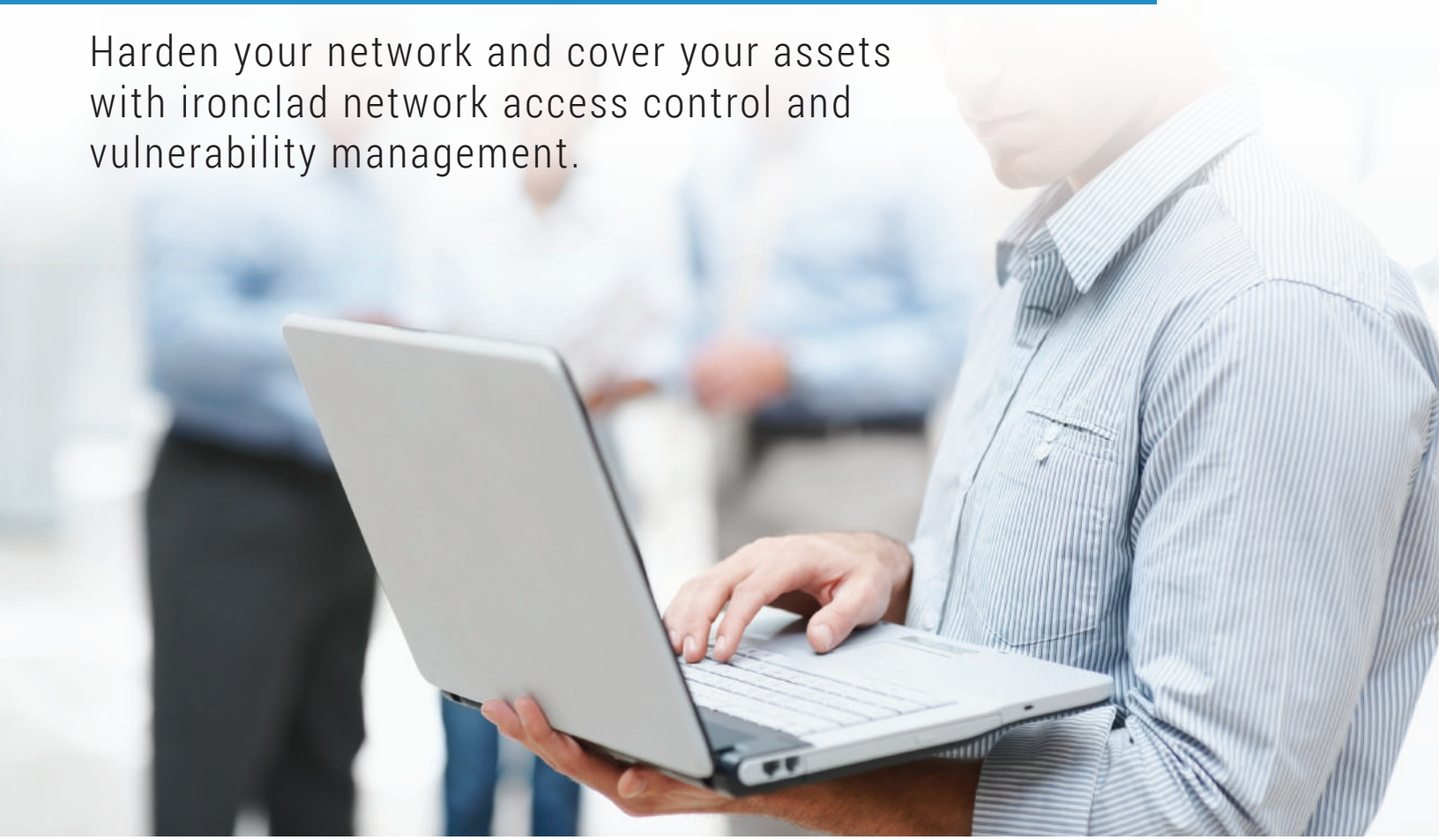
NetSHIELD™ APPLIANCES

MANAGE YOUR NETWORK FROM THE INSIDE

Do you know who's on your network?

