



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.

At Rest Data Protection

Data at rest in the InformaCast Fusion cloud is not encrypted, but it is well protected. Singlewire employs the following methods to keep our customers' data secure:

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.

Two-Factor Authentication

The Ops Team uses two-factor authentication to access the AWS console.

Reduced Attack Surface

In the InformaCast Fusion cloud, each server is stripped to its bare essentials to reduce its attack surface. 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.

Redundant Backup

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

Dual Logging

Servers, applications and databases utilize operational and security logging.

24/7 Monitoring

Operations and security are monitored 24/7.

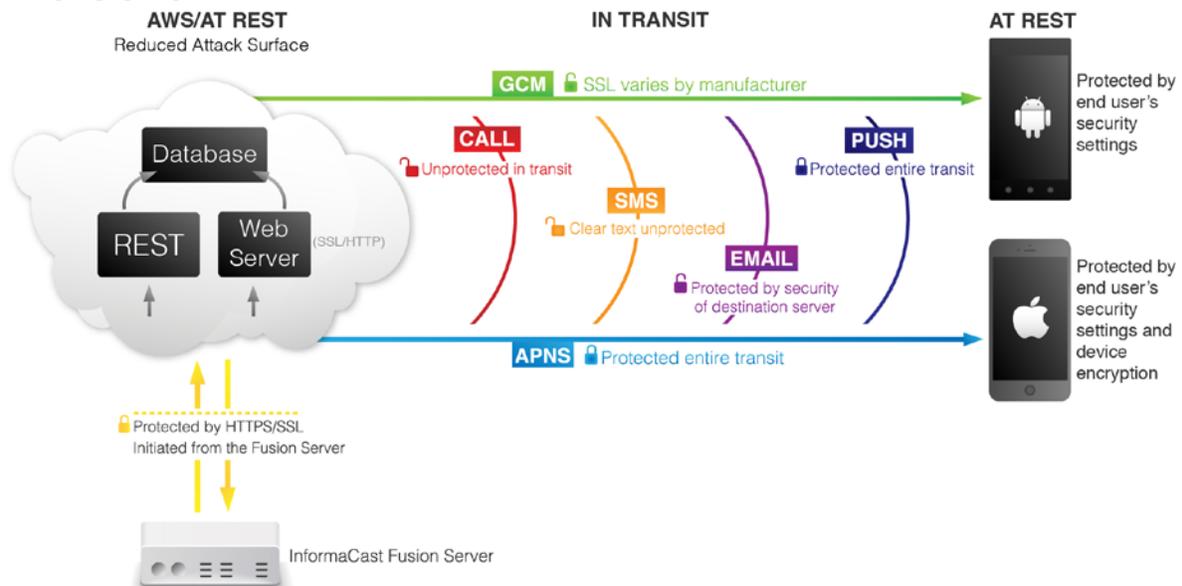
Regular Security Audits

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

Quarterly Disaster Recovery Drills

Once a quarter we exercise the Fusion disaster recovery protocol to ensure our ability to maintain service delivery.

Data Protection



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 Mobile App requests the remaining message content, including the remaining body, image, audio, and confirmation request. This is sent over SSL and secured with InformaCast Mobile App certificates. The 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 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 SSL, then the content is protected. If it doesn't, then it is not.

Fusion Server Security

- Initiated by the server
- Secured by 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.

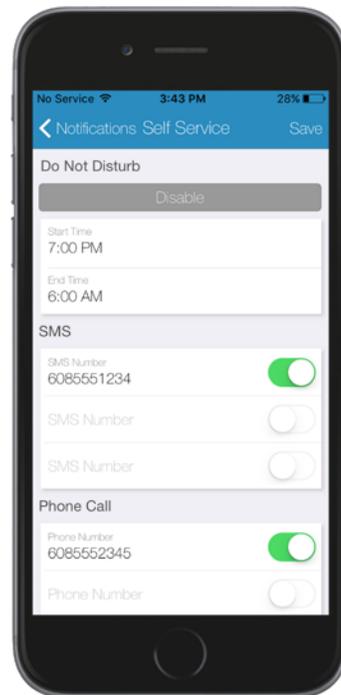
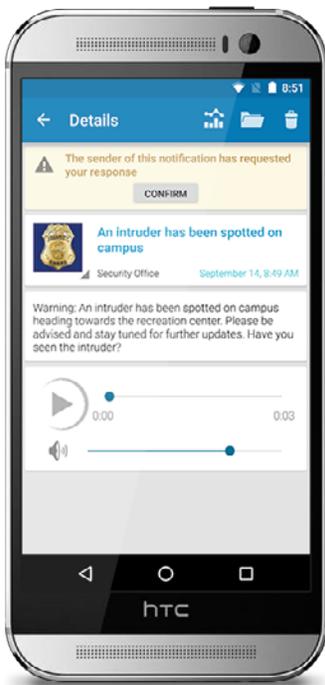
On Device Data Security

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 Mobile 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.



User Authentication

ADFS, Google and Azure

- For ADFS, Google and Azure, Singlewire asks those systems for permission, delegating authentication to the user. Singlewire does not store user passwords.

IDP

- 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 Mobile, 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.

Contact Singlewire Software

+1 608-661-1140, option 1 | sales@singlewire.com