rhombus

INDUSTRY REPORT

Rhombus for Manufacturing

Safer environments, improved compliance, and operational intelligence.

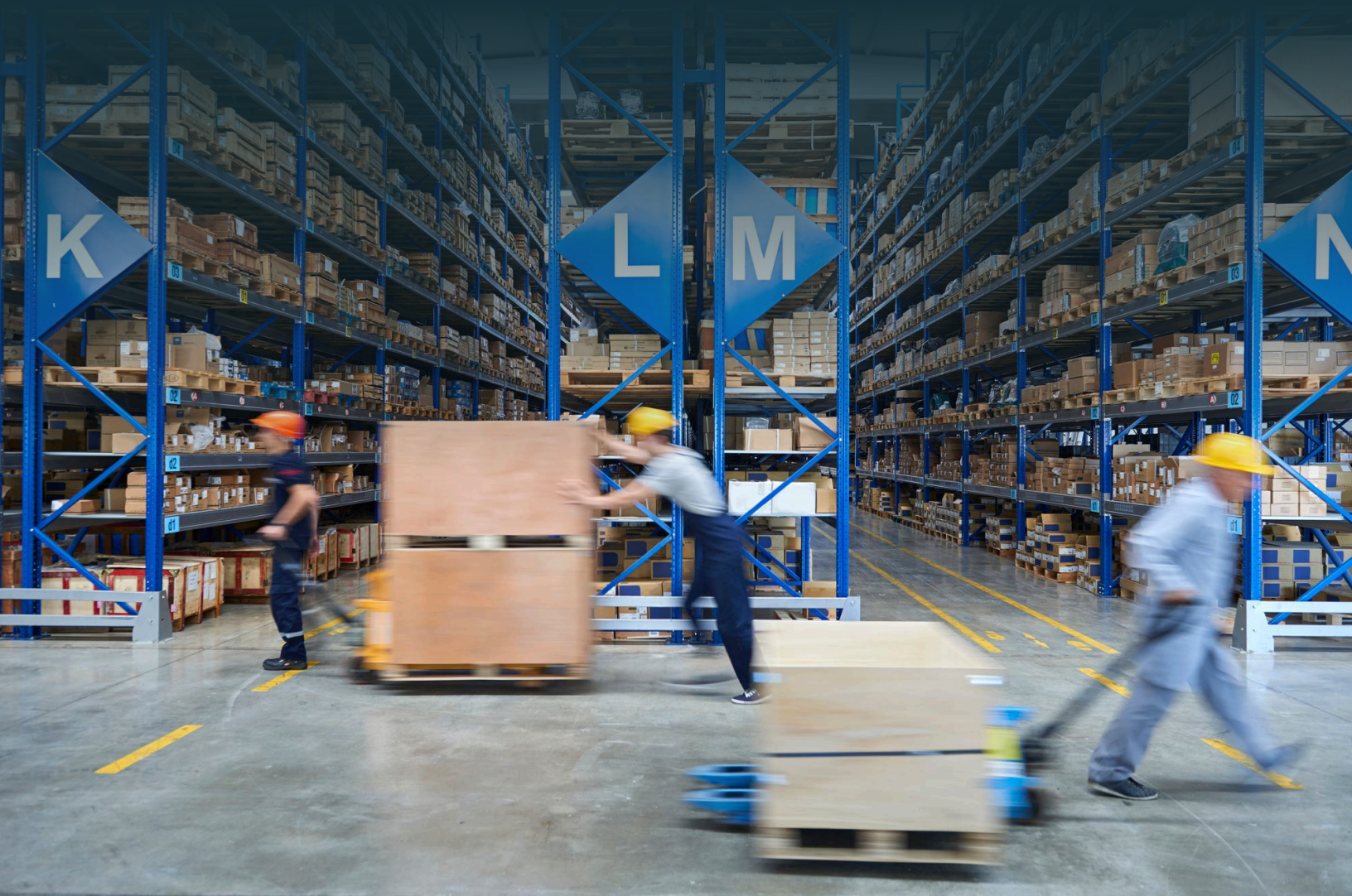


Table of Contents

03 Executive Summary

04 The Threat Landscape: Connected Plants, Exposed Systems

06 Physical Threats: Theft, Intrusion, and Insider Risk

07 Worker Safety and Workplace Violence

08 Aligning With Industry Frameworks

09 Our Perspective: One Platform, Fewer Blind Spots

11 Rhombus Studio

12 Recommendations for Manufacturers

13 The Road Ahead

14 Sources

Copyright © Rhombus, Inc. All rights reserved.

Executive Summary

Manufacturing has changed faster than the way most plants secure it.

Production lines are connected, sites are spread out, and security teams are expected to cover more ground with fewer people.

The data reflects that shift. Manufacturing was the most-cyber attacked industry for the fifth straight year in 2025, accounting for 27.7% of the incidents IBM X-Force responded to. On the physical side, cargo theft losses rose 60% to roughly $725 million. Meanwhile, new workplace violence rules now apply to every employer in California.

Three trends define plant security in 2026:

- Convergence. IT, OT, and physical security now share the same network. Cameras, door controllers, and sensors are connected devices, and they need the same care as any other endpoint.
