January 2022

Doorway security Whitepaper

Introduction

At Doorway, we know how important security should be when considering our future success. Our product is focused on handling sensitive contact information for companies - from small local businesses to large multinational organisations with well-known brands - but no matter the size of our customer we take security and privacy standards to the highest degree when making business decisions; our future success depends on it.

Contents

Security at our core

Doorway's Digital Business Cards run on a technology platform that is conceived, designed and built to operate securely.

Data Security (Data-at-Rest Security)

Doorway makes multiple investments to ensure our customers' data is secure and available. Physically, Apple pass files and organisation assets are stored in AWS' S3 storage service. Access to S3, even within AWS, requires encryption, providing additional insurance that the data is also transferred securely. For Google passes we connect to Google's Cloud services via API, more information about their security practices can be found here: https://cloud.google.com/security/overview/whitepaper

Within AWS S3, we restrict access to non-public files at both the bucket and object level, and only permit authenticated access by the bucket and/or object creator—Doorway.

As of writing Doorway utilises Heroku as their primary hosting platform. More information about their security can be found here: https://www.heroku.com/policy/security

Securing Data in Transit

Data is vulnerable to unauthorised access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for Doorway. The Doorway Front End supports strong encryption protocols such as TLS to secure the connections between customer devices and Doorway's web services and APIs.

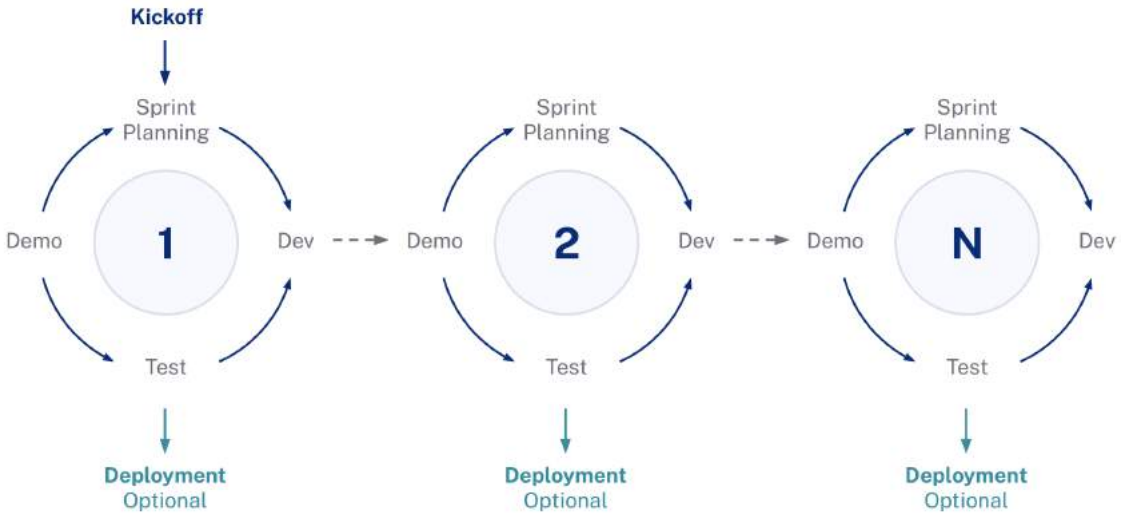
Development Practices

Doorway continuously instructs its developers on secure development practices. The continuous instruction & discussion helps to ensure developers will provide adequate protection for the various types of potential attacks are identified, such as:

- Malformed input
- SQL injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Other Open Web Application Security Top 10 threats (OWASP's Top 10).

Software Development Lifecyle

The Doorway software development lifecycle uses an iterative approach to development by leveraging the Agile/Scrum framework:



The iterative approach concentrates on producing frequent new versions of the software in incremental, short cycles. The process loops round with each of the stages being carried out many times in small iterations (in the Agile method these are called “Sprints”).

This results in small incremental releases with each release building on previous functionality. Each release is thoroughly tested to ensure software quality is maintained.

In Agile, development testing is performed in the same iteration as programming.

Doorway incorporates security into various stages within the Software Development Lifecycle.

Certifications

SOC 2

In order to give further proof of our commitment to the highest Security Standards, we’ve decided to pursue the SOC 2 Certification. With this, an independent third party assessor will be auditing our security and privacy standards based on international standards. We hope, by pursuing this certification, we’re able to give further proof of our continued efforts to maintain our promised culture around systems security.

As an update to our progress towards this certification (as of February 2022), we’re making significant progress to achieve our Type 1 Certification this calendar year and are streamlining our efforts by engaging Compliance Automation software services. We also are looking forward to achieving our Type 2 Certifcation, with the assessment for this involving a continuous security monitoring window of 5 months. Progress updates are available, for enterprise customers, upon request.

Data usage

Our philosophy

Doorway customers own their data, not Doorway. The data that customers put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. Doorway will not process data for any purpose other than to fulfill our contractual obligations. Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days.

Administrative access

Only a small group of Doorway employees have access to customer data. For Doorway employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Doorway employees are only granted a limited set of default permissions to access company resources.

For customer administrators

Within customer organisations, administrative roles are designated by the project owner. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and data.

Conclusion

The protection of your data is a primary design consideration for all of Doorway's infrastructure, products and personnel operations. Ensuring that our solution provides the highest degree of security and privacy is paramount and this will always be reflected in our efforts.

For these reasons and more, Doorway is proud to be the Digital Business Card provider to companies the world over.

We are, of course, always looking to improve our standards and so are very welcome to all feedback / requests from our customers.

Please share your feedback on the following link and we'll get back to you ASAP.

https://www.getdoorway.com/privacy-and-security-feedback