WHITE PAPER

Cyber Resilience in Healthcare: A Strategic Approach to Securing the Patient Journey

Insights from Armis and Fortinet on a Holistic Cybersecurity Program

Executive Summary

Amidst the increasing rate of cyberattacks on healthcare organizations, it is increasingly clear that the expansive technology ecosystems that power efficient care can also put care at risk. Healthcare delivery organizations (HDOs) must adopt a holistic approach to cybersecurity to ensure that all of the technology that powers the patient journey from the doors to the facility to traditional medical devices are cataloged, secured, and proactively protected.

This white paper recaps key insights and guidance from a webinar presented by Armis, Fortinet, and Roche Diagnostics, **"From Intake to Discharge"**, focusing on the fundamentals of effective cybersecurity strategy for modern healthcare environments. The discussion highlights the expanding attack surface that comes with patient care innovation, the evolving threat landscape and modern tactics healthcare organizations should be wary of, increasing regulatory pressures that contribute to more regimented security and reporting, and strategic approaches to build cyber resiliency into every step of the patient journey.

Key Learnings

- A holistic cybersecurity approach inclusive of all asset types is key to securing the entire patient journey
- Mapping regulatory frameworks to patient safety initiatives fosters collaboration and buy-in
- Establishing cyber resilience requires a robust program and accountability throughout the organization and the industry at large
- Aligning the definition of risks with patient impacts and clinical outcomes is central to becoming more proactive and secure.

The Expanding Attack Surface in Healthcare

Healthcare technology environments present some of the most diverse asset ecosystems in any industry. The patient journey, from admission and diagnosis to treatment and discharge, involves numerous interconnected systems. Beyond traditional IT assets like Electronic Medical Records (EMR) systems and patient portals, the “care-enabling services” are often overlooked but equally critical. This technology supports getting patients where they need to be to receive treatment from the more visible medical technology. These assets include:

Physical Infrastructure: Parking gates, automated doors, elevators, digital signage, HVAC units, and airflow regulation systems (crucial for maintaining sterile environments in operating rooms or preventing infection outbreaks in wards).

Medical Devices: Infusion pumps, bedside monitors, laboratory equipment, medication dispensing systems, and imaging systems (e.g., MRIs).

IT Infrastructure: Hospital and patient registration apps, cloud infrastructure, Wi-Fi access points, VoIP phones, and nurse call systems.

This expansive and interconnected attack surface, encompassing IT, OT, and IoMT assets, creates significant challenges for healthcare security teams.

The Evolving Threat Landscape

The webinar discussion confirmed that healthcare is the most targeted critical infrastructure industry. Research presented by Geri Révay, Principal Security Researcher - FortiGuard Labs at Fortinet, showcased the perfect storm happening in healthcare cybersecurity and the complex challenges IT security professionals are facing.

The frequency of attacks is staggering, with over 90% of healthcare organizations experiencing cyberattacks in the past year. This is caused, in part, by the sheer volume of assets involved throughout the patient journey. 99% of hospitals have IoMT or OT devices with known exploited vulnerabilities, exacerbated by legacy devices and the lack of readily available security protocols.

Ransomware attacks in particular remain a key concern for the healthcare industry. Ransomware is continuously a top attack vector for healthcare, and causes long-term impacts beyond the initial downtime, which averages nearly 18 days according to CISA and FBI incident analyses.

The Real Impacts of Ransomware

A recent ransomware attack on a healthcare provider in Spring 2025 is a stark example of the scale and impact of such attacks. A healthcare provider was targeted by the Interlock Ransomware Group, resulting in significant data theft of 1.5TB of patient information, exposing sensitive personally identifiable data, treatment information, and medical images. The attack cost the provider $13M in various costs, not to mention the impact of the disruption on patient trust, operational continuity, and the organization’s reputation.

There may be a perception that ransomware in OT or medical environments is not as impactful as in IT environments, as the crown jewel is the integrity of the operation and not the data. However, the risks are still prevalent due to the operating systems used to run medical devices. In these cases, off-the-shelf ransomware is as effective against these devices. Unfortunately, even though the data for IoMT and OT devices might not be deemed significant, the availability certainly is. When ransomware disrupts the function of medical devices like MRI machines, this is what pressures healthcare organizations into paying the ransom and perpetuates the challenge of combating ransomware attacks.

Increasing Regulatory Pressure

The hybrid attack surface challenge is compounded by increased pressure from regulatory bodies to bolster cybersecurity measures. Healthcare organizations are increasingly looking to improve and increase compliance not just in terms of coverage, but the speed with which organizations can demonstrate effective protection of their environment and complete audits. The industry is also experiencing a tide shift of regulatory scrutiny. Key frameworks such as the European Medical Device regulation (MDR) or the NIST Cybersecurity Framework apply stringent requirements on medical device manufacturers regarding clinical data, patient information, and technical documentation to help emphasize patient safety throughout every touchpoint. The focus on security is beginning to shift left to enforce security requirements not solely on healthcare delivery organizations, expanding the scope to manufacturers and technology vendors for a more comprehensive approach.

Effective cybersecurity solutions should address common themes that apply across multiple regulations, including:

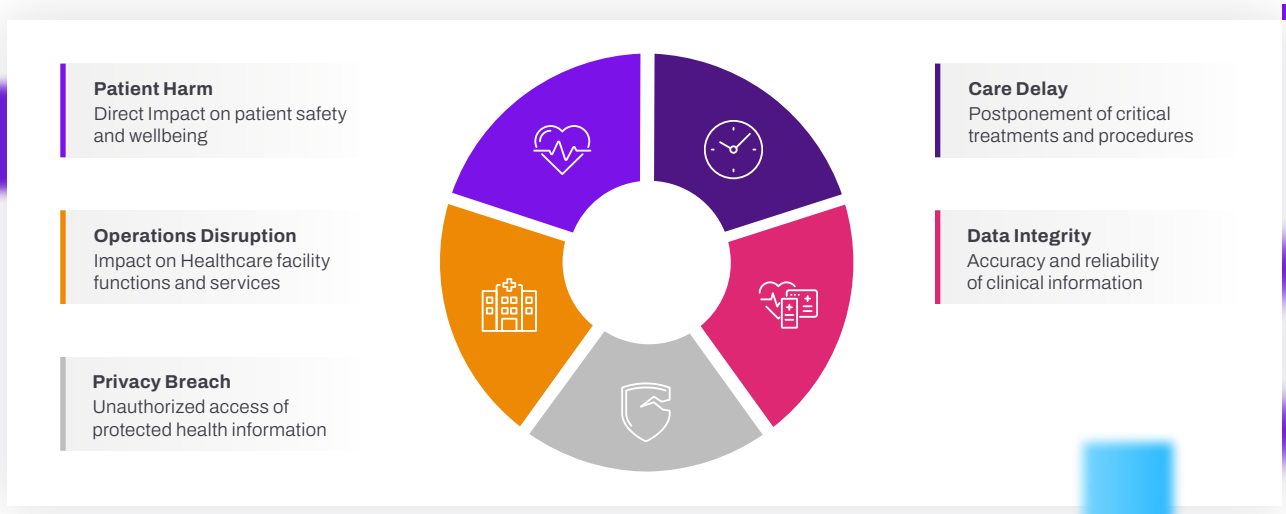
- **Real-time Asset Visibility:** Beyond traditional lists of laptops and servers, this extends to unmanaged OT, IoT, cloud infrastructure, and software inventory (including in-house applications and cloud portals). A focus on identifying patient-critical applications and services is emphasized.
- **Vulnerability and Risk Management:** This involves not only addressing technical CVEs but also insecure configurations, access controls, flat networks (which increase blast radius), and downtime procedures. Holistic and continuous assessment and prioritization of risk are crucial.
- **Security Controls:** Implementing direct patching, robust processes, and compensating controls to better manage third-party access and device security.
- **Supply Chain Risk Management:** Addressing third-party risks from vendors with network access, outdated VPN tunnels, a lack of multi-factor authentication, and insecure libraries embedded in medical devices.
- **Incident Response:** Establishing processes to limit downtime and impact, along with increasing regulatory reporting requirements for incidents involving patient data leakage.

The ultimate goal of these regulations is to ensure patients have the right access to the right care at the right time, minimizing disruptions that can lead to scheduling delays, revenue loss, and cascading negative effects.

The best practice guidance in navigating the various regulatory frameworks and requirements is to align the definition of risks with real patient outcomes. By bolstering security and embedding a secure-by-design mindset throughout the organization, healthcare facilities can reduce patient harm, minimize operational disruption, prevent care delay, maintain data integrity, and prevent costly privacy breaches.

Mapping Risk to Outcome

From A Device To A System To Patient Care Impact



Building Cyber Resiliency: A Strategic Approach

Cyber resilience is not a one-off project. Establishing, cultivating, and nurturing cyber resiliency is a continuous journey that requires a comprehensive program aligned with established healthcare security frameworks. To have the necessary impact and keep pace with the expanding threat landscape, such programs must be hybrid in nature, and factor in every asset used in healthcare facilities—from medical devices, IT, OT, IoMT, cloud, and beyond.

