CiscoWorks Network Compliance Manager Alert Center

CiscoWorks Network Compliance Manager (NCM) Alert Center is a subscription offering that provides customers with new and changing security and compliance policies to help maximize the return on investment in CiscoWorks Network Compliance Manager. It uses the extensible CiscoWorks NCM automation platform to deliver new automation capabilities on an ongoing basis.

Applications

Alert Center will support the following IT functions:

- **Acting upon new security vulnerabilities:** As new security vulnerabilities are found, Alert Center will deliver these vulnerabilities to the CiscoWorks NCM server in the form of actionable compliance policies to allow customers to quickly identify all vulnerable devices on their network and rapidly remediate them before hackers can compromise their security.
- **Staying up to date with industry-standard compliance policies:** Alert Center will deliver to CiscoWorks NCM updates to CIS and PCI compliance policies for Cisco IOS and PIX platforms.

Features and Benefits

CiscoWorks NCM Alert Center provides the following capabilities:

1. **Actionable security alerts:** CiscoWorks NCM Alert Center provides a one-of-a-kind security service that delivers alerts on network security vulnerabilities. Unlike traditional alerts, which are typically delivered by e-mail and therefore very hard and very time consuming to act on, these alerts are delivered as actionable CiscoWorks NCM compliance policies that allow customers to quickly identify all vulnerable devices on their network and rapidly remediate them before any hackers can compromise their security.
2. **Industry-standard compliance policies:** CiscoWorks NCM Alert Center provides CIS audit policies for Cisco IOS and PIX platforms. CIS is a nonprofit enterprise consisting of members from the public and private sectors that develops and promotes the widespread use of security configuration benchmarks for workstations, servers, network devices, and software applications.

   CiscoWorks NCM Alert Center also provides PCI DSS policy for the Cisco IOS platform. PCI DSS version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.
3. **Live, real-time availability of security and compliance policies:** Since CiscoWorks NCM Alert Center is a subscription service, it allows customers to use new automation capabilities as soon as they are available. The latest security and compliance policies can be downloaded and installed automatically with the Alert Center Utility, a component that is installed on the CiscoWorks NCM core.

Table 1 lists features and benefits of CiscoWorks NCM Alert Center.

Table 1. Features and Benefits

Feature	Benefit
Dedicated content development team	
Cisco® content development team that tracks, triages, analyzes, and converts vendor security alerts into actionable policies	Eliminates the need for customers to track vendor alerts, translate vulnerabilities into actionable tasks, identify vulnerable devices, and make sure of ongoing compliance
Security alerts delivered as actionable policies	
Delivers security vulnerabilities as CiscoWorks NCM compliance policies that automatically run vulnerability tests to identify affected network devices	Automatically identify all vulnerable devices in minutes rather than depending on a manual, error-prone, and time-consuming process
New and updated compliance policies	
Industry-standard compliance policies such as CIS and PCI DSS. Updates to existing policies and new policies are released on an ongoing basis	Automatically download and install compliance policies to allow customers to keep up with the rapidly changing compliance regulations and standards
Automated download of security alerts	
Configures customer's CiscoWorks NCM server to automatically download new security vulnerabilities on a periodic basis	Automatically obtain the latest security vulnerability information rather than depend on a manual and error-prone process
Remediation of all vulnerable devices concurrently	
Provides the remediation solution as part of a compliance policy that can be pushed out to all vulnerable devices simultaneously	Remediate all vulnerable devices on the network concurrently by performing software updates, making required configuration changes, or both
Compliance policies are tied to the event system	
Automatically generates an alert when network devices don't comply with CiscoWorks NCM compliance policies	Automatically provide alerts when a vulnerability is reintroduced due to either a regression in the existing environment or the addition of a new vulnerable device to the network
Historical alerts across all supported vendor platforms	
Delivers historical alerts for the past 13 years across all supported vendor platforms	Help ensure that network devices aren't exposed to known historical vulnerabilities

