IMPERVA

Imperva Incapsula Website Security

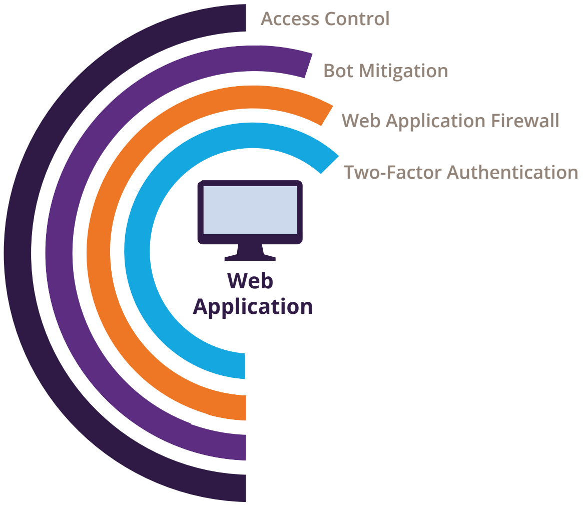
DATASHEET

Application Security from the Cloud

Imperva Incapsula 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 by 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 requirements.

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 that analyzes all incoming traffic
- Easy-to-use API for integration with backend systems



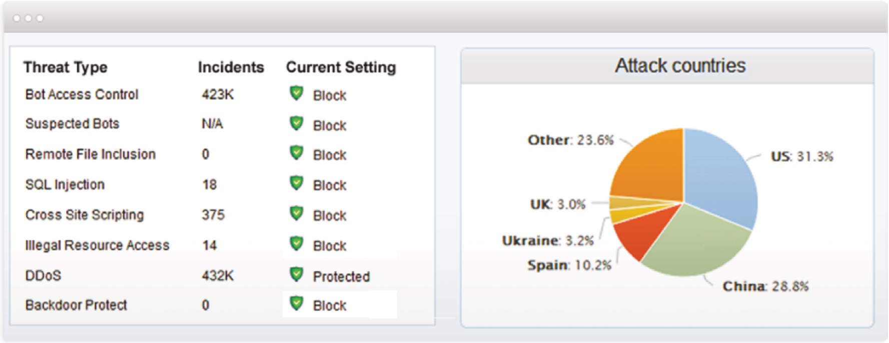
Why Incapsula?

- 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
- 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 is aligned to meet the most stringent 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 and new attack sources. We then use this data to develop new signatures that are deployed across our network.



Threat Type	Incidents	Current Setting
Bot Access Control	423K	✓ Block
Suspected Bots	N/A	✓ Block
Remote File Inclusion	0	✓ Block
SQL Injection	18	✓ Block
Cross Site Scripting	375	✓ Block
Illegal Resource Access	14	✓ Block
DDoS	432K	✓ Protected
Backdoor Protect	0	✓ Block

Web Application Firewall (WAF)

Industry Leading WAF Technology

Incapsula offers a cloud-based WAF that 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, our WAF defends against all OWASP Top 10 threats including: SQL injection, cross-site scripting, illegal resource access, and remote file inclusion. Security experts behind Incapsula ensure optimum protection against newly discovered vulnerabilities to prevent disruption to your application and improve website performance.

Proactive Remediation

The Incapsula security team monitors hackers' activities and zero-day exploits to make sure that websites and applications using our service are protected. Using a exclusive 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. Incapsula delivers protection against newly discovered vulnerabilities to prevent disruption to your application and improve website performance.

PCI Certification and Reporting

Our 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. The Incapsula PCI compliance report audits security rule configuration changes and periodically reports on your compliance with PCI 6.6 requirements. Rich real-time reporting capabilities enable organizations to easily understand security status and meet regulatory compliance.

