Network Computing For IT By IT

Web Security Services Put to the Test

Posted by Randy George on December 3, 2010

The Web is a dangerous place. Web-based malware can cripple a PC in seconds and take hours to remove--if it can be removed at all. Enterprises have turned to on-premises products, both gateway-based and client-based, to filter inbound malware and stop users from surfing to compromised or outright malicious sites. Now enterprises have another option: A growing number of providers offers Web security as a service. These software as a service (SaaS) offerings promise protection similar to what you'd get with an on-premises product, but without the capital outlay or ongoing operational costs. We tested Web security services from Barracuda, McAfee, Symantec, Webroot and Zscaler.

You can find the full report, complete with a detailed analysis of each service reviewed, here. Generally speaking, SaaS-based Web security works like this: Proxy your outbound Internet traffic through the closest point of presence that your Web security vendor provides, and the provider skims out the malware mixed in with legitimate Web traffic.

As we prepared to launch this review, we were skeptical about the whole concept of Web security in the cloud. The idea of routing your outbound Web traffic through a third-party proxy seemed like mayonnaise on a hamburger: just not appealing. We can now say that after completing this review, we'll eat that mayo burger.

But that doesn't mean we're giving up ketchup. The fact is, premises-based Web malware products from the likes of Bluecoat, Finjan, Websense, McAfee and others are still our first choice for protecting users in corporate offices. They have proven themselves to be scalable, reliable and effective. We can't yet say the same for SaaS Web security products--the market is simply too immature. We need more assurance that these services will scale sufficiently before we're ready to recommend wholesale adoption.

However, there's never been an efficient way to extend on-premises protection to remote users. Bluecoat and others offer half-hearted products via proxy clients, but routing traffic from an employee on the West Coast to a Web gateway filter on the East Coast isn't efficient. This is where a Web security service can make a difference. We think that at present, midsize and large enterprises that need to protect road warriors and small branch and remote offices should consider supplementing an on-premises product with a SaaS-based offering. A service is easy to deploy, particularly for a subset of your entire employee base, and has low capital and operational costs. In addition, user groups will get a similar level of protection as with an on-premises product.

Without fail, everyone we speak with about Web security in the cloud asks about the overhead added to the browsing experience, so latency testing was a key element of our reviews. As we report our latency findings, keep these points in mind: First, many factors go into the latency equation, so your mileage may vary from ours. Second, each provider's cloud may have served us content out of cache, potentially making one provider's latency better than another's. In addition, cloud providers have different geographical points of presence; those with sites closer to our Boston-based lab had an advantage. Third, latency measurements should not be used to "rate" one vendor over another, but rather should be used to broadly illustrate the impact of routing traffic through any provider's service.

The key takeaway for us in the labs is that the average user will probably never know that he or she is using a third party for Web security. We generally found that most sites added only 0.1 or 0.2 seconds of latency. For sites that had many objects to fetch, we saw a few extra seconds of latency, but that was at the absolute highest end of the spectrum.

The accuracy of each provider's URL and malware filter was another key component of our testing. There were no curveballs in this section of the testing: The goal was to simply see how well each vendor appropriately categorized and blocked our attempts to access a set of well known spyware/malware domains.

We randomly selected 10 URLs from a huge database of known malware domains maintained from malwaredomains.com, and we ran each vendor through the testing simultaneously. Because of the random nature of our domain selection, it's fair to argue that our results may not tell the entire story in terms of just how accurately each vendor can filter malware. For the most part, we were extremely pleased with how well each malware filter worked. With so many sites compromised on the global Internet, it's impossible to expect any URL filter to stop each and every potential threat. However, if nine out of 10 sites that are known to host malware can be filtered right from the get-go, IT managers have a tiered security capability when the service is combined with endpoint antivirus and malware protection.

We also set out to see how well each vendor implemented Web security above and beyond simple URL filtering. We stuffed the eicar test virus, which antivirus vendors support for testing signature-based detection systems, into an encrypted zip file, a self extracting zip, and a zip file that was recursively zipped multiple times. All the providers in our roundup were able to detect the virus stuffed inside the self-extracting and recursively zipped file.

We were initially able to slip the encrypted zip file past everyone. However, Barracuda, Zscaler, and Webroot have administrative controls that can be configured to disallow password-protected and encrypted zip files. Symantec did not natively provide this functionality, and McAfee had no administratively configurable attachment policy at all.

Next, we tried to slip a booby-trapped PDF through each provider's security scanners. Our infected PDF contained active code that could be used to install a downloader for distributing malware to infected clients. Every vendor detected and filtered the exploit. We also threw a booby-trapped JPG and SWF file at each provider, with the same results. While not every service was extremely configurable from a management perspective, all of the providers performed well at the core function of detecting nefarious attachments and filtering them in the cloud.

For other attacks, we felt Zscaler had the most robust security capability. For example, Zscaler was the only provider that was able to prevent cookie theft via cross-site scripting attacks. Zscaler accomplished this by applying a watermark to each cookie dropped onto the computer. If those cookie contents were acessed by a third-party site, the Zscaler cloud assumed a cookie theft was underway and blocked the transaction. Zscaler can also enforce policy at the cloud level against other XSS attacks. The Zscaler service offers application, P2P, and file control features, bringing the most impressive array of security features to the cloud.

The SaaS Web security providers offered good out-of-the-box reporting capabilities. In fact, there are some big name on-premises appliances that can learn a lesson from how the cloud vendors are doing it. Most of the vendors in our lineup have very useful dashboards that quickly displayed a range of pertinent information. You can get snapshots of top URLs, bandwidth consumed by user and spyware/virus activity from all the players in our roundup. On the whole, Barracuda and Zscaler offered the most robust and elegant reporting engines in the group. Both services offer a good selection of pre-canned reports, and you can drill down for more detailed usage. All of the vendors, except for McAfee, offered the ability to download PDF-based reports, as well as the ability to schedule the creation of new reports for quick access when needed.

In terms of value-added features, Zscaler includes basic data loss prevention functions as part of its core offering. Customers can turn on dictionaries and enforce DLP policies for the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) Data Security Standard and others through the management interface. Zscaler can also apply those DLP policies to attachments and instant messages, so long as the transaction traverses the Zscaler proxy.

Webroot impressed us with its ability to execute proactive vulnerability scans against any system protected by its cloud. The vulnerability assessment results were linked to explanations of each vulnerability, along with remediation instructions.

Compared with the cost of on-premises protection, cloud-based Web security is a relatively reasonable proposition. And, if cash is tight, the Web services model may be a much more appealing option for smaller organizations. Prices are relatively similar across the board, ranging from $1.50 to $5.00 per user per month.

If you're not ready to do Web Security in the cloud, you're not alone. But based on our experience in the labs, the protection technology is robust. Organizations with no on-premises Web security should consider adopting a provider. The sell will be tougher for organizations with significant investments in on-premises equipment. As mentioned before, we see remote access and protection of small branch/home offices as the best use of these services for midsize and large organizations that already have Web security gateways in place at the main office. Meanwhile, as the market and the providers mature, we expect Web security services to grow into a viable option across the board.

Copyright 2009 United Business Media LLC, All rights reserved.