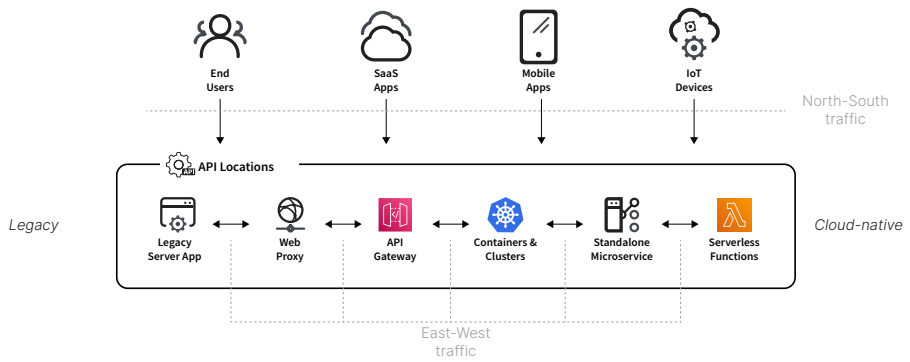
imperva
a Thales company

DATASHEET

API Security

Protect your APIs from modern cyberattacks

APIs (Application Programmable Interface) are the cornerstone of digital transformations for many enterprises. Whether developing applications in new cloud-native microservice and serverless architectures, automating business-to-business processes or providing a back-end for mobile applications, APIs are rising in significance to the enterprise. Unfortunately, cybercriminals have seen this shifting towards an API-centric world and are discovering new attack vectors as fast as the API growth itself. This creates the critical need for enterprises to adopt new security measures that can better protect their APIs and all things digital.



While Digital Transformation is driving innovation, many security teams struggle with API visibility which as a consequence increases business risks.

Imperva API Security

Through automatic detection of API endpoints, Imperva API Security enables comprehensive API visibility for security teams – without requiring development to publish APIs via OpenAPI or by adding resource-intensive workflow to their CI/CD processes – by providing full contextual data and tags and automatically determining risks around sensitive data. Security teams can incorporate a positive security model to protect their organization from API-based threats. Moreover, every time an API is updated , security teams can stay on top of the change, understand any new risks and incorporate changes, which leads to faster, more-secure software release cycles. Imperva API Security enables security teams to keep pace with innovation without impacting development velocity.

KEY CAPABILITIES

Continuous API discovery and risk classification

In-depth protection against OWASP API Top 10

Positive security model built from OpenAPI specifications

Shift left by empowering developers with real-time API state for any change or abuse to optimize performance

Unified solution for website and API security from legacy to cloud-native applications

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

Comprehensive edge API discovery and risk classification

Whether it's a known edge API , an unknown shadow API or internal API driving transactions on the backend, discovering APIs is essential for establishing a positive security model for API Security. Imperva API Security provides continuous discovery of your APIs. More importantly, Imperva offers contextual insights, ranging from detection of sensitive data such as personal identifiable information (PII) to classification of APIs based on data and coding risks.

In-depth protection against OWASP API Top 10

Imperva protects you from the latest Open Web Application Security Project (OWASP) API Security Top 10 as your developers build microservices and APIs across different environments.

Positive security model enforces correct behavior

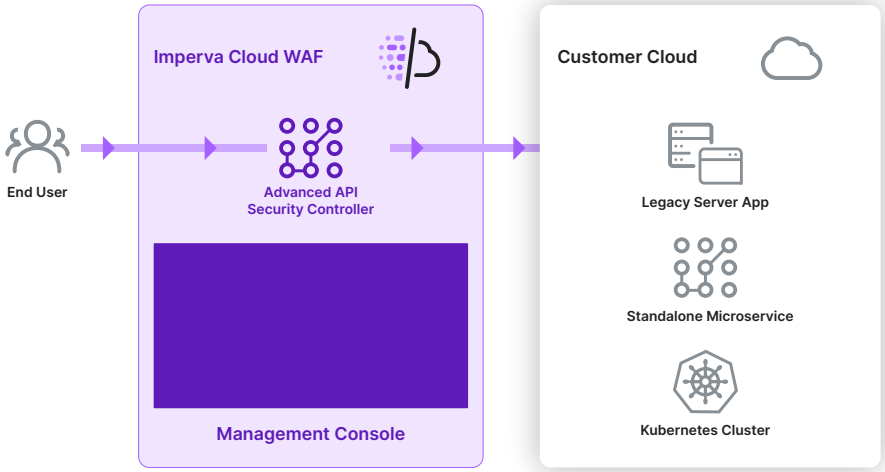
Protect your APIs against critical security attacks enforcement of a positive security model, built from your own API inventory. This helps to remove the burden of API specification validation on developers and the load on your application in runtime.

Shift left by empowering developers with real-time API state

Aligning with DevOps and other modern development practices, security teams need to offer agile quality assurance services as the code moves through the CI/CD pipeline. API Security provides API data (from correlated metrics to traces and logs) to work with developers in delivering products that delight customers.

Flexible deployment model without slowing down development

Quickly enabled by Imperva Cloud Web Application Firewall (WAF) or deployed as a standalone to gain visibility into all API traffic.



Imperva API Security can be seamlessly activated for Imperva Cloud WAF customers

KEY BENEFITS

API Security is a key component of Imperva Application Security, which reduces risk while providing an optimal user experience. The solution safeguards legacy or cloud-native by:

Protection for any backend applications anywhere that Cloud WAF can route

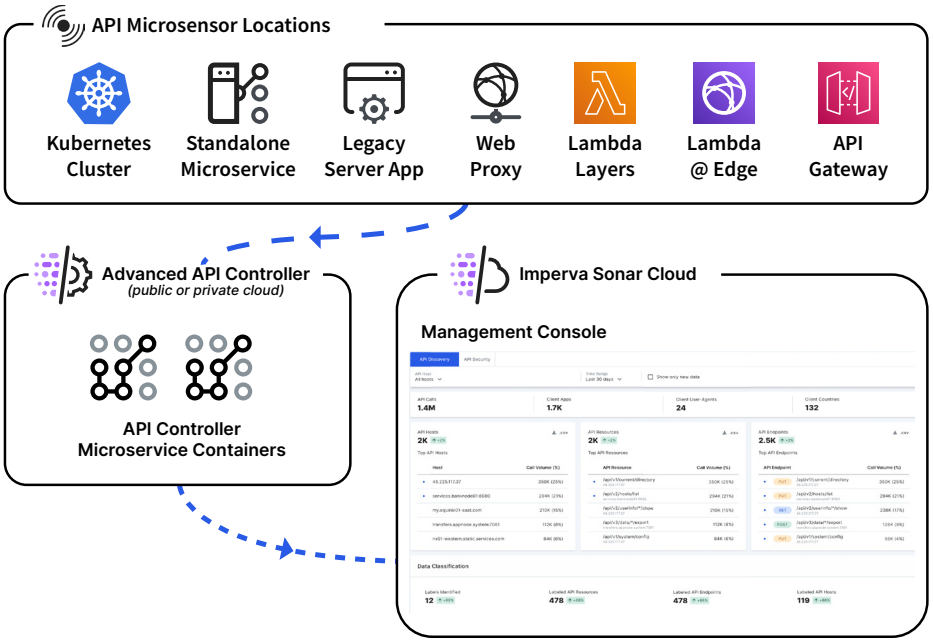
From legacy to cloud-native applications, get continuous API discovery with automatic data classification

Flexible deployment model without slowing down development

Quickly identify and establish a positive security model with zero impact on DevOps

Effortlessly ensure API governance around sensitive data

imperva.com
+1.866.926.4678



Imperva API Security can be deployed within your own cloud architecture

Unified solution for website and API security for both legacy and cloud-native applications

Imperva API Security, part of the Imperva Application Security suite, simplifies security management with an integrated CDN, Load Balancer, and DDoS Protection for both website and API traffic.

KEY DIFFERENTIATORS

Innovative & Proven Market-Leading Solution
The industry's first API Security solution to be fully integrated with analyst-recognized leading Web Application Firewall, Advanced Bot Protection, and DDoS prevention

ML Driven Discovery, Classification, & Insights
Automatically detect and generate complete API schemas across all endpoints with sensitive data classification

Coverage for External & Internal APIs
Imperva Anywhere provides a single solution to detect and protect North/South & East/West API communications

Simple Frictionless Deployment
Easily deploy API security using Cloud WAF or by using a microsensor that works within hybrid / cloud-native environments, no gateways or coding required.

Learn more about Imperva Application Security at +1.866.926.4678 or online at imperva.com