LiveTiles Reach Architecture & Security Whitepaper

July 16, 2020 | LiveTiles | Version 2.4

LiveTiles Corporation
137 West 25th Street
New York NY 10024
A public company – ASX: LVT

Content

Version History

Version	Description	Authors	Date
1.0	First release	Matthias Weibel	07.02.2018
1.1	Adaptation architecture	Matthias Weibel	08.04.2018
2.0	Supplements cloud services	Matthias Weibel	29.09.2018
2.1	Adaptation of certifications	Matthias Weibel	31.09.2019
2.2	Adaptation of data storage	Matthias Weibel	17.10.2019
2.3	Supplements Disaster Recovery	Matthias Weibel	18.10.2019
2.4	LiveTiles branding changes	Urs Wermelinger	16.07.2020

Note on the document: For the sake of readability, the male form has been chosen in the text, even if the following information relates to persons of both sexes.

1 Introduction

For us as a software and SaaS company, information security is an important aspect of our own development processes and the information architecture of our applications. On the following pages you will find a summary of the operational and technical measures taken by LiveTiles regarding information security.

2 Architecture

2.1 Overview

The architecture of the Reach application consists of a client area and a multi-layer back end. The client area consists of a web client and a mobile app, via which users can use the functions of Reach. The Web Client runs in Microsoft Azure in a Web App Service. The mobile apps are provided as native IOS and Android apps. The back-end area is used to execute the entire business logic and data management. Most of the back-end area runs on services within Microsoft Azure. The following functionalities run on cloud services outside of Microsoft Azure:

- **OneSignal:** Mobile Push Notifications
- **SendGrid:** Email Notifications
- **Kraken.io:** Processing of images
- **Unsplash:** Picture archive

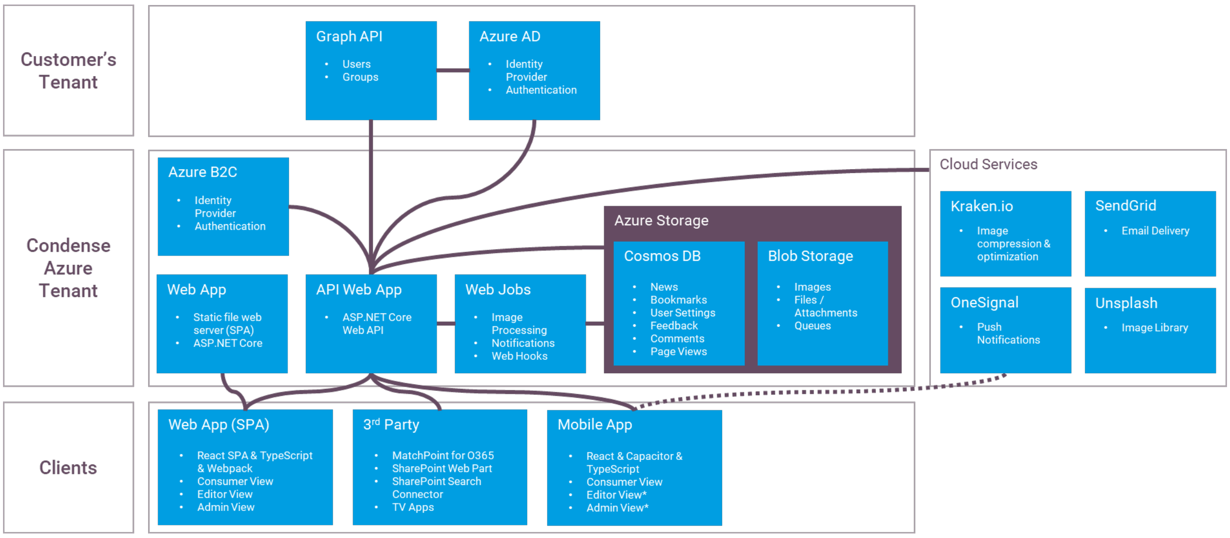

Figure: High-level Architecture LiveTiles Reach

2.2 Application Permissions

LiveTiles Reach can use Azure Active Directory to identify and authenticate users in your organization. Reach requires access to the Azure Active Directory and the Microsoft Graph. The required permissions can be approved by an administrator via App Permissions.

