

Sophos Web Appliance

WEB SECURITY

The web is today's number one means of malware getting on to employees' computers. Organizations in every sector – public and private – are turning to Sophos to protect them against fast-moving web-based threats. By blocking infected webpages, inappropriate websites, and unwanted applications, the Sophos Web Appliance is giving IT departments worldwide the comprehensive control they need to enable safe, productive web browsing.



Business challenge

With one new infected webpage discovered every five seconds* organizations are vulnerable to a wide spectrum of web-based attacks, including spyware, viruses, Trojans, worms, and phishing campaigns.

In addition, there can be significant staff productivity loss if office hours are spent surfing social networking, shopping, hobby, or personal interest websites. Similarly valuable network bandwidth and resources are consumed by this activity, particularly when websites hosting media-rich content or unauthorized content types are involved. There is also an issue with anonymizing proxies, which allow users to bypass traditional web filters, thereby creating loopholes that expose organizations

to significant risks. One such risk is the legal implication of employees receiving inappropriate content in the workplace.

To secure themselves against these wide-ranging threats, organizations are seeking greater insight and control over web traffic and placing an emphasis on real-time malware detection. With the majority of web threats now being delivered from trusted sites, it is no longer sufficient simply to block access to questionable content. As a result, organizations are now looking for alternatives to traditional URL filtering solutions. Today's environment requires more sophisticated but easy-to-manage secure web gateway appliances that can scan content in real-time for threats before they enter the network.

Sophos WS1000

- » Proactive protection via Behavioral Genotype™
- » Blocking of spyware, viruses, malicious websites, anonymizing proxies and unwanted applications
- » HTTPS traffic filtering and automatic SafeSearch enforcement
- » Productivity filtering against 54 categories of web content
- » Easy deployment and use
- » Simplified "three clicks to anywhere" management
- » Group policy management
- » Remote heartbeat monitoring
- » 5-minute updates direct from SophosLabs™
- » 24x7x365 support
- » 3-year warranty

Sophos technology solution

SophosLabs™ analyzes billions of webpages every day, providing the Sophos WS1000 web appliance – part of Sophos Web Security and Control – with the most comprehensive reputation database available. With Sophos Behavioral Genotype™ Protection anti-malware technology providing protection against unknown “zero-day” threats, the web appliance gives IT administrators the confidence to safely open up the internet to support the needs of their employees.

The result is that organizations are turning to the Sophos WS1000 to combat the threat of web-based attacks and unwanted content, both to support their endpoint and email protection, and to replace obsolete URL filtering solutions.

Security

One such company is Heinz. When a web-based thin-client was introduced for company-wide use, it became imperative to bolster gateway security. At the same time as deploying Sophos protection at the email gateway and across thousands of employees' computers, it also implemented the WS1000.

The Sophos web appliance blocks websites based on their reputation – whether they are known to be bad, but also by scanning their content. With over 90 percent of infected webpages on legitimate websites, this ability to scan by content is crucial, as is the ability to proactively block new and unknown zero-day, threats before they have a chance to execute.

Heinz was impressed that in blocking infected websites the WS1000 did not create the false positive problems exhibited by some other solutions, ensuring that employees are not



inconvenienced when accessing non-malicious websites. “It was vital that we deployed a solution that was able to offer a high level of accuracy when analyzing websites, rather than restricting access to legitimate websites and stopping our workforce from doing its job,” says Heinz .

“We’ve been delighted by the high level of dedicated support and expertise delivered by Sophos, particularly given our need for a fast implementation.”

Chris Leonard, European IT Security and Compliance Manager, Heinz

The WS1000 also provides further security by scanning https traffic, by blocking the anonymizing proxies that are used to bypass web filters, and by recognizing true file types, however hackers might have tried to disguise them. This comprehensive protection delivers real value to organizations. “Now that we have better protection we have been able to relax our internet access policies to allow users to use things like webmail,” says legal firm Ison Harrison.

Productivity

The WS1000 filters webpages across 54 categories with sophisticated wizard-driven policy controls enabling organizations to manage employee productivity simply and easily. Flexible policies allow for access control to be set for particular times to allow more relaxed control during lunch hour or outside of core office hours, for example. Similarly, the appliance prevents IT time and resource being consumed fixing network productivity problems caused by malware and spam.

There is also a growing concern about unauthorized applications that are downloaded by end users taking up unnecessary bandwidth. The analytic capabilities of the appliance allows a high degree of insight into, and control over, traffic. “When we experienced an almost total loss of web bandwidth we were able to use the Sophos web appliance to trace this to an automatic updater for an application we were running. It was then a simple job to establish a policy that disabled this and any similar automatic updates”, says Ed Williams Senior Technical Engineer at At-Bristol, a science center which welcomes thousands of visitors onto its public network.

Ease of management and use

This management support starts with the WS1000's deployment. When US-based Northern Engraving decided to install the Sophos Web Appliance, alongside the Sophos Email Appliance and Sophos Endpoint Security and Control, installation of everything was completed in five business days – and it took just one day to set up the WS1000, and to configure internet use policy and proxy settings in Active Directory.

The company originally had Websense deployed. However, Chris Halverson, Network Administrator Northern Engraving, says “the amount of management that went into this product was stifling, sucking up already limited IT resources”. Now they benefit from the WS1000's easy-to-use “three-clicks-to-anywhere” management tools, the flexibility of wizard-driven policy options, and the range of reports that allow real visibility into traffic, performance and user behavior.

“The key factors in choosing Sophos were integration, simplicity of management, maximum protection and minimal impact on users.”

Ed Williams, Senior Technical Engineer, At-Bristol

Best value

Backed up by a high level of dedicated support and expertise from Sophos, the WS1000 is proving to be the investment of choice of organizations who take their web security seriously. Says Joey Elam, Systems Administrator of US-based Maple Knoll Communities “Sophos is definitely one of the best financial decisions to make as it's great value”.

