Come gli MSP possono costruire un'offerta di servizi per il settore sanitario, in forte crescita

La posta in gioco della cyber security in ambito sanitario è di importanza prioritaria. I guasti ai sistemi e i periodi di inattività possono avere conseguenze devastanti per i pazienti. Purtroppo, molte organizzazioni sanitarie faticano a gestire la cyber security in modo efficace. Per gli MSP (Managed Service Provider) si tratta di un'opportunità concreta di intervenire e offrire supporto, generando al contempo nuovi flussi di fatturato.

I dati della ricerca Black Book Market per il 2025 illustrano la dimensione della sfida:

68%
dei fornitori di servizi sanitari afferma di non poter affrontare in modo adeguato i rischi informatici a causa di fondi insufficienti.

60%
Quasi il 60% delle organizzazioni sanitarie segnala difficoltà nell'assumere e trattenere professionisti IT qualificati.

28%
percentuale di violazioni attribuita all'errore umano, con minacce interne all'organizzazione causate principalmente dal phishing.

Come conseguenza di questi dati, l'adozione di servizi di sicurezza gestiti in ambito sanitario è aumentata del 35% dal 2024 al 2025. Per gli MSP si tratta di un'opportunità ampia e in continua crescita.[1]

Erogare un'offerta diversa dai servizi gestiti standard

Gli ambienti clinici dipendono da sistemi che devono essere sempre operativi: cartelle cliniche elettroniche, piattaforme di imaging e strumenti di monitoraggio dei pazienti. Un guasto in uno qualsiasi di questi sistemi ha ripercussioni dirette sui pazienti. Gli MSP possono andare oltre il tradizionale supporto IT e diventare Partner indispensabili per mantenere attivi e funzionanti i sistemi critici, garantendo continuità clinica, sicurezza e conformità alle strutture sanitarie.

Tuttavia, operare con successo in questo ambito richiede un'offerta diversa dai servizi gestiti standard. Gli MSP devono essere in grado di gestire requisiti normativi complessi, mettere in sicurezza i sistemi medicali legacy ed evitare qualsiasi interruzione operativa in ambienti dove ogni minuto è prezioso.

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

Sfide aziendali e tecnologiche

Operare con successo in ambito sanitario non è facile. Fornire servizi ai clienti di questo settore implica una serie di sfide con cui molti service provider potrebbero non avere familiarità. Sugli MSP grava una combinazione unica di pressioni operative, rischi per la sicurezza e complessità tecniche.

L'impatto delle interruzioni operative sulla sicurezza dei pazienti

Le organizzazioni sanitarie non possono tollerare momenti di inattività. I guasti ai sistemi possono ritardare le prestazioni, dirottare i pazienti e compromettere i flussi di lavoro delle cure critiche. Inoltre, le interruzioni hanno costi elevati: secondo IBM, il costo medio di una violazione dei dati per le organizzazioni sanitarie è di 7,42 milioni di dollari.[2] Gli MSP devono garantire obiettivi di ripristino prossimi allo zero e l'alta disponibilità costante dei sistemi.

La superficie di attacco dei sistemi legacy è in espansione

Gli ambienti sanitari continuano a dipendere da infrastrutture legacy e dispositivi medicali connessi alle reti. Molti di questi sistemi non possono essere aggiornati senza interrompere le cure, lasciando agli MSP la responsabilità di proteggere tecnologie obsolete e vulnerabili.

L'elevato valore dei dati sanitari per i criminali informatici

Le informazioni sanitarie protette sono tra i dati di maggior valore nel dark web e nel mercato criminale. Le organizzazioni sanitarie sono perciò bersagli primari per gli attacchi ransomware e il furto di dati. Gli MSP devono essere in grado di fornire protezione avanzata e ripristino rapido.

Minacce ransomware in aumento

Gli attacchi ransomware che prendono di mira il settore sanitario sono in costante aumento. Secondo l'FBI, gli incidenti ransomware segnalati indirizzati alle organizzazioni sanitarie sono aumentati del 93% dal 2024[3] al 2025.[4] Gli attaccanti sfruttano l'urgenza delle operazioni cliniche. Gli MSP devono implementare difese a più livelli che includano prevenzione, rilevamento e ripristino affidabile.

Ambienti ibridi complessi

Gli ambienti IT sanitari si estendono ai sistemi in locale, alle piattaforme cloud e alle applicazioni cliniche specializzate. Dover garantire l'interoperabilità in sicurezza tra sistemi come le cartelle cliniche elettroniche e le piattaforme di imaging aggiunge una significativa complessità tecnica.

Proliferazione degli strumenti e inefficienza operativa

Molti MSP si affidano a più strumenti non integrati tra loro per backup, sicurezza e gestione. Questo approccio aumenta il lavoro di gestione, crea lacune nella visibilità e riduce l'efficienza della risposta durante gli incidenti.

[2] IBM. (2025). Cost of a data breach report 2025: The AI oversight gap. IBM & Ponemon Institute.

[3] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2024). 2024 Internet Crime Report.

[4] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). 2025 Internet Crime Report.

Sfide normative e operative

Oltre alle difficoltà tecniche, operare con i clienti nel settore sanitario implica il rispetto di rigidi requisiti normativi e operativi.

Conformità normativa e pressione degli audit

Gli MSP devono soddisfare requisiti di conformità rigorosi, assumendosi spesso responsabilità legali dirette. La preparazione agli audit e la gestione della documentazione sono aspetti critici che possono richiedere molte risorse.

