

State of Wireless 2026

Unlocking the Multiplier Effect: How Strategic Wireless Investments Drive Outcomes for Growing Enterprises in the AI Era

Midsized Enterprise



Executive summary

Midsize enterprises occupy a demanding position in the modern corporate ecosystem. Growing businesses, with between 1,000 and 4,999 employees face many of the same operational and technology challenges as global corporations, but do so with more constrained resources, particularly leaner IT teams that operate with greater efficiency.

This unique position shapes how growing businesses approach technology strategy. Wireless connectivity is no longer a basic convenience; it is the primary medium of business execution. Robust networks power physical facilities and enable artificial intelligence (AI) applications. Moreover, **four out of five growing businesses report operational efficiency gains (82%) and increased employee productivity (80%) from strategic wireless investments.** These operational improvements reflect a multiplier effect that helps leaner teams achieve enterprise-level outcomes. Yet a critical anomaly emerges regarding financial returns. Just over half (51%) of midsize organizations report a positive impact on revenues from wireless investments, compared with 68% across all organizations surveyed. While these firms excel at controlling costs and driving productivity, their leaner resources make it harder to translate connectivity into direct revenue streams.

To unlock this financial value, business leaders must resolve a complex paradox. AI represents the most promising path to network automation and organizational growth. In fact, **81% of leaders prefer automated wireless networks powered by AI.** Yet, deploying these advanced technologies introduces operational strain and amplifies three interconnected barriers that prevent organizations from monetizing their investments.

First, operational complexity traps lean technology teams in reactive troubleshooting cycles. **There is near-complete agreement among our respondents (98%) who believe wireless operations are becoming more complex.** Tool sprawl creates severe visibility gaps, causing the majority (55%) of teams to spend most of their time managing

support tickets instead of proactively designing better network architectures.

Second, security threats are escalating rapidly. **Nearly nine in 10 (86%) growing businesses have experienced at least one wireless security incident in the past twelve months.** Automated cyberattacks probe networks relentlessly, with 36% of respondents citing AI-generated attacks as the primary driver of escalating threats. Lean teams cannot deploy manual countermeasures fast enough to protect sensitive data across hybrid workforces.

Third, an acute talent shortage compounds these operational and security challenges. **Over half of organizations cite a severe shortage of candidates possessing advanced wireless or AI integration skills.** Growing enterprises find themselves outmatched in the labor market, unable to compete with global conglomerates for elite professionals.

Organizations that confront all three challenges together see substantially stronger returns from their wireless investments. Those attempting to solve problems in isolation remain stuck in operational patterns that resist modernization and drain valuable resources.

To resolve the paradox, leaders must transition away from disparate tools and embrace intelligent platforms. They must deploy unified dashboards and implement networking solutions with native, built-in security protections. Integrating AI directly into the network architecture allows enterprises to automate routine maintenance and enforce security policies dynamically. This holistic approach empowers lean technology teams to elevate their focus from daily troubleshooting to driving strategic business growth.

Organizations moving decisively to resolve this complex paradox in 2026 will capture disproportionate market share.

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

Business leaders increasingly view network infrastructure as a significant determinant of corporate success. Regardless of size or budget, organizations allocate capital with an understanding that their success – or even survival – depends on maintaining robust, continuous access to digital resources.

The historical perception of wireless access as an employee convenience has disappeared. Today, digital infrastructure is tied directly to productivity, competitiveness, and financial outcomes, making wireless connectivity a critical engine for organizational growth.

The demand for robust connectivity accelerates rapidly as organizations scale. Hybrid work models mandate seamless access to corporate resources from multiple physical locations. More devices, more users, more applications, more AI workloads, and more experiences that depend on connectivity. Together, these forces place

immense strain on legacy networks and organizations looking to scale must support enterprise-level expectations without enterprise-level budgets.

To meet these pressures, growing companies are investing ahead of the curve in advanced wireless standards. Adoption of Wi-Fi 6E and 7 is already higher among midsize organizations than larger enterprises (20% vs 17%), despite having leaner IT teams and tighter budgets. This faster uptake highlights how growth-stage firms are pushing for resilient networks that can absorb the demands of AI and IoT, even without the scale advantages enjoyed by their larger counterparts.

Investments in wireless technology generate measurable technical and operational advantages. Organizations that deploy modern wireless standards experience fewer service interruptions and superior application performance. These technical improvements translate directly into business value with employees spending less time waiting for systems to respond and more time executing strategic tasks. Operations run more smoothly; inventory systems update instantly; and customer transactions process

without delay. In short, a modernized network eliminates the friction that slows down daily corporate momentum.

Wireless modernization also helps scale infrastructure capabilities while maintaining strict control over costs and security policies, a challenge that is magnified with growing companies. The rapid growth of connected devices, AI-enabled workloads, cloud applications, and bandwidth-intensive experiences is placing significant strain on wireless environments. These pressures increase operational complexity for lean technology teams, while fragmented management tools and disconnected systems further slow visibility, troubleshooting, and strategic planning. All of which means that lean technology teams spend their days putting out fires instead of designing better network architectures.

To capture the full opportunity presented by modern wireless technology, companies looking to scale must transition away from disparate tools and embrace unified network platforms that simplify deployment and monitoring. Centralized management allows lean teams to oversee sprawling hybrid environments easily, providing the visibility necessary to enforce consistent security policies across all devices. When organizations consolidate their infrastructure tools, they recapture the time and resources needed to drive strategic business growth.

Expanding use cases drive new infrastructure requirements

The diversity of wireless applications continues to expand, with organizations deploying connectivity to support a wide variety of critical business functions.

Software applications hosted in the cloud, for example, depend entirely on reliable local networks. When these applications experience latency, entire departments lose their productivity instantly. Video communication platforms require uninterrupted bandwidth to maintain clear audio and visual quality, with network performance directly dictating the quality of internal collaboration and external client meetings.

Physical premises increasingly rely on wireless sensors and automated systems. Smart office environments utilize connected devices to monitor space utilization, control ambient temperature and manage lighting systems efficiently. These environmental systems generate massive volumes of continuous network traffic.

AI workflows are creating the most significant new infrastructure requirements. Machine learning applications consume vast amounts of data and require minimal network delays to function properly. As enterprises integrate these tools into their daily operations, those with legacy networks struggle to maintain adequate performance. Network architecture needs to evolve quickly to handle these extreme pressures without compromising security or connection speed.

Adding to these pressures is the challenge of managing cloud and on-premises environments without unified visibility. It drains limited resources and makes compliance and audit reporting a constant, heavy burden, with administrators spending hours gathering data from disconnected systems to satisfy strict regulatory requirements. Without built-in network segmentation, organizations struggle to enforce consistent security policies across users, devices, and applications, leaving sensitive data and regulated workloads open to attack.

These expanding use cases are forcing technology teams to reevaluate their core infrastructure strategies. Yesterday's networks simply cannot support tomorrow's applications. Organizations face an inability to scale efficiently and will struggle to grow without re-engineering their core systems, forcing a difficult choice: continue with fragmented legacy tools, or invest in scalable platforms that accommodate rapid technological growth without demanding complete and expensive system redesigns.

The multiplier effect: Wi-Fi drives measurable business value

Strategic wireless investments create a powerful multiplier effect across the organization. A single infrastructure upgrade generates compounding benefits across multiple operational domains, something our survey confirms clearly: when growing businesses upgrade their technology, the entire organization feels the positive impact immediately.

82% of growing businesses achieve operational efficiency gains due to wireless investments, which compares well with the average among small organizations (75%). This is likely because organizations at this scale are large enough for wireless to ripple across multiple functions, yet still compact enough to embed those gains quickly.

Growing businesses also overwhelmingly report gains in employee productivity (80%) due to wireless investments, compared to the average of 75%. Modern connectivity removes the micro-frictions that slow down daily tasks,

with employees no longer waiting for slow applications to load or struggling to collaborate using high-definition video tools. This seamless experience keeps employees focused on their primary business objectives.

That is the upside.

Our research also reveals an anomaly specific to growing businesses: just over half (51%) report a positive impact on revenue from their wireless investments, compared to the average of 68% across all respondents. This deficit exposes a critical challenge in the growing businesses: many successfully utilize technology to optimize their operations but struggle to monetize their investment.

This is in part due to a relative lack of engineering resources, especially the dedicated teams typically needed to build custom revenue-generating applications. Global enterprises are able to deploy large teams to develop location-based marketing overlays and advanced behavioral analytics, for example. Growing businesses, on the other hand, tend to operate with lean or outsourced technology teams. Not only do they lack the capacity to

innovate on the front lines of revenue generation, they also spend their time managing fragmented tools and resolving complex security alerts. This constant firefighting consumes the technical talent needed to drive digital innovation.

Refresh with purpose: Modernization as a strategic foundation

Modernizing wireless infrastructure has shifted from a routine infrastructure upgrade to a strategic foundation for AI readiness, operational automation, integrated security, and scalable digital growth.

As growing organizations embrace AI applications, more connected devices, and hybrid work, legacy networks struggle to deliver the resilience and visibility needed at scale. Modern wireless standards such as Wi-Fi 6E and Wi-Fi 7 deliver faster connectivity while providing the operational foundation for intelligent automation, stronger security, and real-time visibility.

Early adopters of Wi-Fi 6E and Wi-Fi 7 are nearly twice as likely to report the deployment of AI applications and workloads (45% vs 26%) compared to non adopters, along with greater confidence in scaling across devices, sites, and bandwidth intensive applications.

Even with smaller IT teams and tighter budgets, midsize businesses are adopting Wi-Fi 6E and Wi-Fi 7 at higher rates than large enterprises (20% vs 17%), underscoring how modern infrastructure has become the baseline for escaping reactive operations and enabling sustainable growth.

Organizations that refresh infrastructure around business outcomes rather than simply newer standards are better positioned to reduce operational complexity, improve visibility, strengthen security posture, and empower lean teams to focus on strategic initiatives instead of constant troubleshooting.

Wireless strategy in a perfect storm: Navigating the AI paradox

Growing businesses face a profound strategic challenge when it comes to AI, creating a highly complex paradox. AI represents the most promising path to overcoming operational complexity. However, AI simultaneously introduces unprecedented security vulnerabilities and intensifies an already severe talent shortage in the labor market. Organizations must navigate this perfect storm to achieve sustainable financial growth. That navigation requires confronting three deeply interconnected barriers: operational complexity, escalating security threats, and an acute talent shortage.

Technology leaders recognize the potential of automation clearly. More than four in five (81%) leaders in growing businesses would prefer automated wireless networks powered by AI. They understand that machine learning algorithms can analyze network traffic, identify performance anomalies, and resolve issues autonomously.

For a lean technology team, this capability is invaluable, transforming network management from a reactive struggle into a proactive, intelligent strategy.

Deployment reality fails to match this overwhelming desire for automated systems. Only 30% of growing organizations use automated systems for wireless ticket management; the same percentage deploy automation for security monitoring and incident response; and just 25% leverage automation for capacity planning and provisioning. Organizations understand the solution perfectly but lack the ability to implement it, remaining trapped in legacy operational models due to severe resource constraints.

Lean technology teams cannot dedicate the time required to deploy modern automated platforms. They are consumed by the daily demands of keeping the current network functional. This delay creates a dangerous vulnerability: the very technology that promises to save lean teams also arms malicious actors with sophisticated attack tools. Growing organizations often find themselves defending against highly advanced threats without the benefit of automated defense mechanisms.

Growing businesses must resolve this paradox by adopting network solutions that embed AI directly, eliminating the need for complex custom integrations and helping teams escape the troubleshooting cycle. This allows them to elevate their focus from basic maintenance to strategic business enablement, and help them overcome the barriers that prevent them from reaping the rewards of their wireless investments.

Barrier 1: Operational complexity overwhelms current capabilities

Operational complexity severely restricts the potential of growing businesses. Lean technology teams manage fragmented environments across networking, cloud services, and security. The drivers are real and multiplying: rapid growth in mission-critical AI workloads, escalating network security risks, and unpredictable bandwidth surges from high-performance applications. Together they produce tool sprawl that overwhelms lean teams, slows deployment schedules, and transforms basic network troubleshooting into a frustrating, time-consuming process.

Our survey illustrates the severity of this operational strain. Almost every single respondent (98%) from a growth-stage business told us that wireless operations are becoming more complex and nearly half (47%) say their teams handle at least 50 wireless support tickets every week. Large enterprises face this at a slightly higher rate (52%), but with far bigger teams to absorb the load – leaving midsize organizations uniquely exposed to the drag of constant troubleshooting. This volume forces network professionals to spend hundreds of hours managing often minor issues. The consequence is that 55% of teams spend the majority of their time on reactive troubleshooting and incident management.

Three primary drivers accelerate the pressure on technology teams. Mission-critical workloads like AI are increasing, with 43% of teams reporting rapid growth. High-performance applications are testing network limits, with 38% experiencing unpredictable bandwidth surges. And according to 42% of respondents, network security risks are escalating. Together, these demands stretch lean teams to breaking point.

A pervasive lack of visibility exacerbates the problem. Nearly nine in 10 (86%) growing companies face severe visibility gaps that prevent effective troubleshooting. The most significant gap is basic visibility of client devices (44% of respondents) while 39% suffer from poor packet-level visibility. When engineers cannot see the flow of data, they cannot solve performance problems efficiently.

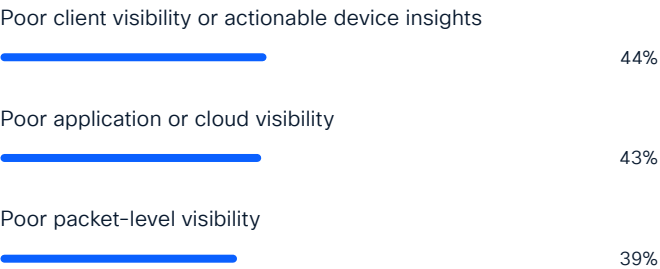
This blindness creates a culture of misattribution. Nearly two thirds (65%) of growing companies report that more than 10% of all technical incidents are wrongly blamed on wireless networks. It means that when a cloud software platform experiences a remote outage, for example, employees immediately report a local wireless failure. Technology teams waste countless hours investigating perfectly healthy networks instead of addressing the real failure.

To escape this complexity, organizations must deliver clarity across the entire digital environment. Administrators need a single interface to manage policies, review security alerts, and monitor application performance. Deploying unified dashboards through a consolidated management approach will help eliminate the friction of tool sprawl and restore operational control to the technology team.

Top complexity drivers in growing enterprises



Top visibility gaps impairing technology teams in growing companies



Barrier 2: Wireless security under siege

Security threats represent an existential risk for growing businesses. Organizations face highly sophisticated attacks but lack the deep financial reserves of massive corporations. They do not, for example, possess the extensive security operations centers found in global conglomerates, but often face the same threats.

This threat environment is hostile and deteriorating rapidly. Nearly nine in 10 (86%) have experienced at least one wireless security incident within the past twelve months. Furthermore, 41% report that security threats have escalated noticeably over the past two years, at a higher rate than both large (34%) and small (33%) organizations. That faster escalation leaves growing firms under greater strain, with lean teams facing a steeper climb against increasingly damaging attacks.

Our research shows that more than half (53%) of midsize organizations reported losses exceeding US\$1 million in the past twelve months, compared with 41% of large enterprises. Larger firms may face greater absolute exposure, but their deeper defenses and broader teams help mitigate risk, making the higher incidence among growing firms a clear signal of disproportionate vulnerability.

These challenges are exacerbated when teams rely on legacy monitoring tools to defend against malicious actors that are constantly adapting their methodologies. More

than a third (36%) identify AI-generated cyberattacks as the primary driver of increased security threats. These automated tools probe networks relentlessly, identifying vulnerabilities with frightening speed. Remote and hybrid work models contribute significantly to this vulnerability – 33% of organizations reported that distributed workforces expand the attack surface drastically.

Unmanaged endpoints connecting to corporate resources are also a major security threat. Additionally, 32% of firms are struggling to secure the rapid proliferation of connected devices across premises and locations. Security protocols that worked five years ago are failing against intelligent, automated attacks while lean teams are battling to combat them with manual tools.

The result can be devastating for a growing company, suffering immediate operational downtime, severe reputational damage and massive financial penalties.

Growing businesses should adopt network solutions that integrate advanced security natively. Every connection must receive rigorous inspection automatically without slowing down the user experience. Zero-trust architectures and automated threat response protocols should play a significant part in helping organizations secure their perimeter. This proactive security posture will help protect brand reputation and ensure compliance with industry regulations.

Top security threat drivers in growing enterprises



AI-generated cyberattacks and automated intrusion tools



Remote and hybrid work models expanding the corporate attack surface



Increased use of connected devices and environmental sensors

Barrier 3: Wireless competition for AI skills

An acute talent shortage threatens the digital progression of growing businesses. Organizations desperately need professionals capable of managing advanced networks, yet they find themselves outmatched in the labor market. They cannot compete with global technology conglomerates or large financial institutions for top-tier engineering talent, creating a capability gap.

The competition for skilled professionals is fierce and unforgiving. Nearly half (49%) of growing companies name AI and machine learning as the top field drawing IT talent away from wireless, followed by cybersecurity (48%) and software engineering or application development (38%).

