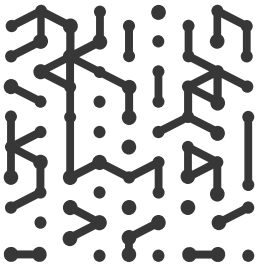
ARMIS®

WHITE PAPER

A New Era of Unified Vulnerability Management in Healthcare: Putting Patients First

Table of Contents



Executive Summary

Healthcare organizations manage some of the most sensitive and critical data, making them prime targets for cyber threats. In medical facilities, healthcare delivery organizations, and patient care clinics, the effects of a cyberattack extend far beyond data loss. Missed patches, delayed remediation, or a lack of effective strategy can compromise patient safety, cause medical equipment to operate unsafely, disrupt clinical operations, and negatively impact care outcomes. A patient-centric approach to vulnerability management isn't just a security measure—it's a commitment to protecting patient trust, privacy, and safety.

The risks of not evolving are severe, as shown by the pace and complexity of cyberattacks in healthcare. It's time for a shift in perspective. This white paper explores strategies to build a robust, patient-focused unified vulnerability management program, emphasizing key elements such as proactive risk assessment, a true clinical impact lens on risk scoring, efficient workflow integration across multiple teams, and compliance with industry regulations. We will provide guidance on selecting security tools with the patient experience in mind to make more effective progress in reducing cyber risks for healthcare providers.

The Downfalls of Traditional Vulnerability Management in Healthcare

Fighting Advanced Attacks with Outdated Methods

The healthcare industry is one of the most targeted by advanced cyberattacks, with widespread threats from ransomware, unpatched vulnerabilities, third-party risks, and data breaches. Increased reliance on innovation and digital patient care translates to more assets, devices, and interconnections between them. The technology landscape has dramatically expanded, bringing with it an influx of cyber exposure risk, alerts, and vulnerabilities. Without a clear prioritization and remediation strategy, the volume of alerts and security findings can overwhelm already under-resourced teams, creating massive security gaps that can compromise patient safety and the continuity of care.

Standard Patch Management Puts Patient Care at Risk

Traditional vulnerability management falls short in healthcare. A missed patch or delayed remediation, or worse, a lack of strategic process, means more than just potential data loss; it can result in compromised patient safety and severe health risks. From imaging systems and wearable monitors to supporting IT infrastructure, security teams at healthcare delivery institutions are tasked with managing a wide attack surface.

Increased Responsibilities, Fewer Resources

Healthcare delivery has undergone significant transformation in recent years. Now, the scope of what cybersecurity looks like extends beyond IT or medical devices alone and must support the full spectrum of connectivity in modern patient care environments. To minimize the risk of exploits, impacts on care availability and patient outcomes, all vulnerabilities, as well as risk factors such as end-of-life (EOL) assets, must be viewed through both a cyber exposure management and clinical lens for effective prioritization and remediation.

Overwhelmed Remediation Teams

Remediation teams are increasingly overwhelmed as they receive numerous requests from various security groups, often lacking a cohesive prioritization strategy. Lack of focus and a massive volume of security findings create inefficiencies, delayed remediation efforts, and the potential for high-risk vulnerabilities to linger unresolved. This creates organizational bottlenecks that leave healthcare organizations exposed to risks.

What Vulnerabilities Are Prevalent in Healthcare?

Software Vulnerabilities

1. **Unpatched Software -** Outdated software that contains security flaws that attackers can exploit.
2. **Code Vulnerabilities -** Flaws in the code can lead to security breaches.
3. **Zero-Day Vulnerabilities -** Newly discovered vulnerabilities for which no patches or fixes are available.
4. **Ransomware -** Ransomware attacks have doubled in frequency over the past two years, with an average cost of $11M per incident.
5. **Third-Party -** Software or services provided by third-party vendors often introduce additional risk due to lack of security oversight. 62% of organizations experienced a third-party data breach or cybersecurity incident in 2024. High-profile attacks have exposed sensitive records, impacting millions of patients worldwide.