- Physical loss. Theft of finished goods, metals, and parts is climbing. Large, multi-building sites that run around the clock are difficult to cover with legacy tools.
- Safety and compliance. Regulators and insurers increasingly expect plants to document what happened and how they responded.

The practical answer is one cloud platform for video, access control, sensors, and alarm monitoring. It gives security, EHS, and operations teams shared visibility across every site, without adding on-premises servers that require their own patching. Later in this report, we share how Rhombus approaches this, along with results from manufacturers such as Metalsa and Middleby Outdoor.

#1

Most attacked industry for the 5th straight year.

27.7%

Share of incidents IBM X-Force responded to that involved manufacturing in 2025.

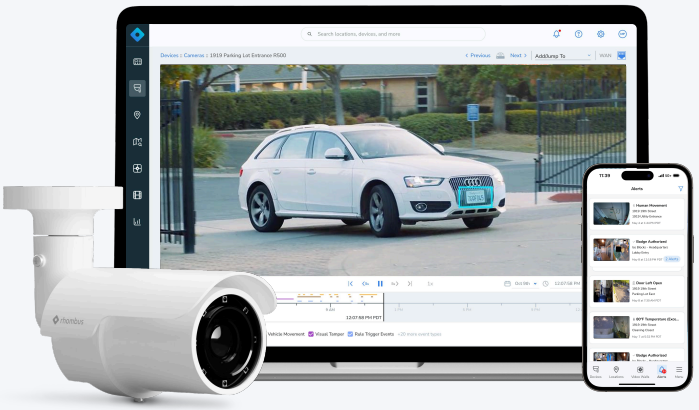
60%

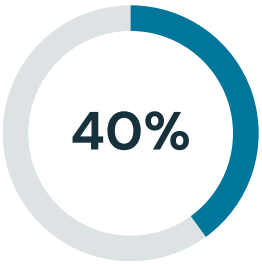
Increase in cargo theft losses in 2025, to roughly $725 million.

Copyright © Rhombus, Inc. All rights reserved.

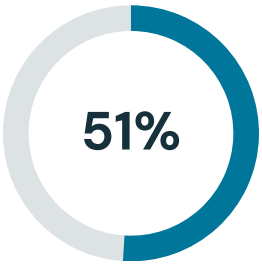
The Threat Landscape: Connected Plants, Exposed Systems

Ransomware attacks on industrial organizations rose 64% in 2025, and manufacturers accounted for more than two-thirds of the victims. Most attackers don't need exotic exploits. They get in through exposed, unpatched systems and stolen credentials.

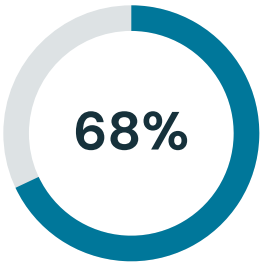




of attacks on manufacturers involved data theft.



