eBook

Imperva Cloud WAF

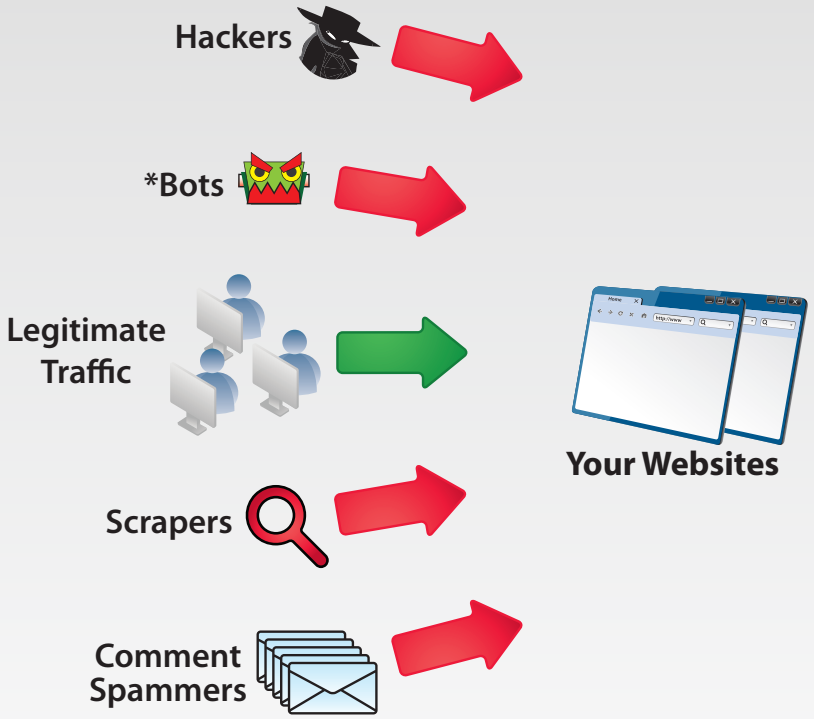
How to Protect Your Website from Hackers

Table of Contents

Web attacks are the greatest threat facing organizations today. In the last year, Web attacks have brought down businesses of all sizes and resulted in massive-scale data breaches. Regulations like the PCI Data Security Standard attempt to reign in these threats by mandating Web application protection.

There's a smart and easy way for businesses to safeguard their Website and achieve compliance.

In this eBook, we look at today's most dangerous Website threats. We also examine PCI DSS compliance requirements. Then, we introduce Imperva Cloud WAF, a managed security service that protects applications from Web attacks, and profile Keystone RV, a company that stopped a devastating DDoS attack with Imperva Cloud WAF.



Website Threats

Web Attacks Are Your Number One Risk

Web application attacks are the most prevalent and devastating threat facing organizations today.

Web attacks are responsible for some of the largest information security breaches in history, including four of the top credit card breaches between 2005 and 2011. At one retailer, hackers used SQL injection to compromise servers and steal 45 million personal information records, costing the organization an estimated $256 million.

Web Attacks Are Increasing

Web attacks are growing in number, with 64% of organizations in a 2011 survey reporting they had suffered a Web attack in the past four weeks.[1] The same survey found that Denial of Service (DoS) and Web application attacks, both of which target Websites, were the two most costly types of cyber crime.

Web Attacks Are Becoming More Advanced

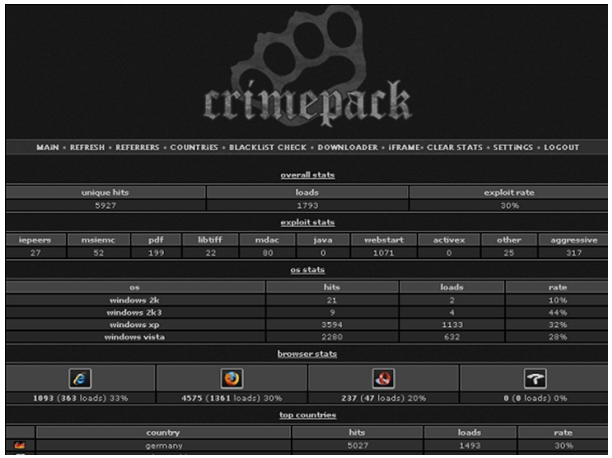
Sophisticated attack techniques have enabled hackers to launch large-scale attacks more quickly. Hackers have also become more organized, pooling resources, and sharing exploits in underground forums.

