imperva

CAPABILITY BRIEF

Web Application Firewall (WAF) Gateway

Protect your critical web applications

Web Applications are a prime target of cyber-attacks because they are readily accessible and offer an easy entry point to valuable data. Organizations need to protect web applications from existing and emerging cyber-threats without affecting performance, time to market, or uptime. The rapid pace of application changes can make it very difficult for security teams to keep up with updating rules that properly secure web assets. This can create security gaps and vulnerabilities that cybercriminals can exploit, leading to costly data breaches. Additionally, organizations look to deploy security solutions that can scale with their applications to match growth in user demand, ensuring that web assets are properly secured while preserving the end-user experience.

Imperva WAF Gateway

The market-leading Imperva WAF Gateway empowers organizations to protect their applications through automated web security and flexible deployment. WAF Gateway provides comprehensive protection and granular capabilities, making it the ideal solution to secure valuable web assets, achieve PCI compliance and provide iron-clad protection against OWASP Top Ten security attacks.

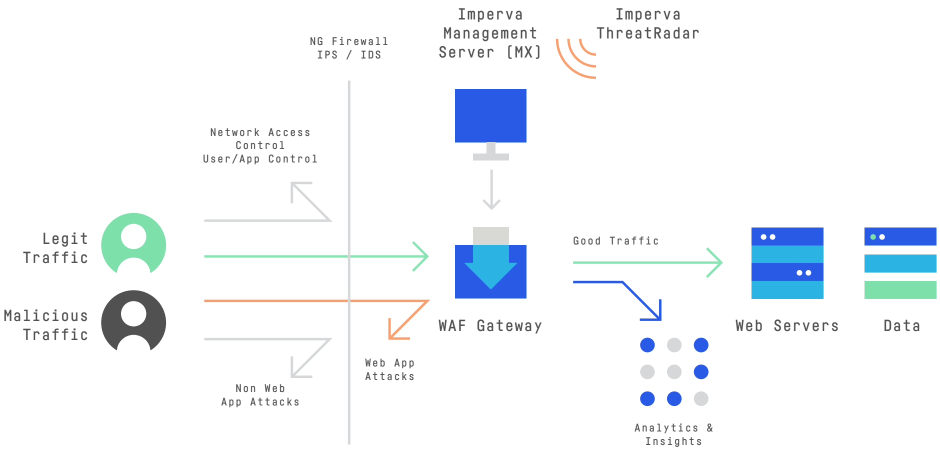

Figure 1: Imperva WAF Gateway protects applications from web based attacks leveraging research-driven intelligence.

KEY CAPABILITIES

- Dynamic profiling learns protected applications and user behavior, automatically applying a positive security model
- Flexible deployment to support hybrid environments (on-premises and cloud)
- Updates web defenses with research-driven intelligence on current threats
- Correlates security violations to detect sophisticated, multi-stage attacks
- Automated virtual patching
- High performance; transparent, drop-in deployment
- Fully PCI compliant
- Simplified event investigation with Attack Analytics

Protect critical web applications and data

Imperva WAF Gateway can identify and act on dangers maliciously woven into seemingly innocuous website traffic – traffic that slips through other layers of defense – preventing application vulnerability attacks such as SQL injection, cross-site scripting and remote file inclusion or business logic attacks such as site scraping or comment spam.

Automated application learning

WAF Gateway uses patented Dynamic Profiling technology to automate the process of profiling applications and building a baseline or "whitelist" of acceptable user behavior. This positive security model approach is benefited by automatic incorporation of valid changes on the application profile over time. Dynamic Profiling eliminates the need to manually configure and update countless application URLs, parameters, cookies and methods in your security rules.

DevOps automation

A robust set of APIs enables DevOps and Security teams to integrate WAF Gateway deployment and day-to-day tuning activities into existing DevOps processes.

Flexible deployment options

WAF Gateway can be deployed as a physical appliance, a virtual appliance or in the cloud via Amazon Web Services or the Azure marketplace. Additionally, WAF Gateway can be deployed transparently, requiring virtually no changes to the network. Granular policy controls enable superior accuracy and unequaled control to match each organization's specific protection requirements.

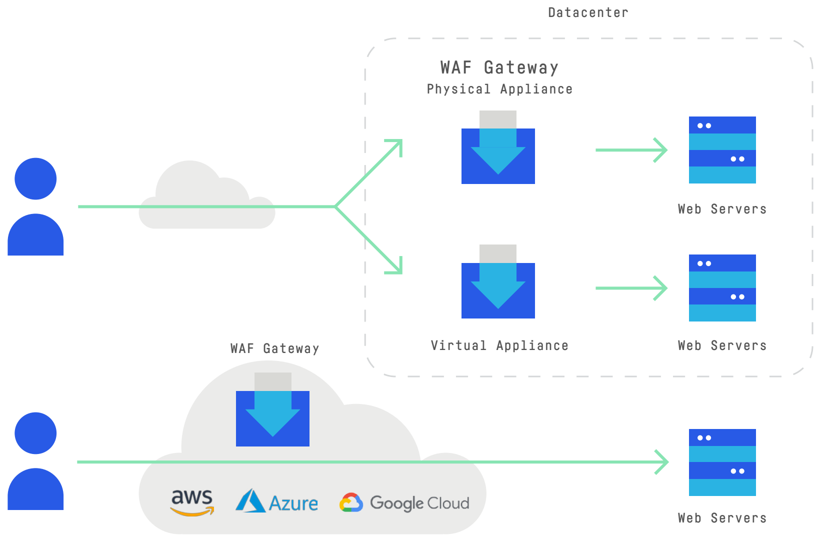

Figure 2: Imperva WAF Gateway can be deployed as a physical appliance, virtual appliance or in the cloud.

