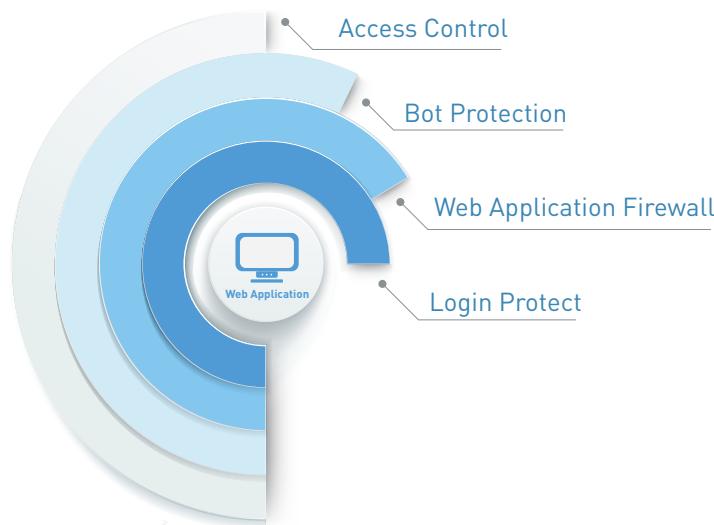


End-to-End Application Security from the Cloud

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 enterprises. Our cloud-based website security solution features the industry's leading WAF technology, as well as strong two-factor authentication and bot access control. An advanced client classification engine analyzes all incoming traffic to your site, preventing access to malicious and unwanted visitors. Complementing the WAF's built-in security capabilities, Incapsula provides easy-to-use tools that enable enterprises to build custom security rules tailored to their specific use cases.



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 security criteria.

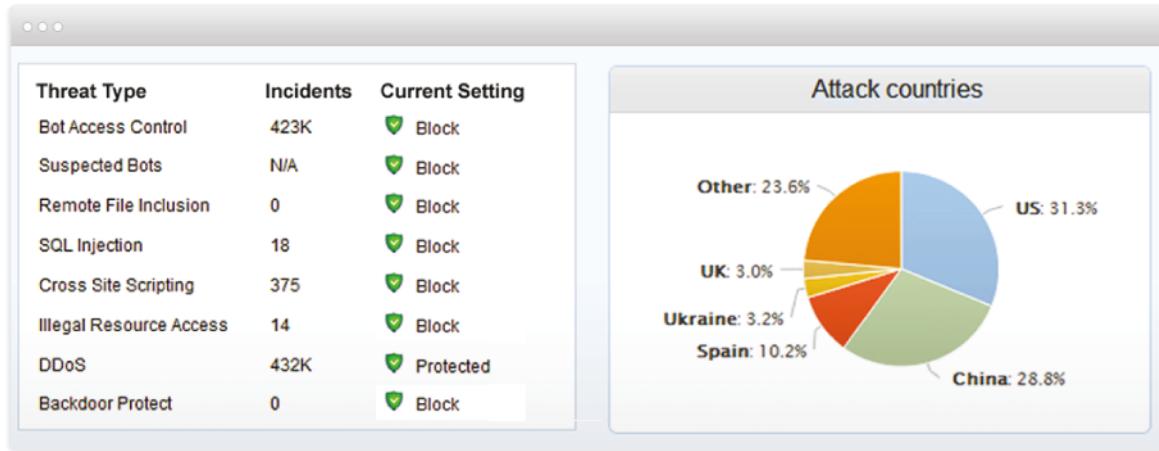
What You Get

- Best-in-class, PCI-certified web application firewall
- Custom rules tailored to your enterprise's security policy and use cases
- Two-factor authentication for website access
- Advanced client classification engine analyzes all incoming traffic
- Easy-to-use API for integration with backend systems

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

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 cloud-based 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 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 application and improve website performance.

Proactive Remediation

Incapsula's security team monitors hackers' activities and zero-day exploits to make sure that websites and applications using our service are protected. Using a home-grown database of all common website stacks, 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. It 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 organizations to easily understand security status and meet regulatory compliance.

Blacklisting Prevention

Legitimate websites are added to the malware blacklists of security software firms, search engines, and browser vendors on a daily basis due to application vulnerabilities. In this scenario, customers and partners cannot access your website 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.

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.

Custom Security Rules

Custom security rules allow each enterprise to enforce its security policy in an optimal manner within the Incapsula website security service. A simple-to-use GUI lets you configure tailored security rules to meet your business' particular needs.

Custom security rules enhance Incapsula's best-in-class web application security capabilities by giving you the flexibility, for example, to tighten security policies around sensitive areas or to generate alerts for specific events that require investigation. Not only do these rules improve security, they also help to eliminate false-positives by taking into account specific user behavior anomalies.

The screenshot shows a 'Add New Rule' dialog box. The top section, 'Rule Details', contains fields for 'Rule Name' (empty), 'Revision Comments' (empty), 'Rule Action' set to 'Disabled', and a checkbox for 'Send E-mail' which is unchecked. The bottom section, 'Rule Editor', shows a configuration for a new rule. It includes an 'Add filter' button, dropdown menus for 'ClientType' (set to 'bot'), operators ('=='), and values ('PageHitsCounter == 200 & ClientId == "GoogleAds Bot" & HeaderExists == "no"'). There is also an 'Add' button. Below this is a large text area containing the generated rule logic, and at the bottom right is a 'Validate Rule' button.

Both technical and non-technical users can define custom rules using the intuitive GUI rule builder or a syntax text editor. Rule actions may include Alert, Block Request, Block IP, or Request CAPTCHA, while rule triggers are based on multiple filters such as URL, client type, and user-agent.

