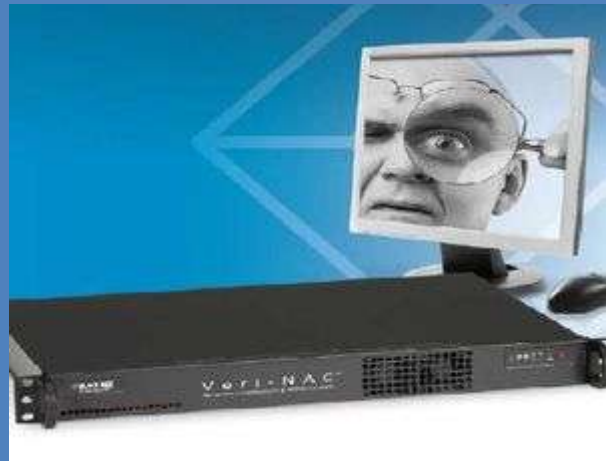


Control de Acceso a Redes (NAC)

¿Se encuentra a un 'clic' del desastre?

Refuerce su red y proteja sus activos con un control férreo de acceso a la red y gestión de vulnerabilidad.



Conozca los hechos y obtenga la protección con la que no puede vivir.

Veri-NAC™

NETWORK VULNERABILITY & ACCESS CONTROL



Gestión de Vulnerabilidad y Control de Red

Controlar quién puede conectarse a la red. Ordenadores desconocidos y puntos de acceso inalámbricos ya no son un problema.

Descubrir y entender la topología de su red, con una completa documentación.

Proteger su red — encontrar y arreglar los agujeros de seguridad antes de que alguien pueda explotarlos.

Cumplir con los requerimientos de GLBA, HIPAA, PCI, ISO 27001, y otros estándares de privacidad y seguridad.



Más del 95% de las brechas de seguridad son el resultado directo de la explotación de una vulnerabilidad y exposición común (CVE)®.

¿Puede permitirse una intrusión en su red?

Una intrusión en la red no es sólo algo incómodo; puede exponer a su organización a todo tipo de responsabilidades y gastos. Basta con mirar los siguientes ejemplos:

- Recientemente, una importante cadena hotelera avisó a sus clientes por medio de cartas y anuncios en los periódicos, a toda página, que los números de las tarjetas de crédito de los huéspedes que se alojaron en sus instalaciones entre Noviembre del 2008 a Mayo del 2009 podrían estar en peligro.
- En Abril del 2005, alguien entró en la red super segura del Centro Espacial Kennedy de la NASA, e introdujo un programa de software maligno, que subrepticamente enviaba datos a un sistema informático de Taiwan.
- En 2007, al menos 45,7 millones de números de tarjetas de crédito fueron robadas de una serie de minoristas. El hacker tuvo acceso a la red mediante la conexión segura inalámbrica de las tiendas.
- En 2009, un hacker fue acusado del robo de datos más grande jamás visto — 130 millones de números de tarjetas de crédito de un gran número de organizaciones.
- En 2008, el Identity Theft Resource Center (ITRC) informó de un aumento del 50% en los robos de datos y de accesos no autorizados en la red con respecto al año anterior.

¡No sea el siguiente en sufrir una violación de seguridad en la red!

Usted ya dispone de un servidor de seguridad para detener a los hackers, virus y malware en la entrada de su red. Un servidor de seguridad es vital para trabajar con una red segura, pero, debido a que opera en la entrada de su red, sólo puede protegerle de amenazas procedentes del exterior.

Los dispositivos NAC, por el contrario, protegen su red contra amenazas que se originan en el interior. Dispositivos no autorizados conectados a la red son las principales amenazas en cualquier organización. Los dispositivos NAC están diseñados para prevenir la vulnerabilidad de un puerto LAN de un vestíbulo o sala de conferencias o de un punto de acceso inalámbrico.

Veri-Nac™ es la familia de Control de Acceso a Redes (NAC) de Black Box, que garantiza que sólo los dispositivos y los usuarios autorizados obtengan acceso a la red. También protegen contra vulnerabilidades respecto a los ordenadores conectados a la red, usuarios con accesos móviles, equipos inalámbricos y nuevos dispositivos. Si Veri-Nac™ detecta un equipo activo sin confianza, responde al instante cerrando el acceso a la red para ese dispositivo — Protege su red y mantiene a los dispositivos de confianza de forma segura.



