DATA AND SYSTEM SECURITY

AWAREX DIGITAL OMNI-CLIENT

TECHNICAL PAPER

2020

200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

TABLE OF CONTENTS

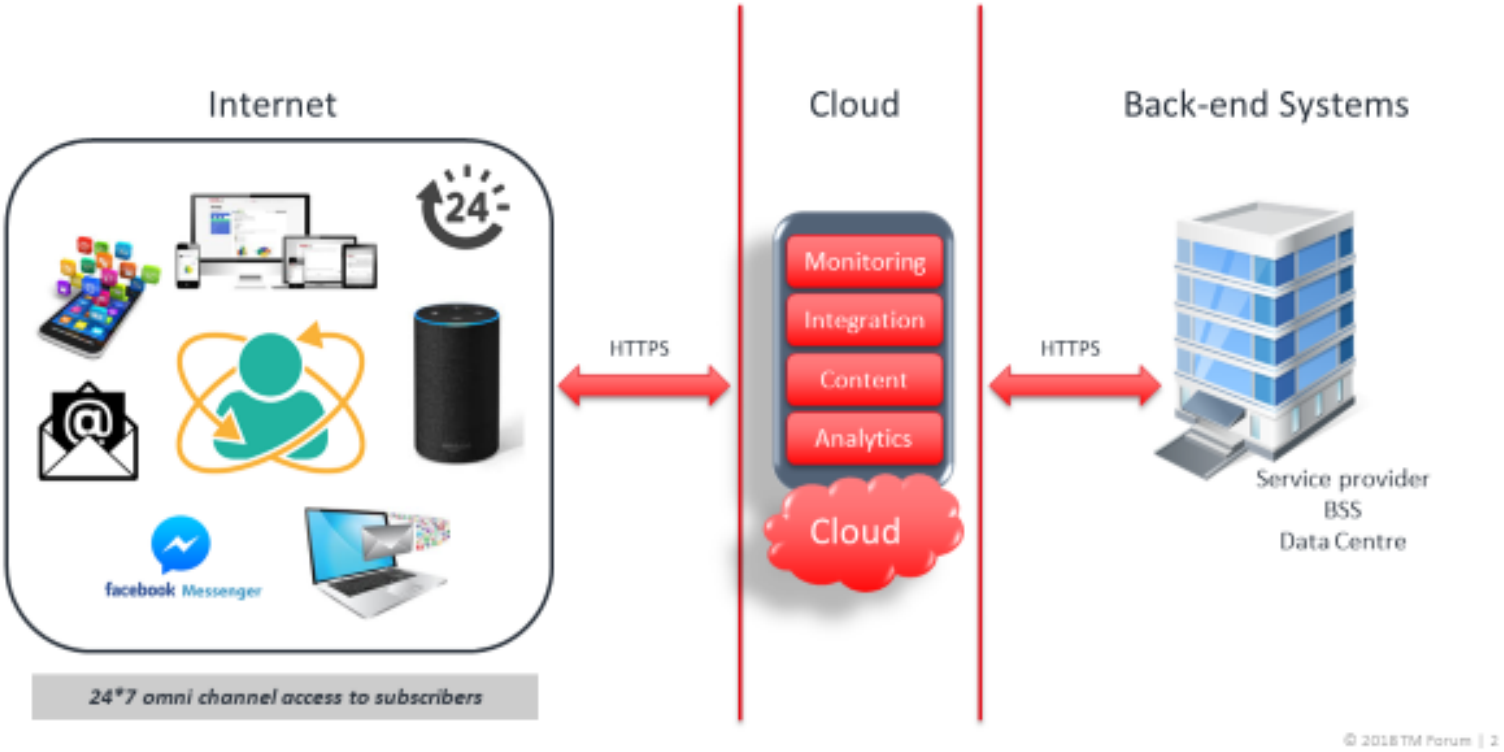
200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

SUMMARY

Data security, system security and personal data protection are key issues for the Communications Service Provider industry. As a regulated industry it is even more under scrutiny than other industries and pays special attention to protecting its customers data. The recent GDPR personal data regulations place a further layer of awareness and compliance requirements for protecting personal data and controlling its usage. This document explains how AwareX handles end user data and explains the security aspects of AwareX's digital Omni-Client SaaS product.

