Boardingware

Cloud Security Overview

TECHNICAL WHITEPAPER

LAST UPDATED: May 1, 2018 11:18 AM

Contents

Introduction

Boardingware provides a SaaS (Software as a Service) for schools to keep track of their students activity online. Traditionally schools have had to rely on manual systems like pen and paper or on-site IT systems to manage their students and the concept of using a cloud service to manage sensitive student information presents major concerns over data security.

At Boardingware, we understand the importance of data privacy and security and take our role in processing and handling personal information very seriously. We pride ourselves on being a trusted partner to our schools and are fully-committed to ensuring the Boardingware service is aligned with international standards for cloud security and data protection.

This document describes Boardingware's procedures and responsibilities for ensuring the protection of customer information in the cloud. It includes roles and responsibilities, AWS security practices, Boardingware security practices and customer security practices.

Point of Contact Regarding Security

Boardingware has an assigned CISO (Chief Information Security Officer). We encourage our customers and end users to contact our CISO if they require more information about our security practices or if they wish to report a security event.

CISO: Mario Blazevic
Email: security@boardingware.com

Shared responsibility model in the cloud

Data protection obligations are the same whether data is stored on-site or in the cloud. However, security methods in the cloud are slightly different to traditional on-site methods where the installer or customer is solely responsible for the security of the on-site resources. SaaS companies like Boardingware often adopt a shared responsibility model with IaaS (Infrastructure as a Service) providers like AWS (Amazon Web Services).

IaaS companies provide highly scalable and available global infrastructure such as servers, databases and networking services. This gives SaaS companies access to unlimited cloud resources and also improves their default cloud security posture. This model also provides cost efficient availability and security benefits to SaaS companies and their customers.

Essentially, the shared responsibility model incorporates new security methods that can be effectively managed when all layers of the service comply with industry standard best practices.

AWS Responsibilities

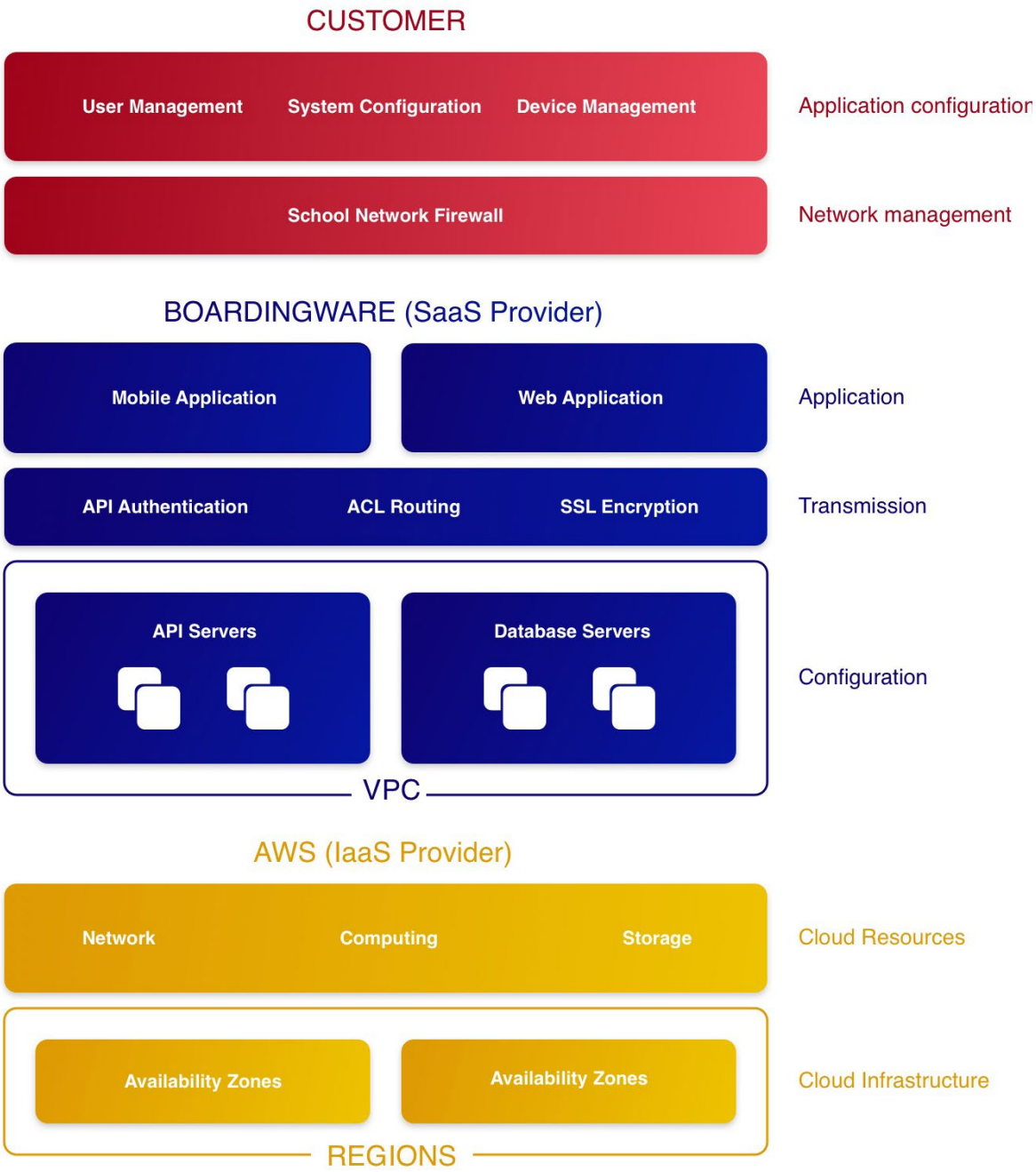
AWS is responsible for protecting all the global infrastructure that it provides to the SaaS company. This is comprised of hardware, software, networking and facilities that run AWS services.

Boardingware Responsibilities

As the SaaS provider Boardingware is responsible for the configuration within the cloud. This includes customer data, hosted applications, firewall configuration and network traffic protection.

Customer Responsibilities

Boardingware customers are responsible for the configuration and use of Boardingware in their school. This includes account management, system configuration and the management of public devices used for Boardingware.



AWS Cloud Security

Boardingware has partnered with AWS (Amazon Web Services) as our chosen cloud infrastructure provider. This partnership has given Boardingware the ability to securely configure and monitor our cloud architecture in compliance with our data protection obligations and industry best practices. This section summarizes AWS's security practices at a high level to convey their proficiency as an IaaS provider.

Compliance

The IT infrastructure that AWS provides to SaaS companies are designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001/ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

In addition, the flexibility and control provided by the AWS platform allows customers to deploy solutions that meet several industry-specific standards, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulations (GDPR)

More information on AWS's compliance programs can be found at:

https://aws.amazon.com/compliance/programs/

On-site Security

AWS data centers are state of the art and are housed in non-descript facilities. Physical access is strictly controlled both at the perimeter and at the building ingress points by professional security staff utilizing CCTV and intrusion detection systems. All physical access to data centers are logged and audited routinely. Data centers have advanced fire, power, climate and infrastructure management systems.

Availability

AWS has clusters of data centers within specific countries which they refer to as 'Regions'. Within each geographical region there are multiple availability zones. This gives software companies like Boardingware the ability to architect applications that can move customer data and traffic away from any affected availability zones in the event of a failure. This allows SaaS companies to remain resilient in the face of most failure incidents, including natural disasters. Availability zones can also be used for load balancing so spikes in traffic can be spread across multiple zones to prevent server crashes.

Managed Services

In addition to protecting the global infrastructure, AWS is responsible for the security configuration of it's products that are considered managed services. These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed

by AWS. For these services, AWS will handle basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery. An example of a managed service that Boardingware takes advantage of is the Amazon Relational Database Service (RDS).

More Information

More information on AWS's security practices can be found at:

https://aws.amazon.com/security/security-resources/

Boardingware Cloud Security

As a SaaS provider, Boardingware is responsible for the secure configuration of cloud resources and the protection of customer information in the cloud. This section describes the technical and organisational practices Boardingware employs to achieve these objectives.

Secure Cloud Configuration and Procedures:

Management of Secret Authentication

Boardingware users authenticate against our API with a secure username and password. Passwords must have a minimum of 6 characters and can have up to 128 characters including special characters and are encrypted with an 11 factor cryptographic hash function upon creation. Authentication is processed on server side and returns a token over a SSL connection. Tokens are encrypted with 256 bit entropy and is signed with a RSA signature.