IMPERVA APPLICATION SECURITY

WAF Gateway is a key component of Imperva Application Security, which reduces risk while providing an optimal user experience. Our solutions safeguard applications on-premises and in the cloud with:

- Web application firewall (WAF)
- Distributed Denial of Service (DDoS) protection
- Botnet attack mitigation
- Runtime Application Self-Protection (RASP)
- Actionable security insights
- Security-enabled application delivery

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

Virtual patching

Thanks to vulnerability scanner integration, WAF Gateway can perform “virtual patching” for your web application. Instead of leaving a web application exposed to security threats for weeks or months following a vulnerability discovery, virtual patching actively protects the application from attack. This narrows the window of exposure, buying time until resources are available to patch the vulnerability.

Robust reporting and analytics

Imperva WAF offers rich graphical reporting capabilities to easily understand security status and meet regulatory compliance. Predefined and customizable reports enable teams to quickly asses security posture and streamline demonstration of compliance with PCI, SOX, HIPAA, FISMA and other compliance standards. Additionally, WAF Gateway alerts feed our best-in-class Attack Analytics, where security teams can view critical insights in intuitive, single pane of glass narratives and dashboards. Attack Analytics combats alert fatigue by distilling millions of security alerts into a prioritized set of actionable security insights.

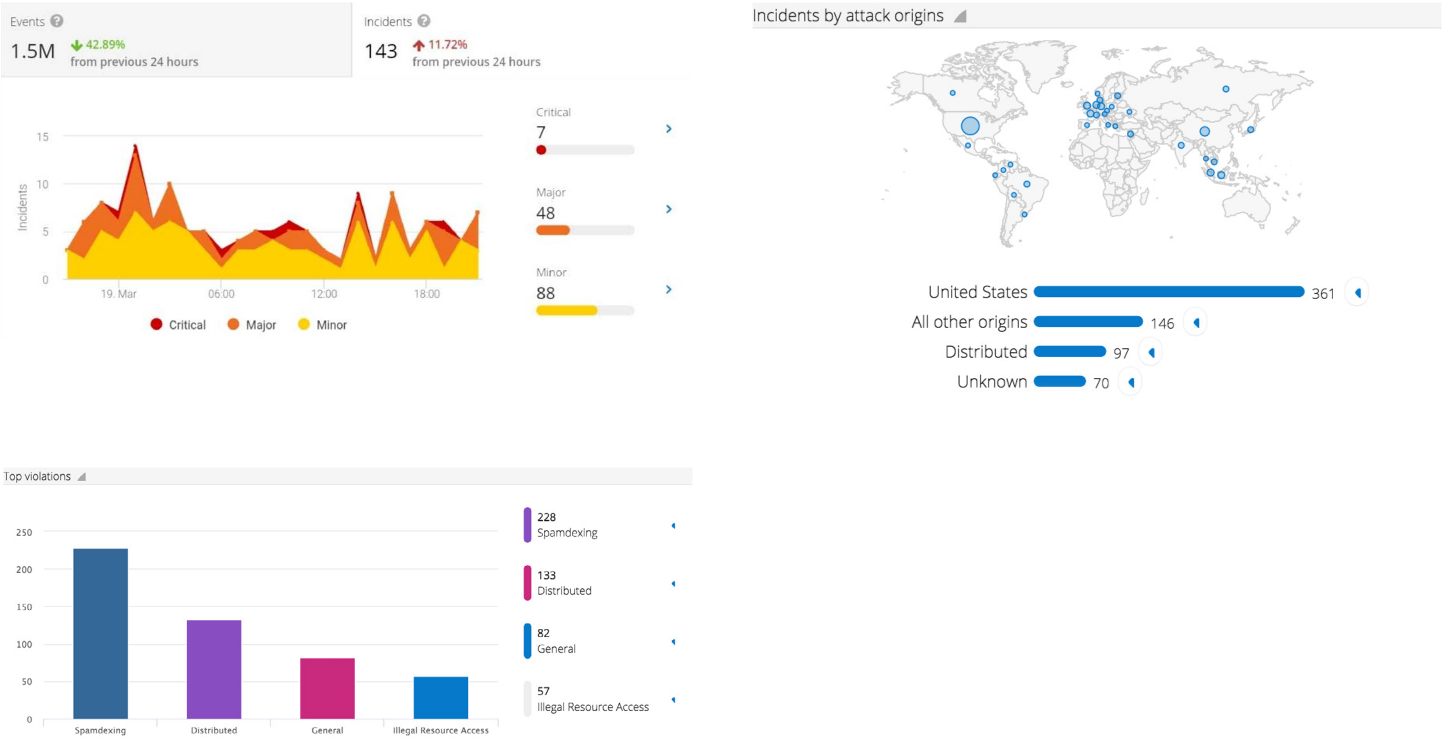

Figure 3: Imperva WAF Gateway offers rich graphical reporting capabilities to easily understand security and meet regulatory compliance.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com

Copyright © 2020 Imperva. All rights reserved