

Insight report

Keeping Goods and Information Moving

From site-level connectivity to visible, resilient and scalable logistics operations

What logistics-sector discussions and independent industry evidence reveal about the networks connecting warehouses, distribution centers, applications and global supply chains.

Explore the report

Evidence and methodology

This report examines connectivity across distributed warehouse, fulfillment and distribution operations, focusing on the networks linking sites, mobile workforces, enterprise applications and external logistics partners. It considers how network performance, service ownership and resilience affect the movement of goods and information. It does not treat a managed WAN or Internet provider as responsible for every warehouse-control system, automated machine or shipment outcome.

Our research used AI-assisted audience profiling and inferential analysis to classify 357,957 publicly expressed online opinions associated with senior enterprise technology, infrastructure and network leaders in logistics organizations. Discussions were drawn from X, Quora, Reddit, Bluesky, TikTok and Threads over the 12 months ending 12 October 2026.

The source methodology specifies a 95% confidence level and 5% margin of error, although those statistical claims have not been independently validated for this publication. These findings represent modeled interpretations of online discussion, not direct survey answers, authenticated executive profiles or audited records of network deployments.

The source opinion analysis is US-focused. The report's strategic interpretation is intended for a global audience, supported by independent international research and technical guidance. Results from distinct questions must not be combined as if they have a shared sampling denominator. Where reported answer categories are incomplete or inconsistent, we discuss the operating implications without estimating missing percentages or presenting the result as an industry adoption benchmark.





Executive summary

Logistics organizations increasingly rely on connected sites to receive goods, locate inventory, direct workers, coordinate transport and fulfill customer commitments. Warehouse management systems, enterprise applications, scanners, communications tools and automated equipment all depend on digital services working at the right moment. When connectivity is degraded, the consequence may be a delayed picking wave, an unavailable inventory record, a disrupted booking process or a failure to coordinate activity across facilities. The effect depends on which service is affected, not merely whether an access circuit is online.

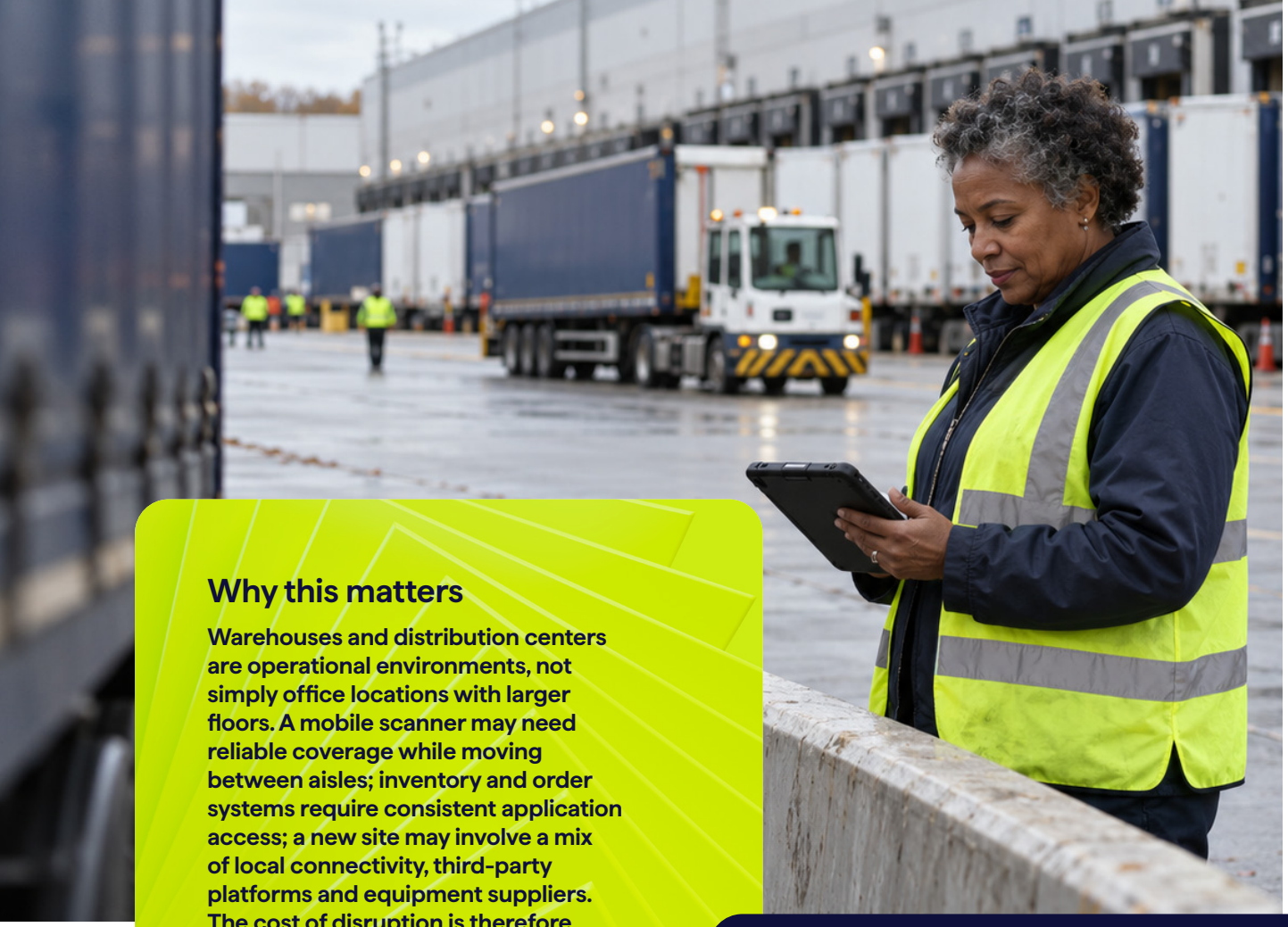
Our audience research points to two practical priorities. **31% of analyzed opinions** identified visibility and monitoring as the top connectivity priority, while **28%** highlighted scalability for new sites. These are directional classifications, but their combination is telling: as distribution estates change, leaders need to bring sites into service repeatedly and understand whether the resulting network supports day-to-day operations. Additional findings show interest in flexible access technologies, emerging satellite options and AI-assisted capacity planning, alongside complexity in managing suppliers and equipment across locations.