HIGH LEVEL ARCHITECTURE

This diagram shows the high-level architecture of the end-to-end system.



200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

SOLUTION OVERVIEW

The awareX digital Omni-Client solution consists of the following main components: -

1. **Client applications** – These consist of native mobile applications (iOS and Android), web application, SMS Chatbot, Facebook Messenger Chatbot and Amazon Alexa skill. These are the digital channels used by end users for self-service.
2. **Integration Platform** – This connects to the service provider's backend system and uses APIs exposed by the backend systems, to get end user specific data. The integration platform **does not** store any data and does not use a database. It simply passes the data through to the clients after applying business rules and transformations.
3. **Monitoring Platform** – Log files from the Integration Platform and metrics from the operating system are analyzed and displayed in the monitoring platform.
4. **CMS –** Content Management system stores information that is not user specific and information that is/can be publicly accessible. Examples include marketing banners, store list, FAQ etc.
5. **Analytics–** The analytics platform is used for app analytics, dashboards, reporting, segmentation for marketing purposes and push messaging during marketing campaigns. AwareX analytics is an integrated substantiation of a cloud based 3rd party SaaS product.

CUSTOMER DATA ACCESS

AwareX systems are not the systems of record for the data that is viewed by end users. AwareX does not store information displayed to customers in any databases in the cloud. When a request is made for data by the client application, the Integration platform makes a request to the backend and returns the data to the client after performing validations and data transformations.

USER AUTHENTICATION AND IDENTITY MANAGEMENT

END USERS

AwareX is NOT the system of record for user identity, authentication and authorization. AwareX works with a variety of mechanisms provided by the Service Providers existing enterprise architecture to manage user authentication. AwareX will ensure that user data can only be accessed after successful validation of user credentials.

AwareX generates a token after successful authentication by the service provider's identity management system and this token is specific to a user. This prevents token reuse for unauthorized data access. Tokens also have a short expiration time and expire after inactivity.

AwareX supports two features related to user authentication that impact security: -

- **Touch ID / Face ID –** AwareX mobile applications use iOS and Android supported standard mechanisms to enable this feature. User's password is stored on the device and unlocked by the operating system after successful fingerprint recognition/facial recognition**.**

200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

- **Keep Me Logged In –** When this feature is enabled, the user's password is encrypted and stored on the device. iOS utilizes the keychain to store this information.

Both of these features are optional and can be turned off.

ADMIN USERS

AwareX provides admin console access to the following systems to users from the service provider's organization.

- CMS Platform
  - AwareX will set up and manage access credentials. In addition, access to the console requires the admin user to install an SSL certificate as an additional security measure. Under our default configuration, we do not use a default username for the administrator, and we maintain very strong and unique passwords in order to defeat dictionary attacks or brute force attacks. Brute force attacks are also protected by the AWS cloud firewalls. A report from – howsecureismypassword.net shows it will take at least 1 Octillion years for a brute force attack to crack the password.
- Analytics Platform
  - AwareX will send invitations to specific email addresses specified by the service provider for access to view analytics data and set up marketing programs. Users can then set up their own credentials.
- Monitoring Platform
  - AwareX will set up and manage access credentials.

AwareX plans to support SAML 2.0 compliant security providers in the future for admin access to the systems listed above.

DEVICE SECURITY

In order to provide the best possible user experience, some of the data that is displayed to end users is stored on the user's phone by the mobile applications. AwareX expects that device security is the end user's responsibility and the end user will take sufficient steps to protect his/her device. All iOS and most Android devices require and/or provide security features from password enforcement to biometric security.

INFRASTRUCTURE SECURITY

AwareX uses Amazon Web Services (AWS) for infrastructure and other services to drive self-service application. AWS provides industry leading security and reliability, which we are then able to make available to our customers. Within AWS, AwareX uses the following security measures: -

- Each customer system is isolated and runs in its own independent AWS VPC.
- Production environment is isolated from non-production environments in a separate VPC
- AWS accounts are accessed by AwareX team members using Multi Factor Authentication ('MFA')
- AWS services and systems are accessed using AWS recommended best practices such as IAM roles (as opposed to keys)

200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

AwareX uses AWS regions that are geographically closest to the majority of the service provider's customers. However, for service availability and performance reasons AwareX may use multiple or different regions.

