nile

WHITEPAPER | MANUFACTURING & LOGISTICS

Security, AI and Autonomous Operations:

The Network That Keeps Every Line Running

How global manufacturers and logistics operators can keep plants running, contain breaches, and stay ahead of regulators and attackers — using Nile's AI-driven, Secure Network-as-a-Service to protect uptime and run autonomously, without writing hard checks or staffing every site.

AUTHORED BY

Shashi Kiran & Chris Liou

v1.0

Executive Summary

In 2025, a single cyberattack forced Jaguar Land Rover into a global production shutdown — lines stopped and plants idled, with the cost measured not in one ransom note but in every vehicle that did not get built. For any manufacturing or logistics leader, the question is no longer whether an attack will reach the plant floor, but how far it travels once it does — and how many shifts you lose finding out.

Manufacturing was the most attacked industry in the world in 2025, by a wide margin. It has held this top rank for multiple consecutive years due to its vital role in supply chains, vulnerable legacy computer networks, and the devastatingly high cost of production downtime. Per KELA's 2025 ransomware data, attacks on the sector surged 61 percent year-over-year, with average ransom demands crossing $1.16 million. The named incidents span continents: Bridgestone disrupted plants across multiple countries, while Thailand's Bangchak Group and Romania's largest power producer, Oltenia Energy Complex, were both hit in late 2025. South Korea saw a 540 percent year-over-year jump in ransomware activity. In India, 65 percent of affected manufacturers paid, with average payments of $1.35 million — the highest in Asia-Pacific. Dragos summarized the pattern in early 2026: industrial organizations significantly underestimate the reach of ransomware into operational technology because they treat it as an IT problem.

The three groups that dominated manufacturing extortion in 2025 — Akira, Qilin, and Play — rarely needed a malware exploit. They entered through VPN accounts without multifactor authentication, exploited unpatched edge devices, or compromised contractor laptops, then moved laterally into the OT layer. Industry-wide, the average detection-and-containment time for an industrial ransomware incident in 2025 was 42 days. Organizations with comprehensive OT visibility cut it to five.

At the same time, what runs on a plant or logistics network has changed beyond recognition. Robotic arms, autonomous mobile robots, PLCs, RFID portals, IP surveillance, handheld scanners, environmental sensors, and tens of thousands of contractor and supplier devices now share infrastructure with the systems that move production. Safety-critical control is often isolated; the much larger attack surface is everything around it. This whitepaper is written for the CIOs and CISOs accountable for that infrastructure. In plain business terms, it explains what a modern site needs from its wired and wireless network, why the legacy approach no longer scales, and how Nile's AI-driven, autonomous Network-as-a-Service narrows the blast radius of the next incident while delivering consistent uptime and global regulatory alignment.

The bottom line for CIOs and CISOs

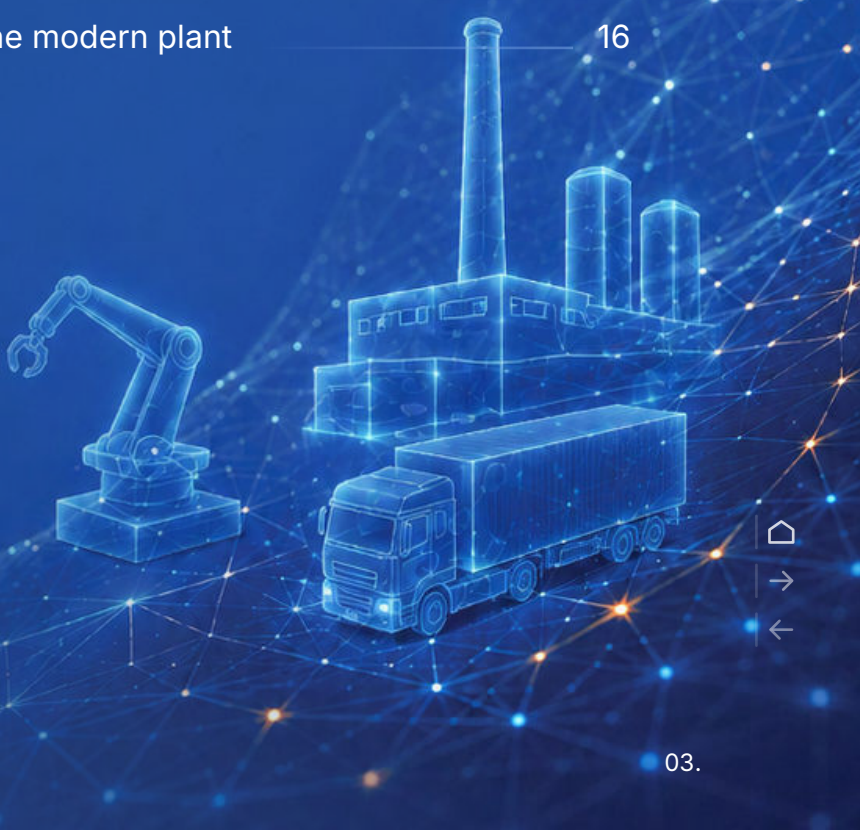
Every minute of unplanned downtime in a plant or a distribution facility has a measurable cost in shipments lost, contracts at risk, and SLAs missed — and every flat or fragile network is a path attackers will exploit. If your site network is more than five years old, the question is not whether you have firewalls. It is what stays reachable the next time a human-targeted attack succeeds anywhere in your stack. Nile turns the network from a sprawling, locally managed liability into a single, centrally governed service that limits what any one intrusion can reach — the same in every site, in every region, 24 hours a day.

