Recognize

Security | Overview

Overview

Preserving the confidentiality and integrity of your information is one of Recognize's highest priorities. This document summarizes the key measures we take in ensuring your data is always protected. Please consult your Recognize contact for the latest security overview.

How Recognize is Protected

Recognize utilizes an iterative approach in designing and improving security procedures and controls. We continuously analyze the effectiveness of our security policies to ensure we are providing optimal protection for our customers.

- Data Center Security: Recognize's servers are located in Amazon web service's world-class, highly secure data centers utilizing state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations.
- Secure Connections: All connections to Recognize are secured via SSL/TLS. Any attempt to connect over HTTP is redirected to HTTPS.
- Application Security: Recognize utilizes secure development best practices that integrate security reviews throughout design, prototype and deployment.
- Customer Data Protection: All data is classified as confidential and treated as such. Inbound and outbound low-level logical firewalls ensure that data is protected from unauthorized access.
- Hardened Operating System: Recognize runs on hardened Linux servers. Externally exposed critical patches are addressed within 24 hours.
- Internal and Third Party Testing: Recognize routinely runs internal and external vulnerability scans and penetration tests. Third party firms are utilized to perform daily application testing.
- Business Continuity: Recognize customer data is backed up daily and protected with strong encryption on disk. Backups are transferred off-site over SSH and properly deleted after 6 months.

Authentication and Authorization

Access to Recognize is restricted to employees within your organization. We provide robust features and integrations to manage your users and control your data. The browser extensions connect via Oauth.

- User Provisioning: User Provisioning is accomplished via manual invite, bulk invite, or automatic login via Oauth 2.0 or User Sync. User sync can be accomplished via Yammer, Office 365, or ActiveDirectory(LDAP) via standard queries from their respective apis.
- Password Policies: Recognize implements industry standard password policies by requiring minimum length (six characters) and are stored with a salted one-way 256 bit encryption algorithm. Brute-force password attacks are mitigated with CPU and memory bound computational constraints.
- Oauth 2.0 Authentication: Access to Recognize can be granted via an Oauth 2.0 flow. Recognize supports Google, Yammer, and Office365 Oauth. Passwords are never transmitted to Recognize via Oauth 2.0. Upon successful authentication, an api token is provided to make api requests on behalf of the authenticated user. See technology references below for more information.

> SAML Authentication: Please see our SAML Security Document - https://recognizeapp.com/recognize-security-saml.pdf

Personal information

We store the following personal user information in our database:

- Name
- Email
- Hire date(optional for service anniversary recognitions)
- Birthday(optional for birthday recognitions)
- Phone(optional - for SMS notifications)
- Password(unless 3rd party authentication such as Google, Yammer, Office365, or SAML)
- Job title(optional)
- Recognition messages, comments, approvals and other data generated via Recognize platform.

Yammer feed data and Office365 data will never be stored, however, aggregate information may be collected or analyzed.

More information at: https://recognizeapp.com/privacy

Technology References

- https://developer.yammer.com/v1.0/docs/oauth-2
- **https://msdn.microsoft.com/en-us/office/office365/howto/common-app-authentication-tasks**
- **https://developers.google.com/identity/protocols/OAuth2**