Harden your network and cover your assets with ironclad network access control and vulnerability management.



GET THE FACTS. THEN GET THE PROTECTION YOU CAN'T LIVE WITHOUT.

1-800-991-3871 | snoopwall.com/secure-your-network

Control who can connect to your network. Detect, alert, and block unauthorized laptops, other network devices, and wireless access points.

Protect your network—find and fix vulnerabilities before they're exploited.

Detect malware and quarantine infected assets.

Comply with requirements for GLBA, HIPAA, HITECH, PCI, ISO 27001, and other security and privacy standards.

Who is on your network?

In this day of BYOD—bring your own device—it's challenging to know what kind of devices want access to your local area network (LAN) and how to protect your corporate network from non-corporate assets who still should be able to access the Internet.

BYOD to work.

You have a firewall to stop hackers, viruses, and malware at the network's edge. A firewall is vital to safe network operation, but, because it operates at the edge of your network, it can only protect you from threats coming from outside your network.

NAC devices, on the other hand, protect your network from threats originating on the inside. Unauthorized devices connected to your network make your organization vulnerable to malware, viruses, and even internal spying and data theft. This is what a NAC appliance is designed to prevent, whether the vulnerability is a LAN port in a lobby or conference room, or a wireless access point.

In this age of bring your own device (BYOD) to work, it's even more difficult for your network to know what devices should be blocked. Most of the time, BYOD users are employees, guests, or contractors who should have access to certain network areas, but as noncorporate assets, they should be steered away from others. A NAC that works with your network infrastructure can easily address that concern.

NetSHIELD is a family of Network Access Control (NAC) appliances from SnoopWall that ensures that only authorized devices gain access to your network. It also screens for vulnerabilities in computers connected to your network, returning mobile users, wireless devices, and new devices. If NetSHIELD detects an untrusted asset, it responds instantly to shut off network access for that device — protecting your network while keeping your trusted devices securely on-line.

Designed for simplicity.

Traditonal NAC solutions have been slow to catch on because they've been expensive, time-consuming, and often require extensive equipment upgrades. In short, they're just too complicated to be worthwhile.

NetSHIELD, on the other hand, is designed to provide maximum security in a simple, agentless design that's also very affordable. No need for extensive training or dedicated personnel, no need to install software agents, no need to upgrade switches—NetSHIELD is easy to integrate into your network.

More than 95% of security breaches are a direct result of exploiting a common vulnerability and exposure (CVE)®.

Control your network.

NetSHIELD only lets computers and devices onto your network if they comply with standards that you specify.

NetSHIELD assembles a profile of each device on your network, including the device's IP address, host name, MAC address and operating system (OS), and only grants access to trusted devices on the network. It can even detect and stop a machine trying to get in under a spoofed MAC address.

NetSHIELD offers a multilayered response to perceived threats. First, if NetSHIELD detects a device with an untrusted user/MAC address, it issues an alert (text, e-mail, SNMP, Syslog) to the administrator while simultaneously streaming its patented denial-of-service block. If switch integration has been implemented (optional), network switches can lock out that device entirely or limit the asset to a guest VLAN that has been set up.

If you have visitors who want to "BYOD" and use their own laptops or smartphones to access the Internet, NetSHIELD uses the network switches to grant them access only to the Internet via a guest VLAN while restricting them from your organization's protected network.

NetSHIELD works with all 802.1q-enabled switches to protect multiple VLANs. It will permit users to connect to authorized VLANs but will deny access if they attempt to access restricted VLANs, even without switch integration. You can also assign trusted assets to multiple VLANs. Each Ethernet port on a NetSHIELD unit is able to protect up to 10 VLANs, with the 5800 protecting up to 80.

Protect your network.

