

Protect Desktop and Servers with Cisco and Trend Micro Endpoint Security Solutions

White Paper

WHY CISCO AND TREND MICRO

Organizations want to protect their desktops and servers while controlling the costs of deploying and maintaining a secure network. Cisco and Trend Micro each provide a complete solution that prevents worm and virus attacks, theft of information, inadvertent release of information, and application misuse. They are easily centrally provisioned, administered, and managed as part of the overall Self-Defending Network. Together, the Cisco Security Agent and Trend Micro OfficeScan increase productivity by:

- Preventing and mitigating attacks from known and unknown worm and viruses
- Repelling spyware, Trojans, and hacker attacks
- Automatically enforcing endpoint security policies
- Tracking information access and flow throughout the organization
- Cleaning endpoints of all worms, viruses, and spyware
- Restoring infected endpoints to normal operation after an outbreak
- Eliminating the need for continuous, reactive patch management

Securing laptops, desktops, and servers is an essential part of any organization's security strategy. With thousands of these devices in an enterprise network, endpoint security solutions must be comprehensive, easy to administer, and integrated into the existing computing, network, and security infrastructure.

SUMMARY

Laptops, PDAs, desktops, and servers (collectively referred to as "endpoints") are the elements most targeted in attacks on an organization's network. They are also the origin of most security breaches, both deliberate and unintentional. As the speed and severity of security breaches increases, one compromised endpoint can quickly affect the entire organization. Endpoint security must be proactive and automatic. At the same time, some of the biggest security challenges facing organizations today are a fragmented security strategy, poor integration across security products and a shortage of security staff available to manage them. Cisco® and its partners provide endpoint security solutions as part of a comprehensive security strategy. Cisco Security Agent and Trend Micro Office Scan are proven endpoint security solutions integrated seamlessly into the Cisco Self-Defending Network. A self-defending network integrates security into all parts of the network, allowing organizations to use their existing investments in computing, network, and security infrastructures while reducing their IT burden and lowering the total cost of ownership.

ENDPOINT SECURITY CHALLENGES

Keep the Bad Guys (and Bad Things) Out

An effective security policy protects endpoints from external attacks that threaten the organization. Worms and viruses are the most common external threats. The effects of worm and virus outbreaks on organizations range from bad to worse—lost productivity, lost or corrupted data, even lost sales. While corporate anti-virus solutions do an excellent job of catching and eliminating known worms and viruses, they can still be foiled by new, unknown worms or viruses: the "day zero" class of threats. Meanwhile, the burden to ensure that all endpoints have the latest anti-virus updates falls to security managers and users.

Worms and viruses are not the only attacks that threaten endpoints. Hackers often target large corporations to steal information, exact revenge, or earn bragging rights. Attacks may come directly from hackers, who target a particular server. Attacks may also be indirect, through software inadvertently installed on endpoints by users. In particular, spyware is a growing problem for many organizations. Many spyware or adware programs install other programs, increasing the risk that "zombie" or "Trojan horse" programs can infiltrate and infect endpoints.

Compounding the problem, most anti-spyware products are still in their infancy, limiting their effectiveness or ease of use.



Protect Desktop and Servers with Cisco and Trend Micro Endpoint Security Solutions

While not intended to attack organizations, more benign software can still threaten an organization's productivity. For example, adware consumes endpoint computing or network resources, resulting in more calls to the help desk.

Let the Good Guys In

Security policy also encompasses user and device access control. An effective access control policy allows only trusted users using trusted devices to connect to the network. Trusted devices are free of viruses, other malicious programs, or unsupported software, and are provisioned with appropriate and up-to-date security software and operating system patches.

Keep Confidential Information In

Organizations are more accountable than ever for the veracity or confidentiality of their information. Worldwide, new regulations such as Health Insurance Portability and Accountability Act (HIPAA) in the United States and the European Union directives on privacy and data protection are placing more requirements on organizations to protect their data. Organizations and their security staffs must not only keep confidential information within the organization, but must also demonstrate, through audits, that confidential information has not been compromised. The dynamic nature of today's networks makes security policy enforcement more challenging. Mobile workers, contractors, wireless access points, and supplier and partner extranets enhance organizational productivity, but complicate security. How can an organization's security staff ensure its productive, accessible environment does not actually increase the risk of attack? And how do they keep sensitive information from leaving the enterprise, either intentionally or accidentally?

