blackwell
Cybersecurity Made for Healthcare

Managed Healthcare Extended Detection and Response

MHXDR Solution Overview

blackwell
Cybersecurity Ally for Modern Healthcare

Advanced Threat Detection & Response

Expert Cyber Response When Minutes Matter

Whether your organization specializes in direct patient care, developing new models and technology for accessing care, or tackling innovative medical research, you cannot improve patient lives when business operations are down due to a cyber incident. Healthcare ransomware attacks and cyber breaches are on the rise,[1,2] making your security operations the final line of defense against everything from cyber criminals to accidental data leaks. Healthcare security operations need the right expertise, intelligence, playbooks, and tools to support a resilient delivery of improved patient outcomes and to secure protected health information (PHI).[3] Unfortunately, many healthcare security programs are brittle in the face of overwhelming technology complexity and vendor fragmentation, non-traditional digital assets, and sensitive data sprawl. A new adaptive form of cyber defense is needed to stay ahead of cyber threats in the ever-evolving global arena of healthcare cybersecurity.

Main Challenges & Why Current Solutions Fall Short

Shortage of Cybersecurity Professionals – Healthcare delivery and public health organizations are a primary target of cyber-attacks.[4] Adequately patching and managing legacy systems, securing patient data flows across internal teams and third parties, and maintaining 24/7 visibility across the environment is a lot to handle.

Securing a medium to large hospital or health system can require teams of 10-50 highly trained security personnel.[5] Smaller organizations have just as many cyber threats, but an even shorter supply of talented security staff. It is also increasingly harder to find the

[1] Eric Decker *et al*. (2023). Hospital Cyber Resiliency Initiative: Landscape Analysis. https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf
[2] Cyentia Institute. (2022). Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents. https://www.cyentia.com/iris-2022/
[3] Ponemon Institute. (2023). The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking. https://www.censinet.com/impact-of-ransomware-on-patient-safety-and-value-of-cybersecurity-benchmarking
[4] HHS 405(d) Program. (2023). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. https://405d.hhs.gov/Documents/HICP-Main-508.pdf
[5] IANS, Artico Search. (2023). Security Organization and Compensation Study: Benchmark Summary Report. https://newsletter.radensa.ru/wp-content/uploads/2023/12/2023SecurityOrganizationandCompensationSummaryReport.pdf

right talent.[6] Staffing an effective security team with the right experience that provides around the clock vigilance is cost prohibitive for many healthcare organizations.[7]

Securing PHI Across a Fragmented Vendor Landscape – Given the breadth of the threat landscape and the shortage of security expertise, Security Operation Programs must continually invest in innovative technologies to secure against emerging cyber threats. This introduces new challenges as program owners must stitch together and configure multiple third-party systems and processes across a fragmented vendor portfolio while maintaining a line of sight into the movement and integrity of PHI across these tools.

This leads to endless personnel swivel chair activities and no centralized view across the entire medical attack surface. Many programs struggle to identify where PHI is being stored, if it is being accessed for an appropriate business purpose, and if it has been misused or compromised.

Medical Technology and Legacy System Vulnerabilities – Healthcare providers and health systems leverage some of the most diverse and unique asset classes that need protection: patient-facing and critical care devices, diagnostic and support applications, legacy and cutting-edge research technologies make up a cumbersome host of connected medical devices and clinical IoT. It is calculated that known vulnerabilities are present in at least 53% of connected medical devices and other IoT devices in hospitals.[8] Maintaining visibility across this complicated attack surface requires teams with healthcare-specific knowledge and a deep understanding of the organization's infrastructure to protect devices that directly affect patient care delivery and patient health outcomes.

Many legacy devices and applications were not built with cybersecurity as top of mind, yet these tools are instrumental to providing patient care and maintaining routine business operations. Securing connected medical devices and clinical applications requires visibility and understanding of data sources outside of the classic endpoint detection tooling or classic infrastructure vulnerability scanner. Yet many security programs struggle to incorporate these input sources within their operations without being flooded with extraneous alerts, false positives, and noisy logs.

[6] Eric Ahlm *et al*. (2023). SOC Model Guide. Gartner.
[7] IANS, Artico Search. (2023). Security Organization and Compensation Study: Benchmark Summary Report. https://newsletter.radensa.ru/wp-content/uploads/2023/12/2023SecurityOrganizationandCompensationSummaryReport.pdf
[8] Willa Hahn. (2022). Medical Device Risks Continue to Threaten Hospital Security and Patient Safety. *Cynerio*. https://www.cynerio.com/blog/cynerio-research-finds-critical-medical-device-riskscontinue-to-threaten-hospital-security-and-patient-safety.

blackwell
Cybersecurity Ally for Modern Healthcare

Blackwell Security Managed Healthcare Extended Detection and Response (MHXDR)

With Blackwell Security's MHXDR Offerings, healthcare organizations have the best detection and support to accurately identify and respond to critical threats across raw security data sources, including the detection of PHI, across classic endpoints, infrastructure, cloud, and legacy systems, as well as expanding visibility into connected medical devices and clinical applications. Blackwell MHXDR prioritizes appropriate investigation, containment, and remediation actions with healthcare-specific workflows and response playbooks. This reduces the burden on your internal security team by eliminating the need to chase non-critical alerts by prioritizing the detection of PHI across the full medical attack surface. Blackwell's MHXDR offering focuses threat detection on alerts that pose the largest risk to patient care delivery, patient safety, business operations, and exposure to PHI.

