

With enough funds, most organizations would opt for single security tools to tackle each type of threat, but multi-purpose devices now offer a real alternative, says Rob Jaques

Enterprises have shifted towards using appliances to fight a range of threats, particularly multi-purpose security devices that combat more than one type of attack. Organizations want to put bandwidth through one device to clean it up and make it suitable for use within the infrastructure.

When we started testing, we had in mind a scenario where the security professional wanted an appliance that, once set up, could be easily managed and upgraded to counter new threats as and where they inevitably arise.

We were reasonably pleased with all the products tested.

They all carried out basic tasks very well and defended against everything we could throw at them. They also had to be capable of bearing up under the heavy loads expected at the enterprise level. Most products were able to carry out these tasks without too much hassle.

## Auditor Enterprise



<b>Version</b>	4.0
<b>Supplier</b>	NetClarity
<b>Price</b>	from \$19,995 for 256 IPs
<b>Contact</b>	<a href="http://www.netclarity.net">www.netclarity.net</a>

Netclarity's distinctive green 1U rack mount Auditor Enterprise device is described as a CVE (Common Vulnerabilities and Exposures)-compliant network security system. It offers vulnerability assessment functions to help firms comply with corporate governance legislation by conducting an audit against predefined CVE vulnerabilities. This helps endpoint security by quarantining infected systems until they are remediated.

It also integrates with a range of firewalls and switches from third parties like Juniper, Cyberguard, Secure Computing and Cisco.

A clearly laid-out, single sheet setup guide helped us get the device up and running with very

little fuss.

The Linux-based unit performed a self check as it loaded its Auditor Network Configuration v4 application, but strangely kept failing to recognize our network's DHCP server. To get around this, we configured a static address directly.

When we fired up the web-based management interface over http, we were prompted to enter the user name and the supplied, very strong, complex password. This fired up the system setup GUI, which was clearly laid out and easy to navigate.

We were then presented with a screen listing the regulations and security programs the device supports, along with major charge and credit card security programs.

We were then moved onto the asset discovery phase, where Auditor Enterprise managed to find all of the devices hosted on

our test network. But it was vague when it came to reporting one of our clients as running either Windows ME, 2000 Pro, Advanced Server or XP. It also scanned itself and reported its OS and MAC address as hidden to improve security.

We used the one-click audit wizard to audit one of the test clients on our networks. Its scanning through the subnet was impressively fast – as was its scanning of a client. The device completed both these tasks in just a matter of a few seconds.

The system returns impressively detailed PDFs analyzing the vulnerabilities on each client machine scanned.

SC MAGAZINE RATING	
Features	★★★★☆
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★☆
Value for money	★★★★☆
<b>OVERALL RATING</b>	<b>★★★★★</b>
<b>For</b> Very good, fast, powerful endpoint security compliance tool that does what it does very well.	
<b>Against</b> Limited functionality.	
<b>Verdict</b> As corporate governance legislation gets ever tighter, this device will help companies cope.	



Very good, fast, powerful endpoint security compliance tool that does what it does very well.

Rob Jaques



NetClarity - Preemptive, Proactive Protection.™  
 54 Middlesex Turnpike, Bld. C  
 Bedford, Massachusetts, USA 01730  
 Web: [www.netclarity.net](http://www.netclarity.net) • E-mail: [sales@netclarity.net](mailto:sales@netclarity.net)  
 SKYPE: netclarity • International Line: 781-276-4555  
 USA Toll Free: 877-677-3328