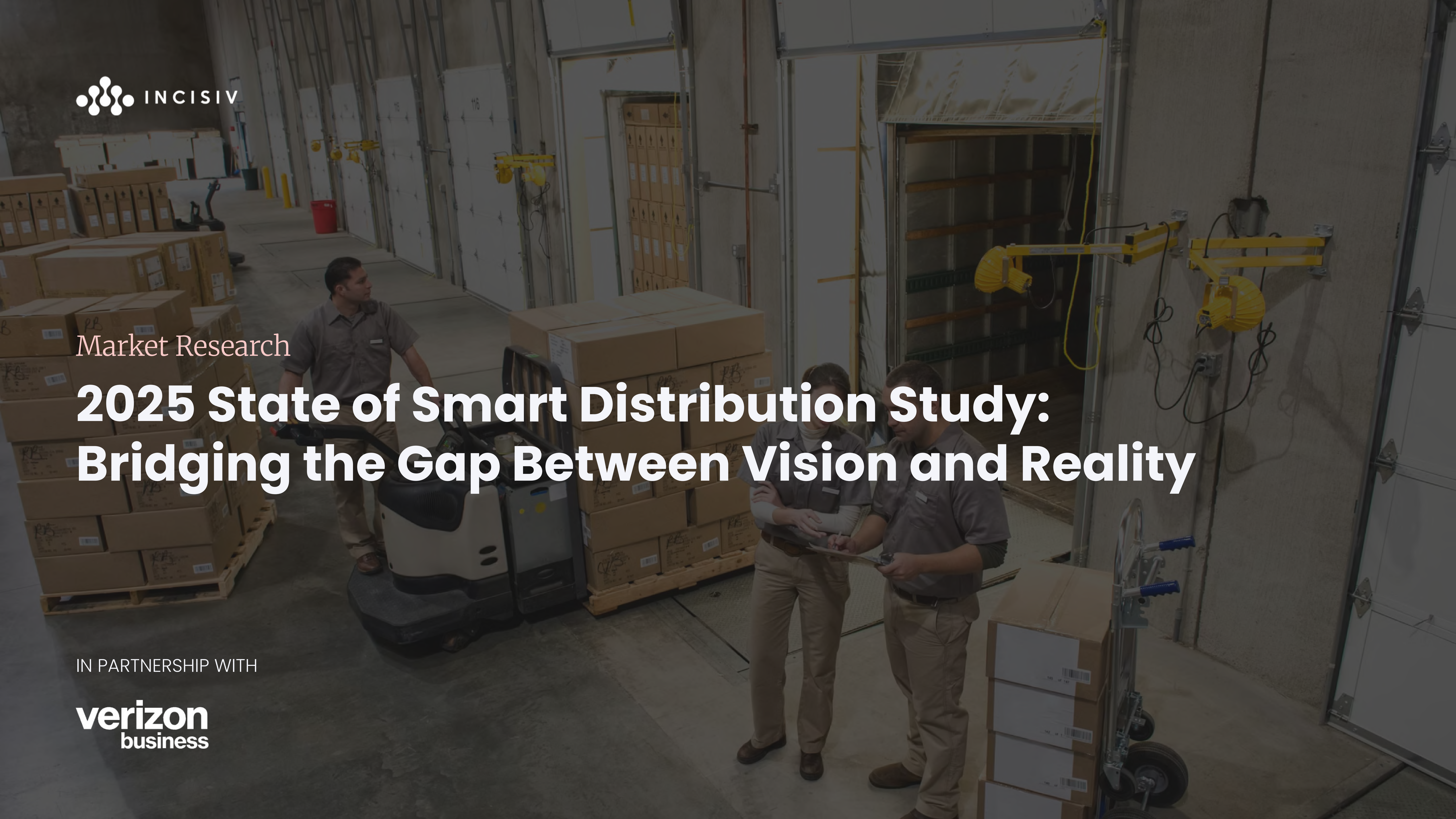


Market Research

2025 State of Smart Distribution Study: Bridging the Gap Between Vision and Reality

IN PARTNERSHIP WITH

Executive summary

Distribution is at a crossroads. Automation, AI, and digital tools are scaling fast, but improvements in connectivity, cybersecurity, and integration are necessary to support continued expansion.

The 2025 State of Smart Distribution Study shows the industry facing multiple challenges: supply chain disruptions, labor shortages, cost escalation and technology complexity. While automation in warehouses and DCs is advancing, AI strategies remain fragmented, and many leaders lack the network foundation needed to orchestrate robotics, IoT, and fulfillment systems at scale. Private wireless is emerging as the network foundation for throughput, reliability, and data protection.

Winners will not be those who adopt the most tools, but those who integrate them seamlessly. Closing today's connectivity, orchestration, and execution gaps is what will separate tomorrow's resilient distribution leaders from those left managing disruption.

Note: Respondents in the survey were involved in or responsible for distribution operations

Why did we do this research?

Incisiv and Verizon conducted this study to explore how distribution leaders across retail, manufacturing, and logistics are addressing operational challenges, scaling automation, and strengthening networks. The survey captures priorities, technology adoption, and infrastructure readiness, providing an executive view into where investments are being made and where execution gaps remain.

143

51% Manufacturing and logistics warehouses executives

49% Retail distribution center executives

Company size

8% < $100 million

25% $100 million - $499 million

24% $500 million - $999 million

26% $1 billion - $4.9 billion

17% $5 billion+

Executive title

5% SVP/EVP/CXO

20% VP

60% Director/Supervisor

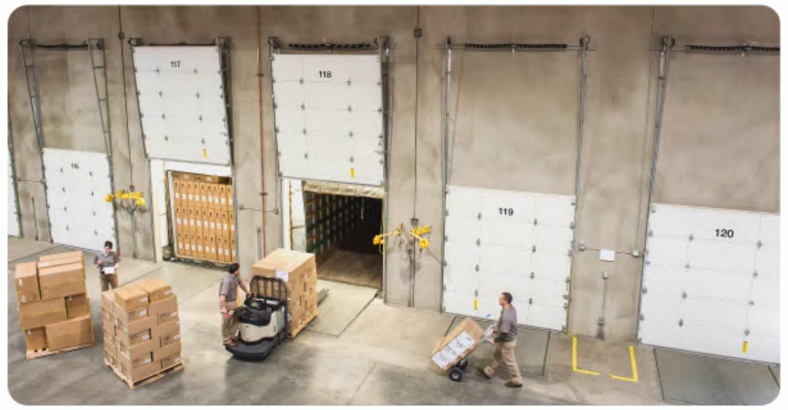
15% Manager

Note: Respondents in the survey were involved in or responsible for distribution operations

KEY RESEARCH INSIGHTS

Distribution leaders are betting on automation and AI. Closing connectivity and integration gaps is the key to unlocking value.

Automation scales within blended work environments



Distribution centers are layering automation onto manual workflows rather than replacing them outright.

Conveyors, autonomous mobile robots (AMR) and automated storage and retrieval systems (ASRS) are scaling in pockets, creating blended environments that require orchestration across tasks like picking, put-away, and dock operations.

85%

of warehouse/DC leaders report the adoption of mobile workforce tools

AI is critical but deployments lag

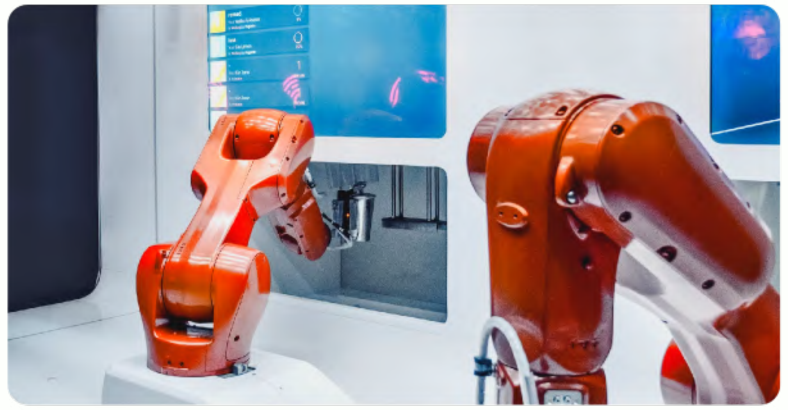
Executives view AI as central to forecasting, labor scheduling, and anomaly detection, but most lack a clear strategy for deployment.

This gap is widening the divide between business optimism and IT readiness, slowing enterprise adoption.

89%

say AI is necessary to compete, however, 41% state that budget allocations are a concern for AI execution

Connectivity gaps block scaling of automation reliably



Dead zones across aisles, racks, and yards disrupt mobility and automated flows, leading to delays and rework.

Without seamless connectivity, scaling robotics, mobile devices, and vision systems across facilities is severely constrained.

