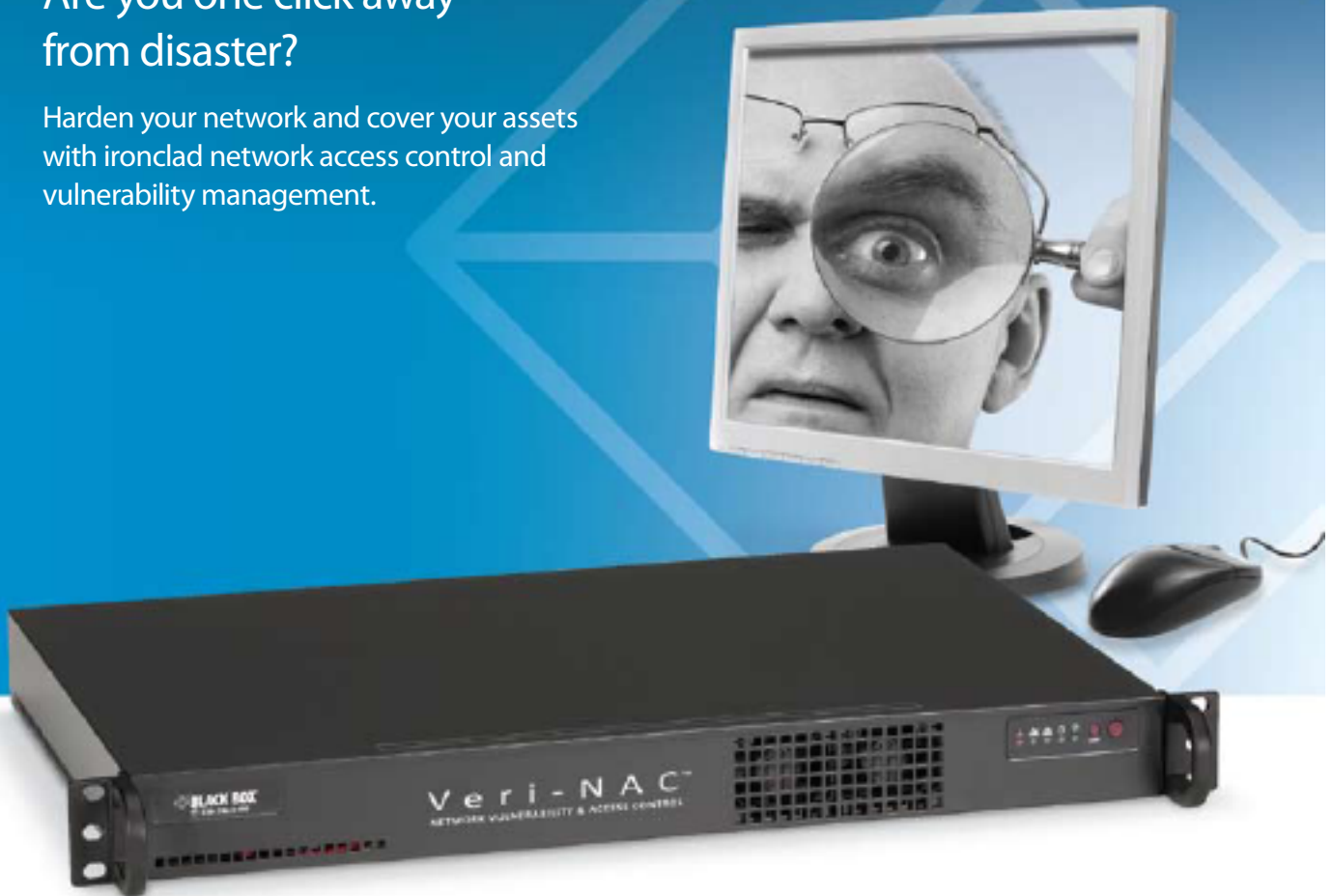


Network Access Control

Are you one click away from disaster?

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.

V e r i - N A C[™]
NETWORK VULNERABILITY & ACCESS CONTROL



Vulnerability Management and Network Access Control

Control who can connect to your network. Unknown laptops and unauthorised wireless access points are no longer a problem.

Discover and understand your network asset topology, complete with documentation.

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

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



More than 95% of security breaches are a direct result of exploiting a Common Vulnerability and Exposure (CVE) .

Can you afford a network breach?

A network breach is more than just embarrassing — it can expose your organisation to all kinds of potential liabilities and expenses. Just look at these examples:

- Recently a major hotel chain advised guests by way of letters and full-page newspaper ads that guests who stayed at their properties between November 2008 and May 2009 may have had their credit card numbers compromised.
- In April 2005, someone broke into NASA's super-secure Kennedy Space Centre network and inserted a malignant software program, which surreptitiously sent data to a computer system in Taiwan.
- In 2007, at least 45.7 million credit and debit card numbers were stolen from a number of retailers. The hacker was thought to have accessed the network through an unsecured wireless connection at a store.
- In 2009, a hacker was charged with the greatest data theft ever seen—130 million debit and credit card numbers from a number of organisations.
- In 2008, the Identity Theft Resource Center (ITRC) reported a 50% increase in reported data thefts and network breaches from the previous year.

Don't be the next security breach headline!

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. Unauthorised devices connected to your network are major threats to any organisation. This is what a NAC appliance is designed to prevent, whether the vulnerability is a LAN port in a communal area or conference room, or a wireless access point.

Veri-NAC™ is a family of Network Access Control (NAC) appliances from Black Box that ensures that only authorised devices and users 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 Veri-NAC 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.



- 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.
- Works with both wired and wireless devices.
- Protects your network from vulnerabilities that firewalls can't defend against.

Designed for simplicity

NAC solutions have been around for a while, but 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.

Veri-NAC, 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—Veri-NAC is easy to integrate into your network.



80% of all successful network attacks originate inside your network from uncontrolled connections from, for instance, rogue access points or unauthorised laptops.

SC Magazine Product Rating

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

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. We give Veri-NAC our Recommended this month.



Only the trusted

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

Every device has a unique, factory-installed MAC address. Veri-NAC assembles a profile of each device, including the MAC address, and only lets known, trusted devices on the network. It can even detect and stop a machine trying to get in under a spoofed MAC address.

Veri-NAC also checks to make sure each connected machine complies with your standards, including up-to-date operating system, patch management, and hardened configurations. If a machine isn't up to snuff, its user is locked out of the network except for the resources the user needs to bring the computer into compliance.

Protects continuously

Veri-NAC continually scans your network, looking for unauthorised devices attempting to obtain an IP address. In addition, you can schedule the Veri-NAC to scan attached devices to search for security vulnerabilities.

No agents

Unlike many other NAC systems, Veri-NAC doesn't require that you install software agents on connected machines. This both simplifies installation and improves security because agents are vulnerable to hacking.

Cost effective

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

Veri-NAC works with your existing network and legacy infrastructure, so there's no need for expensive upgrades. Plus, Veri-NAC requires no formal training and minimal installation time, so even organisations with a limited IT staff can easily add it to their network security plan without straining resources.

Fast, straightforward setup

This capable NAC system takes just minutes to install. Veri-NAC is literally a turnkey network appliance — just plug it in, turn it on, and follow the simple on-screen instructions to configure it. There's no need to upgrade your hardware or operating systems. The simplified user interface has practically no learning curve.

NAC setup

Find Network Assets

IP Subnet Range:

Base IP Address:

Subnet Mask:

NIC:

