

# Nevis Networks

*Persistent LAN Security at LAN speed*

## LANenforcer™ datasheet

Nevis' Persistent LAN Security solutions provide the following benefits:

- Reduce Cost and Complexity of Risk Management
- Tighter Control and Visibility of Regulatory Compliance
- Control Access to Sensitive and Confidential Data
- Provision Appropriate Network Access for Non-employees
- Mitigate the Risk of Endpoint Vulnerabilities
- Common Standard for Wired, Wireless, Remote and Branch Office Users

The Nevis LANenforcer product line provides a highly scalable, enterprise-class Persistent LAN Security solution with 10Gbps performance. LANenforcer integrates all LAN security functions into an ASIC-based security policy processing engine that provides deep inspection of every packet to ensure data integrity, confidentiality, threat containment, and user accountability.

### *Prevent Unauthorized Access*

- ◆ Clientless endpoint integrity check for OS version and patch level; updated and active antivirus and anti-spyware
- ◆ Supports endpoint integrity verification at admin-defined intervals after system gains admission to the network
- ◆ Performs user authentication supporting a variety of common industry protocols, including transparent Windows login
- ◆ Easy integration into existing networks
  - Leverages existing AAA and directory services simplifying deployment and maintenance
  - No network reconfiguration of existing switches and VLANs required

- Centralized multi-site configuration and management
- Deployment options at Layer 2 and Layer 3

### *Control and Monitor Activity*

- ◆ Identity-based policies enforce data integrity and confidentiality
- ◆ Location-independent access control across users, endpoint devices, network resources and applications
  - Managed and Unmanaged users
  - Wired, Wireless, Remote Access, Branch office
  - VoIP phones, printers, etc.
- ◆ Per user stateful firewall for policy enforcement
- ◆ Centralized real-time user-level visibility and reporting
  - Powerful event correlation engine enables faster problem identification and forensic analysis
  - Associates user identity, user location, IP address, port, and MAC address for fast pinpointing of root cause
  - Policy violation monitoring for regulatory compliance reporting requirements

### LANenforcer Configurations

#### **LANenforcer 2024 and 2012 Appliances**

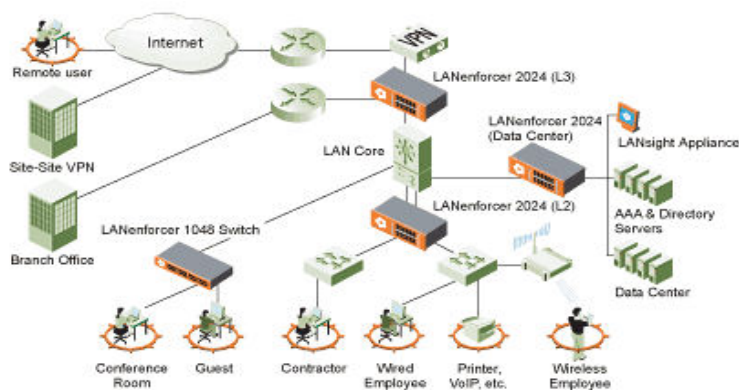
Inline LAN security appliances deployed transparently, aggregating any existing access layer switches and access points, enabling rapid rollout to a large number of users at unmatched price/performance.

#### **LANenforcer 2124**

A family of higher capacity version of the LANenforcer 2024 appliance, available in 3000, 5000 and 10000-users versions, reducing overall per user cost.

#### **LANenforcer 1048 Switch**

Secure access switches that provide the most secure method for locking down the LAN by reducing the threat envelope down to the individual user. Implemented at the access layer, they are ideal for securing high risk and high value assets, and preventing user-to-user exploits in high risk areas, such as conference rooms, lobbies and other public areas.



### Detect Threats at Wire speed

- ◆ Microsecond zero-day threat containment
- ◆ Aggregates multiple detection mechanisms in parallel to capture the broadest range of threats
  - Stateful Firewall
  - Protocol, Traffic and Behavioral Anomaly Detection
  - LAN-based IPS
  - Layer 2-7 Security
- ◆ Per-endpoint quarantine for remediation to contain threats in real-time—before, during and after authentication

Feature	LANenforcer 2124	LANenforcer 2024	LANenforcer 2012	LANenforcer 1048
<b>Form Factor</b>	LANenforcer LAN Security Appliance			LANenforcer Secure Access Switch
<b>Max Secured Users</b>	10000*	2000*	1000	500
<b>Full Security Policy Throughput</b>	10 Gbps			
<b>VLAN Support</b>	4096 (IEEE 802.1Q)			
<b>Switching</b>	N/A			STP, RSTP
<b>Quarantine and Remediation</b>	Based on Endpoint Integrity Check, Policy Violation and Malware Infection			
<b>Clientless Endpoint Integrity</b>	Integrity Check OS and Patch level, Anti-virus and Spyware running and up-to-date			
<b>User Authentication</b>	Transparent Kerberos, RADIUS, TACACS+, AD, LDAP, MAC, Captive Portal, Via Nevis Agent, White-list/Blacklist			All as per N2000 series and 802.1X
<b>Threat Signature Control</b>	Optimized Malware Recognition Signatures, Nevis Labs Signature Update Service**			
<b>Anomaly Detection</b>	Zero-day Worm Protection, Traffic Anomalies, Protocol Anomalies, Behavior Anomalies			
<b>Layer 2 Security Protection</b>	MAC Spoofing and Flooding, ARP Spoofing and Poisoning, VLAN Hopping and Double Tagging, DHCP Address Exhaustion, Switch Impersonation and Spanning Tree Attacks			
<b>Management Features</b>	Configuration, Policy, Monitoring, Reporting, Event Correlation, Root Cause Analysis			
<b>Management Interface – Direct</b>	Direct CLI, SNMP V2c and V3, MIB II			
<b>Interface Ports</b>	24 unpopulated 10/100/1000 SFPs	24 unpopulated 10/100/1000 SFPs	12 unpopulated 10/100/1000 SFPs	48 10/100/1000 Cu + 4 unpopulated SFPs
<b>Dimensions</b>	17.5" x 20" x 3.4" (2U)			17.5" x 18.2" x 1.7"(1U)
<b>Weight</b>	22 lbs			14 lbs
<b>Temperature</b>	Operating: 0° - 40° C / Storage: -10° to 70° C			
<b>Humidity</b>	Operating: 5% to 90% RH, Non-Condensing			
<b>Certifications</b>	Emissions: FCC (Part 15 Class A)/EN55022 (Class A), Safety: US-TUVR-2044, UL60950/EN60950, CSA22.2, CE, RoHS, WEEE			
<b>Power</b>	90 – 240 V AC Full, Range, 47 – 63 Hz, 175 W (no expansion module)/ 350W (w/ ALG modules)			



The two form factors of the Nevis security appliance are shown: The 48-port LANenforcer1048 secure switch (top), and the LANenforcer 2024/2124 security appliance.



### Nevis Networks, Inc.

1175 Saratoga Avenue, Suite 11  
San Jose, CA 95129  
Tel: +1 408 624 1234  
[www.nevisnetworks.com](http://www.nevisnetworks.com)

### Nevis Networks India

C401 Pune IT Park  
Bhau Patil Marg  
34 Aundh Road  
Pune 411020, India  
Tel: +91 990262 8702

\* For Kerberos Authentication \*\* Sold Separately