Independent evidence reinforces the importance of an integrated operating model. The **2026 MHI Annual Industry Report, produced with Deloitte**, examines the pressures pushing supply chains toward connected, automated and more adaptable operations. The **DHL Logistics Trend Radar 8.0** similarly presents AI, automation, workforce change and resilience as interacting trends rather than isolated technology decisions. Neither source validates our research percentages; together they explain why dependable connectivity must be understood in the context of the logistics operation it serves.

Five connected priorities emerge from the research, highlighting the capabilities that can turn warehouse connectivity into visible, resilient and scalable logistics operations:

1. **Make service visibility operational.** Relate network conditions to warehouse applications, workflows and interruption causes, not only circuit status.
2. **Build repeatability into new-site deployment.** Define standard service requirements, responsibilities and acceptance tests while allowing for local constraints.
3. **Coordinate resilience across providers.** Maintain a consistent view of carriers, paths, incidents and recovery actions without forcing every site onto one supplier.
4. **Match connectivity design to warehouse workloads.** Combine fixed, wireless and local processing capabilities according to equipment, mobility, security and application needs.
5. **Introduce intelligence through evidence and governance.** Use trustworthy telemetry and controlled AI assistance to improve capacity planning and incident response.

The central argument is that modern logistics requires more than connected facilities. It requires a network operating model that can demonstrate service quality, absorb change and restore critical activities across a diverse estate.



Why this matters

Warehouses and distribution centers are operational environments, not simply office locations with larger floors. A mobile scanner may need reliable coverage while moving between aisles; inventory and order systems require consistent application access; a new site may involve a mix of local connectivity, third-party platforms and equipment suppliers. The cost of disruption is therefore shaped by timing, service dependency, workforce workarounds and the ability to recover accurately.

For global logistics leaders, the strategic opportunity is to bring together site rollouts, application priorities, supplier coordination, monitoring, security and continuity within an operating model that remains manageable as operations expand. Consistent governance does not mean identical physical architectures at every warehouse. It means common expectations of what services must deliver, how problems are identified and who is responsible for putting them right.

The mission is to keep goods and information moving with greater predictability, while making connectivity investment accountable to operational outcomes such as site readiness, service continuity, fulfillment reliability and efficient recovery.

Expereo perspective:

“

In logistics, the network is part of the operation. It isn’t the circuit going down that stops a warehouse; it stops because a scanner can’t update an order or a team can’t reach the inventory system. That’s why connectivity has to be judged by what it keeps moving, not just whether it’s online. The logistics leaders getting this right treat their network as one coordinated service across every site, partner and provider.

”

Kevin Brown
Chief Operating Officer (COO), Expereo



Theme 1:
Visibility is the foundation of connected logistics

The value of a network is demonstrated through the warehouse services it supports, not only the connections that remain online.

A distribution network may contain dozens of warehouse locations, partner sites and application environments. The same order can depend on receiving data, local scans, enterprise inventory records, workforce instructions and transport coordination. Different teams may monitor different elements, creating a gap between the indicators displayed by network tools and the experience of people operating the site. A circuit can remain available while a warehouse system is slow, a login fails or a device roams poorly between wireless access points.

For leaders responsible for large estates, the challenge is to build a shared understanding of which digital dependencies matter, what good performance looks like and how to identify where degradation begins.

Better visibility should reduce the time between noticing that a process is failing and determining which technical or operational team can act.

Visibility and scalability emerge as leading priorities

Our research classified **31% of modeled discussions** as making visibility and monitoring the top warehouse connectivity priority, with another **12%** treating it as important.

