforms

Hardware Integrity

Provides counterfeit hardware protection and acts as a trust anchor

Boot Integrity

Ensures integrity of the boot process

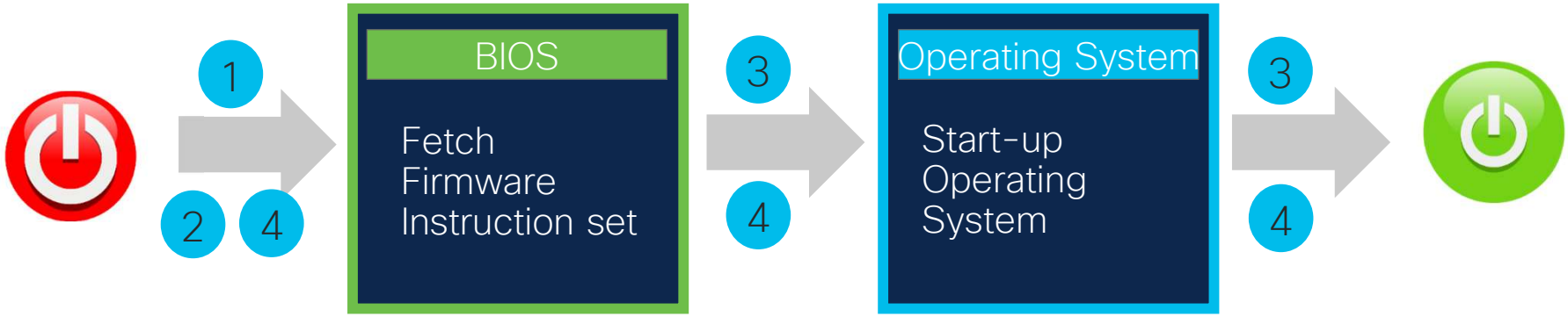
Runtime Integrity

Ensures integrity of the IOS-XR runtime

Trust Visibility

Provides visualization of Trust

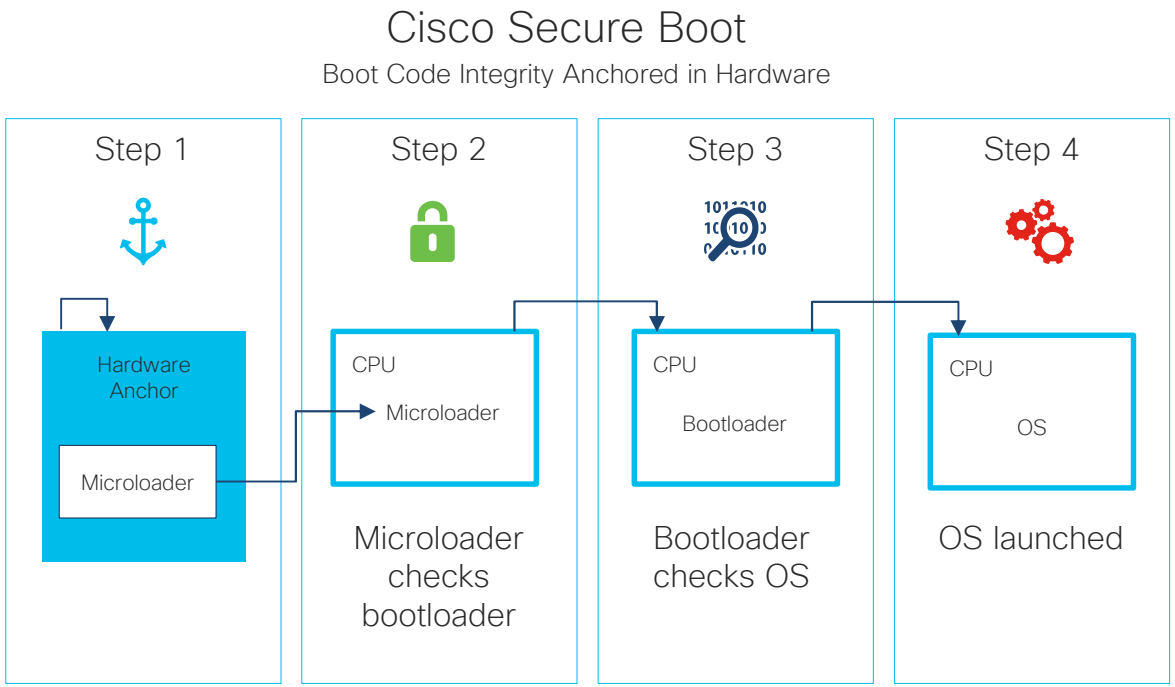
Attacking the Boot Sequence



1. Changing the boot interface
2. Booting from alternate device
3. Bypassing Integrity checks
4. Adding persistent code

Cisco Secure Boot – Overview

Anchors Secure Boot in Hardware to Create a Chain of Trust



Software Authenticity:

- Only authentic signed Cisco software boots up on a Cisco platform
- The boot process stops if any step fails to authenticate
- Each step validates the signature of the next stage before proceeding
- The TAm chip / IOFPGA acts as the anchor to the secure boot and the chain of trust starts from hardware

Can we do more?

Tampering of Critical Components

Increase in Supply Chain Attacks

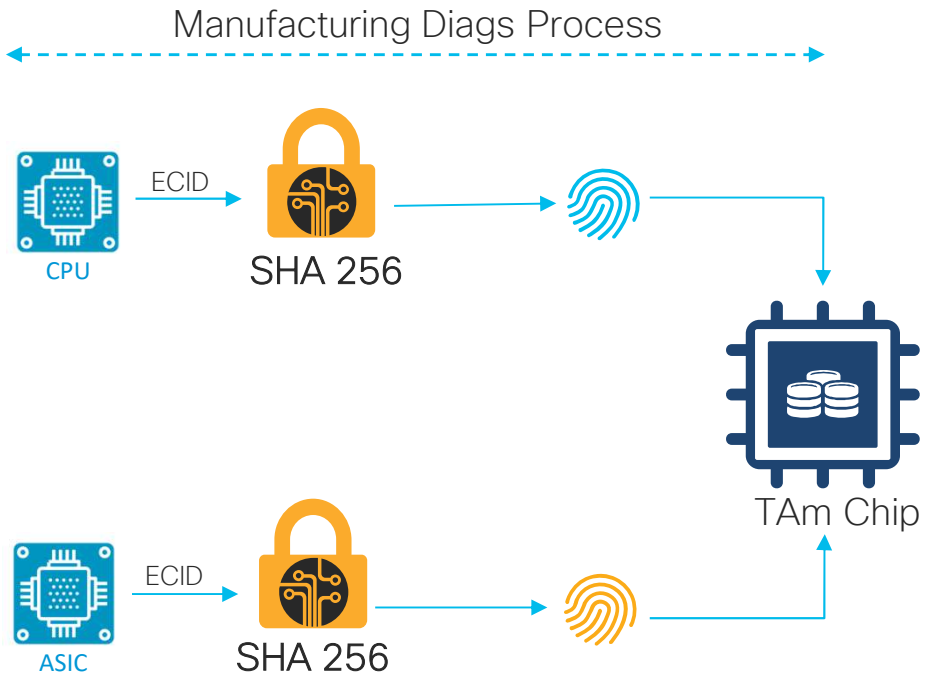
Increasing attempts to put Trojans on Chips

- CPU Integrity
- ASIC Integrity
- Detect in-transit tamper
- Validate Mission Critical Components

Introducing Chipguard

1. Detects counterfeit CPU/NPU on rout
2. Enabled by ImprintDB in TAm chip
3. Part of BIOS sequence during boot
4. Chipguard verification failure halts the boot

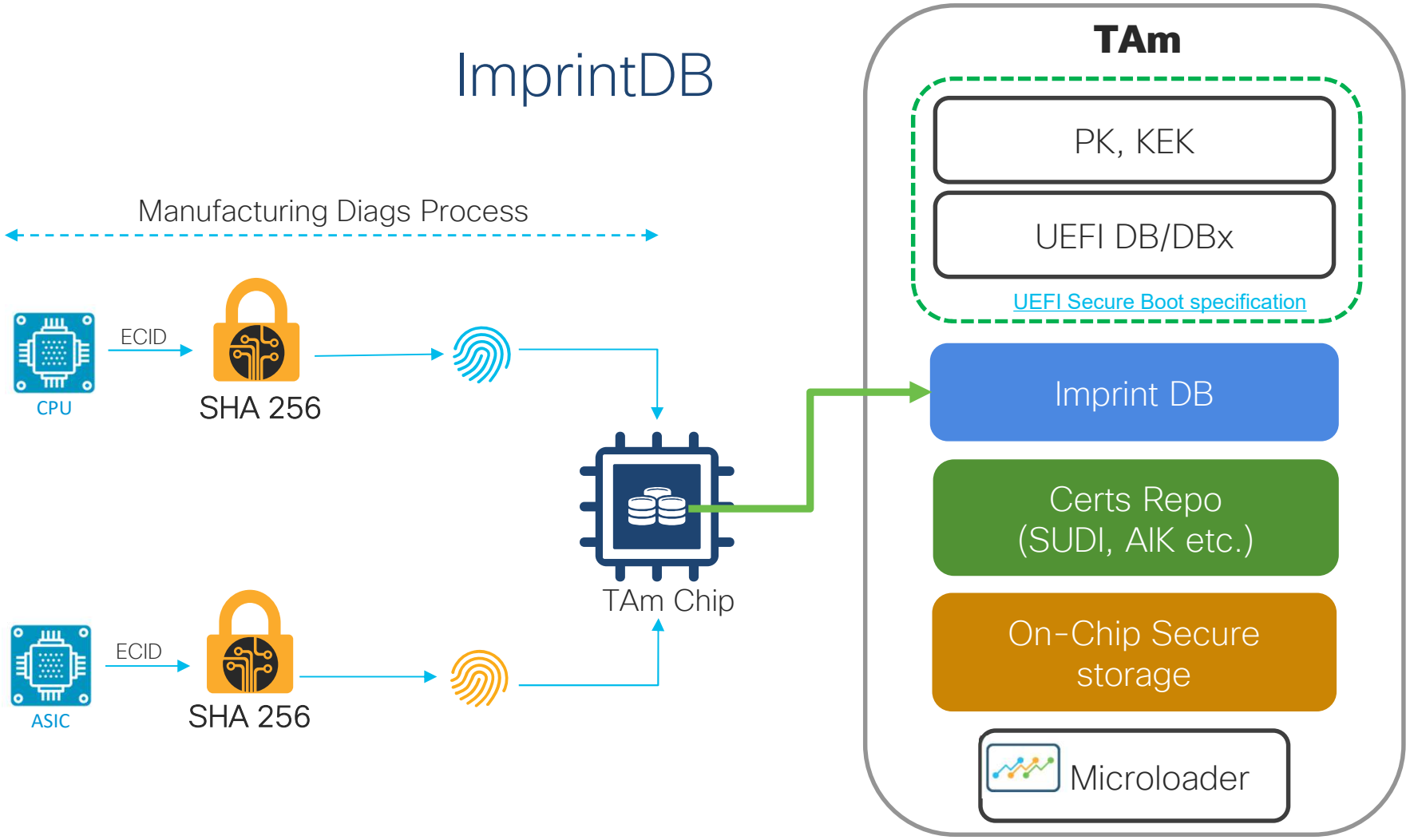
What is ImprintDB?



