MSP : comment sécuriser et faire évoluer leurs services pour les clients du secteur manufacturier

Introduction : les industriels dans le viseur

Le secteur de la fabrication est dans la ligne de mire des cyberattaquants, et de nombreuses entreprises ne sont pas prêtes à se défendre. Bien qu'il s'agisse d'un problème majeur pour les fabricants, il représente une opportunité pour les fournisseurs de services gérés (MSP).

Toute personne responsable d'un environnement de technologie opérationnelle (OT) sait à quel point les interruptions d'activité peuvent être coûteuses. IBM a également indiqué qu'en 2025, le coût moyen d'une violation de données dans le secteur industriel s'élevait à 5,6 millions de dollars[2], plaçant l'industrie manufacturière juste derrière les secteurs de la santé et des services financiers en termes de coût total d'une violation.

> Selon IBM, l'industrie manufacturière est le secteur le plus fréquemment visé par les cyberattaquants, et ce depuis cinq ans[1]. IBM a constaté que plus d'un quart, voire la totalité, des cyberattaques visent les fabricants.

L'opportunité de la technologie opérationnelle pour les MSP

Les organisations dotées d'environnements OT ne sont pas comme les autres entreprises. Beaucoup d'entre elles, en particulier les PME, n'ont pas l'expertise interne nécessaire pour gérer la convergence des environnements informatiques et OT. Dans les environnements isolés, où une usine fonctionne indépendamment du reste de l'organisation, il peut n'y avoir aucun personnel informatique.

C'est là que les MSP peuvent saisir une opportunité considérable. Les fabricants ont besoin de l'aide des MSP pour garantir la disponibilité, protéger les systèmes critiques et assurer la conformité. Cependant, pour les fournisseurs de services, réussir dans le secteur manufacturier exige bien plus que la maîtrise des services informatiques traditionnels.

Pour réussir dans le secteur manufacturier, les MSP doivent passer du statut d'opérateurs informatiques standard à celui de partenaires de confiance, capables de prendre en charge les systèmes critiques pour la production, où les interruptions d'activité ont un impact direct sur le chiffre d'affaires, la sécurité et les engagements de la chaîne d'approvisionnement.

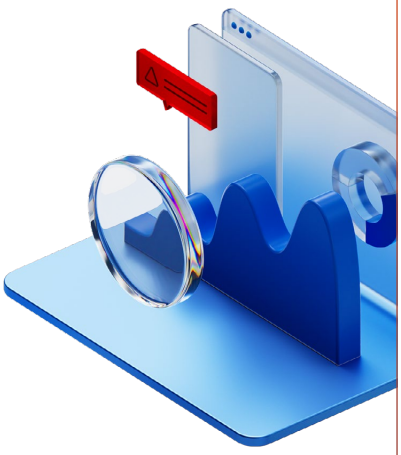
[1] IBM. (2026). Index de cyberveille X-Force 2026

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

Principaux risques dans les environnements de production

La première chose que les MSP doivent savoir sur la protection des opérations OT, c'est que les clients du secteur manufacturier sont confrontés à une combinaison unique de risques commerciaux et de cyberrisques :

- **Interruption d'activité opérationnelle :** même de brèves pannes peuvent interrompre les chaînes de production et entraîner des pertes financières importantes.
- **Attaques par ransomware :** le secteur de la fabrication est une cible de premier plan en raison du coût élevé des perturbations et de la valeur des données volées.
- **Perturbation de la chaîne d'approvisionnement :** les cyberincidents peuvent se répercuter en cascade sur les fournisseurs et les partenaires, comme l'a démontré la cyberattaque massive de 2025 contre Jaguar-Land Rover.
- **Exposition des systèmes à longue durée de vie :** les systèmes industriels conçus pour durer peuvent malheureusement accroître la vulnérabilité aux attaques et limiter les possibilités de correctifs.



