Putting Web Threat Protection and Content Filtering in the Cloud

Why secure web gateways belong in the cloud and not on appliances

Contents

The Cloud Can Lower Costs — Can It Improve Security Too? .......................... 1
The Standard Case for Cloud Adoption ......................................................... 2
Reasons for Putting Secure Web Gateways in the Cloud ............................. 3
The Webroot® Web Security Service .............................................................. 5
Conclusion ..................................................................................................... 7

The Cloud Can Lower Costs — Can It Improve Security Too?

Should IT managers deploy secure web gateways as software or appliances on-premises?
Or should they utilize a cloud-based service?

You probably know the standard reasons in favor of cloud-based solutions, like fast implementation, lower costs, less administration and rapid scalability.

But there are additional reasons to put web threat protection and content filtering in the cloud, factors that produce better security. These include better defense against zero-day attacks, more protection of roaming users and high reliability backed by extremely strong service-level agreements.

In this paper, we will look at:

- Factors favoring cloud and SaaS solutions in general.
- Reasons why secure web gateways in the cloud can provide better security than appliances and local servers.
- How the Webroot® Web Security Service can maximize security and minimize costs using a cloud-based architecture.
The Standard Case for Cloud Adoption

By now everyone knows that software-as-a-service (SaaS) and cloud-based solutions are rapidly being adopted by all types of companies, and most people agree on the reasons for that.

A recent Microsoft-sponsored survey of small and midsize businesses in 13 countries found that 60% of those with 101 to 250 employees have implemented cloud-based services. Among those companies with 51 to 250 employees already using cloud-based applications, top drivers were “we will save money” (54%), “we will be more productive” (54%), “we will be more flexible” (43%) and “we will be more innovative” (35%).

Research firm Gartner estimates that SaaS revenue worldwide will reach $14.5 billion in 2012 and $22.1 billion in 2015. Figure 1 shows the primary reasons for adopting SaaS solutions. They include lower total cost of ownership (TCO), faster deployment, support for remote users, lower capital expenses, higher user acceptance and lack of IT resources to implement on-premises solutions.

---


Reasons for Putting Secure Web Gateways in the Cloud

Most IT managers agree on a well-known list of advantages of moving applications and services into the cloud. But for security solutions like secure web gateways, there are even more reasons for doing so.

An overview of secure web gateways is provided in the box on this page.

And here we discuss why it makes so much sense to deploy secure web gateways in the cloud, rather than on local servers and appliances.

**a. Better defense against zero-day threats and spam servers**

Speed is one of the key weapons of hackers and cybercriminals. They race to disseminate new and unknown zero-day attacks before threat signatures can be developed and deployed.

Similarly, hackers and spammers move infected web sites and spam distribution servers to new domains to try to stay ahead of blacklists.

When secure web gateways are deployed on local servers and appliances, new malware signature files and blacklists need to be distributed and applied on each system. Until the updates are complete, users are vulnerable to the new attacks.

**Cloud-based secure web gateways**, in contrast, start using malware signatures and blocked URL lists as soon as they are available.

In addition, some cloud-based systems can reclassify web sites on the fly if malware is detected, so everyone using the service is immediately protected from those sites.

**b. More comprehensive signature and URL databases**

On-premises systems are necessarily limited by their processing and storage capacity. Vendors are forced to limit the size of signature and URL databases deployed locally.

What Is a Secure Web Gateway?

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

A secure web gateway typically includes technologies like:

- **Threat protection** – Scans HTTP and FTP over HTTP traffic to block malware and spyware before it reaches the company network.

- **URL and web content filtering** – Monitors web page requests and prevents users from reaching web sites likely to contain malware or violate company policies.

- **Quota policy support** – Applies limits to individuals on time spent online and bandwidth consumption to increase productivity and protect network performance.
Cloud-based secure web gateways can maintain databases of millions of threat signatures and hundreds of millions of URLs. Threat protection is more comprehensive, and network performance is not impacted by downloads of thousands of new signatures every day.³

c. Better performance
IT managers face a trade-off between performance and hardware cost with on-premises systems. Underpowered servers and appliances can slow down the network, which hurts productivity and annoys employees. But it is very costly to purchase systems scaled to handle peak network traffic.

