

## NAC alternatives hit the mark

Got framework phobia? All-in-one products provide basic NAC features.

BY MANDY ADDRESS, NETWORK WORLD LAB ALLIANCE

Network-access control is a buzzword of epic proportion. And as is the case with much of larger-than-life industry vernacular, products with even the slightest aspect of access control are being pitched by their makers as integral components of the NAC fray.

In April, we assessed the role that more than 30 NAC products play in the larger NAC schemes defined by Cisco's Network Access Control (CNAC) initiative or the Trusted Network Connect (TNC) working group of the Trusted Computing Group (see "What can NAC do for you now?" at [www.nwdocfinder.com/9721](http://www.nwdocfinder.com/9721)).

We found that the basic functions of NAC can be carried out within CNAC or TNC, but not all IT shops have the time, inclination, network infrastructure or resources to deploy a full-blown NAC framework.

Enter the all-in-one approach to NAC — single products that provide authentication and authorization, endpoint-security assessment, NAC policy enforcement and overall management.

We tested 13 products from Bradford Networks, Check Point Software, Cisco, ConSentry Networks, ForeScout Technologies, InfoExpress, Juniper Networks, Lockdown Networks, McAfee, StillSecure, Symantec, Trend Micro and Vernier Networks.

To ensure continuity between our previous assessment of NAC architectures and these all-in-one NAC products, our testing was based on the same methodology. Authentication and authorization testing homed in on the options available for connecting to the network physically, the authentication options supported, and how authorization is handled by each product. While deploying NAC in an environment with standard

802.1X authentication was a focal point of our NAC-architecture testing, in this round we deployed products using other authentication options — for example, facilitating inline monitoring, controlling an installed network switch and acting as the access-layer switch itself — because many organizations will want to deploy NAC before they can do so using the 802.1X standard. All the vendors tested offer at least one alternative approach, so the good news is that there is no shortage of options.

Our environmental-information evaluation — sometimes referred to as an endpoint-security assessment — looked at how effectively each product gathers pertinent information from endpoints. The details collected range from general machine information to specific security settings, and all are used to enforce policy decisions.

The enforcement piece of this test evaluated the options available for handling offending systems once assessment is complete and the applicable policy identified. The final management section looked at the tools available for keeping the whole NAC system running, including defining new policies, receiving alerts and reporting, all within an accessible and usable interface.

The good news is that these products consistently functioned as advertised. Pretty much across the board, they identified, authorized (or blocked, as required) and helped remediate failed systems as their makers said they would. However, they carried out these measures in different ways and to varying degrees (see [www.nwdocfinder.com/9723](http://www.nwdocfinder.com/9723)), so to help determine which product is the best fit for you, you'll need to have a clear understanding of which areas covered by these NAC products are the most critical for your own environment.

### NETRESULTS

Product	Symantec Network Access Control V5.1	ForeScout CounterACT CT100	Lockdown Networks Enforcer 4.5.2	Unified Access Control 2.0
Vendor	Symantec <a href="http://www.symantec.com">www.symantec.com</a>	ForeScout Technologies <a href="http://www.forescout.com">www.forescout.com</a>	Lockdown Networks <a href="http://www.lockdownnetworks.com">www.lockdownnetworks.com</a>	Juniper Networks <a href="http://www.juniper.net">www.juniper.net</a>
Price	\$18,000 for 1,000 users.	Starts at \$14,000.	\$25,000 per appliance, which supports up to 2,000 users.	\$30,000 for 1,000 users.
Pros	Unique and powerful location-based policies; supports user- and device-based policies; intuitive; easy-to-navigate interface; very wide breadth of endpoint assessment capabilities.	Endpoint assessment timing can be configured on a check-by-check basis; wide variety of enforcement options; unique network portal is useful for data analysis; one of the stronger reporting engines tested.	Great administrative interface; strong reporting tools; very capable vulnerability scanning tool included.	Strong basic NAC components; integrates well into existing Juniper environment; easy to use.
Cons	Reporting engine could be improved to provide more options and functionality.	Workarounds to maintain agentless architecture may not sit well with some organizations.	Complex policy management.	Minimal reporting capabilities.
Score	<b>4.48</b>	<b>4.38</b>	<b>4.35</b>	<b>4.18</b>

# CLEAR CHOICE TEST NAC POINT PRODUCTS

Symantec came out on top as the best-all-around all-in-one NAC product. Although other products performed better in single categories, we found that Symantec's Network Access Control provided the most solid NAC functions across the board. ForeScout, Lockdown and Juniper rounded out the top finishers.

