# InformaCast® Fusion™ Security

InformaCast Fusion delivers secure messages to mobile and on-premises devices. Singlewire protects data at rest and in transit, which safeguards messages that may contain sensitive or proprietary information.

Singlewire understands data security is top of mind, and utilizes security best practices to ensure your data is never at risk.

singlewire® software

# At Rest Data Protection

Data at rest in the InformaCast Fusion cloud is encrypted. InformaCast users are encouraged to familiarize with the security policies relevant to their organizations to avoid violations. Only enter information into InformaCast as is allowed under your organization's guidelines and regulations. Additionally, Singlewire employs the following methods to keep our customers' data secure:

## PRODUCT DEVELOPMENT

Every InformaCast feature goes through a security audit to look for data handling, privacy, authentication or authorization issues. New features are examined using threat modeling to imagine how it could be misused. Protections are put in place for any potential issues that are uncovered.

## REDUCED ATTACK SURFACE

InformaCast is designed to include only the necessary components and data and limit what and how services are provided to limit the tool's attack surface. In the InformaCast Fusion cloud, each server is stripped to its bare essentials. Applications only have access to the APIs and the data within the cloud they need to perform properly. All applications use app-specific credentials to authenticate each API or database call.

## VULNERABILITY MANAGEMENT

DevOps installs regular upgrades to keep the systems that run notifications up to date.

## WORK TRACKING

Singlewire Software uses a ticketing system to track changes in development, in DevOps and in fulfillment.

## BACKUP/RESTORE AND BUSINESS CONTINUITY

Hierarchical data backups are stored in AWS at Singlewire and offsite. Recovery procedures are practiced monthly.

## NON-REPUDIATION

Singlewire employees do not use shared accounts to administer our production system. Each change can be traced back to an individual.

## AUTHENTICATION

Administrative interfaces require multifactor authentication.

# At Rest Data Protection (cont.)

## ENCRYPTION AND HASHING

Information stored in our software uses encrypted storage.

## LOGGING

IInformaCast Fusion creates administrative and security logs. Singlewire investigates security events when they occur.

## DATA PRIVACY

Singlewire only collects user information needed to perform the tasks users sign up for. Services are hosted in US data centers, and we comply with GDPR and CCPA regulations.

## RESTRICTED ACCESS

Only Singlewire Ops Team members have access to our production cloud. The Ops team can only access InformaCast Fusion from the Singlewire corporate network. Each team member uses their own credentials, and external superuser access is not available.

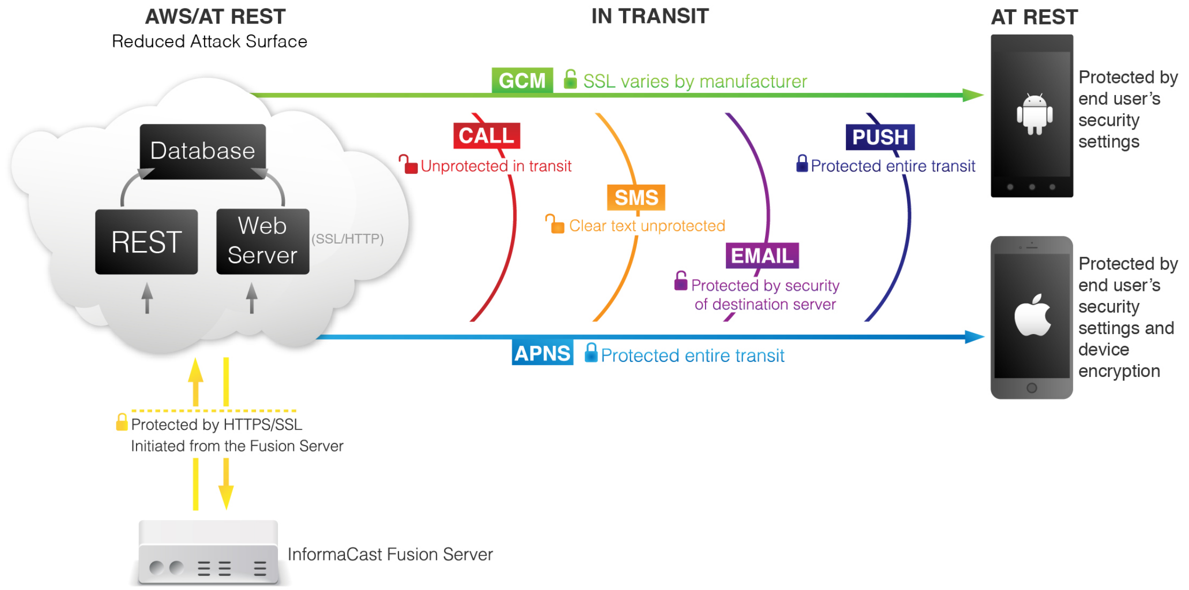
## 24/7 MONITORING

Operations and security are monitored 24/7.

## REGULAR SECURITY AUDITS

Internal audits are conducted on a quarterly basis, in addition to an annual external security audit.

