Armored Things provides a crowd and spatial intelligence platform that shows where people are, where they are going, and where they are likely to be in the future. This whitepaper provides an overview of the architecture and answers to frequently asked questions around areas such as security and deployment requirements.

Overview

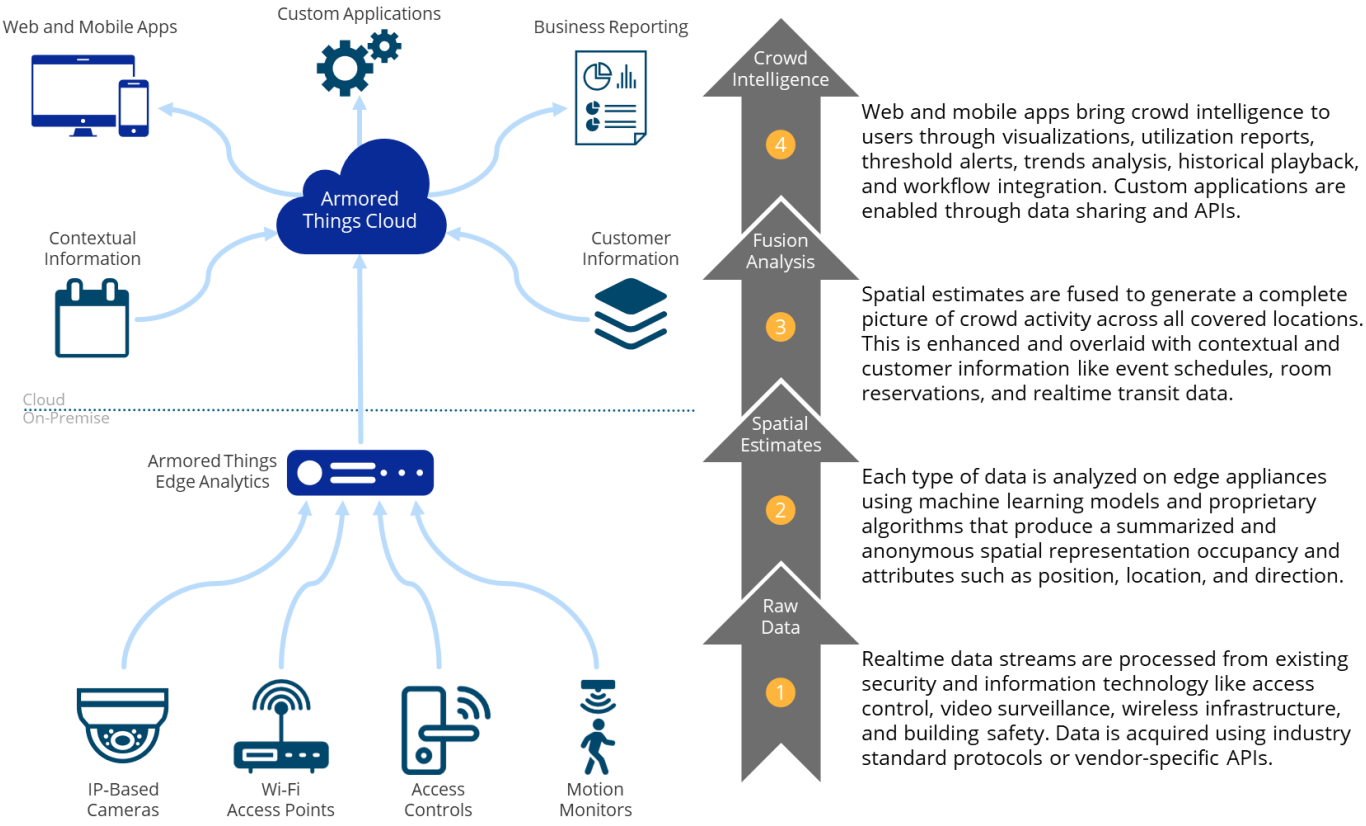
The Armored Things platform delivers a common operating picture of people and movement in a facility, stadium, or campus through detailed live and historical heatmaps, visualizations and alerts on web-based dashboards and mobile apps.