Risques liés à la convergence de l'informatique et de l'OT : les surfaces d'attaque s'élargissent à mesure que les systèmes sont interconnectés.

Ce sont ces risques que les MSP peuvent atténuer pour générer des revenus, à condition de savoir comment faire et de disposer de la bonne plateforme. Les MSP qui travaillent pour des entreprises disposant d'environnements OT subissent une pression considérable pour assurer non seulement la protection, mais aussi une récupération rapide des données et une continuité opérationnelle garantie. Et ils doivent mettre en œuvre leurs services sans perturber la production. Dans le secteur de la fabrication, les Interruptions d'activité ne sont tout simplement pas envisageables.

Défis métier et technologiques

Quelques éléments clés rendent la gestion d'un environnement OT particulièrement difficile pour les MSP.

Gérer des environnements hybrides complexes
Les environnements de production combinent des systèmes informatiques modernes avec des technologies opérationnelles à longue durée de vie telles que SCADA, les API et les IHM. Ces systèmes peuvent être difficiles à mettre à jour, un problème récurrent susceptible de créer des failles de sécurité.

Visibilité limitée entre l'informatique et la technologie opérationnelle
Les MSP doivent surveiller et sécuriser à la fois les réseaux d'entreprise et les environnements de production, mais la visibilité sur ces deux domaines est souvent fragmentée. Cela complique la détection des menaces et la réponse à y apporter.

Pression croissante des rançongiciels
Les cybercriminels ciblent spécifiquement les fabricants en raison de leur faible tolérance aux Interruptions d'activité. Les MSP doivent garantir à la fois des capacités de prévention et de récupération rapide.

Outils fragmentés et complexité opérationnelle
De nombreux MSP s'appuient sur des solutions ponctuelles multiples pour la sauvegarde, la sécurité et la surveillance La multiplication des outils augmente les coûts, ralentit les temps de réponse et pose des problèmes d'intégration lors des incidents.

Défis sectoriels et opérationnels

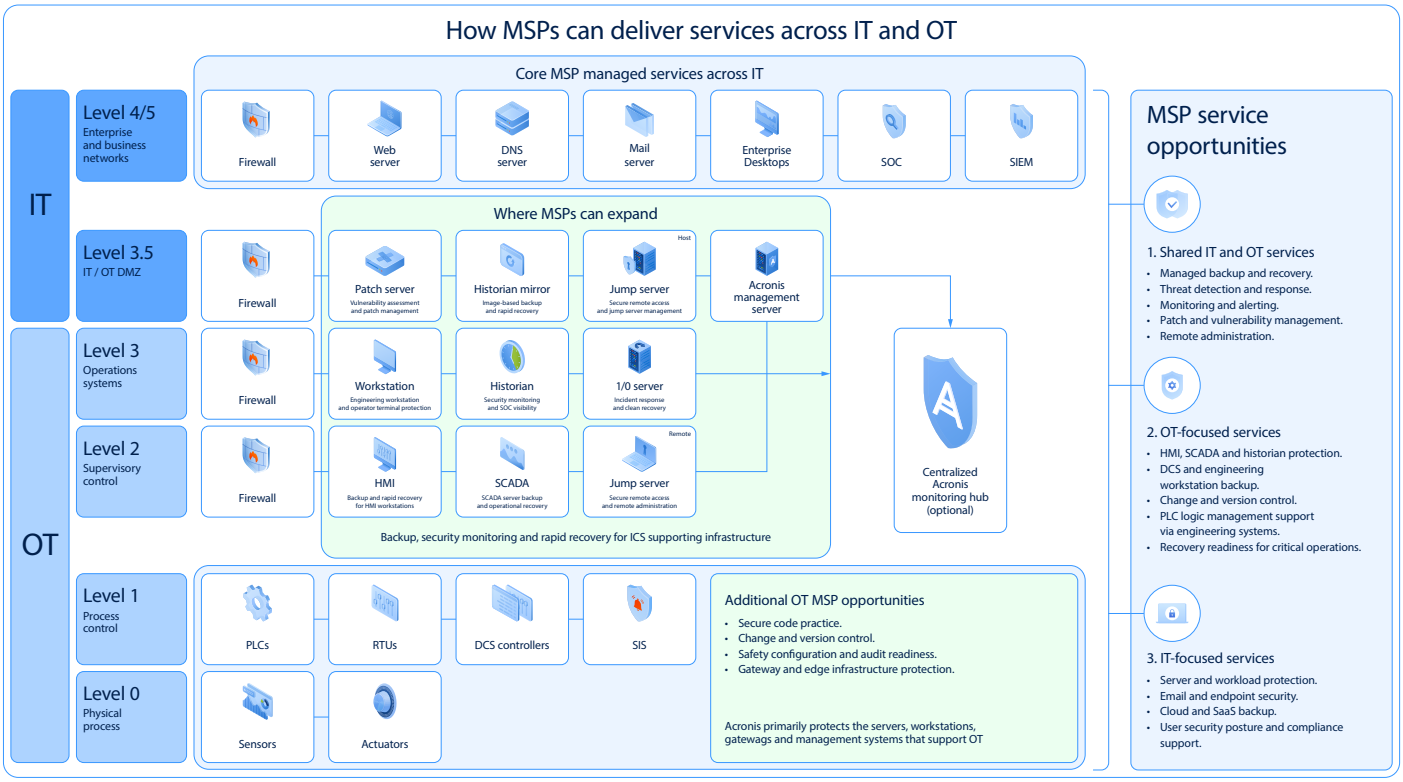
Les MSP sont également confrontés, dans le secteur de la fabrication, à des défis et à des exigences qu'ils ne rencontrent peut-être pas dans d'autres environnements, du moins pas dans la même mesure.