# Data Protection


AWS/AT REST
Reduced Attack Surface
IN TRANSIT
AT REST
Database
REST
Web Server
(SSL/HTTP)
GCM
SSL varies by manufacturer
CALL
Unprotected in transit
SMS
Clear text unprotected
EMAIL
Protected by security of destination server
PUSH
Protected entire transit
APNS
Protected entire transit
Protected by end user's security settings
Protected by end user's security settings and device encryption
Protected by HTTPS/SSL
Initiated from the Fusion Server
InformaCast Fusion Server

## PUSH NOTIFICATION SECURITY

- InformaCast Fusion sends a notification via Apple Push Notification Service (APNS). It is secured with APNS certificates/tokens, and contains the notification ID and the subject.
- The InformaCast app requests the remaining message content, including the remaining body, image, audio, and confirmation request. This is sent over TLS (SSL) and secured with InformaCast app certificates. The TLS (SSL) connection is terminated on load balancers behind Singlewire's cloud-based firewalls.
- InformaCast Fusion sends the remaining message content and confirmation responses, which are protected by TLS (SSL).
- InformaCast Fusion's use of Google Cloud Messenger (GCM) is analogous to its use of APNS.

## SMS SECURITY

- SMS notifications are not protected in transit, nor are they protected on the phone.

## CALLING SECURITY

- Calling notifications are not protected in transit.

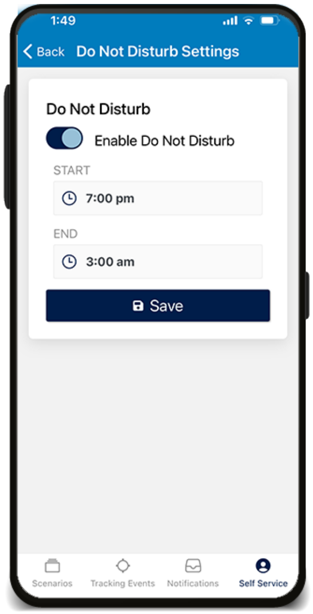
## EMAIL SECURITY

- Email notification security depends on the receiving email server's configuration. If it supports TLS (SSL), then the content is protected. If it doesn't, then it is not.

## FUSION SERVER SECURITY

- Initiated by the server
- Secured by TLS (SSL)
- API, web console and logins are disabled
- Minimalist operating system also has a minimal attack surface
- Fusion server backups encrypted with customer supplied keys and stored in AWS. Customers are responsible for setting the encryption key on first boot. This keeps customer information separate, providing an added level of protection.

# On Device Data Security



Do Not Disturb Settings

Do Not Disturb

Enable Do Not Disturb

START 7:00 pm

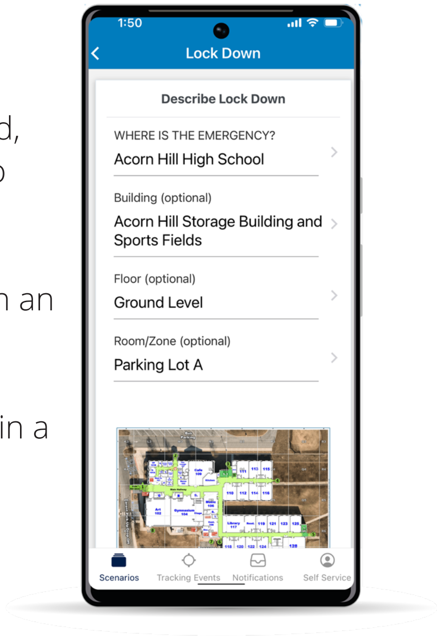
END 3:00 am

## IOS DEVICES

- Images and audio are stored unencrypted in the user's document directory, but access to these files is limited by iOS to the InformaCast app.
- The Subject, Header, Confirmation Requests, Responses, etc. are stored, unencrypted, in a database.

## ANDROID DEVICES

- Images and audio are stored, unencrypted, on the user's emulated SD card. Access to these files is available to any application with file system read permissions. No method is available to protect this data on an Android device.
- Subject, Header, Confirmation Requests, Responses, etc. are stored, unencrypted, in a device cache.



Lock Down

Describe Lock Down

WHERE IS THE EMERGENCY? Acorn Hill High School

Building (optional) Acorn Hill Storage Building and Sports Fields

Floor (optional) Ground Level

Room/Zone (optional) Parking Lot A

# User Authentication

## CUSTOMER-PROVIDED IDENTITY PROVIDER

- Singlewire asks those systems for permission, delegating authentication to the user. Singlewire does not store user passwords.

## SINGLEWIRE NATIVE IDENTITY PROVIDER

- User IDs and passwords are stored encrypted in the InformaCast Fusion service database.
- Users are able to select two-factor authentication with the IDP.

# Security Practices

## LEAST PRIVILEGED ACCESS

- All services run with the least privileged access required to function.

## SERVER SEGREGATION

- In InformaCast, all server types are segregated and only allowed to talk between servers of different classes or types through tightly controlled ACLs.

## PROTECTED SERVERS

- There is no direct access to any of Singlewire's protected API, web or database servers.

## CONTROLLED ACCESS

- Access is controlled through a Bastion server. Access to the Bastion server is restricted to Singlewire's corporate network.

## DEFAULT DENY FIREWALL RULES

- Only the minimum amount of traffic is allowed between the various InformaCast servers. Rules are audited quarterly to ensure only the required traffic is allowed.

# Data Management

## STORED DATA

- The only data InformaCast has to store is a user's first and last name, email address and phone numbers. This information is required to store the user in the system, but does not automatically include the user in distribution groups.

## NOTIFICATION DATA

- Data is tracked for the notifications a user receives, as well as distribution lists and security groups the user belongs to.
- Statistics for sent notifications are also stored.