

Defending Against Worms, Trojans and Bots

Detecting and Containing Malware Threats on the LAN

A single worm or other malware incident can cause widespread disruption to business systems and business processes, and cost up into the millions of dollars per site in remediation costs and lost business. In the constantly escalating battle between hackers and the security industry, it is practically impossible to stay ahead of all threats, particularly newly emerging zero-day threats which can spread worldwide within hours. These threats are designed to disrupt business, steal data, overwhelm systems and coordinate cyber crimes.

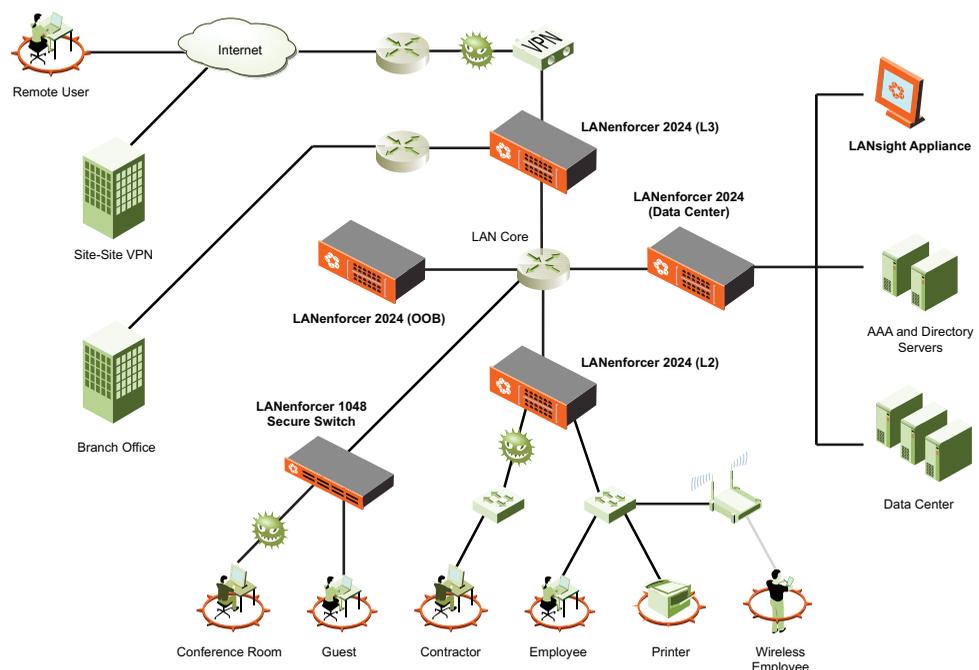
Malware threats are a constant possibility as enterprises open their internal LAN networks to external users and unmanaged endpoints, such as remote or mobile systems, and guests, contractors, or business partners. It is a daunting task to ensure that these untrusted systems conform to the system health policies of the network, as well as to detect and contain zero-day threats which desktop anti-virus programs are not capable of recognizing. To thwart all outbreaks, a coordinated combination of countermeasures, on the desktop, and in the network, are required.

Key challenges to implementing a malware or intrusion prevention solution:

- Performance constraints of in-line appliances limit the sophistication of packet analysis algorithms to detect traffic and behavioral anomalies
- Out-of-band intrusion prevention systems are slow to detect and almost certain to not remediate the threat until long after it has propagated through the network
- Remediation steps are limited to severe countermeasures, such as shutting down an entire subnet or system. The many false positives that generate a response that materially impacts the business makes such a solution impractical for most organizations.

Solution Highlights:

- Remote endpoint health validation and quarantine
- Identity-based access control of remote users to internal network assets
- Intrusion detection system for threat containment
- Audit log for each user of resources accessed
- High-performance in-line appliance (10GBps)



The Nevis LANenforcer appliance can be deployed at any of multiple points throughout the network to detect and contain malware arising from both trusted and unmanaged endpoints on the LAN.

“There are five key technologies enterprises should include in their NAC deployment strategy. The Nevis solution offers elements to support each of these requirements and differentiates itself through advanced persistent threat detection and containment.”

Joel Conover
Research Director,
Enterprise Networks and
Security

Current Analysis



The Nevis LANenforcer 1048 and 2024 are scalable rack-mounted devices that easily install into any network topology (both shown on top of the LANSight appliance).



Nevis Networks, Inc.
 295 Bernardo Ave., Suite 100
 Mountain View, CA 94043
www.nevisnetworks.com
 (650) 254-2500

Nevis Networks International HQ
 Delegate House
 30 Hart Street
 Henley on Thames, UK RG9 2AL
 Tel: +44 1491 635 339

Nevis Networks India
 C301 Pune IT Park
 Bhau Patil Marg
 34 Aundh Road
 Pune 411020, India
 Tel: +91 98450-05047

The Nevis Networks LANenforcer™ LAN security solution

Nevis Networks is a leader in providing LAN security solutions that protect the internal core network from all threats arising from endpoint systems, whether internal or unmanaged external systems. The Nevis LANenforcer appliance forms a four-pronged countermeasure to defend against all categories of network security threats from untrusted systems accessing the internal network:

- **Endpoint validation:** pre-connect and post-connect authentication of the user and system and ensuring the health and compliance of the system's operating environment;
- **Identity-based access control:** ensuring that specified user groups and roles are constrained within the internal network to only specific systems and applications;
- **Threat containment:** going beyond ensuring anti-virus signatures are up to date, Nevis uses state-of-the-art deep packet inspection algorithms, including behavioral, protocol and traffic anomaly detection to protect against new malware attacks (worms, Trojans, bots, etc.);
- **User activity monitoring:** keeping a detailed audit trail of which users accessed which resources and systems for regulatory and compliance purposes.

Specifically regarding that ability to detect and contain malware threats, Nevis offers the following key advantages:

- **In-line Appliance:** By moving detection into the network, and off the desktop, LANenforcer is easy to deploy, manage and less vulnerable to compromise than desktop software.
- **Maximum Detection:** Nevis implements the most strategies for detecting malware: signatures and all types of anomaly detection. Nearly all recent threats missed by competitors were caught by Nevis
- **Maximum Performance:** Nevis detects threats without slowing down the network, performing deep packet analysis at wire-speed (10Gbps) with its custom ASIC architecture
- **Effective Containment:** As a high-performance, in-line solution, Nevis can filter out malicious packets from a user's traffic without impacting valid activity, reducing adverse impact of remediation and false positives.
- **Event Correlation:** The ability to correlate events across devices and across the network provides further analysis to detect threats

LANenforcer is a highly scalable solution that integrates NAC capability with IPS and identity firewall functionality for holistic LAN security.