ActZero

Case Study

ActZero helps southwest U.S. medical technology provider scale its cybersecurity efforts

ORGANIZATION OVERVIEW

Our client is a mid-sized medical business technology provider based in the U.S. southwest. The organization employs approximately 400 full-time staff, operating more than 600 endpoints, mostly operating from remote locations.

THE BUSINESS CHALLENGES

- Increasing cyber attacks targeted at the healthcare sector
- Too many disparate tools
- Low visibility into cybersecurity readiness
- Inefficient Response capability
- High cost of hiring in-house cybersecurity staff

THE BUSINESS RESULTS

- Onboarded seamlessly
- MDR provided great value on a limited budget availability
- Gained 24x7 threat coverage
- Immediate reduction in false positive alerts
- Elimination of alert fatigue across their small IT team
- Increased visibility and clarity into risks and gap closure priorities

Lack of or unfocused investment in the right people and tools, minimal due diligence into the cybersecurity of third-party vendors, providers and suppliers', and a general misunderstanding of the organizational security posture has resulted in a general unpreparedness across the healthcare industry. Layering on new resources, and managing legacy tools or even current ones that solve individual challenges rather than holistically addressing foundational security needs simply won't scale. This had become a reality for an healthcare service organization prospect.

Understanding the Business Requirements

In late 2021, southwest U.S.-based provider of revenue cycle services for healthcare provider organizations approached ActZero. They had built their physical and logical infrastructure strategically, to ensure protections against unauthorized access, loss of PHI, or third-party interception of information. However, there remained concerns about its existing cybersecurity preparedness.

Beyond general security training and processes, their existing cybersecurity solution set included an antivirus solution, and a well known endpoint detection and response service (EDR) - used to secure their endpoints and Microsoft 0365 environment.

The clients needs were clear:

Avoid disparate & insufficient tooling

The client was increasingly unhappy with their costs, the disparate functionality between the tools, the lack of customer service, and the dismal remediation of threats

Eliminate alert fatigue

The client wished to significantly reduce the needless alerts that they had been receiving, swamping their limited security resources

Increase visibility

The client wished to receive regular insight into their logs, their security hygiene, and understand how to prioritize security improvement

ActZero

CASE STUDY

THE TECHNICAL SOLUTION

- Comprehensive coverage for endpoint, network and cloud-based applications
- CrowdStrike EDR detections
- Stellar XDR detections
- NextGen Antivirus
- ActZero's ML-enabled threat modelling to find threats quicker, and with better results

THE NUMBERS

< 10-day
onboarding

90% reduction
in overall alerts

< 15%
false positive alerts

$250K+ savings
in additional staffing and annual operational costs

To minimize cyber risk, healthcare provider and service organizations must be postured to quickly identify and respond to threats. ActZero is purpose-built to detect, identify, block, contain and respond to threats across the organization, and provide the guidance needed to close their risk gaps.

Discovering compromised endpoints

During the rollout of ActZero sensors, indicators of threats were found on multiple machines within the client's environment. Early indications were that 10-15% of systems were potentially infected. Extrapolating that to the total number of systems, which was in the hundreds, this could have led to a very large problem if not resolved quickly; including significant risk of data loss or compromise of their PHI.

It became imperative that the client escalate the installation of ActZero agents on to all systems as soon as possible, so that any infected or compromised machines could be identified and dealt with promptly. ActZero was able to deploy to all client endpoint within 10 days.

ActZero's MDR solution met the client's requirements by delivering the following security improvements, and so much more:

- **Around the Clock, Scalable, Threat Coverage**: The right people (threat hunters, security engineers, data scientists, and more), the right technology (EDR, XDR, log analysis, vulnerability scanning, and threat intelligence) and the right processes to respond to sophisticated threats.
- **Better Detection Signal to Noise ratio**: Reduced false positives means more time focusing on real threats, not needless alerts
- **Strong Visibility & Guidance**: The best guidance needed to stay ahead of threats.
  - Technical Account Managers to oversee monthly progress
  - Customer Portal to gain visibility
  - Security maturity model to help assess cybersecurity readiness, prioritize risk, plan accordingly.

Delivering on the promise of improved security

Within days of deploying ActZero's virtual machines, sensors, and any necessary cloud application integrations, the client was already seeing the desired result. They no longer felt overwhelmed by alerts, and the customer portal was providing them with the clear information on their security hygiene, risk exposures, missing patches, etc. ActZero's MDR helped them avoid significant additional expenditures and future pain.

CONTACT US

Learn how our MDR solution can safeguard your healthcare services organization against attacks

Email: info@actzero.ai
Phone: +1.855.917.4981