

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.

Veri-NAC™
NETWORK VULNERABILITY & ACCESS CONTROL



Vulnerability Management and Network Access Control

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

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

Detect malware and quarantine untrusted assets.

Manage IPs with Active Director.

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 organization 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 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 organizations.
- 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. Unauthorized devices connected to your network are major threats to any organization. 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.

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

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.

- 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 black holing and VLAN quarantining of untrusted assets.
- Detects malware on infected devices.

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 user login and 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. If Veri-NAC detects an untrusted asset, it will automatically send administration an alert to investigate and correct the problem.

Veri-NAC models 5250 and higher also include an endpoint vulnerability auditing engine featuring the common vulnerability and exposures (CVE) database, which checks to make sure each connected device complies with your standards, including up-to-date operating system patches. This auditing function works for all connected devices, not just PCs.

Protects continuously.

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



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

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	★★★★★



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.

Detection and blocking.

Quarantine or block malware-infested PCs—even zero-day malware that would otherwise go unchecked by standard virus-protection software. You can then use a file retrieval product, such as our Data Rescue Engine, to get important files without spreading the infection.

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. Agentless design means that Veri-NAC also works with devices such as printers, smartphones, and wireless access points that can't have agents installed in them.

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 organizations with a limited IT staff can easily add it to their network security plan without straining resources.

Vulnerability Management and Network Access Control

Perceiving threats.

Veri-NAC offers a great deal of flexibility in how it responds to perceived threats. For instance, if Veri-NAC detects a device with an unknown user/MAC address, it can lock out that device entirely or limit it to only a guest VLAN that you set up.

Guests.

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, Veri-NAC can grant them access only to the Internet via a guest VLAN while restricting them from your organization's intranet.

Remote operations

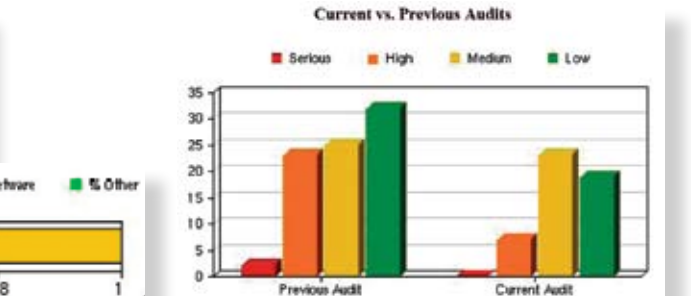
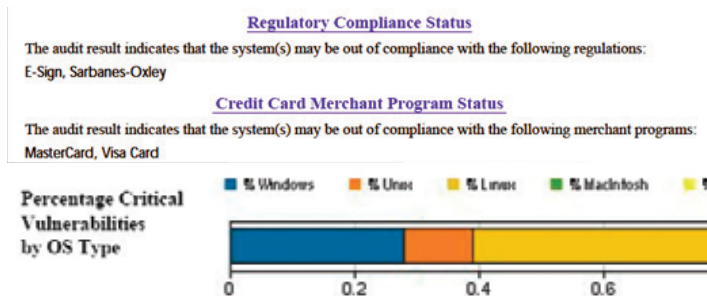
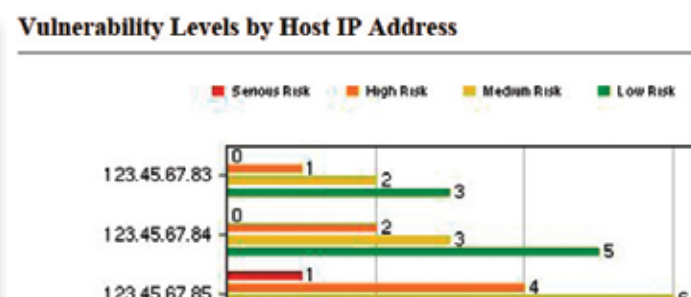
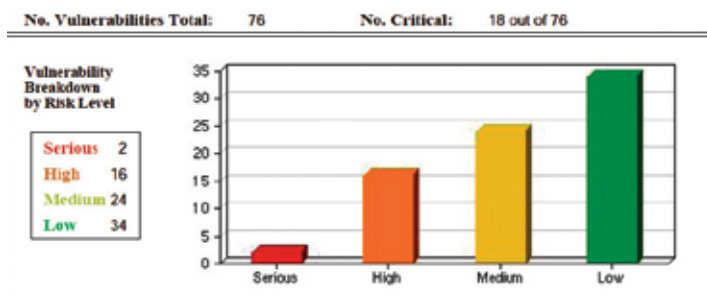
Device Status	Threat Potential	CVE Audit Status	Location
			Corporate
			Corporate
		—	Sales Offices
		—	Mfg. Group
			Device
		—	Pittsburgh
		—	Dallas
		—	San Jose

VLAN quarantining.

Veri-NAC works with all 802.1q-enabled switches to protect VLANs. It will permit users to connect to authorized VLANs but will deny access if they attempt to access restricted VLANs. You can also assign trusted assets to multiple VLANs. Veri-NAC 5800 protects up to 80 VLANs. Other Veri-NAC models protect fewer.

