SOPHOS
Security made simple.

Next-Generation Web Security – Staying secure in today's aggressive environment

By **Peter Craig**, Senior Product Marketing Manager

This paper explains why organizations like yours need next-gen web protection as a strong first-line of defense to keep your systems and users secure. It also identifies the critical features that every web solution needs in order to give your organization true next-gen protection.

Sophos Whitepaper May 2016

Malware today – smarter and nastier

It's the unfortunate reality for today's organizations that malware attacks are growing increasingly more personalized and sophisticated. In the modern world hacking is big business, meaning big money and professional hackers looking to turn a profit.

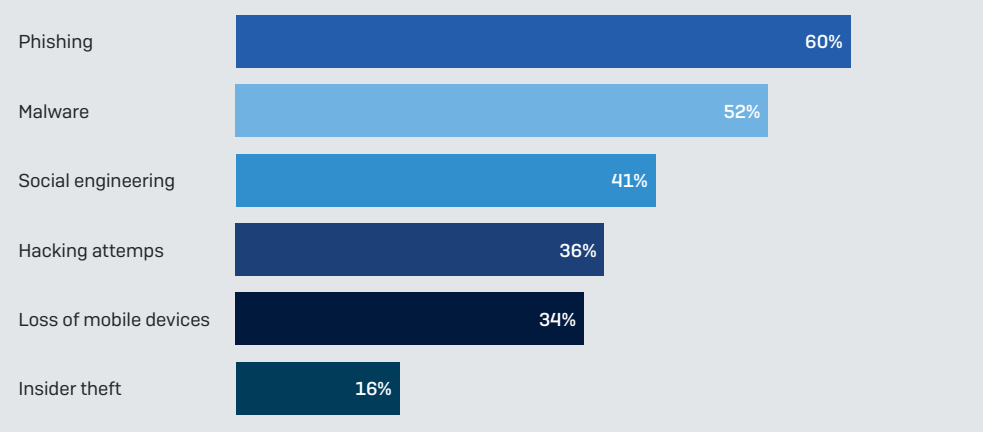
Barely a day goes by without a news of another organization being breached hitting the headlines. And these are just the big ones; organizations of all sizes are being targeted.

And it all starts on the web.

SophosLabs sees an average of 30,000 new malicious URLs every day and 59% of them are legitimate sites that have been compromised. 85% of all malware, including viruses, worms, spyware, APTs and Trojans comes from the web.

And according to a study by the ISACA - 52% of organizations have suffered a malware attack that penetrated their network.

Which of the following attack types have exploited your organization in 2015?



(Source: ISACA 2016, State of Cybersecurity - Implications for 2016)

Intercepting these threats at your network's frontline is the most effective way to deal with them. The best way to achieve this is with strong web protection that utilizes numerous techniques to stop threats slipping through the net. And it's becoming increasingly important to supplement this with a coordinated security setup where multiple solutions share contextual information to enable faster detection and response.

What organizations should look for in a next-gen web solution

Comparing and contrasting solutions from multiple vendors can be an uphill struggle. Terminology is often fluid, similar features may function in different ways and some vendors claim to offer next-gen solutions without including the necessary features.

To help we've identified the 3 critical areas that you should evaluate when choosing your web solution:

1. Protection
2. Performance
3. Simplicity

The following section discusses the key features that come under these areas. While this paper doesn't go into granular technical detail for each, it will give you a solid understanding of what constitutes a next-gen web solution.