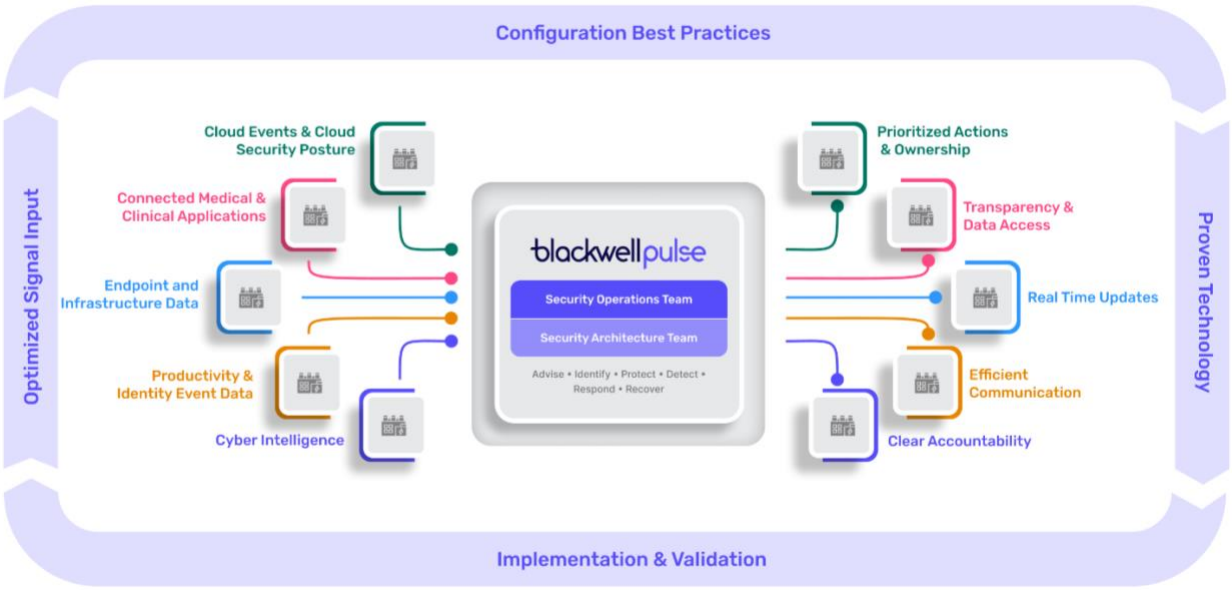
Bring healthcare-specific, and battle tested expertise into your security program. Blackwell's Security Operations, Services, and Incident Response Teams have an average of 15 years in the field, responding to some of the biggest cyber threats healthcare organizations have seen. Staffed fully in the United States, Blackwell's Cyber Fusion Center MHXDR provides compliance-aligned attack surface security with 24/7 eyes on screen and advanced threat detection and response. With unparalleled visibility and transparency, you are in the driver's seat with access to your data, service analytics, and security program insights.

Key Customer Benefits

- **Breadth of Additional Technology Integrations** allows you to extend and centrally manage detection and response across your organization's unique medical footprint
- **Connected Medical Device and Clinical Applications** security integrations and connectors provide extended visibility across the medical attack surface
- **PHI Data Detection,** workflow and response handling across source tools and applications
- **Healthcare-specific playbooks** tailored to your health system's needs, driven by healthcare-specific threat intelligence insights
- **Expert Response Team** with an average of 15 years of experience, fully and exclusively staffed in the United States

- **Direct Access** to battle-tested 24/7 security expertise in an emergency, and collaborative healthcare-attuned guidance for non-emergency security needs
- **No Blackbox** keeping you from your security data, analytics and insights
- **Clear Communication** and constant visibility into all actions taken on your behalf and in conjunction with the Blackwell Security team

Process Overview & Diagram



Cybersecurity Made for Healthcare

Blackwell's MHXDR is purpose built for healthcare organizations. Let us focus your security program through complete coverage and collection of your medical attack surface and expand your threat detection beyond endpoint and infrastructure vulnerability data. Our Cyber Fusion Center provides you with best of breed threat detection and response services, while partnering with you to ensure full transparency and growth of your security program.

With an average of 15 years of on-the-job cybersecurity expertise, Blackwell's US-based Security Operations & Services team has managed some of the largest incidents and cyber threats in the industry. You get a fully trained and operational staff with 24/7 eyes on screen and continuous visibility and transparency in the work being done on your

behalf. There is no black box separating you from your organizations alerts, investigations, and incidents. You have direct access to a team of experts when everything is on the line.

Free up your security team to work on longer-term strategic initiatives while Blackwell Security's Security Operations and Incident Response Teams tackle alerts, reduce noise, locate PHI, and manage the most important threats to patient care, patient safety, and business operations. Blackwell's MHXDR extends visibility into the full attack surface unique to healthcare to ensure that you not only can identify vulnerabilities, but you are equipped with recommendations and actions to defend around them.

Let Blackwell Extend Your Cyber Operations

Blackwell Security is a dedicated Managed Healthcare Extended Detection & Response provider. With decades of security experience working inside healthcare delivery organizations and healthcare assurance teams, we are purpose-built to safeguard patient care delivery and patient data with the understanding that a monthly services report is not sufficient to maintain or mature your program's security posture.

Leverage your existing security tooling and maximize your existing team. Blackwell Security experts will optimize your current technology, fine tune your security processes, expand visibility across the full medical attack surface, detect and defend PHI exposure, and remove the burden of maintaining 24/7 eyes on screen security staff in-house.

Looking to upgrade your threat detection technology? Blackwell Pulse offers best in breed security technology underlying our Security Operations and Incident Response Teams as part of our Cyber Fusion Center.

Contact us at blackwellsecurity.com | info@blackwellsecurity.com