RUNSAFE SECURITY

RunSafe Security's 2026 MEDICAL DEVICE Cybersecurity Index

Insights from Healthcare Decision-Makers on Medical Device Procurement, Risk, and Resilience

Cybersecurity drives procurement, vendor trust, and patient safety—and the stakes are rising.

RunSafeSecurity.com

Table of Contents

Executive Summary

Healthcare Is Improving Device Security—But Attacks Are Still Rising

Medical device cybersecurity has entered a new phase. Healthcare organizations are strengthening procurement requirements, increasing investment, and adopting new security practices. Yet despite this progress, cyberattacks on medical devices are becoming more frequent—and more harmful to patient care. RunSafe Security's 2026 Medical Device Cybersecurity Index, based on a survey of 551 healthcare professionals throughout the U.S., UK, and Germany involved in device purchasing decisions, reveals an industry under pressure from regulators, attackers, and the compounding risks of legacy devices that cannot be patched.

Key Takeaways

This year's Index moves beyond surface-level trends to examine the forces driving them. For the first time, the report captures how healthcare organizations are confronting:

- The rapid adoption of AI-enabled medical devices and the risks they introduce
- The continued reliance on unsupported, vulnerable systems in clinical environments
- The emergence of runtime protection and continuous monitoring as adaptive defenses

Together, these additions reveal that cybersecurity risk in healthcare is increasing and defenses need to keep up.

Progress Signals

Healthcare organizations are making measurable progress in integrating cybersecurity into procurement, operations, and investment decisions.

- **Cybersecurity is now a procurement gate:** 84% of organizations include cybersecurity requirements in vendor RFPs—43% with detailed requirements, up from 38% in 2025. More than half (56%) have already rejected a device due to cybersecurity concerns, up from 46% in 2025.
- **SBOM adoption is mainstream:** Nearly 81% of respondents rate a Software Bill of Materials (SBOM) as "important" or "essential" when evaluating devices, up from 78% in 2025. Critically, 35% say they will not consider a device without one.
- **Regulations are driving procurement:** Nearly 79% of respondents say FDA cybersecurity guidance or EU MDR requirements have meaningfully influenced their procurement processes, up from 73% in 2025.
- **Budgets are moving, and confidence is rising:** 77% of organizations increased cybersecurity resources in the past 12 months, up from 75% in 2025. Confidence in detection and containment improved slightly: 22% now feel "extremely confident," compared to 17% who felt "extremely" confident in 2025.
- **Runtime protection is gaining momentum:** 82% of organizations have deployed or are actively piloting runtime exploit protection—of these, 29% have deployed it widely and 53% have deployed it on some devices. This technology defends devices even when patches cannot be applied.
- **Willingness to pay for security remains strong:** 76% of respondents said they would pay a premium for devices with advanced cybersecurity protections, with 49% willing to pay 5% or more. While slightly down from 79% in 2025, the signal to manufacturers is clear and sustained.

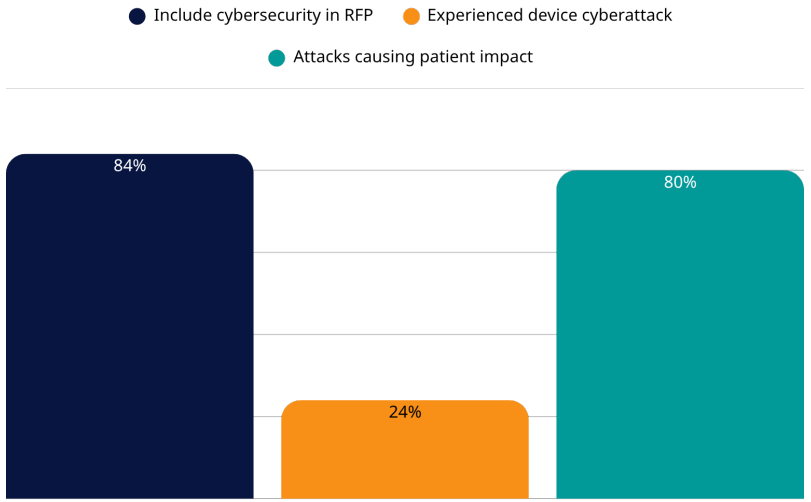
Risk Signals

At the same time, underlying risks remain significant and, in many cases, are increasing in severity and impact.

- **Cyber concern is pervasive:** 59% of respondents are “extremely” or “very” concerned about a cybersecurity incident impacting medical devices, yet 24% of facilities have already experienced an attack.
- **Incidents cause real patient harm:** Of those who experienced a cyberattack, 80% reported moderate or significant impact on patient care, up from 75% in 2025. Extended stays and manual workarounds affected nearly half of the impacted organizations, and recovery times are growing longer.
- **Legacy device exposure is significant:** 28% of organizations operate devices past end-of-support. 44% acknowledge running end-of-support devices with known, unpatched vulnerabilities.
- **AI and security are now part of the picture:** 57% of organizations currently use AI-enabled or AI-assisted medical devices, and 80% express at least moderate concern about the cybersecurity risks they introduce.

Compared to 2025, major procurement metrics have hardened: more organizations are requiring cybersecurity in RFPs, more are demanding detailed requirements, and more are walking away from devices that don’t pass muster. Cybersecurity is an integral part of device procurement, and the bar is rising year over year.

Cybersecurity Is a Procurement Priority But Attacks Still Reach Patients



Introduction

From IT Concern to System-Level Constraint

The past year has provided concrete evidence of how quickly cyberattacks can materialize into patient harm. The ransomware attack on Change Healthcare affected an estimated 190 to 193 million individuals and is cited as the largest healthcare data breach in U.S. history. Seventy-four percent of hospitals reported direct impact on patient care, and a third said the attack disrupted more than half of their revenue.

In March 2026, a cyberattack on Stryker, one of the world's largest medical device manufacturers, disrupted global operations. Some health systems delayed surgical procedures after Stryker temporarily halted its ability to deliver patient-specific products, and its Lifenet electrocardiogram transmission system was reported to be nonfunctional across most of Maryland. Both cases illustrate what happens when device-adjacent systems fail at scale and why the professionals responsible for procurement, security, and patient safety are paying closer attention to cybersecurity than ever before.

The regulatory landscape has shifted in parallel. The FDA finalized updated cybersecurity guidance in June 2025, introducing mandatory lifecycle security requirements for medical devices and superseding its 2023 guidance, raising the bar for new devices entering the market. The EU's Cyber Resilience Act moved into active implementation, imposing cybersecurity requirements on connected products sold across the European market.

These frameworks are consequential for procurement teams, as they define what manufacturers must demonstrate and, by extension, what healthcare buyers can and should demand. But regulation addresses new market entrants. The harder, less tractable challenge is the large installed base of legacy devices already in clinical use—devices that cannot always be patched, cannot be easily replaced, and carry known vulnerabilities into the most sensitive care environments.

RunSafe Security's 2026 Medical Device Cybersecurity Index surveyed 551 healthcare professionals throughout the U.S., UK and, Germany in March 2026, all involved in medical device purchasing and familiar with their organizations' cybersecurity practices. What the data reveals is an industry that has internalized the threat and is responding with greater urgency, more specific procurement requirements, and growing investment. But it also reveals persistent structural gaps in confidence, in legacy device management, and in the emerging security challenges posed by AI-enabled devices that spending alone has not closed.

The result is a paradox: while healthcare organizations are improving how they evaluate and purchase secure devices, they remain exposed to risks that procurement alone cannot solve.

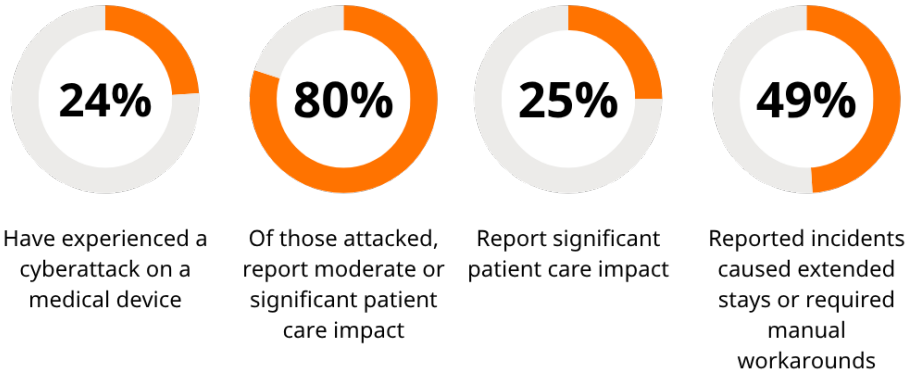
Finding 1:

Incidents Are Happening—and Harming Patients

The data shows that cyber risk in medical devices is not theoretical—it is already impacting patient care at scale.

Cybersecurity risk in medical devices is growing. The share of organizations that have experienced a cyberattack or exploited vulnerability affecting a medical device has risen from 22% in 2025 to 24% in 2026. More troubling is the severity: among those hit, the proportion reporting moderate or significant patient care impact climbed from 75% in 2025 to 80% in 2026. Despite more investment, more awareness, and stricter procurement, attacks are becoming more frequent and more harmful when they land.

Attack Prevalence and Impact



What Was Attacked

Among those who experienced an incident, the most commonly affected systems were:

- Electronic health records systems — 35% of impacted organizations
- Patient monitoring devices — 23%
- Laboratory and diagnostic equipment — 18%
- Networked surgical equipment — 10%
- Imaging systems — 8%

How Long Were Devices Down

Recovery from these attacks was not swift. Most incidents involved significant operational disruption:

- 5–12 hours of downtime — the most common scenario, affecting 39% of impacted organizations
- 1–4 hours — 37%
- 13–24 hours — 11%
- More than 3 days — 5%

The Nature of the Attacks

The incident types cited by respondents reflect the range of real-world threat vectors targeting healthcare environments:

- Malware infection requiring device quarantine — 48%
- Network intrusion requiring device isolation — 41%
- Remote access exploitation — 38%
- Ransomware affecting device operation — 32%
- Vendor-identified vulnerability requiring urgent patching — 32%
- Data exfiltration from connected devices — 21%
- Supply chain compromise - 18%
- Memory-based attack - 14%

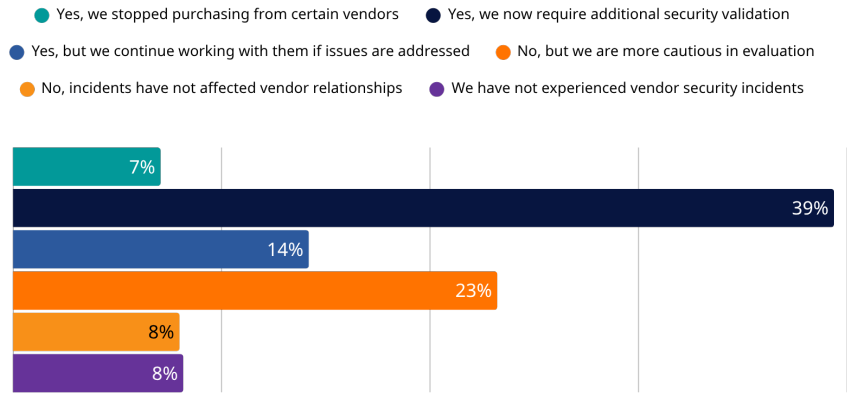
Notably, in 2025, the dominant attack vectors were malware infections (51%) and network intrusions (44%); in 2026, remote access exploitation has emerged as a major threat in its own right at 38%, signaling that attackers are adapting to the growing remote access footprint of connected devices. Organizations that have not implemented network segmentation, access controls, and runtime protections are exposed.

The frequency of remote access exploitation and network intrusion reflects the core risk of device connectivity. Devices that were once air-gapped are now networked, and that expanded attack surface is being exploited.

The Downstream Effect on Vendor Trust

Cybersecurity incidents are also affecting vendor relationships. In 2025, 32% of organizations reported that security incidents had affected their trust in specific vendors and were now requiring additional verification. In 2026, that figure has climbed to nearly 40%. In 2026, 7% report having stopped purchasing from specific vendors entirely, and 23% report heightened caution in vendor evaluation going forward. Each incident wave leaves a longer-lasting tail of damaged trust.

Have cybersecurity incidents affected your trust in specific medical device vendors?



Cybersecurity incidents are no longer isolated technical events—they are operational disruptions with direct consequences for patient care. Organizations that cannot quickly detect, contain, and recover from these incidents face measurable clinical and financial risk.

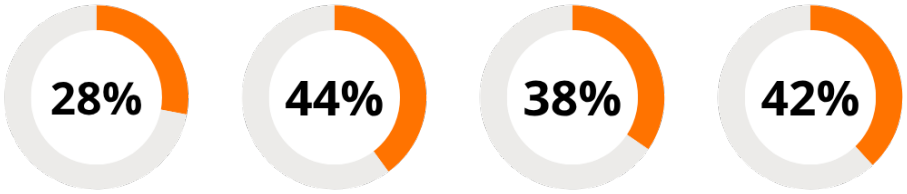
Finding 2:

Legacy Devices Are a Persistent and Underappreciated Risk

A key driver of this growing impact is the large installed base of legacy devices that cannot be patched or easily replaced.

The most difficult cybersecurity challenge facing healthcare organizations may not be the devices they are buying, but the devices they cannot replace. This finding is new to the 2026 Index. Nearly three in ten organizations operate medical devices that are past the manufacturer's end-of-support, and a significant proportion of those devices carry known, unpatched vulnerabilities.

Scale of the Legacy Device Problem



Where Legacy Devices Are Concentrated

End-of-support devices are operating in the critical clinical environments:

- General inpatient wards — 39% of organizations with legacy devices
- Emergency departments — 39%
- Outpatient and ambulatory settings — 38%
- Intensive care units — 36%
- Operating rooms and procedure suites — 33%

Why Organizations Cannot Replace Them

When asked why they continue to operate vulnerable devices, respondents identified a familiar mix of clinical, financial, and structural constraints:

- Clinical constraints — no acceptable replacement available yet (38%)
- Budget constraints — cannot afford replacement (36%)
- Regulatory or approval constraints (34%)
- Operational constraints — replacement would cause too much disruption (33%)
- Vendor has not offered an upgrade path (24%)
- Risk has been formally accepted by leadership (17%)

Despite these challenges, 67% of respondents describe themselves as "extremely" or "very" confident in their device inventory—a confidence level that may not fully account for the legacy and unpatched devices operating in their environments.

The inability to patch, combined with continued clinical reliance on vulnerable devices, creates a structural security gap that cannot be closed solely through procurement alone. This gap is almost certainly a key driver behind the rise in runtime protection adoption seen in 2026. Runtime protection technologies—which defend devices without requiring a patch—act as a compensating control for a problem that buying new devices cannot solve.

