How MSPs can secure and scale services for manufacturing clients

Introduction: Manufacturers are targets

Manufacturing is in the crosshairs of cyberattackers, and many organizations aren't prepared to defend themselves. While it's a significant problem for manufacturers, it represents an opportunity for managed service providers (MSPs).

Anyone responsible for an operational technology (OT) environment knows how expensive downtime can be. IBM also reported that the average data breach in the industrial sector in 2025 cost $5.6 million[2], putting manufacturing behind only health care and financial services in total cost a breach.

> According to IBM, manufacturing is the industry most frequently targeted by cyberattackers — and has been for the last five years[1]. More than a quarter or all cyberattacks target manufacturers, IBM found.

The operational technology opportunity for MSPs

Organizations with OT environments aren't like other operations. Many, particularly in the small and midsized segment, lack the internal expertise required to manage converging IT and OT environments. In air-gapped environments where a factory operates separately from the rest of the organization, there might not be any IT staff at all.

That's where MSPs can take advantage of a massive opportunity. Manufacturers need help from MSPs to ensure uptime, protect critical systems and maintain compliance. However, for service providers, success in manufacturing requires more than mastery of traditional IT services.

To succeed in manufacturing, MSPs need to evolve from standard IT operators into trusted partners capable of supporting production-critical systems where downtime directly impacts revenue, safety and supply chain commitments.

[1] IBM. (2026). X-Force Threat Intelligence Index 2026

[2] IBM. (2025). Cost of a Data Breach Report 2025

Key risks in manufacturing environments

The first thing MSPs need to know about protecting OT operations is that manufacturing customers face a unique combination of business and cyber risks:

- **Operational downtime:** Even short outages can halt production lines and result in significant financial losses.
- **Ransomware attacks:** Manufacturing is a top target due to the high cost of disruption and the value of stolen data.
- **Supply chain disruption:** Cyber incidents can cascade across suppliers and partners, as the massive 2025 Jaguar-Land Rover cyberattack demonstrated.
- **Long-life system exposure:** Industrial systems designed to last decided can unfortunately increase vulnerability to attacks and limit patching options.

IT and OT convergence risks: Attack surfaces expand as systems become interconnected.

Those are the risks MSPs can drive revenue by mitigating — if they know how and have the right platform in place. MSPs that serve organizations with OT environments face intense pressure to deliver not only protection but rapid data recovery and guaranteed operational continuity. And they need to implement their services without disrupting production. In manufacturing, downtime is simply not an option.

Business and technological challenges

A few key elements make managing an OT environment uniquely challenging for MSPs.

Managing complex hybrid environments

Manufacturing environments combine modern IT systems with long-life operational technology such as SCADA, PLCs and HMIs. These systems can be difficult to update, a persistent issue that can open security gaps.

Limited visibility across IT and OT

MSPs have to monitor and secure both corporate networks and production environments, but visibility across both domains is often fragmented. That makes threat detection and response more difficult.

Increasing ransomware pressure

Cybercriminals specifically target manufacturers due to their low tolerance for downtime. MSPs must ensure both prevention and rapid recovery capabilities.

Fragmented tools and operational complexity

Many MSPs rely on multiple point solutions for backup, security and monitoring. Tool sprawl increases costs, slows response times and creates integration challenges during incidents.

Industry and operational challenges

There are also challenges and stipulations MSPs deal with in manufacturing that they might not encounter in other environments, at least not to the same extent.

Strict uptime requirements

Manufacturing operations cannot tolerate disruption. MSPs must be able to meet aggressive recovery time objectives and service-level agreements.

Legacy systems and OEM constraints

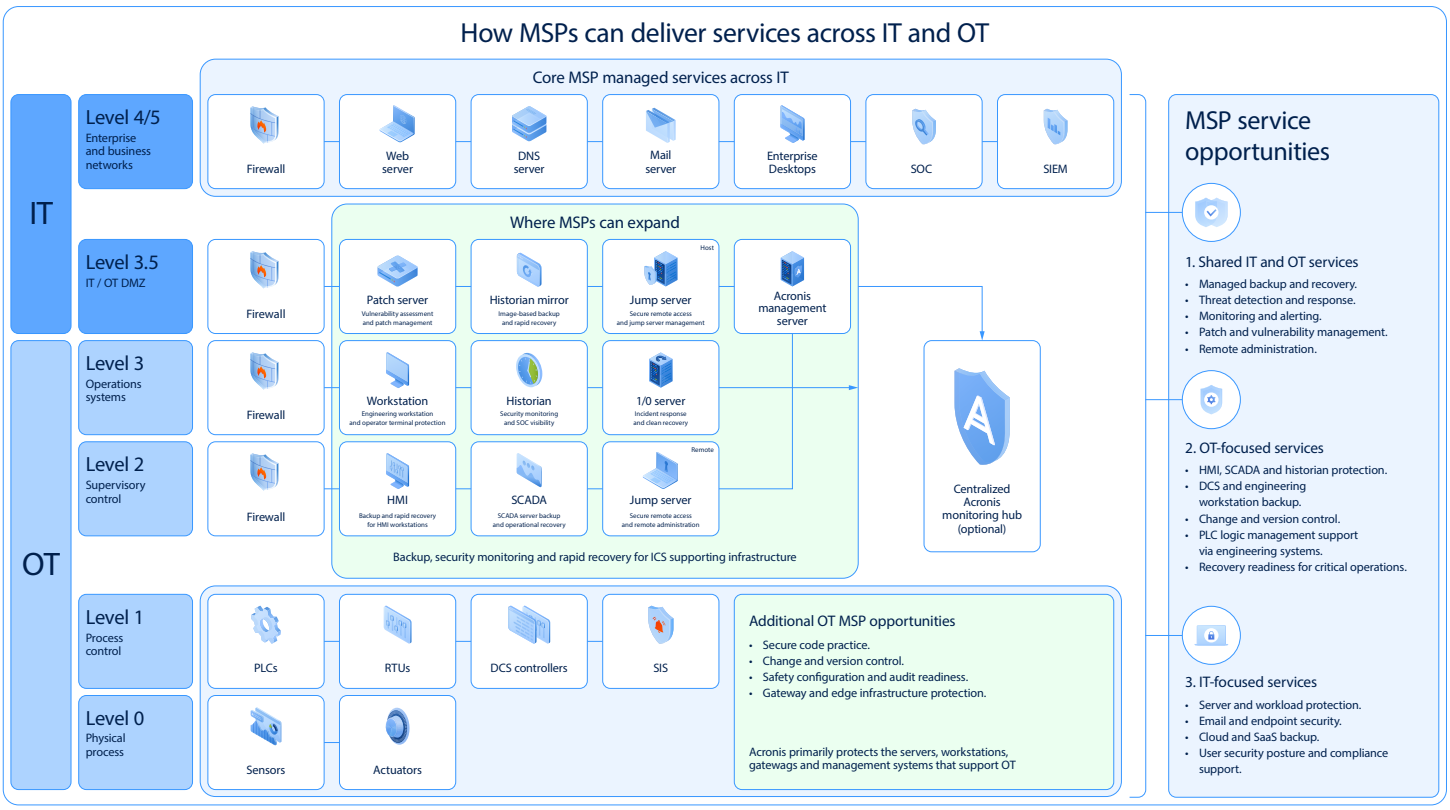
Industrial equipment is designed to run for years, even decades. As a result, it often runs on unsupported operating systems or cannot accommodate third-party agents due to warranty restrictions.

Compliance and regulatory pressure

Manufacturers must comply with frameworks such as NIST, CMMC and IEC standards, which require auditable controls and resilience capabilities.

IT convergence with OT

MSPs typically enter manufacturing through IT services and gradually expand toward OT environments. Supporting engineering workstations, data historians and HMI systems becomes a critical step in delivering full value. Service providers have to have specific OT capabilities if they want to succeed in the manufacturing space.



Solution: Acronis Cyber Platform

Acronis enables the convergence of IT and OT protection by providing a unified platform that enables MSPs to secure both kinds of environments through a single point of control while ensuring business continuity. With Acronis Cyber Platform, MSPs can:

Guarantee production continuity with Acronis One-Click Recovery

Minimize downtime with integrated backup, cybersecurity and near-instant recovery capabilities. Technicians can restore critical systems in minutes with just one click to keep production running.

Secure the multigenerational factory

Eliminate tool sprawl and protect modern cloud workloads alongside legacy industrial systems from a single, natively integrated platform without disrupting operations.

Simplify operations and improve efficiency

Replace multiple tools with one integrated platform for backup, security, patching and monitoring, reducing complexity and improving service delivery.

Enable compliance and supply chain trust

Support regulatory requirements with centralized reporting, vulnerability visibility and audit-ready documentation.

Enable risk-free validation with digital twins

Test patches and updates in virtual environments before deployment to prevent production disruption.

Navigate OEM constraints with agentless protection

Secure critical assets without installing software on sensitive systems, preserving manufacturer warranties and minimizing downtime for implementations.

Acronis Cyber Platform for MSPs

The Acronis Cyber Platform is a natively integrated, unified platform that delivers cybersecurity, data protection, infrastructure management, service automation and cloud infrastructure with a single point of control. It enables MSPs to eliminate tool sprawl and improve technician productivity.

Acronis Cyber Platform delivers:

Backup and disaster recovery

- One-Click Recovery, which enables MSPs to get systems running again rapidly.
- Immutable backups to protect against ransomware.
- Universal Restore for hardware-independent recovery.

Advanced security and XDR

- AI-based ransomware protection.
- Integrated detection and response across endpoints, email and workloads.

Advanced management and patching

- Automated patching with fail-safe rollback.
- Vulnerability assessment across IT- and OT-supporting systems.

Email security and awareness training

- AI-driven phishing protection.
- Industry-specific training for manufacturing users.

In addition, Acronis Cyber Platform provides protection for critical infrastructure supporting SCADA, DCS and HMI systems. Together, those capabilities enable MSPs to deliver a complete resilience layer that complements existing network and OT monitoring tools.

Acronis Cyber Platform for MSPs

The Acronis advantage for manufacturing MSPs

Unlike point solutions that address only backup or security, Acronis delivers a unified cyber protection platform designed for complex environments.

That approach enables MSPs to:

- Reduce operational overhead and eliminate tool sprawl.
- Improve response times during incidents.
- Focus on uptime and resilience
- Expand from IT into OT environments with confidence.

Bottom line: Consolidating protection capabilities into a single platform reduces integration challenges and operational risk while improving overall efficiency.

Make the move into manufacturing

Manufacturers need help from MSPs. They're looking to invest in uptime, resilience and business continuity with trusted partners. Acronis enables MSPs to capture that opportunity.

Start growing your manufacturing practice today:

- Book a demo of Acronis Cyber Platform.
- Launch a trial of Acronis Cyber Platform.

Acronis

Learn more at acronis.com