Is the Security Cure Worse than the Disease?

With the type and frequency of attacks mounting and regulatory environments changing, organizations recognize the need to be vigilant about network security—but they worry that security spending won't solve the problem. At the

same time, two of the biggest security challenges facing organizations today are poor integration across security products, and a shortage of security staff available to manage them. Overburdened IT workers are so busy applying server updates, managing the flood of new security products, and enforcing user and endpoint security policies that they neglect the parts of their jobs that would make the organization more productive. By definition, any satisfactory security solution must be less costly to handle than the security breaches it is trying to prevent. Ideal endpoint security solutions are proven, easily administered, and integrate with existing programs and the organization's network environment

SOLUTION—ENDPOINT SECURITY SOLUTIONS INTEGRATED INTO A LAYERED NETWORK DEFENSE

Attacks or security breaches happen in seconds. Security systems must act instantly and automatically. Any security system must aggressively address endpoint network security, since endpoints are usually both attack targets and originators of security breaches. Security intelligence integrated into the network keeps infections from spreading and automatically enforces security. Security integrated into all aspects of the network can quickly identify, prevent, and adapt to security threats. Endpoint security and network security should work together to make the entire network secure and self-defending.

The Cisco Self-Defending Network

The Self-Defending Network (SDN) is Cisco's vision for integrated network security. In a Self-Defending Network, security is integrated into every endpoint, router, switch, and wireless access point. This allows the network to recognize potential suspicious activity, identify threats, react appropriately, isolate infections, and respond to attacks in an adaptable, coordinated way. Cisco SDN solutions can be centrally provisioned, managed, and monitored, thereby reducing the burden on IT and lowering the total cost of

Protect Desktop and Servers with Cisco and Trend Micro Endpoint Security Solutions

ownership. Cisco SDN endpoint solutions integrate seamlessly with overall network security through solutions such as the Network Admission Control (NAC) program, a Cisco-led industry initiative that uses the network infrastructure to help reduce the threat of worms, viruses, and other security threats.

Enforce Endpoint Security Policy with Network Admission Control

In many cases, users are responsible for keeping their desktops and laptops updated with the latest antivirus updates and operating system patches. This leaves a crucial part of enterprise security in the hands of thousands of individuals. Users may find downloading updates cumbersome, or simply forget, especially when they travel or are away from the office. Meanwhile, their systems are vulnerable to worms, viruses, and other attacks. A single laptop with outdated software threatens the entire organization.

NAC uses the network infrastructure to enforce security policy on all devices attempting to access the network. Using NAC, IT organizations can choose to grant network access only to trusted endpoints that can verify their compliance to network security policies, such as having the latest antivirus update, operating system version, or patch update. NAC can permit, deny, or restrict network access to any device as well as quarantine noncompliant devices. By automatically enforcing security policies, NAC reduces the security burden. IT staffs no longer need to remind users to install updates, greatly reducing the risk of attack.

NAC works in conjunction with:

- Third-party antivirus solutions such as Trend Micro OfficeScan
- Cisco Security Agent

Within the Cisco SDN architecture, these two complementary endpoint security solutions provide unparalleled security coverage.

Trend Micro OfficeScan

Trend Micro OfficeScan is a client/server security solution that integrates the core capabilities of multiple security technologies. OfficeScan includes enhanced antivirus protection (including protection from spyware, adware, and hoaxes) and provides high-performance, network-layer virus scanning, personal firewall capabilities, and the Trend Micro Enterprise Protection Strategy (EPS), which proactively protects endpoints and networks through each stage of a virus lifecycle. EPS performs vulnerability assessments, prevents outbreaks from spreading, removes threats from infected systems, and automatically cleans up and restores infected systems and networks.

To prevent e-mail viruses or other attachments from being delivered to endpoints, OfficeScan offers POP3 Mail Scan or Outlook Mail Scan options, which can be activated on OfficeScan client machines. A Web-based management console enables security staff to easily control how desktops and laptop clients receive new security policies and software updates. Security staff can also grant, deny, or limit the ability of OfficeScan users to change their client configurations.

Cisco Security Agent

Cisco Security Agent uses behavior-based assessment to identify and prevent malicious behavior on endpoints. It analyzes system behavior, and can terminate both known and unknown ("Day Zero") security risks based on this behavior. Cisco Security Agent aggregates multiple security functions by providing a Host-based Intrusion Prevention System (HIPS) distributed firewall capabilities, spyware prevention, malicious mobile code protection, operating system integrity assurance, and audit log consolidation, in a single powerful software package. All Cisco Security Agent policies and activity are easily configured and monitored from a central location through the CiscoWorks VPN/Security Management Solution (VMS).

Protect Desktop and Servers with Cisco and Trend Micro Endpoint Security Solutions

Prevent Worm and Virus Outbreaks on Endpoints

Known and unknown worms and viruses are the most common security breaches for organizations today. Known worms and viruses have been identified and antivirus signature updates have been created to repel them. But just because they have an antidote doesn't mean they aren't dangerous. Virus updates still need to be applied to 100 percent of the organization to be effective. One study predicted that through 2005, 90 percent of all cyberattacks will exploit security flaws for which a patch is available or a solution is known. Re-infection by known worms and viruses is a problem today. Clever infections update registry keys and infect both files and memory in several places. If an endpoint is not totally cleaned of an infection, it will quickly re-infect itself and potentially other devices.

Trend Micro OfficeScan software identifies and eliminates or neutralizes known viruses, worms, and spyware threats. OfficeScan's unique network-level scanning of all packets identifies worms and viruses before they reach host computers. Trend Micro antivirus software is updated automatically from TrendLabs™, a global network of antivirus research and product support centers, ensuring endpoints are protected from newly diagnosed threats ("in the wild") as quickly as possible. If an endpoint does get infected, Trend Micro software quarantines other machines from the outbreak within seconds, and completely self-cleans all infected machines. Unknown or "Day-Zero" worms and viruses are on the rise, and represent a significant threat to endpoints. Cisco Security Agent protects against day-zero attacks by continually monitoring endpoint applications for unusual or unexpected behavior, and correlating any anomalies across the entire network. For example, while the Slammer worm infected thousands of computers within minutes of its release, Cisco Systems was unaffected. All Cisco endpoints run Cisco Security Agent. Cisco Security Agent identified "unusual" behavioral patterns at several points in the Cisco network within seconds of the arrival of the first anomalous packet at a server. Seconds later, without any intervention

from security administrators, Cisco Security Agent's default configuration settings stopped Slammer from affecting Cisco endpoints. In situations like this, Cisco Security Agent can be not only adaptive and responsive, but also flexible. For example, during emergency situations when the network is under attack, Cisco Security Agent can revert to tighter, pre-programmed security controls.

Prevent Theft or Release of Information from Endpoints

The theft of organizational information happens in many ways. It may be as simple as a trusted employee forwarding a file by mistake, not necessarily for profit or revenge. It may be an outside hacker trying to gain control of a server via a Trojan program. Or it may involve spyware; software that attempts to steal sensitive information or intellectual property by recording keystrokes and viewing URLs or opening documents on a user's machine.

Together, the Cisco Security Agent and Trend Micro OfficeScan thoroughly protect against information theft. Cisco Security Agent's Host-based Intrusion Prevention System (HIPS) identifies and stops attempts to hack into endpoints. Cisco HIPS accurately identifies, classifies, and stops malicious or damaging traffic in real time. Cisco HIPS intelligence analyzes all traffic moving across the network, recognizes an attack's behavior, analyzes its severity, raises appropriate alarms to network managers, and takes corrective action.