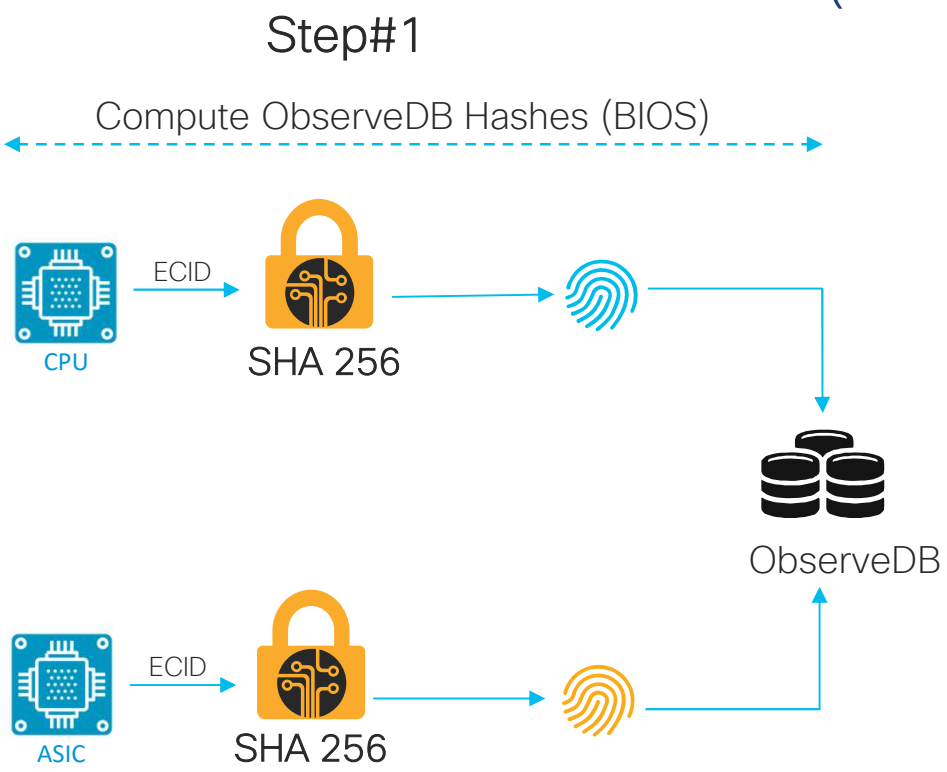
- During manufacturing, the SHA-256 hash of the ECID* of the CPU and NPU are calculated
- These hashes are then programmed inside the TAm chip
- The programmed hash values form the ImprintDB inside the TAm chip
- The ImprintDB cannot be modified during runtime

*Electronic Chip ID

ImprintDB


Manufacturing Diags Process
CPU
ECID
SHA 256
ASIC
ECID
SHA 256
TAm Chip
TAm
PK, KEK
UEFI DB/DBx
UEFI Secure Boot specification
Imprint DB
Certs Repo
(SUDI, AIK etc.)
On-Chip Secure
storage
Microloader

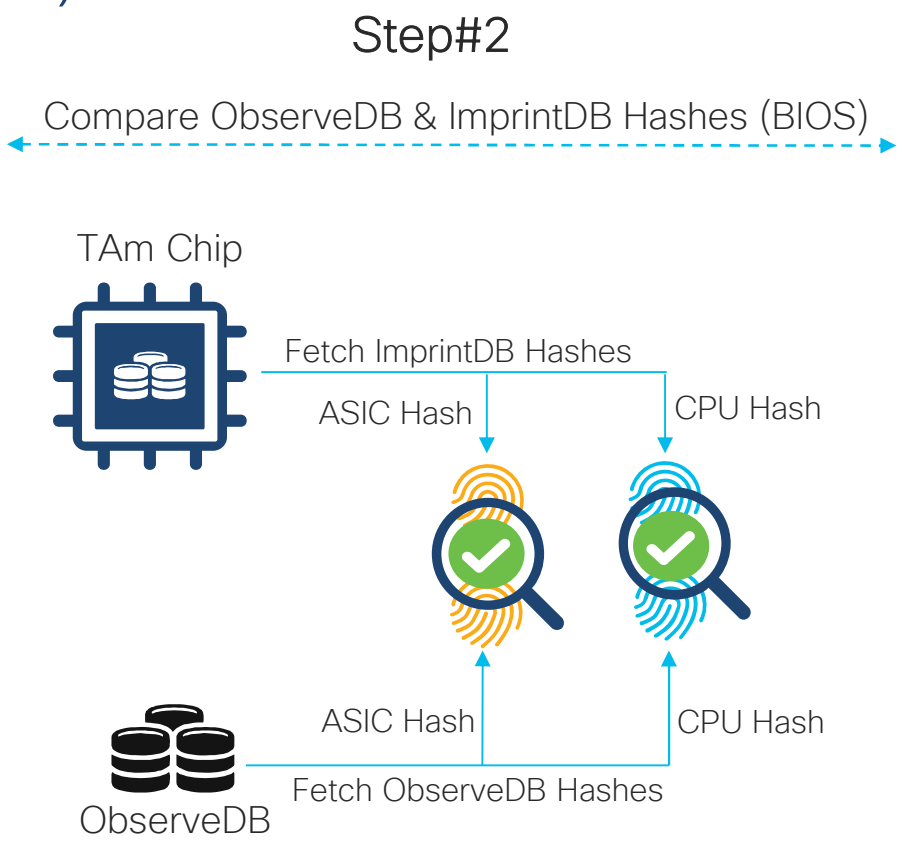
Chipguard Workflow (BIOS)



- BIOS reads the ECID of the chips and computes their hashes
- Each of the hashes is then extended into a PCR inside TAm chip
- These set of observed hashes forms the ObserveDB

Chipguard Workflow (BIOS)

- BIOS fetches the factory programmed hash values from imprintDB
- The hash values are compared with the ObserveDB generated in the previous step
- BIOS continues with boot process if and only if the hashes match



Components of Trustworthy Platforms

Hardware Integrity

Provides counterfeit hardware protection and acts as a trust anchor

Boot Integrity

Ensures integrity of the boot process

Runtime Integrity

Ensures integrity of the IOS-XR runtime

Trust Visibility

Provides visualization of Trust

Maintaining Trust at Run-time

Application Containment and Policy

SELinux

- A Mandatory Access Control (MAC) facility built into the Linux Kernel
- Protection from malicious or misbehaving compromising the system

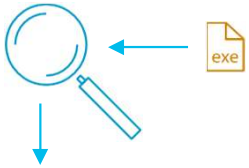
Integrity Visibility and Secure Measurement

Linux Integrity Measurement Architecture

- All processes executed by the kernel are securely measured and reported
- Kernel checks process signature to prevent unsigned code from executing

Linux Integrity Measurement Architecture (IMA)

IMA Logging




```
10 d93ea3e04ba8d68d7bf032f15963467a929a1e30 ima-sig
sha256:db48006f4c5decf1c70abdc849efa4618422420d031c202f6b99f0b185adc0a6 /bin/bash
0302046ebaed830100822239998463f30686f6c0946d4d0ebd95567469866c23a3de0fe210e4c84c3
ea95234a7dbf0565ed2549928b91a45f7bef59787460dc83ccd3ac9c6f39d7e7ef252f863f19afaf7
2fa9b0dbe2a96d2f84aa9ce9007b5bdcbb94d11d7085d9c25be68f6bd1566044f83ec17c770d66ccb
88b5db6a284527d95001d00cff92e14fd544bb2c4c9ffd17364d35c403f895f537c41da37e27b0284
b5f4ce1fde0d0730cef5e93b0971e4325a849e27ac85a6ec546631a3890808667d24411e80d430c7c
c0f93a8c6cf8ce9c5d3baf37423864d238540ea686569f685730a2e96e5fbefbc73be3d3eea716587
598e3df728f7fd3c64b3779d2b19d095c3405242fe40
```

IMA Log: /sys/kernel/security/ima/ascii_runtime_measurements

- IOS-XR adopted Linux IMA which ensures every file loaded during runtime goes through a measurement / appraisal
- All files in an XR image have an IMA signature over a SHA-256 hash of the file contents computed during build
- Kernel measures and verifies the signature and extends the PCRs in TAm chip
- IMA violations will be logged in audit.log
- IMA policy is set in initrd (which is signed) and mode is enabled through grub.cfg (which is signed)

Components of Trustworthy Platforms

Hardware Integrity

Provides counterfeit hardware protection and acts as a trust anchor

Boot Integrity

Ensures integrity of the boot process

Runtime Integrity

Ensures integrity of the IOS-XR runtime

Trust Visibility

Provides visualization of Trust

Trust Visibility Components

1. Boot Integrity Visibility (BIV)
2. Runtime Integrity Visibility
3. Remote Attestation Workflow

How to establish Trust?

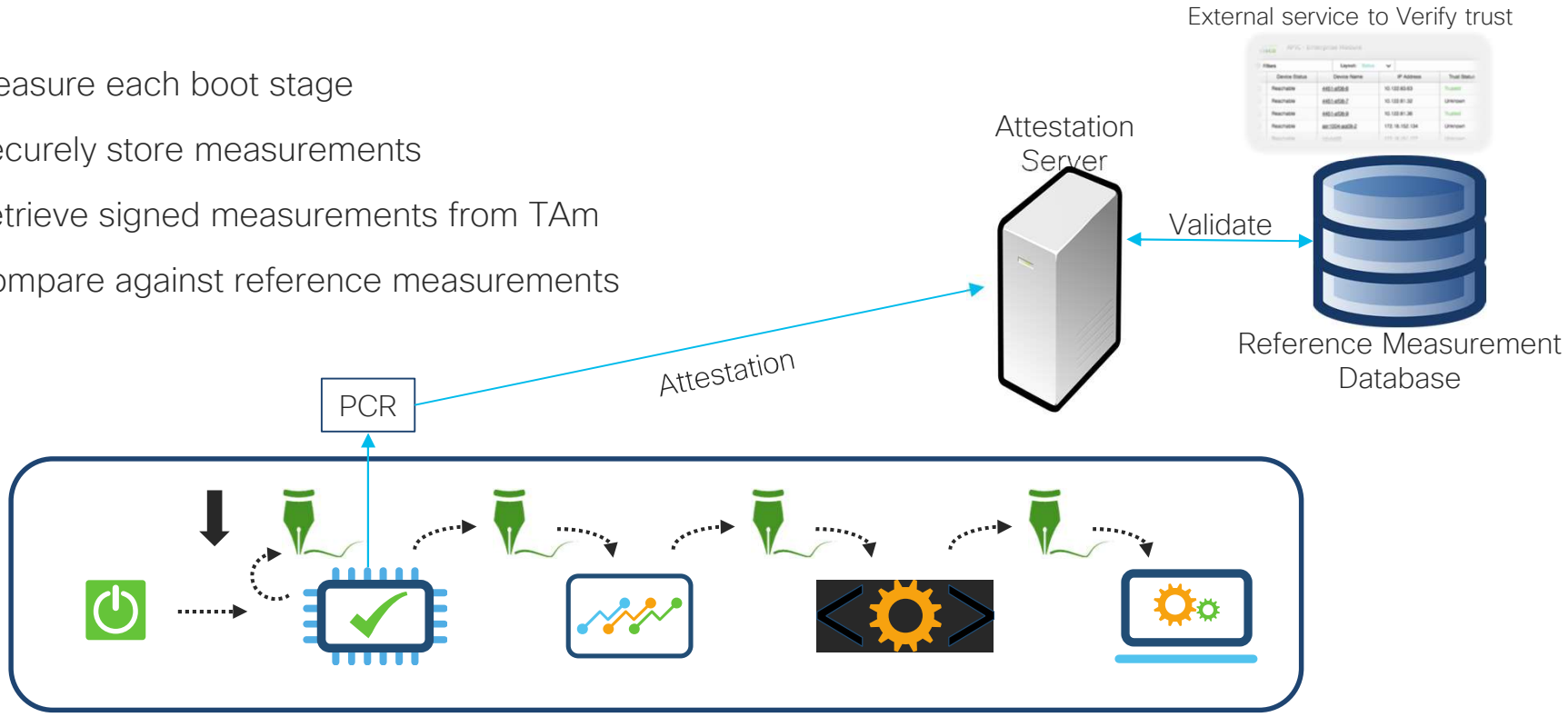
MEASURE

VERIFY

Boot Integrity Visibility (BIV)

