

# Network Admission Control— Trend Micro™ and Cisco Systems®

## A Strategy for Comprehensive Network Security Policy Enforcement

### Solution Guide

#### BENEFITS OF TREND MICRO and CISCO NAC SOLUTIONS

- Provides automatic enforcement of corporate security policies, on all endpoints, regardless of access method
- Integrated antivirus and network policy enforcement controls client access and helps minimize external and internal threats
- Trend Micro OfficeScan management console enables central deployment of Cisco NAC client components
- Automated remediation to noncompliant endpoints using HCAP and the Cisco Secure ACS expedites user's ability to obtain network access
- Integrated security infrastructure increases network availability, resilience, and productivity
- IT costs are lowered by maximizing the return on investment in an organization's network infrastructure and software, easing administrative burden and helping to ensure business continuity

#### PROBLEM

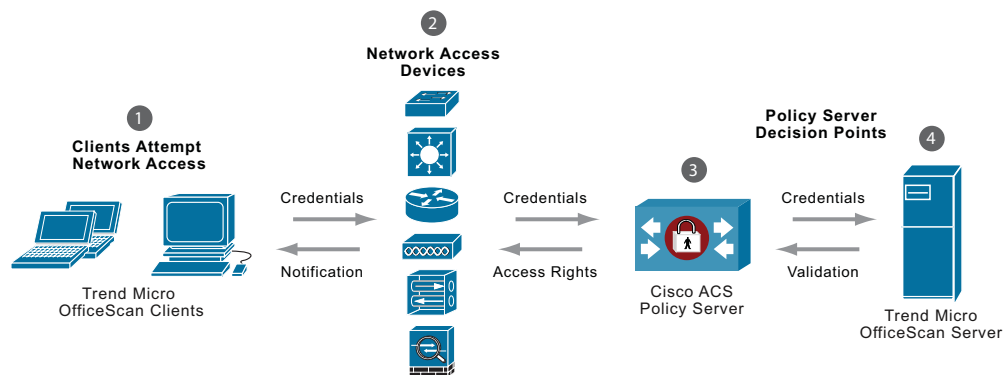
Viruses, worms, and hackers continue to attack networks and disrupt business. While file-based viruses spread when users open infected e-mail attachments, worms and network viruses self-launch through operating system vulnerabilities. The unprepared network is open to assault when users with outdated patches or unprotected devices log on.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 Network Admission Control (NAC), an industrywide, 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 based on Trend Micro OfficeScan 7.0 (also OfficeScan Corporate Edition 6.5) integrated with the Cisco Trust Agent and Cisco Secure Access Control Server (ACS). This solution runs over a Cisco infrastructure, and allows organizations to enforce system compliance and remediation before allowing access to network resources and data. Enterprises using 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. 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 solution and includes Trend Micro OfficeScan Corporate Edition 7.3. 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.



#### How the Trend Micro and Cisco Offering Works

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.



# Trend Micro and Cisco NAC

## INTEGRATED SECURITY AND NETWORKING INFRASTRUCTURE

The Cisco NAC initiative focuses on controlling threats to the network by enforcing admission privileges. NAC enables endpoint devices to communicate with the network about their security status relative to defined corporate security policy. Network access is granted only to devices that comply with corporate security policy, including antivirus security policies.

Through its NAC integration, Trend Micro OfficeScan provides the Trend Micro Policy Server to communicate antivirus information about user devices to Cisco Secure ACS, and allows the ACS to determine whether devices should be allowed on the network. The Cisco network access device enforces the access decision (allow, deny, restrict, or quarantine) made by Cisco Secure ACS.

Trend Micro OfficeScan allows for easy and automated distribution of the Cisco Trust Agent with the installation of the OfficeScan Client. OfficeScan also supports the Host Credential Authorization Protocol (HCAP) and can provide automatic policy updates on the Cisco Secure ACS while automated endpoint remediation provides cost savings and allows for increased productivity. Nonsupported solutions require end users to either manually install updates on their computers, or contact the company's IT department for support.

## SUPERIOR NETWORK SECURITY FROM INDUSTRY LEADERS

The synergy between the Cisco Self-Defending Network strategy and Trend Micro Enterprise Protection Strategy (EPS) helps ensure the development of fully interoperable solutions that help customers maximize their investments in software and network infrastructures to identify, prevent, and adapt to security threats.

The Trend Micro EPS security approach combines multiple layers of products and services—for intelligent, comprehensive protection against known and unknown threats. EPS includes innovative solutions that monitor customer-specific networks while accurately detecting unknown threats in real time. Tightly integrated, centrally managed security helps extend IT resources and decrease costs with quick, consistent deployment of outbreak management policies networkwide. Trend Micro OfficeScan is the desktop and endpoint protection component of the EPS.

The Cisco NAC solution uses the network infrastructure to enforce security policies on all devices seeking to access network computing resources. NAC helps ensure that all hosts comply with the latest corporate security policies, such as antivirus, security software, and operating system patch, prior to obtaining normal network access. Vulnerable and noncompliant hosts are isolated (quarantined) or given limited access until they reach compliance. In addition, Cisco NAC has the ability to perform user authentication at the network level so that only devices with proper user credentials are permitted network access. Cisco NAC is core to the Self-Defending Network, Cisco's strategy to dramatically improve the network's ability to identify, prevent, and adapt to security threats.

With the comprehensive protection across security and networking domains offered by Trend Micro and Cisco Systems, organizations can block noncompliant devices from access, prevent threats from exploiting vulnerabilities on the network, contain and eliminate worms and viruses, and centrally deploy outbreak security actions to pre-empt or diffuse attacks.

"Recent worm and virus infections have made client security policy enforcement a top priority for enterprises today. Many organizations fall victim to exploits when mobile or guest users connect infected devices directly to internal LANs. Eliminating this threat requires strengthened policies and network admission control technology."

— Mark Bouchard,  
Senior Program Director,  
META Group

## CISCO SYSTEMS INCORPORATED

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at [www.cisco.com](http://www.cisco.com)

### 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

## 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](http://www.trendmicro.com)

For more information about Cisco and NAC, including current system requirements, visit:

[www.cisco.com/go/nac](http://www.cisco.com/go/nac)

For more information about Trend Micro and NAC, including current system requirements, visit:

[www.trendmicro.com/en/partners/alliances/cisco/nac/overview.htm](http://www.trendmicro.com/en/partners/alliances/cisco/nac/overview.htm)