Product Architecture

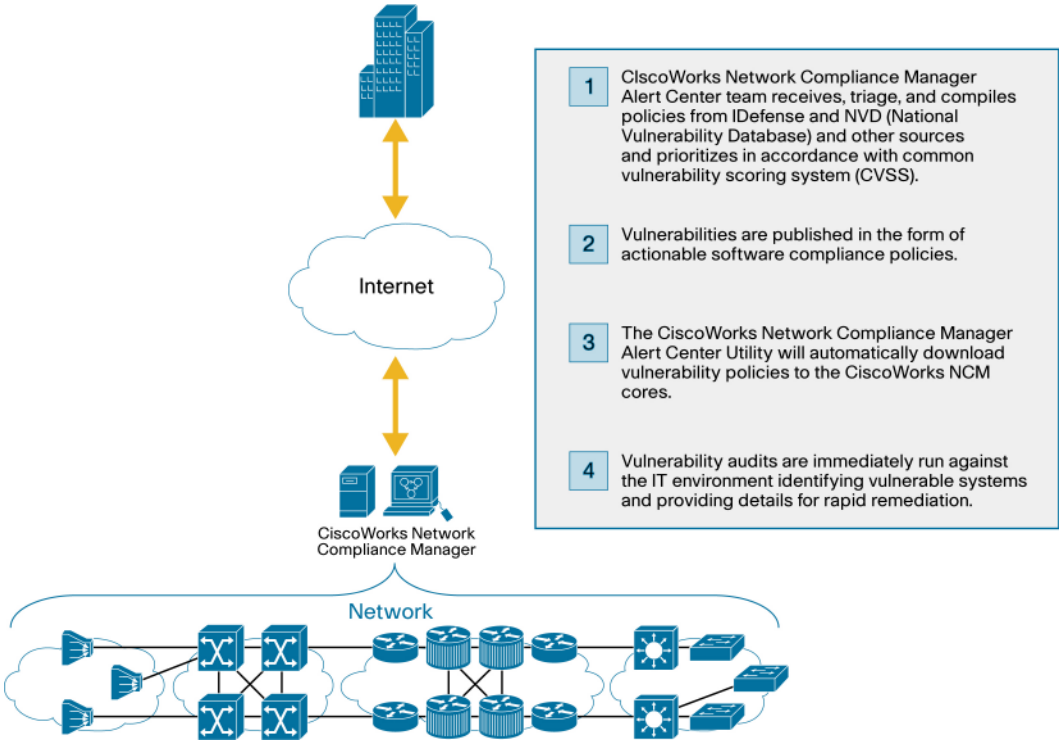
How Does the Security Alert Service Work?

Traditionally, vendors have delivered security vulnerability alerts by e-mail, making them very hard and very time consuming to act on. In today's highly networked environments, hackers attack customer networks and compromise their security often within minutes or days of a vulnerability announcement.

Consequently, the most pressing concerns facing customers today are the time to resolution on breaking vulnerabilities and the assurance that all vulnerable devices on their network have been remediated. Furthermore, customers want to know that their network won't be prone to future attacks on known vulnerabilities as a result of any regression in their existing environment or because a new device with a known vulnerability was added to their network. Unfortunately, today's vulnerability management solutions don't effectively address these concerns.

In response to these challenges, CiscoWorks NCM Alert Center delivers a unique Security Vulnerability Service that provides customers with actionable alerts on new vulnerabilities. This allows customers to quickly identify all vulnerable devices on their network and rapidly remediate them (Figure 1).

Figure 1. Overview of the Alert Center's Security Vulnerability Service



The vulnerability alerts are packaged and uploaded into the Alert Center distribution tools in the form of CiscoWorks NCM compliance policies. Customers configure the Alert Center Utility that is installed on the CiscoWorks NCM server to either automatically download the new alerts on a periodic basis or perform the download on demand. When the Alert Center Utility calls home to Cisco, it downloads all new alerts that have been uploaded to the Website since the last download. These alert policies include rich details on the vulnerabilities such as detailed descriptions, disclosure dates, severity levels, and remediation solutions. Once these alerts are downloaded onto the CiscoWorks NCM server, customers can quickly and easily run a compliance check to identify all vulnerable devices on their network. After the vulnerable devices are identified, customers can configure CiscoWorks NCM to remediate these devices concurrently. Typically, the remediation process involves a device software update, specific changes to configuration files, or both. Besides providing alerts on new security vulnerabilities, CiscoWorks NCM Alert Center also includes historical alerts for the past 13 years across all supported vendor platforms. Since all new and historical alerts are delivered as software compliance policies, if a vulnerability is introduced into a customer's network, CiscoWorks NCM will immediately notify the customer of this event and help rapidly remediate the situation.

Anyone who has used traditional methods to identify and remediate security vulnerabilities will appreciate the inherently manual nature of this task, which renders it very time consuming, labor intensive, expensive, and unreliable. Using the Security Alert feature of CiscoWorks NCM Alert Center, customers can easily, reliably, and rapidly remediate all vulnerable devices on their network. CiscoWorks NCM Alert Center provides an unparalleled security alert service that addresses the vulnerability management challenges of today's highly networked environments.

Product Specifications

CiscoWorks Network Compliance Manager Alert Center is compatible with CiscoWorks NCM version 1.3 SP2 or higher.

Device Support

CiscoWorks NCM Alert Center supports an extensive range of Cisco equipment plus devices from 35 other vendors. Categories include routers, switches, firewalls, wireless access points, VPN devices, network accelerators, network load balancers, and other appliances that serve dedicated functions such as terminal and proxy servers. CiscoWorks NCM Alert Center can be easily upgraded to support new devices as they become available or to meet market demand.

Ordering Information

Please see the CiscoWorks NCM product bulletin for ordering information at http://www.cisco.com/go/cwncm.

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about CiscoWorks NCM Alert Center, visit http://www.cisco.com/go/cwncm, contact your local account representative, or send an e-mail to ask-ncm-pm@cisco.com.

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.

Printed in USA C78-458269-01 12/08