Omdia
by informa techtarget

Sovereign Enterprise: Securing Global Business from Space

Author: Ruth Brown

June 2026

In partnership with:

ses™

This Omdia White Paper was commissioned by SES.

Introduction

A succession of subsea cable cuts across the Baltic and Red Seas between February 2024 and December 2025 has exposed the fragile reality of global data paths, transforming geopolitical risk from an abstract concern into an immediate vulnerability. These disruptions are forcing enterprises to reconsider network connectivity designs. Coverage, performance, and cost remain important, but are no longer sufficient. Network resilience now includes consideration of infrastructure governance, data path segregation, and operational independence.

At the same time, satellite connectivity has evolved into a scalable infrastructure that adds network flexibility and extends connectivity beyond the limits of terrestrial network footprints. For global organizations operating across borders or transmitting private data, this evolution creates new opportunities while also raising new questions as to how to reorient network architecture around sovereignty and business continuity.

This paper examines the advantages, use cases, and architectural components of "sovereign enterprise" satellite solutions. It also explores how organizations can use these solutions to strengthen operational resilience, support regulatory requirements, and maintain greater control over their network critical communications infrastructure.

This Omdia White Paper was commissioned by SES.

Satellite for the sovereign enterprise

The case for the sovereign enterprise and the inclusion of satellite into enterprise infrastructure is being shaped by converging market, regulatory, and operational pressures.

Market momentum

Recent geopolitical friction, natural disasters, and the fallout from prolonged countrywide blackouts such as those in 2025 across the Iberian Peninsula have exposed critical enterprise network vulnerabilities. Uninterrupted network access is now a vital business imperative. According to Heavy Reading's *Satellite Networks: Expanding Reach, Reliability, and Performance – 2025 Survey Analysis*, 81% of enterprises acknowledge that connectivity loss immediately impacts operations and customer experience.

The financial case for sovereign satellite investment is grounded in the quantifiable cost of disruption. According to *Computer Weekly* (November 2025), IT outages cost on average £600,000 ($800,000) per hour for a UK investment bank—and costs are rising across the 10 highest dependency verticals, including banking, energy, government, and healthcare.

Organizations are prioritizing not only availability but also security, operational independence, and governance over their communications infrastructure, driving investment across the energy, finance, defense, and government segments. Omdia's *Critical Communications Broadband Report – 2025 Analysis* (April 2026) values the critical broadband infrastructure market at $1.5bn in 2025, with growth projected at a 23% CAGR through to 2030.

While this initial wave of funding heavily targets terrestrial networks, traditional infrastructure alone cannot close coverage gaps or deliver the flexibility needed to meet network resiliency expectations. This market gap is driving demand for satellite solutions—particularly those that are designed to deliver reach, redundancy, and security for remote sites, international operations, and mission-critical applications. Both governments and commercial satellite operators are actively deploying dedicated, sovereign-focused satellite solutions to meet rising enterprise demand.

This Omdia White Paper was commissioned by SES.

Sovereign enterprise

Satellite infrastructure designed for the sovereign enterprise delivers distinct competitive advantages to enterprise resilience, security, and growth. These include the following:

- **Strategic autonomy:** Shielding sensitive information from geopolitical volatility by prioritizing direct, single-hop sovereign links over managed multi-hop connections. This provides transparency and ensures that traffic does not traverse unauthorized airspace or orbits.
- **Architectural resilience:** Providing a hardened backbone for disaster recovery that extends secure coverage via diverse paths to remote offices, strategic assets, critical infrastructure, and geopolitically sensitive regions. Automated failover mechanisms ensure uninterrupted network continuity when primary gateways or terrestrial links are compromised, with all operations anchored by sovereign oversight and control of the space-based infrastructure.
- **Regulatory compliance and cloud integrity:** Enabling high capacity cloud on-ramps for heavily regulated sectors—such as energy, finance, government—through strict physical, regional control and fully auditable data residency. Strict data governance directly addresses sector-specific mandates, such as DORA for finance, NIS2 for critical infrastructure, and broader cross-sectoral regulation under the EU Data Act, thereby mitigating the severe financial and operational risks of noncompliance.

Sovereign enterprise components

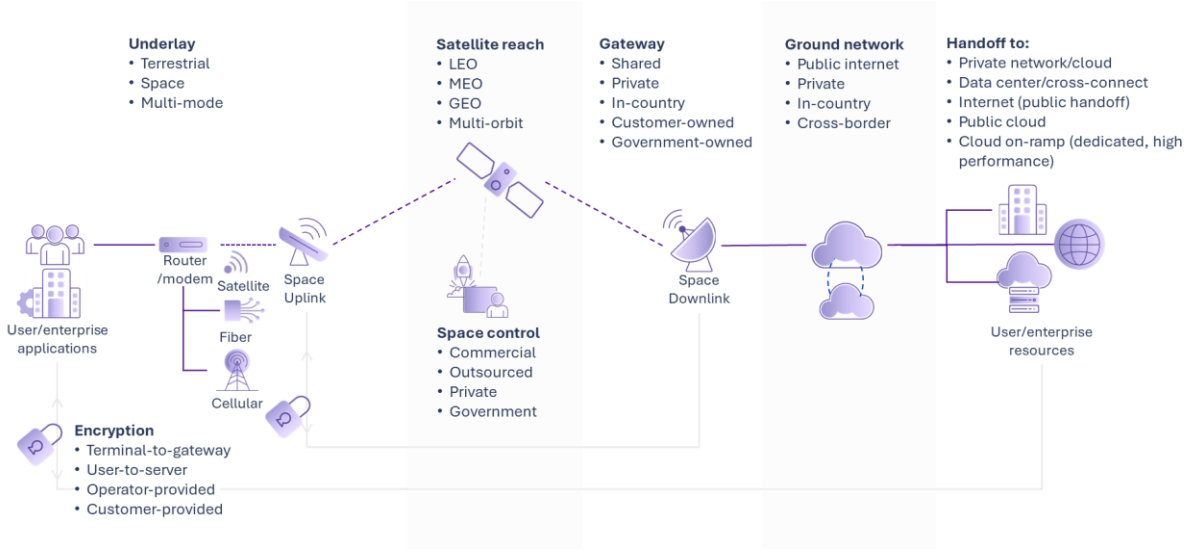
For organizations designing to meet sovereign enterprise goals, sovereignty is not one-size-fits-all—it is a multi-layered connectivity architecture. The challenge is to match enterprise sovereignty requirements with the right combination of space, ground, and terrestrial components without overengineering or unnecessarily inflating project costs.

This Omdia White Paper was commissioned by SES.

Mapping architecture to requirements

Figure 1 illustrates end-to-end infrastructure options for enterprise sovereignty. Organizations can evaluate sovereign levels for each transit segment—from access underlay and space control to gateway, ground network choice, and handoff destination.

Figure 1: Sovereign enterprise end-to-end network and infrastructure options



Source: Omdia, SES

Satellite as an underlay network

Whether used as the sole underlay for a remote site or alongside fiber and cellular as part of a hybrid terrestrial/non-terrestrial (TN/NTN) infrastructure, satellite services introduce considerations unique to space transport.

Space control of satellite assets will vary widely based on the enterprise, industry regulations, and the organizational need to ensure ongoing access to space. Where options are limited, other network components, such as encryption and gateway location, may be sufficient to address sovereignty requirements.

- **Commercial (shared):** Scalable and cost-efficient for standard enterprise requirements. Traffic shares hardware with other customers; no physical data isolation. Availability and routing decisions are controlled by the satellite operator.
- **Outsourced (hosted):** Satellite operators allocate specific onboard capabilities, such as localized beams, dedicated frequencies, or entire satellite payloads, to individual customers, providing separation without the full cost of private satellite ownership.

- **Private:** A dedicated single-tenant satellite providing exclusive control over link parameters and operations.
- **Government:** Fully isolated, government-controlled satellite. May be built to defense-grade specifications for classified data and security workloads or designed for commercial use for approved organizations.

Satellite orbit (e.g., LEO, MEO, GEO, or multi-orbit) will affect application performance and how well a given space solution may address different enterprise use cases. The result will impact network reach, the number of space and ground hops, latency, and jitter.

Data encryption can be applied by the user and/or as part of the infrastructure. Typical configurations rely on software-based security, which can be customer-managed (e.g., user-to-server VPN) or operator-provided (e.g., satellite-modem-to-gateway). Tighter sovereign architectures may enforce customer- or government-controlled hardware encryption, using dedicated cryptographic modules to ensure data integrity.

Gateway infrastructure

Consider a typical data flow: a remote site transmits data via antenna uplink to a satellite, then downlinks to a gateway before reaching a central cloud resource. The gateway acts as the space-to-ground interface between the satellite and the terrestrial network. Options range from shared, satellite-operator-owned, multi-tenant teleport facilities to dedicated, single-tenant private gateways. Gateways may be deployed in-country (in the same country where the remote site resides) or located to aggregate traffic from across a broad region. Customer- or government-owned gateways eliminate third-party dependencies and security concerns.

