Microsoft Commvault

Cyber Resilience That Meets Manufacturing's Critical Standards

Manufacturers are under attack

The manufacturing industry saw a 61% increase in ransomware attacks in 2025 and has been the number one targeted industry for the past 4 years.[1] While IoT and smart devices drive production efficiency and innovation, they also expose critical operational technology (OT) and production environments to increased risks:

- Operational disruptions from ransomware and targeted attacks.
- Theft of intellectual property impacting competitive advantage.
- Exploitation of vulnerabilities in complex supply chains and legacy OT systems.

Downtime affects compliance with rigorous standards including ISO 9001 (Quality Management), ISO 14001 (Environmental Management), ISO 45001 (Occupational Health and Safety), ISO 50001 (Energy Management), and IATF 16949 (Automotive Quality Management).

Cyber resilience meets operational intelligence

By 2034 the global industrial cyber security market is projected to grow to $57 billion.[2] Manufacturers must maintain compliance and address the hidden cost of not knowing:

- Are we equipped to protect our production assets and critical OT environments?
- Can we detect and respond to cyber threats targeting our production lines?
- How quickly can we restore production to minimum viability after an incident?

1 https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index
2 https://www.precedenceresearch.com/industrial-cybersecurity-market?

Minimize production downtime. Maximize operational efficiency.

Commvault and Microsoft help manufacturers maintain:

- **Resilient operations:** Quickly recover production lines and optimize Overall Equipment Effectiveness (OEE).
- **Secured innovation:** Protect intellectual property critical to R&D, production processes, and proprietary manufacturing techniques.
- **Regulatory confidence:** Navigate complex, industry-specific compliance standards and regulations.
- **Adaptive security:** Continually protect both legacy OT infrastructure and emerging IoT technologies to reduce risk without disrupting existing operations.

Enable enterprise-scale resilience with Commvault and Microsoft's unified, secure end-to-end ecosystem designed to connect people, assets, workflows, and business processes with:

Air Gap Protect: Safeguard critical production data and keep Programmable Logic Controller (PLC) configurations safe from ransomware through isolated, immutable backups.

Cleanroom Recovery: Safely test and recover in a controlled, secure environment before returning restored systems to production without risking live operations.

Identity Resilience: Recover Active Directory & identity services to reduce risk across human and non-human access in IT, OT, and data platforms using secure, isolated recovery.

Cyber threats require a unified response

Manufacturers moving to the cloud are challenged to securely manage diverse data, from production analytics to supply chain management. Commvault and Microsoft help provide the comprehensive security, compliance, and accessibility manufacturers need to securely modernize, maintain operational continuity, and enhance resilience.

Schedule your demo

Buy on Marketplace

Better together: Commvault + Microsoft

Commvault and Microsoft have partnered for 29+ years to deliver trusted, enterprise-grade data environments with cyber resilience solutions. Our solutions, built on Azure, enable cloud resilience with NIST standards and zero-trust principles. Commvault and Microsoft provide cyber resilience and rapid recovery for continuous business.

Why Commvault

14th consecutive year: 2025 Gartner Magic Quadrant Leader for Backup and Data Protection Platforms

Highest product scores in five of six use cases: Gartner's 2025 Critical Capabilities for Backup and Data Protection Platforms

Learn more at:
microsoft.com/commvault

Contact us:
microsoft@commvault.com