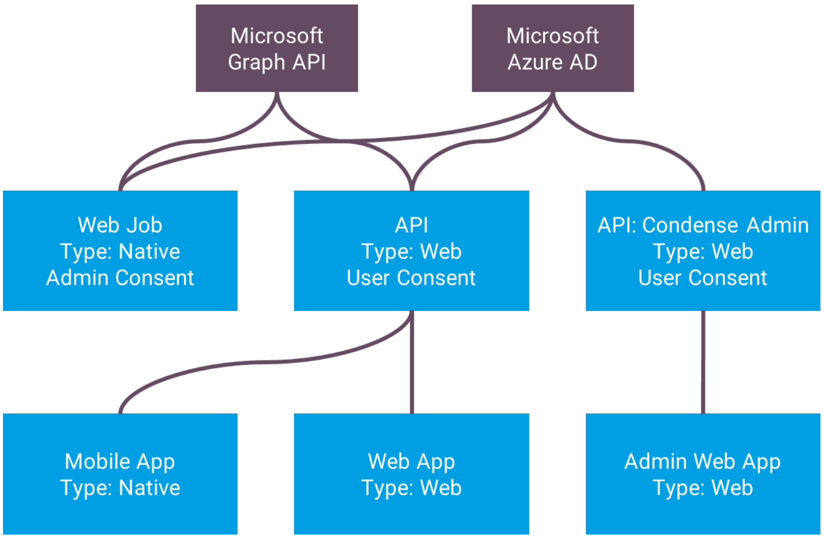
Microsoft Graph API
Microsoft Azure AD
Web Job Type: Native Admin Consent
API Type: Web User Consent
API: Condense Admin Type: Web User Consent
Mobile App Type: Native
Web App Type: Web
Admin Web App Type: Web

Figure: Application permissions of LiveTiles Reach

The information about your organization and users retrieved from the Azure Active Directory or Microsoft Graph is used to authenticate users or display user information within the application. Of this data, only a minimal set is stored within Reach. An overview of the stored data can be found in Chapter6.4.1 Overview of Stored Data.

3 Server and Infrastructure Protection

3.1 Physical Security

Reach's services are hosted on Microsoft Azure. The Microsoft Azure services are operated in the Azure region "Europe West", which is located near Amsterdam (Netherlands).

3.2 Network Security

3.2.1 Protective Measures

Intrusion detection and prevention is regularly performed by Microsoft on Azure to ensure the best possible protection of our system. Furthermore, Microsoft Azure servers are protected against Distributed Denial of Service (DDoS) attacks.

3.2.2 Access Rights

Access to Reach's servers and services is limited to a limited group of system engineers who perform regular monitoring and verification of access. A mandatory two-factor authentication is required for access to the production environment.

3.2.3 Security Incident Management

With the help of a Security Incident Event Management System (SIEM), the available logs of all services running on Azure are collected and analyzed for correlating events. The security team is automatically notified by the SIEM in case of conspicuous events. In the event of a system alarm, security incidents are escalated 24/7 to our Reach Security Team. Our employees are trained to respond to security incidents. This includes both communication channels and escalation channels.

3.3 Data Encryption

3.3.1 Transport Encryption

All communication between client and services as well as between services is done via HTTPS using the TLS 1.2 protocol (if supported by the customer), which is secured with 2048-bit RSA key and AES encryption. The older, weaker SSL protocol is disabled.

3.3.2 Memory Encryption

Reach data is stored encrypted in all Microsoft Azure services (Encryption at Rest). Encryption is performed using the AES-256 algorithm.

3.4 Disaster Recovery, Backup and Redundancy

3.4.1 Availability

The availability of Reach is 99.9% based on Microsoft's guaranteed minimum availability of the underlying Azure Services. In the event of a system failure, our system engineers can completely restore the system in accordance with the guarantees set out in the SLA.

Based on this, the following services achieve a higher value:

- Azure App Service 99.95%
- Azure Cosmos DB 99.99%
- Azure SQL 99.99%

3.4.2 Backup Retention

If a database is accidentally deleted, the database can be restored within 30 days. In addition, seven daily and four weekly backups are maintained in the event of manipulation or data corruption.

3.4.3 Disaster Recovery

Recovery Time Objective (RTO)

By using high availability technologies and triple replication within a data center, Azure can meet the recovery target time after an incident of 8 hours and initiate failovers independently.

Recovery Point Objective (RPO) Cosmos DB

If a database is accidentally deleted, the database can be restored within 30 days. Microsoft makes automatic snapshots every 4 hours, which can be restored by Azure Support. In addition, a backup is created every 12 hours in the event of manipulation or data corruption.

Recovery Point Objective (RPO) SQL DB

For SQL databases, automatic transaction log backups are made every 10 minutes and differential backups every 12 hours. Transaction log backups with full and differential backups allow you to restore a database at a specific point in time of all backups made.

Recovery Point Objective (RPO) Storage

For the Azure Storages, a copy is backed up every 4 hours at a data center in another region (Europe North).

3.4.4 Emergency Plan

The recovery team's approach to the various disaster scenarios is defined in our disaster recovery plan. This allows a quick recovery of the systems in the event of a disaster. The Disaster Recovery Plan records all restore processes, as well as a proven step-by-step guide that allows each engineer in the team to rebuild the Reach infrastructure in a new tenant.

3.4.5 Monitoring

Server logs that are relevant to security are stored in a centralized manner, are analyzed and have an automated alert system. 24x7 review and automated warning ensures that Reach system engineers can act quickly in the event of a service interruption, such as unexpected restarts, security incidents, update requests or performance bottlenecks.