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



Two ways to detect the bad guys.

Veri-NAC™ can do far more than just provide network access control. Daily Vulnerability and Malware Update software is available separately in one- and three-year packages. It enables Veri-NAC to check over the Internet for common vulnerabilities and exposures plus malware trying to call home. You can choose from one- or three-year plans for all Veri-NAC models. See the Buyer's Guide ([back cover](#)).

Daily vulnerability updates.

Veri-NAC uses Daily Vulnerability Updates to track and log common vulnerabilities and exposures (CVEs). It alerts you whenever an attached device has a problem that would leave it vulnerable to a hacker, so you can take steps to rectify the situation.

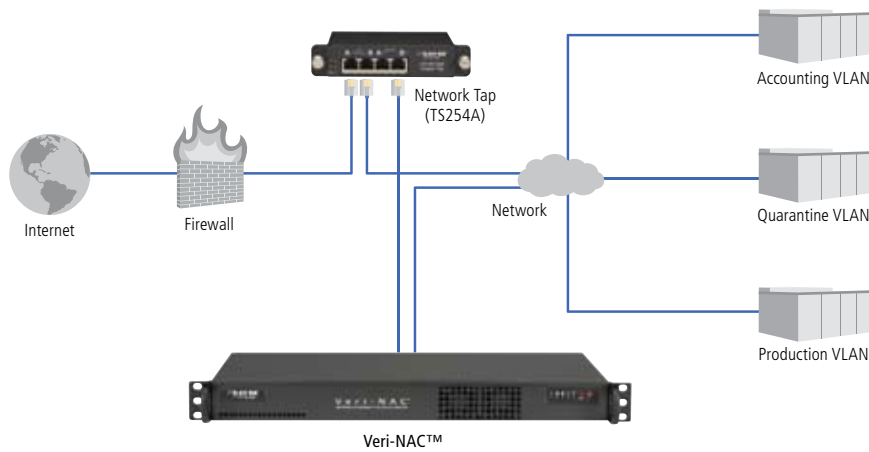
Daily malware updates.

Veri-NAC now gives you two methods for detecting previously undetectable malware. It takes advantage of the fact that most malware tries to “call home.”

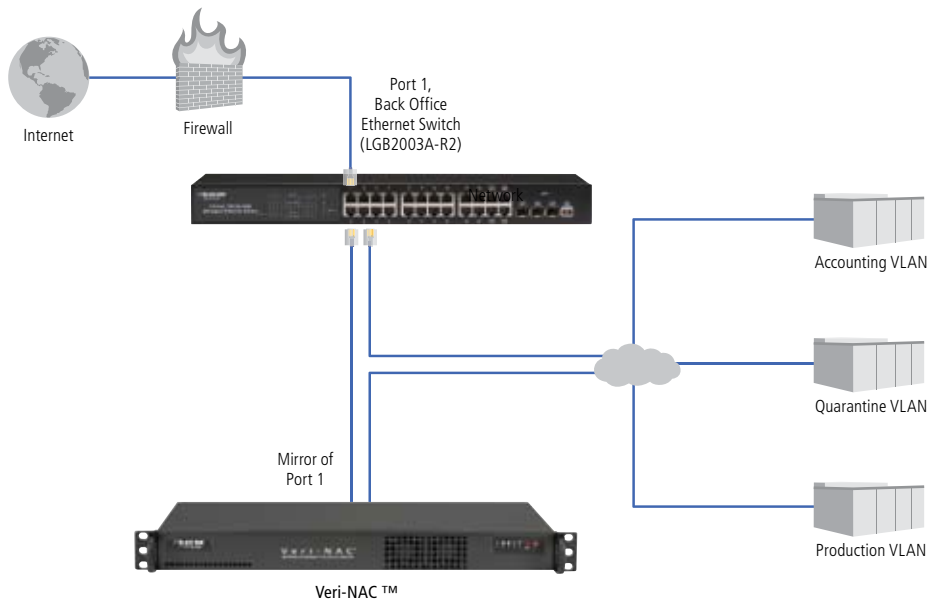
In the first method, simply add a network tap near the firewall. The second method involves setting up a mirror port on your network switch. In both applications, Veri-NAC will keep watch for outgoing network traffic going to known malware repositories.

The second method, switch port blocking, works with Cisco, 3Com®, HP® and Extreme Networks® switches. If Veri-NAC detects an untrusted asset, it physically turns off the switch port by location so it is, in essence, “dead” until the administrators turn it back on.

Malware Detection — Application 1: Network Tap



Malware Detection — Application 2: Ethernet Switch Port Mirroring



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

Detailed reports

Veri-NAC displays network vulnerability information in colorful, 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.

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-exempt lists

Trust and Firewall/SmartSwitch safe lists

Trust list

* Required field

Data detected by Asset Discovery

Managing assets: trusted or untrusted

Trust / Untrust List

IP Address	Trusted	Host Name	Operating System	Remove Selected IPs
Subnet 192.168.1 <input type="button" value="Remove All"/>				
<input type="checkbox"/> 192.168.1.1	N	192.168.1.1	Other, Mac: 00:14:6C:15:0E:AA	
<input type="checkbox"/> 192.168.1.2	Y	MALW-C13CCB4A01	Microsoft Windows 2003 Server or XP SP2, Mac: 00:30:BD:1E:B8:DB (Belkin Components)	
<input type="checkbox"/> 192.168.1.3	Y	192.168.1.3	Unknown, Mac: 00:25:BC:AF:CF:D3	
<input type="checkbox"/> 192.168.1.4	Y	192.168.1.4	Unknown, Mac: 00:04:76:DE:3E:DD (3 Com)	
<input type="checkbox"/> 192.168.1.5	Y	192.168.1.5	Unknown, Mac: 00:0B:7D:1E:6E:3F	
<input type="checkbox"/> 192.168.1.220	Y	192.168.1.220	Linux 2.4.0 - 2.5.20, Mac: unknown	
Subnet 192.168.20 <input type="button" value="Remove All"/>				
<input checked="" type="checkbox"/> 192.168.20.220	N	192.168.20.220	Linux 2.4.0 - 2.5.20, Mac: 00:E0:ED:09:DC:9F	
Subnet 192.168.30 <input type="button" value="Remove All"/>				
<input type="checkbox"/> 192.168.30.220	Y	192.168.30.220	Linux 2.4.0 - 2.5.20, Mac: 00:30:48:B9:6F:4E	
Subnet 192.168.40 <input type="button" value="Remove All"/>				
<input type="checkbox"/> 192.168.40.220	Y	192.168.40.220	Linux 2.4.0 - 2.5.20, Mac: unknown	
Subnet 192.168.50 <input type="button" value="Remove All"/>				
<input type="checkbox"/> 192.168.50.220	Y	blackbox	Linux 2.4.0 - 2.5.20, Mac: 00:E0:ED:09:DC:A0	

Auto-detecting assets

Found 31 hosts ...

IP Address	Host Name	Operating System	MAC Address
192.168.254.1	my.firewall	Linux 2.4.6 - 2.4.26 or 2.6.9	00:08:DA:53:CA:6C (SofaWare Technologies)
192.168.254.4			00:15:60:2D:36:40 (Hewlett Packard)
192.168.254.54			00:11:43:74:FD:0F (Dell)
192.168.254.100	192.168.254.100	FreeSCO 0.27 (Linux 2.0.38), Linux 2.4.0 - 2.5.20	00:04:96:34:CB:AF (Extreme Networks)
192.168.254.103			00:0C:41:97:7C:B2 (The Linksys Group)
192.168.254.132	192.168.254.132	Linux 2.4.6 - 2.4.26 or 2.6.9	00:03:6D:14:D1:D9 (Runtop)
192.168.254.158	192.168.254.158	Linux 2.4.0 - 2.5.20	00:90:A9:01:9B:72 (Western Digital)
192.168.254.159	192.168.254.159	Linux 2.4.0 - 2.5.20	00:40:63:FA:E3:32 (VIA Technologies)

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 non-compliant, NAC may deny access or quarantine it.

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 smartphones to access the Internet, Veri-NAC 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 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 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 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, 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. 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 Center, 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.

Q: Why would I use 802.1q VLAN tagging?

A: This feature makes your Veri-NAC even more efficient. It enables you to protect a large or complex network that uses VLANs without adding another Veri-NAC appliance. To have one Ethernet port of your Veri-NAC 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 Veri-NAC appliance to the port on your smart switch where you have the tagged VLANs mapped.



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 Command Center software for secure central management of multiple Veri-NAC 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 | Veri-NAC

Model	5200	5250	5400	5600	5800
Feature	1U High, 11.5" Deep	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	(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	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-R2	LVN5250A-R2	LVN5400A-R2	LVN5600A-R2	LVN5800A-R2
Daily Vulnerability and Malware Updates (12 Months)	LVN5200A-R2-XW-1*	LVN5250A-R2-VW-1	LVN5400A-R2-VW-1	LVN5600A-R2-VW-1	LVN5800A-R2-VW-1
Daily Vulnerability and Malware Updates (36 Months)	LVN5200A-R2-XW-3*	LVN5250A-R2-VW-3	LVN5400A-R2-VW-3	LVN5600A-R2-VW-3	LVN5800A-R2-VW-3

*The 5200 package only includes firmware updates and does not include vulnerability and malware updates.

About Black Box

Black Box Network Services is a leading network and security solutions provider, serving 175,000 clients in 141 countries with 195 offices throughout the world. The Black Box catalog and Web site offer more than 118,000 products, including network security products such as Optinet™ for bandwidth management and network optimization. More information is available at <http://www.blackbox.com/go/Optinet>.

Black Box also offers firewalls, Ethernet switches, and media converters, as well as cabinets, racks, cables, connectors, and other networking and data infrastructure products. To view Black Box's comprehensive offering, visit our Web site at blackbox.com.

Black Box is also known as the world's largest technical services company dedicated to designing, building, and maintaining today's complicated data and voice infrastructure systems.

© 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.

BR00016-Veri-NAC_v5-unpriced.indd