



WHITE PAPER

# Can You Prove What's on Your Plant Network?

---

Customers, auditors, and insurers now want evidence, not a spreadsheet. How manufacturers answer across every plant, device, contractor, and AI agent.

# Executive Summary

Manufacturing has been the world's most attacked industry for five consecutive years, and the pressure is no longer only from attackers. Customers now audit supplier access controls before they place orders, and a failed questionnaire costs a contract rather than a fine.

Both audiences ask the same question: who and what is on your network, what can they reach, and should that still be true? Most manufacturers cannot answer quickly, for reasons specific to this industry.



## **MOST OF WHAT CONNECTS CANNOT LOG ITSELF IN**

Plant equipment, IoT endpoints, and controllers need network access and cannot present a credential.



## **ACCESS IS GRANTED FASTER THAN IT IS GOVERNED**

Third parties are involved in 61 percent of manufacturing breaches.



## **PLANTS ARE DISTRIBUTED AND THINLY STAFFED**

Any model requiring an appliance at every site stops scaling around the third one.



## **AI ARRIVES AS ANOTHER IDENTITY**

Autonomous agents authenticate, reach data, and act around the clock on someone else's behalf.

Closing the gap does not require a new security philosophy. It requires extending the one plants already trust at the gate to every network port, application, and administrative session, with one policy engine rather than three.

## Table of Contents

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| The Question You Cannot Answer Today .....                                    | 4  |
| What It Costs When You Cannot Answer .....                                    | 5  |
| Why Manufacturing Cannot Answer It Without Continuous Access<br>Control ..... | 7  |
| What Answering the Question Takes .....                                       | 9  |
| Start With One Plant .....                                                    | 12 |

## The Question You Cannot Answer Today

A security questionnaire arrives from your largest customer. It asks for a current inventory of every device connected to networks that touch their data or their production schedule. It asks how contractor and vendor access is provisioned, scoped, and revoked, and for the records proving it. It asks whether your production network is segmented from corporate IT, and for evidence of the enforcement rather than a description of the policy. You have three weeks.

This is not hypothetical. It is contractual, and it is spreading across industries.



### AUTOMOTIVE

Trusted Information Security Assessment Exchange (TISAX), built on ISO/IEC 27001 by the German automotive association and administered by the ENX Association, runs to more than 300 requirement questions covering asset management, personnel security, and access control. Volkswagen, BMW, and Mercedes require it contractually, and their tier one suppliers pass the requirement down.



### SEMICONDUCTOR

SEMI E187 sets a cybersecurity baseline for fab equipment covering operating system support, network security, endpoint protection, and logging. TSMC wrote it into procurement contracts in 2023, and Intel requires it as well. Equipment that cannot demonstrate compliance faces delayed acceptance or outright rejection.



### DEFENSE

NIST SP 800-171 and DFARS 252.204-7012 require contractors to safeguard controlled defense information, and the obligation flows down through the supply chain regardless of where the CMMC certification timeline currently sits.

Different industries, one pattern. Assessors ask for complete asset lists, current network documentation, and traceable access controls. The most common failure is not a missing firewall. It is an IT inventory that is incomplete or out of date, because a spreadsheet from last quarter does not meet the requirement.

**There are two audit types, and manufacturers prepare for the wrong one.** A regulatory assessment is annual, scheduled, and survivable. A failed customer questionnaire costs a contract, and nobody publishes those. Cyber insurance carriers now ask many of the same questions at renewal, where device inventory and segmentation evidence shape both premium and coverage.

Underneath it all is a question most manufacturers struggle to answer quickly: **what's on our network right now and should it be there?** Not knowing costs production hours. Increasingly, it costs contracts.

## What It Costs When You Cannot Answer

Manufacturing has been the most targeted industry for cyberattacks five years running, according to IBM's *2026 X-Force Threat Intelligence Index*. Check Point counted 1,466 publicly reported manufacturing ransomware incidents in 2025, up 56 percent from 937 the year before. Attackers concentrate here because downtime creates leverage that stolen data alone does not. The real-world cases below are not about sophistication in attacks; they are about access that wasn't sufficiently tracked.

