imperva

THALES CYBERSECURITY

Control your Application Sovereignty with Imperva Cloud WAF

SOLUTION BRIEF

Digital sovereignty adds layers of complexity for global companies. Across the world, 71% of countries have already passed data protection legislation, and a further 9% are drafting it. And in each country or region, regulations are different, and often in conflict. In addition, new regulations and frameworks such as the European Union's DORA and the NIS2 mandate organizations to cover risks related to 3rd party cloud providers. In fact, 83% of organizations globally are concerned that sovereignty or privacy regulations will affect their organization's cloud deployment plans.

While digital sovereignty may be seen primarily as a data governance and security question, there are many aspects that can affect applications and workloads. Specifically, in order to provide essential protection for applications, Cloud Web Application Firewalls (WAFs) must process data that could be subject to sovereignty or privacy regulations.

COULD YOUR WEB APPLICATION FIREWALL BE PLACING YOUR DIGITAL SOVEREIGNTY IN JEOPARDY?

Here are a few questions to ask your Cloud WAF provider:

- Is my Cloud WAF processing network traffic in the correct location based on regulation requirements?
- Can my Cloud WAF enforce jurisdiction-aware access?
- How is my Cloud WAF protecting the privacy of personal data?
- What are the security safeguards for customer data processed by my WAF?
- Is my Cloud WAF certified on the latest standards and regulations?

Control your Application Sovereignty with Imperva Cloud WAF

Imperva Cloud WAF helps organizations achieve digital sovereignty by giving enterprises technical control and enforceable governance over how applications and data are accessed—independent of where the cloud infrastructure or users are located.

Enforce jurisdiction-aware access controls

Imperva Cloud WAF can restrict or allow traffic based on geography, jurisdiction, or regulatory zone, because even if workloads are global, access is governed according to sovereign rules. Block or throttle traffic from countries outside approved regions and enforce regional policies for regulated applications (EU-only, US-only, etc.).

Protect sensitive data flows at the application layer

Digital sovereignty isn't just about storage—it's about runtime behavior. Imperva Cloud WAF can detect and block injection attacks (SQLi, XSS) that expose regulated data, enforce API schemas and payload validation and apply rules to prevent excessive data returned via APIs. This is critical for AI-enabled and API-driven apps, where data leakage can happen without a traditional breach.

Reduce exposure to foreign access attempts

Many sovereignty concerns stem from who can access data, not just where it's stored. Imperva Cloud WAF can prevent unauthorized API calls, scraping, and data exfiltration, shielding applications from automated abuse that could extract sensitive data. It also adds a security control layer that is customer-configured, not provider-controlled.

Enable consistent control across clouds

Enterprises often operate across multiple cloud service providers, including public, private, hybrid, sovereign or national clouds. Imperva Cloud WAF can apply uniform policies across environments, reduce dependency on native cloud controls tied to a single provider and serve as an independent security layer aligned to enterprise governance.

Imperva Cloud WAF Sovereignty, Privacy and Security Controls

Imperva Cloud WAF provides granular sovereignty and privacy controls as well as extensive security safeguards for customer data and compliance commitment.

