

Imperva Corporate Overview

Security threats – full stop

Data is your enterprise's vital intelligence. Applications are how you run your business. Both are mission-critical. At Imperva, we equip you to manage your data and application security – seamlessly and with more actionable insights. Security experts at Imperva Research Labs work tirelessly to understand the changing threat landscape, as seen in our [Cyber Threat Index](#) which utilizes data from Imperva sensors all over the globe. As cybercriminals evolve their tactics, we have the tools to evolve our solutions and to protect the pulse of your business.

ABOUT US

Imperva is a leading, analyst-recognized cybersecurity company championing the fight to secure data and applications wherever they reside: on premises, in the cloud, or both.

AT-A-GLANCE

Year Founded: 2002

Headquarters: Redwood Shores, CA

Employees: 1,000+

Partners: 500

Customers: 6,000+

OUR CUSTOMERS INCLUDE

- 38 Fortune 100 companies
- 7 of the top 10 global telecom providers
- 56 of the top 100 global banks

OUR ACCOLADES

6x Leader
in the Gartner Magic Quadrant for Web Application Firewalls

2x Leader
in the Forrester New Wave for Bot Management

2x Leader
in the Forrester Wave for DDoS Mitigation Solutions

Leader
in the Forrester Wave for Runtime Application Self-Protection

Learn more at imperva.com.
Call us at +1-866-926-4678, or email us at sales@imperva.com

“We’re paying a small price to avoid lost business and bad customer experiences.”

Aaron Blakeley
Director of Global Security Operations,
DigiCert

“We now spend less time on issues such as software changes and can direct more energy on protecting our members’ data and company information.”

Sharon Black
Sr. Manager of Information Security,
BlueCross BlueShield of Tennessee



**1 million
attacks blocked
every minute**



**3 million
databases
protected**

Imperva Application Security

Strong defense against DDoS attacks, malicious bots and more, with protection from the end-user to the application.



WEB APPLICATION FIREWALL (WAF) with cloud-based and on-premises or virtual appliance deployments protect business-critical applications and their data from the most sophisticated cyberattacks.

- Cloud WAF and WAF Gateway allow legitimate traffic through and keep bad traffic out
- Out-of-the-box deployment in blocking mode with little to no tuning and near-zero false positives
- Policies automatically updated based on live, crowdsourced data and backed by security experts at Imperva Research Labs
- Highly configurable via self-service to allow tight security for your specific applications



API SECURITY gives DevOps and security teams the flexibility to quickly publish their APIs with the added visibility required to secure all your endpoints.

- Automatic positive security model generation with each OpenAPI Specification file
- Simplified management of protection for both websites and APIs
- Seamless integration with leading API Management vendors



APPLICATION DELIVERY combines a content delivery network, content caching, load balancing and failover delivered as a built-in service of Cloud WAF.

- Enables websites and applications to run faster, safer, and more reliably
- Maximizes application performance by load balancing web traffic in the cloud
- Optimizes website performance with intelligent caching and optimization tools



ATTACK ANALYTICS is a service that correlates and distills thousands of events into the most critical attack narratives across Cloud WAF, WAF Gateway, DDoS Protection, API Security, and more.

- Simplifies threat discovery using artificial intelligence and machine learning
- Improves efficiency of security operations centers by reducing the number of events to investigate
- Provides recommended actions to improve security posture in your particular environment



DDoS PROTECTION provides always-on, cloud-based DDoS attack detection and mitigation.

- Automatically stops attacks on websites, networks, DNS servers and individual IPs
- Includes a 3-second DDoS mitigation SLA against any type, size or duration of attack
- Gives you real-time attack visibility and investigation into both Layer 3 / 4 and Layer 7 attacks



RUNTIME APPLICATION SELF-PROTECTION protects applications by default.

- Protects both legacy and modern applications with a single, autonomous plugin
- Neutralizes attacks with exceptional accuracy
- Provides immediate, permanent patches that mitigate vulnerabilities in production



ADVANCED BOT PROTECTION protects your websites, mobile applications, and APIs from automated threats without affecting the flow of business-critical traffic.

- Accurately detects and stops web scraping, online fraud attempts, account takeover, credential stuffing, vulnerability scanning, and more
- Correlates real-time bad bot behavior across the Imperva network with the largest known violators database
- Pinpoints anomalies with biometric data validation and rate limits based on device fingerprints

Imperva Data Security

Protect your data from theft and extortion—all while meeting compliance requirements.



CLOUD DATA SECURITY enables fast time to compliance, providing ongoing visibility into cloud databases with zero installation.

- Achieve compliance within minutes
- Automate ongoing database discovery, data classification, and incident detection
- Set custom alerts and audit policies for maximum control
- Enables DevOps with API-driven protection that's scalable



DISCOVERY AND ASSESSMENT finds unknown databases, classifies sensitive data and detects database vulnerabilities.

- Automates database discovery and uncovers hidden risks
- Classifies data using dictionary and pattern matching classification methods
- Identifies vulnerabilities that expose databases to increased risk



DATA ACTIVITY MONITORING AND PROTECTION reliably monitors and protects databases and files with little or no impact on performance or availability.

- Gives visibility into what's happening with your data
- Alerts or blocks unauthorized activity in real-time
- Protects databases, file shares, mainframes and big data repositories



DATA MASKING reduces risk in non-production environments by replacing sensitive data with realistic, fictional data.

- Masks large volumes of data quickly and easily
- Accelerates data-driven business processes
- Helps comply with data privacy and protection regulations



DATA RISK ANALYTICS uses machine learning and behavior analytics to identify suspicious data activity.

- Distills millions of alerts to pinpoint high-risk incidents
- Assigns a risk score to prioritize incidents
- Provides actionable insights in plain language

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

imperva.com