SOPHOS

simple + secure


# The four rules of complete web protection

By **Chris McCormack**, Product Marketing Manager

As an IT manager you've always known the web is a dangerous place. But with infections growing and the demands on your time and budget rising, it's time to revisit your strategy. This whitepaper discusses the major web threats and provides four rules to help you stay protected. When you follow them, these rules will also save you time and money.

# Why the web is a scary place

Your users are working on the web more than ever, reaping its benefits for increased mobility and easy access to the tools they need. But the web is also a dangerous place.

Cybercriminals constantly launch attacks designed to penetrate your digital defenses and steal sensitive data. During the first half of 2011, we saw an average of 19,000 new malicious URLs every day at SophosLabs—that's one every 4.5 seconds.

In a recent study of 50 organizations, 64% of those companies were victim to a web-based attack during a four week period.[1] And web-based attacks are the second most costly type of attack, topped only by denial of service attacks.[2] This type of cybercrime exposes you to enormous risks, including financial losses, regulatory and compliance issues, data breach liabilities, damage to brand and reputation, and loss of customer confidence.

In this whitepaper we'll discuss the types of threats and explain how these four rules can help you build a better web protection strategy.

# The four rules of complete web protection

1. Reduce the attack surface
2. Protect everywhere
3. Stop attacks and breaches
4. Keep users working

### Websites: The good, the bad and the risky

Malware is software designed to infiltrate a computer system without the owner's informed consent. It can include viruses, worms, spyware, adware and Trojan horses. And 85% of all malware comes from the web.[3]

1 Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011, http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

2 Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011, http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

3 SophosLabs

Cybercriminals set up websites hoping to lure people into their malware trap with a range of devious tactics. For example, sites offering content such as free screensavers or toolbars often bundle them with adware, spyware, viruses or other malicious code.

Sites hosting pornographic or gambling content are a boon for malware since they attract large amounts of traffic. A study by the International Secure System Lab found that approximately 12% of all websites offer pornography and 3.23% of these sites are booby-trapped with malware. The study also showed that almost half of all visitors used a computer and browser combination that was vulnerable to at least one exploit.[4]

And yet the vast majority of infected URLs found by SophosLabs—more than 83%—are legitimate websites that have been hacked to distribute malware. Because these sites are generally trusted and may be popular, high-traffic venues, they are attractive to hackers who want to silently distribute malware to unsuspecting visitors.

**4.5**

**A new web threat is detected every 4.5 seconds**

SophosLabs saw an average of 19,000 new malicious URLs every day in the first half of 2011—that's one every 4.5 seconds.

**23,000**

**Per day cost (in dollars) of a web-based attack**

On average, it takes a company 23.5 days to resolve a web-based attack, at a cost of nearly $23,000 per day.[5]

**90**

**Percent of attacks that could be prevented with a patch**

90% of attacks against software vulnerabilities could be prevented with an existing patch or configuration setting.

**83**

**Percent of malicious URLs that are compromised websites**

More than 83% of the malicious URLs found by SophosLabs are legitimate websites hacked by cybercriminals.

4 BBC, "'Shady' porn site practices put visitors at risk," June 11, 2010, http://www.bbc.co.uk/news/10289009

5 Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011, p. 20 http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

## Unpatched vulnerabilities: The unlocked door

For a threat to successfully infect a website visitor, it needs to exploit some weakness in the user's browser, browser plugin, application or operating system—that is, an unpatched vulnerability. Unpatched vulnerabilities are like secret unlocked doors that let the bad guys sneak onto your network.

Every year, hackers uncover thousands of vulnerabilities that become the focus of commercial exploit packs. These packs make it easy for cybercriminals to prey on browser vulnerabilities, add-ons and web applications, operating system weaknesses, media players and PDF viewers.

## More and more malware

With some types of malware, you may not even know you're infected. Many web malware attacks are designed to steal personal information and passwords or use your machine for distributing spam, more malware or inappropriate content without your knowledge.

On the other hand, one of the most common types of malware, fake antivirus, makes itself obvious by pretending to find dangerous security threats—such as viruses—on your computer. The initial scan is free, but if you want to clean up the fraudulently-reported threats, you need to pay. Fake antivirus scares the victim into handing money over directly to the malware author. Victims typically pay around $120 via credit card to purchase the junk software that will supposedly fix the problem.

Millions of dangerous and inappropriate files present an enormous risk of infection, create legal liability issues and place a burden on your infrastructure. These include risky executable files, virus-infected files, illegal content and pirated software. Files downloaded from websites can be vehicles for malware, and those with .exe and .dll extensions are often disguised as something legitimate but may harbor a virus or other malicious code.

## Drive-by download: The combo platter

Drive-by downloads attack multiple vulnerabilities in web browsers or plugins to execute code on a user's computer when they visit a website. Hackers inject the malicious code into the webpage content, and it downloads and executes automatically within the browser.

Common on both hijacked and known malicious sites, drive-by downloads are the cause of most malware infections today. The malware is typically part of a professional exploit kit marketed and sold to hackers.

## Today's landscape for web threats

Here are just a few of the techniques cybercriminals commonly use to distribute malware on the web:

**Blackhat search engine optimization (SEO)** ranks malware pages highly in search results.

**Social engineered click-jacking** tricks users into clicking on innocent-looking webpages.

**Spearphishing sites** mimic legitimate institutions, such as banks, in an attempt to steal account login credentials.

**Malvertising** embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites.

**Compromised legitimate websites** host embedded malware that spreads to unsuspecting visitors.

**Drive-by downloads** exploit flaws in browser software to install malware just by visiting a webpage.

Malicious code typically installs spyware or malware by exploiting known vulnerabilities in your browser or associated plugins. These malware threats include:

**Fake antivirus** to extort money from the victim.

**Keyloggers** to capture personal information and account passwords for identity or financial theft.

**Botnet software** to subvert the system into silently joining a network that distributes spam, hosts illegal content or serves malware.

# The four rules of complete web protection

So, what will it take to combat all of these threats? We recommend that you layer your defenses and follow our four rules of complete web protection. And we explain the technology solutions that your IT team can implement to support your web protection strategy.


## Rule 1: Reduce the attack surface

To reduce the attack surface, you have to avoid obvious threats and eliminate vulnerabilities.

**Malicious and inappropriate URL filtering** Security vendors now combine reputation-based data with URL filtering to stop users from accessing known infected sites or those that repeatedly host malware or other unwanted content. Reputation-based URL filtering that performs real-time lookups against the security vendor's database is especially effective at blocking the thousands of new malware sites, SEO poisoning attacks and hijacked trusted sites that pop up daily. Learn more about live URL filtering.

**Application control** Application control cuts your security risk and management overhead by stopping users from installing non-business-related software on their machines. Unnecessary and unauthorized applications increase the attack surface area by exposing more potential targets.

Hackers exploit holes in applications such as web browsers, PDF readers, media players, toolbars, instant messaging (IM) clients and peer-to-peer (P2P) clients. These applications introduce possible productivity, legal and data loss issues. And they increase the number of applications for IT to manage and patch.

But your organization may find that a blanket application control policy is overly restrictive. In response, some users will resort to even less desirable workarounds to get what they need.

Granular application control gives you the flexibility to employ different policies that are appropriate for different groups of users. Learn more about application control.

**Patching** It's estimated that 90% of attacks against software vulnerabilities could be prevented with an existing patch or configuration setting.[6] Despite this fact, many computers do not have the latest security patches installed. This puts organizations at serious risk from a variety of malware threats.

Why are patches so often ignored? Because they are painfully time consuming to track and administer. Therefore, it's important to follow three best practices for security-focused patch assessment:

1. Monitor the latest patches from widely-used commercial software

2. Prioritize patches tied to critical, in-the-wild threats

3. Don't leave patching up to users—identify which endpoints have the latest patches.

An intelligent patch assessment system, such as the one integrated into our Endpoint Protection security solution, tells you which patches you need to apply to stay protected, instead of presenting you with a daunting list of all the patches available. We call it patching for the real world. Learn more about patching.

