

DECEMBER 2004

# INFORMATION SECURITY

WWW.INFOSECURITYMAG.COM



**ONLY  
THE  
BEST**

**WIN**

**PLUS**

**The Year in Review**

**2005 Threat  
Forecast**

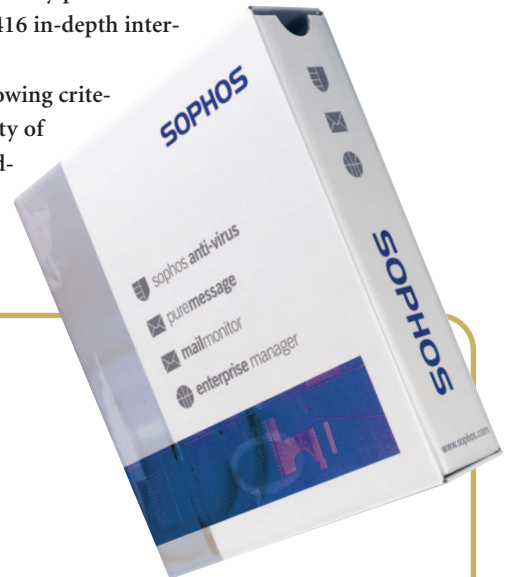
**Firefox vs. IE**

Seasoned security pros recognize that security isn't just about products; it's about people, process and policy. But products are inarguably the most visible, tangible and accessible tools of IT risk management. They are the mechanisms for carrying out the strategic policies and processes that drive security's success in any organization.

*Information Security's* 2004 Products of the Year is a compilation of the best commercial products across 13 categories. Unlike other security product awards, the judge for these awards was you, the information security practitioner.

*Information Security* and our research partner, TheInfoPro ([www.theinfo.pro.net](http://www.theinfo.pro.net)), conducted 416 in-depth interviews of security managers working in 273 companies, evaluating a total of 1,239 products.

The rating for each gold, silver and bronze winner is a composite score based on the following criteria: vendor's brand or reputation, quality of product, delivery of product as promised, quality of technical support, technical innovation, strategic vision, competitive positioning of the product, quality of the sales team, interoperability and ease of doing business with the vendor.



## Sophos Anti-Virus

Sophos, [www.sophos.com](http://www.sophos.com)

**RATING: 80**



Sophos continues to compete with the antivirus giants through an effective combination of technical know-how, expedient response to new malware and good, old-fashioned customer service. Sophos Anti-Virus isn't just winning the gold award, it's setting the standard for AV excellence.

"Sophos makes an excellent product; it's very focused on AV signature generation," says the corporate security manager at a telecommunications company.

Fighting viruses has become a speed game. As attacks keep increasing in volume and severity, AV companies have to continuously update their products and signature databases.

Sophos uses a series of internally developed approaches to rapidly identify new viruses, including code emulation, online decompression for scanning, and an engine for detecting and disabling macro viruses. It scans incoming documents not by extension but by analyzing their format, making the scanner harder to trick.

Sophos developed its real-time InterCheck technology to counter viruses regardless of their delivery medium: e-mail, CD, floppy disk, instant message or network share. InterCheck scans for infections upon access to a system. Sophos also uses a Remote Update feature to protect machines not regularly connected to the corporate network. Business users rate both features highly.

And they appreciate that Sophos doesn't employ the hype or jargon that other vendors use to blow new viruses out of proportion. A senior security analyst at a large financial services firm says, "Sophos uses plain English to tell me what something does and how it does it, which is more than some other AV vendors."

Enterprise customers also cite Sophos' antispam capability in its e-mail server/gateway products, PureMessage and MailMonitor. "It effectively quarantines spam," says the director of information security at a large consumer goods company. ▶

# SOPHOS