eset
Internet Security

WHITE PAPER

CONTENT FILTERING: NO LONGER JUST FOR THE ENTERPRICE

SUMMER 2013

Abstract

Controls on employee web surfing are being increasingly adopted by businesses. The aims are to limit exposure to malware and data breaches, improve productivity and reduce business liability due to employees accessing inappropriate content. Small businesses are no exception and in some ways face greater exposure than larger enterprises. Of the three predominant models for deploying web content filtering, integrating the functionality within an endpoint security suite is the most recommended for small businesses. Such a deployment is less expensive to implement and easier for a small IT staff to manage. It improves performance and protects both remote workers as well as those onsite. Most importantly, it supports flexible policies that apply business-appropriate restrictions while allowing specific employees the access needed to perform their jobs.

Introduction

When employees carry their web surfing habits into the business, they introduce business risks: malware-laden websites that can infect office computers, diversions that drain productivity and employees accessing inappropriate content. To control those risks, web content filtering is a mechanism that allows or blocks access to specific sites. Filtering allows or denies access based on a site's web address, more technically known as the uniform resource locator (URL). To allow administrators to manage and control access to a large number of sites at once, sites are categorized based on their content, placed into groups and assigned ratings.

Placing limits on employee use of the Internet is a balancing act. Restrictive policies can control use of bandwidth, improve worker productivity and limit the liability exposure. However, overly stringent policies carry a "big brother" message and can negatively impact employee morale. Any web content filtering system has to be flexible to accommodate and enforce a policy well-tuned to the needs of the business.

Why the need is critical

Web content filtering does not solve a problem; it solves several of them. Businesses might be grappling with one of them or all three. These are driving the growing interest in content filtering, with the market forecast to grow by 12 percent annually through 2015.[1] The distinct issues are:

1. Protection against data breaches.

Every day, on average, there are 9,500 new malicious sites created. These include innocent sites that have been compromised and new sites specifically created for phishing attacks. Every day, Google sends from 12 to 14 million warnings to users about current malware threats, 300,000 malware warnings for downloads and thousands of notifications to webmasters about infected sites. An employee accessing one of these malicious websites by accident can infect an office computer with malware, often with no knowledge that anything has happened because these "drive-by downloads" are invisible by design and install in seconds.[2] The installed malware typically includes spyware such as password sniffers, keyloggers or backdoor remote-control software, creating the conduit for a data breach. Stolen data can hurt the reputation of a business, lead to fines if in a regulated industry or even lead to potential liability if a computing asset is then used to compromise a business partner.

Content filtering market is forecast to grow by

12%

annually through 2015.[1]

2. Keeping employees productive.

Studies have found that employees spend from one to three hours daily surfing the Internet for personal use.[3] Non-business use of the Internet by employees during working hours has been termed cyberloafing by one study. It found that 60 to 80 percent of peoples' time on the Internet has nothing to do with work and includes watching media or pornography, attending to personal e-mails, managing personal finances and shopping online. Companies spend time and money monitoring usage and writing and enforcing policies, but the study found that policies alone are not enough to stop the practice. Policies coupled with detection mechanisms are effective at stopping the most inappropriate behavior, but behaviors deemed to be less inappropriate, such as personal e-mail and social networking, are harder to stop—even among employees who know they are being monitored. The study concluded that enforcement is the only real deterrent; however, it also acknowledged that overly restrictive policies negatively impact employee morale.[4]

3. Controlling liability concerns.

Distasteful websites are popular to block, partly because of productivity concerns but also because of possible liability. Employees looking at inappropriate content that is seen by other employees, partners or customers can be grounds for hostile work environment lawsuits.[5] According to the Equal Employment Opportunity Commission, a workplace in which such images are shared can constitute such a "hostile environment"—one that "unreasonably interfer[es] with an individual's work performance" or that creates "an intimidating, hostile, or offensive working environment."[6] Even off-color cartoons or inappropriate Facebook activity can be grounds for a complaint.[7]

Implementation models

To counter these risks, businesses can adopt one of three general deployment models for content filtering.

