INNERSPACE SECURITY FEATURES & PROTOCOLS

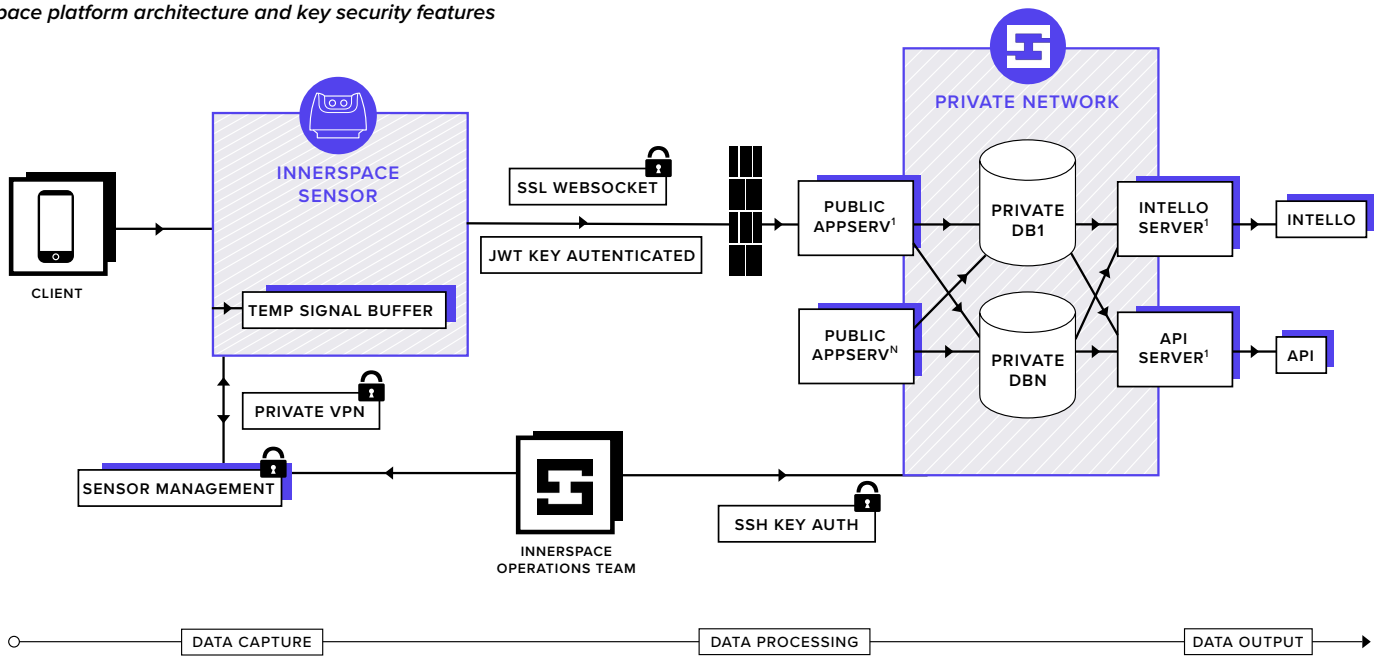
InnerSpace is a location intelligence solution that leverages proprietary IoT (Internet of Things) sensors and its cloud-based platform to provide companies with a suite of business solutions and APIs . The InnerSpace sensors capture point cloud data using LiDAR, and monitor traffic patterns of people and things using radio frequencies (WiFi, Bluetooth, Ultrawideband) emitted by smart devices and tags. The company has built its platform to comply with the privacy requirements of GDPR and does not store any personally identifiable information.

The following document, outlines how InnerSpace approaches data storage, device security, and data security.

Key Points:

- InnerSpace sensors collect, temporarily buffer, and then forward data via an encrypted, secure connection to its cloud servers.
- These servers are inaccessible to the public and are only reachable by the InnerSpace operations team via a protected private network.
- InnerSpace application servers collect and anonymize data prior to processing. This is in compliance with GDPR guidelines. The data is protected and stored within a private network and inaccessible to the public.
- The InnerSpace server environments scale to meet customer deployment demands.

InnerSpace platform architecture and key security features



Security Features & Protocols Summary

SECURITY FEATURES SUMMARY	IN PLACE	ROADMAP
SENSOR SECURITY FEATURES		
+ Protected by Private VPN	X	
+ Data at Rest: Signal Buffer - cached pending successful transmission to InnerSpace servers	X	
+ Data in Transit: SSL WebSocket	X	
SERVER SECURITY FEATURES		
Production Servers		
+ DB Servers within Private Network	X	
+ Protected by SSH Key-Based Authentication	X	
+ Firewalled	X	
+ API calls SSL encrypted	X	
+ API protected by JWT Key Auth	X	
+ API protected by Rate Limiter	X	
Release Management		
+ Environment hierarchy: dev, test, prod	X	
+ Weekly scheduled releases	X	
+ App/DB Server push-button deploys via SSH key-based auth	X	
+ Sensor - Management portal deploys via VPN	X	
+ Deployment Review/Approval Process	X	
Data Security		
+ GDPR described MAC address hashing	X	

PROCEDURES	IN PLACE	ROADMAP
Release Management		
+ Weekly scheduled releases	x	
Malware Protection		
+ Rootkit scans run against all environments periodically	x	
+ Automated rootkit scans		x
+ Rootkit scans run against all containers		x

PROTOCOLS	IN PLACE	ROADMAP
Intrusion Detection & Prevention		
+ Protected against SSH brute force attacks	x	
+ SSH Key-based Authentication on all servers	x	
+ UFW Firewalls	x	
+ SSL Protected APIs and webservers	x	
+ Isolated execution environments	x	
+ Database servers within private environment	x	
+ File Auditing and Intrusion Detection - Aide (TBD)		x
+ Quarterly Service Audits	x	
+ Quarterly Patches & Logs	x	
Data Security		
+ Client Data - continuous backup and restoration procedure	x	
+ Map and Scan artifacts - Backed up to s3 buckets	x	
Outages		
+ Catastrophic Failure Protocol + Environment rebuilt via script + DBs rehydrated via script + Healthy environment in X hours	x	
+ Hot standby DBs		x
Monitoring		
+ Automated monitoring and alerting	x	
+ 18/7 on call	x	
Incident Reporting		
+ Triggered by Automated Monitoring	x	
+ Triggered by Manual Monitoring	x	
Opensource Projects Utilized		
+ Dropwizard (Microservice Framework)	x	
+ TimescaleDB (Community Edition)	x	
+ Kong API Gateway (Community Edition)	x	