State of Wireless 2026

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

Manufacturing

Executive summary

Wireless connectivity has evolved from a supporting technology in manufacturing to mission-critical infrastructure that drives operational excellence and competitive advantage. Modern facilities depend on robust, resilient networks to coordinate production systems, enable autonomous machinery, manage supply chains, and protect sensitive operational technology.

The stakes are high: a network failure can halt production lines, disrupt guided vehicles, and compromise safety systems. Security breaches expose industrial control systems, violate integrity, and risk severe financial and safety consequences.

Manufacturers recognize this imperative. Over four in five report efficiency gains (81%), three-quarters (79%) enhanced customer engagement, and 78% improved employee productivity from wireless investments. Nearly three-quarters (73%) also see positive revenue impacts, exceeding the global average of 68%. For an industry under pressure from global competition, supply chain complexity, and rapid Industry 4.0 adoption, wireless has become the foundation of manufacturing excellence.

Leaders face a paradox: wireless is essential for deploying AI applications that optimize scheduling, enable predictive maintenance, and coordinate autonomous systems. Yet these same AI capabilities introduce complexity, create new security vulnerabilities across IT and OT, and intensify competition for specialized talent. Manufacturers need advanced wireless and AI-integrated skills precisely when attracting talent has become more difficult.

This report explores this paradox in the manufacturing sector. It examines how manufacturers can harness strategic wireless investments to unlock a multiplier effect, delivering measurable returns across operational efficiency, production quality, worker safety, and financial performance. It also identifies three interconnected barriers that currently prevent many manufacturing organizations from realizing the full potential of their wireless infrastructure: mounting operational complexity driven by converged IT and OT environments; escalating security threats targeting industrial control systems; and acute talent shortages as skilled professionals gravitate toward AI and cybersecurity roles. 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 manufacturing

Spending on wireless infrastructure in the manufacturing sector continues to accelerate across global markets. Organizations have invested heavily in wireless over the past five years, recognizing that reliable connectivity directly impacts production uptime, operational safety, and quality outcomes. Looking ahead, this investment looks set to increase.

More than a quarter (28%) of manufacturing organizations report budget increases of more than 50% during this timeframe. That trend looks set to continue with more than a third (34%) telling us that they expect budget increases of at least 50% over the next four to five years, signaling that wireless will play an increasingly critical role in manufacturing competitiveness and innovation.

Manufacturing leaders understand that investing in wireless enables use cases that are essential to modern production. Automated guided vehicles and autonomous mobile robots depend on seamless connectivity to navigate factory floors, transport materials between production stages, and coordinate with manufacturing execution systems. Real-time asset and equipment tracking systems enable managers to locate critical tools, monitor work-in-progress inventory, and prevent costly misplacement incidents.

Mobile devices in the hands of production workers provide immediate access to digital work instructions, quality control data, and safety protocols, reducing errors and improving throughput. IoT sensors monitor machine health, track environmental conditions, and alert maintenance teams to potential failures before they cause unplanned downtime.

New applications highlight wireless as a strategic growth catalyst in manufacturing. Robotic systems for welding, assembly, and material handling depend on ultra-reliable, low-latency connectivity to coordinate safely with human workers and machinery. Smart factory technologies use wireless sensors to optimize energy consumption, monitor air quality, and adjust climate control for precision production. Digital twin applications stream data from

equipment to create virtual replicas of processes, enabling engineers to simulate changes, predict outcomes, and optimize operations without disrupting the factory floor.

For the manufacturing sector, wireless modernization translates directly into business impact. Manufacturers report the highest average positive impact (78%) across operational efficiency, employee productivity, customer engagement, and revenue generation when compared to the complete global dataset. When manufacturers prioritize wireless and align investments with production priorities, operational technology requirements, and safety goals, they achieve a multiplier effect: one investment in modern wireless infrastructure yields measurable returns across multiple dimensions simultaneously. This can include a reduction in unplanned downtime, higher equipment effectiveness, improved worker safety, accelerated time-to-market for new products, and stronger financial outcomes.

Modernizing wireless infrastructure accelerates manufacturing transformation. Leaders recognize that aging standards like Wi-Fi 5 cannot support the density of connected devices, real-time video analytics, or the latency needs of autonomous systems. Already, 10% of manufacturers have deployed Wi-Fi 6E, with 28% planning rollouts in the next 12 months. Meanwhile, 9% have adopted Wi-Fi 7 and 31% plan to implement it within a year – the highest rate across all industries surveyed. These figures reflect manufacturers' understanding that the 6 GHz spectrum and Wi-Fi 7 deliver the clean bandwidth, performance, and ultra-reliable connectivity required for guided vehicles, collaborative robots, and time-sensitive production control. Organizations using 6 GHz spectrum also show higher rates of AI deployment, underscoring advanced wireless as a prerequisite for Industry 4.0 innovation.

Manufacturers are leveraging wireless across a variety of use cases

	Currently deployed (%)	Planning to deploy (%)
Physical Security (CCTV)	62%	36%
Internet of Things	59%	38%
Operational Visibility and Flow Analytics	57%	41%
AI Applications and Workloads	57%	41%
Real-time Asset and Equipment Tracking	57%	41%
Supply Chain and Inventory Intelligence	55%	42%
Customer and User Experience Enhancement	54%	44%
Remote Worker Connectivity	54%	44%
Guest Wireless	52%	46%

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

The wireless AI paradox in manufacturing

Manufacturing leaders face a central strategic tension that defines the wireless opportunity over the next two to three years. Artificial intelligence is both the leading driver of wireless return on investment and the primary source of escalating challenges that constrain those returns.

Our research shows that organizations recognize wireless as strategically critical in the deployment of AI applications. 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 real-world needs:

- AI workloads demand higher performing, more resilient wireless networks than traditional manufacturing applications.
- Predictive maintenance systems require continuous access to sensor data from production equipment throughout the factory floor.
- Quality control AI analyzes real-time video streams from inspection cameras to detect defects at speeds impossible for human inspectors.
- Production optimization tools need immediate connectivity to manufacturing execution systems, enterprise resource planning databases, and supply chain management platforms.
- Automated systems for coordinating autonomous vehicles, optimizing production schedules, or managing energy consumption all depend on reliable, low-latency connectivity that cannot tolerate interruption.

Manufacturers that are able to optimize wireless as part of their AI rollouts are seeing significant outcomes. More than three quarters (77%) of organizations deploying AI told us they had seen positive impacts from wireless investments on revenue generation, exceeding non-AI organizations by 13%. This demonstrates that AI and wireless are mutually reinforcing investments in manufacturing environments, where production uptime and operational efficiency translate directly to competitive advantage.

However, AI is simultaneously amplifying the very challenges that prevent manufacturing organizations from realizing the full potential of their investment in wireless. The same AI technologies that enable predictive maintenance and autonomous coordination are also creating operational complexity for nearly every (98%) manufacturing organization, with new security threats and intensified competition for talent preventing them from achieving the full benefit of wireless modernization.

This paradox is particularly acute in manufacturing because the consequences of failure extend beyond financial impact to operational safety and regulatory compliance. A security breach in manufacturing does not simply compromise data; it disrupts production control systems, threatens worker safety, enables theft of intellectual property, and can violate industrial control system security standards such as ISA/IEC 62443. An operational failure that degrades network performance does not simply reduce productivity: it can cause collisions between autonomous vehicles, delay time-sensitive production processes, or prevent safety systems from responding to hazardous conditions.

The financial, safety, and competitive consequences make the wireless AI paradox one of the most pressing strategic challenges facing leaders in the manufacturing sector.

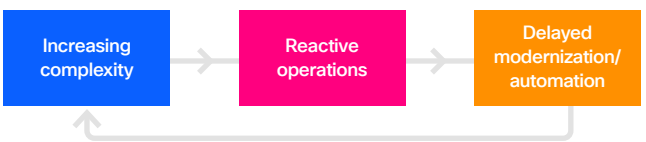
Barrier 1: Operational complexity overwhelms current capabilities

Nearly every manufacturing wireless leader (98%) reports that operational complexity is on the rise and represents a transformation of the operational landscape that reflects the convergence of information technology and operational technology networks on manufacturing floors.

Manufacturers identified three main drivers of growing network complexity. Security tops the list for 41%, reflecting expanded attack surfaces where compromised devices threaten both data integrity and physical safety. An equal share (41%) point to the demands of mission-critical IT, IoT, and OT workloads — increasingly AI-driven — from production control systems that cannot tolerate downtime to autonomous vehicles requiring ultra-reliable handoffs and diagnostic tools needing real-time sensor data. Finally, 35% cite client unpredictability, as diverse mixes of fixed equipment, mobile devices, autonomous systems, and legacy industrial technologies must coexist on modern manufacturing networks.

This complexity creates real strain for support teams. More than one third (38%) of manufacturing organizations report that their wireless support teams receive at least 50 tickets per week on average, representing hundreds of hours spent each month managing wireless issues rather than implementing strategic improvements. The situation intensifies when we delve into how that time is spent. More than half (52%) 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 focused on production continuity.

This reactive approach creates a cycle that reinforces itself and is particularly damaging in manufacturing environments where unplanned downtime carries immediate financial consequences. Complexity drives reactive work. Reactive work demands all available resources and attention. Strategic work, including infrastructure modernization, protocol optimization for industrial applications, training on OT security requirements, and certification programs, gets deferred.



As modernization is delayed, complexity persists and often increases as new production equipment, additional IoT sensors, and more autonomous systems are added to networks designed for simpler connectivity requirements. Teams remain trapped, unable to escape the reactive cycle that prevents them from implementing solutions that would reduce complexity.

A significant barrier to tackling this challenge is the lack of visibility across converged IT and OT environments. More than four in five (82%) manufacturing organizations report visibility gaps that impair their ability to troubleshoot Wi-Fi issues effectively, slightly below the global average but representing millions of hours wasted across the industry. The most frequently reported visibility challenges in manufacturing are poor client visibility or actionable insights (39%), followed by poor application or cloud visibility (38%), and poor packet visibility (31%).

Without clear insight into network behavior at each layer from access points through industrial protocols to production applications, support teams cannot rapidly isolate problems that can span office networks, production control systems, and factory floor equipment.

Wireless networks often become scapegoats for problems originating elsewhere. An autonomous vehicle navigates erratically. More than half (56%) of respondents in manufacturing report that at least 10% of incidents are inaccurately attributed to wireless, with each misattributed incident wasting an average of 18 hours. Those wasted hours of troubleshooting translate directly into delayed attention to actual problems and extended periods of production uncertainty during critical manufacturing windows.

As a response to escalating complexity, our respondents overwhelmingly believe that AI represents the most promising path forward. More than four in five (81%) would prefer AI with automation to fully or mostly handle routine wireless operational tasks – a percentage that matches the global average across industries.

82% face visibility gaps, including:

Poor client visibility	39%
Poor application/cloud visibility	38%
Poor packet visibility	31%

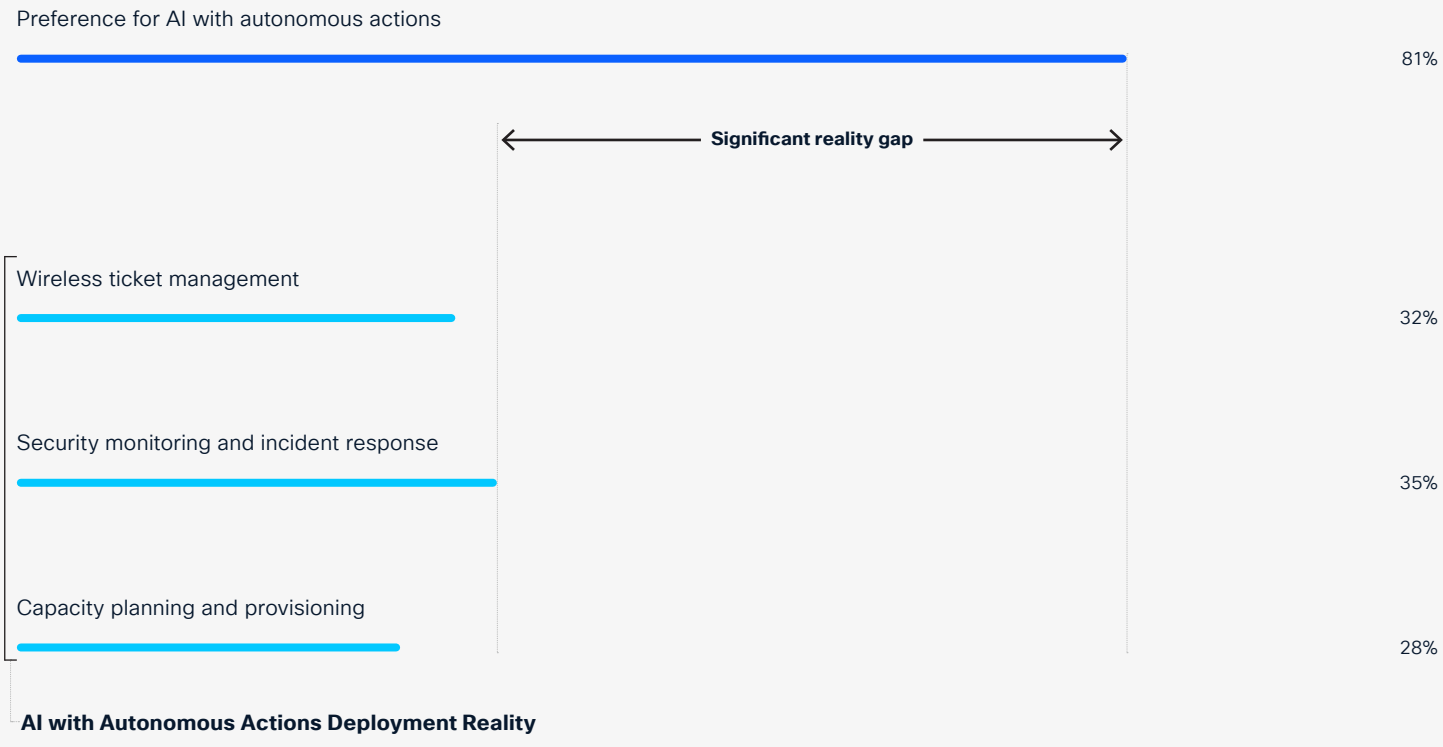
The appeal is straightforward: automation would free manufacturing-focused IT and OT professionals to work on strategic priorities directly supporting production goals rather than handling repetitive support tickets that divert time and attention from more productive uses of their time. AI systems could detect and resolve many incidents before humans become aware problems exist, maintaining service continuity during continuous production operations where downtime costs can exceed thousands of dollars per minute.

Despite recognizing the value of AIOps, there is a significant reality gap, with just a third (32%) of manufacturing organizations having implemented automation for wireless ticket management. That said, manufacturing organizations are starting to use AI for security monitoring and incident response which, at 35%, is the highest percentage of all sectors surveyed and reflects manufacturers' recognition that security failures in converged IT and OT environments carry consequences extending to production safety. However, only 28% have deployed automation for capacity planning and provisioning. Manufacturing leaders recognize the solution but face constraints implementing at scale across distributed factory sites with diverse production equipment, legacy industrial systems, and operational technology requirements that differ fundamentally from enterprise IT environments.

The impact on manufacturing performance is measurable and directly affects production outcomes. Organizations that have implemented autonomous AI 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 and resolve wireless tickets 12% faster than manual operations.

Scaling these benefits would translate into thousands of hours freed for proactive, strategic initiatives each month. Yet that scaling remains constrained by the very complexity and talent shortages that AIOps would help resolve, particularly in manufacturing environments where IT and OT staff must collaborate across organizational boundaries and technical specializations that have historically operated independently.

The AI gap in manufacturing: Desire versus reality



Barrier 2: Wireless security under siege

Manufacturing organizations face security threats that are more frequent, more damaging, and more difficult to detect and remedy than in previous years. The threat environment is particularly severe in manufacturing because wireless networks in factories carry both information technology traffic and operational technology communications that directly control production equipment, autonomous vehicles, and safety systems. More than four in five (84%) manufacturing organizations have experienced at least one wireless security incident in the past 12 months, slightly below the global average but representing substantial risk across an industry where compromised control systems can threaten worker safety and production integrity.

More than one third (38%) report escalating wireless threats over the past two years, saying they have become more frequent, damaging, and difficult to detect and remedy. Significantly, manufacturing organizations show more measured expectations for future threats, with 65% anticipating increased wireless security incidents over the next two years, the lowest rate across all industries surveyed. This may reflect either stronger confidence in security measures or potentially underestimation of evolving threats targeting industrial control systems and operational technology environments.