There are additional and specific financial and structural barriers which prevent growing firms from building their capabilities. Over half (52%) cite a severe shortage of candidates possessing the requisite, advanced wireless or AI integration skills. The labor market simply lacks enough qualified individuals to satisfy corporate demand. Furthermore, four in 10 (40%) of organizations face internal budget constraints or active hiring freezes. They cannot offer the salaries required to attract elite specialists.

Geographic limitations also compound the recruitment problem. More than a third (37%) struggle with geographic constraints or complex remote work challenges during the hiring process. Not only do on-site demands shrink the talent pool, but teammates also need to absorb the workload of personnel working away from HQ. In turn, this drives burnout and accelerates further employee turnover.

Organizations need to acknowledge that their infrastructure challenges cannot be solved purely through recruitment. The traditional process of hiring additional engineers to manage increased network complexity is not working. Instead, organizations must pivot toward technology platforms that require significantly less human intervention. They must invest in smart platforms that automate routine maintenance and enforce security policies dynamically. By focusing on intelligent systems rather than expanding their payroll, growing businesses can secure their digital future.

Top domains attracting talent away from wireless networking



Resolving the paradox

Growing businesses face a paradox that ranks among the most consequential strategic challenges in the modern corporate environment. Wireless infrastructure has become essential to scaling operations, managing distributed workforces, and processing massive volumes of data effectively. AI-enabled applications and intelligent network operations carry the promise of optimizing lean technology teams, enabling them to accelerate digital transformation, automate network management, and streamline complex operations across multiple regions.

Yet delivering on this enormous potential requires business leaders to address simultaneously the three barriers we have identified, while also recognizing that growing businesses do not have access to enterprise-level financial resources.

Barrier one is operational complexity, and it is trapping lean technology teams in reactive troubleshooting patterns. The rapid growth of connected devices, AI-enabled workloads, and bandwidth-intensive applications consumes the limited capacity needed for strategic modernization, while fragmented tools further increase operational friction for lean teams. The second barrier is security, with threats evolving faster than organizations can deploy manual countermeasures. Automated cyberattacks probe networks relentlessly, jeopardizing sensitive data and threatening to inflict financial penalties that smaller organizations simply cannot absorb.

The final barrier is an acute talent shortage which amplifies both challenges while severely constraining the internal resources available to build proactive solutions. Growing businesses find themselves outmatched in the

labor market, unable to compete with global technology conglomerates for elite network engineering professionals.

Addressing one barrier in isolation will not resolve the broader operational paradox. Organizations that modernize infrastructure without automation, security integration, and intelligent management platforms often remain trapped in reactive operational models that continue to drain lean technology teams.

Organizations that align infrastructure modernization, automation, and integrated security are better positioned to convert operational improvements into measurable business value. By reducing operational friction and enabling lean teams to focus on more strategic initiatives, they are more likely to bridge the revenue impact gap identified throughout this report.

The multiplier effect compounds rapidly when all dimensions align: modern infrastructure enables absolute business agility; automation liberates lean teams to focus on more strategic and revenue-generating work; robust security protects corporate data and customer trust; and intelligent platforms ensure sustainable operations without requiring a massive expansion in payroll.

The financial argument is compelling. Organizations deploying modern wireless platforms, AI-enabled automation, and integrated security solutions are better positioned to reduce operational friction and improve organizational agility. By simplifying management environments and reducing the burden on lean technology teams, they can redirect more time toward strategic initiatives instead of reactive troubleshooting. Evidence across the market reinforces this point: organizations that simultaneously address legacy infrastructure and the three barriers are four times more likely to achieve strong wireless ROI (4:1 or higher), with strategic investments delivering compounding returns across multiple dimensions.

This holistic approach empowers growing businesses to punch above their weight, utilizing technology to outmaneuver larger, slower competitors.

The window of opportunity for true competitive advantage is open. Growing businesses acting decisively and holistically in 2026 will establish intelligent wireless connectivity as a strategic foundation for sustainable growth.

Conclusion

In 2026, growing enterprises sit at a critical inflection point. Wireless connectivity drives operational efficiency for 82% of organizations, and 80% report measurable gains in employee productivity. Yet only 51% achieve a positive impact on their revenue from their wireless investments, compared to 68% across all organizations surveyed. That gap is the central problem this report addresses.