Use deeper probes for low bandwidth networks

Use NetBIOS Scans for host names

Use NetBIOS Scans for MAC addresses

Auto-Detecting Assets

IP Address	Host Name	Operating System	MAC Address
192.168.254.1	myServer	Linux 2.4.6 - 2.4.26 or 2.6.9	00:0D:5A:52:CA:4C (SafeWare Technologies)
192.168.254.8			00:15:00:2D:16:43 (Hewlett Packard)
192.168.254.54			00:11:42:34:8D:05 (Dell)
192.168.254.930	192.168.254.930	FreeBSD 6.27 (SMP) (SMP) Linux 2.4.0 - 2.5.20	00:04:56:34:05:A7 (Extreme Networks)
192.168.254.303			00:0C:41:9F:1C:81 (The Linksys Group)
192.168.254.392	192.168.254.392	Linux 2.4.6 - 2.4.26 or 2.6.9	00:09:4D:34:D5:D9 (Lenovo)
192.168.254.390	192.168.254.390	Linux 2.4.0 - 2.5.20	00:90:AF:01:0B:7D (Novera Digital)
192.168.254.859	192.168.254.859	Linux 2.4.0 - 2.5.20	00:04:2F:A8:22 (VIA Technologies)
192.168.254.340	192.168.254.340	Linux 2.6.8 - 2.4.11	00:0D:49:5A:59:83 (Dell)
192.168.254.361	192.168.254.361	Linux 2.4.0 - 2.5.20	00:30:4B:54:A3:5C (Supermicro Computer)
192.168.254.363	192.168.254.363	Linux 2.4.0 - 2.5.20	00:30:4B:3E:37:C2 (Supermicro Computer)
192.168.254.364	192.168.254.364	Linux 2.4.0 - 2.5.20	00:30:4B:3E:04 (Supermicro Computer)
192.168.254.366			00:30:4B:5A:AC:0C (Supermicro Computer)
192.168.254.957			00:40:1F:A:85:40 (VIA Technologies)
192.168.254.370	192.168.254.370	Microsoft Windows	00:15:72:7A:AF:41 (Dell)

Adding and deleting nodes from subnet

System Information

IP Address:

MAC Address:

Host Name:

Operating System:

Manufacturer:

Value:

System Name:

System Type:

Serial Number:

Location:

Data Outlet Num:

Asset Notes:

Add system to:

- Untrust list
- Trust and Audit-...
- Trust and Firewall
- Trust list

* Required field

• Data detected by Asset Discovery

Managing Assets: Trusted or Untrusted

Refresh Page Legends Explained

IP Address	Trusted	Host Name	Operating System	Remove Selected IPs
Subnet: 192.168.1				
192.168.1.1	N	192.168.1.1	Other, Mac: 00:14:6C:15:CE:AA	Remove All
192.168.1.2	Y	MA1W-C15OCB4A01	Microsoft Windows 2003 Server or XP SP2, Mac: 00:50:BD:1E:88:DB (Belkin Components)	Remove All
192.168.1.3	Y	192.168.1.3	Unknown, Mac: 00:25:BC:AF:CF:D3	Remove All
192.168.1.4	Y	192.168.1.4	Unknown, Mac: 00:04:76:DE:3E:DC (3Com)	Remove All
192.168.1.5	Y	192.168.1.5	Unknown, Mac: 00:0B:7D:1E:4E:3F	Remove All
192.168.1.220	Y	192.168.1.220	Linux 2.4.0 - 2.5.20, Mac: unknown	Remove All
Subnet: 192.168.20				
192.168.20.220	N	192.168.20.220	Linux 2.4.0 - 2.5.20, Mac: 00:E0:ED:09:DC:9F	Remove All
Subnet: 192.168.30				
192.168.30.220	Y	192.168.30.220	Linux 2.4.0 - 2.5.20, Mac: 00:30:4B:39:6F:4E	Remove All
Subnet: 192.168.40				
192.168.40.220	Y	192.168.40.220	Linux 2.4.0 - 2.5.20, Mac: unknown	Remove All
Subnet: 192.168.50				
192.168.50.220	Y	192.168.50.220	Linux 2.4.0 - 2.5.20, Mac: 00:70:ED:05:DC:A0	Remove All

Detailed reports

Veri-NAC displays network vulnerability information in colourful, easy-to-interpret graphs and charts. With one glance, you can view the status of your network and of each node within your network. Veri-NAC tracks and logs common vulnerabilities and exposures (CVEs), documenting end-user policies for regulatory compliance initiatives.