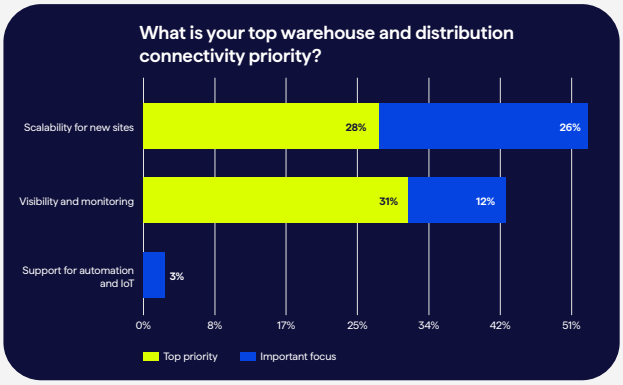


Figure 1. The leading connectivity priorities

Separately, **28%** identified scalability for new locations as their top priority and **26%** as an important focus. These are classifications of expressed priorities, not evidence of measured investment or service maturity. The results nevertheless raise a practical question: as organizations connect new sites, can they sustain a reliable, comparable view of services across all of them?

The relationship matters because every additional facility introduces more endpoints, application dependencies, local access providers and incident pathways. Without consistent service records and comparable performance indicators, operational complexity can grow faster than the estate itself. Monitoring must therefore be designed as part of a new-site operating model, not added after an outage exposes a visibility gap.

Distinguish visibility of goods from visibility of networks

The **GS1 EPCIS 2.0.1 standard** provides a useful distinction. It enables the sharing of event data about what happened to products and assets, where and when, across supply-chain participants. That is supply-chain visibility. Network observability addresses a different question: whether the applications, devices and data paths producing or consuming those events are performing as expected. Both are useful, but neither automatically substitutes for the other.

For example, a delayed inventory update may reflect an application queue, an unavailable external endpoint, a local wireless issue or a wide-area route problem. A useful operational view joins signals across those boundaries rather than allowing every technical supplier to report that its own component is healthy. This does not require one platform to control every element. It requires clear service maps, telemetry-sharing arrangements and a common incident language.

The same principle applies to distributed operations that depend on transport management, enterprise resource planning and warehouse management applications.

Source research classified 46% of opinions as treating ERP access as absolutely reliant on connectivity and 32% as considering it important. These figures should not be interpreted as an objective ranking against warehouse management systems: the response categories are uneven and do not establish application criticality across all logistics businesses. The more defensible conclusion is that connectivity assurance needs to be application- and workflow-specific.

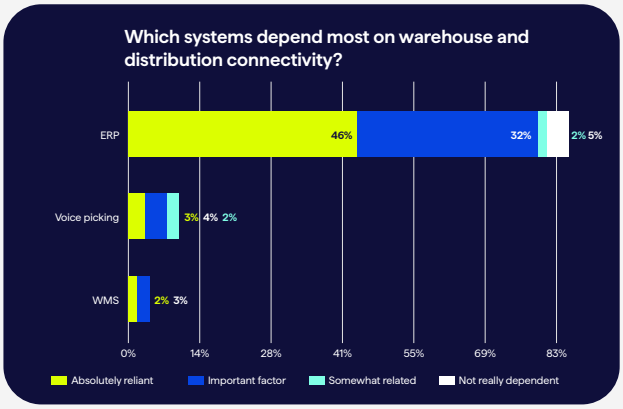


Figure 2. The systems organizations are most dependent on for warehouse and distribution connectivity

Turn network data into operational evidence

A meaningful assurance framework can begin with critical applications, then identify the paths, services and suppliers that enable them. Metrics might include application reachability, response variation, packet loss, wireless roaming performance where relevant, time to isolate an incident and time to restore a usable operational workflow. Where a distribution process relies on local systems during a WAN failure, the test should establish what can continue, what must queue and what needs reconciliation when service returns.

This approach also improves investment decisions. An access upgrade may be justified where it removes repeated delay for a high-priority application. Elsewhere, better incident ownership or monitoring might deliver more value than additional bandwidth. Evidence helps teams distinguish genuine capacity needs from failures arising in applications, devices or third-party systems.

The **2026 MHI-Deloitte industry report** identifies supply-chain visibility, agility and resilience among the pressures reshaping digital logistics. It provides broad industry context for this discussion, not a network-level benchmark. The operational implication is to connect the effectiveness of infrastructure with the processes it exists to support.

Strategic insight

Warehouse connectivity creates business value when monitoring becomes evidence of application performance, incident causes and operational impact across locations.

For distributed logistics organizations, the priority is to translate technical signals into a shared understanding of service health, with named owners and agreed performance expectations for critical workflows. This makes resilience measurable and gives teams an evidence base for deciding what to improve.

Once services can be understood consistently, the next task is to apply those standards whenever a new warehouse or distribution location comes online.

Expereo perspective:

“Every supplier can tell you its piece of the network is healthy while the warehouse still can’t work. Real visibility means joining those views together, so teams can see where a problem starts and who needs to fix it. When monitoring becomes evidence of how critical workflows are performing, you stop debating whose fault it is and start restoring service faster.”

Jean-Philippe Avelange
Chief Information Officer, Expereo



Theme 2:

Scaling distribution networks without multiplying complexity

New sites need repeatable service readiness, not a new network operating model every time.

Logistics networks change as businesses add fulfillment capacity, enter new markets, combine acquired operations or adjust their regional footprint. Some facilities are planned years in advance; others may be seasonal, temporary or managed by partners. A newly opened warehouse needs far more than an Internet circuit. It needs working application paths, local coverage, security boundaries, incident contacts and a clear process for proving that critical operations can begin safely and reliably.