- Gestión de vulnerabilidad y control de acceso de red (NAC) en 'una sola caja'.
- Sin agente y el diseño no-en línea proporciona una seguridad sólida, como una roca, en un dispositivo fácil de instalar.
- No es necesario mejorar la infraestructura — trabaja con los conmutadores existentes.
- Trabaja con todos los tipos de dispositivos, ya sean por cable o inalámbricos.
- Protege su red contra vulnerabilidades que los cortafuegos no pueden defenderse.

Diseñado para la sencillez

Desde hace tiempo las soluciones NAC están disponibles, pero han tardado en tener éxito porque son muy caras y a menudo tenemos que actualizar los equipos existentes. En pocas palabras, son demasiado complejos para poder ser útiles.

Por el contrario, Veri-NAC está diseñado para proporcionar la máxima seguridad fácilmente. No hay necesidad de un excesivo entrenamiento, ni personal especializado; no necesita instalar agentes de software, ni actualizar los conmutadores — Veri-NAC es fácil de integrar en su red.



El 80% de todos los ataques a la red con éxito se originan dentro de su red, por conexiones incontroladas, como puntos de acceso o portátiles no autorizados

Sólo confianza

Veri-NAC sólo permite el acceso a los ordenadores y dispositivos de red si cumple con las normas que usted especifique.

Cada equipo tiene una dirección única MAC instalada de fábrica. Veri-NAC crea un perfil para cada dispositivo,

incluyendo la dirección MAC, y sólo permite el acceso de equipos de confianza en la red. Incluso puede detectar y detener una máquina que está tratando de entrar con una dirección MAC falsa.

Calificación Producto por SC Magazine

Características	*****
Facilidad de Uso	*****
Rendimiento	*****
Documentación	*****
Soporte	*****
Relación calidad/ precio	*****
Evaluación total	*****



Para: Control absoluto de acceso dinámico y auditoría de dispositivos de red.

Votos en contra: No encontramos ninguno.

Veredicto: Una sólida suite de productos NAC con un claro enfoque en los sistemas de mantenimiento de los sistemas no autorizados u los usuarios de la red.

Nombramos a Veri-NAC como equipo recomendado de este mes.

Protección continúa

Veri-NAC escanea continuamente su red, en busca de dispositivos no autorizados que intenten obtener una dirección IP. Además puede programar Veri-NAC para escanear los dispositivos conectados a la búsqueda de vulnerabilidades de seguridad.

Ausencia de agentes

A diferencia de muchos otros sistemas NAC, Veri-NAC no requiere la instalación de un agente software en las máquinas conectadas. Esto simplifica la instalación y mejora la seguridad, ya que los agentes son vulnerables a intrusiones de Hackers.

Rentable

Veri-NAC no sólo tiene el precio más bajo comparado con otras soluciones NAC, sino que también la instalación y los costes de mantenimiento son más bajos. Veri-NAC funciona con su red e infraestructura existente, por lo que no hay necesidad de costosas actualizaciones. Además, Veri-NAC no requiere ninguna formación especial y el tiempo de instalación es mínimo, por lo que incluso las organizaciones con personal reducido pueden fácilmente agregarlo a su plan de seguridad de red, sin forzar los recursos.

Rápido, Fácil de Instalar

Esta solución NAC tarda sólo unos minutos en instalarse. Veri-NAC es, literalmente, un dispositivo de red llave en mano — basta con conectarlo, encenderlo y seguir las sencillas instrucciones en pantalla para configurarlo. No hay necesidad de actualizar el hardware o los sistemas operativos. La sencilla interfaz de usuario no requiere aprendizaje.

Configuración NAC

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

Detección Automática

Found 31 hosts ...

IP Address	Host Name	Operating System	MAC Address
192.168.254.1	my firewall	Linux 2.4.5 - 2.4.26 or 2.5.9	0008DA53CA6C (SofaWare Technologies)
192.168.254.4			0015602D3540 (Bowling Packard)
192.168.254.54			00114374FD0F (Dell)
192.168.254.100	192.168.254.100	FreeSOO 0.27 (Linux 2.0.38) Linux 2.4.0 - 2.5.20	00045634C5AF (Extreme Networks)
192.168.254.103			000C41977CB2 (The Linksys Group)
192.168.254.132	192.168.254.132	Linux 2.4.5 - 2.4.26 or 2.5.9	00036D14D1D9 (Rastop)
192.168.254.158	192.168.254.158	Linux 2.4.0 - 2.5.20	0090A9019D72 (Western Digital)
192.168.254.159	192.168.254.159	Linux 2.4.0 - 2.5.20	004063FAE332 (VIA Technologies)
192.168.254.160	192.168.254.160	Linux 2.4.8 - 2.6.11	000E609A58B0 (IBM)
192.168.254.161	192.168.254.161	Linux 2.4.0 - 2.5.20	00304884AB5C (Supermicro Computer)
192.168.254.163	192.168.254.163	Linux 2.4.0 - 2.5.20	0030485B57C2 (Supermicro Computer)
192.168.254.164	192.168.254.164	Linux 2.4.0 - 2.5.20	00304883FD84 (Supermicro Computer)
192.168.254.166			003048BA90BC (Supermicro Computer)
192.168.254.167			004063FAE340 (VIA Technologies)
192.168.254.170	192.168.254.170	Microsoft Windows	0013727AAEA1 (Dell)

Agregar y eliminar nodos de la subred

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

Trust and Firewall/Smart

Trust list

* Required field

Data detected by Asset Discovery

Gestor equipos activos: De confianza o No Confianza

Asset Count: 56
Manage
Trust / Untrust List

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:15:0EAA	<input type="button" value="Remove All"/>
192.168.1.2	Y	MALW-C13CCB4A01	Microsoft Windows 2003 Server or XP SP2, Mac: 00:30:ED:1E:B8:DB (Belkin Components)	
192.168.1.3	Y	192.168.1.3	Unknown, Mac: 00:25:BC:AF:CF:D3	
192.168.1.4	Y	192.168.1.4	Unknown, Mac: 00:04:76:DE:3E:DD (3 Com)	
192.168.1.5	Y	192.168.1.5	Unknown, Mac: 00:0E:7D:1E:6E:3F	
192.168.1.220	Y	192.168.1.220	Linux 2.4.0 - 2.5.20, Mac: unknown	
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	<input type="button" value="Remove All"/>
Subnet 192.168.30				
192.168.30.220	Y	192.168.30.220	Linux 2.4.0 - 2.5.20, Mac: 00:30:48:B9:6F:4E	<input type="button" value="Remove All"/>
Subnet 192.168.40				
192.168.40.220	Y	192.168.40.220	Linux 2.4.0 - 2.5.20, Mac: unknown	<input type="button" value="Remove All"/>
Subnet 192.168.50				
192.168.50.220	Y	blackbox	Linux 2.4.0 - 2.5.20, Mac: 00:E0:ED:09:DC:9F	<input type="button" value="Remove All"/>

Informes detallados

Veri-NAC muestra la información de vulnerabilidad en colores y en gráficos y tablas de fácil de interpretación. De un vistazo, puede ver el estado y cada nodo de su red. Veri-NAC crea registros y da pistas de las vulnerabilidades comunes y las exposiciones (CVE).

Operaciones Remotas

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

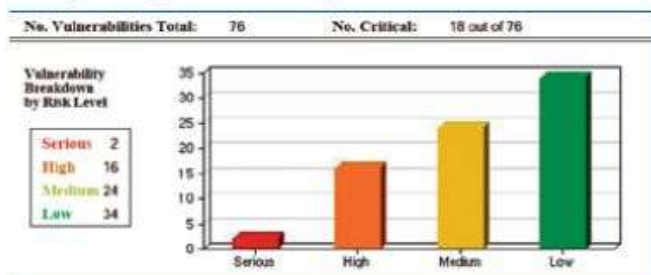
Threat Potential

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

CVE Audit Status

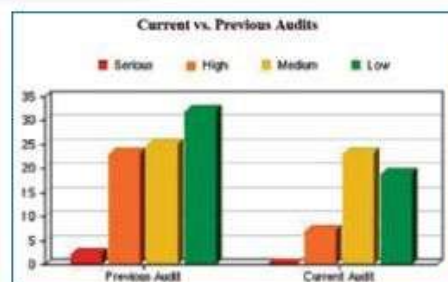
- CVE Audit currently running
- Audit revealed critical vulnerabilities - fix immediately
- Audit revealed moderate vulnerabilities
- Audit revealed no vulnerabilities

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 programs:
MasterCard, Visa Card



P: ¿Es necesario NAC si ya tenemos un servidor de seguridad?

R: Para tener un plan de seguridad completo, usted necesita un firewall y NAC, ya que protegen de manera muy diferente.

Un servidor de seguridad normalmente se coloca a la entrada de su red, inspecciona los datos procedentes de Internet, y niega o permite el tráfico de red basado en un conjunto de reglas.

Los firewall son 'policías de tráfico' y sólo protegen contra las amenazas procedentes de fuera de su red.

NAC por su parte, protege a los ordenadores y dispositivos móviles conectados a la red y decide si procede o no conceder el acceso a ellos. Si un dispositivo o equipo no cumple con las disposiciones, NAC puede negar el acceso o ponerlo en cuarentena. Las aplicaciones NAC son 'policías de servicio' y protegen su red contra las amenazas interiores.

P: ¿Cómo trata Veri-NAC a los ordenadores de los clientes?

R: Dispositivos y usuarios desconocidos - de clientes, por ejemplo - o bien se pueden permitir en la red, pero marcándolo como un activo en que no se confía, o bien se bloquean por completo. Si usted tiene visitantes que quieran utilizar su propio portátil o smart-phones para acceder a Internet, Veri-NAC puede conceder el acceso sólo a Internet, restringiendo el acceso a la intranet de su organización.

P: ¿Tiene un equipo que no cumpla con las normas bloqueado fuera de la red?

R: Puede configurar Veri-NAC para responder de manera diferente a los equipos no conformes, en función de la situación. Por ejemplo, si Veri-NAC detecta un dispositivo con una dirección MAC desconocida, puede bloquear ese dispositivo por completo o limitarlo a sólo una red de invitados. Si detecta un sistema vulnerable con el software obsoleto, puede bloquearlo o poner en cuarentena los puertos vulnerables, proporcionando acceso parcial a la red, mientras envía un mensaje a su personal IT para actualizar el software.

P: La mayoría de las ofertas de otros fabricantes NAC requieren un agente. ¿Puede Veri-NAC ser eficaz sin un agente?

R: ¡Sí! Inicialmente se pensaba que los agentes ayudaban a verificar la integridad de los dispositivos de red. Pero ahora todos los agentes son conocidos por ser fácilmente hackeables, creando una vulnerabilidad en su arquitectura de seguridad. Además, los agentes no pueden ejecutarse en la mayoría de dispositivos no PC, como los teléfonos VoIP, impresoras de

red, Smart-phones o PDA, escáneres de código de barras, cerraduras de puertas IP y puntos de acceso, dejando a muchos dispositivos fuera de las soluciones NAC basadas en agentes. Por estos motivos Black Box ha diseñado Veri-NAC sin agentes.

P: ¿Hay alguna manera de controlar de forma centralizada múltiples dispositivos Veri-NAC en nuestra red de la empresa?

R: Sí, Los modelos Veri-NAC 5400, 5600 y 5800 disponen un centro de mando, el cual le permitirá acceder a todas las unidades a nivel mundial o a través de lugares alejados de un punto central. Múltiples Veri-NAC pueden compartir la misma lista de direcciones MAC de confianza y el mismo conjunto de políticas. También es posible asignar la misma contraseña para todos los Veri-NAC.

P: ¿Perjudica Veri-NAC el rendimiento de la red?

R: No, Veri-NAC no es un dispositivo en-línea, y no afecta negativamente al rendimiento de la red. En condiciones normales, Veri-NAC utiliza sólo 7kbps de ancho de banda para bloquear usuarios y entre 40 y 120 kbps para la auditoría de las vulnerabilidades.

Esta pequeña cantidad de ancho de banda no es suficiente para hacer notar una diferencia en el rendimiento de la red.

P: ¿Veri-NAC require conmutadores 802.1x?

R: No. Veri-NAC trabaja con todos los conmutadores Ethernet, incluso con conmutadores de bajo coste. No hay necesidad de actualizar su infraestructura con conmutadores 802.1x.



La solución Competitiva

Veri-NAC de Black Box no sólo tiene precios competitivos, sino que también ofrece más funciones y requiere menos exigencias en su sistema que muchas otras soluciones NAC. Además, Veri-NAC dispone del Soporte Técnico Black Box gratuito.

Guía del comprador | Guía de comparación NAC

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

Tamaño para cada red.

Veri-NAC está disponible para todos los tamaños de red, desde las pequeñas oficinas a las grandes empresas con miles de dispositivos. Los modelos 5400/5600/5800 incluyen un centro de mando para la gestión segura de los equipos centrales Veri-NAC para que pueda proteger a toda su organización. Estos modelos también incluyen la Política de herramientas ISO 27001.



Guía del comprador | Guía de comparación 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	\$2850	\$4950	\$9850	\$18,950	\$33,950
Extension of Service/Support/Warranty (12 Additional Months)	\$425	—	—	—	—
Extension of Service/Support/Warranty (36 Additional Months)	\$1020	—	—	—	—
Extension of Daily Vulnerability & Extended Warranty (12 Additional Months)	—	\$980	\$1945	\$3680	\$6880
Extension of Daily Vulnerability & Extended Warranty (36 Additional Months)	—	\$2352	\$4668	\$8832	\$16,512

* Información de precios facilitada por SC Magazine y pueden no corresponder con la realidad.