# Security, Privacy, and Architecture Overview

Reach is designed with the most security-conscious Security and IT teams in mind. Understanding the security practices of an organization you're looking to trust with your data can feel intentionally confusing and more often than not, frustrating. We strive at Reach to keep things simple and secure.

This article provides an up-to-date overview of the state of Reach's security and how it applies to our system. We take advantage of cloud security best practices and adhere to strict policies and requirements that enable Reach to maintain the security and integrity of the data our customers entrust us with.

## Overview

Sections outlined in this document

- Corporate Governance
- Data Security
- Data Privacy
- Product Security
- Security Architecture

## Corporate Governance

Every Reach employee is committed to the security and privacy of our customers and their information. This starts with accessible information security policies that are reviewed on a quarterly cadence and being leveraged throughout the organization. These policies guide how Reach does business, builds products, and operates. Some examples:

- Data security and privacy training as part of onboarding
- Employees sign agreements to preserve and protect the confidentiality of customer information they may interact with while doing their jobs
- Background checks for all employees
- Multi-factor authentication is required for all business applications that interact with customer data.
- Employee security awareness training
- Incident Response plan and subsequent playbooks are reviewed on an annual cadence

## Data Security

### Data Security

- Customer data sent to Reach is encrypted in transit using best practice and compliant cypher suites.

### Data in Rest

- Data at rest is encrypted using AES-256 encryption
- Storage level encryption will be used when data is stored in the cloud
- File system encryption is used in cases where a Reach employed customer success researcher needs to access data and move information to their local device to improve a prospect or customer's experience.
- Data searched for and accessed within an event management solution such as a SIEM will default to the customer's local configuration

### Least Privilege

- User and service accounts are granted roles based on their requirements. These roles are defined with least privilege principals in mind. A user or service must have an applicable set roles which are inventoried and reviewed on a quarterly basis

## Data Privacy

### Customer Privacy Options

#### Data Retention and Data Deletion

- Data retention is set to 15 months by default for all security event and identity data that is processed by Reach. The timeframe is defined as is to enable your organization to benchmark and track improvement from Year-to-Year
- Once you have cancelled or terminated your use of our service, the Personal Data will be deleted within 30 days of the termination date, with the exception of data that is required to establish proof of a right or a contract, which will be stored for the duration provided by enforceable law.
- Once deleted, your data cannot be restored.
- Data deletion can be requested by the customer by contacting support@reach.security.

### Data Access and Disclosure

#### Customer Access

- You are able to view a processed representation of your data through the Reach product UI at app.reach.security with the appropriate permissions. User permissions are set by the Reach product admin in your instance settings.
- 30 days of user access logs can be requested by contacting support@reach.security. Support will respond to the request within 48 hours from the time of the request.

### Reach Access

- Access to production systems is restricted to Reach employees who need to analyze customer data for efficacy purposes and to improve the overall product for Reach customers. These employees are U.S Persons on U.S soil and go through the necessary background checks to let our customers adhere to regulations like those enforced by International Traffic in Arms Regulations. All access privileges are managed by Reach engineering leadership and audited for privilege access violations.

### AI for making mission-critical decisions

AI comes in many different flavors. We developed AI for Reach to meet the rigorous demands of enterprise security.

#### A dedicated AI Model

Reach develops a custom AI model dedicated to:

- Your enterprise
- Your users
- The threats you face

Built to be unique to your company's inputs, the model is created with your tenant and destroyed when required. This is done without impacting other Reach customers.

#### Private

By keeping third-party LLMs out of the mix, Reach AI relies on verified, domain-specific data to power its configuration engine. This means all data processed by Reach is private and not shared with third parties; nor do third parties interact with Reach.

### Mission-critical decision making

Because security decisions are critical to enterprises, Reach brings the highest level of rigor to its AI. We've built it to ensure no hallucinations. This allows your team to focus on critical security decisions, while letting data power cross-platform configuration decisions to land you at the single best result.

### Information Processed by Reach

Reach sits at the center of a few data types. Data types fall into three categories; Identity service data, Security event logs, Security product configurations. Some of the data in the Identity service data and Security event logs may contain Personally Identifiable Information.

Identity service data can come from any number of sources. Most commonly the data comes from an Identity Provider within the company, like Microsoft AzureAD or Active Directory.

Security event logs will be analyzed by Reach for a number of products when connected to Reach. You must connect these products to Reach in order for security event ingestion to occur.

Note: Reach is not a Security Incident Event Management (SIEM) product. We are only gathering a subset of the security events for processing purposes.

Security product configurations will be analyzed by Reach for a number of products when connected to Reach

The following data can be processed by Reach:

| Data Type | Data | May be Considered Personally Identifiable Information | Can be Anonymized |
|---|---|---|---|
| Directory Service Data | Name | Yes | Yes |
| | User name | Yes | Yes |
| | Email address | Yes | Yes |
| | Department | No | N/A |
| | Role Title | No | N/A |
| | Organization | No | N/A |
| | Security Groups | No | N/A |
| | Distribution Lists | Yes | Yes |
| | Proxy Addresses | Yes | Yes |
| | Location (typically office location | No | N/A |
| | userAccountPropertyFlag | No | N/A |
| | whenCreated | No | N/A |
| | whenChanged | No | N/A |
| | guid_lookup (if needed to join threat logs) | No | N/A |
| | OktaWorkerType | No | N/A |
| Security Product Logs* | Domain and username | Yes | Yes |
| | Email Address (sender) | Yes | Yes |
| | Email Address (recipient(s)) | Yes | Yes |
| | MAC address | No | N/A |
| | Hostname | Yes | Yes |
| | Qualified hostnames | Yes | Yes |
| | Operating system | No | N/A |
| | Name of Security device | No | N/A |
| | IP Address (Source) | Yes | Yes |
| | IP Address (Destination) | No | N/A |
| | URL | No | N/A |
| | File name | Yes | Yes |
| | Forensics | Yes | Yes |
| Security Product Configurations | Security product configuration files | No | N/A |

### Data Processing Locations

All customer data is processed within Amazon Web Service locations in the United States.

Current AWS Regions:

- us-west-1 (N.California)

### Access Logs

- Access logs are immutable, tamper proof and available for review upon request.

## Product Security

Reach is built with industry-tested technology and security practices.

- Reach employees are required to use Multi-factor authentication to access systems and services
- Reach adheres to OWASP guidelines and security best-practices
- Reach performs automated and manual peer review to verify application correctness and security. This invludes automated unit and integration tests run end-to-end on live systems, pre-release, and post-release scenarios
- Annual 3rd party pentest assessments are performed against Reach and all operating infrastructure

## Security Architecture