About Crosswork Cloud Trust Insights

About Trust Insights

Crosswork Cloud Trust Insights provides a way to protect and test the integrity of Cisco IOS XR devices on your network. Crosswork Cloud Trust Insights gathers secure measurements and proves that the data was collected at a certain time, which allows you to measure, verify, and audit the integrity of your network. Crosswork Cloud Trust Insights automatically interprets and verifies the integrity of Known-Good-Values (KGVs) measurements from IOS XR routers. This provides a unique visibility into hardware and software integrity and trustworthy status of production routers in your environment.

Crosswork Cloud Trust Insights helps you understand what is true on your network now and what was true in the past. It also helps you answer the following questions:

- How do I know that my router is running the software I want it to be running?
- How can I track what hardware and software has changed?
- How do I know if someone has modified the hardware or software running in my network?
- How can I prove where and when critical security updates were applied and are currently active?
- How can I be sure that the running software was built by Cisco?
- How can I verify what hardware and software was running in a particular date in the past?
- How can I prove that my systems are running compliant hardware and software?

Data Used by Trust Insights

In order to verify and prove the integrity of the hardware and software in your network, Crosswork Cloud Trust Insights uses the following data:

- Known Good Values (KGVs)—Cisco produces and publishes KGVs for its hardware and software products. The KGV.json file is signed by Cisco and contains measurements for various components such as boot integrity visibility, boot0 image measurements, boot OS image measurements, and running image file measurements. KGVs provide a standard of known, good values which test validity.
- Signed evidence dossiers from IOS XR devices—New features in IOS XR allow the ability to generate a dossier that contains trust information about the running hardware and software such as the operation status, inventor, and hardware, boot, and run-time integrity. Crosswork Data Gateway gathers the dossier and forwards it to Trust Insights.

How Trust Information is Gathered from Devices

The following steps explain the process by which Crosswork Cloud Trust Insights gets the trust dossier from devices.

1. Crosswork Data Gateway connects to Crosswork Cloud (HTTPS).
2. An administrator adds Crosswork Data Gateway information and devices to Crosswork Cloud Trust Insights.
3. Trust Insights sends Crosswork Data Gateway a list of devices to query.
4. Crosswork Data Gateway logs in to the devices and gathers the trust dossier.
5. Crosswork Data Gateway forwards the trust dossier to Crosswork Cloud Trust Insights.
6. Crosswork Cloud Trust Insights performs verification and analytics.

How Trust Insights Measures Trust

To test and measure trust in your network devices, Crosswork Trust Insights performs the following steps:

- Trust Insights securely request and collects a signed-evidence dossier from IOS XR devices by using the Cisco Crosswork Data Gateway.
- The dossier evidence is verified and added to the timeline of running hardware and software.
- Crosswork Trust Insights compares the data contained in the dossier against KGVs from Cisco for the hardware and software.
- Crosswork Trust Insights displays assured inventory reporting with history and trust visibility for the devices.

What Trust Insights Can Verify

Crosswork Cloud Trust Insights gathers and reports on evidence of software and hardware changes. For example, if you need to apply an SMU to address a security vulnerability on a device, Trust Insights can provide evidence that you're running the correct SMU and that the code you installed has fixed the vulnerability.

Trust Insights cannot:

- Determine if a router is up or down. Trust Insights isn't an operational tool.
- Verify the integrity of any code that Cisco didn't create. If we recognize the data from the operating system or an SMU, we can verify that your devices are running the software you think they are running. However, if we see data that we don't recognize, Trust Insights can’t determine its validity or integrity.