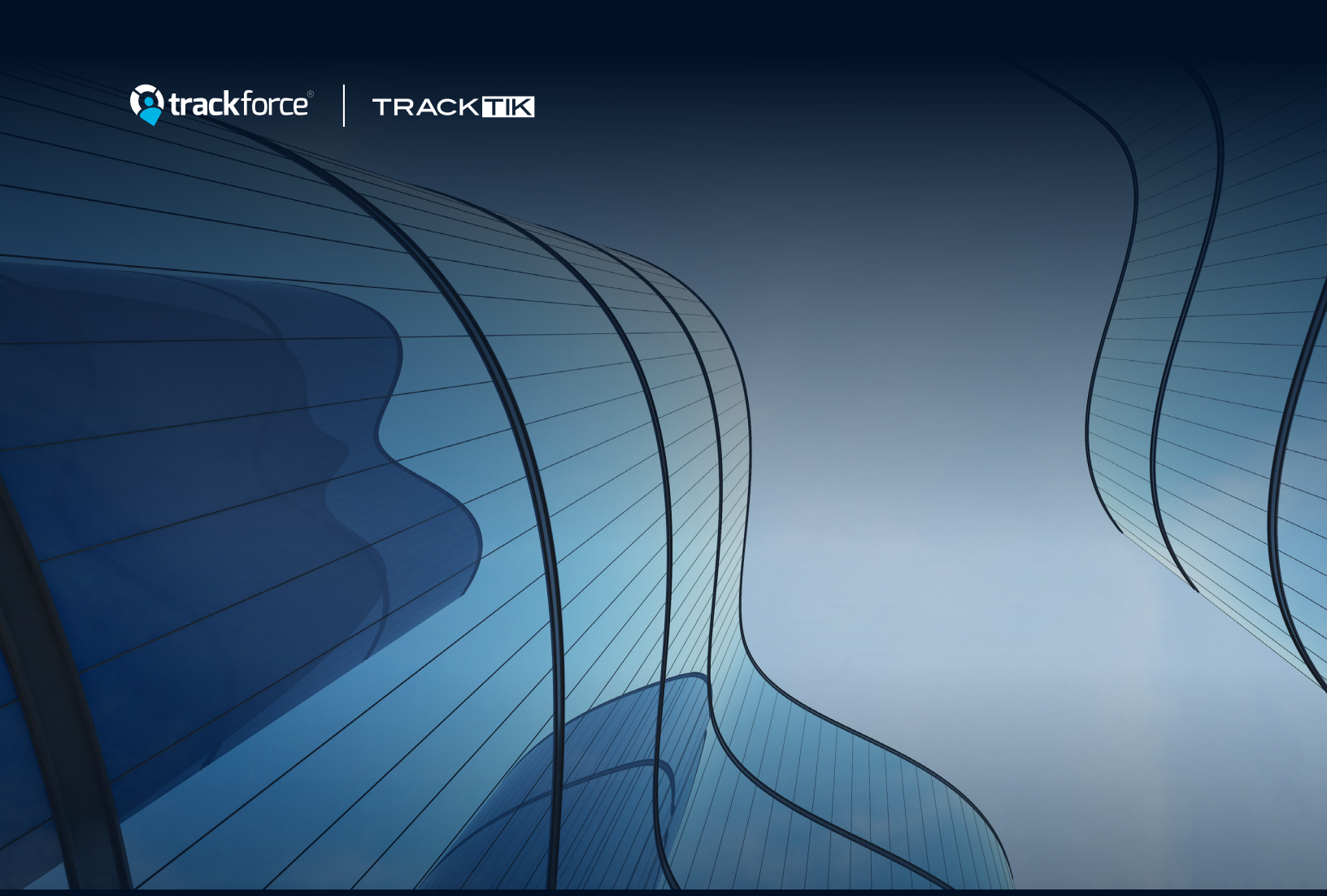
trackforce | TRACKTIK



Security Workforce Management

AN IT & CISO EVALUATION GUIDE

Table of Contents

Physical Security is Now an Enterprise IT Problem

Physical security workforce management platforms are no longer departmental tools confined to the security operations center. Modern solutions collect real-time GPS data, manage employee identities, generate compliance-relevant audit logs, integrate with core business systems, and store sensitive client and personnel information in the cloud. These tools are part of the organization's infrastructure, and those infrastructure decisions belong in the IT and CISO conversation.