Technology and supply arrangements vary. An urban cross-dock facility may have several viable fiber providers. A remote cold-chain warehouse may depend on alternative access methods or face practical lead-time constraints. A high-volume automated center may have equipment and local-network requirements that do not exist at a smaller manual site. A common operating model must therefore distinguish consistent management requirements from local engineering choices.

Standardize the deployment process, not every warehouse design

The **World Economic Forum's Global Value Chains Outlook 2026** describes how supply chains need orchestration, distributed scale and optionality as volatility becomes a continuing feature of global operations. The report is about supply-chain strategy rather than network deployments. The implication for infrastructure leaders is that the ability to connect and support different kinds of location predictably is an operational capability in its own right.

A practical rollout model begins before technology selection. Site teams should define essential workflows, peak operating periods, hand-held and fixed device profiles, security requirements, cloud and on-premises dependencies, local provider choices and the consequences of delay. IT and operations then agree which services can run locally if external connectivity is degraded and which must be available from day one.

A shared deployment playbook can cover discovery, procurement, design approval, installation, validation, go-live and operational handover. It should specify who accepts each stage, what documentation is required and how exceptions are managed. The exact physical connections may differ by country and site; the standardization lies in the questions answered and the evidence collected.

Make readiness a tested operational outcome

The most important distinction is between a connected site and a site ready to operate. Acceptance testing should include the critical user journeys: scanning an item, updating an order, accessing the warehouse management or ERP platform, communicating with transport partners and recovering from a plausible service interruption. Tests should establish not only whether a path responds, but also whether the process works at expected volumes and within agreed tolerance for delay.

Site-specific risk matters. During a peak order period, even a short service degradation can create an operational backlog. An outage at a low-volume overflow facility may allow alternative working arrangements. Availability commitments should therefore follow business criticality. The source report contains different preferences for percentage-uptime targets, but those percentages are not a substitute for defining site-specific recovery requirements and testing real failure scenarios.

Measures of rollout quality could include the time from approved design to verified service readiness; the proportion of critical applications passing acceptance tests; the completeness of provider and circuit records; avoidable rework after launch; and time taken to resolve the first operational incidents. These indicators reveal whether a standard rollout process is improving outcomes rather than simply accelerating installation.

Connect the new site into existing management

New facilities should enter the same inventory, monitoring, escalation and change-control processes as established warehouses. Without that handover, operational teams may inherit undocumented local exceptions and become dependent on the individuals who managed installation. Shared records should identify access technologies, equipment responsibilities, physical diversity where relevant, application routes, security contacts and support procedures.

An effective model also recognizes local operating capability. A global network partner may coordinate access provision and network performance, but cannot guarantee how quickly every equipment supplier, building contractor or warehouse software integrator completes its work. Realistic accountability separates the contributions while aligning them around the agreed service-readiness date.

Strategic insight

Scaling connected logistics requires repeatable service assurance and clear operational ownership, not identical network configurations in every building.

For global infrastructure leaders, a consistent deployment model enables faster decisions, clearer handovers and more predictable service quality across varied facilities. It also helps distinguish controllable connectivity delays from dependencies outside the network team's remit.

That repeatability becomes more valuable as the number of carriers and connectivity partners grows, making coordinated resilience the next priority.



Expereo perspective:

"A connected site and a site that's ready to operate are not the same thing. The fastest-growing logistics businesses don't reinvent the process for every new warehouse. They use the same playbook every time: the same requirements, the same acceptance tests and the same handover into day-to-day support, while leaving room for local choices. That's what turns expansion from a project into a repeatable capability."

Kevin Brown
Chief Operating Officer (COO)
Expereo



Theme 3:

From multi-carrier complexity to coordinated resilience

Supplier diversity is useful only when the resulting services remain visible, accountable and recoverable.

A logistics organization spanning multiple regions rarely encounters the same carrier availability, commercial terms and access technologies at every location. Some markets offer several fiber providers; others may rely on wireless or satellite alternatives. One global access supplier might simplify commercial oversight, while a portfolio of local suppliers may improve reach or enable route diversity. Neither arrangement guarantees resilience on its own.

The source research illustrates sharply different carrier configurations, from single-provider environments to estates involving 11 to 20 carriers. Its categories do not provide a usable intermediate range, so these figures cannot defensibly be relabeled as a one-to-ten versus eleven-to-twenty split or represented as a complete distribution. The more useful strategic issue is what an organization can actually see and control across whichever providers it uses.

Coordinate the whole service lifecycle

Contracts, circuits, contact details, service levels and incident records often sit in separate systems. That fragmentation makes a seemingly simple outage difficult to resolve: a warehouse reports that its cloud application is unreachable, the local carrier reports a healthy access line and the application provider reports no platform fault.

Without a shared map of dependencies and responsibilities, teams can spend more time locating the right owner than repairing the failure.

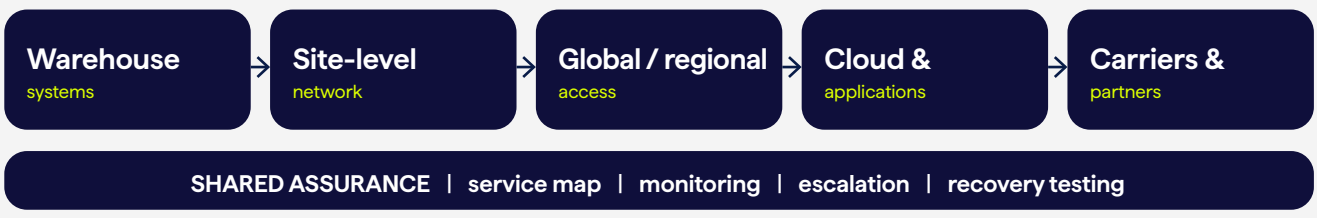
The **Mplify/MEF Network-as-a-Service Industry Blueprint** provides relevant industry context. Its emphasis on standardized services and lifecycle orchestration across providers demonstrates why business and operational coordination matters in multi-network environments. It is not a claim that one technical standard already resolves every supplier handover.

The operating model should maintain consistent information about service locations, carriers, contracts, physical access, performance commitments, escalation paths, planned works and restoration procedures. Such visibility can be maintained through a managed network partner, shared data and agreed processes without insisting that all underlying connections come from one operator.

Understand diversity rather than assume it

Two connections supplied by different carriers may still share the same physical duct, building entry point, upstream provider or power dependency. Conversely, a wireless backup may offer useful diversity but have different coverage, capacity and performance limits. Resilience decisions should examine failure scenarios and critical applications rather than count suppliers or lines as though each adds an equal amount of protection.

Coordinated service assurance across a logistics estate



Illustrative service-assurance operating model developed for this report; responsibilities depend on the organization and its suppliers.

The **ISO/TS 22318:2021 guidance on supply-chain continuity management** extends business-continuity thinking to supplier relationships and upstream and downstream dependencies. Although not a telecommunications standard, it offers a relevant principle: organizations should identify which relationships are critical to continued delivery and agree realistic arrangements for disruption.

For network services, this means documenting how failover works in practice, who triggers it, which workloads continue to operate and what evidence is needed before normal service resumes. Testing should include interactions between access networks, cloud services, identity systems and site operations. Repeated incident reviews can show where an alternative path exists on paper but does not restore an actual business workflow.



Use alternatives, including LEO satellite, for specific conditions

Low-Earth-orbit satellite may be useful where terrestrial infrastructure is limited, for temporary logistics locations or as a diverse backup path. In our source research, 22% of modeled opinions were associated with LEO as primary access at remote sites and 12% with backup use. The summary also classified 32% as planning adoption within two years. These are directional discussion patterns, not verified deployments or a global forecast.

Satellite is not a universal substitute for terrestrial fiber or cellular access. Site geography, installation conditions, availability, throughput variation, latency, business continuity and application tolerance all matter. A remote warehouse may benefit from LEO as part of a portfolio while retaining a different primary service. The question is whether each option reduces a material risk at a proportionate cost.

Similarly, SD-WAN can help manage traffic and policy across multiple WAN paths, while SASE brings together network access and security capabilities. They are not opposing deployment choices. Our source groups them as though they were mutually exclusive in one question, so this report does not treat the resulting adoption percentages as a reliable distribution. Technology selection should follow the operational requirements, not a simplified product contest.

Strategic insight

Multi-provider resilience depends on coordinated service information, tested diversity and unambiguous restoration responsibility, not on carrier count or a single networking product.

Global logistics leaders should be able to identify critical access dependencies, compare service performance, escalate incidents through the correct supplier and verify that alternative paths restore the affected workflow. This gives organizations the flexibility to use different access technologies while retaining a coherent operating model.

With the external connectivity estate more manageable, the next challenge is matching service design to the very different technology requirements inside and between warehouses.

Expereo perspective:

> Having more carriers doesn't make you more resilient, but knowing exactly how they fit together does. Two lines from two providers can still share the same duct or the same weak point. Global logistics operators need one clear view of every service, every contract and every escalation path, so when something fails, the backup actually restores the workflow and someone owns the fix.

Jean-Philippe Avelange
Chief Information Officer, Expereo



Theme 4:

Automationis reshaping connectivity requirements

Connectivity design must reflect how people, equipment, applications and local processes interact.

The modern warehouse can combine wired devices, mobile scanners, voice-picking equipment, cameras, sensors, automated storage systems, robotics and cloud-hosted business applications. But there is no single warehouse technology stack and no universal network requirement. Some operations rely on highly mobile devices and dense radio coverage. Others have fixed automation zones, stringent segmentation needs or local control systems that must remain functional when the WAN is unavailable.

The network architecture must therefore distinguish layers. Local wired and wireless systems connect equipment and workers inside the building. Wide-area networks and managed Internet access connect sites to enterprise platforms and external partners. Cloud and application services host or process essential information. Failure in one layer can affect the workflow, but the correct technical remedy depends on which layer is responsible.



Wireless access is useful, but the workload defines the design

The source research classified **40% of analyzed opinions** as considering 4G or 5G wireless essential for warehouse and distribution connectivity, with a further **29%** describing it as a strong option. These figures indicate perceived usefulness, not a measured proportion of warehouses using cellular connectivity or a prediction that cellular access will displace fixed networks.

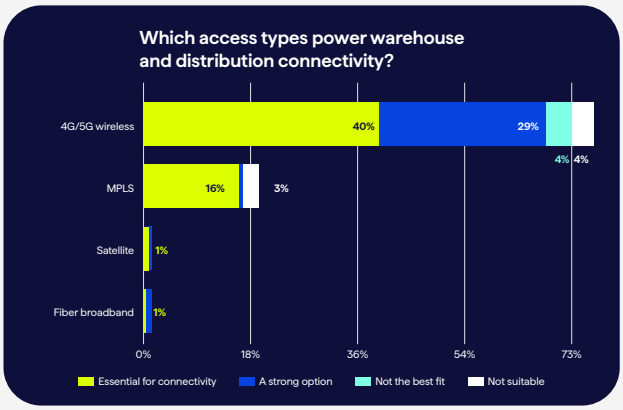


Figure 3: The access types powering warehouse and distribution connectivity

For a distributed operator, cellular access might support temporary locations, backup connections, mobile equipment or specific coverage challenges. Within a warehouse, Wi-Fi, private cellular networks and industrial wired connections address different operational needs and constraints. It would be misleading to treat Wi-Fi 6, Wi-Fi 6E, Wi-Fi 7 and 5G as simply competing answers to the same question. The relevant design choices include radio coverage, interference, device compatibility, mobility, segmentation, availability and how local services continue through a WAN interruption.

The **NIST Guide to Operational Technology Security, SP 800-82 Revision 3** explains why systems interacting with physical processes can have distinct performance, reliability and safety requirements.

Although it is US technical guidance, those engineering principles help illustrate why a warehouse automation environment should not be managed exactly like ordinary office connectivity. A remote change or security response that is harmless to a general-purpose application may disrupt equipment or local operations if introduced without appropriate controls.

Recognize uneven digital estates without inventing a middle category

The research includes examples of relatively small connected-device populations and estates involving thousands of IoT devices. Its reported percentages refer only to fewer than 100 devices and 2,001 to 10,000 devices, without identifying the 100-to-2,000 range. We therefore do not assign a share to that middle segment or claim the reported categories form a valid complete distribution.

The real operating implication is that device populations are heterogeneous. A smaller warehouse with handhelds and a few environmental sensors will have different support and capacity needs from an automated distribution campus with fixed equipment, sensors and dense mobile workflows. Designing around inventory, device criticality and traffic patterns is more defensible than assigning all sites to one IoT adoption stage.

Application dependencies also vary. Enterprise resource planning, warehouse management, picking and transport systems may exchange data with different frequency and criticality. The **GS1 EPCIS standard** provides a common way to represent visibility events across a supply chain; it does not determine whether the supporting network or software application will meet every performance requirement. Data interoperability and network reliability are complementary capabilities.



Strategic insight

Connected warehouse performance depends on workload-appropriate local and wide-area networks, with clear boundaries between industrial operations, application services and connectivity providers.

A sound architecture identifies which services require low latency, which benefit from local processing, which need wide-area resilience and which can tolerate a controlled delay. This enables organizations to modernize warehouse technology without confusing technology adoption with operational assurance.

As more systems become observable and connected, logistics organizations can begin using that information more intelligently, provided AI-assisted actions are governed and measurable.

Expereo perspective:

> There's no single blueprint for the modern warehouse. A site built around handheld scanners needs something very different from a highly automated distribution center. The right design starts with the work being done, then brings Wi-Fi, cellular, fixed access and local systems together around it. What matters is that every one of those layers connects to an enterprise network the business can depend on.

Matthew Lea
Product Development Director, Expereo



Theme 5: **From reactive networks to intelligent operations**

AI can improve decisions about capacity and incidents, but dependable information and controlled action come first.

Interest in AI across logistics extends from demand forecasting and route planning to robotics, inventory management and workforce support. Network operations are a narrower domain: diagnosing service degradation, forecasting capacity requirements, interpreting alerts and recommending changes to connectivity policies. A logistics company may already use AI in its supply-chain operations without using AI to manage its network. These should not be described as equivalent forms of adoption.

The **2026 DHL Logistics Trend Radar 8.0** describes AI, robotics and workforce change as related developments, while emphasizing human expertise and governance. Its broader industry perspective provides context for what may follow, not confirmation of AI adoption rates inside enterprise network teams.

Separate exploration from live network deployment

Our research classified **42% of modeled discussions** as indicating no current use of AI specifically for warehouse and distribution connectivity; **31%** as exploring use cases; **26%** as piloting AI for network monitoring; and **1%** as using AI for predictive maintenance in that context. These classifications are narrow and directional.

