Building Intelligent Networks with Cisco 5G Converged SDN Transport

Security and Programmability

Mustafa Bostanci, 5G Architecture Product Manager

Phil Bedard, Principal Engineer

14 Sep 2021

Agenda

1. Market and Evolution

2. Trustworthy Platforms & XR Security
   for 5G Converged SDN Transport

3. XR Programmability
   for 5G Converged SDN Transport

Agenda

1 Market and Evolution

2 Trustworthy Platforms & XR Security
for 5G Converged SDN Transport

3 XR Programmability
for 5G Converged SDN Transport

A Changing World Served by Telecommunications

$12.3T

revenue growth
in industries by 2035*

$3.5T

mobile industry growth and 22 million jobs by 2035*

7X mobile traffic growth

980 EB/year in 2024
79% will be video**

More people, more things

5.8 billion mobile users in 2024**

3X speed increase**

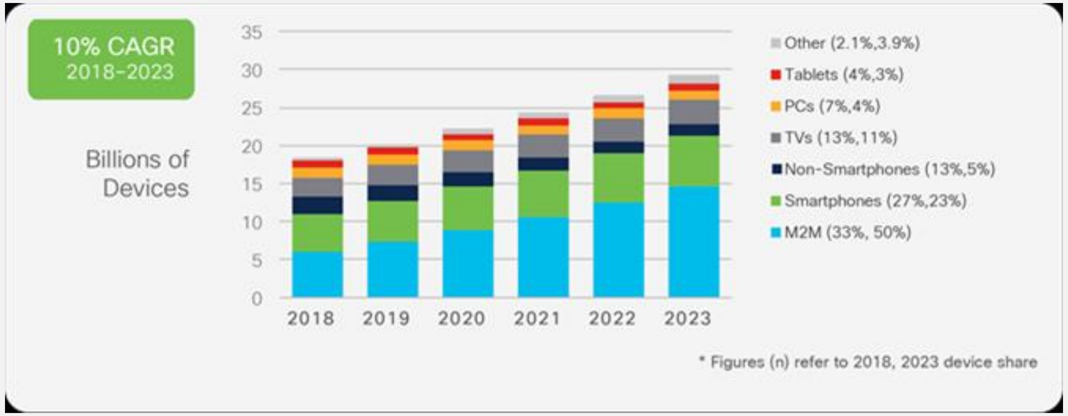
IoT/M2M traffic grows 8x by 2024**

smart cities, connected cars, AR/VR,
telehealth, smart grid, etc.

* IHS Markit
** Cisco VNI 2021

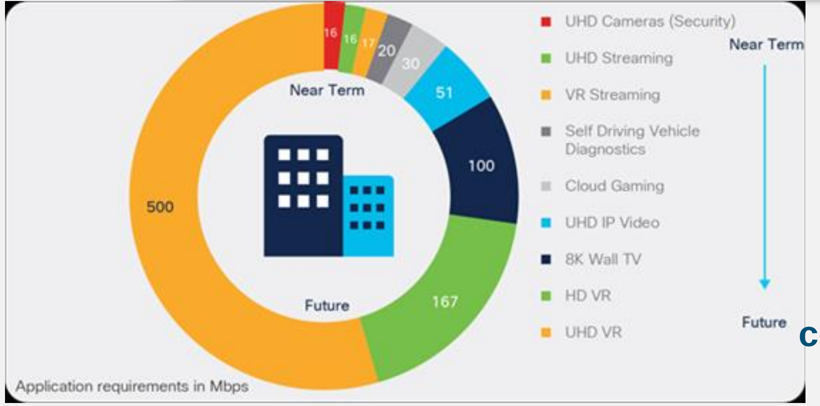
Why we need Converged SDN Transport Network?

Machines are Becoming The Consumer



A different Machine Type Communication Dominates Connectivity

Bandwidth demand remains in parallel to data density



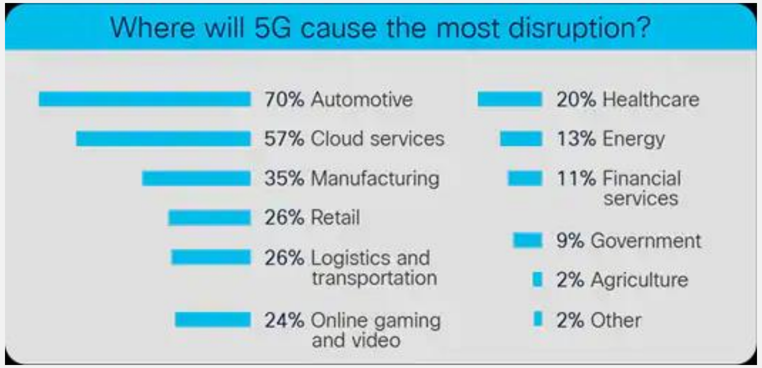
13Mbps today

44Mbps

Global Average connection speed by 2023

5G drives up to 100x traffic capacity

Diversified Services becoming de-facto

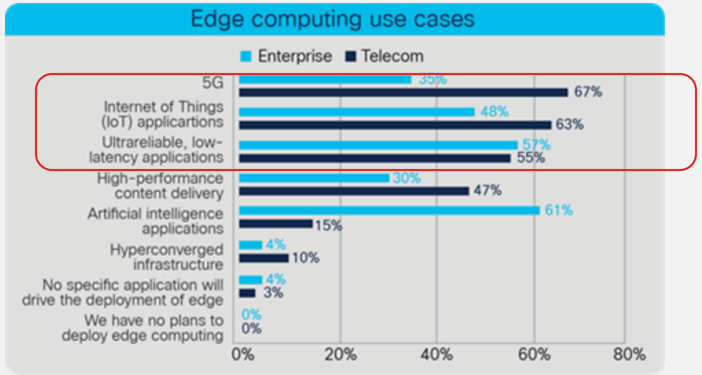


Static today

Adaptive

A single network “Sliced” in to sub networks to meet economics

Edge Services will require SLA based Access



63%

Edge compute services require URLLC by 2023

Networks will evolve deeper to edge for low Latency

Architecture Evolution

1. Decomposition of network functions (e.g., CUPS) &
   - Distribution to network data plane functions deeper into network
   - Centralization of policy and control functions
2. Automate and Program Network Connectivity
   - Dynamic placement of functions and interconnectivity across network
   - Connectivity isolation and SLA management using network slicing
   - Mass Scale Networks employ scalable fulfillment, assurance and visibility
3. Securing network devices and connectivity
   - Integrity and confidentiality of platforms and network slices

Agenda

1 Market and Evolution

2 Trustworthy Platforms & XR Security
for 5G Converged SDN Transport

3 XR Programmability
for 5G Converged SDN Transport

Why Security is Mandatory for Service Providers!

Targeted attacks on Critical Infrastructure

Impact on Economy

Untrusted Locations

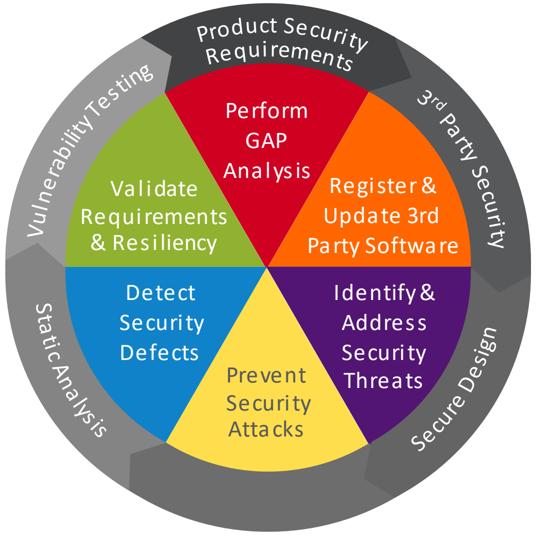
Complex to Manage

Foundations of Trustworthy Platforms

Process ◀┈┈┈ Technology ┈┈┈▶ Policy

Secure Process

Lifecycle / Security Baseline


Product Security Requirements
3rd Party Security
Secure Design
Static Analysis
Vulnerability Testing
Perform GAP Analysis
Register & Update 3rd Party Software
Identify & Address Security Threats
Prevent Security Attacks
Detect Security Defects
Validate Requirements & Resiliency

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 — Common Criteria

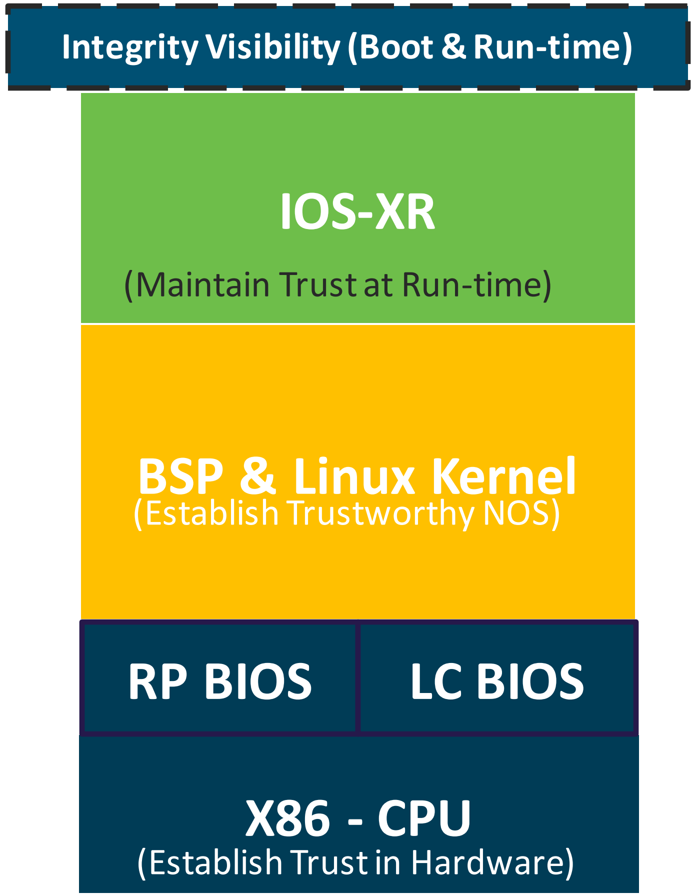
ISO — ISO 27034

NIST — FIPS / USGv6

Trusted Computing Group — TCG

Trustworthy Platforms – Network OS View

NOS



Integrity Visibility (Boot & Run-time)

