Trend Micro

Network VirusWall™ Enforcer

Prevent network viruses from using system vulnerabilities to attack endpoints

Internal attacks are on the rise. The security of your enterprise is at risk every time a remote user connects to your corporate network. PCs, laptops, and mobile devices with outdated security can open the door to attack, and infected machines can spread malware throughout the enterprise. To prevent these attacks, all devices must be checked for the correct security profile—before they can access the network.

Trend Micro™ Network VirusWall™ Enforcer protects your corporate network by ensuring that all devices comply with your corporate security policy before entering your network. As an agentless NAC solution, it can scan any device—managed or unmanaged, local or remote—for the most up-to-date security and critical Microsoft patches. Non-compliant devices are automatically quarantined and sent through remediation. Once a device meets security requirements, it is allowed access to the network. Network VirusWall Enforcer also filters network traffic to detect and block network worms—with zero false positives. The easy-to-manage appliance isolates infected areas from the rest of the network so threats cannot spread.

KEY FEATURES

Security Policy Enforcement

- Filters network traffic based on granular security policies
- Enables you to block specific file transfers, file types, IM channels, IP/MAC addresses, and TCP/UDP ports and protocols
- Automatically checks for the latest signatures so policies remain current

Flexible Quarantine and Automatic Remediation

- Quarantines infected or unsecured devices and sends them through automatic remediation
- Removes malicious remnants and spyware, repairs system registry and modifications, terminates viruses in system memory, and restores damaged files
- Grants network access as soon as a device meets security policy requirements

Network Worm Prevention

- Filters network traffic to stop worms and ARP spoofing viruses
- Blocks variants of a threat with the use of vulnerability signatures
- Isolates infected network segments so threats cannot spread

Ease of Management

- Provides an easy-to-manage, lower cost NAC solution—as a true plug-and-protect appliance
- Offers flexible deployment options and includes a built-in web management console for standalone appliance deployments
- Integrates with Trend Micro Control Manager™, a single central console for managing complex deployments

HARDWARE

Protection Points

- Network Access

Threat Protection

- Infected devices
- Non-compliant devices
- Viruses
- Network worms
- APR spoofing viruses

KEY BENEFITS

- **Lowers security risks:** blocks noncompliant devices from accessing the network
- **Checks every device:** scans managed and unmanaged devices—with or without an agent installed
- **Secures network traffic:** blocks worms using highly-effective vulnerability signatures
- **Minimizes damage:** isolates infected network segments to stop threats from spreading
- **Simplifies management:** deploys automatically and removes the burden of managing a client on all endpoints

> "Network VirusWall saved us from extensive network damage! It allowed us to manage the outbreak response more quickly, rapidly secure the network, and stop the worm before it could spread throughout our entire network."

Tony Man
Project Manager
UTStarcom Security

NETWORK VIRUSWALL ENFORCER FLEXIBLE DEPLOYMENT OPTIONS

Network VirusWall Enforcer appliances offer flexible deployment options for single or multiple network segments, remote VPN users, unmanaged users, or mission-critical applications.

- **Local users:** protects up to four segments from the network as well as from each other
- **Remote users:** protects the network from VPN users at home or branch office
- **Unmanaged users:** protects the network from unmanaged devices of non-employees
- **Mission-critical applications:** protects mission-critical server farms

Appliance Specifications	Network VirusWall Enforcer 1500i	Network VirusWall Enforcer 3500i
PERFORMANCE		
Maximum inline throughput	1.4 Gbps	1.5 Gbps
Maximum concurrent connections	100,000	350,000
Maximum users	1,000	7,000
SCALABILITY		
Network interfaces	10/100/1000 Gigabit Ethernet	10/100/1000 Gigabit Ethernet-Copper+Fiber
Optional fiber interfaces	No	Dual port fiber (LX/SX) or Quad port copper
Number of Ports	4 ports *	8 ports **
VLAN support	Yes	Yes
Management interface	Yes	Yes
HIGH AVAILABILITY		
Power supply	Single	Single
Device failure detection	Yes	Yes
Port redundancy	No	Yes
Link failure detection	Yes (SNMP)	Yes (SNMP)
Failover	No	Yes (Active-Active)
Failopen (LAN Bypass)	Yes	Yes
MANAGEMENT		
Central management console	TMCM 5.0	TMCM 5.0
Web-based management console	Yes	Yes
Automatic updates	Yes	Yes
Trend Micro™ Outbreak Prevention Services	Yes	Yes
Trend Micro™ Damage Cleanup Services	Yes	Yes
PHYSICAL/OPERATIONAL		
Form factor	1U rack mountable	1U rack mountable
Height	4.26 cm	4.26 cm
Width	44.7 cm	48.24 cm
Depth	39.7 cm	77.2 cm
Weight	11.8 Kg	17.69 Kg
Operating environment	10o ~ 35oC	10o ~ 35oC
Nonoperating (storage) environment	-40o ~ 65oC	-40o ~ 65oC
AC Input Voltage	100 to 240VAC	90 to 264VAC
AC Input Current	1.6 Amps	Max. input current (high output): 10.5A@90VAC
Frequency	50/60Hz	47 to 63Hz
Power Dissipation	223W max	447.2W max

* By default provide 2 data ports (power-off LAN By Pass) and 2 ports for management/mirror purpose
** By default provide 4 data ports (Power-off LAN By Pass) and 4 ports for management/mirror/sniffer/HA purpose

Network VirusWall Enforcer 1500

- Protects a Network Segment

Network VirusWall Enforcer 3500

- Protects Multiple Network Segments and Mission-Critical Server Farms

TrendLabs℠

Network VirusWall Enforcer is backed by TrendLabs, a global network of research centers committed to constant threat surveillance and attack prevention. By continuously monitoring the Internet and customer networks, TrendLabs' security specialists develop both Internet and customer-specific threat intelligence. With accurate, real-time data, TrendLabs delivers more effective, timely security measures designed to detect, pre-empt, and eliminate attacks. For more information about Trend Micro service and support, contact TrendLabs at: www.trendmicro.com/trendlabs.

www.trendmicro.com