Integrity Verification Services

Gain Visibility Into the Integrity of Your Network

Integrity Verification Services

Gain Visibility Into the Integrity of Your Network

White Paper

Executive Summary

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.

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 and security 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 taking full advantage of this visibility, you can improve your overall network infrastructure security posture while reducing unnecessary operational risks.

Introduction

Whether you're part of a company, organization or government body, your Information Technology (IT) network enables critical capabilities and supports core operations all while protecting employees, customers, and intellectual property. Given the persistent threat of attack in today's increasingly interconnected world, combined with its broadening attack surface, it is imperative that the network infrastructure itself be trustworthy.

At Cisco, we believe security is everyone's responsibility. We are accountable for trustworthy product development, supply chain security, customer data protection, and transparency that earn the verifiable trust of our customers, partners, shareholders, and employees. It is Cisco's intention to provide our customers with verifiable proof that not only are we a trustworthy partner, but just as importantly, we offer trustworthy solutions.

To help protect your organization, Cisco has developed a set of services that provide visibility into the integrity of your Cisco IOS 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 trustworthiness of your network components themselves through validation of their genuineness.

This paper focuses on the risks to trustworthiness posed by two sets of threats: non-genuine or tainted hardware and software and unauthorized channel risks.   It also describes the solutions available to understand your network's exposure to this type of threat. By taking advantage of this insight, your organization will be able to improve its overall network infrastructure security posture while reducing unnecessary operational risks.

Hardware and Software Integrity Background and Risks

Non-genuine or tainted hardware and software introduce risks with regard to the quality, reliability, performance, and safety of network devices, whether through substandard components, inadequate testing and manufacturing, or the use of pirated, unauthorized, unlicensed, or malicious software.[1]

Counterfeit and Unauthorized Hardware

Hardware integrity threats fall into two main categories: non-genuine and unauthorized secondary market (commonly referred to as grey market or unauthorized channel). Non-genuine IT hardware and electronic parts have received increased attention by corporations[2], organizations, and governments in recent years.

The emergence of counterfeit networking hardware is not a new phenomenon. Most companies making reputable, high-demand products face the threat of having their portfolios counterfeited, with trans-national, organized crime playing an increasing role.[3]

[1] Memorandum For Assistant To The President For Homeland Security Assistant To The President For Economic Affairs; DOD and GSA Report: Improving Cyber security and Resilience through Acquisition (14 Jan 2014):

"Recently, the problem of counterfeit, "grey market," or other nonconforming ICT components and subcomponents has gained significant attention as well. These materials can be introduced into systems during both initial acquisition and sustainment. As they are unlikely to have the benefit of testing and maintenance appropriate to their use, they create vulnerabilities for the end customer and increase the likelihood of premature system failure or create latent security gaps that would enable an adversary.

"Additionally, significant risks are also presented in the operations and maintenance phase and the disposal process. For example, failure to maintain up to date security profiles, install a software patch in a timely fashion, or failing to include identity and access management requirements all introduce cyber risks, but can be managed through the ICT acquisition process.

"In addition, the ICT supply chain is vulnerable to events such as intellectual property theft, service availability disruption, and the insertion of counterfeits. When dealing with a critical system or component, the consequences of these events can be significant, impacting the safety, security, and privacy of potentially millions of people.

"When the Federal government acquires a solution that has inadequate cyber security "baked in," the government incurs increased risk throughout the lifespan and disposal of the product or service, or at least until it incurs the added cost of "bolting on" a fix to the vulnerability. It is the lasting effects of inadequate cyber security in fielded solutions that makes acquisition so important to achieving cyber security and resiliency."

See "Improving cybersecurity and resilience through acquisition," Final Report of the Department of Defense and General Services Administration (GSA), Joint Working Group, November 2013.