### ACCESS THAT OUTLIVED THE PERSON

In 2014, a systems administrator at a Georgia-Pacific paper mill was terminated and escorted off site. His network credentials still worked. Over the next two weeks he connected from home through the company VPN and transmitted commands that damaged the distributed control system and quality control system at the Port Hudson plant. The court ordered restitution of \$1,134,828 and a 34-month federal sentence. The badge came back at the gate. Nothing else did.

That was 2014, and this failure mode has not aged. Verizon still finds stolen credentials somewhere in the attack chain in 41 percent of manufacturing breaches. The reason is rarely sophistication. It is that someone's access outlasted their reason to have it.

**BUSINESS IMPACT:** Production loss and equipment damage from a person the company believed it had already removed.

### ACCESS GRANTED BY A PHONE CALL

On August 11, 2023, a caller impersonating a Clorox employee asked an outsourced service desk to reset that employee's password. The agent did it without verifying who was calling. The attackers, linked by researchers to the group Scattered Spider, phoned back the same day to have the same employee's multi-factor authentication reset as well, then ran the identical play against a second target, a member of Clorox's own cybersecurity team.

With privileged access established by the attacker, Clorox suspended production and shipping, reverted to manual order processing, and dealt with product shortages for weeks. It later sued the vendor for \$380 million in claimed damages, including roughly \$49 million in direct remediation. The filings describe no exploit and no malware at the point of entry. Someone asked for credentials and received them.

**BUSINESS IMPACT:** A supplier relationship became an unmonitored path into production, and the entry point was a conversation.

## ACCESS THAT LEADS TO LATERAL MOVEMENT

In late August 2025, Jaguar Land Rover suffered a cyberattack that forced the company to shut down its systems and halt global manufacturing for roughly five weeks. JLR has never publicly confirmed how the attackers initially gained access. Early reporting widely attributed the intrusion to social engineering and compromised employee credentials, but that account has since been challenged.

What is clear is that the attack disrupted JLR's IT environment and had consequences that reached its manufacturing operations. With systems shut down and the extent of the compromise unclear, JLR had to take production offline while it worked to determine what could safely be brought back online.

Jaguar Land Rover didn't just lose a network segment. It lost the ability to continue business for the whole company — every plant, every dealer system, every supplier connection — because there was no segment to lose. A properly zoned network lets you sacrifice a limb to save the body. With a flat network, the company had no limbs to sever. Just one body, fully connected, and the only tool left for containment was amputating all of it at once.

The Cyber Monitoring Centre put the total UK financial impact at 1.9 billion British pounds, roughly USD 2.6 billion, across more than 5,000 affected organizations. To date, this is the most economically damaging cyber event in UK history.

**BUSINESS IMPACT:** Production stops because nobody can prove which systems are safe. The shutdown isn't a direct consequence of the attack — it's a containment decision made in the dark, because the network gave nobody the visibility to make it in the light.

### DOWNTIME IS THE NUMBER THAT MATTERS.

Before weighing anything else here, work out what one hour of stopped production costs you: lost revenue, plus idled labor, plus recovery, before scrap, expedited freight, and contractual penalties. In Forrester's study of Portnox Cloud, the composite organization cut annual network downtime by 95 percent, recapturing 34 hours a year that had previously come out of production. Multiply your own hourly figure by 34, and you have the size of the problem in your own currency.

|                                                             |                                                                        |                                                                |
|-------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Georgia-Pacific</b><br>Paper mill, 2014                  | <b>Clorox</b><br>Consumer goods, 2023                                  | <b>Jaguar Land Rover</b><br>Automotive, 2025                   |
| <b>ATTACK VECTOR</b><br>Retained VPN access                 | <b>ATTACK VECTOR</b><br>Help desk phone call                           | <b>ATTACK VECTOR</b><br>Lateral movement                       |
| <b>ACCESS CONTROL GAP</b><br>Credentials outlived the badge | <b>ACCESS CONTROL GAP</b><br>No identity check before credential reset | <b>ACCESS CONTROL GAP</b><br>No containment at the IT boundary |
| <b>BUSINESS IMPACT</b><br><b>\$1.1M restitution</b>         | <b>BUSINESS IMPACT</b><br><b>\$380M claimed</b>                        | <b>BUSINESS IMPACT</b><br><b>£1.9bn, 5 weeks down</b>          |

Sources: U.S. Department of Justice; The Record; Cyber Monitoring Centre.