+61%
RANSOMWARE GROWTH IN MANUFACTURING, 2025

$1.16M
AVERAGE RANSOM DEMANDED, 2025

30-60%
TCO REDUCTION REPORTED BY NILE CUSTOMERS

Table of Contents



01. What's at stake on the production floor

A modern plant or distribution center is one of the most demanding network environments in the enterprise — and almost none of the assets that run it are ones the network team gets to choose.

Walk a plant or a fulfillment center today and the connectivity footprint looks nothing like a corporate office. The systems that move work are themselves networked, and almost everything carries a microcontroller or a radio.

What's connected on a typical site

- **Industrial control**
  Robotic arms, PLCs, and HMIs running real-time control, often speaking Modbus, EtherNet/IP, OPC UA, or Profinet — and almost never on a supported OS.
- **Autonomous movement**
  AMRs, AGVs, and conveyor lines needing continuous coverage with deterministic, sub-50 ms roaming. A coverage gap is a stalled robot.
- **Mobile productivity**
  Pickers, forklift terminals, voice-directed pick, label printers, RFID portals, and barcode scanners. A failed scan is a missed shipment.
- **Surveillance and vision**
  IP cameras for safety, quality, and AI-driven defect inspection — each a live endpoint with credentials, firmware, and a vendor cloud.
- **Building and environmental**
  HVAC, refrigeration, dust collection, lighting, access, and energy sensors — usually from a different vendor than the production systems.
- **People**
  Engineers, contractors, suppliers, auditors, and regulators — each arrives expecting connectivity, and each becomes a potential entry point.

This is the environment ransomware groups have learned to attack with precision. With the emphasis on timely production and cost structures, other elements can become a casualty. Akira, Qilin, and Play repeatedly entered through VPN accounts without MFA, exploited unpatched edge devices, or compromised contractor laptops, then moved laterally into OT. The defense is consistent too: identity-based segmentation, default-deny posture, and continuous visibility, applied uniformly across every site.

The fundamental tension

Resilience, the cybersecurity insurer, identified the dynamic that made manufacturing the most attacked sector in the world: the perceived risk of taking production offline to implement security controls feels greater than the risk of operating without them. So plants run with legacy controls, flat networks, and visibility gaps that adversaries find with depressing reliability. Modern infrastructure has to solve both sides of that equation at once.

What downtime really costs

A single Saturday-night outage at a regional logistics site translates directly into shipments that did not go out the door. A single millisecond of jitter on a control loop can scrap a batch. The cost isn't theoretical — it has a name on the income statement every shift, and bills measured in millions when something goes wrong.

> The lesson isn't that any single product would have prevented the breach. It is what it costs to operate a network you can't quickly vouch for under pressure — when there is no way to trust the line, or the data it is carrying.