Exigences strictes en matière de disponibilité
Les opérations de fabrication ne peuvent tolérer aucune perturbation. Les MSP doivent être en mesure de respecter des objectifs de temps de récupération et des accords de niveau de service très stricts.

Systèmes existants et contraintes des OEM
Les équipements industriels sont conçus pour fonctionner pendant des années, voire des décennies. Par conséquent, ils fonctionnent souvent sur des systèmes d'exploitation non pris en charge ou ne peuvent pas intégrer d'agents tiers en raison de restrictions liées à la garantie.

Conformité et pression réglementaire
Les fabricants doivent se conformer à des cadres tels que les normes NIST, CMMC et IEC, qui exigent des contrôles vérifiables et des capacités de résilience.

Convergence de l'informatique avec l'OT
Les MSP pénètrent généralement le secteur manufacturier par le biais de services informatiques et s'étendent progressivement aux environnements OT. La prise en charge des postes de travail d'ingénierie, des historiques de données et des systèmes IHM devient une étape cruciale pour offrir une valeur ajoutée complète. Les fournisseurs de services doivent disposer de capacités OT spécifiques pour réussir dans le secteur de la fabrication.



Solution : Acronis Cyber Platform

Acronis permet la convergence de la protection informatique et de la protection OT en offrant une plateforme unifiée qui permet aux MSP de sécuriser les deux types d'environnements via un point de contrôle unique, tout en assurant la continuité des activités. Avec Acronis Cyber Platform, les MSP peuvent :

Garantir la continuité de la production avec Acronis One-Click Recovery
Minimiser les Interruption d'activité grâce à des fonctionnalités intégrées de sauvegarde, de cybersécurité et de restauration quasi instantanée. Les techniciens peuvent restaurer les systèmes critiques en quelques minutes, d'un simple clic, afin de maintenir la production en fonctionnement.

Sécuriser l'usine multi-générationnelle
Éliminez la prolifération des outils et protégez les ressources cloud modernes ainsi que les systèmes industriels existants depuis une plateforme unique, intégrée nativement, sans perturber les opérations.

Simplifier les opérations et gagner en efficacité
Remplacez les outils multiples par une plateforme intégrée unique pour la sauvegarde, la sécurité, les correctifs et la surveillance, afin de réduire la complexité et d'améliorer la prestation de services.

Assurer la conformité et la confiance dans la chaîne d'approvisionnement
Répondez aux exigences réglementaires grâce à des rapports centralisés, à une visibilité des vulnérabilités et à une documentation prête pour les audits.

Permettre une validation sans risque grâce aux jumeaux numériques
Testez les correctifs et les mises à jour dans des environnements virtuels avant leur déploiement pour éviter toute perturbation de la production.

Contourner les contraintes des constructeurs grâce à une protection sans agent
Sécurisez les actifs critiques sans installer de logiciel sur les systèmes sensibles, tout en préservant les garanties du fabricant et en minimisant les Interruption d'activité lors des implémentations.

Acronis Cyber Platform pour les fournisseurs de services managés

Acronis Cyber Platform est une plateforme unifiée et intégrée en natif qui offre la cybersécurité, la protection des données, la gestion de l'infrastructure, l'automatisation des services et l'infrastructure cloud, le tout à partir d'un point de contrôle unique. Elle permet aux MSP de réduire la prolifération des outils et d'améliorer la productivité des techniciens.

Acronis Cyber Platform offre :

La sauvegarde et reprise d'activité après sinistre

- La restauration en un clic, qui permet aux MSP de remettre rapidement les systèmes en service.
- Des sauvegardes immuables pour se protéger contre les ransomwares.
- Universal Restore pour une restauration indépendante du matériel.

Sécurité avancée et XDR

- Protection contre les ransomwares reposant sur l'intelligence artificielle.
- Détection et réponse intégrées sur l'ensemble des terminaux, des e-mails et des workloads.

Gestion et correctifs avancés

- Application automatisée des correctifs avec restauration à toute épreuve.
- Évaluation des vulnérabilités sur l'ensemble des systèmes informatiques et opérationnels.

Formation sur la sécurité des e-mails et la sensibilisation

- Protection contre le phishing basée sur l'intelligence artificielle.
- Formation spécifique au secteur pour les utilisateurs de l'industrie manufacturière.

De plus, Acronis Cyber Platform protège les infrastructures critiques qui prennent en charge les systèmes SCADA, DCS et HMI. Ensemble, ces fonctionnalités permettent aux MSP d'offrir une couche de résilience complète qui vient compléter les outils de surveillance réseau et OT existants.

Acronis Cyber Platform pour les fournisseurs de services managés

L'avantage Acronis pour les MSP du secteur manufacturier

Contrairement aux solutions ponctuelles qui se concentrent uniquement sur la sauvegarde ou la sécurité, Acronis propose une plateforme de cyberprotection unifiée, conçue pour les environnements complexes.

Cette approche permet aux MSP de :

- Réduire les frais opérationnels et éliminer la prolifération des outils.
- Améliorer les temps de réponse en cas d'incident.
- Se concentrer sur la disponibilité et la résilience
- Passer en toute confiance des environnements informatiques aux environnements opérationnels.

En résumé : regrouper les capacités de protection sur une plateforme unique réduit les difficultés d'intégration et le risque opérationnel, tout en améliorant l'efficacité globale

Faire le pas vers le secteur de la fabrication

Les fabricants ont besoin de l'aide des MSP. Ils souhaitent investir dans la disponibilité, la résilience et la continuité des activités avec des partenaires de confiance. Acronis permet aux MSP de saisir cette opportunité.

Commencez dès aujourd'hui à développer votre activité dans le secteur de la fabrication :

- Bénéficiez d'une démonstration d'Acronis Cyber Platform
- Faites un essai d'Acronis Cyber Platform.

Acronis

en savoir plus sur acronis.com