
cisco
You make possible

Unprecedented Visibility and Forensics

Analyze system integrity and trustworthiness of network devices

Deepak Bhargava, Product Manager @deebhargava
Dan Backman, Portfolio Architect @jonahsfo

BRKSPG-1415

Barcelona | January 27–31, 2020

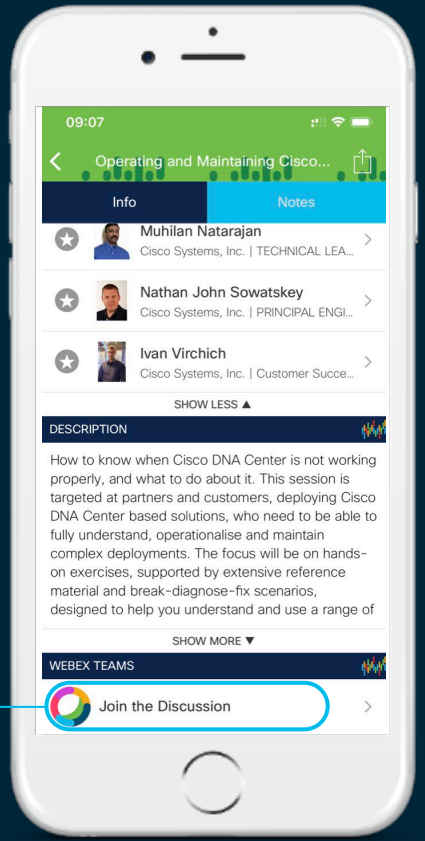
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



“Network devices are ideal targets. Most or all organizational and customer traffic must traverse these critical devices.”

Source: US-CERT Alert (TA18-106A)

Original release date: April 16, 2018

“The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations.”

Source: US-CERT Alert (TA16-250A)

Original release date: Sep 6, 2016

You need the ability to analyze the Trustworthiness of your network devices

Agenda

- Risks to the Network Infrastructure
- What is Trust and Why does it matter?
- Measuring and Validating Trust in Cisco IOS-XR routers
- Trust Visualization and Attestation requires a Service
- Demonstration
- Implementing closed-loop automation
- Conclusion

Growing Concerns for Service Providers

Targeted attacks on Critical Infrastructure

Impact on Economy

Untrusted Locations

Complex to Manage

Service Provider Security Concerns

Denial of Service

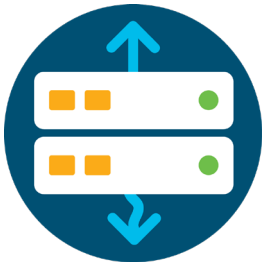
MitM attacks

Cloud Security

IoT Security

Ransomware

Credential/Service Theft



Third Party Security

Malware and Botnets

Known Vulnerabilities

Segmentation Issues

Tough Questions for Critical Infrastructure

If hardware or software running my critical systems was modified, how would I know?

How can I track what hardware and software has changed?

How would I prove where & when critical security updates are applied and are active?

How do I know that the running software is built by Cisco?

In an audit, how can I prove my systems are running compliant hardware and software?

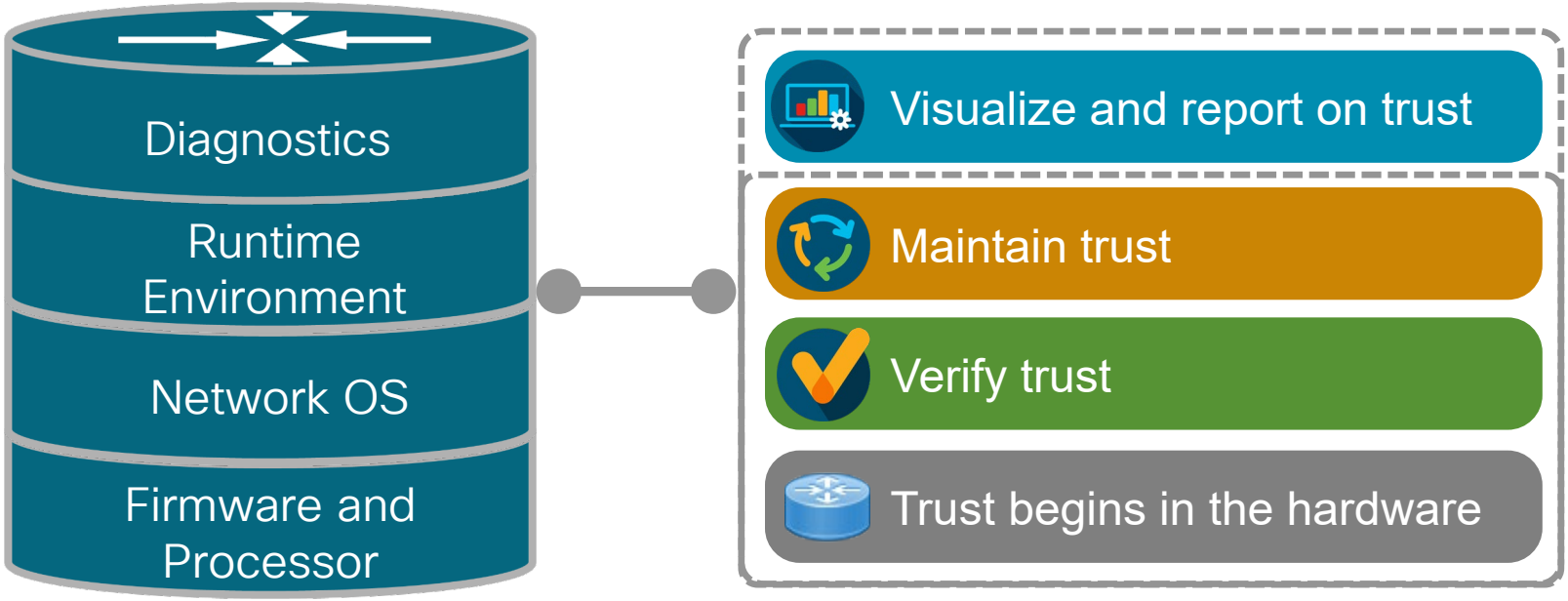
How do I prove what HW & SW was running in the past?

What is Trustworthy and Why Does It Matter?

To build a trustworthy platform

The network infrastructure must be constructed on a platform of trustworthy technologies to ensure devices operating are authentic and can create verifiable evidence that they have not been altered.

Trustworthy Platform: Mandatory for Operators



Would you trust a device to tell you that it's trusted?

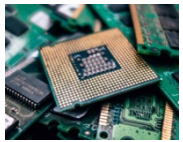
Measuring and Validating Trust

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

Cisco Trust Anchor Module (TAm)

Anti-Theft and Anti-Tamper Chip Design

Built-In Crypto Functions

Hardware Entropy

Secure Storage

- Hardware designed to provide both End-user and supply chain protections
  - End-user protections include highly secure storage of user credentials, passwords, settings.
  - Supply chain protections -- Cisco SUDI (secure unique device identifier) inserted during manufacturing
- Secured at Manufacturing. No user intervention required
- Ideal for embedded computing like routers and Wi-Fi access points

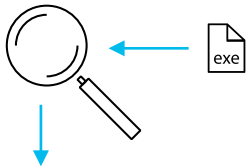
Unique hardware Identity (SUDI)

"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

Process Fingerprinting and Signatures (IMA)

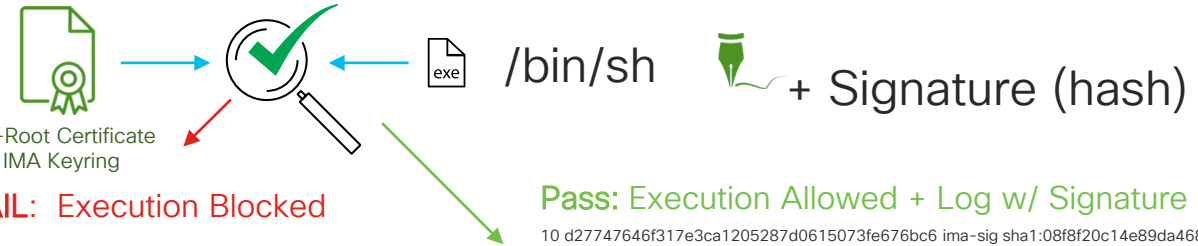
Logging
(Process Fingerprint)



10 7103f91ed91be355abeef84853301e11dccd9e4a ima-sig
sha256:0b46fb8e7635a02320aceed326128b0f146c369476dfe5fd704aceca4a135b88 /bin/sh

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

Appraisal
(Signature Validation)



FAIL: Execution Blocked

Pass: Execution Allowed + Log w/ Signature

10 d27747646f317e3ca1205287d0615073fe676bc6 ima-sig sha1:08f8f20c14e89da468bb238
d2012c9458ae67f6a /bin/sh 030202afab451100802b22e3ed9f6a70fb5babf030d1181
8152b493bd6bfd916005fad7fdcfd7f88d43f6cffaf6fd1ea3b75032dd702b661d4717729e4a3fa4
ee95a47f239955491fc8064eca8cb96302d305d59750ae4ffde0a5f615f910475eee72ae0306e4ae
0269d7d04af2a485898eec3286795d621e83b7dedc99f5019b7ee49b189f3ded0a2

Analyzing IMA

What can we do with this?
> Identify known-good signatures <

```
Read till seqno 38857
                                                                                Package  Knowns files  Found running  Missmatch
0                xrv9k-sysadmin-xrv9k-7.0.1.118I-r701118I.x86_64_signed.rpm          160            64           0
1                           xrv9k-bgp-2.0.0.0-r701118I.x86_64_signed.rpm          171           105           0
2                 xrv9k-sysadmin-mgbl-7.0.1.118I-r701118I.x86_64_signed.rpm          161           100           0
3   xrv9k-sysadmin-hostos-7.0.1.118I-r701118I.admin.x86_64_signed.rpm            0             0           0
4                         xrv9k-iosxr-os-5.0.0.0-r701118I.x86_64_signed.rpm          994           573           0
5                   xrv9k-iosxr-routing-4.0.0.0-r701118I.x86_64_signed.rpm          244           112           0
6                           xrv9k-base-2.0.0.0-r701118I.x86_64_signed.rpm          172           114           2
7                     xrv9k-spirit-boot-2.0.0.0-r701118I.x86_64_signed.rpm           21            16           1
8                          xrv9k-parser-2.0.0.0-r701118I.x86_64_signed.rpm           61            32           0
9                      xrv9k-gcp-fwding-4.0.0.0-r701118I.x86_64_signed.rpm          200            94           0
10                  xrv9k-common-pd-fib-2.0.0.0-r701118I.x86_64_signed.rpm           34            29           0
11   xrv9k-sysadmin-hostos-7.0.1.118I-r701118I.host.x86_64_signed.rpm          234            97           0
12                   xrv9k-iosxr-fwding-4.0.0.0-r701118I.x86_64_signed.rpm         2858          1440           0
13                    xrv9k-iosxr-infra-4.0.0.0-r701118I.x86_64_signed.rpm         3408          1669           0
14                                                                    base        22557           760          10
15          xrv9k-sysadmin-shared-7.0.1.118I-r701118I.x86_64_signed.rpm          647           231           1
16                     xrv9k-os-support-3.0.0.0-r701118I.x86_64_signed.rpm           79            53           0
17          xrv9k-sysadmin-system-7.0.1.118I-r701118I.x86_64_signed.rpm          596           208           1
18            xrv9k-sysadmin-topo-7.0.1.118I-r701118I.x86_64_signed.rpm           46            21           0
19                          xrv9k-fwding-2.0.0.0-r701118I.x86_64_signed.rpm          297           214           0
-------
```

What can we meaningfully learn from this?

... This is a very useful whitelisting engine for RUNTIME measurements

... know FOR SURE what has been running, match to known-good

... can also be used to track known 3rd party code

... can be used to track execution of code (hashes) with known vulnerabilities

What would you do with this?

Verifiable evidence is the foundation for Trust Attestation

Why Evidence matters?

- It's a cryptographically verifiable view into what was running in the past
  - You want this to troubleshoot things
  - You want this to know WHAT CHANGED
  - You want this to be a SIGNED and SECURE audit trail
  - You want to be able to report on this flexibly
  - You want a standard way to gather this type of data

What is Evidence?

- Basic Inventory Information
  - Hardware and Software Inventory
  - Running and/or Persistent Configuration
- Boot-Time Integrity Measurements
  - Hardware BIV attestation with PCRs (Boot Integrity)
  - Traditional TPM-style PCR values
  - New forms of hardware measurements
- Run-time Integrity Measurements
  - Kernel IMA Values
- Operational Reports
  - Any “show” command
  - Ex: Reboot history, etc

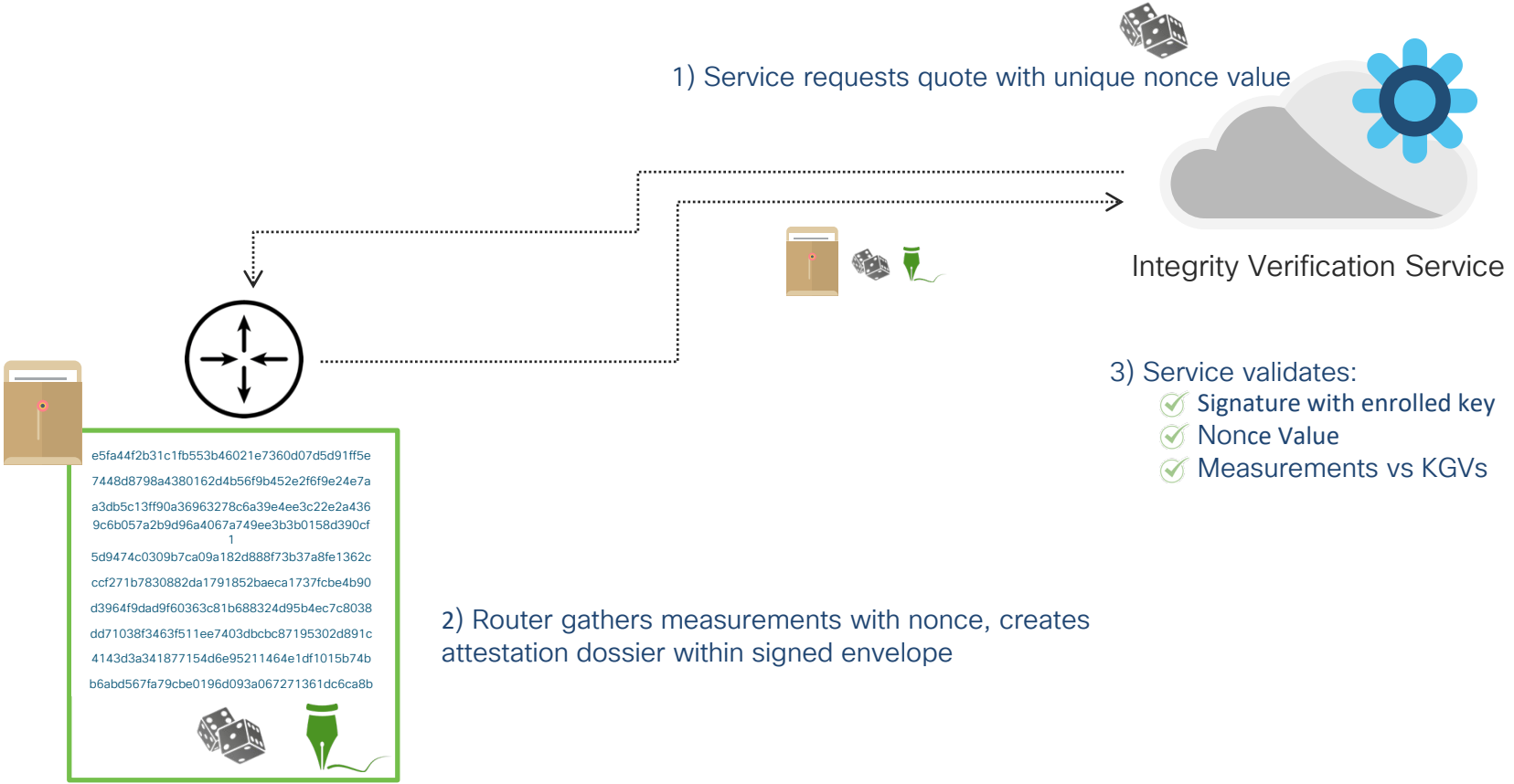
Operational Value of Trust Evidence

- Inventory:
  - Track hardware and software history and changes
  - Query hardware SUDI to validate PID / Serial number / Authenticity
- Reporting on runtime IMA measurements
  - Track running SW vs installed SW
  - Track 3rd party code
  - Track code with known vulnerabilities
  - Which version of a binary is running where
  - Software inventory based on observed running code
  - … a totally new view into your systems and operations

What would you do with Trust Evidence?

- Secure quote process
  - A more complete data model to include more extensive evidence gathering
  - Support for complex systems (modular platforms with many running OS kernels)
- Signature
  - Considerations for signing keys and device enrollment?
  - What key do you use to sign the data?
  - Key usage in modular systems
- Reporting on evidence timeline
  - Build extensible reporting for useful operational values
  - Dashboard (What changed since yesterday)
  - Device lifecycle and history

Secure Quote Process



Known-Good-Values

Where can you get known-good values?

- Source: Cisco
  - Extract hashes from known-good images/ISO
  - Published KGV from Cisco (HW and SW)
- Source: 3rd Party or user-provided code
  - Extract hashes from known-good packages
  - Signed KGV output from developers
  - Track known software installed onto IOS XR systems

Trust Visualization and Attestation requires a Service

The product, features and releases described are currently unavailable, remain in varying stages of development, and will be offered on a when-and-if-available basis.

The information provided is for informational purposes only and is subject to change at the sole discretion of Cisco.

Cisco will have no liability for delay in the delivery, or failure to deliver, any of the products or features described.

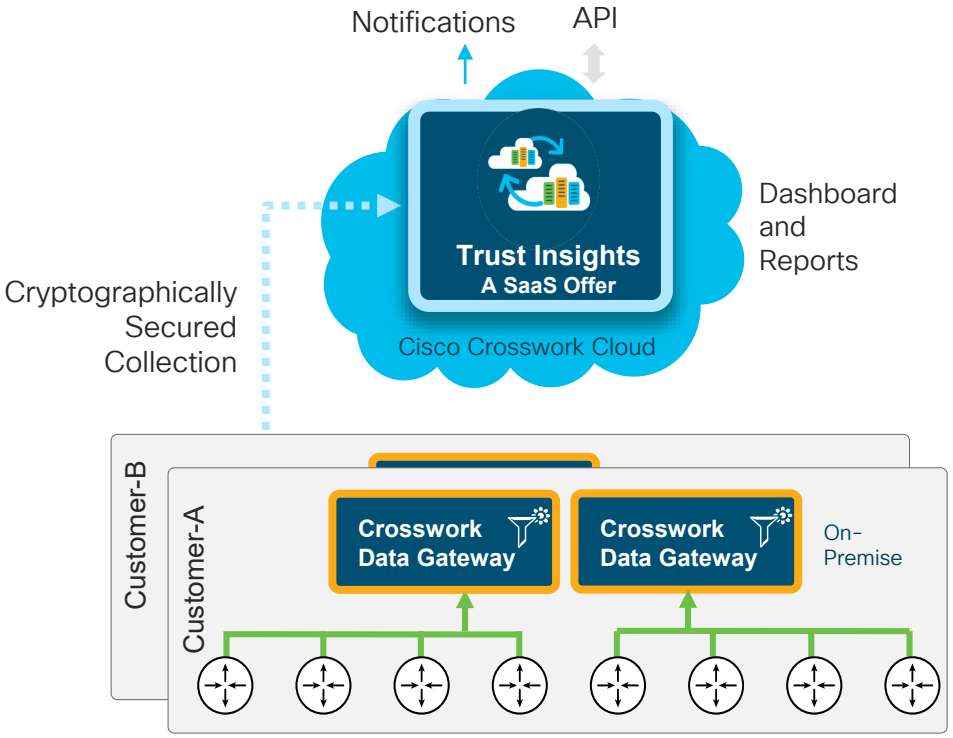
You need the ability to analyze the Trustworthiness of your network devices

Introducing Crosswork Trust Insights

- Visualize Trustworthiness
- Track & Verify Inventory
- Utilize Trusted Data for Automation

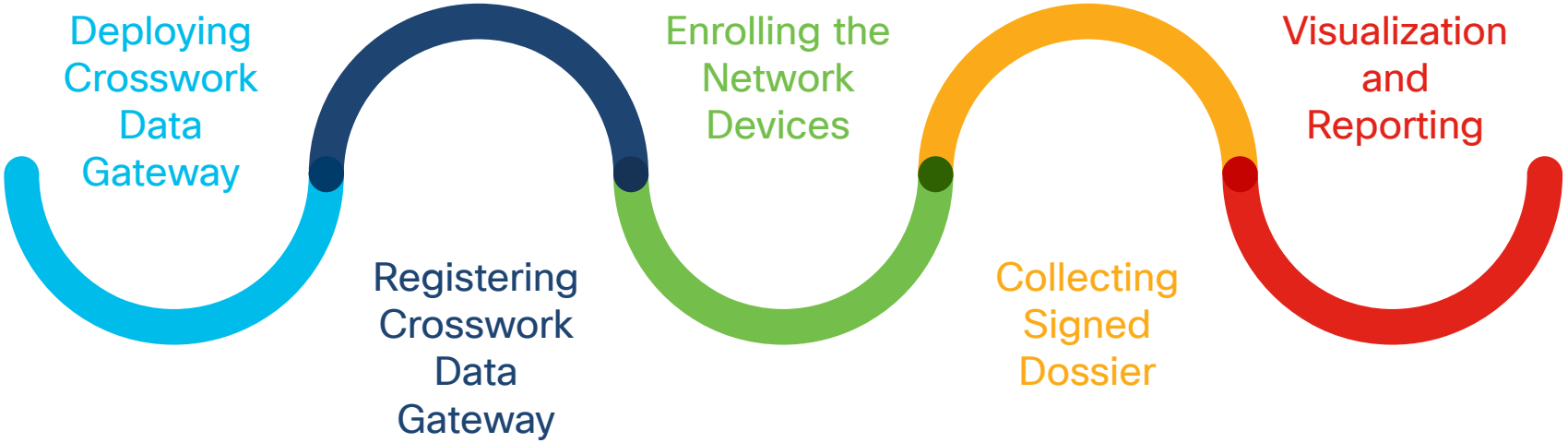
A Cloud-based SaaS offer that reports on the trustworthiness of network devices and provides forensics for assured inventory

Crosswork Trust Insights Components

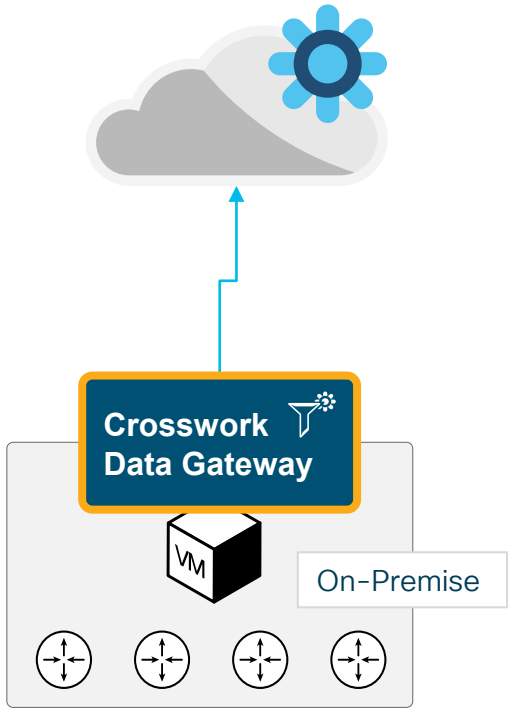


- On-Premises Data Gateway collects signed trust dossier from IOS XR Routers
- Dossier is human-readable
- Utilizes up-to-date feed of Known-Good-Values (KGV) from IOS XR Build and Regression
- Constantly evolving analytics of hardware and software fingerprints in Cloud Service

