ARMIS®

SOLUTION BRIEF

Top 10 Things to Consider When Choosing a Healthcare Cybersecurity Solution

Executive Summary

Healthcare security professionals and executive leadership are all too familiar with the influx of cyberattacks facing the industry. Cyber risks are not theoretical or a 'what if.' The question instead is, will we be prepared when something inevitably impacts our organization? Is our technology adequately suited to keep patients, their data, and the integrity of the operation safe?

Static visibility or a view of a single asset type, like medical devices and equipment, is not enough. Healthcare organizations and security professionals, clinical engineers, and clinicians alike need context. An effective solution should prioritize risks and subsequent actions based on the actual threats and their clinical impact. And paramount to this is actionability, tangible risk reduction, and the workflows needed to move the needle. Identifying exposure without a path to remediation, after all, only leads to more alert fatigue, which allows risks to slip through the cracks.

A patient-centric approach to healthcare cybersecurity places the patient experience and journey throughout the facility as the focal lens for any security program or solution. Every piece of technology that supports the patient experience, from medical assets to building management, and the underlying IT infrastructure, all form the entire ecosystem of digital patient care. This approach provides a proactive, resilient, and continuous approach to security for healthcare organizations for the most comprehensive patient care protection.

Not all healthcare security solutions are suitable for today's digital care environment. With a static or limited view of medical device security, healthcare delivery organizations may be left focusing on yesterday's threats and missing key exposures that put patients or healthcare delivery at risk.

At Armis, we work with healthcare delivery organizations of all sizes worldwide to protect every connected asset and close security gaps before they become headlines. This brief outlines the top 10 things we believe every organization must consider when selecting a healthcare cybersecurity solution.

1. Complete Asset Visibility Across the Entire Environment

Security starts with knowing what you have. In most healthcare environments, that's easier said than done. Shadow IT, BYOD, legacy devices, rogue access points, third-party systems, and dispersed sites are all part of the attack surface.

A healthcare security platform should give you real-time visibility into every connected device and asset, even those you can't install agents on. That includes IT & OT systems, unmanaged medical equipment, IoT sensors, logical environments, and cloud-based workloads. Without full visibility or a limited focus on medical devices alone, you're flying blind. A centralized, real-time view of every asset, exposure, and remediation workflow provides a single source of truth, cutting manual overhead and saving millions of dollars and hours annually.

Key requirement: Real-time discovery of every asset, with deep detail on device type, location, function, and status.

2. Seamless Integration, Deployment, and Collaboration

A healthcare security solution must plug into the tech stack that is already in use by the security and clinical engineering/HTM teams. Whether it's a SIEM, SOAR, EDR, or CMMS, you need exposure data to collaborate with each other and be actionable across platforms.

Look for open APIs, prebuilt integrations, and connectors that make it easy to share context, enrich telemetry, and accelerate triage. Rapid deployment, aided by a rich integration library, speeds up time to value, and ease of use powers effective collaboration across teams.

Key requirement: Deep integration with existing security stack, break down siloes and facilitate better collaboration.

3. Clinical Contextualization of Assets and Risks

Not all vulnerabilities matter equally when it comes to patient care protection. A missing patch on a dormant laptop isn't the same as a known exploit on a device directly involved in patient care, like a patient monitor. Yet, too many tools treat all risks the same in healthcare environments.

We recommend a solution that ties asset data to its clinical function and operational criticality. Whether it's a patient monitoring system, infusion pump, imaging device, or an IT/IoT asset, you need to understand what the asset does, what it touches, and what happens if it goes down. Classify the clinical context of every asset by its role, criticality, behaviors, and risk level to prioritize the biggest potential impacts on patient care first.

Key requirement: Clinical context and healthcare-specific risk scoring for operational and patient impact during failure for more strategic prioritization and mitigation.

4. Real-Time Threat Intelligence and Exploitability Correlation

A long list of CVEs doesn't help unless you know which ones are being exploited, and more specifically, what is relevant to your environment.

Your healthcare cybersecurity solution should correlate live threat intelligence with your asset inventory to surface which threats are active, which are targeting your industry, and where those exposures exist in your environment.

Key requirement: Built-in, continuously updated threat intel mapped directly to your environment and prioritized by exploitability.

5. Continuous, Risk-Based Vulnerability Prioritization

Vulnerability management can't be about finding everything or the old method of "first-in-first-out." It has to be about fixing what matters. And that requires intelligent prioritization.

