Como os MSPs podem proteger e dimensionar os serviços para clientes do setor de fabricação

Introdução: os fabricantes são alvos

A fabricação está na mira dos ciberatacantes, e muitas organizações não estão preparadas para se defender. Embora seja um problema significativo para os fabricantes, ele representa uma oportunidade para os provedores de serviços gerenciados (MSPs).

Qualquer pessoa responsável por um ambiente de tecnologia operacional (OT) sabe o quanto o tempo de inatividade pode ser caro. A IBM também relatou que a média de uma violação de dados no setor industrial em 2025 custou US$ 5,6 milhões[2], colocando a fabricação atrás apenas da saúde e dos serviços financeiros no custo total de uma violação.

A oportunidade de tecnologia operacional para MSPs

As organizações com ambientes de OT não são como outras operações. Muitas, especialmente no segmento de pequenas e médias empresas, não têm a expertise interna necessária para gerenciar ambientes convergentes de TI e OT. Em ambientes isolados, onde uma fábrica opera separadamente do restante da organização, pode não haver equipes de TI.

De acordo com a IBM, a fabricação é o setor mais frequentemente visado por ciberatacantes — e tem sido assim nos últimos cinco anos[1]. A IBM descobriu que mais de um quarto de todos os ciberataques têm como alvo os fabricantes.

É aí que os MSPs podem aproveitar uma grande oportunidade. Os fabricantes precisam da ajuda dos MSPs para garantir a disponibilidade, proteger os sistemas críticos e manter a conformidade. No entanto, para os provedores de serviços, o sucesso na fabricação exige mais do que domínio dos serviços tradicionais de TI.

Para ter sucesso nesse setor, os MSPs precisam evoluir de operadores padrão de TI para parceiros confiáveis, capazes de dar suporte a sistemas críticos para a produção, nos quais o tempo de inatividade afeta diretamente a receita, a segurança e os compromissos da cadeia de suprimentos.

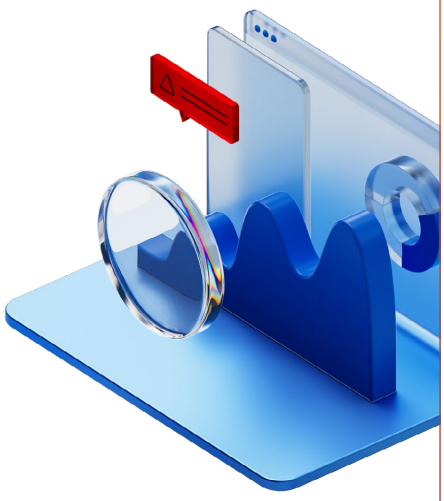
[1] IBM. (2026). Índice de Inteligência de Ameaças X-Force 2026

[2] IBM. (2025). Relatório sobre o custo de uma violação de dados de 2025

Principais riscos em ambientes de fabricação

A primeira coisa que os MSPs precisam saber sobre a proteção das operações de OT é que os clientes de fabricação enfrentam uma combinação única de riscos de negócios e cibernéticos:

- **Tempo de inatividade operacional:** mesmo interrupções curtas podem paralisar as linhas de produção e resultar em perdas financeiras significativas.
- **Ataques de ransomware:** a fabricação é um dos principais alvos devido ao alto custo da interrupção e ao valor dos dados roubados.
- **Interrupção da cadeia de suprimentos:** incidentes cibernéticos podem se propagar por fornecedores e parceiros, como demonstrou o enorme ciberataque de 2025 à Jaguar Land Rover.
- **Exposição de sistemas de longa vida útil:** sistemas industriais projetados para durar décadas podem, infelizmente, aumentar a vulnerabilidade a ataques e limitar as opções de patch.



Riscos da convergência de TI e OT: as superfícies de ataque se expandem à medida que os sistemas se tornam interconectados.

Esses são os riscos que os MSPs podem gerar receita ao mitigar — se souberem como e tiverem a plataforma certa em vigor. Os MSPs que atendem organizações com ambientes de OT enfrentam intensa pressão para oferecer não apenas proteção, mas também recuperação de dados rápida e continuidade operacional garantida. E eles precisam implementar seus serviços sem interromper a produção. Na fabricação, o tempo de inatividade simplesmente não é uma opção.

Desafios de negócios e tecnológicos

Alguns elementos importantes tornam o gerenciamento de um ambiente de OT um desafio único para os MSPs.

Gerenciando ambientes híbridos complexos
Ambientes de fabricação combinam sistemas modernos de TI com tecnologia operacional de longa vida útil, como SCADA, PLCs e HMIs. Esses sistemas podem ser difíceis de atualizar, um problema persistente que pode abrir lacunas de segurança.

Visibilidade limitada entre TI e OT
Os MSPs precisam monitorar e proteger tanto as redes corporativas quanto os ambientes de produção, mas a visibilidade em ambos os domínios costuma ser fragmentada. Assim, fica mais difícil detectar e responder a ameaças.

