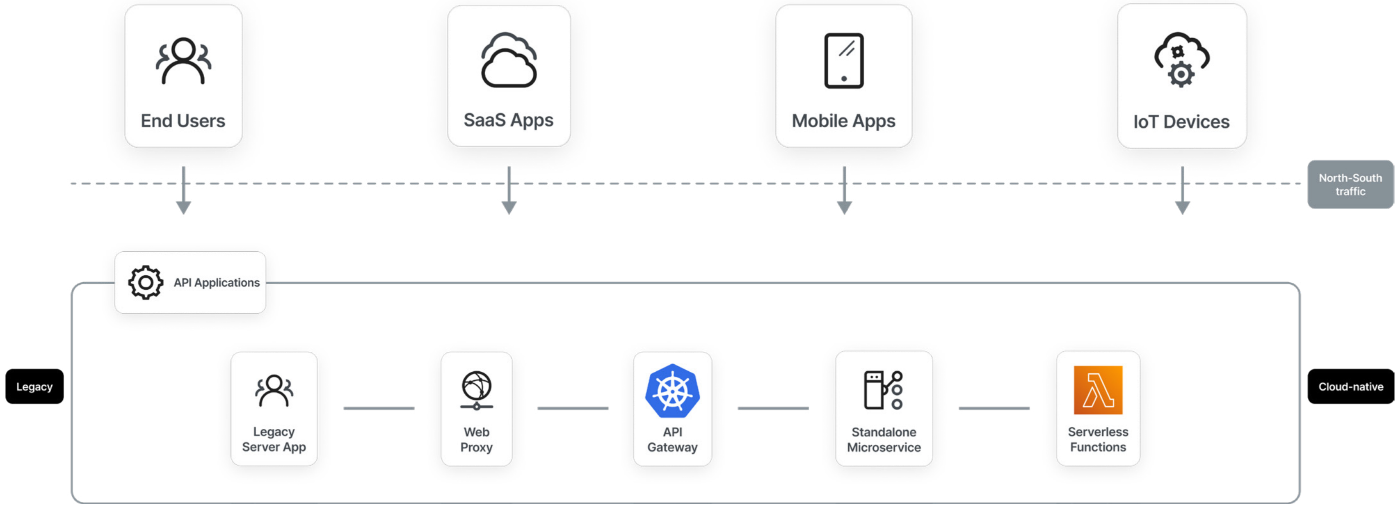
imperva
a Thales company

DATASHEET

# Imperva API Security

APIs (Application Programmable Interfaces) serve as the backbone of digital transformations across numerous enterprises. Whether developing applications within cloud-native microservice architectures or automating business-to-business processes in legacy non-cloud environments, APIs are increasingly vital to enterprise operations.



Cybercriminals are exploiting this API-centric landscape, discovering new attack vectors as API usage grows. Consequently, robust security measures are essential to safeguard both public and private APIs and the sensitive data they handle.

The diagram illustrates APIs as the primary entry point for bad actors seeking to access organizations' valuable data.

## Imperva API Security

Imperva API Security offers full API visibility, automatically discovering API endpoints and assessing risks. It classifies sensitive APIs using call data, displayed in a user-friendly interface, enabling proactive security measures to safeguard at-risk APIs. Teams can enforce policies based on risk assessment without slowing development. Continuous monitoring ensures timely responses to changes, promoting faster, secure software releases. Imperva API Security offers versatile deployment options to meet diverse operational needs available as an add-on to your Cloud WAF or as part of the API Security Anywhere offering.

