WEBROOT®

How Web Security Improves Productivity and Compliance

Why business managers, HR, legal, compliance and IT all like content filtering and web policy controls

Contents

Introduction: Web Security Is Not Just Security 1
What Are Secure Web Gateways? 2
Helping the IT Security Staff 3
Improving Productivity for Business Unit Management 3
Managing the Workplace for the Human Resources and Legal Departments 4
Verifying Compliance for Compliance Officers and Auditors 5
Reducing Costs for CIOs and IT Managers 5
Educating Employees on Acceptable Use of the Internet 6
Why the Webroot Web Security Service Is the Most Effective Cloud-based Secure Web Gateway 7
Conclusion 9

Brought to you compliments of
WEBROOT®

Introduction: Web Security Is Not Just Security

Many people think of "security" in terms of its dictionary definition: "measures taken to guard against espionage or sabotage, crime, attack, or escape."[1] But in the case of information security, the same technologies that protect against bad guys can also create positive outcomes like increased productivity, reduced costs and improved regulatory compliance.

In this white paper, we will look at how secure web gateways, one type of information security technology, can provide benefits to many departments within any business or government agency.

[1] Merriam-Webster.com: http://www.merriam-webster.com/dictionary/security

After providing a brief overview of secure web gateways, we will look at how they can help:

- **IT staff** *improve security.*
- **Business units** *increase productivity.*
- **Human resources and legal departments** *apply labor laws and avoid lawsuits.*
- **Compliance officers and auditors** *demonstrate compliance with government and industry regulations.*
- **CIOs and IT managers** *reduce costs.*
- **Employees** *follow Internet acceptable-use policies and accept them as fair and reasonable.*

We will close by introducing Webroot® Web Security Service and discussing why it is the most effective cloud-based secure web gateway available.

What Are Secure Web Gateways?

A secure web gateway is a perimeter, or edge, security solution designed to protect companies from web-based threats, enforce Internet acceptable-use policies and help companies manage web usage.

Threat Protection

Secure web gateways scan web traffic to detect and block viruses, worms, Trojans, spyware and other types of malware before they reach the corporate network. This adds an extra layer of protection in front of server and desktop antivirus packages.

URL and Content Filtering

Secure web gateways improve security by blocking employees from visiting websites that contain malware, phishing and spam senders, botnets and other threats.

Secure web gateways also enforce Internet acceptable-use policies by blocking access to sites that violate company policies, such as sites devoted to pornography, weapons and hate speech.

Secure web gateways can filter content selectively, applying different policies to different groups — for example, allowing people in HR and legal roles to access sites related to their work while blocking other employees from those sites.

And some secure web gateways include advanced features like:

- The ability to identify suspicious web sites on the fly and place them on a blacklist until they can be reviewed.
- Employee guidance that explains why certain web sites are blocked or warns them that certain sites are suspicious.

Activity Quotas

Secure web gateways can also be used to impose reasonable limits on employee activities. For example, they can limit how much time employees can spend online in a day or the number of megabytes they can download. The gateway can also control the use of social media applications during work hours or block them altogether.

Usage Reporting

Secure web gateways can provide dashboard-type overview charts and detailed reporting on web usage and present aggregate information such as company Internet usage by time period and department. They can also allow managers to drill down and look at details, such as the web sites visited most often, the employees using the most bandwidth and employees using questionable search terms.

Helping the IT Security Staff

Of course secure web gateways help the IT security staff fulfill its mission of protecting company information and resources in the following ways:

- Threat protection capabilities block malware before it reaches the corporate network.
- URL content filtering keeps employees away from web sites infected with malware.
- URL content filtering can block outbound traffic to command-and-control servers used by hackers and cybercriminals.
- Content filtering by file type can control what files can be downloaded from and uploaded to web sites.
- Controls on applications, games and social media can reduce the risk of confidential company and personal information being disseminated and later used for phishing attacks.
- Usage reporting can be used to monitor web usage, investigate potentially dangerous web sites and identify employees who are engaging in risky behaviors on the web.

But the benefits of secure web gateways go far beyond these classic security features.

Improving Productivity for Business Unit Management

While business unit and functional managers are, of course, interested in maintaining IT security, they also place a high value on improving worker productivity. That includes stopping workers from engaging in time-wasting activities. And today, surfing the web is the number-one time-wasting activity for many employees. Figure 1 shows the results of a recent survey: 11% of employees spend at least five hours per week on non-business web sites, and another 21% spend two to five hours on such activities.

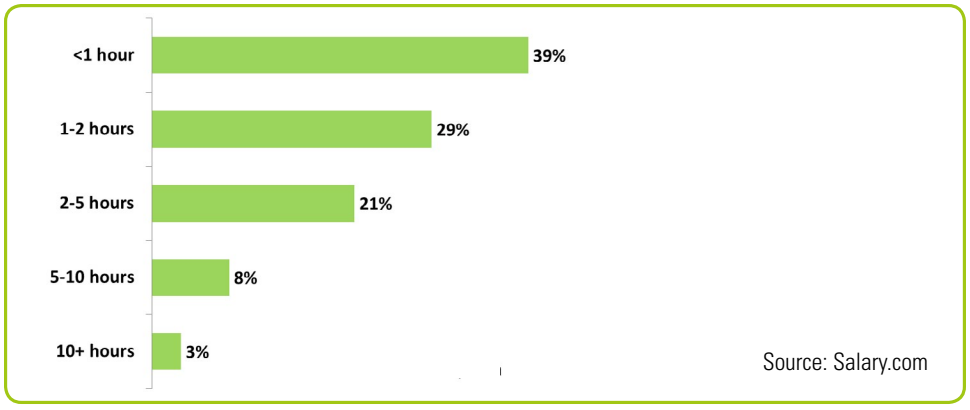

Figure 1: Hours spent on personal web sites per week.

Figure 2 shows the most popular time-wasting sites.[2]

Content filtering gives business unit managers the ability to block or limit employee visits to web sites that don't serve a business purpose and undermine productivity. Those might include online games, shopping sites, sports sites, gambling sites, job search firms, and personal sites and blogs.

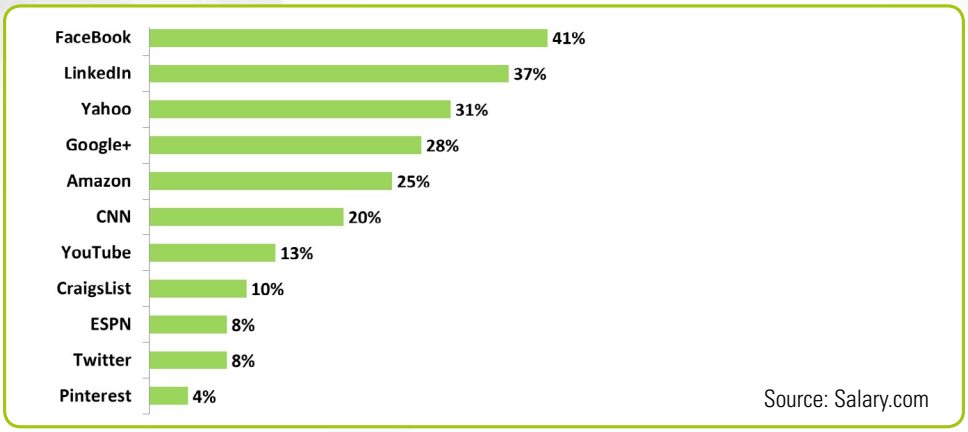

Figure 2: Most popular time-wasting websites.

And business managers can apply controls selectively, so people are not prevented from doing their jobs. For example, they could:

- Allow marketing employees to access Facebook and Twitter to communicate with customers, but prevent others from wasting time on those sites.
- Allow the legal staff to research controversial topics, while blocking access to other employees.
- Block YouTube and streaming video sites, except for employees that have a legitimate need for instructional videos.
- Allow employees to access shopping and online game sites only outside of business hours.
- Limit access to job sites to HR personnel. (In the survey cited above, 46% of respondents said they have spent time job hunting during work hours.)

Business unit managers can thus improve productivity by applying acceptable-use policies in ways that reduce web surfing without interfering with legitimate business activities.

Managing the Workplace for the Human Resources and Legal Departments

Content filtering can be an important tool for the HR and legal departments.

HR, for example, must ensure that no employee is subject to an intimidating, hostile or offensive work environment in the form of unwelcome comments or conduct based on sex, race and other legally protected characteristics. This can include "sending, forwarding or soliciting sexually

[2] Salary.com Wasting Time at Work 2012 survey: http://business.salary.com/why-how-your-employees-are-wasting-time-at-work/

suggestive letters, notes, emails, or images."[3] Preventing employees from accessing web sites related to pornography, weapons and hate speech can help keep some types of inflammatory materials out of the workplace.

The HR department may also be responsible for managing a social media policy that provides guidelines on how employees should and should not post information and express opinions on social media sites, blogs and community web sites and forums. Content filtering and application controls can help enforce these policies.

> *"IT now provides a service to HR that enforces corporate web usage policies via web-site category blocking. From a corporate risk perspective, there are just certain types of web sites we do not want people visiting…These days, there is so much risk involved from an HR and legal perspective that web filtering must be part of your basic tool kit."*
>
> Bruce Godfrey, IT infrastructure manager, Cascade Microtech

In addition, the legal staff may need to address issues like employees downloading copyrighted materials. Preventing workers from using peer-to-peer networking sites to download copyrighted music and videos could help avoid lawsuits.

Verifying Compliance for Compliance Officers and Auditors

Compliance officers and auditors have the unenviable task of verifying compliance with government and industry regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley, PCI DSS, HIPAA, HITECH and various European Union data protection directives.

Secure web gateways can simplify this task by:

- Showing that Internet acceptable-use policies are in place and being enforced.
- Providing security measures mandated by some of the regulations.

For example, SQL injection and cross-site scripting attacks are referenced in the OWASP Top 10 application security risks and in security requirements and guidelines from the Cloud Security Alliance, the Defense Information Systems Agency, the European Network and Information Security Agency, the Federal Financial Institutions Examination Council, the National Institute of Standards and Technology, and the Payment Card Industry Security Standards Council. Some secure web gateways can scan web traffic and detect these two types of attack.

Content filtering is most explicitly required by the Children's Internet Protection Act, which requires that public schools and libraries use content filtering technology as a condition of receiving federal E-Rate funding. A school or library requesting federal funds for Internet access must certify that it is using technology to block child pornography and other material deemed to be obscene or "harmful to minors."

Reducing Costs for CIOs and IT Managers

CIOs and IT managers not only have a responsibility to improve security, but they also have a strong interest in reducing IT costs.

[3] See, for example, the Federal Communications Commission web site, Understanding Workplace Harassment: http://www.fcc.gov/encyclopedia/understanding-workplace-harassment-fcc-staff

Secure web gateways can reduce network and storage costs by limiting streaming media, very large file downloads and spam. In most organizations, these are among the top bandwidth and storage hogs.

Secure web gateways can also reduce support costs by blocking malware, so that fewer computers need to be cleaned or reimaged.

Finally, secure web gateways can reduce the cost of data breaches by blocking attacks that use spam, spear phishing and "drive-by" downloads. Many advanced persistent threats use these methods to gain a foothold in corporate networks.

> *"The impact on our productivity [of deploying a secure web gateway] has been unbelievable! That was the whole reason behind [the deployment] — so it would free up our time to work on other projects. We have not had one infection since deployment."*
>
> Eric Leiss, support systems administrator, University of Missouri

Educating Employees on Acceptable Use of the Internet

Employee acceptance of security measures and acceptable-use policies is a key success factor for IT security. Employees who feel they have been treated unfairly or in an arbitrary way will try to evade security policies, potentially by transferring confidential information to unprotected personal systems.

A secure web gateway can not only enforce acceptable-use policies, but it can also improve employee acceptance by:

- Educating employees on why controls and policies are in place — for example, by displaying an information screen when blocking access to web sites (Figure 3).
- Enforcing policies in an appropriate manner — for example, by blocking games, shopping sites and YouTube during the workday but allowing them after work hours.

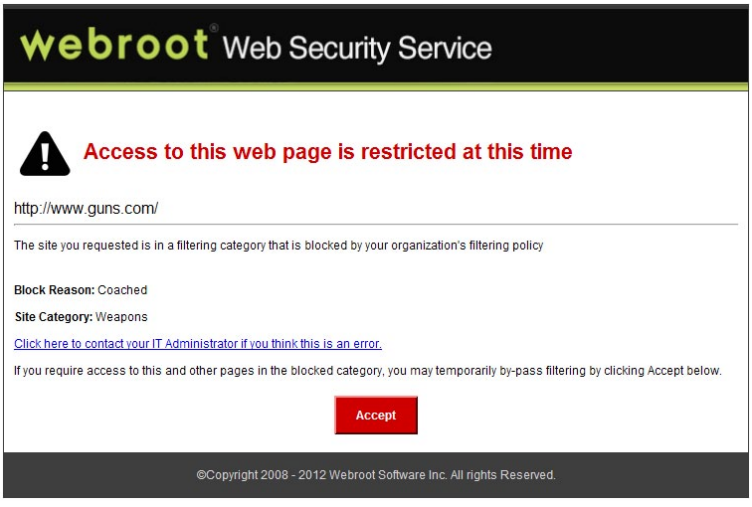

Figure 3: Warning messages educate users on why web sites are blocked.

A secure web gateway can also give the IT security and operations groups tools to identify those who violate policies and abuse legitimate resources (Figure 4).

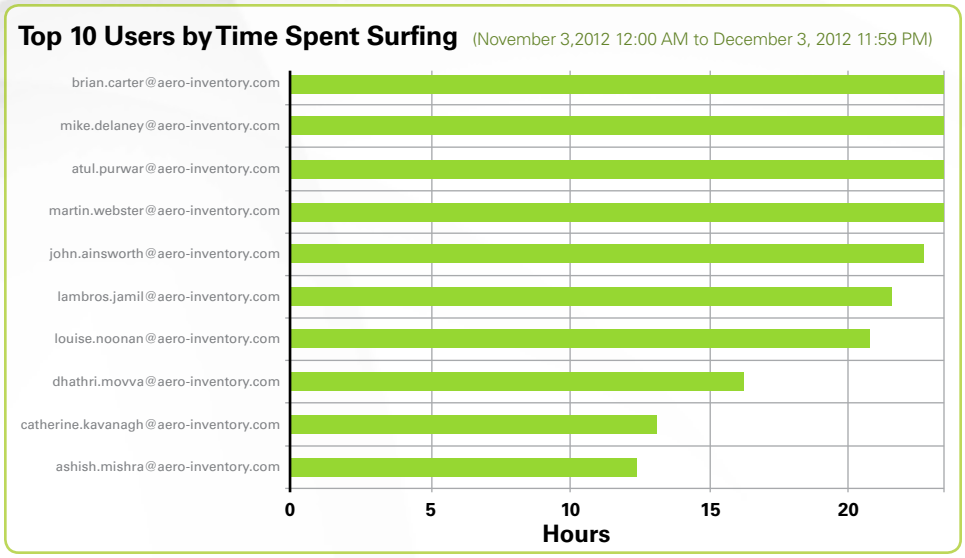

Figure 4: Reports can identify the most serious policy violators so they can be educated.

These individuals can be contacted, informed about how they are violating company policies (accessing questionable web sites, watching streaming video during working hours), and educated about the consequences to the company (increasing the risk of malware infections, slowing down the network for other employees).

These capabilities improve security as well as employee goodwill, while giving IT and compliance staff tools to fine-tune policies and their application.

Why the Webroot Web Security Service Is the Most Effective Cloud-based Secure Web Gateway

The Webroot Web Security Service has a number of characteristics that make it the most effective cloud-based secure web gateway available.

Comprehensive threat prevention

The Webroot Web Security Service scans HTTP and FTP over HTTP traffic to block viruses, worms, Trojans and other types of malware. It takes advantage of the Webroot Intelligence Network, a cloud-based resource that identifies threats based on over 75TB of threat data from a full-time staff of analysts, independent test laboratories, malware clearinghouses, and over 25,000 business partners and enterprise customers (See Figure 5 on the following page).

The service also identifies many types of zero-day attacks using behavioral analysis and heuristic methods that protect against JavaScript, shellcode, cross-site scripting and phishing.