Learn More About the Threat of Ransomware Attacks

Asset Vulnerabilities

1. **Legacy Equipment -** The majority of medical devices and equipment are either aging out or operating on legacy systems, often lacking basic cybersecurity safeguards.
2. **Misconfiguration -** Incorrect settings or insecure configurations.
3. **Device Malfunction or Recalls -** Safety issues revealed in medical equipment that pose potential risks to patients if used.

Human Vulnerabilities

1. **Social Engineering -** Exploiting human trust and gullibility to gain access (e.g., phishing, vishing, baiting).
2. **Weak Passwords -** Easily guessed, found, or used credentials.
3. **Lack of Security Awareness -** Employees who are not trained in security best practices can unknowingly create vulnerabilities.
4. **Budget Restrictions -** With limited budgets and resources for security, potential risks are left unaddressed, leaving healthcare organizations consistently exposed to threats.

Network Vulnerabilities

1. **Weak Network Security -** Poorly configured devices can create entry points for attackers.
2. **Unprotected Services -** Services running on the network without proper security measures (e.g., open ports, weak authentication).
3. **Insider Threats -** Malicious or negligent actions by employees or insiders.
4. **Data Breaches -** 725 breaches were reported to the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and exposed or impermissibly disclosed more than 133 million records. Breaches violate privacy laws and risk financial and reputational damage.

Physical Vulnerabilities

1. **Physical Security Breaches -** Unauthorized access to physical locations or equipment.
2. **Environmental Factors -** Extreme weather, natural disasters, or other environmental events can damage or compromise physical security.

The Risks of Not Evolving – The Impact of Ineffective Healthcare Risk Management

The biggest cybersecurity threat to healthcare delivery organizations may not be threat actors themselves. In an industry that is constantly being asked to do more with less, IT security is no exception. Amidst increased attacks and new breach headlines seemingly daily, vulnerability management and security teams are still drowning in alerts, vulnerabilities, and potential threats. The frequency and ferocity of cyberattacks and breaches in healthcare have only increased in recent years. A new way forward in vulnerability management, effective healthcare-specific prioritization capabilities, and actual risk mitigation are essential to combat the rampant external threats that put patient care in jeopardy.

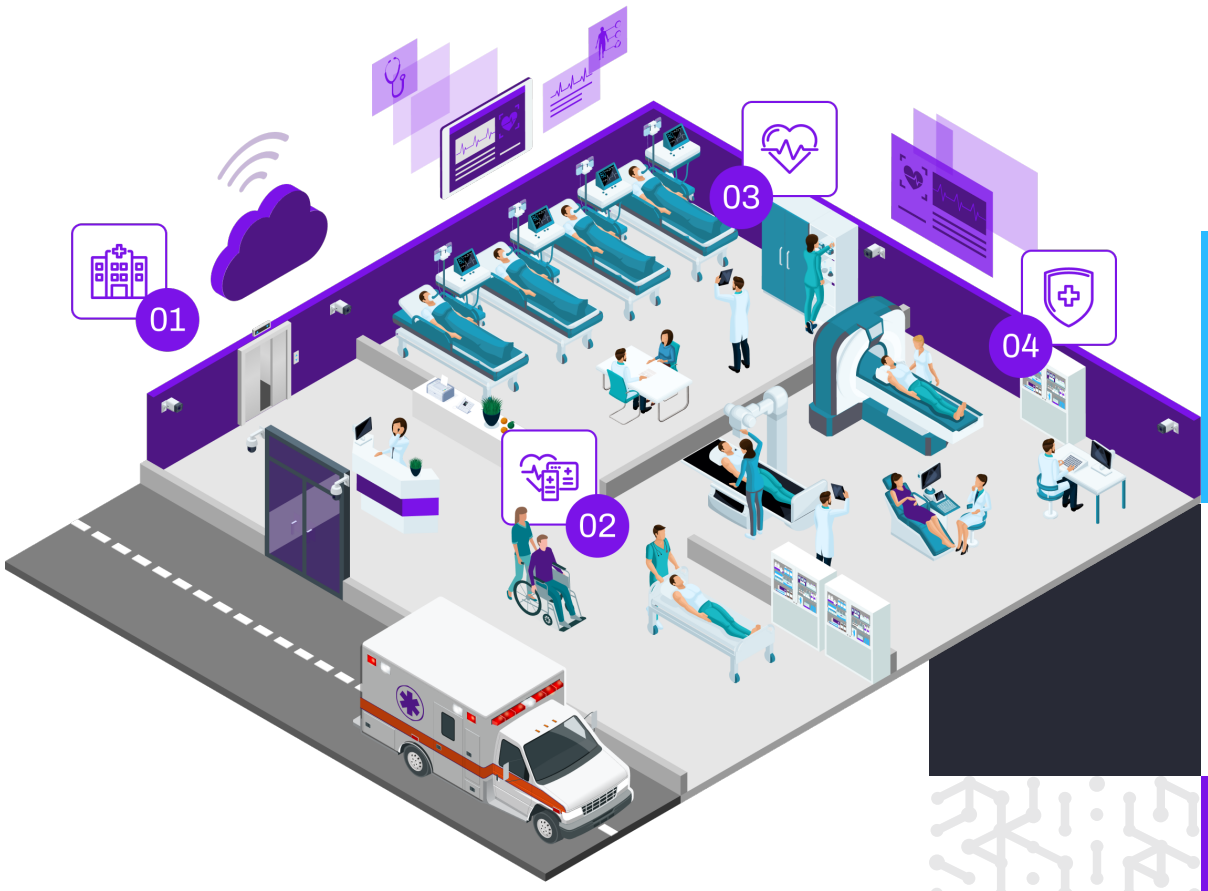
- **60%** of cyberattacks exploit known but unpatched vulnerabilities and **53%** of medical devices have known vulnerabilities
- While initial response to cybersecurity threats can take **hours**, full recovery can take around **7.34 months**
- Ransomware Attacks cause, on average, **21 days** of downtime, putting patients at risk
- With **17 connected devices per hospital bed** and **up to 23 vulnerabilities** on each medical device, the average hospital can have **over 50,000 vulnerabilities** directly touching patients

Using the Patient Perspective to Transform Vulnerability Management

Traditional vulnerability management lacks one key component: the patient perspective. By reframing risk management and reduction initiatives around the patient journey, we can shift the focus from technology or arbitrary scores to a true view of the clinical impact on operations, safety, and security.

Across every element of vulnerability management programs—visibility, asset context, prioritization, remediation workflows, and ongoing monitoring and reporting—future-focused security vendors will achieve success by viewing security as an inherent facet of the clinical care process. After all, cybersecurity in healthcare is not just about technology. It is about keeping patients, their data, and their experience protected when they are at their most vulnerable.

Every asset, every security finding, and every risk should be managed within a central location. Whether it is building management systems that power the facility entrance, electronic patient records, or computers used at intake, the medical equipment used for diagnostics or monitoring, every step of the patient journey from intake to discharge should be treated equally.



Key Components of Patient-Centric Unified Vulnerability Management

Vulnerability management in healthcare should look different than other industries. Organizations must have the ability to take a patient-first perspective on any potential risks to maximize their efforts, speed up time to resolution, and prevent care delivery disruption.

In order to address the downfalls of traditional vulnerability management methods, we've assembled a list of the key components of patient-centric unified vulnerability management that can effectively meet the needs of modern patient care delivery. At the core of this methodology is the belief that every asset, every piece of technology, and indeed every potential risk is evaluated from the patient's perspective first and foremost. Leveraging intelligent automation, comprehensive attack surface visibility, and leading proactive vulnerability management techniques allows healthcare organizations to not only mitigate risks already in their environment but also get ahead of potential risks to prevent any impact on their patients and the overall operation.

The fundamental questions you should answer when seeking to take a patient-centric approach to unified vulnerability management are:

> **Do I have full visibility of the technology in my environment?**
>
> Basic asset inventory is table stakes for effective cybersecurity. A dynamic inventory of every asset type, spanning medical equipment, IoT or OT assets, and IT infrastructure, is essential to give a foundational view of the attack surface and its associated risks. An ideal tool should employ multiple detection methods, including network traffic or behavior-based anomaly detection, to find more and secure more.
>
> **Learn More** ↗

> **Does this solution allow me to take a proactive approach to risk management or am I constantly chasing threats after they have already taken hold?**
>
> Moving the dial from reactive to proactive is essential in maintaining uptime for patient care delivery. A single fault can result in exploits that have catastrophic impacts on operations, leaving care in limbo for weeks and months. Proactively identify actively exploited vulnerabilities using AI and threat intelligence, including zero-day and ransomware, enabling timely mitigation and protecting healthcare organizations from disruptions.
>
> **Learn More** ↗

Can I differentiate between assets directly used in patient care and those on the periphery?

Standard asset visibility is not enough to secure smart hospitals and modern healthcare environments. Detailed asset insights about clinical usage, location, patient proximity, and behavioral context are necessary to power comprehensive cybersecurity.

Learn More ↗

Does the prioritization logic consider patient safety and the impact of failure on care delivery and operational uptime?

Your vulnerability management solution should be able to determine the clinical impact of device malfunction or exploit and manage vulnerabilities accordingly. Ensure to include medical device recalls and MDS² files for comprehensive risk assessment and faster response for IT security and clinical engineering.

Learn More ↗

Does the solution leverage automation and free up our resources for more strategic efforts?

The average organization already uses dozens of security tools. Does the vulnerability management solution require dedicated resources to take action on security findings manually or does it leverage automation and workflows to free up resources and reduce operational overhead? An effective solution should streamline remediation with a single platform for security, IT, and clinical teams. Automation can reduce manual intervention bottlenecks. Companies that extensively employ AI and automated security tools lower breach costs in some instances by an average of USD 2.2 million.

Learn More ↗

Am I able to measure risk reduction for executive and compliance reporting?

Demonstrate secure processes and manage compliance requirements with dashboards and reporting. Monitor security advisories, medical device recalls, and patient data exposure to prevent costly data breaches.

Learn More ↗

Did You Know

Healthcare organizations with effective cybersecurity and vulnerability management programs boast better overall patient outcomes.

Patients can bear the brunt of ransomware attack fallout, with a **28% increase in mortality rate for affected healthcare organizations in 2023**.

Ensuring you have systems and processes in place across the key components of a patient-centric vulnerability management program can prevent costly attacks and maximize the impact of your patient care services.

Building a Patient-Centric Approach to Unified Vulnerability Management in Healthcare

When selecting tools and partners for your unified vulnerability management program, keep the following considerations in mind to ensure alignment with a patient-focused approach:

1. Comprehensive Coverage for Every Asset

Ensure the solution safeguards records, devices, and systems comprehensively, eliminating gaps that could impact patient safety or data.

- **Dynamic inventory and discovery** to build and maintain a live asset inventory without disrupting essential clinical operations.
- **Auto-classify devices** by type, vendor, function, and proximity to patient to support clinical risk scoring and segmentation planning.

2. Ease of Integration and Collaboration

Opt for tools that seamlessly integrate with existing workflows and systems, minimizing disruption to patient care. Open APIs, pre-built integrations, and connectors make it easy to share context, enrich telemetry, and accelerate triage. Foster communication between IT, clinical staff, and leadership to align decisions with patient protection at every level.

- **Pre-built integrations** maximize your existing investments and provide seamless deployment, extensive visibility, and ease-of-use throughout the organization.
- **Single pane of glass visibility** within a single platform, ensuring all information is accessible regardless of the means.