Manufacturing security threat environment

The threat environment in manufacturing is worrying, with attacks increasingly targeting the convergence of information technology and operational technology systems. Research revealed five critical contributors to increased security vulnerability in manufacturing:

1. AI-generated or automated cyberattacks rank as the leading driver of increased wireless security threats at 33%, matching the global sector average. These attacks identify vulnerabilities in industrial control systems, adapt attack strategies in real time based on defensive responses, and can work at a scale and speed far exceeding human capabilities.
2. Increased use of IoT and connected devices ranks second at 29%, reflecting the proliferation of sensors, cameras, autonomous vehicles, and smart equipment throughout manufacturing facilities.
3. Lack of skilled personnel or bandwidth to monitor and respond to threats are also at 29%, the highest rate across all industries surveyed.
4. Poor user practices, human error, and insider risks also tie at 29%. Manufacturing environments face unique challenges where production workers, contractors, maintenance technicians, and temporary staff connect personal devices to factory networks, often with minimal security training or awareness of how compromised devices can threaten production control systems.
5. Remote and hybrid work models expanding the attack surface also stand at 29%. As manufacturing organizations enable engineers to access production data remotely and provide contractors with network access for equipment maintenance, the perimeter that once protected factory networks has dissolved, creating new vulnerabilities.

For manufacturing, the implications of compromised IoT or operational technology devices are particularly severe and extend beyond typical IT security incidents. More than one third (36%) of affected manufacturing organizations report disruption from compromised IoT or OT devices, matching the global average but representing far more severe consequences in manufacturing contexts.

The financial impact can be severe. More than half (52%) of manufacturing organizations have experienced financial losses from wireless security incidents, slightly below the global average but representing substantial costs across an industry where production downtime and compromised

quality carry immediate bottom-line consequences. More than two in five (43%) report losses exceeding US$1m dollars in the past year, with 19% experiencing losses between US$10m and US$50m and 7% absorbing losses exceeding US$50m.

Financial losses from wireless security incidents in manufacturing

Less than US$1 million	33%
US$1-10 million	21%
US$10-50 million	19%
Over US$50 million	7%

These figures capture only direct costs such as remediation, forensic investigation, production recovery, and incident response. Indirect impacts compound the damage: 32% of manufacturers report loss of customer trust, while an equal share face regulatory penalties or compliance consequences. In manufacturing, security incidents can violate industrial control standards, trigger OSHA investigations if injuries occur, and compromise intellectual property tied to proprietary processes.

Despite these risks, 83% of organizations express confidence in current wireless protections, yet 65% simultaneously predict rising failures over the next two years. This contradiction reflects a gap between executive leaders, who view defenses as adequate based on approved policies and investments, and technical staff, who see firsthand how evolving threats and the limits of IT security tools leave operational technology exposed.

Manufacturing organizations note three primary barriers to improving wireless security: implementation complexity (55%), legacy infrastructure (51%), and performance concerns (50%). However, these barriers carry distinctive weight in manufacturing contexts. Operational complexity makes security implementation difficult across environments where production cannot be interrupted for security system deployment. Legacy infrastructure constraints are particularly acute in manufacturing where operational technology equipment may operate for decades and cannot be easily replaced or patched. Performance concerns reflect manufacturing's need for reliable network behavior where security measures cannot introduce unpredictable latency that might disrupt time-sensitive production control communications.

These barriers do not exist in isolation but reflect the broader wireless challenges that manufacturing faces. Talent shortages mean organizations lack the specialized expertise needed to deploy modern security protocols across converged IT and OT environments. Visibility gaps prevent security teams from understanding the actual threat environment spanning office networks, production control systems, and factory floor equipment with fundamentally different communication patterns and security requirements.

The net result is a vulnerability gap which continues to expand, and means that even as threats escalate, manufacturing organizations remain constrained by outdated systems, complexity spanning IT and OT domains, and talent limitations.

Barrier 3: Wireless competition for AI skills

Manufacturing faces a significant talent crisis that impedes modernization and aggravates both complexity and security challenges. More than four in five (86%) manufacturing organizations report difficulty hiring wireless professionals with the skills required for modern network operations. This represents a structural problem affecting the sector's ability to maintain and modernize infrastructure spanning office networks, production control systems, and factory floor equipment with increasingly demanding connectivity requirements.

Talent competition in manufacturing is both fierce and unequal, with the sector vying not only against other industries but also against specialized technical domains. AI and machine learning are the top draw, pulling IT talent away from wireless in 52% of organizations – the highest rate across all industries surveyed – reflecting manufacturing's heavy investment in predictive maintenance, quality control, production optimization, and autonomous systems.

