ScreenCloud

Security Essentials overview

Ravi Gurbani
Cyber Security Officer

ScreenCloud, 3rd Floor,
28 Brunswick Place, London, N1 6DZ, UK
Last Updated: March 2022

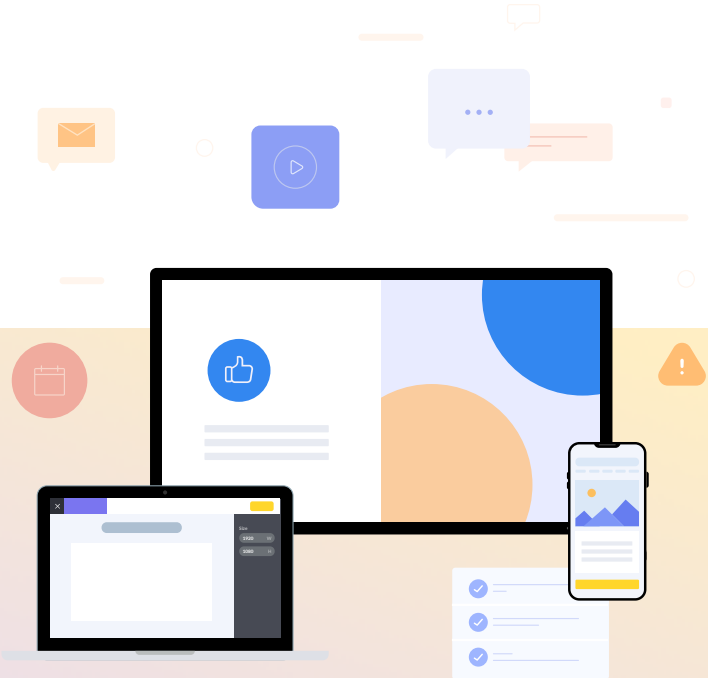
screencloud.com

Overview

ScreenCloud is the easiest way for your business or organization to visualize what's important using digital signage - whether that's dashboards, team notices, the latest promotions or digital menu boards.

At ScreenCloud, security is a top priority. ScreenCloud customers trust us with their data, and we do not take this responsibility lightly.

We handle data with the utmost care and integrity. Whether it's encrypting your data over the Internet or at rest, we want you to have confidence in how your data is being processed, transported, and stored. In addition to our public resources, we frequently get questions that fall into a handful of major groupings surrounding your data and who has access to it. These are the same questions we ask of third-party services handling our data. We hope that this document will give you a better view into the exact mechanics we use to secure your data within our systems.



If you have any further questions regarding security at ScreenCloud please contact us by visiting

screencloud.com/security

Contents

01

Securing data in transit

ScreenCloud acts as a configuration and client content management service for the content made viewable on a ScreenCloud Player running on your digital signage and screens. Users access the ScreenCloud Content Management Service (CMS) through a web browser on an internet connected desktop, tablet or smartphone. Internet connected devices running the ScreenCloud Player are authenticated by users, permit access to the service and display configured content.

Data from users and players to the SaaS services are transferred over HTTPS and encrypted using TLS1.2 or TLS1.3 only (ECDHE_RSA with P-256, and AES_128_GCM).

- **Data you provide to ScreenCloud**
  ScreenCloud requires user account and billing information for your service to be enabled. We limit this particular data to the minimum required (email address, billing address, billing info). In the event that you wish to configure Single Sign On and depending on your identity provider, individual user account information is provided by your IDP.

  Data that you wish to display on screens managed by our service is uploaded by you to your account using Filestack. Additionally you may configure other content to be displayed by our apps that you can integrate.

- **Data accessed by players**
  You will need to authenticate players to enable access to your account. For specific instructions please review **this article.**

  Data is sent back to devices that have our player app installed, connected and paired with your account. These players receive a playlist schedule and content instructions configured by you from our service. The player then displays this content according to your schedule.

- **Data from other sources**
  Depending on the app integrations you select to enable for your service, ScreenCloud may receive data from other systems or services.

02

Securing data at rest

There are two key types of data at rest that the ScreenCloud service manages which are Configuration Data and Content Data:

- **Configuration data**
  We use AWS RDS to manage this configuration data, this is connected to our AWS environment using a private VPC link and secure API using TLS. Backups are encrypted at rest and in transit.

- **Content data that you upload**
  This is securely stored in Amazon S3. The data is logically partitioned by the ID of the data source, and access is controlled via IAM permissions. Data in S3 is encrypted at rest using Amazon's SSE offering and replicated to a separate bucket for redundancy. Customers can elect to have this data deleted at any time.

  All data at rest within our service is encrypted using AES256. We use the Key Management Service provided by AWS.

- **Data retention**
  We retain data for as long as necessary to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for fraud prevention purposes.

  ScreenCloud has defined a retention period for AWS, AWS RDS and Auth0 hosted log data which is 90 days and backups which is 30 days. Our subscription management service provided by Chargebee only keeps data for as long as needed for the provision of service. Chargerbee erases all your Personal Identifiable Information (PII) 120 days after your account with us has been cancelled.

- **What happens to your data if you leave ScreenCloud?**
  If you terminate or cancel your subscription with ScreenCloud you can request an immediate deletion of your account and data ; otherwise we will initiate a deletion of your data within 30 days. You may request a copy of your data but this must be made within 15 days of the date of cancellation.

03

Data access

We provide customers the ability to manage this access on a per-user level. We designed our access management system with flexibility in mind with teams and pre-made roles. This means that your users can be organized and enabled with access to the appropriate resources they need in ScreenCloud, but nothing more.