The service includes a service-level agreement **that guarantees 100% protection against known viruses and spyware.**

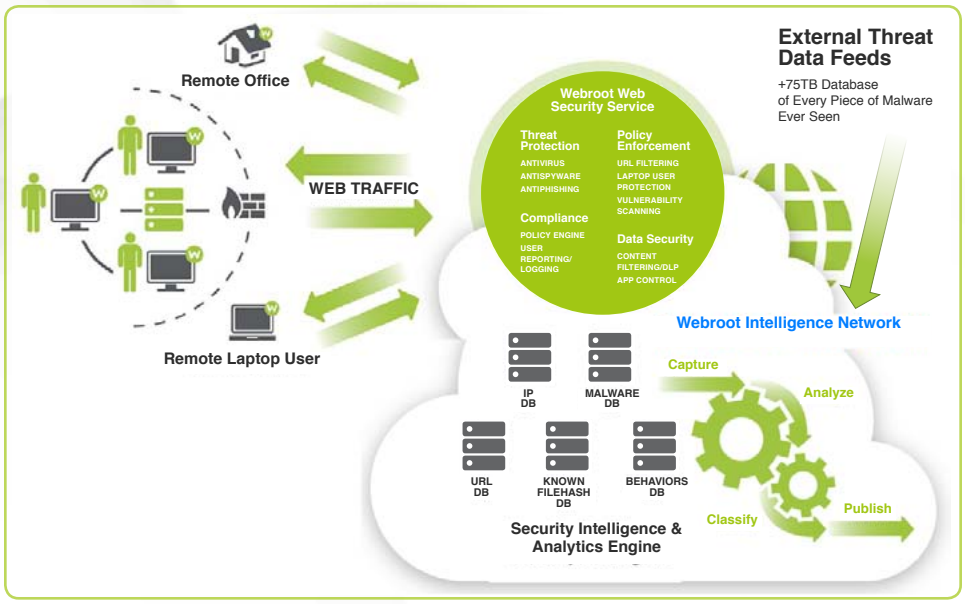

Figure 5: The Webroot Web Security Service takes advantage of the Webroot Intelligence Network.

The most comprehensive and accurate web filtering database

The Webroot Web Security Service enforces Internet acceptable-use policies using the world's largest database of classified web pages: over 300 million web sites divided into over 80 categories. New web sites are classified quickly with sophisticated web-site reputation scoring techniques, supplemented by the work of a global, multilingual web analyst team.

Granular quotas and activity controls

The Webroot Web Security Service lets administrators place limits on bandwidth consumption and time spent online for departments and individuals.

Administrators can also set Internet access policies for groups and individuals and apply access rules by time and location.

Access to individual web sites can be set to "Allowed," "Blocked" and "Coached." Users can access web sites with the Coached setting, but only after reading a warning message informing them that their site visit will be logged so that it can be analyzed later by IT security or operations personnel.

Aggregate and detailed reporting

The Webroot Web Security Service provides dashboard-type charts so managers can view key measures at a glance. Graphs and reports show key data in both aggregate and individual levels. These include graphs and reports showing web traffic trends, top blocked URLs, top users surfing, blocked malware and bandwidth usage.

Roaming and mobile user protection

Roaming users can be authenticated directly with the Webroot Web Security Service, so they are protected as soon as they connect to the Internet, without needing a VPN connection to the company.

Cloud-based service

The Webroot Web Security Service is cloud-based, so it offers all of the benefits of software as a service: lower cost of ownership, rapid implementation, scalability and less work for the IT operations staff.

The service also takes advantage of high-end servers that can analyze millions of threat signatures and URLs in fractions of a second.

Unique Global Server Load Balancing technology routes users' web traffic to the nearest of several data centers around the world, ensuring rapid response times. And there is no single point of failure, as there could be with an on-premises secure web gateway.

Industry-leading SLAs

The Webroot Web Security Service offers outstanding service-level agreements (Figure 6).

Service-Level Agreements
Service-Level Availability: 99.99% uptime
Virus Detection Rate: 100% of known viruses
Spyware Detection Rate: 100% of known spyware variants

Figure 6: Webroot Web Security Service SLAs

Conclusion

Secure web gateways address many key issues above and beyond security. These include:

- Productivity
- Enforcing labor laws and company policies
- Regulatory compliance
- Cost reduction
- Employee acceptance of security policies and goodwill toward IT

IT security staff should therefore have a lot of allies in implementing or improving these solutions, including business unit management, HR and legal, compliance officers and top IT management.

The Webroot Web Security Service was designed to provide benefits to all of these groups, while winning the acceptance of employees.

Find more information on the Webroot Web Security Service at http://www.webroot.com/En_US/business/.

Or apply for a no-obligation 14-day FREE trial at http://www.webroot.com/En_US/business/land/security-risk.html.