## API Security Anywhere

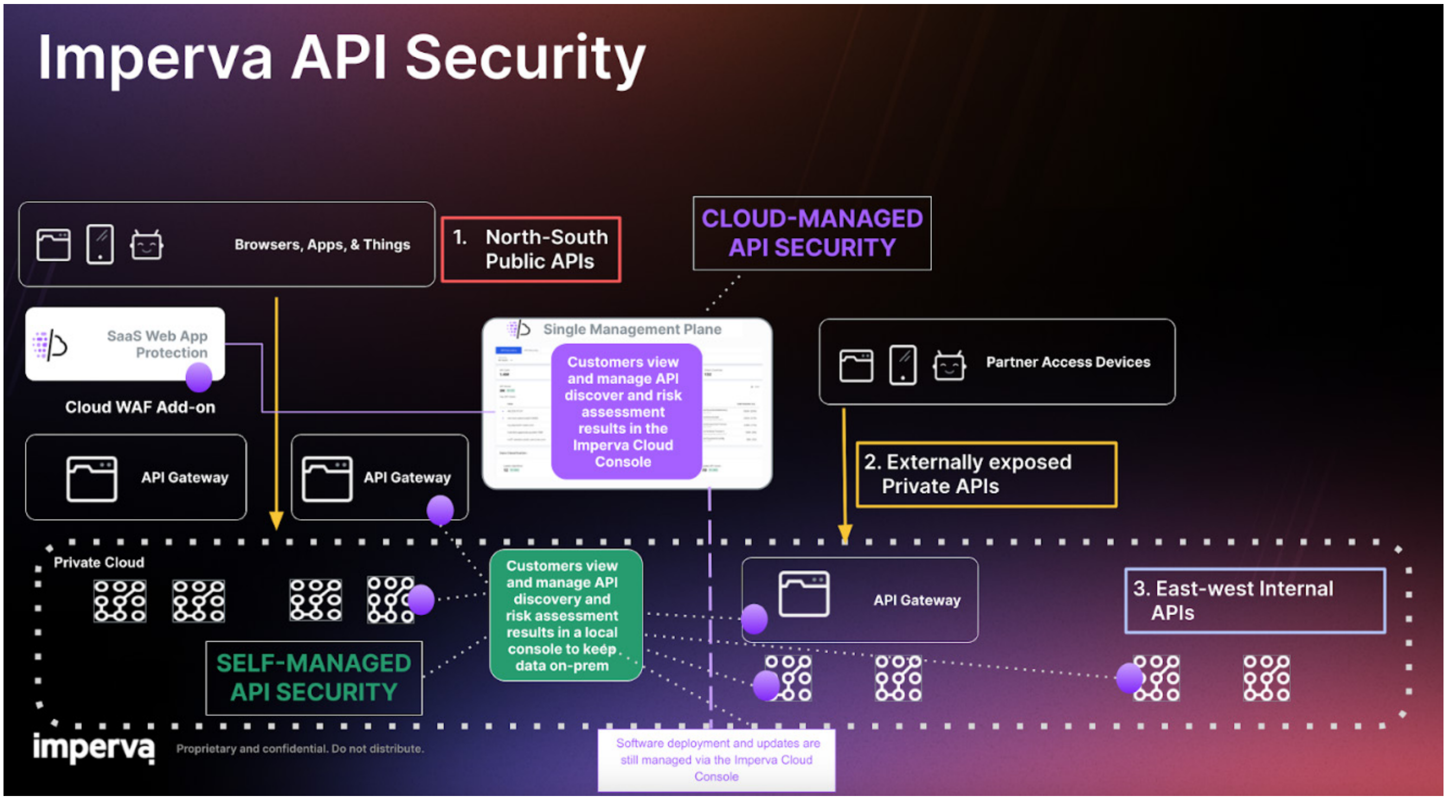
Imperva API Security Anywhere can be deployed across various environments, including other cloud platforms, on-premises, or hybrid setups, and is available in two management options: Cloud-Managed or Self-Managed.

- **Cloud-Managed API Security Anywhere** is administered through the Imperva Cloud WAF management console for customers whose operational environments support integration with external cloud services.
- **Self-Managed API Security Anywhere** is managed via a local console in a controlled environment for customers whose operational environments do not support connection to external clouds.

## Flexible Deployment Options

Imperva API Security offers flexible deployment options for effective API management and security, including

- Integration with leading API Gateways such as Kong, Mulesoft, Azure APIM Gateway, and Apigee for streamlined deployment and management.
- Integration into microservices architecture as a lightweight sidecar sniffer
- Availability as an API Security sensor for inspecting APIs in Kubernetes environments.
- Availability as a standalone network sniffer
- Integration with proxies such as F5



Imperva API Security

Browsers, Apps, & Things
1. North-South Public APIs
CLOUD-MANAGED API SECURITY
SaaS Web App Protection
Cloud WAF Add-on
Single Management Plane
Partner Access Devices
API Gateway
API Gateway
2. Externally exposed Private APIs
Private Cloud
API Gateway
3. East-west Internal APIs
SELF-MANAGED API SECURITY
imperva
Proprietary and confidential. Do not distribute.

Customers view and manage API discover and risk assessment results in the Imperva Cloud Console

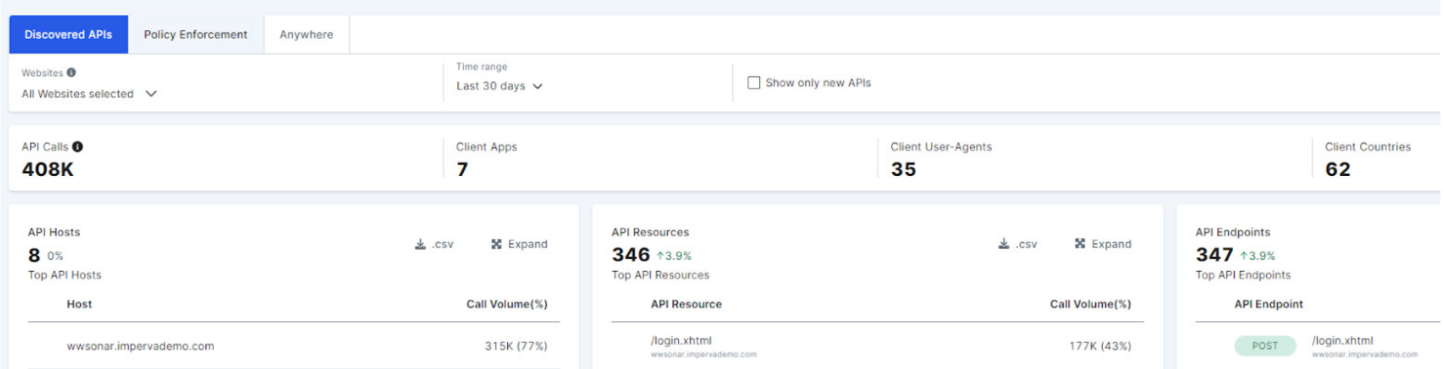
Customers view and manage API discovery and risk assessment results in a local console to keep data on-prem

Software deployment and updates are still managed via the Imperva Cloud Console

# Key Capabilities

## #1 Continuous API Discovery, Classification, and Risk Assessment

Imperva API Security continuously monitors your infrastructure to identify all APIs, including unknown and shadow APIs, to enable data classification and the enforcement of security policies based on risk assessment processes. Continuous monitoring ensures an always-up-to-date API inventory.



Websites: All Websites selected
Time range: Last 30 days
□ Show only new APIs

| API Calls | Client Apps | Client User-Agents | Client Countries |
|---|---|---|---|
| 408K | 7 | 35 | 62 |

API Hosts
8 0%
Top API Hosts

| Host | Call Volume(%) |
|---|---|
| wwsonar.impervademo.com | 315K (77%) |

API Resources
346 ↑3.9%
Top API Resources

| API Resource | Call Volume(%) |
|---|---|
| /login.xhtml<br>wwsonar.impervademo.com | 177K (43%) |

API Endpoints
347 ↑3.9%
Top API Endpoints

| API Endpoint | |
|---|---|
| POST | /login.xhtml<br>wwsonar.impervademo.com |

## #2 Protection Against Business Logic Abuse

API business logic abuse can stem from design flaws or weaknesses within an API exposing your business to attacks and allowing threat actors to manipulate backend processes or access sensitive data undetected. Continuous API Discovery offers contextual insights, including identifying sensitive data transfers and exposing risks related to business logic abuse.

## #3 Integrated Imperva API Security and Advanced Bot Protection

API Discovery identifies APIs that transmit sensitive data or are susceptible to abuse, as determined by API Security classifications. This empowers customers to prioritize API onboarding to ABP at the touch of a button, ensuring that their most critical APIs are protected against malicious automated attacks.

## #4 Protection Against the OWASP Top 10 API Security Risks

Imperva API Security aligns with the OWASP Top 10 API Security Risks, focusing on the six most common threats to minimize the risk of business logic abuse. These include BOLA, BOFLA, and Broken Authentication. The API Security dashboard promptly highlights any detected OWASP API Security risks discovered through API Discovery.

### Key Differentiators:

- Fully integrated with market-leading Imperva Comprehensive Application Security Platform for unparallelled protection
- Combined offering with Imperva Advanced Bot Protection to protect high-risk APIs
- Enhanced protection against the OWASP API Security Top 10 Risks
- Flexible deployment options with unique API Security Anywhere

## #5 API Security within a Comprehensive Application Security Platform

When used alongside Imperva's robust Application Security platform, which encompasses Web Application Firewall (WAF), Distributed Denial of Service (DDoS) Protection, and Advanced Bot Protection (ABP)/Fraud Prevention, Imperva API Security protects against nine out of the OWASP top ten API Security risks. The only exception is the vulnerability associated with Unsafe Consumption of APIs (A10).

## #6 Improved API Security Posture through API Verification Capabilities

Imperva API Security offers advanced API Verification capabilities, including thorough API specification assessment and targeted API fuzzing test generation based on API discovery insights. By utilizing these features, you can comprehensively evaluate your API specifications and create precise fuzzing tests, strengthening your defenses against potential vulnerabilities and fortifying your overall API security posture. existence.

## Learn More:

Contact us at +1.866.926.4678 or visit imperva.com to explore Imperva Application Security solutions.