IOS-XR

(Maintain Trust at Run-time)

BSP & Linux Kernel

(Establish Trustworthy NOS)

RP BIOS **LC BIOS**

X86 - CPU

(Establish Trust in Hardware)

Protection against

Ransomware

MitM attacks

3rd Party Security

Known Vulnerabilities

Credential Theft

Malware Attacks

Malware Attacks

Boot Vulnerability

Counterfeit Hardware

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

Cisco TAm – Hardware-based Trust Anchor

Hardware Integrity

Provides counterfeit hardware protection and acts as a trust anchor

* NIST 800-90 certified

Anti-Theft and Anti-Tamper Chip Design

Built-In Crypto Functions

Hardware Entropy for RNG*

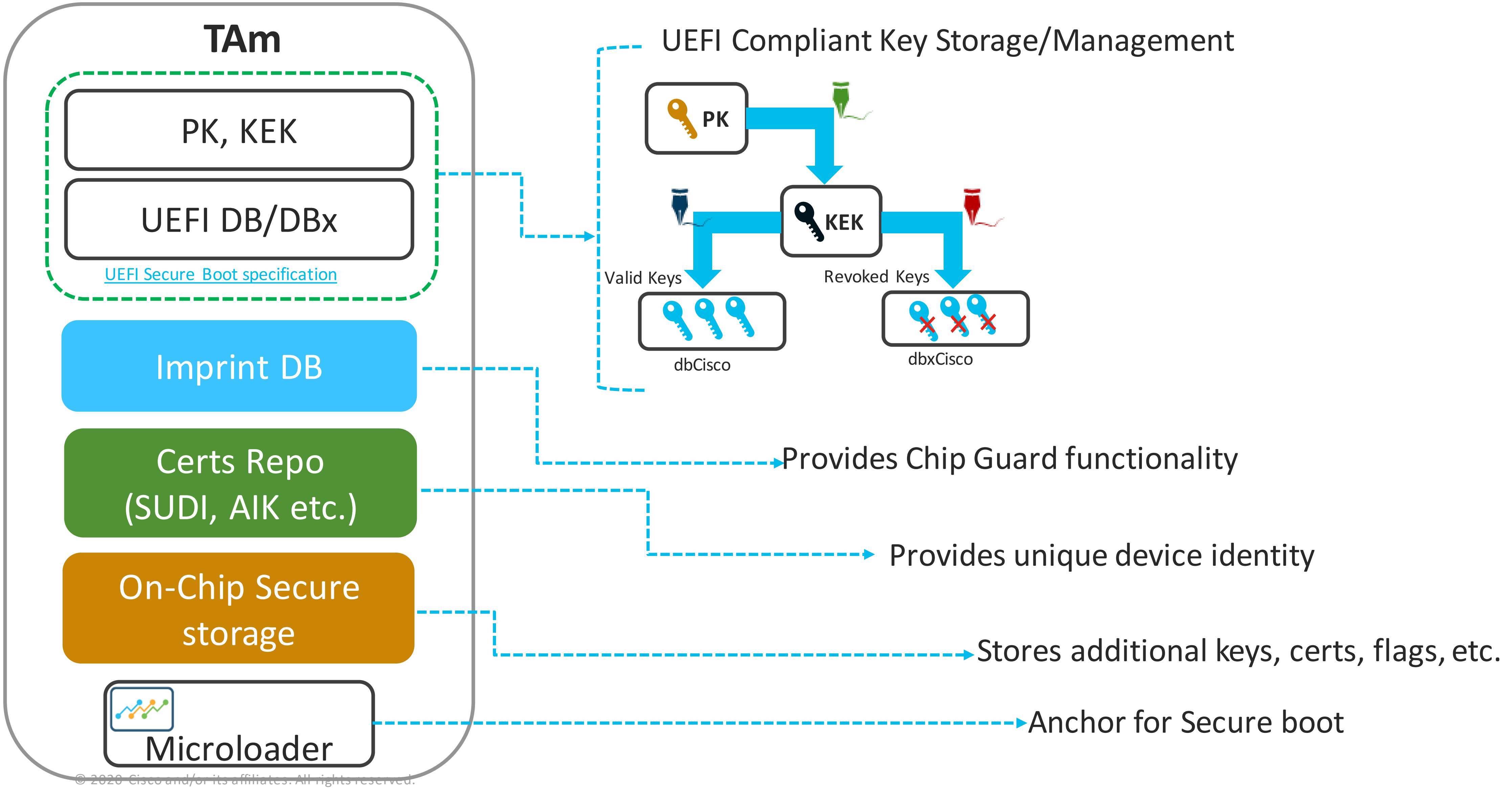
Secure Storage

- 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

TAm Chip Module Overview

Hardware Integrity

Provides counterfeit hardware protection and acts as a trust anchor



TAm

PK, KEK

UEFI DB/DBx

UEFI Secure Boot specification

Imprint DB

Certs Repo (SUDI, AIK etc.)

On-Chip Secure storage

Microloader

UEFI Compliant Key Storage/Management

PK

KEK

Valid Keys

Revoked Keys

dbCisco

dbxCisco

Provides Chip Guard functionality

Provides unique device identity

Stores additional keys, certs, flags, etc.

Anchor for Secure boot

Cisco Secure Boot - Overview

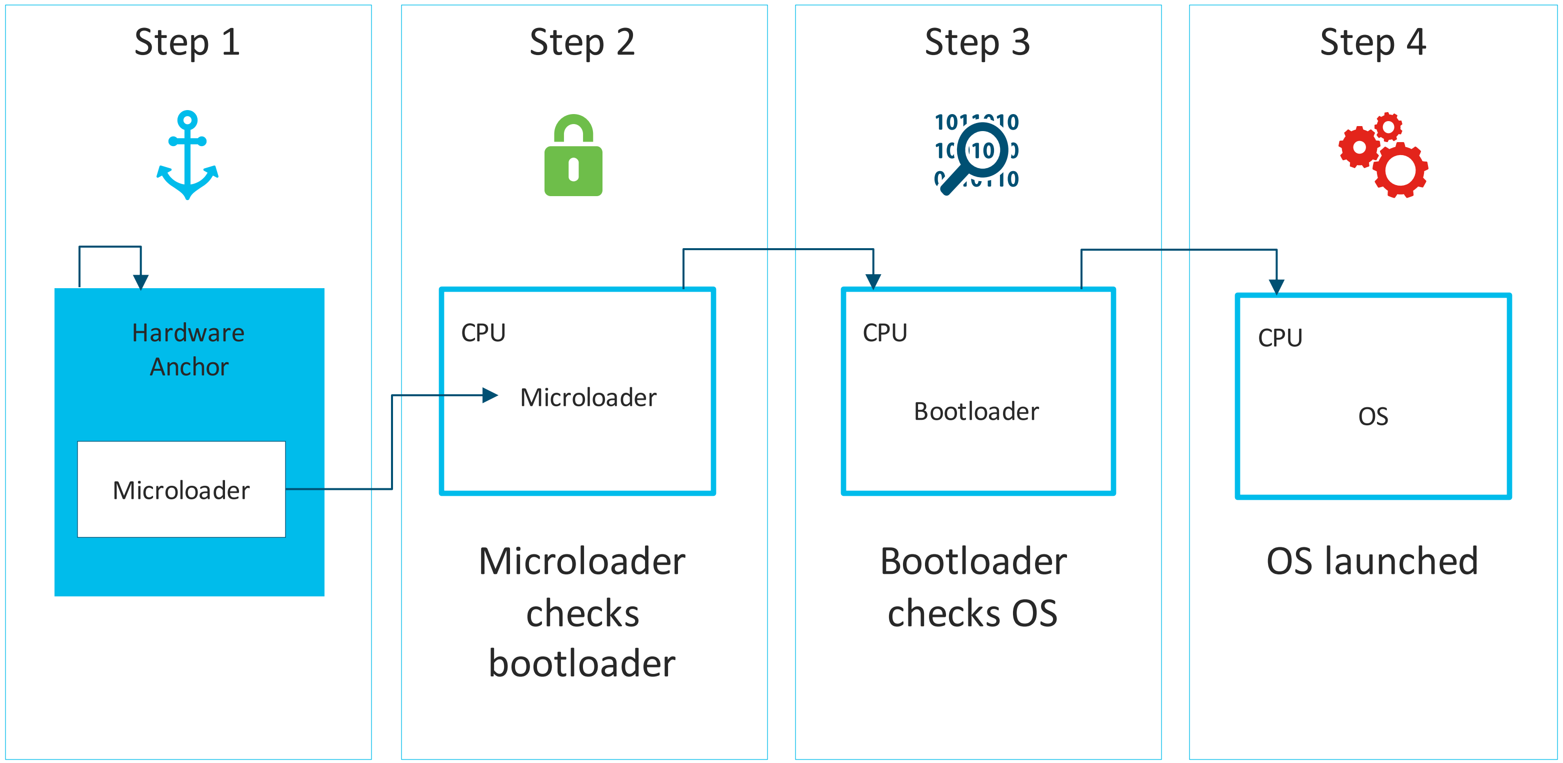
Anchors Secure Boot in Hardware to Create a Chain of Trust

Boot Integrity

Ensures integrity of the boot process

Cisco Secure Boot

Boot Code Integrity Anchored in Hardware



Step 1

Hardware Anchor

Microloader

Step 2

CPU

Microloader

Microloader checks bootloader

Step 3

CPU

Bootloader

Bootloader checks OS

Step 4

CPU

OS

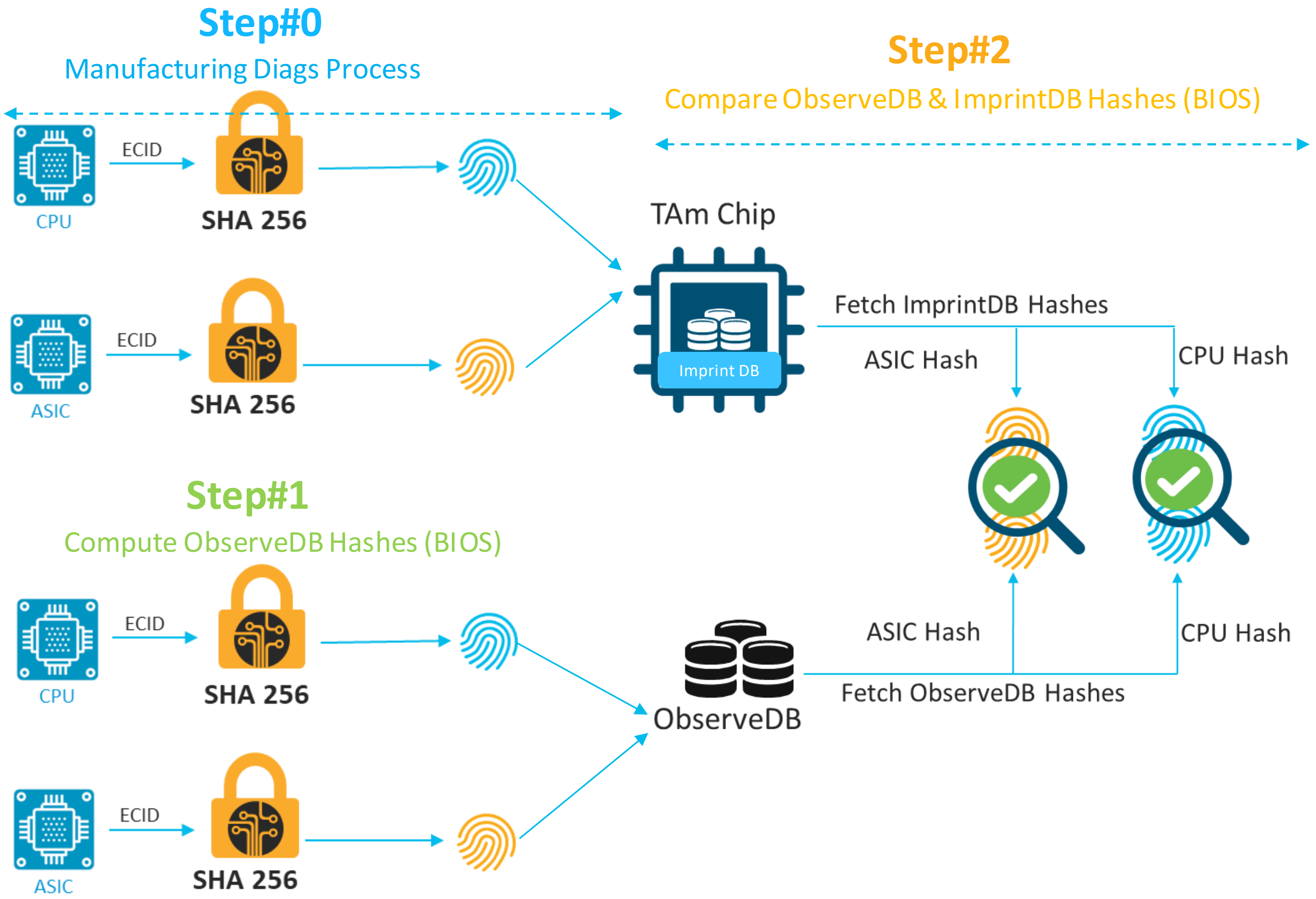
OS launched

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 acts as the anchor to the secure boot and the chain of trust starts from hardware

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

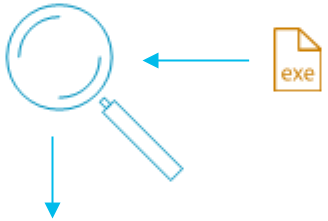


Linux Integrity Measurement Architecture (IMA)

