

Persistent LAN Security



Sandy Hawke, CISSP
Senior Product Marketing Manager
Nevis Networks

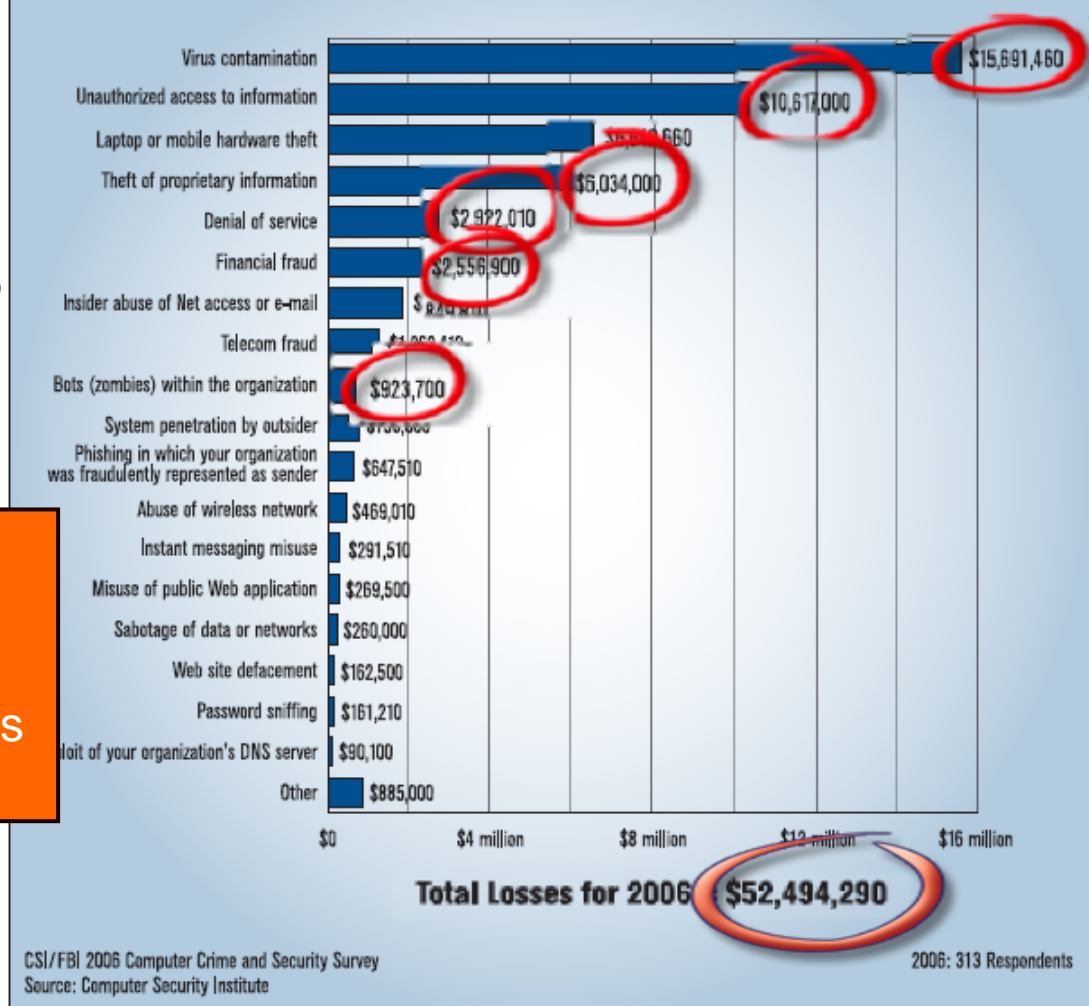
LAN Security Pain Points



- Loss of **Network availability**
- Violation of **Confidentiality**
- Loss of **Productivity**
- Penalties from **Non-compliance**
- Organizational **Liability** issues

Despite increases in security budgets and innovative technologies, organizations continue to lose billions of dollars to data security exposures.

Figure 16. Dollar Amount Losses by Type



Blended Threat Protection is Mandatory



Malware Type / Name	Business Impact	NAC Point Solutions	Requires	Nevis
<u>Virus:</u> BlackWorm/Nyxem	Over 300,000 systems were infected worldwide.	Cannot detect	Anomaly Detection	
<u>Rootkit:</u> VirTool (DRM)	Installed by Sony/BMG from CD; Exploited by websites and Trojans like Win32/Ryknos.A	Cannot detect	Threat signature matching	
<u>Spyware:</u> CoolWebSearch	Half of all PCs worldwide infected , resulting in profits of \$300M/year for the author.	Cannot detect	Threat signature matching	
<u>Trojan:</u> Exploit WMF	Over 70 variants and dozens of outbreaks worldwide. Due to the number of variants, anti-virus vendors have been slow to respond.	Cannot detect	Threat signature matching	
<u>Worm:</u> Zotob	Over 13% of global enterprises affected, with an average cost of \$97,000 for each outbreak.	Cannot detect	Combination of: Threat Signature Matching; Anomaly Detection	

