Cisco Integrity Verification Services

Gain Visibility Into the Integrity of Your Network Hardware and Software

Visibility into the integrity of your network is essential to protecting your organization’s data, employees, customers, and brand. As today’s network threats increase in sophistication, the resulting risks to your network may go undetected for days, months, or even years.

> According to the Ponemon Institute’s 2015 Cost of Data Breach Study, malicious attacks take an average of 256 days to identify.

To help protect your organization, Cisco has developed a set of services that provide visibility into the integrity of your network hardware and software as a critical first step in maintaining the health of your network. Cisco’s integrity verification services help defend your network by providing visibility into the risks that affect the trustworthiness of your network infrastructure, such as non-genuine hardware and software. By leveraging this visibility, organizations can improve their overall network infrastructure security posture while reducing unnecessary operational risks.

What Problems Does Integrity Verification Solve?

Cisco understands that non-genuine or suspect networking hardware and software are a serious threat to network performance and cyber security. In response, Cisco has developed integrity verification services to help you identify and mitigate the following types of threats:

Counterfeit Risks

- Hardware and/or software that was not built by Cisco or was altered post manufacture without Cisco’s consent with the intent to imitate a genuine Cisco product
- Devices contain pirated, tampered, or malicious software
- Cisco cannot warrant performance, reliability, or security of non-genuine equipment
- Non-genuine hardware is not entitled to Cisco service and warranty support

Unauthorized Channel Risks

- Cisco-manufactured equipment procured through an unauthorized distribution channel may be stolen or second-hand
- Hardware may not be entitled to Cisco service and warranty support
- Equipment from unauthorized channels poses a higher risk for pirated, tampered, or malicious software
- Unauthorized third-party components could compromise the quality of your equipment

Non-Genuine Software Risks

- Software that has been modified and sourced outside of Cisco’s authorized supply channel can compromise the operation of the device
- Malicious software can provide an attacker with the ability to monitor and/or exfiltrate information
- Non-genuine software could disable or “brick” hardware while attempting to perform platform maintenance or software upgrades

Cisco Integrity Verification Services

Cisco's integrity verification services deliver key visibility into the authenticity of your network infrastructure by leveraging device data and proprietary Cisco analytic capabilities along with Cisco design, development and manufacturing records. The initial integrity verification service offer covers the verification of Cisco IOS devices. Additional integrity verification services for newer platforms and operating systems are being planned for future updates.

The current suite of integrity verification capabilities include:

Net Authenticate

- Net Authenticate hardware integrity verification service for Cisco IOS devices and pluggable modules
- Detailed analysis into the authenticity of each device
- Counterfeit analysis yields classifications of Generic, Counterfeit, or Unresolved/ Open Questions
- Unauthorized Channel analysis yields classifications of Authorized, Grey Market, Missing Sales Data, or Unresolved/Open Questions

Software Integrity Verification

- Analysis of running images on Cisco IOS devices
- Image verification yields software classifications of authentic or non-genuine
- Additional forensics services available to determine the intent of the modifications

The process for performing hardware and software verification consists of four main steps: data collection leveraging tools such as the Cisco Common Services Platform Collector (CSPC), data processing/analysis, report generation, and customer discussion (see figure 1).

To learn more about how to identify trustworthy IT business partners, download a free copy of our eBook at:

https://trust.cisco.com

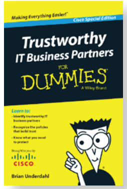
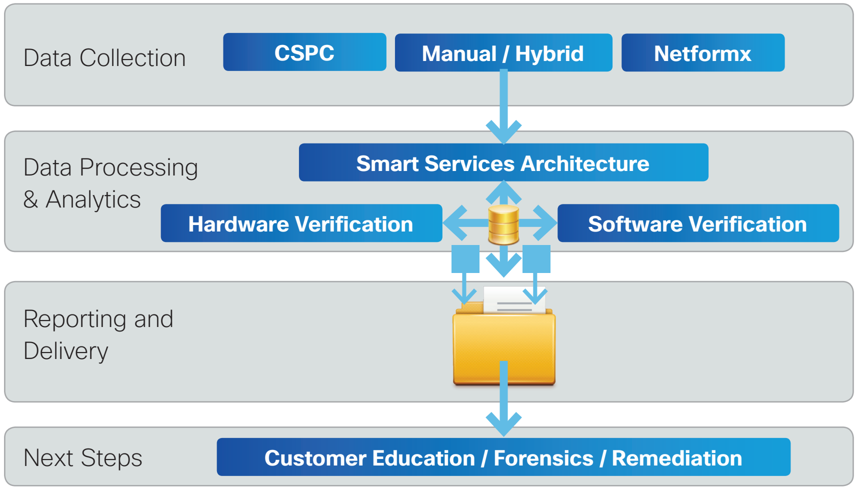


Figure 1: Integrity Verification Service Flow



Benefits of Cisco Integrity Verification Services

- Improves network infrastructure security
- Proactive identification of device vulnerabilities that pose security risks
- Minimizes risk for threats that impact network infrastructure reliability
- Improves the availability of vital business processes and information
- Improves risk management and satisfaction of compliance requirements

Why Cisco?

As cyber threats against organizations continue to grow in number and sophistication, your ability to gain visibility into the integrity of your network is critical. Only Cisco can provide visibility into the integrity and authenticity of your Cisco equipment. By being able to combine your device data with Cisco's design, development, and manufacturing records, Cisco's analytic capabilities deliver an accurate view of your network infrastructure risks.

For more information on Cisco's integrity verification services, contact your Cisco account manager or email **integrity-verification@cisco.com.**