EVIDEN

Case study
Managed Detection and Response

Leading healthcare firm uncovers existing hidden cyber threats

At a glance

Challenge

The company ran a network spanning 120+ locations and thousands of employees. The client wanted to protect sensitive patient data from regulatory ramifications.

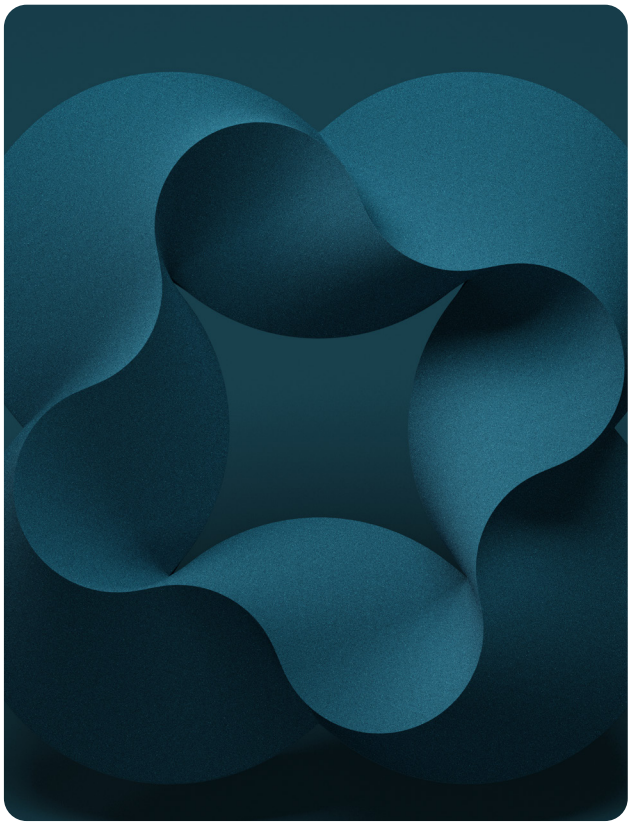
Solution

Eviden focused on providing managed detection and response services spanning their entire network. In addition, Eviden worked hand-in-hand with internal security staff to provide compliance-ready responses to potential threats.

Results

By partnering with Eviden, this healthcare company:

- Uncovered existing unknown threats within their network on the first day.
- Protected themselves against accidental, malicious link clicks.
- Reduced false positives by over 85%.
- Reduced Mean Time to Detect (MTTD) by over 90%.
- Achieved and maintained perfect HIPPA Compliance.
- Integrated into legacy security systems



> Eviden was able to offer a fully integrated security solution and integrated perfectly with our legacy security systems. The solution covered every stage of threat detection and prevention that we desired- including some enhanced response capabilities mindful of our regulatory situation.
>
> **CISO, Healthcare Company**

U.S.-based high-tech healthcare organization with thousands of employees spread throughout dozens of locations chose Eviden to monitor their dispersed network for threats continuously.

Overview

This leading healthcare organization ran 10+ hospitals and 120 office locations throughout the United States.They employed over 30,000+ individuals and utilized thousands of endpoints.

Their hospitals maintained electronic medical records for over a decade, but recently saw an increase in the cyber-attack volume and sophistication targeting their network's sensitive data.

Challenge

This U.S.-based, high-tech healthcare organization ran a network spanning 100+ locations and thousands of employees. The client was tasked with securing highly sensitive patient data. Operating in a highly regulated industry, they would face compliance consequences that would extend well beyond the immediate costs of any successful attack they suffered.

Despite the severe ramifications of suffering an attack, their security teams faced strong pressure to keep costs down, limiting the internal service they could provide. In addition, their employees operated in a stressful, high-speed environment where cyber security was rarely top-of-mind. The client used Qradar SIEM and Endgame EDR to monitor threats, but the out-of-the-box use cases were inadequate to keep the network secure.

So, despite best efforts by the organization's in-house IT security team, breaches continued. By the time they brought Eviden in to test their systems, they had already suffered various infections and compromised accounts (some known, some unknown).

Solution

After performing initial tests on their network and discovering existing malware and compromised accounts, we determined they first needed to monitor their network for known and unknown threats continuously. We solved these gaps in their detection by adding custom use cases and bringing the Eviden AI platform.

To continuously monitor their network, we deployed our cloud-based, AI-driven MDR service powered by our AI platform - AIsaac. The service provided complete visibility into all of their endpoints and assets and did so quickly, with full integration into their existing security technologies and legacy systems.

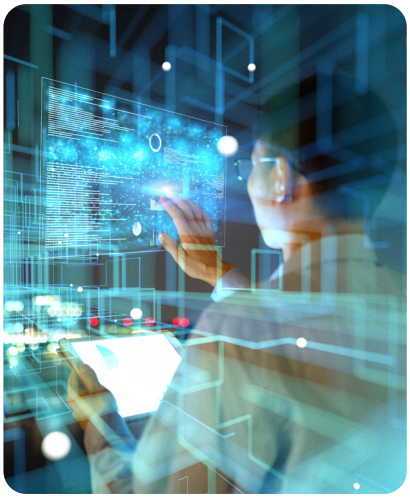
Immediately, this healthcare company gained greater ability to protect themselves from web-based attacks by plugging into our threat intelligence feeds. We also began to continuously monitor and actively hunt for threats throughout their thousands of endpoints, applications, and networks. We augmented their existing internal security team with dozens of globally-located security experts to ensure their network was protected at all times.

> Given the severity of regulatory damages we suffer when even one attack succeeds, we knew we had to find help monitoring and protecting our network.
>
> **CISO, Healthcare Company**

Our MDR service covered:

By continuously monitoring over 100+ threat intelligence feeds, Eviden began to scour the global threat landscape for those emerging threats that were most likely to attack this company. Whenever a potential attack was identified, we were able to prepare their defenses proactively. We began to deploy over 50+ security analytical models to continuously monitor, analyze, and detect threats within the company's data (including network, user, application, and endpoint sources). This threat detection extended the company's traditional security monitoring and proactively detected, contained, and responded to unknown threats that otherwise would have gone undetected.

Our team also provided a full-spectrum analysis of what it would take this company to achieve and maintain compliance, despite the threats they faced and the attacks they currently suffered. In addition, we built expanded regulatory considerations into the company's incident response plan, providing actionable steps to take (and hands-on assistance) to return to compliance if they suffered an additional attack.



Results

This healthcare company experienced an improved security posture from day one. We quickly integrated Eviden's AI-Driven MDR into their current security posture and immediately gained critical security capabilities they lacked, including a greater understanding of which emerging global threats they needed to protect themselves from, technical improvements to their existing infrastructure, and the ability to continuously monitor-and proactively hunt for-threats throughout their network. On the third day of our hunting expeditions, we identified hidden threats and successfully closed backdoors that could have welcomed the attacker back. By deploying Eviden's expanded visibility into their network, the company discovered-and responded to-existing threats and compromised assets and began remediating resulting compliance concerns.

As Eviden fully integrated its AI-Driven MDR service, the company gained power, speed, and accuracy to its security capabilities. They reduced their volume of false positives by over 75% and reduced their Mean Time to Detect (MTTD) by over 80%. They increased their ability to detect, block, and remediate any potential damage from their employees clicking malicious links and continued to be able to detect new threats their traditional security measures would have missed.

By partnering with Eviden, this healthcare company was able to achieve and maintain near-perfect compliance by detecting and responding to potential threats in near-real-time-all in a cost-effective manner they could never have achieved by deploying their internal security staff and platforms alone.

Connect with us

eviden.com

ECT-231129-AR-MDR-FS-Leading healthcare firm uncovers existing hidden cyber threats-en-v1-103133