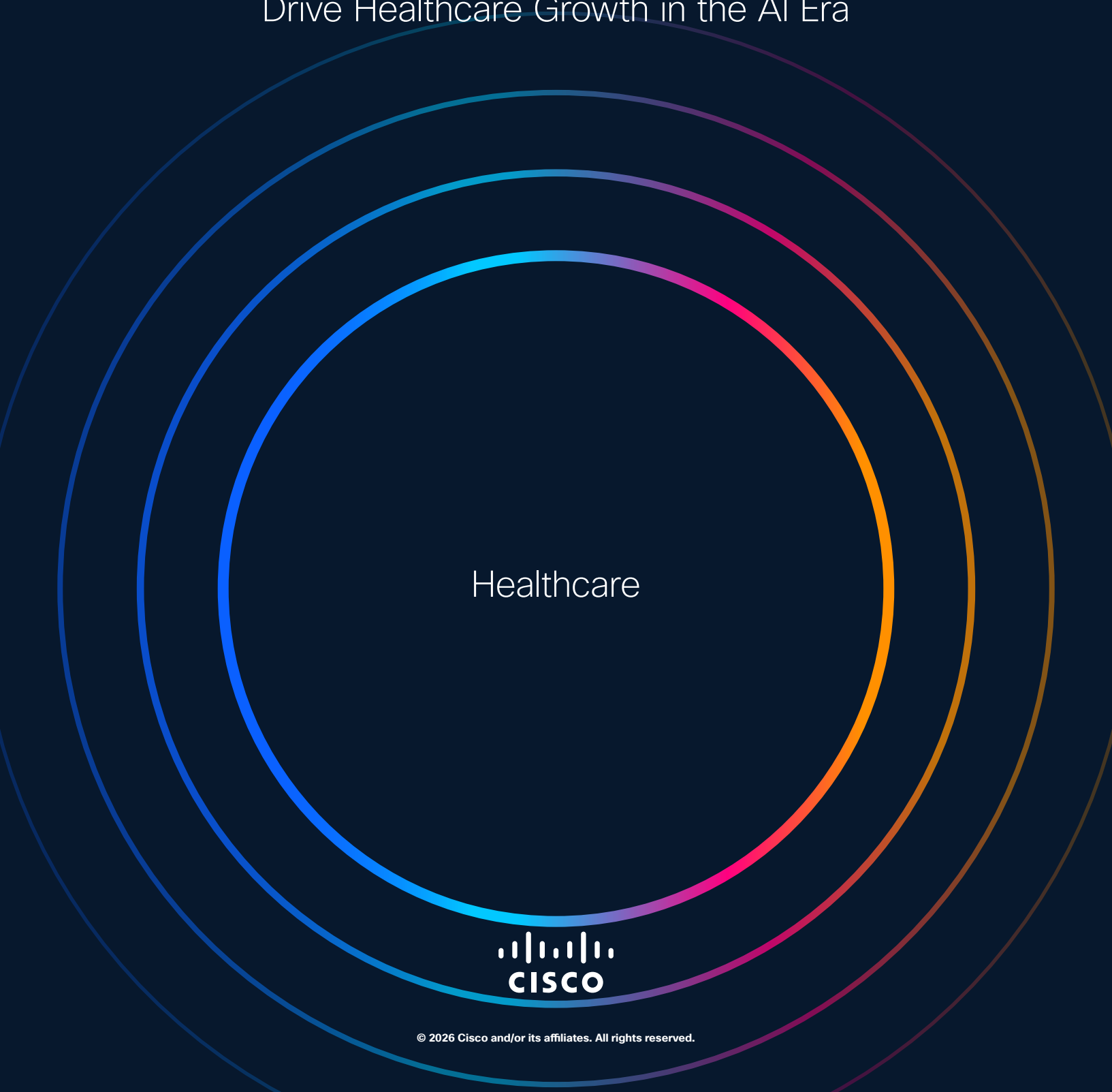
State of Wireless 2026

Unlocking the Multiplier Effect: How Strategic Investments Drive Healthcare Growth in the AI Era



Executive summary

Wireless has evolved from a convenience in healthcare settings to a mission-critical infrastructure investment. Modern care facilities rely on robust, resilient networks to deliver patient care and protect sensitive health information.

The stakes are exceptionally high: disruptions to hospital networks can delay procedures, affect patient monitoring, and undermine care quality, while security breaches expose protected health information, violate regulatory mandates, and erode patient trust. In modern healthcare environments, network infrastructure is one critical layer within a broader system of safeguards, making resilience and security essential to supporting clinical operations.

Healthcare organizations recognize this imperative: more than three-quarters of organizations report operational efficiency gains (78%), see employee productivity gains (74%), and report enhanced customer engagement (74%). For an industry under constant pressure from the need to deliver exceptional care outcomes, staffing shortages and regulatory demands, wireless is increasingly the foundation on which clinical and operational excellence rest.

Yet healthcare leaders face a paradox that is both opportunity and threat. Wireless is essential for deploying artificial intelligence applications that can deliver huge leaps in diagnostic capabilities, helping accelerate treatment decisions. However, these same AI capabilities introduce unprecedented complexity, create new security vulnerabilities, and intensify competition for specialized talent. Healthcare organizations need advanced wireless skills precisely when attracting talent to this domain has become more difficult.

This report explores this paradox within healthcare. It examines how healthcare systems can harness strategic wireless investments to unlock a multiplier effect, delivering measurable returns across clinical and operational workflows and financial performance. It also identifies the three interconnected barriers that currently prevent many healthcare organizations from realizing the full potential of their wireless infrastructure: mounting operational complexity; escalating security threats; and acute talent shortages. Organizations able to address all three barriers simultaneously achieve substantially higher returns while those that address only one or two remain trapped in reactive cycles and are less able to modernize.

This report is grounded in Wi-Fi as the primary enterprise connectivity layer, while examining the broader wireless ecosystem it enables, including AI-driven applications, IoT and OT environments, and emerging enterprise use cases.

The opportunity:
Wi-Fi as a strategic growth engine for healthcare

Healthcare spending on wireless infrastructure continues to accelerate. Organizations have invested heavily in wireless over the past five years, recognizing that reliable connectivity supports the infrastructure necessary for healthcare providers to pursue better patient outcomes and operational efficiency. Looking ahead, the momentum intensifies.

While more than a quarter (28%) of healthcare organizations report budget increases of more than 50% over the past four to five years, an even more substantial 34% expect budget increases exceeding 50% over the next four to five years. This represents one of the highest anticipated investment increases across all industries surveyed.

This investment is not speculative; healthcare leaders see wireless as essential to modern medicine. Real-time patient monitoring relies on seamless connectivity across wards and remote care, while telemedicine expands access and reduces travel. Clinicians use mobile devices for bedside records, imaging, and medication histories, increasing patient time. IoT sensors track equipment, monitor environments, and flag failures before care is disrupted.

Emerging uses reinforce wireless as strategic growth infrastructure. Hospitals deploy autonomous robots to transport supplies, smart building systems optimize conditions for patients, and space analytics use wireless-enabled cameras to improve flow and reduce

waiting times. These applications depend entirely on reliable connectivity, underscoring wireless as the backbone of modern healthcare.

For healthcare, wireless modernization directly translates to business impact. Healthcare organizations report that 78% see improvements in operational efficiency, 74% report employee productivity gains, and 74% see improved patient engagement from wireless investments. When healthcare providers prioritize wireless strategically, aligning investments with clinical priorities and operational goals, they achieve a multiplier effect: one investment in modern wireless infrastructure yields measurable returns across multiple dimensions simultaneously including faster patient throughput, higher staff satisfaction, supporting healthcare organizations in their initiatives to improve clinical quality, and stronger financial outcomes.

Infrastructure modernization is accelerating this effect. Healthcare leaders understand that aging wireless standards like Wi-Fi 5 cannot support the density of devices, bandwidth demands, and latency requirements of contemporary care delivery. 15% of healthcare organizations have deployed Wi-Fi 6E, with a further 30% planning rollouts in the next 12 months, illustrating their understanding of how the 6 GHz spectrum can provide clean bandwidth for telemedicine systems. In turn this enables high-bandwidth streaming of surgical footage and diagnostic imaging, and supports the proliferation of IoT sensors and smart devices. Organizations deploying 6 GHz spectrum show measurably higher rates of AI application deployment compared to non-adopters, suggesting that advanced wireless infrastructure is a prerequisite for modern clinical innovation.

Healthcare organizations are leveraging wireless across a variety of use cases

	Currently deployed (%)	Planning to deploy (%)
Autonomous systems and robotics	46%	49%
Immersive collaboration and training	51%	46%
Space Analytics and optimization (footfall traffic, etc.)	49%	45%
Indoor Wayfinding	49%	45%
High-definition streaming	51%	44%
Smart facilities and energy management	54%	44%
Supply chain and inventory intelligence	54%	43%
AI applications and workloads	55%	43%
Operational visibility and flow analytics	56%	42%
Internet of Things	57%	41%
Customer and user experience enhancement	59%	40%
Guest wireless	59%	39%
Remote worker connectivity	60%	38%
Real-time asset and equipment tracking	60%	38%
Physical Security (CCTV)	62%	36%

Current footprint = Deployed + Pilot stage
Future expansion = Planned next year + Planned in next 2–5 years

The wireless AI paradox in healthcare

Healthcare leaders face a central strategic tension that defines the wireless opportunity in 2026 and beyond. Artificial intelligence is simultaneously the leading driver of wireless return on investment and the primary source of escalating challenges that constrain that return.

On one hand, organizations deploying AI applications recognize wireless as strategically critical to clinical delivery. More than 62% of leaders whose organizations are deploying AI view wireless as strategically critical, compared to 46% of organizations not deploying AI. This heightened recognition reflects reality:

- AI workloads demand higher performing, more resilient wireless networks than traditional applications.
- AI-enabled applications for clinical workflows require rapid access to large medical imaging databases. Clinical decision support tools need real-time connection to patient records.
- Automated systems for identifying equipment failures, supporting the monitoring of patient data trends, or optimizing staff scheduling all depend on reliable, low-latency connectivity. These AI-driven solutions serve as operational workflow tools designed to assist clinicians and staff in their daily operations.*

Healthcare organizations that integrate wireless optimization into their AI deployment strategies realize substantially stronger returns with more than 63% of healthcare organizations deploying AI report positive impacts from wireless investments on revenue. This performance exceeds organizations with no AI deployment by meaningful margins, demonstrating that AI and wireless are mutually reinforcing investments.

On the other hand, AI is simultaneously amplifying the very challenges that prevent healthcare organizations from realizing wireless potential. The same AI technologies that enable clinical innovation are also creating operational

* Please note that these tools are intended to augment, not replace, professional clinical judgment, and they should not be relied upon as the sole source of information in their for clinical or operational decision-making.

complexity for almost every (98%) healthcare organization with new security threats and intensified competition for talent preventing them from achieving the full benefit of wireless modernization.

This paradox is especially acute in healthcare because the consequences of failure are exceptionally high. A security breach in healthcare does not simply compromise data. It disrupts patient care delivery, violates HIPAA and other privacy regulations, triggers substantial regulatory penalties, and destroys patient trust in the organization and the caregivers who work there.[1]

An operational failure that slows network response times does not simply reduce productivity: it can delay diagnosis, postpone treatment, or compromise monitoring of critically ill patients. The financial, regulatory, and human stakes make the wireless AI paradox one of the most pressing strategic challenges healthcare leaders face.