Ground network and handoff

The ground network is the final transit leg. As with satellite control, options may be limited based on the operator delivering satellite service to a particular remote location. The coverage and design of the operator ground network will determine where customer traffic flows and what borders it traverses, which can impact overall application performance.

Organizations may choose to hand off traffic to the public internet or public cloud, or connect to a data center via cross-connect with the operator’s terrestrial network. For sovereign architectures, a dedicated connection at the gateway to a private network or a dedicated cloud on-ramp can keep data physically isolated and under better enterprise governance.

This Omdia White Paper was commissioned by SES.

Sovereign enterprise models with satellite

Sovereignty requirements vary significantly across organizations and use cases. Some enterprises require complete separation and control across data, infrastructure, and operations; others may only need to address specific elements, such as data residency, the data path, encryption, or network management. **Table 1** provides examples of how different requirements could map to satellite sovereignty models across government, finance, energy, and critical infrastructure.

Table 1: Example sovereign satellite enterprise models

Sector	Challenges	Sample sovereign satellite enterprise architectures	Key outcomes
Civil defense and critical comms	Terrestrial networks may fail during disasters, cutting emergency services	**Space:** Government-controlled, priority access **Gateway:** Government-owned, Secure teleport **Underlay:** Fully resilient, automated fallback terrestrial fiber and satellite	• Maintained operations during blackout • Fast failover • Full sovereign isolation
Government Embassy & diplomatic networks	Ensuring consistent access to secure networks, ensuring privacy for sensitive information	**Space:** Private/dedicated satellite **Gateway:** In-country, enterprise on-prem landing **Encryption:** Customer-provided, hardware-based	• Zero foreign data transit • Extremely high uptime across vulnerable remote sites
Finance Regulated banking	Branch networks in underserved regions may require secure, compliant connectivity for real-time transactions, regardless of the condition of local infrastructure	**Space:** Outsourced/hosted satellite, single-hop P2P **Gateway:** Private, single-tenant landing on-prem **Encryption:** Customer-managed, strict-in-country network routing	• Full regulatory compliance • 24/7 transaction capability
Energy Smart grids, infrastructure, extraction	Remote pipelines, wind farms, and offshore platforms often lack terrestrial connectivity and are strategic national/ continental grid infrastructure	**Space:** Outsourced/hosted satellite for primary connectivity **Gateway:** Private landing **Ground/handoff:** Isolated cross-border private fiber routing	• Extremely high uptime • Low latency • Path auditability across jurisdictions • Internet of Things (IoT) telemetry continuity
Global enterprise connectivity Corporate traffic	Prolonged terrestrial outages disrupt core office operations and sever vital customer systems, leading to revenue and reputational loss	**Space:** Commercial satellite sovereign backup path **Gateway/encryption:** Commercial (shared), enterprise-managed software security (zero-trust network access/SD-WAN)	• Logical sovereignty, data isolation over public infrastructure • Cost-effective continuity • Mitigate operational and customer downtime

Source: Omdia

Conclusions

Satellite connectivity has grown in relevance for enterprise networking solutions in the last few years, offering unique benefits for network designers while introducing new network components and concepts around data privacy and network ownership. As part of a sovereign enterprise design, space-based connectivity can offer data path resiliency and operational independence, enabling organizations to insulate themselves from terrestrial vulnerabilities and geopolitical friction.

Operationalizing strategic resilience requires organizations to assess their financial and regulatory requirements and map them against the space, gateway, and ground architectures outlined in this paper. With this knowledge, enterprises can engage sovereign-capable providers and architect solutions that will ensure operational continuity while safeguarding competitive advantage in an unpredictable global market.

Appendix

Methodology

This report and its findings are based on research and discussions with satellite connectivity providers, carriers, and communications service providers (CSPs). Omdia considered research from the Heavy Reading *Satellite Networks: Expanding Reach, Reliability, and Performance – 2025 Survey Analysis* and the Omdia *Critical Communications Broadband Report – 2025 Analysis* in the course of writing this report.

Further reading

Satellite Networks: Expanding Reach, Reliability, and Performance – 2025 Survey Analysis, Heavy Reading (June 2025)

Critical Communications Broadband Report – 2025 Analysis, Omdia (April 2026)

Ruth Brown, Senior Principal Analyst, Mobile Networks, GTM Telecom Insights and Advisory

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B Materials information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.