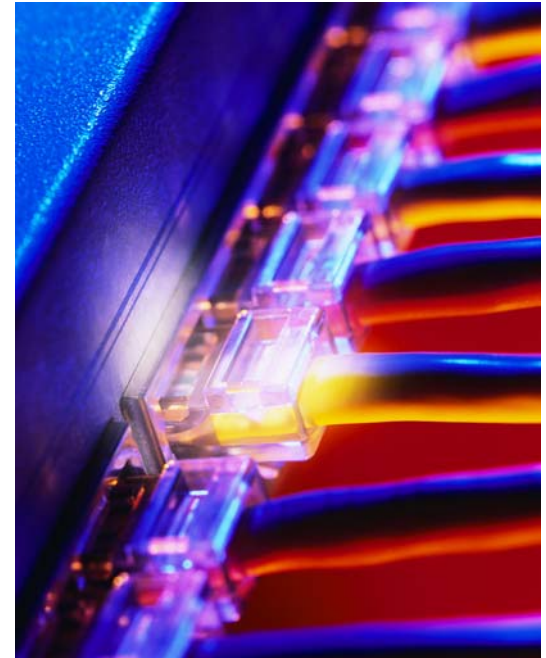
97% of enterprises use anti-virus, yet virus outbreaks remain the most costly security threat for enterprises = >\$15M in 2006*

**2006 CSI/FBI Computer Crime and Security Survey*

Key Elements for a NAC Solution



1. Pre-connect host posture assessment
2. Host quarantine and remediation
3. Network access control based on user identity
4. Network resource control based on identity and policy
5. Ongoing threat analysis and containment

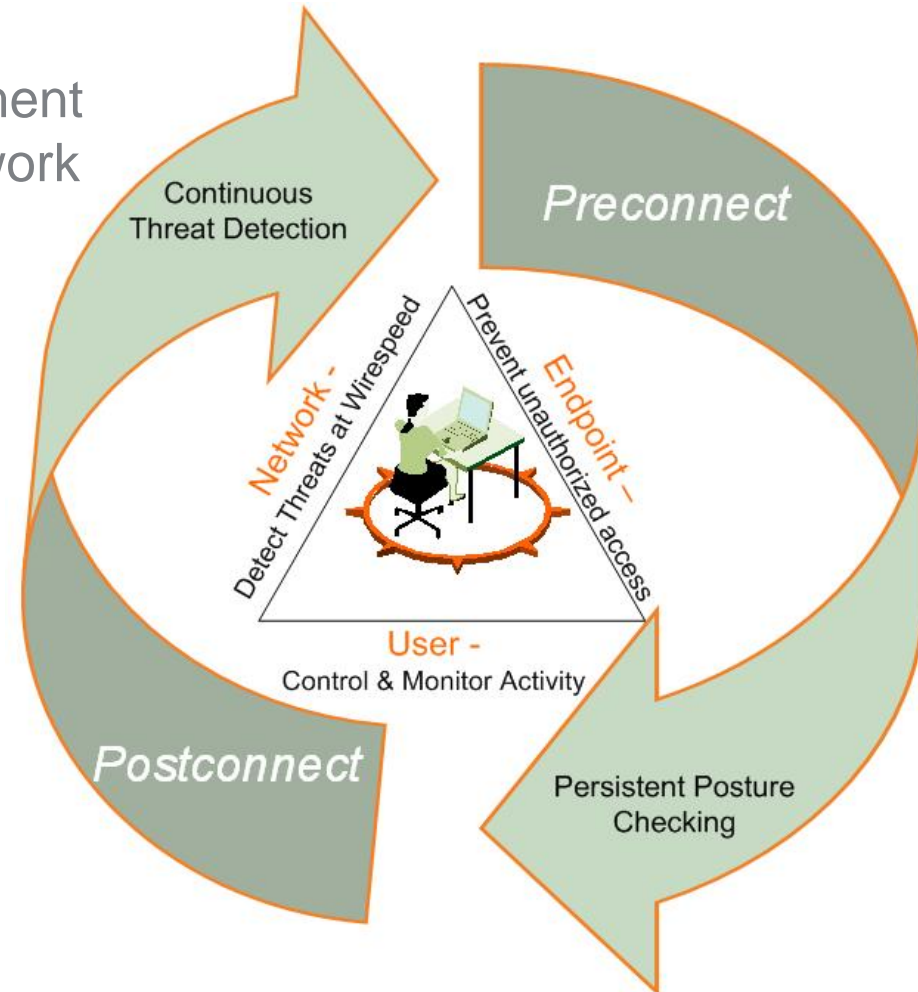


Source: *Current Analysis*, 2006

Nevis Provides Persistent LAN Security



- Nevis builds upon NAC adding access control and threat containment after users gain access to the network
- Why?
- LAN Security requires persistent visibility and policy enforcement before, during, and after users gain access to the network



The majority of insider attacks occur after authentication, so only a persistent LAN security solution gives complete protection.

Nevis Solution Overview



Continuous NAC

- Clientless endpoint admission
- User authentication
- Integrated user, endpoint network and application access policy control
- Policy-based encrypted application access

Centralized policy management

- Multisite, multidevice
- Security event correlation
- Reports – events, policy violations, regulatory compliance



Personal DMZ

Deepest and fastest threat protection

- Only 10Gbps LAN security solution
 - Stateful firewall
 - LAN-optimized intrusion prevention
 - Anomaly detection (protocol, traffic, behavioral)
 - Layer 2
- Microsecond quarantine
- Nevis Labs - global LAN vulnerability monitoring

Two Deployment Options

- Transparent overlay appliance (up to 1,000 users)
- Secure access switch (up to 100 users, PoE enabled)

Thank You!



- Thanks to Mike Rothman
Phone +1 (678) 449-7183
www.securityincite.com



- For further information about Nevis Networks, please contact us at:
Email: sales@nevisnetworks.com
Phone: (650) 254-2500
www.nevisnetworks.com
- Q&A

