

Trend Micro™ Network VirusWall™ 300

Outbreak Prevention Appliance for Mission-Critical Devices

PROBLEM

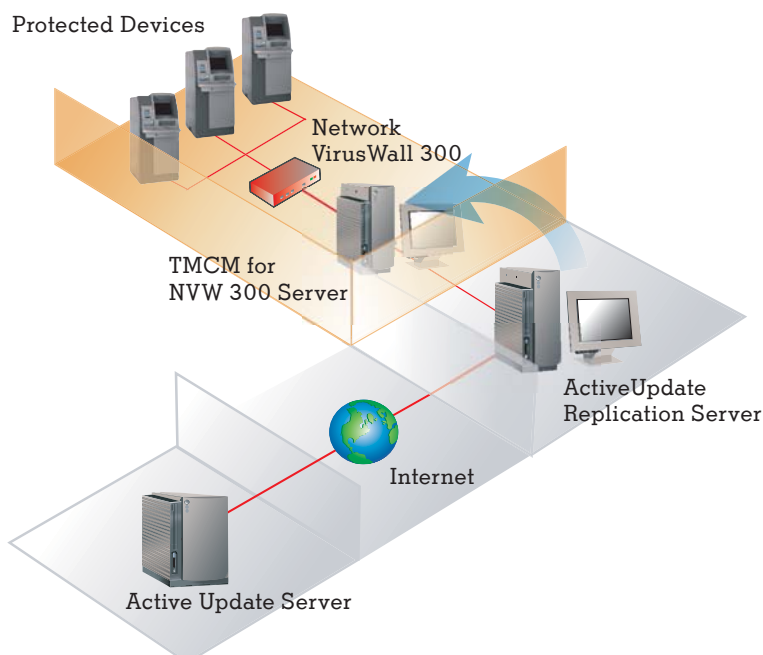
Mission-critical devices, including ATM machines, self-service kiosks, and medical devices, are migrating from proprietary operating systems and closed networks to take advantage of popular operating systems and open Internet Protocol (IP) networks. The new devices improve business performance and cost less to operate; however, they are vulnerable to attack from network worms. Any infected device that plugs into your IP network can result in lost revenues and dissatisfied customers. For example, in 2003 the SQL Slammer network virus prevented customers of a US bank from withdrawing money from ATMs while the Nachi network virus delayed or cancelled flights at a Canadian airline. Security products such as desktop or host-based antivirus, firewalls, and intrusion detection systems cannot effectively stop network worms from propagating to remote devices, which can degrade network performance and take devices offline. Mission-critical devices need protection to offset the risks of malicious network worms.

SOLUTION

Trend Micro™ Network VirusWall™ 300 is an outbreak prevention appliance designed to protect mission-critical devices such as ATMs from network worms and to clean up infected devices. Because there are no hardware or software compatibility issues with the appliance, enterprises can deploy Network VirusWall 300 to protect any IP-enabled device. Unlike security solutions that monitor threats or provide threat information only, Network VirusWall 300 deploys threat-specific knowledge from TrendLabs™ at network end points to help organisations proactively detect, prevent or contain, and eliminate outbreaks. Network VirusWall appliances help organisations improve their operational resilience by mitigating security risks, easing the virus outbreak management burden, and reducing system downtime.

KEY BENEFITS

- Improves operational resilience by preventing network worms and intrusions (unauthorised access) from reaching mission-critical devices
- Centralised management ensures consistent deployment of the latest security updates and flexible configuration manages threats by risk
- Automated outbreak prevention and damage clean-up services mitigate outbreaks and reduce the cost of recovery
- Appliance form factor avoids hardware and operating system compatibility, stability, and performance concerns
- Integrates with major SNMP frameworks to enhance system and network management investments



Trend Micro™ Network VirusWall™ 300 Prevents Attack.

Network VirusWall 300 blocks worms at network end points to prevent infection from spreading to mission-critical devices such as ATMs, self-service kiosks, and medical devices.

Trend Micro Network VirusWall 300

KEY FEATURES

NETWORK WORM PREVENTION AND ELIMINATION

- Scans network traffic to detect and eliminate infected network packets, based on the latest network signatures and outbreak prevention policies from TrendLabs™
- Supports Trend Micro™ Enterprise Protection Strategy for proactive outbreak management and includes Trend Micro™ Outbreak Prevention Services and Trend Micro™ Damage Cleanup Services
- Outbreak prevention policies may be deployed automatically or manually to block virus transport mechanisms including specific IP addresses/range; ports and protocols (TCP, UDP, ICMP); instant message channels (AIM, MSN, Yahoo, ICQ); file type extensions; and file transfers (FTP, HTTP, Windows file sharing)
- Minimises manual clean up with automatic, agent-less, remote clean up of infected host devices (for most popular operating systems) including removal of unwanted registry entries created by virus remnants or Trojans, and restoration of system file configuration (i.e. system.ini)
- Firewall helps prevent unauthorised access by controlling incoming or outgoing network traffic according to specified source IP, protocol, destination IP, and destination port(s), and takes corresponding actions based on specific user-defined rules

FLEXIBLE, CENTRALISED MANAGEMENT AND EASE OF DEPLOYMENT

- Coordinated, automatic deployment of security updates and prevention policies is managed from Trend Micro Control Manager™ for Network VirusWall 300, an easy-to-use Web-based management console
- For maximum protection from the latest threats, TrendLabs™ ActiveUpdate server can be mirrored locally to accelerate security updates and clean up of malicious code
- Real-time client status monitoring and event notification deliver network-wide client status without latency
- Supports integration with Simple Network Management Protocol (SNMP) frameworks such as IBM Tivoli and HP OpenView to extend management capabilities
- Firewall can be configured at various security levels to manage threats according to risk
- Outbreak prevention appliance sits in-line with network traffic to ease deployment and provide comprehensive protection

SYSTEM REQUIREMENTS

Box Contents

- One Network VirusWall 300 appliance
- One Power cord
- One Ethernet cable (straight CAT-5 cable with RJ-45 connectors)
- Trend Micro Solutions CD for Network VirusWall 300
- Trend Micro Getting Start Guide
- Safety Recommendations and Warning Card

Configuration Requirements

- All box contents
- Two or more Ethernet cables (standard CAT-5 Cables with RJ-45 connectors): one to connect to the external network segment and the other(s) to the end point device(s)
- One Microsoft™ Windows™-based computer for the Trend Micro Control Manager™ for Network VirusWall 300 Server. Note: A CD-ROM drive is required on this machine only to install Control Manager, configure the appliance, or access the documentation on CD.
- A Web browser for pre-configuring Network VirusWall 300

TECHNICAL HARDWARE REQUIREMENTS

Physical

Height: 1.18" (30mm)
Depth: 5.12" (130mm)
Width: 8.46" (215mm)
Weight: 1.58 lbs. (0.72Kg)

Throughput

Maximum Throughput: 30 Mbps

Ethernet

Internal Port: 4 x 10/100 Base-T Ethernet RJ-45 port, auto-negotiation and auto MDI/MDI-X support

External Port: 1 x 10/100 Base-T Ethernet RJ-45 port, auto-negotiation and auto MDI/MDI-X support

USB

USB ports: USB 2.0

Power Adaptor

Input: AC voltage 100–240 V
Output: DC voltage 12V, 1.5A

Operating condition

Temperature: 32–113°F (0–45°C)
Humidity: 35%–85%

Non operating condition

Temperature: -4–113°F (-20–45°C)
Humidity: 5%–90%

TrendLabs™

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 and COPC-2000 Standards-certified headquarters. A team of more than 300 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 www.trendmicro-europe.com/trendlabs

ENTERPRISE PROTECTION STRATEGY

Trend Micro™ Enterprise Protection Strategy (EPS) is designed to deliver comprehensive protection at both application and network layers to proactively manage the outbreak lifecycle, from vulnerability prevention to malicious code prevention and elimination. Through coordinated delivery of Trend Micro's industry-leading products, services, and threat-specific expertise from TrendLabs™, EPS helps organisations minimise outbreak-related costs and damages.

TREND MICRO

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services, focused on helping customers prevent and minimise the impact of network viruses and mixed-threat attacks through its award-winning Trend Micro™ Enterprise Protection Strategy. Trend Micro has worldwide operations and trades stock on the Tokyo Stock Exchange and the NASDAQ.

Trend Micro (UK) Limited

Pacific House
Third Avenue
Globe Business Park
Marlow
Buckinghamshire
SL7 1YL
England
Tel: +44 (0) 1628 400500
Fax: +44 (0) 1628 400511

www.trendmicro-europe.com