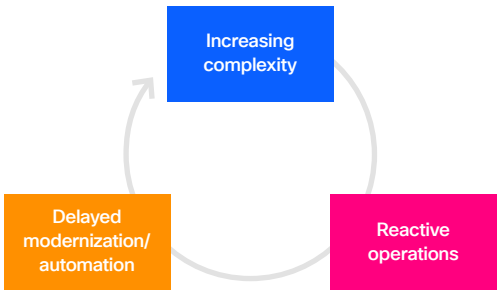
Barrier 1: Operational complexity overwhelms current capabilities

Nearly every healthcare wireless leader reports that operational complexity is escalating, representing not just a challenge but a structural transformation of the operational landscape.

Healthcare organizations cite three main drivers of rising complexity, with security risks ranking highest for 42% of respondents. Expanded attack surfaces from IoT devices, remote care platforms, and AI systems heighten vulnerability. Close behind are mission critical IT, IoT, and OT workloads; from patient monitors that must never lose connectivity, to robotic surgical systems requiring deterministic performance, to AI diagnostics needing real time imaging access. Finally, growing bandwidth demands add pressure, as video consultations, remote patient monitoring, and high definition surgical streaming strain older wireless infrastructure.

This complexity manifests in tangible operational strain. 38% of healthcare organizations report that their wireless support teams receive at least 50 tickets per week on average. This ticket volume means that IT teams spend hundreds of hours monthly managing wireless issues rather than implementing strategic improvements. The situation worsens when examining how that time is spent. More than 53% of healthcare wireless teams spend most of their time on reactive troubleshooting and incident management, addressing urgent problems as they arise rather than preventing problems through proactive planning and optimization.

This reactive posture creates a self-reinforcing cycle. Complexity drives reactive work. Reactive work demands all available resources and attention. Strategic work, including modernization, training, and certification programs, gets deferred. As modernization delays, complexity persists and often increases. Teams remain trapped, unable to escape the reactive treadmill.



A critical factor amplifying this challenge is the pervasive lack of visibility. 90% of healthcare organizations report visibility gaps that impair their ability to troubleshoot Wi-Fi issues effectively. The most frequently reported visibility challenges in healthcare are poor client visibility followed by poor application poor packet visibility. Without clear sight into network behavior at each layer, from access point to application, healthcare IT teams cannot rapidly isolate problems.

This visibility gap creates a particularly dangerous dynamic in healthcare settings. Wireless networks become scapegoats for problems originating elsewhere. A patient deteriorates. A clinician attempts to access the monitor reading and suspects the network is slow. IT teams spend hours – our research shows an average of 18 – investigating wireless performance, only to discover the problem was a malfunctioning sensor or a database query timeout. More than 60% of healthcare respondents report that at least 10% of incidents are inaccurately attributed to wireless. Those wasted troubleshooting hours translate directly into delayed attention to actual problems.

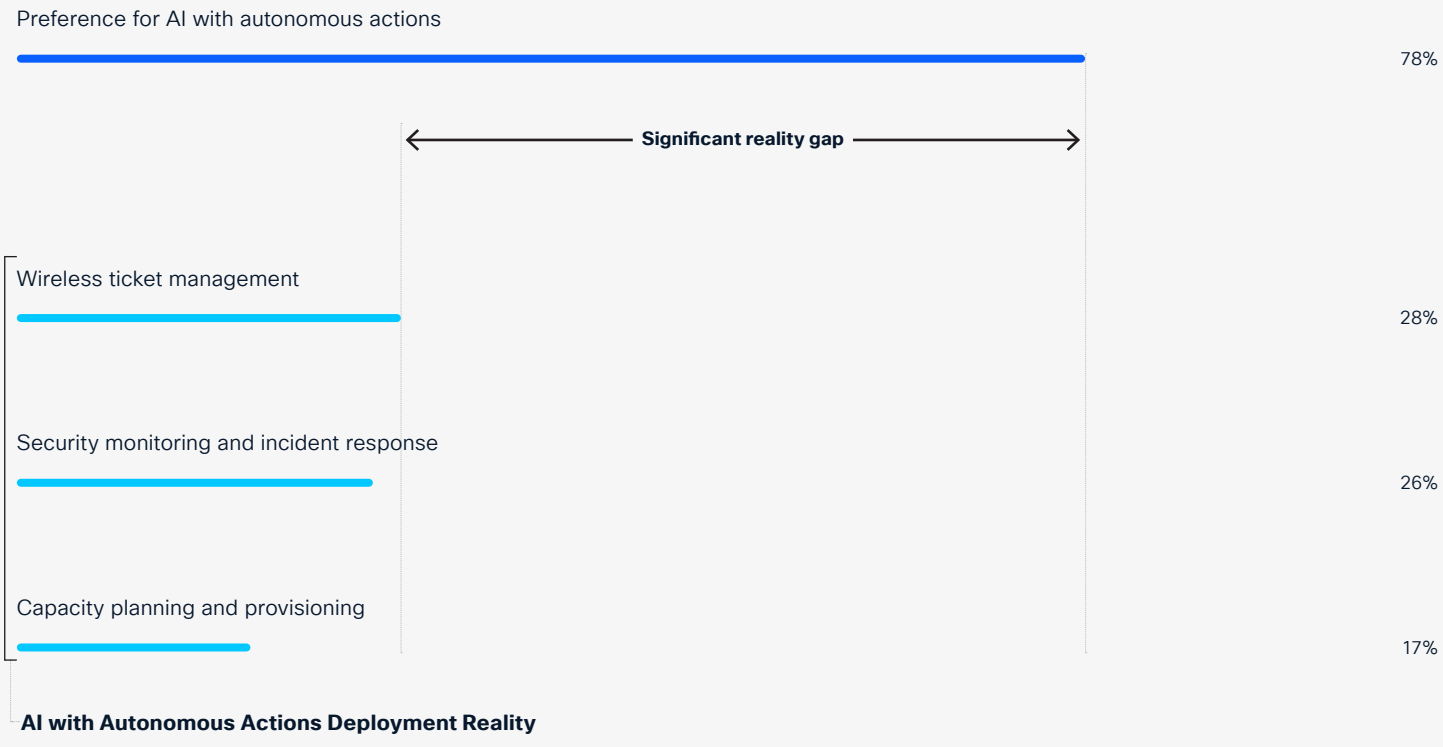
1. Cisco provides security solutions that support organizations in meeting their HIPAA compliance obligations. The ultimate responsibility for maintaining a HIPAA-compliant environment rests with the healthcare organization.

In response to this escalating complexity, healthcare wireless leaders overwhelmingly believe that AI represents the most promising path forward. More than 7 in 10 (78%) would prefer AI with automation to fully or mostly handle routine wireless operational tasks. The appeal is obvious – automation would free clinically-focused IT professionals to work on strategic priorities rather than handling repetitive ticket work. AI systems could detect and resolve many incidents before humans become aware problems exist.

Yet a significant gap separates preference from reality: only 28% of healthcare organizations have implemented automation for wireless ticket management, 26% automate security monitoring and incident response and just 17% have deployed automation for capacity planning and provisioning. Healthcare leaders recognize the solution but lack the resources, expertise, or organizational readiness to implement at scale.

The impact on healthcare performance is measurable. Organizations that have implemented high-level AI with autonomous actions report dramatic time savings, freeing an average of three hours 20 minutes per person per day. These organizations are four times more likely to rate their network operations as very simple. They resolve wireless tickets 12% faster than manual operations. Scaling these benefits across all healthcare organizations would translate into thousands of hours freed for patient care each month. Yet that scaling remains constrained by the very complexity and talent shortages that AIOps implementation would help resolve.

The AI gap in healthcare: Desire versus reality



Barrier 2: Wireless security under siege

Healthcare faces intensifying security threats that are more frequent, more damaging, and more difficult to detect and remedy than in previous years. 87% of healthcare organizations have experienced at least one wireless security incident in the past 12 months, and 43% report escalating wireless threats over the past two years. These organizations expect the situation to deteriorate further, with 70% anticipating increased wireless security incidents over the next two years.

