



Manufacturing Security Readiness Checklist

A Self-Assessment for Facilities, IT, and Operations Leaders

Modern manufacturing facilities depend on more than cameras and card readers. Today, security must work across physical and digital environments, production workflows, shift schedules, and compliance requirements all without slowing operations.

Use this checklist as a fast, honest assessment of your current security posture. Identify gaps, uncover vulnerabilities, and see where intelligent video and access control can strengthen safety, efficiency, and uptime.

SECTION 1

Facility Security & Physical Infrastructure

Access Control

- ☐ Are all access points centrally managed from a unified platform?
- ☐ Do badge permissions align with real job roles and shift schedules?
- ☐ Are visitor/contractor access workflows consistent across the plant?
- ☐ Are there any outdated, standalone readers still in use?
- ☐ Does the current system provide real-time alerts instead of only historical logs?

Perimeter & Production Floor Monitoring

- ☐ Are blind spots mapped and eliminated with optimized camera placement?
- ☐ Can your system detect anomalies such as:
 - Forklifts in restricted areas
 - People entering incorrect zones
 - Unauthorized after-hours movement
- ☐ Does surveillance integrate with thermal/IR or smart sensors to detect equipment overheating or safety risks?
- ☐ Is your control room overwhelmed by too many screens or low-value alerts?

Incident Response & Reliability

- ☐ Does your team receive actionable alerts rather than false alarms?
- ☐ Can you quickly retrieve high-quality video evidence when needed?
- ☐ Are maintenance, updates, and troubleshooting centralized?
- ☐ Are there concerns your current system cannot scale across multiple plants?

SECTION 2

Cybersecurity & IT Infrastructure

Network Security & Compliance

- ☐ Are all cameras and access control devices treated as secured network endpoints?
- ☐ Have firmware vulnerabilities or legacy devices been addressed?
- ☐ Is your video/access control system compliant with IT standards (FIPS, SOC 2, ISO27001)?
- ☐ Do you know exactly where video is stored, how long it is retained, and who can access it?
- ☐ Is the system segmented to prevent security devices from exposing the broader network?

System Integration & Management

- ☐ Is everything (video, analytics, access control, sensors) manageable from a single interface?
- ☐ Can the system integrate with existing identity management (e.g., Active Directory)?
- ☐ Are you avoiding "yet another console" that adds workload and complexity?
- ☐ Can your IT team remotely monitor events, alerts, and device health from anywhere?
- ☐ Is bandwidth optimized to prevent video from overwhelming the network?

Cloud / Hybrid Architecture

- ☐ Is your organization clear on cloud vs. on-prem requirements and risks?
- ☐ Are encryption, redundancy, and backup processes in place?
- ☐ Do you have visibility into data flows between devices, servers, and cloud storage?





SECTION 3

Operations & Production Workflow Security

Workflow Alignment

- ☐ Is security aligned with actual production workflows and traffic patterns?
- ☐ Are shift changes optimized so security doesn't slow gate entry?
- ☐ Can analytics identify process deviations that could cause downtime?
- ☐ Are contractors or visitors ever found wandering into restricted production areas?

Efficiency & Uptime

- ☐ Does security deployment avoid interrupting operations or lines during installation?
- ☐ Do new devices (cameras, badge readers) require minimal training?
- ☐ Are automated alerts tuned to reduce noise but highlight real operational risks?
- ☐ Are credentials and permissions updated fast enough to keep the line moving?

Asset Protection & Loss Prevention

- ☐ Is theft, tampering, or unauthorized movement monitored in real time?
- ☐ Are raw materials, finished goods, and high-value equipment covered?
- ☐ Does video correlate with access data for clear event verification?
- ☐ Are there analytics to detect:
 - Material diversion
 - Station downtime
 - Unauthorized workflow changes

SECTION 4

System Integration & Future-Readiness

Scalability & Standardization

- ☐ Are all facilities using uniform systems, standards, and credentials?
- ☐ Can new plants or expansions be deployed quickly without custom builds?
- ☐ Are analytics configurable for different zones or production types?

Automation & Intelligence

- ☐ Do your systems automatically identify unusual behavior (equipment or human)?
- ☐ Are alerts prioritized and filtered to reduce fatigue?
- ☐ Can the platform grow into new capabilities like AI-powered analytics or remote monitoring?

ROI & Cost Efficiency

- ☐ Do you have a clear understanding of ROI from proactive alerts vs. reactive investigations?
- ☐ Does your current system reduce staffing load in the control room?
- ☐ Are you confident your technology investment is preventing downtime or loss?

Security Readiness Score

[COUNT HOW MANY BOXES YOU CHECKED]

0-12
HIGH RISK

Your facility has significant exposure to operational and security threats.

13-22
MODERATE RISK

You have a foundation, but major gaps exist.

23-32
STRONG FOUNDATION

A few optimizations can bring you to best-in-class.

33+
PROACTIVE & INTELLIGENT SECURITY

You are operating at high maturity with advanced safeguards and analytics.

Security Modernization is just a call away
678-430-3116 www.gotchasecurity.net

GOTCHA
SECURITY.NET