Integrità dei dati e fiducia

Le organizzazioni sanitarie devono garantire l'accuratezza e l'integrità dei dati clinici. Il danneggiamento non rilevato dei dati e la disomogeneità dei registri possono comportare seri rischi diagnostici che gli MSP devono mitigare.

Requisiti di imaging e prestazioni dei dati

I sistemi di imaging medicale generano grandi volumi di dati che devono essere sempre disponibili per l'accesso immediato. Gli MSP devono progettare architetture ibride in grado di bilanciare le esigenze di prestazioni con quelle di archiviazione sicura.

Vincoli di budget

Spesso le organizzazioni sanitarie operano con budget IT limitati, nonostante le esigenze di sicurezza in continua crescita. Gli MSP devono garantire livelli elevati di protezione mantenendo al contempo la convenienza economica.

Una piattaforma pensata per gli MSP del settore sanitario

Per operare con successo nel settore sanitario, gli MSP hanno bisogno di una piattaforma che offra sicurezza, protezione dei dati ed efficienza operativa in un'unica soluzione. Acronis Cyber Platform consente agli MSP di proteggere l'intero ambiente clinico, semplificando al contempo le operazioni e migliorando la redditività.

Con Acronis Cyber Platform, gli MSP possono:

Garantire la continuità clinica

- Assicurare la disponibilità dei sistemi critici grazie al ripristino immediato con Instant Restore e a tempi di ripristino prossimi allo zero.
- Mantenere l'accesso alle cartelle cliniche elettroniche, ai sistemi di imaging e ai dispositivi medici a bordo letto anche durante gli incidenti informatici.

Garantire protezione all'intero ambiente sanitario

- Proteggere le moderne piattaforme cloud e i sistemi medici legacy con un unico agente integrato.
- Ridurre il rischio su endpoint, workload e dispositivi IoMT (Internet of Medical Things).

Semplificare la conformità e la preparazione agli audit

- Automatizzare i processi di conformità con mappe della protezione dati e report pronti per gli audit.
- Evolvere da un'offerta di servizi IT di base verso offerte ad alto valore che prevedono la conformità normativa.

Ripristinare in sicurezza

- Abilitare ripristini privi di malware con funzionalità di ripristino sicuro.
- Eseguire la scansione e la pulizia dei dati di backup prima del ripristino.

Ridurre la complessità e migliorare i margini

- Eliminare la proliferazione degli strumenti consolidando backup, sicurezza e gestione in un'unica piattaforma.
- Migliorare l'efficienza dei tecnici e aumentare la redditività dei servizi.

Acronis Cyber Platform: funzionalità progettate per il settore sanitario

Acronis offre una serie completa di funzionalità progettate specificamente per gli ambienti sanitari:

Piattaforma unificata di Cyber Protection: Acronis integra cyber security, backup, Disaster Recovery e gestione degli endpoint in un'unica piattaforma, riducendo la complessità operativa e migliorando la visibilità.

Backup e ripristino avanzati: gli MSP possono proteggere i sistemi critici con backup dell'immagine, storage immutabile e ripristino rapido per ambienti clinici e di imaging.

Protezione degli endpoint ed EDR: la funzionalità EDR consente ai service provider di proteggere workstation, server ed endpoint remoti degli ambienti clinici.

Conformità e protezione dei dati automatizzate: Acronis Cyber Platform consente agli MSP di identificare e proteggere i dati sanitari sensibili tramite strumenti di individuazione automatica e creazione di report centralizzati per la preparazione agli audit.

Protezione di Microsoft 365: poiché molte organizzazioni sanitarie utilizzano la suite di produttività Microsoft, gli MSP possono garantire la continuità di Microsoft 365 e di altri strumenti di comunicazione e collaborazione, tra cui e-mail, storage di file e piattaforme di coordinamento dei pazienti.

Supporto per sistemi legacy: gli MSP possono estendere la protezione ai sistemi operativi più datati e alle apparecchiature mediche specializzate senza richiedere aggiornamenti invasivi.

Backup forense e integrità dei dati: i service provider possono acquisire dati forensi per le indagini sugli incidenti e garantire l'integrità dei registri con tecnologie di verifica basate su blockchain.

Vantaggi di Acronis Cyber Platform

Invece di soluzioni specifiche assemblate in modo approssimativo, Acronis offre una piattaforma integrata in modo nativo con un unico punto di gestione che consente agli MSP di:

- Garantire una Cyber Protection completa negli ambienti sanitari.
- Ridurre il carico operativo e la proliferazione degli strumenti.
- Migliorare i tempi di risposta e i risultati dei ripristini.
- Espandersi verso un'offerta di servizi ad alto valore in ambito di conformità normativa e sicurezza.
- Aumentare i margini con offerte scalabili specifiche per il settore sanitario.

Consolidando le funzionalità essenziali in un'unica piattaforma, gli MSP possono ridurre i costi e semplificare le operazioni, offrendo al contempo la resilienza che le organizzazioni del settore sanitario richiedono.

Sviluppa la tua offerta di servizi per il settore sanitario

Le aziende del settore sanitario esigono Partner affidabili che garantiscano continuità, sicurezza e conformità. Acronis Cyber Platform permette agli MSP di cogliere questa opportunità con sicurezza.

↘ Prenota una demo per scoprire come Acronis supporta gli MSP che operano con i clienti del settore sanitario

↘ Avvia la tua prova gratuita e inizia a offrire servizi MSP resilienti per il settore sanitario

Acronis

Per saperne di più, visita acronis.com