Remote operations

Device Status	Threat Potential	CVE Audit Status	Corporate	Description
			Corporate	Main Campus
		—	Sales Offices	N.A. Sales
		—	Mfg. Group	Assembly Sites
		—	Device	
		—	Pittsburgh	
		—	Dallas	
		—	San Jose	

Veri-NAC 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

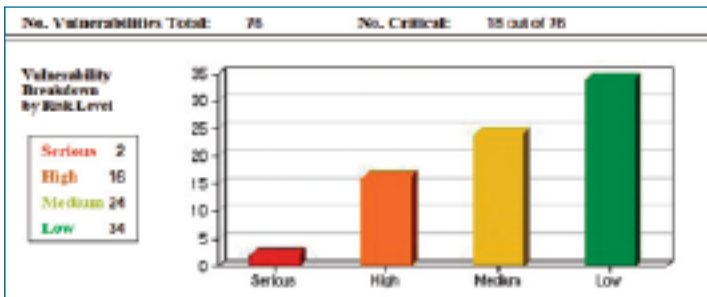
Threat Potential

- Untrusted Asset blocked by Veri-NAC
- Untrusted Asset on network - confirm identity
- All connected devices are known, trusted assets

CVE Audit Status

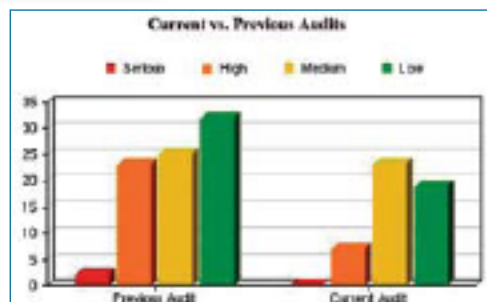
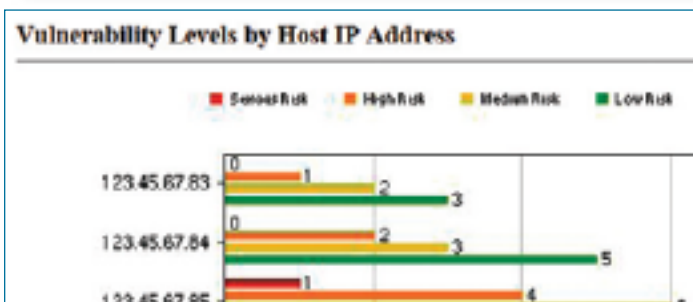
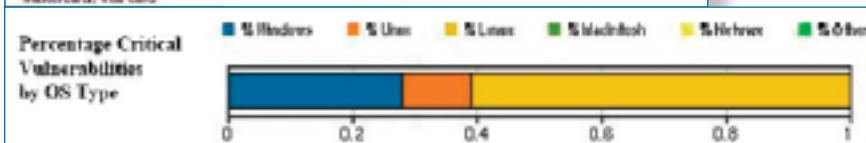
- CVE Audit currently running
- Audit revealed critical vulnerabilities - fix immediately
- Audit revealed moderate vulnerabilities
- Audit revealed no vulnerabilities

Interpreting vulnerability



Regulatory Compliance Status
The audit result indicates that the system(s) may be out of compliance with the following regulations:
E-Sign, Sarbanes Oxley

Credit Card Merchant Program Status
The audit result indicates that the system(s) may be out of compliance with the following merchant program:
MasterCard, Visa Card



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

A: For a complete security plan, you do need both a firewall and 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, on the other hand, 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 non-compliant, NAC may deny access or quarantine it. NAC appliances, on the other hand, are “asset cops” and protect your network from inside threats.

Q: How does Veri-NAC 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 smart-phones to access the Internet, Veri-NAC can grant them access to only the Internet while restricting them from your organisation’s intranet.

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

A: You can set Veri-NAC to respond differently to non-compliant computers, depending on the situation. For instance, if Veri-NAC detects a device with an unknown MAC address, it can lock that device out 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 Veri-NAC 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, smart phones or PDAs, barcode scanners, IP door locks, and access points, leaving many network devices outside of the capabilities of agent-based NAC solutions. Black Box intentionally designed Veri-NAC without agents.

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

A: Yes, the 5400, 5600, and 5800 Veri-NAC models have a Command Centre, which enables you to access all units globally and across remote locations from a central point. Multiple Veri-NAC appliances may share the same trusted MAC address list and the same set of policies. You may also assign the same password to every Veri-NAC appliance in your network.