3. Effective Third-Party Risk Management

Extend visibility beyond proprietary assets to include third-party vendor-managed assets, dispersed facility locations, and remote access software. Continuously monitor and protect against exploits across the entire attack surface beyond your four walls.

- **Catalog all vendor-managed assets,** assess vendor credentials, site-to-site tunnels, and remote access software.
- **Foster collaboration and accountability** between security teams and other organizations for a successful cybersecurity program on all fronts.
- **Manage access** to prevent unsanctioned or unsecured apps on unmanaged vendor servers.

4. Scalability for Future Innovation

Choose a solution that can grow with your organization's needs to address future challenges and expansions. Integrations, use of AI, and proactive detection mechanisms help adapt protection for changing environments and emerging threat tactics.

- **Continuous innovation** and a strategic roadmap to address the latest threats and tactics.
- **Healthcare center of excellence** program to support maturity and security posture improvement over time.

5. Clinical Risk Context

Not all vulnerabilities matter equally when it comes to patient care protection. A fit-for-purpose solution in healthcare should tie asset data to its clinical function and operational criticality to understand every asset's role, behaviors, and risk level based on the biggest potential impacts to patient care.

- **Assign a clinical impact score** for every asset to determine the impact of failure, patient dependence, and overall risks to operational uptime to tailor approaches for the most essential clinical assets.
- **Manage medical device recalls** to automatically associate advisories with impacted devices for effective remediation.
- **Support preemptive maintenance** with remediation guidance, utilization insights, and alerts for impending end-of-life or end-of-support to schedule work outside of peak patient care hours.

6. Automated Exposure Remediation Capabilities

Look for tools with strong automation features to reduce manual workloads and improve response times. A platform should integrate with your ticketing systems, patching tools, firewalls, and compensating controls so you can automate responses based on clinical asset risk and internal policy.

- **Automate ownership assignment** to eliminate guesswork and avoid wasted time in the remediation process.
- **Integrate directly with ticketing systems** to initiate work orders for maintenance and risk mitigation within a single platform.

7. Healthcare Compliance Features

Verify that the solution includes pre-configured support for healthcare-specific regulations like HIPAA or GDPR, FDA guidelines, and patient data protection. Closing visibility and security gaps ensures ongoing compliance and more effective reporting, reducing complexity and saving time.

- **Automated tracking** of security advisories, medical device recalls, and manufacturer disclosure statements.
- **Scheduled reports and dashboards,** and dedicated healthcare data views to effectively demonstrate risk reduction and security posture over time.

8. Proactive Threat Detection

Select tools with advanced threat monitoring to identify and mitigate vulnerabilities before they can impact patients. Real-time threat intelligence should correlate to your asset inventory to determine which threats are active, which are targeting your industry, and where exposures exist in your environment.

- **Identify vulnerable, exposed, or anomalous devices** using behavioral baselining and vulnerability mapping.
- **Correlate local findings with global threat intelligence** from honeypots, malware analysis, and dark web activity to understand what attackers are actually targeting.

9. Continuous, Risk-Based Vulnerability Prioritization

Leverage real-world risk scoring, tailored for healthcare, that evolves with your environment. Machine learning, behavioral analysis, and threat telemetry allow you to prioritize where to act first, beyond the CVE list.

- **Develop healthcare-specific risk scoring** based on evolving risk tactics and the performance of your unique environment.
- **Compare multiple sources** to avoid reliance on a single source and broaden your vulnerability management focus.

10. Vendor Support and Training

Partner with a vendor that offers ongoing support, training, and resources to ensure your teams are equipped for long-term success. Build a culture of cybersecurity awareness across the organization by training staff to identify and respond to risks effectively.

- **Develop a security-first culture** with incident response processes that maintain safe and continuous care.
- **Emphasize personal accountability,** making everyone responsible for secure processes to reduce risks over time.

11. Healthcare-Specific Insights

Unified Vulnerability management is not the end stage of cybersecurity. A comprehensive solution must provide insights on medical equipment, healthcare-specific requirements, specialized asset intelligence, behavioral analysis, and operational insights. A cybersecurity or vulnerability management vendor should take ownership of their role in the patient experience.

