Enterprise-Grade Security from the Cloud

Unmatched web application security experience, enhanced by real-time big data analytics, enables Incapsula to provide best-of-breed security to the world’s most security-conscious businesses. Our website security solution redefines and extends the WAF beyond traditional concepts. In addition to our enterprise-grade, PCI-certified WAF, Incapsula’s service also includes backdoor protection, two-factor authentication, and bot access control. An advanced client classification engine analyzes and classifies all incoming traffic to your site, preventing access to malicious and unwanted visitors.

What You Get

- Enterprise-grade, PCI-certified Web Application Firewall
- Protection from malicious bot traffic and backdoors
- Two factor authentication for website access
- Granular website access control based on URL, IP, country, etc.

Why Incapsula?

- Cloud-based, big data approach leverages customer base for 360-degree visibility into attack landscape
- Proven against hundreds of penetration tests and millions of attacks every day
- Dedicated security research team monitors, tunes and updates the service to ensure protection against new and emerging threats
- Decades of security experience and best practices leveraging Imperva’s market-leading WAF technology
- Dynamic profiling and application-aware technologies minimize false positives
- Activated by simple DNS change - no hardware or software installation, integration or changes to the website
Cloud-Based, Big Data Security Approach

A cloud-based approach enables us to harness real data from our customer base to better understand the global attack landscape and continually improve our security. Sandboxing lets us silently test new features on real websites before their launch. Servicing thousands of customers and subjected to hundreds of penetration tests and millions of attacks every day, Incapsula’s service is aligned to meet the most stringent enterprise-grade security criteria. Using crowdsourcing techniques, Incapsula protects your website with collective knowledge about the current threat landscape. Threat information is aggregated across the entire Incapsula community using big data analytics. This data is used to identify new attacks as they happen and simultaneously apply mitigation rules to all websites protected by Incapsula.

Web Application Firewall (WAF)

Best-of-Breed, End-to-End Web Application Security

Incapsula’s enterprise-grade WAF ensures that your website or application is always protected against any type of Application Layer hacking attempt. Based on Imperva’s industry-leading WAF technology and experience, Incapsula’s cloud-based WAF defends against OWASP top 10 threats including: SQL injection, cross site scripting, illegal resource access and remote file inclusion. Security experts behind Incapsula’s service ensure optimum protection against newly discovered vulnerabilities to prevent disruption to your website and improve website performance.

Custom Security Rules

Incapsula’s custom security rules allow you to apply your organization’s security policy within Incapsula’s Web Application Firewall, by configuring a variety of rule triggers and adding different rule actions.
Proactive Remediation
Incapsula’s security team monitors hackers’ activities and zero day exploits to make sure that websites using our service are protected. Using a home-grown database of all common website attacks, content management systems and e-commerce solutions, Incapsula applies dedicated security rules to proactively remediate known vulnerabilities from these sources.

PCI Certification and Reporting
Incapsula’s WAF is certified by the PCI Security Standards Council. The WAF protects you from liabilities and non-compliance penalties, while protecting your customers’ sensitive data from exposure on your site. Incapsula’s PCI compliance report audits security rule configuration changes and periodically reports on your compliance with PCI 6.6 requirements. Rich graphical reporting capabilities enable customers to easily understand security status and meet regulatory compliance.

Blacklisting Prevention
On a daily basis legitimate websites are added to the malware blacklists of security software firms, search engines, and browser vendors due to application vulnerabilities. As a result, access to your website is blocked to customers and partners and your business is effectively shut down. The WAF enables you to close vulnerability gaps in your applications to avoid blacklisting and ensure your website is always accessible.

Customer-Specific Threat Policy Management
Each security rule can be configured specifically according to the customer’s blocking policy (block request, block IP, block session or alert only). The security policy can be fine-tuned to address specific URLs, fields, IP addresses and countries. Powerful access control capabilities enable you to define exceptions and minimize false positives.

In-Depth Threat Monitoring and Analysis
Alerts can be easily searched, sorted, and directly linked to corresponding security rules. Incapsula’s monitoring and reporting framework provides instant visibility into security, compliance and content delivery concerns. A dashboard provides a high-level view of system status and security events. Incapsula provides customers with a detailed analysis of every threat that was posed to your website including: IP address, user agent, location, and other pertinent session information. Weekly graphical reports visualize trends in website traffic, threats, and performance improvements.

Automated Learning of Applications and User Behavior
To accurately detect attacks, a WAF must understand application structure, elements, and expected user behavior. Our Dynamic Profiling technology automates this process by profiling protected applications and building a baseline or “white list” of acceptable user behavior. It also automatically learns application changes over time, minimizing false positives to ensure that every legitimate user reaches your website.

24x7 Security Coverage
Using a “Security as a Service” approach, Incapsula’s security experts manage and update the WAF 24x7 to ensure that you are always protected against new and emerging threats. Incapsula provides organizations with continuous website health monitoring by world-class security researchers. In addition, Incapsula provides email threat alerts, proactive security event management, policy tuning and configuration management, and weekly reporting. For enterprise plan customers, Incapsula assigns a personal account manager to act as a single point of contact for all website security needs.

Backdoor Detection
Hackers covertly install malicious code (known as a backdoor) on your website that gives them full access to your application and data. Incapsula’s WAF monitors website traffic to detect and prevent backdoor install attempts and to quarantine backdoors already installed, rendering them useless.

Datasheet: Website Security
Bot Protection

More than 95% of all website attacks are carried by malicious bots. Using advanced client classification, crowdsourcing and reputation-based techniques, Incapsula distinguishes between “good” and “bad” bot traffic. This lets you block known bad or suspicious bot activity such as comment spam, scraping and vulnerability scanning, while making sure that legitimate bots such as Google, Facebook and Pingdom can freely access your website. In addition to the improved security, blocking malicious bots also improves website performance as they can account to up to 50% of all website traffic.

Login Protect: One-Click Two-Factor Authentication

This feature lets you implement strong authentication on any website or application without integration, coding or software changes. Single-click activation lets you instantly protect administrative access, secure remote access to corporate web applications, and restrict access to a particular webpage. Login Protect manages and controls multiple logins across several websites in a centralized manner. Two-factor authentication is supported using either email, SMS or Google Authenticator.
Website Access Control

With Incapsula, you can take full control over who and what can access your site. Our service provides granular filters and controls to prevent access from unwanted visitors (e.g., countries, specific bots, URLs, IPs), while enabling uninterrupted access to legitimate visitors (customers, leading search engines, etc.). IP address shielding hides your web server’s IP address, preventing access to it via SSH, FTP, Telnet and other methods.

Traffic Analytics

Easy-to-understand traffic analytics give you full visibility into what is happening on your website, from high level statistics and down to a single request related to a security event. Our visualized analytics include statistics of your daily visits – humans and bots, top countries and client applications, stats on your daily hits (bots, humans and blocked), hits per second, accumulated bandwidth and bits per second. Statistics can be sorted by different time frames.