This information is essential for security and operations personnel to detect, predict, and respond to security risks; measure and improve guest, student or employee experience; increase the efficiency and utilization of staff and resources; and comply with evolving safety, occupancy and distancing requirements.

Architecture

The Armored Things platform is a distributed set of computing services running in the cloud and on analytics appliances in a customer environment. Collectively, these services turn raw sensor data into actionable crowd intelligence for different users and applications, as illustrated in the diagram below.

info@armoredthings.com
@ArmoredThings
617.326.8273
4 Liberty Square, Boston, MA 02109



How is Privacy Maintained?

Armored Things safeguards the privacy of customer data through a distributed design that processes most sensitive data at the edge of the network where it is produced, retains only a small subset necessary for machine learning and only for bounded periods of time, and maintains anonymous information about occupancy, movement, and location in the cloud. Higher-level modeling and analytics are done without personally identifiable information.

How is Security Assured?

Customer data is logically separated and encrypted in transit and at rest. Appliance to cloud communication is over industry standard VPNs with uniquely provisioned certificates, and all transport-level communication is encrypted using TLS. Armored Things maintains controls and safeguards to ensure systems are protected against unauthorized access, disclosure, or damage that might compromise customer data or system operation.

Is the Platform Highly Available?

The Armored Things platform is built around proven technologies and industry-leading cloud providers to ensure robust high-availability. The platform utilizes auto-scaling services with geo-redundant storage, service meshing to discover, connect and secure communications, and uses container orchestration for update, migration, and recovery.

info@armoredthings.com
@ArmoredThings
617.326.8273
4 Liberty Square, Boston, MA 02109

How is Reliability Provided?

Platform software components are continuously monitored for operational health and all systems are instrumented for telemetry and traceability so that issues can be identified and resolved before they affect customers. Armored Things maintains a public-facing incident reporting and uptime measurement system for transparency.

What Data Sources are Used?

Armored Things leverages existing information and security technology like IP-based cameras, Wi-Fi, access control, people counters, ticketing, and scheduling systems. Data access is strictly read-only and is acquired using industry standard protocols (e.g. RTSP, SNMP, GTFS) or vendor-specific APIs (e.g. HTTP REST and Webhooks).

How Long is Data Retained?

Data is retained on appliances for up to 30 days to allow reprocessing. Anonymized Wi-Fi data and periodic samples of video data are used to train and validate machine learning models and may be retained in the cloud for up to 180 days. Summarized depersonalized information about occupancy, location and movement is retained in the cloud for the lifetime of the deployment. Access to data is restricted to Armored Things employees or affiliated personnel with a specific need and only for the time required.

What Hardware is Required?

The platform software use edge services running on one or more virtual or physical analytics appliances in a customer's environment, in the cloud, or in a hybrid between the two. Resources vary depending on the sensors and sources used but will typically require a recent generation NVIDIA GPU such as the RTX 2080S, 24 cores on Intel Xeon or AMD EPYC CPUs, 64GB RAM and 512GB storage for every 75-100 devices.

How Long Does It Take to Deploy?

Getting up and running usually takes 4-6 weeks and consists of the following three steps:

1. *Planning* – High quality maps or CAD drawings of the space, details in sensor locations and information on integrations provided to Armored Things team.
2. *Setup* - Analytics appliance is hardware installed, remotely provisioned by Armored Things team and data sources connected and data access verified.
3. *Learning* - Machine learning models are trained and tuned for the environment, occupancy information is validated, and additional contextual sources evaluated.

After the last step, users will have access to web-based crowd intelligence dashboards and mobile apps.

info@armoredthings.com
@ArmoredThings
617.326.8273
4 Liberty Square, Boston, MA 02109