BeeCastle Security Whitepaper

Introduction

Security is paramount at BeeCastle, and we have worked very hard to ensure that your data is secure. Protection of our customers vital contact and interaction data is a top priority and this paper outlines the technical controls we have in place to ensure your data is safe.

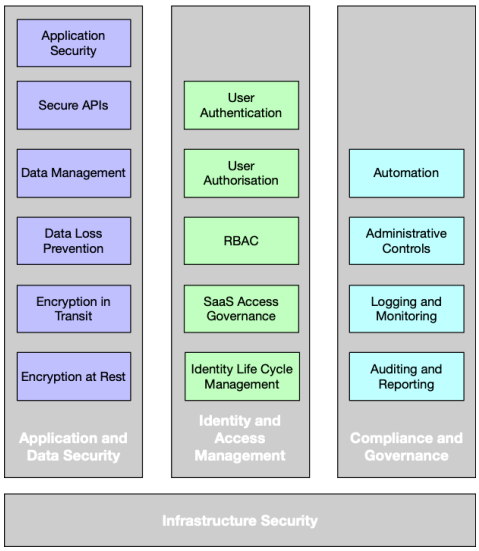
Shared Responsibility Model

Security is a shared responsibility between BeeCastle and the customer. Each party is responsible for different elements to keep the system secure and data safe. Specifically, the BeeCastle team is responsible for the application and data security, identity and access management, and compliance and governance. The customer and its users are responsible for not disclosing passwords or authentication keys/token and keeping user accounts up to date.

A further breakdown of the BeeCastle responsibilities and how we enforce those responsibilities is included below.

Security Reference Architecture

BeeCastle views technical application security through four main lenses: Application and Data Security, Identity and Access Management, Compliance and Governance, and Infrastructure Security.



Application and Data Security

Application and Data Security covers management of data and application services, to keep data secure and safe while in transmission, application processing, and storage/at-rest.

All inbound and outbound data from the BeeCastle system is transmitted over secure encrypted links, typically HTTPS for user-initiated actions such as data retrieval or submission from the web or mobile applications, or via TLS/SSL for system-system connections such as database connections.

The application and APIs are secured via strong access checks, and system-enforced query segregation, ensuring data for across different organisations accounts cannot be queried.

BeeCastle stores every request to alter data in an event log. This log ensures that all data changes are tracked at a user level and can be audited/recovered if needed.

Data stored within BeeCastle is encrypted-at-rest. This ensures that in the event of a physical attack on a data centre, theft of a disk would not result in data being readable.

Identity and Access Management

Identity and Access Management covers ensuring that users only read and alter data that they are allowed to, as defined by their role within the BeeCastle system. All access to the web application, mobile applications, or system APIs are subject to the same authentication and authorisation controls, ensuring uniform application of user access rules.

Compliance and Governance

Compliance and Governance covers BeeCastle internal processes and procedures to ensure the BeeCastle application and data is secure and kept secure.

Changes to the application and processing logic are reviewed in line with industry best-practice code review and management processes. Deployments of changes are automated, reducing the human risk factor of deployment failure, or introduction of changes post-review.

Access to the backend services are provided internally on an as-needs basis. Only technical staff with specific responsibility for system maintenance have access to the backend services. These controls are enforced with user/account policies on a role and function basis by our infrastructure partners (AWS, Google).

Changes to our infrastructure services are tracked and audited with monitoring services provided by our infrastructure partners.

All inbound requests to the BeeCastle application and APIs are monitored, tracked, and logged, with date/time, IP address, and the request made.

Infrastructure Security

Infrastructure Security is provided by our infrastructure Partners, Amazon/AWS and Google. They are responsible for security of the cloud, and we are responsible for security within the cloud.

More information on Infrastructure Security can be viewed at the links below:

- https://aws.amazon.com/compliance/shared-responsibility-model/
- https://cloud.google.com/security/overview/whitepaper

Further Information

If you require further information or wish to have a discussion with a BeeCastle team member about any of the topics raised in this paper, please get in touch at help@beecastle.com