## Trends in NAC products

Our authentication and authorization tests showed that for the most part, these all-in-one NAC products slide pretty effectively into existing networks in a variety of ways. Authorizing access for known and guest users via general LAN links, remote-access connections and wireless LANs are all measures supported by most products. The technical implementation methods differ, but the goals of flexibility and pervasive coverage remain the same.

Common to the vast majority of products is integration with standard user directories, such as Microsoft's Active Directory and other Lightweight Directory Access Protocol-based repositories, and authentication servers, such as a RADIUS server. A key difference is that some products provide authentication by monitoring authentication traffic (for example, Kerberos authentication packets) passively and making note of the event, while others require the user to enter credentials actively.

Another key difference among the products is the endpoint information used during the authorization and enforcement processes. Some products rely on user information to enforce policies, while others grant access based solely on device information. A few products provide support for both approaches.

Juniper, Symantec and Vernier performed the best in our authorization and authentication testing. These products provided well-integrated deployment scenarios for our four connection methods (LAN, remote access, guest and wireless). They also supported a variety of technologies for authentication and let us configure authorization parameters based on either user or device.

Endpoint assessment tests evaluated out-of-the-box options for system compliance checks, focusing on antivirus software, Windows security patches, host firewall status, endpoint vulnerability status and identification of actively infected systems. Most products provided basic coverage and functions on the fundamental items. What differ-

entiated these products was how broadly they covered these assessment mechanisms; how easily they configured checks; how they manipulated the timing of checks; and whether they could implement more-detailed checks, such as when a product supports a general vulnerability-scanning engine. Products' ability to define custom security checks ranged from checking for certain registry keys and file properties to full scripting engines.

Symantec excelled in endpoint assessment and the collection of environmental information by providing the best all-around assessment function. ForeScout also performed well, providing enhanced assessment functions, such as anomaly detection and a full vulnerability-assessment platform.

Enforcement capabilities generally depended on the product's implementation. For example, in products that approached NAC by controlling the access switch, primary enforcement mechanisms included virtual LAN (VLAN) and access control list (ACL) changes. Inline deployments most frequently offered firewall rules to control network access, although some also provided VLAN changes by modifying 802.1Q tags.

While VLAN changes are easy to implement, the bigger issue for users is the network infrastructure's overall VLAN design and management, compared with how detailed their NAC policies will be. Having different access policies for different corporate functions — and even different access policies if endpoint systems are not in compliance — could quickly become a VLAN management nightmare.

Another common enforcement mechanism is self-enforcement, facilitated by heavy-handed client software in which an agent controls network access. Self-enforcement is beneficial in that it helps ensure compliance when a user isn't connected to the corporate network, but you've got to factor in that the endpoint could be compromised. We recommend using self-enforcement along with a network-based enforcement mechanism, such as pushing a firewall rule, making a VLAN change or facilitating an ACL change on a switch.

Remediation efforts tended to guide users through the process of bringing their own machines up to NAC snuff. The measures provided generally included displaying a message containing a URL leading users to information or software that will let them self-remediate. Some products provided more proactive remediation functions, such as killing a process or automatically executing a program — for instance, launching a patch-

