InfoBrief, sponsored by Orange Business | October 2025

Digital Sovereignty

The Crucial Role of the Network in a Sovereign Cloud

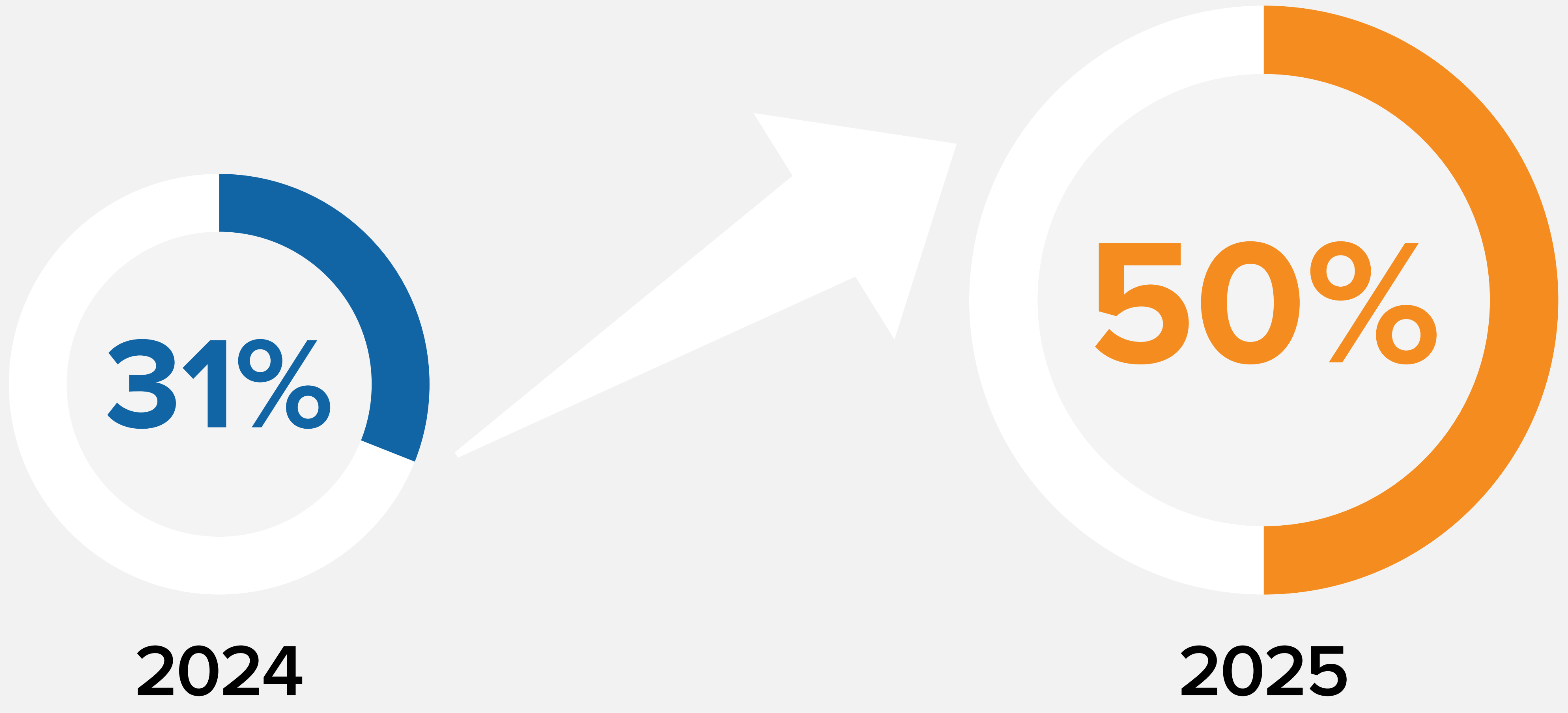
Cyrille Chausson
Research Manager, European
Application Modernization Strategies

Rahiel Nasir
Research Director, European Cloud Practice,
Lead Analyst, Digital Sovereignty

Reinforcing Network Ecosystems Is a Strategic Priority

Building secure, resilient networks is now crucial for European organizations seeking control, compliance, and leadership in a rapidly evolving digital landscape.

Current Use of Sovereign Cloud Solutions Continues to Grow



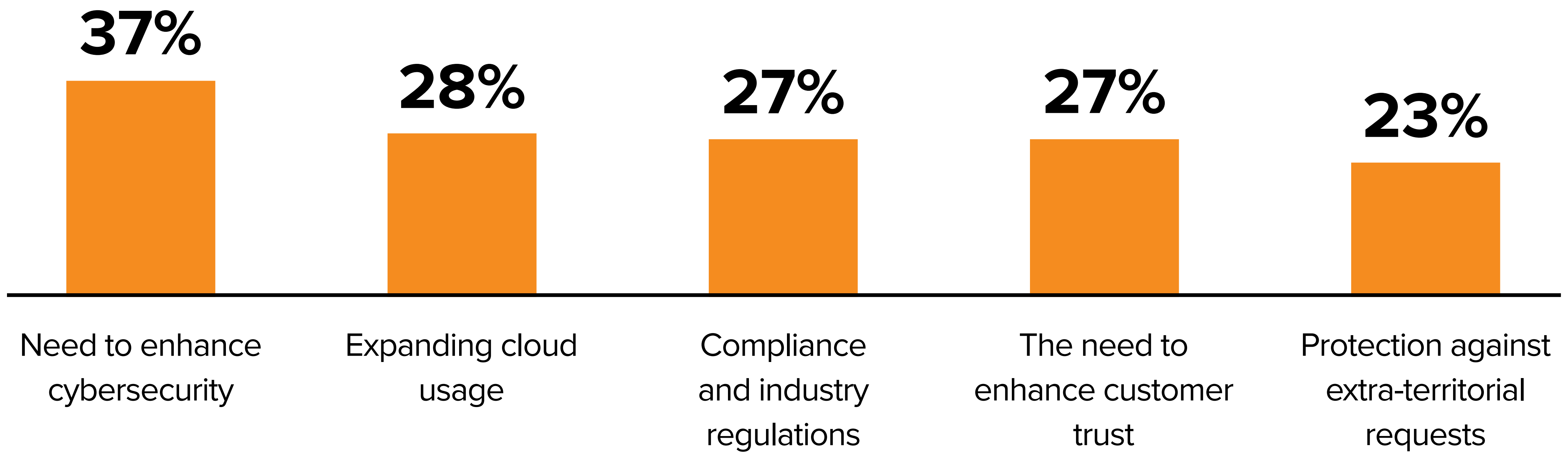
Q: Does your organization use or plan to use a sovereign cloud solution?

Sovereign Cloud Solutions Now a Key Strategic Priority for CEOs in Europe

25% of Western European CEOs consider digital sovereignty to be a key emerging technology investment for the next 12 months.

(Source: IDC's *CEO Survey 2024* (N = 67)

Top 5 Drivers of Sovereign Cloud Usage in Europe



Source: IDC's *European Cloud Survey 2024, September* (N = 1,325)

Network Sovereignty Business Value

Evolving market requirements push organizations to see network sovereignty not only as a compliance goal but as a source of business resilience, differentiation, and value creation.

€5.63 billion

Global spending on the network aspects of sovereign cloud in 2027

(Source: IDC's Worldwide Sovereign Cloud Market Forecast, 2022–2027)

43% of organizations in Europe are willing to pay **11–20%** on top of their existing IT budgets to implement a sovereign cloud solution and the associated networking layer in 2025.

54% **of organizations in Europe** indicated they would allocate up to 10% of their sovereign cloud budget to solutions supporting **technical sovereignty**. This was followed by 17% who would spend 11–20%.

55% of organizations in Europe reported that they plan to allocate up to 10% of their sovereign cloud budget to solutions focused on **operational sovereignty**.

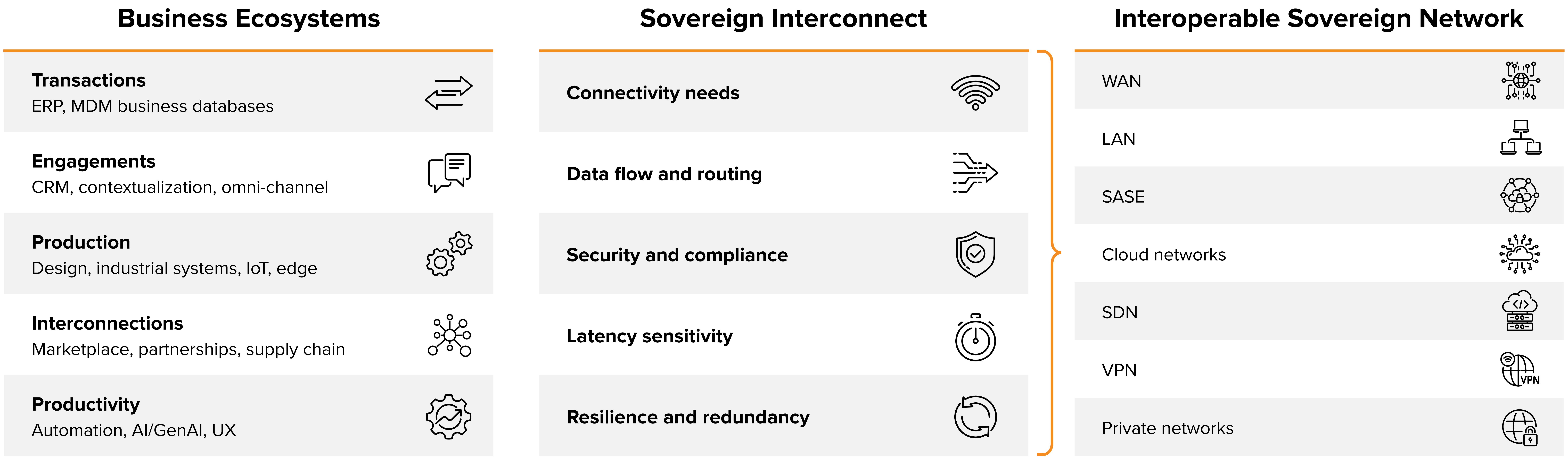
Most of the global spending on sovereign cloud solutions is expected to be on **PaaS applications**, followed by integrated infrastructure for compute and networking.

Source: IDC's *Worldwide Digital Sovereignty Survey*, Europe, 2024 (n = 250), 2025 (n = 370)

Sovereign and Adaptive Networks

Digital operations now require networks that are both sovereign (ensuring control and compliance) and adaptive (enabling real-time agility and resilience in an ever-evolving landscape).

Data and control must remain within jurisdictional boundaries, while robust, adaptable networks driven by workload and data demands are essential to a sovereign digital posture and resiliency.



Business Ecosystems

Transactions
ERP, MDM business databases

Engagements
CRM, contextualization, omni-channel

Production
Design, industrial systems, IoT, edge

Interconnections
Marketplace, partnerships, supply chain

Productivity
Automation, AI/GenAI, UX

Sovereign Interconnect

Connectivity needs

Data flow and routing

Security and compliance

Latency sensitivity

Resilience and redundancy

Interoperable Sovereign Network

WAN

LAN

SASE

Cloud networks

SDN

VPN

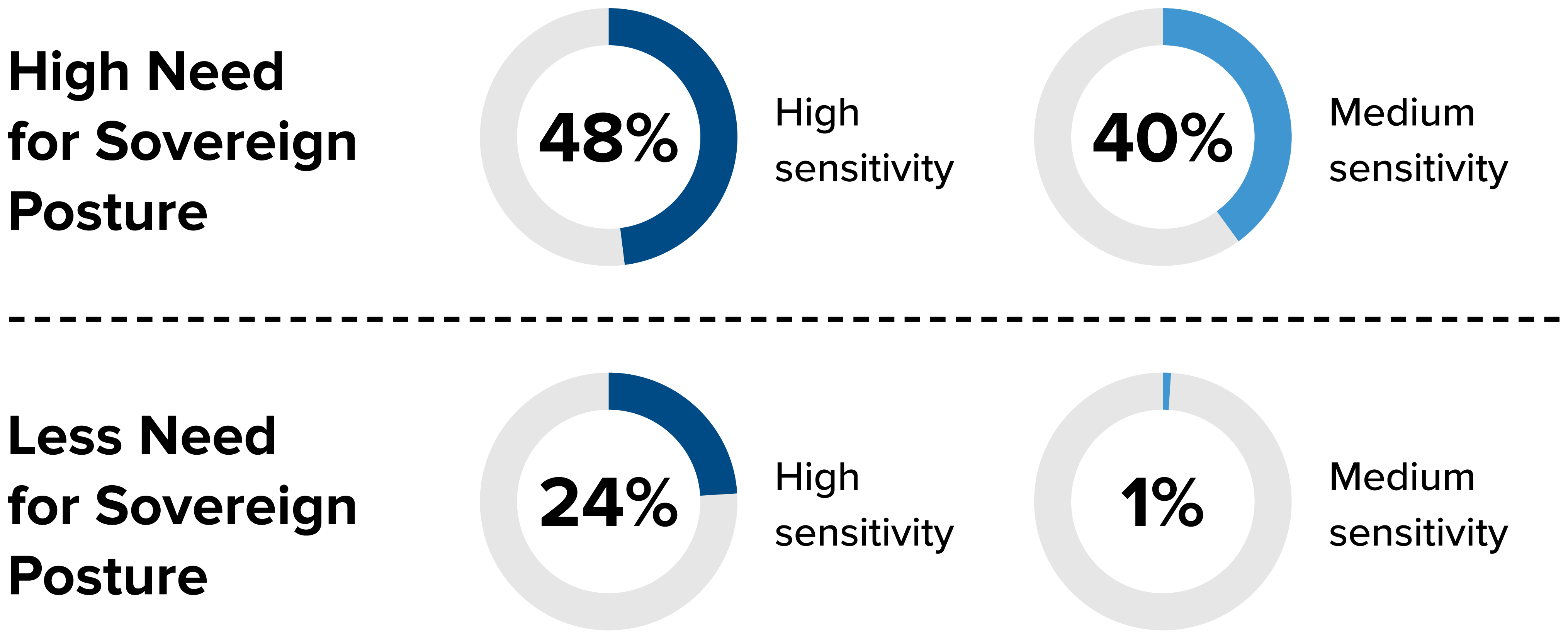
Private networks

Migration of Classified Data and Workloads

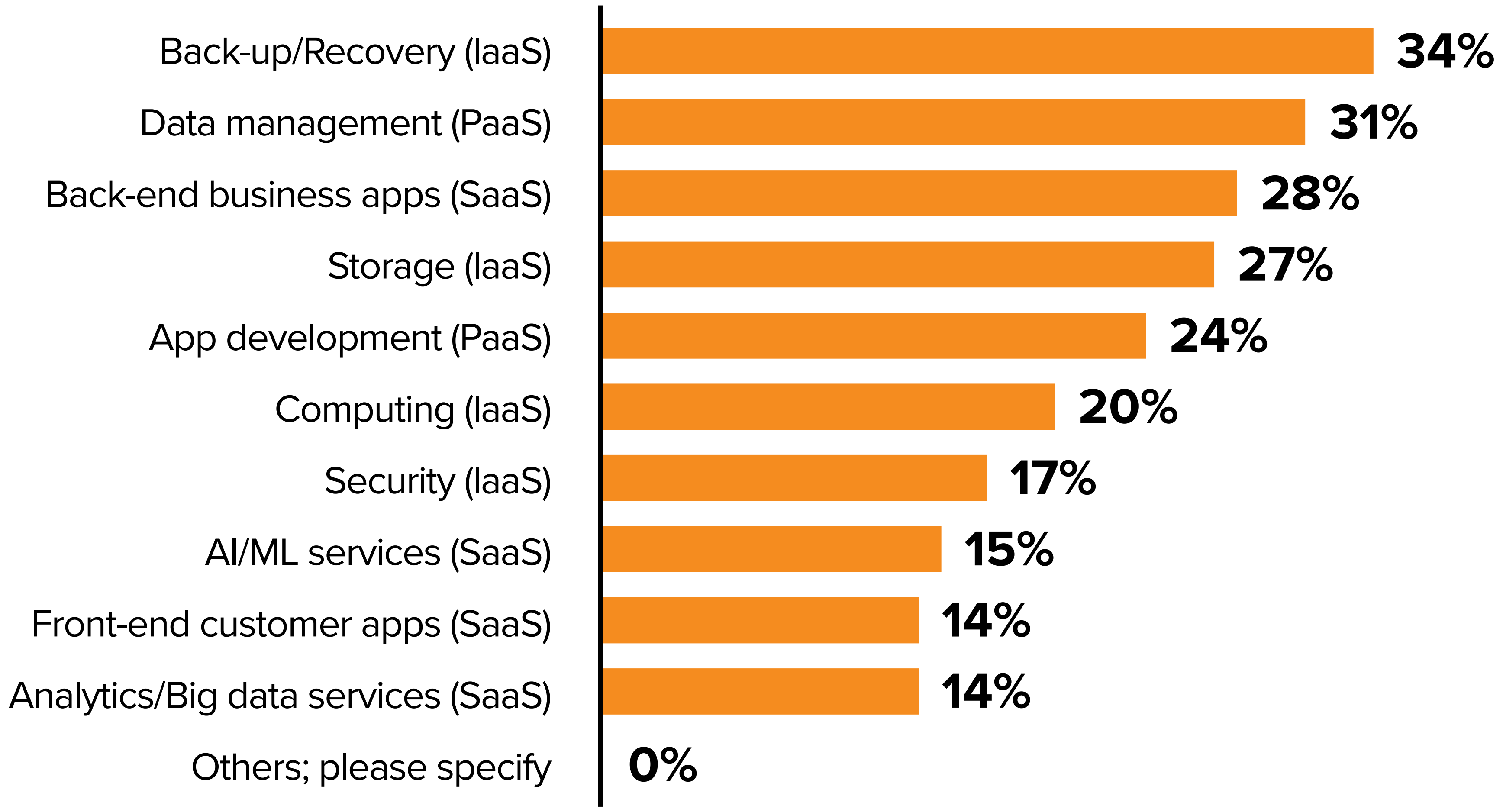
As sensitive workloads move to sovereign clouds, networks must evolve for compliance, security, and rigorous control.

In today's distributed landscape, networks must support diverse workloads, adapt to diverse environments, and **ensure sensitive data is securely managed in transit.**

European organizations are **increasingly demonstrating a strong preference for adopting a sovereign approach** to managing certain applications and workloads.



Q: Does your organization have any data that it currently classifies, or plans to classify in the next 12 months, with the following sensitivity ratings? [Choose all that apply]



Q: Which workloads did your organization migrate of expect to migrate to sovereign cloud?

Sovereign network requirements must be evaluated and aligned with flexible network architectures that support specific workloads and data demands, ensuring alignment with data localization needs (including edge deployments), encryption standards, regulatory compliance, and low-latency and high I/O performance expectations.

Source: IDC's *Worldwide Digital Sovereignty Survey*, Europe, 2024 (n = 250), 2025 (n = 370)

Urgency of Network Transformation

Compliance with digital sovereignty requirements is compelling organizations to accelerate network transformation and invest in secure, resilient infrastructure.

The urgency of network transformation is driving priority investment decisions.

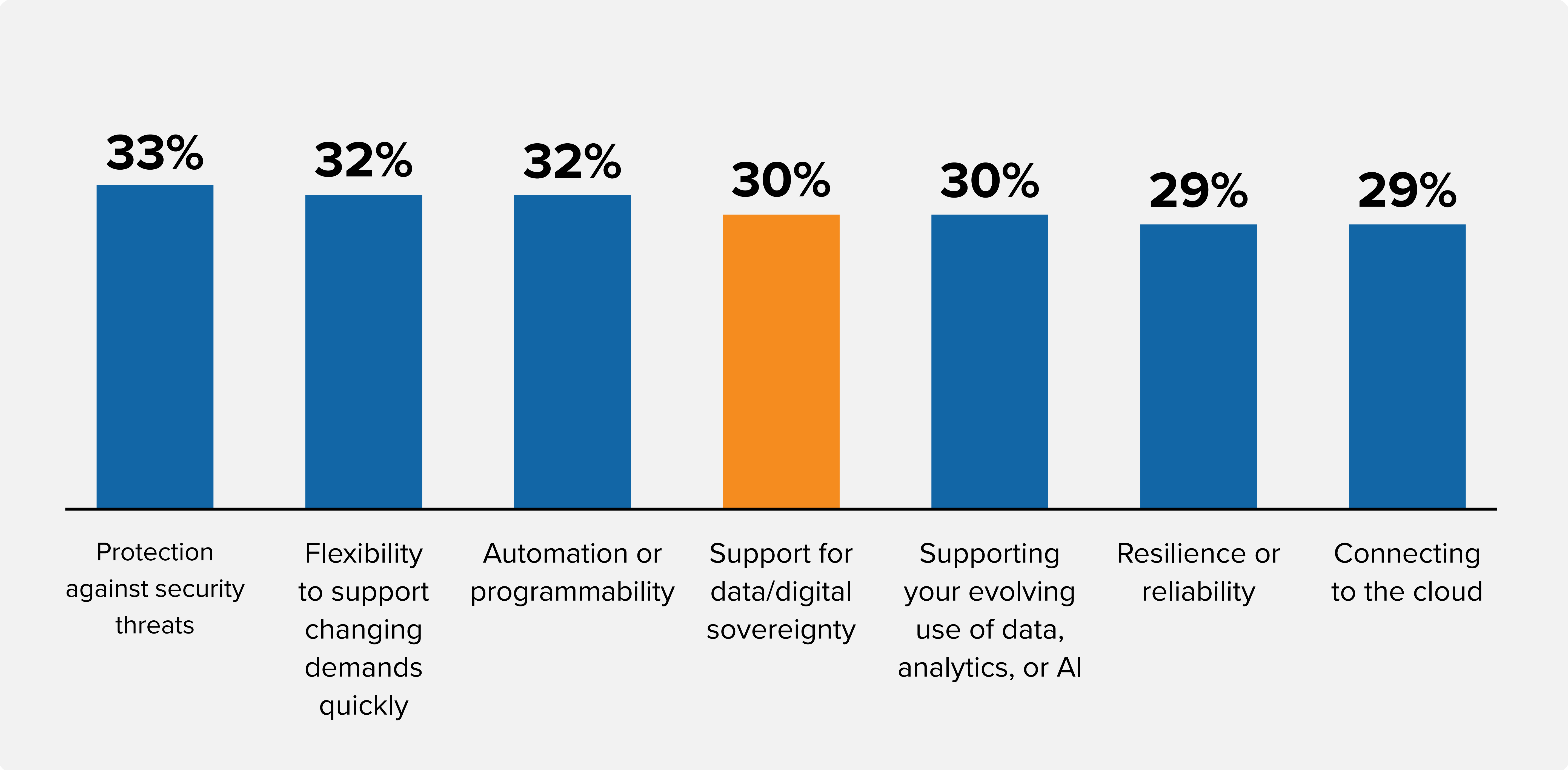
Network security and agility, enhanced by automation, support business alignment while ensuring continuous compliance for network and IT systems.

European organizations are increasingly compelled to realign their network connectivity strategies (including WAN and VPN) to comply with digital and data sovereignty requirements. This ensures the resilience and continuity of their broader business objectives.

38%

of respondents said treating network enhancement as an urgent response to sovereignty pressures is a pragmatic investment. The effects of sovereignty on network operations are anything but marginal. (*WAN and VPN users)

Q: In which areas does your organization need to improve its networks urgently? [WAN and VPN users only]



Source: WW C-Suite Tech Survey, IDC, August, 2023, n DNB=130

Building the Sovereign Foundation

A sovereign network is the cornerstone of digital independence, resilience, and compliance, laying a secure foundation for the organization's future.

No Digital Sovereignty Without Network Sovereignty

Enhancing control of all data assets, including all underpinning sovereign cloud infrastructure (e.g., datacenters and networks), software and services, and all administrators and support personnel with access to those assets

Ensuring resilience against physical disruptions (e.g., natural disasters), cyberthreats, and external pressures (e.g., geopolitical tensions and regulatory constraints) while safeguarding continuous service delivery and uninterrupted connectivity

Mitigating the risks of compromising data over the network, including traffic interception, cable cuts, loss of confidentiality and integrity, and DDoS attacks. It is crucial to apply sovereign controls not only to data at rest but also to data in transit. Without network sovereignty, creating a sovereign cloud stack is impossible, as data in transit risks being compromised.

Building a Sovereign Network

Operational Sovereignty

25% of European organizations classify the network equipment used for data and voice traffic (including WAN optimization and WLAN) as "extremely important" for **achieving operational sovereignty.**

Technical Sovereignty

Surveyed solutions organizations in Europe consider the following aspects as "extremely important" for achieving technical sovereignty:

45%	32%	29%	24%
Network infrastructure software to enable virtualized networking	Integrated infrastructure systems and platforms	Network security appliances	Network management software

Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, Europe (n = 370)

Building Blocks of Sovereign Network Operations and Connectivity

Modern sovereign networks are defined by foundational elements working together to assure digital independence and trusted connectivity in a complex regulatory environment.

1

Infrastructure Control and Operational Independence

- Full governance of the cables, infrastructure, and technologies supporting the core network
- Secure, qualified/certified equipment
- Operational resiliency with limited dependencies
- Secure co-management environment (RBAC, IAM)
- Control over operators' location and nationality

2

End-to-End Data Protection

- Secure data management and control — data localization, residency, data integrity, and data confidentiality
- End-to-end encryption (In transit and stored)
- Traffic segmentation and critical workflow classification
- Secure network management and control data (inventory, configurations, and logs)

3

Service Delivery and Organizational Efficiency

- Continuous training of internal teams (compliance and cybersecurity)
- Trusted and transparent ecosystem of partners and solutions
- Infrastructure testing (including PCA/PRA)

4

Active Defense and Cybersecurity Assurance

- Zero-trust network access
- Network micro-segmentation
- Threat intelligence services
- Security solutions (e.g., SASE)
- DDoS protection

Cost of Inaction

Failing to invest in digital and strategic sovereignty exposes European industries to security, economic, and innovation risks that threaten long-term resilience and competitiveness.

What vulnerabilities emerge when network sovereignty is not enforced?

IT RISKS

- **No dedicated and isolated network:** In case of disasters or attacks, physical and mobile networks (including emergency services) and cyberdefense posture will suffer from devastating downtime.
- **Erosion of cybersecurity resilience:** Increased exposure to data breaches, cyberattacks, cybersurveillance, and unauthorized network access puts sensitive data at significant risk.
- **Route hijacking and BGP leaks:** Organizations may suffer from temporary unavailability due to a loss in connectivity, traffic interceptions, data theft, or redirection to a malicious server.
- **Dependence, vendor lock-in, and unexpected reversibility costs:** Proprietary formats and egress fees may be very restrictive, limiting PRA/PCA and migration capabilities.
- **Technical non-compliance with EU regulations:** The lack of MFA or weak network segmentation may expose organizations to penalties and audits.

BUSINESS RISKS

- **Lack of customer trust** due to uncontrolled data privacy, protection, and compliance policy. Reputation loss may be highly prejudicial.
- **Loss of resiliency:** The organization is exposed to unexpected network cuts, supply-chain disruptions, and degradation of operations. IT/OT systems could be compromised.
- **Untrusted ecosystem:** The lack of robust, secure regional IT infrastructure and interoperable networks poses a significant barrier to efficient and cohesive collaboration within the European Union.
- **Delayed innovation:** Organizations may suffer from the leakage of industrial secrets, leading to delays in bringing products to market and innovations.
- **Contractual or regulatory obstacles to exports or international growth:** Some jurisdictions impose restrictions on data export or mandate reversibility and traceability requirements.

Selecting a Strategic Sovereign Network Partner

Choose a partner with local data center ownership, national certifications, and global cloud alliances for true sovereignty and seamless connectivity on a local and international level.

41% of European organizations consider reliance on cloud to be driving **urgent network upgrades** to meet sovereignty constraints (*WAN and VPN users)

20% struggle to find network infrastructure providers who offer sovereign connectivity options.

This highlights the need for clearer sovereign criteria and reference selection points.

20% of European organizations view reliance on non-EU suppliers for network infrastructure equipment as a key concern in maintaining digital sovereignty.

Important Attributes When Choosing a Sovereign Network Partner or Provider

47%	Ownership of in-country datacenters
45%	Country-level certifications for cybersecurity and cloud
42%	Sovereign control of all network infrastructure and connectivity options
36%	Solutions to support operational resilience
35%	Ability to reverse data from cloud to on premises
30%	Strong ecosystem of partners that adhere to sovereign principles
25%	Employment of local citizens for all technical operations
20%	Local player with national or regional footprint only

Source: IDC's *Worldwide Digital Sovereignty Survey, 2025*, Europe (n = 370)

Orange Business's "Trust by Default" Infrastructures as the Foundation for Trusted Connectivity

Full Control of the Infrastructure

- Orange ownership of our network, cables and routing plans with no dependence on third parties
- Full control over investments, routing policies, and technological developments
- Transparency and traceability to ensure sovereignty and compliance
- Increasing the share of core network equipment developed in open source by Orange

Autonomous Operational Model

- 24 x 7 operations managed by our in-house Orange teams
- Expertise from Level 1 to 3, covering all technologies
- Dedicated processes and tools to ensure responsiveness, agility, and independent decision-making

Integrated Security and Resilience

- Redondances eServices designed as "secured by design" with DDoS protection and 24 x 7 proactive monitoring
- Redundancies and robust architectures ensure continuity and availability, even in the event of an incident
- Unmatched SLA results and advanced cyberthreat mitigation capabilities

Talk to our experts to boost your connectivity security and resilience.

Message from Sponsor

orange™ Business

Orange Business, the enterprise division of the Orange Group, is a leading network and digital integrator, supporting customers to create positive impact and digital business. The combined strength of its next-generation connectivity, cloud, and cybersecurity expertise, platforms, and partners provides the foundation for enterprises around the world. With 30,000 employees across 65 countries, Orange Business enables its customers' transformations by orchestrating end-to-end secured digital infrastructure and focusing on the employee, customer, and operational experience. More than 30,000 B-to-B customers put their trust in Orange Business globally. Orange is one of the world's leading telecommunications operators with revenues of 40.3 billion euros in 2024 and 300 million customers worldwide at 30 June 2025. In February 2023, the Group presented its strategic plan "Lead the Future", built on a new business model and guided by responsibility and efficiency. "Lead the Future" capitalizes on network excellence to reinforce Orange's leadership in service quality.

Orange is listed on the Euronext Paris (ORA).

For more information: www.orange-business.com
or follow us on LinkedIn and on X: @orangebusiness

Orange and any other Orange product or service names included in this material are trademarks of Orange or Orange Brand Services Limited

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

IDC UK
1st floor, Whitfield Street, London, W1T 2RE, United Kingdom
T 44.208.987.7100

𝕏 @idc   in @idc   idc.com