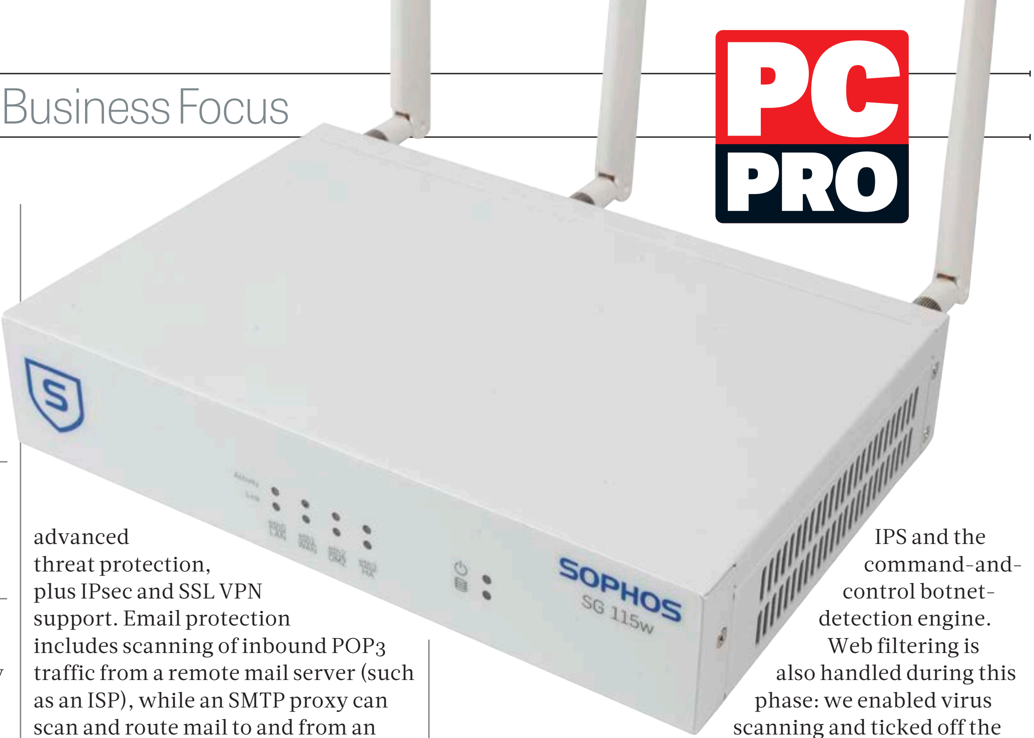
Sophos SG 115w

A wealth of wired and wireless security measures at a price that's perfect for small businesses

SCORE ★★★★★

PRICE Appliance with 1yr FullGuard, £809 exc VAT from sophos.com



ABOVE The SG 115w's firewall throughput of 2.3Gbits/sec shames similarly priced rivals

Small businesses seeking total security at their network gateway will find that Sophos' SG 115w offers everything on their wishlist. It crams in an incredible range of features, and its firewall throughput of 2.3Gbits/sec shames many other appliances in this price bracket.

The hardware costs £482 exc VAT, with the firewall activated as standard. A one-year FullGuard subscription ups the price to £809, but unlocks a wealth of extra features, such as dual-engine antivirus, anti-spam, IPS, web filtering, HTTPS inspection, application controls and advanced threat protection, plus IPsec and SSL VPN support. Email protection includes scanning of inbound POP3 traffic from a remote mail server (such as an ISP), while an SMTP proxy can scan and route mail to and from an internal mail server.

This tough treatment isn't limited to wired connections: the appliance also functions as a 2.4GHz 802.11n access point (AP). It provides secure guest wireless and hotspot services on its own, setting up a secure SSID to which you can add web-protection and anti-spam profiles. The SG 115w can also manage Sophos' own wireless 2.4GHz and 5GHz APs: add them to a group, and they'll automatically pick up assigned SSIDs and protection profiles.

It took us around 15 minutes to set it up, with a wizard guiding us through securing admin access and configuring network ports. Activating services such as HTTP, FTP and email created a set of default firewall rules, while enabling advanced threat protection activated IPS and the command-and-control botnet-detection engine.

Web filtering is also handled during this phase: we enabled virus scanning and ticked off the site categories we didn't want users accessing. Later, we were able to create custom profiles from the 18 available categories, and enforce safe search for Google, Bing and Yahoo.

POP3 mail protection was easy to set up: we chose which networks to apply it to, selected Sophos' antivirus engine (Avira is also available) and asked for spam to be tagged. Unusual at this price is the internal 320GB hard disk, which is used for storing logs and reports and as a spam-quarantine repository.

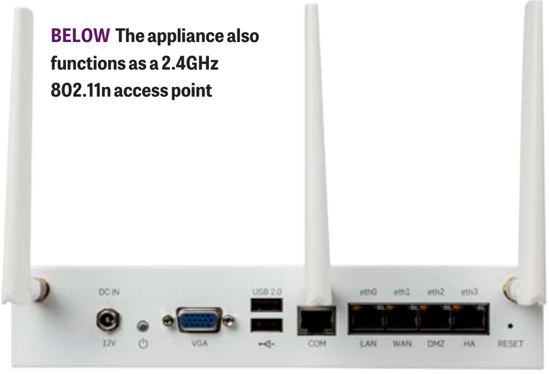
In a month of scanning mail, Sophos correctly tagged 900 spam messages and missed only 16, giving it a 98.3% detection rate. Even better, not one of the 3,500 emails it handled was incorrectly tagged.

