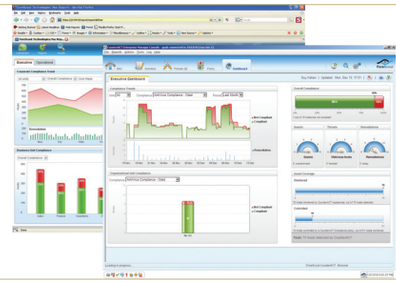
CounterACT 6.3.4 from ForeScout Technologies



PRODUCT REVIEW PRODUCT REVIEW PRODUCT REV

Businesses that focus exclusively on guarding their network perimeter are leaving themselves wide open to some significant threats as most breaches now occur inside the network. NAC (network access control) is the answer and ForeScout CounterACT stands out; this third generation solution is easy to deploy and capable of providing total control over all network devices and users.

This latest version has a sharp focus on the security issues posed by mobile devices and it can manage a wide range of products, including iPhones, iPads, Blackberry, Android and Windows Mobile devices. These devices are detected using real time data such as vendor, model, OS and version, and their connection status. Policies are then applied to control what users can do.

In this version, asset tracking has been improved to provide even greater visibility on network activity. The system will monitor users, applications and processes, along with an impressive range of external devices, allowing it to detect vulnerabilities and block them before they present a problem.

We found deployment in the lab to be a simple process as the appliance operates in out-of-band (OOB) mode, so it just requires port mirroring to be configured on the switch it's connected to. This agentless approach allows it to reside alongside all existing network equipment and infrastructures. The appliance passively monitors all network traffic and uses a 'response' port to enforce NAC policies with functions such as virtual firewall blocking, HTTP redirection, and VLAN quarantining. It isolates all management on a third network port where access is provided through the CounterACT Console.

The console is very intuitive and opens with an overview of all discovered devices, as well as all of the security policies and the status of each one. You can apply filters to this information so that devices with common attributes can be grouped together and have specific security policies applied to them. Policies cover an impressive range of security issues and ForeScout provides a collection of templates that will get you started. Usefully, policies can be run passively with all actions deactivated, allowing you to assess their impact before going live.

Once CounterACT has admitted a device onto the network it can provide full protection against day-zero threats. Any end point behavior which the system considers unusual or threatening will trigger policies that can, for example, quarantine suspect systems and safely remove them from the network.

Compliancy checks ensure that end points such as desktops and laptops have required components such as anti-virus software before being granted network access. Service Packs and the latest security patches can be checked for and self-remediation tools applied to reduce the burden on support departments. External storage devices pose significant data leakage threats, but CounterACT can control access to USB ports allowing policy to govern who may use them. IM and P2P activities can also be easily controlled as CounterACT can identify these applications and prevent them from running.

For guest access, the registration processes have been enhanced so that you can apply authentication, compliancy checks, and NAC policies to guest users, tracking the access attempts that they make. Wireless networks come under CounterACT's remit allowing policies to be applied to wireless devices, and if necessary blocking rogue Access Points.

Point a web browser at the appliance and you can access an impressive range of reporting tools. We found these capable of delivering high levels of information about network activity. ForeScout also offers optional reporting modules for all the main regulatory standards.

Its ease of deployment and agentless operation makes CounterACT superior to other solutions in this market. Its ability to combine NAC with IPS functions allows it to provide full protection against the latest threats and its policy based security can significantly reduce support overheads. NC

Product: ForeScout CounterACT 6.3.4
Supplier: ForeScout Technologies
Tel: 01256 843633
Web site: www.forescout.com
Price: £3,400 excluding VAT