Protection

The bread and butter of any security solution, but this is also the area most open to interpretation – especially when it comes to next-gen protection. Your web solution should include:

Advanced web threat protection	Automated threat updates	Anonymized proxy detection
Scan all downloaded web page content using techniques such as JavaScript emulation	Constant threat updates that are applied automatically	Stop users getting around your safe surfing policies

Sandboxing	URL & live protection filtering	Safe surfing policies
Detonate and monitor suspect files - blocking evasive and targeted threats	Automatically block newly infected sites as well as historic	Block sites based on key words, categories, IP & domains

Traffic scanning	Application control	Mobile management
Inspect HTTP, HTTPS, IMAP, SMTP, UTP, DNS traffic for suspicious activity	Identify, classify and control apps and inspect data used in them	Secure mobile devices both on and off the corporate network

Performance

Top tier protection means little if it results in snail-paced browsing speeds for end-users. Look for the following in your web solution:

Intelligent traffic routing (FastLane)	Global infrastructure
Route traffic to the optimal gateway to enhance download speeds	Infrastructure deployed close to your location for the best performance and with zero downtime

Simplicity

Powerful protection doesn't mean a solution has to be complicated to use. Save some of your valuable time and look for the following:

Detailed reporting	Centralized management
Pre-built reports to give you the information you need at your fingertips – e.g. network logs, user activity	One management console that you can use for all of your security solutions. One login, one password

Defeating targeted threats – Why organizations need sandboxing protection

As noted earlier in this paper malware attacks are becoming much more sophisticated and increasingly targeted at specific organizations. In simple terms this means that much of this type of malware is new and hasn't been seen before – making it more difficult to detect and neutralize for conventional security solutions.

That's why sandboxing is such a critical aspect of web security.

A properly configured sandbox works with your web solution to catch these new, advanced threats before they can do any damage. When a suspicious file hasn't been seen before by the web solution it's passed over to the sandbox. At this point the file is detonated and observed in the secure sandbox environment to see whether it is malicious or not.

Detailed threat and incident information is then passed on allowing for deep forensic analysis. And if you choose a cloud-sandbox solution you get the benefit of collective threat intelligence from organizations around the world.

On the network or off the network? Keeping up with mobile devices and 3rd-party apps

With the increasing popularity of Bring Your Own Device (BYOD) in organizations, securing and managing mobiles is a hot topic. On-top of this are 3rd-party apps that often operate outside the bounds of your corporate network, e.g. Dropbox, TOR, Salesforce.com; that also need securing to protect against data leakage and inappropriate usage.

For mobiles this means remote-policy deployment that ensures devices are kept safe and compliant whether they are on or off the corporate network. And for applications (both on mobiles and computers) that your web solution is capable of identifying, classifying and controlling them.

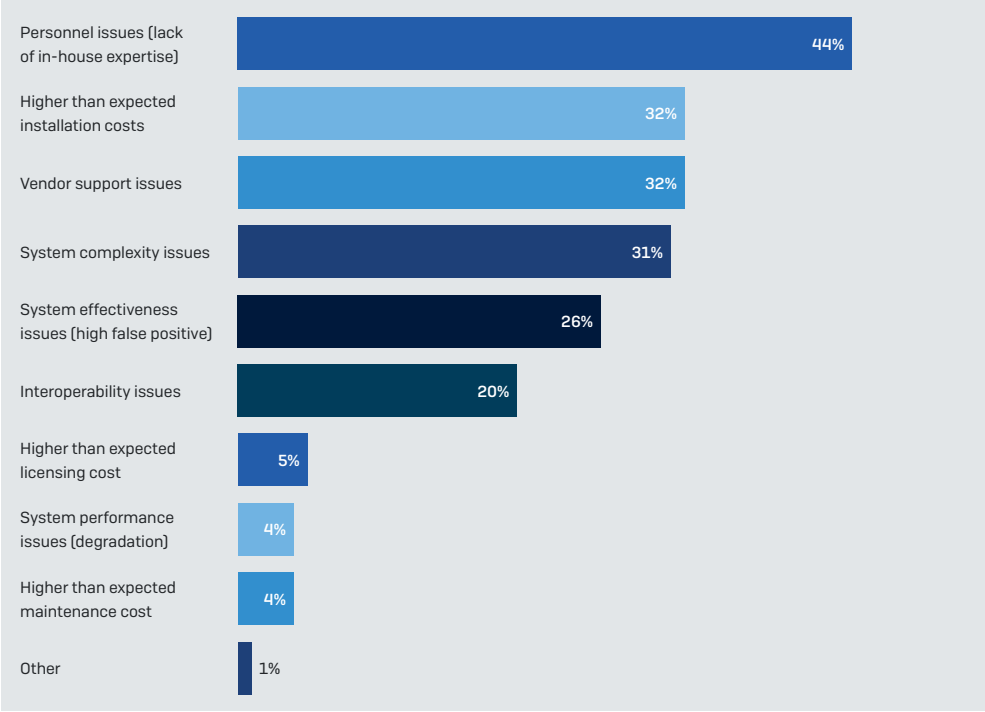
Making your security setup synchronized, stronger and straightforward

There are two main ways that organizations can choose to implement next-gen web protection. As an integrated solution that provides even more comprehensive protection against malware and DLP (Data Leakage Protection), or as a complex mesh of technologies that require manual integration to correlate and prioritize alerts.

Manual integration requires the IT manager to intervene and analyze data by hand from each solution in order to decide upon and coordinate a response. This can be a struggle for many mid-size organizations, as dedicated security resource and expertise is in very short supply.

And as the graph below highlights, this lack of in-house expertise is the top reason for disappointment with security technology purchases.

Why companies regret some of their investments in enabling technologies (two responses permitted)



(Source: Ponemon Institute 2015, 2015 Global Study on IT Security Spending & Investments)

And this isn't an issue that's going away anytime soon according to Enterprise Strategy Group:

"...46% of organizations now claim that they have a problematic shortage of cybersecurity skills... up significantly from last year (28%)..."[1]

Despite this critical skills shortage many vendors and their solutions are doing little to address the underlying issues. And while they are competent in their own right, they are lacking when it comes to addressing issues of complexity and giving organizations the automation and coordination they need to get the best protection possible.

The reality is that many organizations don't have the luxury of a dedicated cybersecurity team. Some won't have any employees whose sole responsibility is security. When this is compounded by security solutions that don't coordinate information, it can result in critical alerts being missed and systems being compromised.

Even enterprise-size IT teams will waste cycles with systems that don't coordinate. Multiple logins and consoles, duplicated information and alerts – these can all add up to more time than you might realize.

Introducing Sophos Next-Gen Web Protection

Sophos Next-Gen Web Protection delivers advanced web threat protection, improves users' browsing speeds and is easy to install, configure and manage through a central control engine. It keeps your users and devices safe and secure both on and off the corporate network.

- Next-generation web protection including advanced threat detection, URL and live protection filtering, traffic scanning, anonymized proxy detection and more
- 24/7 threat monitoring from Sophos Labs with automated updates throughout the day
- Scans HTTP, HTTPS, IMAP, SMTP, UDP and DNS traffic for malicious activity
- Real-time site reputation data
- Fast Lane technology intelligently routes traffic to the optimal Sophos gateway to enhance download speeds
- Safe surfing policies - block sites based on key words, categories, IP & domains
- Simple to install, configure and manage
- Over 10 locations available worldwide

In addition, Sophos Web Protection is part of Sophos' integrated portfolio of products that are engineered to work together to deliver better protection. Simplified management through Sophos Central lets you control your Web, Endpoint, Server, Email, WiFi and Mobile security from a single, intuitive interface. Which means you get the latest advanced protection while saving time and effort.

Conclusion

Web threats continue to grow in number, complexity and savagery, but the skills and resources to combat them are lagging behind. Sophos answers these problems with powerful, integrated solutions that have ease of use and performance at their core. These are the critical areas that every organization should consider when evaluating solutions.

[1] Enterprise Strategy Group 2016, Cybersecurity Skills Shortage: A State of Emergency

Try it now for free

Register for a free 30-day evaluation
at sophos.com/freetrials

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

16-06-24 WPNA (DD-2373)

SOPHOS