62%

say current networks cannot support planned deployments

Integration challenges limit operational efficiency

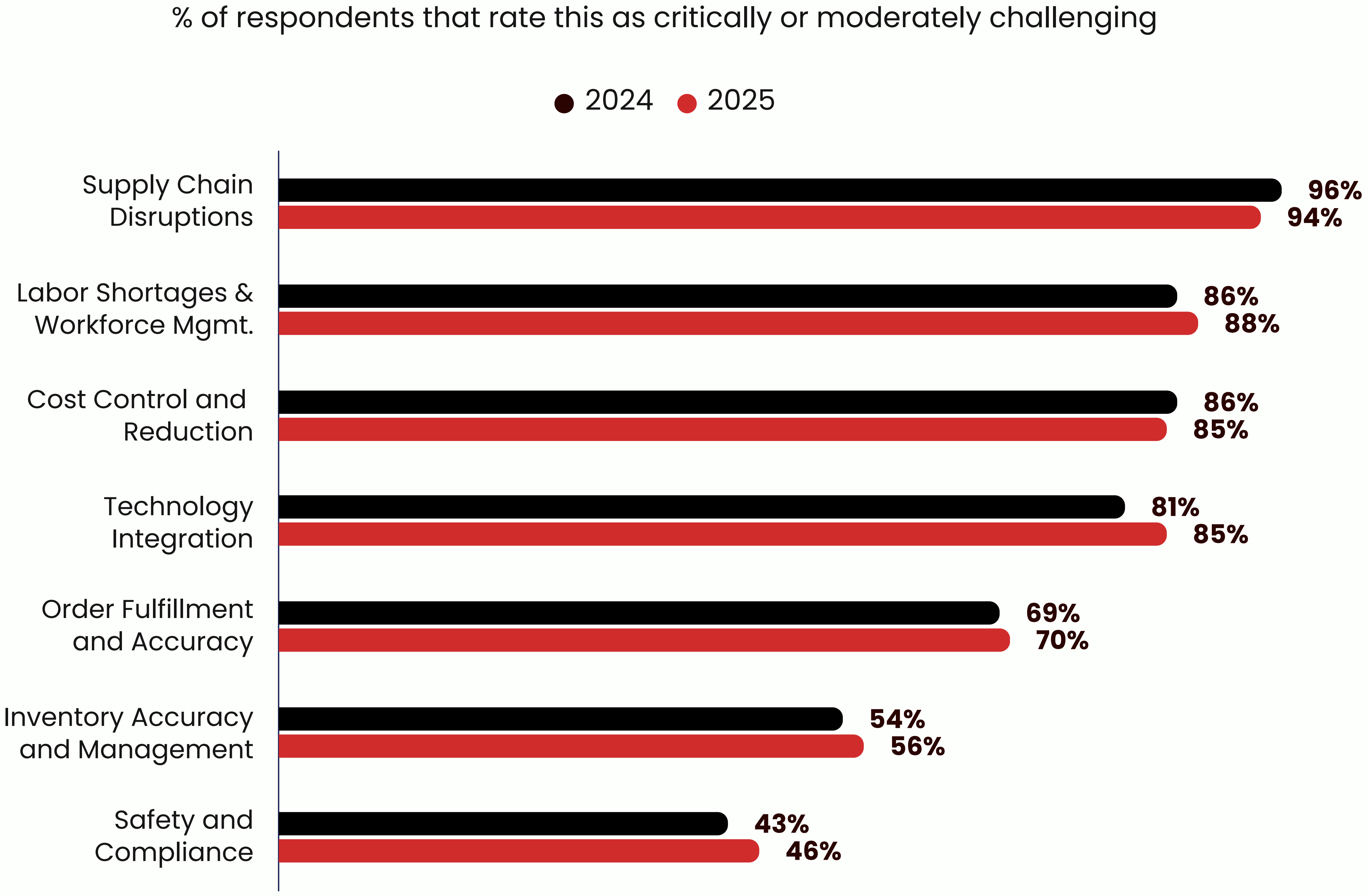
As more technologies are deployed, integration across WMS, WES, and partner systems is emerging as the hardest mile.

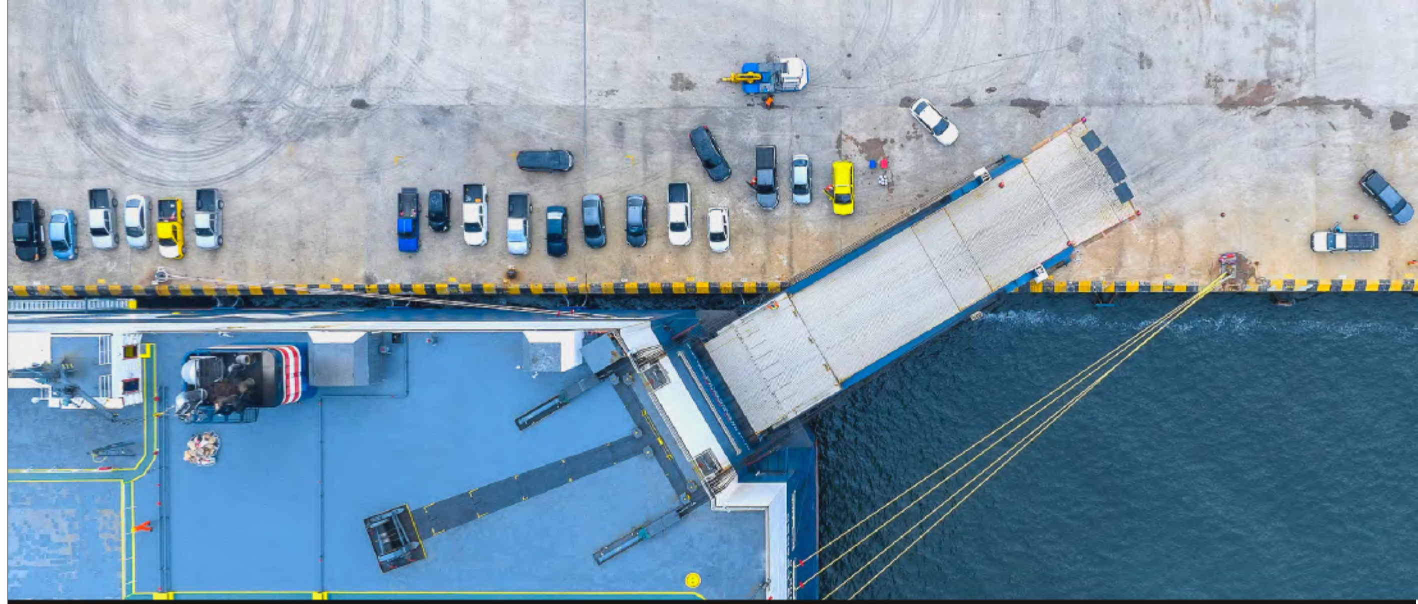
Poor interoperability reduces visibility and slows the execution of critical workflows, from inventory control to order fulfillment.

85%

cite technology integration as a major challenge

Supply chain disruptions dominate, while labor shortages and cost pressures intensify operational strain





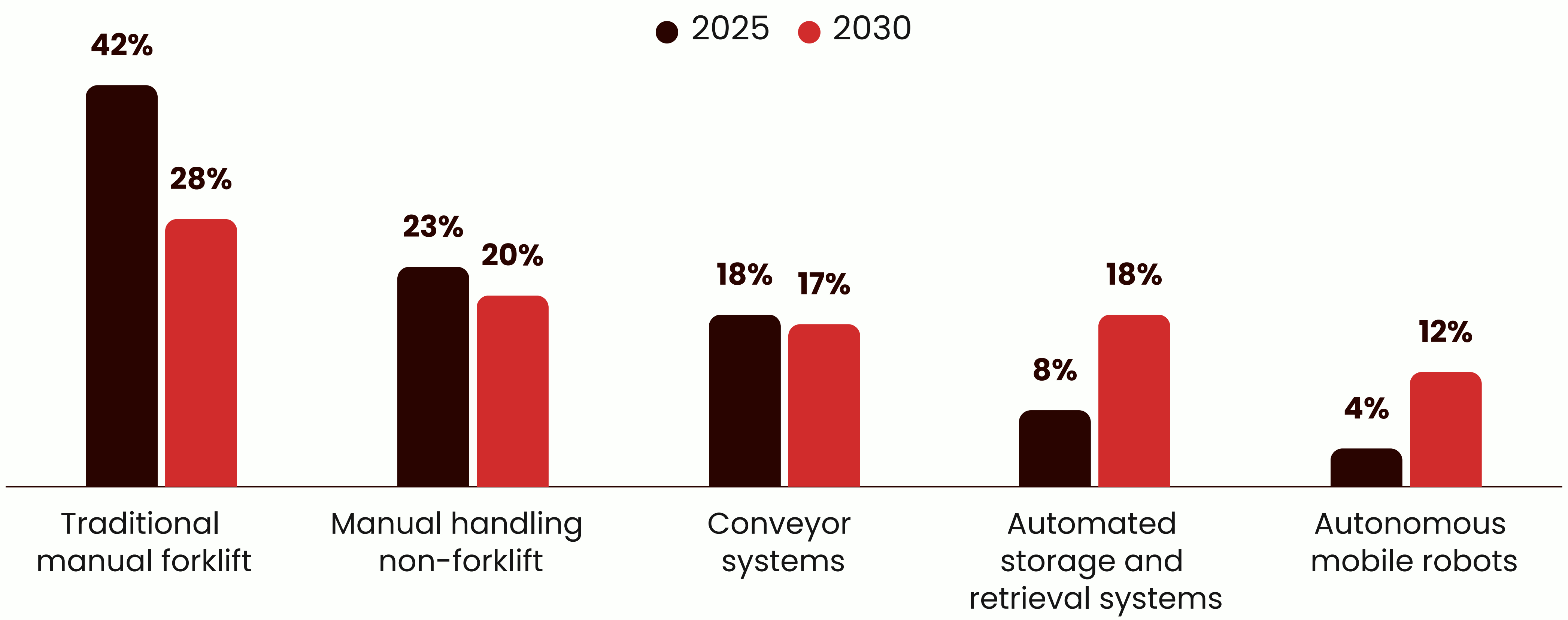
Supply chain disruptions remain the most pressing challenge, with leaders citing them as a persistent driver of instability. Demand swings often trigger the bullwhip effect, where small changes in customer orders amplify upstream, disrupting inventory positions and fulfillment cycles.

Labor shortages and rising costs follow closely. Recruiting and retaining workers in high-turnover roles such as picking, packing, and dock operations remain difficult, while wage pressures, energy costs, and automation investments intensify the financial strain.

Technology integration, order fulfillment, and inventory accuracy rank lower but are still viewed as critical enablers of resilience. Executives point to advanced planning systems, warehouse integration, and reliable connectivity as essential to closing these structural gaps.

Material handling shifts from manual forklifts to AMRs, ASRS, and robotics as automation gains momentum

% of material handling performed by various methods

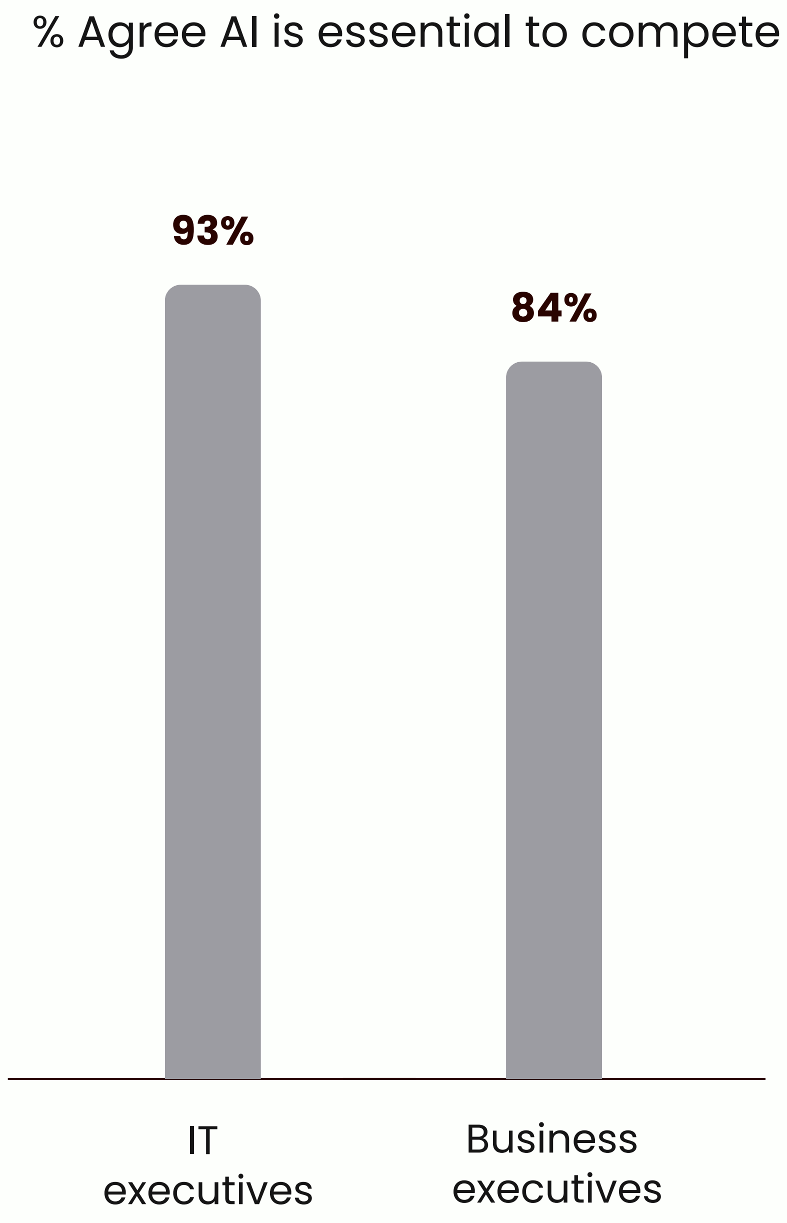


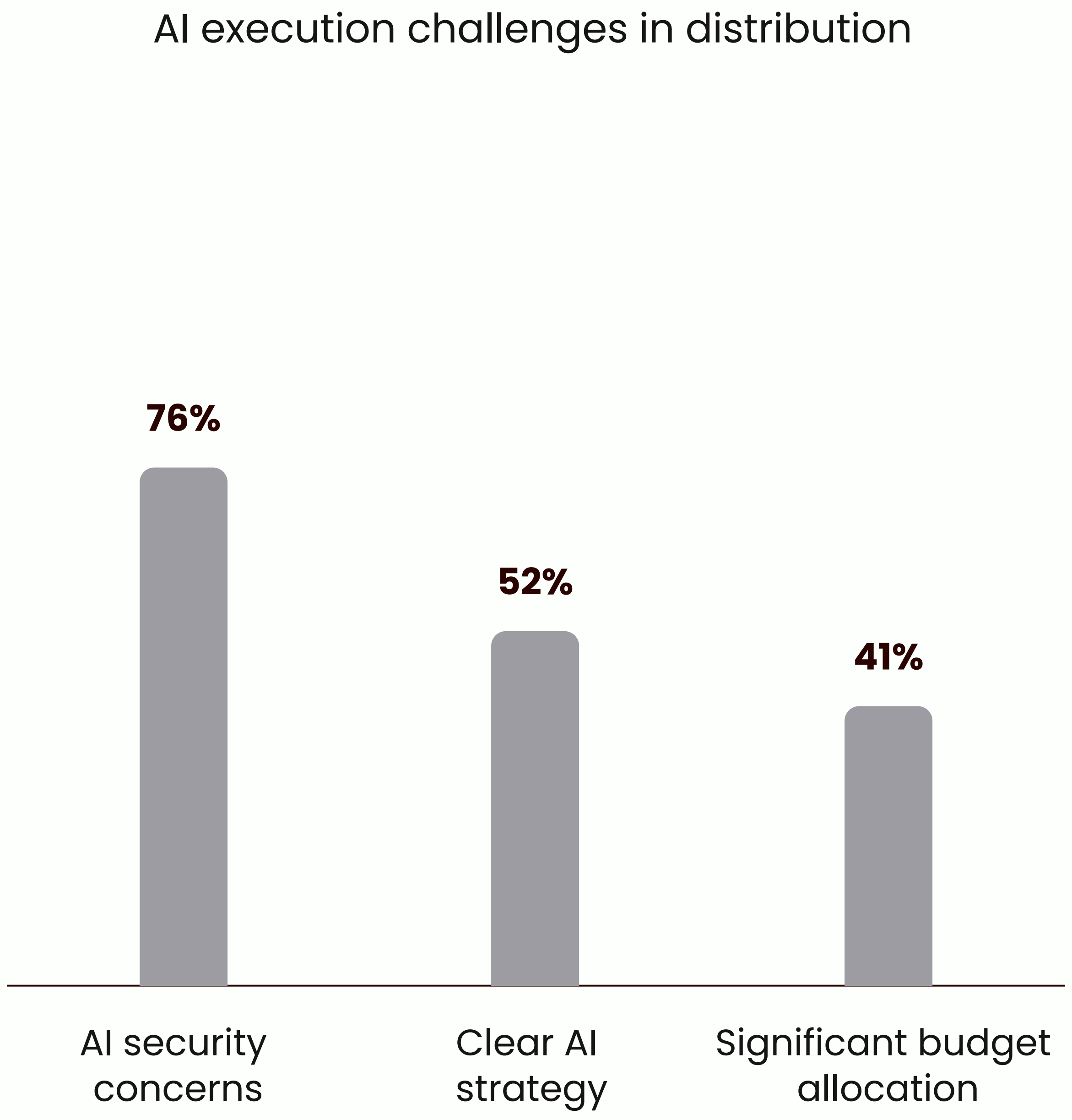
Material handling continues to rely heavily on manual labor and forklifts, which dominate throughput because of their flexibility and familiarity. Yet this dependence comes at a cost, as skilled operators grow harder to recruit and retain.

By 2030, the balance is shifting as conveyors expand their role as high-volume backbones, Autonomous Mobile Robots (AMRs) take on dynamic picking and put-away, and Automated Storage and Retrieval Systems (ASRS) establish footholds in high-bay storage. Robotic palletizing and depalletizing are reducing repetitive, injury-prone dock operations, strengthening both safety and efficiency.

This evolution is not wholesale replacement but a blended model. Manual handling, conveyors, and robotics will coexist, requiring seamless orchestration across warehouse management systems (WMS), warehouse execution systems (WES), and resilient connectivity to sustain performance.

AI recognition grows, but gaps in strategy, budget, and IT–business alignment stall execution



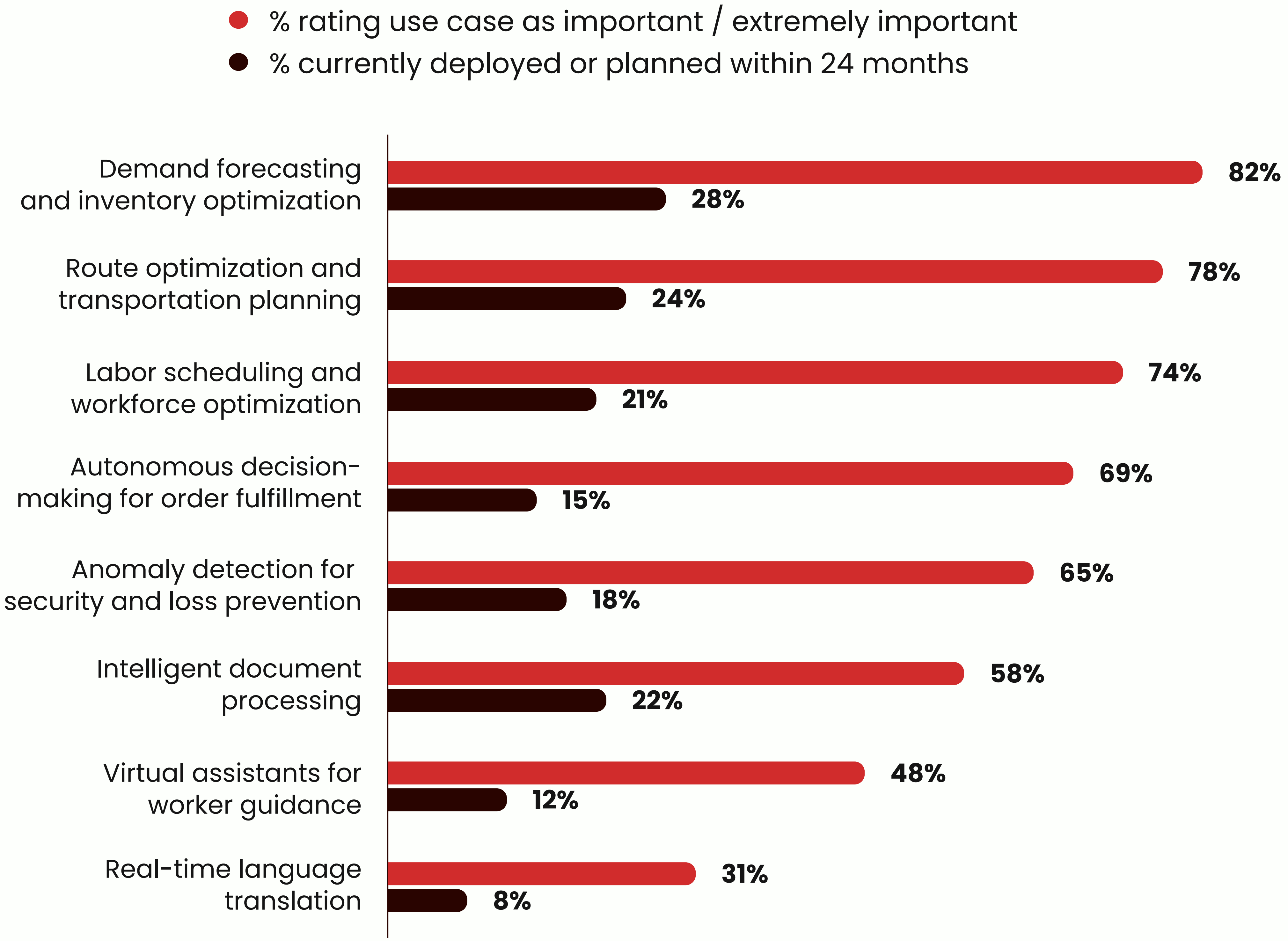


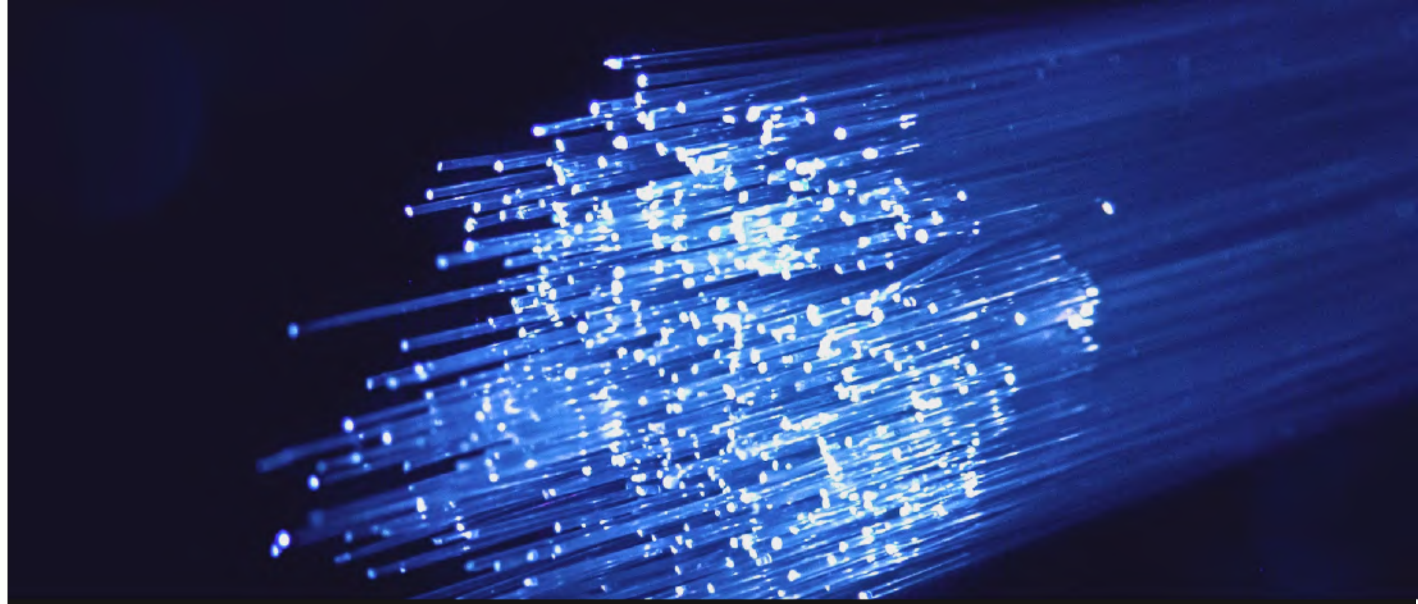
AI is now widely seen as a competitive necessity in distribution, with nearly nine in ten executives acknowledging its importance. This marks a steady increase from last year (84% to 89%), confirming that AI has moved from an emerging concept to a board-level priority.

Yet recognition has not translated into execution. Fewer than half of organizations report having a clear AI strategy or meaningful budget allocation. Security concerns remain a significant barrier, with many leaders citing uncertainty around governance and ROI measurement. The result is a widening gap between ambition and implementation.

This gap is most evident between IT and Business functions. IT leaders report greater clarity and optimism, particularly around use cases like forecasting, route optimization, and anomaly detection. Business leaders, by contrast, remain cautious, reflecting less confidence in readiness and slower commitment to investment.

AI deployment trails strategic priorities, leaving critical use cases underserved





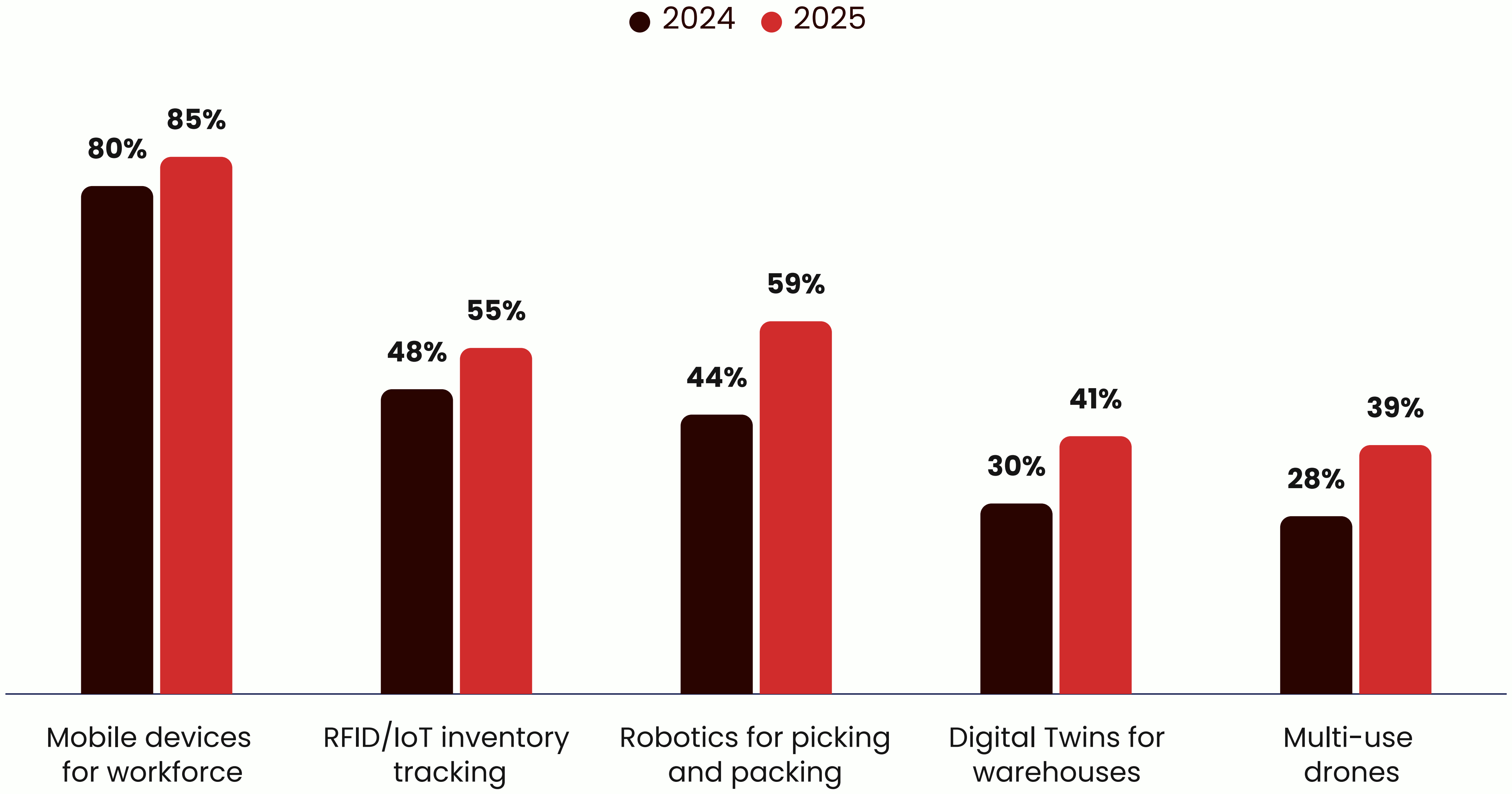
Executives are clear on where AI could add the greatest value in distribution: forecasting demand, optimizing routes, and scheduling labor. These functions represent core execution challenges in warehouses and distribution centers, where accuracy, speed, and efficiency directly shape service levels and cost performance. Leaders increasingly view AI as essential to improving planning, aligning labor with demand, and sustaining throughput under pressure.

Yet deployment remains limited. Many distribution firms are stuck in pilots, slowed by integration with legacy warehouse management systems (WMS), transportation management systems (TMS), and partner platforms. Data silos, governance concerns, and difficulty proving ROI continue to stall progress, leaving adoption far behind intent.

This widening execution gap carries strategic risk. Without accelerated deployment, networks risk missing AI's potential for resilience, productivity, and competitive advantage.

Mobile workforce tools anchor technology adoption as firms prioritize proven productivity enablers

Current deployment of efficiency-enhancing capabilities

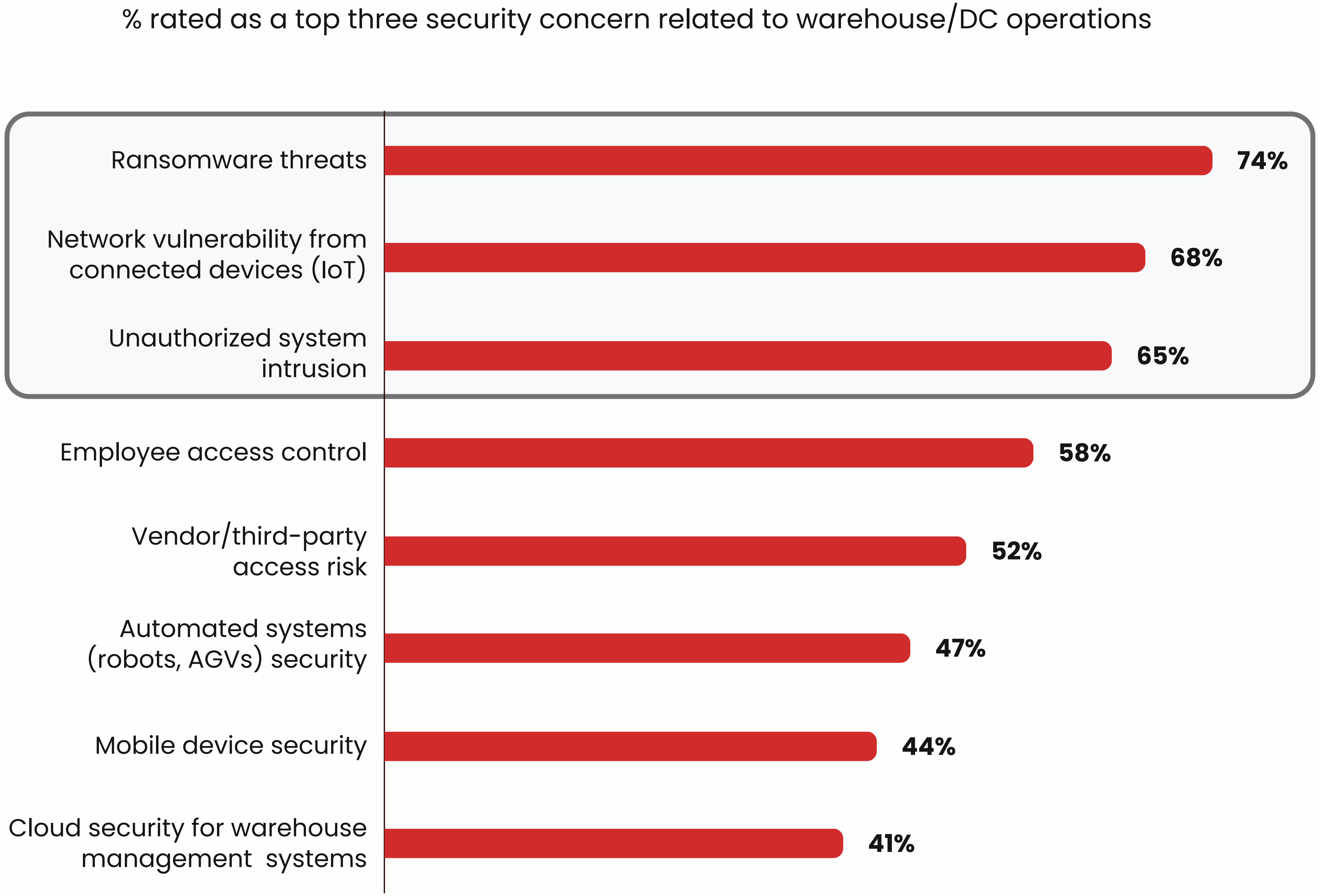


Mobile devices have become the default platform for distribution workforces, enabling quick productivity gains without disrupting existing processes. They act as the bridge between legacy systems and emerging automation, giving associates the digital interface needed to execute tasks more effectively.

Investments are also concentrating on technologies with proven operational impact. Robotics for picking and IoT-enabled inventory tracking are scaling because they directly support throughput and accuracy in high-volume environments. By contrast, advanced solutions such as digital twins and drones remain in exploratory phases, constrained by complexity and integration demands.

An optimism gap persists between IT and business leaders. IT teams are more bullish on adoption timelines, while business leaders remain cautious. Closing this divide will be critical to aligning strategy with operational execution.

Cybersecurity becomes a core operational risk in digitally connected warehouses



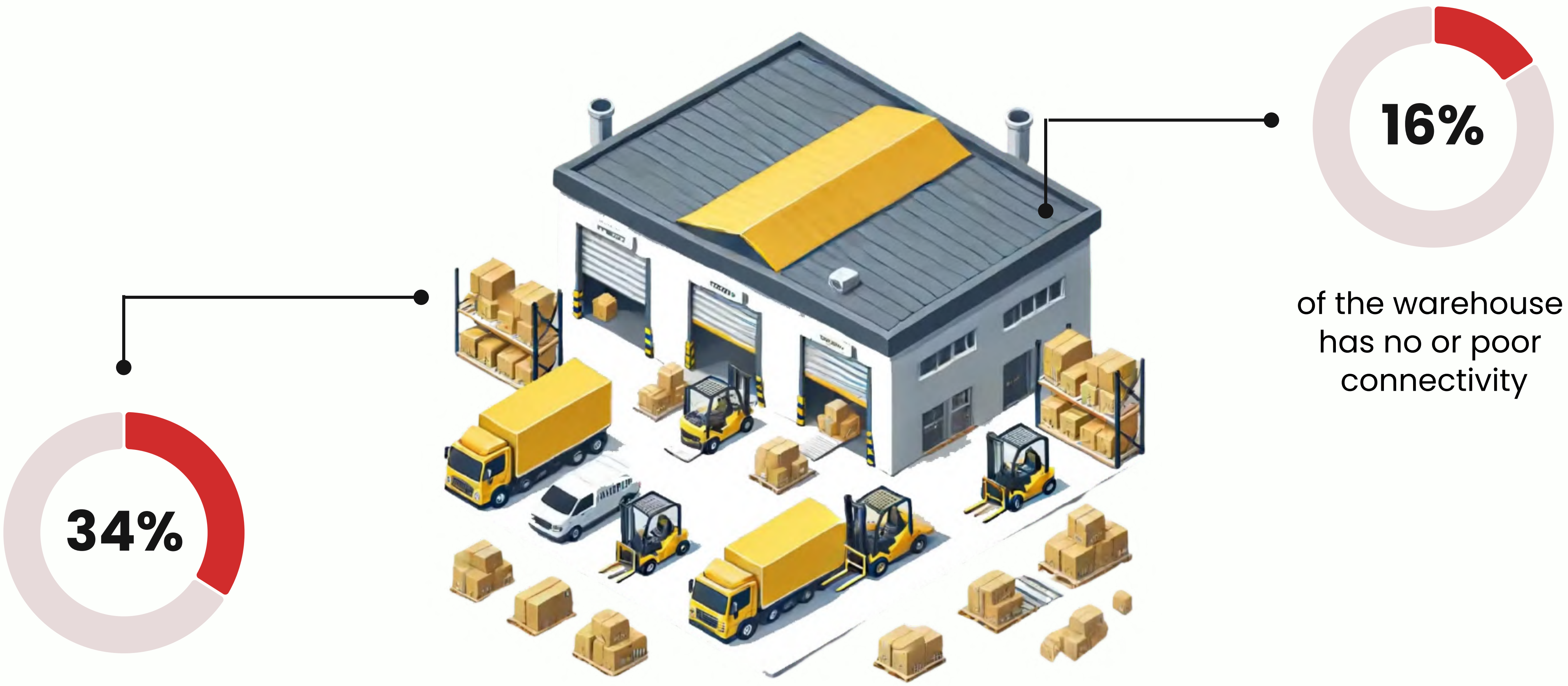
Cybersecurity has become a core operational risk as warehouses digitalize. Ransomware, unsecured IoT endpoints, and unauthorized system intrusions top the list of executive concerns, showing how digital threats now directly disrupt the flow of goods as much as data. The convergence of IT and OT makes every connected device a potential vulnerability.

Executives also point to workforce-related risks; employee access control, and third-party vendor exposure as persistent gaps. As automation scales, even robots, AGVs, and mobile devices introduce new security demands, underscoring that no layer of the distribution environment is immune.

To protect continuity and trust, leaders are embedding cybersecurity into operations. Layered defenses across IT and OT, stronger governance, and workforce training are becoming essential to ensure digital transformation delivers safely and at scale.

Network infrastructure becomes a strategic imperative for technology deployment

62% of companies say their current network cannot support their needs over the next 24 months



16% of the warehouse has no or poor connectivity

34% of the yard has no or poor connectivity

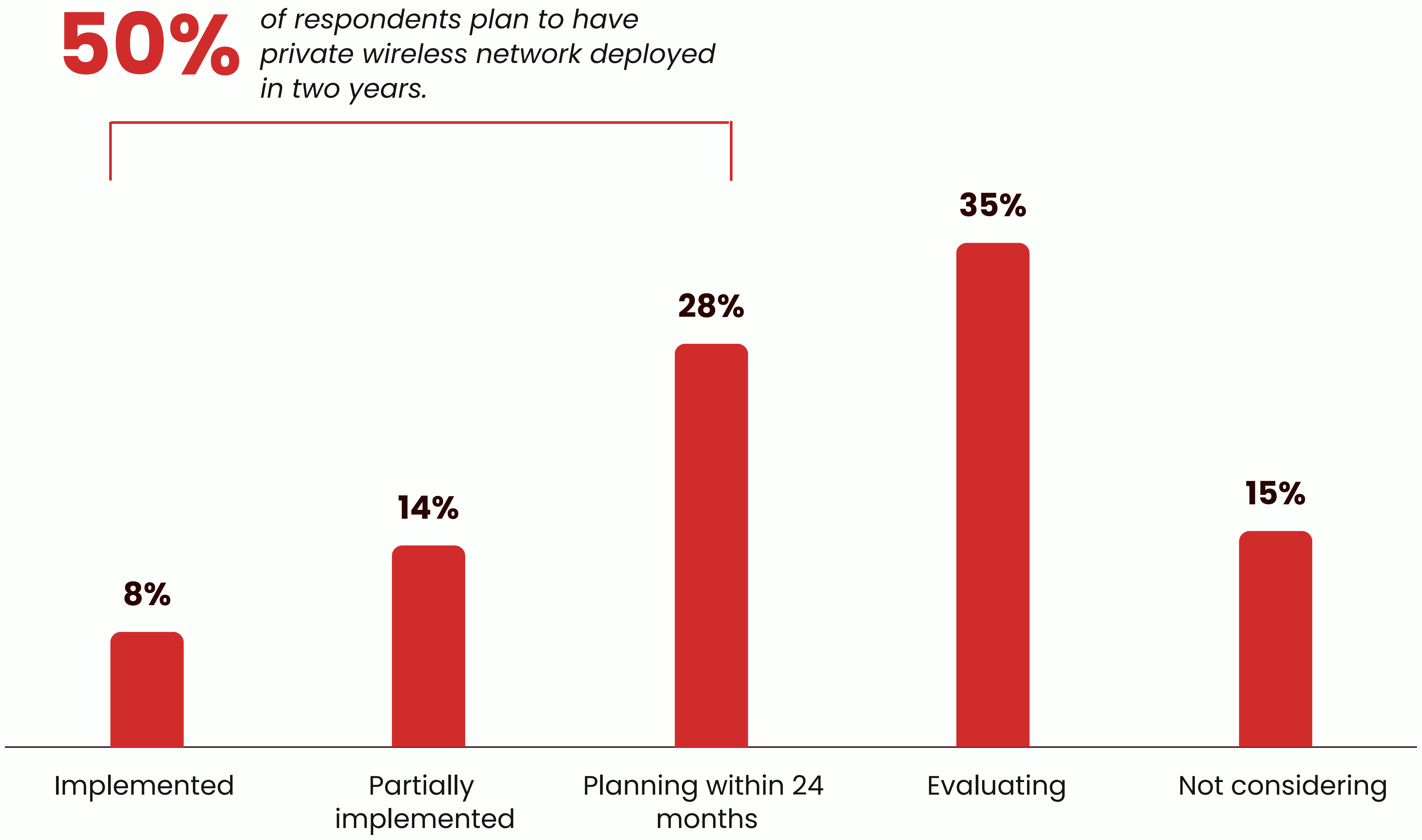
Warehouses are layering in robotics, IoT, and automation, but network infrastructure has not kept pace. Connectivity limitations are now a defining factor in whether organizations can move forward with their technology roadmaps.

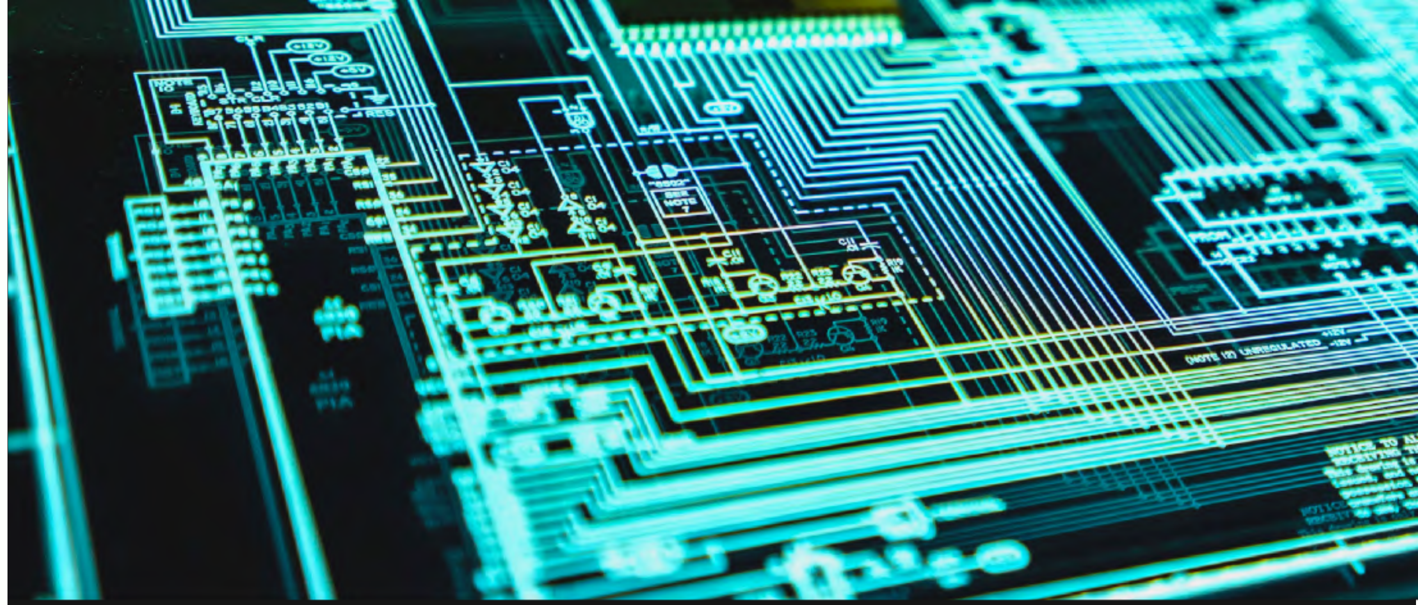
Gaps in coverage across warehouse floors and yards reveal the scale of the challenge. IT leaders are particularly cautious, pointing out that legacy infrastructure often isn’t designed to handle today’s real-time, data-intensive workloads.

This growing divide underscores a larger truth: advanced automation cannot scale on weak foundations. Without robust, facility-wide connectivity, organizations risk stranded investments and will struggle to deliver the reliability, efficiency, and resilience modern distribution requires.

Private wireless emerges as the foundation for next-generation warehouse connectivity

Current and planned deployment of private wireless networks in warehouses/DC





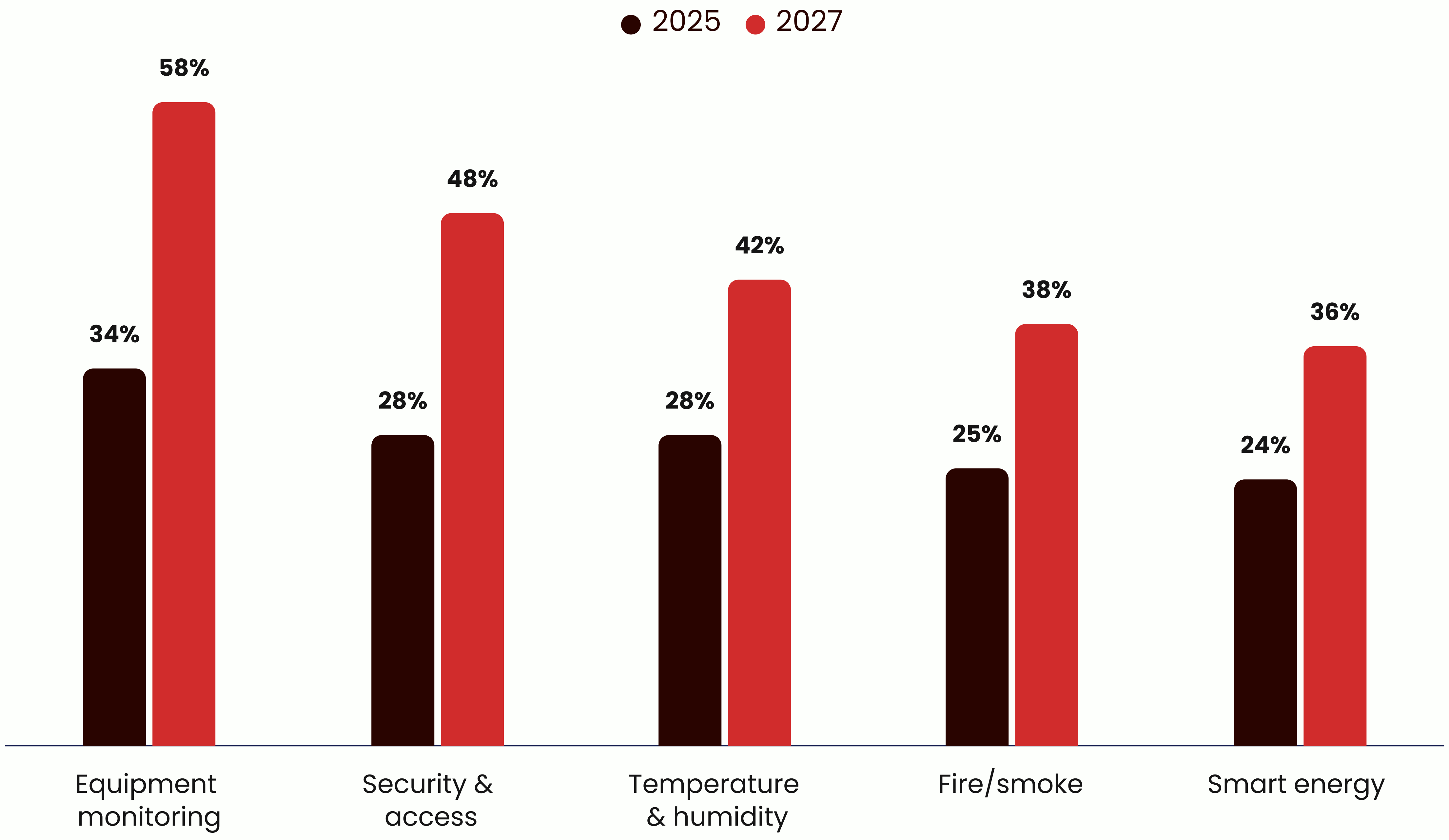
Connectivity gaps remain a persistent barrier to warehouse efficiency, undermining efforts to scale automation and digital tools. Traditional Wi-Fi struggles to deliver the coverage and reliability complex facilities demand, leaving critical workflows exposed to disruption.

Private wireless is emerging as the preferred alternative, providing dedicated bandwidth, low-latency performance, and stronger security. Executives increasingly view it as the backbone for mission-critical applications, where uninterrupted connectivity underpins throughput, safety, and compliance. Controlled networks also offer greater confidence in protecting sensitive data from intrusion or leakage.

Looking forward, private LTE and 5G will be catalysts for scaling advanced use cases such as robotics coordination, digital twins, and AI-driven decision-making. For many, this signals a shift from piecemeal fixes to building true digital infrastructure for the future warehouse.

IoT deployment advances in stages, anchored in foundational monitoring

Current and planned deployment status of IoT capabilities for facility monitoring



IoT adoption is advancing in deliberate stages, anchored first in equipment monitoring. Leaders view machine health as the most critical application, ensuring asset reliability, preventing downtime, and building confidence in daily operations. Security and access controls follow, underscoring the growing need to safeguard digitally connected facilities from unauthorized risks.

Beyond the foundations, IoT is extending into environmental monitoring, such as temperature, humidity, and fire detection. These mid-tier use cases balance operational continuity with regulatory compliance, strengthening product integrity and workplace safety.

More advanced applications, from energy optimization to inventory tracking, remain on the horizon. The progression reflects a pragmatic strategy: organizations are prioritizing resilience and visibility today while laying the groundwork for fully automated, smart facilities tomorrow.

Computer vision adoption advances step by step, led by barcode scanning and quality control applications

% of computer vision applications that are currently deployed or will be deployed in 24 months

69%
barcode/QR code scanning

45%
quality control inspection

42%
security surveillance deployed

35%
safety monitoring

32%
real-time process monitoring

Adoption of computer vision in distribution environments is progressing steadily, anchored in applications that deliver clear, immediate value. Barcode scanning and quality control lead the way, as firms look to standardize inspections, reduce defects, and maintain compliance in high-volume operations. Security surveillance follows closely, reflecting ongoing concerns about loss prevention and the need to safeguard increasingly automated facilities.

Mid-tier applications such as safety monitoring and real-time process oversight show growing interest but face hurdles around integration and reliability at scale. These use cases highlight the operational pressure to improve worker safety and identify process issues proactively, yet deployment remains cautious.

The most advanced applications, AI-driven optimization and predictive analytics remain nascent. This underscores a measured adoption path, with firms prioritizing practical reliability before advancing into more complex, future-oriented scenarios.

KEY TAKEAWAYS

Connectivity challenges limit automation deployments. Building resilient distribution requires hybrid networks, private wireless, and expert execution.

Seamless facility coverage is the foundation for automation

Distribution leaders continue to face “dead zones” across aisles, racks, and yards, limiting the effectiveness of robotics, mobile devices, and IoT systems. These blind spots disrupt workflows and stall even well-funded automation programs.

Closing coverage gaps is the baseline requirement for resilience, reliability, and productivity at scale.
Seamless, facility-wide connectivity is imperative for automation to deliver the expected performance and value.

Hybrid networks reflect operational realities of 2025

A single network may not always meet the full spectrum of warehouse demands. Distribution centers are increasingly adopting layered models that combine Wi-Fi for routine tasks, private LTE/5G for mission-critical workflows, and public wireless for flexibility.

This hybrid approach mirrors the reality of blended environments where automation and manual work coexist. By offering redundancy and adaptability, hybrid networks reduce downtime risk and provide the agility needed to scale digital transformation with confidence.

Private wireless becomes the digital backbone

Private wireless has shifted from pilot projects to strategic investment. In 2025, leaders view LTE and 5G as essential for orchestrating robotics, enabling computer vision, and powering AI-driven workflows.

Unlike traditional Wi-Fi, private wireless offers dedicated bandwidth, low latency, and robust security, making it the most reliable choice for mission-critical applications. Companies embracing private wireless are building the backbone for next-generation distribution, while laggards risk under-performing their competitors.

Implementation expertise is a key to success

The 2025 study underscores a familiar reality: technology adoption fails without expert deployment. Many firms underestimate the complexity of network design, resulting in misconfigured equipment, bandwidth shortfalls, and poor system interoperability.

Successful rollouts require not only technical skill but also deep operational expertise. Leaders emphasize that expert-led implementation ensures reliable coverage, seamless integration across systems, and measurable improvements in efficiency, resilience, and throughput.

Executive Perspective

Michael Weller
Practice Leader - Manufacturing,
Energy and Utilities
Verizon Business

To address ongoing challenges, distribution companies are continuing to deploy innovative technologies to improve the efficiency of their facilities, employees and supply chains.

There continues to be progress in shifting manual material handling processes to automated solutions like AMRs, ASRS and robotics, yet the evolution is not so much a wholesale replacement as a blended model. While distribution company executives recognize that AI will be essential to compete, it is also apparent that AI project execution still lags due to a lack of a clear strategy and use cases, security concerns and budgets.

Cybersecurity has become a core operational concern for distribution organizations driven by a number of factors including system intrusions and the increased security vulnerabilities due to more connected devices in distribution facilities. The top three security concerns are ransomware threats, network vulnerability from connected IoT devices and unauthorized system intrusions.

Innovative new use cases are heavily dependent upon the availability of reliable wireless connectivity across the entire facility. However, inconsistent connectivity or dead zones result in technologies and devices that are often rendered ineffective, resulting in reduced operational efficiency.

Traditional Wi-Fi in industrial environments too often delivers insufficient coverage, unreliable quality of service, mobility hand-off issues between access points and requires an extremely high density of Wi-Fi access points. The best connectivity option for bandwidth intensive technology that requires continuous connection is often a private wireless network that provides a reliable, secure connectivity environment to support a large number of connected devices, data volume and high-fidelity applications in a variety of operating environments.

Glossary of key terms

What is a private wireless network?

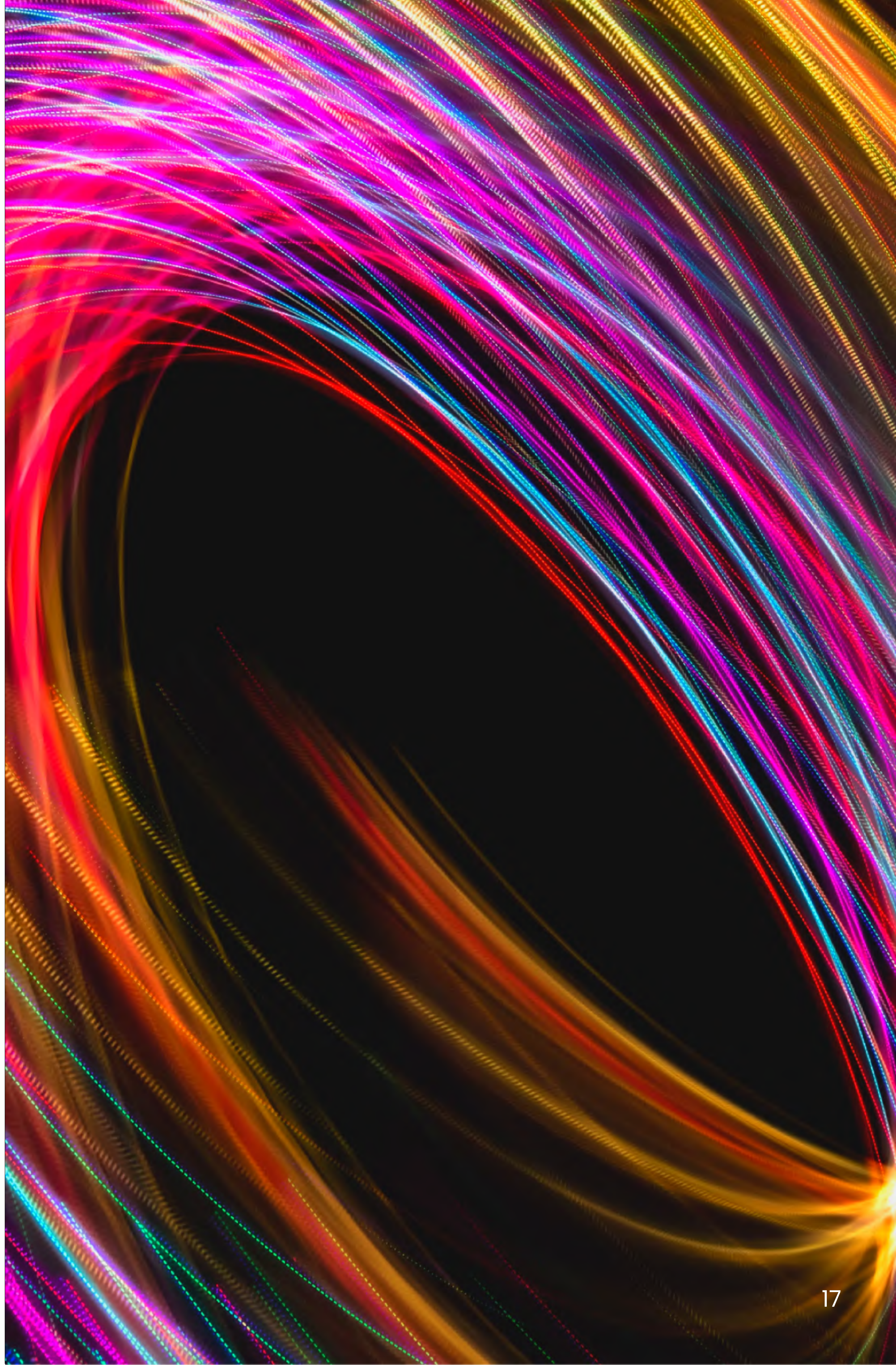
Private wireless networks are enterprise-specific 4G LTE or 5G wireless implementations that can be created for indoor or outdoor environments. Because they are enterprise-specific, they are segregated from public networks – cellular communication stays on premises – and can be configured to the organization's specific security and performance requirements.

Private 5G networks are considered relatively easy to integrate for organizations that already have 4G LTE connectivity. They enhance organizational capabilities by providing high bandwidth, low latency coverage that can support scaled implementations of artificial intelligence and machine learning, virtual and augmented devices, remote monitoring, IoT devices and other networked devices. Controlled authorized user access and device management and the inherent privacy of on-premises networking help keep the network secure. Private networks can operate on licensed or unlicensed spectrum.

Licensed spectrum is dedicated for the use of the entity that holds the license, for example a telecom provider or the military. By purchasing separate spectrum licenses, Verizon and other wireless providers avoid interfering with each other's networks.

Unlicensed spectrum (also known as "CBRS," or Citizens Band Radio Services) comes without some of the regulatory protections that apply to standard, licensed bandwidth. Although unlicensed spectrum can enable some higher performances, the lack of regulatory protections increases the risk of interference and can reduce the overall value proposition of the deployment.

A **neutral host network** provides cellular coverage for distinct private and public use cases; it can allow employees and the general public, no matter their mobile provider, to achieve a strengthened mobile signal via dedicated network infrastructure on a specific premises or campus. Combined with a private network, enterprises can manage both business-critical connected operations (via the private 5G network) and conventional but strengthened public-network connectivity to phones and tablets (via the neutral host network), where signals might otherwise be weak.



SPONSORED BY

INCISIV

verizon business

ABOUT INCISIV

Incisiv is an industry insights & strategy firm that takes a different approach to research and GTM strategies. With close to a decade of industry trend data, we integrate the latest AI tools to provide interactive, solution driven offerings that enable our clients to gain actionable insights from any project.

From benchmark to primary research, from messaging architectures to sales enablement, from partner ecosystem strategies to content/campaign development, our flexible approach reduces complexity & cost, and engages customers more effectively. By leveraging a unique blend of industry expertise & marketing savvy, we provide our clients with programs that are quicker to market and produce better results.

incisiv.com

ABOUT VERIZON

Verizon powers and empowers how its millions of customers live, work and play, delivering on their demand for mobility, reliable network connectivity and security.

Headquartered in New York City, serving countries worldwide and nearly all of the Fortune 500, Verizon generated revenues of $134.8 billion in 2024.

Verizon’s world-class team never stops innovating to meet customers where they are today and equip them for the needs of tomorrow.

verizon.com