[2] Deloitte "When Channel Incentives Backfire" (2011)

[3] See interpol.int/Crime-areas/Trafficking-in-illicit-goods-and-counterfeiting/Trafficking-in-illicit-goods-and-counterfeiting; and Interpol's "Turn Back Crime" Campaign at turnbackcrime.com/

Cisco actively captures counterfeit hardware bearing our name. Careful study of these devices as well as evidence provided at the locations producing them reveals that:

- Constituent components (integrated circuits, processors, etc.) used in counterfeit products often do not meet the performance standards found in genuine Cisco products and have not been subjected to the same degree of quality and performance testing.
- These products do not hold safety standard certifications, such as Underwriters Laboratory, Canadian Standards Association, TUVRheinland, etc., that genuine Cisco products attain following testing. In fact, producers of counterfeit products, in an effort to make their products appear genuine, usually infringe on the trademarks of these safety testing organizations by marking their products as if they have, in fact, been tested. As a result, fuses and other protective circuitry used in counterfeit products may present serious health and safety issues and fail to guard the end user from overvoltage situations.[4]
- Very little/no Electro Static Discharge (ESD) equipment is employed, presenting an increased risk of equipment failure to the end user.
- The hardware's Operating System contains pirated, counterfeited, or modified software to enable illegal upgrades.

Sales of unauthorized Cisco hardware misrepresented to customers as new, genuine Cisco devices have led to criminal prosecutions with significant prison sentences and financial restitution.[5]

Cisco, like many IT manufacturers, has an approved sales channel authorized to distribute genuine Cisco products. When solutions are procured from outside Cisco's authorized sales channel, product traceability is also lost as such products usually enter the market through deception and misrepresentation. They are typically assembled, configured, and shipped for a different end user, commonly in countries with little sales channel oversight.

Once traceability is lost, end users have very little to no insight regarding where the product has been located, what environmental conditions the product was exposed to during transit or storage, or whether it has been altered prior to installation at the end-user location.

Cisco products, like nearly all electronic goods, have a finite temperature range in which they should be stored. Outside of that temperature range, product operation can be compromised. For example, a Cisco Catalyst 3750 switch that has been exposed to temperatures outside of the -13° F to 158° F or -25° C to 70° C[6] range may exhibit reduced performance and/or reduced reliability.

[4] Please see cisco.com/web/partners/program/other/brand-protection/index.html for a short video illustrating this point.

[5] KC Business Owner Among Three Sentenced For $1 Million Scheme To Defraud The Army (Oct. 31, 2014). justice.gov/usao/mow/news2014/dillard.sen.html

Virgie Dillard, Roland Evans, and Mark Morgan pled guilty and were sentenced for fraud for selling to the Army Recreation Machine Program more than $1 million worth of counterfeit products and Cisco products that were used, modified post-manufacture, and obtained outside Cisco's authorized distribution channels.

Evans was sentenced to 37 months in federal prison without parole. Morgan was sentenced to 30 months in federal prison without parole. Dillard was sentenced to five years of probation. The court also ordered Dillard, Evans and Morgan to pay $1,073,022 in restitution to the U.S. Army.

[6] Please visit cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/product_data_sheet0900aecd80371991.html for the Cisco 3750 series product data sheet which lists storage temperatures along with several other operational and non-operational parameters.

Non-Genuine Software

Software obtained outside of Cisco's authorized supply channel, either pre-installed on an IT device or sold independently, poses a risk to the network, as it may be counterfeit or malicious. Depending on the motives of the actors who misrepresent the genuineness of their offerings, the level of risk inherent in non-genuine software can vary widely.