Runtime Integrity

Ensures integrity of the IOS-XR runtime

IMA Logging



/bin/bash

```
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)

Boot Integrity Visibility (BIV) – Validate Trust

Trust Visibility

Provides visualization of Trust

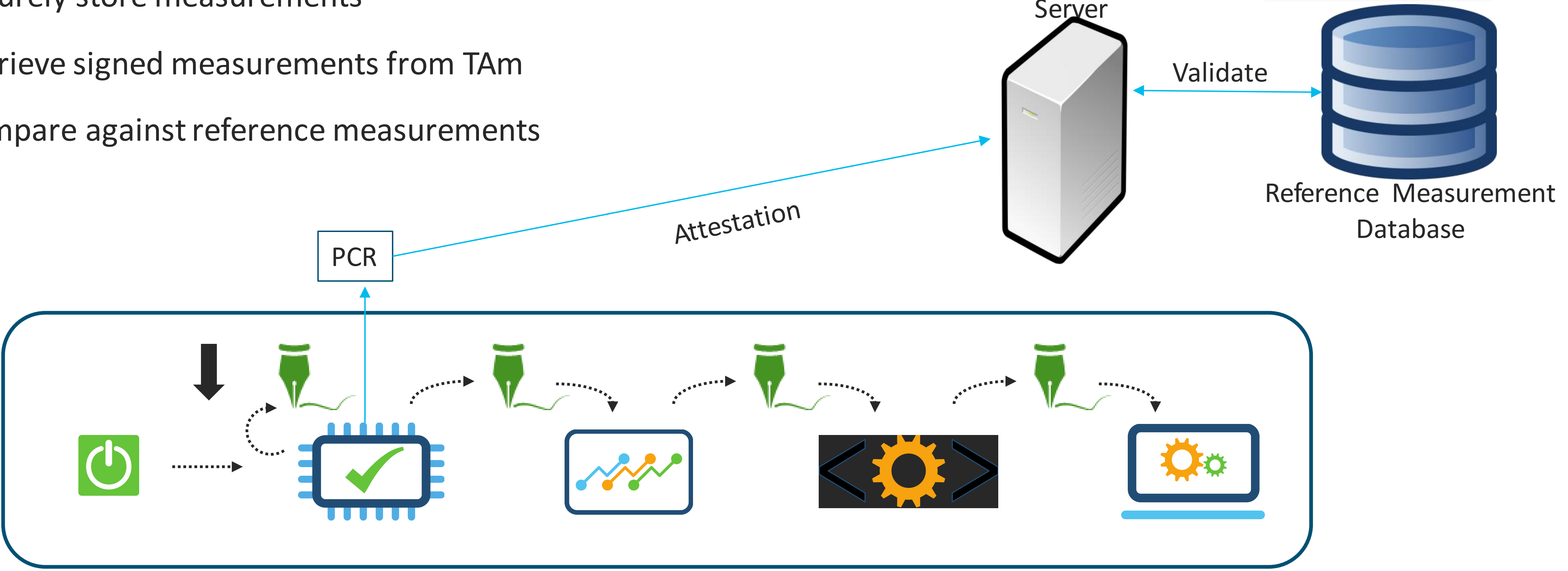
- Measure each boot stage
- Securely store measurements
- Retrieve signed measurements from TAm
- Compare against reference measurements

External service to Verify trust

APIC - Enterprise Module

Filters | Layout

Device Status	Device Name	IP Address	Trust Status
Reachable	[illegible]	[illegible]	Trusted
Reachable	[illegible]	[illegible]	Unknown
Reachable	[illegible]	[illegible]	Trusted
Reachable	[illegible]	[illegible]	Unknown
Reachable	[illegible]	[illegible]	Unknown



How Trust Validation Works – Trust Insights

Trust Visibility

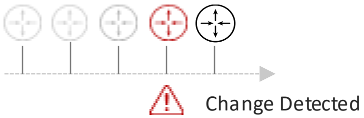
Provides visualization of Trust

1

IOS XR
Trust Insights

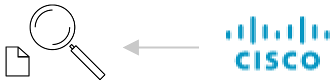
Trust Insights securely requests and collects signed evidence dossier from IOS XR devices

2



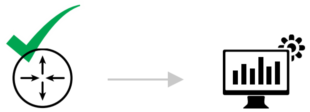
Dossier evidence verified and added to timeline of running hardware and software

3



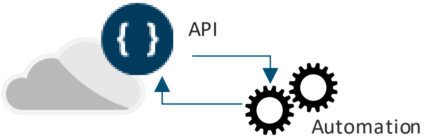
Trust data verified against Known-Good-Values (KGV) for hardware and software from Cisco

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

Examples of 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

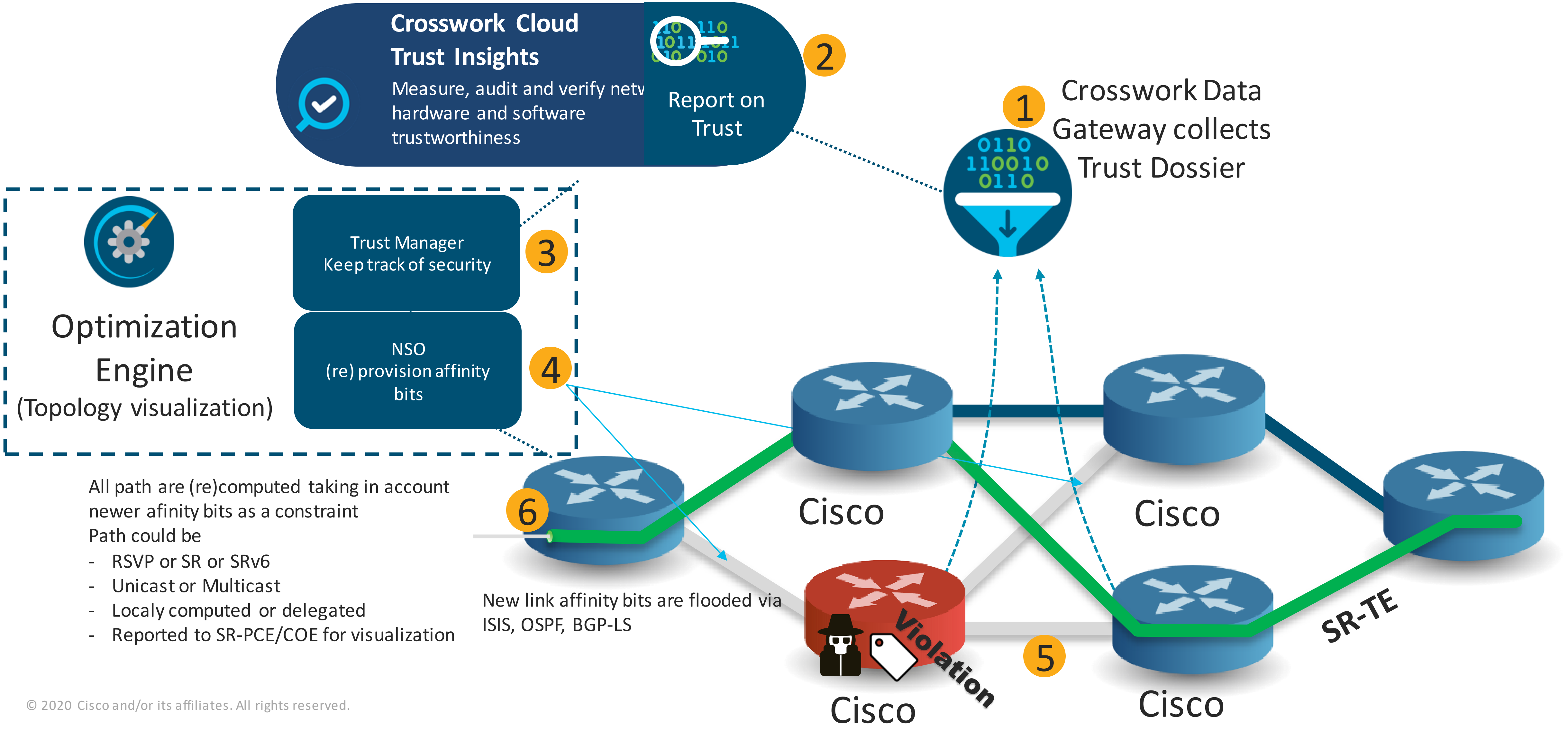
Anti-theft Mechanisms

Provides re-image protection for routers to deter thefts

Trusted Path Routing - Centralized

Trusted Path Routing

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



Crosswork Cloud Trust Insights

Measure, audit and verify netv hardware and software trustworthiness

Report on Trust

Crosswork Data Gateway collects Trust Dossier

Optimization Engine (Topology visualization)

Trust Manager
Keep track of security

NSO
(re) provision affinity bits

All path are (re)computed taking in account newer afinity bits as a constraint
Path could be

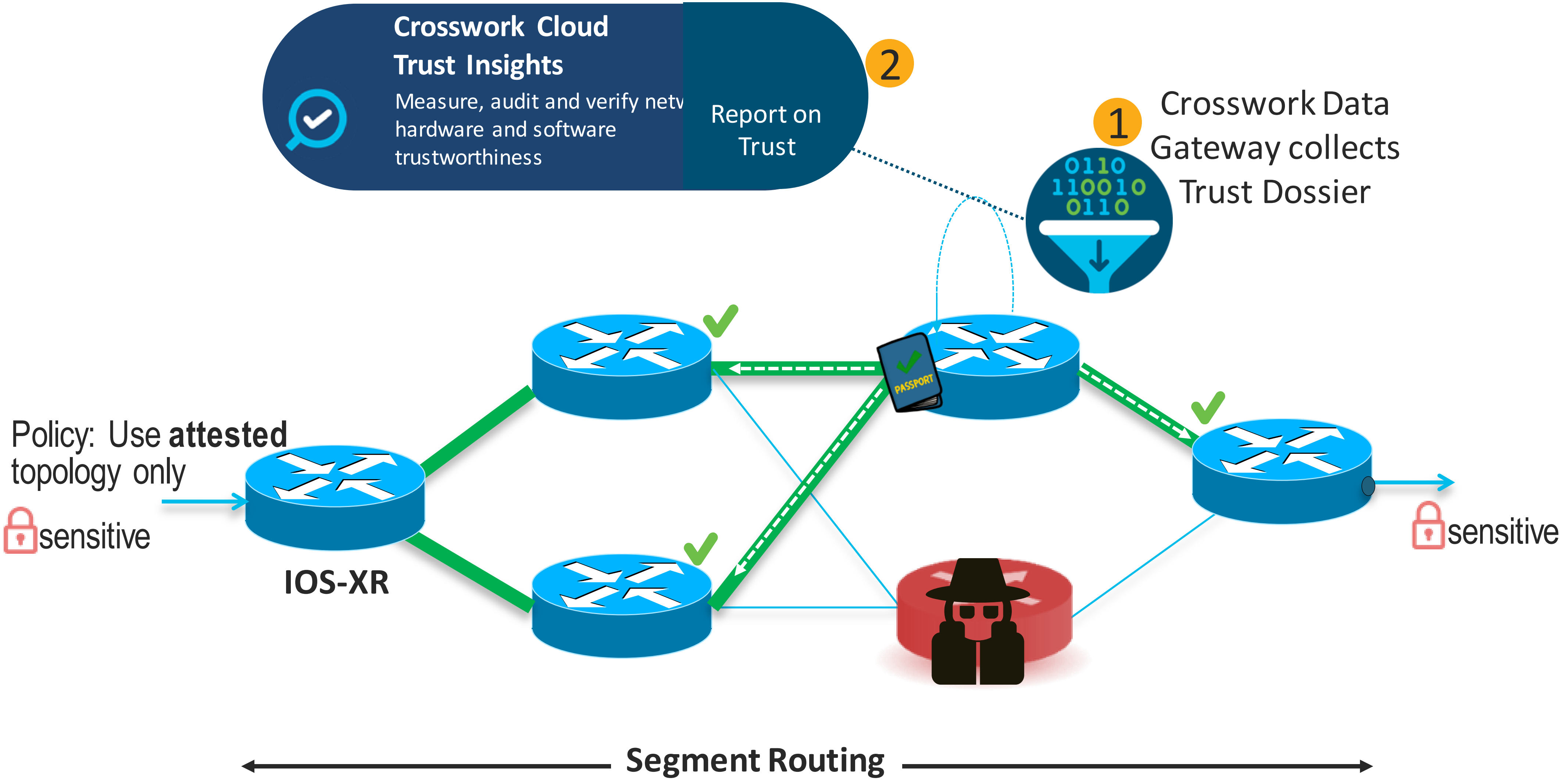
- RSVP or SR or SRv6
- Unicast or Multicast
- Localy computed or delegated
- Reported to SR-PCE/COE for visualization

New link affinity bits are flooded via ISIS, OSPF, BGP-LS

Distributed Trusted Path Routing

Trusted Path Routing

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



Crosswork Cloud Trust Insights

Measure, audit and verify netv hardware and software trustworthiness

Report on Trust

2

1

Crosswork Data Gateway collects Trust Dossier

Policy: Use **attested** topology only

sensitive

IOS-XR

sensitive

Segment Routing

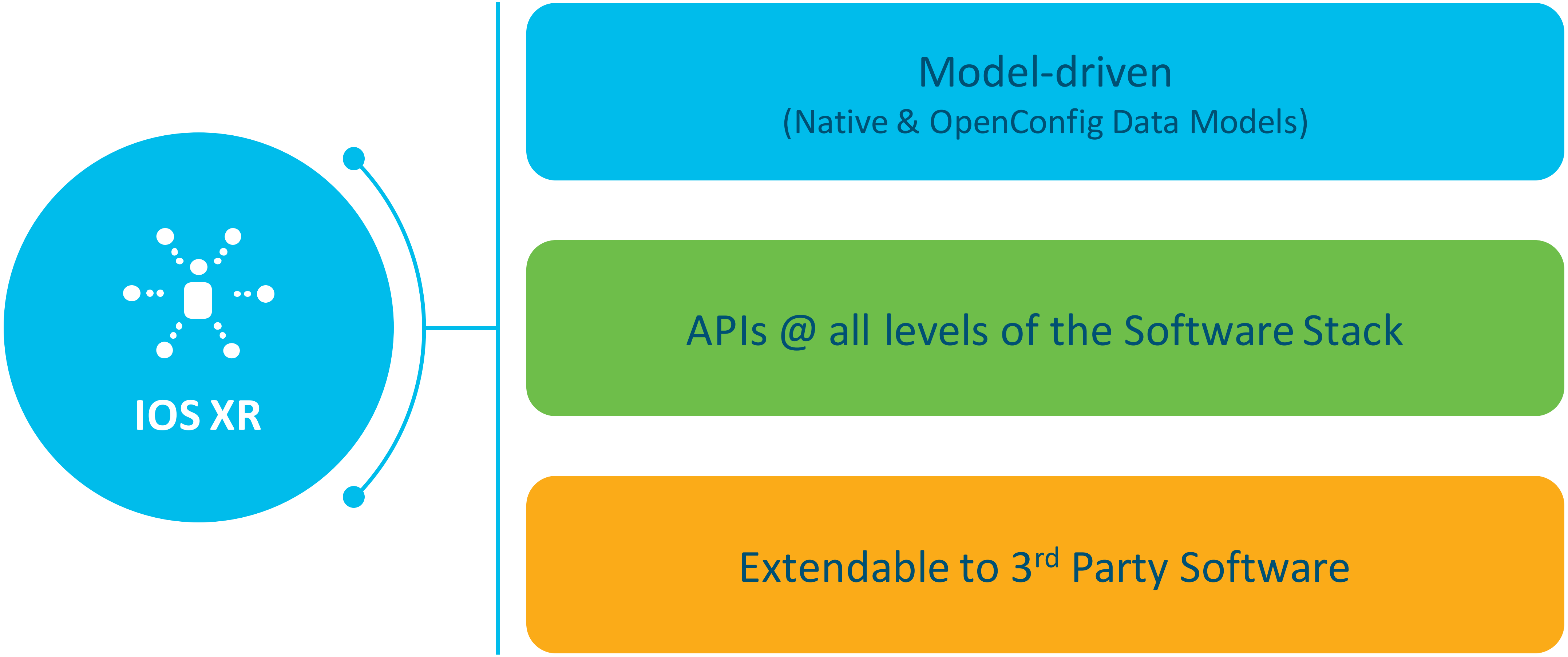
Agenda

1 Market and Evolution

2 Trustworthy Platforms & XR Security
for 5G Converged SDN Transport

3 XR Programmability
for 5G Converged SDN Transport

Advanced Device Programmability for 5G Era



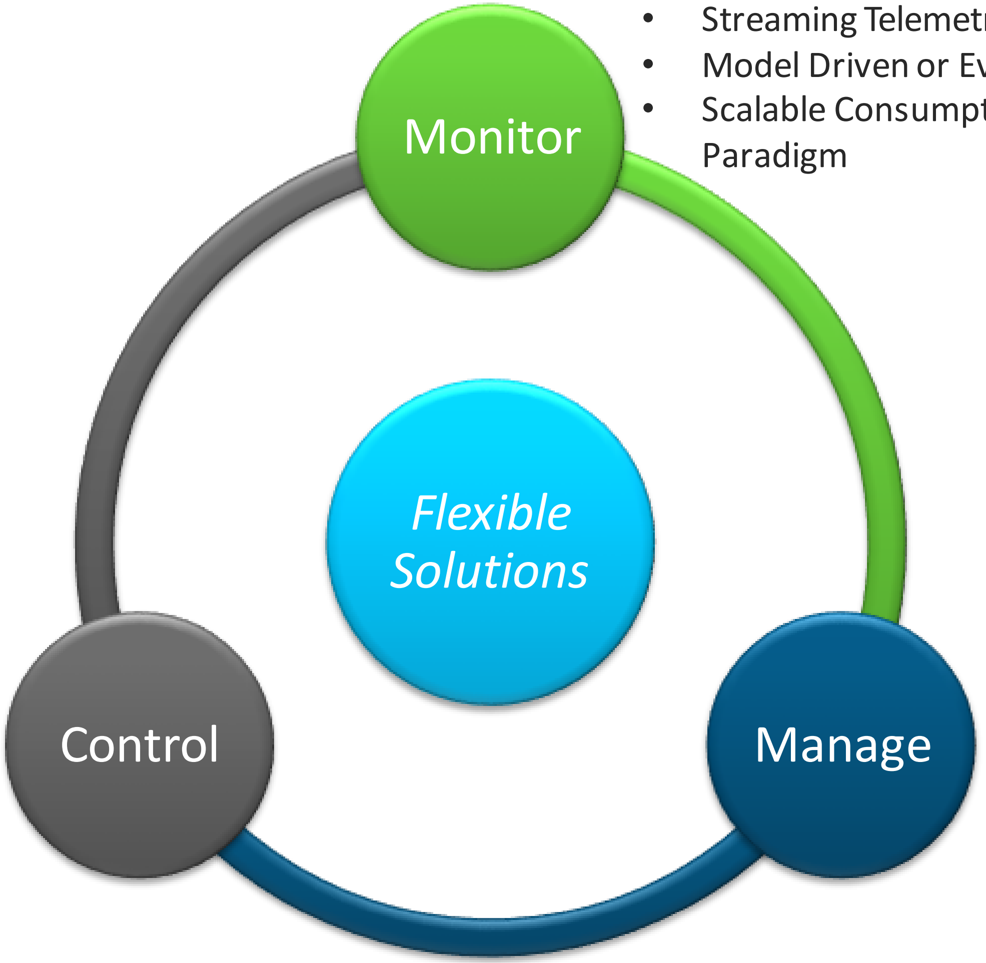
IOS XR

Model-driven
(Native & OpenConfig Data Models)

APIs @ all levels of the Software Stack

Extendable to 3rd Party Software

IOS XR Programmability – Key Components



Monitor

- Streaming Telemetry
- Model Driven or Event Driven
- Scalable Consumption driven Paradigm

Flexible Solutions

Control

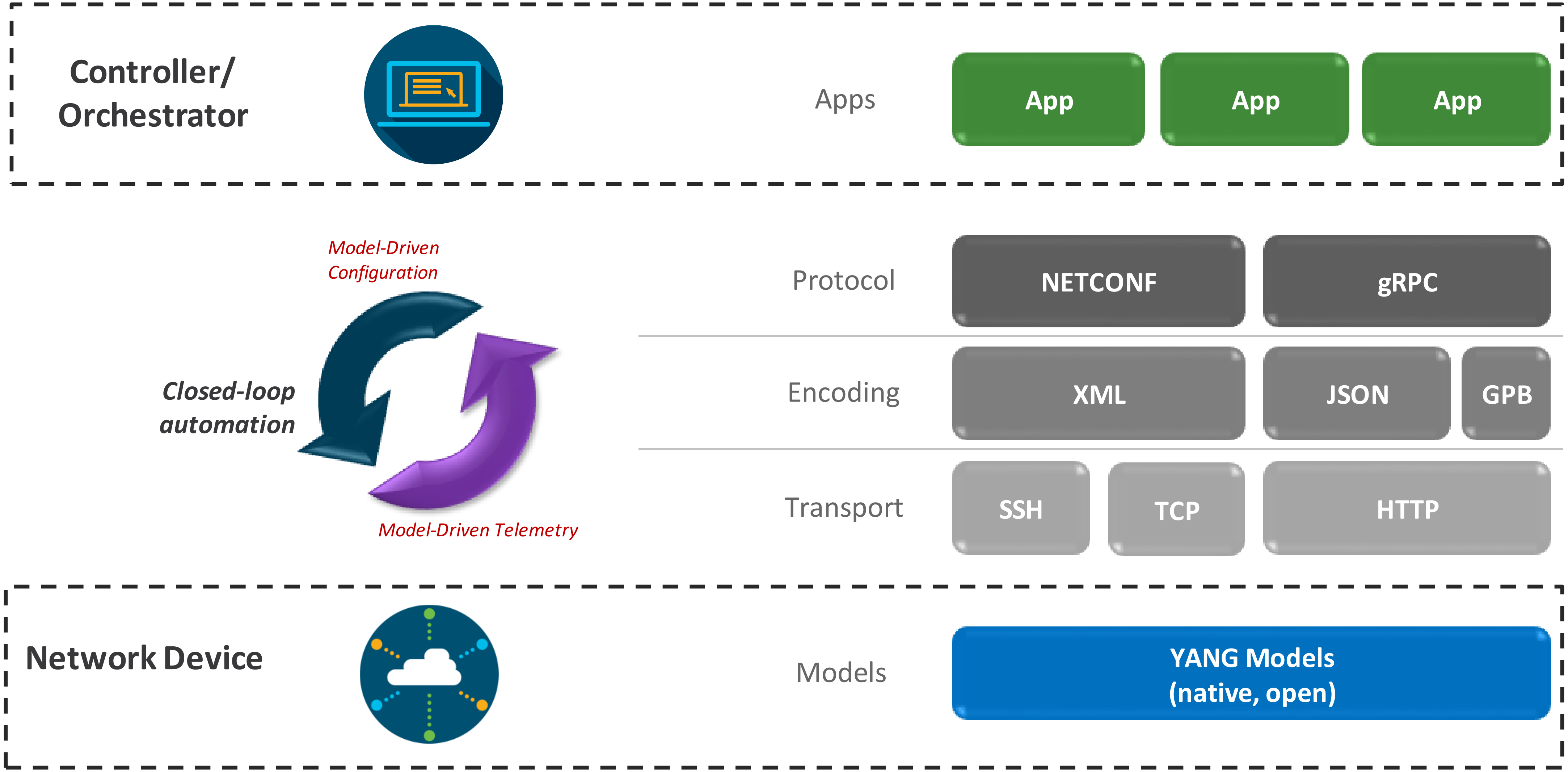
- Route/Forwarding level Control functions
- RIB/FIB Level (SL-API) & Protocol Level (PCEP, BGP FS)

Manage

- Device & Network level Configuration
- Scope
  - Day 0 (ZTP)
  - Day 1 (Operate)
  - Day 2 (Service)

Flexible Solutions = Cisco Internal (CrossWork, NSO) or External (HomeGrown or 3rd Party)

IOS XR Programmability – A Primer



Controller/ Orchestrator

Model-Driven Configuration

Closed-loop automation

Model-Driven Telemetry

Network Device

Apps	**App**	**App**	**App**	
Protocol	**NETCONF**		**gRPC**	
Encoding	**XML**		**JSON**	**GPB**
Transport	**SSH**	**TCP**	**HTTP**	
Models	**YANG Models (native, open)**			

IOS XR Models – Styles

Manage

Native Models

OpenConfig Models

Comes integrated in IOS XR today (~1100 Native and ~100 OC models – XR 7.3.1)

Note: There is no "one standard" – In programmability it does NOT matter – APIs matter

https://github.com/YangModels/yang/tree/master/vendor/cisco/xr

Manage

IOS-XR Configuration Model Examples

		Deploy	Deploy	EC
7.0.1	**7.1.1**	**7.2.1**	**7.3.1**	**7.4.1/7.5.1**