Journey to Unprecedented Visibility & Forensics

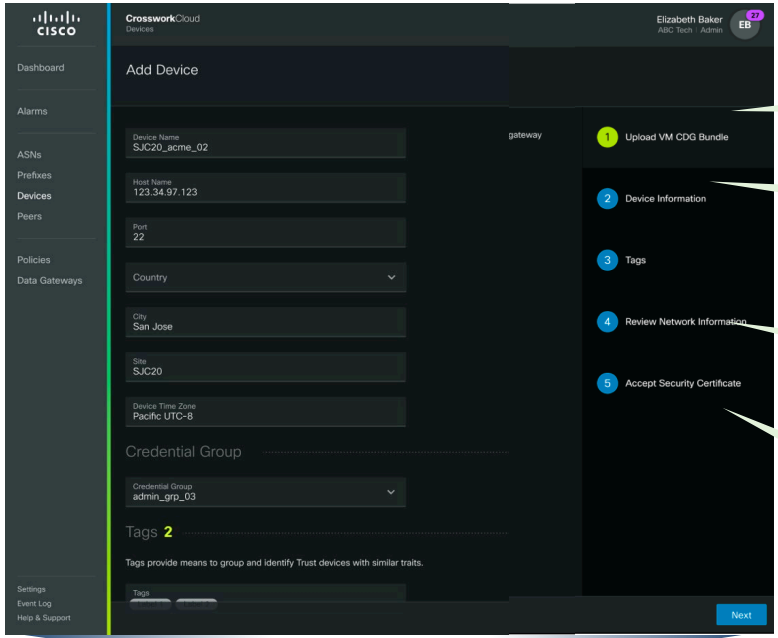


Deploying Crosswork Data Gateway



- Deployed as Base VM
  - Configure network settings
  - On-Premise with access to Crosswork.cisco.com
- Generates an Enrollment Package (JSON encoded) for registration, includes:
  - Name, Description
  - UUID
  - Certificate chain, etc.
- Export the enrollment package from CDG

Registering Crosswork Data Gateway



Crosswork Trust Insights

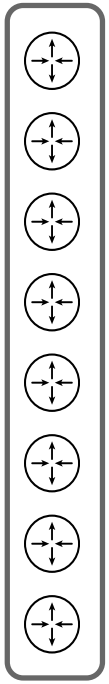
Upload the registration file with enrollment package

Verify the Data Gateway Information

Review the Network configuration

Review the Security Certificate and Accept the registration

Enrolling the Network Devices

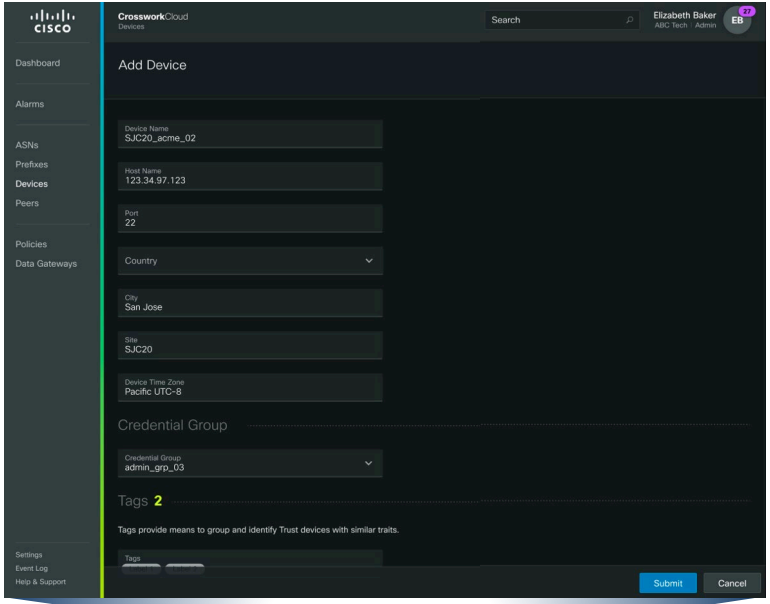


Routers

Create enrollment key with certificate chain in the router

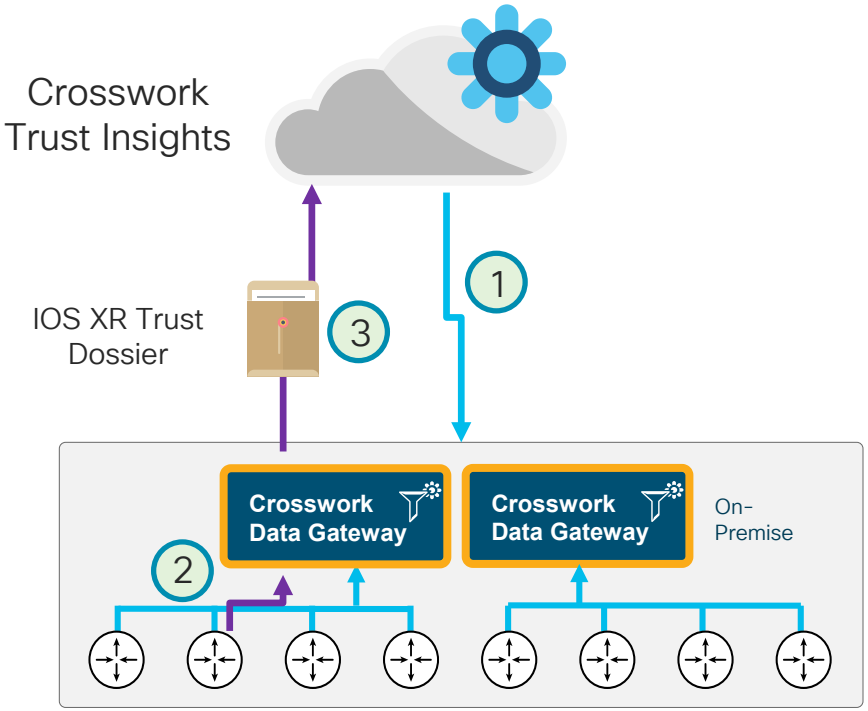
Provide device IP address, hostname, login credentials, certificate chain, tags and other descriptors

Enroll



Crosswork Trust Insights

Collection of Signed Dossier

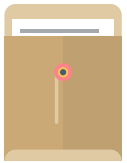


1. Cloud service assigns list of routers for collection to each Crosswork Data Gateway instance

2. Data Gateway logs into routers (SSH) and query Trust Dossier (CLI) per assigned schedule

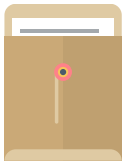
3. Crosswork Data Gateway forwards Trust Dossier to cloud service for verification and analytics

