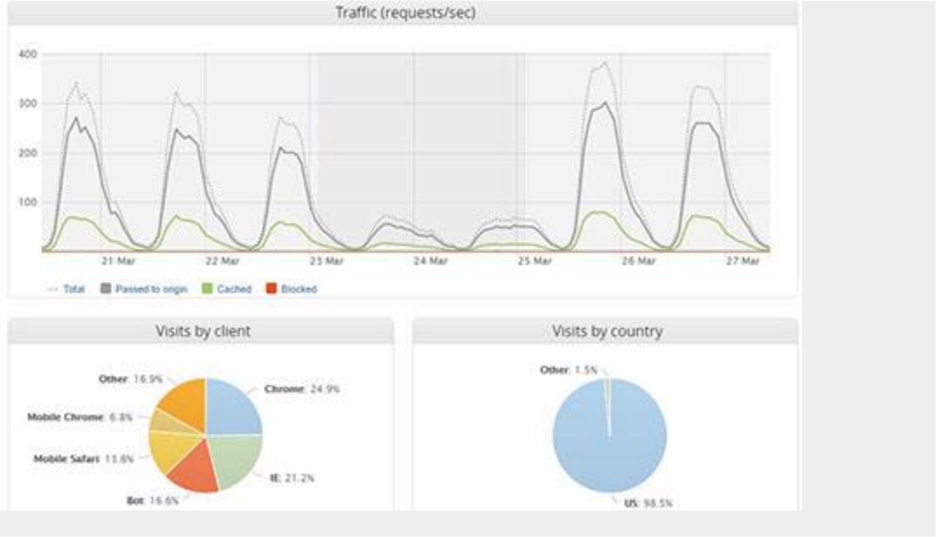
Cloud Web Application Firewall

Application Security from the Cloud

Modern web applications have become mission-critical for major Fortune 500 organizations that rely on their applications to drive revenue, develop a desired brand image and cultivate customer relationships. Yet they face global threats from all parts of the world. Cybercriminals seek to exploit an organization's digital presence to establish a foothold into their IT environments and gain access to valuable corporate data. Further, the move of web application software towards agile development practices often means that software has not been thoroughly tested, and may be released with critical vulnerabilities that can be exploited by a cybercriminal. Organizations are looking for web security solutions that not only provide comprehensive security protection but also the flexibility to scale for their users around the world.

Imperva Cloud WAF

Imperva Cloud WAF offers the industry's leading web application security firewall, providing enterprise-class protection against the most sophisticated security threats. As a cloud-based WAF, it ensures that your website is always protected against any type of application layer hacking attempt.



Cloud WAF defends against the latest advanced web threats

KEY CAPABILITIES

- Best-in-class, PCI-certified WAF
- Advanced client classification engine analyzes all incoming traffic
- Custom rules tailored to your enterprise security policy
- Two-factor authentication for website access
- 24/7/365 Security Operations and Support Team

Defending Against Web Threats

Imperva Cloud WAF prevents the exploitation of OWASP Top 10 threats like SQL injection, cross-site scripting, illegal resource access, and remote file inclusion. Security is further enhanced by an advanced client classification engine that analyzes all incoming traffic to your site, preventing access by malicious visitors. This allows Imperva to accurately distinguish between malicious bot traffic and legitimate visitors, long before traffic reaches your site. A simple-to-use GUI lets you configure custom security rules that meet your organization's particular needs.

Powerful Client-Classification Engine

An advanced identification engine profiles all incoming traffic in real time, distinguishing between legitimate and malicious clients long before they reach a web application. This security process is used to identify and block automated bots often used to launch malicious cyberattacks against web applications. In this way, customers can obtain increased web security, lower web-server utilization and reduced bandwidth consumption.

OWASP Top 10 Protection

Imperva Cloud WAF protects against all OWASP Top 10 security threats, blocking attacks in real time. The Imperva research team actively discovers emerging threats. New security signatures that defend against recently discovered threats are added daily – providing the up-to-date security protection you need in today's fast-changing attack landscape.

Easy-to-Use Management Interface

Imperva Cloud WAF is configurable through an easy to use web interface, protected via two-factor authentication. Users can configure custom security rules which allow an enterprise to optimally enforce security policies within their unique environments. Plus, a high-level dashboard provides a summary overview of the overall threat landscape for your organization.

IMPERVA APPLICATION SECURITY

Cloud WAF is a key component of Imperva Application Security, which reduces risk while providing an optimal customer experience. The solution safeguards applications on-premises and in the cloud by:

- Monitoring all data activity
- Protecting against DDoS attack
- Mitigating botnet attacks
- Providing actionable security insights
- Providing RASP protection

Learn more about Imperva Application Security at www.imperva.com.