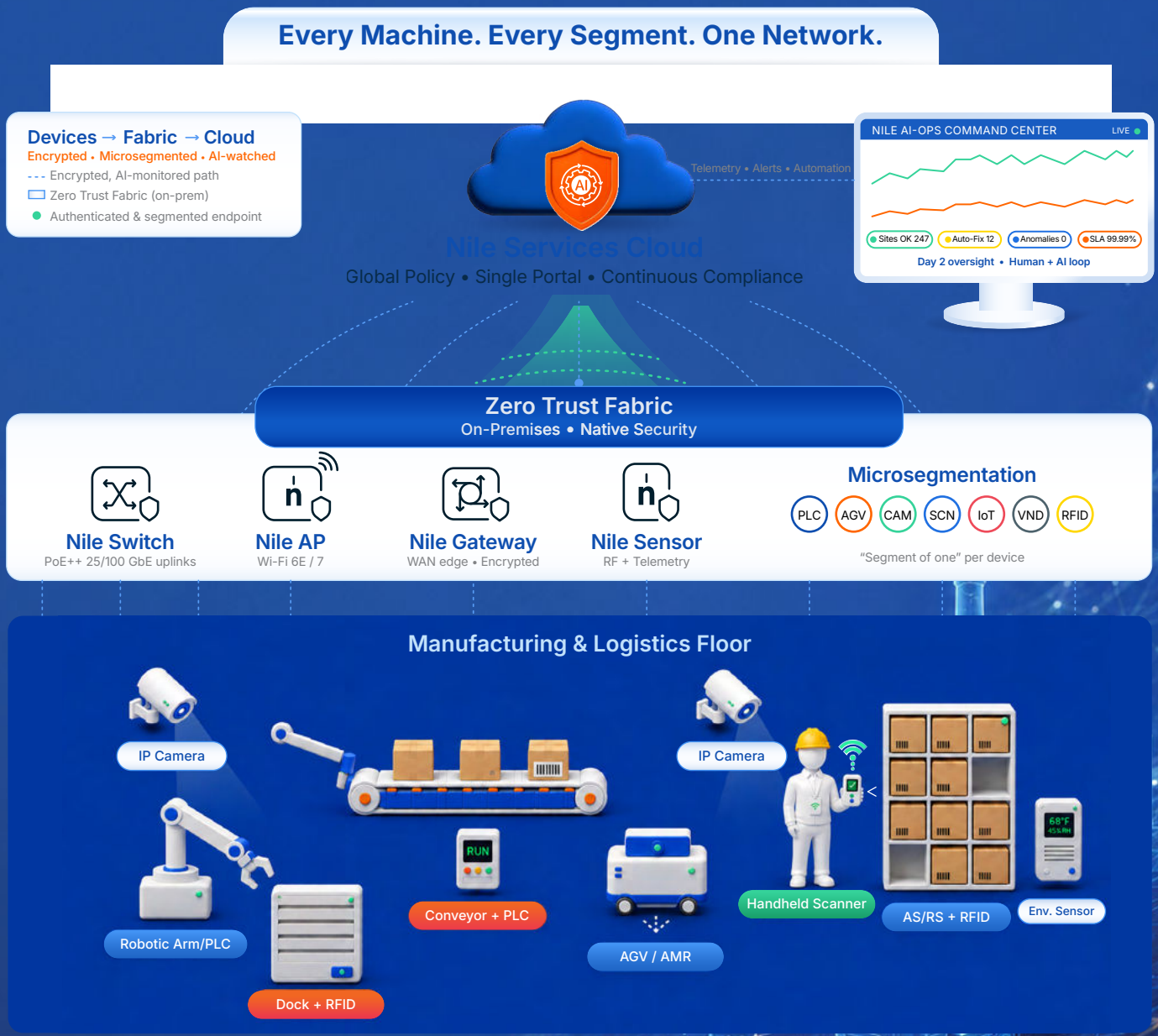


Figure 1. Level 1 control devices aggregate behind an industrial (Purdue Level 2) switch. Nile's enforcement point for that cluster is the switch's uplink port, while directly-connected IT/IoT devices — and APIs where the design allows — receive a per-device segment of one.

02. Can the network really help the plant?

Three audiences. One connected floor. Zero room for a stalled line — or a breach.

A manufacturing or logistics network has to satisfy three audiences at once: regulators who require provable controls over the systems that touch safety, quality, and intellectual property; operations leaders who require uninterrupted throughput; and IT and security leaders who need something they can run consistently across dozens or hundreds of sites with the people they actually have. The requirements below reflect what these constituencies — plus modern attackers — now force onto every property.

Wired Connectivity

- **Always on.** The line cannot tolerate a switch reboot mid-shift. Redundant fabric, sub-second failover, and high availability are baseline.
- **Built for OT bandwidth.** Industrial systems, vision inspection, and 4K surveillance need 25 and 100 GbE uplinks at the distribution layer. Yesterday's gigabit fabric is no longer sufficient.
- **Power for everything.** Cameras, RFID readers, access points, and sensors all draw power over the network — hundreds of ports delivering PoE+/PoE++ reliably, with diagnostic visibility.
- **Defensible segmentation.** Segmentation that maps to IEC 62443 zones and conduits, defensible to a NIS2 or CMMC auditor — without a four-week services engagement to configure a new line.

Wireless Connectivity

- **Wi-Fi 6E and 7.** The bandwidth, density, and deterministic behavior that AGVs, voice picking, AR-guided maintenance, and machine-vision inspection demand.
- **RF that works in metal boxes.** Coverage that survives racking that reflects RF, freezers that absorb it, and steel that distorts both — AI-tuned RF that adapts as layouts change, not a quarterly site survey.
- **Deterministic roaming.** AMRs and AGVs cannot tolerate roaming gaps; sub-50 ms handoff is the floor. Real-time control loops run on millisecond budgets with hard jitter limits.
- **Contractor and guest isolation.** Suppliers, auditors, and third-party engineers connect quickly without ever touching the production network.

