DOORDECK SECURITY OVERVIEW

MISSION STATEMENT

With Doordeck, security is our main concern. Doordeck was built from the ground up using the core principles of Information Security, also known as the CIA triad:

Confidentiality
Prevent the disclosure of information to unauthorized individuals or systems.

Integrity
Maintain and assure the accuracy and consistency of data over its entire lifecycle.

Availability
Ensure the information is available when needed.

Doordeck is committed to achieving and maintaining these principles and the trust of our customers. Integral to this is providing a robust security and privacy program that carefully considers data protection matters across our suite of services where applicable.

Architecture
All sensitive data at rest is encrypted with AES256. All data being transmitted is protected using HTTPS with TLS.

Doordeck server based hardware and control software is hosted at third-party facilities ("data centres") managed Amazon – known as Amazon Web Services (AWS). Prior to selection, the facility was subjected to a stringent assessment for the presence, implementation, and ongoing administration of physical security controls. All our infrastructure sits in a virtual private cloud

Our EC2 instances are separated into different security groups with restricted policies. Instances do not have direct internet access rather access is done by elastic load balancer

Doordeck Cloud Security Procedures
All of Doordeck's cloud infrastructure is hosted in Amazon Web Services (AWS).
Access to cloud infrastructure is restricted to senior developers.
Cloud management is conducted via an audited bastian server, with communication being protected with a VPN.

Each facility is fully protected 24x7x365 by security guards, high-security fencing, and video cameras. Facilities have an annual audit by industry-leading firms for ISO 27001 and/or SSAE 16 Type II compliance in addition to many other certifications as seen on the following diagram 1.

SECURITY LOGS
All systems (for example, firewalls, routers, network switches, and operating systems) used in the provision of the Doordeck systems provision and access systems will log information to their respective system log facility and to a centralized syslog server.

All data access by customer and staff is monitored and logged.
All data changes by customer and staff are monitored and logged.
Logging will be kept for a minimum of 365 days.
Logging will be kept in a secure area to prevent tampering.

System Maintenance
Maintenance is carried out during non-business hours, typically weekdays 7pm onwards or weekends and bank holidays. Maintenance windows are used for new version releases, typically every 2-4 weeks. These releases follow a very strict change management process.

Change Management
Doordeck follows fully documented change management procedures for all tiers of the service covering application, operating system, server, and network layers.

All configuration changes are tracked and managed through a written ticketing system.

Deletion of Customer Data
Upon contract termination, customer data held by DoorDeck will be retained for a period of 30 days and is retained in "inactive status" within DoorDeck for 30 days and a transition period of up to an additional 30 days, after which it is overwritten or deleted. DoorDeck reserves the right to reduce the number of days it retains such data after contract termination. This process is subject to applicable
Legal and/or contract requirements.

Event Management
Doordeck maintains event management policies and procedures.

Hardware and software security information
Hardware

- Each controller has a unique 2048-bit RSA key generated at manufacturing time.
- Operating system image is built internally to ensure audibility.
- Controllers do not accept incoming TCP/UDP connections (No open ports on controllers).
- Controllers use private keys to connect to cloud infrastructure with TLS 1.2 & strong cipher suite.
- Controllers store a list of permitted user's public keys so they may independently verify requests.
- Local console access is denied.

Cloud
Cloud management is conducted in the following way:

- All changes are code reviewed.
- Software is signed with digital signatures.
- Access to code repository is controlled via ACL (Access Control List).
- Unit testing.
- Changes are deployed to staging first.
- Done with automation tools.
- Tested internally.
- When it's ready, code is promoted to production.
- All access is via TLS & strong encryption.

AWS Security overview: https://aws.amazon.com/security/

Secure Communication Protocols:
The following processes are implemented:

- Each user has a private key.
- Private keys are stored encrypted on the cloud using AES 256 with a key derived from the users password.
- Passwords hashes are stored in the cloud using PBKDF2 tuned to take 100 millisecond per computation to prevent brute forcing.
- Password hashes are generated using a salt and pepper.
- Requests to interact with the controllers are digitally signed using the user's private key and verified on the cloud and on the controller.

How the Doordeck application works:
A general breakdown of the application security protocols:

- A user generates a request using their key.
- Request is sent to the cloud
- The cloud verifies the request
- Cloud forwards request to the controller
- Controller verifies request again
- 2 step verification process means that if the cloud server was ever compromised, an attacker cannot unlock your controlled door
- Only port open is port 22, but it's heavily locked down