Product Brief

Imperva

Application Security

thalestct.com

THALES
Building a future we can all trust

THALES

Protection that keeps organizations running continuously

In today's modern application landscape, maintaining critical applications, APIs, and their data has never been more essential. 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 providing an optimal user experience. Imperva also makes vendor consolidation and management simplicity a reality, with application security components offered as part of an integrated solution set.

Secure your critical applications

Imperva deploys an integrated defense-in-depth model which provides a layered approach to enforcing security from the application to the end user. Through Imperva R**untime Application Self-Protection (RASP)**, a lightweight agent is incorporated during the software development cycle.

An analyst leader in reports like Gartner® Magic Quadrant™, Imperva provides **Web Application Firewalls (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. Imperva API Security provides continuous protection of all APIs using deep discovery and classification to detect all public, private and shadow APIs. It also protects against business logic attacks and many more of the OWASP API Top Ten. The easy-to-deploy solution empowers security teams to implement a positive API security model.

Key Capabilities

Uncover and act upon key critical security incidents by utilizing artificial intelligence and machine learning.

Secure out-of-the-box against OWASP Top 10 threats across both the cloud and on-premises WAF deployments.

Prevent data theft from client-side attacks and other online skimming techniques to maintain compliance.

Mitigate all bot-driven account takeover attacks and prevent account based fraud.

Support faster application release cycles while ensuring application protection during runtime.

Ensure high availability even when under attack from malicious bots and DDoS.

Imperva Security Defense-in-Depth Architecture

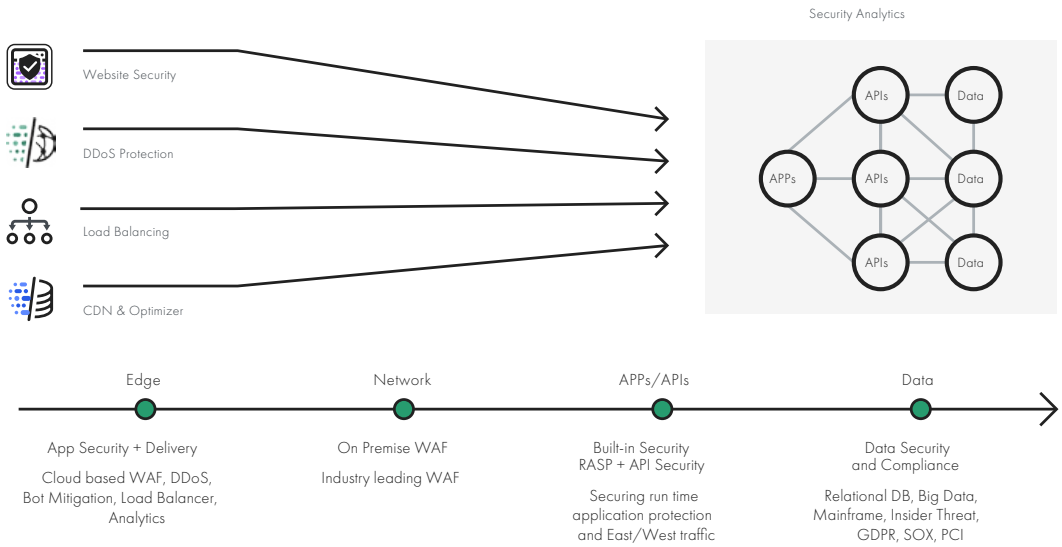

Figure 1: Imperva Security Defense In Depth Architecture

Act on critical insights with machine learning

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 organization

Cybercriminals often wage disruption campaigns against high-profile targets. 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 for network protection, 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 websites, mobile apps and APIs against all OWASP 21 automated threats, including account takeover, web scraping, business logic abuse and fraud.

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 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.

Imperva Application Security

Our solution safeguards applications on-premises and in the cloud by:

Providing actionable security insights

Providing a complete WAAP solution

- Protecting against DDoS attacks
- Mitigating sophisticated automated threats
- Discovering, classifying and protecting APIs
- Enabling protection at runtime
- Ensuring optimal Content delivery

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

Protect sensitive customer data and ensure compliance

Client-side protection further helps organizations secure every aspect of their web applications and ensure the safety and privacy of their data. It mitigates the risk of client-side attacks that exfiltrate sensitive data, resulting in devastating, costly data breaches. By providing clear visibility with actionable insights and easy controls, Imperva empowers your security team to effortlessly determine the nature of each service and block any unapproved ones. This enables your organization to meet data security and privacy compliance standards, including those set in the latest version of PCI DSS.

Consolidated Protection, Powerful Packaging

AppProtect is a flexible and comprehensive 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.

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

.