Product Brief

Imperva Web Application Firewall (WAF) Gateway

thalestct.com

THALES
Building a future we can all trust

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 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.

Key Capabilities

Dynamic profiling learns protected applications and user behavior, automatically applying a positive security model

Flexible deployment to support hybrid to cloud-native environments

Can be deployed in-band and as a listener with support for Envoy and Nginx

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

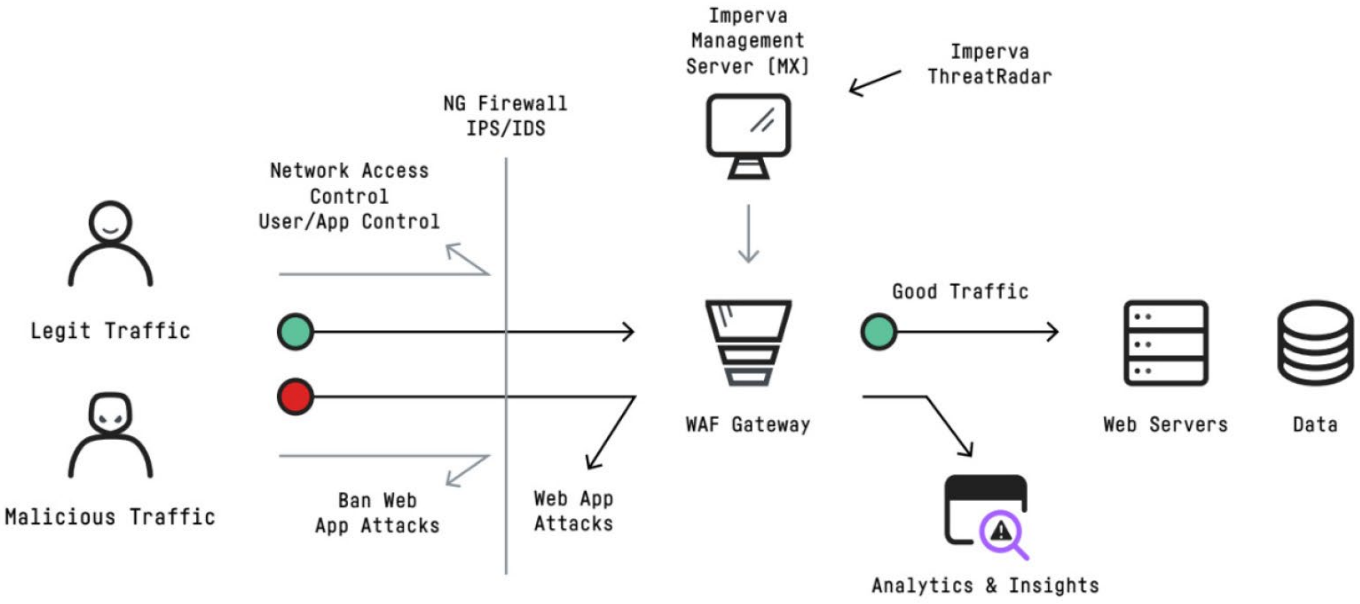

Figure 1: Imperva WAF Gateway protects applications from web based attacks leveraging research driven intelligence.

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.

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

Imperva Application Security is available for sale to the U.S. Federal Government through Thales TCT.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

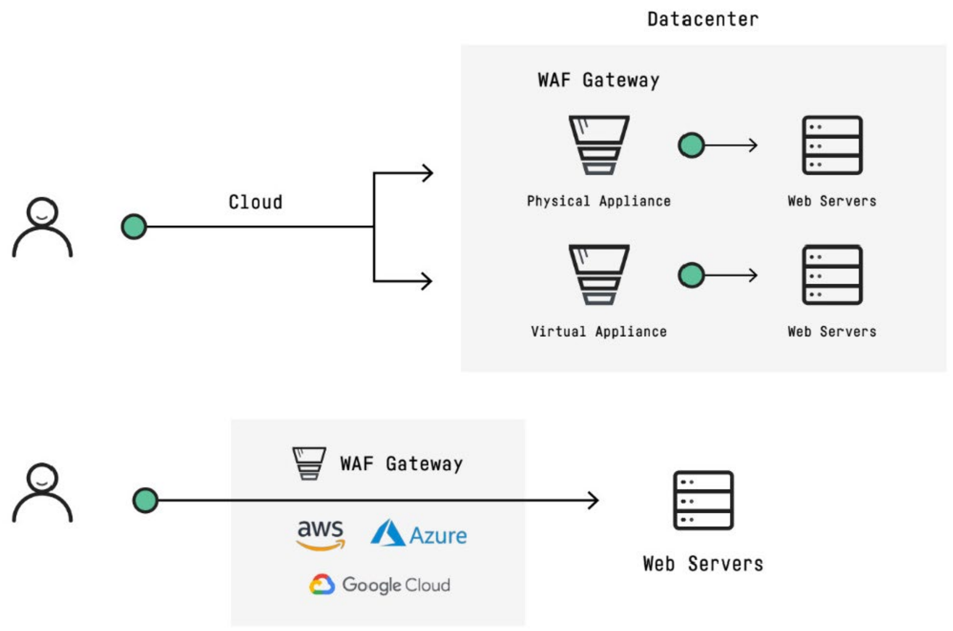

Figure 2: Imperva WAF Gateway can be deployed as a physical appliance, virtual appliance or in the cloud.

©2024 Thales 3.28.24