## NETRESULTS

Product	ConSentry LANShield switch and InSight Manager 3.1.1	StillSecure Safe Access	Check Point Integrity NGX	Vernier EdgeWall 8800
Vendor	ConSentry Networks www.consentry.com	StillSecure www.stillsecure.com	Check Point www.checkpoint.com	Vernier Networks www.verniernetworks.com
Price	\$14,000 for LANShield switch; \$3,000 for 100 agents; \$8,000 for Insight Manager.	Pricing starts at \$20 per IP address.	\$37,000 for 1,000-user license.	\$45,000 for chassis, support for 1,000 users and one Control Server management appliance.
Pros	Security functions reside directly in the switch; strong reporting features.	Minimal endpoint impact noted during integrity assessment; intuitive, easy-to-use management GUI.	Easy to deploy and manage; offers flexibility and detail in policy definition.	Provides flexible, detailed security for groups of users; has built-in intrusion-detection engine.
Cons	InSight Manager console not intuitive; endpoint assessment not well integrated.	Minimal reporting; powerful, Python-based custom checks require a skill set many organizations may not have in-house.	No preconfigured Windows patch support for posture checking; minimal custom checks functionality.	Not easy to use; offers no reporting functionality beyond log review.
Score	<b>3.93</b>	<b>3.83</b>	<b>3.7</b>	<b>3.55</b>

# CLEAR CHOICE TEST NAC POINT PRODUCTS

management agent such as PatchLink, pushing an enterprise-software upgrade via Microsoft's SMS or running a custom script.

ForeScout, Juniper, Lockdown and Symantec all performed well in our remediation tests, with ForeScout the remediation leader based on its flexible and extensive options, from VLAN changes to killing a rogue process.

The big area of disappointment generally across the board was the general lack of information these products provided about a user's or device's history. If a device was placed in quarantine, what check failed? What was the response? What user was logged in at the time? What action was taken? What other devices had the user connected to? What is the historical information about this device or user? Very few products were capable of this level of detail, which is required for any useful NAC deployment.

The tools to manage a NAC deployment adequately — the general interface for policy creation and day-to-day administration, help and documentation, and alerting and reporting capabilities — generally were the weakest components of the products tested.

GUI interfaces were cluttered and not intuitive to use or navigate. Often the tools for defining NAC policies — a critical part of NAC administration — were buried deep within the system and required multiple clicks just to get to the starting point. Very few products launched administrators into a dashboard of useful information. Lockdown's Enforcer had the best: A full-summary dashboard appeared when the administrator initially logged on that gave a clear picture of the system's risk posture and high-level details of its current state.

Policy creation generally was overly complex. While NAC vendors generally provide a lot of flexibility and detail with their NAC policy development engines, most have fallen short in making those engines easy to drive with the supplied management applications. Vernier's EdgeWall had the most challenging NAC methodology, but in the end, it was the most flexible and detailed of the products tested.

Another area we focused on was support-account administration,

to see the level of detail supported for access control and role definition. We also looked at whether a product managed administrator accounts within an enterprise-user repository instead of maintaining a local database of administrative users. Most products supported a multiple-role structure, but some products provided more detail than others.

Reporting was the most problematic area. Some products contained no reporting function, and others provided only very basic searches. While it's important to identify and enforce network access based on endpoint integrity and defined policies, it is almost more important in today's environment to show the historical results of assessments and what action was taken concerning systems that did not adhere to defined policy.

While all the products we tested can use improvement in overall management, Check Point, ForeScout and Lockdown have the strongest showing in this area of evaluation. Their products provided the reporting and enterprise-management functions we expected to see, such as multiple alerting options to tie into enterprise management tools, delegated administrative functions, and adequate help and product documentation.

## NAC futures

Post-admission control is where most vendors are spending their development resources, and that's only natural. Once a system is admitted to the network, it needs to stay in compliance. Most products achieve this now by performing assessment checks on a schedule, such as every 15 minutes.

