Sophos XG 135w

A highly versatile UTM appliance combining top performance with stunningly good value

SCORE ★★★★★
PRICE Appliance and TotalProtect/1yr, £1,607 exc VAT from sophos.com

The union of Sophos and Cyberoam is bearing fruit as the new XG security appliances amalgamate all the best features offered by both vendors. Sophos has done a superb job of integrating everything, and goes even further as the appliances talk to its cloud service and provide instant readouts on endpoint security status.

Cyberoam provides the majority of security services, which means that along with anti-malware, anti-spam, web filtering, application controls, IPS and a web-application firewall, you get its patented identity-based security. This adds extra versatility, allowing policies to be applied to users and groups as well as systems.

The XG 135w on review looks fit for duty in mid-sized businesses, with the manufacturer claiming a remarkably high UTM throughput of 1.4Gbits/sec. It's excellent value: the appliance and a year's TotalProtect subscription, which activates all features, costs just over £1,600 exc VAT.

There's more. As well as eight Gigabit ports, the XG 185w provides dual-band 802.11ac wireless services. It also has an internal 64GB SSD, which is used for log and report storage and as a quarantine area.

It supports routed or transparent bridge modes and a wizard deftly handles installation. This offers a choice of operations, and the option to start in passive mode or apply a default security policy.

The new web console is a pleasure to use and opens with a complete overview of all network activity and security issues. It provides a smart web-traffic graph showing hit rates at five-minute intervals, along with bar charts for blocked and allowed applications, and detected network attacks.

Below these are counters showing the number of risky apps, dodgy websites and intrusions being spotted. Security policies are simple to deploy; ports can be grouped into zones with options for LAN, WAN and DMZ or your own custom zones.

You can organise wireless SSIDs in separate zones, which will allow you to set up guest access and enforce special security policies. Firewall rules are applied to source and destination zones and each can include app control, web filtering, IPS and traffic-shaping policies.

To use the identity-based security, users authenticate to an external directory server or log in to the appliance using the Sophos Client Authentication Agent. This can be downloaded directly from the appliance's captive web portal, which also has links for Linux and OS X clients, and certificates for Android and iOS.

We were impressed by its controls for users and groups, which allowed us to apply web filtering, internet access and bandwidth-usage policies individually. Furthermore, you can enforce data-transfer limits on uploads and downloads, and have discrete daily, weekly, monthly and yearly quotas.

Its Security Heartbeat feature sends all endpoint activity data to the appliance, on the basis of which it displays a coloured status icon on its homepage. Setting it up was as simple as entering our Sophos Cloud account credentials. The clever bit comes next: we could specify that our security policies should require a minimum Heartbeat condition. If a single Sophos Cloud-protected endpoint is compromised, the status turns red and the policy can be used to instantly block access to all users and devices in that zone.

At the same time, the embedded iView syslog server stores all logs and presents a range of activity reports. These provide impressive levels of information, including details on firewall, virus and spam activity, as well as web-content filtering. Clicking on a graph provides a breakdown of all traffic types and iView includes compliance reports for HIPAA, PCI, SOX and more. User Threat Quotient reports use security data aggregated for up to a fortnight so you can easily spot high-risk users.

The XG 135w mixes together a superb range of security measures and serves them up at a price that beggars belief. The high performance makes it a great long-term investment, and its slick integration with Sophos Cloud is yet another reason why it takes the top spot on the *PC Pro* A-List.

ABOVE The union of Sophos and Cyberoam is paying off, with the vendors' best features being combined

"The new web console is a pleasure to use, and opens with a complete overview of all network activity and security issues"

LEFT The web console kept us posted on all the action, including activity on our Sophos Cloud account

SPECIFICATIONS

Desktop chassis • 2.4GHz Intel Atom C2558 CPU • 6GB RAM • 8 x Gigabit Ethernet • 64GB SSD • 2 x USB 2 • RJ45 serial • VGA • dual-band 802.11ac wireless • external PSU • web browser management • Options: appliance and TotalProtect/3yr, £2,612 exc VAT