

COUNTERACT 6.3.3 FROM FORESCOUT TECHNOLOGIES

The majority of security threats come from inside of the network, making it imperative that businesses implement strong NAC (network access control) policies. Unfortunately, many solutions can be difficult to deploy and manage, but CounterACT from ForeScout aims to avoid these pitfalls and not only can it enforce multiple NAC policies, but it is capable of detecting and blocking malicious behavior.

CounterACT is deployed as an appliance and functions in out-of-band mode, so it just needs port mirroring to be configured on the switch it's connected to. For testing, we installed it in the lab and set up our 48-port HP ProCurve Gigabit switch to mirror all traffic to it. Two network ports are used with one passively monitoring all traffic and the other 'response' port, used to enforce NAC policies with functions such as HTTP redirection, VLAN quarantining and, virtual firewall blocking.

The appliance is accessed via the CounterACT Console, which offers a quick start wizard where you provide information such as the protected network ranges, AD credentials, SNMP details and authentication servers. Once this phase is completed, the appliance gets straight down to business by identifying all devices on the network and automatically populating the console with their details.

We found that, after a few minutes, CounterACT had picked up all of our servers, workstations, switches, printers and firewalls. The interface is a tidy affair with a central view showing discovered devices, another displaying policies and their status, and a third allowing views to be quickly filtered, allowing you to group hosts with common attributes, and apply NAC policies.

Policies cover a multitude of security issues and templates help to get you started with the common tasks. Devices



need to be classified by their assets and a policy can automate placing them in the appropriate group. Guest policies keep your contractors and visitors under control, as users that can't, for example, authenticate to a known AD server, will be placed in a different VLAN with restricted network access. The new guest registration feature goes further, as all access attempts by these types of users are tracked for regulatory purposes.

Compliance policies check group members to see that they have required components such as anti-virus software, Service Packs or patches, and the appliance can then provide self-remediation tools to reduce demands on the support staff. You can also check and block specific IM and P2P application activity, and a useful feature is the ability to control USB devices. This latest version adds enhanced USB port controls as it can now block the use of any external device.

Malicious traffic is detected easily as this deviates from the patterns CounterACT expects to see and policies are used to quarantine the perpetrators, or promptly boot them off the network. We were able to use CounterACT to control our switch ports by disabling those the suspect systems were attached to. Even wireless

access points don't get off lightly as CounterACT can spot rogues and quarantine them. A unique new feature is the ability to dynamically configure switch ACLs (Access Control Lists), allowing CounterACT to provide a more sophisticated solution to enforcement, than simple port blocking, or VLAN segregation.

We found the console easy to use and its reporting tools capable of providing high levels of detail. You get a new dashboard that provides a complete overview of your compliance policies and ForeScout also offers optional reporting modules for PCI, SOX, HIPPA and FISMA regulatory standards.

CounterACT's major strengths lie in its agent-less approach and out of band monitoring, which require minimal intervention during deployment. ForeScout's NAC policies are very versatile; they provide strong protection against zero-day threats, and add valuable controls over host USB ports.

Product: CounterACT 6.3.3
Supplier: ForeScout Technologies
Telephone: +44 (0)7739 732805
Web site: www.forescout.com
Price: From £3,607 excluding VAT