1. Gateway appliance.

Under this model, all web traffic flows through a server (typically in the form of a self-contained hardware device) located at the perimeter of the business's network. With all traffic flowing through, managed and enforced within a single device, this is a straightforward solution. However, it also constitutes a chokepoint and a single point of failure, which is a consideration if continuous web access is fundamental to the core business. There are two other potential drawbacks: For employees working offsite, their computers remained unprotected from malicious websites unless they log on to the corporate network via a VPN connection. In addition, tech-savvy users can bypass the filtering, depending on how it is implemented, by using proxy servers, customizing their DNS settings or other methods.

2. Cloud-based (software-as-a-service) offering.

Fundamentally, this places the functions of a gateway appliance in the cloud. It typically involves setting up a proxy to redirect the web requests to the cloud service, either by deploying a physical server to redirect the web requests or by configuring proxy settings in each user's web browser. Since authentication and statistical reporting is handled by the cloud-provider's server and database, there are security concerns surrounding business data in third-party hands. Additionally, these services are usually not as cost effective as other options and initial setup and configuration are time consuming. Like the gateway appliance model, cloud services can be bypassed by reconfiguring browser proxy settings.

3. Endpoint security solution.

Content filtering is enforced on each individual machine through software installed as part of a security suite that typically also includes antivirus, antispyware and a personal firewall. It can be centrally managed at each machine by an administrator through a console but applies the protection at each endpoint. This offers the same advantage of central administration as a gateway appliance, but the distributed enforcement means there is no single point of failure. This approach can provide the best of both worlds, especially where an endpoint solution for antivirus/antispyware is already in place or is being considered.

Content filtering for small businesses

The familiarity that comes with being a close-knit small business might provide a feeling of security but is of little protection when otherwise legitimate websites are compromised with malware every day. Smaller businesses are in many ways more at risk than large enterprises when it comes to employees falling for phishing schemes and clicking on malicious websites. As large enterprises with the resources to enact more sophisticated security are doing so, hackers and cybercriminals see small businesses as easier prey.[8] Even if a small business feels it can trust its employees—and many do—even the most diligently productive and tech-savvy worker can be duped into clicking on the wrong button and infecting the entire business.

A recent survey found that "Internet site blocking" is the third-highest priority among small businesses. It ranked just behind endpoint antimalware and data-loss prevention.[9] All three, in fact, have much in common. These are proactive measures that allow forward-thinking businesses to put a stop to security incidents before they happen. Putting content filtering and other measures in place allows the business to focus its often-limited IT resources on more productive tasks that have a more direct return on investment.

Advantages of the endpoint model

In a survey of 500 IT managers in companies of 1,000 or fewer employees, 80 percent stated that web content filtering was a somewhat or very important feature in an endpoint security suite.[10] By putting antivirus, antispyware and other security measures at the endpoints and allowing them to be administered through a central console, small businesses avoid investing in multiple solutions that have to be managed separately. With the integrated approach, there are fewer security holes and small businesses are able to achieve more comprehensive protection.

Specifically, the endpoint model has these advantages:

Reduced implementation expense.

Businesses that might be reluctant to implement web content filtering because of the time and expense might have everything they need already in place. If they are currently using some form of endpoint security, content filtering can be enabled as part of the existing security suite. This means there is no additional hardware or implementation time and all features are covered under the same license, which delivers clear cost savings. On the other hand what if there is no security in place and the business is just beginning to roll out a solution? Then an integrated endpoint security suite is far more cost effective and quick to deploy than setting up a hardware gateway for content filtering at the perimeter, plus an antivirus/antispyware solution and personal firewall on the desktops.

Integrated security management.

The entire security suite, including content filtering, is centrally managed using a remote administration console. This affords more granular control, with all features of the security suite sharing the same defined groups for setting various polices. In addition, IT manages the entire suite using the same user interface, avoiding the need to switch between tools for managing various aspects of security. If IT resources are limited, the content filtering capability can be rolled out during the initial configuration, then adjusted over time to suit the needs of the business.

