

ZERO TRUST, EVERYWHERE

**Identity- and Context-Driven Access for Engineers, Contractors and Remote Workers
Across Global Manufacturing Operation**



**A GTT SOLUTION BRIEF
MANUFACTURING**

ZERO TRUST, EVERYWHERE

Identity- and Context-Driven Access for Engineers, Contractors and Remote Workers Across Global Manufacturing Operation

Contents

THE LANDSCAPE 2

WHERE GTT COMES IN 3

THE APPROACH 4

THE SOLUTION..... 4

THE PROOF 6

WHY GTT..... 7

NEXT STEPS..... 9

ABOUT GTT..... 10



THE LANDSCAPE

The Manufacturing Workforce Now Works From Everywhere. Legacy Access Architecture Was Not Built for That.

In the current manufacturing workforce, production teams, engineers and OT specialists operate across plant floors, remote offices and home environments. Contractors and OEM partners connect directly into operational systems to commission equipment, perform maintenance and resolve incidents. Suppliers integrate into MES and ERP platforms to coordinate production schedules and logistics in real time. The perimeter that access controls were designed to protect no longer exists.

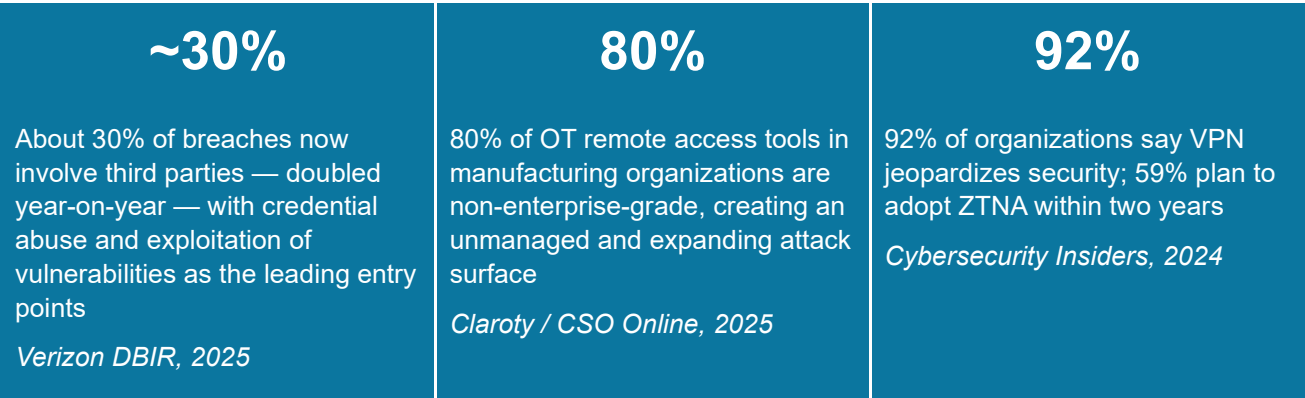
Third-party breaches involving manufacturing organizations doubled year-on-year to approximately 30% of all incidents, with credential abuse (22%) and exploitation of vulnerabilities (20%) representing the leading initial access vectors.¹ 55% of manufacturing organizations run four or more remote access tools in their OT environments, and approximately 80% of those tools are non-enterprise-grade, creating an unmanaged attack surface that expands with every additional vendor, contractor or remote worker.²

¹ Verizon, Data Breach Investigations Report, 2025 ² Claroty / CSO Online, Too Many Companies Use Non-Enterprise-Grade Remote Access Tools in OT Networks, 2025

The constraint is found in the structure of the access model.

Most manufacturing organizations still rely on VPN architectures that place users broadly on the network and rely on perimeter trust. When credentials are compromised, the blast radius is wide. A contractor with VPN access to a plant network has access to everything that network touches. 92% of organizations express concern that VPN jeopardizes security, and 59% plan to adopt Zero Trust Network Access within two years.³ the gap between intent and implementation is where exposure lives.

³ Cybersecurity Insiders, 2024 VPN Risk Report, HPE, 2024



THE PROBLEM IS NOT THE NUMBER OF USERS ACCESSING SYSTEMS REMOTELY. IT IS THE ARCHITECTURE THAT GOVERNS HOW THEY DO IT.



Legacy VPN access trusts the network by default, granting broad connectivity that expands risk with every user added. Zero Trust replaces that assumption with identity, device posture and context so access is granted precisely, verified continuously, and revoked immediately when conditions change.

Access sprawl Contractors, OEM partners and regional teams require temporary or limited system access, but most architectures have no mechanism for scoped, time-bound permissions.	Overexposed VPNs Legacy remote access places users on the network by default, widening the blast radius of any compromised credential across the entire connected estate.	No audit trail IT and security teams lack a single view of who accessed what system, from which device, under which conditions, making compliance evidence manual and incomplete.
---	---	---

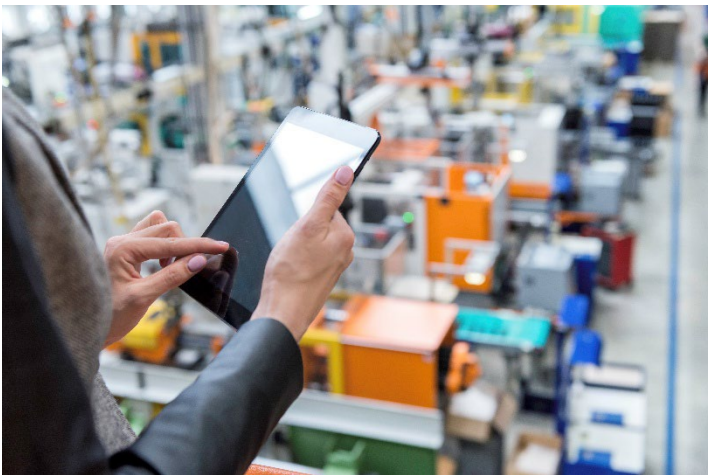
WHERE GTT COMES IN

Built for the Access Complexity of Global Manufacturing Environments

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 a workforce that spans plant floors, corporate offices, remote sites and third-party partner networks — and the access architecture required to keep that workforce productive without exposing production systems to unnecessary risk.

We make consistent, identity-driven access achievable at global scale through GTT's top ranked Tier 1 backbone and the GTT Envision platform, which provides centralized policy orchestration, real-time access telemetry and compliance reporting across every user, device and site in the estate. GTT takes end-to-end accountability for access delivery, policy management and in-life service management, so internal IT teams are not carrying the operational burden of managing access controls independently across dozens of countries.

In manufacturing, GTT replaces legacy perimeter trust with access that follows the user, granting precisely what is needed, continuously verifying the conditions under which it is granted and giving security teams the visibility to prove it.



THE APPROACH

Why Zero Trust, Everywhere Is an Architecture Argument, Not a Product Selection

Manufacturers evaluating access security typically begin with point solutions — VPN replacements, standalone identity tools, regional firewall deployments — procured separately and applied inconsistently across the estate. This creates a patchwork of access policies that behave differently depending on region, device or application, with no unified view of who is accessing what and no central mechanism to enforce change.

GTT delivers an integrated Zero Trust architecture. The GTT Envision platform sits across all of it, providing unified access policy control, session telemetry and compliance reporting from a single interface. This is the operational difference between an access environment that requires constant internal administration and one where identity-driven controls are enforced consistently, automatically, across every user and every site.

WITH LEGACY VPN AND POINT ACCESS TOOLS	WITH GTT ZERO TRUST, EVERYWHERE
Users placed broadly on the network by default, with trust granted at connection rather than verified continuously.	Session-level access governed by identity, device posture and context — no implicit network trust at any stage.
Access policies defined per region or site applied inconsistently, with no central enforcement mechanism.	Centralized policy orchestration via GTT EnvisionCORE, propagated uniformly across every site and user.
Contractors and third parties receive the same broad access as internal users, with no scoping or time-limiting capability.	Just-enough, time-bound access for contractors, OEM partners and vendors — scoped precisely to the systems they require.
No single view of sessions, device posture or access history across the global estate.	Unified visibility via GTT EnvisionDX — every session, policy event and compliance datapoint in one view.
Audit evidence assembled manually from fragmented logs before compliance reviews.	Continuous access logging of access sessions policy events, with audit-ready reporting available on demand through the GTT Envision Platform.

THE SOLUTION

One Access Architecture. Enforced Everywhere

GTT's zero trust, everywhere is built on a single integrated architecture that replaces perimeter-based trust with identity- and context-driven access controls, enforced consistently across every user, device, application and site in the global manufacturing estate.

Unlike providers that bolt Zero Trust capabilities onto existing VPN infrastructure, GTT delivers access controls as part of a managed service architecture. This covers employees, contractors, OEM partners and remote engineers from a common policy framework managed through the GTT Envision platform. In environments where access sprawl across dozens of third-party relationships is the norm and change windows are limited, GTT's centralized policy management provides the consistency that distributed, independently managed access tools cannot.

Core Capabilities Supporting Manufacturing Zero Trust Access:

- ✔ Zero Trust Network Access (ZTNA)

✔ Secure Connect SASE

✔ Secure Remote Access

✔ Managed Firewall
- ✔ Centralized Identity Policy Management

✔ 24/7 Access Monitoring and Session Telemetry

THE PLATFORM ADVANTAGE

Unified Access Visibility and Policy Control Across Every Site

The GTT Envision Platform delivers zero trust governance without adding operational complexity. It adapts to the access realities of each site — from a cloud-connected corporate campus to an OT environment with strict change controls — while maintaining centralized policy enforcement and compliance visibility

GTTENVISIONEDGE

Real-time network and access telemetry at every plant edge. Session events, device posture checks are visible as they occur, giving security teams the data needed to detect and respond to access issues rapidly.

GTTENVISIONCORE

Centralized policy and configuration control across all GTT-managed infrastructure. Policy changes made centrally propagate consistently to every site, eliminating the drift that occurs when regional teams manage configurations.

GTTENVISIONDX

Unified visibility and reporting across GTT-managed network and security infrastructure. Operations, security and leadership teams share the same current view of performance and compliance, without manual reporting cycles.

Zero Trust, Everywhere

Page 5 of 10

THE PROOF

What Manufacturing Customers Achieve with GTT

The manufacturer below deployed GTT's Secure Remote Access and managed security architecture across a distributed workforce and multi-site estate. Results are drawn from a verified, publicly available case study.



MITSUBISHI ELECTRIC UK | Electronics & Industrial Manufacturing — 15 sites across UK & Ireland

As cloud adoption accelerated and hybrid working expanded, Mitsubishi Electric UK faced a specific and urgent access challenge: a European VPN pool of approximately 1,000 licenses for 3,500 combined employees exhausted within days of a sudden shift to remote operations. The organization needed to secure 700+ UK and Ireland workers with a brokered, managed remote access solution — rapidly, without requiring on-site installation at each location.

GTT deployed Secure Remote Access across the full UK and Ireland workforce, with multi-factor authentication, centralized policy management and split tunnelling to reduce load on the corporate network. New sites were brought live through the GTT portal within a single day — compared to a lead time of up to three months under the prior MPLS architecture.

Outcome: 700+ users secured for remote access at scale, new locations connected within one business day, improved network performance and visibility across 15 sites, and a managed access foundation aligned to zero-trust principles as cloud adoption continues.



CONNECT



SECURE



SIMPLIFY



WHY GTT

Built for the Demands of Global Manufacturing

Most access providers can deploy a VPN replacement reliably in a single environment. The challenge that determines whether a Zero Trust transformation succeeds or fails is different: can a provider deliver consistent, identity-driven access controls across hundreds of sites, across multiple continents, covering employees, contractors, OEM partners and remote engineers, with different device estates, different regulatory requirements — GDPR in Europe, CMMC in North America, data-sovereignty obligations across Asia-Pacific — and different levels of on-site IT capability, without the policy management 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	END-TO-END POLICY OWNERSHIP
GTT's top-ranked global IP backbone covers 400+ points of presence across six continents. Access services delivered over this infrastructure provide consistent, low-latency performance for remote users and contractors regardless of location — including markets where reliable last-mile connectivity is difficult to source independently. Manufacturers do not need to manage separate access arrangements in each country. GTT does.	The GTT Envision Platform is the operational difference between managing access globally and simply deploying tools. GTT EnvisionCORE enforces consistent identity and access policies across every site. GTT EnvisionEDGE provides real-time session telemetry at the plant edge. GTT EnvisionDX delivers unified access reporting and compliance evidence for security teams and auditors. Together, a manufacturer with sites across four continents has one accurate, current view of its access posture.	GTT's teams own access policy deployment, ongoing configuration management and in-life service management across the entire estate — not just the initial implementation. This includes policy updates, device posture integrations, identity provider connections and 24/7 access monitoring. Internal IT and security teams retain strategic direction. GTT retains accountability for consistent enforcement and performance

MANUFACTURING SUB-VERTICALS SERVED

Zero Trust Architecture Adapted Across Every Manufacturing Sub-Vertical

Zero trust, everywhere addresses distinct access challenges across manufacturing sub-verticals, with architectures adapted to the operational, regulatory and technology environments of each:

Automotive & EV	TISAX-aligned access controls, scoped supplier and OEM partner connectivity, identity-based access for plant automation and engineering systems
Food & Beverage	Secure contractor and vendor access across 100+ sites, consistent policy enforcement for cloud-dependent supply chain platforms
Chemicals & Materials	Just enough access for engineering and R&D teams in safety-critical environments, COMAH and SEVESO-aligned access governance
Packaging	Scoped third-party access for logistics partners and equipment vendors, consistent access controls across distributed manufacturing and warehouse sites
Building Materials	Identity-driven access across geographically dispersed estates, audit-ready reporting for compliance reviews across European and global operations
Industrial Equipment & Automation	Controlled access for complex supplier ecosystems and field engineering teams, session logging for production-critical OT systems



NEXT STEPS



Starting the Conversation

Access is the first line of defense for every system your operations depend on. To modernize your manufacturing access architecture:

- ✔ **Map current access tools and third-party connections:** Identify every active remote access method, VPN deployment and third-party integration across the global estate. This is the starting inventory for a Zero Trust transition.
- ✔ **Assess contractor and vendor access controls:** Evaluate whether current architectures support scoped, time-bound access for non-employee users or whether contractors receive the same broad network access as internal staff.
- ✔ **Audit access visibility:** Determine whether your security team can produce a complete, current view of who accessed which systems, from which devices, and under which conditions. If that requires manual effort, the architecture is the gap.
- ✔ **Engage GTT:** Contact GTT to map Zero Trust, Everywhere to your manufacturing access environment and establish the identity-driven, centrally governed access foundation your operations require.

ACCESS IS THE FIRST LINE OF DEFENSE FOR EVERY SYSTEM YOUR OPERATIONS DEPEND ON.

GTT replaces perimeter trust with identity-driven access across every user, every site and every partner relationship — consistently enforced, continuously verified and fully visible across the entire global manufacturing 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.