Authorization

All requests to the Boardingware API are authorized individually meaning user credentials must be authenticated each time data is accessed. Tokens are authenticated on the API level of which access is determined by server side policies and ACPs (Access Control Policies).

Multi-regional Cloud Architecture

Boardingware has architected its cloud infrastructure to support multi-national data storage. This allows Boardingware customers to store their school data in the country that best suits their data protection regulations. Boardingware has set up application and database servers in multiple AWS regions.

The available regions are:

- Northern America (Virginia): 5 availability zones
- Europe (Ireland): 3 availability zones
- Asia Pacific (Sydney): 3 availability zones

Schools can choose to save their data in any one of these three regions. All data relating to the school, including data generated from users accessing the service elsewhere in the world will be stored in the school's chosen geographical region. This can help schools comply with each of their countries data sovereignty regulations which may discourage them from storing data outside their country or economic zone.

Availability

Boardingware's cloud services are designed to provide our customers with a minimum of 99.95% monthly uptime.

The use of multi-regional architecture allows global traffic to be divided by each region reducing the risk of a global service interruption. This also allows for scheduled maintenance to occur at the lowest traffic times for each region.

Multiple Availability Zones are assigned within each Region. Identical VPC environments are replicated within each availability zone. Traffic can be directed to healthy Availability Zones in the event of failure. This protects against disaster incidents within a Region which may affect one or more availability zones. Load balancers are also used to spread traffic across multiple availability zones reducing individual server loads.

Boardingware's native iPad application supports an offline mode so if the connection to the service is interrupted, staff users and kiosks can still operate while saving data locally to the device. Once the application reconnects to the service all data will be synced and updated.

System Change Control

Boardingware has put in place appropriate change control procedures for all technical staff to follow and to record changes to the Boardingware service and other changes to software packages. Any changes that may adversely affect customers will be communicated clearly by Boardingware, including:

- Categories of change
- Planned data and time of change
- Technical description of the changes
- Notification at the start and completion of changes

Segregation of Cloud Tenants

Boardingware supports it's customers within each Region in a multi-tenancy environment. This means customers within the same Region share cloud resources including databases and servers. Boardingware has put in place robust safeguards to prevent customers from gaining access to unauthorised data.

Data segregation is enforced on multiple levels within the application. Once a user is authenticated granular server side ACPs (Access Control Policies) define which API calls a user can access based on their school, user type and any other system permissions set by the school. Further conditional operations check user's credentials every time they make a request to the API. This ensures users can only make requests to data they are authorised to access and any attempts to access unauthorised data will be forbidden. This protects against unauthorised API requests to the database.

Actions such as delete, create and update are also restricted by ACPs so users cannot create or modify data they are not authorised to. These actions are checked against the user's credentials every time a request is made and any unauthorised requests will fail. This means users can only create and modify data within their own school and user access level.

On the UI (User Interface), all resources which are sent to the users are obfuscated. This impedes the users' ability to reverse-engineer the application or parts of the application. To see what other interface of other account types looks. For example a student will not be able to view the parent or staff app.

Secure VPC Environment

Boardingware takes a 'defense in depth' approach and has provisioned an Amazon Virtual Private Cloud (Amazon VPC) within each Region with multiple layers of security controls. Within the VPC a range of private (RFC 1918) IP addresses are assigned to create an isolated network within the AWS cloud which is separate from all other Amazon VPCs. This VPC is similar to a traditional network but operates completely within the cloud.

Within each VPC we have defined public and private subnets. Subnets are a range of IP addresses within our VPC that we can use to specify which services should be launched in a private or public network. Public subnets can connect to the Internet whereas private

subnets cannot. Boardingware has only launched resources that need to be connected to the Internet like the API server within a public subnet and has contained resources that don't need to be connected to the Internet like the database server within a private subnet. Data transferred between resources in the public subnet is secured with SSL encryption and the connection between the public and private subnet is secured with VPC Security Group firewalls.

VPC Security Groups allow Boardingware to control both ingress and egress traffic between the public and private subnet. ACLs are also used to add a further layer of security between subnets within the VPC. The use of ACLs and Security Groups allows traffic to be restricted by IP protocol, Port as a well as source and destination IP address within the VPC.