Boot Integrity Visibility (BIV) – Validate Trust

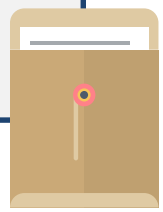
- Measure each boot stage
- Securely store measurements
- Retrieve signed measurements from TAm
- Compare against reference measurements

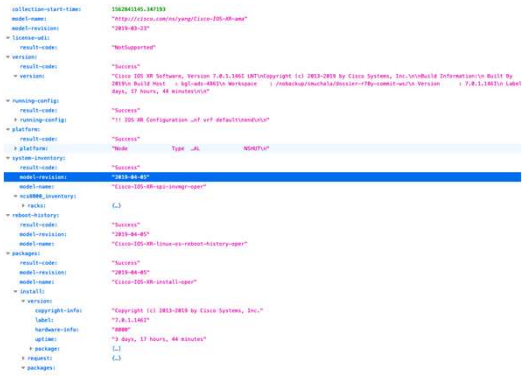


Runtime Integrity Visibility

Example of IOS-XR Trust Dossier

- OS Version + Platform Output
- Anti-Replay *Nonce*
  - Specified as CLI option
- System Hardware inventory
  - Cisco-IOS-XR-invmgr-oper.yang
  - Cisco-IOS-XR-spi-invmgr-oper.yang
- Hardware Attestation Data
  - Cisco-IOS-XR-remote-attestation-act.yang
- SUDI (Hardware Identity) Certificate
  - Separate signature per FRU (includes nonce)
- Software Package inventory
  - Cisco-IOS-XR-spirit-install-instmgr-oper.yang
  - Cisco-IOS-XR-install-oper.yang
- Reboot History
  - Cisco-IOS-XR-linux-os-reboot-history-oper.yang
- Rollback History
  - Cisco-IOS-XR-config-cfgmgr-exec-oper.yang





- Human-readable JSON formatted output via CLI command
- Signed envelope (not encrypted)

Measuring and Validating Trust

Boot & Runtime Measurements

e5fa44f2b31c1fb553b46021e7360d07d5d91ff5e
7448d8798a4380162d4b56f9b452e2f6f9e24e7a
a3db5c13ff90a36963278c6a39e4ee3c22e2a436

9c6b057a2b9d96a4067a749ee3b3b0158d390cf1
5d9474c0309b7ca09a182d888f73b37a8fe1362c

ccf271b7830882da1791852baeca1737fcbe4b90
d3964f9dad9f60363c81b688324d95b4ec7c8038

dd71038f3463f511ee7403dbcbc87195302d891c
4143d3a341877154d6e95211464e1df1015b74b
b6abd567fa79cbe0196d093a067271361dc6ca8b
136571b41aa14adc10c5f3c987d43c02c8f5d498

Known Good Values (KGV)

e5fa44f2b31c1fb553b46021e7360d07d5d91ff5e
7448d8798a4380162d4b56f9b452e2f6f9e24e7a
a3db5c13ff90a36963278c6a39e4ee3c22e2a436

9c6b057a2b9d96a4067a749ee3b3b0158d390cf1
5d9474c0309b7ca09a182d888f73b37a8fe1362c

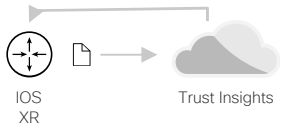
ccf271b7830882da1791852baeca1737fcbe4b90
d3964f9dad9f60363c81b688324d95b4ec7c8038

dd71038f3463f511ee7403dbcbc87195302d891c
4143d3a341877154d6e95211464e1df1015b74b
b6abd567fa79cbe0196d093a067271361dc6ca8b
136571b41aa14adc10c5f3c987d43c02c8f5d498

Remote Attestation Workflow

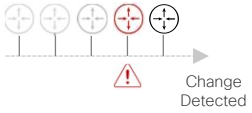
How Trust Validation Works – Trust Insights

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

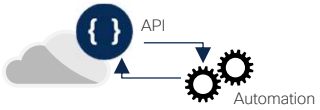
3

Trust data verified against Known-Good-Values (KGV) for hardware and software from Cisco

4

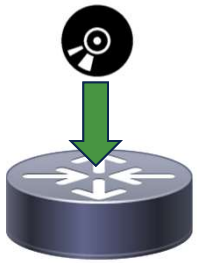
Trust Insights delivers assured inventory reporting with history, and trust visibility for IOS XR systems

5



Trust and Assured Inventory data accessible via API to enable Closed-Loop Automation

Security Features Built on Foundations of Trust



Secure ZTP

RFC8572 compliant secure zero touch provisioning of routers

Disk Encryption

Provides data-at-rest protection for configuration data

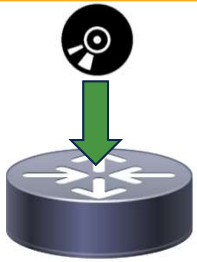
Secure Vault

Protects sensitive data of non-XR applications

Anti-theft Mechanisms

Provides re-image protection for routers to deter thefts

Security Features Built on Foundations of Trust



Secure ZTP

RFC8572 compliant secure zero touch provisioning of routers

Disk Encryption

Provides data-at-rest protection for configuration data

Secure Vault

Protects sensitive data of non-XR applications

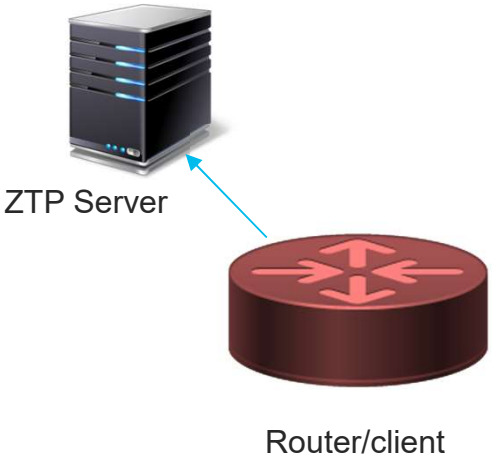
Anti-theft Mechanisms

Provides re-image protection for routers to deter thefts

Security Considerations for ZTP

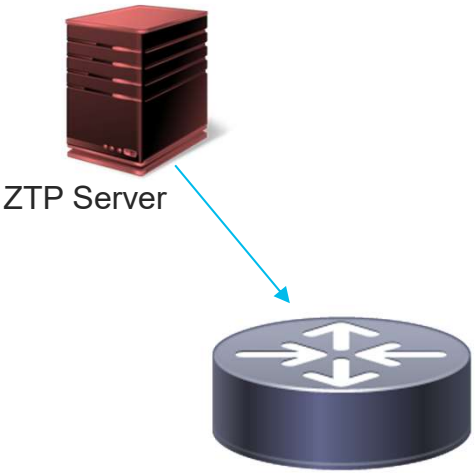
Router/Client Validation

Server must validate router/client cert (SUDI cert) before offering artifacts/secrets/configs



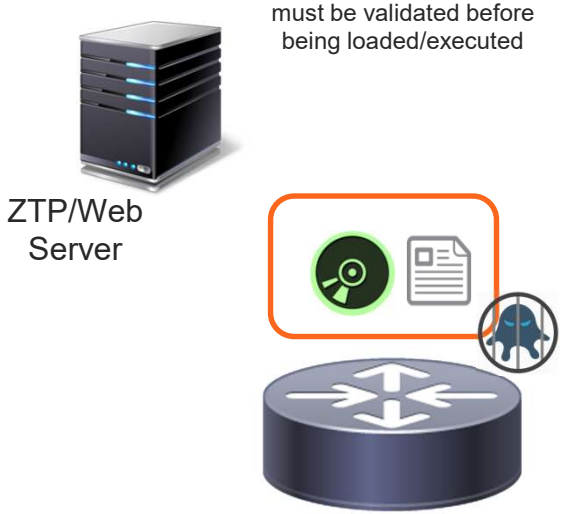
Server Validation

Router/client must validate the server offering artifacts

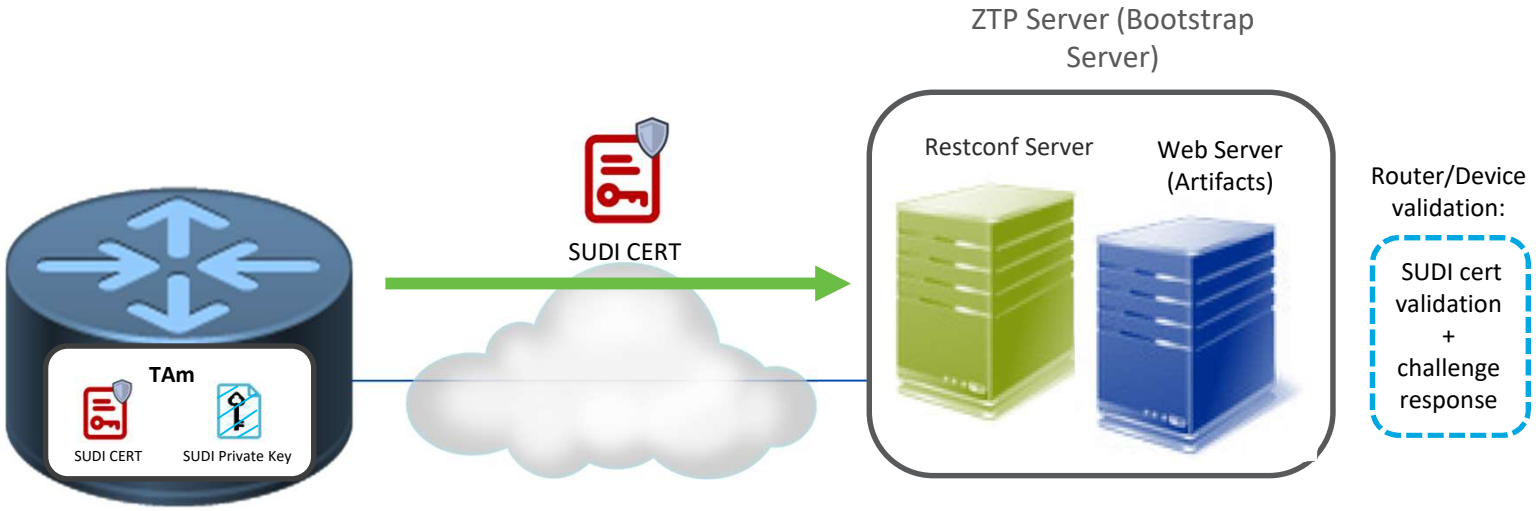


Artifact Validation

The artifact downloaded from the ZTP/Web server must be validated before being loaded/executed