Three barriers explain why operational success has not translated into financial returns at the same rate for growing organization as the market average. Operational complexity overwhelms lean teams: 98% of growing organizations say wireless management is growing more complex, and 55% of technology staff spend most of their time on reactive troubleshooting rather than strategic work. Security threats compound the pressure, with 86% experiencing at least one wireless security incident in the past twelve months and AI-generated cyberattacks identified as the fastest-growing threat vector. And a severe talent shortage compounds the challenge further, with 52% unable to find candidates with advanced wireless and AI integration skills. While more than half of growing businesses report positive financial returns from wireless investments, they still trail the 68% average across all organizations surveyed.

Conversely, growing organizations that tackle all three barriers in unison see markedly stronger financial outcomes. By integrating unified network management with AI driven automation and built in security controls, they transform operational efficiency into measurable returns. This holistic approach allows lean teams to move beyond troubleshooting and unlock the full value of their wireless investments.

The path forward requires a strategic shift in thinking. Growing businesses cannot solve infrastructure challenges by hiring more engineers or adding more tools. They need intelligent platforms that reduce the burden on lean teams and convert wireless connectivity from an operational cost into a measurable growth driver. Organizations that make that transition in 2026 will be better positioned to compete against larger rivals in the decade ahead.

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 four recommendations that, when implemented together, can break the reactive cycle and potentially unlock four times ROI advantage.

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 AI and automation

Organizations should prioritize building toward AI for networking to break the reactive cycle that constrains wireless teams. Organizations must go beyond simple AIOps or AI-assisted insights (e.g. alerts, recommendations) to AI-driven autonomous actions that diagnose and resolve issues at machine speed. The operational benefits of AI with autonomous actions 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 AI with automation 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 set 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. Mature AI networking strategies can then lead to zero-touch, fully autonomous network operations capable of supporting increasingly demanding workloads. With AI itself cited as the top field drawing talent away from wireless, AI 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 AI with autonomous actions across key functions achieve substantially higher ROI.

Investing in AI for networking helps to stitch together context from across the network providing end-to-end visibility and observability. With 87% of organizations

reporting visibility gaps that impair effective Wi-Fi troubleshooting, it's 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 operations. AI requires rich data inputs to make effective operational decisions, so organizations should view broad and deep visibility as a prerequisite for AI for networking.

3

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 as a priority for managing business risk, which means looking at wireless security in the context of the entire business. 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.
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.

4

Strengthen and sustain wireless talent

Organizations should invest in developing their talent through training, certification, and career advancement opportunities. For smaller teams, this investment has an outsized impact across security outcomes, incident response times, and job satisfaction.

Investment should target advanced skills, including optimizing Wi-Fi 6E and 7 standards, security protocol modernization (WPA3), AI implementation, and automation platform expertise. In growing organizations, these skills can help a small team, or even a single specialist, handle multiple responsibilities.

Midsized organizations also need to recognize wireless specialization as a strategic role and compensate accordingly, given that the impact of certification is quantifiable. In growing organizations, retaining the small number of individuals with this expertise is essential.

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. For small teams, this means avoiding burnout and operational bottlenecks. Delaying investment leads to higher reliance on external consultants and costly disruption.

Beyond direct investment in talent, midsized organizations should look at investment in AI with automation (specifically Recommendation 2) to reduce reactive workload and free capacity for strategic tasks. This improves morale and makes wireless roles more sustainable, reversing talent drain to AI fields.

The multiplier effect: Why integrated implementation matters

These four recommendations compound when they are implemented together:



Modern infrastructure without AI and automation = overwhelmed teams



AI 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

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 AI paradox will not resolve itself. Organizations that act decisively and holistically in 2026 will establish competitive advantages that compound over the years to come. Organizations 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.

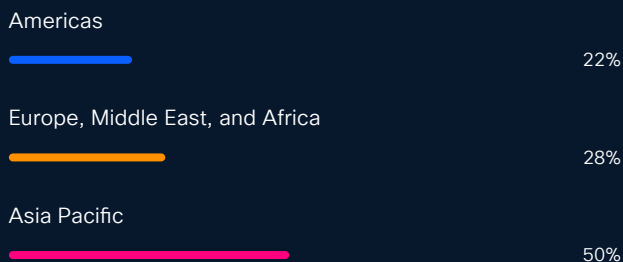
Methodology



This research comprised interviews with 6,098 organizations, including 1,843 midsize organizations 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.



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)