



Optomate.Net Security Information

Updated 08/01/2025

Security Overview

Our technology stack is secured using a multi-layered approach that leverages Microsoft Identity, Multi-Factor Authentication (MFA), and robust token-based authentication mechanisms. Below are the key components of our security infrastructure:

1. Microsoft Identity and MFA (TOTP)

- We utilize Microsoft Identity for user authentication, ensuring secure access to our applications.
- Multi-Factor Authentication (MFA) is implemented using passkeys through Microsoft Entra ID, providing a secure, passwordless authentication experience. Users verify their identity using biometrics, a PIN, or device-based authentication on trusted devices, reducing the risk of phishing attacks, credential theft, and unauthorised access.

2. Token Authentication Layer

- When making calls to the Optomate.Net database, we employ a token authentication layer that generates a new token for every call and has a lifespan of 3 minutes.
- This ensures tokens are short-lived and reduces the window of opportunity for their misuse.

3. Private Network Hosting

- The application and database are hosted within an Azure virtual private network.
- This setup uses data isolation services to protect your data from malicious access, ensuring that only authorised entities can access the network.

4. Data Hosting and Backup

- Databases are hosted on Australian servers, complying with local data residency requirements.
- We use the Azure Backup Service to ensure that all data is consistently backed up, providing resilience against data loss.

5. Data Encryption

- Data is encrypted at rest and in transit using industry-standard encryption protocols.

- Even if a hacker manages to access and transfer data, they cannot decrypt it without the appropriate encryption keys, ensuring the confidentiality and integrity of your data.

This comprehensive security approach ensures that our technology infrastructure is well-protected against various threats, providing peace of mind for both our users and IT professionals.

If you need further details or have any questions, feel free to [email](#) us.