BLACKSWAN CYBERSECURITY

SOLUTIONS BRIEF

MDR & Open XDR with AI-Driven NDR for Healthcare Delivery Organizations

Providing 24/7 protection to prevent major operational disruptions caused by ransomware, business email compromise, system exploitation, and insider threats.

The healthcare sector has become a prime target for cyberattacks due to its heavy reliance on cloud services and electronic health records across clinics, hospitals, and business associates.

Factors such as third-party exposure, flexible patient access, human error, outdated systems, and the growing use of internet-connected medical devices have significantly expanded the attack surface.

Cybercriminals are increasingly targeting healthcare organizations for access to sensitive electronic protected health information (ePHI). Given the rising severity and speed of these attacks, security teams must focus on minimizing attacker dwell time and responding rapidly to contain threats, reducing both operational disruption and data exposure.

Healthcare Attack Timeframes to Breach the Perimeter and Exfiltrate Data

23% *<5 hours*

18% *5-10 hours*

20% *10-15 hours*

23% *15-20 hours*

11% *20-25 hours*

5% *25 hours*

As healthcare breaches continue to make national headlines, many healthcare delivery organizations (HDOs) are turning to Managed Detection and Response (MDR) providers to safeguard patient data and critical operations through continuous threat detection, investigation, and response.

One Partner » One Phone Call 855.BLK.SWAN (855-255-7926)

Why is Healthcare Sector a Growing Target?

- Electronic protected health information (ePHI) is more valuable than other types of information and often fetch top dollar on the Dark Web
- Healthcare institutions are likely to pay the extortion or ransomware demands in the wake of massive operational disruptions
- HDOs struggle with prioritizing investments in security tools and digital transformation to migrate off of outdated systems while also prioritizing patient care
- Third-party risk exposure stemming from a lack of due diligence to ensure third-party vendors and service providers are taking the proper steps to protect sensitive information
- Insufficient investment in hiring enough skilled cybersecurity practitioners
- Insufficient investment in security tools and technology to mitigate a data breach
- Difficulty identifying malicious insiders

Blackswan Protects Healthcare Delivery Organizations

- Providing secure services to support patient care with continuous threat detection, investigation, and comprehensive incident response.
- Preventing operational disruptions in healthcare organizations caused by ransomware groups and state-backed cyber threats.
- Safeguarding patients' electronic protected health information (ePHI) from unauthorized access and breaches.
- Reducing risks associated with third-party vendors and supply chain vulnerabilities.
- Helping healthcare providers and business associates maintain compliance with HIPAA Security requirements.

855-BLK-SWAN
contact@blackswancybersecurity.com
blackswancybersecurity.com

BLACKSWAN CYBERSECURITY

SOLUTIONS BRIEF

MDR & Open XDR with AI-Driven NDR for Healthcare Delivery Organizations

KEY HEALTHCARE INDUSTRY CHALLENGES	HOW BLACKSWAN MDR & OPEN XDR HELPS
Protecting Patient Healthcare Information	We are adept at securing all forms of sensitive data, such as electronic protected healthcare information (ePHI), HIPAA protected data, along with financial information (PII) and credit card or payment transfer services (PCI). Our 24/7 Cyber Fusion Center (SOC) Cyber Analysts actively hunt for threats across your environment. We detect intrusions and contain attacks before attackers can establish a foothold to steal patient data or disrupt your critical operations.
Operational Disruption	We detect malicious administrative activity through remote access tools and stop intrusions before malware payloaders and multiple ransomware attacks can be deployed throughout your environment.
Avoiding Regulatory and Compliance Violations	Our MDR and Managed Risk services are designed to help you navigate the complexity of HIPAA Security Standards and put corrective controls in place. Our Cyber Fusion Center leverages multi-source intelligence, including proven runbooks which include detectors mapped to requirements and reporting measures for PCI, PII, SOX, GDPR, CCPA as well as state-level regulations.
Third-Party Risk: Securing Business Associates and Technology	We can assist with creating a third-party risk management program for your business and support securing M&A and digital transformation activities. We identify core services, including electronic medical records (EMR), drug management, time tracking, file share and document signing, and prioritize these services for monitoring. Our MDR services have repeatedly caught and stopped vendor compromises before the vendor reported the vulnerability.
Becoming a Victim of Ransomware Attacks	We monitor your attack surface 24/7 to discover intrusion attempts and prevent the pervasive deployment of malware and ransomware. • We support multi-signal coverage, ensuring visibility across endpoint, network, log, cloud, and other data sources for deep investigation and response capabilities. • We offer endpoint protection to prevent your defenses from being disabled.

ANTICIPATE

PREPARE & COMPLY

TAKE CONTROL AS WE MANAGE & PRIORITIZE CYBER RISK

Strategic services including Managed Vulnerability, Risk, and Readiness Assessments, Dark Web Monitoring, vCISO and Managed Phishing & Security Awareness Training to identify gaps, dark web exposure, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

WITHSTAND

MONITORED DETECTION & RESPONSE

PREVENT THREATS BECOMING BUSINESS DISRUPTING EVENTS

We deliver Response + Remediation you can trust. By combining our cutting-edge XDR platform, 24/7 SOC support, around the clock threat hunting and security operations leadership, we hunt and stop known & unknown threats before they disrupt your business.

RECOVER

DIGITAL FORENSICS & INCIDENT RESPONSE

EMERGE STRONGER FROM ANY CYBER INCIDENT WITH OUR IR

- **Incident Response Planning:** Tailored, actionable plans to minimize confusion and accelerate response.
- **Incident Response Execution:** Swift containment and neutralization of threats to protect critical ops.
- **Remediation Support:** System restoration, secure reconfiguration, and long-term resilience.
- **Digital Forensics & Litigation Support:** Providing technical analysis during legal/regulatory challenges.

ADAPT/EVOLVE | Cyber Risk Advisor Model, 24/7 Insight Portal Access, Resilience Roadmap and more

855-BLK-SWAN
contact@blackswancybersecurity.com
blackswancybersecurity.com