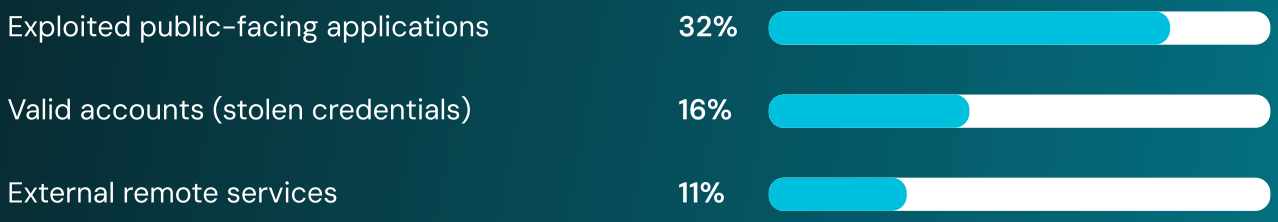
of manufacturing ransomware victims paid the ransom.



of vulnerable manufacturing OT devices are linked to ransomware groups.

How attackers got in

Top initial access methods in manufacturing incidents, 2025



Sources: IBM X-Force 2026; Sophos 2025; Claroty Team82 2025 Source: IBM X-Force 2026

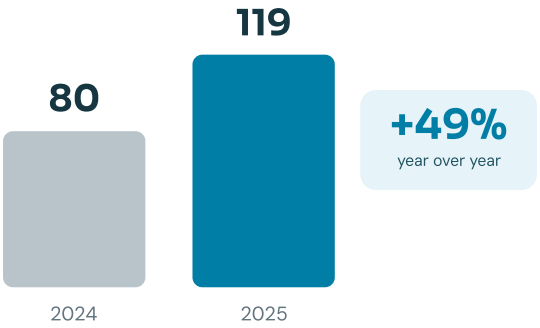
Copyright © Rhombus, Inc. All rights reserved.

Industrial Cyber Threats Are Growing

Two indicators of rising risk and the value of OT visibility

Ransomware Groups Targeting Industry

Number of groups targeting industrial organizations



Time to Contain OT Intrusions

Average attacker dwell time, in days



Finding	Figure	Source
Manufacturing's share of all incidents IBM responded to (fifth straight year at #1)	27.7%	IBM X-Force 2026
Attacks that involved data theft	40%	IBM X-Force 2026
Top initial access: exploited public-facing apps / valid accounts	32% / 16%	IBM X-Force 2026
Growth in ransomware attacks on industrial organizations	+64% (~3,300 orgs)	Dragos 2026 Year in Review
Average ransomware dwell time in OT vs. with full OT visibility	42 days vs. 5 days	Dragos 2026 Year in Review
Manufacturing ransomware victims who paid / average payment	51% / $1.0M	Sophos 2025
Average recovery cost, excluding ransom	$1.3M	Sophos 2025
Manufacturing OT devices with known exploited vulnerabilities (68% tied to ransomware groups)	96,000+	Claroty Team82 2025

Why it matters for physical security

Legacy DVRs and NVRs often expose security risks through open firewall ports and outdated firmware. With third-party breaches nearly doubling in 2025, vendor security is more critical than ever.

Copyright © Rhombus, Inc. All rights reserved.

Physical Threats: Theft, Intrusion, and Insider Risk

Cargo theft losses surged 60% to $725M in 2025, despite flat incident rates.

The difference is value. Thieves are targeting larger, more specific loads, and the raw materials and finished goods that move through manufacturing rank high on that list (Verisk CargoNet).

