imperva

CAPABILITY BRIEF

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. Whether your websites and applications are hosted in the public cloud or on-premises, Cloud WAF ensures your critical assets are always protected against any type of application layer hacking attempt.

Cloud WAF is part of an integrated, defense in depth suite of application security and delivery services including CDN, DDoS Protection, Advanced Bot Protection, and Load Balancing at every single one of our global points of presence. All components share intelligence so that security and delivery logic can be applied right from the edge, as soon as the request hits our network. The solution integrates with leading SIEMs, and Imperva Attack Analytics uses artificial intelligence (AI) to distill thousands of Cloud WAF events into distinct narratives, significantly improving security operations center (SOC) efficiency and reducing risk.

KEY CAPABILITIES:

Best-in-class, PCI-certified WAF

Out of the box, automated protection

Deploys in blocking mode with near-zero false positives

Terraform integration enables automated DevOps provisioning

Backed by security experts at Imperva Research Labs who de-risk use of third party code

Self-service custom rules

24/7/364 Security Operations and Support Team

Part of comprehensive cloud application security and delivery

Delivers threat information for actionable insights in Attack Analytics

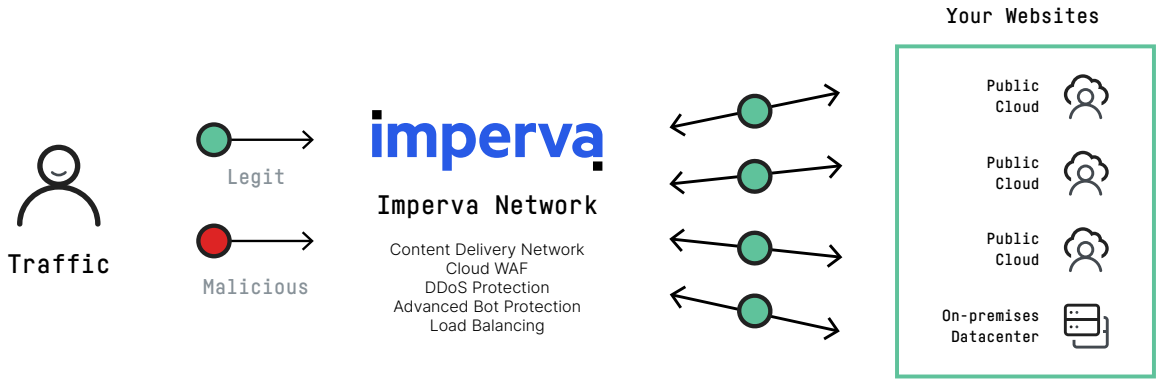

Figure 1: Cloud WAF inspects every request, filtering out malicious activity

Defending against web threats

Always-on protection

An advanced identification engine profiles all incoming traffic at the edge in real time, accurately distinguishing between legitimate and malicious clients long before they reach a web application. This automated security process means not only increased web security, lower web-server utilization and reduced bandwidth consumption but also less reliance on in-house security experts and the decrease in accuracy that comes with manual controls. It's no wonder that the vast majority of Imperva Cloud WAF customers deploy in blocking mode out of the box, as the solution allows legitimate traffic through with near-zero false positives.

Beyond OWASP Top 10 protection

Imperva Cloud WAF protects against all OWASP Top 10 security threats like cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. The solution works in conjunction with the Imperva Application Security solution stack, utilizing the different mitigation capabilities that different attacks require - whether it's a DDoS attack or a bot utilizing a SQL injection to attack your API.

Moreover, the team at Imperva Research Labs actively discovers emerging threats to provide the up-to-date security protection you need in today's fast-changing attack landscape. Security experts monitor external sources like new vulnerability disclosures and help you reduce the risk of third party code. The team analyzes all traffic going through Imperva via crowdsourced intelligence, automatically vetting then propagating new mitigation rules to all our customers. New security signatures that defend against recently discovered threats are added daily.

Easy to use and scale

Imperva Cloud WAF is configurable through an easy-to-use web interface, protected via two-factor authentication. A simple GUI allows for configuration of custom security rules to optimally enforce security policies within unique environments. With DevOps automation provisioning through our Terraform provider, policy propagation of tens of thousands of rules can happen in seconds. A high-level Cloud WAF dashboard provides a summary overview of the overall threat landscape for your organization, and management is centralized alongside other functionality like API Security, DDoS Protection, and more.

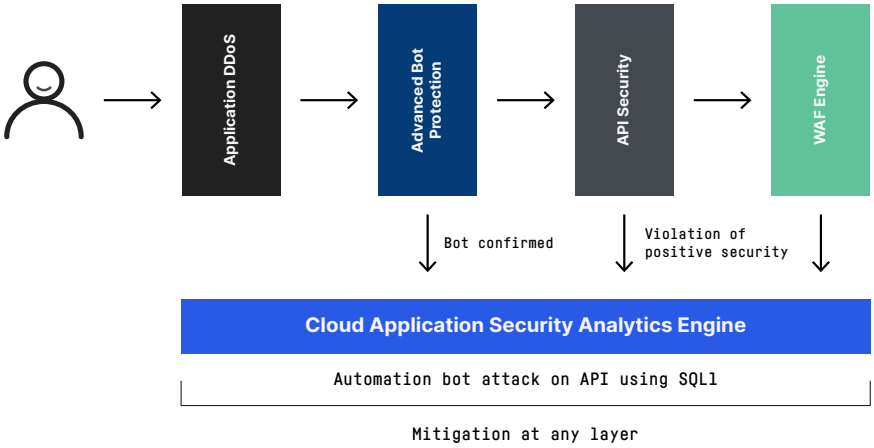

Figure 2: Cloud WAF Role in Defense in Depth

IMPERVA APPLICATION SECURITY

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

Providing actionable security insights

Providing WAF protection

Protecting against

DDoS attacks

Mitigating botnet attacks

Blocking cyber-attacks that target APIs

Enabling RASP protection

Ensuring optimal content delivery

Learn more about Imperva Application Security at +1.866.926.4678 or online at imperva.com

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