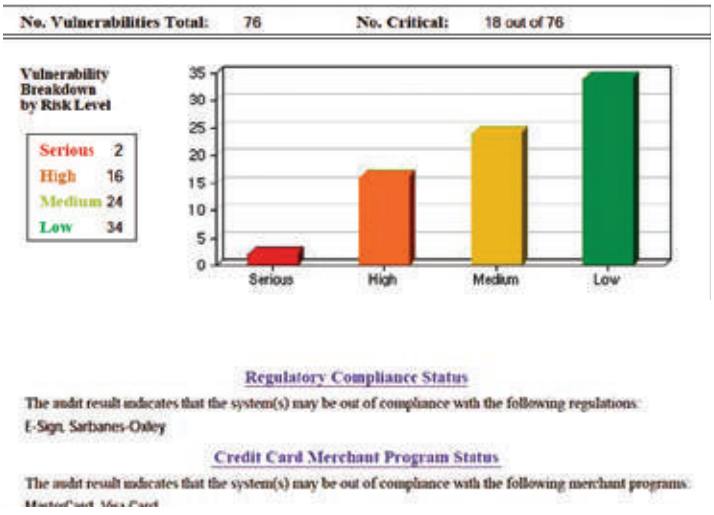
Using daily vulnerability updates from the National Vulnerability Database (http://nvd.nist.gov), which is curated by the National Institutes of Standards and Technology (NIST), NetSHIELD enables IT staffs to set up audit wizards or one-click audits. Audits include differential, full, incremental, and top 20 options. These audits will help your organization with compliance and due diligence.

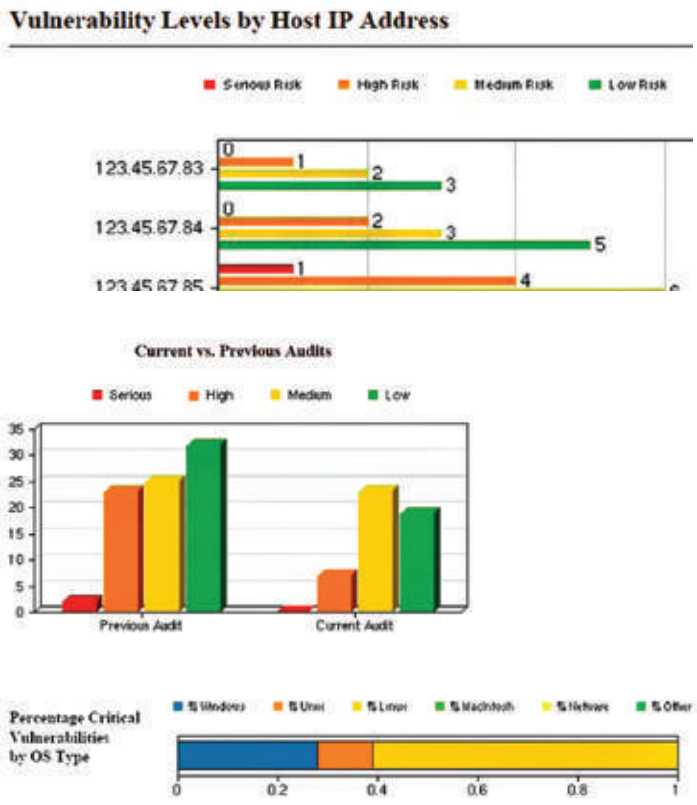
This auditing function works for all connected devices, not just Windows® based PCs. You are now able to audit your firewall, switches, routers, and other key assets for vulnerabilities.

The NetSHIELD CVE scanner helps you identify the most urgent patches needed to harden your network against attack. After you run a scan, detailed reports alert you if an attached device has a problem, or you can set a threshold to block an asset if it fails a scan. This powerful vulnerability scanner is included in all NetSHIELD models.

