● **CONTENT SECURITY APPLIANCE**

CyberGuard Webwasher 1000 CSM Appliance

PRICE £6,395 exc VAT

**BASIC WARRANTY** 1yr on-site 4hr response, £1,536 exc VAT

SUPPLIER CyberGuard Corporation 0870 460 4766

INTERNET www.cyberguard.com

VERDICT A content security appliance that offers an extensive range of features, easy installation, good management and reporting, plus good value.

The CyberGuard can scan SSL-encrypted connections.

CyberGuard's Webwasher 1000 (WW1000) aims to deliver complete content security by amalgamating the company's entire CSM software suite into one easily deployed appliance. It supports a wide range of deployment scenarios and in its simplest form functions as an HTTP proxy. It can also be configured to forward mail to one mail server or use MX records for multiple servers.

Our test clients were configured to use the WW1000 as a web proxy, and for our mail server we just needed to provide the WW1000 with its IP address. The appliance supports a wide range of third-party proxies such as Microsoft's ISA Server, NetCache and Blue Coat appliances. It also functions as an ICAP (Internet Content Adaptation Protocol) server, allowing it to integrate with many other third-party proxies and appliances that support this.

The appliance is easily managed, as the web interface provides a single point of access to the myriad functions. All component updates are carried out automatically at user-defined intervals, which can be as often as every hour. However, downloads of, say, virus signatures or the web content filtering database can be run manually whenever required. A couple of buttons at the top of the interface allow you to switch easily between system configuration and filtering policies, with each option providing a neat row of tabbed folders.
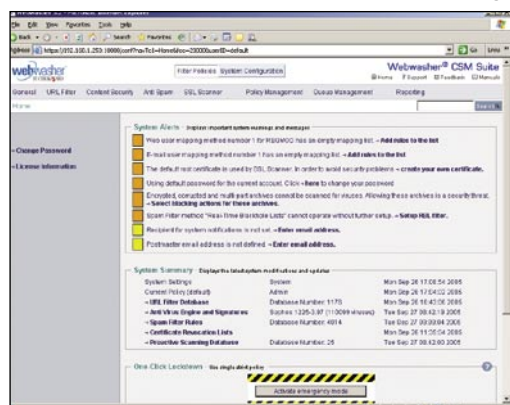
All CSM suite components are easily accessed and the system can be locked down in the event of an alert.

From the system configuration page, you can set up HTTP, HTTPS and FTP proxy services, mail gateway and delivery details, and ICAP server parameters. Usefully, all component updates are handled under one heading, where each one is accompanied by a log file showing the last few download details. The WW1000 uses the concept of corporate filtering policies, which it applies at the gateway for different users, groups, email senders and recipients or IP addresses. You can create multiple policies each with different content filters, anti-virus and anti-spam actions and apply them to different user types. Changes to any component may be applied to a specific policy or you can make them global.

Virus scanning is a particularly powerful feature of the WW1000, as it can use multiple engines from Sophos, Computer Associates and McAfee. Alternatively, you can pick any one or two and license them easily from the main interface. You can even decide the order of priority that each engine is used for filtering. Either way, scanning is activated by default and the settings may be accessed from the Content Filtering policy section, where you can switch on or off all scanning activity and decide what to do with ActiveX controls, executables and JavaScript, along with embedded objects and scripts. One smart feature is that in the event of a virus outbreak alert you can lock the system down with a single press of a soft-button. This has the effect of

immediately overruling all policies applied to every user group and implementing an emergency policy for everyone.

The barrage of anti-spam measures starts with Mailshell's SpamCatcher. This is partnered by RBLs, header and message body rules, URL filters and Bayesian analysis. It also uses the Habeas SWE DNS-based service, which provides safelists of audited and certified senders and aims to reduce false positives. CyberGuard's URL filtering covers all the usual suspects in terms of dubious content, and you can pick and choose which ones you want to have control over. Options extend beyond simply blocking or allowing selected categories. You can add criteria such as allowing some during the weekend and blocking others during the working week. Controls over Internet access go even further, as you can use time and volume quotas as well. This only allows users a specific amount of web minutes on a daily, weekly and monthly basis and also restricts their download quota to so many megabytes over the same periods. You can even restrict users' individual sessions to a specific number of minutes.

The WW1000 scores heavily with its ability to scan encrypted SSL content. This is beyond the abilities of virtually all anti-virus and most content-filtering products. It presents a nasty hole where employees could easily evade the company security policies, as encrypted content can't normally be scanned. Another important function of CyberGuard's SSL Scanner is that by carrying out certificate validation it takes the decision process away from the employee as to whether the issuing party is trustworthy. For expired certificates, the connection will be denied and a predefined list of Certificate Authorities allows you to pick and choose who you want to trust. WW1000 includes a Document Inspector too, which can be used to block file downloads and uploads, mail attachments, files that contain embedded active content and specific file types.

With the WW1000, CyberGuard has all the content-security angles covered. It's easy enough to install and manage, and offers extensive reporting facilities. When compared with similar products from companies such as BorderWare and IronPort, it's far better value as well.

DAVE MITCHELL

PC PRO RATINGS

PERFORMANCE	★★★★☆
FEATURES & DESIGN	★★★★★
VALUE FOR MONEY	★★★★☆
OVERALL	★★★★☆

SPECIFICATIONS 1U rack chassis; Intel SE7501WV2 motherboard; 2 x 3.06GHz Xeon; 1GB PC2100 ECC SDRAM; Adaptec Ultra320 SCSI chipset; 36GB Seagate Cheetah Ultra320 hard disk; 2 x Intel Gigabit Ethernet; CGLinux kernel; anti-virus; anti-spam; URL filtering; scans SMTP, HTTP, HTTPS, FTP; web browser management. CyberGuard CSM Suite 5.2 software pre-installed.