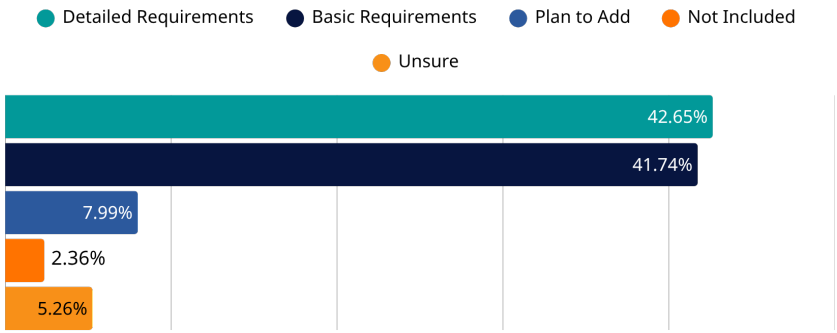
Finding 3:

Cybersecurity Has Become a Procurement Gate

In response to rising risk, healthcare organizations are changing how they evaluate and purchase medical devices.

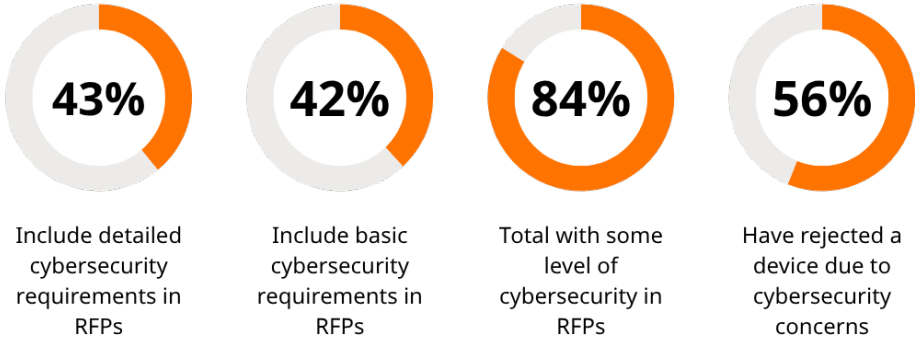
Cybersecurity is now a key consideration in medical device procurement, and the 2026 data shows the trend accelerating. Survey data shows that the overwhelming majority of healthcare organizations have integrated cybersecurity requirements into their vendor evaluation processes and that these requirements are having a measurable impact on purchasing outcomes.

Cybersecurity Is Now Standard in Device Procurement



Compared to 2025, when 83% included cybersecurity in RFPs, that figure has edged to 84% in 2026. More significantly, the depth of those requirements is growing: 43% now include detailed security specifications, up from 38% in 2025.

Cybersecurity in RFPs Is Now the Norm



Only 2.4% of respondents say cybersecurity is entirely absent from their RFP process, and nearly 8% plan to add it. This means fewer than 1 in 10 organizations are not yet including security criteria in vendor evaluations.

The Most Common Cybersecurity Requirements

When organizations specify cybersecurity requirements in purchasing processes, the most commonly requested capabilities focus on ongoing security management rather than point-in-time compliance.

- Secure software update mechanisms — required by 62% of organizations
- Secure authentication and access controls — 61%
- Third-party security testing or certification — 48%
- Runtime or exploit protection technologies — 37%
- Vendor vulnerability disclosure programs — 36%
- Software Bill of Materials (SBOM) — 31%
- Post-market patching commitments — 25%

The prevalence of secure update mechanisms and access controls as top requirements reflects organizations' growing awareness that device security requires sustained vendor engagement throughout the device lifecycle, as well as the influence of regulatory updates.

Devices Are Being Rejected on Security Grounds

The procurement filter is working and tightening. Among the 56% of organizations that have rejected a device for cybersecurity reasons—up from 46% in 2025—the most cited grounds were:

- Known vulnerabilities — 48% of those who rejected a device
- Lack of security patching support — 47%
- Weak authentication or access controls — 46%
- Poor overall vendor security practices — 42%
- Lack of SBOM or software transparency — 34%
- Unsupported or legacy operating system — 31%

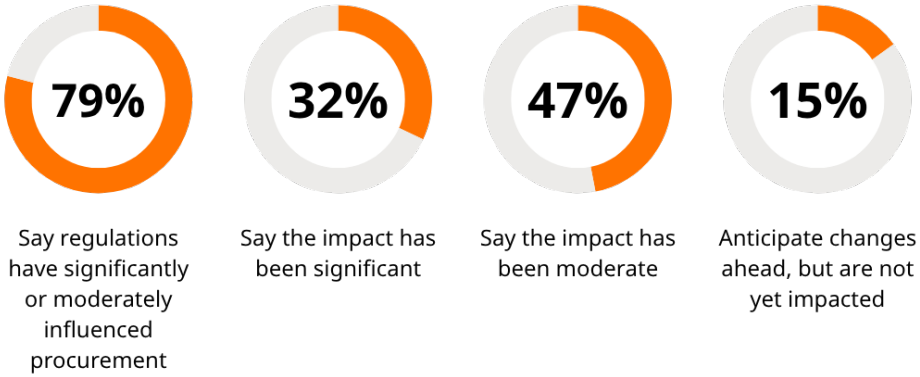
These rejection drivers map directly to the requirements organizations are embedding in their RFPs, indicating that vendors who cannot demonstrate basic security hygiene are being filtered out before purchase. The 10-point jump in device rejections since 2025 suggests this filter is now being applied more aggressively, not just more broadly.

Finding 4:

Regulation Is Reshaping Procurement

Regulatory signals from the FDA and EU are translating into operational changes at healthcare organizations. In 2025, 73% of organizations reported that FDA cybersecurity guidance or EU regulations were influencing their procurement decisions. By 2026, that figure has risen to 79%, with the share describing the impact as significantly increasing as well. The survey finds broad awareness of cybersecurity guidance and deepening behavioral change as a result.

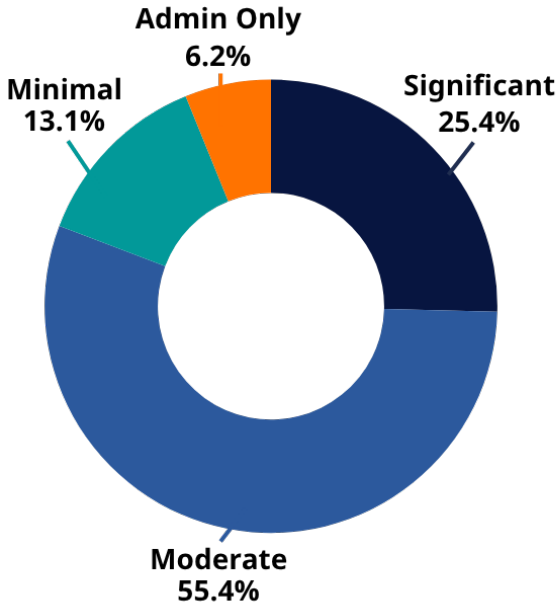
Regulatory Impact Is Widely Felt



Fewer than 3% of respondents report that regulations have had no impact on their procurement processes. This reflects a healthcare sector that is actively monitoring evolving regulatory frameworks and adjusting its vendor expectations accordingly. One of the clearest manifestations of this regulatory influence is the widespread adoption of Software Bills of Materials (SBOMs), which have quickly become a standard requirement in device evaluation.

Regulatory guidance is translating directly into purchasing requirements, effectively setting a minimum security standard for market participation. Organizations are no longer waiting for enforcement—they are operationalizing these expectations now.

Most Cyber Incidents Impact Patient Care

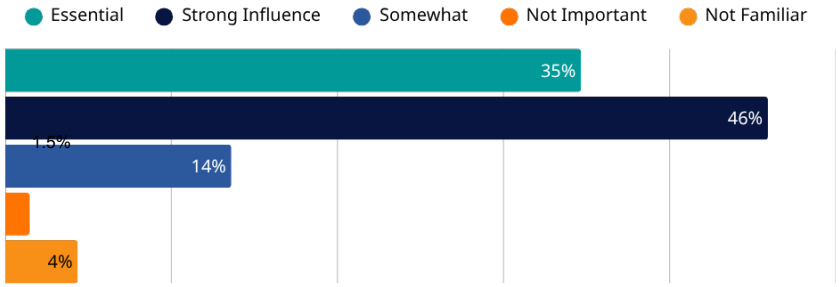


Finding 5:

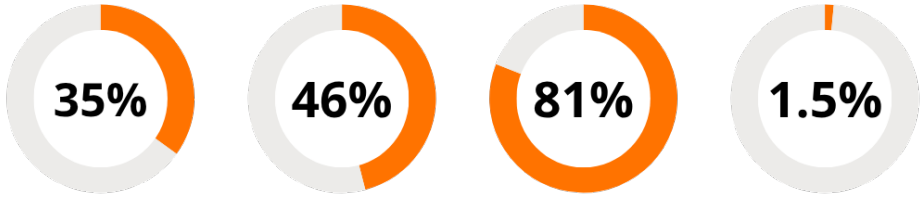
SBOM Adoption Has Reached Mainstream

Software Bills of Materials (SBOMs) have become a standard element of medical device security evaluation, and 2026 data shows the shift has hardened into a near-universal expectation. In 2025, 78% of organizations rated SBOMs as important or essential; that figure has risen to 81% in 2026. An even stronger signal of the importance of SBOMs is that 35% of buyers will not consider a device without an SBOM, a strong line in the sand.

SBOMs Are Now a Requirement for Many Buyers



SBOMs Are a De Facto Procurement Requirement



Say an SBOM is "essential" — won't consider devices without one

Say SBOMs "strongly influence"their decision

Rate SBOMs as important or essential overall

Say SBOMs are not currently important

Only 4.4% of respondents say they are unfamiliar with SBOMs, a sign that the concept has permeated beyond IT and security into clinical and procurement leadership. SBOMs are also being operationalized across procurement, security tooling, and cross-functional teams.

How SBOMs Are Being Used

Once received, SBOMs are being used across multiple organizational functions. Survey respondents noted that SBOMs are:

- Reviewed during procurement or security evaluation — 28%
- Integrated into a security or asset management tool — 26%
- Shared across teams, including IT and clinical engineering — 21%
- Stored for reference in a repository or documentation system — 18%

Fewer than 1% of respondents say their organizations do not use SBOMs in any structured way, and fewer than 3% say they do not receive them at all.