Examples of custom rule triggers:

- (ClientType == Browser | Referrer contains google.com)
- (User-Agent contains googlebot & CaptchaState == Failed | ClientIP == 120.0.0.1).

Bot Protection

More than 95% of all website attacks are carried out 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, for they can account for 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 web page. 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.

We need to verify your identity

Access to this page is restricted. Please enter your email address and passcode to login:

E-mail

Enter passcode from Google Authenticator / SM

Text Me

Submit

Trust this computer for 14 days

Didn't Activate Login Protect?

Protected Pages

Choose pages or areas on your website that would require extended authentication

URL starts with	/administrator		
-----------------	----------------	--	--

Protect Common Applications

Add Page

Methods and Notifications

Choose the extended authentication methods that will be available for visitors of the protected pages or areas

Authentication Methods	SMS <input checked="" type="checkbox"/>	Google Authenticator <input checked="" type="checkbox"/>	E-mail <input checked="" type="checkbox"/>
Send Notifications on Login to protected URL	<input type="checkbox"/>		

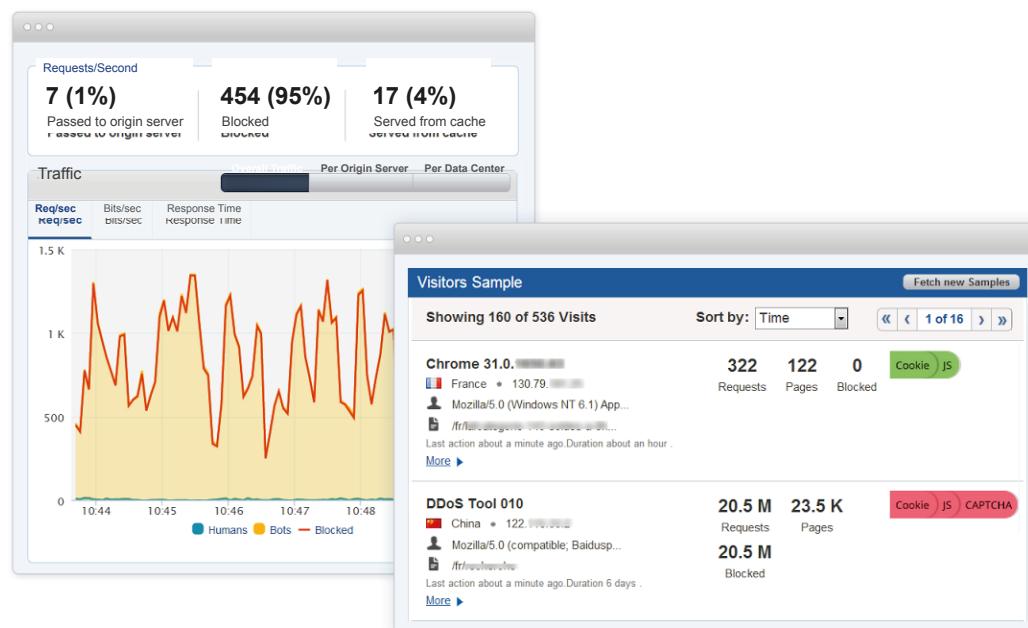
Traffic Monitoring and Analytics

In-Depth Threat Reporting 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 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.

Real-Time Statistics

A real-time Statistics dashboard enables users to get instant access to live information about their website's traffic and performance. This premium feature allows rapid response to security events and supports real-time, data driven decision-making. In the case of a DDoS attack, for instance, live traffic statistics enable your security team to quickly identify abnormal activity patterns of bot and human visitors. They can also evaluate how well their servers are coping with an attack's load, and use the data to optimize load distribution across their servers.



Premium Service Support

Managed Service

Incapsula offers a managed service option, allowing enterprises to free up IT resources for other business-critical tasks. Based on a dedicated team of security experts and support engineers, our fully-managed service provides you with the highest level of security and performance around the clock. Incapsula provides organizations with continuous website health monitoring, as well as email threat alerts, proactive security event management, policy tuning and configuration management, and weekly reporting. A 24x7 NOC performs ongoing security monitoring and ensures that you are always protected against DDoS attacks, as well as other new and emerging threats. Managed service customers are assigned a personal account manager who acts as a single point of contact for all your website security and performance needs.

API for Provisioning, Management, and Events

Incapsula's experts understand the world of enterprise web applications and work closely with IT teams to address their specific integration and customization requirements. Incapsula's API is designed for easy integration with your backend systems, enabling streamlined customer provisioning and account management.

Plug-and-Play SIEM Integration

To help enrich your existing solutions and workflows, Incapsula has developed a "productized connector" for seamless integration with several leading SIEM platforms—including HP ArcSight, Splunk, and McAfee. Residing on your network, it serves as a link between the SIEM and the Incapsula API. In addition to near real-time event reporting and strong data encryption, Incapsula's productized offering features pre-made custom dashboards and reports, permitting easy viewing of incoming data from within the SIEM according to security best practices.



T: +1 (866) 250-7659 | E: info@incapsula.com | www.incapsula.com
3400 Bridge Parkway, Suite 200, Redwood Shores, CA 94065

© 2015, Imperva, Inc. All rights reserved. Imperva, the Imperva logo, SecureSphere, Incapsula and Skyfence are trademarks of Imperva, Inc. and its subsidiaries. All other brand or product names are trademarks or registered trademarks of their respective holders.