You need a system that uses machine learning, behavioral analysis, and threat telemetry to prioritize where to act first. Prioritization should be based not just on CVSS scores, but also on asset criticality, exploitability, network exposure, and business impact.

Key requirement: Real-world risk scoring, tailored for healthcare, that evolves with your environment and shows you which issues need fixing now, and which can wait.

6. Manage Third-Party Risks

Third-party breaches are increasingly becoming the main attack vector for healthcare organizations. Visibility within the four walls of the facility is not enough to continuously monitor and protect against exploits.

An effective platform must not only catalog all internal assets but also maintain visibility of any vendor-managed assets, assess vendor credentials, site-to-site connections, and remote access software. This is especially important during mergers and acquisitions to maintain a complete register of the extended attack surface. Manage access to prevent unsanctioned or unsecured apps or unmanaged vendor servers.

Key requirement: Extend visibility beyond proprietary assets to include third-party vendor-managed assets, dispersed facility locations for the complete picture.

7. Threat Detection and AI-Powered Early Warnings to Preempt Attacks

It's not enough to react to what's happening now. You need to understand how attackers might move through your environment next. That's where AI and predictive modeling become game-changers.

A modern healthcare security platform should apply AI to contextually assess your environment and identify likely attack paths, provide early warning capabilities, detect anomalies, and flag combinations of risk that could lead to a breach.

Key requirement: AI-powered exposure analysis that can simulate attack paths, provide early warnings of threats, predict lateral movement, and preemptively surface combinations of risk.

8. Healthcare-Specific Insights and Expertise

Most cybersecurity and exposure management tools were built for IT environments, and dedicated medical device-only tools leave massive exposure blindspots for IT, OT, IoT, and cloud assets.

A comprehensive healthcare security platform must provide understanding and coverage for all technology involved in the patient journey and in keeping hospitals or healthcare facilities operational. The platform should understand medical equipment, traditional and innovative technology, and provide best practice coverage from every asset, informed by broad-spectrum expertise. This should be supported by personnel with intimate knowledge of the requirements within healthcare organizations. Effective healthcare cybersecurity should be intrinsically linked with operational excellence, patient experience, and organizational transformation initiatives.

Key requirement: Purpose-built cybersecurity tooling with specialized asset intelligence, behavioral analysis, and operational insights, forming part of the domain expert team for healthcare.

9. Automated Exposure Assignment & Remediation Workflows

Once you've identified exposure, the next step must be remediation. Doing that manually across thousands of assets and multiple teams throughout the organization just doesn't scale, especially for medical devices, which often require alternative remediation processes like network segmentation to keep patient care operational and secure.

Look for a platform that can appropriately assign tasks to the right person or team is essential. Further, be sure it integrates with your ticketing systems (like ServiceNow), patching tools, firewalls, and compensating controls so that you can automate response based on clinical asset risk and internal policy. Allow clinical engineers and HTM to make better informed decisions and track risk reduction efforts over time.

Key requirement: Integration with CMDB, ITSM, and remediation tools to automatically open, assign, track (with evidence) the resolution of high-risk issues.

10. Preventive Cyber Care – Ongoing Dynamic Protection

An effective security solution for healthcare organizations must endeavor to change processes from reactive to proactive. Effective cybersecurity programs ultimately lead to better overall patient outcomes and more consistent care delivery.

Seek out a platform that monitors security trends and leverages automation to proactively build a security posture in advance of an attack taking place to reduce response time and prevent malware attacks. Dynamic protection methods, risk assessments, and continuous reporting for security improvements help embed security as a priority throughout the organization.

Key requirement: Proactive, innovative methods that leverage AI and automation to protect against the real threats of tomorrow, not the stale risks of yesterday.

Checklist: Top 10 Considerations for a Patient-Centric Healthcare Cybersecurity Solution

01 Complete Asset Visibility Across the Entire Environment

02 Seamless Integration, Deployment, and Collaboration

03 Clinical Contextualization of Assets and Risks

04 Real-Time Threat Intelligence and Exploitability Correlation

05 Continuous, Risk-Based Vulnerability Prioritization

06 Manage Third-Party Risks

07 Threat Detection and AI-Powered Early Warnings to Preempt Attacks

08 Healthcare-Specific Insights and Expertise

09 Automated Exposure Remediation Workflows

10 Preventive Cyber Care – Ongoing Dynamic Protection

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

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo