State of Wireless 2026

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

Executive summary

Wireless connectivity has evolved from a back-office necessity in retail environments to a strategic growth platform that shapes every dimension of the shopping experience.

Modern retailers depend entirely on robust, resilient networks to serve customers, empower employees, manage inventory, and protect sensitive payment data. The stakes are exceptionally high: a network failure during peak shopping hours can halt transactions, frustrate customers, and drive sales to competitors. Security breaches expose payment information, destroy customer trust and can invite scrutiny from regulators.

Retail organizations recognize this imperative. More than 84% of retail organizations report that wireless investments have had a positive impact on operational efficiency, eight in 10 (80%) see employee productivity improvements, and more than three quarters (77%) report enhanced customer engagement from wireless investments. For an industry operating on thin margins and facing intense competition from digital-native competitors, wireless is increasingly the foundation on which retail excellence rests.

Yet retail leaders face a paradox that is both opportunity and threat. Wireless is essential for deploying artificial intelligence applications that can support critical functions including optimizing inventory, personalizing the customer experience, and predicting demand patterns.

However, these same AI capabilities introduce unprecedented complexity, create new security vulnerabilities, and intensify competition for specialized talent. Retail organizations need advanced wireless skills precisely when attracting talent to this domain has become increasingly difficult.

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

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

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

Retail spending on wireless infrastructure continues to accelerate. Organizations have invested heavily in wireless over the past five years, recognizing that reliable connectivity directly impacts customer satisfaction, employee effectiveness, and revenue generation. Looking ahead, the momentum intensifies. While more than a fifth (27%) of retail organizations report budget increases of more than 50% over the past four to five years, an even more substantial 33% expect budget increases exceeding 50% over the next four to five years. This represents one of the highest anticipated investment increases across all industries surveyed.

This investment is not speculative. Retail leaders understand that wireless enables use cases that are essential to modern commerce. Mobile point-of-sale systems allow employees to complete transactions anywhere on the sales floor, reducing checkout friction and improving customer satisfaction. Real-time inventory tracking systems enable staff to locate products instantly, reducing customer wait times and preventing lost sales. Guest wireless access keeps shoppers connected while they browse, enabling them to research products, compare prices, and access digital loyalty programs. IoT sensors monitor refrigeration systems, track merchandise movement, and optimize store layouts based on traffic patterns.

Emerging uses further illustrate wireless as strategic growth driver. Retailers are deploying autonomous robots to monitor inventory. These robots depend entirely on wireless connectivity to navigate safely and communicate with inventory management systems. Smart building technologies use wireless sensors to optimize lighting, temperature, and energy consumption, improving customer comfort while reducing operational costs.

Space analytics applications use wireless-enabled cameras to understand customer flow, identify congestion points, and reallocate staff to improve service levels during peak hours.

For retailers, wireless modernization directly translates into business impact. Retail organizations report that 84% see improvements in operational efficiency, 80% report employee productivity gains, and more than three-quarters (77%) see improved customer engagement from wireless investments. When retailers prioritize wireless strategically, aligning investments with customer experience priorities and operational goals, they achieve a multiplier effect: one investment in modern wireless infrastructure yields measurable returns across multiple dimensions simultaneously, including faster transaction processing, higher staff effectiveness, improved customer satisfaction, and stronger financial outcomes.

Infrastructure modernization is accelerating this effect. Retail leaders understand that aging wireless standards such as Wi-Fi 5 cannot support the requirements of contemporary retail operations. Only 22% of retail organizations have fully deployed Wi-Fi 6E or Wi-Fi 7 so far, with a further 57% plan implementation within the next year. This adoption trajectory reflects growing recognition that the6 GHz spectrum provides the clean bandwidth for mobile point-of-sale systems, high-definition digital signage, real-time inventory tracking, and the proliferation of IoT sensors throughout stores. Organizations deploying 6 GHz spectrum show measurably higher rates of AI application deployment compared to non-adopters, suggesting that advanced wireless infrastructure is a prerequisite for innovation in today's retail environment.

Retail organizations are leveraging wireless across a variety of use cases

	Currently deployed (%)	Planning to deploy (%)
Space Analytics and Optimization (Footfall)	49%	47%
Indoor Wayfinding	52%	42%
Operational Visibility and Flow Analytics	57%	41%
Supply Chain and Inventory Intelligence	59%	40%
AI Applications and Workloads	58%	40%
Real-time Asset and Equipment Tracking	58%	39%
Guest Wireless	60%	37%
Customer and User Experience Enhancement	63%	36%
Physical Security (CCTV)	63%	33%

Current footprint = Deployed + Pilot stage

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

The wireless AI paradox in retail

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

On one hand, organizations deploying AI applications recognize wireless as strategically critical to retail operations. Nearly two-thirds (62%) of leaders whose organizations are deploying AI view wireless as strategically critical, compared to 46% of organizations not deploying AI. This heightened recognition reflects reality:

- AI workloads demand higher performing, more resilient wireless networks than traditional applications
- Inventory optimization systems require real-time connection to point-of-sale data
- Customer behavior analytics tools need continuous access to traffic flow patterns
- Automated systems for predicting demand, optimizing product placement, or personalizing promotions all depend on reliable, low-latency connectivity.

Retailers that integrate wireless optimization into their AI deployment strategies realize substantially stronger returns. More than three quarters (77%) of retail organizations deploying AI report positive impacts from wireless investments on revenue, exceeding non-AI organizations by meaningful margins. This performance demonstrates that AI and wireless are mutually reinforcing investments in retail environments.

All of that said, however, AI is simultaneously amplifying the very challenges that prevent retail organizations from realizing wireless potential. The same AI technologies that enable customer personalization are also creating operational complexity for almost every (97%) retail organization, with new security threats and intensified competition for talent preventing them from achieving the full benefit of wireless modernization.

This paradox is especially acute in retail because the consequences of failure are exceptionally high. A security

breach in retail does not simply compromise data; it disrupts payment processing, violates PCI compliance standards, triggers substantial regulatory penalties, and destroys the customer trust that is fundamental to repeat business.

Similarly, an operational failure that slows network response times does not simply reduce productivity: it can halt transactions during peak shopping periods, prevent inventory replenishment, or compromise loss prevention systems.

The financial, regulatory, and competitive stakes make the wireless AI paradox one of the most pressing strategic challenges retail leaders face.

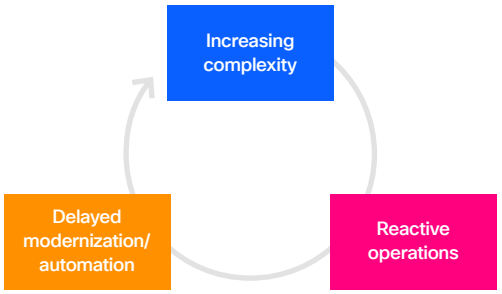
Barrier 1: Operational complexity overwhelms current capabilities

Nearly every retail wireless leader (97%) reports that operational complexity is escalating, representing a structural transformation of the operational environment. Retail organizations cite three primary drivers of this growing complexity. The need to support mission-critical IT, IoT, and OT workloads ranks first, reported by 43% of respondents. This reflects the operational demands created by mobile point-of-sale systems that cannot lose connectivity, inventory tracking systems that demand real-time accuracy, and AI tools that require continuous access to sales data.

Security risks follow closely at 41%, reflecting the expanded attack surface created by payment systems, customer devices connecting to guest networks, and IoT sensors throughout stores. Rising bandwidth demands from new use cases add to the challenge at 39%, with high-definition digital signage, video analytics, and streaming content consuming bandwidth that previous generations of wireless infrastructure could not supply.

This complexity manifests in tangible operational strain. Nearly half (42%) say their teams receive at least 50 tickets per week on average. This ticket volume means IT teams spend hundreds of hours each month managing wireless issues rather than implementing strategic improvements. The situation worsens when examining how that time is spent. More than 57% of retail wireless teams spend most of their time on reactive troubleshooting and incident management, addressing urgent problems as they arise rather than preventing problems through proactive planning and optimization.

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



A critical factor amplifying this challenge is the lack of visibility. 86% of retail organizations report visibility gaps that impair their ability to troubleshoot Wi-Fi issues effectively. The most frequently reported visibility challenges in retail are poor application or cloud visibility (44%), followed by poor packet visibility (39%) and poor client visibility (39%). Without clear sight into network behavior at each layer, from access point to application, retail IT teams cannot rapidly isolate problems.

Wireless networks often become scapegoats for problems originating elsewhere. More than 62% of retail respondents report that at least 10% of incidents are inaccurately attributed to wireless. Each misattributed incident wastes an average of 18 hours across teams. Those wasted troubleshooting hours translate directly into delayed attention to actual problems and extended periods of degraded service during peak shopping hours.

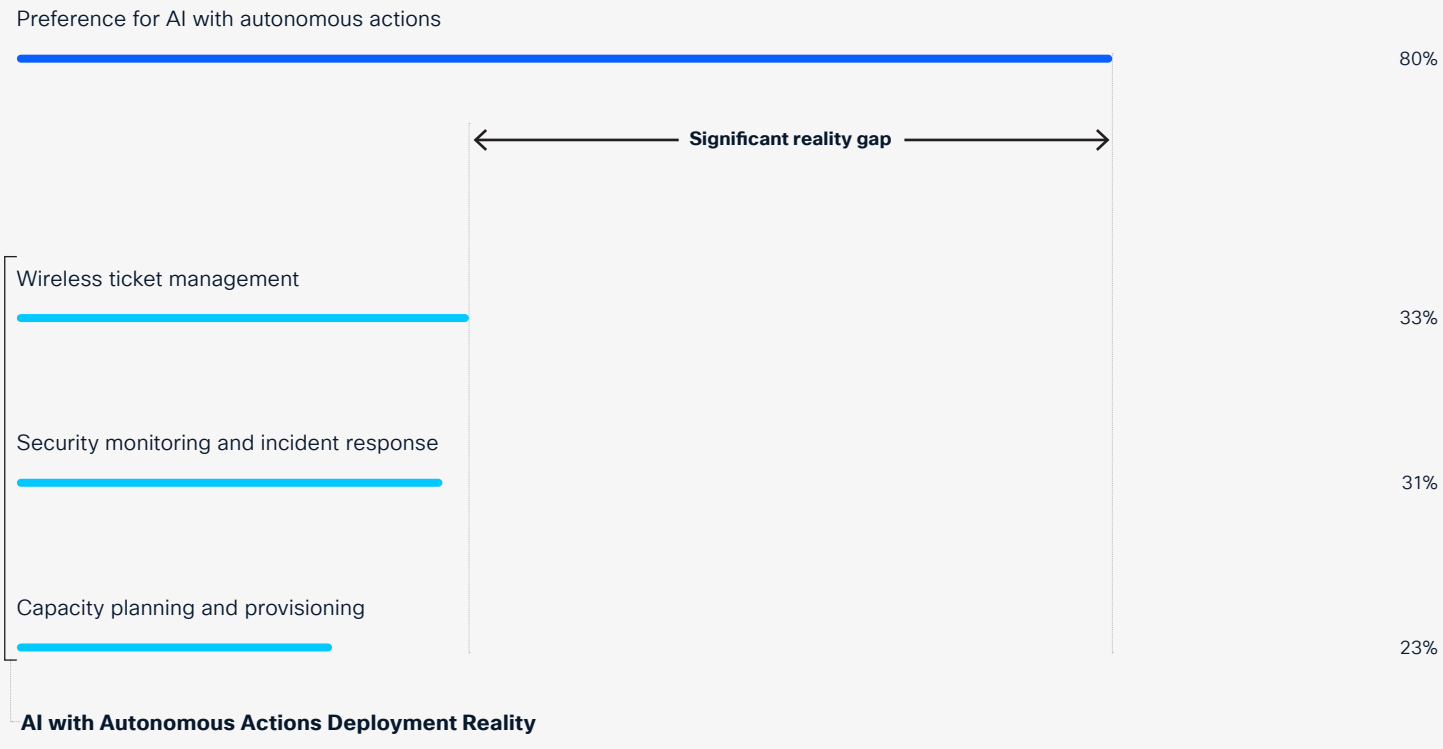
In response to this escalating complexity, retail wireless leaders overwhelmingly believe that AI represents the most promising path forward. More than 80% would prefer AI with automation to ‘fully’ or ‘mostly’ handle routine wireless operational tasks. The appeal is clear: automation would free retail-focused IT professionals to work on strategic priorities rather than handling repetitive ticket

work. AI systems could detect and resolve many incidents before humans become aware problems exist, maintaining service continuity during critical shopping periods.

Yet a significant gap separates preference from reality. Only a third (33%) of retail organizations have implemented automation for wireless ticket management, 31% automate security monitoring and incident response, and less than a quarter (23%) have deployed automation for capacity planning and provisioning. Retail leaders recognize the solution but lack the resources, expertise, or organizational readiness to implement at scale.

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

The AI gap in retail: Desire versus reality



Barrier 2: Wireless security under siege

Retail faces intensifying security threats that are more frequent, more damaging, and more difficult to detect and remedy than in previous years. 86% of retail organizations have experienced at least one wireless security incident in the past 12 months, and 38% report escalating wireless threats over the past two years. These organizations expect the situation to deteriorate further, with 70% anticipating increased wireless security incidents over the next two years.

Retail security threat environment

The threat environment in retail is distinctive and alarming. Research revealed five critical contributors to increased security vulnerability in retail:

1. AI-generated or automated cyberattacks rank as the leading driver of increased wireless security threats at 33%. These attacks can identify network vulnerabilities in payment systems, adapt attack strategies in real time based on defensive responses, and operate at a scale and speed far exceeding human capabilities.
2. Remote and hybrid work models have expanded the attack surface at 31%, creating unmanaged endpoints as corporate staff access retail systems remotely, often through less secure connections.
3. Difficulty managing multiple security layers and segmentation at 27% reflects the challenge of maintaining separate, secure networks for payment processing, guest access, employee devices, and IoT systems within the same physical environment.
4. Increased use of IoT and connected devices at 26% creates proliferating vulnerabilities, as individual device weaknesses in sensors, cameras, and tracking systems compound into network-wide exposure.
5. Lack of skilled personnel or bandwidth to monitor and respond to threats at 25% amplifies all other vulnerabilities, as understaffed teams cannot maintain vigilant security monitoring during extended retail operating hours.

For the retail sector, the implications of compromised IoT or OT devices are particularly severe. A third (33%) of affected retail organizations report disruption from compromised IoT or OT devices. In a retail environment, this means a point-of-sale terminal becomes unreliable, digital signage displays malicious content, inventory tracking systems provide false data, or security cameras fail to record theft incidents. These are not abstract IT problems; they are revenue-impacting operational failures.

The financial impact is staggering with more than half (54%) of retail organizations reporting financial losses from wireless security incidents. More than 45% experienced losses exceeding US$1 million in the past year. These losses compound through multiple channels. Direct losses include breach remediation, forensic investigation, and incident response costs. Indirect losses include loss of customer trust (35%), regulatory penalties or compliance consequences (33%), and reputational damage that extends far beyond the immediate incident. For retailers, customer trust is irreplaceable; once lost, it is extraordinarily difficult to rebuild, and research revealed 35% of retail organizations have already lost that trust.

Financial losses from wireless security incidents in retail

Less than US$1 million	46%
US$1-10 million	20%
US$10-50 million	22%
Over US$50 million	4%

Despite these threats, 85% of retail organizations report that they are doing enough to protect wireless networks, yet 70% expect security failures to increase over the next two years. This paradox reflects a gap between executive perception and frontline reality: executives perceive their organizations as adequately protected, while technical staff managing the networks understand the actual threat environment and the limitations of current defenses.

Retail organizations cite four primary barriers to improving wireless security: implementation complexity, performance concerns, lack of skilled personnel, and legacy infrastructure concerns. These barriers do not exist in isolation and reflect the broader wireless challenges that retail faces. Operational complexity makes security implementation difficult during extended operating hours. Talent shortages mean organizations lack the specialized expertise needed to deploy modern security protocols. Visibility gaps prevent security teams from understanding the actual threat environment across distributed retail locations.

The result is a widening vulnerability gap, which means that even as threats escalate, retail organizations remain constrained by outdated systems, complexity, and talent limitations, slowing security modernization and eroding resilience. The competitive pressure is particularly acute in retail, where security failures can immediately drive customers to competitors who are perceived as more trustworthy.

Barrier 3: Wireless competition for AI skills

Retailers face an acute talent crisis that directly inhibits modernization and exacerbates both complexity and security challenges. 89% of retail organizations report difficulty hiring wireless professionals with the skills required for modern network operations. This is not a minor hiring challenge; this is a structural problem affecting the sector's ability to maintain and modernize network infrastructure across distributed store locations.

The talent competition is fierce and asymmetrical. AI and machine learning rank as the number one domain attracting IT talent away from wireless, with 49% of retail organizations identifying this as a primary competitor for staff. Cybersecurity follows in second place at 48%, reflecting the high visibility and rapid career growth in that field. Cloud infrastructure and DevOps (42%) also pull skilled professionals away from wireless. Retail organizations lose their best wireless talent to roles perceived as more innovative, better compensated, and more aligned with technology industry priorities.

Retail talent competition and hiring challenges

Domains attracting talent away from wireless

AI / Machine learning	49%
Cybersecurity	48%
Cloud Infrastructure/DevOps	42%

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	35%

The root cause is straightforward. A shortage of candidates with advanced wireless or AI-integrated skills ranks as the primary barrier to hiring wireless talent for 51% of our respondents. There simply are not enough people with deep wireless expertise in the labor market, particularly those who also understand retail-specific requirements such as PCI compliance, distributed network management, and high-density connectivity in customer-facing environments. Making matters worse, internal budget constraints and hiring freezes further limit recruitment at 37%. The result is a skills gap that translates into higher operating costs (47%, the highest among all industries surveyed), lower morale among wireless teams (37%), and reduced capacity for innovation (31%).

The correlation between talent shortages and poor outcomes is unmistakable. Organizations struggling to hire wireless specialists expect wireless security failures to increase at substantially higher rates, and they already experience significantly higher costs for security incidents annually than those facing no recruitment challenges.

Wireless resilience in retail starts with certified expertise. 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% more likely to implement full WPA3 security, reducing exposure to legacy threats. They are also 17% more likely to use certificate- or profile-based authentication, minimizing access conflicts and lowering troubleshooting volume during peak shopping hours.

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

Conclusion

Retail organizations face a paradox that is among the most consequential strategic challenges in the industry. Wireless is essential to modern retail operations and customer experience excellence. AI-driven applications promise to optimize inventory, personalize customer engagement, and streamline operations. Yet realizing this potential requires retail leaders to address three deeply interconnected barriers simultaneously.

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

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

The financial case is compelling. Retail organizations deploying modern wireless infrastructure, automation, security protocols, and certified talent are substantially more likely to achieve strong wireless ROI. They experience lower security incident costs, they resolve operational issues faster, and they achieve better customer satisfaction scores that translate directly into repeat business and revenue growth.

The window for competitive advantage is now. Retail organizations that act decisively and holistically in 2026 will establish wireless as the strategic foundation of customer excellence for the next decade. Those that delay will find themselves trapped in reactive cycles, struggling with escalating security incident costs, and unable to capitalize on AI-driven transformation while competitors advance. In an industry where customer loyalty is won and lost in moments, the organizations that move first to resolve the wireless AI paradox will capture disproportionate market share and profitability in the years ahead.

Methodology

This research comprised interviews with 6,098 organizations, including 472 in retail, across 30 markets. It was conducted in November 2025 by Sandpiper Research and Insights.

Research Scope

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

Americas — 22%

Europe, Middle East, and Africa — 28%

Asia Pacific — 50%

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

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

Timing: Research was conducted in November 2025.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

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