Healthcare security threat environment

The threat landscape in healthcare is distinctive, and alarming. Our research revealed six areas contributing to increased security vulnerability:

1. AI-generated or automated cyberattacks rank as the leading driver of increased wireless security threats. These have the ability to identify network vulnerabilities, adapt attack strategies in real time based on defensive responses, and operate at a scale and speed far exceeding human capabilities
2. Remote and hybrid work models have expanded the attack surface, creating unmanaged endpoints beyond the traditional hospital network perimeter
3. Increased use of IoT and connected devices creates proliferating vulnerabilities, as individual device weaknesses compound into network-wide exposure
4. Budget constraints limit security improvements
5. Staffing shortages reduce the bandwidth available for security monitoring and response
6. Legacy infrastructure and protocols create persistent vulnerabilities that cannot be remediated without expensive replacement

For healthcare, the implications of compromised IoT or OT devices are especially severe. 32% of affected organizations report disruption from compromised IoT or OT devices. In a hospital, this means a vital sign monitor becomes unreliable, a medication pump malfunction goes undetected, a surgical robot loses safe communication with its operator, or a diagnostic imaging system becomes corrupted. These are not abstract IT problems; they are patient safety events.

The financial impact is staggering. More than half (58%) of healthcare organizations have experienced financial losses from wireless security incidents. More than half (53%) report losses exceeding US$1 million in the past year. These losses compound through multiple channels. Direct losses include breach remediation, forensic investigation, and incident response costs. Indirect losses include loss of patient trust (40%), regulatory penalties or compliance consequences (35%), and reputational damage. For healthcare, patient trust is irreplaceable and, once lost, it is extraordinarily difficult to rebuild and our research revealed 40% of organizations have already lost that trust.

79% of healthcare organizations report that they are doing enough to protect wireless networks, yet 70% expect security failures to increase over the next two years. This paradox reflects a gap between executive perception and frontline reality: executives perceive their organizations as adequately protected. Technical staff managing networks directly understand the actual threat environment and the limitations of current defenses.

Financial losses from wireless security incidents in healthcare

Less than US$1 million	24%
US$1-10 million	27%
US$10-50 million	18%
Over US$50 million	8%

Organizations cite three primary barriers to improving wireless security: implementation complexity, legacy infrastructure, and performance concerns. These barriers do not exist in isolation and reflect the broader wireless challenges that healthcare faces:

- Operational complexity makes security implementation difficult
- Talent shortages mean organizations lack the specialized expertise needed to deploy modern security protocols
- Visibility gaps prevent security teams from understanding the actual threat environment

The result is a widening vulnerability gap which means that even as threats escalate, healthcare organizations remain constrained by outdated systems, complexity, and talent limitations, slowing security modernization and eroding resilience.

Barrier 3: Wireless competition for AI skills

Healthcare faces an acute talent crisis that directly inhibits modernization and exacerbates both complexity and security challenges. 88% percent of healthcare organizations report difficulty hiring wireless professionals with the skills required for modern network operations. This is not a minor hiring challenge; this is a structural problem affecting the sector's ability to maintain and modernize network infrastructure.

The talent competition is fierce and asymmetrical. AI and machine learning rank as the number one domain attracting IT talent away from wireless, with 52% of healthcare organizations identifying this as a primary competitor for staff. Cybersecurity follows in second place, reflecting the high visibility and rapid career growth in that field. Software engineering and app development also pull skilled professionals away from wireless. Healthcare organizations lose their best wireless talent to roles perceived as more innovative, better compensated, and more aligned with organizational priorities.

Healthcare talent competition and hiring challenges

Domains attracting talent away from wireless

AI / Machine learning	52%
Cybersecurity	44%
Software engineering/app development	38%

Primary reasons for difficulty in hiring wireless talent

Shortage of candidates with advanced wireless or AI-integrated skills	53%
Internal budget constraints or hiring freezes	38%
Geographic limitations or remote work challenges	35%

The root cause is straightforward. A shortage of candidates with advanced wireless or AI-integrated skills ranks as the primary barrier to hiring wireless talent. There simply are not enough people with deep wireless expertise in the labor market. Making matters worse, internal budget constraints and hiring freezes further limit recruitment. The result is a skills gap that translates into higher operating costs, lower morale among wireless teams, and reduced capacity for innovation.