Security

- **Zero Trust by default.** Every device, user, and connection authenticated and explicitly authorized before any traffic flows. Trusting whatever plugs into a port behind the firewall is over.
- **Continuous OT visibility.** OT and IT assets inventoried, classified by function, and isolated by policy. You cannot protect what you cannot see — and most plants cannot see most of it.
- **Identification without agents (IT and IoT).** Continuous agentless fingerprinting — DHCP attributes, MAC/OUI, protocol behavior, and flow telemetry — identifies the IT and IoT endpoints that will never run an agent. For example, the Nile solution can actually differentiate between an IT/OT device that belongs to the enterprise vs an off-the-shelf printer. This has led to large enterprises with device proliferation adopting Nile, as fingerprinting alone cannot differentiate between a rogue device and an actual enterprise device. The admin provides credentials, which Nile can use alongside fingerprinting to distinguish enterprise devices from store-bought devices. Nile automatically quarantine a device if the credential validation check fails.
- **OT identification.** OT fingerprinting is a different problem: a significant proportion of control devices use static IPs, so DHCP- and MAC-based methods don't apply. Nile is also looking into these approaches including deep-packet inspection of industrial protocols matched against vendor device databases, and integration with a dedicated OT visibility platform to extend device identification to the control layer.
- **Containment, matched to the device.** If a contractor laptop or IoT sensor is compromised, containment can be automatic. For production OT, response is configurable so a control device is never isolated in a way that could stop a line — Nile alerts the operator and leaves the kill switch in their hands (see Section 05).
- **Audit-ready in every region.** NIS2 requires 24-hour incident notification across the EU; IEC 62443, CMMC, and ISO 27001 require evidence on demand. Segmentation, access control, and continuous monitoring are built in today; AI-assembled audit evidence is on the roadmap, covering the network-control portion of a broader, process-oriented compliance picture.

03. Why the legacy network is a bad bet

Most multi-site manufacturers run a network architecture designed twenty years ago and quietly patched ever since. It is costing real money every quarter, even when nothing visibly breaks.

The traditional industrial network is a stack of switches, wireless controllers, access points, firewalls, VLANs, and overlay tools — with NAC appliances and RADIUS servers at the IT and upper-OT levels where they apply, rather than throughout the control stack — that nobody on a single site fully understands and nobody can fully defend. Multiply that by every plant and DC the business operates and the result is the worst of all worlds: high cost, fragmented policy, inconsistent compliance posture, and a steady stream of operational fires.

The Legacy Reality	What It Actually Costs the Business
Dozens of vendors per site, multiplied by sites worldwide, each with its own license, support contract, and end-of-life cycle.	Capital costs spike at every refresh. Each acquisition or new site multiplies the integration burden rather than amortizing it.
Security stitched together from VLANs and overlay tools — with NAC and RADIUS at the levels where they fit — that nobody owns end to end.	Misconfiguration is the leading cause of breaches, and MFA misconfiguration alone was the single costliest weakness in manufacturing in 2025.
Patching, RF tuning, segmentation policy, and audit-evidence collection all done by hand at each site by people who have other jobs.	Mean time to repair is hours or days. The site IT team becomes a bottleneck for every business initiative.
No real performance accountability. Hardware vendors sell boxes, not outcomes.	When the line slows or the picking aisles fall silent, nobody is contractually on the hook. The plant absorbs the loss.
OT and IT systems sharing infrastructure across a missing or weak enforcement boundary — or a Purdue-model separation that holds but is costly to maintain by hand.	Where the boundary is missing or weak, a compromised contractor laptop, a vulnerable RDP gateway, or an unpatched edge device becomes a path to PLCs, MES, and ERP. Where teams do enforce Purdue zones with industrial firewalls between levels, the separation holds — but the upkeep is a standing tax on the site.

Then there is the staffing problem. McKinsey's analysis of distributed industrial operations found that highly fragmented site networks consistently fail to scale improvements from one location to the rest. A regional logistics site may have one IT generalist, often a contractor. A plant in a smaller market may have nobody. The assumption that each location will operate its own switching fabric, manage its own segmentation, tune its own RF, and prepare its own audit evidence has collided with reality in every multinational manufacturer we have spoken to.

What that looks like in practice

Akira, the most prolific ransomware operation against manufacturing in 2025, repeatedly gained initial access through VPN gateways without MFA, then moved laterally through environments where IT and OT were not effectively separated. The pattern is consistent enough that it has become the playbook. Manufacturers are being asked to write larger checks for the same architecture that just failed publicly across the sector. There is a smarter bet.