- **Higher value per theft.** The average theft reached $273,990, up 36%. Confirmed cargo thefts rose 18% to 2,646.
- **Raw materials and parts.** Metals theft rose 77%, driven by copper demand. Food and beverage theft rose 47%. Auto parts and engines bound for assembly plants remained frequent targets.
- **Regional hotspots.** California led with 1,218 incidents. New Jersey (+50%), Indiana (+30%), and Pennsylvania (+24%) saw the fastest growth, and all three are dense manufacturing and logistics corridors.
- **Perimeter and yard.** Large lots, loading docks, and idle buildings are common sites for after-hours copper and scrap theft (Manufacturing Management).
- **Insiders and intellectual property.** FBI leadership has cited more than 1,000 active investigations into China-linked theft of U.S. technology, much of it involving manufacturers (Winston & Strawn summary). Day-to-day insider losses, such as timecard fraud and missing inventory, are smaller but more frequent.

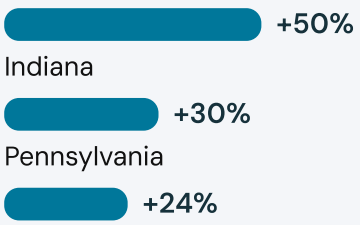
Cargo theft, 2025 vs. 2024

Year-over-year change



Fastest-growing states

Change in incidents

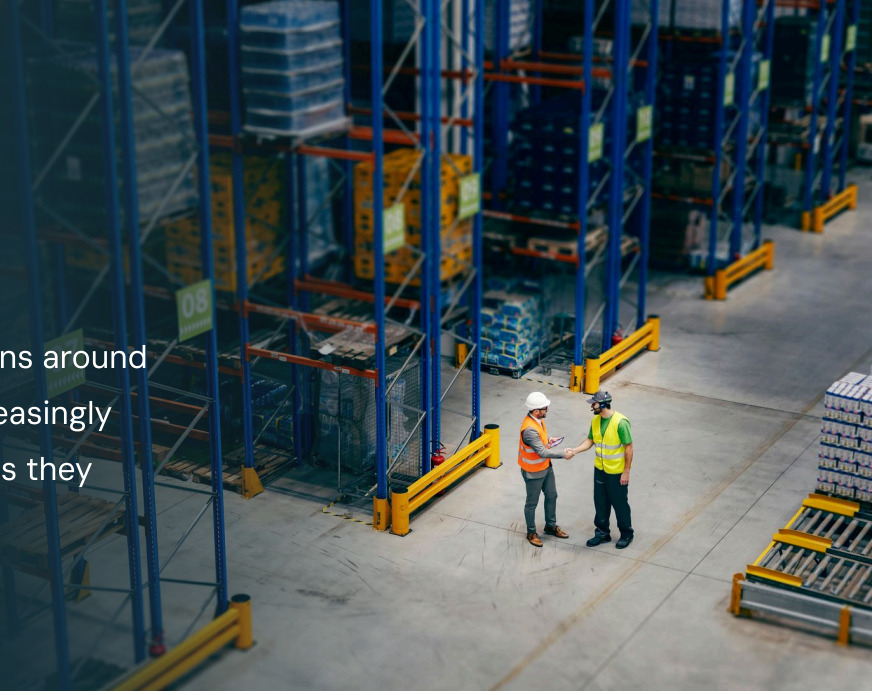


Source: Verisk CargoNet 2025 analysis

Copyright © Rhombus, Inc. All rights reserved.

Worker Safety and Workplace Violence

Injury rates are at record lows, yet expectations around violence prevention are rising. Plants are increasingly asked to show what happened and what steps they took in response.



California's Evolving Workplace Safety Requirements

Workplace Injuries at Record Lows

Workplace injuries fell to a record-low 2.3 cases per 100 workers in 2024, with manufacturing also seeing declines.

Nearly 400 Manufacturing Fatalities

Nearly 400 manufacturing workers lost their lives on the job in 2023.

Workplace Violence Remains a Threat

Production workers face some of the highest workplace homicide rates.

Safety Regulations Are Tightening

California now requires workplace violence prevention plans, incident logs, and employee training.

Key Milestones in Workplace Violence Prevention

JULY 2024

SB 553

Workplace violence prevention plans, incident logs, and employee training required.