An annual software license is required for each NetSHIELD appliance. The license includes daily vulnerability and malware updates, as well as all software and feature updates. Licenses are available in one- and three-year packages

Interpreting Vulnerability





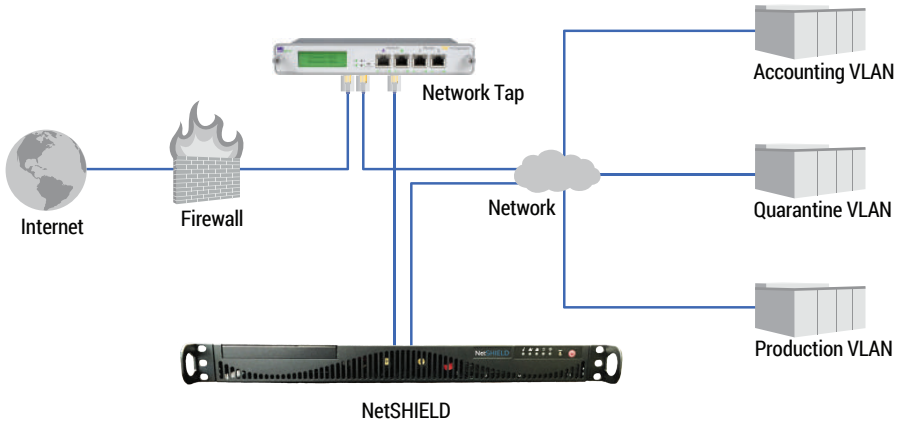
Zero-day protection.

Quarantine or block malware-infested PCs — even zero-day malware that would otherwise go unchecked by standard virus-protection software. Or NetSHIELD can simply issue an alert and you can decide how to proceed with remediation.

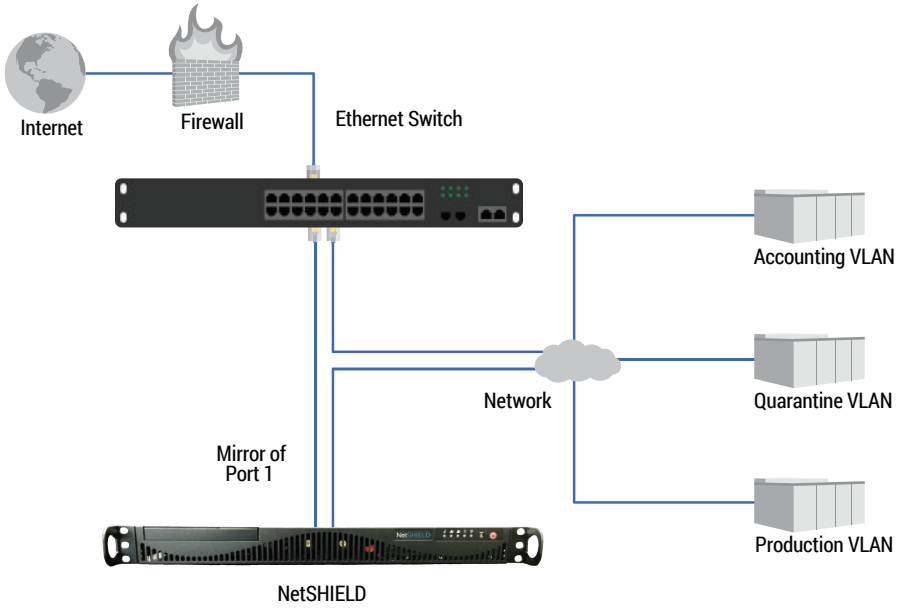
NetSHIELD now gives you two installation options for detecting previously undetectable malware. It takes advantage of the fact that most malware tries to "call home."

In the first method, simply add a network tap near the firewall. The second method involves setting up a mirror port on your network switch. In both applications, NetSHIELD will keep watch for outgoing network traffic going to known malware repositories.

Malware Detection — Application 1: Network Tap



Malware Detection — Application 2: Ethernet Switch Port Mirroring



- Protect your network from vulnerabilities firewalls can't defend against.
- One-box vulnerability management and network access control (NAC).
- Agentless and non-inline design provides rock-solid security in an easy-to-deploy appliance.
- No infrastructure upgrade needed — works with existing switches.
- Provides blackholing and VLAN quarantining of untrusted assets.
- Detects malware on infected devices.