The first steps of establishing an effective and holistic cybersecurity program are securing leadership support and funding. Regulatory compliance requirements can also support in building a strong business case to secure funding for security projects. The other fundamental step is building the right team. Fostering collaboration between IT, cloud, IoT, medical, and OT experts is essential to manage the evolving, hybrid attack surface. Once the vision is established and support is secured, healthcare organizations can begin the true task of building their cybersecurity program.

- **Identify Risks and Requirements:** Gain a complete view of all regulatory requirements, architectural risks, business risks, and establish an inventory of all assets and vulnerabilities.
- **Establish Policies and Best Practice Procedures:** Implement zero-trust segmentation and defense-in-depth strategies to ensure clinical processes can run without disruption.
- **Implement Thorough Threat Detection:** Deep anomaly detection, behavioral analytics, and threat intelligence to surface malicious activities quickly.
- **Map Response Capabilities and Processes:** Automated containment, playbook-driven actions, and clear communication between SOC and clinical teams power an effective and timely response.
- **Execute and Iterate:** Adopt an agile approach, setting small milestones, starting with proof-of-concepts, and evolving policies as risk understanding matures.

Roche Diagnostics: A Digital Trust Case Study

Roche Diagnostics is a leader in the development of innovative products and services that address the prevention, diagnosis, monitoring, screening, and treatment of diseases. With over 125 years in healthcare and decades in digital expertise, Roche Diagnostics is a trusted partner in safeguarding data and systems.

When talking about product security, particularly related to medical devices, we talk about connectivity as well as interoperability and system integrations. None of this can occur without a very strong cybersecurity framework. As Olivier Convard, Global CISO, Product Security and Privacy at Roche Diagnostics, put it, “when medical devices become compromised, they are not easily replaced, like you would do with your credit card. We launched the Digital Trust program, our cross-functional initiative that helps healthcare providers protect patient data and clinical operations while meeting global regulations.”

Challenges in Labs

Customers in diagnostics are labs, hospitals, and point-of-care settings. Labs, post-pandemic, are increasingly targets for ransomware (projected cost of over $57 billion in 2025). They also face growing regulatory frameworks (ISO/IEC 27001; CAF; NIS2; C5; ENS; HDS), which force labs to continuously adapt. Finally, labs are also burdened with the high reputational and financial costs associated with data breaches. A potential disruption in services is a major concern for hospitals and labs. It goes beyond rescheduling or intervention and can have severe impacts on patient well-being and even cause direct harm. Security risks are therefore more than simply risks and vulnerabilities; they are intrinsically linked with patient safety.

Digital Trust Pillars

The framework identified by Roche is centered around protecting data, enabling trust, and empowering healthcare organizations.

- **Transparency and Shared Responsibility:** Open communication and timely response in collaboration with partners are essential to address issues in a timely manner and provide the best possible experience for patients.
- **Cybersecurity:** Ensuring confidentiality, availability, and integrity of data, combined with robust data governance.
- **Data Privacy:** Adhering to regulations, obtaining patient consent, and responsibly using data for new developments.
- **Trusted Data Use:** Safeguarding the confidentiality, integrity, and availability of data with zero trust strategies and multi-layered security measures wherever a patient (or their proxy) interacts with care delivery entities.

Fortinet and Armis: A Reference Architecture for Healthcare Cybersecurity

The Fortinet reference architecture, integrated with Armis, provides a robust blueprint for protecting clinical operations without disruption.

The “better together” approach and architecture is informed by healthcare industry frameworks, enabling high security levels adjusted to zones and risk profiles.

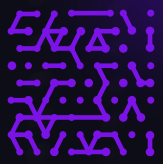
Armis Centrix™ and Fortinet’s Security Fabric unify networking and security, offering visibility, secure networking, and advanced threat protection across hybrid estates for a comprehensive approach to managing complex security requirements in healthcare. Security must follow the data from clinical operations to the cloud while remaining compliant and context-aware. Whether in core IT infrastructure or more specialized assets, Fortinet and Armis support secure-by-design programs that support patient care innovation, new technologies and AI adoption for safer, more efficient patient care.

Strategic Takeaways and Impact

Establishing an effective cybersecurity initiative in healthcare all comes to having a clearly defined program. By implementing the guidance put forth in this white paper, healthcare delivery organizations can enhance their security posture while benefiting from wider business outcomes and efficiency gains over time.

Secondary outcomes of a mature security program can include operational integrity, process optimization and improved patient flow, and efficiency gains from reduced manual effort and more proactive response.

Ultimately, the tight integration and complementary capabilities of Armis and Fortinet provide a strong technical foundation that bolsters the maturity of security programs and directly translates into safer patient care and enhanced resilience for healthcare organizations. This approach, built on people, processes, and technology working together, aims to make healthcare not just more secure but also more resilient, efficient, and patient-focused.



ARMIS®

Go deep into the platform powering the future of security.

Explore Armis Centrix™

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com