Aumento na pressão de ransomware
Cibercriminosos visam especificamente os fabricantes devido à sua baixa tolerância ao tempo de inatividade. Os MSPs precisam garantir recursos de prevenção e recuperação rápida.

Ferramentas fragmentadas e complexidade operacional
Muitos MSPs dependem de várias soluções para backup, segurança e monitoramento. A proliferação de ferramentas aumenta os custos, desacelera os tempos de resposta e cria desafios de integração durante incidentes.

Desafios do setor e operacionais

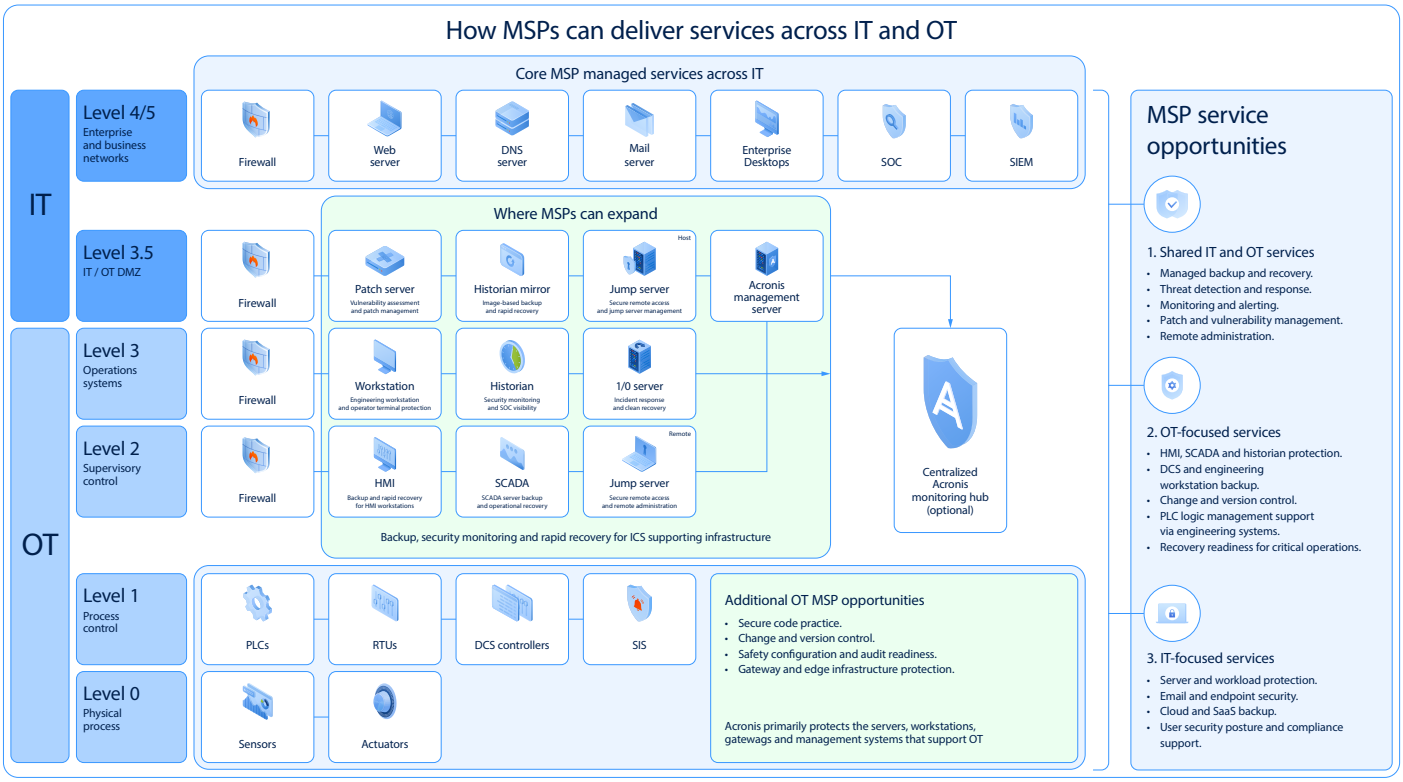
Também há desafios e exigências com os quais os MSPs lidam na fabricação que talvez não encontrem em outros ambientes, pelo menos não na mesma medida.

Requisitos rígidos de disponibilidade
As operações de fabricação não podem tolerar interrupções. Os MSPs precisam ser capazes de atender a objetivos de tempo de recuperação agressivos e acordos de nível de serviço.

Sistemas legados e restrições de OEM
Equipamentos industriais são projetados para funcionar por anos, até décadas. Como resultado, muitas vezes executam sistemas operacionais sem suporte ou não conseguem acomodar agentes de terceiros devido a restrições de garantia.

Conformidade e pressão regulatória
Os fabricantes precisam cumprir estruturas como NIST, CMMC e padrões IEC, que exigem controles auditáveis e recursos de resiliência.

Convergência de TI com OT
Normalmente, os MSPs entram no setor de fabricação por meio de serviços de TI e expandem gradualmente para ambientes de OT. Dar suporte a estações de trabalho de engenharia, data historians e sistemas HMI torna-se uma etapa crítica para entregar valor total. Os provedores de serviços precisam ter recursos específicos de OT se quiserem ter sucesso no setor de fabricação.



Solução: Acronis Cyber Platform

A Acronis permite a convergência de proteção de TI e OT ao fornecer uma plataforma unificada que possibilita aos MSPs proteger ambos os tipos de ambientes por meio de um único ponto de controle, garantindo ao mesmo tempo a continuidade dos negócios. Com a Acronis Cyber Platform, os MSPs podem:

Garantir a continuidade da produção com o Acronis One-Click Recovery
Minimize o tempo de inatividade com backup integrado, cibersegurança e recursos de recuperação quase instantânea. Os técnicos podem restaurar sistemas críticos em minutos com apenas um clique para manter a produção em funcionamento.

Proteger a fábrica multigeracional
Elimine a dispersão de ferramentas e proteja cargas de trabalho modernas na nuvem, junto com sistemas industriais legados, a partir de uma única plataforma nativamente integrada, sem interromper as operações.

Simplificar as operações e melhore a eficiência
Substitua várias ferramentas por uma única plataforma integrada para backup, segurança, patching e Monitoramento, reduzindo a complexidade e melhorando a entrega do serviço.

Permitir conformidade e confiança na cadeia de suprimentos
Atenda aos requisitos regulatórios com relatórios centralizados, visibilidade de vulnerabilidades e documentação pronta para auditoria.

Permitir validação sem risco com gêmeos digitais
Teste patches e atualizações em ambientes virtuais antes da implantação para evitar interrupções na produção.

Lidar com as restrições do OEM com proteção sem agente
Proteja ativos críticos sem instalar software em sistemas sensíveis, preservando as garantias do fabricante e minimizando o tempo de inatividade para implantações.

Acronis Cyber Platform para MSPs

A Acronis Cyber Platform é uma plataforma unificada, nativamente integrada, que oferece cibersegurança, proteção de dados, gerenciamento de infraestrutura, automação de serviços e infraestrutura de nuvem com um único ponto de controle. Ela permite que os MSPs eliminem a dispersão de ferramentas e melhorem a produtividade dos técnicos.

A Acronis Cyber Platform entrega:

Backup e recuperação de desastres

- Recuperação com um clique, que permite aos MSPs colocar os sistemas em funcionamento novamente rapidamente.
- Backups imutáveis para proteção contra ransomware.
- Restauração universal para recuperação independente de hardware.

Segurança avançada e XDR

- Proteção contra ransomware baseado em inteligência artificial.
- Detecção e resposta integrada em endpoints, e-mail e cargas de trabalho.

Gerenciamento e patching avançado

- Aplicação automatizada de patches com reversão à prova de falhas.
- Avaliação de vulnerabilidades em sistemas de suporte de TI e OT.

Segurança de e-mail e treinamento de conscientização

- Proteção contra phishing alimentada por inteligência artificial.
- Treinamento específico do setor para usuários de fabricação.

Além disso, a Acronis Cyber Platform oferece proteção para infraestrutura crítica de suporte a sistemas SCADA, DCS e HMI. Juntas, essas capacidades permitem que os MSPs ofereçam uma camada completa de resiliência que complementa as ferramentas existentes de Monitoramento de rede e OT.

Acronis Cyber Platform para MSPs

A vantagem da Acronis para MSPs de fabricação

Ao contrário de soluções pontuais que tratam apenas de backup ou segurança, a Acronis oferece uma plataforma unificada de proteção cibernética projetada para ambientes complexos.

Essa abordagem permite que os MSPs:

- Reduzir a sobrecarga operacional e a dispersão de ferramentas.
- Melhorem os tempos de resposta durante incidentes.
- Foque em disponibilidade e resiliência
- Expanda com confiança de ambientes de TI para ambientes de OT.

Em resumo: consolidar os recursos de proteção em uma única plataforma reduz os desafios de integração e o risco operacional, ao mesmo tempo que melhora a eficiência geral.

Faça a mudança para a fabricação

Os fabricantes precisam de ajuda dos MSPs. Eles estão buscando investir em disponibilidade, resiliência e continuidade dos negócios com parceiros confiáveis. A Acronis permite que os MSPs aproveitem essa oportunidade.

Comece a expandir sua empresa de fabricação hoje:

- Agende uma demonstração da Acronis Cyber Platform.
- Inicie uma avaliação da Acronis Cyber Platform.

Acronis

Saiba mais em
www.acronis.com