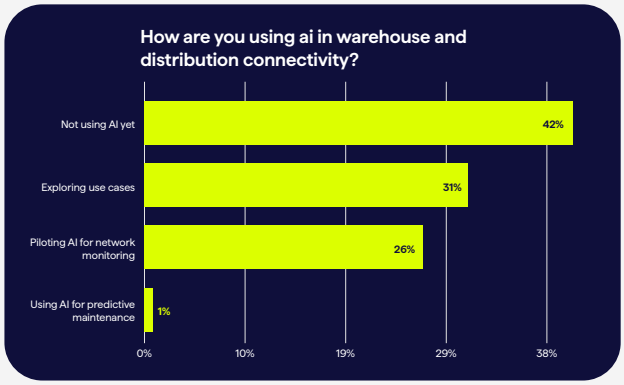


Figure 4. AI use in warehouse connectivity

They do not measure AI adoption across all warehouse operations or prove that particular companies have deployed specific tools.

The distinction matters operationally. Exploring an AI tool does not establish data quality, integration with existing service-management processes or evidence that suggested changes are safe. A pilot may improve alert triage but still require careful testing before it can trigger network rerouting or alter access controls. Maturity should be measured by the quality of decisions and the outcomes of the process, not the number of AI features enabled.

Capacity planning is an attractive early use case

A separate question classified **18%** of analyzed opinions as calling AI-assisted capacity planning the best fit, **40%** a strong contender and **27%** somewhat helpful. The result indicates substantial interest in this particular application, but it does not establish quantified benefits. Capacity planning is a practical starting point because warehouse connectivity demand can change with seasonality, new equipment, site expansion and new applications. Better forecasting might help identify when bandwidth, access coverage or monitoring thresholds need to change before operational performance suffers.

AI-assisted analysis could combine historical utilization, application trends, incident recurrence and planned site or device changes. The value lies in helping specialists test hypotheses and make more informed decisions. A model that detects rising traffic is not sufficient if the traffic does not affect the critical service, or if the real issue is a local Wi-Fi dead zone rather than WAN saturation.

Useful success measures include fewer avoidable capacity-related incidents, earlier identification of recurring patterns, reduced time to isolate a fault and more accurate planning for new-site launch. Teams should compare those outcomes against baselines and identify circumstances where algorithmic recommendations should be disregarded.

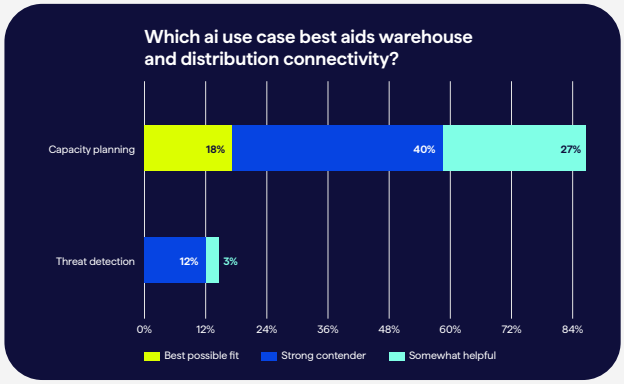


Figure 5. AI-assisted capacity planning.

Keep engineering and operational governance in the loop

Network automation must operate within defined controls. Changing a route, security policy or service priority can affect operational systems and may have consequences for physical warehouse processes. Important actions should have approved boundaries, suitable maintenance windows, clearly assigned authority, a rollback process and evidence showing what data drove the decision.

The **NIST AI Risk Management Framework** provides a useful governance reference through its Govern, Map, Measure and Manage functions. It is not a warehouse connectivity standard, but its focus on context, testing, oversight and ongoing risk management supports responsible AI deployment. In operational networks, this means starting with decision support, validating recommendations against real incidents and expanding automation only when safe outcomes can be demonstrated.

A network team might first use AI to group related alerts, enrich service tickets or flag an unusual capacity pattern. More consequential interventions, such as automated path changes for critical applications, should require stronger testing and carefully defined approval thresholds. Industrial engineers, application owners, security specialists and network providers should understand which decisions remain human-led and how unexpected effects are detected.

Strategic insight

Intelligent logistics networking is demonstrated through better capacity decisions, more dependable services and safer incident response, not by the number of AI tools deployed.

For logistics leaders, AI-assisted network operations should build on trusted telemetry, shared service information, measurable outcomes and accountable change processes. The opportunity is to make monitoring and planning more proactive while preserving the operational control needed in connected physical environments.

Across all five themes, the conclusion is consistent: keeping goods moving requires connectivity that can be observed, managed, recovered and improved as part of a coordinated logistics operating model.

Expereo perspective:

“

AI will help logistics networks see problems coming, but it’s only as good as the data behind it. Capacity planning is a sensible place to start: spotting demand building ahead of peak season or a new site launch before performance suffers. Let AI support engineers’ decisions first, and give it more room only once its forecasts have held up through a peak.

”

Jean-Philippe Avelange
Chief Information Officer, Expereo





Summary:

Five priorities for the next era of warehouse and distribution connectivity

Turning connected logistics ambition into visible, resilient and scalable operations



Five connected priorities emerge from the research, highlighting the capabilities that can help logistics organizations manage more connected sites and increasingly demanding operational workflows.

1 Measure connectivity against critical logistics services

Identify the order, inventory, picking, transport and workforce applications that matter most; set service-specific performance targets and measure restoration in operational terms.

2 Make site launch a repeatable capability

Standardize requirements, discovery, documentation, acceptance tests and handover while allowing local engineering and provider choices to vary.

