

While the selection is narrower than it once was, there might be some anti-malware gateway product right for you, says **Peter Stephenson**.

Last year I predicted that this year we would see almost no pure anti-malware gateways. I'll eat a bit of crow for that prediction, but only a bit because the trend continues. We saw nowhere near the number of anti-malware gateway products this year that we saw last year.

That does not mean that the vendors are turning out lackluster products. Far from it, these products we saw were slick, well conceived and easy to setup and manage. The big strength of these gateways is their ability to manage endpoint anti-malware products, as well as provide a solid gateway.

Managing malware at the perimeter is a difficult problem and, frankly, I question whether it can be built into a unified threat management environment effectively. Time will tell whether I'm right. For now, just keep the crow warm. I may need to eat a bit more of it next year at this time.

Web Appliance WS1000



Vendor	Sophos
Price	\$32,000 (500 users, including hardware support and three years of updates)
Contact	www.sophos.com

The Sophos Web Appliance WS1000 effectively and seamlessly blocks spyware, phishing, virus, malware and other unwanted web-borne threats at the gateway. It also allows granular administrative control over permitted actions. The use of Sophos Behavioral Genotype Protection is, according to the vendor, the key to stopping malicious threats, malware and even encrypted malware prior to allowing malicious code to run within your enterprise. The WS1000 uses bi-directional traffic inspection of in- and outbound web traffic. This product features a web-based management console that is easy to navigate for administration,

user activity, policy configurations, compliance and web traffic load, all in a user-friendly dashboard configuration.

The WS1000 is easy to use from the moment it is taken out of the box and placed in the rack. Setup and initial configuration via the setup wizard took just a few minutes, and the appliance was up and running. The default policy was quite comprehensive and required little configuration. We also liked the clean and organized web GUI, which was not only very nice to look at, but it was intuitive and easy to navigate.

This product has some excellent performance features. It can become a web proxy and plug directly into Active Directory or existing LDAP infrastructures.

Documentation is complete, administrator friendly and provides administrators installing the device

with all the information needed to get the appliance online and operational.

Sophos support includes 24/7 telephone technical support and, since the WS1000 is a managed appliance, Sophos proactively monitors it for connection failures and event-driven alerts, and offers on-demand remote access assistance, included in the base price.

At \$32,000, this product's high functionality comes at a very high price. Nonetheless, we find this product to be a good value for the money for organizations that have the ability to make this investment and have the need for the power of a managed appliance.

SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★☆

OVERALL RATING ★★★★★

Strengths Highly flexible policy configuration with high-end technology.

Weakness Very high cost.

Verdict Big capability at a big price.



...we find this product to be a good value for the money...

– Peter Stephenson

SOPHOS www.sophos.com