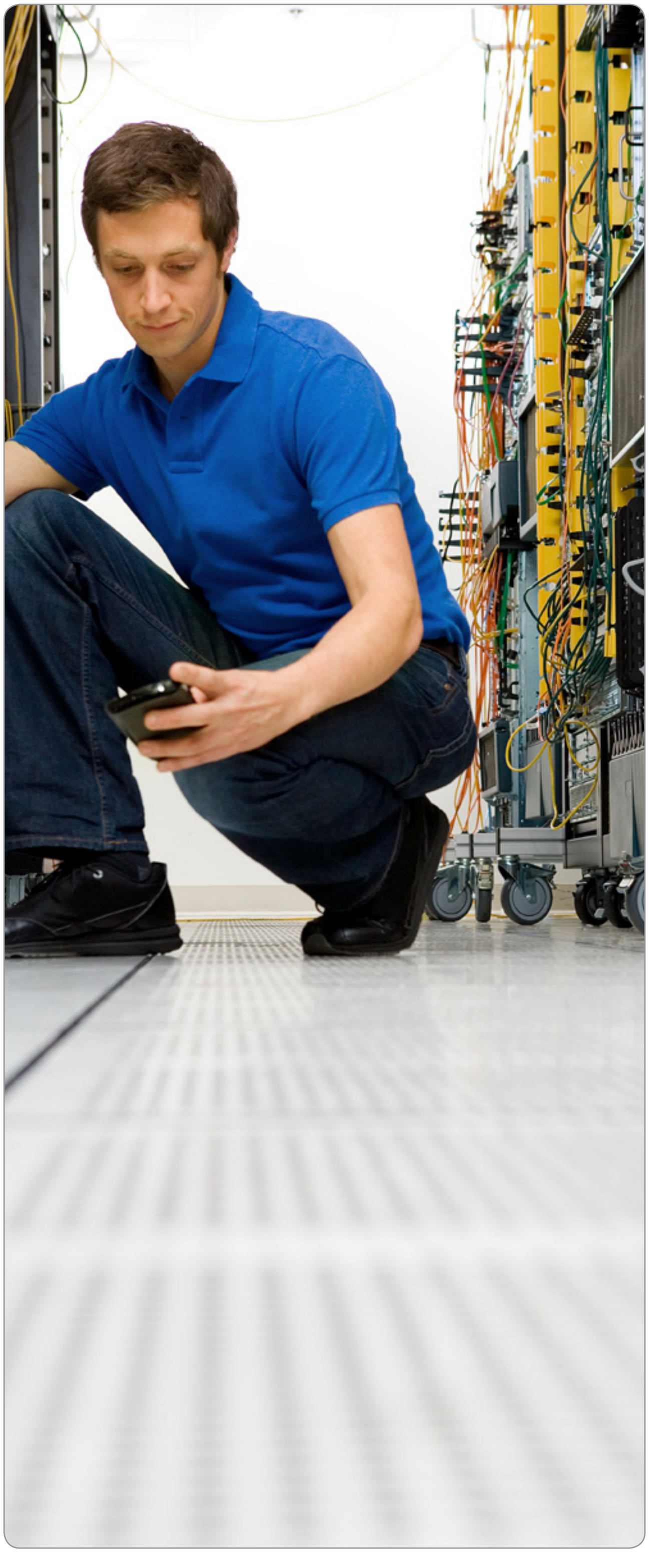
The lower end of the risk spectrum involves running non-genuine software that impacts the performance and reliability of the network hardware. Built specifically to enable the counterfeiting or illegal aftermarket modifications of Cisco hardware, these counterfeit or pirated Cisco IOS software images typically encounter problems when users attempt to perform software updates. The problems often manifest themselves as error messages shown on the console output. In certain cases, upgrading pirated IOS software may cause the unit to "brick" or become unusable until diagnostic action is taken.

