Wie MSPs ihre Services für Fertigungsunternehmen sichern und ausbauen können

Einleitung: Fertigungsunternehmen im Visier von Kriminellen

Fertigungsunternehmen stehen im Fadenkreuz von Cyberkriminellen – und viele Unternehmen sind nicht ausreichend auf ihre eigene Verteidigung vorbereitet. Während dies für die Fertigungsbranche ein erhebliches Problem darstellt, bietet es für Managed Service Provider (MSPs) eine große Chance.

Alle Personen, die für eine OT-Umgebung (Operational Technology) verantwortlich sind, wissen, wie teuer Ausfallzeiten sein können. IBM berichtete zudem, dass eine durchschnittliche Datenschutzverletzung im Industriesektor im Jahr 2025 Kosten in Höhe von 5,6 Millionen US-Dollar[2] verursachte. Damit liegt die Fertigungsbranche bei den Gesamtkosten eines Vorfalls direkt hinter dem Gesundheitswesen und den Finanzdienstleistungen.

> Laut IBM ist die Fertigungsindustrie die Branche, die am häufigsten von Cyberkriminellen angegriffen wird – und das bereits seit fünf Jahren[1]. Mehr als ein Viertel aller Cyberangriffe zielen auf Hersteller ab, wie IBM herausfand.

Die Operational-Technology-Chance für MSPs

Unternehmen mit OT-Umgebungen unterscheiden sich von anderen Betrieben. Vielen von ihnen – insbesondere im KMU-Segment – fehlt die interne Expertise, die für das Management konvergierender IT- und OT-Umgebungen erforderlich ist. In Air-Gapped-Umgebungen, in denen eine Fabrik vollständig getrennt vom restlichen Unternehmen betrieben wird, gibt es unter Umständen überhaupt kein eigenes IT-Personal.

Genau hier bietet sich für MSPs eine enorme Geschäftschance. Hersteller benötigen die Unterstützung von MSPs, um ihre Betriebskontinuität zu gewährleisten, geschäftskritische Systeme zu schützen und die Compliance einzuhalten. Für Service Provider erfordert der Erfolg in der Fertigungsbranche jedoch mehr als nur die Beherrschung herkömmlicher IT-Services.

Um in der Fertigungsbranche erfolgreich zu sein, müssen sich MSPs von standardmäßigen IT-Betreibern zu vertrauenswürdigen Partnern weiterentwickeln. Mit diesen können Sie produktionskritische Systeme unterstützen, bei denen Ausfallzeiten direkte Auswirkungen auf den Umsatz, die Sicherheit und Lieferkettenverpflichtungen haben.

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

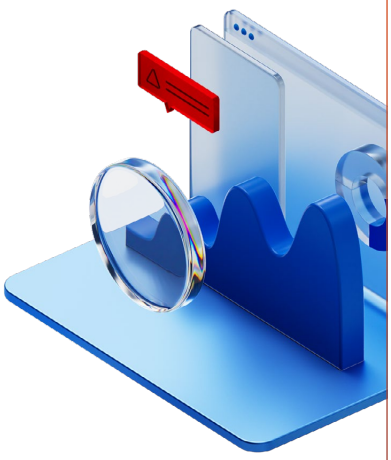
[2] IBM. (2025). „Cost of a Data Breach"-Bericht, 2025

Copyright © 2003–2026 Acronis International GmbH.

Zentrale Risiken in Fertigungsumgebungen

Das Erste, was MSPs über den Schutz von OT-Betrieben wissen müssen, ist, dass Fertigungskund:innen mit einer einzigartigen Kombination aus geschäftlichen und Cyberrisiken konfrontiert sind:

- **Betriebliche Ausfallzeiten:** Selbst kurze Ausfälle können ganze Produktionslinien stoppen und zu erheblichen finanziellen Verlusten führen.
- **Ransomware-Angriffe:** Die Fertigungsbranche ist aufgrund der hohen Kosten von Betriebsunterbrechungen und des Werts von gestohlenen Daten zu einem Hauptangriffsziel geworden.
- **Unterbrechung der Lieferkette:** Cybervorfälle können sich kaskadenartig auf Zulieferer und Partner auswirken, wie der massive Cyberangriff auf Jaguar Land Rover im Jahr 2025 eindrucksvoll gezeigt hat.
- **Risiken durch langlebige Systeme:** Industriesysteme, die für eine jahrzehntelange Nutzung ausgelegt sind, können leider die Anfälligkeit für Angriffe erhöhen und die Möglichkeiten zum Einspielen von Patches einschränken.



Risiken durch die Konvergenz von IT und OT: Die Angriffsflächen vergrößern sich, da die Systeme zunehmend miteinander vernetzt werden.