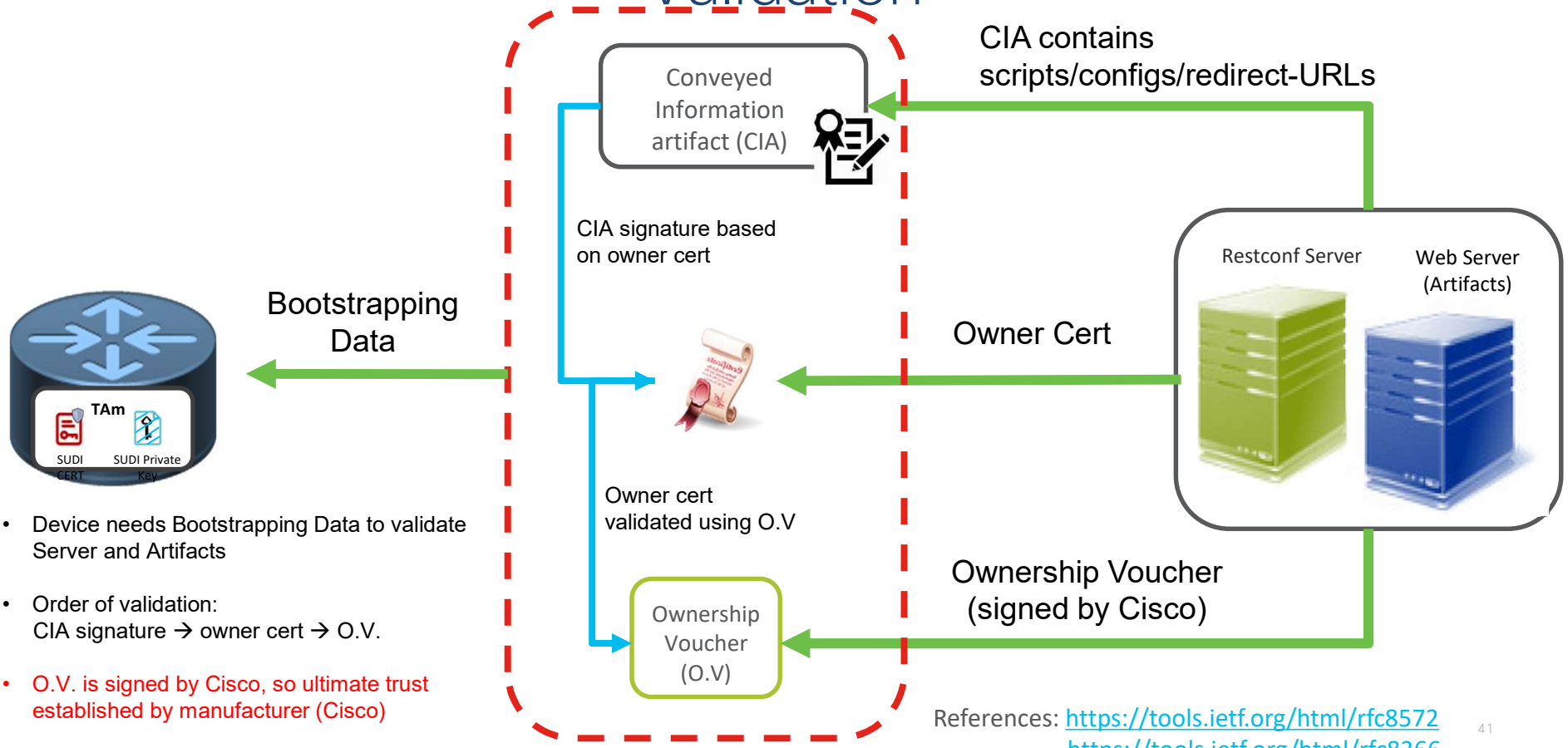


Secure ZTP (RFC8572): Router Validation



Reference: https://tools.ietf.org/html/rfc8572

SZTP Artifacts (RFC 8572): ZTP Server + Artifact Validation



- Device needs Bootstrapping Data to validate Server and Artifacts
- Order of validation:
  CIA signature → owner cert → O.V.
- O.V. is signed by Cisco, so ultimate trust established by manufacturer (Cisco)

References: https://tools.ietf.org/html/rfc8572
https://tools.ietf.org/html/rfc8366

Ownership Voucher (O.V) (RFC 8366)

Yang model for O.V.

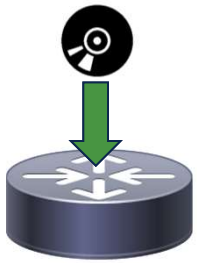
```
module: ietf-voucher

  yang-data voucher-artifact:
      +---- voucher
         +---- created-on                        yang:date-and-time
         +---- expires-on?                       yang:date-and-time
         +---- assertion                         enumeration
         +---- serial-number                     string
         +---- idevid-issuer?                    binary
         +---- pinned-domain-cert                binary
         +---- domain-cert-revocation-checks?    boolean
         +---- nonce?                            binary
         +---- last-renewal-date?                yang:date-and-time
```

- **Serial Number**: Serial number of the router/pledge being bootstrapped
- **Pinned-domain-cert (PDC):** The owner cert is rooted to the chain of trust leading to the pinned-domain cert. This means PDC can be the root cert for OC or an intermediate cert for OC or the same as OC (self-signed).

Reference: https://tools.ietf.org/html/rfc8366

Security Features Built on Foundations of Trust



Secure ZTP

RFC8572 compliant secure zero touch provisioning of routers

Disk Encryption

Provides data-at-rest protection for configuration data

Secure Vault

Protects sensitive data of non-XR applications

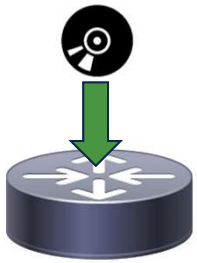
Anti-theft Mechanisms

Provides re-image protection for routers to deter thefts

Disk Encryption

1. Provides data-at-rest protection
2. Encrypts disk partitions
3. Encryption key protected by TAm
4. Zeroization CLI for RMA scenarios

Security Features Built on Foundations of Trust



Secure ZTP

RFC8572 compliant secure zero touch provisioning of routers

Disk Encryption

Provides data-at-rest protection for configuration data

Secure Vault

Protects sensitive data of non-XR applications

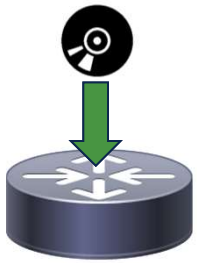
Anti-theft Mechanisms

Provides re-image protection for routers to deter thefts

Secure Vault

1. Store secrets of non-XR applications
2. Hashicorp's secure vault in IOS-XR
3. Hashicorp front-end and middleware
4. Backend protected by TAm

Security Features Built on Foundations of Trust



Secure ZTP

RFC8572 compliant secure zero touch provisioning of routers

Disk Encryption

Provides data-at-rest protection for configuration data

Secure Vault

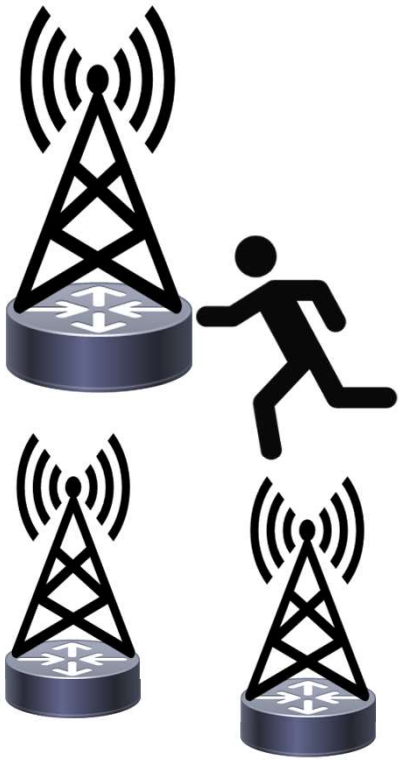
Protects sensitive data of non-XR applications

Anti-theft Mechanisms

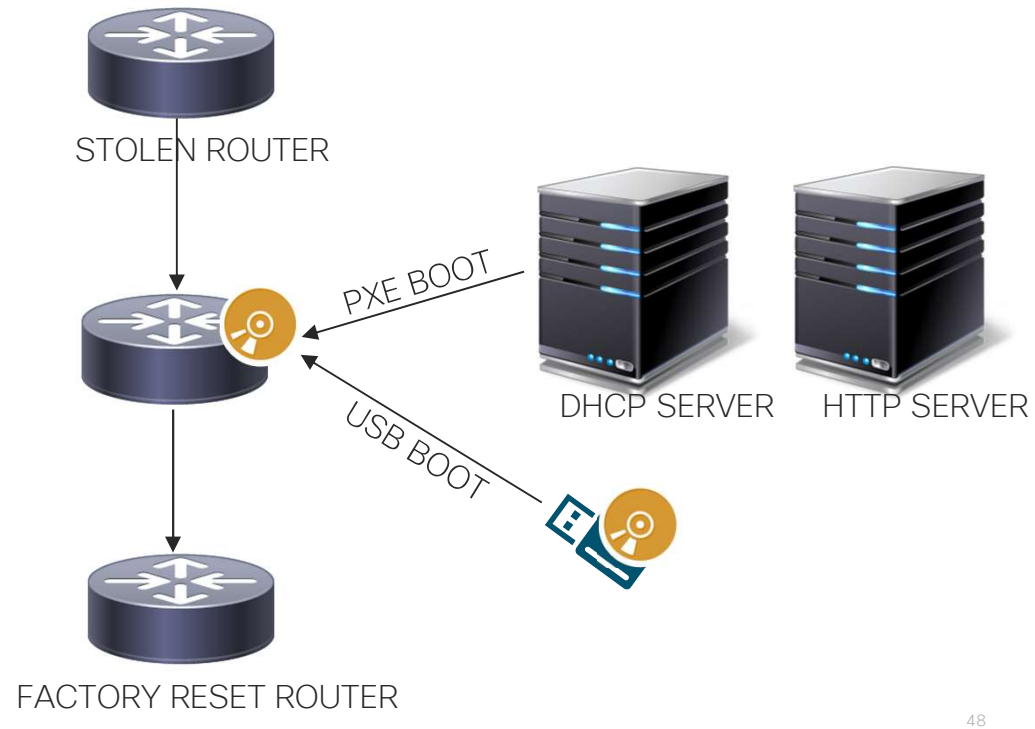
Provides re-image protection for routers to deter thefts