The higher end of the risk spectrum involves the potential for software to be malicious in nature. Malware (malicious software) is software created to modify a device's behavior for the benefit of a malicious third party (attacker). One of the characteristics of effective malware is that it can run stealthily on a device in privileged mode. Malware is usually designed to monitor and exfiltrate information from the operating system where it is running without being detected. In addition, sophisticated Cisco IOS malware could attempt to hide its presence by modifying Cisco IOS command output that would normally reveal information about the malware's presence.[7]

In general, malware can be installed by using various methods: by exploiting vulnerabilities on the system or by manipulating an authorized user via social engineering attacks. Cisco IOS Software implements several techniques, including the use of safe coding libraries, Address Space Layout Randomization (ASLR), digitally signed software, and Cisco Secure Boot to help protect against memory and code manipulation and provide assurances of genuineness. Administrators should make sure their hardware and software support these features to ensure protection of the integrity of the device. However, these technologies will not protect Cisco IOS Software from unauthorized access due to compromised credentials. It is therefore important that administrators protect credentials for privileged accounts with appropriate controls and by implementing credentials management policies.[8]

[7] cisco.com/web/about/security/intelligence/integrity-assurance.html

[8] cisco.com/web/about/security/intelligence/integrity-assurance.html



Related Risk: Counterfeit and Unauthorized Services

Counterfeit and unauthorized services, while less publicized, have the potential to negatively impact network performance as well as create a direct path for non-genuine hardware and software to compromise an otherwise trustworthy network.

Many of Cisco's customers have partnered with our Brand Protection team to thwart advances from companies attempting to sell illegitimate versions of our most common service, SMARTnet. SMARTnet is not dissimilar to other IT OEM's (Original Equipment Manufacturer) offerings and is comprised of 4 pillars:

- TAC (Technical Assistance Center) access for 24 hour/ day support
- Online Cisco tools, forums, and library access
- Advanced hardware replacement (RMA or Return Materials Authorization)
- IOS (Cisco's Operating System) Updates and Upgrades

When procured through an authorized channel reseller, SMARTnet both reduces downtime and helps optimize network performance. Given that each pillar of SMARTnet provides an access point into the network, malicious actors could exploit these avenues to create vulnerabilities. For example, a genuine Cisco device "RMA'd" via a non-genuine services contract may be replaced by a counterfeit version of that device. Or, a user could obtain an IOS update or upgrade through the non-genuine services contract and unknowingly download malware. Additionally, some Cisco IOS devices offer sets of commands for use by Cisco Technical Assistance Center (TAC) engineers when troubleshooting a technical problem. Such advanced troubleshooting and diagnostic commands require privileged EXEC level and valid credentials to execute. If these device credentials are compromised, an attacker may be able to use the commands to inject code in memory during run time and modify the behavior of a Cisco IOS device.

If you have reason to believe that your SMARTnet coverage may be non-genuine, Cisco recommends contacting your Account Team for verification. Note that you may be asked to provide the Serial Numbers of all devices in question. You may also reach out to Cisco's TAC at 1-800-GO-CISCO.

Integrity Verification Services

Gain Visibility Into the Integrity of Your Network

White Paper

Integrity Verification Services Overview

In light of the substantial risks posed to the network infrastructure's security posture by counterfeit and unauthorized hardware and software, Cisco offers integrity verification services.   These services allow customers to validate the trustworthiness of their Cisco IOS assets by utilizing Cisco's intellectual property and human capital.

