

State of Wireless 2026

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



Contents

3	Executive summary
5	The opportunity: Wi-Fi as a strategic growth engine
5	Investment momentum continues to accelerate as the benefits are realized
8	Expanding use cases drive new infrastructure requirements
10	The multiplier effect: Wi-Fi drives measurable business value across multiple areas
11	Infrastructure at a crossroads: Bridging the Wi-Fi performance gap
13	Wireless strategy in a perfect storm: Navigating the AI paradox and the barriers limiting ROI realization
13	Defining the wireless AI paradox and why it matters
15	Barrier 1: Operational complexity overwhelms current capabilities
19	Barrier 2: Wireless security under siege - IoT sprawl meets AI-powered attacks
23	Barrier 3: Wireless competition for AI skills
25	Resolving the paradox: Recommendations for maximizing ROI
28	Methodology

Executive summary

Wi-Fi has transcended its origins as a convenience feature to become a strategic growth engine—delivering measurable returns across multiple business dimensions simultaneously. This ‘multiplier effect’ distinguishes wireless from other IT investments that typically optimize for a single outcome. In 2026, as organizations face the inflection point of connectivity demand and AI-driven transformation, strategic wireless investments are proving to be a catalyst for enterprise-wide success.

The evidence is compelling: more than three-quarters of organizations report operational efficiency gains (78%), see employee productivity improvements (75%), and report enhanced customer engagement (75%), while almost seven in ten (68%) experience positive revenue impacts from wireless investments. When organizations prioritize wireless strategically, they achieve returns that compound across the enterprise—a true multiplier effect, with one network delivering multiple business outcomes.

However, this opportunity emerges alongside mounting complexity. Organizations must adapt to diverse connectivity needs and support a growing spectrum of users and devices—from employees and contractors to autonomous robots, smart sensors, and AI-powered applications. New use cases appear daily, and IT teams are challenged to keep pace. This inaugural Cisco report explores the global state and future trends of wireless enterprise networking, revealing a “wireless AI paradox”: AI is both the leading driver for wireless return on investment (ROI) and the primary source of escalating challenges.

We surveyed 6,098 wireless professionals from across the world who agree that AI-driven operations simplify operations and free up over 850 hours per IT person per year. But simultaneously AI is challenging their infrastructure, representing the number one security threat, and the biggest talent risk.

Three key, interconnected barriers must be addressed to resolve this paradox and unlock the full multiplier effect of wireless:

1. Solving operational complexity:

98% of organizations report increasing complexity, driven by factors like organizational mergers and the proliferation of IoT workloads. Most IT teams remain trapped in reactive ticket management. While 81% of wireless leaders prefer AIOps to simplify operations, only 26% have achieved high-level implementation.

2. Mitigating intensifying security threats:

AI-generated attacks are the leading driver of increased wireless security risk. Over half (58%) of organizations report financial losses from wireless security incidents, with 40% of organizations exceeding US\$1 million annually. Over a third (36%) of affected organizations report compromised IoT or OT devices as the culprit, representing a substantial threat to Wi-Fi as the most common connectivity technology for IoT.

3. Addressing talent shortages:

A shortfall of qualified staff amplifies complexity and threat vectors. Nearly 9 in 10 (86%) wireless leaders struggle to hire professionals, driving 70% higher security incident costs and trapping teams in reactive operations. While IT talent gravitates towards AI and cybersecurity, wireless teams need advanced AI expertise to fully realize the benefits of modern wireless.

These barriers are intertwined, compounding risk and making holistic action essential.

Organizations that successfully address all three barriers unlock significant opportunities, becoming four times more likely to achieve strong wireless ROI (4:1 or higher). Strategic wireless investments yield measurable, compounding returns across multiple dimensions. This explains why wireless investment momentum continues to accelerate, especially as AI usage expands and innovations advance.

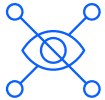
Our research identifies five key recommendations to capture the multiplier effect and drive competitive advantage:



1. Accelerate your Wi-Fi refresh timeline



2. Implement AgenticOps with high levels of automation



3. Establish end-to-end visibility and observability



4. Prioritize holistic security modernization



5. Build wireless talent pipeline through training and certifications

Now is the time to drive competitive advantage. Organizations that act decisively and holistically – by simplifying operations, mitigating wireless security threats, and augmenting talent with technology – will position Wi-Fi as a strategic growth engine for the next decade. Delaying action risks being trapped in reactive cycles, unable to resolve the wireless AI paradox as competitors pull ahead.

Organizations investing holistically in AI, automation, modern security, and certified expertise have an edge on those that do not:

+4X

more likely to achieve strong returns on wireless investments



63%

higher average ROI on wireless investments

The opportunity: Wi-Fi as a strategic growth engine

Investment momentum continues to accelerate as the benefits are realized

The business case for Wi-Fi investment is now undeniable. Organizations are seeing measurable ROI and the rise of business-critical AI deployments amplify the need for more resilient, higher performing Wi-Fi. Wireless budgets are growing accordingly, a trend that will intensify in the years ahead.

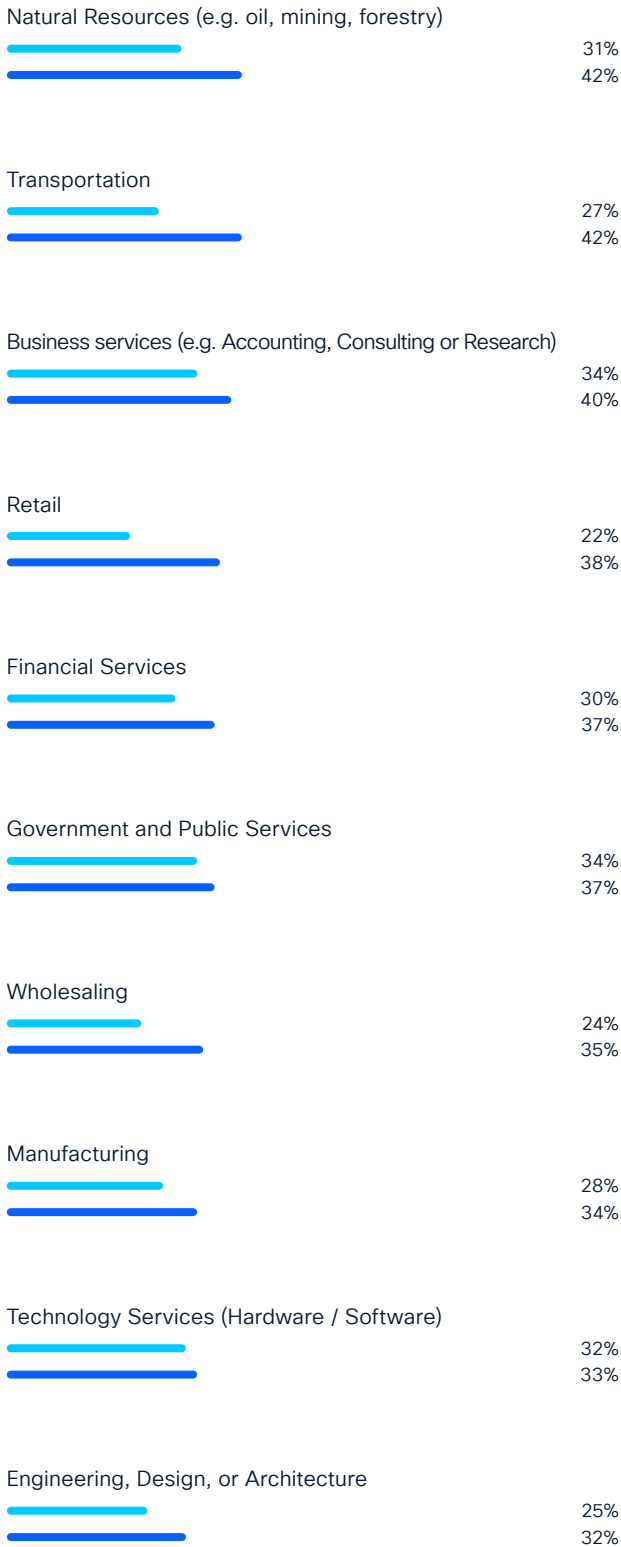
Eight in 10 organizations increased wireless investment over the past five years, with 29% implementing significant budgetary increases of 50% or more. What's more, 82% forecast that wireless budgets will continue to rise, with over a third (35%) expecting investment increases of 50% or more over the next four to five years. This is a clear signal that wireless will play an increasingly critical role in enterprise strategy.

This acceleration extends beyond aggregate spending. Three times as many organizations (32%) expect high returns from wireless tech over the next two years compared to the previous two. This trajectory is driven by use cases that are increasingly wireless-first (see page 10).

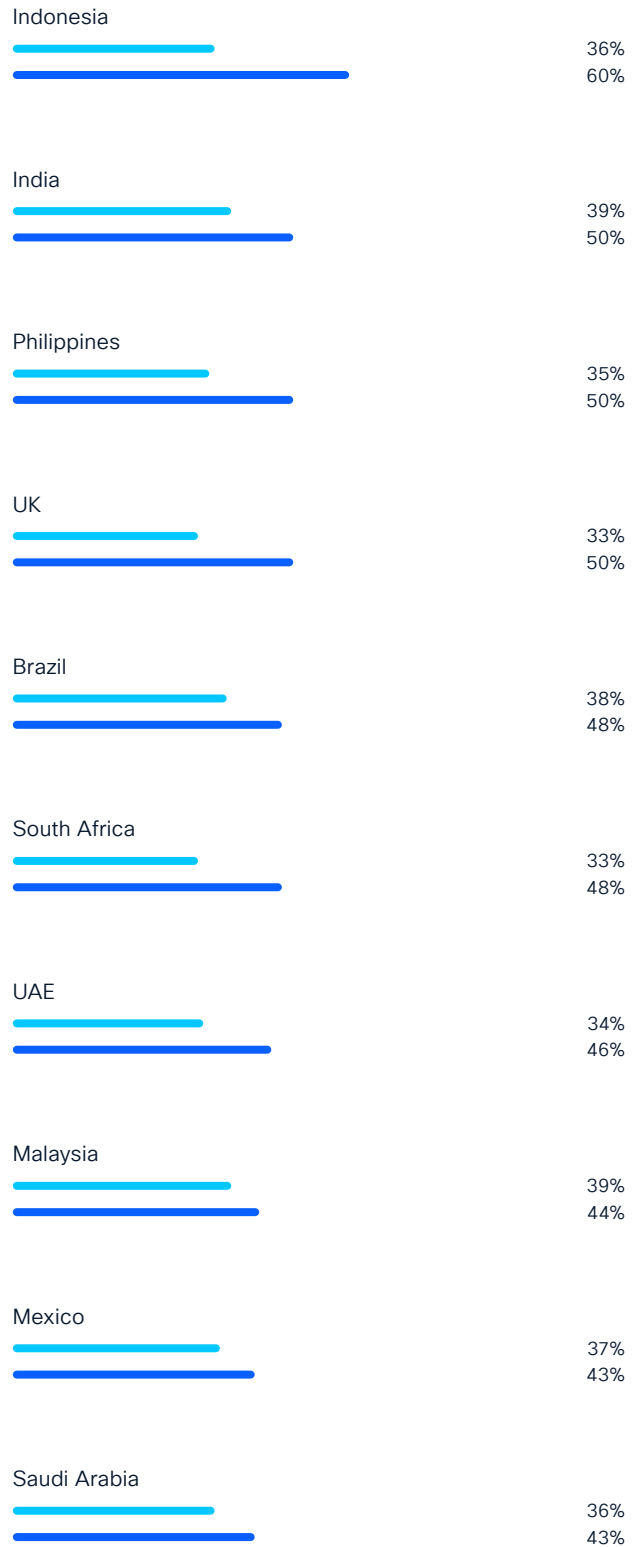
The pace of wireless change is increasing across industries and markets

● >50% budget increase over past 4-5 years ● >50% budget increase over next 4-5 years

Top industries by % predicting >50% budget increases



Top markets by % predicting >50% budget increases



Average annual wireless infrastructure spending per organization stands at approximately US\$13 million, though significant variations exist based on organization size and industry. Smaller organizations typically operate within US\$5 million budgets, while large, multi-site enterprises frequently exceed US\$50 million annually.

Capital expenditure typically accounts for 61% of wireless budgets on average, with the remainder allocated to operational expenditure.

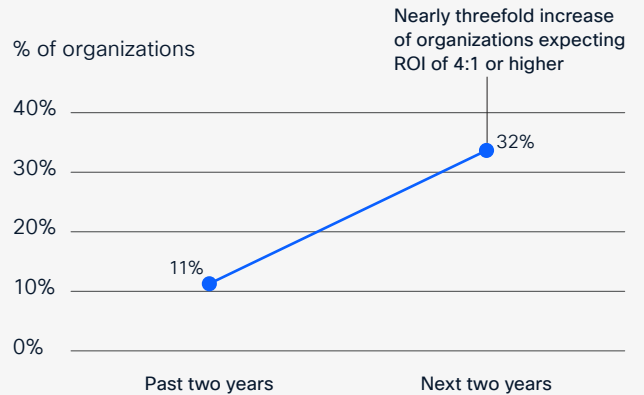
The composition of wireless budgets further reveals organizational priorities. Organizations cite reducing operational risk as their number one budget priority, followed by security enhancement. The relatively even split across these priorities signals that organizations are weighing the opportunities and risks of wireless in almost equal measure when making investment decisions.

This increased investment is directly enabling organizations to deploy Wi-Fi to meet changing business needs and address emerging AI-powered use cases.

Top investment drivers for next wireless investment



High-ROI expectations for wireless are accelerating



Average annual wireless spend, by industry

Business services	\$17.2M
Construction	\$12.3M
Education (primary/secondary)	\$5.4M
Education (university-level)	\$15.2M
Engineering / Design / Architecture	\$11.5M
Financial Services	\$15.6M
Government & public services	\$11.0M
Healthcare	\$9.5M
Manufacturing	\$10.3M
Media & Communications	\$8.2M
Natural Resources	\$14.9M
Real Estate	\$13.1M
Restaurant Services	\$8.3M
Retail	\$10.6M
Technology Services	\$15.7M
Transportation	\$12.3M
Travel services	\$12.5M
Wholesaling	\$9.2M

Average annual wireless spend, by organization size

250-499	\$6.15M
500-999	\$9.63M
1,000-4,999	\$12.74M
5,000-9,999	\$19.94M
10,000+	\$39.01M

Expanding use cases drive new infrastructure requirements

The breadth and diversity of wireless use cases now extend across entire organizations, further illustrating how wireless has become foundational to how modern enterprises operate and compete.

No longer relegated to employee connectivity, Wi-Fi enables everything from critical AI workloads to physical security, customer experience, and operational intelligence. This expansion of wireless ‘purpose’ creates new performance and reliability demands that traditional infrastructure cannot meet.

More than a quarter of organizations (28%) have already deployed AI workloads. This figure is estimated to climb to over three quarters (79%) by 2027, with an additional 29% in pilot stage and 22% planning deployment over the next 12 months. This rapid trajectory further highlights that AI deployment is indeed the defining use case for next-generation wireless infrastructure.

While core use cases such as wireless for physical security are already widely deployed, the next phase of wireless growth is being driven by emerging applications that depend on high-performing, resilient networks. Organizations are increasingly piloting or planning wireless investments to support autonomous systems and robotics, smart facilities and energy management, space analytics, and immersive collaboration.

Organizations are leveraging wireless across an array of use cases

	Currently deployed (%)	Planning to deploy (%)
Autonomous systems & robotics	45%	50%
Space analytics & optimization (footfall, etc.)	50%	44%
Smart facilities & energy management	51%	43%
High-definition streaming	54%	43%
Immersive collaboration & training	54%	43%
Indoor wayfinding	53%	42%
Supply chain & inventory intelligence	55%	42%
AI applications & workloads	57%	41%
Operational visibility & flow analytics	57%	41%
Real-time asset & equipment tracking	57%	41%
Internet of Things	59%	38%
Guest wireless	61%	38%
Customer & user experience enhancement	60%	37%
Physical security (CCTV)	62%	36%

Current footprint = Deployed + Pilot stage

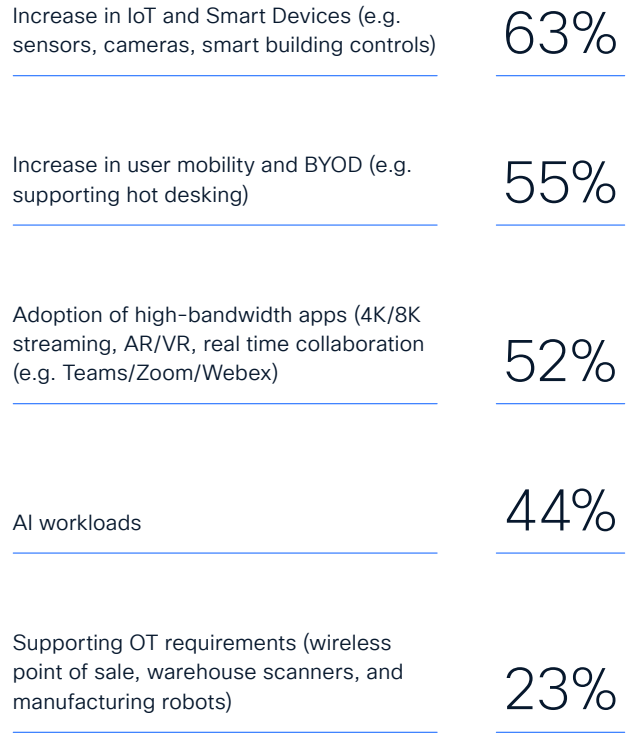
Future expansion = Planned next year + Planned in next 2-5 years

Wireless leaders cite five primary drivers of increased wireless dependence that is driving these use cases. Supporting the growth of the Internet of Things (“IoT”) ranks as the leading driver, followed by increased user mobility and bring-your-own-device adoption, high-bandwidth application adoption including real-time collaboration, AI workloads, and operational technology requirements for point-of-sale systems and manufacturing.

These drivers reflect concerted industry transformation affecting the entire enterprise landscape simultaneously. IoT proliferation, remote work normalization, high-bandwidth application adoption, and AI deployment are occurring across every geography and industry. This common pressure further explains why organizations are increasing wireless investments. And they must continue to invest to take advantage of the multitude of opportunities presented by Wi-Fi amid AI advancements and transformation and maintain a competitive edge.

Supporting new use cases aligned to business goals will help position Wi-Fi as business-critical and accelerate ROI.

Key drivers of growing wireless dependence



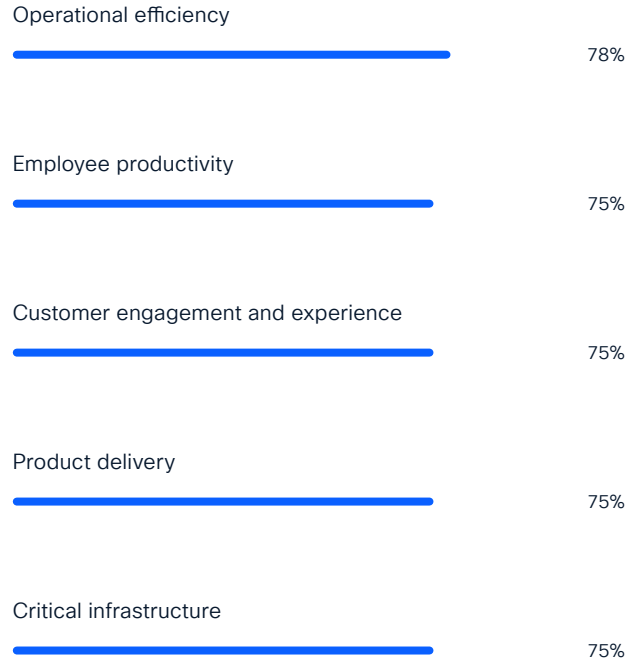
The multiplier effect: Wi-Fi drives measurable business value across multiple areas

Wi-Fi has evolved into a strategic growth engine, delivering tangible returns across multiple dimensions. This 'multiplier effect' distinguishes it from other IT investments that typically optimize for a single outcome.

The evidence is compelling: More than three quarters of organizations report operational efficiency gains (78%), see employee productivity improvements (75%), and report enhanced customer engagement (75%), while almost seven in 10 (68%) are experiencing positive revenue impacts from wireless investments. When organizations strategically prioritize wireless in line with business goals, they achieve returns that compound across the enterprise.

This multiplier effect – one network delivering multiple business outcomes – explains why strategic wireless investments correlate directly to strong ROI and will amplify as AI usage increases and innovations advance. This measurable impact is the reason why wireless investment momentum continues to accelerate.

Most organizations see positive operational and commercial impacts from wireless investments



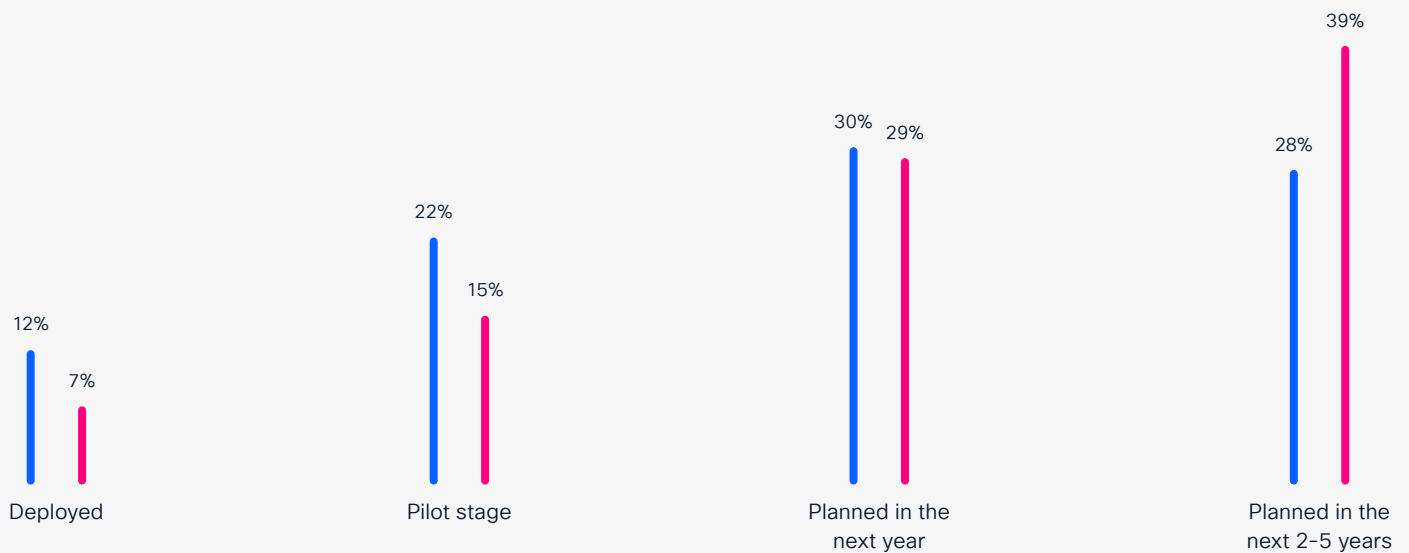
Infrastructure at a crossroads: Bridging the Wi-Fi performance gap

To capture the opportunities outlined above including emerging AI workloads, organizations need to reconsider whether their current infrastructure can support their business needs. The performance gap between legacy and modern Wi-Fi is clear, but adoption is still slow.

Wi-Fi 5 is still the most widely used Wi-Fi standard (43%), but since it is an aging standard, it's questionable whether it is ready to scale many of the above use cases. A small (19%) yet growing number of organizations are presently deploying Wi-Fi 6E or 7. While, three in five organizations (59%) plan to deploy Wi-Fi 6E or 7 in the next year, suggesting that organizations are beginning to react to enterprise needs. Legacy Wi-Fi simply can't scale high bandwidth and low latency needs, especially in device-dense environments. This explains why there has been a 23% increase in Cisco Wi-Fi 6E and 7 access point deployments across its 5 million networks in the second half of 2025 (June–December).

Organizations increasingly factor Wi-Fi 7 into deployment plans

● Wi-Fi 6E ● Wi-Fi 7



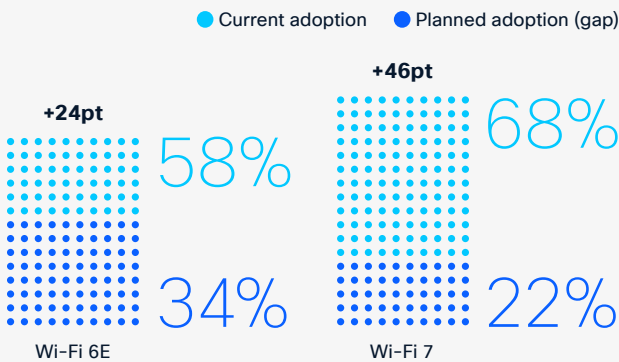
Each successive Wi-Fi generation builds on the previous one, adding features, spectrum availability, and functionality. Built in response to business needs, they determine which use cases organizations can support and which competitive advantages they can realize.

One such advance is the addition of the 6 GHz band added by Wi-Fi 6E, and utilization further improved with Wi-Fi 7. Organizations are using it to solve capacity and congestion issues (46%), enable high-bandwidth applications (32%), and support AI workloads (31%). And the research shows that those adopting this added spectrum are seeing strong benefits.

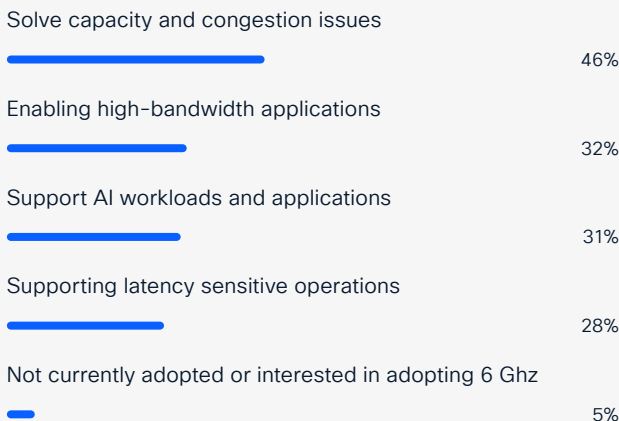
Organizations already deploying 6 GHz show almost double the rate of AI applications and workloads (45%) compared to non-adopters (26%). The 6 GHz band supplies the bandwidth required by AI-powered applications and correlates with improved scalability – 6 GHz users report higher readiness to scale Wi-Fi across devices, sites, capacity, and bandwidth-intensive apps. It’s no surprise that Cisco telemetry highlights a 60% increase in 6 GHz clients going live in 2025. Wireless professionals are seeing the 6 GHz opportunity and helping their organizations deliver on that.

Wireless modernization is a driver of the value creation shared earlier in the report, but alone it is not enough. The research reveals the rise of a ‘wireless AI paradox’ that is both a key path to ROI for Wi-Fi, but also the biggest source of risk.

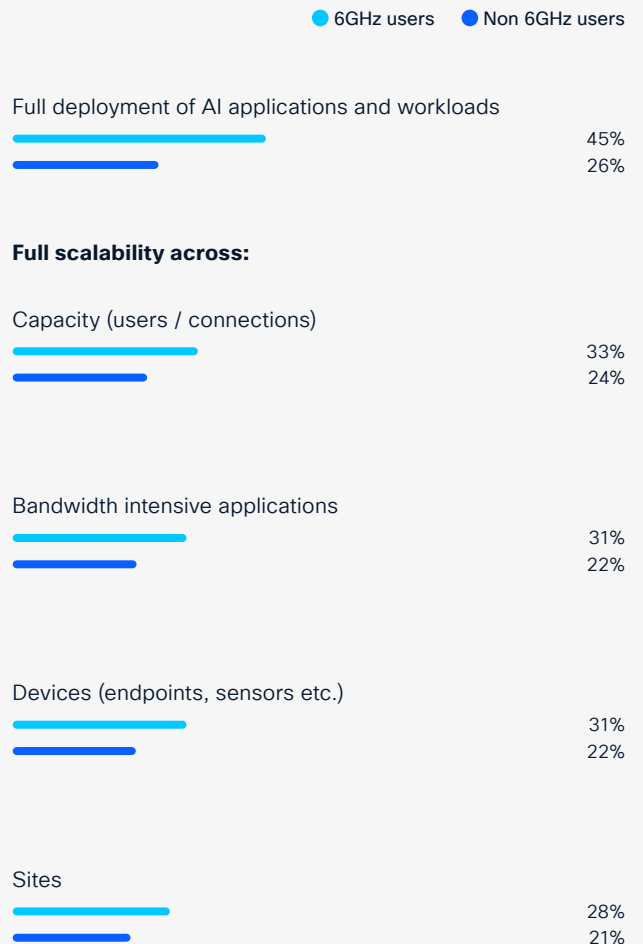
Next-generation Wi-Fi adoption gap signals upgrade pressure



Top cited 6 GHz use cases



AI deployment and scalability differs by 6 GHz deployment status



Wireless strategy in a perfect storm: Navigating the AI paradox and the barriers limiting ROI realization

Defining the wireless AI paradox and why it matters

The wireless AI paradox lays out the central strategic challenge for enterprise leaders in 2026 and the opportunity for first movers. AI is simultaneously the leading driver of wireless ROI and the source of its greatest challenges. Organizations deploying AI view wireless as strategically critical and achieve substantially stronger returns when they integrate wireless optimization into AI deployment strategies. Yet this same AI is introducing new security threats, and intensifying talent competition.

The Wireless AI Paradox AI is both the solution and the challenge



Solution

- AI-driven operations simplify wireless complexity
- Automation frees IT teams to focus on strategy
- Streamlined ticket resolution and faster workflow



Challenge

- AI-generated cyberattacks are a top security threat
- Talent shortages in advanced wireless/AI skills
- Shift in IT talent prioritization from wireless toward AI

AI is the leading path to ROI in wireless – but also the biggest source of risk.

Organizations deploying AI workloads recognize wireless criticality differently than others. Among wireless leaders in organizations deploying AI workloads, three in five (62%) view wireless as strategically critical compared to 46% overall. Wireless leaders in organizations deploying AI are more likely to have experienced 6 GHz adoption drivers first-hand, including solving congestion issues (72% versus 46%) and enabling high-bandwidth applications (70% versus 32%).

The reason for this heightened strategic importance is straightforward: AI workloads demand higher-performing and more resilient wireless networks. Those that integrate wireless optimization into their AI deployment strategies realize substantially greater returns. Around eight in 10 organizations deploying AI workloads report positive impacts from wireless investments in the areas of operational efficiencies, customer engagement, employee productivity, and revenue gains – which was at least seven percentage points higher than average. The conclusion here is that organizations see higher ROI from wireless modernization when paired with investments in AI.

How are these opportunities, challenges, and risks around AI advancements connected?

While AIOps – Artificial Intelligence for IT operations – is the preferred model of wireless leaders to simplify wireless operations and resolve complexity issues, AI-generated or automated cyberattacks are also the top driver of increased wireless security threats. In addition, there is a shifting trend in prioritization of talent from wireless to AI-oriented roles.

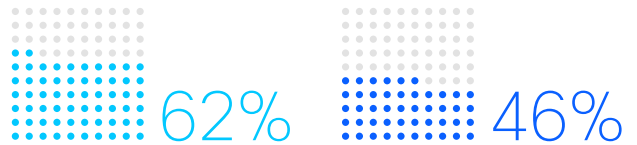
This convergence of factors is giving rise to the wireless AI paradox that organizations must resolve. To do this organizations must overcome three key barriers: (1) operational complexity; (2) wireless security challenges; and (3) major talent gaps.

Organizations that are already actively resolving this paradox—simplifying wireless operations, mitigating security challenges, and addressing talent gaps—are benefiting with 63% higher average wireless ROI than those who have not.

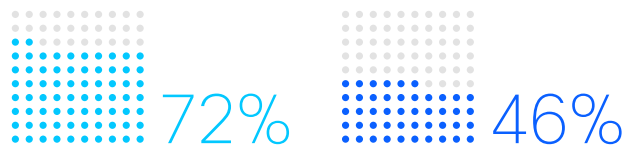
Organizations deploying AI workloads recognize the criticality of wireless and potential of 6 GHz use cases

- Organizations deploying AI workloads (%)
- Organizations without AI workloads (%)

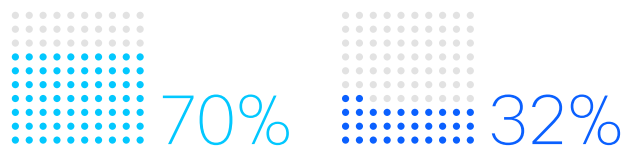
View wireless as strategically critical



Solving congestion issues is a 6 GHz use case



Enabling high-bandwidth applications is a 6 GHz use case



Organizations see greater benefits from wireless modernization when paired with AI deployments

- Organizations deploying AI workloads (%)
- Organizations without AI workloads (%)

Operational efficiency



Customer engagement



Employee productivity



Revenue generation



AI poses multifaceted challenges to wireless teams

Top drivers of security threats

#1 AI -generated or automated cyberattacks / automated intrusion tools

#2 Increased use of IoT and connected devices

#3 Lack of skilled personnel or bandwidth to monitor and respond to threats

Top domains attracting IT talent away from wireless

#1 AI / Machine Learning

#2 Cybersecurity

#3 Software engineering / app development

Top barriers to hiring wireless talent

#1 Shortage of candidates with advanced wireless or AI-integrated skills

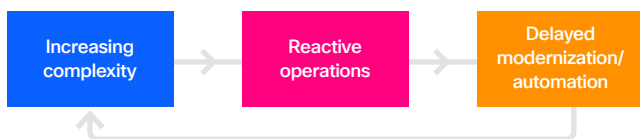
#2 Internal budget constraints or hiring freezes

#3 Geographic limitations or remote work challenges

Barrier 1: Operational complexity overwhelms current capabilities

The first barrier limiting organizations from resolving the AI paradox is mounting operational complexity. Nearly every wireless leader (98%) reports that wireless operations are becoming more complex, creating a reactive posture that drains resources, prevents strategic work, and directly undermines the AI initiatives that help reduce complexity. This creates a vicious cycle: complexity drives reactive work, reactive work limits modernization, and delayed modernization perpetuates complexity.

Organizations cite three primary drivers of this growing complexity: mission-critical IT, IoT, and OT workloads – increasingly including AI-driven applications (43%); need to mitigate new security risks (42%); and rising bandwidth demands from new use cases (38%).



Organizations often cite AI, security risks, and rising bandwidth demand among the top three drivers of growing wireless complexity

Supporting mission-critical IT/IoT/OT workloads (including AI) **43%**

Security risks **42%**

Bandwidth demand increase or unpredictability **38%**

Client unpredictability (usage patterns, mobility) **36%**

Proliferation of devices **25%**

This complexity translates into tangible operational strain. Nearly half (43%) report that their team receives at least 50 wireless support tickets a week, with the average standing at 68. This means IT teams are spending hundreds of hours per month consumed by managing wireless tickets.

Wireless leaders expect this burden to compound. Nearly two-thirds (64%) expect ticket resolution times to increase over the next two to three years, suggesting a growing need to address this complexity.

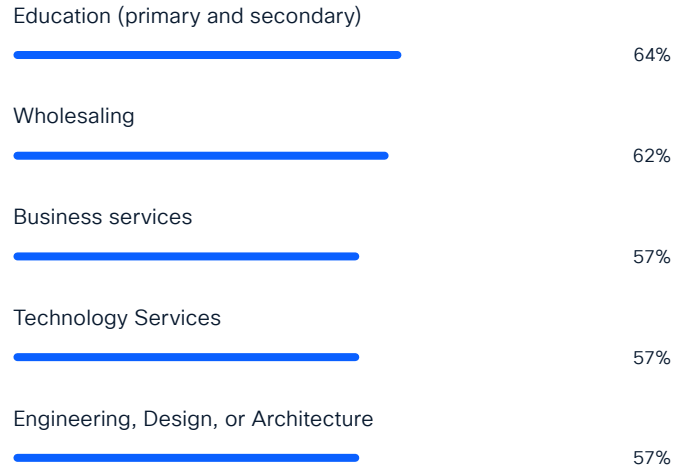
An area of concern is the reactive posture typically stemming from this complexity. A majority of wireless teams (55%) spend most of their time on reactive troubleshooting and incident management. This reactive burden is most pronounced in K-12 Education (64%), Wholesaling (62%), and Business Services (57%).

This reactive operational posture directly undermines modernization efforts. Teams constrained to reactive troubleshooting may divert resources and attention from other pursuits, such as strategic wireless planning, training and pursuing certifications, or implementing automation. The result is a reinforcing cycle: complexity contributes to reactive tasks, reactive tasks redirect teams from implementing solutions that would otherwise help reduce complexity, and unresolved complexity contributes to reactive work.

A critical factor compounding this operational challenge is the lack of visibility. Nearly nine in 10 (87%) organizations report visibility gaps that impair their ability to troubleshoot Wi-Fi issues effectively. The most frequently reported challenges are with poor client visibility, application and cloud visibility, and packet visibility.

Without end-to-end visibility, from the access point to the application, teams cannot rapidly isolate problems. This creates a particularly dangerous dynamic: wireless networks become scapegoats for problems originating elsewhere. A quarter (25%) of complaints are inaccurately attributed to wireless, with each misattributed incident wasting an average of 18 hours across teams. The true culprits are most commonly application problems (25%), client or endpoint issues (22%), and cloud or external service failures (18%).

Industries with respondents most likely to spend the majority of time on reactive tasks



87% face visibility gaps, including:



The operational challenges directly impact organizations' ability to realize ROI.

Amid rising AI-driven organizational transformation, wireless leaders overwhelmingly believe AIOps represents the most promising solution to overcome these rising complexity challenges. Over eight in 10 (81%) would prefer a fully or mostly automated wireless network with AI-driven operations handling routine tasks and optimization.

This demand for AI with autonomous actions suggests a need beyond simple AIOps. It indicates that wireless professionals are looking for AI to do more than assist with alerts and recommendations. Their preference is for AI-driven autonomous networking where issues may be reasoned through and act at machine speed coupled with an appropriate level of human oversight. Cisco defines this as AgenticOps, a new operating model for IT—one that is agent-first, purpose-built for autonomous action with oversight, and designed to unify the experience for both humans and machines.

AgenticOps for wireless is not tomorrow’s innovation; fast movers are already acting as we’re observing a 64% increase in usage of wireless AgenticOps features in the second half of 2025 – a significant uptake that is helping to bring immediate value to organizations.

The benefits are substantial and measurable. Almost all organizations (98%) that have implemented high-level AIOps with automation report dramatic time savings, freeing up an average of three hours 20 minutes per day per person. These organizations benefit from operational improvements: they are four times more likely to rate their network operations as very simple with 12% faster ticket resolution times than manually operating counterparts.

However, a significant gap exists between preference and reality. Only 29% of organizations have automation supporting wireless ticket management. Just 29% automate security monitoring and incident response, while 23% have automation supporting capacity planning and provisioning. This gap reflects multiple constraints. Two-thirds (66%) do not expect to achieve high-level automation within five years, which may signal technical, organizational, or resource barriers to AIOps deployment despite strong organizational preference.

The AIOps gap: Desire versus reality

Preference for Automated Wireless Network with AIOps



Organizations with fully automated operations with AI-driven operations outperform those with mostly manual operations substantially. Wireless leaders from these organizations are three times more likely to expect reduced ticket resolution times over the next two years; four times more likely to describe network management as very simple; and nearly twice as likely to describe infrastructure as fully scalable.

Organizations with high levels of automation and AIOps show far greater confidence in infrastructure scalability. They are almost twice as likely to describe their infrastructure as fully scalable compared to those with mostly manual operations. And organizations reporting strong ROI show substantially higher deployment of automation and AIOps across ticket management (31%), capacity planning (28%), security monitoring (31%), vendor coordination (28%), and network optimization (30%).

Operational complexity alone represents a significant challenge to resolving the wireless AI paradox and thus improving wireless ROI. When combined with escalating security threats, the second barrier, the impact on organizational resilience and financial performance becomes even more severe.

Organizations with fully automated operations and AI-driven operations outperform those with mostly manual operations in several key areas:

3x more likely to forecast significant reduction in ticket resolution times over the next two years

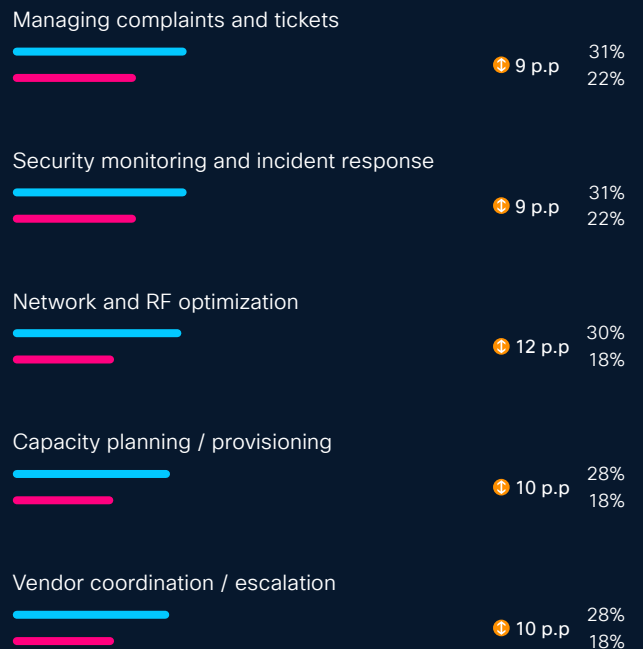
4x more likely to describe management of their networks as 'very simple'

Almost **2x** more likely to describe device infrastructure as fully scalable

12% lower average ticket resolution time

Area of automation and AIOps deployment

● Organizations with strong ROI
● Organizations with negative ROI



Barrier 2: Wireless security under siege – IoT sprawl meets AI-powered attacks

Wireless security represents the second critical barrier preventing organizations from resolving the AI paradox and realizing strong wireless ROI. Organizations cannot confidently deploy Wi-Fi as a platform for business-critical workloads while facing escalating security threats and mounting financial losses.

Eighty five percent of organizations have experienced at least one wireless security incident in the last 12 months. Further to this, more than one-third report experiencing escalating wireless threats over the past two years (38%). Wireless leaders state security threats have become more frequent and damaging, while also being more difficult to detect and remedy.

AI has emerged as the most significant new security threat vector. Wireless leaders are most likely (35%) to cite AI-generated or automated cyberattacks among the top three drivers of increased wireless security threats. These attacks can identify network vulnerabilities, adapt attack strategies based on defensive responses, and operate at a scale and speed far exceeding human attacker capabilities. Additionally, AI-generated or automated cyberattacks may lower the barrier to entry for attacking Wi-Fi networks, allowing threat actors to operate with a sophistication and speed that previously required more significant resources.

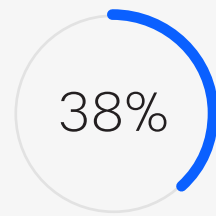
AI-driven attacks on wireless networks confront underprepared defenses

Feature	Traditional Wi-Fi Attack	AI-Powered Wi-Fi Attack
Speed	Limited by hardware and wordlist size.	Optimized by AI models that 'guess' faster.
Detection	Easier to spot via repeated failed attempts.	Can mimic human patterns to stay under the radar.
Automation	Requires manual setup and monitoring.	Can autonomously 'pivot' from one device to another.
Social Engineering	Generic phishing emails.	Hyper-personalized lures using Deepfakes/GenAI.

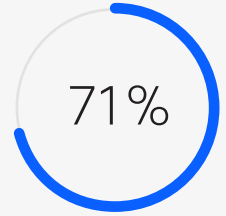
The nature of Wi-Fi cybersecurity threats is also shifting from passive reconnaissance and credential theft toward active compromise and operational disruption. Rogue access points, compromised credentials, and denial-of-service attacks represent the top attack vectors.

The attack surface continues to expand as well. Over a third (36%) of affected organizations report disruption from compromised IoT or OT devices, representing a substantial threat to Wi-Fi since it is the most common connectivity technology for IoT. The proliferation of IoT devices, especially when unmanaged, creates an aggregated vulnerability as individual weaknesses compound into network-wide exposure.

Wireless threats are accelerating over time



38% report increases in wireless security incidents in the past two years



71% expect such incidents to increase in the next two years

Key contributors to increased threat level for wireless networks

AI-generated or automated cyberattacks / automated intrusion tools	35%
Remote and hybrid work models expanding attack surface / unmanaged endpoints	31%
Increased use of IoT and connected devices (rapid device growth)	30%
Lack of skilled personnel or bandwidth to monitor and respond to threats	27%
Difficulty managing multiple security layers and segmentation	25%
Budget or resource constraints limiting security improvements	25%
Poor user practices, human error, or insider risks	24%
Limited network and application visibility	21%
Legacy infrastructure and protocols	20%
Difficulty managing security patching	20%
Limited client visibility	16%

Losses incurred over the past 12 months from wireless security incidents



Organizations most likely to lose over US\$ 1m from wireless security incidents

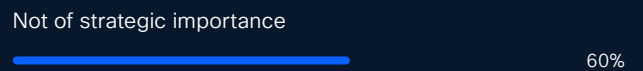
Industries:



Company size:



Outlook on wireless:

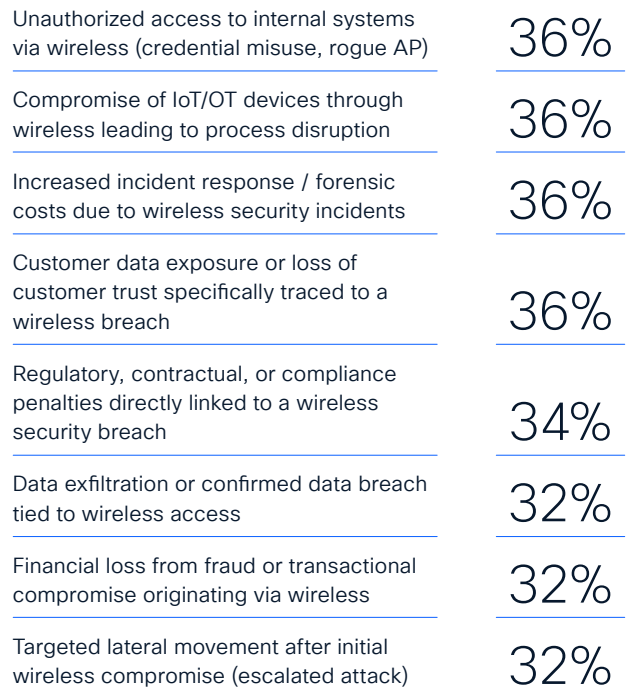


The financial impact of these security incidents is substantial. Fifty-eight percent of organizations have experienced financial loss due to wireless security incidents. Half (50%) report losses exceeding US\$1 million in the past year, representing a sizable financial impact that alone justifies Wi-Fi security investment.

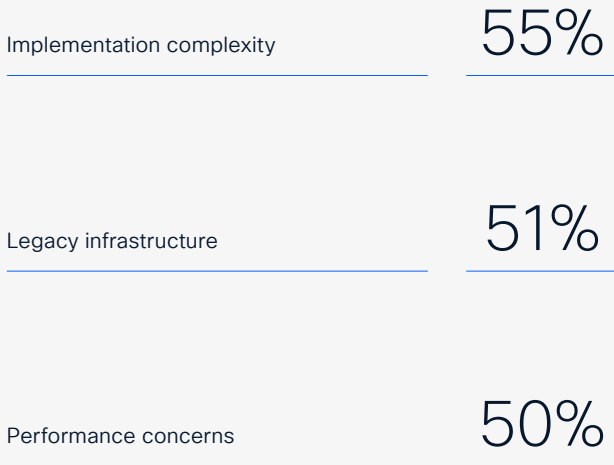
Organizations are losing more than money due to wireless security incidents. In addition to financial losses, One in three (36%) experienced loss of customer trust, and a similar number (34%) faced regulatory penalties or compliance consequences as a result to these security incidents. The impact of reputational damage and regulatory exposure often extends well beyond direct incident costs.

Yet most organizations have still maintain confidence in their wireless security. Eighty three percent report that their organization is doing enough to protect wireless networks despite also expecting wireless security failures to increase in the next two years (71%). Executive level respondents show far greater confidence in wireless defenses than frontline staff, suggesting that organizational leadership

The hidden costs of wireless security incidents



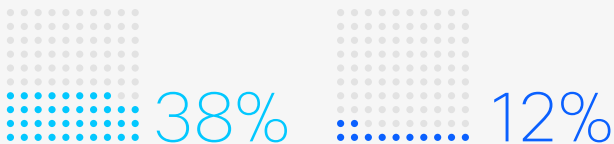
Top cited barriers to improving wireless security



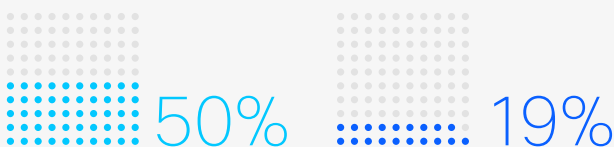
WPA3 implementation drives safety and ROI for wireless operations

- Organizations using full WPA3
- Organizations with no WPA3 or in transition mode

Expects less security failures in the next 2 years



Expects strong wireless ROI (4:1+) in the next 2 years



may underestimate security challenges compared to technical staff who directly manage networks.

Organizations cite three primary barriers to improving wireless security: implementation complexity, legacy infrastructure, and performance concerns. These barriers do not exist in isolation but reflect the broader wireless challenges of talent shortages, visibility gaps, and rising operational strain that restrict organizations' ability to modernize security.

The result is a widening vulnerability gap: even as risks escalate, organizations remain constrained by outdated systems, complexity, and performance concerns, slowing transformation and eroding resilience.

The last point is especially important because the research shows organizations that implement modern authentication and encryption protocols demonstrate better security outcomes, plus outsized business performance than those that do not. For example, those using certificate or profile-based authentication are almost three times more likely to predict a decline in wireless security failures compared to those using only passwords and four times more likely compared to those operating open networks. They also experience approximately 18% lower financial losses on average than those not using modern authentication protocols.

These advantages are further reinforced when organizations adopt WPA3 where adoption is directly correlated with stronger security and stronger ROI. Over a third (38%) of respondents from organizations using full WPA3 expect fewer security failures in the next two years compared to 12% of organizations with no WPA3 or in transition mode. Half (50%) of respondents from organizations with full WPA3 expect strong ROI (4:1 or greater) in the next two years compared to 19% without WPA3.

Organizations leveraging the embedded security of next generation Wi-Fi are around three times more likely to expect strong ROI and to predict fewer security failures over the next two years. Organizations now have a clear path to reducing operational risk and financial losses, while improving user and customer trust. However, implementing modern security protocols requires specialized expertise—expertise that is increasingly difficult to find. This brings us to the third barrier: the competition for wireless talent.

Barrier 3: Wireless competition for AI skills

Talent represents the third barrier and, in tandem with operational complexity and increasing security threats, is creating a strong catalyst that inhibits organizations from scaling wireless ROI.

Talent shortages do not merely slow modernization; they directly amplify operational strain and security exposure, while making it more difficult to implement AIOps. This creates a vicious cycle: organizations lacking talent struggle to modernize, modernization remains delayed, complexity and security risk escalate, costs rise, and the best talent leaves for more modern organizations.

Eighty six percent of organizations report challenges in hiring, with IT talent shifting to other technology fields such as AI and cybersecurity. Respondents have indicated that AI and machine learning ranks as the number one area that attracts talent from wireless (50%), while a shortage of

candidates with advanced wireless or AI-integrated skills is the number one barrier to hiring wireless talent.

This is creating a skills gap that translates into higher operating costs (39%), lower morale (37%), and reduced innovation (32%). Talent pressure is most evident in Technology and Manufacturing, where competition from AI, cybersecurity, and OT roles further constrain the ability to scale wireless expertise.

The correlation between talent and negative outcomes is clear. Organizations facing high difficulty in hiring have wireless teams spending far more time on reactive tasks. Half (50%) of those facing high recruitment difficulty spend most of their time on reactive tasks compared to 37% of those facing no difficulty.

The impact is not just operational: organizations struggling to hire wireless specialists expect an increase in wireless security failures at substantially higher rates (85% versus 59% for those with no hiring difficulty – a 26-percentage-point gap).

AI-linked to wireless brain drain and skills shortages

Ranking among the top three domains attracting talent away from wireless

AI / Machine learning	50%
Cybersecurity	48%
Software engineering / app development	40%
Cloud infrastructure / DevOps	37%
Data science / analytics	34%
Smart building / sustainability tech	31%

Primary reasons for difficulty in hiring wireless talent

Shortage of candidates with advanced wireless or AI-integrated skills	51%
Internal budget constraints or hiring freezes	37%
Geographic limitations or remote work challenges	36%
Lengthy hiring process or internal bottlenecks	34%
Lack of interest in wireless as a career domain	34%
Competition	28%

Talent constraints create a reactive, low-automation trap

	Organizations facing no difficulty in recruitment	Organizations facing high difficulty in recruitment
Wireless team time spent on mostly reactive tasks	37%	50%
Average automation of wireless network functions	34%	23%
Expectation of increase of wireless security failures	59%	85%
Annual cost of wireless security incidents	US\$12,448,230	US\$21,169,950

More concerning, they already experience 70% higher costs of security incidents annually than those with no recruitment challenges. Wireless leaders at organizations facing no recruitment difficulties say they average annual security incident costs of US\$12.4 million compared to US\$21.2 million for those facing high difficulty.

Wireless resilience starts with certified expertise. Less than half of those managing wireless operations (46%) are certified in wireless technologies. Teams with deeper wireless credentials deploy modern security protocols faster and more comprehensively. Those with at least 50% of personnel certified in wireless technologies are 17 percentage points more likely to implement full WPA3 security, reducing exposure to legacy threats. They are also 17 percentage points more likely to use certificate or profile-based authentication, minimizing access conflicts and lowering troubleshooting volume.

The implication is clear: organizations facing recruitment challenges while lacking certified talent face compounding disadvantages, including higher operational costs, greater security exposure, lower automation, and diminished capacity to modernize. Those investing in talent and certification early gain competitive advantage as complexity increases and specialized skills become essential to operational success, particularly amid the growing competition for talent.

The talent crisis reveals the interconnected nature of the wireless AI paradox. Without bringing AI to the core of wireless operations organizations will continue to lose talent. Without the talent, strategic projects such as security modernization becomes harder to realize. Without modern security, incident costs rise, making it harder to invest in both talent and technology. This compounding dynamic explains why organizations must address all three barriers simultaneously to escape the paradox.

Resolving the paradox: Recommendations for maximizing ROI

Organizations achieving strong wireless ROI are addressing operational complexity, security threats, and talent gaps together. They recognize that solving one and not the others leaves the wireless AI paradox intact. When organizations take this holistic approach to Wi-Fi they create compounding returns that multiply technology and business outcomes.

Our research supports five recommendations that, when implemented together, can break the reactive cycle and make organizations four times more likely to achieve strong ROI.

1

Revisit your Wi-Fi refresh timeline

Modern Wi-Fi enables substantially higher infrastructure scalability, AI deployments, and emerging business use cases. Organizations cannot deliver on the opportunities discussed earlier in this report without modern infrastructure foundations.

The business case is compelling: fast movers with a focus on ROI are continually investing in technology to support their business goals – for example those with strong wireless ROI are 24% more likely to have deployed 6 GHz.

Migration should target application-driven deployment with organizations identifying the highest-impact use cases, conducting business case analysis, and deploying infrastructure in phases that align with business value delivery. This approach ensures that infrastructure investment directly supports business outcomes rather than technology for its own sake.

Organizations should prioritize Wi-Fi 6E and 7 deployments, particularly looking at how using 6 GHz can support those high-impact use cases. Early adopters of 6 GHz have been able to realize stronger ROI and higher AI deployment rates, underscoring its role in scaling modern workloads and unlocking the wireless AI paradox opportunity.

2

Get on the path to AgenticOps

Organizations should prioritize building towards AgenticOps to break the reactive cycle that constrains wireless teams. AgenticOps is the evolution of AIOps from AI-assisted insights (alerts, recommendations) to AI-driven autonomous actions by intelligent agents that diagnose and resolve issues at machine speed. The operational benefits of bringing AI and automation are substantial and immediate: wireless teams free up over three hours per day, enabling them to shift from reactive operations to a more strategic, proactive approach.

Getting on the path to AgenticOps delivers benefits extending beyond time savings. It improves security posture, enables faster incident resolution, and creates a foundation for future innovation. Organizations should view this not as a cost-reduction initiative but as a strategic investment in operational excellence.

Prepare your team with training and setting clear rules for the role of AI in their work. Start small, implementation should begin with bringing AI features and more autonomous actions to high-impact areas first. Ticket management and network automation are starting points for immediate value. Deployment can then broaden to include security monitoring and capacity planning.

Mature AIOps strategies can then lead to zero-touch, fully autonomous agent led network operations – AgenticOps, capable of supporting increasingly demanding workloads.

With AI itself cited as the top field drawing talent away from wireless – AgenticOps for wireless can stem the flow and ease time constraints. Organizations with fully automated AI-driven operations are three times more likely to forecast significant acceleration in ticket resolution, four times more likely to describe networks as very simple, and almost twice as likely to describe infrastructure as fully scalable. Organizations deploying automation across key functions achieve substantially higher ROI.

3

Establish end-to-end visibility and observability

With 87% of organizations reporting visibility gaps that impair effective Wi-Fi troubleshooting, it is critical to address this blind spot. Organizations should explore how they can better connect visibility across IT and lines of business – achieving end-to-end insight across clients, applications, cloud services, and network packets. The operational benefit is immediate, eliminating wireless scapegoating and focusing troubleshooting on actual problem sources by the right team.

For wireless teams, the first three areas to target are improving visibility into: client device behavior, application and cloud service performance, and packet-level analytics. This three-dimensional approach enables rapid root cause identification and faster incident resolution.

End-to-end visibility supercharges AIOps. AI systems require rich data inputs to make effective operational decisions, so organizations should view broad and deep visibility as a prerequisite for modern network operations.

4

Prioritize holistic security modernization

Wireless security modernization should be treated as a strategic initiative aligned with broader enterprise security posture. Organizations should treat wireless security not as an infrastructure concern but as a priority for managing business risk. This means looking at wireless security in the context of the larger network. This would enable security investment to compete for capital alongside other strategic IT priorities.

Organizations that want to minimize exposure to losses from security incidents should accelerate deployment of modern wireless security protocols, particularly full WPA3 and certificate or profile-based authentication. Organizations with more modern security postures also tend to see a better return on their wireless investments. For example, organizations using full WPA3 have a 50% likelihood of predicting strong ROI compared to 19% among those without WPA3.

Legacy infrastructure needs to be addressed systematically rather than be allowed to persist indefinitely. Organizations should align their security lifecycle planning with new infrastructure investments.

Organizations implementing modern authentication and encryption protocols demonstrate superior outcomes: four times more likely to predict declining security failures, and experience 18% lower financial losses from incidents. These findings show that modern wireless security is not merely more secure but also delivers measurable financial benefits by preventing incidents that would generate losses.

Wi-Fi security alone is insufficient. To secure the network effectively, organizations must: (1) Implement network segmentation to dynamically verify user identity, enforce security policies, and organize clients into appropriate groups; and (2) Extend visibility beyond access points to monitor and protect the entire network from wireless threats (reinforcing Recommendation 2). These measures ensure comprehensive network protection, not just wireless access control.

5

Build wireless talent pipeline through training and certification

Organizations should invest in developing their talent through training, certification, and career advancement opportunities. This investment creates measurable impact across security outcomes, incident response times, as well as job satisfaction.

Investment should target advanced skills including making the most of Wi-Fi 6E and 7 standards, security protocol modernization (WPA3), AgenticOps implementation, and automation platform expertise. Organizations also need to recognize wireless specialization as a strategic career path and compensate accordingly given the impact of certification is quantifiable: organizations with at least 50 % of personnel certified in wireless technologies are 17% more likely to fully implement WPA3. They are also 17 percentage points more likely to use profile or certificate-based authentication.

Training and certification investment compounds over time, with organizations starting talent development programs early gaining competitive advantage as complexity increases and specialized skills become essential to operational success. Those delaying investment until talent shortage becomes acute face substantially larger hiring costs and operational disruption.

The multiplier effect: Why integrated implementation matters

These five recommendations compound when they are implemented together:

-  Modern infrastructure without automation = overwhelmed teams
-  Automation without security modernization = efficiently managed vulnerable networks
-  Security modernization without talent = protocols that can't be properly implemented
-  Talent development without modern infrastructure = skilled teams managing outdated systems
-  Any of the above without visibility = flying blind regardless of other investments

As this report clearly outlines, organizations that address all dimensions simultaneously are four times more likely to achieve strong ROI compared to those neglecting these areas.

The wireless AI paradox will not resolve itself. Organizations that act decisively, and holistically, in 2026 will establish competitive advantages that compound over years. Those that delay will find themselves trapped in reactive cycles, bleeding budget to security incidents, and unable to capitalize on AI-driven transformation while competitors pull ahead.

The choice, and the window to choose, is now.

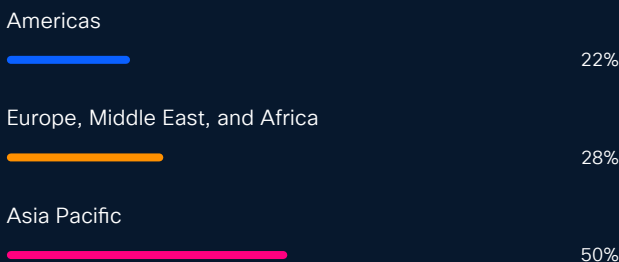
Methodology



This research comprised interviews with 6,098 organizations in 30 markets 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.



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>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to www.cisco.com/go/trademarks.
Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)