

MapTiler Security Whitepaper

1. Executive Summary

At MapTiler, security is not a feature; it is a foundational principle. As a leading provider of geospatial data and mapping technology, we recognize that our customers entrust us with their most sensitive location-based assets. This document outlines our multi-layered approach to security, covering our infrastructure, product development, and commitment to data sovereignty.

See also our web pages on Security and Privacy.

- <https://www.maptiler.com/security/>
- <https://www.maptiler.com/privacy-policy/>

2. Our "Privacy-First" Philosophy

Unlike traditional mapping providers, MapTiler's business model is built on software and data licensing rather than advertising.

- **Zero-Tracking:** We do not track end-user activity on our maps.
- **No Spy Code:** Our SDKs and APIs do not contain telemetry designed to harvest user locations for third-party sale.
- **Data Minimization:** We collect only the minimum information required to provide our services (e.g., account management and billing).

3. Infrastructure & Cloud Security

MapTiler Platform is hosted on a highly secure, redundant infrastructure designed for 99.9% availability.

- **Data Residency:**
 - MapTiler ensures high-performance mapping through a distributed, sovereign infrastructure:
 - **Account & Identity Data:** All personal information (emails, account settings) is stored and processed exclusively within the **European Union (France/Ireland)**.
 - **Customer Content & Rendering:** To provide global low-latency processing, customer-uploaded data (tilesets/maps) is processed and stored on dedicated MapTiler infrastructure in **France and Canada**. Canada is recognized by the EU and Switzerland as providing an adequate level of data protection.

- **Global Edge:** We utilize **Cloudflare** for global API key validation and edge caching, ensuring that map delivery is fast regardless of the user's location, while keeping the core data storage within protected regions.
- **Strategic Hosting:** We utilize ISO/IEC 27001 and SOC 2 certified data center providers. While our global base maps are cached via Cloudflare CDN for performance, all customer-specific data layers remain on MapTiler's sovereign infrastructure.
- **Encryption:**
 - **In Transit:** All data sent to and from MapTiler is encrypted using TLS 1.2 or 1.3.
 - **At Rest:** Sensitive customer data is encrypted using industry-standard AES-256 encryption.

4. Product Security Features

Online Mapping Service

We provide developers with the tools to secure their own implementations:

- **Authentication:** Access to APIs is governed by API Keys for client-side use and **Service Tokens** for high-security backend operations.
- **Access Control:** Customers can restrict API keys by **HTTP Referrer** or IP address to prevent unauthorized use of their quotas.

On-Premise Mapping Deployment

For organizations with the most stringent security and compliance mandates (including government, defense, and critical infrastructure), we offer a fully self-hosted solution designed to operate within your private, controlled environment.

1. Air-Gapped Environment Support

MapTiler Server is engineered for environments with **zero internet connectivity**. We provide specialized "Pre-Activated" builds for enterprise customers that do not require online license validation. This ensures that sensitive geospatial data and system metadata never leave your secure perimeter.

2. Complete Data Sovereignty & "Zero-Knowledge"

MapTiler has no access to the data hosted on the customer's server. Whether you are hosting proprietary satellite imagery or sensitive infrastructure layers, the data remains exclusively on your hardware. MapTiler has no technical backdoors, no remote access, and no visibility into the content you host. All liability and control lie entirely with you!

3. Flexible Deployment (Binary & Containerized)

To fit into any enterprise IT stack, MapTiler Server is provided in multiple formats:

- **Native Binaries:** We provide managed packages for **Windows (.exe)**, **macOS (.dmg)**, and Linux distributions, including **Debian-based (.deb)**, **RedHat-based (.rpm)**, and universal **AppImages**.
- **Architecture Agnostic:** We provide native support for both **x86_64** and **ARM64** architectures, allowing for deployment on everything from high-density cloud servers to energy-efficient edge computing devices.
- **Containerization:** A hardened Docker image for seamless integration into orchestration frameworks like Kubernetes, enabling resource isolation and easy scaling.

4. Simplified Administrative Access

Access to the MapTiler Server management console is secured via a local, encrypted administrative password, granting your IT team total control over map styles and tilesets without reliance on external cloud dependencies. To meet advanced enterprise security requirements, we recommend deploying MapTiler Server behind your organization's VPN or a Reverse Proxy (such as Nginx, Apache, or IIS), allowing for seamless integration with your existing authentication and access control layers.

Comparison Table for Online and On-prem

Feature	MapTiler Cloud	MapTiler Server (On-Prem)
Hosting	Secure EU-Cloud (France/Ireland/Canada)	Customer Infrastructure
Internet Req.	Required	For license activation only. (Pre-activated binaries available for Air-Gapped environments)
License Check	Real-time / Online	Pre-Activated / No Outbound Calls
Data Access	Managed by MapTiler	Customer-Only

Maintenance	Automatic Updates	Manual/Controlled Updates
Compliance	GDPR / ISO 27001	Customer-Defined
Resilience	Backups are automated, distributed, and tested	Backups are the customer's responsibility

5. Operational Security (OpSec)

- **Access Management:** We follow the **Principle of Least Privilege (PoLP)**. Access to production environments is strictly limited to authorized personnel and requires Multi-Factor Authentication (MFA).
- **Security Audits:** We perform **regular vulnerability assessments** of our codebase and **continuous scanning of container images** for known CVEs prior to deployment..
- **Employee Training:** All team members undergo mandatory security and privacy training as part of their onboarding and annual review.

6. Compliance & Data Privacy

MapTiler is built to meet the world's most stringent privacy standards:

- **ISO 27001 Certified**
- **GDPR:** We are fully compliant with the General Data Protection Regulation. Since our infrastructure is centered in the EU, we offer superior data sovereignty for European enterprises.
- **PCI-DSS:** All online payments are handled by certified third-party providers (FastSpring, Stripe), ensuring MapTiler never stores or sees your credit card information.
- **Incident Response:** In the event of a security incident, MapTiler commits to notifying affected customers within **72 hours** of discovery.