- **User authentication**
  We use Auth0 to provide authentication and authorization within our service. Users can use OAuth services provided by Google or other OAuth providers to login to their account, users can also provide an email/password combination. Credentials are transmitted securely using TLS, user accounts are hashed, salted and stored using bcrypt.

  We can integrate with several major SSO providers such as Azure AD, OKTA and Google. Please contact our Enterprise Professional Services team for more information at screen.cloud/enterprise.

  Once a user has been authenticated we make use of JSON web tokens **(https://jwt. io)** for continued authentication throughout a session.

- **Roles**
  The following user roles are available within our Studio service:

  Owner
  As an owner you have access to everything in the organization and are able to do anything, to any screen. You are also the primary contact.

  Admin
  As an admin you have access to everything in the organization, except billing, and are able to do anything, to any screen, in any space. You are able to invite users in the organization.

03

Data access

Manager
As a manager you are able to manage the screens in the space you are assigned to. You are also able to delete and modify all content in the spaces you have access to.

Creator
As a creator you are able to create ‘Channels’, ‘Playlists’ and add ‘Media’. You cannot change what’s playing on a screen.

Viewer
As a viewer you can view only in the spaces you have access to.

On ScreenCloud’s side, only members of the Engineering, Operations and Support team have access to your data for debugging purposes only. The following safeguards are in place to ensure this access is strongly protected:

1. All production access is federated through SSH and IAM.
2. The only nodes open to the outside world are our bastion nodes which are secured with individual user auth and individual SSH keys.
3. Our employees have no IAM user keys and can only access AWS through SSO. In order to perform administrative actions, users must use multi-factor authentication (MFA) to authenticate with our identity provider and switch to an administrative role.
4. All changes are logged and tracked through source control and deployment automation.

04

Continuous monitoring

Amazon Web Services (AWS) serves as the front-line of protection for all network level attacks. AWS manages the software and selection of cipher suites on our load balancers. To ensure that Segment adheres to security best practices, we maintain relationships with our vendors and perform regular assessments on our key service providers. Our source code is continuously scanned for dependency vulnerabilities and we undertake an annual independent external penetration test of our service with a comprehensive test scope.

We keep audit logs provided by AWS Cloudtrail on all administrative actions. ScreenCloud has a comprehensive incident response and incident management process in addition to a security and data breach notification policy. We do not require any special category data from you to use our service, our requirements are minimal and limited to data required to maintain relevant billing information and account access. ScreenCloud shall provide timely and appropriate notice to affected individuals or organizations when there is a reasonable belief that a breach in the security of private information has occurred.

If it is determined that an external notification to the affected users or Customer Organizations are warranted, you will be contacted by our support and comms teams. This contact will be to the administrative owner for your account.

Contact will be made by our support and communications teams via standard channels, such as email, our website and any other appropriate channels. A blog post will be written with a combined email and knowledge article if appropriate for further actions that may require customer actions.

Our notification policy, owned by the Data Protection Office, is aligned with the guidance outlined in EU-GDPR which is 72 hours to notify the relevant supervisory authority. If the breach is likely to result in a high risk or adversely affecting individuals' rights and freedoms we will inform those individuals without delay.

05

Modern service based infrastructure

We do not maintain any physical or server infrastructure with our service being built upon code defined cloud infrastructure and PaaS services provided by AWS and additional cloud service providers that manage data centre facilities.

Our AWS infrastructure is contained within ScreenCloud managed VPCs which provides total isolation. Our VPCs are divided into public and private subnet layers, the only public facing listeners are our load balancers which are managed by AWS. ScreenCloud maintains separate development, staging and production accounts for each layer of our service.

Static content is delivered using AWS Cloudfront.

Our service is built upon industry leading platform services which include:

- Auth0 for authentication and Authorisation
- Chargebee for subscription management
- Stripe for payment processing
- AWS RDS for Database services

- **Payment processing**
  We do not store any PCI information within our service.
  We use **Chargebee** to manage invoicing and subscriptions.
  For payment processing we use **Stripe**, **PayPal** and **GoCardless**.

  Stripe, PayPal and GoCardless hold actual payment information like credit card or bank details. Stripe is certified to PCI Service Provider Level 1, which is the most stringent level of certification available in the payments industry (https://stripe.com/docs/security/stripe). PayPal's security policy is **detailed here**.

  GoCardless accesses the Direct Debit system provided by some of Europe's major banks, who have approved their systems. All customer data is treated in accordance with General Data Protection Regulation (GDPR). Their financial data server is separated from the application server by multiple firewalls. All client-server communication is 256-bit SSL encrypted. They are ISO 27001 certified for information security.

06

Commitment to security compliance

In alignment with ScreenCloud's commitment to the privacy and protection of customer and corporate data, we have developed a comprehensive Information Security and Privacy Program. The ScreenCloud ISPP is structured in alignment with AICPA SOC2 Trust Service Criteria and ISO 27001 guidance. Our ISPP is continually enhanced to align with new and evolving regulatory requirements such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

We are independently audited as part of our annual SOC2 Type II assessment, with our most recent assessment having been undertaken in May 2021. The next assessment is scheduled for May 2022 with the reports available upon request.

Security is everyone's responsibility at ScreenCloud and our teams devote themselves to its practices to ensure the protection of your data.

Everyone at ScreenCloud undertakes a rigorous onboarding process that includes confirmation and acknowledgement of Information Security and Employee Handbook policies.

- **Staff training**
  ScreenCloud operates a security awareness training program which is mandatory for all staff as part of onboarding practices and refreshed at least annually. Upkeep of training is monitored by the Security function via a training compliance dashboard. In addition monthly security topics or reminders are disseminated covering newly identified risks, threats or recurring themes.

  All personnel are instructed on how to report a security breach and what necessary actions that should be taken.