4 Development Safety

4.1 Environment Separation

LiveTiles Reach development, test and production environments are logically separated. Production data is never used for testing purposes and is never transferred from the production environment to the test environment.

4.2 Quality Assurance

Every time Reach code is changed, automated test series are performed, and the changes are not implemented until all tests have been successfully completed. In addition, manual testing and quality assurance are performed in an isolated test environment that is not accessible to normal users.

4.3 Review Process

All changes in Reach's code are peer reviewed by senior developers with a broad knowledge of application security.

4.4 Framework Security Controls

In the development of Reach, best-practice mechanisms are applied to protect against common threats to web applications such as SQL injection, cross-site scripting or cross-site request forgery. In addition, measures are being implemented to avoid the weaknesses listed in the OWASP Top 10.

4.5 Security Checks and Automated Tests

The application undergoes automated and manual testing every time the code is changed and every time it is released. All changes in the application are subjected to a series of extensive API and integration tests as well as unit tests and static analyses.

5 Application Security

5.1 Access Rights and Roles

Reach ensures that users have access to exactly the data they are authorized to access. The security model of the application is based on the fact that within the Reach App access rights and administrator roles can be individually adapted to the needs. Users can be assigned appropriate roles within security groups to control access to content.

5.2 User Management

Users of the Reach App can be invited in several ways. Reach can be assigned to an Azure Active Directory. Users who are members of this directory can access the app directly without having to be invited beforehand. Other users, from outside the Azure Active Directory, can be invited via their email address.

5.3 User Authentication

User authentication is based on OAuth 2.0 using access tokens. Authentication runs via Azure Active Directory or Azure Active Directory B2C. Password strength can be set in your company's Azure Active Directory. A two-factor authentication can also be activated here.

5.4 Single Sign-On (SSO)

Single sign-on is provided via authentication via Azure Active Directory or Azure Active Directory B2C.

5.5 Storage of Login Information

LiveTiles Reach does not store logon information. Because authentication is performed through Azure Active Directory or Azure Active Directory B2C, credentials are managed through these systems or the services associated with Azure Active Directory B2C. Passwords are never stored on the user's device or browser: instead, an OAuth token is securely stored. The token is deleted from the mobile devices when the user logs out or uninstalls the app. Authentication tokens expire automatically if they are not used for a long time.

5.6 API Security & Authentication

Customers who wish to use Reach's Web API directly can do so using dedicated API tokens via HTTPS.

5.7 Data Transmission Security

The communication between the Reach Web Client, the mobile app and the server runs over HTTPS with TLS 1.2 (if possible).

6 Data Protection

6.1 Security Policy

Reach has an assigned privacy officer.

6.2 Confidentiality Agreement

All our employees have signed a privacy statement that governs the handling of data in internal and external relationships. The data protection sheet is in accordance with the Swiss laws on data protection and DSGVO-compliant.

6.3 Limited Access

Access to our production system is limited to a small number of employees who are responsible for maintenance. All employees who access Reach's data must log in using two-factor authentication and are subject to strict password policies.

6.4 Data Storage

The data stored on Reach's servers is used exclusively for the operation of the entire application or is used to improve the application. The quantity and quality of the stored data are minimized, so that as little data as possible, in particular personal data of the users, are stored. Data will only be transmitted to those services (Microsoft Azure, SendGrid, OneSignal) which are required by Reach for the execution of functions.

Stored data can be deleted by Reach system engineers at any time upon request. The deleted data is retained during the lifetime of the data backups. The final deletion of the data takes place with the deletion of the data backups.

LiveTiles Reach is DSGVO compliant.

6.4.1 Overview of Stored Data

LiveTiles Reach

- Azure Active Directory ObjectID
- Azure TenantId
- User Principal Name (UPN) of the user
- E-mail address of the user
- Display name of the user
- Date of the user's last login via the Web Client
- Date of the last login of the user via the Mobile Client
- Bookmarks of the user
- User settings for notifications
- Subscribed channels of the user
- Favorites Contacts of the user

SendGrid

Data of the e-mail messages sent:

- Recipient's e-mail address
- Subject
- Message content

OneSignal

Data of the Mobile Push notification sent:

- Message content

6.5 Certifications

LiveTiles Reach uses services from Microsoft Azure, which are hosted on the servers of Microsoft Azure. Microsoft Azure is provided with the following compliance certifications:

- C5
- CDSA
- CIS benchmark
- CSA-STAR
- EBA
- EN 301 549

- ENISA IAF
- EU Model Clauses
- EU-U.S. Privacy Shield
- FINMA
- GxP
- HIPAA/HITECH
- ISO 20000-1:2011
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 9001
- IT Basic Protection Workbook
- ITAR
- MPAA PCI DSS
- shared assessments

More details about Microsoft certifications can be found here: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings