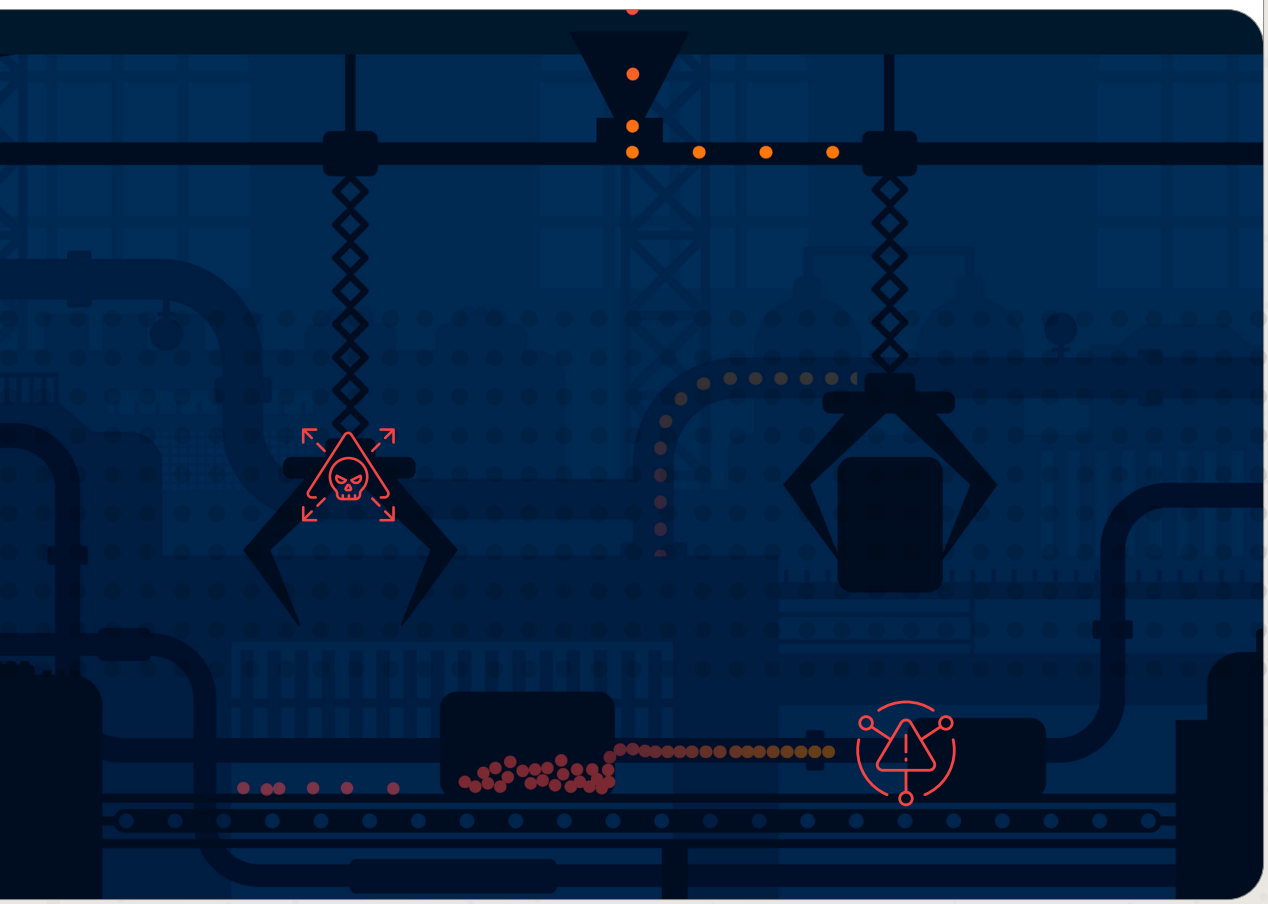
White Paper

halcyon

Production Halted

Top 10 Things Manufacturers Need to Know About Ransomware



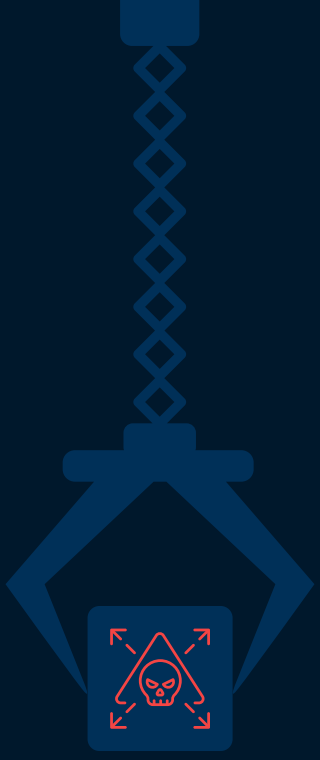
Executive Summary

When ransomware hits manufacturing, the assembly line stops. Orders go unfulfilled. Supply chains break. Unlike many industries, manufacturers can't work remotely while systems are restored. Production requires operational systems, and attackers know it. Ransomware targeting manufacturing organizations accounted for roughly one-fifth (20%) of all activity observed by Halcyon in 2025.

Ransomware Groups Single-Out Manufacturing

Manufacturing was explicitly named as a priority by at least six major ransomware groups and repeatedly cited as a high-leverage environment due to operational continuity dependencies.

- **Qilin:** Primary targeting focused on manufacturing and industrial networks, exploiting downtime sensitivity to amplify extortion leverage.
- **Akira:** Primary targeting focused on manufacturing, healthcare, education, and public-sector organizations.
- **Play:** Primary targeting focused on manufacturing, healthcare, and logistics organizations.
- **DragonForce:** Primary targeting focused on manufacturing, logistics, and healthcare organizations.
- **Sinobi:** Primary targeting focused on mid-market manufacturing, professional services, and technology-adjacent organizations.
- **Sarcoma:** Primary targeting spanned manufacturing, technology, and services organizations.



IT/OT and Industrial Environment Risk

Halcyon analysis found that manufacturing and industrial environments face compounded risk due to tightly coupled IT/OT systems, where identity or remote access compromise can rapidly cascade into operational outages. Downtime pressure escalates quickly due to safety, regulatory, and continuity requirements, increasing attacker leverage. Follow-on attacks after initial incidents were specifically noted in these environments.

This paper examines why manufacturing faces unprecedented ransomware risk, why traditional security fails to protect production environments, and what purpose-built defense delivers.

Top 10 Things Manufacturers Need to Know About Ransomware

1. Manufacturing is the #1 Target for Ransomware

The data is unambiguous: manufacturing consistently leads victim counts. Why? Production downtime is catastrophic, OT/IT convergence creates vulnerabilities, Just-In-Time (JIT) operations amplify pressure, supply chain position creates leverage, insurance coverage enables payment, and global operations complicate response.

Attackers understand manufacturers must continue producing to survive. In December 2025 alone, manufacturing led with 144 attacks (19.8% of all activity). Over the full year, Halcyon observed 1,298 attacks with peaks of 160+ in February and October. This constant assault (averaging over 100 attacks monthly) means no 'safe' period exists.

2. Know the Adversaries Targeting Your Operations

Akira leads with 318 manufacturing victims, Qilin follows with 281, and Play claims 148. These three groups alone accounted for over 700 manufacturing incidents in 2025. Recent victims range from automotive giants to specialty fabricators, including Nissan, Bulk Handling Systems, American Vanguard, and Pilot Automotive.

3. IT/OT Convergence Has Multiplied Your Attack Surface

Modern manufacturing's connected operations create vulnerabilities. Systems that were once isolated are now network-connected, including Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), Manufacturing Execution Systems (MES), and Enterprise Resource Planning (ERP). The convergence of IT and OT networks means a breach in corporate systems can reach the factory floor.

A staggering 73% of OT assets in manufacturing facilities are operating without fundamental security controls like software updates, authentication requirements, or network segmentation. Attackers seek paths from vulnerable IT to critical production infrastructure because encrypting OT causes immediate production stoppage with no workarounds.

2025

1,298 attacks

Manufacturing attacks observed by Halcyon.

2025

100+

Average monthly attacks. There are no "safe" periods.

2025

700+

Manufacturing incidents by Akira, Qilin, and Play alone.

2025

73%

of OT assets in manufacturing operate without security controls.

4. Legacy Systems Create Persistent Vulnerabilities

Legacy systems remain a significant vulnerability in manufacturing environments. The exploitation of remote services is the most common tactic in OT networks, accounting for 20 percent of incidents. Additionally, 62 percent of exploit triggers in OT networks were linked to CVEs aged 6 to 10 years. Legacy PLCs run decades-old firmware. Windows XP/7 systems still control production. Proprietary control systems have no available security updates. These systems often can't run modern security tools, and patching requires production shutdowns manufacturers can't afford. Attackers know these systems exist and target them deliberately.

5. Supply Chain Position Amplifies Impact

Manufacturers occupy critical supply chain positions that attackers exploit. Your downtime delays your customers' production. Just-In-Time inventory means minimal buffer. Contract penalties trigger automatically. In 2024, 62% of manufacturers reported supplier ransomware attacks caused their own production disruptions.

Attackers understand manufacturers face not just their own operational pressure, but pressure from customers who depend on them. This multiplied urgency increases willingness to pay. Major impacts include automotive production lines idled, consumer electronics delayed, and aerospace programs disrupted.

6. Paying Ransom Doesn't Restore Business: It Funds the Next Attack

51% of manufacturers hit by ransomware paid the ransom, the highest rate of any industry, and it is easy to see why. A $2.3M ransom seems rational when 22 days of downtime costs $28.8M. Customer penalties and stock price impacts create additional pressure, but payment is rarely successful.

Less than half (46%) of ransom payers recovered their data successfully. The rest received partial decryption, corrupted files, or nothing at all. Worse: 80% were attacked again within 12 months, with 68% re-attacked within one month. Payment validates the business model and marks you as a reliable target.

7. Double Extortion: Data Theft is Now Standard

While 40% of manufacturing ransomware incidents in 2025 resulted in data being encrypted (the lowest level in five years), extortion-only attack that didn't encrypt data grew grew to 10%, up from 3% in 2024. By 2025, double extortion became standard. Attackers steal IP (CAD files, manufacturing specs, proprietary formulas), customer contracts, and supplier agreements–then threaten public release.

87%

YoY increase in OT attacks.

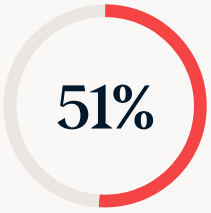
28%

organizations lack an OT-specific incident response plan.

62%

of manufacturers reported supplier ransomware attacks caused their own production disruptions.

2025



of manufacturers hit by ransomware paid the ransom.

2024 VS 2025

3% vs **10%**

2024 to 2025 surge in extortion-only (no encryption) attacks on manufacturers.

halcyon

One automotive manufacturer lost 4.2TB of CAD files and customer contracts. MintEye exfiltrated 6+TB across five victims. Consequences extend beyond the incident: **43% lost customers due to trust concerns.**

8. Traditional Security Cannot Detect and Prevent Manufacturing Ransomware

Every tracked manufacturer that suffered ransomware had security tools in place, including firewalls, antivirus, and EDR. Attacks succeeded anyway because ransomware evolved specifically to evade detection. Today's ransomware operators succeed because they:

- Use legitimate credentials to avoid triggering alerts.
- Disable EDR before deploying ransomware (Akira ransomware is extremely good at this).
- Use trusted system tools that security software allows by default.
- Target backup systems to prevent recovery.
- Time attacks for nights, weekends, holidays when monitoring is reduced.

A 2026 Halcyon-commissioned survey of security leaders confirms this:

- 100% are confident in their ability to detect ransomware, yet 49% detected too late.
- 98% use EDR, yet only 25% trust it to stop, prevent and detect ransomware.
- 49% suffered moderate-to-significant disruption despite security tools.

This gap is not implementation failure. It's a structural mismatch between what traditional security protects (systems) and what ransomware attacks (operational continuity).

9. Why Purpose-Built Anti-Ransomware Protection Works

Manufacturing needs defenses designed specifically for ransomware's unique characteristics. Where traditional cyber risk centered on the probability and impact of data loss–reputational harm, regulatory exposure, competitive disadvantage–ransomware replaces that with **immediate operational and financial disruption.**

Loss is direct, measurable, and time-bound. Impact compounds rapidly. Decision windows compress from quarters to hours. Financial damage accrues regardless of whether data is ultimately exposed.

Most critically, ransomware converts cyber risk from a probabilistic concern into a **deterministic business event**. Once an attack reaches the final stage, losses aren't hypothetical, they're actively accumulating. That's why the Halcyon Anti-Ransomware Platform provides:

2026

99% vs 49%

99% are confident in their ability to detect ransomware, yet 49% detected too late.

2026

98% vs 25%

98% use EDR, yet only 25% trust it to prevent ransomware.

2026

49%

suffered moderate-to-significant disruption despite security tools.

Once an attack reaches the final stage, losses aren't hypothetical, they're actively accumulating.

- **Ransomware-specific behavioral detection** trained exclusively on ransomware (not general threats)
- **Data Exfiltration Protection (DXP)** blocking IP theft before double extortion leverage is created.
- **Encryption key material capture** enabling recovery in minutes.
- **EDR Tamper Detection** alerting when attackers disable security tools
- **24/7 Ransomware Operations Center (ROC)** expert monitoring included at no additional cost.

10. What Manufacturers Must Do Now: A Three-Part Defense

Manufacturers need capabilities to **ensure business operations continue**, **attackers are denied leverage, and leaders are not forced into decisions under duress**. This requires moving beyond traditional security to purpose-built anti-ransomware protection.

1. Ensure Business Continuity

Deploy ransomware-specific detection. Behavioral AI trained exclusively on ransomware catches attacks that bypass EDR and other security tools.

Segment IT/OT networks. With 73% of OT assets in manufacturing operating without security controls, limiting lateral movement from corporate to production systems is critical. Monitor network boundaries for ransomware-specific behaviors.

Enable rapid recovery. The average ransomware recovery takes 22 days. Halcyon's encryption key material capture technology restores operations in minutes.

2. Deny Attackers Leverage

Stop data exfiltration. The overwhelming majority of ransomware attacks include data theft. In one case, a manufacturer lost 4.2TB of CAD files and proprietary IP. Halcyon Data Exfiltration Protection (DXP) automatically detects and alerts you to unauthorized data movement before attackers can steal it.

Protect backup systems. Attackers routinely target backups to force ransom payment. Offline and air-gapped copies are essential, but recognize that less than half of organizations recover their data successfully after paying the ransom. Halcyon's key recovery technology provides an alternative restoration path if data is encrypted.

2025

80%

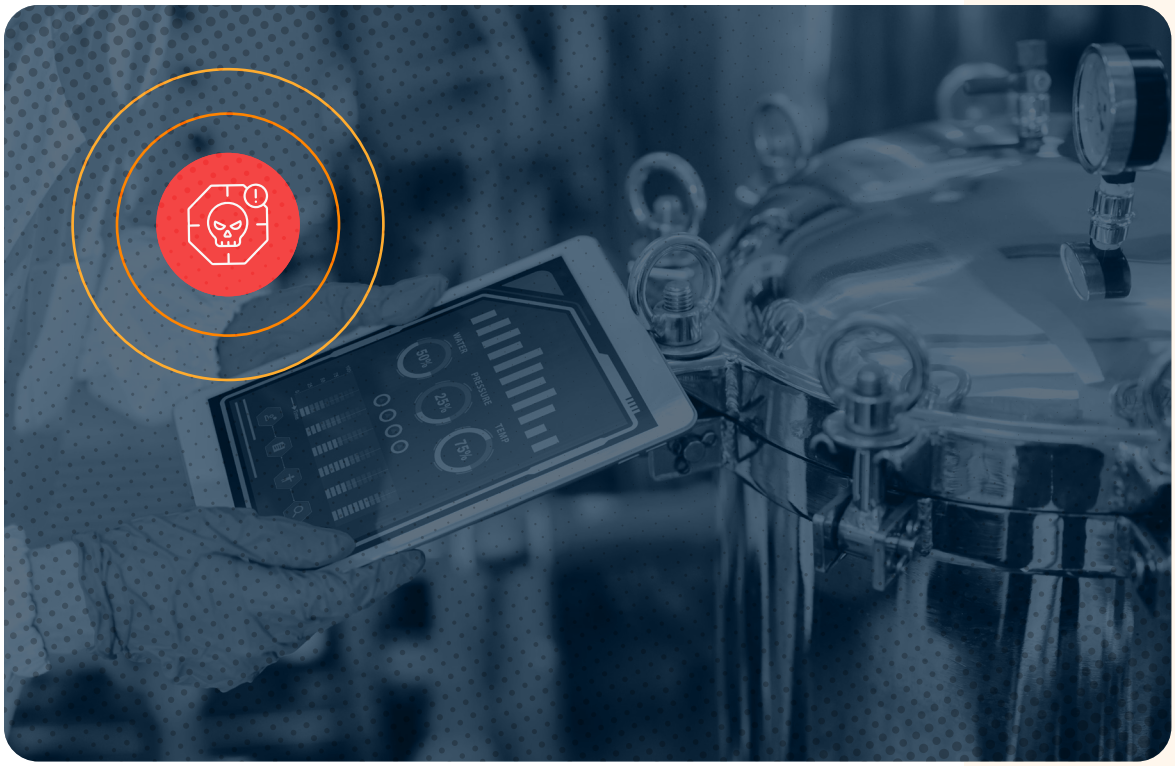
of ransom payers were attacked again within 12 months.

2025

46%

of ransom payers recovered their data successfully.

Halcyon's key material capture technology provides an alternative restoration path if data is encrypted.



Deploy 24/7 monitoring. Attackers deliberately time strikes for nights, weekends, and holidays. Manufacturers need around-the-clock expert monitoring, not overstretched internal teams making time-compressed decisions under pressure. Consider a third-party partner who provides 24x7x365 coverage.

3. Prevent Decisions Under Duress

Maintain viable alternatives. When leaders face only two choices (pay the ransom or endure weeks of downtime) decisions are made under duress. Purpose-built protection creates a third option: rapid recovery without ransom payment.

Access expert guidance. Most executives face a ransomware decision once or twice in their careers. Attackers make ransom demands almost daily. Ransomware specialists provide experienced guidance so leaders don't have to make high-stakes technical decisions under pressure.

Preserve operational control. A Halcyon-commissioned survey found that 49% of security leaders suffered moderate-to-significant disruption from ransomware attacks despite investing in a range of security tools. When attackers cannot encrypt systems, cannot steal data for double extortion, and cannot eliminate recovery options, they lose their leverage. And leaders can make rational decisions, not desperate ones.

When attackers cannot encrypt systems, cannot steal data for double extortion, and cannot eliminate recovery options, they lose their leverage.

Real-World Manufacturing Impacts from 2025

The statistics become very real when examining actual manufacturing ransomware incidents from 2025. These cases illustrate the operational, financial, and strategic consequences of ransomware attacks on production environments.

The AI-Powered Acceleration

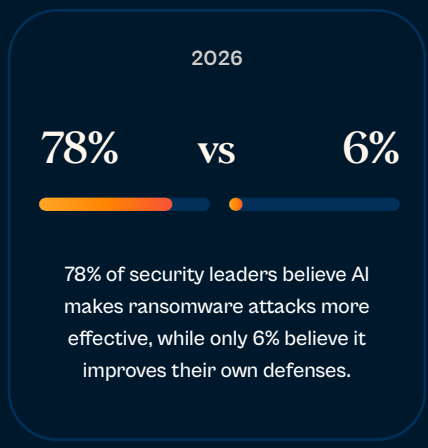
Manufacturing faces an additional challenge: AI-powered ransomware attacks. The 2026 Halcyon survey revealed that 78% of security leaders believe AI makes ransomware attacks more effective, while only 6% believe it improves their own defenses. This 13:1 asymmetry means attackers leverage AI for:

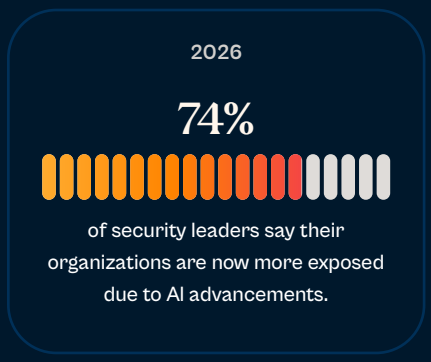
- Generating convincing phishing emails targeting manufacturing employees.
- Reconnaissance to identify high-value IP and optimal production schedules.
- Understanding when to strike for maximum operational disruption.
- Evading signature-based detection through polymorphic techniques.

74% of security leaders say their organizations are now more exposed due to AI advancements. Traditional security tools weren't designed for AI-powered threats, creating a growing vulnerability gap that manufacturers must address with purpose-built defenses.

Geographic Concentration: U.S. Manufacturing Under Siege

Nearly half of all global manufacturing attacks targeted on U.S. manufacturers. **In December 2025 alone, the United States absorbed 47.6% of all ransomware attacks across all industries.** This concentration reflects both the size of U.S. manufacturing and its perceived value to ransomware operators.





halcyon

Manufacturing Can't Afford to Learn the Hard Way

Manufacturing is the most targeted sector because production downtime translates directly to lost revenue, broken supply chains, and competitive damage. Ransomware operators have built entire operations around exploiting this vulnerability.

The manufacturers that will weather this threat are aware traditional security isn't enough:

- Traditional security protects systems; ransomware attacks operations.
- **EDR trust collapse: 98%** use it, **25%** trust it to prevent ransomware.
- **Ransom payment doesn't work: 46%** recovery rate, **80%** re-attack rate.
- **Purpose-built protection changes outcomes:** enabling recovery in minutes vs. 22-days of downtime

Your production capabilities are the foundation of your business. Protecting them demands a strategy built specifically to defeat ransomware in manufacturing.

Halcyon is purpose-built to defeat ransomware at every stage of the attack lifecycle.

Learn more at halcyon.ai/manufacturing or schedule a demo today.