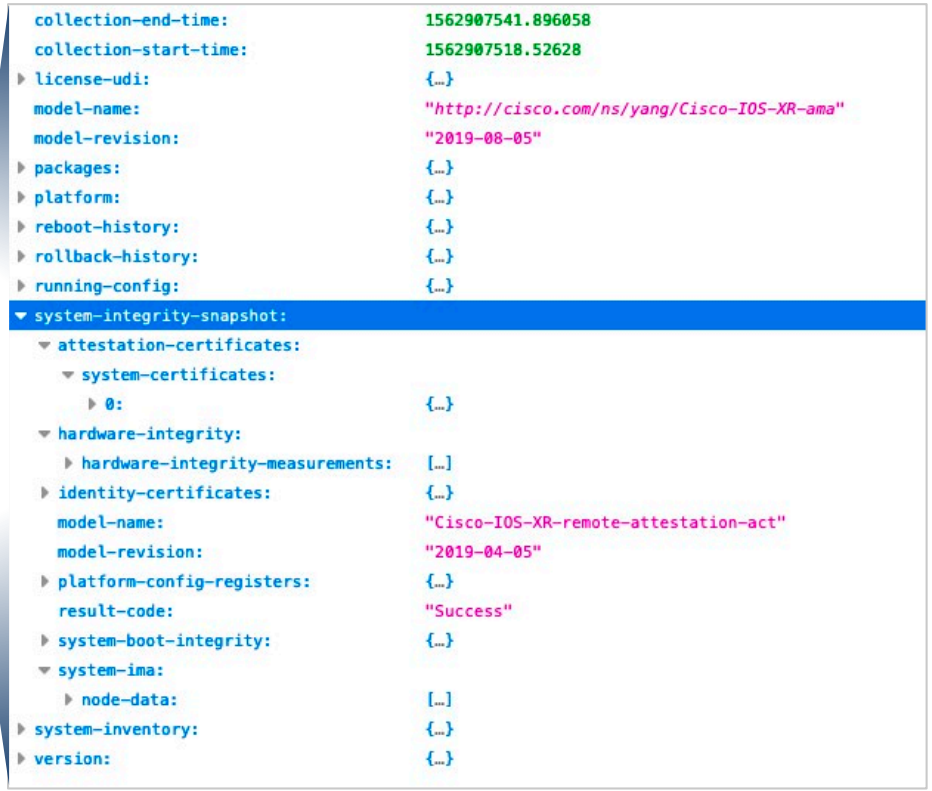
Cisco IOS XR Trust Dossier
Based on YANG models



Content Type	Data Model
IOS XR 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
Running Configuration (Optional)	*Crosswork Trust Insights does not gather config*

Cisco IOS XR Trust Dossier
Signed with Enrollment key (Not encrypted)

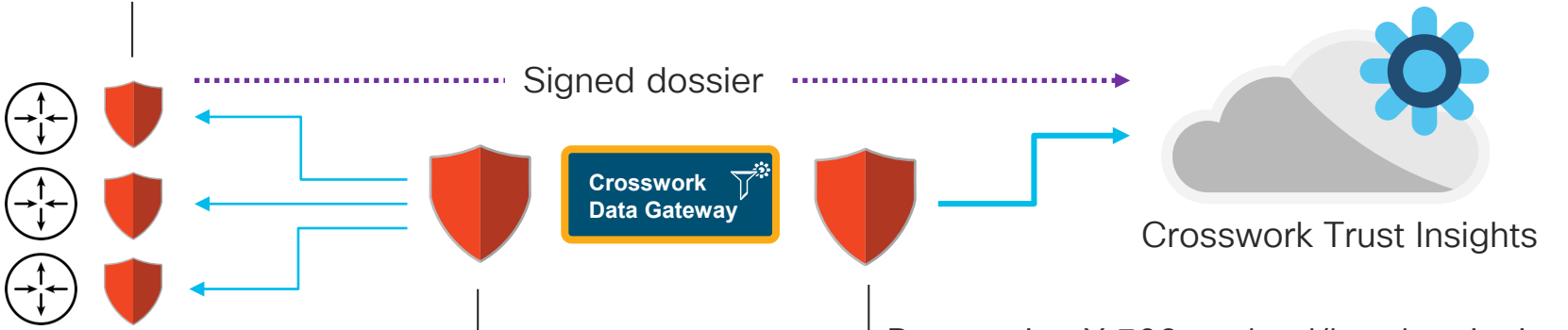




- Human-readable JSON encoding with signature envelope
- Supports nested signatures for hardware-signed values (ex: SUDI or BIV)

Secured Communication
Multiple Points of Security Control

IOS XR AAA Controls for Read-only login and CLI access

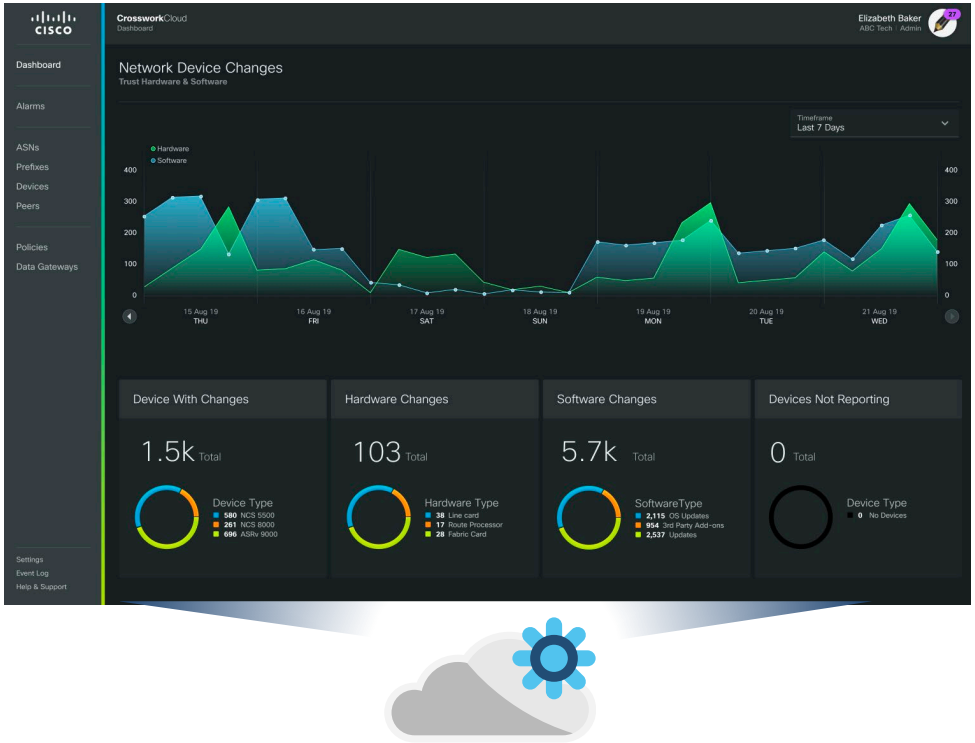


Per session X.509 payload/header signing using ED25519 public key mechanism

Limit to outbound SSH access to authorized systems

Control outbound access to HTTPS/TLS to Crosswork Cloud

Visualization and Reporting

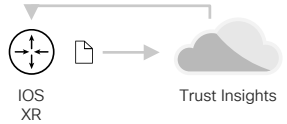


- Visualize trust and inventory data
- Analyze changes related to hardware and software integrity
- Maintain authoritative proof and evidence to support audits, compliance and forensic analysis
- Increased visibility illuminates security blind spots

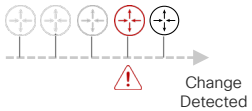
Why Trust Attestation must be a Cloud Service?