DATA SECURITY IN TRANSIT

As seen in the high-level architecture diagram, client applications use HTTPS to use industry standard data encryption during data transmission. As long as the backend systems support TLS, the Integration Platform will also use https to communicate with the backend systems. AwareX has used a variety of mechanisms to securely connect to backend systems such as the use of IPsec VPN Tunnels, use of secret keys for system to system communication as well as asymmetric key encryption. AwareX's preferred mechanism is the use of an industry standard mechanism such as JWT Token.

DATA STORED IN LOGS

The Integration platform logs all requests that reach the server. User specific information that is logged include: -

- SHA-256 of line/account number used during app data access
- An anonymous device identifier specific to a device

Log files are stored on the server for 2 weeks and then archived in AWS S3 storage.

DATA COLLECTED FOR APP ANALYTICS, PUSH NOTIFICATIONS AND CRASH REPORTING

AwareX uses industry standard SaaS products, the details of which are listed below.

Crash Reporting and Analysis

AwareX mobile applications include the Crashlytics SDK (owned by Google), which collects data for crash reporting.

Data points collected as part of this include: -

1. Anonymous device identifier
2. App Version, OS Version, Device Model
3. IP Address
4. Usage time, duration
5. Jailbroken status
6. Details of crashes if any

App Analytics and notifications

AwareX mobile applications include the Localytics SDK and Google analytics SDK for app analytics. These SDKs send information respectively to the Cloud based Localytics and Google analytics systems.

Data sent to Localytics and Google include: -

1. Anonymous device identifier

200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

2. App Version, OS version, Device Model
3. IP Address
4. Usage time, duration
5. Jailbroken status
6. Device locale

Data sent only to Localytics

Features utilized by the user during app usage are sent only to Localytics. This helps AwareX and the service provider in understanding which features are being utilized by end users, leading to the evolution of a better product.

Examples of data sent: -

- Login screen viewed
- Home screen viewed
- Top-up purchased along with amount
- Service type of the account used to access a feature such as 'prepaid', 'postpaid' etc.
- A SHA-256 hash of the user id used to login (if available). All non-fixed length user identifiers are considered anonymous due to the properties of a standard hashing function such as SHA-256. This is an optional data identifier and can be turned off if needed with trade-offs in functionality.
- A SHA-256 of the line number/account number used to view the home screen. This is optional and can be turned off if needed.

Data collected as part of push notifications

AwareX uses Google and Apple provided mechanisms to support push notifications. Google requires android apps to include the firebase SDK to support push notifications. Firebase collects information from the apps – typically a device identifier and information such as app version, OS version, device model, usage times, duration etc. This data goes to Google and is stored according to Google's data storage and use policies.

PEN TESTING

PEN testing is recommended and has been performed and completed with prior customer implementations (within the EU). This is not included as standard in the awareX offering due to its service intensive nature but is available upon request. Permission is required (but not unreasonably withheld) from AWS for testing to be performed on a scheduled basis.

GDPR

The GDPR came into force on the 25th May 2018. It contains extensive provisions for personal data protection, usage and individual rights regarding data held about them. AwareX is not the system of record for any personally identifiable data but it does connect to such systems. AwareX will enable any back-end functionality which is required for GDPR compliance in the apps. The AwareX system itself does not hold any personally identifiable data.

Specific GDPR functions

200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

AwareX assess that the following functions are required to be compliant with GDPR requirements: -

Analytics

1. Prompt users prior to analytics data collection. This will apply to app analytics data (Google and Localytics) and not to Crashlytics, since AwareX believes that only anonymous data is stored as part of Crashlytics
2. Make it possible for end users to turn off analytics data collection
3. Make it possible for end users to request all their data collected
4. Make it possible for end users to ask for their data to be deleted

Logs

1. AwareX will stop recording SHA-256 hashed MSISDNs or any known fixed length numeric identifiers
2. AwareX will work with 3rd party services to ensure GDPR compliance

Note that: -

AwareX will continue to record SHA256 hashed user identifiers that are not fixed length, since those are considered anonymous

GDPR does not require data storage within the EU as long as the data processor has appropriate DPAs in place.

