

A man and a woman are standing in a server room, looking at a laptop. The man is wearing glasses and a blue sweater, and the woman is wearing a black top and a grey cardigan. They are both wearing blue lanyards with ID badges. The background shows rows of server racks with blue lights.

AI advantage starts with a trusted digital infrastructure

Three key takeaways from Orange Business Summit

- Trusted digital infrastructure is a strategic foundation for resilience, compliance, security, sovereignty and better decision-making
- Platformization gives enterprises the scalability, flexibility and integration needed to support AI through control points and open architectures
- Secure data access, governance and observability are essential for trustworthy, compliant AI outcomes

The AI opportunity (and threat) is forcing enterprises to reassess their digital foundations. Public cloud and SaaS strategies that promised simplicity and speed are now under greater scrutiny as regulatory pressure, resilience demands, and sovereignty concerns drive the need for greater control, transparency and choice. Digital infrastructure – spanning networks, cloud, cybersecurity and data centers – has become central to business performance.

Many multinational organizations have already modernized parts of their estate, moving workloads to public cloud and adopting SaaS to reduce overhead and accelerate deployment. But in many cases, this has created fragmented environments, uneven compliance across regions and limited end-to-end visibility. Others have modernized piecemeal, upgrading individual components without end-to-end transformation, leaving them with inconsistent performance, scalability constraints and greater exposure to risk.

This is now becoming an AI problem as well as an infrastructure problem. AI workloads depend on high-bandwidth, low-latency, secure and reliable connectivity across distributed environments. They also require infrastructure that can handle complex data flows while maintaining governance, resilience and compliance. “Controlling key technological components is essential, otherwise we risk unpleasant surprises,” said Guillaume Poupard, Chief Trust Officer, Orange.

According to IDC, by 2029, tech debt and a lack of modernization will lead to \$100 billion in annual losses for the world’s largest companies as they struggle to meet the demand for AI and protect older infrastructure¹.

“

“Trust and strong digital foundations are now the true pillars of strategic autonomy in an unpredictable world.”

Aliette Mousnier-Lompré
CEO of Orange Business

”



Resilience cannot come at the cost of complexity

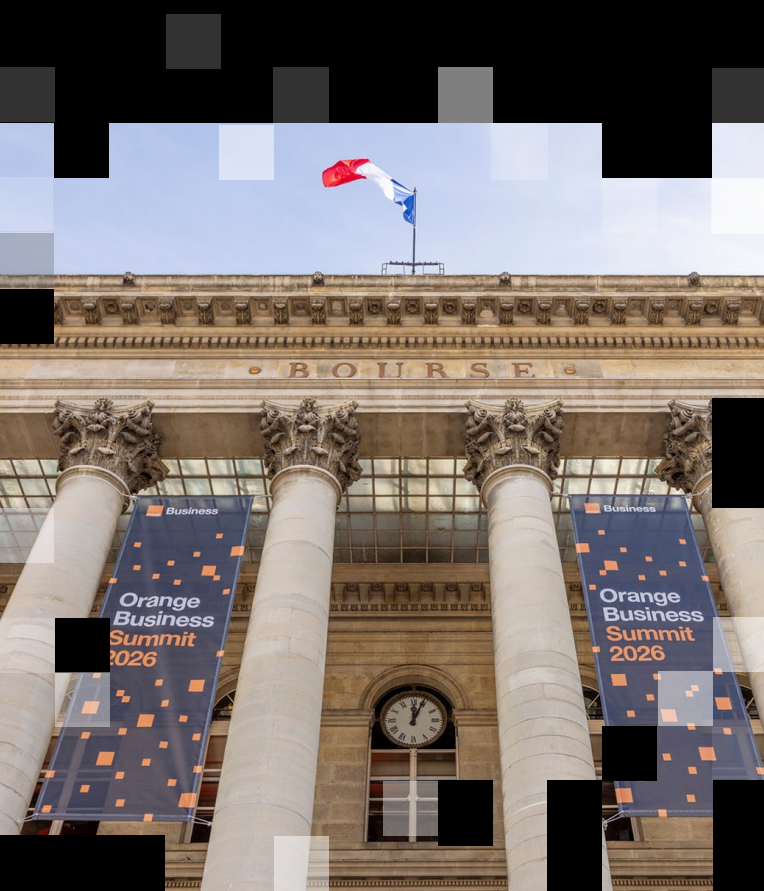
A patchwork of sovereignty requirements makes a single global infrastructure model impractical. Data residency rules, national regulations and local operating constraints require systems that can be adapted locally while still being governed centrally. At the same time, no single provider can meet every need across cloud, network, security, data and AI. That is why many organizations are moving towards multicloud strategies to improve flexibility and reduce lock-in.

But multicloud also creates new complexity. Instead of one unified system, enterprises are left managing multiple interconnected environments, each with its own tools, standards and risk profile. Integration becomes harder. Governance becomes harder. Security becomes harder. Enterprises need strategic autonomy, the ability to remain in control while staying connected to a broader ecosystem.

But multicloud also creates a more fragmented operating environment. Instead of one unified system, enterprises are left managing interconnected platforms with different tools, standards and risk models. Complexity rises across integration, governance and security. Enterprises need strategic autonomy, the ability to remain in control while staying connected to a broader ecosystem.