Automated attack tools use search engines to rapidly discover vulnerabilities and attack thousands of sites. For even greater efficiency, hackers have built networks of bots – remotely controlled computers – to unleash large-scale attacks.

Most Web Applications Have Vulnerabilities

Most Web applications – over 80%[2] – have had serious vulnerabilities. This is due in part to the lack of effort applied to secure coding; most developers are motivated to write code quickly or add advanced new functionality rather than write applications securely.

1 Second Annual Cost of Cyber Crime Study, Ponemon Institute, 2011
2 WhiteHat Website Security Statistic Report," WhiteHat Security, 2011



Example of a Botnet Management Dashboard

Traditional Solutions Don't Stop Web Attacks

Firewalls and Intrusion Prevention Systems (IPSs) prevent network attacks, but they are not designed to stop Web application attacks. They cannot differentiate between bots and human users, so they cannot block business logic attacks like site scraping and comment spam. Since they rely on signatures, hackers can use encoding, comments, and other evasion techniques to circumvent them. Most firewalls and IPSs cannot inspect HTTPS traffic, leaving SSL-enabled sites completely unprotected.

Web Application Firewalls Stop Web Attacks

Web Application Firewalls (WAFs) are purpose-built to protect against Web attacks. WAFs combine several security measures together to offer accurate protection for a myriad of threats, including SQL injection, Cross-site scripting (XSS), CSRF, site scraping, application DDoS attacks, and many more.

Website Threats By the Numbers

230 is the average number of vulnerabilities on a Website[1]

75% of all cyber attacks target Web applications[2]

89% of compromised records are due hacking and external threats[3]

64% of organizations feel that they can't fix Web vulnerabilities quickly[4]

$7.2 Million is the average cost of a data breach[5]

1 "WhiteHat Website Security Statistic Report," WhiteHat Security, 2011
2 Gartner Research
3 "2011 Data Breach Investigations Report," Verizon Business, 2011
4 "State of Web Security," Ponemon Institute, 2011
5 "US Cost of a Data Breach," Ponemon Institute, 2011

PCI DSS 6.6 Compliance

Does your organization process, store, or transmit credit card data? If so, you probably need to comply with the Payment Card Industry Data Security Standard (PCI DSS). To address PCI, you must satisfy 12 high-level requirements, including requirement 6.6, which governs Web security.

PCI 6.6 offers two ways for organizations to protect public-facing Web applications:

- Review web applications at least annually and after any changes
- Protect applications with a Web Application Firewall

First, you must decide whether you want to scan and fix applications or use a Web Application Firewall (WAF) to address PCI 6.6. Then, you must select a WAF solution or a Web scanning or consulting company to achieve compliance.

Option 1: Review Web Applications

All organizations should follow secure application coding best practices. However, addressing PCI# 6.6 by reviewing and fixing applications has the following challenges:

- Organizations must hire an organization that specializes in application security or train internal staff that are independent of the development team
- Organizations must assess application annually and after any changes
- Organizations must fix any vulnerabilities and retest applications

Reviewing and fixing Web vulnerabilities is costly and may impact application development schedules.