- Always-On, Automated KGV Feeds, Up-to-Date Analytics
- Vaulted Immutable Storage of Evidence
- Ease of Operational Integration
- Reduced Operational Cost and Seamless Scalability

Synopsis: How Trust Insights Works

1. 

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

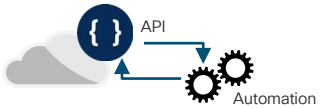
2. 

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

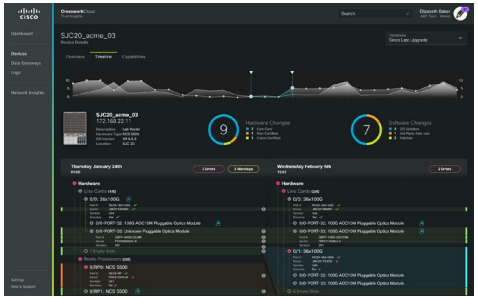
Demo-1: Trustworthiness Reporting

Use-case: Trustworthiness Reporting & Audit

Goal: Visualize 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

Demo-2: Run-time Integrity Analysis

Use-case: Software Update & Compliance

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

Demo-3: Tracking Inventory Changes

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

Implementing closed-loop automation with Cisco Crosswork

Applying Automation to Network Operations Lifecycle

Day -1

Phases

- Prepare
- Plan
- Integration
- Design

WAN Automation Engine

Planning and predictive modelling to analysis potential scenarios

Network Insights

Provides routing data analytics to significantly reduce mean time to repair

Integration Qualification Environment

Rapid qualification and integration to support new feature and software delivery into production

Trust Insights

“always on monitoring” to determine the integrity of infrastructure

Day 0

- Implement

Network Service Orchestrator

mass scale intent-based configuration across multi-vendor

Day 1

- Operate
- Optimize

Situation Manager

Connect events across multi domains and provide root cause analysis.

Health Insights

learn and measure health of network elements.

Change Automation

safely execute operational tasks with structured workflows.

Optimization Engine

optimize network paths to improve utilization & efficiency (SR-PCE)