Interfaces Bundles ARP LACP VRF Static routing RIB MPLS (LDP, LSD, L3VPN) Telemetry NETCONF gRPC SNMP	BGP ISIS OSPF (v2/v3) MPLS (TE) RSVP	QoS ACL (IPv4, IPv6, Ethernet, prefix list, object group) Multicast (AMT, IGMP, MLD, MSDP, PIM)	Around 40 new models under testing	Over 200 models under development

- XR or platform specific
- Full coverage of device functionality
- Single abstraction for YANG and CLI

- Full parity and deterministic coverage
- Same help/doc strings
- Expected to be current

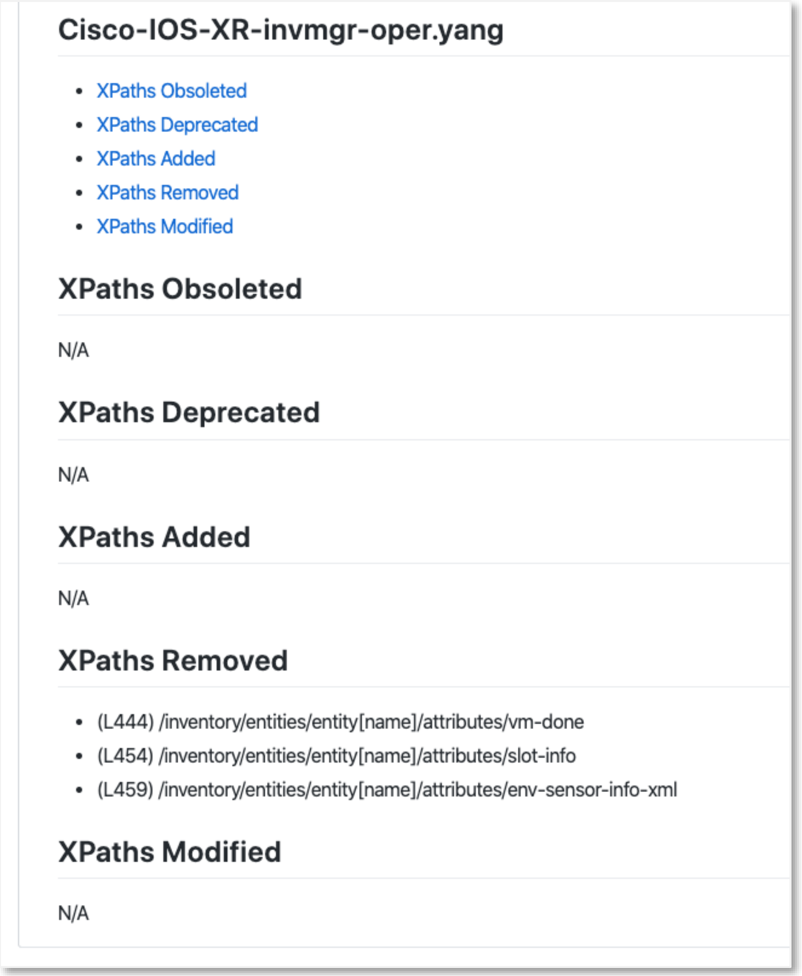
IOS XR Yang Model Documentation

Deploy

XR 7.0.2 / 7.1.1

Manage

- Backwards incompatible changes are documented on GitHub
  - https://github.com/YangModels/yang/tree/master/vendor/cisco/xr/731/BIC
  - Definitions based on RFC6020, Section 10
- Format
  - HTML
  - JSON (available)
- Full list of Models available in per XR release
  - https://github.com/YangModels/yang/blob/master/vendor/cisco/xr/731/Available-Content.md



Cisco-IOS-XR-invmgr-oper.yang

- XPaths Obsoleted
- XPaths Deprecated
- XPaths Added
- XPaths Removed
- XPaths Modified

XPaths Obsoleted

N/A

XPaths Deprecated

N/A

XPaths Added

N/A

XPaths Removed

- (L444) /inventory/entities/entity[name]/attributes/vm-done
- (L454) /inventory/entities/entity[name]/attributes/slot-info
- (L459) /inventory/entities/entity[name]/attributes/env-sensor-info-xml

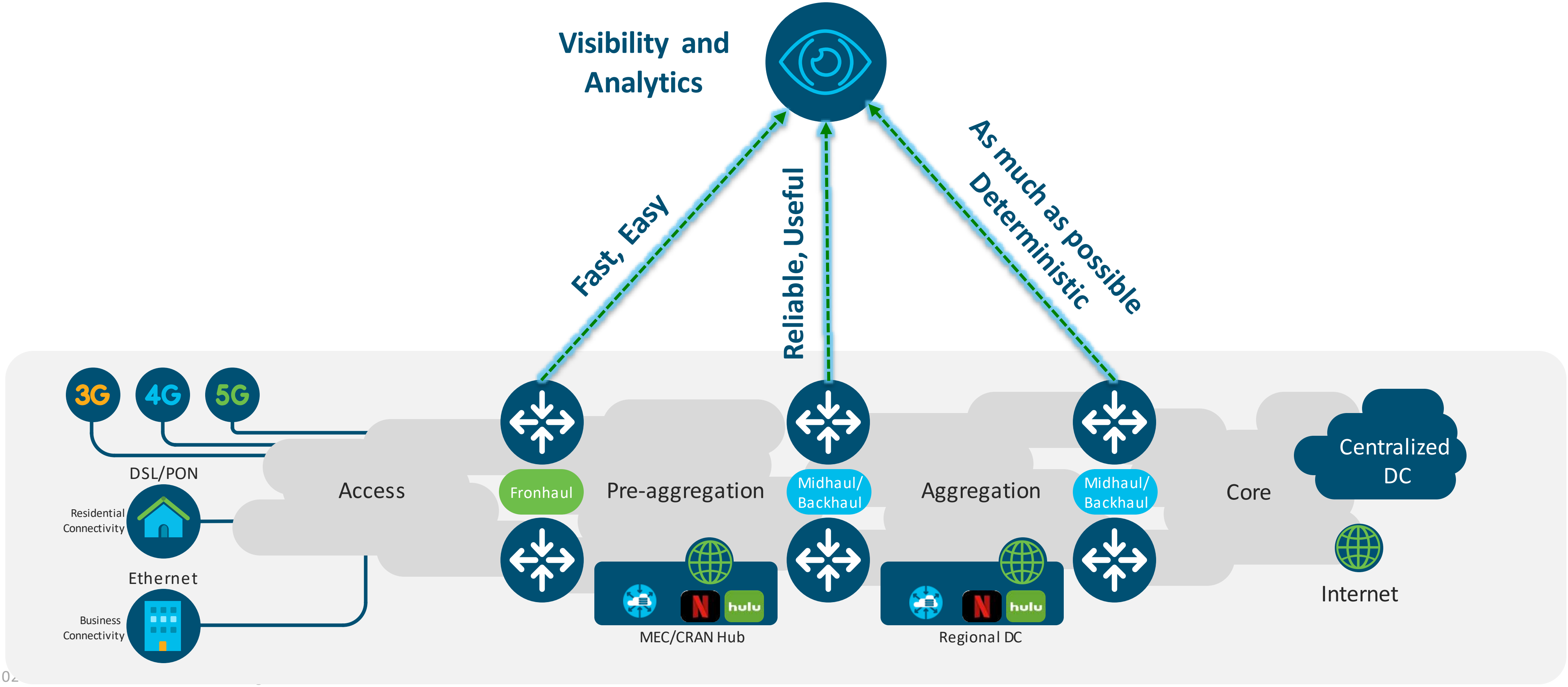
XPaths Modified

N/A

Model-driven Telemetry

Monitor

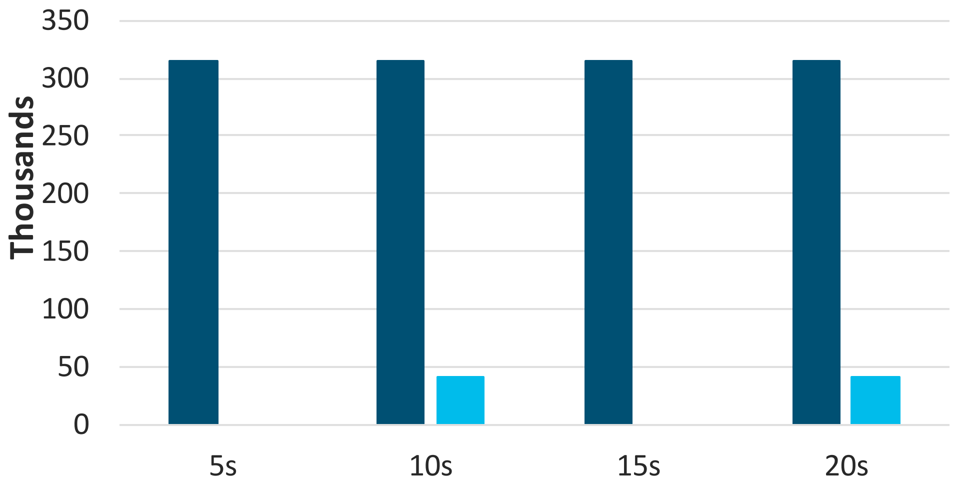
Three key changes: Push, not pull. Based on Data Models. Ready for analytics



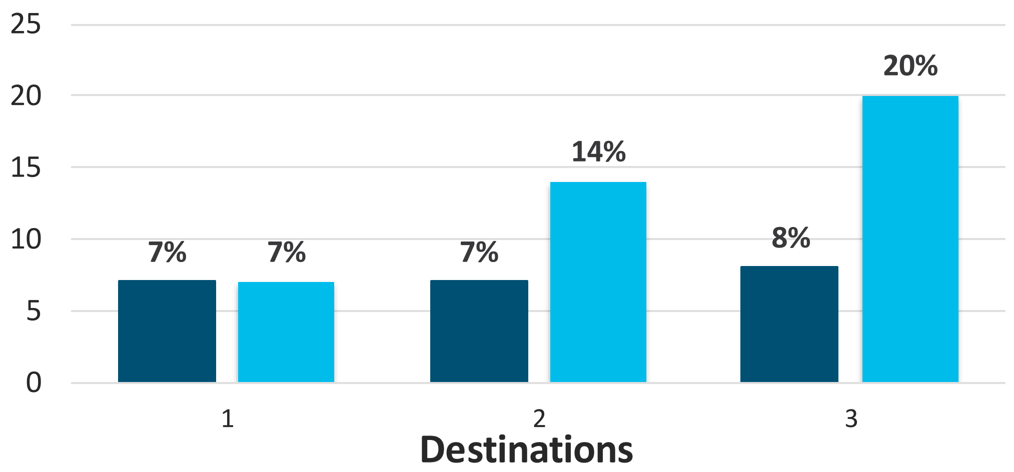
Telemetry vis-à-vis SNMP – “No Contest”

Monitor

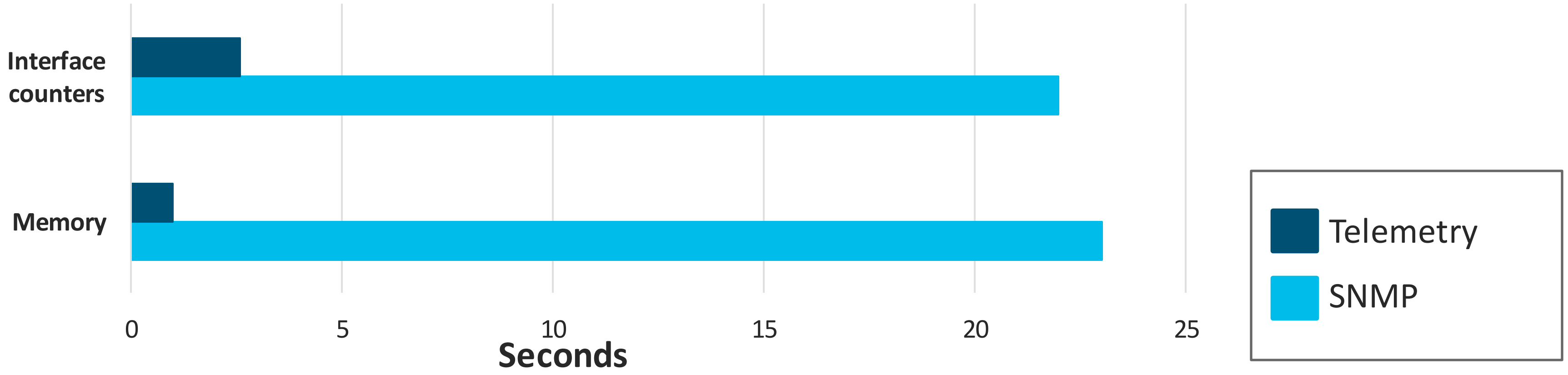
Counters



CPU load



Time to collect all data
(chassis, 576x100GE)



- ✓ **More counter data**
- ✓ **Reduction in CPU load**
- ✓ **Faster collection**

Deploy

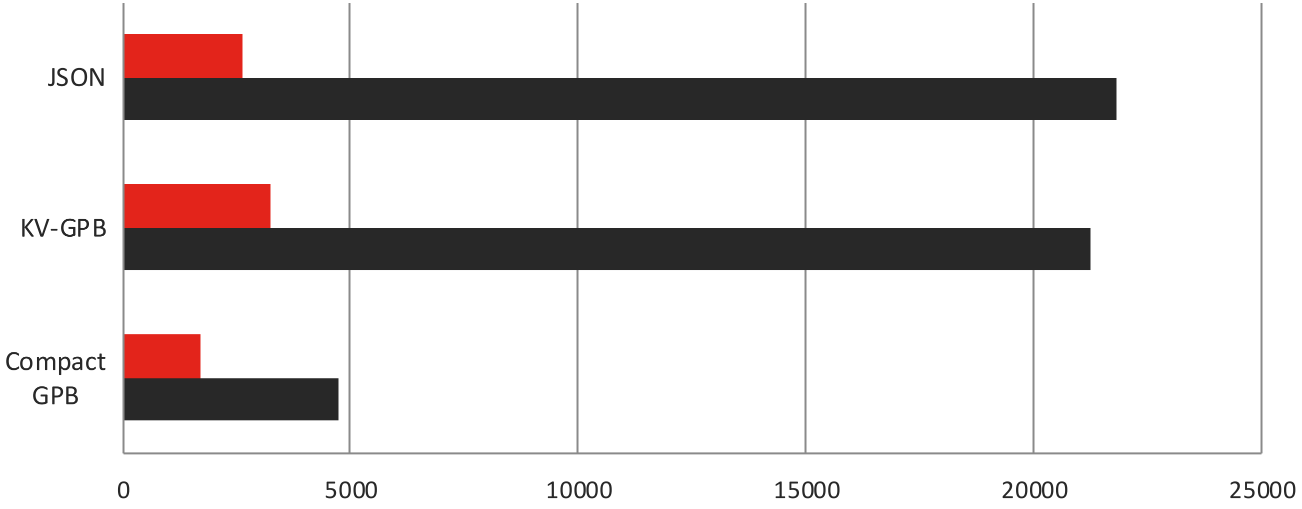
gRPC compression

XR 7.1.2 / 7.2.1

Monitor

- Support for compression has been added to XR gRPC implementation
- No configuration required for gNMI clients
  - Clients use CallOption “UseCompressor”
- New configuration under *protocol grpc per destination* ***(dialout)***