The Problem

CUSTOMER PREMISES

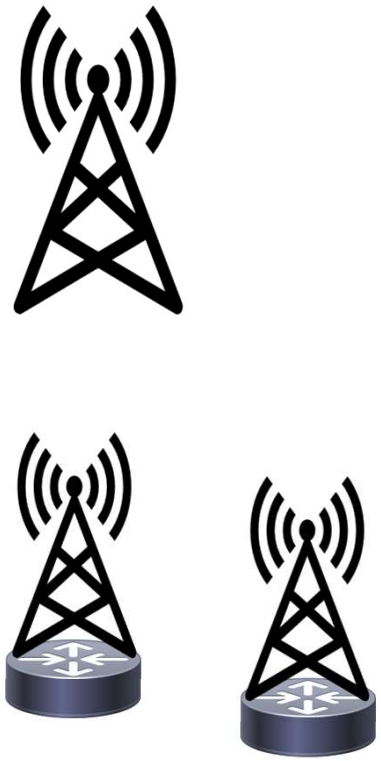


ATTACKER'S PREMISES

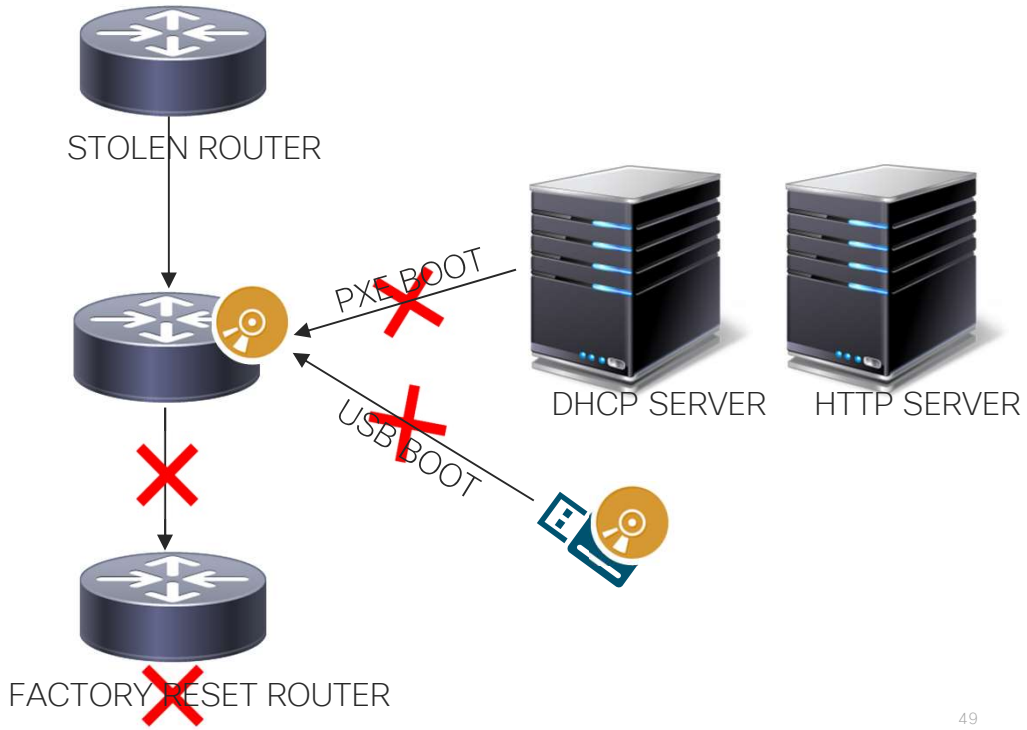


Proposed Solution

CUSTOMER PREMISES



ATTACKER'S PREMISES



The Proposed Solution

Workflow

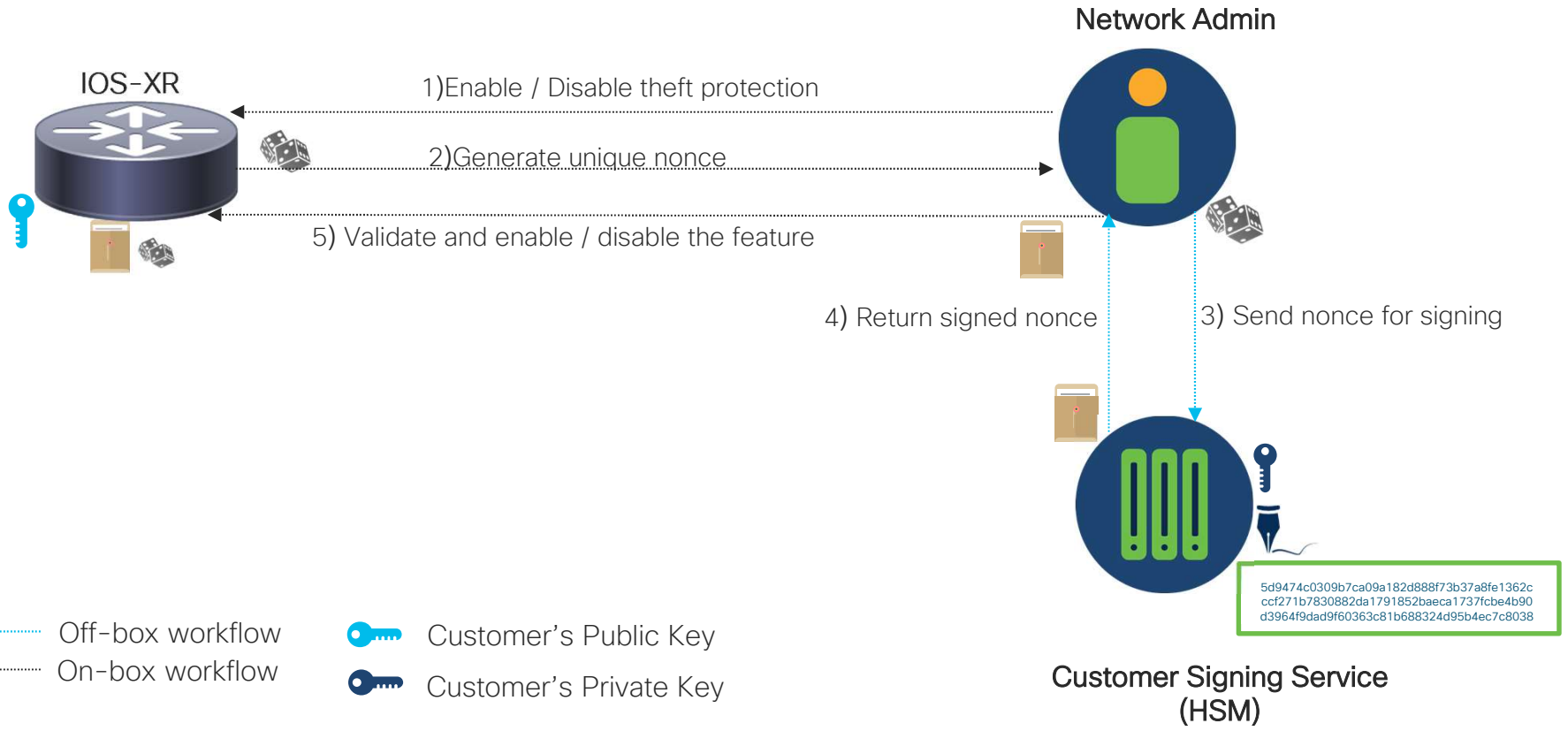
- New XR CLI to disable USB/PXE boot
- Store the flag in the router's hardware secure storage
- Persistent across disk erasure & reload
- Secure storage is tamper-resistant
- BIOS disables USB/PXE boot if flag is enabled

Can we do more?

New Threats

- Remote attacker locking the router upgrades
- Rogue employee scenarios
  - Disabling the feature with intent of stealing
  - Enabling the feature with intent of disruption

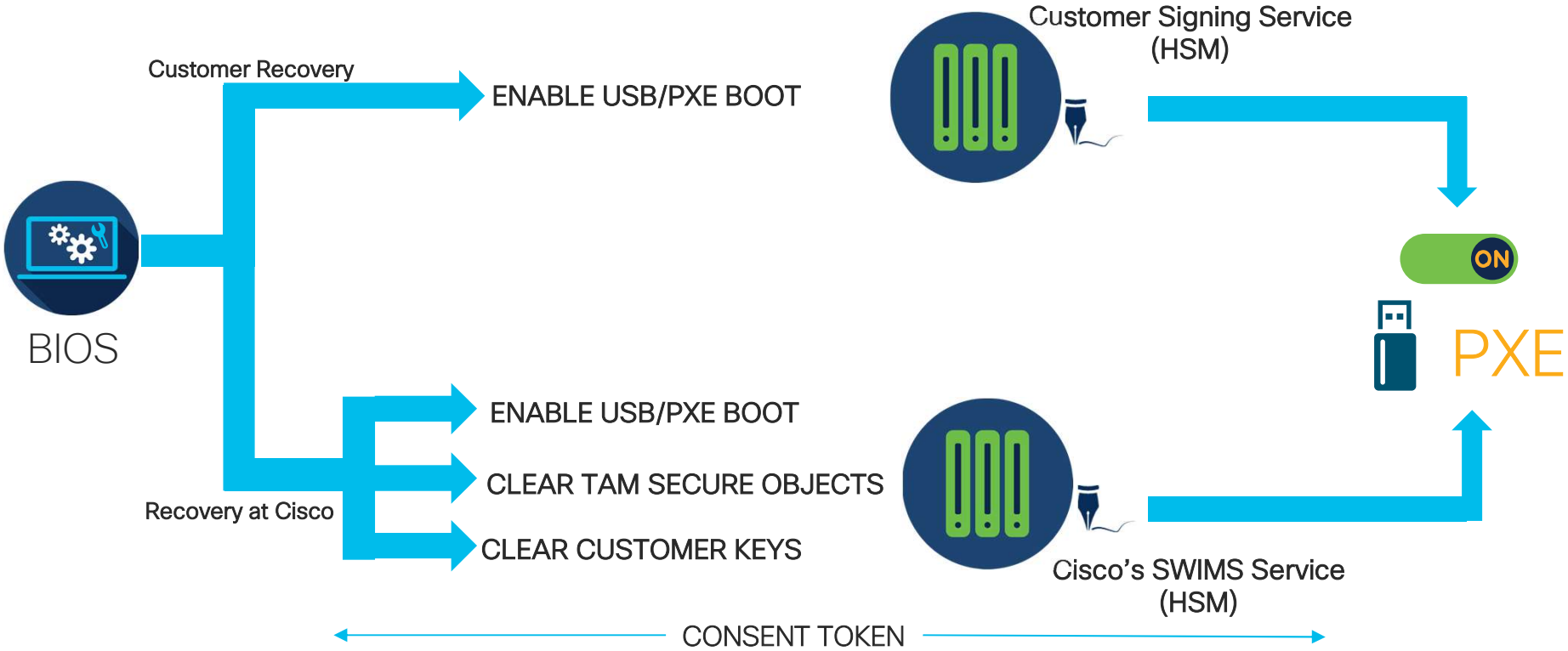
CLI Challenge-Response Workflow



What about these scenarios?

