

# Security and data protection

Where your data lives, who can reach it, what is kept and for how long, and what the software on your players may and may not do. This describes the platform as it runs in September 2026.

## AT A GLANCE

|                           |                                                                                                                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosting                   | Google Cloud in Finland, region europe-north1.                                                                                                                                            |
| Database                  | Reachable on a private network address only; never exposed to the public internet.                                                                                                        |
| Backups                   | Daily, seven retained.                                                                                                                                                                    |
| Access                    | Four roles, from Platform admin to Viewer. Each organisation sees only its own screens, users and audit trail.                                                                            |
| Audit log                 | Sign-ins, failed sign-ins, reboots, outages, configuration changes and user administration — with who and when.                                                                           |
| Third-party credentials   | Encrypted at rest with authenticated encryption; never stored on a device.                                                                                                                |
| Device agent              | Runs as a system service, updates itself and rolls back a release that will not start. Every command is role-checked on the server. Site network scanning can be switched off per device. |
| Retention                 | Screenshots 24 hours behind each device's newest; raw telemetry 90 days; raw play rows 30 days, then an hourly roll-up reconciled to the exact raw count.                                 |
| Public website            | No cookies and nothing stored in the browser. The IP address of a visitor is never stored.                                                                                                |
| Reporting a vulnerability | support@screenry.io                                                                                                                                                                       |

## 1 Hosting and data residency

Screenry runs on Google Cloud in Finland, in the europe-north1 region. The dashboard, the API, the connections from the players and the database are operated there.

The web application tells browsers to use HTTPS only (HTTP Strict Transport Security), refuses to be framed by other sites and disables content-type sniffing.

## 2 Network isolation

The database has a private network address only. It is not reachable from the public internet, and nothing about the product requires it to be. The application reaches it over the private network; so do the scheduled data jobs, which run inside the same private network rather than connecting from outside.

## 3 Backups

The database is backed up daily, and the last seven backups are retained.

## 4 Roles and organisation isolation

What a person may do is decided by their role. Every request is checked on the server, not only hidden in the interface.

| ROLE               | WHO                          | MAY                                                                                             |
|--------------------|------------------------------|-------------------------------------------------------------------------------------------------|
| Platform admin     | Screenry staff               | Operate the platform across organisations.                                                      |
| Organization admin | The customer's administrator | Manage their own organisation: users, invitations, settings, devices.                           |
| Operator           | Field and operations staff   | View, go live, reboot and mark out of service — nothing that edits a device or reaches its LAN. |
| Viewer             | Read-only users              | View.                                                                                           |

**Organisations are isolated.** Every organisation sees its own screens, users and audit trail only. An organisation admin manages their own organisation and no other, and no invitation can grant the Platform admin role.

## 5 Sign-in and sessions

Sessions use signed tokens (JWT) that are valid for 30 days. Sign-in and the public forms are rate-limited. Every sign-in and every failed sign-in is written to the audit log.

## 6 Audit log

The audit log records who did what, and when. It covers:

- sign-ins and failed sign-ins;
- reboots — those ordered from the dashboard and those the device decided on itself;
- outages: a device marked out of service, and when that ended;
- configuration changes;
- user and organisation administration.

An organisation's members see their own organisation's trail only.

## 7 Third-party credentials

Some features need a login to another system — for example Broadsign, or the web interface of a display controller on a site's network. These credentials are encrypted at rest with authenticated encryption, which detects any tampering with the stored value as well as hiding it. They are never stored on a device.

## 8 The device agent

Each player runs the Screenry agent as a system service. It reports status and screen captures, runs the black-screen and missing-output watch, and carries out commands. Four properties limit what can go wrong:

- **Updates roll back on their own.** The agent updates itself, and if a new release will not start, the player restores the last good version without anyone logging in. Measured on a device: back online in 51 seconds.
- **Commands are role-checked on the server.** A command is accepted only from a user whose role allows it. An Operator can reboot a device or mark it out of service, but cannot change its configuration or reach its local network.
- **Site network scanning can be switched off.** On Operate and Premium the agent can inventory the site's local network — controllers, sister players, sensors — and read controller status. Where a customer's network policy does not allow that, it is switched off per device. Off means no network sweep, no port probes and no controller readings, and the setting is remembered by the device across restarts.
- **Automatic reboots are capped.** At most three automatic reboots per device per day, the third only in the 03–05 night window. Every one is written to the audit log.

## 9 Public website

screenry.io sets no cookies and stores nothing in the visitor's browser, so it needs no consent banner. Visits are counted with an anonymous hash that changes every day: it can tell how many different visitors came on one day and nothing more, and it cannot follow anyone from one day to the next. The IP address is never stored. Automated traffic is recognised and left out of every count.

When someone asks for a demo or a document, we answer that request. Follow-up e-mails go only to people who ticked the consent box, which is unticked by default, and every e-mail carries an unsubscribe link that stops them at once.

## 10 Data retention

Operational data is deleted on a schedule. Deletion runs per device, and every sweep is claimed by one server instance at a time.

| DATA                | KEPT FOR                                     | NOTES                                                                                                                                                     |
|---------------------|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Screen captures     | 24 hours behind each device's newest capture | The newest capture of every device is always kept.                                                                                                        |
| Raw telemetry       | 90 days                                      | Heartbeats and connectivity probes.                                                                                                                       |
| Raw play rows       | 30 days                                      | One row per airing. Kept afterwards as an hourly roll-up; a day of raw rows is deleted only after the roll-up sums to exactly the raw count for that day. |
| Hourly play roll-up | Kept as the analytical record                | One row per hour, device and creative — the basis of proof-of-play and audience reports.                                                                  |
| Database backups    | Seven daily backups                          | Older backups are replaced.                                                                                                                               |
| Website visits      | No IP address stored                         | The visitor hash changes daily, so it identifies no one beyond a single day.                                                                              |

## 11 What this document does not claim

This document describes controls that exist in the product today. It does not claim any third-party certification or audit. If your procurement needs answers to a specific questionnaire, send it to us and we will answer it for the platform as it is.

## 12 Reporting a vulnerability

If you believe you have found a security problem in Screenry, please write to [support@screenry.io](mailto:support@screenry.io). Include what you found, how to reproduce it and how to reach you. Please do not access other customers' data, disrupt service or disclose the issue publicly before we have had a reasonable chance to fix it. We will acknowledge your report and keep you informed.

### Contact

Security questions and questionnaires: [support@screenry.io](mailto:support@screenry.io) · Company details: **[to be completed]**