Cloud-based secure web gateways can utilize the fastest and most advanced hardware systems, so even the most processor-intensive signature matching and URL categorization can be performed without impacting response times for employees.

d. Support for remote and roaming employees
Distributed work is becoming the norm: Employees work at home, on the road and in small distributed offices. Companies are also giving contractors, outsourcing firms and business partners access to their networks.

But premises-based systems are at a severe disadvantage in highly distributed environments. Companies must either put systems in every location, which is extremely expensive, or force users to communicate with servers or appliances at distant locations, which affects productivity.

Also, many secure network gateways provide no protection for remote users who communicate directly with the Internet. They protect roaming users only if the user creates a VPN connection to the company network.

Cloud-based secure web gateways can provide much better protection and performance for remote and roaming employees:

- There are no hardware and software costs for supporting new locations.
- If the service provider has servers and high-capacity network connections around the globe, then remote employees enjoy excellent response times.
- Roaming users can be protected the moment they connect to the Internet, without needing to establish a VPN connection to the company network.
- Companies can reduce the risks of working with contractors, outsourcers and business partners by limiting their access to selected IP addresses and systems.

e. Fault tolerance
Premises-based systems typically include a single point of failure. A problem with one server or appliance can knock an entire office off the Internet or deprive it of web security — unless, of course, the IT department wants to pay for redundant fail-over systems at every location.

Cloud-based secure web gateways are usually configured so that if a system fails, or even an entire data center goes offline, users can be switched over to another data center on the fly.

³ The AV-TEST Institute registers over 75,000 new malicious programs every day and estimates that over 90 million malware variants exist: [http://www.av-test.org/en/statistics/malware/](http://www.av-test.org/en/statistics/malware/)
f. Service-level agreements

Cloud-based secure web gateways are often able to offer outstanding service-level agreements (SLAs), because of their high-performance equipment and fault tolerance. This takes the burden of stringent uptime requirements off the shoulders of the IT operations group.

The Webroot® Web Security Service

The Webroot Web Security Service provides all of the advantages of a sophisticated cloud-based secure web gateway.

Like most SaaS and cloud-based solutions, the Webroot Web Security Service offers lower cost of ownership, rapid implementation, scalability and reduced administration for the IT operations staff.

It also provides the other advantages we have been discussing, like better security, better performance, better support for roaming employees and higher reliability.

The Webroot Web Security Service takes advantage of the Webroot Intelligence Network (See Figure 2 on following page), a cloud-based resource that gives users immediate access to:

- Over 75 terabytes of threat data, updated every five minutes with input from a full-time staff of analysts, independent test laboratories, malware clearinghouses, and more than 25,000 business partners and enterprise customers.
- The world’s largest database of classified web pages: over 280 million URLs divided into 80 content categories.
- An advanced threat processing system that has categorized more than 125 million executables, including their behavioral characteristics.

Malware detection is based not only on signature matching, but also on advanced heuristics and behavior recognition.

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

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

“Cost was definitely one of the deciding factors, but it wasn’t the only reason we chose Webroot. Cloud security is also great because it protects all of the employees regardless of where they are.”

Jerome Jasmin, Toshiba France
Unique Global Server Load Balancing technology routes users’ web traffic to the nearest of several data centers around the world, ensuring rapid response times. Performance can be enhanced even further with on-the-fly web page compression and an option to strip advertisements off web pages and reformat the pages with no blank spaces.

Redundant, fault-tolerant data centers improve reliability and allow Webroot to offer outstanding SLAs (see Figure 3).

**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 2: The Webroot Web Security Service takes advantage of the Webroot Intelligence Network.

Figure 3: Webroot Web Security Service SLAs
Conclusion

Most organizations are turning to Cloud offerings over other solutions to speed up implementation and reduce costs.

For secure web gateways, a cloud-based implementation also offers:

• Better protection against zero-day threats and targeted attacks.
• Larger threat and URL databases for better security.
• High levels of redundancy for more reliable operations.

For most companies, these benefits make an overwhelming case for implementing a cloud-based secure web gateway over on-premises servers or appliances.

For more information, please visit:

For a free trial of the Webroot Secure Web Service, go to: