colt | ANALYST DAY 2026

colt

BE SOVEREIGN-READY OR GET LEFT BEHIND.

MIRKO VOLTOLINI VP Network Platforms and Innovation

ALESSANDRO GALTIERI - Corporate Law & Deputy General Counsel

MARKET TRENDS & OPPORTUNITY FOR DIGITAL SOVEREIGNTY

colt

RISING DEMAND FOR DATA SOVEREIGNTY

European enterprises and local governments are increasingly prioritizing data control due to concerns about foreign access laws like the US CLOUD Act and compliance with EU regulations such as GDPR.

SHIFT TOWARD EUROPEAN SOVEREIGN CLOUD SERVICE PROVIDERS (CSP'S)

Organizations are moving workloads to sovereign cloud platforms (e.g. OVH, Microsoft Sovereign Cloud) to ensure data stays within the EU and is governed by local laws.

HYBRID AND MULTI-CLOUD STRATEGIES EMERGING

Businesses are adopting architectures that combine sovereign clouds for sensitive data and public clouds for scalability, balancing compliance with flexibility. Both Sovereign Cloud & Network in scope.

GEOPOLITICAL AND REGULATORY PRESSURE ACCELERATING ADOPTION

Trade tensions, digital autonomy goals are driving public and private sectors to reduce reliance on US hyperscalers and strengthen European cloud ecosystems.

- » Analysts expect sovereign-cloud infrastructure as a service (IaaS) spending to reach $169 billion by 2028 — a CAGR of 36%
- » By 2028, 65% of governments worldwide will introduce some technological sovereignty requirements

Source: BCG – 2025: https://web-assets.bcg.com/f7/14/83ae5e934701880e7112cbdcda31/price-swings-sovereignty-demands-and-wasted-resources-aug2025.pdf

THE EU COMMISSION CLOUD SOVEREIGN FRAMEWORK

colt

Cloud Sovereignty definition applicable to Colt - the European Commission definition is a good place to start:

Strategic Sovereignty	Providers are anchored within the European Union legal, financial, and industrial ecosystem. It assesses ownership stability, governance influence, and alignment with EU strategic priorities.
Legal & Jurisdictional Sovereignty	Exposure to foreign authority, and enforceability of rights that govern the services of a technology provider. It determines the extent to which the services are anchored in European jurisdiction and insulated from external legal claims.
Data & AI Sovereignty	Independence of data assets and AI services within the EU. It addresses how data is secured, where it is processed, and the degree of autonomy customers retain over AI capabilities.
Operational Sovereignty	Run, support, and evolve a technology independently of foreign control. It focuses on continuity of operations, skill availability, and resilience against external dependencies.
Supply Chain Sovereignty	Transparency, and resilience of the technology supply chain, focusing on the extent to which critical components and processes remain under EU control or exposed to non-EU dependencies.
Technology Sovereignty	Transparency, and independence in the underlying technological stack, ensuring EU actors can interoperate, audit, and evolve solutions without lock-in to foreign proprietary systems.
Sec & Compliance Sovereignty	Security operations, compliance obligations, and resilience measures are controlled within the EU, ensuring independence from foreign jurisdictions and long-term operational assurance.
Environmental Sovereignty	Services over the long term in relation to energy usage, dependency and raw material scarcity.

ON ALL OF THESE ASPECTS, COLT CAN CONFIDENTLY PRESENT AN EXCELLENT TRACK RECORD

DIGITAL SOVEREIGNTY: WHAT DOES IT MEAN FOR COLT?

Digital Sovereignty for Colt is about ensuring the control of network infrastructure, the control of data in transit and the control of its governing data is kept under legal, operational and technical control within a customer's desired jurisdiction.

DATA & AI SOVEREIGNTY *(INCL LEGAL & COMPLIANCE)*	OPERATIONAL SOVEREIGNTY	TECHNOLOGY & INFRASTRUCTURE SOVEREIGNTY
Control over the location, access and legal ad compliance regime of the customer governing data.	Control on how the network infrastructure and its governing platforms are operated and who operates them.	Control on the technology, infrastructure and data in transit.

COLT HAS THE RIGHT TO BECOME THE LEADING EUROPEAN TELCO FOR DIGITAL SOVEREIGNTY

ISO27701 CERTIFIED

EU &UK BCR's

EU Ops Centre

Sovereign Professional Services

colt iq network Smart Path

SCION ELEVATING SECURE COMMUNICATION

DCA to Sovereign Clouds


colt
DATA & OPERATIONAL
SOVEREIGNTY.
ANALYST DAY
2026

COLT´S INTEGRATED COMPLIANCE STRUCTURE

EU & UK BCRS

Colt is the only telco with GDPR-compliant binding corporate rules, approved under both **EU GDPR** & **UK GDPR**, covering Controller + Processor roles

- Cross-border transfers within Colt are subject to a binding, regulator-approved privacy framework
- Gold standard Certification in Data Protection Compliance
- BCRs serve as Colt's global privacy backbone, embedding strict data governance into operations and digital resilience activities
- BCR audits encompass all privacy controls, including AI governance.

ISO 27701 PIMS

Colt is the sole Telecom company that has obtained this certification in February 2024 on a country-by-country basis for both controller and processor.

- Global Compliance certification on Privacy & Security standards to protect Personal Data.
- ISO 27701 as the standard for data security shows customers that Colt supports GDPR compliance and privacy legislation. An ISO certificate also ensures a reduced risk of liability.
- ISO 27701 should be partially audited externally on an annual basis, and for its maintenance, it needs to be audited for renewal every three years. This is a further guarantee for customers.

MATURE DP GOVERNANCE MODEL

Colt has a single, harmonised data protection governance model that ensures clear accountability, effective oversight, and consistent GDPR application across the group.

- Effective data protection compliance requires coordinated action at all levels of the organisation and alignment with the Group's defined strategic objectives
- To achieve this, Colt clearly identifies the roles and responsibilities involved in managing data protection activities
- This structure operates through a vertically integrated, balanced planning and management system, with a clear hierarchy aligned to each function's decision-making responsibilities

AI GOVERNANCE FRAMEWORK WITH EU AI

Colt has implemented an enterprise-wide AI Governance framework, incorporating EU AI Act principles. AI Governance SteerCo provides oversight.

- Oversight provided by an AI Governance Steering Committee, supported by mandatory AI risk and impact assessments and formal reviews before deployment.
- Controls on full AI lifecycle, including documentation, logging, monitoring, human-in-the-loop safe-guards, vendor due-diligence for AI tools.
- Responsible AI principles embedded throughout, and regulators should view Colt's AI controls as fully integrated with the global privacy governance model and BCR audit perimeter.

COLT DELIVERS SERVICES BETWEEN EUROPEAN SITES WITH LOCAL COUNTRY CONTRACTS

OPERATIONAL SOVEREIGNTY

Network governing platforms located in Europe

Customer metadata residing in Europe

Customer managed encryption keys

Legal contracts in Europe local countries

Service delivery entirely in Europe [optional]

Global teams (eg Ops) operate under Colt BCR

EU Desk to coordinate global ops [optional]

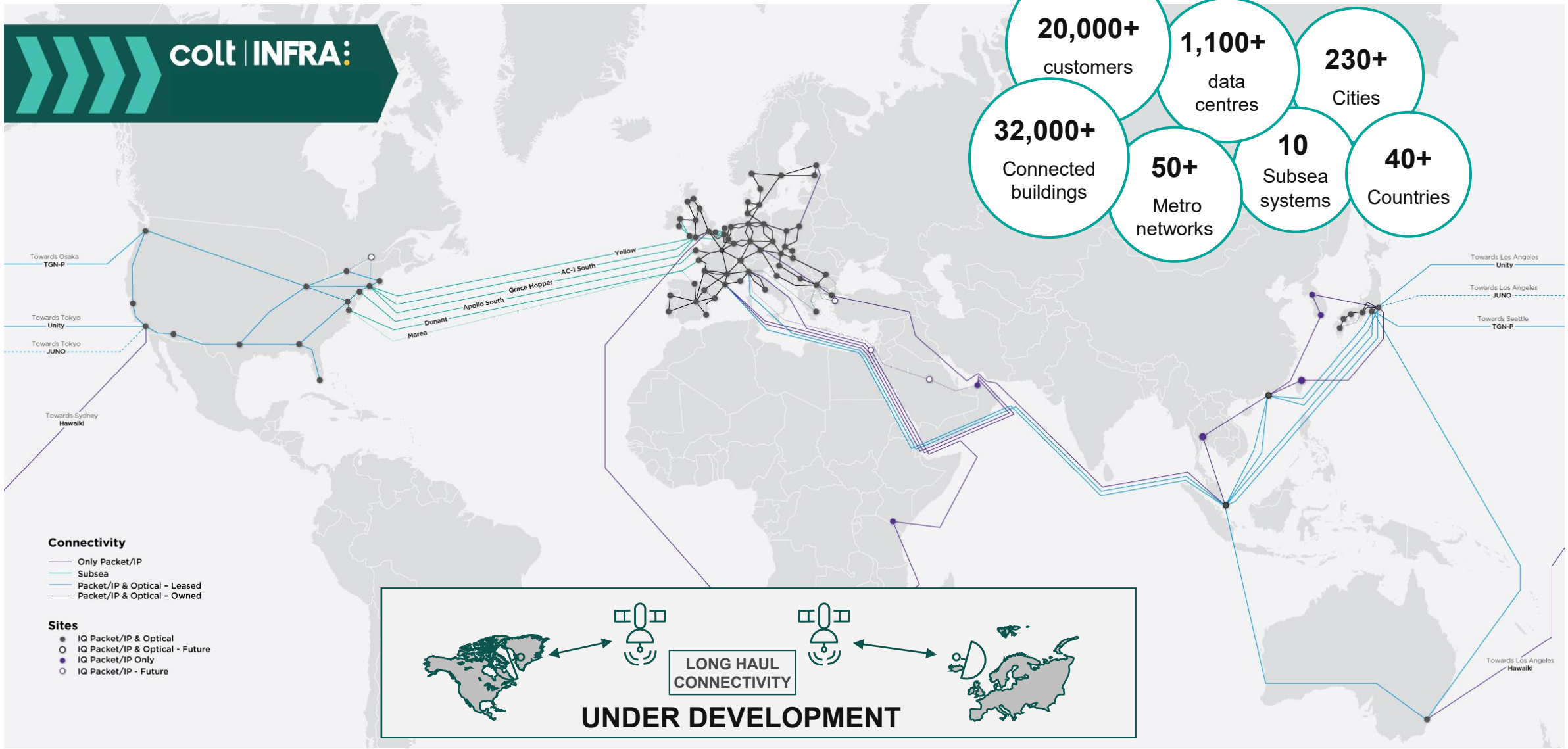
Operational Sovereignty: Control on how the network infrastructure and its governing platforms are operated and who operates them.

TECHNOLOGY & INFRASTRUCTURE SOVEREIGNTY.

