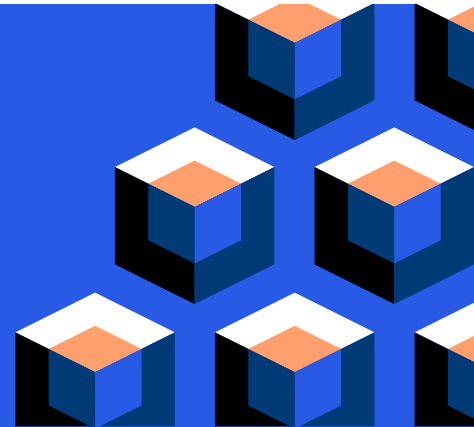# imperva.

Imperva Application Security

Flexible security when and how you need it.

Introduction

Applications have become mission-critical to organizations looking to drive rapid growth. An increasing reliance on the web has ensured that applications are in the critical path for organizations seeking exponential growth. For many business, such as those that are exclusively online, applications have become their primary business model, helping to facilitate customer reach around the world and rapid financial growth. Organizations recognize that end-users demand a high-quality experience when accessing applications, regardless of where they are in the world. The end-user experience must be secure, consistent and seamless, reducing the risk of any disruption to the revenue model of countless organizations around the world that rely on their applications to drive their business. Imperva Application Security empowers organizations to protect their applications, while ensuring their customers have an optimal user experience. Through Imperva, organizations can not only prevent unforeseen disruptions to their business but also mitigate risk.

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 blindside organizations from discovering critical attacks that actually pose an imminent threat that often can result in a data-breach through an application exploit. Many security teams unable to cope with the avalanche of security alerts, often succumb to alert fatigue which leads to ignoring critical incidents that actually matter. Imperva Application Security's Attack Analytics empowers organizations to quickly crush security alerts into a few meaningful security incidents that can be quickly investigated and acted on by security teams. Powered by artificial intelligence, Attack Analytics can distill millions of security alerts into a prioritized set of security insights which you can act upon. This can help organizations to recognize the level of cyber risk that they are actually exposed to across their environment.

KEY FEATURES AND BENEFITS

- 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 attack before they even reach your application.

- Accelerate web content delivery ensuring users consistently have optimal user experience.

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

- Ensure high availability of your application despite web workload failures.

CISOs can view high-level summary reports that illustrate the countries where attack campaigns haven launched against their organization, the type of security attacks and the malware tools that were employed during each attack campaigns.
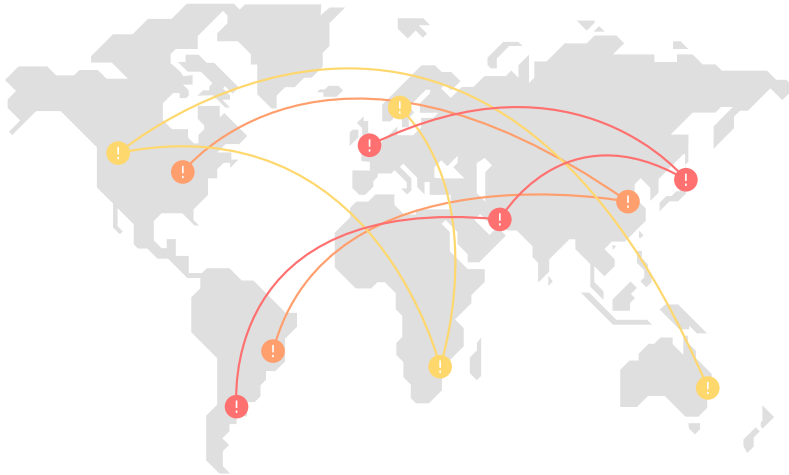

Figure 1: Critical Insights into the attacks that matter

Secure Your Critical Applications

At Imperva, we deploy a security-in-defense model which provides a layered approach to enforcing security across from the application towards the end-user. We can provide full-spectrum protection from within the application, in the cloud or on-premises deployments. At the application level, we can directly protect applications through Imperva Autonomous Application Protection (AAP), a light-weight agent that is incorporated during the software development cycle. AAP learns the unique behavior of the application and fortifies a security defense model around inherent security vulnerabilities. This reduces pressure on development teams to immediately fix critical vulnerabilities before releasing to production, all the while ensuring immediate and effective protection against malicious exploits. Imperva also provides Web Application Firewalls that defend against all OWASP Top 10 threats including SQL injection, cross-site scripting, illegal resource access, and remote file inclusion. For broader protection, customers can deploy Imperva Cloud WAF that provides inspection and enforcement of user traffic across Imperva's global network of PoPs. Web traffic that is destined to customer websites is quickly distinguished between legitimate and malicious traffic. Malicious traffic is quickly remediated at the nearest Imperva PoP, allowing only legitimate traffic to flow safely to a customer website. For customer who have on-premises deployments, Imperva provides Web Application Firewall (WAF) gateways that can be deployed on customer sites providing immediate protection by combining automatic application learning with up-to-date protection policies and signatures from Imperva Security Research team.

