

DATASHEET

# 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. As cybercriminals evolve their tactics, we’re evolving our solutions, in order 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: 550+  
 Customers: 5,800+

### OUR CUSTOMERS INCLUDE

- 10 of the top 10 global telecom providers
- 5 of the top 10 U.S. commercial banks\*
- 4 of the top 5 global diversified insurance companies
- 2 of the top 5 global biotech companies
- 3 of the top 10 global computer hardware companies

Learn more at [www.secez.com](http://www.secez.com) Call us at +91 - 120-2423448, or email us at [enquiry@secez.com](mailto:enquiry@secez.com)

## Imperva Application Security

Combining cloud services, virtual and physical appliances for strong application security and DDoS defense.



**CLOUD APPLICATION SECURITY** offers a multi-function application delivery service that secures websites.

- Shields critical online assets against web attacks
- Mitigates application and infrastructure DDoS attacks
- Ensures high website availability and performance
- Provides actionable insights about external threats



**WEB APPLICATION FIREWALL (WAF)** protects business-critical applications and their data from the most-sophisticated cyberattacks.

- Automatically learns application structure with dynamic profiling
- Maintains high performance with rich security features enabled
- Mitigates advanced targeted attacks by correlating multiple attack conditions
- Provides enterprise-wide scalability with broad deployment options



**RUNTIME APPLICATION SELF-PROTECTION**

(formerly Prevoty) 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



**ATTACK ANALYTICS** is a service that correlates and distills thousands of events into a few, actionable attack narratives.

- Simplifies threat discovery using artificial intelligence and machine learning
- Consolidates events from both Cloud WAF and WAF Gateways into a single feed
- Improves efficiency of security operations centers by reducing the number of events to investigate



**THREAT INTELLIGENCE** is a security reputation feed that combines threat research from Imperva security research, live crowdsourced intelligence and threat intelligence from multiple partners.

- Automatically learns application structure with dynamic profiling
- Automatically blocks emerging threats
- Identifies good bots, bad bots and humans



**DDOS PROTECTION** provides an always-on DDoS mitigation service that manages any type, size or duration of attack.

- Detects and mitigates attacks against websites, networks, DNS servers and individual IPs
- Includes a 3-second DDoS mitigation SLA
- Gives you real-time visibility over attacks and provides actionable insights for Layer 7 attacks



**APPLICATION DELIVERY** combines content caching, load balancing and failover delivered as a service.

- 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

## Imperva Data Security

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



**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