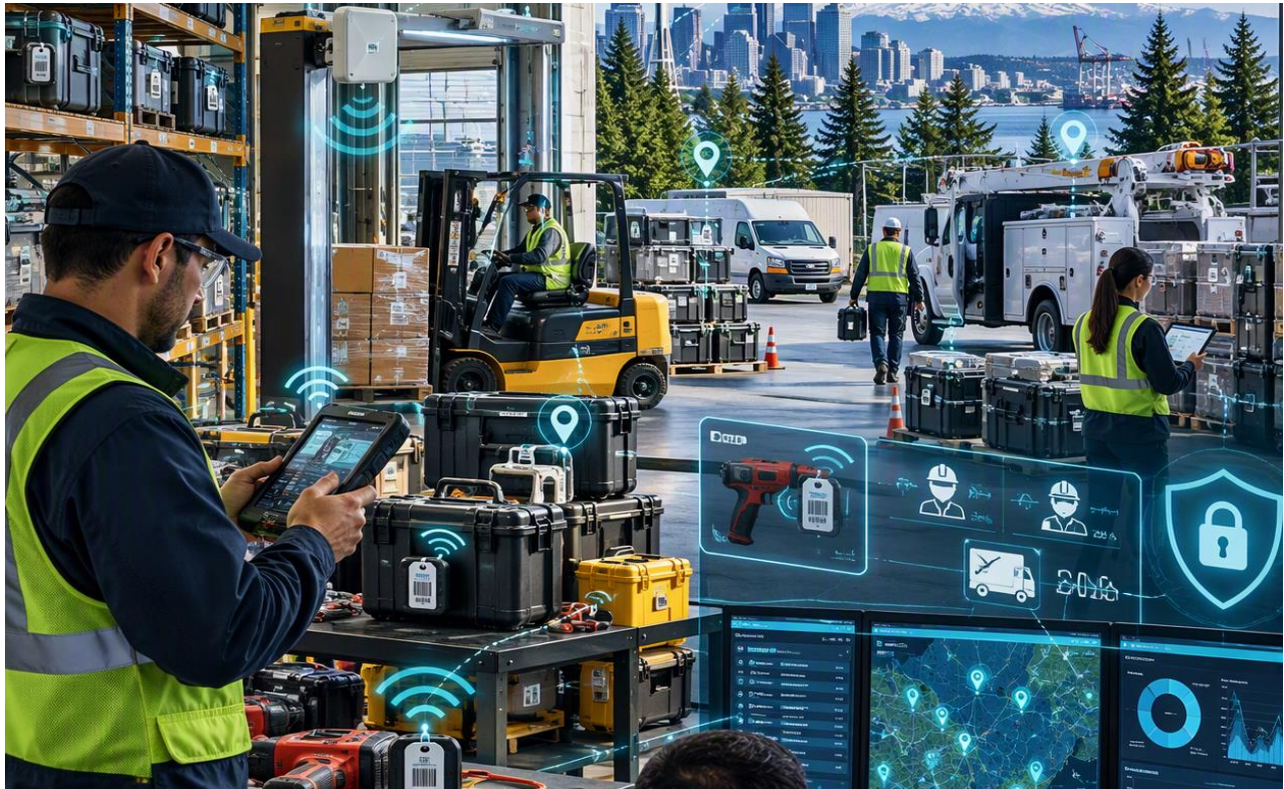




TURNING LOCATION DATA INTO OPERATIONAL VISIBILITY

Connected Asset, Inventory and Personnel Visibility Framework

RFID | RTLS | BLE | GPS | Barcode | AI Intelligence | Cybersecurity | Enterprise Integration



Solution Overview and Implementation Framework | October 2026

Connect what moves to the workflows that matter

Horizon IoT helps organizations assess, design, source, integrate, deploy, and support connected visibility solutions that improve asset awareness, inventory intelligence, personnel accountability, safety, and operational coordination.

Executive Overview

Operational visibility improves when identification, location, condition, and movement data connect to accountable processes and enterprise systems. The right solution begins with the operational problem, required accuracy, environment, privacy and security obligations, integration needs, and measurable outcome.

Horizon IoT can combine passive and active RFID, RTLS, BLE, GPS, barcode and QR, sensors, readers, handhelds, gateways, mobile devices, connectivity, cloud or local applications, analytics, AI-assisted insights, cybersecurity, and approved enterprise integrations according to customer requirements.

Technology should follow the use case

Different environments require different tag types, ranges, accuracy levels, workflows, safeguards, connectivity, and support models. Horizon IoT uses a technology-neutral approach to select and integrate the appropriate components.

What the framework connects

Assets and equipment

Location, movement, status, assignment, history, condition, alerts, and utilization.

Inventory and supplies

Counts, receiving, issuing, check-in and check-out, availability, replenishment, and exceptions.

Authorized personnel workflows

Presence, zone, credential, visitor, attendance, access, and emergency-accountability workflows.

Enterprise systems

ERP, inventory, facilities, HR, access control, maintenance, GIS, identity, and reporting.

AI-assisted intelligence

Forecasting, anomaly detection, utilization, movement patterns, decision support, and optimization.

Security and resilience

Identity, encryption, segmentation, logging, device lifecycle, continuity, and incident procedures.

Connected Visibility Architecture

A layered architecture supports the appropriate mix of identification, sensing, connectivity, applications, analytics, safeguards, and operating workflows.

Architecture layer	What it includes
1. Assets, inventory and authorized personnel	Vehicles, equipment, tools, supplies, specialized assets, facilities, yards and approved personnel workflows.
2. Identification and sensing	Passive RFID, active RFID and RTLS, BLE, GPS, barcode and QR, sensors, readers, gateways and handheld devices.
3. Secure connectivity and cybersecurity	Wi-Fi, cellular and wired networks with identity, encryption, segmentation, secure APIs, monitoring and resilience.
4. Visibility applications and integrations	Asset and inventory applications, personnel accountability, alerts, reporting, maps, ERP, WMS, CMMS, GIS and access control.
5. AI and analytics	Forecasting, anomaly detection, utilization intelligence, movement patterns, decision support and optimization.
6. Operational outcomes	Visibility, inventory accuracy, accountability, efficiency, resilience, cybersecurity and compliance support.

Architecture principles

Use-case first. Define the operating decision, workflow, range, precision, speed, environment, and outcome before selecting technology.

Interoperable by intent. Connect approved applications and data to enterprise systems through governed APIs and interfaces.

Secure across layers. Protect devices, readers, gateways, networks, identities, applications, APIs, data, and remote-support pathways.

Governed for people. Personnel-related capabilities require purpose, proportionality, authorization, privacy, legal, labor, and policy review.

Core Capabilities

Capabilities can be configured individually or combined into a broader operational-visibility environment. Final functionality depends on selected technologies, facilities, integrations, data quality, safeguards, and operating procedures.

Asset tracking

Real-time or near-real-time location, history, assignment, geofencing, exception alerts, condition, and utilization.

Tool and equipment accountability

Custody, assignment, kits, vehicle-borne equipment, maintenance tools, inspections, and readiness.

Access and safety integration

Badges, entry and exit events, restricted zones, alerts, incident workflows, and assembly-point status.

Remote operations

Reader and gateway health, diagnostics, secure administration, updates, replacement, and lifecycle support.

Inventory management

Automated counts, receiving, issuing, check-in and check-out, replenishment, availability, and audit workflows.

Personnel accountability

Authorized presence, zone, credential, attendance, visitor, mustering, and emergency workflows.

Analytics and reporting

Search, maps, KPIs, alerts, movement, utilization, inventory history, accountability, and exceptions.

Enterprise integration

ERP, inventory, facilities, HR, access control, maintenance, GIS, identity, and approved systems.

RFID, RTLS and Identification Technologies

Different technologies solve different problems. Passive RFID can support identification and inventory workflows; active RFID, RTLS, or BLE can support higher-frequency location awareness; GPS can support outdoor and mobile assets; and barcode or QR can provide practical user-driven identification.



Passive RFID

High-volume identification, portal reads, inventory counts, receiving, issuing, and item or container workflows.

BLE and mobile technologies

Proximity, beacons, mobile interaction, indoor awareness, and selected personnel or asset workflows.

Barcode and QR

Low-cost user-driven identification, labeling, verification, and complementary workflows.

Active RFID and RTLS

Frequent location, zone awareness, movement history, alerts, and selected real-time workflows.

GPS and cellular

Outdoor assets, mobile equipment, vehicles, trailers, remote sites, and wide-area visibility.

Sensors and condition monitoring

Temperature, humidity, shock, motion, door state, pressure, and other approved conditions.

AI-Driven Operational Intelligence

Tracking and inventory environments generate continuous identity, location, movement, count, condition, maintenance, and workflow data. AI-assisted analytics can help identify patterns and exceptions that are difficult to detect through manual review alone. Human oversight remains central.



Inventory forecasting

Analyze history, demand, availability, replenishment, and exception patterns for planning support.

Anomaly detection

Surface unusual movement, count variance, missing reads, zone events, condition changes, or data gaps.

Maintenance decision support

Combine condition, location, utilization, inspection, and work-history inputs.

Utilization and right-sizing

Identify idle, underused, shared, or constrained assets and equipment.

Search and loss-prevention insights

Analyze recurring search, movement, custody, exception, and incident patterns.

Operational planning

Support allocation, staging, inventory, labor, maintenance, and emergency-readiness decisions.

Responsible AI use

Define purpose, data quality, access, human review, acceptable use, documentation, monitoring, escalation, and the accountable decision supported by each insight.

Cybersecurity and Operational Resilience

Connected visibility solutions expand the operating environment across tags, readers, handhelds, gateways, mobile devices, networks, cloud or local applications, APIs, administrators, vendors, and enterprise systems. Security must be designed across the full lifecycle.



Identity and access

Strong authentication, role-based access, least privilege, privileged administration, and separation of duties.

Network protection

Segmentation, encrypted communications, secure remote access, private connectivity, and monitored pathways.

Reader, gateway and edge security

Secure configuration, inventory, firmware lifecycle, approved management, device health, and replacement.

Data and API security

Encryption, governed interfaces, approved exchange, logging, retention, backup, and recovery.

Mobile and endpoint security

Managed handhelds, approved applications, device controls, credentials, updates, and lost-device procedures.

Resilience and continuity

Fallback workflows, synchronization, out-of-band options where appropriate, recovery priorities, and lifecycle support.

Monitoring and response

Security logging, alert ownership, escalation, vulnerability coordination, incident procedures, and recovery.

Third-party responsibility

Document boundaries for devices, networks, applications, integrations, data, updates, support, and incident handling.

Governance, Privacy and Personnel Safeguards

Tracking should improve operations without creating unnecessary surveillance. Personnel-related capabilities require a defined purpose, proportional collection, authorization, transparency, access controls, retention limits, correction procedures, and accountable governance.

Purpose and necessity

Define the operational need, intended users, affected groups, and why the data is necessary.

Transparency and policy

Document notices, approved uses, responsibilities, escalation, retention, and prohibited uses.

Integration governance

Limit exchange to approved systems, fields, interfaces, uses, and accountable owners.

Data minimization

Collect only the identifiers, events, precision, duration, and history required for the approved workflow.

Accuracy and exceptions

Define expected performance, reconciliation, manual overrides, dispute, and correction procedures.

Lifecycle management

Plan issuance, batteries, reader and device health, replacement, decommissioning, and secure disposal.

Use cases across operating environments

Healthcare

Medical equipment, supplies, pharmaceuticals, staff or visitor workflows, maintenance, and audit support.

Warehousing and logistics

Receiving, counts, movement, availability, replenishment, shipment status, and exceptions.

Utilities and field operations

Tools, parts, mobile assets, crews, vehicles, and distributed resources.

Government and public safety

Property, emergency supplies, field equipment, responder coordination, and mustering.

Education and campuses

Technology, lab equipment, shared resources, access, visitors, and emergency accountability.

Manufacturing and industrial

Tools, work-in-process, materials, equipment, zones, safety, and maintenance.

Business Value and Measurement

Value depends on accurate data, adopted workflows, clear ownership, appropriate safeguards, reliable support, and measurable operational improvement.

Visibility

Coverage, location confidence, search time, status completeness, movement history, and exception awareness.

Utilization

Availability, assignment, idle time, shared-resource use, asset turns, and right-sizing.

Efficiency

Receiving, issuing, check-in and check-out, search, audit, maintenance, and coordination time.

Inventory accuracy

Count accuracy, reconciliation time, availability, replenishment, shrinkage, and audit readiness.

Safety and accountability

Mustering completion, zone exceptions, alert response, visitor workflows, and incident follow-up.

Cybersecurity and resilience

Asset coverage, access review, update health, alert handling, recovery, and continuity testing.

Deployment choices and delivery model

Hardware only

Authorized tags, readers, handhelds, gateways, sensors, accessories, and connectivity.

Off-the-shelf solution

Commercial tracking, inventory, RTLS, or accountability applications with standard capabilities.

Managed or SaaS

Subscription services with agreed monitoring, reporting, maintenance, administration, or support.

Hardware plus services

Site review, staging, configuration, installation coordination, onboarding, training, or support.

Integrated solution

Multiple technologies connected to existing systems, workflows, reporting, security, and governance.

On-premises or hybrid

Local services combined with cloud applications or management based on data, security, and continuity needs.

Implementation Framework

Phase	Core activities	Outputs
1. Assess	Goals, assets, inventory, personnel workflows, facilities, systems, privacy, cybersecurity, and measures.	Readiness summary, use cases, scope, and constraints.
2. Design	Tag strategy, readers, zones, applications, connectivity, data, integrations, safeguards, deployment, and support.	Solution design, bill of materials, responsibility matrix, and test plan.
3. Source and configure	Procurement, staging, tagging, provisioning, roles, workflows, alerts, dashboards, and integrations.	Configured pilot environment and deployment package.
4. Pilot	Coverage, read performance, accuracy, workflows, data quality, security, privacy, usability, and value.	Findings, issue register, adjustments, and go-forward decision.
5. Deploy	Tagging, installation, integration, migration, onboarding, training, documentation, and launch support.	Operational deployment and support materials.
6. Optimize	Monitoring, support, lifecycle management, reporting, governance review, and expansion.	Performance actions and visibility roadmap.

Horizon IoT as the accountable solution lead

Horizon IoT can lead strategy and advisory services, authorized technology sourcing, systems integration, deployment coordination, demonstrations, pilots, adoption, support, lifecycle management, and ecosystem coordination. Horizon IoT serves as the prime contractor and central point of accountability. Delivery can draw on team-based experience and qualified consultants, contractors, technology providers, distributors, connectivity resources, cybersecurity specialists, and field-service organizations according to each engagement.

Define a Practical Connected Visibility Pilot

A focused pilot should test performance in a representative operating area, using real assets, inventory, authorized users, workflows, integrations, safeguards, and measurable acceptance criteria.

- Which operational problem comes first: search time, inventory accuracy, custody, utilization, safety, mustering, or maintenance readiness?
- Which assets, inventory, tools, equipment, zones, authorized personnel workflows, and facilities belong in scope?
- What read range, location precision, event frequency, environmental rating, and battery or maintenance profile are required?

- What must integrate with ERP, inventory, maintenance, GIS, identity, access control, HR, or reporting systems?
- How will cybersecurity, privacy, device management, remote access, logging, support, escalation, and recovery operate?
- How will success be measured, and what evidence supports expansion?

Pilot outputs should include validated coverage and accuracy, tested workflows, security and privacy findings, integration results, an issue register, user feedback, support responsibilities, and a go-forward recommendation.