Healthcare IT Team Rests Easy with Increased Managed Detection and Response Coverage

Hackley Community Care Center Augments Cyber Workforce with CRITICAL**START**®

CASE STUDY

AT A GLANCE

- Healthcare
- Employees Upwards of 330

CORE AGENDAS

Challenge
A small security team didn't allow for 24x7x365 coverage, over long weekends or holiday breaks

Solution
Turning to MDR for 24x7x365 coverage, with a human element, to always have eyes on their systems

Results
Improved team efficiency with augmented security coverage and strengthened security operations, resulting in more protection and less texts and messages to management during off-hours

The healthcare industry is often a target of cyberthreat actors, with 25% of ransomware attacks targeting the industry in 2022.[1]

The HIPAA Journal also reports that over 5,000 data breaches were reported to the Office for Civil Rights from 2009 – 2022, which left 314,063,186 healthcare records vulnerable.[2]

Hackley Community Care has been caring for their community for over three decades, with the mission of bringing basic care and education to individuals and families in their greatest need. Beyond working together as a team to serve their county, Hackley Community Care also maintains a technology infrastructure that both manages a variety of patient records and elevates their cybersecurity initiatives.

Hackley Community Care Center's network is built out of Microsoft servers, using Palo Alto Networks Cortex® for endpoint detection. Their IT environment includes electronic systems for both dental and health records, supported by a Virtual Desktop Infrastructure (**VDI**).

Their security team historically has not been able to provide coverage 24x7x365, but it wasn't until a recent holiday break when a community partner in healthcare was hit with a ransomware attack while their IT team was at home that the threat became more real.

> **I think everyone should have a Managed Detection and Response service if they don't have someone there who is an expert or if you can't have eyes 24x7.**
>
> **- Gary Szatkowski, IT Director**

[1]*Becker's Hospital Review. "25% of ransomware attacks aimed at healthcare industry, FBI says." Becker's Hospital Review, 11 Apr. 2019*

[2]*HIPAA Journal. "Healthcare Data Breach Statistics." HIPAA Journal, 17 Mar. 2022*

A Need for More Coverage to Reduce Risk

Over a long holiday weekend, Hackley Community Care Center's community healthcare partner learned that ransomware had been in their systems for a couple of months, waiting for the right time to strike. The IT team believes the bad actors knew that the organization had a small team that would be largely unavailable over the holiday break and took advantage.

After this event, Hackley Community Care knew their team did not have the resources to maintain complete visibility after work hours, or over holidays and long weekends and that they needed expert help as soon as possible. The cyberthreat landscape is ever evolving and dangerous, especially in the healthcare industry and they needed eyes on their systems around the clock.

> **We can't afford to hire an expert, that's why we have you.**
>
> **- Gary Szatkowski, IT Director**

Evaluating Providers: The Critical Start Difference

For Gary Szatkowski, IT Director at Hackley Community Care, evaluating MDR providers was a fairly simple process. His team looked at about five different providers, with the goal of finding a solution that would integrate with Palo Alto Networks Cortex Endpoint Detection and Response (**EDR**) and would provide the most effective MDR service per dollar invested. Critical Start has long worked with Palo Alto Networks as a strategic partner and can adapt and understand the needs of the business and their requirements, versus using a "one-size-fits-all" approach.

During his team's discussions with Critical Start, Szatkowski noted feeling very comfortable, especially since no one on his team had gone through a vendor vetting process like this before. He appreciated Critical Start's honesty, even with hard questions and ultimately knew that Critical Start was the proven expert provider to augment his team.

Critical Start simplifies breach prevention with MDR services that flex to business objectives and cybersecurity vision, regardless of the complexity. With the only technology in the industry that allows organizations to detect every threat and solve every alert whenever and wherever cyber leaders are and an expert Security Operations Center (**SOC**) team that acts on behalf of the organization, Critical Start detects threats, responds with the right actions and effectively stops breaches.

Critical Start's MDR services reduce risk and act as an extension of existing cybersecurity teams by eliminating false positives at scale through the Zero-Trust Analytics Platform® (**ZTAP®**) and industry leading Trusted Behavior Registry® (**TBR**). Critical Start provides 24x7x365 investigation and response services by integrating with powerful solutions from vendors, like Palo Alto Networks.

Choosing the Right MDR Provider

Szatkowski's team quickly learned there are many vendors out there who will tell you the things you want to hear. For a more realistic view, it was important for him to speak with references directly and he recommends that any other companies searching for an MDR provider do the same. He spoke to multiple Critical Start customers, who answered all his questions. He went through this process for all five MDR providers his team was considering, but Critical Start's references stood out amongst the rest. The Critical Start customers all loved the solution.

Critical Start provides provable metrics, peer benchmarking, shared customer learnings and best practices – while directly collaborating with SOC analysts to reduce risk.

> **Everyone I have dealt with at Critical Start has been top notch.**
>
> **- Gary Szatkowski, IT Director**

Creating Peace of Mind

Critical Start services quickly proved value and made an impact after being implemented, when PowerShell commands, a task automation and configuration management program from Microsoft, were being run on the Hackley Community Care Center network over a weekend. It was late on a Saturday night when the IT team was off work and at home, but Critical Start was already on it.

In the past, whenever the security team had ransomware scares or experienced different viruses, they were unsure who they should contact or what they should do next to properly mitigate the attack. Critical Start has a process, threat intelligence and the experience of working with hundreds of customers, while knowing exactly how to communicate and handle any cybersecurity incident. This creates peace of mind for Szatkowski, since his team is not large enough to a have a specialist for every type of cyberthreat.

By consolidating visibility, Hackley Community Care has been able to increase their awareness and take informed action to reduce risk. Critical Start has become an extension of their team, helping them to improve protection, no matter the day or time.

Modernizing and Optimizing Security Operations in Healthcare

Critical Start MDR services eliminate over 99% of alerts for customers that are confirmed good behavior through its ZTAP platform, built to automatically resolve vast amounts of false positives at scale.

Leveraging ZTAP dramatically improves visibility and reduces investigation and response time, giving users the confidence that every single alert is resolved.

Between Critical Start's ZTAP platform and specialized security experts, customers see improved protection and gain peace of mind. Through Critical Start's MDR services, customers can offload Tier 1 and Tier 2 tasks, while positively impacting team morale and strengthening their security operations.

To learn more about how Critical Start can help your organization simplify breach prevention and stop business disruptions, contact an expert today.

For more information, contact us at:
https://www.criticalstart.com/contact/