

# **GFI** WHITE PAPER

## **Towards a Comprehensive Internet Security Strategy for SMEs**

Small and medium-sized enterprises (SMEs) need a comprehensive Internet security strategy to be able to protect themselves from myriad web-based threats. Defining and implementing such a strategy requires proper preparation, a clear understanding of the technologies and methods that can be adopted, a good user-education program and a proactive approach to security. This White Paper discusses the elements of an Internet security strategy.



## Introduction

The web is an integral part of how all businesses, especially small to medium enterprises (SMEs) and their employees communicate, collaborate and succeed.

As discussed in detail in the GFI White Paper, *Web-Based Threats*, the prevalence of malware as a vehicle for organized Internet crime, along with the general inability of traditional anti-malware protection products to protect against the continuous stream of unique and newly produced malware, means that SMEs operating on the Internet must start from the premise that a percentage of their Internet customers will be infected for one reason or another, and that they need to continue doing business with infected customers.

The growth of web threats is a result of the popularity of the web – a relatively unprotected, widely and consistently used medium that is crucial to business productivity, online banking, and e-commerce as well as the everyday lives of people worldwide. Accessing applications on the web and the popularity of social networking are just two examples of advancements that new security concerns to everyone – particularly for SMEs.

The most viable approach is to implement multi-layered protection – protection in the cloud, at the Internet gateway, across network servers and on the client. The most important defense, and perhaps the most difficult to achieve, is to educate users as part of a comprehensive strategy against these threats.

In today's business environment, every business has to manage more risks with fewer resources. Prioritization and risk management need to be integral parts of that strategy. The alternative is to react to every threat and hype and buy point solutions for what may seem to be an economical price but end up with complex configurations that lead to high operation costs.

Managing Web 2.0 is far more difficult and challenging because these services are free and open. Employees can use web-based emails, social networking websites, P2P networking and download media files. Downloaded files can then be transferred to a portable device and then viewed in company computers where threats can be spread.

## What worked before doesn't now

Although they remain critical and effective components of endpoint security, desktop firewall, antivirus, anti-spam, anti-spyware and other signature-based protection tools are not sufficient to stop modern web attacks.

Antivirus and anti-spyware applications traditionally identify and stop infiltration of viruses, worms, Trojans, adware and keystroke loggers. They provide real-time protection as well as detection and removal capabilities. However, they struggle in the face of today's highly complex, blended and constantly mutating viruses and worms. Threats change their signature on every PC they infect and signature-based protection, as a defense for some 0-hour web based attacks, are ineffective.

Desktop firewalls, while they certainly provide an excellent first line defense by blocking non-allowed sites and controlling traffic, do not protect against users' behavior and do little to prevent direct online contact with malware. Malware programs can indeed be installed automatically without even requiring any user interaction. Most studies show indeed that 80% of the PCs running firewalls end up being infiltrated with spyware and other malware.



Too many enterprises overly rely on traditional endpoint protections and assume they already have sufficient Internet security to prevent web-based attacks. In fact they remain insufficiently protected. Today's attacks require a third generation solution that uses a dual approach combining the benefits of traditional security controls with web-focused controls that thwart attacks from today's dominant vector for security exploits.

As mentioned, implementing layers of security protection would help but not many SMEs actually do that due to budget constraints. Still there many technologies and processes available to help SMEs keep web-based threats at bay.

### **Start by educating the user**

The web is a war zone, and the only way to really win is to enlist the help of employees. Not educating users is much like not teaching a soldier how to use his rifle. It's a basic thing and without it you've lost your most powerful allies.

Teach users about threats and encourage them to speak up if something looks odd or out of place. Convert them from trusting to being suspicious of outside requests to install or uninstall an application. Encourage them to call the help desk. Make sure they understand that file swapping, porn, gambling, and social networking sites are havens for criminals and malware. Provide them with security best practices that they can use on their home computers too, that will reinforce the online safety message. If you have to deny a privilege or block a site, make sure users understand the reasons why.

### **Have an Acceptable Use Policy**

Nearly every enterprise has a specified set of rules, usually spelled out in an employee handbook that an employee has to acknowledge by signature that he or she has read and understood. Some of these policies, such as that against racial or religious discrimination and mandatory email archiving are required by law or regulation. Other may reflect common business ethics or a particular company's culture such as prohibitions against drinking, unexcused absences, sexual harassment and the like. Policies also include a set of sanctions that can be used against persons who violate the company's policies. They also provide a legally defensible basis for disciplinary action, up to and including termination.

One key advantage to policies like this is that while, traditionally, employers have been held responsible and liable for their actions in the workplace, the presence of policies prohibiting such actions has served as a liability shield that can completely or partially protect that company from lawsuits arising actions from employees acting in contravention of the policies.