Hardware Verification: Net Authenticate

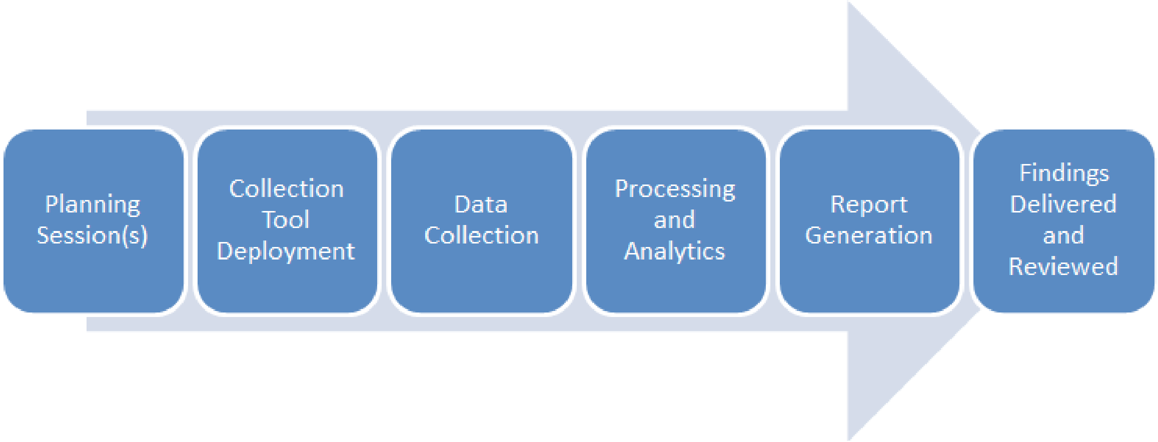
Cisco's Net Authenticate service combines proprietary analytics with automation to deliver efficient, consistent, and repeatable assessments as to whether the surveyed devices are genuine, untainted Cisco devices sourced through authorized supply channels.

After the completion of the Net Authenticate analysis, reports are generated to communicate findings. These reports include an executive summary that displays the results in a graphical format to quickly assimilate the information for management consideration and decision making on remediation and corrective action. Customers can use the results to:

- Immediately isolate and remove hardware deemed unacceptable for network performance, safety, or security risks
- Identify network components to be collected for physical examination and evidentiary use in enforcement or contract claims
- Evaluate necessary procurement or operational changes to mitigate against recurring risk.

The standard Net Authenticate service implementation comprises five phases as detailed below in Figure 1.

Figure 1. Major Implementation Steps



Software Integrity Verification

Cisco’s software integrity verification service detects non-genuine or tainted software operating within a network. This section provides information on the standard software integrity verification solution.

The software integrity verification service cryptographically validates that a Cisco IOS version is genuine and has not been tampered with or modified. This analysis requires that hashes of the IOS images running in memory on the devices under assessment be compared to the hash values of Cisco’s “Golden Images” to verify their genuineness.

After the completion of the software integrity verification process, reports are generated to communicate findings. These reports include an executive summary that displays the results in a graphical format to quickly assimilate the information for management consideration and decision-making on remediation and corrective action. Customers can use the results of software integrity verification to:

- Remediate pirated and unlicensed software and take other actions as appropriate to comply with policy or regulations
- Remove devices running non-genuine software from their network
- Initiate forensics services to determine whether the non-genuine software was inserted for counterfeit or malicious purposes

Integrity Verification Services Workflow

Data Collection

Net Authenticate and software integrity verification can be performed in tandem or delivered independently. The following sections address the engagement specifics in further detail.

There are three options for the tool deployment and data collection phases. The first two entail deployment of a collector tool and the third supports manual data collection.

A collector is a network management tool, which is used to survey the network landscape and discover what devices are connected. It then polls each device for the relevant data needed to execute integrity verification services.

The Cisco Common Services Platform Collector (CSPC) tool is the preferred option. CSPC is utilized when the service is provided directly by Cisco. In addition, a tool called Netformx DesignXpert supports the collection of integrity information and can be offered by Cisco's partner community.

The manual data collection option can be exercised if the use of network collection tools is not possible. With this option, a collector tool is not utilized and the customer captures device information manually or via a custom script. Strict data format requirements involving both Simple Network Management Protocol (SNMP) and IOS show commands must be observed to ensure that the automated processing tools can properly execute with the manually collected data. This is a complex endeavor and should only be exercised if use of network collection tools is deemed unacceptable after careful consideration, as manual collection will likely extend the time of engagement and may increase the total cost. Cisco recommends exploring these options during the Planning Session(s) to avoid unnecessary delays.

Once the device data has been collected, the network management tools connect to Cisco and deliver the information. The CSPC tool does this via an https connection. In the case of manually collected or scripted data collection, the file can be either physically or electronically transmitted to Cisco personnel who will upload the information.