1. Corrupted IOS-XR binary
2. Customer key compromise
3. Devices sent back to Cisco (RMA)

BIOS Recovery Utility



Security Services

Trusted Path Routing

Extends trust into routing domain steering sensitive flows to bypass compromised devices

IPsec

Transport security for 5G deployments

Anti-DDoS Solutions

Arbor & Radware DDoS Solutions for peering and mobility use-cases

Security Services

Trusted Path Routing

Extends trust into routing domain by steering sensitive flows to bypass compromised devices

IPsec

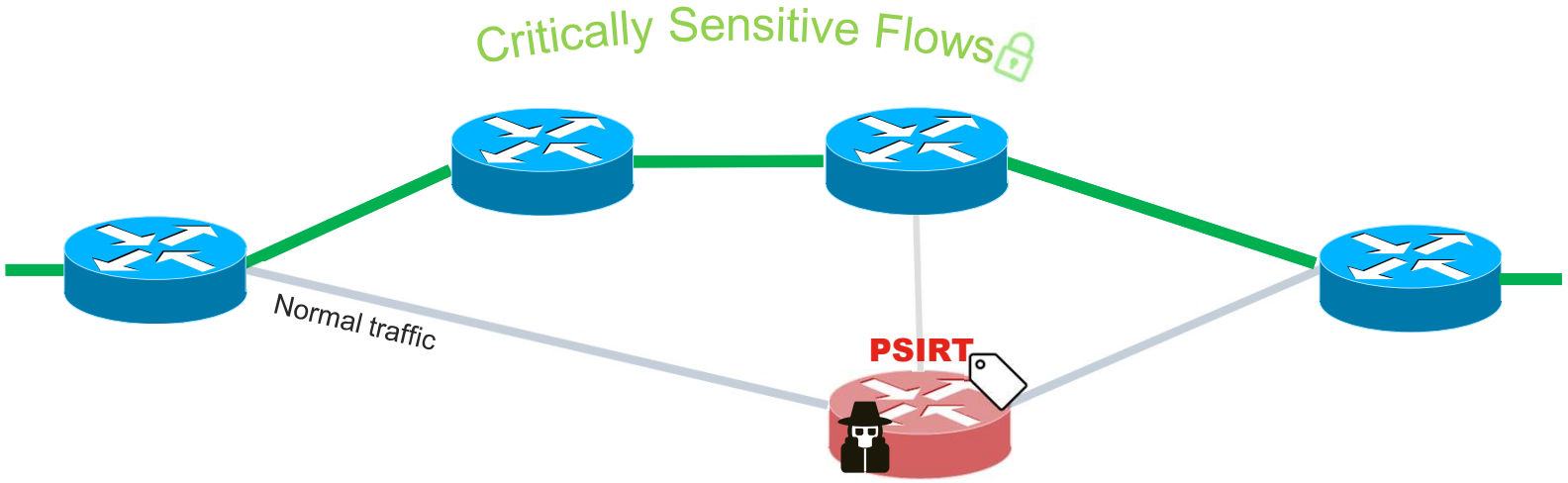
Transport security for 5G deployments

Anti-DDoS Solutions

Arbor & Radware DDoS Solutions for peering and mobility use-cases

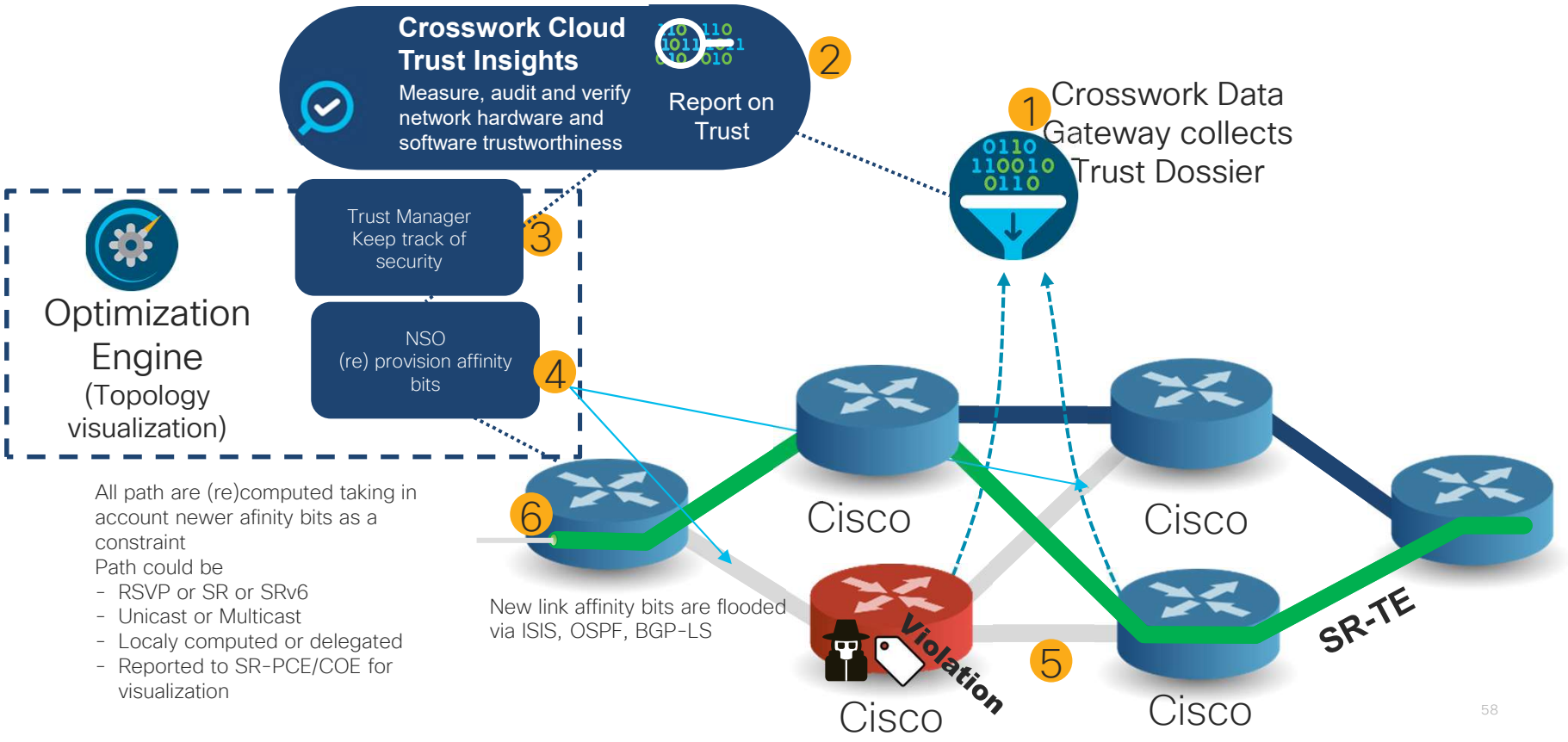
Trusted Path Routing

Bypass less trustworthy Routers

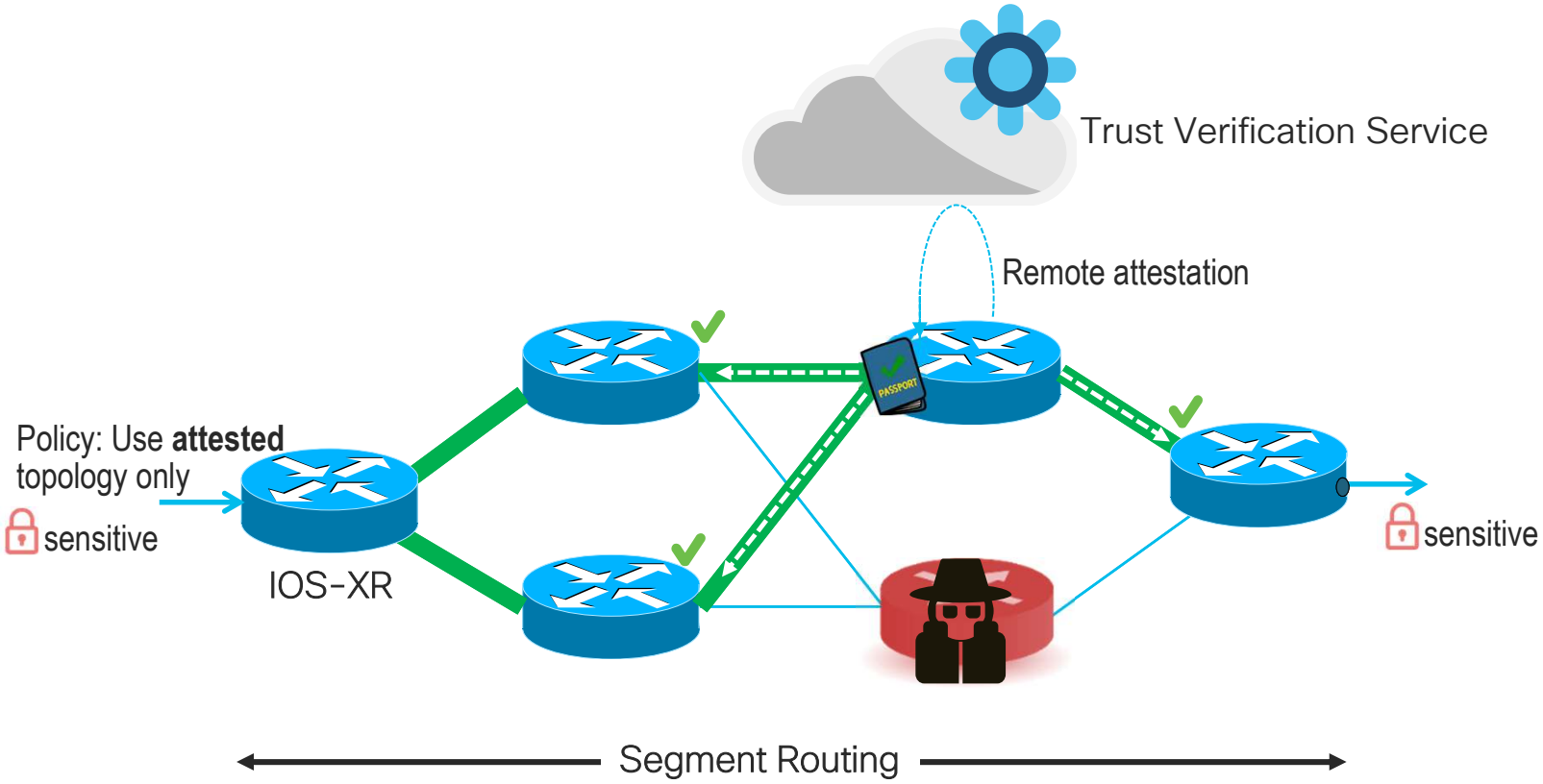


- Untrustworthy equipment vendor
- Unpatched / Vulnerable software
- Active compromise underway

Trusted Path Routing – Centralized



Distributed Trusted Path Routing



Security Services

Trusted Path Routing

Extends trust into routing domain by steering sensitive flows to bypass compromised devices