Q: Does Veri-NAC impair network performance?

A: No, Veri-NAC isn’t an in-line device, and won’t negatively affect network performance. Under normal conditions, Veri-NAC 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 Veri-NAC require 802.1x switches?

A: No. Veri-NAC 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.



Company	Product	Price per Class C subnet	Average setup time and training	Completely agentless and non-inline hardened	IP and MAC spoof protection	Includes compliance and assessment reporting tools	Includes CVE certified auditing	Includes workflow and CVE reporting
Black Box Veri-NAC	5200 5250	£	30 Minutes	Yes	Yes	Yes	Yes	Yes
Black Box Veri-NAC	5400 5600 5800	£	45 Minutes	Yes	Yes	Yes	Yes	Yes
Cisco Systems Inc.	Network Access Control (NAC)	££££	2 Weeks	No	No	No	No	No
Microsoft Corporation	Network Access Protection (NAP)	££££	2 Weeks	No	No	No	No	No
Juniper Networks	Unified Access Controller (UAC)	££££	1 Week	No	No	No	No	No
Enterasys Networks, Inc.	Sentinel	£££	2 Days	No	No	No	No	No
Check Point Software Technologies Ltd.	Integrity	£££	3 Days	No	No	No	No	No
ForeScout Technologies	CounterACT*	££	2 Days	No	No	No	No	No
Mirage Networks, Inc.	CounterPoint	££	2 Days	No	No	No	No	No
Symantec Corporation	Network Access Control 11	££	4 Days	No	No	No	No	No
Bradford Networks	NAC Director*	££	2 Days	No	No	No	No	No
Sophos Plc.	NAC Advanced	££	3 Days	No	No	No	No	No

Sized for every network

Veri-NAC comes in models for every application from small-office networks to large enterprise networks containing thousands of devices. Models 5400/5600/5800 include the Command Center for secure central management of multiple Veri-NAC appliances so you can protect your entire organisation from edge to core. These models also include ISO 27001 Policy Tools to simplify your organisation's compliance efforts.



Buyer's Guide | Veri-NAC

Model	5200	5250	5400	5600	5800
Form Factor	1U High, 11.5 " Deep	1U High, 11.5 " Deep	1U High, 14 " Deep	1U High, 14 " Deep	1U High, 14 " Deep
Agentless NAC	✓	✓	✓	✓	✓
Endpoint Vulnerability Auditing	—	✓	✓	✓	✓
Maximum Simultaneous Device Audits	—	10	50	100	250
Auto Device Discovery	✓	✓	✓	✓	✓
Inventory Alerting	✓	✓	✓	✓	✓
MAC Spoof Detection	✓	✓	✓	✓	✓
MAC and IP Spoof Block	✓	✓	✓	✓	✓
Protected Nodes (Directly Connected)	Up to 250	Up to 500	Up to 1000	Up to 1500	Up to 2000
Total Protected and Managed Nodes (Via multiple Veri-NAC appliances)	Up to 250	Up to 500	Up to 6000	Up to 50,000	Up to 100,000
Subnets (Directly Connected)	2	2	4	6	8
Multi-VLAN Protection	10 VLANs	20 VLANs	40 VLANs	60 VLANs	80 VLANs
Command Center Software	—	—	☒	☒	☒
Number of Other Veri-NAC 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	LVN5200A	LVN5250A	LVN5400A	LVN5600A	LVN5800A
List Price	CALL	CALL	CALL	CALL	CALL
Extension of Service/Support/Warranty (12 Additional Months)	CALL	—	—	—	—
Extension of Service/Support/Warranty (36 Additional Months)	CALL	—	—	—	—
Extension of Daily Vulnerability & Extended Warranty (12 Additional Months)	—	CALL	CALL	CALL	CALL
Extension of Daily Vulnerability & Extended Warranty (36 Additional Months)	—	CALL	CALL	CALL	CALL

© Copyright 2010. All rights reserved. Black Box Corporation. Black Box® and the Double Diamond logo are registered trademarks, and Veri-NAC™ and Optinet™ are trademarks, of BB Technologies, Inc. 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.