DECEMBER 2026

Cal/OSHA

General-industry workplace violence standard due.

Copyright © Rhombus, Inc. All rights reserved.

Align With Industry Frameworks

CISA organizes manufacturing security into four areas: physical, cyber, personnel, and supply chain. That structure offers a practical way to see where a unified physical security platform supports the broader program.



CISA's Four Areas of Manufacturing Security

01 Physical

02 Cyber

03 Personnel

04 Supply Chain

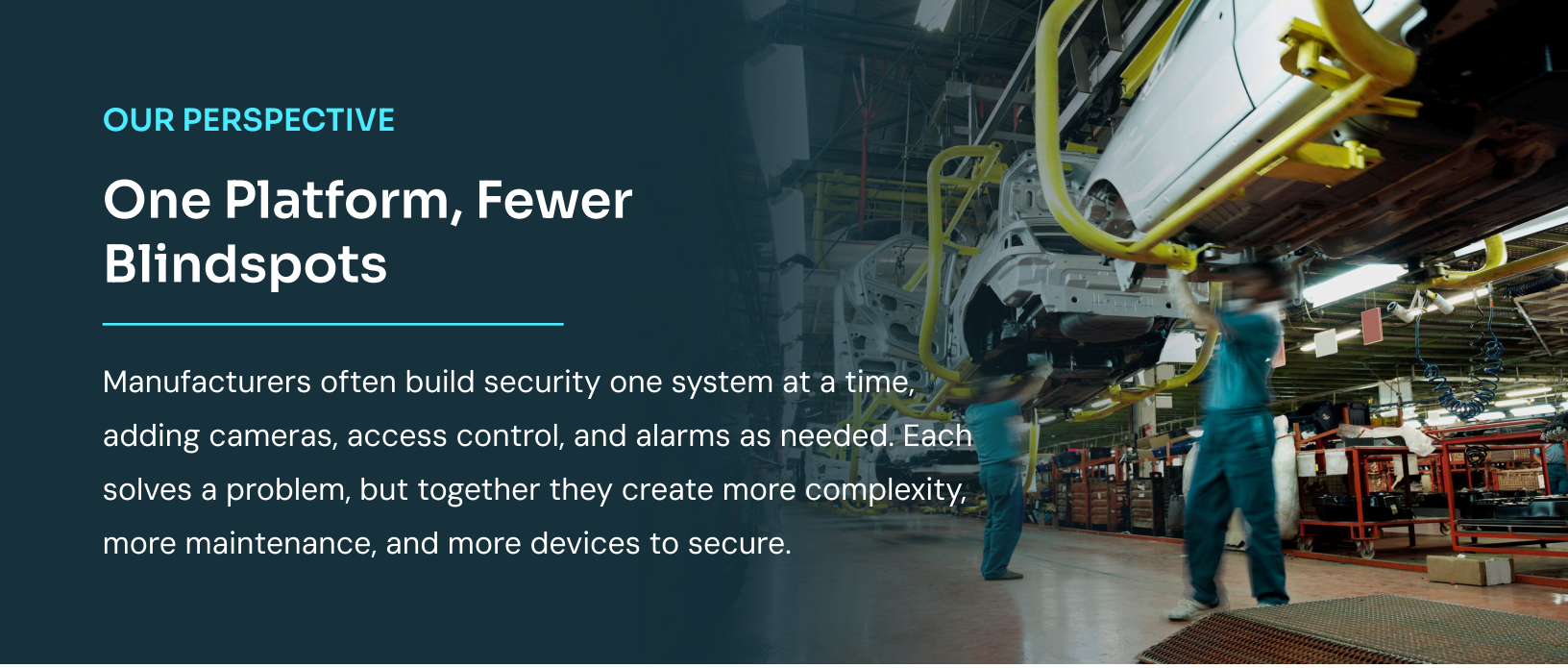
Where Physical Security Meets Compliance