IPsec

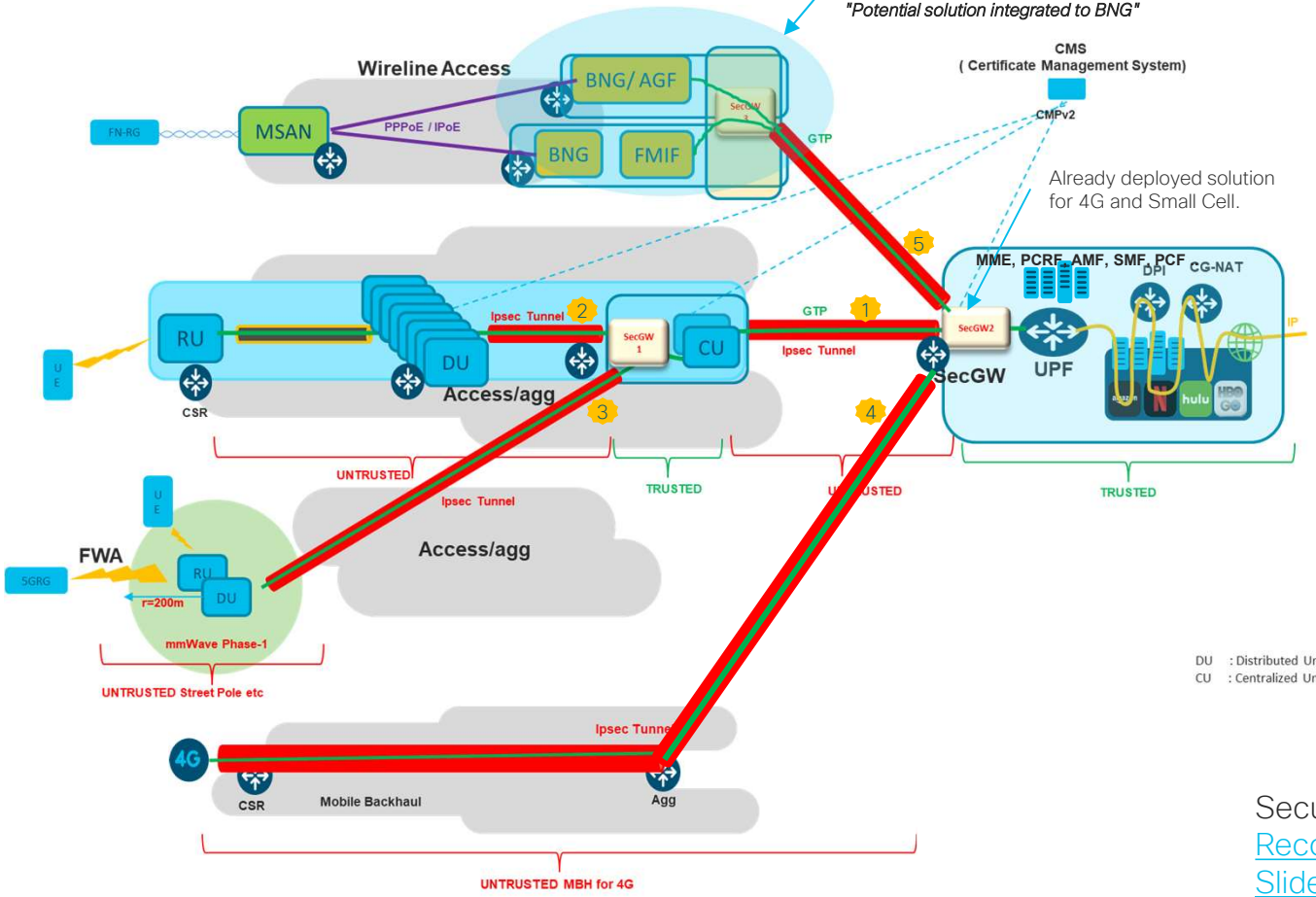
Transport security for 5G deployments

Anti-DDoS Solutions

Arbor & Radware DDoS Solutions for peering and mobility use-cases

IPsec Placeholder

BBF 02.CY20 Meeting June 2020
WWC draft driven by 3GPP and BBF
"Potential solution integrated to BNG"



Use cases

1. CU-UPF are not co-located and in an untrusted transport segment
2. Multiple DU to CU mapping – above CU IPsec Scale Limits
3. mmWave Phase-1 – On-boarded in untrusted outdoor sites
4. 4G/LTE current use-case
5. AGF/Non-3gpp access use case
6. pLTE and p5G on-prem use case

IPsec Variants

Physical and Virtual form factors

DU : Distributed Unit RAN
CU : Centralized Unit of RAN

Securing the 5G xHaul Network
Recording
Slides

Security Services

Trusted Path Routing

Extends trust into routing domain by steering sensitive flows to bypass compromised devices

IPsec

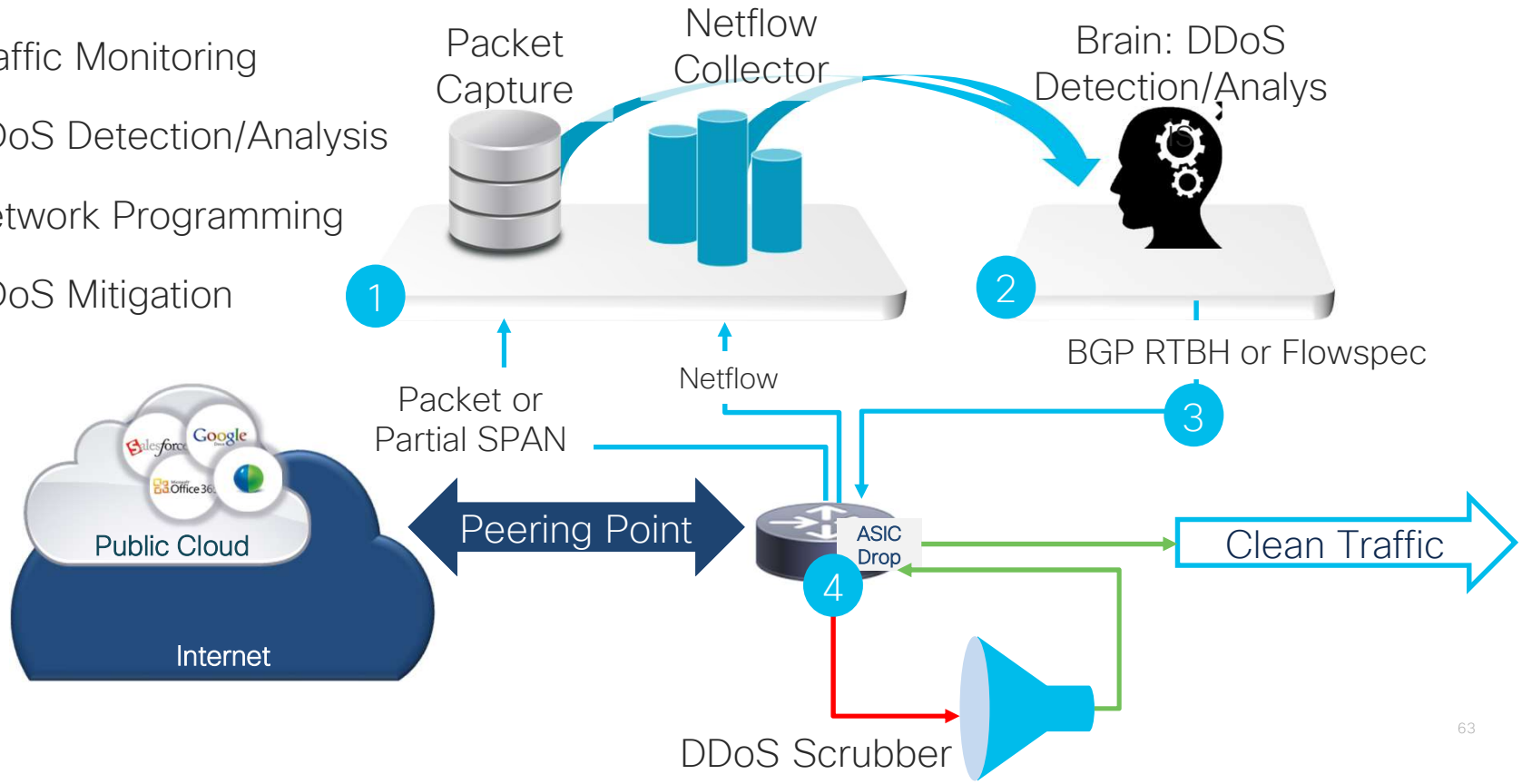
Transport security for 5G deployments

Anti-DDoS Solutions

Arbor & Radware DDoS Solutions for peering and mobility use-cases

Understanding the DDoS Solutions

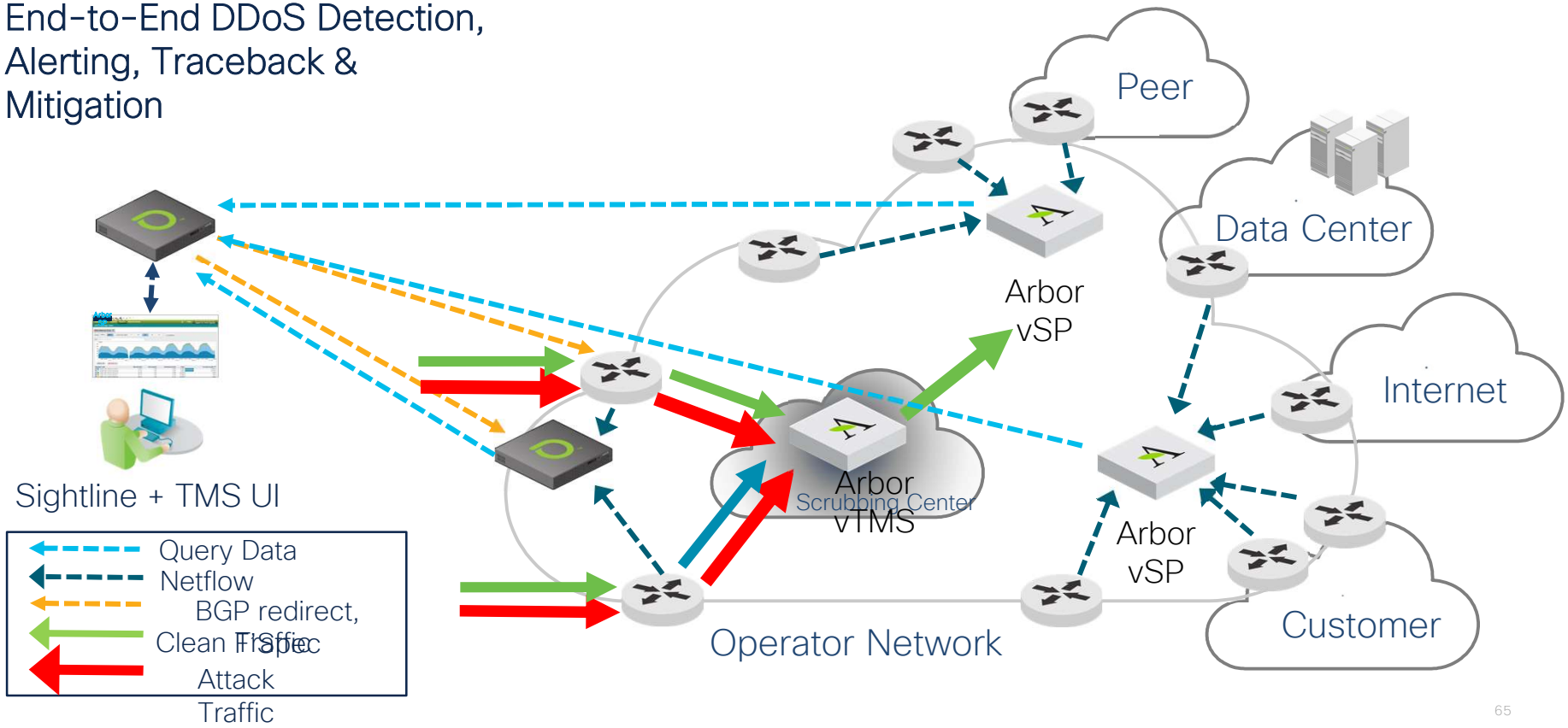
1. Traffic Monitoring
2. DDoS Detection/Analysis
3. Network Programming
4. DDoS Mitigation



