State of Wireless 2026

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

Malaysia

Executive summary

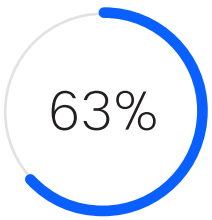
In 2026, Wi-Fi has transcended its role as a convenience feature to become a strategic growth engine. Globally, organizations that invest holistically in wireless are four times more likely to achieve strong ROI and measurable gains across every business function – from operational efficiency to revenue growth. This multiplier effect distinguishes wireless from other IT investments, delivering compounding returns across the enterprise.

Yet almost all (98%) report that complexity is intensifying, security threats are multiplying, and the talent needed to navigate these challenges is increasingly scarce. 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.

Global 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



higher average ROI on wireless investments

This inaugural report reveals a wireless AI paradox: AI is simultaneously the leading driver of wireless ROI and the greatest source of escalating risks. While AI-driven operations can free hundreds of hours per IT professional annually, they also amplify infrastructure demands, security threats, and talent shortages. The 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.

Our research identifies legacy infrastructure plus three interconnected barriers limiting organizations from fully unlocking wireless ROI: operational complexity, intensifying security threats, and talent gaps. These challenges reinforce one another, leading to compounding risk.

Organizations that address these operational, security, and talent barriers holistically achieve an ROI 63% higher than those that do not, showing 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.

Across the board, the findings show that when organizations in Malaysia strategically prioritize wireless, measurable returns are gained across multiple dimensions. More than 82% report improvements in operational efficiency, employee productivity (81%), and customer engagement (79%), while 72% report positive revenue impacts. This demonstrates that modern wireless infrastructure translates directly into business growth.

The window for competitive advantage is now. Organizations in Malaysia that act decisively in 2026 – simplifying operations, modernizing wireless security, and building certified expertise – will position Wi-Fi as a strategic growth engine for the next decade.

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 Malaysia's 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. Globally, organizations that deploy AI are more likely to view wireless as strategically critical and achieve substantially stronger returns when they integrate wireless optimization into AI deployment strategies. Yet this same AI is creating unprecedented operational complexity, contributing to 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
- IT talent pulled away from wireless toward AI

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

AI poses multifaceted challenges to wireless teams

Top drivers of security threats	Top domains attracting IT talent away from wireless	Top barriers to hiring wireless talent
#1 AI-generated or automated cyberattacks / automated intrusion tools	**#1** AI / Machine Learning	**#1** Shortage of candidates with advanced wireless or AI-integrated skills
#2 Remote and hybrid work models expanding attack surface / unmanaged endpoints	**#2** Cybersecurity	**#2** Lengthy hiring process or internal bottlenecks
#3 Lack of skilled personnel or bandwidth to monitor and respond to threats	**#3** Software engineering / app development	**#3** Internal budget constraints or hiring freezes

Organizations in Malaysia deploying AI workloads recognize wireless criticality differently than others. Among global wireless leaders in organizations deploying AI workloads, 56% view wireless as strategically critical compared to 46% of non-deployers.

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. In Malaysia, more than seven in 10 report positive impacts from wireless investments in the areas of operational efficiency, customer engagement, employee productivity, and revenue gains.

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

While AI is seen as the path to simplify wireless operations and resolve complexity issues, AI-generated or automated cyberattacks are the among the top drivers of increased wireless security threats and the domain most likely to attract talent away from wireless in Malaysia.

Barrier 1: Operational complexity overwhelms current capabilities

The first barrier is limiting organizations from resolving the AI paradox is mounting operational complexity. Nearly every wireless leader (97%) in Malaysia reports that wireless operations are becoming more complex, leading to a reactive posture that hinders resources, prevents strategic work, and directly undermines the AIOps and automation initiatives that help reduce complexity. This contributes to a vicious cycle: complexity drives reactive work, reactive work limits modernization, and lack of modernization perpetuates complexity.

Organizations in Malaysia cite three primary drivers of this growing complexity: mission-critical IT, IoT, and OT workloads – increasingly including AI-driven applications (56%); client unpredictability (39%); and new security risks (35%).

This complexity translates into tangible operational strain: 49% report that their team receives at least 50 wireless support tickets a week, meaning IT teams can spend hundreds of hours per month consumed by wireless ticket management.

An area of concern is the reactive posture typically stemming from this complexity. 52% spend most of their time on reactive troubleshooting and incident management. This means proactive work, including strategic projects, training, certifications, and network optimization is deprioritized.

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.

A critical factor compounding this operational challenge is a lack of visibility. 88% of organizations report visibility gaps that impair their ability to troubleshoot Wi-Fi issues effectively. The most frequently reported challenges are with poor application and cloud visibility, packet visibility, and roaming visibility.

Without end-to-end visibility, teams cannot rapidly isolate problems. This contributes to a particularly dangerous dynamic: wireless networks become scapegoats for problems originating elsewhere, with 67% of respondents reporting that more than 10% of incidents are inaccurately attributed to wireless.

Amid rising AI-driven organizational transformation, wireless leaders overwhelmingly believe AI is the most promising solution to overcome these increasingly complex challenges – and the benefits are substantial and measurable including significant time savings, simplification of network operations and faster ticket resolution times.

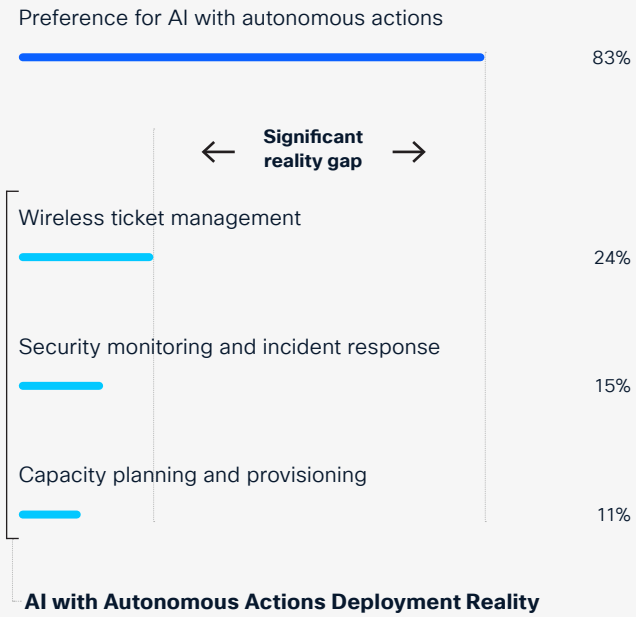
However, a significant gap exists between preference and reality in Malaysia's rollout of AI capabilities for wireless.

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.

88% face visibility gaps, including:

Poor application/cloud visibility	46%
Poor packet visibility	45%
Poor roaming visibility	43%

The AI gap: Desire versus reality



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

Wireless security represents the second critical barrier hindering organizations in Malaysia 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.

84% of Malaysia's organizations have experienced at least one wireless security incident in the last 12 months. 48% report escalating wireless threats over the past two years, saying they have become more frequent, damaging, and difficult to detect and remedy.

AI-generated or automated cyberattacks are frequently cited among the top three drivers of increased wireless cybersecurity threats. These threats 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 lowers the barrier to entry for attacking Wi-Fi networks, allowing AI-generated or automated threat actors to operate with a sophistication and speed that previously required more significant resources.

The attack surface continues to expand for organizations in Malaysia. 44% of those affected by incidents 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, leads to an aggregated vulnerability as individual weaknesses compound into network-wide exposure.

The financial impact of these security incidents is substantial. 65% of organizations in Malaysia have experienced financial loss due to wireless security incidents. 54% report losses exceeding US$1 million in the past year, representing a sizable financial impact that alone justifies Wi-Fi security investment.

Organizations in Malaysia are losing more than money due to wireless security incidents. 44% experienced loss of customer trust while 45% faced regulatory penalties or compliance consequences, showing impacts extend well beyond direct incident costs.

Key contributors to increased threat level for wireless networks

AI-generated or automated cyberattacks / automated intrusion tools	43%
Remote and hybrid work models expanding attack surface / unmanaged endpoints	37%
Lack of skilled personnel or bandwidth to monitor and respond to threats	35%
Budget or resource constraints	32%
Increased use of IoT and connected devices (rapid device growth)	32%

Yet most organizations have still maintained confidence in their wireless security. 87% report that their organization is doing enough to protect wireless networks despite 78% also expecting wireless security failures to increase in the next two years.

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.

However, the research shows that organizations using modern, certificate or profile-based authentication demonstrate better security outcomes, plus outsized business performance than those that do not. They also experience lower financial losses on average than those not using modern authentication protocols.

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 loses the competition for AI skills

Talent represents the third barrier and in tandem with operational complexity and increasing security threats, is creating a 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 contributes to a vicious cycle: organizations lacking talent are slower to modernize, complexity and security risk escalate, costs rise, and the best talent leaves for more modern organizations.

92% of organizations in Malaysia report challenges in hiring, with IT talent prioritizing other, more visible technology fields such as AI and cybersecurity. This contributes to a skills gap that translates into higher operating costs (55%), lower morale (49%), and reduced innovation (43%).

The correlation between talent and negative outcomes in Malaysia is clear. Organizations facing extreme difficulty in hiring wireless talent spend far more time on reactive tasks. And the impact is not just operational; organizations experience higher costs of security incidents annually than those with no recruitment challenges.

Organizations facing recruitment challenges while lacking certified talent see compounding disadvantages: 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 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.

AI-linked to wireless brain drain and skills shortages

Ranking among the top three domains attracting talent away from wireless

AI / Machine learning	49%
Cybersecurity	47%
Cloud infrastructure / DevOps	46%

Primary reasons for difficulty in hiring wireless talent

Shortage of candidates with advanced wireless or AI-integrated skills	65%
Lengthy hiring process or internal bottlenecks	53%
Internal budget constraints or hiring freezes	48%

Methodology

This research comprised interviews with 6,098 organizations in 30 markets, including 101 organizations in Malaysia. The research 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**