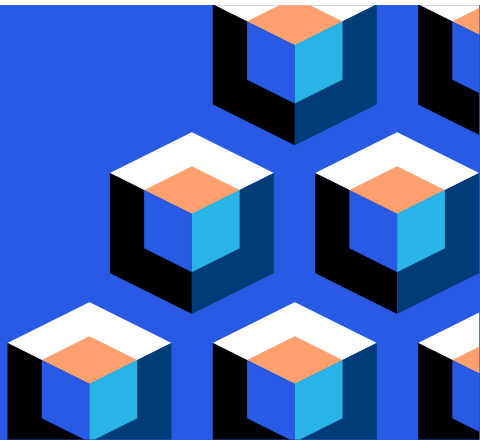
imperva

DATASHEET

Imperva Application Security

Keep business up and enemies down.



Introduction

Applications have become mission-critical for organizations looking to drive rapid growth. They help facilitate customer reach around the world and can act as the primary business model. These applications require protection from security threats, yet end-users demand high availability and an uninterrupted experience, which can make for a tough balancing act. To meet this need, Imperva Application Security empowers organizations to protect their applications and mitigate risk while also providing an optimal user experience.

Secure your critical applications

Imperva deploys a defense-in-depth model which provides a layered approach to enforcing security from the application to the end user. Through Imperva **Runtime Application Self-Protection (RASP)**, a lightweight agent is incorporated during the software development cycle. RASP learns the unique behavior of the application and fortifies a security defense model around inherent security vulnerabilities, reducing pressure on development teams to immediately fix critical vulnerabilities before releasing to production, while ensuring immediate and effective protection against malicious exploits. A six-time Leader in the Gartner Magic Quadrant for Web Application Firewalls, Imperva provides WAF solutions (cloud-based **Cloud WAF** and on-premises or virtual appliance **WAF Gateway**) to defend against all OWASP Top 10 threats including SQL injection, cross-site scripting, illegal resource access, and remote file inclusion. Inspection and enforcement of user traffic occurs across Imperva's global network of PoPs, each also a DDoS scrubbing center. Policies and signatures are kept up-to-date for your WAF and **API Security** based on live, crowdsourced intelligence and from security experts at **Imperva Research Labs**.

KEY FEATURES

- Uncover and act upon key critical security incidents by utilizing artificial intelligence and machine learning.
- Secure against OWASP Top 10 threats across both the cloud and on-premises WAF deployments.
- Mitigate potentially devastating DDoS attacks before they even reach your application.
- Accelerate web content delivery ensuring users consistently have an optimal user experience
- Support faster application release cycles while ensuring application protection during runtime.
- Ensure high availability even when under attack from malicious bots and DDoS.

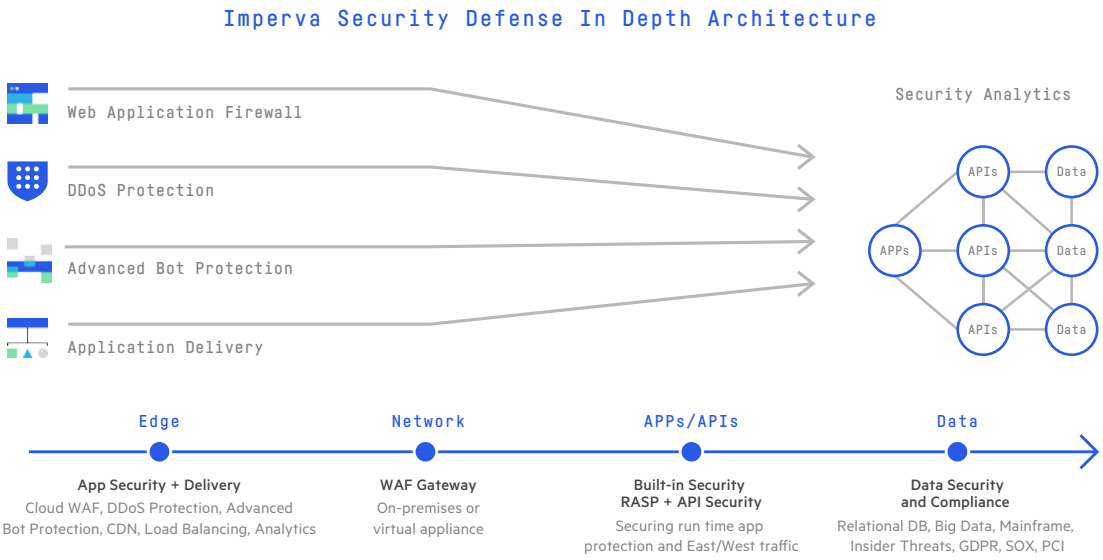


Figure 1: Imperva Security Defense In Depth Architecture

Act on critical insights

With today's complex and ever-changing threat landscape, it's more important than ever to gain visibility across your data and applications. An explosion of security alerts can keep organizations from discovering critical attacks that actually pose an imminent threat. **Attack Analytics**, a key part of Imperva Application Security, combats alert fatigue by distilling millions of security alerts into a prioritized set of security insights. It gives recommended actions to improve your security posture, helping you recognize your cyber risk and help bring it down.

Avoid disruption to your business

Cybercriminals often wage disruption campaigns against high-profile targets like bank, retail or political organizations. They are driven by revenge, blackmail or political activism and utilize vast botnet networks to wage devastating attacks. Organizations without proper protection from malicious bots and Distributed Detail of Service (DDoS) attack are exposed to the risk of users experiencing slowed or denied access to their websites. Constant attack campaigns can drive users from returning, fulfilling the goal of the attacker. Imperva Application Security provides powerful **DDoS Protection** and **Advanced Bot Protection** to eliminate attacks long before malicious traffic even has a chance to reach a customer's website. Multiple DDoS protection services are available, with always-on protection for websites, DNS servers, and individual IPs, and always-on or on-demand protection for networks. With near-zero latency and backed by a 3-second service level agreement, DDoS traffic is mitigated without disruption to legitimate traffic. And with Imperva Advanced Bot Protection, fingerprinting and client classification categorizes whether traffic is coming from a human, a good bot or a bad bot. It does so quickly and accurately, with a very low false positive rate, protecting against account takeover and all business logic attacks on websites, APIs and mobile apps.

Ensure a seamless user experience

Organizations that depend upon return users often require designing their website infrastructure so that web content may be quickly delivered to meet global user demand at anytime. Imperva **Application Delivery** with its **Content Delivery Network (CDN)** optimizes website delivery by providing content closest to the end-user. With a global network of PoPs, Imperva is able to provide quick and reliable access to web content. An application-aware CDN dynamically profiles a website, identifying all cacheable content (dynamic and static), and provides dynamic content acceleration. Profiling and frequency analysis ensure the most frequently accessed resources are detected and served directly from memory, allowing website optimization, improved performance, and lowered bandwidth costs.

To further help organizations deploy applications that are highly scalable, load balancing in the cloud replaces costly appliances. When high availability and redundancy in the event of a web server failure is crucial, Imperva is able to prevent any impact of service to end-users. Imperva **Load Balancer** supports a single data center with multiple servers, site failover, and global server load balancing. Real-time health monitoring and notifications ensure traffic is always routed to a viable web server.

Complete Investment Protection

FlexProtect is a flexible approach to securing applications. A single license offers you the ability to deploy Imperva Application Security how and when you need it. FlexProtect for Applications allows customers the flexibility to adapt their security without regard to infrastructure. You're protected regardless of the number, location or type of devices or services used. FlexProtect helps you protect apps wherever you deploy them - in the cloud, or on-premises or as a hybrid model.

imperva