Genau bei der Minimierung dieser Risiken können Sie als MSPs neue Umsatzströme generieren – vorausgesetzt, Sie wissen wie und nutzen die richtige Plattform. MSPs, die Unternehmen mit OT-Umgebungen betreuen, stehen unter enormem Druck. Sie müssen nicht nur Schutz bieten, sondern auch schnelle Datenwiederherstellungen und eine garantierte Betriebskontinuität gewährleisten. Zudem müssen Sie die entsprechenden Services implementieren, ohne die Produktion zu beeinträchtigen. Denn für Fertigungsunternehmen sind Ausfallzeiten schlichtweg keine Option.

Geschäftliche und technologische Herausforderungen

Einige zentrale Faktoren machen das Management einer OT-Umgebung für MSPs zu einer ganz besonderen Herausforderung.

Das Management komplexer Hybrid-Umgebungen
Fertigungsumgebungen kombinieren moderne IT-Systeme mit langlebiger Operational Technology (OT) wie SCADA-Systemen, SPS (Speicherprogrammierbaren Steuerungen) und HMIs (Mensch-Maschine-Schnittstellen). Diese Systeme lassen sich oft nur schwer aktualisieren – was ein hartnäckiges Problem ist, das Sicherheitslücken öffnen kann.

Eingeschränkte Transparenz über IT und OT hinweg
MSPs müssen sowohl Unternehmensnetzwerke als auch Produktionsumgebungen überwachen und absichern. Die Transparenz über beide Bereiche hinweg ist jedoch oft fragmentiert. Dies erschwert die Erkennung von und die Reaktion auf Bedrohungen.

Zunehmender Druck durch Ransomware-Angriffe
Cyberkriminelle nehmen gezielt Hersteller ins Visier, da diese nur eine sehr geringe Toleranz für Ausfallzeiten haben. Als MSPs müssen Sie daher sowohl Präventionsmaßnahmen als auch schnelle Wiederherstellungsfähigkeiten gewährleisten.

Fragmentierte Tools und betriebliche Komplexität
Viele MSPs verlassen sich auf mehrere Einzellösungen für Backup-, Cyber Security- und Monitoring-Aufgaben. Diese Tool-Anhäufung erhöht die Kosten, verlangsamt die Reaktionszeiten und führt bei Vorfällen zu Integrationsproblemen.

Branchenbezogene und betriebliche Herausforderungen

Zudem gibt es in der Fertigungsbranche Herausforderungen und Vorgaben, mit denen MSPs konfrontiert sind und die ihnen in anderen Umgebungen – zumindest nicht in diesem Ausmaß – nicht begegnen würden.

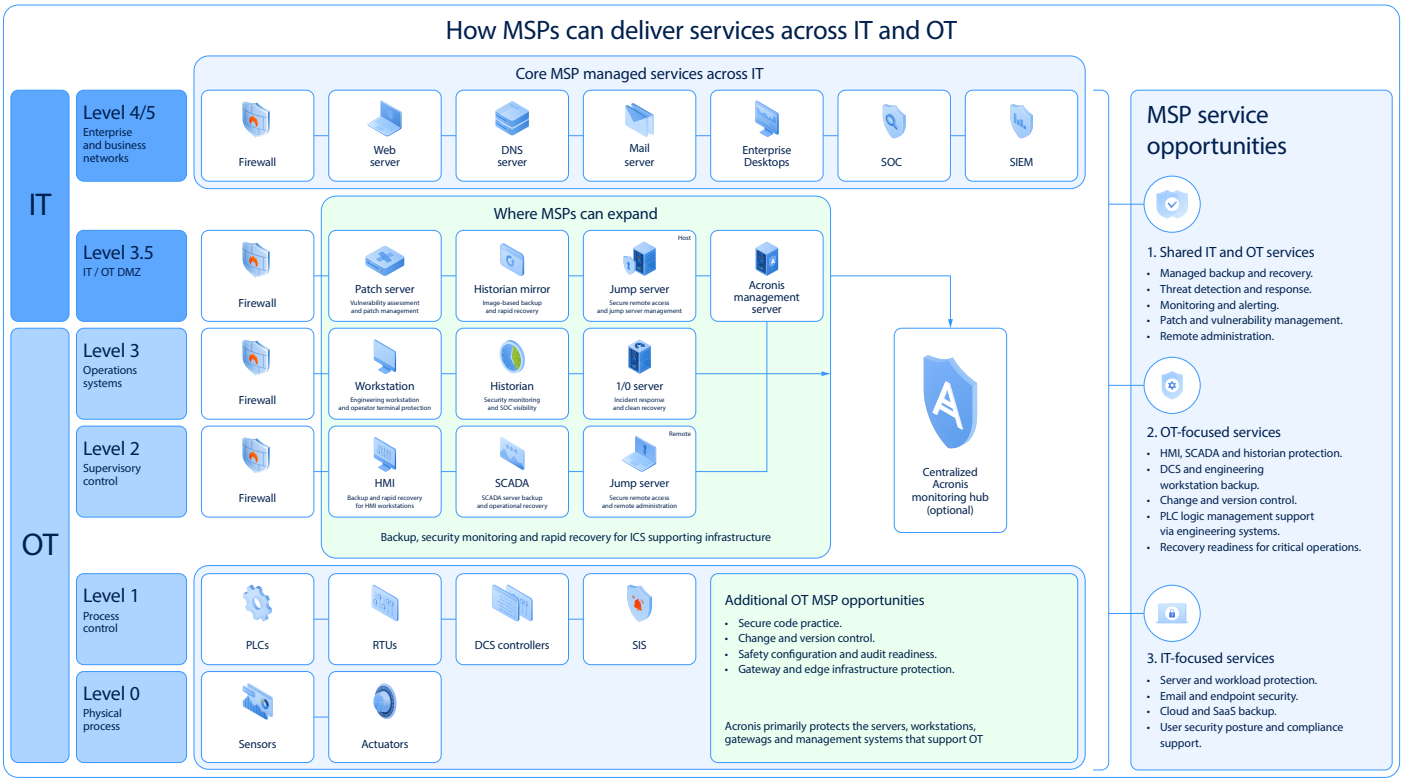
Strenge Anforderungen an die Betriebskontinuität
Fertigungsbetriebe können keine Unterbrechungen tolerieren. Als MSPs müssen Sie in der Lage sein, ambitionierte Wiederherstellungszeitvorgaben (RTOs) und Service-Level-Agreements (SLAs) einzuhalten.

Altsysteme und OEM-Einschränkungen
Industrieanlagen sind für eine jahre- oder sogar jahrzehntelange Nutzung ausgelegt. Infolgedessen laufen sie häufig mit nicht mehr offiziell unterstützten Betriebssystemen oder können aufgrund von Garantiebeschränkungen keine Agenten von Drittanbietern installiert werden.

Compliance- und Regulierungsdruck
Hersteller müssen Richtlinien (wie die NIST-, CMMC- und IEC-Standards) einhalten, die überprüfbare Kontrollen und Cyber-Resilienz-Fähigkeiten erfordern.

IT-Konvergenz mit OT
MSPs steigen in der Regel über IT-Services in die Fertigungsbranche ein und erweitern ihr Angebot schrittweise auf OT-Umgebungen. Die Unterstützung von Engineering-Workstations, Daten-Historians und HMI-Systemen wird dabei zu einem entscheidenden Schritt, um den vollen Mehrwert zu erbringen. Wenn Sie als Service Provider im Fertigungssektor erfolgreich sein wollen, müssen Sie also über spezifische OT-Fähigkeiten verfügen.

Copyright © 2003–2026 Acronis International GmbH.



Die Lösung: Acronis Cyber Platform

Mit Acronis können Sie die Konvergenz von IT- und OT-Schutz realisieren: Die einheitlich integrierte Plattform ermöglicht es MSPs, beide Arten von Umgebungen über eine einzige zentrale Konsole abzusichern und gleichzeitig die Betriebskontinuität zu gewährleisten. Mit der Acronis Cyber Platform können MSPs Folgendes erreichen:

Gewährleisten Sie mit Acronis One-Click Recovery einen kontinuierlichen Produktionsbetrieb

Sorgen Sie mit den integrierten Backup-, Cyber Security- und Near-Instant-Recovery-Fähigkeiten für minimale Ausfallzeiten. Techniker:innen können geschäftskritische Systeme bei einem Vorfall mit nur einem Klick innerhalb weniger Minuten wiederherstellen, damit die Produktion weiterläuft.

Sichern Sie Fabriken mit gemischten Technologie-Generationen ab

Eliminieren Sie Tool-Anhäufung: Schützen Sie moderne Cloud-Workloads sowie industrielle Altsysteme über eine einzige, nativ integrierte Plattform – und das ganz ohne Beeinträchtigung des laufenden Betriebs.

Vereinfachen Sie Abläufe und sorgen Sie für mehr Effizienz

Ersetzen Sie mehrere Einzeltools durch eine einheitlich integrierte Plattform für Backup-, Cyber Security-, Patching- und Monitoring-Aufgaben. So können Sie die Komplexität reduzieren und gleichzeitig die Service-Bereitstellung verbessern.

Sorgen Sie für Compliance und stärken Sie das Vertrauen in die Lieferkette

Unterstützen Sie geltende regulatorische Anforderungen durch zentrale Berichtserstellungen, Schwachstellen-Transparenz und Audit-konforme Dokumentationen.

Ermöglichen Sie risikofreie Validierungen durch digitale Zwillinge

Testen Sie Patches und Updates in virtuellen Umgebungen vor deren Bereitstellung, um Produktionsunterbrechungen schon vorab zu vermeiden.

Umgehen Sie OEM-Einschränkungen durch agentenlose Schutzfähigkeiten

Sichern Sie geschäftskritische Assets ab, ohne Software auf empfindlichen Anlagen installieren zu müssen. So können Sie Vorgaben zur Herstellergarantie wahren und Ausfallzeiten bei der Implementierung minimieren.

Copyright © 2003–2026 Acronis International GmbH.

Acronis Cyber Platform für MSPs

Die Acronis Cyber Platform ist eine nativ integrierte, vereinheitlichte Plattform, die Cyber Security-, Data Protection-, Infrastruktur-Management-, Service-Automatisierungs- und Cloud-Infrastruktur-Fähigkeiten über eine einzige, zentrale Konsole bereitstellt. Damit können Sie als MSPs eine Tool-Anhäufung eliminieren und die Produktivität Ihrer Techniker:innen steigern.

Die Acronis Cyber Platform bietet:

Backup und Disaster Recovery

- Eine One-Click-Recovery-Funktion: Mit dieser können Mitarbeiter:innen Systeme schnell wieder betriebsbereit machen.
- Unveränderliche Backups, um gesicherte Daten effektiv vor Ransomware-Angriffen zu schützen.
- Die Universal-Restore-Technologie für hardwareunabhängige Wiederherstellungen.

Advanced Security- und XDR-Fähigkeiten als Add-on-Pakete

- KI-basierter Ransomware-Schutz.
- Integrierte Erkennungs und Abwehrfähigkeiten – übergreifend über alle Endpunkte, E-Mails und Workloads hinweg.

Erweiterte Verwaltungs- und Patching-Fähigkeiten

- Automatisiertes Patching mit ausfallsicherem Rollback.
- Schwachstellen-bewertung über IT- und OT-unterstützende Systeme hinweg:

Email Security-Funktionalität und Security Awareness Training

- KI-gestützter Phishing-Schutz.
- Branchenspezifische Trainings für Benutzer:innen in der Fertigungsindustrie.

Zudem bietet die Acronis Cyber Platform einen umfassenden Schutz für kritische Infrastrukturen, die SCADA-, DCS- und HMI-Systeme unterstützen. Durch das Zusammenspiel dieser Funktionen können MSPs eine lückenlose Cyber-Resilienz-Ebene bereitstellen, die bestehende Netzwerk- und OT-Monitoring-Tools optimal ergänzt.

Acronis Cyber Platform für MSPs

Der Acronis Vorteil für MSPs in der Fertigungsbranche

Im Gegensatz zu Einzellösungen, die meist nur Backup- oder Cyber Security-Funktionen abdecken, bietet Acronis eine einheitlich integrierte Cyber Protection-Plattform, die speziell für komplexe Umgebungen entwickelt wurde.

Mit diesem Ansatz können MSPs folgende Vorteile realisieren:

- Ihre betriebliche Kosten senken und Tool-Anhäufung eliminieren.
- Die Reaktionszeiten bei Vorfällen verbessern.
- Den Fokus auf die Betriebskontinuität und Cyber-Resilienz legen.
- Sicher und souverän von IT- auf OT-Umgebungen expandieren.

Fazit: Die Konsolidierung von Schutzfähigkeiten unter einer einheitlich integrierten Plattform sorgt dafür, dass Integrationsprobleme und operative Risiken verringert werden können – und gleichzeitig die Gesamteffizienz gesteigert werden kann.

Sichern Sie sich Ihren Einstieg in die Fertigungsbranche

Hersteller benötigen die Unterstützung von MSPs. Sie wollen gemeinsam mit vertrauenswürdigen Partnern in ihre Betriebskontinuität und Cyber-Resilienz investieren. Dank Acronis können MSPs diese enorme Geschäftschance jetzt optimal nutzen.

Bauen Sie Ihr Geschäft in der Fertigungsbranche noch heute aus:

- Vereinbaren Sie eine Demo der Acronis Cyber Platform.
- Starten Sie jetzt Ihre Testversion der Acronis Cyber Platform.

Acronis

Erfahren Sie mehr auf acronis.com

Copyright © 2003–2026 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH in den Vereinigten Staaten und/oder in anderen Ländern. Alle anderen Marken oder eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber. Technische Änderungen, Abweichungen bei den Abbildungen sowie Irrtümer sind vorbehalten. Juni 2026