Yet in many enterprise procurement cycles, these platforms are still evaluated and purchased primarily by Chief Security Officers or Facilities teams, with IT brought in late, often only during technical onboarding. The result is predictable: integration friction, governance gaps, renegotiated contracts, and in some cases, costly replatforming when a solution fails to meet enterprise standards.

This guide is written for IT leaders, CISOs, and enterprise technology teams who are being asked to evaluate, approve, or support the implementation of a physical security workforce management platform. It explains what to look for, what questions to ask, and why getting this right the first time matters.

KEY PRINCIPLE

Security workforce platforms should be evaluated as enterprise infrastructure — not departmental tools. When IT and security leaders align on governance requirements from the start, implementations succeed faster and platforms get adopted at scale.

Understanding the CSO's Mandate — and Why It Matters to IT

Before evaluating a platform on its technical merits, it helps to understand why the CSO is pushing for one in the first place. The problems driving this purchase are not primarily operational, they are governance and risk problems that IT leaders will recognize immediately.

The CSO is accountable for outcomes, not activity

Today's Chief Security Officer typically reports to the CEO, CRO, or COO, manages multi-site and often global security operations, oversees significant budgets across multiple guarding vendors, and owns compliance across frameworks including CTPAT, ISO, GDPR, and OSHA. They are expected to defend security spend to executive leadership and the board.

The fundamental challenge: security success is defined by nothing happening. Prevention doesn't generate a visible deliverable. This creates a persistent ROI justification problem as incident logs and anecdotal reports don't resonate in the boardroom. The CSO needs trends, benchmarks, and evidence. A modern workforce management platform is how they get it.

The data continuity problem IT should care about

One of the most concrete risks in physical security operations is what happens when a guarding vendor changes. In many organizations, procurement-driven rebids occur regularly — and when a vendor turns over, the security data walks out the door with them. Incident history resets to zero. Performance benchmarks disappear. Institutional knowledge about site-specific risks is lost.

This is a data governance failure, not just an operational inconvenience. A workforce management platform that the organization owns — independent of any guarding provider — solves this directly. The data stays with the enterprise regardless of which vendor is executing in the field. IT should recognize this as the same argument made for any SaaS consolidation: own your data, control your continuity.

The compliance burden is unsustainable at scale

For CSOs managing dozens or hundreds of sites, audit preparation is a significant operational drain. Stitching together photos, reports, and logs from multiple disconnected systems can consume four to six weeks of team time per audit cycle. A platform with automated, immutable audit trails — time-stamped incident documentation, geolocation evidence, exportable compliance reports — compresses that to hours.

This is directly relevant to IT: the audit burden the CSO is describing is also an IT audit burden. When physical security data is fragmented across point solutions, IT inherits the complexity of securing, maintaining, and producing evidence from all of them. Consolidation onto a governed platform reduces that surface area.

Where CSO and IT priorities actually converge

Despite different mandates and vocabularies, CSO and IT goals overlap more than most organizations acknowledge. The table below maps where shared priorities create a natural foundation for alignment.

CSO NEEDS	IT NEEDS	SHARED OUTCOME
Visibility across all sites & vendors	Centralized, auditable architecture	One governed source of truth
Proof of compliance for audits & regulators	Auditable controls with exportable evidence	Audit readiness without fire drills
Owned, portable data across vendor changes	Data governance & residency compliance	Reduced risk and vendor dependency
Stable operations during vendor transitions	Predictable integrations and data flows	Lower disruption to the business
Board-ready analytics on risk reduction	Security assurance for executive leadership	Executive and stakeholder confidence

THE ALIGNMENT OPPORTUNITY

The right platform doesn't force IT and the CSO to compromise on competing requirements, rather it's designed to satisfy both. Understanding what the CSO is solving for makes IT a more effective governance partner, not just a technical gatekeeper.

