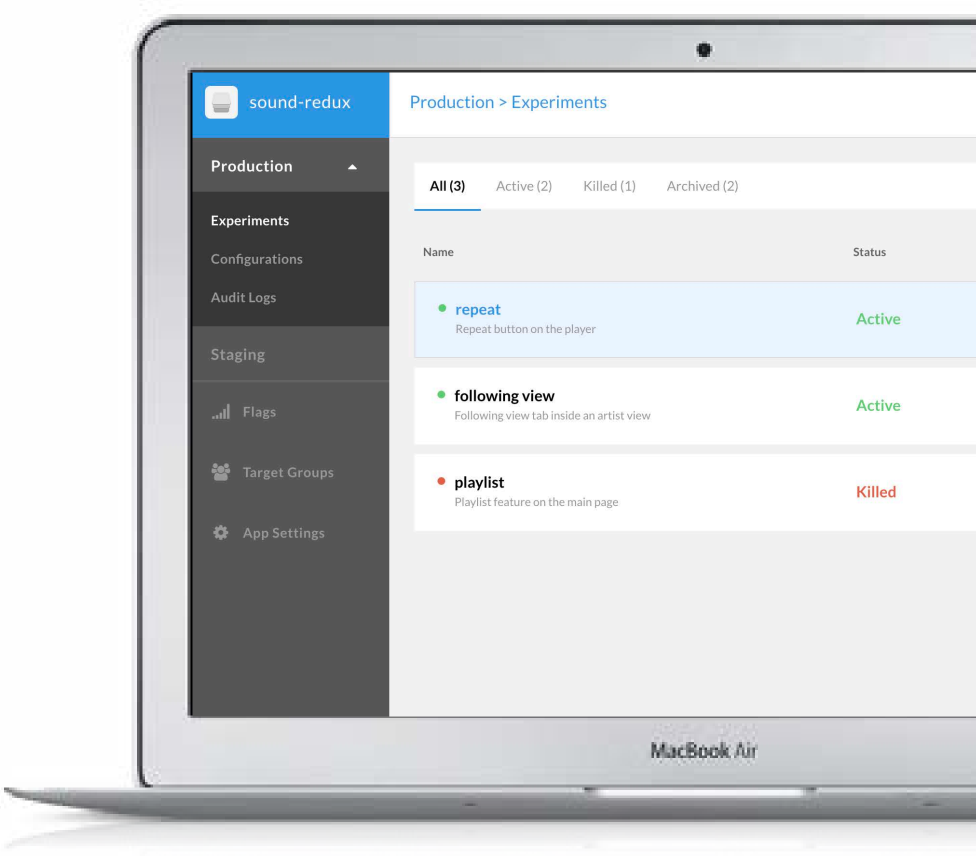
# Security Overview

## Infrastructure, policies and practices

Rollout.io

Rollout is an advanced Feature Management solution, it gives engineering and product teams control over software features post-deployment.  It's the most effective way to roll out features to the right audience while protecting customers from failure.

Rollout is committed to the security & privacy of its customers and their applications. Rollout use a variety of industry standard security technologies and procedures to help protect its customers' information from unauthorized access, use, or disclosure. Rollout's security program covers application security, compliance, privacy, corporate security, and physical security.



| Name | Status |
|---|---|
| ● repeat<br>Repeat button on the player | Active |
| ● following view<br>Following view tab inside an artist view | Active |
| ● playlist<br>Playlist feature on the main page | Killed |

# ROLLOUT SECURITY PROCESS

## Internal R&D Process

Security-oriented environments start with high coding standards that guard against attempted security breaches and are accompanied by rigorous code reviews and tests (such as code coverage testing). Rollout employs the strictest development processes and coding standards to ensure that both adhere to the best security practices.

## Vulnerability Scanning

Rollout is undergoing periodic vulnerability scanning which detect OWASP Top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and un-validated redirection. (Vulnerability report is available upon request)

## Penetration Testing

Rollout is also undergoing rigorous periodic penetration testing performed by App-Sec Labs, an independent third party security consulting firm. (Penetration report is available upon request)

## SOC2 Type II Certified

According to the American Institute of CPAs (AICPA), a SOC 2 report is ideal for SaaS and cloud service organizations that want to assure customers that their information is secure and will be available whenever needed. A SOC 2 report also helps organizations to establish the effectiveness of any controls that may be required by their governance process.

## Two Factor Authentication (2FA)

Rollout is using Two Factor authentication for all its internal tools & utilities, including all infrastructure, email, marketing & sales solutions.

## Change Management

All source code changes are subject to peer a review, peer review is a mandatory and crucial step in Rollout development cycles, peer review assesses functionality, performance and security.

# ROLLOUT INFRASTRUCTURE SECURITY

## Physical Access

Rollout relies on the Amazon's secure cloud infrastructure. AWS infrastructure aligns with IT security best practices and follows a number of compliance standards such as:

- SOC 1/SSAE
- 16/ISAE 3402 (formerly SAS 70 Type II)
- HIPPA
- SOC 2
- SOC 3
- FISMA
- DIACAP
- FedRAMP

All data centers that run the Rollout platform are secured and monitored 24/7, and physical access to AWS facilities is strictly limited to select AWS cloud staff.

*For more information about AWS' secure architecture and compliance certifications, visit [http://aws.amazon.com/security](http://aws.amazon.com/security)*

## Instance and Network Security

Rollout uses AWS VPC (which is an isolated private network dedicated for Rollout). Running our system in a VPC, VPN, subnets and security groups (firewalls) adds additional layer of security. Rollout VPC uses network access control that limits the access from the Internet only to a limited set of resources. Rollout backend services could only be accessed by a secured VPN connection which is available only to a small group of individuals with the applicable internal credentials, 2FA (Two Factor Authentication) and private access keys. DNS and ELB's are also configured with SSL. All data transmissions from and to the Rollout Agent (SDK), are secured via 128bit SSL encryption using a 2048bit RSA encryption key.

## Data verification and Man-in-the-middle attacks

Rollout solution is the only solution that uses Private/Public keys to verify that the data received by the SDK is indeed the data sent by the Rollout system, securing the platform against Man-in-the-middle attacks.

# PRIVACY & END USER DATA

## Rollout does NOT have access to end user data

The Rollout service does not access or save end user data, including any end user Personally Identifiable Information (PII), Rollout architecture is built around privacy, targeting specific end users happens on the client slide (mobile application, web application or a backend system) with locally available attributes and is never transmitted back to Rollout, the SDK generates a random identifier (device ID) on the device to uniquely identify an anonymous user.

## Privacy Shield

Rollout adheres to the EU privacy policy and adheres to the Privacy Shield standards, to learn more about the Privacy Shield program, please visit https://www.privacyshield.gov/

# PRODUCT SECURITY

## Access Security

Rollout is secured using username, password and 2FA (if enabled by the user), Rollout also supports authentication via Google OAuth or GitHub OAuth. Passwords are encrypted with an AES-256 hash and random salt.

## Role Based Permissions

Rollout uses an industry standard Access Control mechanism to allow teams to give different permissions to different users in their team based on Roles and environments.

## Audit Log

Rollout records and presents all feature deployment changes by time, user and type of change. Audit logs are available per environment.

Rollout.io

For more information:

LEARN MORE

visit https://rollout.io

EMAIL US

email us at support@rollout.io