All incoming requests to the API go through an Elastic Load Balancer which redirects any unencrypted requests to the encrypted port (port 443).

Secure Backup Management:

Backup Requirements

Boardingware has a Backup Policy in place which defines the backup requirements of information. Our customer information hosted on our Production Databases are classified as high criticality. The requirements for highly critical information are:

- Backups are required for all databases for all regions
- Full backup completed weekly
- Differential backups completed daily
- Backups are encrypted
- Ready available replica for automatic failover

Backup Locations

Backups of databases are stored within their respective Regions across multiple Availability Zones. This means backups of customer data will be stored within the same Region as the master database.

The available regions are listed in the Multi-regional architecture section of this whitepaper.

Backup Technology

Databases are replicated in multiple Availability Zones in real time. This means that in the unlikely event of failure for an entire data center, backups in other Availability Zones can be accessed without any service interruption to customers.

Boardingware utilizes Amazon RDS (Relational Database Service) to store customer data. As a managed service RDS provides additional backup services such as point in time restoration and entire database snapshots. Boardingware has configured RDS with the maximum retention period meaning data can be restored to any point of time with per second accuracy within the last 35 days. In addition complete database snapshots are taken every day and stored for up to 7 days in continuous rotation.

Each database employs a master slave approach so a backup instance can take over the main server in the event of failure allowing the affected instance to be replaced with a fresh installation. As an added benefit of the RDS managed service, all software patches and updates to the database server are automatically installed within a maintenance time frame specified by Boardingware.

Logical Protection and Physical Separation of Backups

RDS backup volumes are encrypted with 256-bit AES cryptography. Backups are logically separated from direct access to the internet within a secure private subnet. Instances of backups have been physically separated by cloning them across multiple availability zones.

Testing Backups

Boardingware conducts backup restoration tests at least once every 6 months to ensure the reliability of backup procedures and backup data integrity.

Customer Responsibilities and Capabilities

In the event of a backup restoration, customers are not required to participate in the procedure. Boardingware will communicate any downtime which may result from a restoration event, the customer should raise any issues or concerns they have which Boardingware should take into account.

There are exporting features available within the Boardingware web application. Customers can use these features as a means of backing up their data in addition to the backups which Boardingware provides.

Data At Rest

Boardingware encrypts all school data stored on our servers at rest as an extra layer of security against unauthorized access and to allow our customers to fulfill data-at-rest encryption obligations. All Boardingware RDS instances and snapshots are encrypted with industry standard 256-bit AES encryption.

A KMS (Key Management Service) is used to manage encryption keys. Keys are designed not to be exportable and security controls are setup to restrict access to them. The master keys themselves are automatically encrypted with 256-bit AES key-encrypting keys which are periodically rotated.

Data In Transit

All data transferred between Boardingware's API and web and native mobile applications are secured by the TLS (Transport Layer Security) protocol over a HTTPS connection. All attempts to make non-secure requests are directed to the secure port.

Clock Synchronisation

All hosted servers within the AWS hosting environment are clock synchronized with the provided reliable NTP (Network Time Protocol) source.

Cloud Monitoring:

Capacity Monitoring and Management

Boardingware utilises CloudWatch to monitor AWS cloud resources and availability. Rules are created to send alarms to the development team related to latency, errors and request rate. This allows Boardingware to proactively address cloud resourcing issues to minimise the effect on the availability of the service.

Monitoring Access to AWS Resources

All API calls made to Boardingware's Amazon account either through the command line or the AWS web interface including login events are recorded using AWS Cloud Trail. For each event AWS Cloud Trail records what was accessed, what actions were performed and the source of the request. This provides Boardingware with visibility and auditing capabilities on the usage of AWS resources.

Secure Development

Boardingware has defined a Secure Development Policy which embeds secure principles and practices into the development culture of the organisation. This ensures that information security is accounted for at every phase of the development life cycle, especially during development

within the cloud. The secure development process includes planning and analysis, design, testing, deployment, monitoring and maintenance. This ensures the integrity of the developed systems from the early stages through all subsequent maintenance efforts.

Customer Management In The Cloud

Boardingware has developed internal interfaces which allow Boardingware personnel to securely create, access and remove customer accounts for implementation and support purposes. Appropriate controls have been implemented to protect access to these systems.