Sovereignty Controls

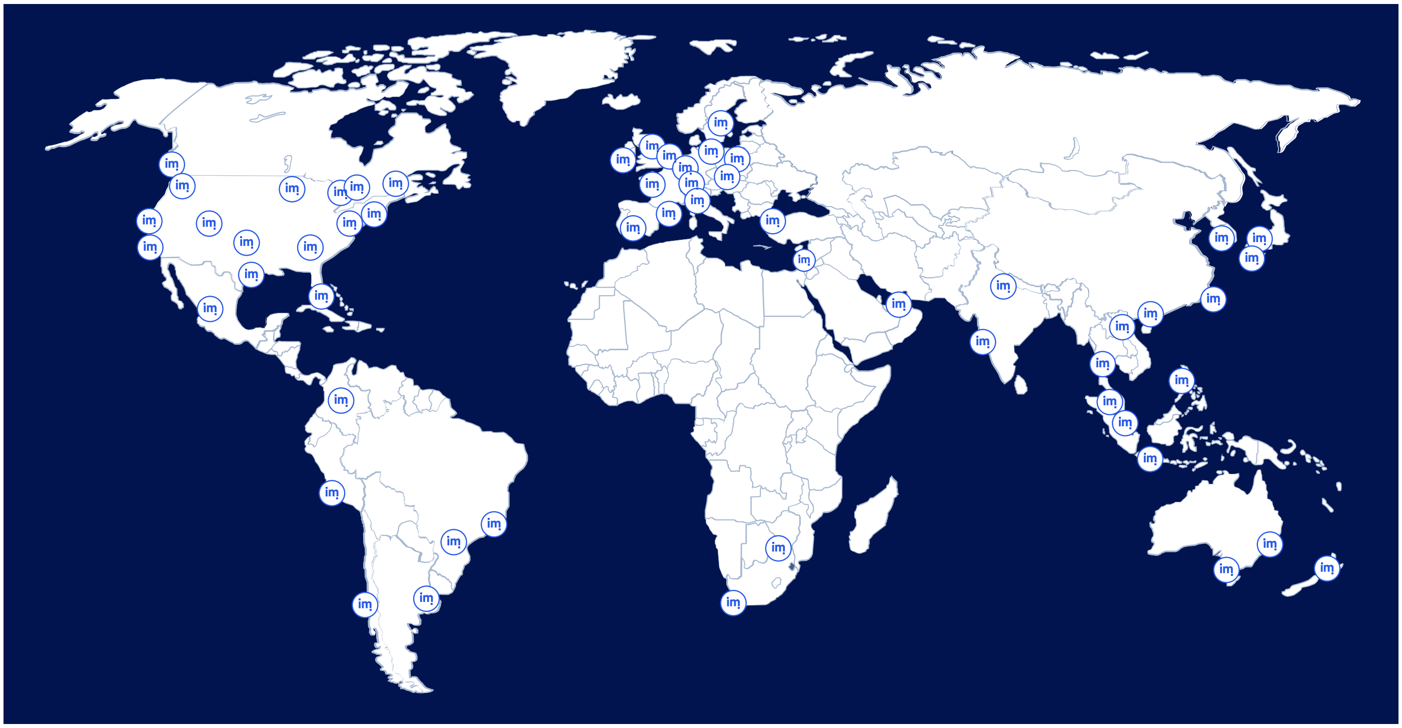
- Imperva Cloud WAF leverages datacenter locations in multiple countries, including 20 in EMEA, 16 in APAC, 24 in the Americas.
- Customers can define network traffic processing location by region or country based on regulation requirements.
- All traffic inspection and enforcement is performed in real time, entirely in-memory, with no customer data stored in our data centers.

Privacy Controls

- All personal data such as names, emails and passwords is automatically masked and not stored.
- Personal data is identified automatically when arriving at Imperva's network.
- Event and statistical data is stored temporarily at regional data center and deleted after 90 days.

Security Safeguards

- All access is logged and continuously monitored.
- Physical, electronic, and procedural security measures safeguard customer data.
- Customer data is only accessible by approved personnel using a multi-layered security interface and MFA.



Cloud WAF leverages datacenter locations in multiple countries, including 20 in EMEA, 16 in APAC, 24 in the Americas.

Compliance Commitment

Thales has a strong commitment to compliance, ensuring Imperva Cloud WAF has all the latest compliance certifications and can help customers achieve their compliance requirements.

Imperva has achieved ISO 27001:2013 certification, as well as SOC 2, Type II certification.

Imperva Cloud WAF is certified as compliant with the PCI DSS 4.0 Service Provider Level 1 standard.

Imperva has obtained GDPR Program Validation from TrustArc and APEC PRP Certification.

About Thales

Thales has extensive experience in helping customers achieve Digital Sovereignty by providing data security & governance, identity & access management and application security solutions to organizations worldwide. As a global leader in cybersecurity, Thales safeguards sensitive data, identities, applications, and software for the most trusted brands in the world. Thales secures cloud environments, defends against cyber threats, ensures compliance, and enables trusted digital experiences.