Framework	What it covers	Where physical security fits
CISA Critical Manufacturing Sector Security Guide	Security practices for owners and operators, organized as physical, cyber, personnel, and supply chain	Perimeter, access, surveillance, and visitor controls; personnel screening
CISA Critical Manufacturing CSF Implementation Guidance	Applying the NIST Cybersecurity Framework across the sector	Managing cameras, door controllers, and sensors as IT assets
NIST CSF 2.0 Manufacturing Profile	CSF 2.0 outcomes tailored to manufacturing systems	Asset inventory, access management, monitoring, and recovery for connected devices
California SB 553	Workplace violence prevention plans, incident logs, and training	Evidence for incident logs; alerting and response workflows

Copyright © Rhombus, Inc. All rights reserved.

OUR PERSPECTIVE

One Platform, Fewer Blindspots



Manufacturers often build security one system at a time, adding cameras, access control, and alarms as needed. Each solves a problem, but together they create more complexity, more maintenance, and more devices to secure.

One Platform. Less Complexity. Better Results.

Unify video, access control, sensors, and alarms in one cloud-managed platform. Give security, EHS, and operations teams shared visibility across every site.

Proven Results:

- 90% faster investigations at Metalsa, saving 80 hours weekly.
- 2 days to 10 minutes: Middleby Outdoor's investigation time.

Results with Rhombus

Real-World Transformation Results



National Beverage Company

~$500K saved in loss and insurance across internal theft, damage & workers' comp claims.



Metalsa

80-labor hours saved per week; Incident resolution time **improved by 90%**



Middleby Outdoors

Cut investigation time from two days to 10 minutes

Copyright © Rhombus, Inc. All rights reserved.

Operational challenge	How Rhombus helps	Customer outcome or resource
Aging DVR and NVR systems	Cloud-managed video with automatic firmware updates, encryption at rest and in transit, NDAA- and TAA-compliant hardware, and SOC 2 adherence	Trust Center; Fitas Flax replaced failing DVRs across five sites
Cargo, yard, and dock theft	Perimeter cameras, license plate recognition, and AI alerts with audio deterrence	Middleby Outdoor uses LPR at entry and exit points, reducing pickup and drop-off discrepancies
After-hours intrusion and metal theft	Alarm Monitoring, which pairs AI alerts with live professional monitoring	Alarm Monitoring overview
Insider theft and restricted areas	Access control (DC10 and DC20 controllers, DR20 reader, DR40 video intercom, cards, fobs, and mobile keys), with every access event linked to video	Access Control; Middleby curbed timecard theft
Worker safety in hazardous zones	Cameras built for welding light and particulates, so teams can monitor robotic cells remotely	Metalsa monitors 40+ robotic cells and has created 350+ training clips
Environmental and air-quality hazards	E50 sensors (gas, chemicals, smoke, and air quality) and E15 sensors (cold storage), synced with video	Sensors
Workplace violence and emergencies	B10 panic buttons, A100 audio gateways for broadcasts, lockdown plans, and an Omnilert weapon-detection integration	Omnilert integration
Slow investigations and quality defects	Natural-language video search, face and license plate recognition, and link-based sharing	AI Analytics; Metalsa reduced six-hour reviews to minutes
Operational blind spots	Rhombus Insights Custom Events: prompt-defined counts and alerts, such as forklift traffic or blocked aisles (limited beta)	Rhombus Insights
Managing many sites	Unlimited devices and locations in one console, with no on-premises servers	Manufacturing solutions
Plant-specific questions that standard features can't answer	Rhombus Studio: custom dashboards and mini-apps built by the Rhombus team on cameras, sensors, panic buttons, and access control, using 900+ open API endpoints	Rhombus Studio examples include production-output counts and a shipping-dispute dashboard

Trusted by Manufacturing Leaders

utz · stryker · accupac · SIETE · Metalsa *Quality as a way of life* · DESIGN READY CONTROLS

A safer future starts here.

Learn how Rhombus can help keep your facilities safe.

