

# Protects web applications in both directions

Years ago I was at a trade show and in a back corner of the show floor there was a vendor offering an early try at a web application firewall. The sign said something to the effect that one could prevent hackers from attacking your website if you bought this product. My immediate reaction was, 'how would one do this? Go on a hacker hunt and kill them all?' Since that is impractical (although I am sure many of us have considered it), uncivilized and illegal, it would seem that accomplishing what this product wanted to do would be pretty much out of the question.

But, that was then and this is now.

WebDefend actually manages this seemingly unlikely feat by keeping the hackers away from target web applications through cooperation with other defensive tools on the enterprise. But wait, as the late night infomercials say, there's more. Not only can WebDefend report and block attacks, it can point out flaws in web application design and implementation, filter bad behavior by insiders, augment vulnerability assessment results, enforce compliance with new payment card industry (PCI) standards, and output a wide variety of reports that actually are useful. Truly, we found that this product is a one-stop-shop for managing web application security in the production environment.

## Key to success

The key to WebDefend's success is twofold. First it is not inline. That means that although it sees everything, it presents no latency threat. The second key is that it is a well-thought-out, two-way analysis tool consisting of several analysis engines that communicate with both the web applications and the protection devices, such as firewalls on the enterprise. This cooperation allows the device to tell a firewall to sever a connection before damage to the web application or exfiltration of PCI-regulated data can occur.

There are two ways to use WebDefend. One is with and the other is without the web server agents. We recommend the use of the agents since that provides the maximum protection

and blocking capability. The product is relatively easy to configure given that you understand your enterprise and your web applications and what they are supposed to do. For example, WebDefend can — and should — decrypt SSL if you are using HTTPS. But this means understanding things, such as where certificates reside, and making sure that the device has access to them. The decryption is, of course, transparent and none of the payload content — beyond that needed to detect attacks — ever is revealed. The reason this is so important is that attacks that use SSL are common and usually are missed by firewalls and intrusion detection systems.

I have said several times in the past that the notion of protecting complicated systems often calls for complicated solutions and this is no exception. However, to Breach Security's credit, WebDefend has been given a very good balance of functionality and ease of use. Still, implementing this type of protection never is for the fainthearted. Know your infrastructure, know your web applications, and know your security architecture and you'll be fine. Otherwise you'll be frustrated.

## Unique functions

A number of WebDefend's functions are unique in that they appear in the same product. For example, because it is able to see all traffic to and from the enterprise, it can see indications of poor web application design, attempts to steal or exfiltrate credit card information, as well as weaknesses that vulnerability scanners may miss.

This is a product that is most effective when used with all of the other security tools that protect the enterprise both proactively and reactively. I have yet to see an appliance of this type that integrates so nicely with the rest of the enterprise's security infrastructure.

You manage the appliance from a remote console and the management interface is clean and comprehensive. Configuration of policies and policy elements is done from the console and is quite straightforward. We had no trouble setting up policies, but in the end, we

## AT A GLANCE



**Product:** WebDefend v. 3.0

**Company:** Breach Security, Inc.

[www.breach.com/products/webdefend.html](http://www.breach.com/products/webdefend.html)

**Availability:** Now

**Price:** Price starts at \$44,995, including 12-month hardware warranty.

**What it does:** Full-featured web application firewall and general security appliance.

**What we liked:** Comprehensive suite of web application protection functions.

**What we didn't like:** Nothing we didn't like, but as with any sophisticated security product, a serious understanding of the network/web application architecture is a must. This is not an indictment, however. Rather it is a caveat. As we've said many times, complicated problems often require complicated solutions.

opted for the defaults. Of course, WebDefend can be used in a distributed arrangement where multiple sensors communicate and correlate events and data.

WebDefend is priced very reasonably at just under \$45,000 and has a full suite of support offerings at extra cost. Documentation is complete and comes on an included CD. The website is replete with resources, including podcasts, white papers and other tools.

Overall, WebDefend is at the top of all of the application firewalls I've seen to date and is well ahead of most. If you are using active web content, such as online banking applications, you cannot afford to be without this product.

— Peter Stephenson

**SC**  
MAGAZINE  
Reprints

  
**BREACH**<sup>™</sup>

**Breach Security, Inc.**

2075 Las Palmas Drive, Carlsbad, CA 92011

[www.breach.com](http://www.breach.com) • [sales@breach.com](mailto:sales@breach.com)

760-268-1924