Trend Micro OfficeScan identifies and removes all types of spyware and Trojans from desktops and laptops. OfficeScan's anti-spyware updates, like its antivirus updates, are frequent and automatic. OfficeScan conducts real-time scans of all data being written to or read from disk, comparing data against signatures of known spyware. Regularly scheduled scans periodically check hard disks for spyware that may have slipped through before its signature was available. An optional service integrated with

Protect Desktop and Servers with Cisco and Trend Micro Endpoint Security Solutions

OfficeScan removes the spyware and restores user settings. Likewise, Cisco Security Agent uses its behavior-based algorithms to detect and block installation of both known and unknown spyware. Once detected, items can be safely removed with OfficeScan.

To prevent confidential information from leaving the organization, Cisco Security Agent implements policy control on all endpoints in an organization. Cisco Security Agent policy control can manage where data is stored and which endpoints can access it. It prevents data from being copied or sent outside the organization. It can also limit what types of devices are used on the network. For example, if organizations are concerned about the portability of information on certain servers, Cisco Security Agent can restrict the use of USB keys on those computers.

Information does not have to be stolen. Sometimes it is released inadvertently when security policies are not followed. For example, one company bought some second-hand servers on an auction Website. Once they received and installed the servers, they discovered that the server hard drives had not been erased before the sale. Each server contained thousands of confidential health records. Cisco Security Agent can help prevent these security breaches from happening by restricting which data is copied to which endpoints, while providing audit logs that track where sensitive information resides on the network.

Prevent Application Abuse or Misuse

Laptops and other mobile endpoints have increased enterprise productivity, but they have created new security challenges. For example, some users take their laptops home and install their own personal programs, which then interfere with the operation of enterprise applications. System administrators have to spend time fixing the laptop and uninstalling applications. Cisco Security Agent can prevent these problems by limiting both the type and versions of applications that can run on corporate-owned endpoints.

Similarly, many workers use their corporate-owned endpoints to surf the Internet outside of office hours. Certain Websites install adware or spyware automatically on computers, affecting productivity, wasting computer resources, or even posing a security risk. OfficeScan together with Trend Micro's Damage Cleanup Services removes any spyware or adware that might have found its way onto the endpoint.

Improve Productivity of Security Teams

OfficeScan and Cisco Security Agent both reduce the management and administrative burden on enterprise IT security staff. Through its flexible Web-based management console, IT security staff can ensure OfficeScan configuration changes and antivirus signature updates are automatically delivered to endpoints, with no user intervention required. Computers that are turned off or disconnected from the network are quickly updated when they re-attach to the network via the OfficeScan Server, or they may receive updates from the TrendLabs server if users are traveling. Rather than sending a new file, pattern updates and configuration changes are changed incrementally, maximizing computer and network efficiency. Once devices reconnect to the enterprise network, OfficeScan verifies the updates were deployed successfully.

OfficeScan keeps comprehensive logs of virus incidents, events, and updates, allowing IT security staff to assess the success of the organization's security policies or identify devices at greater risk of infection. With this information, IT security staff takes targeted action rather than a blanket approach, sparing precious staff resources.

Operating system (OS) and application software security patches and hot fixes are a fact of life. Distributing, downloading, and testing continuous software patches is a laborious and time-consuming task for IT security staff. They must test and verify that each patch does not adversely affect other programs. Manually managing OS and software

Protect Desktop and Servers with Cisco and Trend Micro Endpoint Security Solutions

application patches costs an estimated \$300 per server per patch. With Cisco Security Agent, IT security groups can approach updates in a more efficient, structured manner, and increase their productivity. Cisco Security Agent is always protecting endpoints and never needs signature updates. Because the network is secure, IT staff can take the time to test patches properly, rather than frantically trying to update all servers before an attack is launched. They can then install patches in groups, on a schedule, thereby freeing them from unpredictable and inefficient patch management. Governmental regulation and industry practice mandate data protection and confidentiality in many sectors. To maintain integrity of information and avoid legal and financial liabilities, organizations will have to demonstrate their compliance to security and privacy regulations. Cisco Security Agent can expedite this process by providing audits by application, user, or server.

ADDITIONAL RESOURCES

For more information on the Cisco Security Agent, please contact your Cisco representative or visit www.cisco.com/go/csa

For more information on the Network Admission Control program, please visit www.cisco.com/go/nac

For more information on Trend Micro's OfficeScan please visit www.trendmicro.com/en/products/desktop/osce/evaluate/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