



## Agent-less Network Access Control for the Mobile Workforce

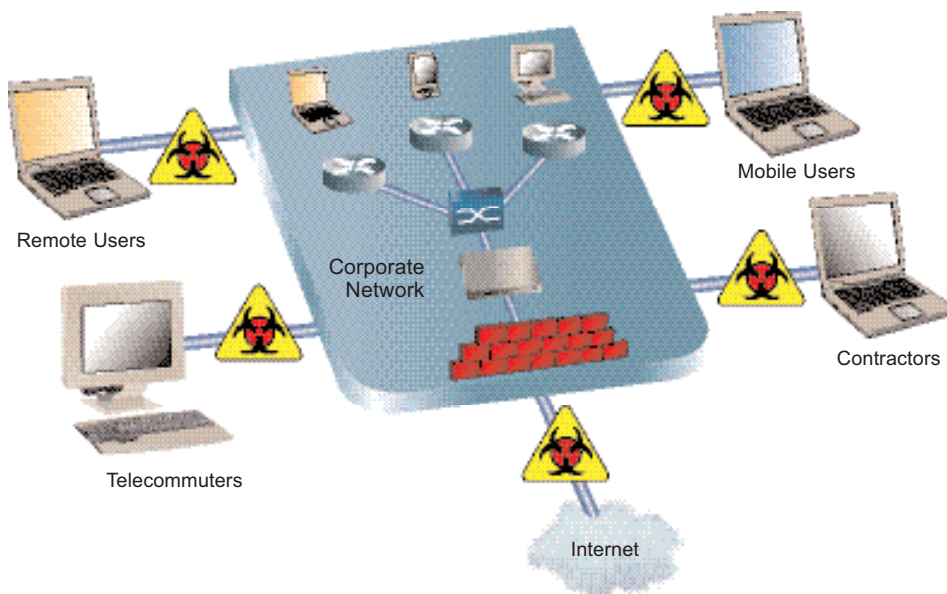
**Internal Attacks on the Rise.** In a survey of 600 companies, Yankee Group found that 50 percent of security problems in 2004 originated from internal sources—up from 30 percent in 2003. Company security is at risk every time a remote user connects to your corporate network. PCs, laptops, and mobile devices with outdated security can open the door to attack, and infected machines can spread malware throughout the enterprise.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 Plug-and-protect security policy enforcement

Trend Micro Network VirusWall Enforcer controls access to the corporate network to ensure that all devices—managed or unmanaged, local or remote—comply with corporate security policies before they connect. It prevents threats from entering the network by scanning devices for the most up-to-date security software and critical Microsoft patches.

As an agent-less solution, it has minimal impact on client devices and requires no end user intervention. Non-compliant devices are immediately quarantined and sent through automatic remediation. As soon as a device is cleaned and meets the security requirements, it is allowed access to the network.

Network VirusWall Enforcer also filters network traffic to detect and block network worms and BOTs—with zero false positives. The easy-to-manage appliance isolates infected areas from the rest of the network so threats cannot spread.



### KEY BENEFITS

- **Lowers security risks** – blocks non-compliant devices from accessing the network
- **Checks every device** – scans managed and unmanaged devices—with or without an agent installed
- **Secures network traffic** – blocks worms and BOTs, using highly-effective vulnerability signatures
- **Reduces damage** – isolates infected network segments to minimise damage
- **Eases administrative burden** – enables automatic deployment and centralised management

*“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, UTStarcom  
Security Project Manager

### The Advantage of Agent-less over Agent-Based Security

Giving network access to a single unmanaged device can defeat an agent-based approach to network security. The unmanaged devices of mobile, remote, or external users can open the door to attack, whereas agent-less security checks every device.

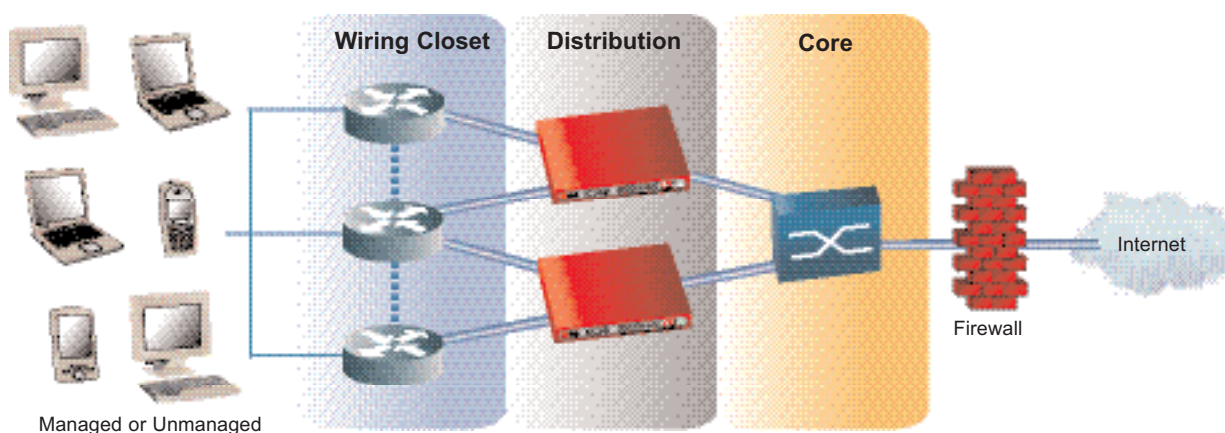
# Network VirusWall Enforcer Enforces Security Policy and Stops Worms

## Reliable access control. No need for a pre-installed agent.

Network VirusWall Enforcer does not require an agent to be pre-installed on a device. This plug-n-protect NAC appliance provides the tools you need, when you need them—including the following:

- **Remote Port Scan** – It can check any device that connects to the network—managed or unmanaged—by performing a network port scan remotely. This ensures everyone—even partners, contractors, and visitors—can connect to your network using a secure, virus-free device.
- **Temporary Dynamic Scan** – A temporary dynamic agent can be installed on any device through the Web browser in order to collect more details on the security profile of the device—including information about hundreds of versions of antivirus software and recent Microsoft™ vulnerabilities. Plus, as a unique feature, it can check registry parameters, enabling administrators to set more precise security policies. The entire scan process is fully automated and does not require end user intervention.
- **On-Demand Security** – If a device does not have any security software installed, the appliance can be configured to automatically install an on-demand security agent on the device for temporary real-time protection while the user remains connected to the corporate network.

## Typical Network Viruswall Deployment



### Security Policy Enforcement

IT administrators can define granular security policies to filter network traffic and block specific file transfers, file type extensions, instant message channels, a range of addresses or an individual IP/MAC address, and TCP/UDP ports and protocols. In addition, Network VirusWall Enforcer can automatically check for the latest signatures from different vendors so policies always remain current.

### Flexible Quarantine and Automatic Remediation

When a device violates security policy, Network VirusWall Enforcer quarantines it to a pre-defined virtual local area network (VLAN) for automatic remediation. For local or remote machines, automatic remediation removes malicious remnants and spyware, repairs system modifications and registry, terminates virus processes and threads in system memory, and restores damaged files. As soon as a device meets security policy requirements, network access is allowed.

### Network Worm Prevention

Network VirusWall Enforcer filters network traffic to stop worms and BOTs. With the use of vulnerability signatures, it can also block variants of a threat. In the rare case a new worm does invade, infected network segments are isolated so the threat cannot spread.

### Ease of Management

As a true plug-and-protect appliance, Network VirusWall Enforcer offers flexible management options whether the deployment is standalone or complex. Standalone appliance deployments can be managed from a built-in Web console while complex deployments of several Network VirusWall Enforcer appliances can be managed using Trend Micro Control Manager™, a single central console.

# Agent-less Network Access Control, Integrated Security

## Intelligent Threat Protection

Network VirusWall Enforcer is a key component of Trend Micro™ Enterprise Protection Strategy, a security framework that combines multiple layers of Trend Micro products and services—for intelligent, comprehensive protection against known and unknown threats.

As a tightly-integrated, centrally-managed security platform, it is designed to:

- **MONITOR** for potential threats
- **ENFORCE** security policy compliance
- **PREVENT** malicious threats from spreading
- **RECOVER** infected devices

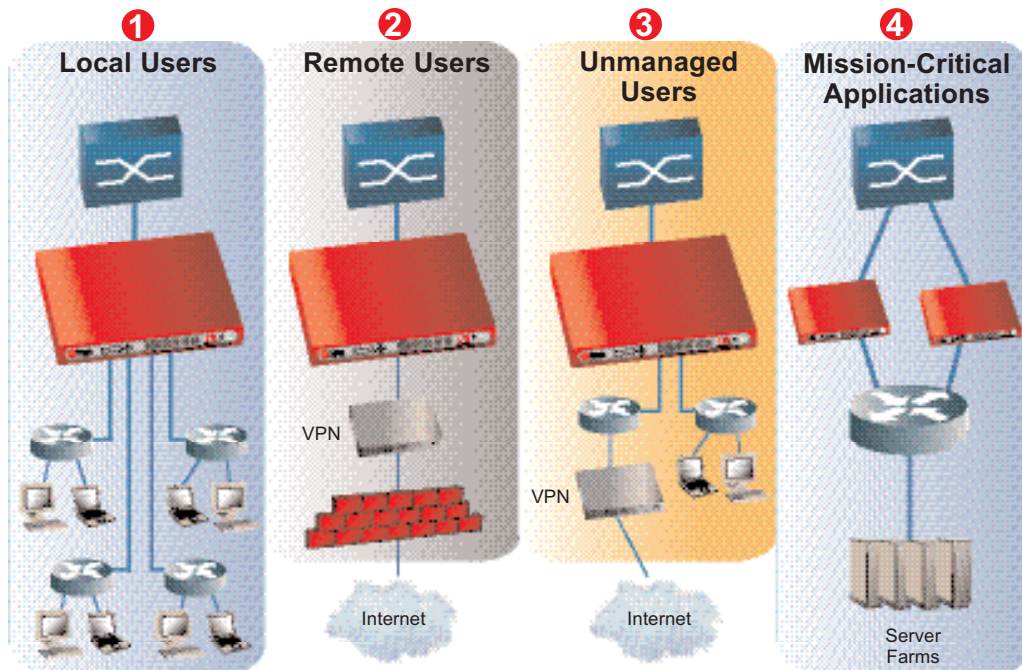


## Network VirusWall Enforcer Flexible Deployment Options

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

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

### Flexible Deployment Options for Network VirusWall Enforcer



# Trend Micro Network VirusWall Enforcer

Agent-less network access control appliances scale to meet security needs at network end points, segments, or multi-segments with enterprise-scale performance, availability, and flexibility built in.

Appliance Specifications	Network VirusWall Enforcer 1200	Network VirusWall Enforcer 2500
<b>PERFORMANCE</b>		
Maximum inline throughput	180 Mbps	1.2 Gbps
Maximum concurrent sessions	68,000	1,000,000
Maximum users (policy enforcement)	256	4,096
<b>SCALABILITY</b>		
Network interfaces	10/100 Fast Ethernet	10/100/1000 Gigabit Ethernet - Copper + Fiber
Optional fiber interfaces		1 or 2 ports (1000BaseLX) 2 or 4 ports (1000BaseSX)
Number of ports	2 ports	5 ports
VLAN support	yes	yes
Management interface	yes	yes
<b>HIGH AVAILABILITY</b>		
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
Hardware status monitoring	no	yes
<b>MANAGEMENT</b>		
Central management console	TMCM 3.0.(NVW v1.x)	TMCM 3.5 (NVW v2.x*) TMCM 3.0 (NVW v1.x)
Web-based management console*	no	yes
Automatic updates	yes	yes
Trend Micro™ Outbreak Prevention Services	yes	yes
Trend Micro™ Damage Cleanup Services	yes	yes
<b>PHYSICAL/OPERATIONAL</b>		
Form factor	1U rack mountable	1U rack mountable
Height	4,45 cm	4,32 cm
Width	42,67 cm	42,49 cm
Depth	32,00 cm	62,05 cm
Weight	4,5 Kg	9 Kg
Operating environment	0 ° ~ 40 °C	5 ° ~ 45 °C
Nonoperating (storage) environment	-20 ° ~ 75 °C	-40 ° ~ 70 °C
AC input voltage	100 to 240VAC	100 to 240VAC
AC input current	4 to 2A	8 to 4A
Frequency	50 to 60Hz	50 to 60Hz
Power dissipation	180W max	450W max



**Network VirusWall Enforcer 2500**  
Protects Multiple Network Segments and Mission-Critical Server Farms



**Network VirusWall Enforcer 1200**  
Protects a Network Segment

### TrendLabs<sup>SM</sup>

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-europe.com/trendlabs](http://www.trendmicro-europe.com/trendlabs).

### Trend Micro, Inc.

Trend Micro, Inc., is a global leader in network antivirus and Internet content security software and services, focused on helping customers prevent and minimize 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](http://www.trendmicro-europe.com)



For Trend Micro Control Manager 3.x system requirements please refer to the product pages at [www.trendmicro-europe.com](http://www.trendmicro-europe.com).