6 Gartner blog, "Improving your 2011 security bang for the buck: patching depth and breadth," by Neil MacDonald, http://blogs.gartner.com/neil_macdonald/2011/01/04/improving-your-2011-security-bang-for-the-buck-patching-depth-and-breadth/

## Rule 2: Protect everywhere

Your users are no longer tethered to the network, so keeping them safe has become more difficult. You need to protect them wherever they are.

**Endpoint web protection** Your offsite users are probably going unprotected when they are out of the office. Or they are forced to backhaul all their web traffic through your gateway or a SaaS service, which can be expensive and full of issues. Protecting all of your users is easy with web protection integrated into the endpoint. This way, they can take their web protection with them, wherever they go. What's more, you can account for their activity and update policy for them, in the same way you would if they were in the office.

**Mobile device control** The explosion in mobile working and superfast connections means that securing data at every point is a priority. You need to be able to set security policies for the latest mobile devices and remote lock or wipe them if they go missing. This includes complete security for files uploaded and accessed from the cloud, whether from PCs or mobile devices.

## Rule 3: Stop attacks and breaches

It's time to move beyond signatures. With innovations like real-time updates, you can stop new threats instantly.

**Anti-malware** A real-time web threat scanning engine is perhaps the single most essential component in a web protection solution. To be effective, it must scan all web traffic, including trusted content, to identify known threats as well as new zero-day exploits. Every time a user accesses a site, the scanning engine inspects the traffic with a combination of anti-malware signatures and behavioral profiling. In-the-cloud, real-time lookups against the security vendor's database provide the timeliest defense against emerging threats.

Malware authors increasingly morph and hide their malicious code with obfuscation. An effective web anti-malware solution helps you fight back by detecting hidden suspect code; for example, by de-obfuscating and emulating JavaScript before it is executed. A Host Intrusion Prevention System (HIPS) stops malware before a specific detection update is released by monitoring the behavior of code.

Scanning HTTPS encrypted traffic is also important, since up to 30% of web traffic is now encrypted for privacy. HTTPS is a secure version of the Hyper Text Transfer Protocol (HTTP) that establishes a secure connection between a user's browser and a target website. HTTPS traffic is normally invisible to most web security solutions, creating an obvious opportunity for web malware authors. However, Sophos HTTPS filtering looks inside encrypted streams using an advanced man-in-the-middle approach to provide a full range of control. Learn more about anti-malware filtering.

**Live antivirus** With so many new and unknown threats emerging daily, your threat protection has to update constantly to protect you against them. Live antivirus technology keeps you safe by checking for new threats in real time. For example, Sophos integrates live antivirus within its endpoint agent. Sophos Live Anti-Virus provides automatic, in-the-cloud checks against the extensive SophosLabs threat database. That makes the latest threat intelligence available to the endpoint, so you're protected even between updates. Learn more about live antivirus.

## Rule 4: Keep people working

Security measures shouldn't get in the way of your daily business. At the same time, you need to keep your employees from accessing risky sites that could bring threats into your environment.

**Productivity filtering** Prohibiting access to illegal, inappropriate or non-business-critical web content is a standard practice for businesses, as it should be. Most organizations blacklist adult and gambling sites, while some go further and block time-wasting sites like Facebook, shopping or sports. But blocking questionable content isn't enough to stop threats from the vast majority of malware.

