

ForeScout CounterACT delivers on agentless NAC

BY MANDY ANDRESS

Cost: Starts at \$13,995

Score: 4.38 (out of 5.0)

The ForeScout CounterACT appliance monitors trunk and span ports on the switch to which its attached, sniffing network traffic to understand the status of devices and ensuring they adhere to the required security policies. For example, employees that are authenticated against an Active Directory domain can adhere to one set of policies while guest users, not being a member of the corporate Active Directory domain, must adhere to a different policy.

CounterACT uses Nmap to identify the role any device on the network and dynamically assign it to a device group for access purposes. For example, a printer is identified and placed in the printers group. This process cuts down on administration overhead, as new devices do not need to be explicitly excluded as they do in some other deployments of network-access control.

In addition to the standard clients and server used as part of the test bed, CounterACT also identified the VoIP phone, TiVo, and PDA on the network. Overall, using Nmap, a staple tool in any security professional's arsenal, makes the management of all the embedded devices the easiest of all products tested.

For testing, we configured the CounterACT appliance on the network core Cisco 3750. That let us to control all aspects of our network from one switch and gave the appliance a view of all network traffic. Scalability is an obvious concern here, in that all network traffic passes through this single box. Testing scalability was beyond the scope of this review, so we don't have a definitive answer on that point. We can say that ForeScout provides multiple appliances to meet varying scalability requirements, with the high end supporting 2,500 devices and 1GB throughput.

To support remote-access connections, ForeScout provides plug-ins for the CounterAct appliance that provide its NAC functions for popular VPN products. The plug-in for the Cisco VPN Concentrator used in our testing supports full endpoint assessment and enforcement functionality.

An 802.1X plug-in is also available from ForeScout that would let the appliance capture and participate in 802.1X connection attempts.

Authentication support is mainly provided passively with ties to Active Directory and repositories for Lightweight Directory Access Protocol if neither the 802.1X plug-in nor the VPN plug-in (which supports RADIUS) is in use. We configured the CounterACT integration with Active Directory – a matter of providing account information and configuring base distinguished names for queries with the directory – which was quick and easy to com-

plete. A company can also push an active authentication process through a captive portal like most other products.

CounterACT administrators can only authenticate locally to the device which we view as a limitation because we'd like to have them authenticate to an existing repository.

ForeScout's agentless approach to endpoint assessment overall pretty strong but does lack some coverage for what other vendors have included as basic components. Out-of-the-box AV support is minimal, covering only a handful of the major vendors like McAfee and Symantec. Other AV products can be tracked via custom checks, which is what we wrote in order to identify our Sophos AV installation. This check ran successfully. Custom checks are constructed through Visual Basic scripts. If you can script it, you can push a system check or trigger an enforcement action. While providing limitless flexibility, not all organizations may have the necessary time or in-house skills to work with a NAC product in this fashion.

With the agentless approach, one challenge is assessing systems that are running a personal firewall and blocking inbound access. For employee systems, the corporate personal firewall could be configured to allow inbound access to the CounterACT system. For non-employees, users could be asked to change their firewall settings, but this is not always a viable option. ForeScout does provide the option of prompting the user to create an outbound SSL connection that CounterACT then uses for its assessment checks. Handling guest users is more challenging than with products that provide the ability to install a dissolvable agent to perform compliance assessment.

Windows patch checks are available as a standard feature and rely on either Nessus (built-in) or Qualys (optional, via a plug-in) vulnerability assessment to identify which patches are missing from the system trying to gain access.

In addition to the host of checks run against any machine entering the network, timing of subsequent assessments is configured for each individual integrity check, making this one of the most flexible products in this area in that regard.

CounterACT collects standard device information like user name and IP and MAC addresses, but its passive monitoring also picks up data such as NIC vendor, operating system, operating system function and any services running on the system. This process was very accurate for the systems on our test network.

Similar to what ConSentry offers with its product, ForeScout also monitors devices for evidence of infection, the original focus of ForeScout's early products. We ran a worm generation tool from an endpoint system. CounterACT correctly identified the traffic and

blocked the system from the network in about 30 seconds.

In terms of enforcement and remediation, CounterAct has the ability to change VLAN links, block traffic to or from the offending machine through firewall rules, kill processes on the system, provide links for self-remediation, and send HTTP, Windows and email message alerts.

For testing, we configured a VLAN assignment change and HTTP notification to the end user acknowledging when a system was out of compliance.

We created firewall rules on the CounterAct appliance to block all network traffic except Internet connectivity and provided a link to download and install the Sophos AV client if missing. These tests ran as expected.

ForeScout provides the best data searching capability to help administrators understand the relationship between devices, users, integrity issues, and remediation. ForeScout provides a web-based network portal that allows authorized users to search based on criteria such as user name, IP address and MAC address, to name a few examples. You can see displayed all the data for a system and see how the system was accessed, what integrity issues the system had, what enforcement actions were taken. You can also run a search and see all the systems a specific user accessed. The available reports are created from this interface. They can be scheduled and emailed when complete and can be exported to pdf and csv files.

System management is performed through a console installed on a separate Windows system. While it's not Web-based like most of the competition, it is fairly intuitive. Policies are created via a wizard, which provides an easy to use interface to accomplish a complex task. Through this wizard you can set policies as flexible as with any other product tested. But instead of making you jump around to eight different screens to configure all your required checks and rule associations, ForeScout walks you through the process step by step. About 20 report templates are available in this management GUI and all can be exported to HTML.

ForeScout is easy to use and deploy, ideal for organizations that want to make as few infrastructure changes as possible. As far as a direct comparison among the other products tested, CounterAct is very similar to ConSentry's LANSheild, except ConSentry sits in-line and ForeScout does not.



ForeScout Technologies • Corporate HQ
10001 N. De Anza Blvd., Suite 220 • Cupertino, CA 95014 USA
Toll-Free (US) 1.866.377.8771 • (Int'l) 1.408.213.3191
www.forescout.com