

# PRODUCT Reviews

IDP/NETWORK ACCESS CONTROL

## CounterACT

REVIEWED BY WAYNE RASH

ForeScout Technologies

[www.forescout.com](http://www.forescout.com)

Price: CT100 Appliance: \$13,995



The idea behind CounterACT is described in its name: Find an intrusion that you can counter, and then act to do something about it. CounterACT provides layered security by combining intrusion prevention and agentless network access control.

### Configuration/Management B

Getting the CounterACT appliance up and running mostly consists of plugging it in. You'll need three Ethernet connections: one is for management, another attaches to a span port on a switch to monitor traffic, and the third connects to an ordinary switch port to send messages and take network-based enforcement action.

The CounterACT console allows you to control virtually every aspect of the appliance's operation, including telling it what to look for on your network, what to ignore, the levels you want to reach before the appliance decides you have a problem, and to make the system settings.

The easy-to-use GUI consists of drop-down lists, check boxes and radio buttons—not particularly sexy, but it does the job.

### Effectiveness A

During testing, CounterACT was able to find and identify everything on the network and follow the rules we set, including blocking where instructed.

Because you can key network access control to the intru-

sion prevention features, the machine can operate on its own once you set and test the rules. It doesn't matter if someone starts sending out worms at 2 a.m.—CounterACT will handle the problem and report back. In our lab, the appliance watched efforts by a simulated worm and then shut it down.

Likewise, it can determine how well users meet other policy requirements, such as update levels and virus definition dates, and put them in network-based quarantine until they are compliant.

### Policy Control B

CounterACT uses predefined rules and your network policies to alert the user and/or the manager, and to take action, such as sending noncompliant users to a remediation page. CounterACT can enforce security policies, such as blocking a connection if a user is in violation.

The policy controls have a lot of flexibility. For example, most organizations don't allow users to add their own network segments, wireless access points or external routers.

With CounterACT, you can spot such unauthorized additions to your network and shut them down. During our testing, CounterACT immediately spotted access points that were outside the portion of the test network being managed and flagged them.

You can define virtually anything on your network that you want to monitor. The device will watch for suspected worm traffic, monitor for prohibited activities such as peer-to-peer sharing software, and let you know when any event you designate takes place on your network.

### Reporting B

CounterACT can be set up to report anything. The appliance constantly collects a database of events and can report on them in a variety of formats. In addition, CounterACT can alert you immediately with reports on infected sources on your network, and it can alert users when they don't meet your policy requirements.

CounterACT's regulatory compliance feature can correlate employee and event information, and provide reports on what happened on your network, when it happened and who did it. And, CounterACT can provide a variety of real-time event reports using SNMP, syslog, OPSEC and SESA.

### Verdict

CounterACT provides a lot of bang for the buck. It's flexible and easy to use, providing intrusion detection/prevention and network access controls. ▶

**Testing methodology:** The test network included managed and unmanaged switches; Windows, Linux and Novell servers; a complete VoIP system and voice gateway; and an Internet gateway. Wireless APs were introduced to test for rogues. We tested custom policies and detected worm simulations.

Reprinted with permission from Information Security Magazine, August 2006.

© 2006 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144



ForeScout Technologies, Inc.  
10001 N. De Anza Blvd., Suite 220 • Cupertino, CA 95014 USA  
Phone: 1.866.377.8771 • Fax: 1.408.213.2283