To test the controls, we loaded the console's network-visibility tool and watched it list traffic and classify each type. To stop all Facebook activity you can simply hit Block, but you can also fine-tune access with custom rules for specific activities, such as apps, posts and video chats.

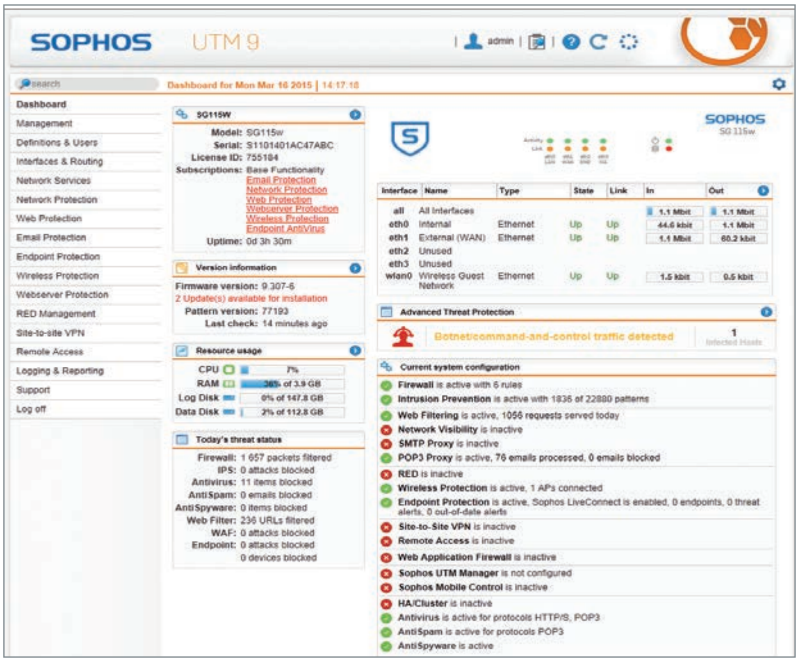
> "Optional endpoint-protection features mean that even mobile workers won't escape Sophos' clutches"

Optional endpoint-protection features mean even mobile workers won't escape Sophos' clutches. We downloaded the Windows agent to selected systems, where it linked up with the LiveConnect cloud service, checked for updates and remotely received security policies.

It all adds up to an appliance that gets it right on almost every level: easy deployment, a huge range of features and a tempting price make the SG 115w the perfect choice for SMBs.



BELOW The appliance also functions as a 2.4GHz 802.11n access point



Dashboard for Mon Mar 16 2015 | 14:17:18

SG115W

Model: SG115w
Serial: S1101401AC47ABC
License ID: 755184
Subscriptions: Base Functionality
Email Protection
Network Protection
Web Protection
Webserver Protection
Wireless Protection
Endpoint AntiVirus
Uptime: 0d 3h 30m

Version information

Firmware version: 9.307-6
2 Update(s) available for installation
Pattern version: 77193
Last check: 14 minutes ago

Resource usage

CPU 7%
RAM 36% of 3.9 GB
Log Disk 0% of 147.8 GB
Data Disk 2% of 112.8 GB

Today's threat status

Firewall: 1 657 packets filtered
IPS: 0 attacks blocked
Antivirus: 11 items blocked
AntiSpam: 0 emails blocked
AntiSpyware: 0 items blocked
Web Filter: 236 URLs filtered
WAF: 0 attacks blocked
Endpoint: 0 attacks blocked
0 devices blocked

Interface	Name	Type	State	Link	In	Out
all	All Interfaces				1.1 Mbit	1.1 Mbit
eth0	Internal	Ethernet	Up	Up	44.6 kbit	1.1 Mbit
eth1	External (WAN)	Ethernet	Up	Up	1.1 Mbit	60.2 kbit
eth2	Unused					
eth3	Unused					
wlan0	Wireless Guest Network	Ethernet	Up	Up	1.5 kbit	0.5 kbit

Advanced Threat Protection

Botnet/command-and-control traffic detected 1 Infected Hosts

Current system configuration

- **Firewall** is active with 6 rules
- **Intrusion Prevention** is active with 1836 of 22880 patterns
- **Web Filtering** is active, 1056 requests served today
- **Network Visibility** is inactive
- **SMTP Proxy** is inactive
- **POP3 Proxy** is active, 76 emails processed, 0 emails blocked
- **RED** is inactive
- **Wireless Protection** is active, 1 APs connected
- **Endpoint Protection** is active, Sophos LiveConnect is enabled, 0 endpoints, 0 threat alerts, 0 out-of-date alerts
- **Site-to-Site VPN** is inactive
- **Remote Access** is inactive
- **Web Application Firewall** is inactive
- **Sophos UTM Manager** is not configured
- **Sophos Mobile Control** is inactive
- **HA/Cluster** is inactive
- **Antivirus** is active for protocols HTTP/S, POP3
- **AntiSpam** is active for protocols POP3
- **AntiSpyware** is active

LEFT The SG 115w is packed with a superb range of security features

SPECIFICATIONS

Desktop chassis ● 1.74GHz Intel Atom E3827 ● 4GB RAM ● 320GB SATA SFF hard disk ● 4 x Gigabit Ethernet (LAN, WAN, DMZ, High Availability) ● 802.11n wireless AP ● 2 x USB 2 ● VGA ● RJ45 console ● external PSU ● web browser management