## 03 Why Manufacturing Cannot Answer It Without Continuous Access Control

The reasons manufacturing companies cannot easily answer the access control question are structural. There is a wide variety of vendors accessing systems and expanding numbers of IoT and OT devices through which to gain access. AI adds more complexity, being able to do what attackers took days and weeks to do in a matter of minutes. Once in, attackers are free to exfiltrate data, lock systems, and demand ransoms, bringing production to a halt while teams scramble to recover.

### MOST OF WHAT CONNECTS CANNOT LOG ITSELF IN

Plant floors run on devices that will never present a credential. IoT and IIoT endpoints, HMIs, the touchscreens operators use to run a line, label printers, handheld scanners, test stands, vision systems, and building automation controllers all need network access. In many environments, without an agent installed, these entities can't be seen and therefore monitored. Ask a plant network engineer to list every device or identity on the production VLAN and the realistic answer is a spreadsheet that was only accurate at commissioning.

This blind spot is where intrusions land. Verizon found that vulnerability exploitation opened 38 percent of manufacturing breaches, and stolen credentials appeared somewhere in 41 percent. Ransomware was the endgame in 61 percent of them.

## ACCESS IS GRANTED FASTER THAN IT IS GOVERNED

A controls integrator arrives to commission a new line. He gets a temporary badge, but no one told IT he only needs access for 60 days. His account gets set up with administrator access, and there's no off-boarding process when he leaves. Verizon found third parties involved in 61 percent of manufacturing breaches, well above the 48 percent across all industries, and attributes most to weak authentication, absent MFA, and missing least privilege.

## PLANTS ARE DISTRIBUTED AND THINLY STAFFED

Six plants often means six network access deployments, multiple RADIUS servers, and zero consistency. Many sites have no dedicated IT presence at all. Any model requiring an appliance and an authentication server at every location stops scaling around the third site, which is why so many manufacturers run a pilot at one plant and never extend it.

## THE AI AGENT ON YOUR PLANT NETWORK PROBABLY BELONGS TO SOMEONE ELSE

In August 2026, more than 100 organizations signed an open letter warning that AI-enabled attacks were about to escalate sharply and that status quo security would not be enough. The signatories were not only security vendors. General Motors signed. So did Dell, HPE, AMD, Arm, Broadcom, and SAP, alongside Microsoft, Google, Amazon Web Services, IBM, CrowdStrike, and Mastercard. When manufacturers and the companies that supply your plant systems put their names to a warning like that, the bar is rising.

- **VENDOR AI IS THIRD-PARTY ACCESS.** Predictive maintenance platforms, vision quality systems, and OEM analytics services all need a feed from plant systems. That is an autonomous agent operating inside your environment on a vendor's behalf. The AI question and the contractor question are now the same.
- **THE USUAL MITIGATIONS DO NOT APPLY.** You cannot put MFA on a service account feeding a Programmable Logic Controller (PLC). You cannot rotate a credential embedded in a vendor integration without a maintenance window. Guidance written for non-human identity assumes an IT environment with none of these constraints.
- **SHADOW ADOPTION REACHES YOUR IP.** Verizon found 45 percent of employees using AI tools on corporate devices in its 2026 report, up from 15 percent the year before, roughly two thirds through personal accounts. On an engineering workstation, that means process parameters, CAD files, and quality records could be leaving through a channel nobody governs.

Endpoint platforms will tell you an agent is behaving anomalously. None of them can take an unmanaged device off the network. That gap between detection and enforcement is where the next section starts.