Option 2: Implement a Web Application Firewall

Web Application Firewalls automatically detect and block attacks before damage can occur. WAFs offer the following benefits:

- WAFs proactively stop Web attacks. WAFs use multiple detection techniques to identify advanced attacks, automated threats, and bots with precision.
- WAFs provide continuous security. WAFs protect Web applications around the clock – not just immediately after a find-and-fix cycle.
- WAFs offer low total cost of ownership and won't impact Web application development or entail expensive consulting engagements.

For many organizations, WAFs offer a secure, cost-effective way to address PCI 6.6.

Selecting a Web Application Firewall

If you've decided to address PCI 6.6 with a WAF, consider the following evaluation criteria when selecting a WAF:

- **Security accuracy** – The WAF should block all Web attacks and bots without creating false positives.
- **Ease of management** – The WAF should not require in-depth knowledge or training to configure. For smaller organizations, a managed WAF service may be ideal.
- **Ease of deployment** – The WAF should be easy to deploy with minimal network changes or new equipment.

Achieving PCI 6.6 compliance is quick and easy once you've considered your options and determined your requirements.

PCI Security Standards Council

Imperva Cloud WAF has been certified by a PCI Qualified Security Assessor (QSA) as a PCI-compliant WAF service.

PCI DSS COMPLIANT

Imperva subsidiary Incapsula has certified the underlying Imperva Cloud WAF technology.

Imperva Cloud WAF

To avoid a costly data breach and stay out of the news headlines, you need to protect your Website against Web attacks. If you sell product or services online, you also need to address PCI compliance.

Imperva Cloud WAF, powered by Incapsula, is an easy and affordable cloud-based Web Application Firewall service that stops Web attacks and meets PCI requirement 6.6. Security professionals at Imperva provide around-the-clock monitoring, policy tuning, and reports, so you can rest assured that your Web applications and data are safe.

Protect Your Website Against Hackers

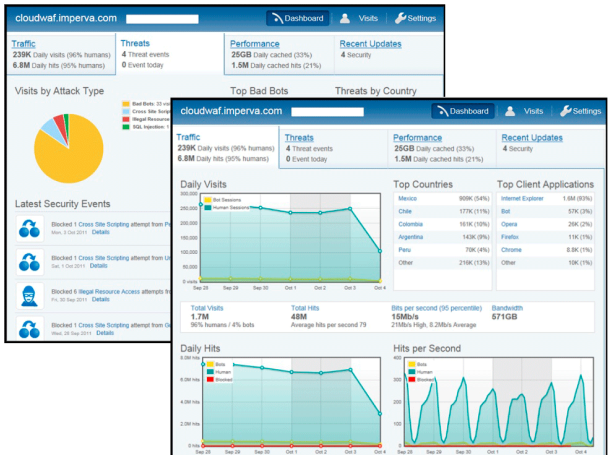
Having an online presence is critical. The challenge is that hackers often prey on smaller organization. Imperva Cloud WAF protects Web applications against current and emerging threats, including SQL Injection, XSS, malicious bots, and other OWASP Top 10 threats.

Achieve PCI 6.6 Compliance

If your company processes credit cards, Imperva Cloud WAF will help you address PCI requirement 6.6 quickly and affordably. With Imperva Cloud WAF, you can protect your Web applications all of the time – not just after a test-and-fix cycle. As a managed, hands-free service, Imperva Cloud WAF will not impact Web development processes and will not entail burdensome consulting costs.

Avoid Search Engine Blacklisting

If a hacker injects malware in your Website, you might not only distribute that malware to your visitors, you might also be blacklisted by search engines – reducing the amount of traffic to your site. Imperva Cloud WAF prevents the attacks, like SQL injection, that allow hackers to upload malware to your site.



Improve Website Performance

Imperva Cloud WAF accelerates the performance of your Website, improving Web page load times and lowering Website bandwidth consumption. It also monitors Website performance and automatically notifies you of errors in your applications and performance issues.

Deploy Cloud WAF Through a Simple DNS Change

Provisioning Imperva Cloud WAF couldn't be easier. Simply update your Website's DNS settings to redirect Web traffic through the Imperva Cloud. This effortless deployment enables you to jumpstart their Web application security initiative while keeping your existing hosting provider and infrastructure.

