

TREND MICRO™ - CISCO® SYSTEMS NETWORK ADMISSION CONTROL

A comprehensive network security policy enforcement solution

Datasheet

KEY BENEFITS OF TREND MICRO-CISCO NAC

- Provides automatic enforcement of corporate security policies, on all endpoints, regardless of access method
- Integrates antivirus and network policy enforcement to control client access and help minimize external and internal threats
- Enables central deployment of Cisco NAC client components using Trend Micro OfficeScan management console
- Reduces help desk calls by automatically remediating noncompliant endpoints using the Host Credential Authorization Protocol (HCAP) in the Cisco Secure ACS—expediting users' ability to obtain network access
- Increases network availability, resilience, and productivity by integrating security policy into the network infrastructure
- Reduces IT costs by maximizing the return on investment in an organization's network infrastructure and software, easing administrative burden and helping to ensure business continuity

PROBLEM

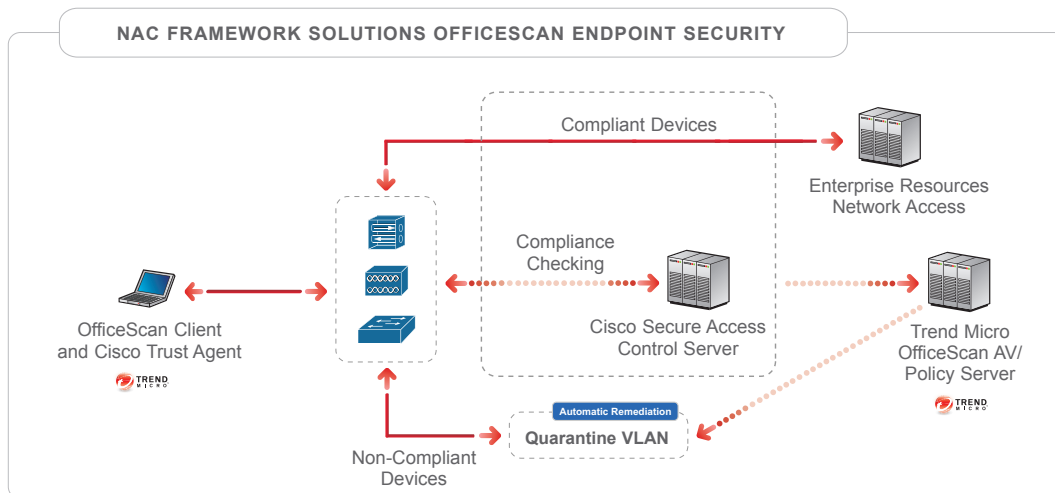
Viruses, worms, and hackers continue to attack networks and disrupt business. While file-based viruses spread when users open infected e-mail attachments, worms and network viruses self-launch through operating system vulnerabilities. The unprepared network is open to assault when users with outdated patches or unprotected devices log on. Locating and isolating infected systems is time- and resource-intensive. With mobile workforces, extranet partners, and remote offices, administrators must share the burden of network protection with end users—where any vulnerable machine can open the door to viruses and intruders. Without the ability to enforce security policy throughout the network and to deny access to noncompliant endpoint devices (PCs, servers, and PDAs, for example), business productivity, network resilience, confidential information, and other corporate assets are at risk.

STRATEGY

In November 2003, Trend Micro™ and Cisco Systems® announced their co-sponsorship of the Cisco Network Admission Control (NAC) framework, an industry-wide, multivendor collaboration led by Cisco® to minimize the damage organizations face from emerging security threats. Cisco Systems, a worldwide leader in networking and founder of the Self-Defending Network strategy, and Trend Micro, a global leader in network antivirus technology and creator of the Enterprise Protection Strategy, are collaborating to address endpoint security issues and policy enforcement through product interoperability. The collaboration between Trend Micro and Cisco provides network admission policy enforcement, antivirus software, and network resources to dramatically improve network security.

The Trend Micro and Cisco NAC solution is available on Trend Micro OfficeScan versions 6.5 and later, which integrates with the Cisco Trust Agent and Cisco Secure Access Control Server (ACS). This solution utilizes an existing Cisco infrastructure, and allows organizations to enforce system compliance before allowing access to network resources and data. Enterprises using Cisco NAC can restrict network access to compliant and trusted endpoint devices only after the devices are verified to be fully compliant with established security policy and allows for automatic remediation of non-compliant devices. The joint NAC solution helps neutralize ever-evolving threats, addresses the environmental complexity of today's networks, and provides global network availability and overall enterprise continuity.

