

CiscoWorks Network Compliance Manager Alert Center

Q. What is CiscoWorks Network Compliance Manager (NCM) Alert Center?

- A.** CiscoWorks Network Compliance Manager Alert Center is a subscription offering that provides customers with additional functionality to maximize their return on investment (ROI) in network automation.

The offering has the following components:

1. **Security Vulnerability Service:** An online security service that delivers security vulnerability policies. Instead of the traditional security alerts from multiple vendors, which are typically delivered by e-mail and therefore very hard and time consuming to act on, these alerts are delivered as CiscoWorks NCM policies. Once these policies are received through CiscoWorks NCM Alert Center and installed on customers' CiscoWorks NCM servers, it's easy for customers to quickly identify all vulnerable network devices across their network and perform rapid remediation before any hackers can compromise their network.
2. **Compliance service:** Currently, CiscoWorks NCM Alert Center provides PCI DSS (Payment Card Industry Data Security Standard) policies for Cisco IOS® Software. PCI DSS represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information.
3. **Security best practices content:** CiscoWorks NCM Alert Center provides CIS (Center for Internet Security) compliant policies for Cisco IOS and Cisco PIX® platforms. CIS is a nonprofit organization that helps CIS members develop and promote the widespread use of security configuration benchmarks.

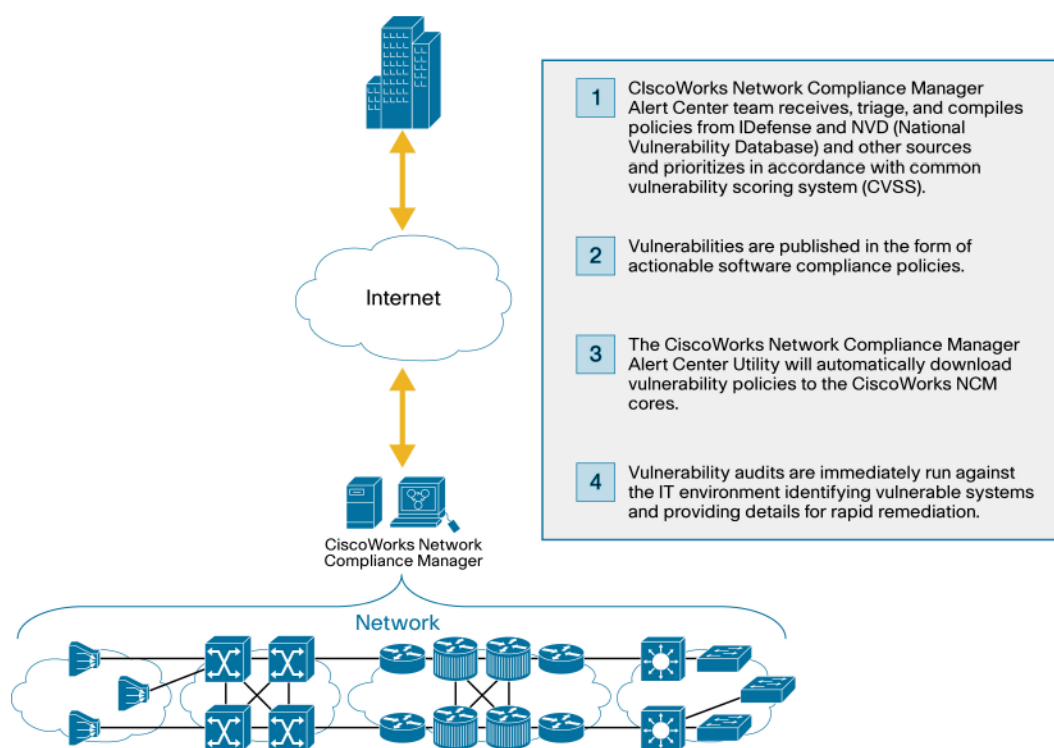
Q. How does the Security Vulnerability Service work?

- A.** The security vulnerabilities are sourced primarily from [iDefense Labs](#) (a division of Verisign), which is a provider of security intelligence information to government and Fortune 500 organizations. A secondary source of network vulnerability content is the [National Vulnerability Database](#) (NVD). NVD is the U.S. government repository of standards-based vulnerability management data maintained by NIST (National Institute of Standards and Technology).

The CiscoWorks NCM Alert Center team analyzes and triages the vulnerabilities every week. The CiscoWorks NCM Alert Center team writes OVAL (Open Vulnerability Assessment Language) scripts for each of these vulnerabilities, packages the content in the form of policies, and loads them to the Cisco Repository Alert Center. In many instances, Cisco is able to make use of OVAL scripts written by other members of the OVAL community.

The latest security vulnerability policies are then detected by the CiscoWorks NCM Alert Center Utility, which is an agent installed on the customer's CiscoWorks NCM core. The CiscoWorks NCM Alert Center Utility can be scheduled to run on a weekly or ad hoc basis, detects the latest content, and then installs it on the CiscoWorks NCM core. Once on the CiscoWorks NCM core, the policies can be run as an audit task to determine the security of the network infrastructure.

The security vulnerability alert process is shown visually in Figure 1.

Figure 1. Cisco's Security Vulnerability Process

Q. How often are the security vulnerability alerts published to the CiscoWorks NCM Alert Center Website?

A. The CiscoWorks NCM Alert Center team releases security vulnerability alert packages on a weekly basis. If customers have their CiscoWorks NCM servers configured to automatically download new alert updates on a periodic basis, they will automatically get their next set of new alerts when the CiscoWorks NCM server “calls home” to the CiscoWorks NCM Alert Center Website. Customers can also perform an “on-demand” download and check for new alerts at any point in time. Any new alerts that have been uploaded to the CiscoWorks NCM Alert Center Website since the last download will get downloaded to their server.

Q. What compliance policies are currently available?

A. Currently, CIS policies for Cisco IOS and Cisco PIX platforms are available. CiscoWorks NCM Alert Center also provides PCI policies for Cisco IOS Software.

Q. Does a customer need to subscribe to CiscoWorks NCM Alert Center in order to use CiscoWorks NCM?

A. No, CiscoWorks NCM is a standalone product that is fully functional without the CiscoWorks NCM Alert Center service.

Q. Are there any specific product dependencies in order to use CiscoWorks NCM Alert Center?

A. Yes, customers that want to use CiscoWorks NCM Alert Center will need to be on CiscoWorks NCM 1.3 SP2 or higher.

Q. How can I get a demonstration of CiscoWorks NCM Alert Center?

A. Please contact your Cisco sales representative, who'll be happy to set this up for you.

- Q. I'm already evaluating CiscoWorks NCM. Can I evaluate CiscoWorks NCM Alert Center too?**
- A.** Yes, please contact your Cisco sales representative, who will get you the evaluation login credentials for CiscoWorks NCM Alert Center. Your CiscoWorks NCM Alert Center credentials will expire at the same time as your CiscoWorks NCM evaluation license.
- Q. How do I get support for CiscoWorks NCM Alert Center?**
- A.** Customers should use Cisco customer support in the same manner as they do today for other product support issues.

For More Information

For more information about CiscoWorks Network Compliance Manager 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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)