

Trend Micro™ Network VirusWall™

Outbreak Prevention Appliance

PROBLEM:

Network viruses (e.g., Internet worms), viruses that propagate from machine to machine at the network layer, have become rampant and unstoppable over the last couple of years due to an increasing number of software vulnerabilities. Current security solutions such as antivirus, firewall, vulnerability assessment, and intrusion detection and prevention systems are unable to stop these network viruses and as a result, the estimated worldwide damages from network viruses such as SQL Slammer, MSBlaster.A, and Nachi have skyrocketed to \$2.15B in 2003.¹ The network virus problem is exacerbated by a growing number of unprotected and unmanaged devices accessing the network from multiple entry points and the decreasing window of time between patch availability and virus attack. For example, when MSBlaster.A struck in August 2003, this window of time was a mere 26 days as compared to the 336 days for Nimda in October 2000.²

PRODUCT DESCRIPTION:

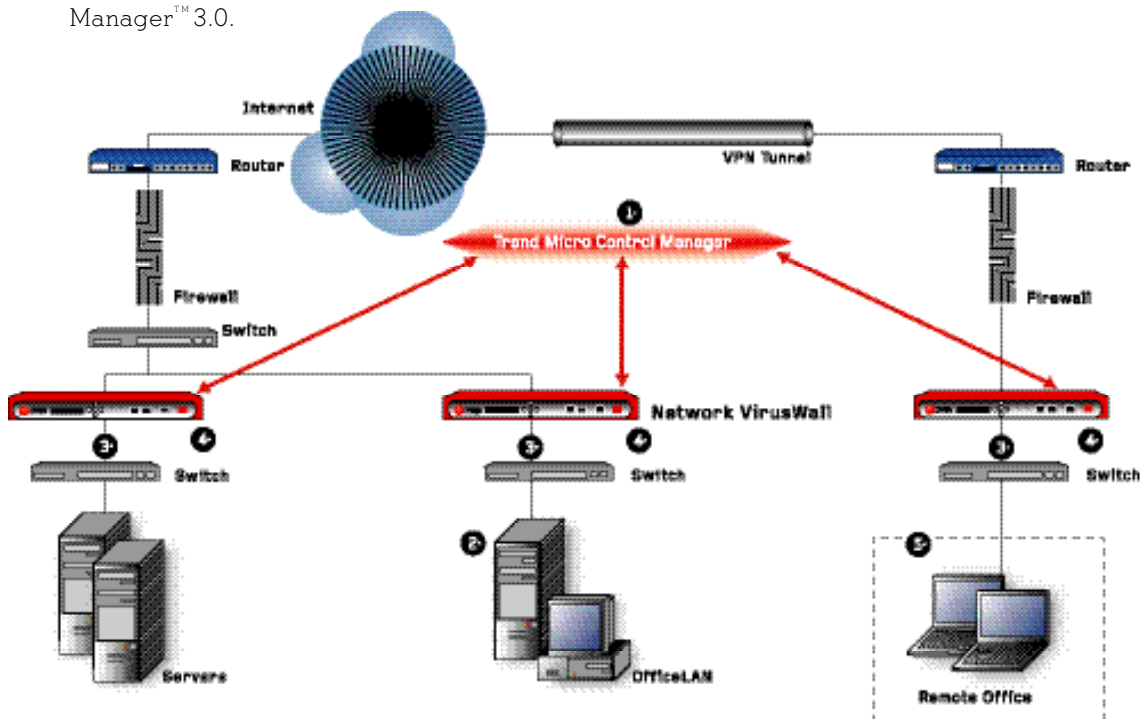
Trend Micro™ Network VirusWall™ is an outbreak prevention appliance that helps organizations stop network viruses (e.g., Internet worms), block high threat vulnerabilities during outbreaks, and quarantine and clean up infection sources including unprotected devices as they enter the network, using threat-specific knowledge from Trend Micro deployed at the network layer. Unlike security solutions that only monitor threats or provide threat information, Network VirusWall helps organizations take precise outbreak security actions and proactively detect, prevent or contain, and eliminate outbreaks. By deploying Network VirusWall in network LAN segments, organizations can significantly reduce their security risk, network downtime, and outbreak management burden. Network VirusWall supports the Trend Micro™ Enterprise Protection Strategy and is managed by Trend Micro Control Manager™ 3.0.

KEY BENEFITS

- Helps lower security risk by enforcing antivirus security policies consistently across the organization and pinpointing cleanup of sources of infections on the network
- Minimizes network downtime by blocking high-threat vulnerabilities and preventing or localizing the attacks in the event of an outbreak
- Eases outbreak management burden by receiving threat-specific expertise from Trend Micro's award-winning global network of security experts, that can be easily and consistently deployed across the network segment(s)

1. Source: Computer Economics, September 2003

2. Source: TrendLabs research



- 1- Early warning of internal network outbreak
- 2- Unpatched machine sheltered
- 3- Outbreak prevention policies deployed
- 4- Network virus signatures deployed
- 5- Machine quarantined & cleaned
- 6- Non-compliant machine blocked & remediated



KEY FEATURES:

Network VirusWall is an outbreak prevention appliance that sits inline to traffic in network LAN segments and offers the following features:

Vulnerability Isolation¹:

- Helps prevent viruses from exploiting vulnerabilities on the network by equipping organizations to selectively isolate vulnerable (e.g. - unpatched) machines for specific high-threat vulnerabilities² before an attack or as an attack occurs
- Designed to minimize network traffic congestion by not allowing unpatched machines to infect machines in other network segments during outbreaks

Network Outbreak Monitoring:

- Enables organizations to take proactive and timely security measures by providing early warning information of outbreaks in the network segment(s) using heuristics
 - Monitoring methods include but are not limited to analyzing traffic flow delta, number of connections initiated to and from a single client at any given time, sudden increases in traffic through specific ports or protocols (TCP, UDP, ICMP, and IGMP)
 - Identifies infected host machines, virus attack targets, and attacks on specific vulnerabilities and notifies IT managers through TMCM 3.0

Network Outbreak Prevention³:

- Prevents or contains network viruses with timely, granular, threat-specific prevention policies from TrendLabsSM that can be deployed at the network LAN segment(s) to block one or a combination of the following in the event of an outbreak:
 - Range of or specific IP addresses (to prevent these machines from infecting machines outside of the LAN segment), ports, and protocols (TCP, UDP, ICMP)
 - Instant Message Channels (AIM, MSN, Yahoo, ICQ)
 - File type extensions
 - File Transfers (FTP, HTTP, Windows file sharing)
 - Deployment of these policies can be automated to maximize protection or manually deployed to provide greater control and flexibility
- Isolates and contains spread of infections by not allowing infections in or out of the affected LAN segment, thereby keeping rest of the network up and running

Network Scanning and Detection

- Eliminates viruses (e.g., Internet worms) propagating at the network layer by scanning and detecting using network signatures from TrendLabs and by dropping infected packets, while antivirus products scan for viruses at the application layer and not the network layer.

Automated Damage Cleanup⁴:

- Helps prevent re-infections by targeting sources of infection on the network and isolating them until cleanup
- Designed to minimize cost and administrative burden associated with manual cleanup and restoration by automating agent-less, remote cleanup of infected host machines with damage cleanup templates from TrendLabs
- Damage cleanup includes cleanup of or fixing of unwanted registry entries created by worms or Trojans, memory resident worms or Trojans, garbage and viral file drop by worms or Trojans, and system file configuration such as system.ini, after it has been infected or altered by viruses

Security Policy Enforcement:

- Enables organizations to enforce antivirus security policies and minimize network infections and re-infections by
 - Detecting antivirus client products (Symantec, Network Associates and Trend Micro) and latest scan engine and pattern files (Trend Micro) as users access the network, blocking network access, if not in compliance, and enabling users to update antivirus scan engine and pattern files or download antivirus products per company's security policies
- Detects Symantec - Norton Antivirus Corporate Edition, NAI - McAfee VirusScan 7.0 with ePolicy Orchestrator agent and Trend Micro OfficeScan and ServerProtect for NT
- Does not require installation of host-based agents, program updates or changes to network configuration

Ease of Use, Manageability, and Security Control:

- Integrated appliance provides ease of use, configuration, installation, and management
- SNMP Monitoring provides enhanced manageability and viewing capabilities
- A built-in local host firewall helps prevent attacks to the Network VirusWall appliance
- ActiveUpdate and Trend Micro Control Manager 3.0 delivers periodic and automated threat-specific updates to Network VirusWall
- Trend Micro's award winning global support organization or certified channel partners deliver high-quality support services

SYSTEM REQUIREMENTS

Box Contents:

- One Network VirusWall 1200 Appliance
- One Power Cord
- One Ethernet Crossover Cable (Crossover CAT-5 Cable with RJ-45 Connectors)
- One Console Cable
- Two Keep Ears & Screws
- Trend Micro Solutions CD for Network VirusWall 1200
- One Quick Installation Guide
- One Warranty Card

CONFIGURATION REQUIREMENTS:

- All box contents
- Two Ethernet Cables (Standard CAT-5 Cable with RJ-45 Connectors)
- Connect the INT Port of Network VirusWall 1200 to the Switch/Hub that you want to establish as your protection segment
- Connect the EXT Port of Network VirusWall 1200 to the Switch/Hub that this protection segment originally connects to
- At least one TCMC server version 3.0 installed with a valid service activation code
- At least one Windows-based computer with a CD-ROM Drive⁵
- A HyperTerminal program to connect to the Console Port through Console Cable⁵

1. Requires Trend Micro™ Vulnerability Assessment
2. Currently identifies major Microsoft vulnerabilities only
3. Requires Trend Micro™ Outbreak Prevention Services (included with Network VirusWall)
4. Requires Trend Micro™ Damage Cleanup Services (included with Network VirusWall)
5. A CD-ROM drive is only required if you want to install TCMC server to configure your Network VirusWall 1200 or access the documentation.
6. A HyperTerminal program is only required if you want to use the console mode to configure Network VirusWall 1200.

TrendLabsSM

24X7 ANTIVIRUS SUPPORT

Trend Micro products are backed by timely, high-quality service from TrendLabs™, a global network of five regional antivirus research and support centers with an ISO9001:2000-certified & COPC-2000 Standards-certified headquarters. A team of more than 250 engineers and antivirus specialists operate around the clock to monitor virus activity, develop information on new threats, and deliver prompt, effective strategies.

For more information about Trend Micro service and support, contact TrendLabs at <http://www.trendmicro.com/trendlabs>.

TREND MICRO

ENTERPRISE PROTECTION STRATEGY

Trend Micro™ Enterprise Protection Strategy is a customer-driven approach designed to manage the outbreak lifecycle, from vulnerability prevention to malicious code prevention and elimination. Through coordinated delivery of industry-leading products, services, and threat-specific expertise from Trend Micro's global network of security experts, Enterprise Protection Strategy helps organizations prevent viruses from exploiting vulnerabilities on the network, enforce security policies to control network access of devices, prevent or contain and eliminate viruses and remnants spreading through application and network layers, and centrally manage and integrate outbreak security actions. Enterprise Protection Strategy has helped customers worldwide prevent malicious code attacks and minimize outbreak-related costs and damages

TREND MICRO INCORPORATED

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