Quick Wins with Website Protection Services

Version 1.4
Released: July 1, 2013

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Licensed by Akamai Technologies

Akamai® is the leading cloud platform for helping enterprises provide secure, high-performing user experiences on any device, anywhere. At the core of the Company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Copyright

Table of Contents

Are Websites Still the Path of Least Resistance?

In the sad but true files, the security industry has become increasingly focused on advanced malware, state-sponsored attackers, and 0-day attacks — to the exclusion of everything else. A stroll around any security conference floor makes that immediately obvious. Which is curious, because 'advanced' attackers are simply not a factor for the large majority of companies. It is easy to forget that most compromises start with attacks against poorly coded and brittle web sites.

Many high-profile attacks target unsophisticated employees with crafty phishing messages, but we cannot afford to forget that if an attacker can gain presence via a website they will. Why would they burn a good phishing message, 0-day malware, or other sophisticated attack, when they can pop your web server with a simple XSS (cross-site scripting attack) and then systematically run roughshod over your environment to achieve their mission?

We wrote about the challenges of deploying and managing WAF products and services at enterprise scale last year. But we mostly jumped straight to Step 2 without spending any time on simpler and faster approaches to protecting websites. Even today, strange as it sounds, far too many websites have no protection at all. They are built on vulnerable technologies without a thought for securing critical data, and then let loose in a very hostile world. These sites are sitting ducks for script kiddies and organized crime.

Even today, strange as it sounds, far too many websites have no protection at all. They are built on vulnerable technologies without a thought for securing critical data, and then let loose in a very hostile world.

So in this paper we took a step back, to write about protecting websites using Security as a Service (SECaaS) offerings. We will use our Quick Wins framework to focus on how Website Protection Services can protect web properties quickly and without fuss. Of course it's completely valid to deploy and manage your own devices to protect your websites; but Mr. Market tells us every day that the advantages of an always-on, simple-to-deploy, and secure-enough service consistently win out over yet another complex device in the network perimeter.

Website Attack Vectors

The industry has made strides toward a more secure web experience, but it rarely takes reasonably capable attackers long to find holes in any organization's sites. Whether due to poor coding practices, poorly configured or architected technology components, or change control issues, attackers routinely defeat applications without adequate protection. And when strong security protections make it difficult to compromise an application directly, attackers opt to knock down the site using a Denial of Service (DoS) attack. Heads they win, tails you lose. Sound familiar? Let's dig into these attack vectors and why we haven't made much progress addressing them.

> Developers still lack incentives to adopt secure coding practices. They are evaluated on their ability to ship code on time — not necessarily secure code.

SDLC what?

The inability of most developers to understand even simple secure coding requirements continues to plague security professionals, leaving websites unprepared to withstand even simple application attacks. But to be honest that characterization may be unfair — it is more a problem of apathy than ability. Developers still lack incentives to adopt secure coding practices. They are evaluated on their ability to ship code on time — not necessarily *secure* code. For his "A Day in the Life of a CISO" presentation, our analyst Mike Rothman wrote the following about application security:

Urgent. The VP of Dev calls you in.
A shiny new app. Full of epic win.
Customers will love it. Everyone clap.
We launch tomorrow. Snoop and Dre will rap.
It's in the cloud. Using AJAX and Flash.
No time for pen test. What's password hash?

Kind of funny, eh? It would be if it weren't so true. Addressing this requires you to be realistic and accept that you cannot change fundamental developer behavior overnight. So you need a solution to protect websites *without* rebuilding code or requiring developers to change. You need to be able to stop SQL injection and XSS *today* — which is already two days late. Josh Corman explained why when he introduced HD Moore's Law. If your site can be compromised by anyone with an Internet connection and 15 minutes to download and install Metasploit, your days as a security professional will be numbered.

Over the long term the answer is to use a Secure software Development Lifecycle (SDLC) to build all your code securely. We have written extensively about building a Web app security program so we won't rehash the details here. Suffice it to say that without sufficient incentives, a mandate from the top to develop and launch secure code, and a process to ensure it, you are unlikely to make much strategic progress.

Suffice it to say that without sufficient incentives, a mandate from the top to develop and launch secure code, and a process to ensure it, you are unlikely to make much strategic progress.