Some vendors, such as McAfee and StillSecure, are starting to take post-admission control a step further, integrating intrusion-detection/prevention systems that trigger an enforcement action if an alert is received about an endpoint device. This information also can be combined with a vulnerability scan to determine if the alert is a

<b>Trend Micro Network VirusWall Enforcer 2500</b>	<b>Bradford Networks NAC Director</b>	<b>InfoExpress Dynamic NAC for Windows</b>	<b>Cisco NAC Appliance 4.1</b>	<b>McAfee NAC 2.5</b>
TrendMicro www.trendmicro.com	Bradford Networks www.bradfordnetworks.com	InfoExpress www.infoexpress.com	Cisco www.cisco.com	McAfee www.mcafee.com
\$25,000.	\$32,200 for 1,000 users.	\$40 per user.	Pricing starts at \$18,000 for Clean Access Server and Clean Access Manager.	\$20,400 for 1,000 users.
Quick to deploy and easy to administer.	Provides easy integration into existing environments by directly controlling network switch flows; supports all access environments; taps into multiple authentication servers; user roles are well integrated with Active Directory.	No network infrastructure changes required for NAC.	Allows for flexible policy creation, because physical endpoint checks are separate from endpoint software requirements; strong authentication and authorization features.	Easy-to-use wizard process for rule creation; overall management through ePolicy Orchestrator is very mature.
No custom check functionality; no ability to assess status of client firewall programs.	Network switch control can be a controversial approach to NAC; management features are not easy to use.	Disparate management tools required; policy management interface needs to be streamlined.	Noticeable performance impact on endpoint during posture assessment; minimal reporting capabilities; Cisco API required to analyze assessment results; overall confusing management interface; checks run only at initial connection time.	Minimal to out-of-box reporting with no custom report capability; no custom check development functionality; can't authenticate using external repositories; no support for guest users.
<b>3.53</b>	<b>3.4</b>	<b>3.15</b>	<b>3.03</b>	<b>3.03</b>

# CLEAR CHOICE TEST NAC POINT PRODUCTS

false-positive. Although some products do vulnerability scans now, this false-positive correlation still is a goal for vendors to reach. The next logical step is integration with security-information and security-incident and -event management products, which should provide the most complete picture to help a NAC product make the best decision on how to provide access to an endpoint device continuously.

Another future integration point for NAC should be the growing number of outbound-content-compliance and data-leakage-protection products. With this combination, companies could block network

access if unauthorized data transfers were attempted or observed.

In its basic form, NAC is ready for prime time. Companies can buy a multitude of products that check the integrity of known endpoints and control access accordingly. And judging from the industry buzz about NAC, vendors are investing R&D dollars that will help facilitate enhanced features and further integration with any organization's network infrastructure. The secret to deploying an effective all-in-one NAC product is aligning yourself with a vendor that has developed its product with the same NAC priorities you've set for your own network. ■

## SCORECARD

Category	Weight	Symantec	Forescout	Lockdown	Juniper	ConSentry	StillSecure
Authentication/authorization	20%	5	4	4.5	5	5	4.5
Endpoint assessment/ environment information	30%	4.5	4	4	3.5	3.5	3.5
Enforcement	25%	4.5	5	4.5	4.5	4	4
Management	25%	4	4.5	4.5	3.5	3.5	3.5
<b>Total score</b>		<b>4.48</b>	<b>4.38</b>	<b>4.35</b>	<b>4.18</b>	<b>3.93</b>	<b>3.83</b>

Category	Weight	Check Point	Vernier	Trend Micro	Bradford	Info Express	Cisco	McAfee
Authentication/authorization	20%	4	5	4.5	5	3.5	4.5	2.5
Endpoint assessment/ environment information	30%	3	3.5	2.5	3	4	2.5	3
Enforcement	25%	3.5	3.5	3	3.5	3.5	3	3
Management	25%	4.5	2.5	4.5	2.5	1.5	2.5	3.5
<b>Total score</b>		<b>3.7</b>	<b>3.55</b>	<b>3.53</b>	<b>3.4</b>	<b>3.15</b>	<b>3.03</b>	<b>3.03</b>

**Scoring key:** 5: Exceptional; 4: Very good; 3: Average; 2: Below average; 1: Subpar or not available.



Symantec Corporation  
World Headquarters  
20300 Stevens Creek Boulevard  
Cupertino, California 95014 USA

For specific country offices and contact numbers, please visit us at [www.symantec.com](http://www.symantec.com)  
For product information in the U.S., call toll-free 1-800-745-6054