Boardingware personnel must be assigned an individual user id and credentials before gaining access. Boardingware super administrators which is only assigned to senior management can control the access and system permission of each user on a strict need to know basis. This includes which Region of customer accounts employees can access and what actions they are able to perform such as the login, creation or deletion of accounts.

Access to these systems are further controlled by whitelisting approved IP addresses, therefore denying access from unapproved IP addresses. Super administrators have the ability to audit every action taken within the system including the timestamp, associated ip address, Boardingware user id, login events, viewing, editing, and deleting of records performed within customer accounts by Boardingware personnel.

Customer Cloud Security

Boardingware provides its customers with the ability to securely configure and manage their Boardingware account within their school's cloud environment.

Auditing Capabilities

Boardingware provides an internal Auditing feature within the administrator web application. This tool allows school administers to record, view and export logs that describe which users have viewed, edited and deleted records including, records containing PII (Personally Identifiable Information). Audit records include Action, Description, Timestamp, Record Type, Package, User ID, User Type and IP Address of actions taken by Staff, Administrator and Student users.

These auditing capabilities can assist customers with key issues such as:

- Allowing schools to comply with regulations relating to keeping access and edit records of the PII which they are controlling
- Providing reliable records when schools are required to produce evidence to authorities relating to security or privacy events
- Investigating the misuse or misconfiguration of Boardingware within their school

User Management:

Individual User Accounts

All users of the Boardingware platform are required to create their own unique Boardingware account. This includes parents, students, staff and administrators. Administrators have the ability to create and remove these accounts when needed.

Depending on our customer's chosen technology stack, Boardingware may offer methods of integrating with their existing user and access management systems to allow schools to manage accounts centrally and avoid creating new Boardingware specific credentials for users.

Admin Controls

Selected school employees are appointed as Administrator Users who are granted privileged access to their Boardingware environment. Schools are responsible for assigning Administrator access to employees who possess the appropriate access level and competencies to manage their Boardingware configuration.

Full Access

By default, administrators can access all the data and controls associated with their Boardingware account. Administrators can be invited by other administrators or by Boardingware personnel.

Access Permissions

Administrators can restrict staff access to view or edit student information by setting up access groups called "Houses". Only staff assigned to Houses can access students within that House. This degree of separation is often useful for boarding environments where certain staff members are only responsible for the students within their dormitories.

System Permissions

Administrators can control the record and feature permissions of staff users. Action permissions restrict what records staff members can view, edit and delete. Feature permissions control what features staff members can use. These permissions are useful for only giving staff members access to the features that are necessary for them to complete their duties.

User Controls

Administrators have key controls over school employee accounts. This includes user deletion, suspension and password resets. User deletion and suspension will kill all active user sessions and immediately remove access. Administrators can also see recent staff activity such as last seen time, last action along with IP address and Date.

Secure Invitation Process

Inviting users to Boardingware is restricted to Boardingware administrators only. This includes inviting new staff members, administrators, students and parents. Administrators send email invitations to users who are then prompted to create their accounts by specifying a username and password. Invitation emails contain a link to a secure sign up page with a non-replicable URL. These invites expire after a specified period after sending the invite. Administrators can view the status of each invite and the information the user has specified to create their account, excluding their password.

Password Management

Boardingware users must specify a password with a minimum length of 6 characters. Users can reset their password through a secure email password reset process. Password reset links expire after 1 day. Users must have access to their Boardingware username and specified email account to complete this process.

Session Times

User session are set to expire after a short period of inactivity, requiring the user to enter a new username and password.

Email Security

No sensitive information such as student leave details are transferred through email. Instead email notifications contain a link to a secure Boardingware generated URL which displays the

necessary information. Users must log into their accounts to view these URLs. These links also expire after they are used or after a certain period of time.

Granular Record Control

Records created to store student information such as leave, pastoral or attendance records are maintained with a granular activity log. This shows which actions have been performed in relation to each record, by which user as well as the time and IP address. This record log helps schools to comply with regulations which enforce tracking view and edit logs to sensitive information.

In addition, schools can view which staff members or Checkpoints performed key actions such as singing in, signing out, approving leave, marking as present.

Retaining Student Information

Schools can retain information for past students by saving their profile to an ex-student database. All information recorded by Boardingware for ex-students can be accessed at anytime by administrators. This helps schools comply with data retention directives and regulations.