- **Healthcare asset intelligence** powered by collective analytics and security, a knowledge base allows you to learn from your peers and become more secure as a community.
- **Align with patient experience and operational excellence goals** to report on the metrics most relevant for healthcare stakeholders.

12. Preventive Cyber Care – Ongoing Dynamic Protection

A robust healthcare security solution must shift from reactive to proactive approaches, ultimately improving patient outcomes. Opt for a platform that leverages automation and security trend monitoring to build a proactive security posture, reducing response time and preventing attacks. Dynamic protection, risk assessments, and continuous reporting are crucial for embedding security as an organizational priority.

- **Leverage cutting-edge technology,** including AI, threat detection, automation, and proactive protection tactics.
- **Continuous development** aligned with emerging threat actors, exploits, and security/operational goals.

Embracing More Comprehensive Unified Vulnerability Management

The way forward in vulnerability management that is fit for purpose in healthcare environments is Unified Vulnerability Management. UVM is a comprehensive, integrated approach to identifying, assessing, contextualizing, prioritizing, and remediating vulnerabilities across an organization's entire attack surface, including traditional IT, OT, IoMT, and IoT assets whether physical or virtual.

As vulnerability management evolves to keep pace with more advanced attacks and exposures in healthcare, adopting this approach will reduce the manual headaches that come with traditional VM and maximize every action to keep patient care protected.

Healthcare organizations that master Unified Vulnerability Management as part of their cyber exposure management programs will benefit from:

- A single view of all prioritized risks based on their clinical context
- Operational efficiency gains by grouping findings with their common fix
- Continuous protection with ongoing asset coverage tracking
- Streamlined workflows with actionable guidance, task assignment, and bulk ticketing
- Focused efforts on the highest impact fixes, eliminating guesswork or manual assessment

Ultimately, adopting Unified Vulnerability Management (UVM) will help healthcare organizations prevent costly disruptions, manage all assets in the modern healthcare environment, and meaningfully reduce the risks directly impacting patient care.

Patient-Centric Unified Vulnerability Management Buyer's Guide Checklist

- ✓ Comprehensive Coverage for Every Asset
- ✓ Ease of Integration and Collaboration
- ✓ Effective Third-Party Risk Management
- ✓ Scalability for Future Innovation
- ✓ Clinical Risk Context
- ✓ Automated Exposure Remediation Capabilities
- ✓ Healthcare Compliance Features
- ✓ Proactive Threat Detection
- ✓ Continuous, Risk-Based Vulnerability Prioritization
- ✓ Vendor Support and Training
- ✓ Healthcare-Specific Insights
- ✓ Preventive Cyber Care – Ongoing Dynamic Protection

Conclusion - Looking Ahead in Healthcare Cybersecurity

With new risks around every corner, the time to adopt a future-focused security strategy is now. Building a patient-centric approach to vulnerability management means putting patient safety, data security, and trust at the forefront of your cybersecurity strategy. By prioritizing risks that impact patient care, fostering collaboration across teams, and leveraging the right tools, healthcare organizations can create a resilient program that supports better outcomes for everyone involved.

Healthcare innovation is centered around improving the patient experience and always striving for better. Cybersecurity and vulnerability management solutions should apply the same ethos for more proactive, resilient systems that keep patients protected. This ensures that healthcare can continue to innovate safely, and cybersecurity vendors become part of the fabric of the patient care ecosystem for more cohesive protection and processes.

By adopting a new approach to unified vulnerability management and putting the patient perspective first, healthcare organizations can:

- **Prevent costly disruptions** before they occur
- **Manage and maintain every asset** used in the modern healthcare environment
- **Meaningfully reduce risk** in the areas that are most directly implicated in patient care

For more insights on implementing, adopting, and operationalizing a strategy like this for a more clinical view on cybersecurity, visit **www.armis.com/healthcare-playbook**

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