04. The Nile difference

A network delivered as a service. Zero Trust built in, not bolted on. Run by AI, not by people. The same in every site, in every region.

Nile has rebuilt the enterprise network from a clean sheet, delivering wired and wireless LAN as a fully managed, AI-driven autonomous service — with Zero Trust security and a financially backed performance guarantee built into the foundation. For a global manufacturer or logistics operator, two things change at once.

1 The network becomes a service, not a project

Nile delivers everything — access points, switches, WiFi sensors, management software, AI operations, and security controls — as a single subscription. Policy is configured once in one portal and enforced uniformly across every site. Where NAC and RADIUS would normally sit — at the IT and upper-OT levels — there are no appliances to size site by site and no separate infrastructure to harden. No regional integration project for every new acquisition. Customers report total cost of ownership reductions of 30- 60% versus their previous architecture — driven by CAPEX-to-OPEX conversion, eliminated truck rolls, and faster site stand-up.

2 Zero Trust and zones-and-conduits, by default

Every Nile network ships with Zero Trust as default behavior, not an upgrade. A device that connects to the fabric directly — a vendor laptop, a contractor phone, an IP camera, or an IP-capable controller or HMI wired straight in — communicates only after it has been authenticated and explicitly authorized, and it lands in its own isolated segment, a "segment of one," so a compromise cannot spread laterally. That per-device model aligns with the zones-and-conduits architecture IEC 62443-3-2 describes — the same enforcement whether the site falls under NIS2, CMMC, China's MLPS, or India's DPDP framework. Where control devices instead sit behind an industrial switch, authorization is applied at the switch's uplink rather than to each device individually, as the next paragraph explains.

One topology reality shapes how far the segment-of-one boundary reaches in OT, and we state it plainly. Level 1 control devices — PLCs, robotic-arm and conveyor controllers, AS/RS — typically sit behind an industrial managed switch that aggregates the control-panel network (functionally Purdue Level 2) rather than connecting to the fabric directly; sometimes for Layer 2 adjacency, sometimes for real-time latency, sometimes because the device doesn't speak IP. Where that is the case, Nile's enforcement point is the switch's uplink port, not the individual controller: the segment-of-one boundary is drawn at that uplink, so host-based isolation of a single PLC or HMI behind the switch is not achievable, and any containment action there applies to every device behind the switch at once. Traffic that stays local to that switch — between the controllers themselves — is outside Nile's enforcement in this topology. True per-device isolation applies to endpoints that meet the fabric directly: IT and IoT devices, and IP-capable assets such as HMIs where the design allows. Per-device containment is strongest at the fabric edge today, and Nile continues to harden it and extend it deeper into the OT stack — ongoing engineering that steadily makes IT/OT security convergence easier.

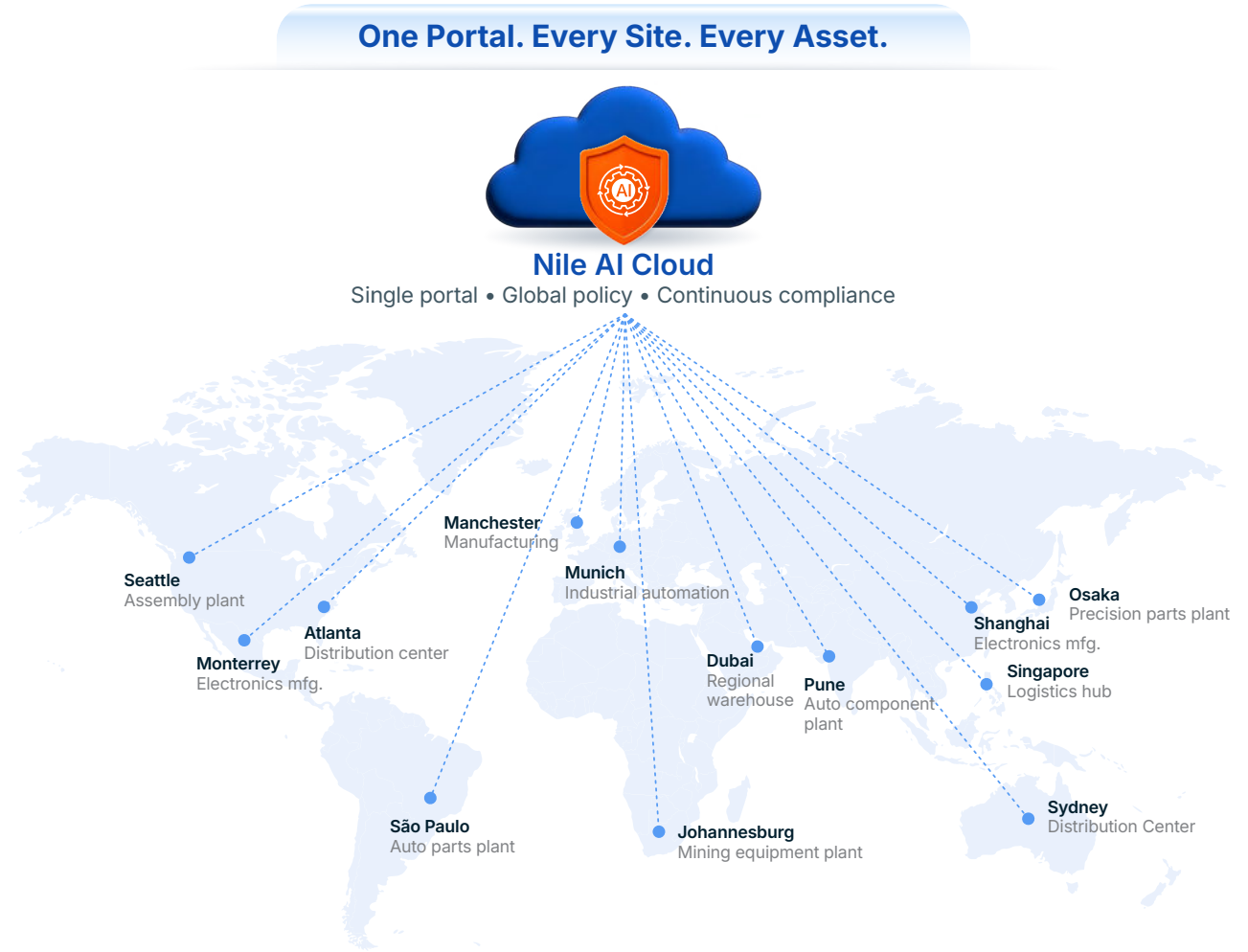
How Nile limits the next industrial-sector incident

Nile does not replace identity and access management. Where it changes the equation is on the day of an incident. Because every device, user, and connection is authorized in advance, and every access rule lives in a single global portal rather than scattered across hundreds of site switches and overlay tools, a security team can verify what is and isn't reachable in minutes, not days. The reach of any single intrusion is constrained by design to what that one identity is authorized to touch — so a vishing call or a compromised contractor laptop can't become a plant-wide shutdown. Just as importantly, the operator can vouch for it: "I know this line is protected" becomes a defensible statement, not a hope. That is what changes whether production keeps running through an incident or has to go dark.

05. AI and autonomous operations: the third revolution

The first shift was wired-to-wireless. The second was on-premise-to-cloud. The third — the one that decides which manufacturers and operators thrive in the next decade — is human-operated to AI-operated networks.

Nile's network isn't just managed by software; it is operated by an AI system that ingests live telemetry from every access point, switch, and sensor across every Nile customer in the world. For an industrial operator with sites across continents and limited IT staff at each, the implications are direct and measurable.



1 Policy framework
Applied uniformly

Configure once. Enforced at every site.

Audit-ready under: NIS2, IEC, 62443, CMMC.

0 On-Site Network Engineers
Required to operate

Remote-managed by Nile's AI service.

Site IT focuses on the business, not patching.

Hours To stand up
A new site

Hardware ships. AI brings it online.

Acquisitions, Expansions, New DCs.

Figure 2. **One Portal. Every Site.** *A single policy framework applied uniformly across every plant and DC, regardless of geography, with regional regulatory mappings handled in software.*

Predictive uptime, not reactive firefighting

Most outages announce themselves quietly first — a radio drifting off-channel, a switch port logging errors, a controller swapping memory. Human teams catch these after the symptom hits the floor, when a picker is idle or an AGV has stalled. AI catches them before. Nile flags degrading components, runs the diagnostic, and either self-heals or opens a pre-investigated ticket — so a human only ever sees the issues that genuinely need a human.

AI-driven threat detection for OT environments

Modern attacks don't announce themselves with malware signatures. They look like a service account logging in at an odd hour, a contractor laptop reaching an IP it has never contacted, or a PLC initiating an outbound connection during the wrong shift. Nile's AI already learns normal from anomalous for IT and IoT across its global footprint in seconds, not weeks. Extending that behavioral layer natively into OT depends on the OT device identification described in Section 02 — fingerprinting is the foundation, and behavioral analytics follows from it — so as that roadmap capability matures, detection reaches deeper into control-system telemetry. Just as important is what happens next, and Nile makes the response configurable rather than one-size-fits-all. For IT devices operating inside the OT environment — laptops, vendor machines, jump hosts — and for non-production OT assets, Nile can contain automatically: see the anomaly, isolate the device, and alert the team. For production OT devices, availability outranks confidentiality — the inverse of IT — and automatically isolating a PLC or DCS controller could halt a line or trigger a safety event, making the fix worse than the attack. There, Nile follows the model OT operators expect: alert with full context and let the operator activate a kill switch on their own terms and timeline.

Autonomous everyday ops: solve the IT-staffing problem

This is the single biggest pain point in industrial IT, and the problem Nile's architecture was built to solve. Configuration drift, firmware patching, capacity planning, RF tuning, port resets, certificate rotations, segmentation enforcement, and audit-log generation are all handled by the service. Stand-up scales to the deployment. For IT-centric sites — a warehouse, distribution center, or corporate location — a site can come online with a single hardware shipment and the same policy as every other site, often in hours to days. A manufacturing plant with an established OT network is a different exercise: that migration is a longer, structured engagement that works around production windows and the control layer, and OT deployment practice is still modernizing toward the speed IT environments now take for granted. Either way, local IT — where it exists at all — shifts from running the network to running the business, standing up new lines, integrating an acquired facility, supporting a peak.

Network intelligence that compounds across the fleet

When Nile's AI detects, diagnoses, or remediates an issue at one customer, the lesson is applied across the entire customer base. A manufacturer that joins Nile in 2026 benefits from every problem already solved for every other Nile customer — including hospitals, universities, financial institutions, and Fortune 500 industrials. The same problem does not happen twice, anywhere in the fleet.

06. Nile delivers outcomes against stringent requirements

Every requirement in Section 02 is addressed natively by Nile's secure Network-as-a-Service.

There is no checklist of optional add-ons, no fragmented tech stack, and no claim that Nile replaces the controls a regulator requires on the safety-critical or process-control network itself.

Operational Requirement	Nile Capability	Business Outcome
24/7 wired availability for production lines and surveillance	AI-driven self-healing on hardened, redundant switching, with a financially backed availability SLA	Predictable uptime; outages prevented before they hit production
High-density Wi-Fi for AGVs, AMRs, voice picking, and inspection	Wi-Fi 6E/7 APs with continuous, AI-tuned RF optimization and sub-50 ms roaming	Pickers and robots keep moving; throughput holds at peak
OT/IT separation defensible to a NIS2 or IEC 62443 auditor	Zones-and-conduits enforcement via identity-based microsegmentation, configured globally	One audit story across every site; faster regulator response
Unmanaged OT and IoT sprawl (PLCs, sensors, cameras, scanners)	Agentless fingerprinting (DHCP, MAC/OUI, protocol behavior, flow telemetry) for IT/IoT today; OT recognition via DPI of industrial protocols and OT-platform integration (for example, Claroty or Armis) on the roadmap	Devices identified and segmented where they meet the fabric — per device when directly connected, at the switch uplink when aggregated behind an L2 OT switch
Threats hidden in normal-looking OT traffic	AI anomaly detection across Nile's global footprint (native OT coverage builds on roadmap OT fingerprinting), with configurable response	Automatic containment for IT and non-production assets; alert-and-human-activated isolation for production OT

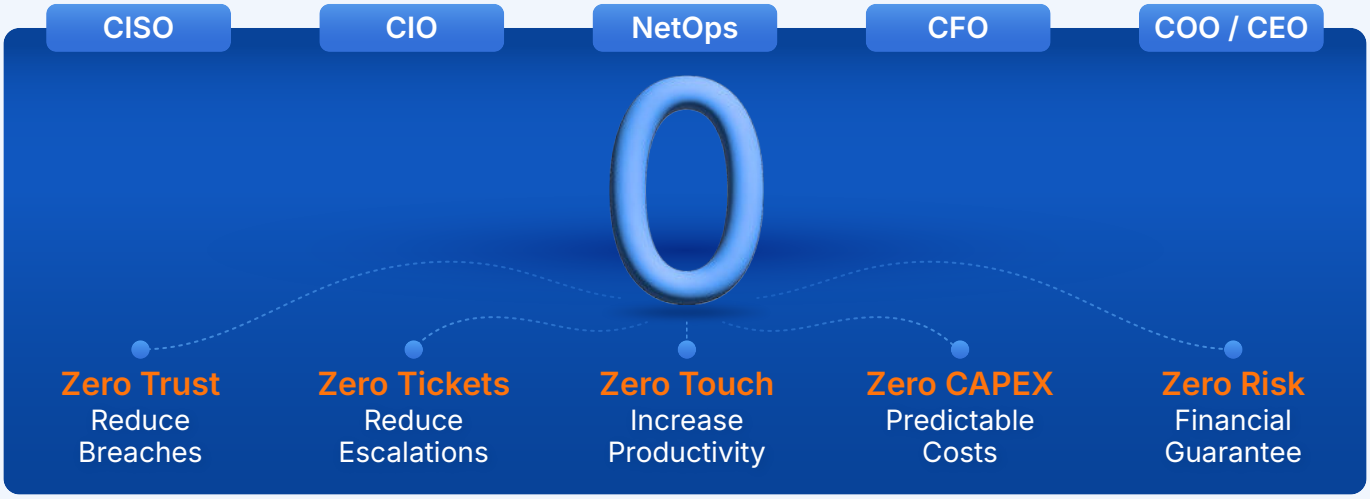
Operational Requirement	Nile Capability	Business Outcome
Compliance across multiple regulatory regimes	Segmentation, identity-based access, and continuous monitoring delivered today; AI-assembled audit evidence — mapped to NIS2, IEC 62443, CMMC, ISO 27001, and regional frameworks — on the roadmap	Substantive network-control evidence toward audits — one part of a broader, process-heavy compliance picture
IT staff shortage at distributed sites	Autonomous operations and remote service delivery from Nile's AI cloud	30–60% TCO reduction; warehouses, DCs, and corporate sites online in days — manufacturing plants via a structured OT onboarding

Backed by a guarantee

Nile is the only enterprise network that contractually commits to wired and wireless availability, coverage, and capacity. If the AI-driven service does not perform, Nile is financially accountable — accountability that does not exist in the box-and-license model the industry has lived with for thirty years.

07. Why this resonates in the boardroom

A manufacturing or logistics operation lives at the intersection of uptime, cost, and risk. The outcomes have to be compelling enough for the business to place the bet — and with Nile's secure NaaS, every stakeholder gets one.



Uptime & Revenue Protection

The largest avoidable financial event most operators will face this decade is a production-halting breach or a sustained outage at peak. Nile's Zero Trust architecture narrows what any single intrusion can reach, and AI operations catch the early signals of failure before they hit a line. One avoided shift of unplanned downtime in a single major site more than pays for the service.

Operational Continuity

Network availability becomes a contractual outcome under Nile's financially backed guarantee, not a vendor's marketing claim. The compounding benefit is what doesn't show up on a P&L: predictable OEE, fewer production excursions, fewer customer-facing SLA breaches, and AMRs, scanners, and conveyors keeping pace with peak demand because the network underneath them never stopped working.

Regulatory Standing

NIS2, IEC 62443, CMMC, China's MLPS, India's DPDP, and ISO 27001 are converging on the same technical expectations: documented segmentation, identity-based access, encrypted management, and continuous monitoring. Nile's architecture delivers those network-security controls by default. AI-generated audit evidence — assembled continuously rather than reconstructed at audit time — is on the roadmap; Nile's AI capabilities are being developed to enable it. Two caveats keep the claim honest: these frameworks are heavily process-oriented,

and much of what an auditor examines lives in those processes, outside what any network can evidence; and the controls Nile captures, while substantive, are one meaningful part of the compliance picture, not the whole of it.

AI-readiness for the operation

The manufacturers that win the next decade will run vision inspection, predictive maintenance, digital twins, and autonomous logistics on AI. None of it performs on a network that is manually operated and constantly congested. Nile gives the floor the high-performance, intelligently managed foundation those investments need to actually pay off.

08. The right solution manufactured for the modern plant

Manufacturers and logistics operators run on a simple principle: every hour of uptime matters, and every hour of downtime has a name on the income statement.

The network is the modern embodiment of that principle, and legacy industrial infrastructure is quietly costing operators real money every quarter, with bills measured in millions when something goes wrong. Nile gives operations and security leaders a different option: a network delivered as a service, with Zero Trust security and AI-driven autonomous operations built in, backed by a financial performance guarantee, and priced as a predictable monthly cost. The same service, in every site, in every region.

Next Step

Nile offers manufacturers and logistics operators a structured assessment of their current wired, wireless, and security posture across all sites — mapped to NIS2, IEC 62443, CMMC, and the regulatory frameworks that matter in each region, with a clear business case for transition. The conversation starts with the floor and the business, not a hardware bill of materials.

About Nile

Founded in 2018, Nile delivers the only enterprise wired and wireless LAN combining Zero Trust, autonomous operations, and a financially backed performance guarantee in one subscription — building the world's most secure networks and delivering them as-a-service, becoming a force multiplier for IT.

Ready to Get Started?

Let's Talk ↗

Figures cited are drawn from public reporting and industry research current as of mid-2026, including KELA 2025 ransomware data, Dragos and McKinsey analyses of industrial operations, and the Resilience cyber-insurance report on 2025 manufacturing breaches, alongside public disclosures of the 2025 Jaguar Land Rover, Bridgestone, Bangchak, and Oltenia Energy Complex incidents. TCO figures reflect outcomes reported by Nile customers and may vary by environment.