## What Answering the Question Takes

Answering the question doesn't take another point product or a separate OT program. It takes three things working from one policy engine: seeing every device and identity as it connects, verifying each one continuously rather than once at admission, and enforcing the same policy across the network, applications, and infrastructure. When those work together, "who and what is on our network" stops being a spreadsheet someone updates each quarter. It becomes a live record you can produce on request.

That record is what customers and auditors are actually asking for. ISO/IEC 27001:2022 controls A 5.15 to 5.18 cover access rights, identity, and authentication, and TISAX, NIST SP 800-171, and customer security questionnaires all draw on the same requirements. None of them accept a description of policy. They want evidence that every contractor, device, service account, and AI agent was verified, given only the access needed, and cut off when that access should end. Most manufacturers already have the policy. What they lack is anything that enforces it continuously and records that it did.

The same discipline that governs who walks through the door should be applied to every identity and device that connects to your environment.

### SEE EVERYTHING, INCLUDING WHAT NOBODY REGISTERED

- Discovery, with an agent or without, identifies managed endpoints, contractor laptops, printers, cameras, handhelds, and unmanaged devices as they connect.
- IoT fingerprinting classifies devices by type, manufacturer, and risk profile from network behavior rather than an installed agent, so equipment that will never run a supplicant receives a policy instead of a permanent MAC bypass exception.

### VERIFY CONTINUOUSLY, NOT ONCE AT ADMISSION

- Legacy access control checks a device when it connects and trusts it for the rest of the session. That fails the moment the endpoint stops running antivirus, misses a critical patch, or has its certificate revoked mid-shift.
- Continuous verification re-evaluates posture during the session and restricts or disconnects when conditions change. This is the digital equivalent of a badge that stops working when the work order closes.
- Blocking a device solves a security problem and creates an operations problem. Automated remediation and guided self-service workflows return the endpoint to compliance without dispatching anyone, which matters when one team covers several plants.

# ENFORCE ONE POLICY ACROSS THREE ACCESS SURFACES

Manufacturers typically buy three products to cover the following, then watch the policies drift apart. One policy engine keeps them aligned.

| Access Surface | What it Governs on a Plant Site                                                                                                                 | Portnox Cloud |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Network        | Wired ports across the plant, plant Wi-Fi, and every device that joins them, using certificate-based authentication instead of shared passwords | NAC           |
| Applications   | Least-privilege access to named applications for remote engineers, contractors, and vendors, replacing broad VPN tunnels into flat networks     | ZTNA          |
| Infrastructure | Privileged access to switches, routers, and firewalls with zero standing privileges, command restrictions, and full accounting of who ran what  | TACACS+       |

**DETECTION IS NOT ENFORCEMENT.** Portnox brings all three access surfaces under one policy engine. It reads risk signals from CrowdStrike, SentinelOne, and Microsoft Defender through built-in integrations and turns each one into an access decision: block, quarantine, or remediate, across network and applications at once. The EDR platform flags that something is wrong. Portnox is what removes it from the network. The same policy extends to AI agents and service accounts that have their own identity, so a compromised agent can be cut off the same way a compromised user is.

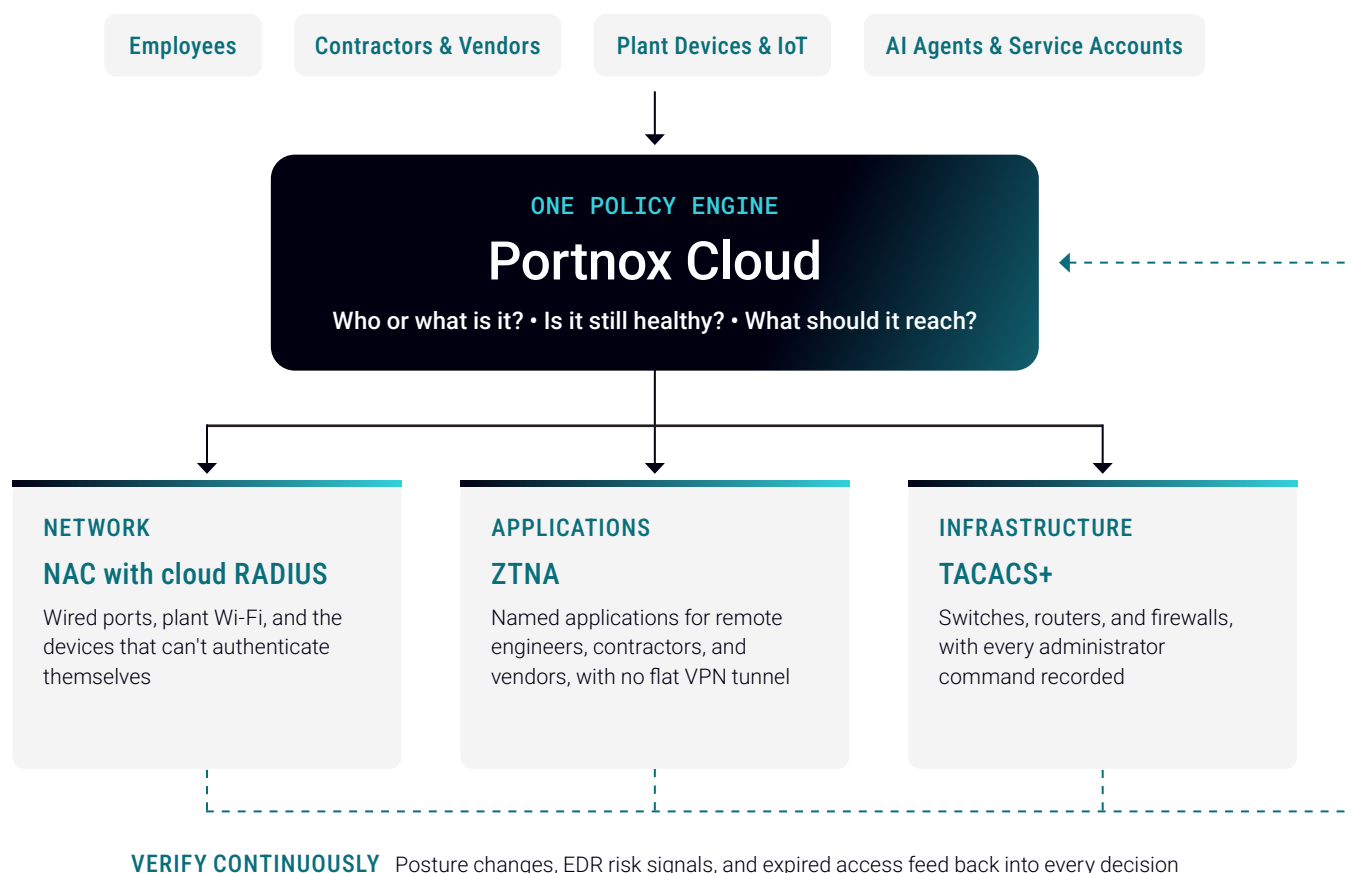
**CLOUD-NATIVE IS WHAT MAKES IT WORK ACROSS PLANTS.** In Forrester’s study, the composite organization cut the time to bring a new site under policy by 90 percent, from weeks of procurement and planning to about five hours. For an acquisitive manufacturer absorbing plants, shorter time to value is the difference between a security backlog and a security baseline.

**EVIDENCE YOU CAN HAND TO A CUSTOMER.** Per-administrator authentication with command accounting produces a record where shared switch credentials produce none, and AI-generated summaries of session activity turn a raw log into something an auditor or a customer can read. The difference between having evidence and being able to produce it on request is usually the difference between passing and stalling.

## HOW FAR THIS REACHES INTO OT

Security tooling that touches running equipment is a genuine operational risk in OT. PLCs, Supervisory Control and Data Acquisition (SCADA) nodes, and legacy controllers can fault under active scanning, and NIST SP 800-82 explicitly cautions against active testing on live industrial systems. Any approach requiring contact with the equipment loses the argument with operations before it starts. Discovery here is passive: device identity comes from traffic the equipment already generates, so the inventory builds without agents, scans, or probes touching a controller.

Identity-driven visibility, enforcement, and segmentation reach further into the plant than most manufacturers expect, and they work now, not after a separate OT program completes. Purpose-built industrial assets get the same enforcement, without waiting on deep ICS protocol parsing project first. For plants running specialist OT threat detection, that's not competition — it's a faster foundation underneath: identity and segmentation controls that are live from day one, with room for deep protocol-level tools to layer in wherever a plant needs that depth.



## Start With One Plant

FIVE QUESTIONS. ANY ANSWER YOU CANNOT GIVE WITHIN A DAY IS THE GAP.

01

Can you produce a current list of every device on your plant networks without a manual collection effort?

02

For every contractor and vendor with access today, can you name the sponsor, the scope, and the expiry date?

03

Do plant devices that cannot authenticate receive a policy, or a permanent exception?

04

Does anyone still log into a switch with a shared local account?

05

If an identity were compromised right now, how long would it take to cut its access across network, applications, and infrastructure?

Portnox Cloud answers the question your customers and auditors ask from a single policy engine, with no appliances or on-premises servers at any site. NAC governs the network: it authenticates every user and device through cloud RADIUS and profiles the equipment that can't authenticate itself. ZTNA scopes contractor and remote engineer access to named applications rather than flat networks. TACACS+ controls and records privileged access to infrastructure. Human and non-human identities are governed by the same policy, and access can be revoked across all three from one place.

To learn more about how the Portnox platform can protect you from audit failure, security incidents, and dreaded downtime, schedule a call with our team. We will walk you through the product and apply it to your environment. We can run access control in monitor mode at a chosen site and show you exactly what is connecting today. You enforce nothing until you have seen the inventory and decided what belongs.

**SCHEDULE A CALL WITH PORTNOX: [PORTNOX.COM/DEMO](https://portnox.com/demo)**

## Sources

1. "Why manufacturing companies are most vulnerable to hacking," IBM blog by Euny Hong, April 22, 2026. <https://www.ibm.com/think/news/x-force-threat-intelligence-index-manufacturing-most-vulnerable-hacking>
2. Industrial Cyber, Manufacturing ransomware surge (Check Point Manufacturing Threat Landscape). <https://industrialcyber.co/manufacturing/manufacturing-absorbs-56-ransomware-surge-of-global-attacks-in-2025-as-raas-legacy-ot-supply-chains-fuel-spike>
3. Verizon 2026 Data Breach Investigations Report and Manufacturing Snapshot. <https://www.verizon.com/business/resources/reports/dbir>
4. ENX Association, TISAX assessment and VDA ISA catalog. <https://portal.enx.com/en-US/TISAX>
5. U.S. DOJ, Former Systems Administrator Sentenced for Hacking Industrial Facility. <https://www.justice.gov/usao-mdla/pr/former-systems-administrator-sentenced-prison-hacking-industrial-facility-computer>
6. The Record, Clorox lawsuit over help-desk credential resets. <https://therecord.media/clorox-cyberattack-lawsuit-cognizant-it-contractor>
7. Cyber Monitoring Centre, Jaguar Land Rover incident statement. <https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025>
8. CyberScoop, open letter on AI-enabled cyber defense signed by more than 100 organizations. <https://cyberscoop.com/ai-cyber-defense-global-surge>
9. Forrester Consulting, Total Economic Impact of Portnox Cloud. <https://www.portnox.com/tei-portnox-cloud>
10. Portnox, Secure access for AI identities. <https://www.portnox.com/portnox-cloud/ai>
11. NIST SP 800-82 Rev. 3, Guide to Operational Technology Security and NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (<https://csrc.nist.gov/pubs/sp/800/82/r3/final> and <https://csrc.nist.gov/publications/sp800>)
12. SEMI E187, Specification for Cybersecurity of Fab Equipment. <https://store-us.semi.org/products/e18700-semi-e187-specification-for-cybersecurity-of-fab-equipment>
13. Infosecurity Magazine, "Russian Hackers Accused of Destructive Cyber-Attack on Jaguar Land Rover", June 2026. <https://www.infosecurity-magazine.com/news/russian-hackers-destructive-jaguar/>