A commanding presence.

NetSHIELD models ENT 10/100/250 feature a Control Center that offers the ability to command and control remote NetSHIELD appliances across your network. Add remote appliances and create groups to simplify management. In one action, policies and configurations can be saved to all remote units included in a group, and perform remote actions. The Command Center also makes it easy to view group and appliance statuses on a single screen. For more information about how many remote appliances models can control, see the Buyer's Guide (back cover).

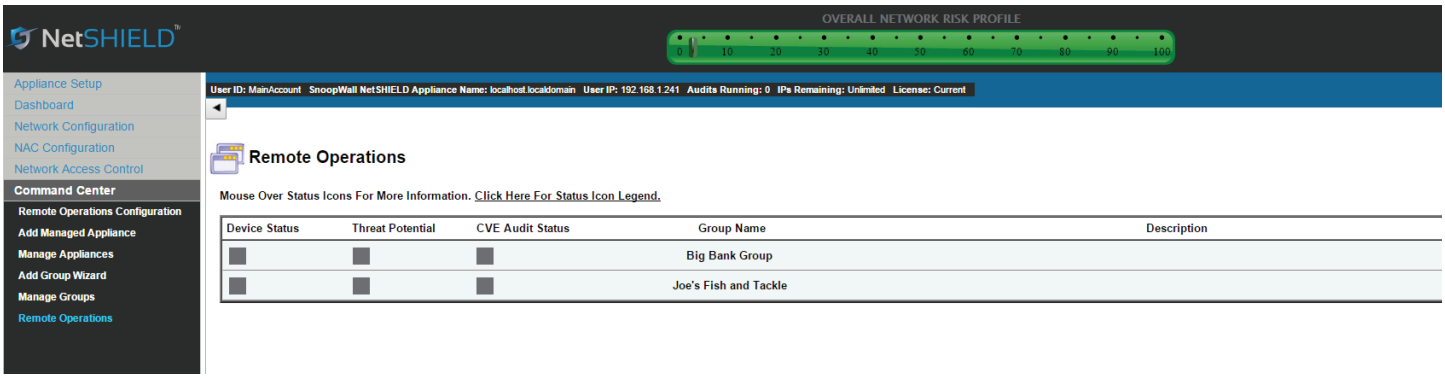
Remote operations.

Device Status	Threat Potential	CVE Audit Status	
			Corporate
		✓	Sales Offices
✓		—	Mfg. Group
			Device
✓	✓	—	Pittsburgh
✓	✓	—	Dallas
✓		—	San Jose

NetSHIELD Status Icon Legend

Device Status	
	Device not powered on or not working
	Device powered on but not logged in
✓	Device powered on and fully operational
Threat Potential	
	Untrusted asset blocked by NetSHIELD
	Untrusted asset on network - confirm identity
✓	All connected devices are known, trusted assets
CVE Audit Status	
	CVE audit currently running
	Audit revealed critical vulnerabilities - fix immediately
	Audit revealed moderate vulnerabilities
✓	Audit revealed no vulnerabilities

Command center.



No agents.

Unlike many other NAC systems, NetSHIELD doesn't require that you install software agents on connected machines. This both simplifies installation and improves security because agents are vulnerable to hacking. Agentless design means that NetSHIELD also works with devices such as printers, smartphones, and wireless access points that can't have agents installed on them.

Cost effective.

Not only is the up-front cost for NetSHIELD often lower than other solutions, installation and ongoing maintenance costs are typically lower, too.

NetSHIELD works with your existing network and legacy infrastructure, so there's no need for expensive upgrades. With our FREE Tech Support and on-going, free training, setting up NetSHIELD is simple and even organizations with a limited IT staff can easily add it to their network security plan without straining resources.

Fast, straightforward setup.

This capable NAC system is a turnkey network appliance. We recommend a phased approach to a successful installation. The initial deployment and fingerprinting of all network assets is typically done in just a few minutes. More advanced features can be activated at a later time.

Third-Party Evaluations:

"Full dynamic access control and auditing of network devices."
- Peter Stephenson, SC Magazine

SC Magazine Product Rating

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★★
Overall Rating	★★★★★

SC MAGAZINE RECOMMENDED

For: Full dynamic access control and auditing of network devices.

Against: None that we found.

Verdict: A solid suite of hardcore NAC products with a clear focus on keeping unauthorized systems and users off the network.

Pre-sales assistance.

For more information, and to set up an in-person demo, call 1-800-991-3871 or visit snoopwall.com/secure-your-network

Tech Support is just a call away!

Let our experts help you find the right solutions right now.

FREE— The advice is absolutely FREE whether you buy or not!
Live — Our techs answer your calls live from our headquarters in Nashua, NH.
24/7 — Call our product experts with questions anytime day or night.

Q: Do we need NAC if we already have a firewall?

A: For a complete security plan, you do need both a firewall and a NAC because they protect in very different ways.

A firewall is usually placed at the edge of your network, inspects data coming from the Internet, and denies or permits network traffic based on a set of rules. Firewalls are "traffic cops" and only protect against threats coming from outside your network.

NAC appliances, on the other hand, are "asset cops" and protect your network from inside threats. A NAC keeps watch over computers and mobile devices connected to your network and decides whether or not to grant them access. If a device or computer is determined to be noncompliant, NAC may deny access or quarantine it.

Q: How does NetSHIELD deal with guest computers?

A: Unknown users and devices — guests, for instance — can either be allowed on the network, but flagged as an untrusted asset, or blocked entirely. If you have visitors who want to use their own laptops or smartphones to access the Internet, NetSHIELD can grant them access to only the Internet while restricting them from your organization's intranet.

Q: Does a non-compliant computer just get locked out of the network?

A: You can set NetSHIELD to respond differently to non-compliant computers, depending on the situation. For instance, if NetSHIELD detects a device with an unknown MAC address, it can lock out that device entirely or limit it to only a guest network. If it detects a vulnerable computer with outdated software, it can lock it out or quarantine the vulnerable ports, providing partial network access, while sending a message to your IT staff to update the software.

Q: Most NAC offerings I see from other manufacturers require an agent. Can NetSHIELD be effective without an agent?

A: Yes! Agents were initially thought to help verify the integrity of network devices. But now all agents are known to be easily hackable, creating a vulnerability in your security architecture. Plus, agents can't run on most non-PC devices such as VoIP phones, network printers, smartphones or PDAs, bar-code scanners, IP door locks, and access points, leaving many network devices outside of the capabilities of agent-based NAC solutions. SnoopWall intentionally designed NetSHIELD without agents.

Q: Is there a way to centrally control multiple NetSHIELD appliances on our enterprise network?

A: Yes. The Enterprise 10/100/250 models have a Command Center, which enables you to access all units globally and across remote locations from a central point. Multiple NetSHIELD appliances may share the same trusted MAC address list and the same set of policies. You may also assign the same password to every NetSHIELD appliance in your network.

Q: Does NetSHIELD impair network performance?

A: No. NetSHIELD isn't an in-line device and won't negatively affect network performance. Under normal conditions, NetSHIELD uses only about 7 kbps of bandwidth to block untrusted users, and between 40 and 120 kbps while it's auditing for vulnerabilities. This small amount of bandwidth isn't enough to make a noticeable difference in network performance in most circumstances.

Q: Does NetSHIELD require 802.1x switches?

A: No. NetSHIELD works with all Ethernet switches, even legacy switches or low-cost generic switches. There is no need to upgrade your infrastructure to 802.1x-enabled switches.

Q: Why would I use 802.1q VLAN tagging?

A: This feature makes your NetSHIELD even more efficient. It enables you to protect a large or complex network that uses VLANs without adding another NetSHIELD appliance. To have one Ethernet port of your NetSHIELD appliance "see" and help manage network access and vulnerabilities in up to 10 VLANs per physical Ethernet connector, simply tag all the VLANs and connect the Eth0 port of your NetSHIELD appliance to the port on your smart switch where you have the tagged VLANs mapped.

Sized for every network.

NetSHIELD comes in models for every application from small-office networks to large enterprise networks containing thousands of devices.

Nano 25/100 are ideal for small offices, either as freestanding NAC appliances or as remote units that can be centrally managed by our NetSHIELD Enterprise models.

Enterprise 10/100/250 include Command Center software for secure central management of multiple NetSHIELD appliances so you can protect your entire organization from edge to core.

These models also include ISO 27001 Policy Tools to simplify your organization's compliance efforts.

Buyer's Guide | NetSHIELD

Model	Nano 25	Nano 100	Branch PRO	ENT 10	ENT 100	ENT 250
Feature	Compact wallmount	Compact wallmount	1U High, 11.5 " Deep	1U High, 14 " Deep	1U High, 14 " Deep	1U High, 14 " Deep
Ethernet Ports	(2) RJ-45 10/100/1000	(2) RJ-45 10/100/1000	(2) RJ-45 10/100/1000	(4) RJ-45 10/100/1000	(6) RJ-45 10/100/1000	(8) RJ-45 10/100/1000
Agentless NAC	✓	✓	✓	✓	✓	✓
Endpoint Vulnerability Auditing	✓	✓	✓	✓	✓	✓
Maximum Simultaneous Device Audits	10	10	10	50	100	250
Auto Device Discovery	✓	✓	✓	✓	✓	✓
Inventory Alerting	✓	✓	✓	✓	✓	✓
MAC Spoof Detection	✓	✓	✓	✓	✓	✓
MAC and IP Spoof Block	✓	✓	✓	✓	✓	✓
Protected Nodes (Directly Connected)	Up to 25	Up to 100	Up to 500	Up to 1000	Up to 1500	Up to 2000
Total Protected and Managed Nodes (Via Multiple NetSHIELD Appliances)	Up to 25	Up to 100	Up to 500	Up to 6000	Up to 50,000	Up to 100,000
Subnets (Directly Connected)	2	2	2	4	6	8
Multi-VLAN Protection	10 VLANs	10 VLAN	20 VLANs	40 VLANs	60 VLANs	80 VLANs
Command Center Software	–	–	–	✓	✓	✓
Number of Other NetSHIELD Appliances That Can Be Managed from Command Center	–	–	–	10	100	Unlimited
Manage Remotely from Command Center	✓	✓	✓	✓	✓	✓
Multiple User Logins	✓	✓	✓	✓	✓	✓
Workflow Engine	✓	✓	✓	✓	✓	✓
ISO 27001 Policy Tools	✓	✓	–	✓	✓	✓
Part Number	LVN5220A	LVN5230A	LVN5250A-R2	LVN5400A-R2	LVN5600A-R2	LVN5800A-R2
Daily Vulnerability and Malware Updates (12 Months) (Required)	LVN5220A-VW-1	LVN5230A-VW-1	LVN5250A-R2-VW-1	LVN5400A-R2-VW-1	LVN5600A-R2-VW-1	LVN5800A-R2-VW-1
Daily Vulnerability and Malware Updates (36 Months) (Optional)	LVN5220A-VW-3	LVN5230A-VW-3	LVN5250A-R2-VW-3	LVN5400A-R2-VW-3	LVN5600A-R2-VW-3	LVN5800A-R2-VW-3

About SnoopWall

SnoopWall is the world's first Counterveillance security company delivering a suite of products from the enterprise to the endpoint, protecting all computing devices from prying eyes and new threats through patented cloaking technology. SnoopWall secures mission critical and highly valuable confidential information behind and beyond firewalls and on mobile devices with next generation technology that detects and blocks all rogue network access, remote control, eavesdropping and spying.

CVE® is a registered trademark of the Mitre Corporation. Any third-party trademarks appearing in this brochure are acknowledged to be the property of their respective owners. The CVE® Program is funded by the U.S. Department of Homeland Security.