Single engine for higher performance.

Antivirus, antispyware and content filtering all run on the same engine, so there is no need to install multiple agents that consume system resources and cause potential system conflicts and compatibility problems.

Protection for remote workers.

With a hardware solution, remote workers are unprotected unless they connect to the corporate network via a VPN. Yet those workers can expose the rest of the business to the same threats as those that work onsite. In one survey, 75 percent of small businesses said they have remote workers, and 66 percent said web control was their number one concern for those offsite devices.[11] An endpoint solution allows the business to protect those devices, regardless of how they connect and keep those workers productive.

Flexibility to formulate policies by role.

Centralized security management, enforced at the desktop, allows businesses to assign users to groups and enforce role-specific policies. This flexibility allows the company to create a policy that lets employees do their jobs and protect the enterprise, while balancing against the impact that overly restrictive filtering can have on employee morale. The following are examples of the scenarios that can be enforced.

- Allow most personal use, but block malware sites and adult content that can pose liability risks.
- Restrict access to file-sharing, video, social media and restricted categories for a majority of employees, or by groups or departments.
- Apply a restrictive policy, but allow specific access for business purposes:
  - Grant sales access to LinkedIn for connecting with customers
  - Give support access to YouTube for locating and posting how-to videos
  - Permit HR to access social media sites for reviewing candidates

In addition, administrators can manage the list of websites and add new permissions as necessary:

- Review new sites that have been accessed by employees to determine whether they should be blocked or allowed.
- Query the data to find permitted sites that have been notable time-wasters and add them to the custom filter list.
- Access summary data by users or sites to determine how well the policies are working, making adjustments that best balance the needs of workers and the business.

A centrally administered endpoint solution gives small businesses the flexibility needed to adjust the levers and optimally protect the business while preserving whatever elements of worker Internet freedom that the employer feels is appropriate.

Conclusion

Small businesses and large businesses alike share the need for web content filtering, but smaller businesses need affordable solutions that can be easily managed by a smaller IT staff. Implementing this functionality as part of an endpoint security suite has distinct advantages for small businesses. Because it shares the same underlying engine and remote administration console as an antivirus/antispyware solution, the capability can be added with very little additional investment and management burden. It provides the key capabilities for enforcing flexible role-based policies that every business needs, in a practical solution that protects the business on multiple fronts.

References

1. IDC. http://www.computerlinks.de/FMS/19646.idc_web_security_exerpt.pdf
2. http://googlepublicpolicy.blogspot.com/2012/06/safe-browsingprotecting-web-users-for.html
3. http://humanresources.about.com/od/technology/a/surfing_web.htm
4. http://www.k-state.edu/media/newsreleases/jan13/cyberloaf13113.html
5. *Pornography (porn) on Computer Screen in the Workplace.* http://www.thearmstronglawfirm.com/Types-of-Sexual-Harassment/Sexual-Harassment-Porn-on-Screen.shtml
6. U.S. Equal Employment Opportunity Commission. Enforcement Guidance, March 19, 1990. http://www.eeoc.gov/eeoc/publications/upload/currentissues.pdf
7. *Keep Yourself Out of the Headlines: Why an Internet Use Policy Is Important, and How to Get Your Own*, November 16, 2012. http://www.covenanteyes.com/2012/11/16/internet-use-policy-keep-yourself-out-of-the-headlines/
8. Parija Kavilanz. *Cybercrime's Easiest Prey: Small Businesses*, CNN|Money, April 23, 2013. http://money.cnn.com/2013/04/22/smallbusiness/small-business-cybercrime/index.html
9. IDC's US SMB Survey, 2011, as reported in an IDC webinar, U.S. SMB Security Market 2011-2015: *The Shift from Defense to Empowerment*, May 31, 2012.
10. Savitz Research Solutions, 2012.
11. Savitz Research Solutions, 2012.