Cybersecurity follows at 47%, driven by the visibility of escalating threats and career growth in protecting converged IT and OT environments. Software engineering and application development ranks third at 40%.

The root cause is straightforward but particularly acute in manufacturing. A shortage of candidates with advanced wireless or AI-integrated skills ranks as the primary barrier to hiring wireless talent for half (50%) of respondents, matching the global average. However, manufacturing requires an even more specialized skill set: deep wireless expertise combined with understanding of industrial protocols, operational technology requirements, and manufacturing-specific challenges such as electromagnetic interference from production equipment, latency requirements for autonomous systems, and ultra-reliable handoff needs for mobile assets moving at high speeds through factory environments.

Labor markets simply lack sufficient professionals with this combination of wireless knowledge and operational technology expertise.

Geographic limitations or remote work challenges compound the problem at 37%, the highest rate across all industries surveyed, reflecting manufacturing's need for on-site presence at factory locations. Lengthy hiring processes or internal bottlenecks affect 34% with a resulting skills gap that translates into higher operating costs (40%, the highest rate compared to other industries), lower morale among wireless teams (34%), and reduced capacity for innovation (32%).

The correlation between talent shortages and poor outcomes is clear, and carries direct consequences for production operations. Organizations struggling to hire wireless specialists expect wireless security failures to increase at substantially higher rates. In manufacturing contexts where security failures can compromise production control systems and threaten worker safety, talent constraints directly impact operational risk management and regulatory compliance with industrial control system security standards.

The implication is clear. Manufacturing organizations that invest early in talent gain competitive advantage as complexity increases. Those that delay investment until talent shortages become acute face substantially larger hiring costs, extended project timelines, and reduced capacity to modernize factory networks supporting Industry 4.0 innovations. In manufacturing, where the cost of delayed modernization includes both financial losses from security incidents and lost competitive advantage as rivals deploy more advanced autonomous systems and AI-driven optimization, this investment becomes mission critical for maintaining production competitiveness in global markets.

Manufacturing talent competition and hiring challenges

Domains attracting talent away from wireless

AI / Machine learning	52%
Cybersecurity	47%
Software Engineering and Application Development	40%

Primary reasons for difficulty in hiring wireless talent

Shortage of candidates with advanced wireless or AI-integrated skills	50%
Geographic limitations or remote work challenges	37%
Lengthy hiring process or internal bottlenecks	35%

Conclusion

Manufacturing organizations face a dilemma that ranks among the most consequential strategic challenges for leaders in the industry. Wireless infrastructure has become essential to modern production excellence, autonomous system coordination, and quality management.

AI applications promise to optimize production scheduling, enable predictive maintenance that prevents costly unplanned downtime, and coordinate autonomous vehicles throughout factory floors. Yet realizing this potential requires manufacturing leaders to address three deeply interconnected barriers simultaneously rather than sequentially.

Operational complexity traps IT and OT teams in reactive cycles, preventing modernization of converged networks supporting both office systems and production control equipment. Security threats escalate faster than organizations can deploy defenses to combat threats which not only threaten data integrity but also worker safety and production continuity. Talent shortages amplify both challenges while limiting the resources available to address them.

Yet manufacturing organizations that address all three barriers simultaneously achieve substantially higher returns on wireless investments, capturing the multiplier effect where one network upgrade generates simultaneous improvements across production uptime, equipment effectiveness, worker safety, quality outcomes, and financial performance. They experience stronger improvements in operational efficiency (81% versus 78% average), faster equipment troubleshooting when wireless connectivity is suspected, lower security incident costs, and improved employee satisfaction as teams shift from reactive firefighting to strategic optimization supporting production goals.

The financial case is persuasive. Manufacturing organizations deploying modern wireless infrastructure, automation capabilities, security protocols, and certified talent are substantially more likely to achieve strong wireless ROI, with 73% reporting positive revenue impacts, significantly exceeding the 68% industry average. They experience lower security incident costs, they resolve operational issues faster, and they achieve better production outcomes including reduced unplanned downtime, higher equipment effectiveness, and improved product quality that translate directly into competitive advantage and market share gains.

The window for competitive advantage is now. Manufacturing organizations that act in 2026 will establish wireless as the strategic foundation of production 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 with more autonomous operations, better predictive maintenance, and faster time-to-market for new products.

Methodology

This research comprised interviews with 6,098 organizations, including 531 in manufacturing, 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**