Systems infrastructure and data security

Security is the foundation of our systems and technology. Systems infrastructure security requires a holistic approach to ongoing processes and practices to ensure that the underlying infrastructure and data therein remain protected. We take a measured, proactive approach to ensure our security is reliable and scalable.

There are three core components to our technology stack which remain under constant evaluation to ensure only those authorised to view or amend critical data have access to them.

The components

The following outlines the three core components and the security measures and considerations contained within each.

Customer and admin dashboards:

- Customer has option for Two-factor (SMS or using authenticator e.g., Authy)
- Two-factor is compulsory on admin dashboard
- Brute force login – logging throttling protection
- Google reCAPTCHA
- Cloudflare additional login (admin only)
- Use of Cloudflare content delivery network to increase security and optimisation (DDOS attacks, caching, loading time)

Development Framework

- Using latest version of Laravel;
- Using latest version of PHP
- Sanctum authentication system
- CSRF (Cross-Site Request Forgery) tokens
- Protection against XSS (Cross Site Scripting)
- SQL Injection
- Centralised API that communicates with all third-party systems and in-house modules

Data

- Using Digital Ocean servers and infrastructure
- Encrypting sensitive information
- Daily backups
- Limited access (IP address) configured with Digital Ocean
- Logging all activities, logins, and changes made in the customer and admin dashboards