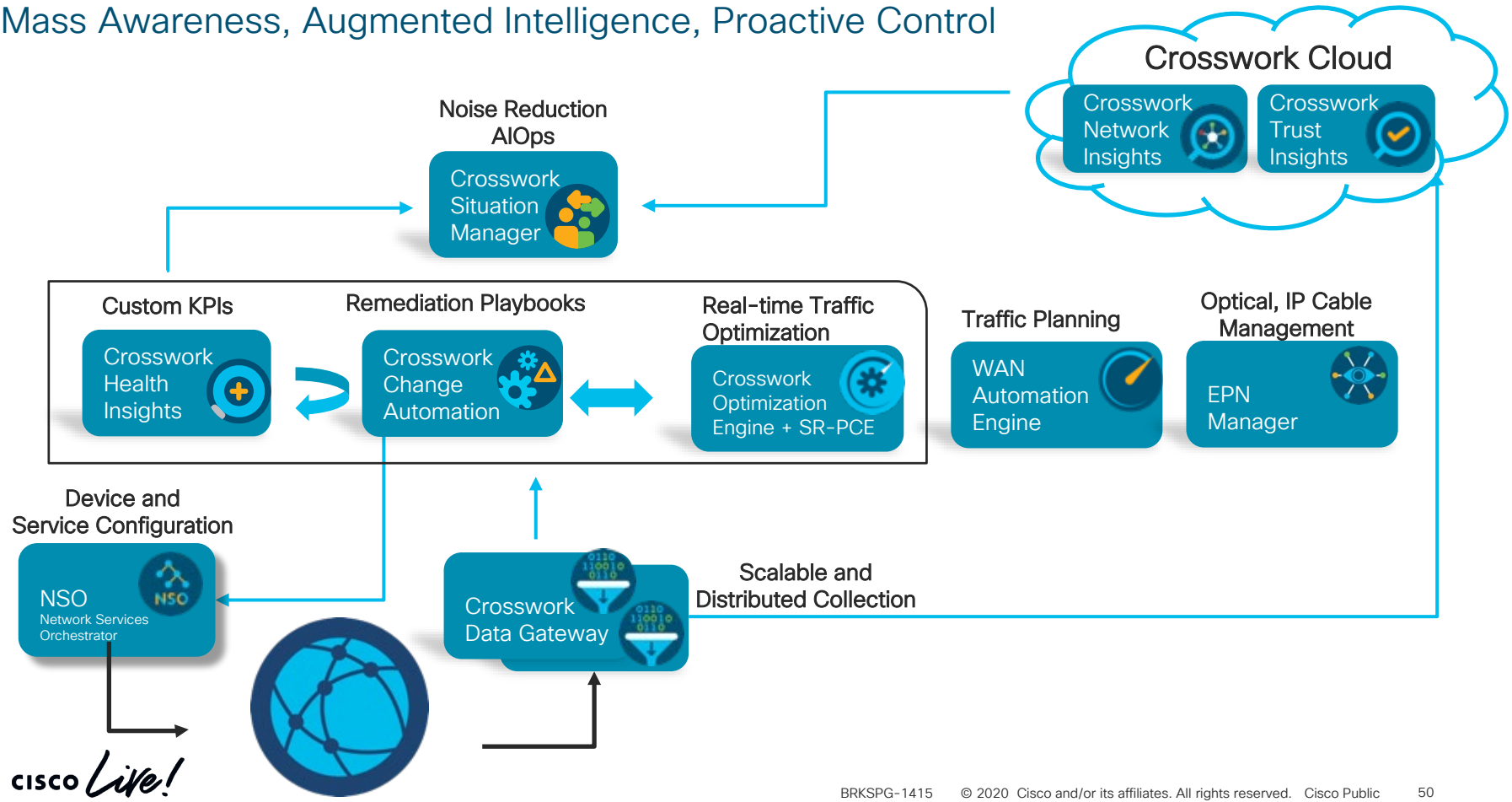
Data Gateway

large scale distributed data collection

Full Portfolio @ cisco.com/go/crosswork

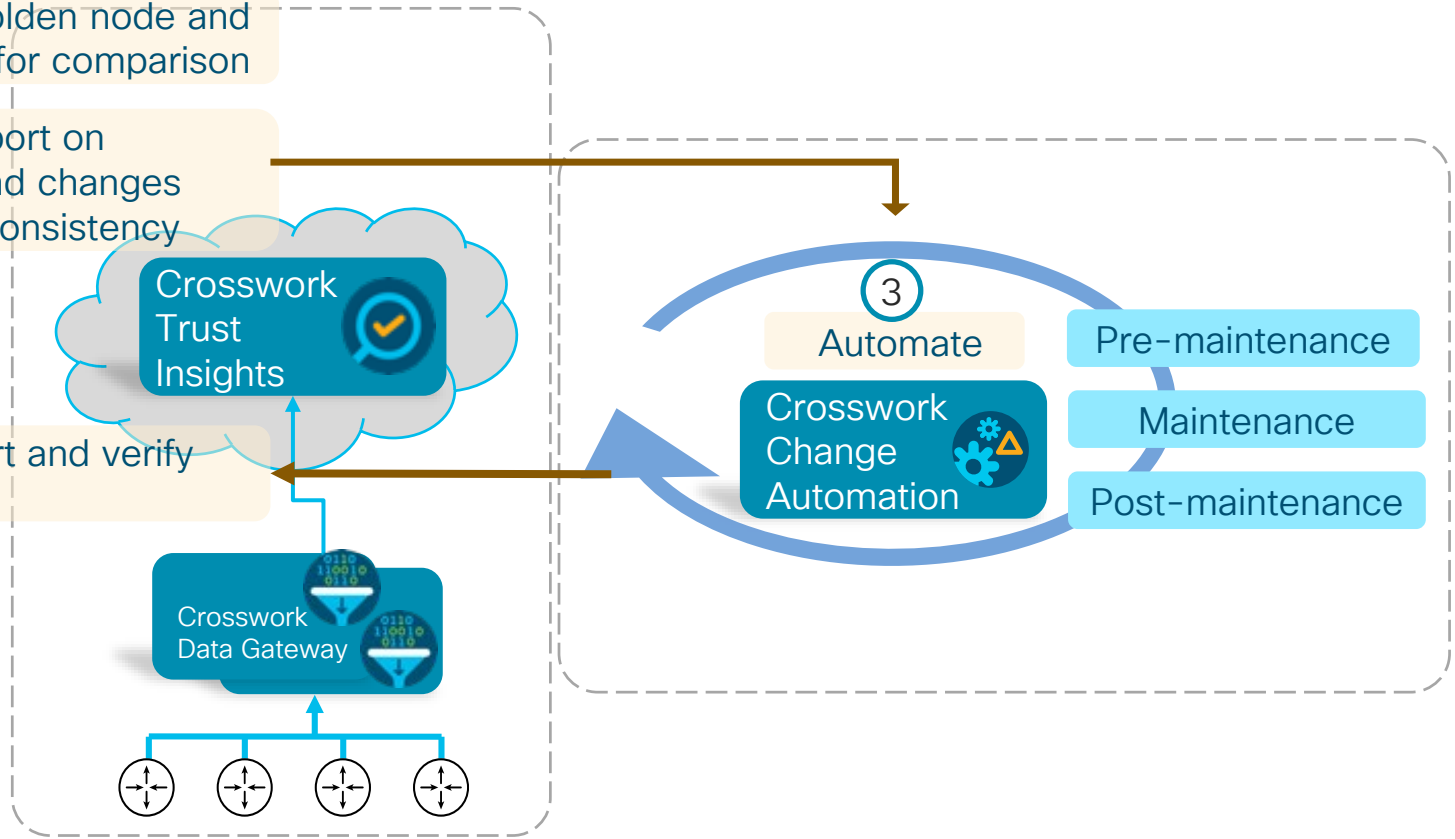
Crosswork Network Automation

Mass Awareness, Augmented Intelligence, Proactive Control



Expedite Consistency and Compliance

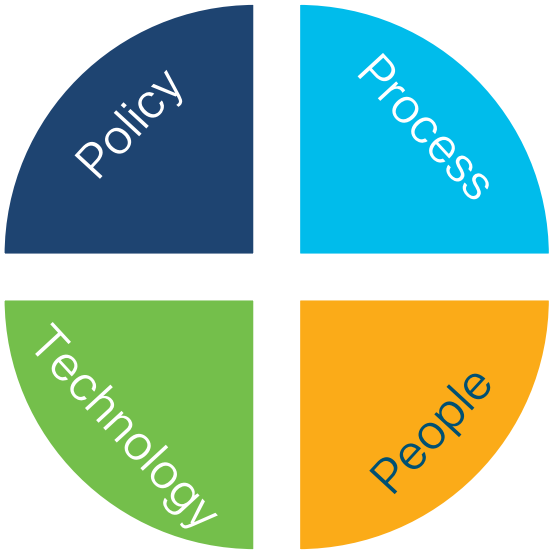
1. Select the golden node and other nodes for comparison
2. Generate report on deviations and changes needed for consistency
3. Automate
4. Update report and verify compliance



Conclusion

Cisco's Multi-faceted Approach to Security

Trust & Pervasive Security



Key Takeaways on Trust

- Trusted Platforms requires a hardware root-of-trust
- Evidence must be collected in verifiable manner
- Visibility and Reporting is critical to attest for the integrity of your Trusted infrastructure

Summary

Service Provider Networks are increasingly being recognized as Critical Infrastructure

Cisco is committed to continually enhancing the security and resilience of our networking solutions

Cisco Crosswork Cloud Trust Insights empowers you with visibility to analyze Trust in your Network Infrastructure

You need the ability to analyze the Trustworthiness of your network devices

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the
Cisco Showcase

Walk-In Labs

Meet the Engineer
1:1 meetings

BRKSPG-1768
cisco.com/go/sp-trust
trust.cisco.com

Thank you

You make **possible**