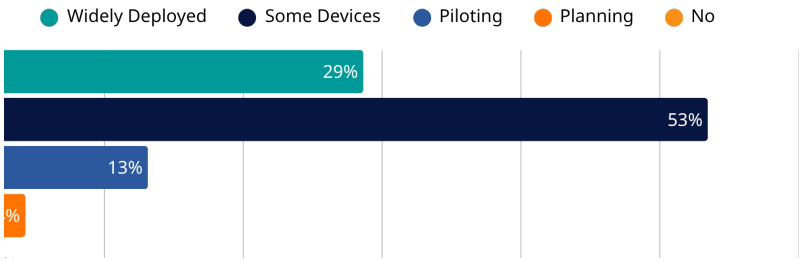
This points to a maturing SBOM ecosystem in which the artifact is requested and then operationalized. SBOMs have transitioned from a best practice to a baseline requirement, and vendors that cannot provide software transparency risk disqualification early in the evaluation process.

For device manufacturers, SBOMs are no longer optional. An organization that rates SBOMs as "essential" will not evaluate devices lacking one. With 35% of healthcare purchasers holding this position, vendors without SBOM capabilities are disqualifying themselves from a substantial portion of the market.

Finding 6:

Runtime Protection Is Gaining Traction

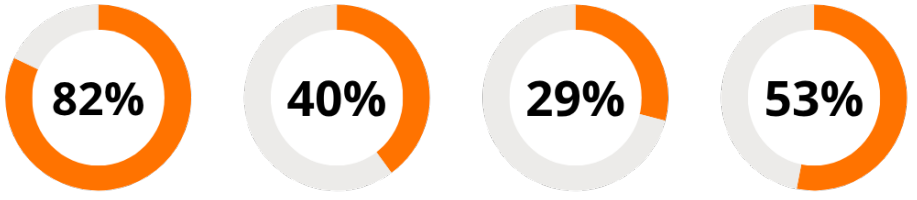
Runtime Protection Is Widely Adopted or Emerging



As organizations confront the reality that many devices cannot be patched, runtime protection technologies are emerging as a critical compensating control.

In 2025, 36% of organizations actively sought devices with runtime protections in procurement, and another 38% were aware of the technology but had not yet required it. The 2026 survey asked respondents about their deployment of these protections, and 82% of organizations report having deployed runtime exploit protection or actively piloting it. The awareness in procurement and the levels of real-world deployment point to the compounding pressure of unpatchable legacy devices and rising attack frequency.

Runtime Protection Deployment and Awareness



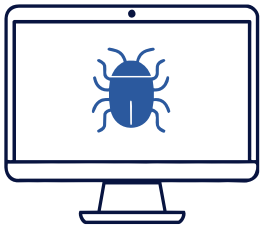
Have widely deployed or are piloting runtime exploit protection

Actively seek devices with runtime protection capabilities

Have widely deployed runtime exploit protection

Have deployed on some devices (partial)

Only 0.5% of respondents who are aware of runtime protection have no plans to use it. Among those unfamiliar with the technology, 16% have heard of it but do not fully understand it, representing an education opportunity for vendors and security teams.



82%

of organizations report having deployed runtime exploit protection or actively piloting it.

Monitoring Capabilities

Organizations are deploying a range of monitoring tools to track device security posture:

- Network monitoring for medical devices — used by 53%
- Vendor security monitoring tools — 44%
- Manual monitoring processes — 41%
- Asset inventory for connected devices — 40%
- Runtime or exploit protection — 38%
- Dedicated OT security platform — 37%

Confidence in detection does not always reflect actual capability. Organizations operating devices with known vulnerabilities, running unsupported operating systems, and without complete device inventories may be overestimating their ability to detect and respond to incidents in those specific device categories.

Confidence in Detection and Response

Organizations express slightly higher confidence in their detection and response capabilities than they did a year ago. In 2025, 17% felt “extremely” confident in their ability to detect and contain attacks on medical devices. In 2026, 22% say they are “extremely confident.”

However, 7% describe themselves as “slightly” or “not at all” confident—a non-trivial proportion given the stakes—and the gap between reported confidence and actual capability warrants scrutiny, especially for organizations still operating unpatched legacy devices.

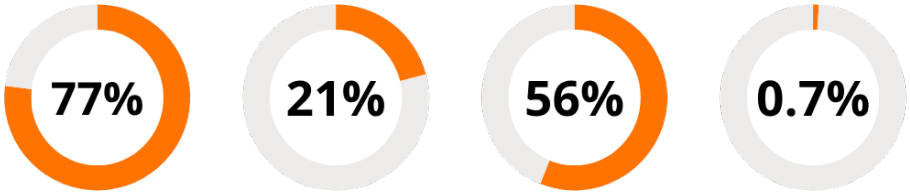
Finding 7:

Investment Is Rising—And AI Devices Add New Concerns

Healthcare organizations are continuing to strengthen their approach to medical device cybersecurity, backed by sustained investment and a growing willingness to prioritize security in purchasing decisions. At the same time, emerging technologies—particularly AI-enabled devices—are introducing new risks that organizations are not yet fully equipped to manage.

Cybersecurity Budgets Are Growing

Organizations are reinforcing their cybersecurity efforts with sustained investment. Budget signals indicate that medical device and operational technology (OT) security are now treated as ongoing strategic priorities rather than one-time initiatives. In 2025, 75% of organizations increased their medical device and OT security budgets. In 2026, that figure has risen to 77%, with 21% reporting a significant increase. The vast majority of surveyed organizations have continued or accelerated their investment:



Only 22.5% of organizations saw no change in security resources, and less than 1% reduced investment. This marks the second consecutive year of strong investment growth, suggesting that healthcare leadership has made device cybersecurity a permanent line item.