SECTION 1

Why IT and CISO Alignment is a Gating Factor

Enterprise-scale rollouts of physical security platforms routinely stall — not because the security team rejected the vendor, but because IT governance requirements weren't met during procurement. Single sign-on integration, audit evidence, data residency, and monitoring compatibility are now standard expectations in enterprise security reviews. A platform that can't satisfy these requirements won't get past procurement, and if it somehow does, it won't survive the first audit cycle.

The Convergence of Physical and Cyber Security

Physical security systems increasingly look like IT infrastructure.
Security workforce platforms now generate:

- Real-time GPS and location data tied to named employees
- Incident reports containing client-sensitive operational detail
- Access logs and activity records with compliance relevance
- API connections into HR, payroll, dispatch, and ITSM systems
- Cloud-hosted data subject to sovereignty and residency requirements

Each of these data streams touches information governance, identity management, and security monitoring — areas that fall squarely under IT and CISO oversight. Treating the platform selection as a purely operational decision creates exposure.

The Hidden Cost of Misalignment

When IT is excluded from the evaluation process, organizations often encounter:

- Integration failures that require custom development work after go-live
- Identity management gaps where offboarded employees retain access
- Audit findings because activity logs aren't exported to the SIEM
- Data residency violations when cloud hosting regions weren't verified
- Expansion stalls when enterprise procurement requires re-evaluation at scale

Engaging IT and the CISO early helps mitigate risk. Platforms built for enterprise governance alignment make this process seamless, while those that aren't often lead to ongoing friction.

SECTION 2

The Six Enterprise Evaluation Criteria

When evaluating a physical security workforce management platform from an IT and CISO perspective, six criteria consistently determine whether a platform will succeed in an enterprise environment.

1. Security & Compliance Assurance

Enterprise risk teams require standardized, third-party assurance, not vendor-written security documentation. The benchmark is SOC 2 Type II, which is specifically designed to provide buyers with independent assurance over a service organization's controls for security, availability, confidentiality, and privacy. ISO 27001 certification provides additional confidence in the vendor's information security management system.

Beyond certifications, evaluate how the vendor handles vulnerability disclosure, patch cadence, and security incident notification. A vendor that can't articulate a clear, documented process for each of these is not ready for enterprise deployment.

WHAT TO REQUEST

Ask for: SOC 2 Type II report (not just attestation), ISO 27001 certificate, penetration test summary, and vulnerability disclosure policy. Review the SOC 2 bridge letter if the report is more than six months old.

2. Identity & Access Management Maturity

IAM maturity is a critical differentiator for enterprise platforms. At minimum, a platform should support SSO via SAML 2.0 or OIDC, enabling centralized authentication through your existing identity provider. But SSO alone is not sufficient.

Lifecycle provisioning (automated user creation, role assignment, and deprovisioning via SCIM) is what eliminates the identity hygiene risk that manual account management creates. In a physical security context, where guards may be onboarded and offboarded frequently, the absence of automated provisioning is a material control gap.

Also assess role-based access controls. Can permissions be scoped to specific sites, clients, or data types? Can security teams and IT teams have separate administrative domains within the same platform?

WHY THIS MATTERS

Offboarding gaps are one of the most common audit findings in SaaS platform reviews. A platform without SCIM support means someone on your team is manually deprovisioning accounts, and at some point, they'll miss one.