3 Coordinate diverse access and supplier relationships

Maintain dependable service inventories, performance information and incident ownership across carriers, regions, managed network partners and cloud providers.

4 Design local and wide-area connectivity around workloads

Assess wireless, fixed access, local processing and security controls against equipment, mobility, data flows, safety and recovery needs.

5 Introduce intelligence through evidence and governance

Improve telemetry and service records before relying on AI-assisted capacity planning or operational interventions, and test results against meaningful outcomes.

Together, these priorities offer a practical basis for evaluating whether current networks can support business continuity, new-site growth and changing warehouse technology without introducing avoidable complexity.



Connected Logistics Network Readiness Scorecard

A qualitative assessment of the capabilities behind dependable warehouse and distribution operations

The following six-dimension scorecard is an editorial assessment framework derived from the themes in this report. It is **not** a statistically validated maturity benchmark or a grading of participating logistics organizations. Use it to compare demonstrated current capability rather than planned technology investment. The goal is to identify material operational gaps, not to maximize every dimension indiscriminately.

Dimension	Developing	Established	Advanced
1. Operational visibility	Circuit and device status is available but incidents are not linked reliably to critical warehouse processes.	Priority applications and sites have consistent performance measures, owners and incident records.	End-to-end service intelligence links network conditions to order, inventory and workflow impacts and drives improvement.
2. Critical service performance	Targets focus on generic uptime or capacity and are not differentiated by workload.	Key logistics applications have defined baselines, failure thresholds and service owners.	Service evidence supports proactive remediation and prioritized investment based on operational criticality.
3. Site readiness and scale	Each new location requires substantial ad hoc discovery and problem solving after go-live.	Common requirements and acceptance tests improve new-site handover and service consistency.	Repeatable rollout, monitoring and recovery processes adapt to site type while demonstrating predictable readiness.
4. Provider coordination	Carrier, path and escalation information is fragmented across teams and contracts.	Critical services, carriers, support contacts and restoration arrangements are documented and reviewed.	A coordinated multi-provider model supports proactive fault isolation, verified diversity and ongoing assurance.
5. Warehouse technology integration	Local wireless, equipment, applications and WAN access are designed separately.	IT, site operations and integrators agree critical flows, separation controls and local continuity needs.	Engineering and operations jointly manage performance and change across local and enterprise services.
6. Intelligent, secure operations	Capacity and incident response are reactive; AI ideas lack trusted data or governing controls.	Reliable telemetry and selected decision-support automation are tested and owned.	Governed AI assistance demonstrably improves planning and recovery, with risk controls, review and rollback.

Framework note: A qualitative self-assessment derived from the report themes, not a validated industry maturity benchmark. Score demonstrated practice, not planned features.



From assessment to action

A readiness assessment becomes useful when it directs investment and accountability. A high-volume distribution center might need stronger local application and wireless assurance; a rapidly expanding third-party logistics operator may need repeatable new-site onboarding; a multinational warehouse network may gain most from coordinated provider management. The most important dimension will vary according to the business model and the consequences of disruption.

A practical first cycle has three steps:

- **Start with critical workflows.** Name the services whose performance or interruption would affect orders, inventory accuracy, dispatch or customer commitments; identify their paths and owners.
- **Establish baselines and test recovery.** Agree meaningful service targets, verify backup paths and test whether normal business activity can continue or resume following disruption.
- **Assign ownership and review change.** Clarify the roles of site operations, central IT, application teams, security, integrators and connectivity providers; reassess after major site or workload changes.

Strategic outlook: From connected warehouses to assured logistics

The next phase of logistics transformation will involve more connected facilities, mobile workflows, automation and data exchange across partners. Different businesses will reach that future through different technologies. Some warehouses will prioritize reliable handheld coverage and core applications; others will invest in local processing, robotics or diverse access paths for remote facilities. Global organizations will need to coordinate all of these decisions without assuming that a uniform technical configuration is either possible or desirable.

The strongest operating models will translate that diversity into a common standard of assurance. They will define the activities connectivity supports, maintain accurate service information, know which suppliers and platforms are critical, and test the ability to recover when conditions change. They will use automation where it improves decisions and keep governance and engineering oversight proportionate to operational risk.

The future of warehouse connectivity is not simply more wireless coverage or more connected devices. It is confidence that goods, information and operations can keep moving as networks, partners and business demands evolve.

Closing perspective

Logistics will only get more distributed, more automated and more dependent on partners. More than simply implementing more technology, the organizations that thrive will be the ones that can coordinate it. A single global partner across network providers takes the complexity out of running many sites in many markets, improves the experience of the applications teams rely on every day, and gives leaders a clear view of how their whole network is performing. That confidence is what keeps goods and information moving.

Kevin Brown
Chief Operating Officer (COO), Expereo



Continue the conversation

The scorecard provides a starting point for infrastructure, operations and procurement leaders to discuss where better service information, provider coordination or tested connectivity resilience would make the greatest difference. A targeted assessment can turn those priorities into a practical roadmap for site readiness, service assurance and continuous improvement. To explore global connectivity and managed networking priorities, visit Expereo.

Visit Expereo