Brittle infrastructure

It is amazing how many high-profile websites are deployed on unpatched components. Really, it's shocking, even to us — and we know better. We understand the challenge of operational discipline, the issues of managing downtime and maintenance windows, and the complexity of today's interlinked technology stacks. That understanding and $4 will buy you a latte at the local coffee shop. Attackers don't care about your operational challenges, except insofar as they can exploit them. They constantly search for vulnerable versions of technology components, such as Apache, MySQL, Tomcat, Java, and hundreds of other common website components.

Keeping everything patched and up to date is harder than endpoint patching, given the issues around downtime and the sheer variety of components used by web developers. And if you don't do it correctly – especially with open source components – you leave low-hanging fruit for attackers, who can easily weaponize exploits and find vulnerable sites with simple strings in their preferred search engine.

When all else fails, knock it down

We have also seen denial of service attacks become increasingly popular. This only makes sense – an increasing number of businesses depend on their websites for revenue, and knocking over a major revenue source creates *urgency* to stop the attacks. Even more problematic is the increasing popularity of DoS attacks to hide traditional exfiltration during data breaches. They blast your site to keep you occupied while taking critical stuff out the back door.

As we recently described in Defending Against Denial of Service Attacks, there are two types. Network-based volumetric attacks oversubscribe network pipes, knocking the site down when it cannot keep up with the flood of inbound requests. The second type is an application-oriented DoS attack — taking advantage of a configuration error, exploiting underlying technology platform vulnerabilities (such as in Apache), and/or gaming legitimate application functions (including search and shopping carts). Or, more likely, all of the above.

Don’t Forget about Compliance

But what about the ‘C’ word? With all the focus on attacks and security it can be easy to fall into the trap of forgetting about the regulatory overhang in industries with mandated application and website protection capabilities. Compliance may not be front and center in your thinking any more, especially if you are dealing with advanced adversaries, but that doesn’t mean you can afford to forget about it. Or you will get a rude reminder when the assessor shows up and thumps you for not having the documentation they want about your SDLC and WAF. Compliance is not an attack *per se,* but many security folks prefer to spend their time fighting off attackers than going through the misery of audit, and you should keep the compliance benefits of a website protection service in mind.

Compliance may not be front and center in your thinking any more, especially if you are dealing with advanced adversaries, but that doesn’t mean you can afford to forget about it.

Protecting the Website

To protect your websites quickly for a Quick Win you need to make sure your protection covers the common attack vectors. Ensure that any Website Protection Service (WPS) addresses the threats to the application, technology platform, and availability aspects of your site.

Application Defense

As mentioned in our Managing WAF paper, it is not easy to keep a WAF operating effectively because they require frequent patching and rule updates to keep applications working and safe from emerging attacks. You cannot afford to sit back and do nothing, relying on your default WAF rules to protect your applications. Attackers will be happy to take your website as the path of least resistance to a foothold in your environment. A key advantage of front-ending your website with a website protection service (WPS) is a built-in capability we call WAF Lite, which we believe is the minimum acceptable protection for any public-facing website

You cannot afford to sit back and do nothing, relying on your default WAF rules to protect your applications. Attackers will be happy to take your website as the path of least resistance to a foothold in your environment.

WAF Lite is, first and foremost, simple. You don't want to spend a lot of time configuring or tuning its application defense. The key to a Quick Win is minimizing required customization while providing adequate coverage against the most likely attacks. You want it to *just work* and block semi-obvious attacks. Stuff like XSS, SQLi, and the other common attacks that make the OWASP Top 10. Building rules to block these standard attacks is not brain surgery. It's amazing that not everyone has this kind of simple defense. But many organizations don't, so we wrote this paper.

Out one side of our mouths we talk about simplicity. But we also need the ability to customize and tune rules as necessary — which shouldn't be that often. You effectively need two different configuration modes. In basic mode you only want a few simple checkboxes to configure the fundamentals. This simple interface should be designed for unsophisticated administrators and sufficient most of the time. But sometimes, such as when you enlist expert help, you will need an advanced mode — with more flexibility and highly granular control over the WAF.

Now for our disclaimer. Although a WPS can be very effective against technical attacks, none of them can protect against logic errors inside your application. If your application or search engine or shopping cart can be gamed using legitimate application functions, no security service (or dedicated WAF, for that matter) can help you. Parking your sites behind a WPS doesn't mean you don't need QA testing and smart penetration testers trying to expose potential exploits.

Two advantages of a managed service to protect your websites are reduced time to deploy and simpler management. Many things can be said about load balancers and WAFs, but simple is not one of them. A Quick Win requires you to work quickly, and a service enables you to deploy within hours, without significant burn-in or tuning before you can bring your new capabilities online.

A Quick Win requires you to work quickly, and a service enables you to deploy within hours, without significant burn-in or tuning before you can bring your new capabilities online.

Platform Defense

The application layer is the primary target for website attacks because it is the most accessible and often most vulnerable, but that doesn't mean you don't also need to pay attention to attacks on your technology stack. In Defending Against Denial of Service we delved a bit into application DoS attacks targeting the building blocks of your application — such as Apache Killer and Slowloris. WPS can help deal with this class of attacks through rate controls on the requests hitting your site, among other defenses.

Search engines never forget, and there is certainly some data you don't want in the great Googly-Moogly, so it is important to control which pages are available for crawling by search bots. You can configure this using a `robots.txt` file but not every search engine plays nice. Especially search engines designed to find vulnerable websites. Some bots jump right to the disallowed sections — that's where the good stuff is, right? Being able to block automated requests and other search bots via the WPS can keep private pages out of search engines. Security by obscurity is not a long term strategy but it can be effective in the short term, and why make things easy for attackers?

You will also want to restrict access to unauthorized areas of your site — not just from search engines. This might include your website control panel, sensitive non-public pages, or the staging environment where you test feature upgrades and new designs. Unauthorized pages could also be back doors left by attackers back into your environment. You should also be able to block nuisance traffic such as comment spammers and email harvesters. These folks don't cause much direct damage but they are a pain in the rear — if you can get rid of them without any incremental effort it's all good.

To be clear, the above security controls on your website are generally also available within the base website and/or application configuration. But you might not have done that, the technology stack

may make good security difficult to achieve directly, or you may lack the expertise to take full advantage of the built-in tools. WPS often provides an easier and more thorough way to lock down the site.

A WPS can restrict not only where visitors go but also where they can come from. For sensitive pages you may want a rule which prevents access except from the corporate network (either directly or virtually via VPN). The WPS then blocks access unless the originating IP is on the authorized list. Like other controls this can be spoofed or gamed, but it is a good way to reduce your attack surface and layer on another level of defense.

Availability Defense

We cannot afford to forget the importance of keeping the site up and serving requests, and a WPS can help in a number of ways. First, WPS providers have bigger pipes than you. Generally *much* bigger, which enables them to absorbs Distributed DoS (DDoS) attacks without disruption. But you need to be wary of bandwidth-based pricing — a volumetric attack won't just hammer your site, but can also hammer your wallet. Successful WPS providers have enough customers that at least one is always under DDoS, so they spend a bunch of money on anti-DoS equipment and extra bandwidth — so you don't have to.

You need to be wary of bandwidth-based pricing — a volumetric attack won't just hammer your site, but can also hammer your wallet.

Another benefit of a WPS fronting your site is that it can obscure your IP addresses. This prevents attackers from bypassing your WAF or other proxy. The WPS provider gives you a list of their IPs, and you restrict inbound traffic to only those addresses in your inbound firewall. This keeps random folks from connecting directly to your site. Similarly, the WPS can be configured as a cloud-based firewall of sorts, blocking protocols such as `ssh`, `FTP` and `telnet` — which should only be used by internal people (and locked down to your internal network, as described above) in limited situations. Obviously this isn't a primary value of a WPS, but useful for cleaning up the traffic into your site.

In all these ways, a WPS can substantially reduce the attack surface of your websites.

Deployment and Ongoing Management

Few projects have more potential downside than ensuring the security of your websites. Your public website is highly visible — to all your customers, to all your employees, and to everybody on the Internet. Your site likely captures private information so its integrity is particularly important. Finally, your organization spends a ton of money to get the latest and greatest functionality on its website, and they don't take kindly to being told their shiny objects aren't supported by security. All this adds up to a tightrope act to protect the website while maintaining expected performance, availability, and functionality. Navigating tradeoffs like these is an essential aspect of the security role.

Planning the Deployment

Start by setting up your website protection service. If you are just dealing with a handful of sites, and your requirements are straightforward, you can probably do this yourself. In that case you don't have much pricing leverage so you won't get much attention from a dedicated account team. On the other hand, if you have enterprise-class requirements (and budget), you have probably already been through the sales fandango with the vendor. This involves a proof of concept, milking their technical sales resources to help set things up, and then playing one WPS provider against another for the best price.

Before you are ready to move your site over (even in test mode) you have some decisions to make. You need to define which sites need to be protected. Ideally your WPS will shield them all but we live in an imperfect world. You also may not know the full extent of your website properties. Finding sites you don't know about shouldn't be a surprise — it wouldn't be the first time a business user did something without going through the proper IT and security authorizations.

The sales fandango with the vendor involves a proof of concept, milking their technical sales resources to help set things up, and then playing one WPS provider against another for the best price.

With your list of high-priority sites which must be protected in hand, you need to understand which pages and areas are okay for the public and search spiders to see, and which are not. It is quite possible that everything is fair game for everybody, but you cannot afford to *assume* this.

Speaking of search engines and other automated crawlers, you need to figure out how to handle those inhuman visitors. A key WPS feature mentioned earlier is control over which bots are allowed to visit and which are blocked. We also talked about restricting inbound network traffic to the WPS, to prevent attackers from connecting directly to your site. To take advantage of these protections you will need to work with your network security team. These are the kinds of decisions you need to make *before* you start routing traffic to the WPS.

One level of abstraction above bots and IP addresses is users and identities. Do you want to restrict visitors by geography, user agent (don't allow IE6 to connect, perhaps), or anything else? WPS services use big data analytics engines (which they just *love* to tell you about) to learn about IP addresses and speculate on the intent of visitors. Using that information you can block suspicious users from connecting — like *Minority Report* for your website. That's all well and good, we learned during the early IPS days that blocking major customers is always embarrassing (and often career limiting) for the security team.

As with any cloud-based service, unauthorized access to the management console is game over. So it is critical to make sure authorizations and entitlements are properly defined and enforced.

Remember, we are still in the planning phase. Once we get to testing you will be able to fully understand the impact of these decisions on your website.

Finally, you need to determine which of your administrators will have access to the WPS console and be able to configure the service. As with any cloud-based service, unauthorized access to the management console is game over. So it is critical to make sure authorizations and entitlements are properly defined and enforced. Another management question is who gets WPS alerts in case of downtime or attacks. It is essential that you define the hand-offs and accountabilities between your security team and the WPS provider *before* you shift traffic.

Test (or Suffer the Consequences)

Now that you have planned your deployment you need to work through a testing process to figure out what will break when you go live. Many WPS services claim you can be up and running in less than an hour, and that is true. But getting a site *up* is not at all the same as getting it running perfectly. We always recommend testing to understand the impact of front-ending your website with a WPS. You may decide any issues are more than outweighed by the security capabilities of the WPS — especially if your current website security defenses are trivial or nonexistent — or not. But you must be able to have an informed discussion with senior management about any trade-offs before you flip the switch.

How can you test these services? Optimally you connect it to an existing staging site where you routinely test functionality before it goes live, so you can run a full battery of QA tests through the WPS. You probably also need to figure out, with the network team, exactly how you will shift traffic over, and how you will switch back if that ever becomes necessary — another one of those things better to have sorted out *before* you're in the middle of a crisis. You may also use DNS *hocus pocus* to route only testing traffic through the WPS, while the public still connects directly to your site. The testing mechanics depend on your internal web architecture but the WPS provider should be able to help you map out a testing plan.

Then it's time to configure the WAF rules. A web application scan may be a good starting point, highlighting things to restrict or block entirely in your initial WPS rules. Some WPS have 'learning' capabilities, where they monitor site traffic during a burn-in period and then suggest rules to protect the application. That is a quick way to start, and in a Quick Wins scenario we cannot argue much. But it may not provide adequate security. We favor an incremental approach: start with the most secure WAF settings you can, see what breaks, and tune accordingly.

Obviously you simply cannot afford to impede certain application functions, so you will need to iteratively loosen WAF rules until you reach a point where critical functionality is available, while security is as strong as possible. Deploying a WPS to get a Quick Win means you shouldn't burn too much time tuning and iterating — try to quickly find a ruleset that balances security against functionality in a reasonable way. Over time you can optimize the WAF ruleset and work on the application developers to factor the WPS into their development process, so they can keep security and the WPS in mind as they design new functionality. But that doesn't happen overnight and in the meantime you need to trade off security against functionality.

In case we haven't been clear enough: testing can easily be the difference between a Quick Win and failure.

Keep in mind that many WPS providers include caching within their services to improve website performance. If your site is dynamic in any way caching is likely to break *something*. So tuning doesn't only apply to security rules — you also need to tune caching and performance enhancements. It is great to get a performance boost from WPS but you may need to shut off caching of some areas to maintain functionality.

In case we haven't been clear enough: testing can easily be the difference between a Quick Win and failure.

Abort the Mission

There is a chance that WPS will fundamentally break your site. This doesn't happen often, but in case it does you need a rollback plan. Spend time on non-disruptive testing with the WPS provider *before* you commit. Make sure everything is sorted before you start funneling real traffic through the WPS.

Ongoing Management

For ongoing management you are likely to interact mostly with the WPS reporting functions, which provide a granular view of security and traffic dynamics. Trend reports can show when you are getting traffic spikes and what percentage are automated requests — bots and search engines. They may identify abnormal activity which requires investigation.

Many WPS providers also offer compliance reports providing artifacts to satisfy regulations concerning web application firewalls, network firewalls, and change control. This is critical — especially if you handle protected information. Audits require you to convince the assessor that you are in control by providing detailed reports substantiating a strong security program. Reports from a WPS — you might even walk the assessor through its interface — may help convince the assessor you know what you are doing. A little dog and pony show never hurt anyone.

We should draw a distinction between a WPS and a MSS service. With a WPS, you monitor the UI, set up the reports, and have to interpret and mitigate issues yourself. For those that may want 24/7 monitoring and/or assistance with attack mitigation, you may want to look at a higher level of service as part of a full managed security service (MSS). If you think this alternative could eventually be a requirement given your resources/skill level, you'll want to ensure your WPS provider can offer the MSS capabilities.

As we mentioned earlier, over time your development and testing processes should evolve to take the WPS into account. How you accomplish that depends on how you develop and deploy web applications. If you take a continuous deployment approach you shouldn't have to do anything differently — the WPS will be in-stream and testing should automatically take it into account. But if you use a staging environment and a structured update/upgrade model you will need to test through the WPS before updates go live.

We cannot neglect the ongoing operational functions you *don't* need with a WPS. First, you aren't responsible for maintenance of the WPS platform. Your provider needs to update, patch, and manage all their equipment and software running the service. That's a lot of fun — we're sure you will miss all that work.

The WPS provider also needs a security research capability to look for common web attacks (including the aforementioned OSWASP Top 10) and suggest rule changes to keep the WAF ruleset current. The provider is on the hook for adding bandwidth to keep pace with escalating volume. In this age of increasingly frequent DDoS attacks this is an expensive proposition. All this is handled by the service so you don't need to think about it.

Summary

When searching for any Quick Win your job is to balance security, functionality, and time to deploy. When considering a website protection service you need to focus on application, platform, and availability defenses. Going operational with the WPS should be done in a quick but measured fashion, providing sufficient time for testing the impact of front-ending your sites with the WPS.

As with any managed security service, WPS can offer a quick way to deploy protection without investing in significant infrastructure and hard-to-find application security skills. Of course there are trade-offs in flexibility and control when using any managed service, and every organization needs to balance those trade-offs when making build or buy decisions on key security initiatives.

Overall, we have found that website protection services can quickly add measurable security to your web presence for a reasonable price compared to deploying and managing your own equipment and infrastructure to provide similar capabilities.

Overall, we have found that website protection services can quickly add measurable security to your web presence for a reasonable price compared to deploying and managing your own equipment and infrastructure.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com or ask via the Securosis Nexus (http://nexus.securosis.com/).

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.