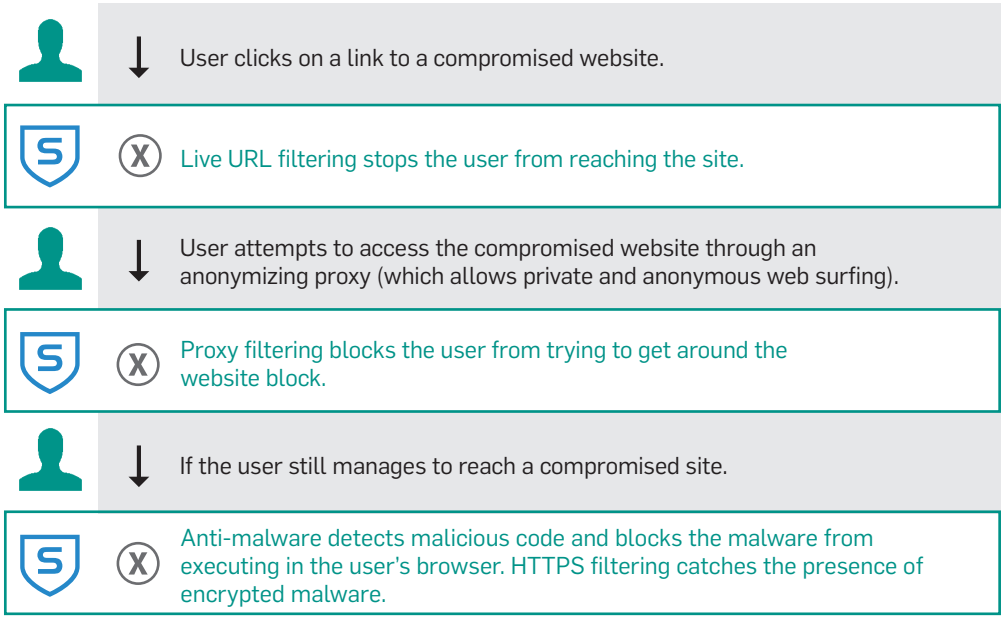
Of course, you have to supplement productivity filtering with live URL filtering and malware detection to block threats. In addition, proxy filtering keeps rogue users from bypassing productivity filtering or acceptable use policies. Learn more about productivity filtering.

**Visibility** It's important to monitor user activity and identify problem behavior before it becomes a real issue. If you offer an open policy and see repeated offensive content being accessed, you can either implement more stringent controls or talk to the offending users before you have a legal case on your hands. Monitoring web activity can help identify infected machines attempting to call home with stolen data.

Activity reports should immediately highlight suspect machines so you can follow-up before it's too late. Finally, in rare situations, forensic investigations into a problem user may be required by human resources, and you'll need to be able to respond to these kinds of investigations appropriately.

### A Layered Protection Strategy

All of your defenses have to work together for complete protection. It's the best defense against complex web threats. Here's an example of how layered defenses can protect you when a user attempts to visit a compromised site.




## Introducing Endpoint 10 and the Sophos Web Protection Suite

Learn about how Sophos can give you complete web protection with Endpoint Protection—Enterprise and the Sophos Web Protection Suite.

**Endpoint Protection—Enterprise**

- Complete security that includes web protection, encryption, and patch assessment
- Proven protection automatically identifies new malware threats and cleans them up
- One agent scans for viruses and controls applications, devices, data and web access

Endpoint Protection—Enterprise gives you everything you need to stop malware and protect your data in one console and agent. We'll work to block threats, not productivity. Our scanning engine takes care of everything, and it works faster than before.

Our live, cloud-based protection checks suspicious files against our database, stopping malware before it can run. We can identify new threats, clean them up and minimize the number of false positives using our practical host intrusion prevention system (HIPS).

We put web malware scanning and inappropriate site filtering in our endpoint agent. Plus, our Patch Assessment identifies, prioritizes and scans for critical threat-related security patches.

**Sophos Web Protection Suite**

- Combines the best of our endpoint, gateway, and cloud protection
- Take your secure web gateway with you everywhere
- Manage all your users, on the network or off
- Gain insights and rich reporting for offsite users too

Keeping offsite users safe and productive on the web can be a major pain. Our Web Protection Suite eliminates costs and complexities by solving your web protection needs in a whole new way. We've integrated our latest cross-browser web filtering technologies into our endpoint agent. They seamlessly block all the latest threats and stop malware downloads wherever your users go. Plus, full productivity filtering keeps your users compliant and protected across all site categories whether they are on the network or off.

Our LiveConnect technology keeps your endpoints connected to your web management console transparently and securely. This way user-policy updates and reporting behave as if every user was on the network. No one else provides this kind of seamless, unified management of both offsite and onsite users.

Providing complete web protection everywhere has never been easier or more affordable. We can keep you fully protected and save you time and money in the process.


## Sign up for a 30-day trial

visit sophos.com.

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

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

Boston, USA | Oxford, UK


A Sophos Whitepaper 12.11v1.dNA

SOPHOS