```
telemetry model-driven
 destination-group notls
  address-family ipv4 192.168.122.1 port 9902
   encoding self-describing-gpb
   protocol grpc no-tls gzip
  !
 !
!
```



Leaf-level filtering

Deploy

XR 7.2.1

Monitor

- Current subscriptions are internally mapped to the corresponding container (gather path)
- New feature to allow subscription at individual leaf level
  - Multiple leaves can be specified in a single subscription
  - Optimized to avoid duplicate internal collections

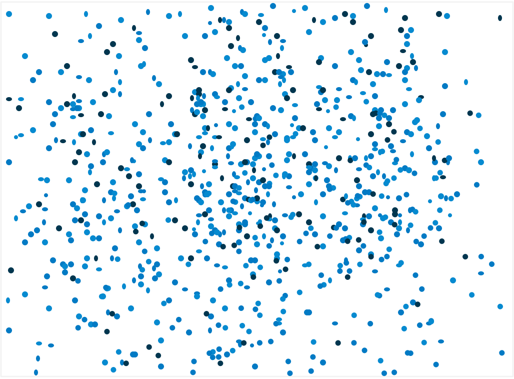
AI Driven Telemetry (ADT)

Deploy

XR 7.3.1

Monitor

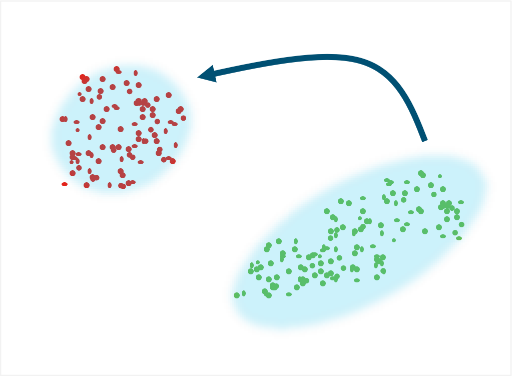
Collect



Holistic view:

Collect all counters all the time.
Currently: MDT data, Netflow/CRFT (future)

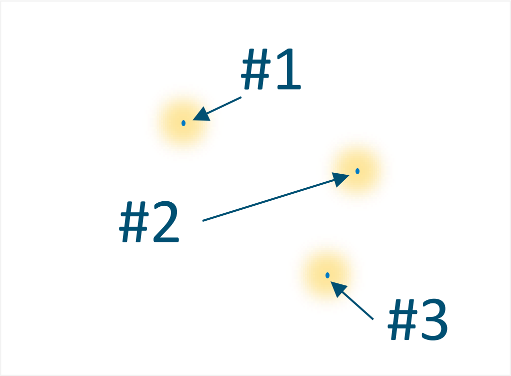
Detect



Macroscopic view:

Catch interesting state changes.
Dim.-Redux, Cluster.
Online, unsupervised.

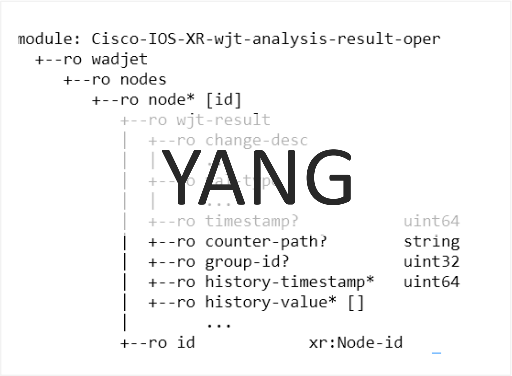
Select



Microscopic view:

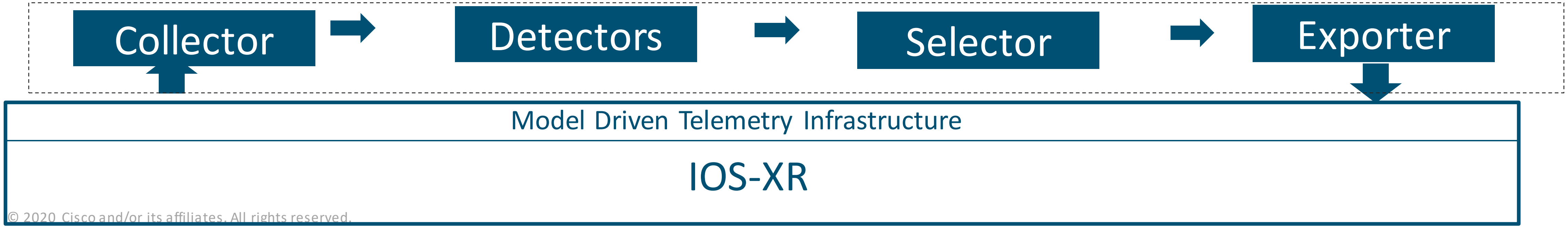
Choose counters which best describe the state change.
Online, unsupervised.

Export



```
module: Cisco-IOS-XR-wjt-analysis-result-oper
  +--ro wadjet
     +--ro nodes
        +--ro node* [id]
           +--ro wjt-result
           |  +--ro change-desc
           |  |     ...
           |  +--ro val-type
           |  |     ...
           |  +--ro timestamp?           uint64
           |  +--ro counter-path?        string
           |  +--ro group-id?            uint32
           |  +--ro history-timestamp*   uint64
           |  +--ro history-value* []
           |        ...
           +--ro id                   xr:Node-id
```

Present results using existing YANG tool-chain:
Counter values, Sensor-paths



Collector → Detectors → Selector → Exporter

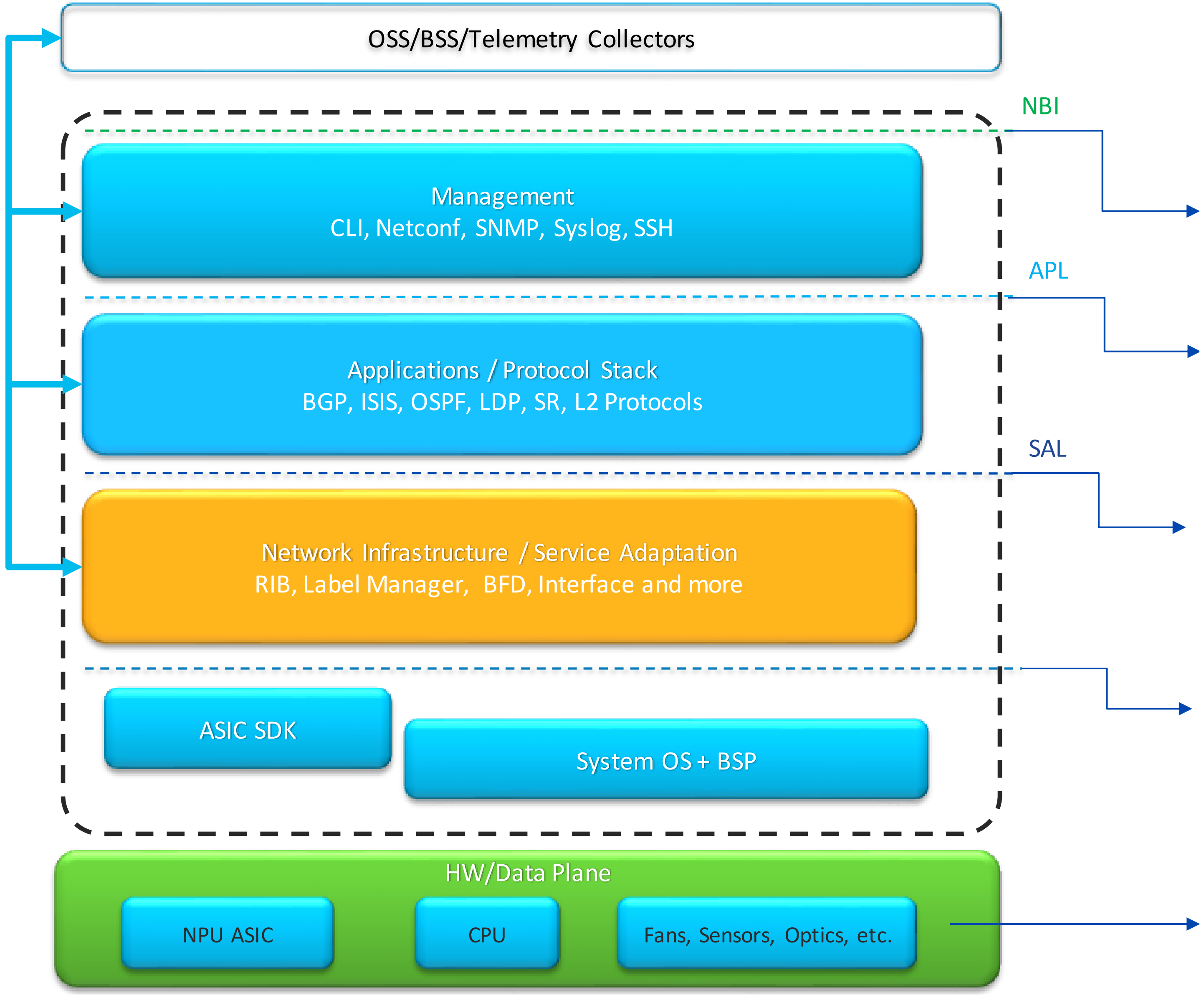
Model Driven Telemetry Infrastructure

IOS-XR

Cisco IOS-XR Router (e.g. Cisco 8000, NCS55xx, ...)

API Layers in IOS XR -> “Control” with SL-API

Control


OSS/BSS/Telemetry Collectors
NBI
Management
CLI, Netconf, SNMP, Syslog, SSH
APL
Applications / Protocol Stack
BGP, ISIS, OSPF, LDP, SR, L2 Protocols
SAL
Network Infrastructure / Service Adaptation
RIB, Label Manager, BFD, Interface and more
ASIC SDK
System OS + BSP
HW/Data Plane
NPU ASIC
CPU
Fans, Sensors, Optics, etc.

Management/Presentation Layer – Yang Models, CLI

- Leverages an extensive set of YANG (native, OC) data models to enable programmatic configuration

Application/Protocol Layer – Routing APIs (BGP FS, PCEP)

- Offers direct programmatic access to the protocol applications – BGP, IGP, etc.

Network Infrastructure Layer / Service Adaptation Layer – SL API

- Offers a scalable and convenient integration point to build/extend devices’ control plane functionality

System OS (Linux), BSP(Board Support Package) & ASIC SDK

- Provides easier and rapid enablement of the software on new platforms and silicon, while ensuring performant forwarding operation

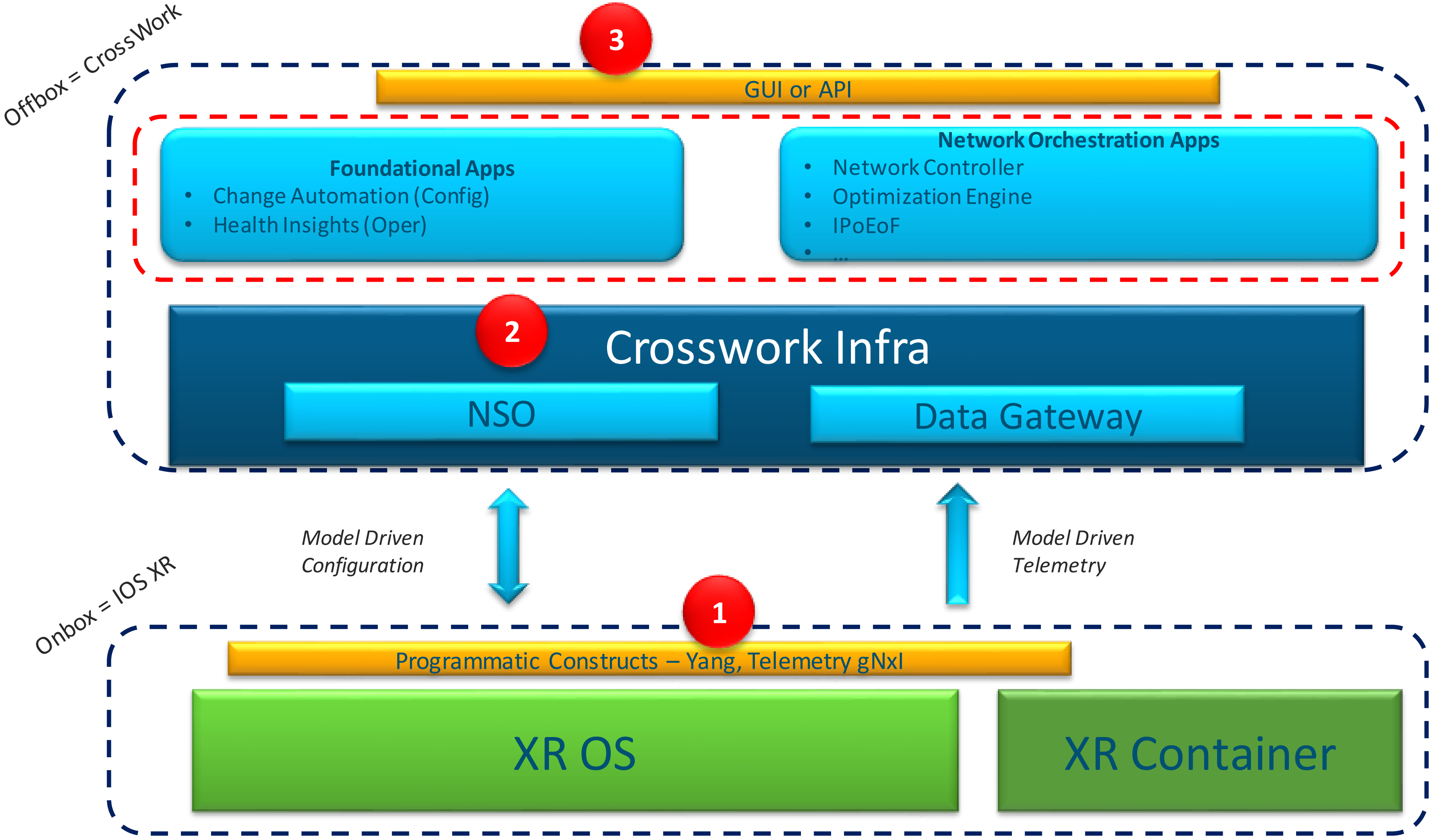
Hardware – ASIC/Chipset, CPU, Fans, Sensors

Examples of Using Service Level API (SL-API)

Control

Use Case	Github Code Location
Open/R running on IOS-XR as an IGP	https://github.com/akshshar/openr-xr
Programmable BGP Route Download	https://github.com/Cisco-Service-Layer/openbmp-controller
Egress Traffic Controller Telemetry based route selection	https://github.com/Maikor/nanog71-hackathon
IPv6 neighbor based path failover (Telemetry+SL-API)	https://github.com/akshshar/xrtelemetry-slapi
Interface Events based path failover (SL-API + YDK)	https://github.com/akshshar/ydk-slapi-remediation

Cisco SP – Full Stack Software Offerings



- Rich Application Ecosystem
- Consume (or extend) via GUI or API
- App Ecosystem leverage APIs internally
- Built for Cloud scale with Microservices architecture

- 'Onbox' Software within Router – the Base Layer
- Fully Open Yang Models – Extend for Provider Software
- Container provides pre-processing capabilities for Crosswork

x *Potential Integration Points*

Summary

Key Take-aways

- Platform security is key to complement 5G transport security
- Trust starts in development stage for HW and SW and is anchored in HW
- Operational Simplification in XR delivered via Data Models
- XR Programmability Infrastructure Hardening
- Wide range of deployment styles envisioned – DIY, Full Stack & Hybrid

Resources

- **Cisco 5G Transport –** www.cisco.com/go/5g-transport

- **White Paper : Trustworthy Converged Mobile xHaul Networks –** https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/mobile-internet/white-paper-sp-trustworthy-converged-mobile-xhaul-networks.pdf

- **White Paper : 5G Security Innovation with Cisco** https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf

- **White Paper : Cisco Converged 5G xHaul Transport–** https://www.cisco.com/c/en/us/solutions/service-provider/mobile-internet/5g-transport/converged-5g-xhaul-transport.html

- **Cisco Trustworthy Technologies -** https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html