CASE STUDY

Hospital Gains New Visibility Into Endpoints and 24/7 Around-the-clock Protection

Customer Profile

A hospital focused on serving women and infants. Being one of the first women's specialty hospitals in the U.S., this women's hospital prides itself on exceeding the expectations and needs of its patients.

Challenges

The hospital's security team struggled with insufficient manpower and expertise to effectively investigate the high volume of alerts they were receiving. Faced with limited resources and the need to comply with regulatory authorities, the hospital urgently required a solution and a partner to ensure the security of their patients' data.

Solution

Managed Detection & Response (MDR)
BDVision MDR Agent

Results

- Increased visibility into over 1,000 endpoints
- Gained peace of mind knowing their organization is protected from threats
- 9700+ alerts were investigated on behalf of the hospital with only 9 alerts requiring action by the hospital's security team
- Security team saved time and resources to reallocate to other initiatives

Challenges

Hospitals face numerous challenges, including safeguarding PHI and PII from attackers and adhering to regulations like HIPAA and HITECH, all while ensuring the delivery of critical patient care. With PHI being highly valuable to threat actors, the healthcare sector remains one of the most targeted and lucrative for exploitation. The aftermath of a security incident can be devastating, causing financial loss, fines, reputational damage, and a loss of patient trust, which can severely hinder a hospital's ability to deliver care. For this Hospital, the looming impacts of potential consequences, combined with a lack of manpower and limited visibility into their endpoints, left this hospital's security team in dire need of an effective solution. Binary Defense BDVision MDR solution provided the ideal answer to their security needs.

Solution

To solve visibility issues across the hospitals' endpoints, they chose Binary Defense nano-agent EDR, BDVision, which deploys across endpoints with minimal CPU usage, ensuring seamless integration without disrupting existing operations. BDVision utilizes advanced behavior-based detection techniques to identify and alert on real-time attacks, including evasive and emerging threats, which traditional signature-based methods might miss. The solution's containment feature allows immediate isolation of compromised endpoints, preventing the spread of threats and enabling swift remediation. Vision also leverages deception technology to divert and neutralize attackers, enhancing overall security. Its contextual alerting provides detailed insights, answers critical questions about incidents, and guides effective responses.

In addition to BDVision, the hospital selected Binary Defense Managed Detection & Response to detect and respond to threats early in the attack lifecycle. Binary

Defense expert security analysts leverage an attacker mindset to work as an extension of the Hospital's security team to monitor their environments 24x7x365 for security incidents. When a security event occurs, analysts provide triage, disposition, prioritization, and full kill chain analysis to provide tactical and strategic recommendations.

Results

The results speak for themselves – Binary Defense's partnership with the hospital has proven to be highly successful. By deploying BDVision across more than 1,000 endpoints and leveraging Binary Defenses MDR expertise, the hospital has significantly improved its threat detection and response capabilities while also strengthening its commitment to patient data protection and regulatory compliance. This implementation provided the hospital's security team with immediate observability and valuable contextual feedback on events within their environment. Since partnering with Binary Defense, the Hospital has significantly saved time and resources, with only 9 out of 9,700+ alerts requiring further action from their security team. Without the 24x7x365 monitoring provided by the SOC, the organization would have needed to allocate additional resources and personnel to thoroughly investigate over 9,700 alerts.

9,700+

alerts were investigated on behalf of the hospital with only 9 alerts requiring action from the hospitals team

In Conclusion

Healthcare institutions are heavily regulated and immense pressure requires hospital security professionals to prioritize their security posture and protect sensitive patient data while also maintaining operational efficiency and delivering quality care. Managed Detection and Response services offer a comprehensive solution for hospitals looking to gain visibility into their endpoints, proactively detect and respond to threats, and remain compliant with regulations like HIPAA. Binary Defense's partnership with the hospital's security team serves as a testament to the success of this approach in protecting critical infrastructure and safeguarding sensitive information. With 24/7 around-the-clock protection, hospitals can rest assured that their endpoints are constantly monitored and protected from potential attacks, allowing them to focus on providing excellent patient care without compromising on security.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

BINARY DEFENSE