The data is then processed through integrity verification data processing engines (Cisco-hosted). Note that the data is intrinsic device data, which is compared to manufacturing records, and not configuration parameters that are specific to the customer's configuration or environment.

Processing and Analytics

The integrity verification service performs data parsing functions to prep the information for the automated engines. Upon completion of this step, data passes through multiple integrity analysis engines to verify both hardware and software integrity. For hardware verification, the system checks several parameters per serial number to verify manufacturing-level genuineness and whether the customer currently in possession of the device is the original end-user customer for whom the product was assembled and configured prior to original shipment and disclosed to Cisco as being the end user. The unauthorized channel assessment also examines Cisco Return Material Authorization (RMA) and repair databases for each serial number.

Concurrently, the software verification system analyzes the IOS version and MD5 hash (fingerprint) of the running image collected during the first phase and compares against Cisco's Golden Images to determine whether or not the IOS images are genuine.

At the conclusion of the verification analyses, Cisco engineers review the assessments to verify the output and add intelligence based on the latest counterfeiting and malware trends. Some of the more complex counterfeit assessments cannot be fully automated. In these situations, trained engineers review the data points returned by the system and make the determination on product genuineness. For products identified as being sourced from an unauthorized channel, engineers review the results and check mergers and acquisitions history and other data sources available within Cisco. A general quality review is also performed by auditing the results on a sampling basis to validate overall report integrity.

Report Generation and Findings Review

The integrity verification service generates two reports. The first is a spreadsheet listing each serial number analyzed and the assessment result. This is intended for personnel at the customer site who will be responsible for acting on remediation activities. The second is an executive summary document, intended to quickly convey the overall results. This second document is targeted for those responsible for overall network health and performance. It lists the overall quantity of non-genuine or tainted hardware and/or software images identified.

The hardware and software assessment categories delivered in the integrity verification service reports are summarized in Table 1.

Table 1. Integrity Verification Assessment Categories

Counterfeit Assessment	Grey Market Assessment	Software Integrity Assessment
Genuine Product	Authorized Product	Genuine Software
Counterfeit Product	Grey Market Product	Non-Genuine Software
Unresolved/Open questions	Missing Product Sales Data	Unresolved/Open questions
	Unresolved/Open questions	

For the purposes of both the counterfeit and software integrity assessments, the use of the term “genuine” implies that that the hardware or software being analyzed has not been tainted or modified either maliciously or otherwise. The “Unresolved/Open questions” and the “Missing Product Sales Data” items may require additional clarification. The Unresolved/Open questions result can occur in the counterfeit determination when a device does not respond as expected to the electronic querying, or in case of a manual data collection, the device information is not complete. It may also occur when the electronic data extracted from the device checks out, but the particular device must also conform to industry specifications for interoperability across network vendors.

In situations where many companies make identical form-factor products, it becomes important to confirm if the associated hardware bears the Cisco logo, as electronic customization is used by Cisco to differentiate our hardware. Therefore, any device with electronic information matching Cisco records which does not feature the Cisco logo may be counterfeit. Transceiver modules are the most likely devices to fall into this assessment category.

In the unauthorized channel analysis, the Unresolved/Open questions result can occur when incomplete sales data is returned to Cisco. The Missing Product Sales Data result could occur when records of the sale are not reported to Cisco. It may also originate from situations where the device sale occurred prior to 2005 or, in the case of transceiver modules, prior to 2008. In previous experiences with the integrity verification service, this assessment result was observed to occur in less than eight percent of the analyzed serial numbers.

Limitations

- Network tools are only capable of analyzing devices that are on the network. Any devices in the inventory that are not connected will not be detected or analyzed and, therefore, no resulting reports will be provided.
- Integrity verification services are limited to the analysis of Cisco devices only.
- Due to the breadth and complexity of Cisco's product portfolio, at any given time, the integrity verification service may not cover every product line and Product ID in Cisco's portfolio. As of September 2015, the integrity verification service only supports Cisco devices running the IOS classic operating system.[9] This provides analysis capability for a large portion of Cisco's installed base and provides protection against non-genuine hardware and software Cisco has seen in the marketplace. A current and complete list of supported products will be provided on request.

Remediation

Remediation can begin immediately after the integrity verification services results are delivered and reviewed. Remediation strategies will vary and depend heavily on a customer's risk tolerance. For this reason, this should be a collaborative conversation between the customer and Cisco. Understanding the physical location, mission, remaining lifespan, and criticality of function of the newly identified non-genuine hardware or software is a recommended consideration, as this information has historically proven useful in prioritizing remediation actions. There may be situations where the customer decides to conduct further physical inspection, engage in a security assessment, or perform software forensics as follow-on work. Customers may engage Cisco for such work that exceeds the scope of the Net Authenticate and software integrity verification.

Benefits

Cisco understands that non-genuine network devices are a serious threat to network performance and cyber security. While Cisco invests heavily in trustworthy and transparent business practices, including a secure supply chain, it acknowledges the sophistication of parties who profit, whether financially or otherwise, from the unauthorized sales, counterfeiting, or other cybercrimes. In response to this reality, Cisco offers integrity verification services to help our customers identify and mitigate the threat of counterfeit and unauthorized products and software that may already exist on their networks.

Benefits of the integrity verification services include:

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

[9] Classic IOS is the software used on the vast majority of Cisco routers and switches. Some newer Cisco hardware runs different flavors of IOS, such as the ASR product family (which runs IOS XE) and Nexus product family (which runs NX-OS).

Integrity Verification Services

White Paper

Gain Visibility Into the Integrity of Your Network

Summary

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 of your Cisco equipment. Through a combination of your device data with Cisco's design, development, and manufacturing records, Cisco's analytic capabilities deliver an accurate view of your network infrastructure risks. By taking full advantage of this visibility, your organization can improve its overall network infrastructure security posture while reducing unnecessary operational risks.

For more information on Cisco's integrity verification services or to begin planning your network assessment, contact your Cisco account manager or email integrity-verification@cisco.com.

Appendix A: Glossary

Authentic – Genuine Cisco hardware or software components that are unaltered.

Counterfeit – A device that was not built by Cisco, or was materially altered post manufacture without Cisco's consent, and in Cisco's opinion, was generally produced with the intent to counterfeit or imitate a genuine Cisco product.

Grey Market – While legal in most countries, these are sales channels that are unauthorized or unintended by the original manufacturer. Cisco warranty typically does not transfer with grey market sales and standard Cisco policy dictates equipment inspection and relicensing is required prior to addition to any maintenance service contact such as SMARTnet.

Malicious modifications - Modifications made for the purpose of gaining unauthorized information, access, or control of a device.

Mitigation - Recommended action to reduce or eliminate risk and/or vulnerability exposure.

Pirated Cisco Software – Unlicensed IOS running on a Cisco device. There are two flavors of pirated Cisco software—genuine pirated and altered/modified pirated.

Refurbished – Used goods, which are checked for functionality and performance, then certified to be equivalent to new equipment. It is important that the manufacturer (vs a third party) refurbish the goods to ensure proper operation.

Relicensed – A product sourced via the grey market, which has undergone the inspection and relicensing process and is now properly titled to the current end user.

Secondary Market – A general term, which refers to all Cisco unauthorized channels. This includes the grey market and the black market.

Software Forensics Service - A paid service designed to detect software-based tampering of IOS and/or boot loader images.

Tainted - A product that is produced by the represented manufacturer that has been tampered, either maliciously or otherwise.

Unauthorized Channel – Any entity selling Cisco product(s) who is not a member of Cisco's partner program. The Cisco partner locator tool can be found by going to tools.cisco.com/WWChannels/LOCATR

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**