To safeguard its electronic communications, every company, large or small, should have an Acceptable Use Policy in place that governs Internet, email and computer use in the business.

In essence, an Acceptable Use Policy serves as guidance for staff and volunteers on the behavior and use of technology that is approved by the organization. The policy should also detail the consequences that company personnel can expect to face for the abuse of this technology.

For more information about acceptable use policies, see the GFI Whitepaper [\*Acceptable Use Policy\*](#).



### Deploy Internet Monitoring Software

Unfortunately educating users and having an Acceptable Internet Use Policy is not always enough. Survey after survey shows that there is always a certain percentage of employees who do not understand the message, lack the necessary computer skills to adhere to them or simply choose to disregard them for any variety of reasons ranging from a rebellious streak to out and out criminal intent. The losses to productivity, exposure to security breaches and liability can be extensive. Web monitoring can provide a powerful solution to this.

Internet monitoring (also known as web monitoring) is a general term for protecting a company or other organization from these threats through the use of software to achieve control of Internet use of the organization by blocking specific sites, filtering against keywords, preventing downloads in general or of specific file types and logging sites an employee visits. In some high quality Web Monitors, multiple scanning engines are used to scan for viruses and other malware.

Among the proven benefits to web monitoring are:

- Effectively enforce an Internet Usage Policy and reduce cyber-slacking
- Increased productivity
- Increased security by preventing visits to dangerous sites or downloading malware
- Increased web security – using multiple AV engines to filter web-based threats
- Maximize bandwidth by minimizing non-work related usage
- Increase data security for the organization.

Internet monitoring also serves an important psychological benefit, in that it demonstrates to employees that the organization is serious about the policies it has made and protecting both the employee and the business from misuse of the system provided for their benefit.

For a fuller discussion on the benefits of Internet monitoring, see the GFI White Paper: *Internet Monitoring: Not “Big Brother” but “Wise Management.”*

### Secure the browser

The Web is a personal playground for many users. You may not be able to get them from taking recess there, but you can provide a safer environment by using security controls built into the browser. For example, Internet Explorer gives you plenty of options for handling cookies. Cookies with user credentials are a popular target for online criminals, and malformed ones are used for cross-site scripting attacks that can steal credentials and redirect users from legitimate to malicious sites. IE also lets you set policies for third-party add-ons and browser plug-ins. You can count on one hand the number of add-ons that have legitimate business value, such as Acrobat PDFs. The other major browsers offer similar controls, so put them to work if your company is using multiple browsers.



### Limit User Administrator Rights

A significant portion of your workforce has little reason to run PCs and laptops with full administrative rights. Restricting admin privileges can prevent installation of unwanted software and malware. Take advantage of Windows' User Account Control feature, which was introduced in Windows Vista and is available in Windows 7. It limits users' rights to perform functions such as changing system state, disabling the local firewall, and installing software. Doing this doesn't guarantee your employees' safety, but it helps limit the number of attack vectors to which they are exposed.

### Use Windows 7 AppLocker

If you are upgrading to Windows 7, AppLocker, is a new feature that works like an application firewall that allows administrators to define which applications can execute what based on a vendor's digital signature or a file revision of a particular executable, among other things. It also lets administrators configure group policies that prevent users from running unapproved applications.

### Deploy Software as a Service (SaaS) Web security

SaaS is software that is deployed over the internet and/or is deployed to run behind a firewall in your local area network or personal computer. With SaaS, a provider licenses an application to customers as a service on demand, through a subscription or a "pay-as-you-go" model.

SaaS allows Web malware filtering as a service. Web traffic is routed through the provider's cloud, where malware is stripped out in real time. Providers also usually bundle other services, such as URL filtering, which keeps employees from exploring the Web's darker corners. Companies get the same functionality that they get from on-premises products, but without the capital expense.

SaaS is not without its problems however, a 2008 Gartner's survey of 333 enterprises in the US and the UK found a low level of approval from customers, describing overall satisfaction levels as "lukewarm." Respondents who decided against SaaS cited high service cost, integration difficulty, and technical requirements.

### Maintain a continuous security monitoring approach

No matter what you finally deploy, the job doesn't end there.

You can solidify your security strategy by constantly monitoring security incidents and by keeping up with the latest hacking tools and methodologies. You can also find websites that host information on how to exploit specific products. These are usually based on out-of-the-box configurations, so keep current with vendors on new features, versions, or newly exposed risks.

It's also important to assure that software is updated, patches are applied to address the latest threats and the operating systems are routinely updated with the latest Service Pack.

None of this alone, or in tandem will stop malware. In fact nothing may ever provide a total solution. But if you are an SME, these methods will go a long way to helping you form a comprehensive Internet security strategy.