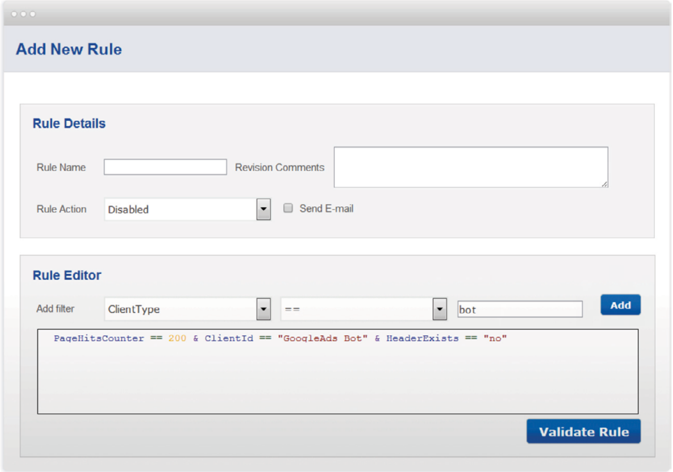
Blacklisting Prevention

Legitimate websites are vulnerable to being 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.

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 custom security rules to meet your organization's particular needs.

Custom security rules enhance our best-in-class web application security capabilities by giving you the capability, 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.



Add New Rule

Rule Details

Rule Name:

Revision Comments:

Rule Action: Disabled

□ Send E-mail

Rule Editor

Add filter: ClientType == bot

```
PageHitsCounter == 200 & ClientId == "GoogleAds Bot" & HeaderExists == "no"
```

Both technical and non-technical users can define custom rules using an intuitive GUI rule builder of a syntax text editor. Rule actions may include alert, block request, block session or block IP or request CAPTCHA, JavaScript or cookie. Rule triggers are based on multiple filters such as URL, client type and user agent.

Examples of custom rule triggers:

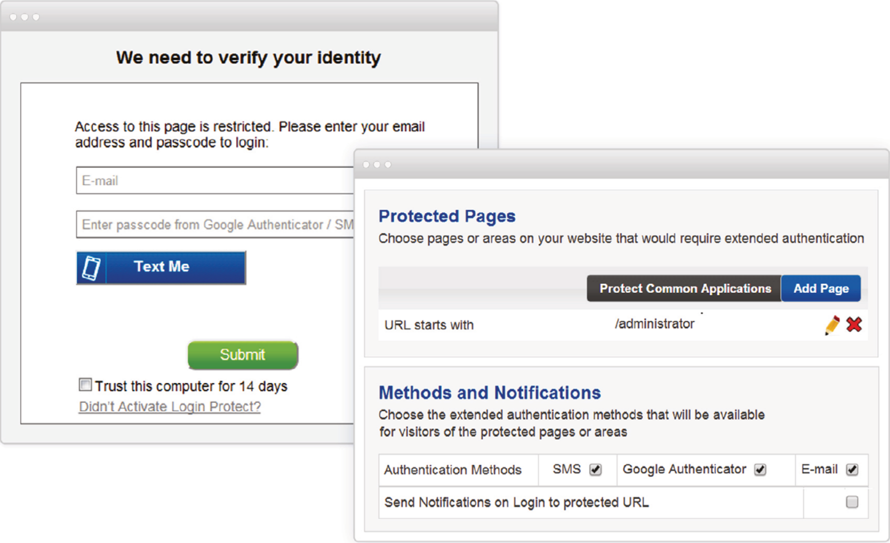
- (ClientType == Browser | Referrer contains google.com)
- (User-Agent contains googlebot & CaptchaState == Failed | ClientIP == 120.0.0.1).

Bot Mitigation

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, because they can account for up to 50% of all website traffic.

Two-Factor Authentication

Incapsula lets you implement strong two-factor 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. Two-Factor Authentication 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

□ 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

Methods and Notifications

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

Authentication Methods	SMS ☑	Google Authenticator ☑	E-mail ☑
Send Notifications on Login to protected URL			□

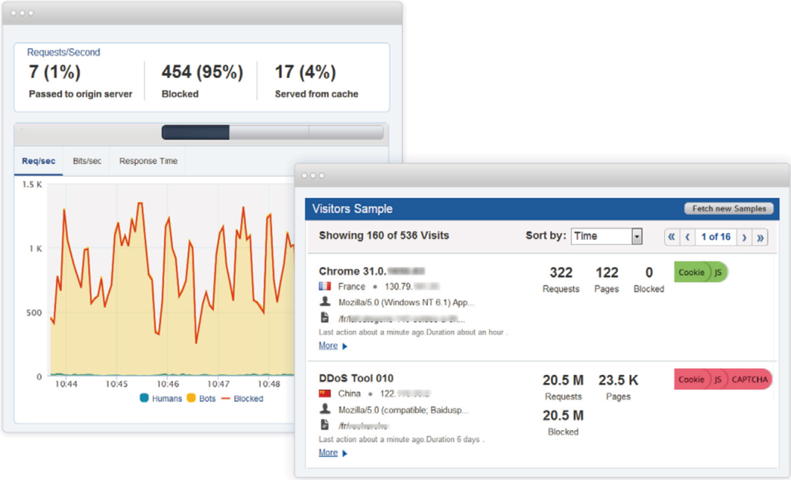
Traffic Monitoring and Analytics

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.



