

# Network Computing

OCTOBER 5, 2006 | WWW.NWC.COM For IT By IT

## ROLLOUTS

### Network Gatekeeper Fights Back

CounterAct NAC enforces complex policies, detects malicious behavior BY MIKE FRATTO

➤ **FORESOUT COUNTERACT 6.0** is an agentless, out-of-band, network-access-control product that combines RPC assessment with passive monitoring for malicious behavior. The powerful and flexible policy definition engine can define complex conditions and use those conditions to select and apply the appropriate policy. Through continuous monitoring, HTTP intervention and scheduled scans, CounterAct deploys policies dynamically, as a host's condition changes.

CounterAct uses passive monitoring, vulnerability-assessment scans and host inspection to assess the host's health, and grant or deny access to network resources. Passive analysis detects unauthorized network activity that might be missed by a host-assessment, antivirus or other

host-protection product. Devices from ConSentry Networks, Nevis Networks and Vernier Networks also use this style of monitoring, but are inline products. Because CounterAct works out of band, it won't degrade network performance. Other NAC products, such as Check Point Software Technologies Integrity and InfoExpress CyberGatekeeper, can be

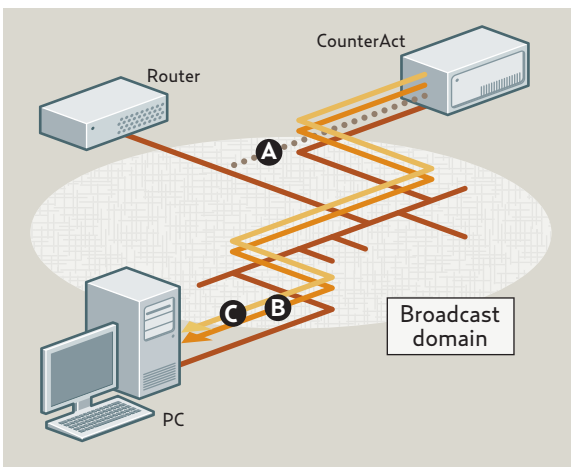
#### the upshot

**CLAIM:** ForeScout's CounterAct 6.0 simplifies implementation of complex network-access policies. Besides being an agentless system that performs scans based solely on a host's conditions, CounterAct uses continuous passive monitoring of those hosts to root out malicious behavior.

**CONTEXT:** Deciding which network-access policy to apply to a host involves several factors about the host's configuration. Defining those host conditions can be complex, and a NAC device must ensure that all policies are properly implemented and enforced. Furthermore, there are agentless products as well as products that operate out of band, but CounterAct's agentless, out-of-band combination is unusual.

**CREDIBILITY:** ForeScout delivers a solid set of policy-definition capabilities that are on par with other NAC products. The clientless, passive monitoring system detects rogue activity and is factored into the enforcement capabilities, but the out-of-band deployment, while useful, adds complexity to networks with multiple subnets running in a single broadcast domain. Nevertheless, CounterAct's approach to behavior assessment makes this product worth considering.

#### COUNTERACT PASSIVE CONTROL



**A)** CounterAct detects new hosts as they communicate on the network. **B)** Hosts can be scanned for vulnerability and configuration settings. **C)** CounterAct enforces policies using TCP resets, ICMP messages and traffic injection. Any malicious network behavior can be detected and blocked.

# ROLLOUTS

deployed out of band, but require agents on every host and don't do passive monitoring.

## SMART POLICY ENGINE

CounterAct's policy engine is the brains of the product. Once the device has gathered the necessary data from all network devices, admins can use a few simple rules to create policies that will automate any host's grouping, check host configuration to ensure compliance and take enforcement actions. To enforce a single policy on all company-owned assets, for example, we used CounterAct to create a policy check that placed all users who authenticated to our Active Directory into our "corporate" group. Many of the product's competitors lack this capability.

Policy assessments can be scheduled, run on demand or run at network admission. As with other NAC products, changes in a host's configuration are detected only by an assessment.

The rule actions give admins a variety of ways to deal with problems, including quarantining hosts and redirecting Web requests to remediation pages. For example, though Internet Explorer may be the approved Web browser, if an inspection of the host turns up different browsers, such as Firefox or Opera, the users can be sent to an HTTP redirection page that describes the violation and repercussions for using nonstandard software, and force the users to accept those terms before proceeding.

## ASSESSING BEHAVIOR AND ENFORCING POLICY

CounterAct has exceptional ability to discover and act on network behavior. Using the technology within ActiveScout, ForeScout's network-intrusion-prevention system, CounterAct can differentiate malicious network activity from simple chattiness on the network and take action. We found it easy to configure a policy to quarantine a host based on that

machine's port scan activity.

Unlike assessment policies, event policies, such as those triggered by host activity, are enforced in real time. CounterAct reacts to the host that's exhibiting malicious behavior immediately. NAC products that base policy solely on assessment—as do Check Point Integrity, Lockdown Enforcer and Symantec Network Access Control—don't detect malicious activity.

CounterAct's shortcomings lie with its inability to interface directly with other host software, such as desktop antivirus, firewalls and patch-management agents, to assess their condition. CounterAct can check for the existence of antivirus software, but not for the version or virus data file. Host-based products can perform that task.

Another problem is that network-based remediation and enforcement needs complete visibility and access to the protected network segments. The deployment complexity mushrooms when multiple subnets are running within the same broadcast domain. With out-of-band products like CounterAct, the monitoring port must see all the traffic on network segments, and the enforcement port must be within the broadcast domain of the subnets to be enforced. If you have one flat subnet, it needs only one enforcement port. But if you have multiple subnets, CounterAct must be attached to an 802.1Q VLAN trunk port or multiple CounterAct interfaces must be connected to individual subnets. You also must ID aggregation points in your network for monitoring as well as for injecting remediation traffic back into the network.

CounterAct offers a robust, low-impact NAC solution that enforces desktop-assessment policies and continuously monitors host conditions based on network behavior. It's free for customers with a support contract from ForeScout; list price is \$13,995. ■

---

MIKE FRATTO IS AN NWC SENIOR TECHNOLOGY EDITOR BASED IN OUR SYRACUSE UNIVERSITY REAL-WORLD LABS<sup>®</sup>. WRITE TO HIM AT [MFRATTO@NWC.COM](mailto:MFRATTO@NWC.COM).