3. Integration & API Capabilities

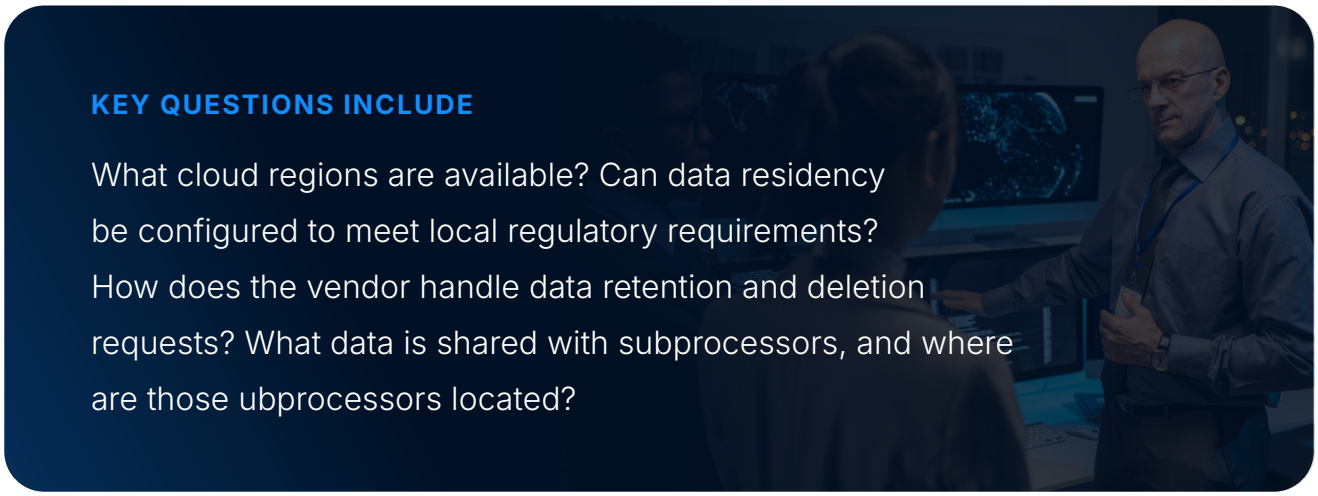
Physical security platforms don't operate in isolation. They need to connect to HR systems for identity lifecycle events, ITSM platforms for incident escalation, SIEM and SOAR tools for security monitoring, and potentially payroll and scheduling systems. The quality of a vendor's integration architecture determines how much custom development your team will be required to do and how fragile those integrations will be over time.

Look for a published, documented Open API with versioning commitments. Understand the vendor's approach to API deprecation as undocumented deprecation cycles are a common source of integration breakage. Pre-built connectors for common enterprise platforms (ServiceNow, Splunk, Workday, Active Directory) reduce implementation burden and are a sign of enterprise readiness.

The goal is not vendor lock-in through proprietary integrations, but genuine interoperability that lets the platform fit into your existing enterprise ecosystem. Platform consolidation benefits are real, but enterprises still expect open integration and strong governance alignment rather than a closed ecosystem.

4. Data Governance & Sovereignty

Physical security platforms handle sensitive data: employee GPS locations, client site details, incident records, and contractual information. Before approving a platform, IT and legal teams should understand exactly where this data lives, who can access it, and how it is managed across its lifecycle.



For organizations operating across multiple jurisdictions, data sovereignty is a baseline requirement. A vendor without configurable regional data residency options may not be deployable in certain markets.