Willingness to Pay for Security Features

This investment is also reflected in purchasing behavior. Healthcare organizations are increasingly willing to pay a premium for devices with stronger built-in security capabilities. A majority of respondents (76%) indicate willingness to pay more for advanced cybersecurity protections:

- Would pay 5–15% more for advanced security features — 38% of respondents
- Would pay up to 5% more — 27%
- Would pay 15% or more — 11%
- Believe protections should be included at no additional cost — 11%
- Do not consider advanced security a priority — 2%

Only a small minority believes these protections should come at no additional cost or are not a priority. Together, these responses signal a market that actively values security and rewards manufacturers that invest in it.

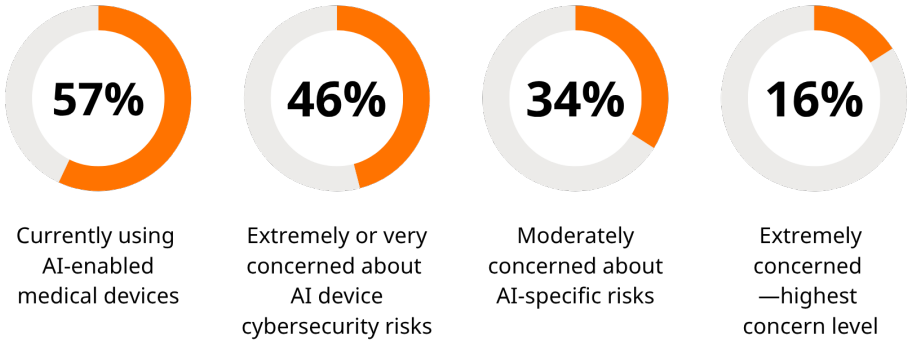
With 76% of purchasing decision-makers willing to pay a premium for built-in security—compared to 79% in 2025—the market is sending a clear and sustained signal.

The dip may reflect maturing expectations: buyers who once paid up simply to get any security are now expecting more rigor for that premium. Manufacturers who invest in cybersecurity not only reduce liability, but they also gain a genuine competitive advantage in an increasingly discerning market.

AI-Enabled Devices Introduce New Risk Dimensions

However, not all areas are keeping pace with this growing security maturity. AI-enabled and AI-assisted medical devices are being adopted rapidly, introducing a new and still poorly understood layer of cybersecurity risk.

More than half of surveyed organizations (57%) are already using AI-enabled or AI-assisted medical devices or clinical systems. This rapid adoption is outpacing confidence in understanding the associated cybersecurity risks.



The gap between AI adoption (57%) and high concern levels (46%) suggests that many organizations are deploying AI-assisted clinical tools without a clear understanding of the cybersecurity implications. This pattern mirrors what the 2025 data showed about connected devices more broadly—rapid adoption outpacing security readiness. The industry appears to be entering a second version of that same curve, this time with AI.

As AI-driven diagnostics and decision support become standard, the attack surface they create—including model manipulation, data poisoning, and adversarial inputs—will demand specific procurement and monitoring frameworks that most organizations have not yet developed.

While investment and security maturity are increasing, new technologies such as AI are expanding the attack surface faster than organizations can secure it. Without dedicated frameworks, this gap is likely to widen.

Implications and Recommendations

The 2026 findings highlight a clear disconnect. Healthcare organizations are making measurable progress in procurement rigor, SBOM adoption, budget allocation, and runtime protection deployment, yet the outcomes remain difficult to improve. Cyberattacks are becoming more frequent, the impact on patient care is worsening, and legacy device exposure persists in critical environments. The data suggests that while organizations are strengthening how they buy and secure devices, the underlying sources of risk—unpatchable systems, expanding connectivity, and emerging technologies—are not being reduced at the same pace.

The following recommendations are informed by where the two years of data show genuine movement, and where the gaps are widening despite investment.

For Healthcare Organizations

For healthcare organizations, the priority is to extend cybersecurity beyond procurement into active risk reduction across the installed base.

Formalize cybersecurity requirements across all device categories

With 84% of organizations already including some cybersecurity criteria in RFPs—up from 83% in 2025—the opportunity is to move from basic to detailed requirements. The 43% who already include detailed requirements (up from 38%) are the model: demanding SBOMs, runtime protection capabilities, post-market patching commitments, and vendor vulnerability disclosure programs as standard terms rather than optional add-ons.

Address the legacy device gap with compensating controls

For devices that cannot be patched or replaced, runtime exploit protection is a viable compensating control available today, and the market has recognized this. 53% of organizations have deployed runtime exploit protection on some devices, with 29% widely deploying the technology. Organizations operating devices with known vulnerabilities in high-acuity settings that have not yet deployed these technologies are falling behind.

Build an accurate, complete device inventory

67% of respondents are “extremely” or “very” confident in their device inventory, but given the prevalence of unpatched and legacy devices also reported, that confidence may be misplaced in some environments. A verified, continuously updated inventory is the foundation of any effective device security program.

