

As laws and industry regulations change, the task of ensuring policy compliance is often a quickly evolving one, reports **Justin Peltier**.

System configurations are getting more complex, and systems no longer are defined as just workstations. Devices such as smart phones, wireless access points and printers are all devices that are capable of storing a security configuration, but they are also devices capable of

introducing vulnerabilities or other security weaknesses into an environment. When new clients or endpoints are combined with the constantly moving target of new vulnerabilities being released and new organizational directives, the task of ensuring policy compliance is often a quickly evolving one.

Many of the products that we reviewed this month used unique approaches to tackle the problem of device policy management. Some products focused on specific types of devices, while other clients focused on more traditional systems, such as workstations and servers.

CounterACT, Version 6



Vendor ForeScout Technologies
Price Starts at \$4,995 plus support
Contact www.forescout.com

The CounterACT product from ForeScout is unique in a few ways. First, the product appliance is based on, and the policy is enforced through, a network tap configuration. The product is designed to be reading network traffic from a switch span port. This would allow the device to see all of the data on that network segment. It is easy to see the placement of the CounterACT device near a backbone switch. This would allow an organization with a small number of devices to enforce policy for a large number of endpoints. The CounterACT product does not require a software client to be installed on workstations or other devices. Rather, the CounterACT product works similarly to other 802.1X authentication mecha-

nisms to move clients in violation to reduced access virtual local area network (VLANs). This type of configuration allows for endpoints to be more than workstations, and endpoints can include wireless access points, smart phones and laptops.

The installation of the CounterACT device is performed through a HyperTerminal-like session and a serial cable, or the installation can be done via a keyboard and monitor attached directly to the device. The configuration is not difficult. The management interface holds an IP address while the monitoring interface has no valid address. The management station has an application installed on it, which allows the station to configure, manage and gather reports.

The documentation is available in both printed and electronic format and the documentation is well done. ForeScout provides support through phone and email, but online resources are for registered users only. Premium and additional support

is available with an associated annual fee.

The cost of the ForeScout CounterACT product is about average. When considering that the features of the CounterACT product mimic the features of an intrusion prevention system, the cost is very reasonable.

SC MAGAZINE RATING

Features	★★★★★
Performance	★★★★★
Ease of use	★★★★☆
Documentation	★★★★★
Support	★★★★☆
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths A well-built application that uses the base of an intrusion prevention system.

Weaknesses The product only sees network traffic on a segment. In some environments, this may necessitate several devices.

Verdict A unique approach to policy management. The clientless install is an administration saver, but the product does not protect devices not on the local network.



A unique approach to policy management.

Justin Peltier



ForeScout Technologies
 10001 N De Anza Blvd. Suite 220
 Cupertino, CA 95014 USA
 Tel: 1.866.377.8771
 Fax: 1.408.213.2283
www.forescout.com