5. Auditability & Security Monitoring

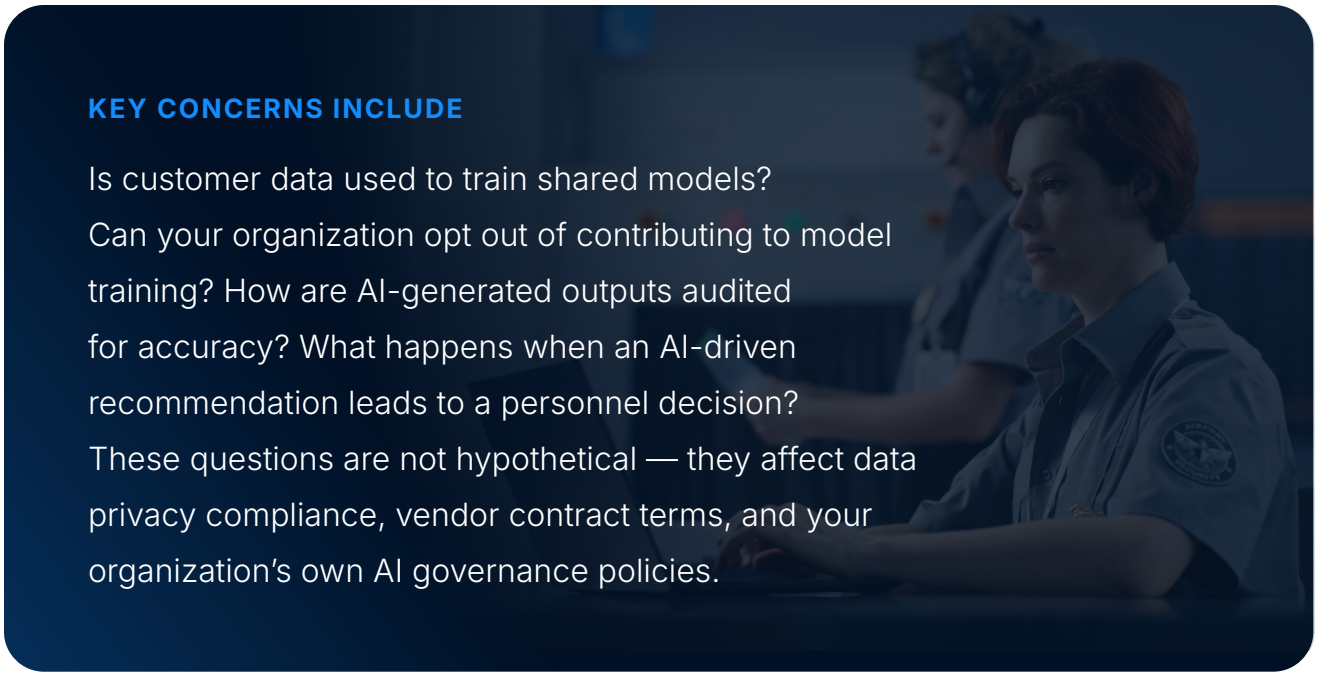
Enterprise security posture depends on visibility. A physical security platform that generates activity but can't export that activity to your centralized monitoring stack creates a blind spot. CISO teams need to know:

- Are all user actions captured in immutable audit logs?
- Can those logs be exported to the SIEM in real time or on a defined schedule?
- Are the log formats compatible with your existing detection and response workflows?

Auditability also matters for compliance. Access reviews, privileged action logging, and data access records may be required as evidence during SOC 2 audits, regulatory reviews, or internal governance assessments. A platform that can't produce clean, exportable evidence on demand creates audit preparation overhead that falls on your team.

6. AI Governance

Many modern security workforce platforms are beginning to embed AI and ML features — predictive scheduling, anomaly detection, automated reporting, and similar capabilities. As these features mature, they introduce governance questions that IT and CISO teams are responsible for answering.



KEY CONCERNS INCLUDE

Is customer data used to train shared models? Can your organization opt out of contributing to model training? How are AI-generated outputs audited for accuracy? What happens when an AI-driven recommendation leads to a personnel decision? These questions are not hypothetical — they affect data privacy compliance, vendor contract terms, and your organization's own AI governance policies.

SECTION 3

IT & CISO Evaluation Checklist

Use the following checklist during vendor evaluation to assess platform readiness against enterprise governance requirements. Request documentary evidence for each confirmed item.

CATEGORY	KEY QUESTIONS TO ASK VENDORS	STATUS
Security & Compliance	Do you hold SOC 2 Type II certification? ISO 27001? How are security incidents disclosed to customers? What is your patch management and vulnerability disclosure cadence?	☐ Confirmed ☐ Pending ☐ Gap
Identity & Access Controls	Do you support SSO (SAML 2.0 / OIDC)? Is SCIM-based automated provisioning/deprovisioning available? Can role-based access controls (RBAC) be configured per department or site?	☐ Confirmed ☐ Pending ☐ Gap
Integration & API Capabilities	Do you provide an Open API with published documentation? What pre-built integrations exist for SIEM/SOAR, ITSM, and HR systems? How is API versioning and deprecation managed?	☐ Confirmed ☐ Pending ☐ Gap
Data Governance & Sovereignty	Where is data hosted? What regions are available? Can we configure data residency to meet local compliance requirements? What is your data retention policy and how is deletion handled?	☐ Confirmed ☐ Pending ☐ Gap
Auditability & Monitoring	Are all user actions captured in immutable audit logs? Can logs be exported to our SIEM in real time? What reporting is available for access reviews and compliance audits?	☐ Confirmed ☐ Pending ☐ Gap
Reliability & Infrastructure	What is your documented SLA/uptime commitment? How is the platform architected for high availability and failover? What is your incident communication and RTO/RPO process?	☐ Confirmed ☐ Pending ☐ Gap
AI Governance	What AI or ML features are embedded in the platform? Is customer data used to train models? Can this be opted out? How are AI-driven outputs audited for accuracy and bias?	☐ Confirmed ☐ Pending ☐ Gap

SECTION 4

Implementation Roadblocks and How to Avoid Them

Even when a vendor meets enterprise governance requirements on paper, implementation can surface additional challenges. These are the friction points IT teams most commonly encounter.

Integration Complexity

The scope of integration work is often underestimated at the point of purchase. A platform with a well-documented Open API and pre-built connectors significantly reduces this burden, but integration planning still requires dedicated time from your team. Before go-live, map all required integrations, assign ownership, and confirm that the vendor's professional services team has experience with your specific enterprise systems.

Identity Lifecycle at Scale

In large organizations with high guard turnover, manual identity management is not viable. Confirm SCIM provisioning is available and tested before go-live. Automated deprovisioning, in particular, should be validated end-to-end, not just assumed based on vendor documentation.

Data Migration and Continuity

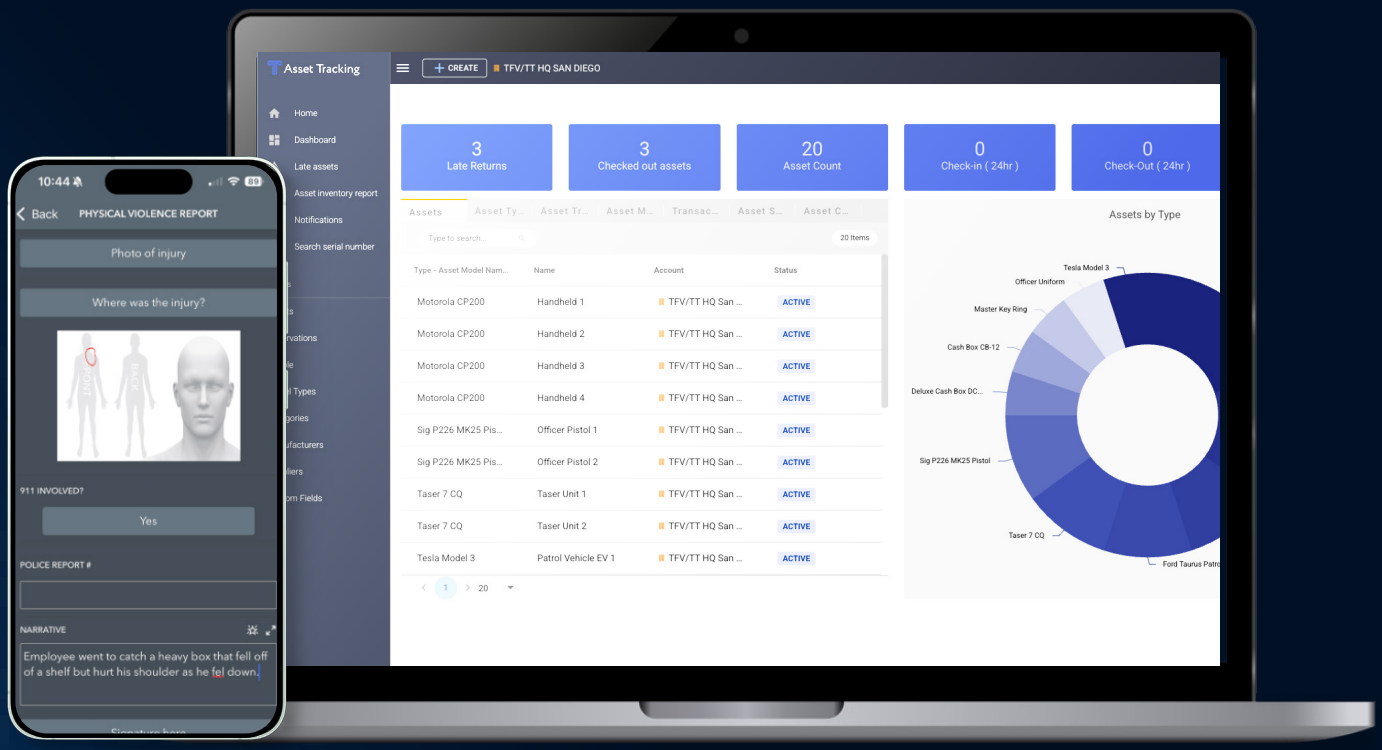
Transitions between platforms create data continuity risk. Incident records, site configurations, client SLA documentation, and historical reporting all have operational and compliance value. Ensure the vendor has a structured data migration methodology and that your contract includes data export rights in a machine-readable format.

Vendor Lock-In Risk

A platform that provides consolidation benefits but restricts data portability or integration flexibility creates long-term dependency risk. Evaluate exit terms, data export capabilities, and API openness as part of your initial assessment — not during contract renewal.

Change Management and Adoption

IT-driven implementations succeed when security operations teams are engaged stakeholders, not passive recipients of a new system. Build adoption into the project plan: involve guard supervisors in configuration decisions, schedule training before go-live, and establish a feedback loop between field users and the platform team.



TRACKTIK
by trackforce

SECTION 5

How TrackTik Addresses Enterprise IT Requirements

TrackTik is designed to meet the governance, integration, and security standards that IT and CISO teams require, while delivering the operational capabilities security teams need. Here is how the platform addresses each of the enterprise evaluation criteria covered in this guide.

Security & Compliance

TrackTik is built on a cloud-based infrastructure with data security processes and safeguards aligned to recognized compliance frameworks, including ISO 27001 and CIS Controls. These certifications provide IT and procurement teams with independent assurance over the platform's security posture, reducing the burden of custom security assessments during vendor review.

Integration-First Architecture

TrackTik supports an Open API ecosystem designed to integrate with existing enterprise systems and scale with your business. Rather than creating new data silos, the platform is built for interoperability, enabling genuine data-sharing across security operations, HR, ITSM, and reporting systems without creating dependency on proprietary integrations. This approach reduces IT development burden while preserving the flexibility enterprises require.

Ease of Implementation

TrackTik is designed for rapid deployment without requiring extensive developer resources. For smaller organizations, implementation can be completed in hours. For enterprise environments, the platform's no-code configuration approach reduces the burden on IT while still supporting the customization and governance controls larger organizations require. This means your team spends less time on deployment mechanics and more time on governance configuration and stakeholder enablement.

Real-Time Visibility and Auditability

The platform provides real-time location data, incident reporting, and comprehensive operational dashboards that create a continuous, accessible record of security workforce activity. Custom dashboards can be built and shared across departments, giving security, IT, and compliance teams a unified view of operational data. This shared data layer is the foundation for the cross-functional collaboration that reduces governance gaps and supports audit readiness.

Data Privacy and Security

TrackTik recognizes that physical security platforms handle sensitive data including employee locations, client information, and incident records that require the same protection standards applied to other enterprise data. The platform is designed with data privacy compliance in mind, and TrackTik operates as a trusted data custodian for the sensitive information your organization and your clients entrust to it.

TRACKTIK by trackforce

TrackTik Brings IT and Security Together

When IT, CISO, and security operations teams evaluate a workforce management platform together — using shared governance criteria — implementations succeed faster, platforms achieve broader adoption, and organizations get the security ROI they invested in. TrackTik is built to support that alignment.

Learn more at : **www.tracktik.com**

BOOK A DEMO

trackforce®

www.trackforce.com
hello@trackforce.com
(USA) +1(888) 454-5606
(CAN) +1(514) 312-2870