ANALYST DAY
2026

SOVEREIGN INTERCONTINENTAL INFRASTRUCTURE

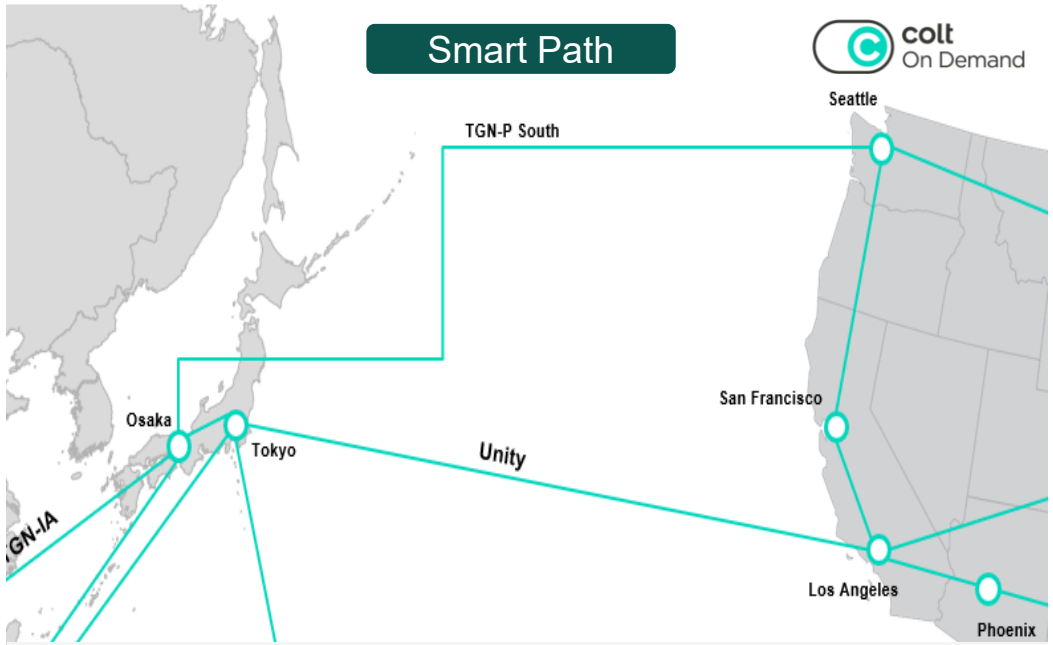
colt



SOVEREIGN WAN INNOVATION – END TO END PATH CONTROL

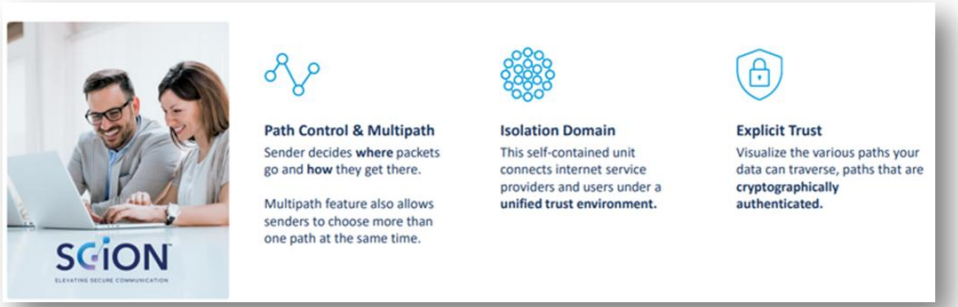
colt

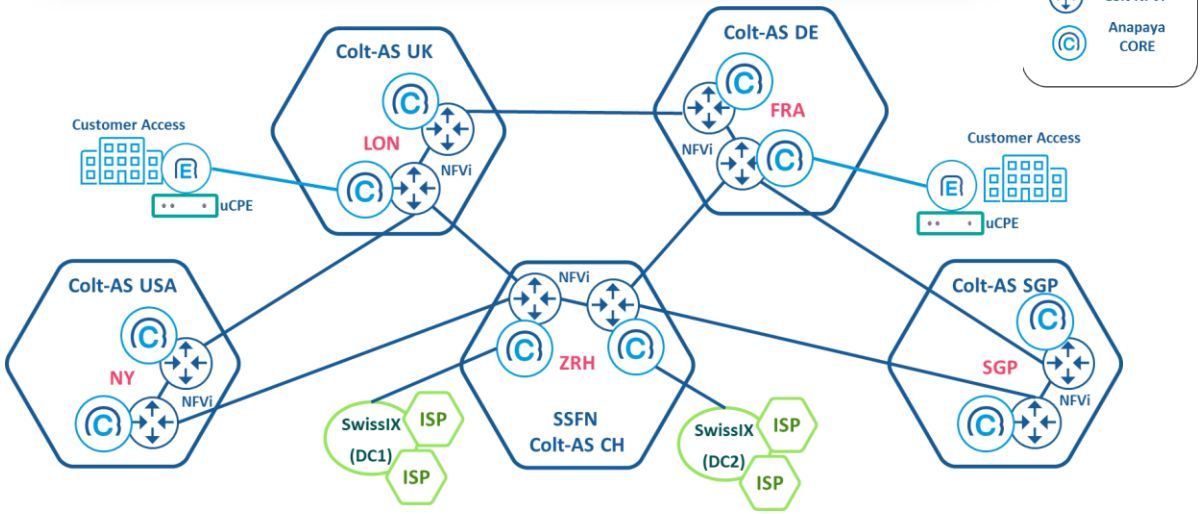
» **Smart Path** enable customers to choose network routes in just a few mouse clicks via our **On Demand NaaS platform (e.g. Sovereign Path)**



Customer chooses "sovereign" route via Smart Path feature. In the event of a failure traffic does not re-route

» **Colt to launch the first global Trusted WAN network** for secure and controllable critical communications in a multi-carrier environment (e.g. SSFN)



