XM Cyber | SOLUTION BRIEF

XM CYBER CONTINUOUS EXPOSURE MANAGEMENT

Proactive Immunity to Healthcare Attacks

Prevent attacks targeting the critical systems and connected medical devices that enable outstanding patient care.

Modern healthcare delivery has evolved into a highly interconnected ecosystem, generating vast amounts of sensitive data including PII, PCI, and PHI, while relying on a complex mix of mission-critical IoT, legacy infrastructure, and third-party tools and software. Traditional tooling and proactive security approaches fail to provide the attack surface coverage and context needed to effectively prioritize the exposures that actually threaten patient care.

XM Cyber provides the exposure intelligence needed to see every exposure and attack path across your hybrid environment, from third-party integrations to medical devices and prioritize those that matter most to patient care and service delivery. We enable teams to act for impact, not just severity, by validating and driving remediation of the exposures and paths that attackers can actually weaponize in your environment to compromise critical systems and data.

SOLUTION BENEFITS

See Every Exposure, Every Path

Uncover and eliminate all viable attack paths leading to medical devices and PHI data before they're exploited

Act for Impact, Not Just Severity

Safeguard patient health and privacy by remediating validated exposures that pose the greatest risk to service delivery

Articulate Risk, Drive Remediation

Communicate risk effectively to drive urgency across teams and prove security posture and ROI to management

XM Cyber: The Cure for Blind Spots and Missing Exposure Context

XM Cyber leverages Attack Graph Analysis™ to provide end-to-end visibility and exploitability-based exposure prioritization across dynamic hybrid environments. Here are some of the key benefits for healthcare organizations:

Secure Legacy Systems and Processes

Healthcare organizations often have to balance updating systems to the latest standards with maintaining legacy devices. XM Cyber assesses risk from legacy devices with validated attack paths and offers alternative mitigation options where patching isn't possible.

Protect Connected Medical Devices (IoT/OT)

IoT and connected devices are vital for the delivery of care, especially as adoption of telehealth grows. XM Cyber uncovers attack paths between connected devices and the corporate network, ensuring attackers can't compromise devices to move laterally and reach the broader environment.

Uncover Shadow IT

Unknown and unapproved devices pose a risk to sensitive data and critical systems safety, as well as issues with compliance. XM Cyber uses low-risk passive scanning to help organizations keep track of the devices within their environments.

Meet Governance and Compliance Needs

Stringent frameworks are commonplace in healthcare. XM Cyber maps security controls to frameworks and regulations (e.g. GDPR, CIS, SOC2), assists with compliance (e.g. HIPAA, EU AI act, NIS2), and helps secure sensitive PII, PHI and PCI data.

Prevent Ransomware Attacks

Ransomware remains a persistent threat that can have a devastating impact. XM Cyber helps security teams proactively identify, prioritize and neutralize validated attack paths that attackers could exploit in order to carry out ransomware or other malware attacks.

Adopt AI Securely

AI has enabled attackers to compress time-to-exploit, and AI adoption in organizations is introducing new types of exposures. XM Cyber continuously discovers AI tools, agents, and workloads and uncovers shadow AI to assess the impact on security posture.

XM Cyber

As the pioneer of exposure management, XM Cyber delivers a continuous and actionable understanding of cyber risk across the entire attack surface, including hybrid, cloud, on-prem, OT, legacy, AI, and container environments. Powered by proprietary Attack Graph Analysis™, the platform continuously validates exploitable exposures against a digital twin of your production environment, applying nearly a decade of offensive security expertise. By revealing the critical choke points where multiple attack scenarios converge, XM Cyber directs security teams to the remediation actions that eliminate the most risk with the least effort. The result is measurable improvement in security posture through prioritized, high-impact remediation, along with clear, business-contextual reporting that enables leaders to communicate risk effectively and demonstrate security ROI.