

Como os MSPs podem desenvolver práticas no setor de saúde de alto crescimento



Os riscos para a cibersegurança na área da saúde são extremamente altos. Falhas de sistema e tempo de inatividade podem ter efeitos catastróficos sobre os pacientes. Infelizmente, muitas organizações de saúde têm dificuldade para gerenciar a cibersegurança de forma eficaz. Os provedores de serviços gerenciados (MSPs) têm uma oportunidade significativa de agir e ajudar, ao mesmo tempo em que impulsionam a receita.

Os dados do relatório Black Book Market Research de 2025 ilustram a magnitude do desafio:

68%

dos provedores de saúde afirmam que não conseguem abordar adequadamente os riscos cibernéticos devido à insuficiência de recursos financeiros.

60%

Quase 60% das organizações de saúde relatam desafios para contratar e reter profissionais de TI qualificados.

28%

das violações são atribuídas a erro humano, com ameaças internas à organização decorrentes principalmente de phishing.

Como resultado, a adoção de serviços gerenciados de segurança na área da saúde cresceu 35% de 2024 para 2025. A oportunidade para os MSPs é grande e continua crescendo.¹

A necessidade de ir além dos serviços gerenciados padrão

Os ambientes clínicos dependem de sistemas que funcionam ininterruptamente, como prontuários eletrônicos, plataformas de geração de imagem e ferramentas de monitoramento de pacientes. Uma falha em qualquer um desses sistemas afeta diretamente os pacientes. Os MSPs podem ir além do suporte de TI tradicional e se tornar parceiros essenciais para manter sistemas críticos funcionando e garantir a continuidade clínica, a segurança e a conformidade.

No entanto, ter sucesso na área da saúde exige mais do que serviços gerenciados padrão. Os MSPs precisam ser capazes de gerenciar requisitos regulatórios complexos, proteger sistemas médicos herdados e garantir tempo de inatividade quase zero em ambientes em que cada minuto é precioso.

¹ Black Book Market Research, [The Black Book of Healthcare Cybersecurity: 2025 Edition](#)

Desafios tecnológicos e de negócios

Ter sucesso no setor de saúde não é fácil. O atendimento a clientes de saúde gera uma série de desafios com os quais muitos provedores de serviços talvez não estejam familiarizados. Os MSPs enfrentam uma combinação única de pressão operacional, riscos de segurança e complexidade técnica.



O impacto do tempo de inatividade na segurança do paciente

As organizações de saúde não podem tolerar interrupções. Falhas de sistema podem atrasar tratamentos, desviar pacientes e interromper fluxos de trabalho críticos de atendimento. Além disso, a inatividade é cara. O custo médio de uma violação de dados para organizações de saúde é de US\$ 7,42 milhões, de acordo com a IBM.² Os MSPs devem fornecer objetivos de tempo de recuperação quase zero e alta disponibilidade de forma consistente.

Superfície de ataque ampliada por sistemas herdados

Os ambientes de saúde continuam dependendo de infraestrutura herdada e de dispositivos médicos conectados. Muitos desses sistemas não podem ser atualizados com patch sem interromper o atendimento, então os MSPs acabam sendo responsáveis por proteger tecnologias desatualizadas e vulneráveis.

O alto valor dos dados de saúde para cibercriminosos

As informações de saúde protegidas estão entre os dados mais valiosos na dark web e no submundo do crime. Como resultado, as organizações de saúde são alvos prioritários para ransomware e roubo de dados. Os MSPs devem fornecer proteção avançada e recuperação rápida.

Aumento das ameaças de ransomware

Os ataques de ransomware direcionados ao setor de saúde continuam crescendo. O FBI diz que os incidentes de ransomware relatados que visam organizações de saúde aumentaram 93% de 2024³ para 2025.⁴ Os invasores exploram a urgência das operações clínicas. Os MSPs devem implementar defesas em camadas que incluam prevenção, detecção e recuperação confiável.

Ambientes híbridos complexos

Os ambientes de TI de saúde abrangem sistemas locais, plataformas de nuvem e aplicativos clínicos especializados. Manter a interoperabilidade segura entre sistemas como registros eletrônicos de saúde (EHRs) e plataformas de geração de imagem adiciona complexidade técnica significativa.

Proliferação de ferramentas e ineficiência operacional

Muitos MSPs dependem de várias ferramentas desconectadas para backup, segurança e gerenciamento. Essa abordagem aumenta a sobrecarga operacional, cria lacunas de visibilidade e reduz a eficiência da resposta durante incidentes.

² IBM. (2025). Relatório de custo de uma violação de dados 2025: a lacuna na supervisão de IA. IBM & Instituto Ponemon.

³ Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2024). [Relatório de Crimes na Internet de 2024](#).

⁴ Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). [Relatório de Crimes na Internet de 2025](#).

Desafios do setor e operacionais

Além dos obstáculos técnicos, o trabalho com clientes na área da saúde envolve exigências regulatórias e operacionais rigorosas.



Conformidade regulatória e pressão de auditoria

Os MSPs devem atender a rigorosos requisitos de conformidade, muitas vezes assumindo responsabilidade legal. É crucial estar pronto para auditorias e manter a documentação, mas isso pode exigir muitos recursos.

Preocupações com integridade de dados e confiança

As organizações de saúde devem garantir a precisão e a integridade dos dados clínicos. A corrupção silenciosa de dados e registros inconsistentes podem levar a sérios riscos de diagnóstico que os MSPs devem mitigar.

Requisitos de desempenho de geração de imagem e dados

Os sistemas de geração de imagem médica produzem grandes conjuntos de dados que devem estar sempre disponíveis para acesso instantâneo. Os MSPs precisam projetar arquiteturas híbridas que equilibrem desempenho com armazenamento seguro.

Restrições de custo

As organizações de saúde frequentemente operam com orçamentos de TI limitados, apesar das crescentes demandas de segurança. Os MSPs devem oferecer altos níveis de proteção enquanto mantêm a eficiência de custos.

Uma plataforma desenvolvida para MSPs de saúde

Para ter sucesso na área de saúde, os MSPs precisam de uma plataforma que ofereça segurança, proteção de dados e eficiência operacional em uma única solução. A Acronis Cyber Platform permite que os MSPs protejam todo o ambiente clínico, ao mesmo tempo em que simplificam as operações e melhoram a lucratividade.

Com a Acronis Cyber Platform, os MSPs podem:

Garantir a continuidade clínica

- Garantir que os sistemas críticos permaneçam disponíveis com restauração instantânea e tempos de recuperação quase zero.
- Manter o acesso aos EHRs, sistemas de imagens e dispositivos de cabeceira, mesmo durante incidentes cibernéticos.

Proteger todo o ambiente de saúde

- Proteger plataformas modernas de nuvem e sistemas médicos herdados com um único agente integrado.

- Reduzir o risco em endpoints, cargas de trabalho e dispositivos da internet das coisas médicas (IoMT).

Simplificar a conformidade e a prontidão para auditorias

- Automatizar processos de conformidade com mapeamentos de proteção de dados e relatórios prontos para auditoria.
- Fazer a transição de serviços básicos de TI para ofertas de conformidade de alto valor.

Recuperar com confiança

- Permitir recuperação sem malware com recursos de recuperação segura.
- Verificar e limpar os dados de backup antes da restauração.

Reduzir a complexidade e melhorar as margens

- Eliminar a dispersão de ferramentas consolidando backup, segurança e gerenciamento em uma única plataforma.
- Melhorar a eficiência dos técnicos e aumentar a lucratividade do serviço.

Acronis Cyber Platform: capacidades desenvolvidas para o setor de saúde

A Acronis oferece um conjunto abrangente de capacidades desenvolvidas especificamente para ambientes de saúde:

Plataforma unificada de proteção cibernética:

a Acronis combina cibersegurança, backup, recuperação de desastres e gerenciamento de endpoints em uma única plataforma, reduzindo a complexidade operacional e melhorando a visibilidade.

Backup e recuperação avançados:

os MSPs podem proteger sistemas críticos com backup em imagem, armazenamento imutável e recuperação rápida para ambientes clínicos e de imagens.

Proteção de endpoint e EDR:

com detecção e resposta de endpoint (EDR), os provedores de serviços podem proteger estações de trabalho clínicas, servidores e endpoints remotos.

Conformidade automatizada e proteção de dados:

a Acronis Cyber Platform permite que os MSPs identifiquem e protejam dados de saúde confidenciais com ferramentas automatizadas de descoberta e relatórios centralizados para prontidão de auditoria.

Proteção do Microsoft 365: como muitas organizações de saúde usam a popular suíte de produtividade, os MSPs podem garantir a continuidade do Microsoft 365 e de outras ferramentas de colaboração e comunicação, incluindo email, armazenamento de arquivos e plataformas de coordenação de pacientes.

Suporte para sistemas herdados: os MSPs podem estender a proteção a sistemas operacionais mais antigos e a equipamentos médicos especializados sem exigir upgrades disruptivos.

Backup forense e integridade de dados: os provedores de serviços podem capturar dados forenses para investigação de incidentes e garantir a integridade dos registros com tecnologias de verificação baseadas em blockchain.

A vantagem da Acronis Cyber Platform

Ao contrário de soluções pontuais reunidas de forma improvisada, a Acronis oferece uma plataforma integrada nativamente com um único ponto de gerenciamento que permite aos MSPs:

- Oferecer proteção cibernética completa em ambientes de saúde.
- Reduzir a sobrecarga operacional e a dispersão de ferramentas.
- Melhorar os tempos de resposta e resultados de recuperação.
- Expandir para serviços de conformidade e segurança de alto valor.
- Aumentar as margens enquanto amplia as ofertas para a área de saúde.

Com capacidades essenciais consolidadas em uma única plataforma, os MSPs podem reduzir custos e simplificar as operações enquanto fornecem a resiliência que as organizações de saúde exigem.

Comece a expandir sua prática na área de saúde

As organizações de saúde precisam de parceiros de confiança para garantir continuidade, segurança e conformidade. A Acronis Cyber Platform permite que os MSPs aproveitem a oportunidade com confiança.

↘ [Agende uma demonstração para ver como a Acronis dá suporte aos MSPs que trabalham com clientes da área de saúde](#)

↘ [Inicie uma avaliação e comece hoje mesmo a oferecer serviços resilientes de MSP para a área de saúde](#)