Leave Security Controls

Boardingware gives schools the ability to create Leave Types with a number of controls to improve the security posture of student leave management. These controls are implemented with the use of assignments, workflows and rules.

Assignments

Assignments determine which students have access to certain leave types. For example, some leave types may be restricted to students based on their age or parental permissions. Assignments, allow schools to create more specific leave types for their various groups of students.

Workflows

Workflows allow schools to define which user role can perform specific actions within the leave lifecycle. For example, schools can decide if students are allowed to sign themselves in or if they must be signed in by a staff member. These controls allow schools to install secure leave processes with a large degree of customisation to suit their specific needs.

Rules

Rules are an additional layer of controls which restrict the departure and return times of leave events. Rules can either be a hard rule which will completely block certain times or a soft rule which will display a warning notification to the user.

Automated IP Matching

When students and parents apply or approve leave, their IP address is recorded within the leave request. This alerts staff to help them discern when students are attempting to approve their own request from their parents account.

Real-Time Updates

Schools can sometimes have dozens of Checkpoint and user devices using Boardingware at any one time, it is important that all these devices display the most up to date information to users. Boardingware utilizes a data-pushing model with the use of websockets, this means updates are instantaneously pushed to all users to keep connected devices in sync.

This method of synchronisation is significantly faster and more reliable than traditional data models where updates are requested periodically. This assures Boardingware users that they are working with a live account of their students data.

Offline Mode

Boardingware staff accounts have access to a native iOS application for the iPad and iPhone. This application has a built in offline mode which allows users to access information stored on the device in the event of a network disruption.

Checkpoint Security Controls

Boardingware provides a self service interface called "Checkpoints". Checkpoints allow students to sign themselves in or out from an on-site publicly facing device. As Checkpoint devices are publically facing it is important to manage...

Remote Configuration

Administrators are able to configure and monitor their Checkpoint network from a central dashboard. This allows for effective Checkpoint management to ensure proper configuration is maintained.

Checkpoint Types and IDs

Schools can create Checkpoint Types which define the system permissions related Checkpoints. Unique identifiers can be associated to each device and linked to a Checkpoint Type which will inherit it's permissions. This allows schools to identify which Checkpoints students used for sign-in and sign-out events.

Checkpoint IDs can also be removed. This will also kill all the active sessions of a Checkpoint device.

Faceless View

Administrators can enable faceless mode for Checkpoint Types which will hide student's identity and location of public facing devices.

PIN Code

Unique student PIN codes can be required when students sign in or sign out from a Checkpoint.

Peer SI/SO

Administrators can allow or restrict students from signing other students in or out from a Checkpoint device.

Emergency Rolls

Schools can create Emergency Roll Type's to use in response to a crisis or disaster event. Roll permissions can control which staff members are allowed to initiate, complete or edit an emergency roll.

Initiating an emergency roll can also push alerts to parents, students and staff members. Administrators can also pre-populate templates for these messages to be sent out immediately when an emergency roll is initiated.

Notifications

Staff members can configure their notification preferences to alert them of key security events including when students are late or if they are absent from a roll check.

Conclusion

We take security seriously at Boardingware, because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we work hard to maintain that trust.

If you have any further questions about our cloud security processes, please contact us via email to security@boardingware.com.

Technical Glossary

Access Control Lists (ACL): A list of permissions or rules for accessing an object or network resource. In Amazon EC2, security groups act as ACLs at the instance level, controlling which users have permission to access specific instances. In Amazon S3, you can use ACLs to give read or write access on buckets or objects to groups of users. In Amazon VPC, ACLs act like network firewalls and control access at the subnet level.

AES encryption: The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

API: Application Programming Interface (API) is an interface in computer science that defines the ways by which an application program may request services from libraries and/or operating systems.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Not only do users need to be authenticated, but every program that wants to call the functionality exposed by an AWS API must be authenticated. AWS requires that you authenticate every request by digitally signing it using a cryptographic hash function.

Auto-Scaling: An AWS service that allows customers to automatically scale their Amazon EC2 capacity up or down according to conditions they define.

Availability Zones: Amazon EC2 locations are composed of regions and availability zones. Availability zones are distinct locations that are engineered to be insulated from failures in other availability zones and provide inexpensive, low latency network connectivity to other availability zones in the same region.