Requests/Second

7 (1%) Passed to origin server

454 (95%) Blocked

17 (4%) Served from cache

Visitors Sample

Showing 160 of 536 Visits

Sort by: Time

« ‹ 1 of 16 › »

Chrome 31.0.[redacted]
France • 130.79.[redacted]
Mozilla/5.0 (Windows NT 6.1) App...
/fr/[redacted]
Last action about a minute ago.Duration about an hour .
More ▸

322 Requests | 122 Pages | 0 Blocked

Cookie | JS

DDoS Tool 010
China • 122.[redacted]
Mozilla/5.0 (compatible; Baidusp...
/fr/[redacted]
Last action about a minute ago.Duration 6 days .
More ▸

20.5 M Requests | 23.5 K Pages | 20.5 M Blocked

Cookie | JS | CAPTCHA

Premium Service Support

Managed Service

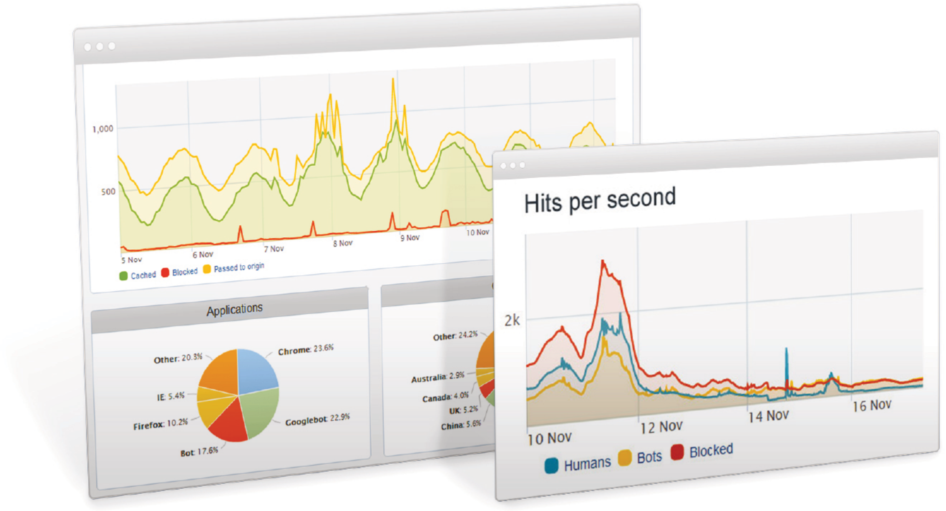
Incapsula offers a managed service option, allowing organizations to free up IT resources for other business-critical tasks. Based on a dedicated team of security experts and support engineers, our fully-managed service provides you with the highest level of security and performance around the clock. 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 24×7 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

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

Plug-and-Play SIEM Integration

To enhance your existing security solutions and workflow, Incapsula supports leading SIEM solutions including HP ArcSight, Splunk, McAfee, IBM QRadar and Graylog. In addition to near real-time event reporting and strong data encryption, SIEM integration features pre-built custom and reports.


1,000
500
5 Nov
6 Nov
7 Nov
8 Nov
9 Nov
10 Nov
🟩 Cached 🟥 Blocked 🟨 Passed to origin
Applications
Other: 20.3%
Chrome: 23.6%
IE: 5.4%
Firefox: 10.2%
Googlebot: 22.9%
Bot: 17.6%
Other: 24.2%
Australia: 2.9%
Canada: 4.0%
UK: 5.2%
China: 5.6%
Hits per second
2k
10 Nov
12 Nov
14 Nov
16 Nov
🟦 Humans 🟨 Bots 🟥 Blocked