Develop AI-specific cybersecurity frameworks

As AI-assisted clinical tools proliferate, procurement teams should be developing specific security evaluation criteria for these devices, including model transparency, adversarial input testing, and post-deployment monitoring requirements.

For Medical Device Manufacturers

For medical device manufacturers, cybersecurity is a prerequisite for market access and a driver of competitive advantage.

Treat SBOM as a baseline, not a differentiator

With 35% of purchasing decision-makers saying they will not consider devices without an SBOM, this is now a minimum viable requirement for market access, not a competitive advantage. The trajectory from 2025 to 2026 suggests this proportion will only grow. Manufacturers who do not provide SBOMs are filtering themselves out of an expanding share of the market.

Build runtime protection into device architecture

53% of organizations have deployed runtime exploit protection on at least some devices. Manufacturers who embed these capabilities at the hardware and firmware levels can address the legacy device problem for their installed base while meeting the procurement requirements of new customers.

Invest in post-market security commitments

Patching commitments and vulnerability disclosure programs are among the most cited cybersecurity requirements in vendor RFPs. Manufacturers with formal, documented post-market security support processes will have a measurable advantage in procurement evaluations.

Engage IT and cybersecurity stakeholders directly

With IT and cybersecurity teams now formally involved in device purchasing at most organizations—a trend that has accelerated alongside rising cyberattack frequency and regulatory requirements since 2025—sales and clinical specialist engagement alone is not sufficient. Device manufacturers should ensure their security teams, documentation, and capabilities are accessible to the technical evaluators who are now at the procurement table and whose influence is growing year over year.

For the Industry (or Regulators & Ecosystem)

For the broader healthcare ecosystem, including regulators and policymakers, the findings underscore the need to address systemic risk factors that procurement alone cannot solve. This includes accelerating the development of frameworks for legacy device security, clarifying expectations for AI-enabled systems, and aligning incentives for long-term device support and lifecycle security.

Ultimately, the industry has made meaningful progress in how it evaluates and purchases secure devices, but exposure to cyber risk remains rooted in factors that extend beyond procurement. Closing this gap will require not only continued investment and stronger requirements for new devices, but also practical strategies to secure the systems already in use and to anticipate the risks introduced by emerging technologies such as AI.

Conclusion

Healthcare has operationalized medical device cybersecurity, but the threat landscape is advancing faster than the controls designed to stop it.

The 2026 data tells two stories simultaneously. The first is a story of genuine progress. Procurement requirements are stricter, SBOM adoption has reached a tipping point, budgets have grown for the second consecutive year, and runtime protection has moved from a niche capability to mainstream deployment in a single year.

The second story is harder. Attacks on medical devices are more frequent than they were twelve months ago, the impact on patient care when incidents occur has worsened, and a quarter of organizations are operating devices with known, unpatched vulnerabilities in their most critical care settings—emergency departments, ICUs, and operating rooms. AI-enabled devices are being adopted faster than security frameworks can keep pace, tracing a curve the industry has seen before with connected devices and has not yet learned to get ahead of.

The lesson of the past year is not that investment and attention are failing but that the risk is moving at least as fast as the response. Closing that gap will require more than procurement rigor and budget growth. It will require security built into devices before they reach clinical environments, as well as the ability to protect devices already in place that cannot be replaced. That is where the industry's work remains.

RUNSAFE SECURITY

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security protects embedded software across critical infrastructure, delivering automated vulnerability identification and software hardening from build-time to runtime to defend the software supply chain and critical systems without compromising performance or requiring code rewrites. The RunSafe Security Platform includes the authoritative build-time SBOM generator fo embedded systems and C/C++ projects, automated vulnerability identification and risk quantification, license compliance, and patented memory relocation techniques to mitigate memory-based vulnerabilities.

Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace and defense, energy, operational technology, industrial automation, transportation and automotive, medical device, and high-tech manufacturing verticals.

RunSafeSecurity.com

571.441.5076

Sales@RunSafeSecurity.com

Methodology and Survey Notes

This report is based on data collected via the Pollfish online survey platform in March 2026. All 551 respondents confirmed involvement in medical device purchasing decisions at their healthcare organizations prior to completing the survey. Respondents who selected "No" to the qualifying question were excluded from the analysis.

Respondents represented a range of organizational roles, including clinical leadership (37%), IT and cybersecurity (23%), procurement and supply chain (15%), executive leadership (14%), clinical and biomedical engineering (5%), and other roles (6%). Facility sizes ranged from under 100 beds to 500+, providing representation across small community hospitals and large health systems.

Certain questions used branching logic. Questions 21–25 (incident characteristics) were only presented to the 130 respondents who confirmed their organization had experienced a cyberattack or exploited vulnerability. Question 27 (runtime protection deployment) was presented to the 419 respondents who confirmed awareness of runtime protection technologies. Question 31 (legacy OS percentage) was presented to the 220 respondents who confirmed operating end-of-support devices.

Percentages may not sum to exactly 100% due to rounding. For multiple-selection questions, respondent percentages will exceed 100% as individuals could select more than one answer.

Looking for last year's data? Read the 2025 Medical Device Cybersecurity Index.