Boardingware: Technical Overview

Refer to the link below for the latest version of this document:

https://s3.amazonaws.com/boardingware/compliance/Boardingware+Technical+Overview+(A4).pdf

© Boardingware International Limited, 2017. All rights reserved.

TABLE OF CONTENTS

© Boardingware International Limited, 2017. All rights reserved.

HOSTING ENVIRONMENT

Boardingware servers are located within enterprise-grade hosting facilities provided by Amazon Web Services (AWS). AWS is the world's leading cloud infrastructure provider, operating 32 separate physically separate data center facilities across 12 geographic regions around the world. All data center facilities include the following features to maximize availability and security:

Robust physical security controls to prevent physical access to servers
24/7/365 monitoring and surveillance by on-site security staff and regular ongoing security audits
Fully redundant electrical power system
Backup generators for entire facility in case of electrical failure
Redundant network access points, housed in separate facilities

AWS takes all commercially reasonable efforts to maintain a Monthly Uptime Percentage of at least 99.95%, and continually manages risk, undergoing regular assessments to ensure compliance with industry standards. The IT infrastructure that AWS provides is designed and managed in alignment with security best practices and a variety of industry standards, including:

SOC 1 / SSAE 16/ ISAE 3402

SOC 2, SOC 3

ISO 9001 / ISO 27001

FISMA

PCI

Access to the management console is strictly maintained using granular permissions and Multi-Factor Authentication for staff within Boardingware, along with IP based access control.

For more detailed information visit:

http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

TECHNICAL CONFIGURATION

© Boardingware International Limited, 2017. All rights reserved.

Boardingware has servers located in three of the AWS regions to create a global service:

North America - Northern Virginia, U.S.A.

Europe - Ireland

Asia Pacific - Sydney, Australia

This has the benefit of reducing latency between the client and server and allows our customers to store their data in compliance with their country's data sovereignty laws.

Within each independent region exists a Virtual Private Cloud (VPC). The VPC is designed to encapsulate all servers within a region and provide network routing and security. A three tier server architecture approach is used, separating the application logic in the API servers from the web and database servers. Current server configurations are as follows:

Application (API) and Web Server

Ubuntu virtual machines with 2 vCPU (virtual) and 8GiB memory running on Intel Xeon E5-2676 v3 Haswell processors with a 2.4GHz base frequency. Both application and web servers supply a RESTful API built in a Node.js environment. Communication with the API servers is implemented using the Secure Websocket Protocol (WSS).

Database Servers

Using same spec machines as the application and web servers, the database servers run a MySQL v5.6 Database Engine.

Network Protection

Boardingware takes a "defense in depth" approach to protecting our system and customer data. Multiple layers of security controls, including security group firewalls, routers and Access Control Lists are implemented according to industry best practice and AWS recommendations. By partnering with certified cloud consultants, we are able to leverage their expertise to ensure our security with regular reviews of our systems.

Data Encryption

All data transferred between the client and Boardingware is encrypted using industry standard TLS (Transport Layer Security). Any non-secure requests are automatically redirected to the secure port. Data is also encrypted while at rest when stored on our servers.

Disaster Recovery and Readiness

To ensure availability of the service, Boardingware servers and databases are distributed between the geographically diverse facilities. Along with performing real time data replication, this ensures

© Boardingware International Limited, 2017. All rights reserved.

that in the unlikely event of an entire data center facility failure, we are able to quickly switch over to our back up and keep the service running. Daily, encrypted, backups of databases are performed and kept for a 7 day period in case of loss of data.

To ensure readiness in the event of an incident, a regularly updated Incident Response Plan is in place to quickly and efficiently remediate the situation. Continuous automated monitoring is carried out with alarms in place to detect potential service interruption.

Authentication and Authorization

All client interface access into Boardingware requires authentication through username and password, with access being revoked after a preset timeout. The ability to implement Multi-Factor Authentication can be provided using a “Virtual MFA Device”, e.g. a smart phone, to input a randomly generated number upon login.

Authorization is controlled through user type permissions (Staff, Parent, Student) at its highest level. More granular permissions for staff are available to be set through the application itself. All permission controls and implemented on the API server.

Integrations

Boardingware has a number of integrations with popular student managment systems is continually increasing its number of partnerships with SIS’s. Custom integrations are also possible with our flexible RESTful API, as we are able to integrate with most web based technologies available, whether it be an event driven or a request driven model.

Portability / Interoperability

In the event of a request by a customer to move their data, Boardingware is able to export the data into an SQL file or a converted format if deemed reasonable.

TECHNICAL REQUIREMENTS

Mobile devices:

- iPad 2 or higher
- IOS 8.0 or higher

© Boardingware International Limited, 2017. All rights reserved.

Internet Browsers:

Ensure that browsers allow cookies and Javascript is enabled.

- Chrome: 40.0+
- Internet Explorer: 10.0+
- Firefox: 40.0+
- Safari: 6.0+
- Android Internet Browser: 4.4+

Internet connection:

School firewall needs to allow access to Boardingware's API and UI domains:

US / Canada

- api-virginia.boardingware.com (HTTPS / WSS)
- app.boardingware.com (HTTPS)

Asia Pacific

- api-sydney.boardingware.com (HTTPS / WSS)
- app.boardingware.com (HTTPS)

Europe

- api-ireland.boardingware.com (HTTPS / WSS)
- app.boardingware.com (HTTPS)

API URLs depends on which region the school is located in.

CONTACTS

Any questions relating to this Technical Overview should be sent to:

support@boardingware.com

MORE INFOFORMATION

© Boardingware International Limited, 2017. All rights reserved.

For more information plese refer to our security whitepaper:

https://s3.amazonaws.com/boardingware/compliance/Boardingware+Security+Whitepaper+(Letter).pdf

© Boardingware International Limited, 2017. All rights reserved.