In October 2005, Cisco expanded its NAC platform support to include Cisco Catalyst® switches and Cisco Aironet® wireless access points, and introduced new versions of the Cisco Trust Agent and the Cisco Secure ACS. Now the solution, also referred to as "NAC2", extends admission control capabilities beyond the perimeter devices supported in the original NAC. Through third-party integration to Cisco Secure ACS, NAC2 also added the capability to identify and control network access for unmanaged or agentless devices, such as guest laptops or printers.



Trend Micro™ – Cisco® Systems Network Admission Control

INTEGRATED SECURITY INFRASTRUCTURE

- 1. Endpoints Attempt Network Access:** Trend Micro's OfficeScan client software is NAC-enabled. It consists of Trend Micro's antivirus software integrated with the Cisco Trust Agent, and it resides on desktops, servers, and laptop hosts. The Cisco Trust Agent collects the client state information from the OfficeScan client.
- 2. Demand Credentials:** NAC-enabled Cisco network access devices, such as routers, switches, wireless access points, and remote-access concentrators, demand security credentials from endpoints.
- 3. Endpoint Validation:** Cisco Secure ACS, the core NAC policy server, validates the endpoint device's security credentials.
- 4. Antivirus Validation:** Cisco Secure ACS works in concert with the Trend Micro OfficeScan policy server to validate endpoint antivirus credentials.
- 5. Enforce Access Rights:** Cisco Secure ACS passes an admission control decision (permit, deny, quarantine for remediation, or restrict access) back to the NAC-enabled network access device, where the decision is enforced.

DRAMATICALLY IMPROVED NETWORK SECURITY

To dramatically improve network security, the seamlessly integrated Trend Micro – Cisco solution allows network access to endpoint clients such as PCs and servers only, after they are verified to be fully compliant with the established security policy.

- NAC supports endpoints running Microsoft™ NT, XP, and 2000 operating systems.
- NAC uses existing network topology to see any device and any degree of security compliance – including non-responsive clients (e.g. printers), for 100 percent validation of hosts and devices.
- NAC provides secure access for multiple connectivity methods including LAN, WAN, IPsec, wireless, and dial-up.
- OfficeScan is designed to protect the desktop environment against the daily threats of viruses as well as secure access from intruders, spyware and other threats.
- The Cisco Trust Agent, integrated with OfficeScan, collects security state information from clients and communicates device status to NAC-enabled devices to permit, deny, quarantine, or restrict access. Cisco Access Control Server (ACS) validates the end-point to ensure that the OfficeScan client is running and up to date.

If the Cisco Security Agent (CSA) is enabled, it protects the server and desktop environment from intrusions and malicious behavior.

SYSTEM COMPONENTS

For the latest system requirements, please refer to the OfficeScan product requirements page at www.trendmicro.com or the Cisco NAC product requirements at www.cisco.com/go/nac. NAC works with clients and servers running Microsoft Windows 2000, NT, or XP, Red Hat Linux Enterprise Edition 3.0 and Microsoft Windows 2003. Trend Micro-Cisco NAC 2 components are listed below.

- **Trend Micro OSCE Version 7.3**
 - OfficeScan Server
 - OfficeScan Web Console
 - OfficeScan Client
- **Cisco Trust Agent 2.x, integrated in Trend Micro OSCE, or available for download from Cisco.com, installed on endpoint devices**
- **Cisco Secure ACS Version 4.x**
- **Cisco NAC-enabled network access devices, including routers, switches, VPN concentrators and wireless access points**
- **Cisco Security Agent software Version 4.0 and above (optional)**

FOR MORE INFORMATION

For more information about Cisco and NAC, visit: www.cisco.com/go/nac

For more information about Trend Micro and NAC, visit: www.trendmicro.com/en/partners/alliances/cisco/nac/overview.htm

CISCO SYSTEMS INCORPORATED
CORPORATE HEADQUARTERS
170 West Tasman Drive
San Jose, CA, 95134, USA
toll free: +1-800-553-NETS (6387)
phone: +1-408-526-4000
fax: +1-408-526-4100
www.cisco.com

TREND MICRO INCORPORATED
AMERICAS HEADQUARTERS
10101 N. De Anza Blvd.
Cupertino, CA, 95014, USA
toll free: +1-800-228-5651
phone: +1-408-257-1500
fax: +1-408-257-2003
www.trendmicro.com



**TREND
MICRO**