The correlation between talent shortages and poor outcomes is unmistakable. 50% of organizations facing extreme difficulty in hiring spend significantly more time on reactive troubleshooting compared to 37% of those facing no hiring difficulty. The impact extends far beyond operational burden: 65% of organizations struggling to hire wireless specialists expect wireless security failures to increase at substantially higher rates compared to 59% of those facing no difficulty.

The implication is clear. Organizations that invest early in talent development and certification gain competitive advantage as complexity increases and specialized skills become more valuable. Those that delay investment until talent shortages become acute face substantially larger hiring costs, longer project timelines, and reduced capacity to modernize. In healthcare, where the cost of delayed modernization includes both financial losses from security incidents and the immeasurable cost of compromised patient care, this investment becomes mission critical.

Conclusion

Healthcare organizations face a paradox that is among the most consequential strategic challenges in the industry. Wireless is essential to modern clinical delivery and operational excellence. AI-driven applications promise to improve diagnostics, accelerate treatment decisions, and optimize workflows. Yet realizing this potential requires healthcare leaders to address three deeply interconnected barriers simultaneously.

Operational complexity traps teams in reactive cycles, preventing modernization. Security threats escalate faster than healthcare organizations can deploy defenses. Talent shortages amplify both challenges while constraining the resources available to address them. Attacking one barrier without addressing the others leaves the fundamental paradox intact. A healthcare system that modernizes infrastructure without implementing automation continues to drown in reactive work. A system that implements automation without deploying modern security efficiently manages vulnerable networks. A system that modernizes security without building certified expertise deploys protections that teams cannot properly implement or maintain.

Yet healthcare organizations that address all three barriers simultaneously achieve substantially higher returns on wireless investments. They experience stronger improvements in operational efficiency, faster patient throughput, lower security incident costs, and improved employee satisfaction. The multiplier effect compounds when all dimensions are aligned: modern infrastructure enables innovation; automation frees teams to execute modernization; strong security protects patient data and organizational trust; and certified talent ensures sustainable operations.

The financial case is compelling. Healthcare organizations deploying modern wireless infrastructure, automation, security protocols, and certified talent are substantially more likely to achieve strong wireless ROI. They experience lower security incident costs, they resolve operational issues faster and support the infrastructure that enables healthcare providers to pursue better patient outcomes.

The window for competitive advantage is now. Healthcare organizations that act decisively and holistically in 2026 will establish wireless as the strategic foundation of clinical excellence for the next decade. Those that delay will find themselves trapped in reactive cycles, struggling with escalating security incident costs, and unable to capitalize on AI-driven transformation while competitors advance.

Methodology

This research comprised interviews with 6,098 organizations, including 441 in healthcare, across 30 markets. It was conducted in November 2025 by Sandpiper Research and Insights.

Research Scope

Respondent Profile: Interviews were conducted with 6,098 wireless decision makers and technical specialists in organizations with at least 250 employees. Six in 10 (61%) respondents work in organizations with annual turnover of at least US$100 million.

Americas — 22%

Europe, Middle East, and Africa — 28%

Asia Pacific — 50%

Geographic Coverage: Research covered 30 markets including Australia, Brazil, Canada, Chinese Mainland, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, United Arab Emirates, United Kingdom, United States, and Vietnam.

Industry Representation: Respondents worked across a range of industries including Business Services, Construction, Education, Engineering, Design and Architecture, Financial Services, Government and Public Services, Healthcare, Manufacturing, Media and Communications, Natural Resources, Real Estate, Restaurant Services, Retail, Technology Services, Transportation, Travel Services, and Wholesaling.

Timing: Research was conducted in November 2025.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**