carbonhalo

Application Security Overview and FAQ

Our application is built with security as a top priority, leveraging cutting-edge technologies and best practices to ensure the protection of your data and the reliability of our services. We utilise a multi-layered security approach, combining the power of Amazon Web Services (AWS) robust infrastructure with Cloudflare's advanced security features.

Key Security Features:

1. **Edge Security with Cloudflare**
    - DDoS protection
    - Web Application Firewall (WAF)
    - Bot mitigation with Bot Management and Turnstile
    - SSL/TLS encryption
2. **Secure Backend Infrastructure**
    - AWS Elastic Container Service with autoscaling
    - Private network isolation
    - Encrypted data storage
3. **Access Control and Authentication**
    - Strict access controls
    - Private endpoints
    - IP allow list for sensitive areas
4. **Data Protection**
    - Encryption in transit and at rest
    - Secure cloud object storage
    - Regular backups

Frequently Asked Questions (FAQ)

Q1: How is my data protected when I use your application?

Your data is protected through multiple layers of security:

- All data in transit is encrypted using HTTPS.
- Data at rest is encrypted in our databases and cloud storage.
- Our backend DB service is isolated in a private network, not accessible from the public internet.
- We use Cloudflare's security features to protect against various cyber threats.

Q2: What measures do you take to prevent unauthorised access to my information?

We implement strict access controls:

- Our database is only accessible through private endpoints or a secure jumpbox with whitelisted IP addresses.
- We use role-based access control (RBAC) to ensure only authorised personnel can access sensitive systems.
- All access attempts are logged and monitored for suspicious activity.

carbonhalo

Q3: How do you protect against DDoS attacks?

We use Cloudflare's robust DDoS protection:

- Cloudflare's global network can absorb and mitigate large-scale DDoS attacks.
- We implement rate limiting to prevent excessive requests from overwhelming our systems.
- Our autoscaling infrastructure can handle sudden spikes in legitimate traffic.

Q4: Do you use HTTPS for all communications?

Yes, we enforce HTTPS for all communications:

- All traffic between users and our application is encrypted using SSL/TLS.
- We also use HTTPS for communication between our services internally.

Q5: How do you prevent bot attacks or automated abuse of the system?

We utilise Cloudflare's advanced bot protection features:

- Cloudflare Bot Management uses machine learning to identify and mitigate bot traffic in real-time, detecting and blocking even sophisticated bots that mimic human behaviour.
- Cloudflare Turnstile provides non-intrusive bot detection without traditional CAPTCHAs, improving user experience while maintaining strong security.

Q6: Is my data backed up? How often?

Yes, we regularly back up all data:

- Our MongoDB databases are backed up daily.
- All backups are encrypted to ensure data protection.
- We have procedures in place for quick data recovery if needed.

Q7: How do you ensure the privacy of my data?

We take data privacy seriously:

- Your data is stored in secure, encrypted databases.
- We use private cloud storage with no public access.
- Our systems are designed with privacy in mind, following principles like data minimisation.

Q8: Do you comply with data protection regulations?

Yes, our security measures are designed to ensure compliance with relevant data protection regulations:

- We adhere to Australian privacy regulations, including the Privacy Act 1988 and the Australian Privacy Principles (APPs).
- Our systems and practices are also aligned with the General Data Protection Regulation (GDPR) to protect the rights of EU citizens and residents.
- We implement encryption, access controls, and secure communication channels to meet these regulatory requirements.

carbonhalo

Q9: Can you explain how you use Cloudflare to enhance security?

Cloudflare provides multiple security enhancements:

- DNS protection against attacks and cache poisoning
- Web Application Firewall (WAF) to filter malicious traffic
- Bot Management and Turnstile for bot protection
- SSL/TLS management for encrypted communications
- DDoS mitigation at the network and application layers

Q10: How do you ensure the security of your backend infrastructure?

Our backend is secured through several measures:

- We use AWS Elastic Container Service, which provides secure, scalable infrastructure.
- Our databases and storage are isolated in private networks.
- We implement strict access controls and encryption for all backend services.

Q11: What should I do if I suspect a security issue?

If you suspect a security issue:

- Contact our support team immediately through our secure channels.
- Do not share sensitive information about the suspected issue in public forums.
- Our security team will investigate promptly and provide updates as appropriate.

Q12: How do you address data sovereignty concerns?

We take data sovereignty seriously and have implemented the following measures:

- Primary Infrastructure: All our core infrastructure, processing, and data storage is hosted in the Amazon Web Services Sydney data centre. This ensures that your primary data remains within Australian borders.
- Cloudflare Processing: We use Cloudflare for edge security and performance optimisation. Cloudflare operates a global network and may process requests at various points of presence (PoPs) for optimal performance. However, this processing is transient and does not involve storing your data.
    - Cloudflare's network includes several PoPs in Australia (including Sydney, Melbourne, Brisbane, and Perth), which means that for many Australian users, request processing likely occurs within the country.
    - For users accessing from other countries, Cloudflare may process requests at the nearest global PoP to optimise performance.
- Data Storage: All persistent data storage and core application processing occur exclusively in the Amazon Web Services Sydney data centre.
- Compliance: Our setup is designed to comply with Australian data sovereignty requirements while also providing the performance benefits of a global edge network.
- Transparency: We're committed to being transparent about our data handling practices. If you have specific data sovereignty requirements, please contact our support team to discuss how we can address your needs.

We are committed to maintaining the highest standards of security and continuously improving our measures to protect your data and ensure the reliability of our services. If you have any additional questions or concerns about our security practices, please don't hesitate to contact our support team.