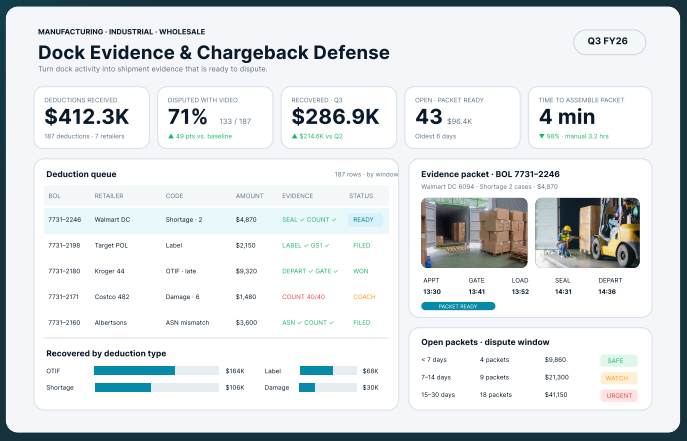
Become our partner in security. Try the platform for free today.

sales@rhombus.com

Copyright © Rhombus, Inc. All rights reserved.

Rhombus Studio

You imagine it, we build it. Transform your ideas into live dashboards and mini-apps.



Turn Physical Data Into Actionable Intelligence

Rhombus Studio is where our expert build team turns "can it do this?" into working, custom experiences tailored for the most unique use cases.

Efficiency Dashboards

Turning cameras into productivity meters that count, measure, and track output in real time.

Space & Occupancy Utilization

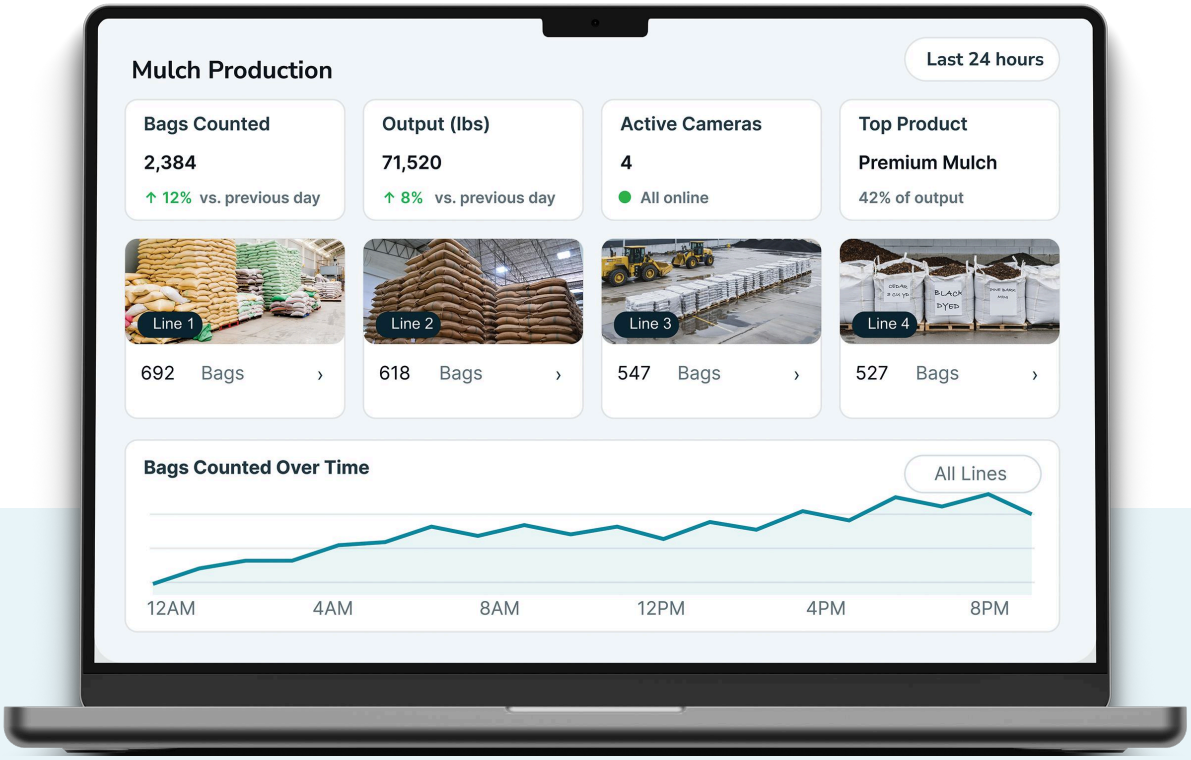
Understand how people actually use a physical space. See where customers go, how long areas sit empty, and when attention or staffing is needed.