Arbor DDoS Solution

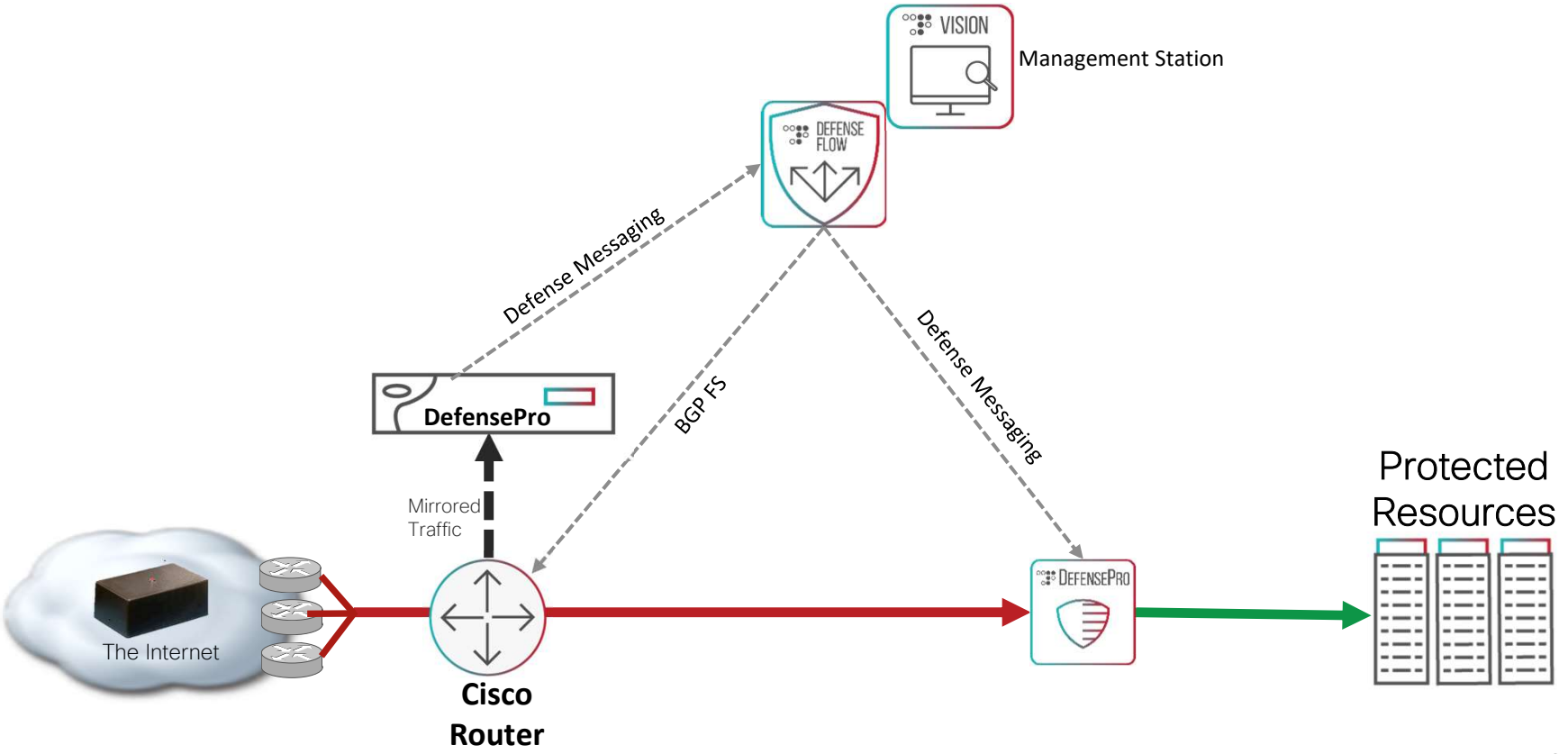
Arbor Sightline + Threat Mitigation System (TMS)

End-to-End DDoS Detection, Alerting, Traceback & Mitigation



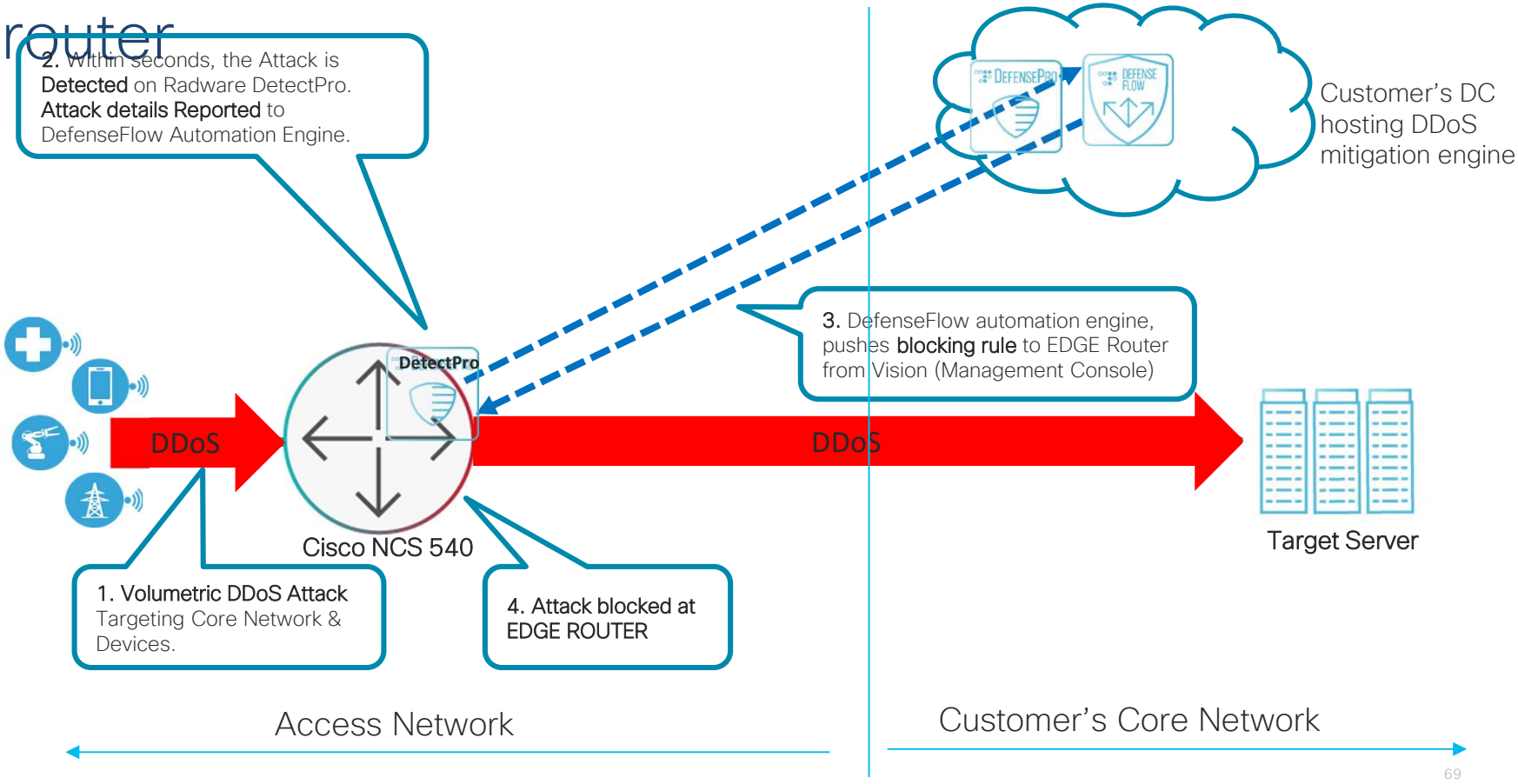
Radware DDoS Solution

Radware DDoS Solution Components



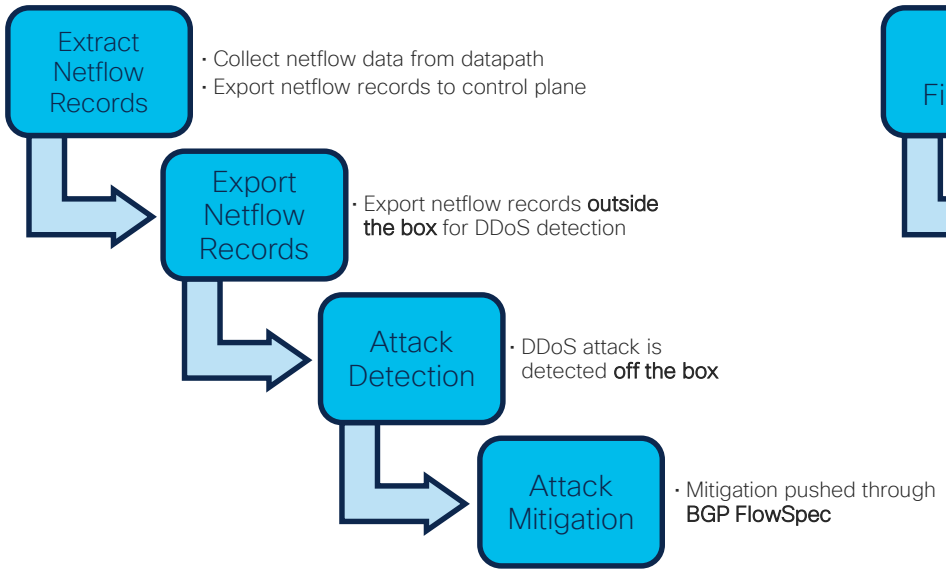
Introducing Radware DetectPro

DDoS Solution with DetectPro container on the router

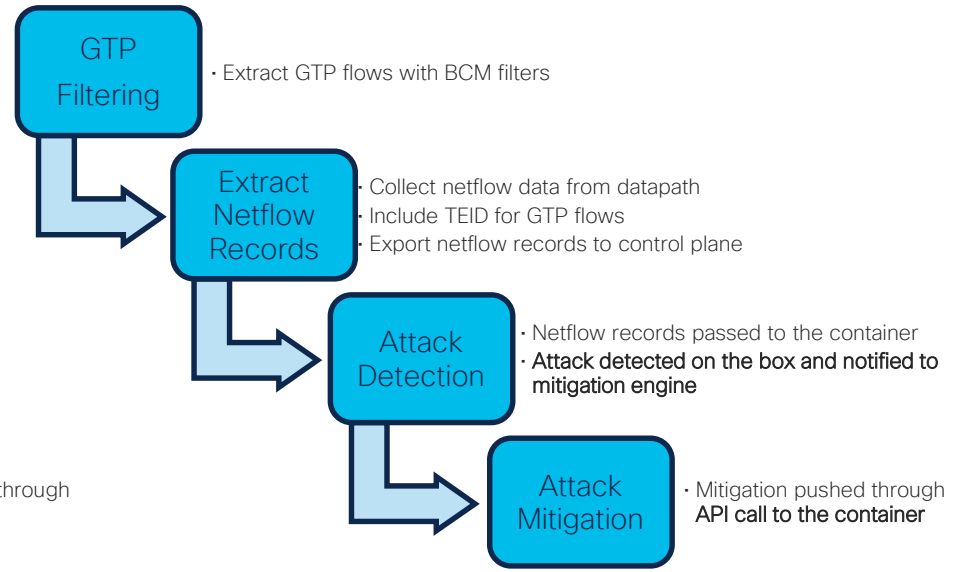


DDoS Workflow Comparison

Existing Workflow

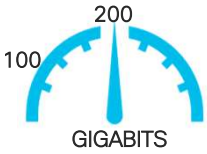


Improved Workflow with DetectPro

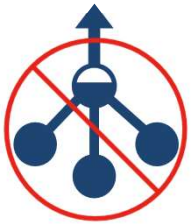


Highlights of Radware Solution

Faster Detection



Higher Attack Bandwidth



No More Flow Export

No Hardware Dependency

To Summarize…

Key Takeaways

- TRUSTWORTHY VENDOR
- PERVASIVE SECURITY
- OPERATIONAL SECURITY
- 5G READY

Questions?


CISCO