London
35 Kingsland Rd
London
UK, E2 8AA

New York
817 Broadway
New York, NY
USA, 10003

Melbourne
172 Wellington St
Collingwood, VIC
Australia, 3066

Proximity Insight: Security Policy

The Retail Hub platform for Shop Floor Engagement

PURPOSE

Proximity Insight is committed to building reliable and secure business applications that our customers can depend on. This Policy provides our customers with transparency in relation to how Proximity Insight has been architected to ensure their information always remains protected, secured and available.

SECURITY FRAMEWORK

Proximity Insight leverages the following cloud-based services:

- Salesforce.com
- Heroku.

These services have been selected in part due to their commitment to ensuring the security of the information hosted on their infrastructure.

Salesforce.com

Salesforce.com understands that the confidentiality, integrity, and availability of their customers' information is vital to their customers' business operations and their own success. They use a multi-layered approach to protect that key information, constantly monitoring and improving their application, systems, and processes to meet the growing demands and challenges of security. For further information please visit the Salesforce.com Security Overview web page.

Heroku

Heroku's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX).

For further information please visit the Heroku Security Overview web page.

ENVIRONMENTAL SAFEGUARDS

Physical Security of Facilities

Proximity Insight employees do not have physical access of any kind to our production facilities, as all of our infrastructure is cloud-based. Each of our cloud-based service providers ensure that their production facilities are physically secured using a number of best-practice security measures including:

- Natural boundary protection
- 24-hour, secured ingress points
- Professional security personnel
- State-of-the art video, audio and electronic surveillance systems
- Stringent authentication processes.

Fire Detection and Suppression

All of our service providers invest heavily to ensure that adequate fire protection and suppression systems are in place. Protective measures include but are not limited to:

- Installation of automatic fire detection and suppression equipment
- VESDA (very early smoke detection apparatus)
- Fire detection systems utilise smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms
- Areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power Protection

Electrical power systems are designed to be fully redundant and operational 24 hours a day, seven days a week:

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage.

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

NETWORK SECURITY

Heroku utilises firewalls to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk. Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications.

Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

Heroku infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Heroku utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

HOST SECURITY

Heroku leverages AWS for all their computing infrastructure. Security groups are provided to limit access to devices. We fully utilize security groups to limit access to our computing resources. Our production environment is completely separate from the other environments, including development and QA.

We adhere to strong password policies and require that all RSA private keys be encrypted with a compliant password.

Automated processes are in place on each host that monitoring for unauthorized login attempts, with the offending IP address being automatically blacklisted and an alert being generated.

The servers utilised by Proximity Insight is an optional multitenant platform or built using repeatable build processes powered by Heroku. All changes to the production environment pass through a peer-review change management process, with all changes logged to a central ticket system.

London
35 Kingsland Rd
London
UK, E2 8AA

New York
817 Broadway
New York, NY
USA, 10003

Melbourne
172 Wellington St
Collingwood, VIC
Australia, 3066

APPLICATION SECURITY

Encryption

We have implemented strong encryption via SSL in our application. By using encryption, we minimize the chances of someone possibly intercepting username/password combinations and/or other sensitive information. Areas where we utilize SSL include:

- All application logins require SSL
- The entire application and API interfaces leverage and requires SSL throughout.

Authentication Tokens

OAuth tokens to external services are encrypted in the database. The encryption keys are stored outside of the codebase and outside of the access from anyone without production access.

Testing

Proximity Insight is dedicated to ensure our product is secure. To do this, we test the application in a three stage process.

1. Production
2. Packaging/QA
3. Development

Before anything is deployed to Production, we work through the Salesforce Security Review Requirements Checklist.

Data Storage & Retention Policies

The only data that is stored outside of Salesforce is a messaging platform on Heroku that stores messages and Salesforce.com IDs, no personal information is stored or cached on this layer. Proximity Insight acts as a conduit to route data between Salesforce and the End-user mobile application. A Postgres database is utilised to store messages to ensure speedy delivery to end users.

All communications between these points are encrypted using SSL.

Access to Customer Data

Proximity Insight employees do not access or interact with customer production data as part of normal operations. There may be cases where we are requested to interact with customer data at the request of the customer for support purposes or where required by law. Proximity Insight employees cannot physically access customer data without authentication approval into the customers Salesforce organisation.

Employee Screening & Policies

As a condition of employment all Proximity Insight employees undergo pre-employment background checks and agree to abide by all company policies.