imperva
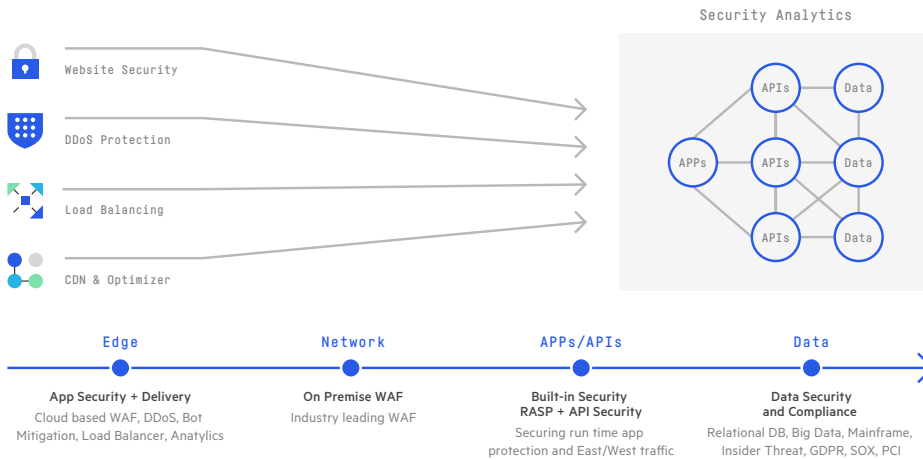
Imperva Security Defense In Dept Architecture

Security Analytics

Website Security

DDoS Protection

Load Balancing

CDN & Optimizer

Edge	Network	APPs/APIs	Data
App Security + Delivery	**On Premise WAF**	**Built-in Security RASP + API Security**	**Data Security and Compliance**
Cloud based WAF, DDoS, Bot Mitigation, Load Balancer, Anatylics	Industry leading WAF	Securing run time app protection and East/West traffic	Relational DB, Big Data, Mainframe, Insider Threat, GDPR, SOX, PCI

Figure 2: Imperva Security Defense in Depth Architecture

Avoid Disruption to your Business

Cybercriminals often wage disruption campaigns against high-profile websites such as bank, retail or political organizations. They are often driven by revenge, blackmail or political activism and utilize vast Botnet networks to wage devastating Distributed Denial of Service (DDoS) attacks. Organizations without proper protections are often exposed to DDoS attacks that can completely deny or slow users from accessing their websites. These constant attack campaigns can drive users from returning back to a websites, fulfilling the goal of the attacker. Imperva Application Security provides powerful DDoS protection aimed at directly eliminating attacks before they even get off the ground, by directly stopping malicious DDoS traffic across Imperva's global-wide network POPs, long before malicious traffic has even a chance to reach a customer website. Imperva provides two DDoS protection solutions. DDoS Protection for Websites, an always-on service that provides protection for any type of DDoS attack of any size, duration or sophistication with near-zero latency – all backed by a service-level agreement. This service can be activated in minutes via a simple DNS change. No on-site hardware or software changes is needed and no changes to your hosting provider or application are required. Imperva also provides DDoS protection for Networks, which is an always-on or an on-demand service that can protect an IT assets from DDoS Attacks. DDoS traffic destined for customer networks is immediately mitigated across the Imperva global network – ensuring no disruption to enterprise traffic.
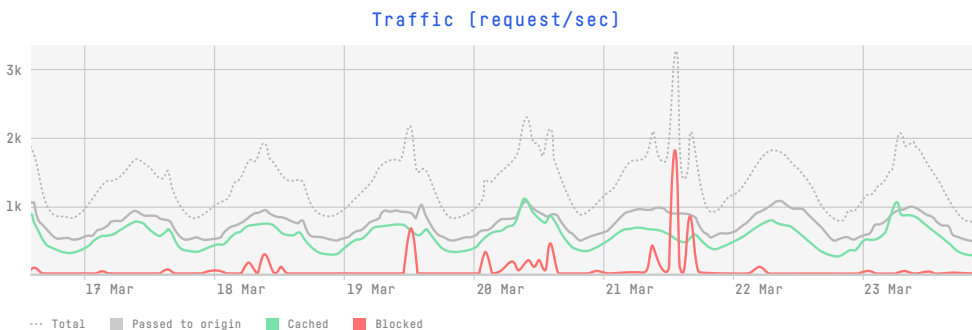

Traffic [request/sec]

··· Total   Passed to origin   Cached   Blocked

Figure 3: Customer DDoS attack being mitigated by Imperva

imperva

Ensure Seamless User Experience

Users demand a consistent and seamless experience when visiting websites. Frequent experiences with slow webpage downloads can contribute to users moving to other websites. Organizations that depend on users returning to their websites often require designing their website infrastructure so that web content can be quickly delivered to meet user demand at anytime from anywhere in the world, ensuring optimal user experience. Imperva content delivery network empower organizations to optimize website delivery with content closest to their end-users. With a global network of CDN sites, Imperva is able to match any content delivery requirements to ensure that users are able to access web content quickly and consistently. Our application-aware CDN dynamically profiles a website and identifies all cacheable content (dynamic and static). Moreover, dynamic profiling and frequency analysis ensure that the most frequently access resources are detected and served directly from memory. This allows customers to optimize their website, improve website performance while lowering bandwidth costs.

To further help organizations deploy applications that are highly scalable, Imperva load balancer provides scalable load-balancing, replacing costly appliances with an enterprise-grade cloud-based solution. Customers who demand and require their applications to be designed for high availability and redundancy in the event of a failure of a web server, can ensure that there is no impact of service to their users. Based on a global CDN, Imperva load balancer supports a single data center with multiple servers, site failover (for DR scenarios), and Global Server Load Balancing (GSLB). Real-time health monitoring and notifications ensure that traffic is always routed to a viable web server.

Figure 4: Imperva Application Delivery: Improving Website Performance

Provides 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, on-premises or as a hybrid model.

KEY FEATURES AND BENEFITS

- Reduce the cost of uncertainty when moving to the cloud

- Predict costs even as your in-the-cloud and on-premises infrastructure change over time

- Flexibility to scale as your business scales

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

+1 (866) 926-4678
imperva.com

imperva