AWS Managed Services: Services that AWS is responsible for security, maintenance and updates. Boardingware utilizes AWS Managed Services such as the Relational Database Service (RDS). Managed services provide extensive security controls which can be configured to suit the needs of Boardingware.

Downtime: The time that the customer or user within a customer's account cannot access the Service. Downtime excludes the time that the user is unable to access the Service due to any of the following:

- Maintenance Time
- Customer or User's own Internet service provider
- Force Majeure event
- Any systematic Internet failures
- Any failure in the user's own hardware, software or network connection
- User's bandwidth restrictions
- User's acts or omissions
- Anything outside of the direct control of Boardingware

FERPA: The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) is a United States federal law that governs the access of American citizens' educational information and records.

HIPAA: HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.

House: Boarding schools often have one or more dormitories also known as houses which physically separate boarding students. Boardingware has adopted this model within its service. This allows schools to organise boarding students into different houses and assign staff to appropriate houses. Each house can have house specific leave types and groups so they can operate independently from each other.

Infrastructure as a Service (IaaS): Services which provide the physical components of the cloud. This includes computing, networking, physical security and maintenance. SaaS companies purchase these services to provide unprecedented scalability, availability, cost savings and improved cloud security posture to their customers.

IP Address: An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes.

Key: In cryptography, a key is a parameter that determines the output of a cryptographic algorithm (called a hashing algorithm). A key pair is a set of security credentials you use to prove your identity electronically and consists of a public key and a private key.

Kiosk: Boardingware provides a method for students to sign themselves in and out without giving them access to any other staff or admin features. The kiosk can be set up on either Boardingware's web application or on it's native iPad app. Access to leave is dependent on leave type controls that are set up by administrators. Unique pin codes can also be set up to control student access on kiosk mode.

Leave Record: A leave record contains all the leave information for each leave event. This includes the leave details, approver history, notes and messages. Leave records are stored within a student's profile and can be access at any time. Records have different states such as leave request, upcoming, active and past leave.

Maintenance Time: The time period during which the Hosted Service may not be available each month so that Boardingware can perform routine maintenance to maximize the performance. This will occur on an as needed basis.

Multi-factor Authentication (MFA): The use of two or more authentication factors. Authentication factors include something you know (like a password) or something you have (like a token that generates a random number). AWS IAM allows the use of a six-digit single-use code in addition to the user name and password credentials. Customers get this single-use code from an authentication device that they keep in their physical possession (either a physical token device or a virtual token from their smartphone).

Multi-tenancy is a reference to the mode of operation of software where multiple independent instances of one or multiple applications operate in a shared environment. The instances (tenants) are logically isolated, but physically integrated. Boardingware customers share physical cloud services with each other but do not have access to each other's data.

Pastoral Record: A pastoral record stores student behavioral and wellbeing events such as disciplinary, merit, medical and academic notes. These records are saved within each student profile. Each record is timestamped and retains a edit history. Access to sensitive records can be controlled through staff permissions.

Region: A named set of AWS resources in the same geographical area. Each region contains at least two availability zones.

Software as a Service (SaaS): In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications differ from other applications in their scalability

Snapshot: A customer-initiated backup of an EBS volume that is stored in Amazon S3, or a customer-initiated backup of an RDS database that is stored in Amazon RDS. A snapshot can be used as the starting point for a new EBS volume or Amazon RDS database or to protect the data for long-term durability and recovery.

SSL: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide

communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP). Major websites use TLS to secure all communications between their servers and web browsers.

Student Profile: Each student within Boardingware has a profile which stores all their leave, pastoral, contact and personal records. Records are stored in a timeline format which can be searched and filtered.

Uptime / Availability: When the customer and users within the customer's account who are active and enabled have reasonable access to the Service provided by Boardingware, subject to the exclusions that are defined in the Downtime definition above.

URL: A Uniform Resource Locator (URL), commonly informally termed a web address (which term is not defined identically) is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL is a specific type of Uniform Resource Identifier (URI), although many people use the two terms interchangeably.

VPC: An AWS service that enables customers to provision an isolated section of the AWS cloud, including selecting their own IP address range, defining subnets, and configuring routing tables and network gateways.

Boardingware