GTT Greater Technology Together

BUILT-IN CYBER RESILIENCE

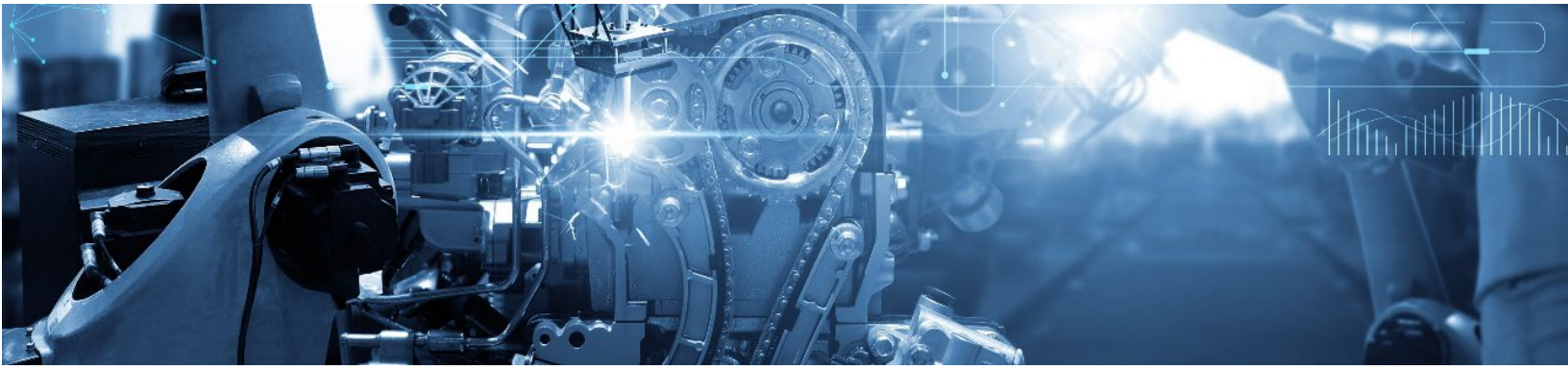
Embedding security into every layer of the network to protect manufacturing

A GTT SOLUTION BRIEF
MANUFACTURING

BUILT-IN CYBER RESILIENCE

Embedding Security into Every Layer of the Network to Protect Manufacturing

Contents



THE LANDSCAPE

Manufacturing Has Become the Primary Target for Cyber Disruption

The convergence of IT and operational technology has transformed what is possible on the factory floor. Cloud-connected Manufacturing Execution Solution (MES) platforms that coordinate production across continents. Industrial Internet of Things (IIoT) sensors that feed real-time data into predictive maintenance platforms. Remote engineering access that keeps specialist skills available across distributed sites. Digital supply chains where partners, logistics providers and systems share data continuously.

The same connectivity that makes these capabilities possible has fundamentally changed the risk environment. Manufacturing is now the most targeted sector for cyberattacks globally, accounting for 22% of all analyzed attacks in 2025.[1] The volume of ransomware incidents rose 61% year-on-year, with operational downtime and supply-chain paralysis as the primary consequences.[2] Jaguar Land Rover's 2025 cyber incident forced weeks of global production shutdowns — not a data breach, but an industrial stoppage.

[1] BitSight, Inside Cyber Threats in Manufacturing, 2025 [2] KELA, 2025

The constraint is the security architecture itself.

Global manufacturers are simultaneously managing fragmented firewall estates across dozens of markets, enforcing policies that were defined centrally but implemented inconsistently, operating monitoring tools procured independently for different parts of the estate while trying to achieve a coherent view of threat posture across an environment that was never designed to be governed as one.

Manufacturing accounts for 71% of ransomware incidents across industrial sectors.[3] 77% of organizations claim to monitor east-west traffic, but 40% of that traffic lacks sufficient context for confident investigation, leaving nearly half of lateral movement incidents undetected.[4] NIS2 in Europe, CMMC in North America and sector-specific frameworks across Asia-Pacific mean the regulatory consequences of a breach now compound the operational ones, and the compliance burden falls on teams already stretched by day-to-day operations.

[3] Dragos, Industrial Ransomware Analysis Q2-2025 [4] Illumio, 2025 Global Cloud Detection and Response Report, October 2025

22%

of all analyzed cyberattacks in 2025 targeted manufacturing, the most attacked industry globally.

BitSight, 2025

61%

year-on-year increase in ransomware attacks against the manufacturing sector.

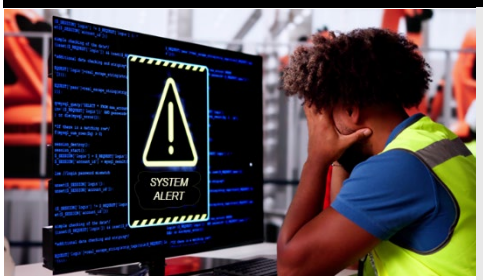
KELA, 2025

71%

of ransomware incidents across industrial sectors target manufacturing with IP theft and production disruption as primary objectives.

Dragos, Q2-2025

THE PROBLEM IS THE SECURITY ARCHITECTURE THE TECH RUNS ON



Consistent threat detection, centralized policy enforcement and clear accountability are not features most manufacturing security environments were designed to deliver. That is precisely where resilience fails.

- **FRAGMENTED SECURITY POLICIES**
  Multiple regional providers and inconsistently applied controls create gaps that are difficult to identify and remediate at scale.

- **LIMITED OT VISIBILITY**
  Security teams lack a unified view across IT, OT and cloud environments, leaving threats to move laterally before detection

- **SLOW INCIDENT RESPONSE**
  Manual detection and remediation processes prolong the window between breach and containment, amplifying production impact.

WHERE GTT COMES IN

Built Specifically for the Security Complexity of Global Manufacturing Operations

GTT manages network and security infrastructure for manufacturers across automotive, chemicals, food and beverage, electronics and industrial automation across Europe, the Americas, Asia-Pacific, the Middle East and Africa. We understand the operational reality of distributed OT environments, legacy production systems, complex compliance obligations and security teams simultaneously responsible for protecting both the corporate network and the plant floor.

We make consistent, enterprise-grade security achievable at this scale through GTT's top-ranked Tier 1 global IP backbone, with 400+ points of presence across six continents and with security services delivered from GTT's global Security Operations Centers providing 24/7 monitoring, threat investigation and rapid response. The platform that makes unified security governance operationally achievable is the GTT Envision Platform. And GTT takes end-to-end accountability for security delivery and in-life management across the entire estate, so internal teams are not absorbing the coordination complexity themselves.

In manufacturing, GTT embeds security into every layer of the network environment, protects OT and IT simultaneously and simplifies the complexity of governing it across every country, sub-vertical and stage of the modernization journey.

THE APPROACH

Why Built-In Cyber Resilience Is an Architecture Argument, NOT a Product Selection

Manufacturers evaluating security typically begin with point solutions like firewalls, endpoint tools, remote access platforms, often procured separately and assembled across multiple vendors. This results in a functionally fragmented security posture with multiple management consoles, inconsistent policies and no unified view of risk.

The GTT Envision platform delivers an integrated security architecture that sits across all of it, providing unified threat visibility, policy control and compliance reporting from a single interface. This is the operational difference between a security program that requires constant internal coordination and one that maintains consistent protection, governance and response capability as a managed service.

WITH DISCONNECTED POINT PRODUCTS	WITH GTT BUILT-IN CYBER RESILIENCE
Multiple security vendors, each managing their own segment of the environment	A single partner with end-to-end security accountability — one SOC, one escalation path, one operations team
Security policies set regionally and enforced inconsistently across sites	Centralized policy control via GTT EnvisionCORE, enforced consistently across all GTT-managed network and security infrastructure.
Threat visibility assembled from multiple dashboards with no single source of truth	Unified real-time threat analytics via GTT EnvisionDX — one accurate, current view across the global estate
OT and IT managed by separate teams with different tools and response processes	Security monitoring across GTT-managed infrastructure with MDR log ingestion from third party IT and OT systems, coordinated through GTT's global SOC
Compliance evidence gathered manually from fragmented systems before audits	Continuous audit trails and compliance reporting available on demand through the GTT Envision Platform

THE SOLUTION

One Integrated Security Architecture. One Managed Service.

GTT's built-in cyber resilience is built on a single integrated architecture, delivering the threat protection, policy consistency and compliance visibility that distributed manufacturing operations require.

Unlike providers that aggregate point security products, GTT delivers security as a managed service embedded into GTT EnvisionCORE, covering IT, OT and cloud environments from a common architecture managed through the GTT Envision Platform. In environments where OT security expertise is scarce and legacy systems create persistent exposure, GTT's global SOC provides the 24/7 coverage and OT-aware response capability that internal teams cannot maintain independently.

CORE CAPABILITIES SUPPORTING MANUFACTURING CYBER RESILIENCE:

- Secure Connect: SASE
- Managed Detection and Response (MDR)
- DDoS Mitigation
- Zero-Trust Network Access (ZTNA)
- Managed Firewall
- 24/7 Global SOC Coverage

THE PLATFORM ADVANTAGE

Unified Security Visibility and Control Across Every Site

The GTT Envision Platform delivers security governance without adding operational complexity. It adapts to the realities of each site, from a fully modernized cloud-connected facility to a legacy OT environment with limited change windows, while maintaining centralized policy and compliance oversight.

GTT ENVISION EDGE

Real-time telemetry at every plant edge. Security events and performance deviations are visible as they occur, giving GTT's SOC the data needed to detect and respond to threats rapidly.

GTT ENVISION CORE

Centralized policy orchestration and standardized change control. A security policy update made at headquarters propagates to every site simultaneously, eliminating the inconsistency that emerges when regional teams implement independently.

GTT ENVISION DX

Executive-ready threat analytics, SLA trendlines, compliance evidence and audit-ready reporting across all locations. Security, operations and leadership teams share the same current view of risk posture, without manual reporting cycles.

THE PROOF

What Manufacturing Customers Achieve with GTT

These manufacturing customers have deployed built-in cyber resilience with GTT across globally distributed operations. Their results are drawn from verified, publicly available case studies and direct customer accounts. No figures here are estimates or projections.

SIEGWERK | Chemicals & Packaging Ins Manufacturing — 35+ countries

Siegwerk operates a large, distributed global footprint across manufacturing facilities, labs, offices and logistics centers in 35+ countries. Their existing environment lacked the integrated network and security approach needed to support modern, secure, always-on global operations.

GTT deployed integrated global network and managed security services — including Managed SD-WAN, Dedicated Internet Access and managed firewall services — to strengthen Siegwerk's performance, reliability and cyber posture across its entire global estate.

"*With GTT's managed services, we can focus more on our core business while ensuring our global operations have a reliable and secure network foundation.*" — *Mohamed El Ashmawy, CIO, Siegwerk*

Outcome: Strengthened global manufacturing operations, enhanced security posture with managed firewall services, 40% increase in available bandwidth and a modernized infrastructure foundation for ongoing digital transformation.

CONNECT

SECURE

SIMPLIFY

WHY GTT

Built for the Security Demands of Global Manufacturing

Most security providers can protect one environment reliably. The challenge that determines whether a manufacturing security transformation succeeds or fails is different: can a provider deliver consistent, managed security across hundreds of sites, across multiple continents, covering both IT and OT environments, with different legacy infrastructures, different regulatory requirements (NIS2 and GDPR in Europe, CMMC in North America, data-sovereignty requirements across Asia-Pacific) and different levels of on-site security capability, without the operational burden falling on the customer's internal team?

This is the problem GTT is specifically built to solve. Three capabilities aligned to GTT's core commitment to connect, secure and simplify combine to make that possible:

TIER-1 GLOBAL BACKBONE	GTT ENVISION PLATFORM	24/7 GLOBAL SOC
GTT's top-ranked global IP backbone covers 400+ points of presence across six continents. Security services delivered over this infrastructure provide consistent, low-latency protection across every site, including markets where sourcing reliable, secure connectivity independently is operationally complex. Manufacturers do not need to manage separate carrier relationships or security monitoring arrangements in each country. GTT does.	**The GTT Envision Platform** is the operational difference between managing global security and simply owning tools. GTT EnvisionCORE enforces consistent policies across every site. GTT EnvisionEDGE detects anomalies at the plant edge before they affect production. GTT EnvisionDX provides real-time threat analytics and audit-ready compliance reporting for security teams, operations and leadership. Together, a manufacturer with facilities across multiple continents has one accurate, current view of its security posture.	**GTT's global Security Operations Centers** provide 24/7 monitoring, threat investigation and rapid response across IT, OT and cloud environments. SOC teams bring OT-aware expertise that most internal security functions cannot resource independently, covering ICS/SCADA protocols, industrial anomaly detection and production-aware incident containment. Internal IT and security teams retain strategic direction. GTT retains accountability for detection, response and performance.

MANUFACTURING SUB-VERTICALS SERVED

Security Architecture Adapted Across Every Manufacturing Sub-Vertical

Built-In Cyber Resilience addresses distinct security challenges across manufacturing sub-verticals, with architectures adapted to the operational, regulatory and technology environments of each:

Automotive & EV	TISAX compliance, secure supplier connectivity, OT segmentation for robotics and automated production lines
Food & Beverage	Multi-continent OT environments, cloud-dependent supply chain security, consistent policy across 100+ sites
Chemicals & Materials	Safety-critical OT protection, COMAH and SEVESO compliance, secure remote access for engineering and R&D teams
Packaging	Distributed manufacturing and logistics security, SAP and cloud workload protection, scalable architecture supporting expansion
Building Materials	Wide geographic security coverage, multi-cloud and ERP protection, standardized posture across European and global estates
Industrial Equipment & Automation	Complex supplier ecosystem security, engineering collaboration protection, high-reliability connectivity for production-critical systems

NEXT STEPS

Starting the Conversation

Security is the foundation production continuity depends on. To strengthen your manufacturing cyber resilience:

- **Map the current security posture against operational risk**: Identify which production systems, OT environments and cloud-connected applications carry the highest exposure, and where current controls leave gaps.
- **Audit security vendor and tool complexity**: Count the number of active security providers, monitoring tools and management consoles across the global estate. This is the coordination overhead a unified managed service removes.
- **Assess detection and response capability:** Evaluate how long it currently takes to detect and contain a security event across the network. This is one of the clearest measures of whether the current architecture can protect production at scale.
- **Engage GTT:** Contact GTT to map Built-In Cyber Resilience to your manufacturing environment and establish the consistent, globally governed security foundation your operations require.

SECURITY IS THE FOUNDATION THAT PRODUCTION CONTINUITY DEPENDS ON.

GTT protects global manufacturers across every region and every stage of the modernization journey, with consistent threat protection, unified governance and a single point of accountability for security across the entire network estate.

ABOUT GTT

GTT is a leading networking and security as a service provider for multinational organizations, simply and securely connecting people and agents to data and applications — anywhere in the world. We serve thousands of organizations, bringing together the right people, partners and technology to reduce the burden on IT teams and solve the most pressing networking and security challenges. Built on our top-ranked global Tier 1 network, GTT Envision is a single global technology platform to connect, orchestrate, virtualize and automate enterprise networks, enabling customers with consumable solutions to achieve business missions and meet ongoing demand when, where and how needed. Our portfolio includes SASE, SD-WAN, security, internet, voice and other connectivity options, complemented by a suite of professional services and exceptional sales and support teams in local markets around the globe. We partner with our customers to deliver Greater Technology Together. For more information, visit www.gtt.net.