As Aliette Mousnier-Lompré, CEO of Orange Business, said at the summit, “Trust and strong digital foundations are now the true pillars of strategic autonomy in an unpredictable world.”

The objective is not independence at any cost. It is a secure, future-ready infrastructure that balances control with openness, and sovereignty with global collaboration. That is what gives enterprises a reliable foundation for AI, while protecting sensitive data, supporting compliance and preserving room to evolve.



Building trusted infrastructure through platformization and choice

Enterprises need infrastructure that is scalable, secure and flexible, without being locked into a single vendor or burdened by unnecessary integration work. The most effective model is modular: best-of-breed components working together through a common management layer, with end-to-end observability and centralized control. That gives enterprises the agility to evolve their estate on their own terms.

This is why platformization is central to the Orange Business strategy. As an operator, integrator and platform provider, we combine networking expertise, systems integration and cloud capabilities to give enterprises greater flexibility, choice and control across the full digital estate.

Platformization allows infrastructure to be built from composable components that can be updated, expanded or replaced independently. This helps enterprises innovate faster, reduce complexity and embed security more consistently across the estate. It also creates a stronger foundation for AI by making it easier to integrate agentic AI, automate processes and scale new services.

Orange Business has structured this approach around three platforms – Evolution Platform, Cloud Avenue and Live Intelligence – which together support connectivity, cloud and AI in a trusted, integrated environment.

“

“Sovereignty is not about being isolated but maintaining one’s capacity for decision-making and action.”

”

Guillaume Poupard
Chief Trust Officer at Orange Group



Stronger protection, faster innovation

Trusted digital infrastructure is not only about architecture, it also depends on the ability to secure critical assets, maintain continuity and respond to new threats. Orange Business and the Orange Group continue to invest globally in the infrastructure that matters most – like cellular networks, fiber routes, submarine cables, data centers and private clouds, security operations centers – to strengthen our resilience and protect your business continuity.

At the same time, Orange Business is innovating in areas that directly strengthen trust, from deepfake detection to quantum-safe security. Trust is not static; it must be reinforced continuously through new capabilities that address emerging risks.

AI is already reshaping how enterprises operate, make decisions and compete. But AI value depends on the quality of the infrastructure beneath it. Enterprise AI at scale requires a robust foundation capable of securely handling growing data, supporting distributed workloads, and maintaining strong governance.

Those that modernize now will be better placed to capture AI’s benefits without losing control of risk, compliance or cost. In an unpredictable world, advantage starts with infrastructure you can trust.





Five priorities for building trusted digital infrastructure

The goal is not to transform everything at once but to focus on the areas that matter most, make the right priorities clear, and build a foundation that can support resilience, compliance and AI innovation over time.

- 1 Map your critical dependencies**
Identify the services, data, suppliers and environments whose disruption would have the greatest impact on the business. Trusted infrastructure starts with a clear view of where your operational, regulatory and technology vulnerabilities lie.
- 2 Protect what matters most**
Not every workload requires the same level of resilience, control or sovereignty. Prioritize the areas that cannot fail: sensitive data, critical operations, customer-facing services, and regulated environments.
- 3 Test your freedom to adapt**
Assess how easily your architecture can evolve. Can you switch providers, scale workloads, or introduce new AI use cases without creating excessive dependency or lock-in? Flexibility and reversibility are becoming essential measures of control.
- 4 Connect the stack**
Network, cloud, cybersecurity, observability and AI can no longer be managed in isolation. Trust is built through coherence across the stack, with shared visibility, stronger governance and more consistent execution.
- 5 Build in phases, with governance from the start**
Begin with a phased roadmap, focused on one critical domain at a time, with clear priorities, defined governance and a long-term view of resilience and innovation.

Secure, integrated, modular platforms from Orange Business



Evolution Platform: brings together multi-cloud connectivity, networking and cybersecurity in one cloud-native environment. Built on Orange's global backbone, and developed with Orange Cyberdefense, it provides enterprises with secure, programmable connectivity, greater visibility and end-to-end control across distributed environments. It is designed to combine the convenience of an integrated platform with the flexibility of specialist tools.



Cloud Avenue: is our sovereign cloud platform, operated in 10 highly secure European data centers. It supports hybrid and multicloud environments, critical workloads and AI use cases, while giving organizations stronger control over governance, compliance and continuity. It is also extending to the edge, helping enterprises manage sensitive data closer to machines, sites and point-of-sale systems.



Live Intelligence: is a trusted AI platform designed to simplify enterprise GenAI deployment. It combines secure European hosting, model flexibility, including BYOM, and expert support, helping organizations apply AI with greater control, portability, and compliance. With Live Intelligence Studio, Orange Business is also extending this into agentic AI in a secure and governed environment.



Business

1. IDC FutureScape Worldwide Digital Infrastructure predictions 2025
<https://my.idc.com/research/viewtoc.jsp?containerId=US51665124>

Copyright © Orange Business 2026. All rights reserved. Orange Business is a trading name of the Orange Group and is a trademark of Orange Brand Services Limited. Product information, including specifications, is subject to change without prior notice.