Some additional security questions that we get asked are as follows: -

- Brute Force Attacks. More than 1 Octillion years to crack the password

- File Inclusion Exploits. This does not affect the system as we do not use the content management system as a public website, we only expose public information under API, and files operates using the cache.

- SQL Injections. This does not affect the system as we do not host a public website with WordPress, we only expose public information under API.

- Cross-Site Scripting (XSS). This does not affect the system for the same reasons as given above. For XSS you require website content, we don't have one.

- Malware. This is managed with operational processes, all software we install are validated by cryptographic signature (official repositories), and only could happen at server upgrade windows.

In addition, our servers are upgraded at least twice per year in order to receive all security updates. In the case of CVE risk, we may upgrade even more frequently, as described in our contracts.

https://www.awarex.com/data-security-policy?

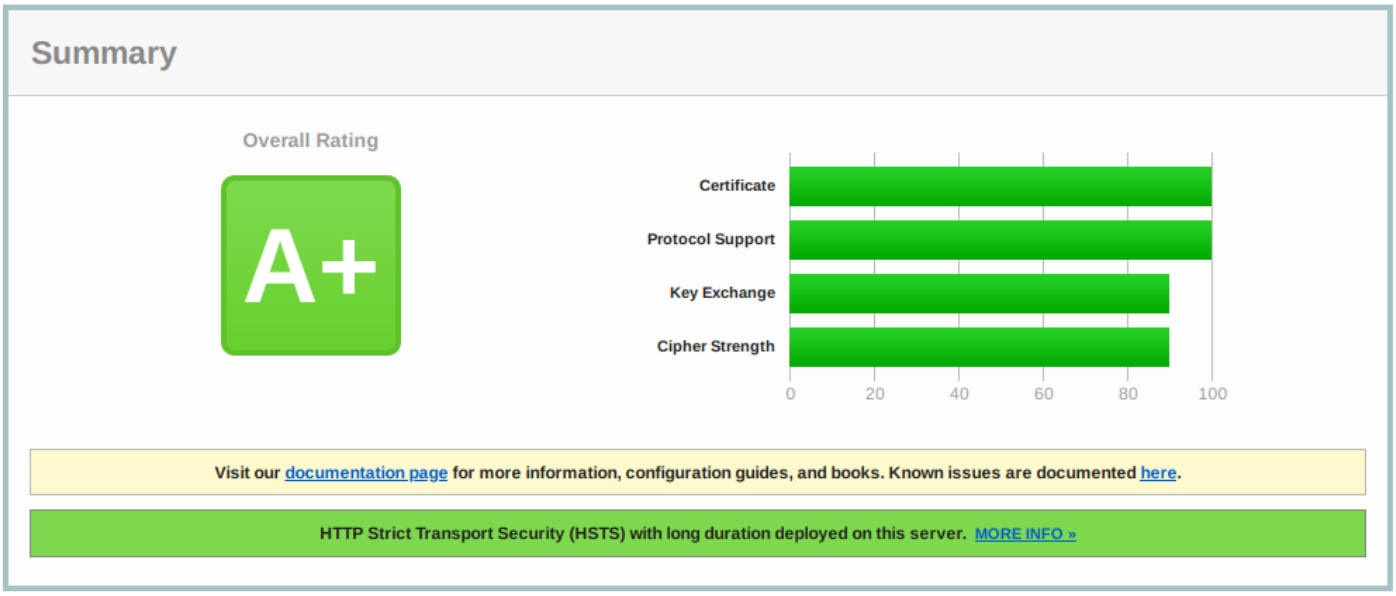
https://www.awarex.com/terms-conditions?

200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com

As of 2019 our SSL security is ranked B from Qualys SSL Labs in order to maintain high security standards. For 2020 and beyond we are upgrading further in order to keep an A rank without affecting legacy devices.

(UPDATE) January 2020.

As per the above commitment AwareX has been awarded a score of A+ under SSL Labs Test. This has been achieved whilst still maintaining support for older devices such as Android 4.4+, iOS 6+, and older versions of Windows and Mac OS desktop browser support.



The impact of this enhanced security is that AwareX is mitigating even better any security vulnerability between the user's device and the data server communication. To achieve this rating whilst supporting older devices is a tremendous achievement of our engineers allowing flexibility of device use by end users.

200 Portland Street Boston Massachusetts 02114 USA | W awarex.com | E Info@awarex.com