Benefit from Low Total Cost of Ownership (TCO)

By leveraging a software-as-a-service (SaaS) delivery model, Imperva Cloud WAF provides businesses with the highest levels of Web security available without requiring a large resource investment. Imperva Cloud WAF couples effortless deployment and dedicated security expertise with low annual costs to avoid hardware and operational costs.

Cloud WAF Benefits

- Stop Web attacks like SQL injection and XSS
- Achieve PCI 6.6 compliance quickly and cost-effectively
- Stop automated attacks like site scraping
- Improve Website performance
- Avoid search engine blacklisting
- Outsource WAF management to security experts

Imperva Cloud DDoS Protection

Imperva Cloud DDoS Protection is a simple, secure cloud-based service that safeguards businesses from the most debilitating and protracted DDoS attacks. As a service, Cloud DDoS Protection can be deployed quickly and can scale on demand to mitigate malicious traffic.

Case Study: Keystone RV

Keystone's Website Hit by a DDoS Attack

Headquartered in Indiana, Keystone RV is the leading manufacturer of recreational vehicles in North America.

In August 2011, the company began receiving reports from its dealers saying that its corporate site and its partner portal were unavailable. Mark Widman, Keystone's lead security administrator, contacted the company's Web hosting provider and learned that they were suffering from a Distributed Denial of Service (DDoS) attack.

At first, Keystone's Web hosting provider attempted to allocate more Web servers and allotted more application bandwidth. Unfortunately, according to Widman, the hosting provider's "solution fell apart under the attack. We were caught behind the eight ball."

Quick Deployment with Instant Results

Mark Widman contacted Imperva at 4:00 PM on a Thursday afternoon. After updating the DNS information for the company's Website, Web traffic was redirected through the Imperva cloud. By 6:00 PM – two hours later – Imperva had stopped the attack and the Website was up and running.

Imperva Foils Distributed SYN Flood Attack

Based on information from Imperva, Keystone learned that a massive DDoS attack, known as a SYN flood, had hammered its Website. At the height of the attack, Keystone's Website bandwidth was over one hundred times greater than typical levels.

Two days after purchasing Imperva Cloud DDoS Protection, the DDoS attack subsided. However, Keystone suffered two follow-on attacks over the next month. Imperva was able to stop these DDoS attacks as well.

Technical Support Exceeds Expectations

From the outset, the sales and support staff at Imperva impressed Keystone's security team. "Everyone we've worked with has been knowledgeable and responsive." The Imperva SOC manages all aspects of the deployment, including security policy configuration, monitoring, and tuning.

Imperva Stops Web Application Attacks

Keystone also provisioned Imperva Cloud WAF. So, Keystone's Websites are not only protected against powerful DDoS attacks, but they are also protected against Web application attacks like SQL injection, cross-site scripting (XSS), and directory traversal. Keystone's security team was surprised to learn that both users and bots were attacking the site and attempting to access sensitive data.

Keystone Gains Visibility into Application Activity

Imperva Cloud WAF and Cloud DDoS Protection not only give Keystone's security team peace of mind, they also offer greater visibility into Web application activity. Email alert notifications inform the security team of attacks and abnormal activity. Notifications list the type of threat and the attacker's IP address, Web browser, and geographic location. A high-level dashboard shows security, performance, and configuration information.

With Imperva Cloud Services, Keystone's Website is safeguarded from future Web application and DDoS attacks. From Widman's perspective, "Every aspect of the service has been stellar."

Keystone RV Company

"When we were under attack, our bandwidth went up one hundred fold. Imperva stopped the attack and kept our site up and running."

Imperva
Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065

Tel: +1-650-345-9000
Fax: +1-650-345-9004
www.imperva.com

#EB-Cloud-WAF-0212rev1