Smart Detection & Predictive Alerts

Go beyond monitoring. Detect events, identify anomalies, and trigger action with real-time intelligence.

Infrastructure & Systems Management

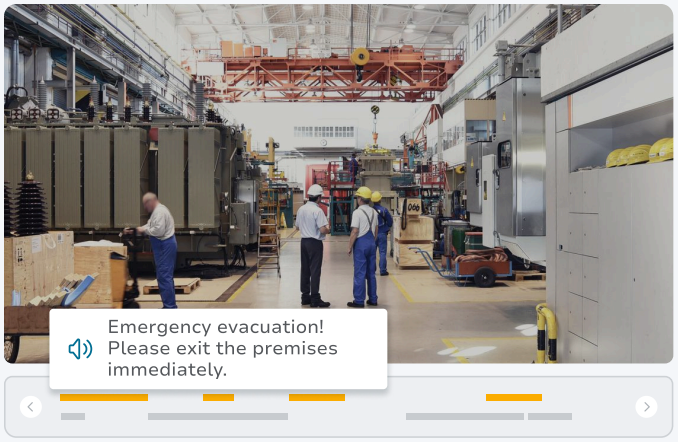
Dashboards that manage security ecosystems such as hardware health across multiple sites.



Copyright © Rhombus, Inc. All rights reserved.

Recommendations for Manufacturers

Start with the systems that carry the most risk and the perimeter that sees the most activity. Then build toward one platform that security, EHS, and operations teams all use.



8 Ways to Strengthen Manufacturing Security

Treat security devices as IT assets.

Inventory every camera, controller, and sensor. Retire DVRs and NVRs that require open ports or no longer receive firmware updates.

Secure the perimeter.

Cover yards, docks, parking, and fence lines with cameras and license plate recognition, backed by monitored after-hours alerts.

Connect access, identity, and video.

Place restricted areas, tool cribs, server rooms, and finished-goods storage behind credentialed access, with each event linked to footage.

Monitor hazards remotely.

Use rugged cameras for robotic cells and environmental sensors for air quality, chemicals, and cold storage.

Build a clear evidence trail.

Combine panic buttons, broadcast audio, and lockdown plans with searchable records that support SB 553-style incident logs.

Measure investigation time.

Establish a baseline for how long it takes to find footage today. With AI video search, Metalsa and Middleby Outdoor cut reviews from hours or days to minutes.

Standardize across sites.

Manage every plant and warehouse from one console with consistent permissions.

Put operational data to work

Build custom dashboards with Rhombus Studio to track production, resolve dock disputes, and optimize space.

The Road Ahead

Modern manufacturing security goes beyond protection, improving uptime, safety, compliance, and cost. The future is connected, measurable, and continuously improving.

Copyright © Rhombus, Inc. All rights reserved.

rhombus

WHAT'S NEXT?

Smarter Manufacturing Starts with Smarter Security.

Modern manufacturers need more than security. They need visibility, intelligence, and control across every facility.

With Rhombus, manufacturers can unify security, streamline operations, and turn real-time data into smarter decisions. The result? Safer workplaces, less downtime, and more efficient operations.



Built to Protect. Designed to Adapt.

Schedule a Free Demo Today

sales@rhombus.com | +1 (877) 746-6228

Scan the QR Code to learn more.