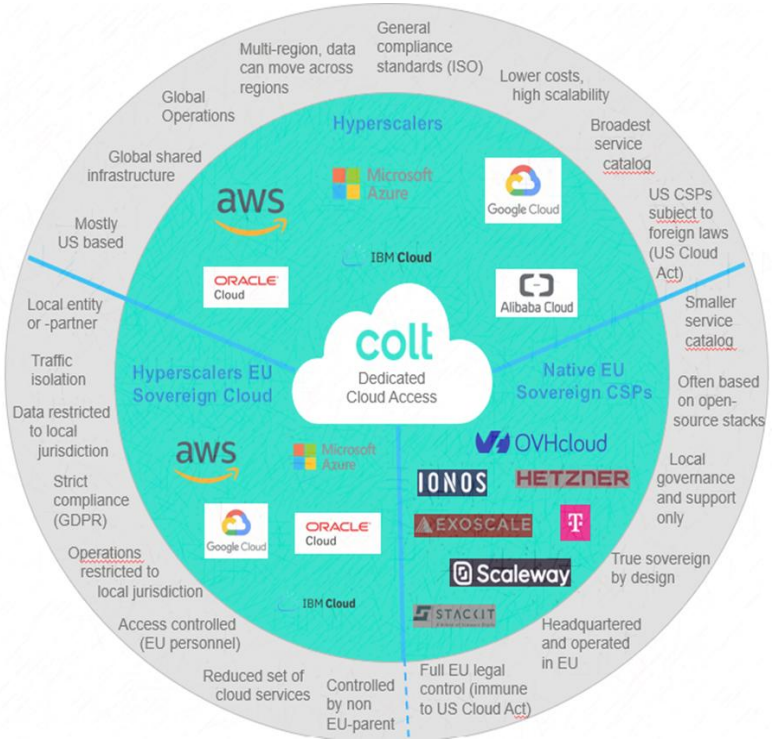


SOVEREIGN WAN INNOVATION – CLOUD ACCESS AND ENCRYPTION

colt

» Colt connects your sites to any **sovereign cloud provider in Europe**, ensuring all traffic remains within approved jurisdictions

» Colt adds **optional encryption** on top of connectivity, using **customer-held keys** and supporting **quantum-safe** options for future-proof protection



Quantum-safe encryption technologies

- **QKD** — Quantum Key Distribution, Quantum Physics
- **PSK** — Pre-Shared Key, Classical Physics
- **PQC** — Post-Quantum Cryptography, Complex Mathematics

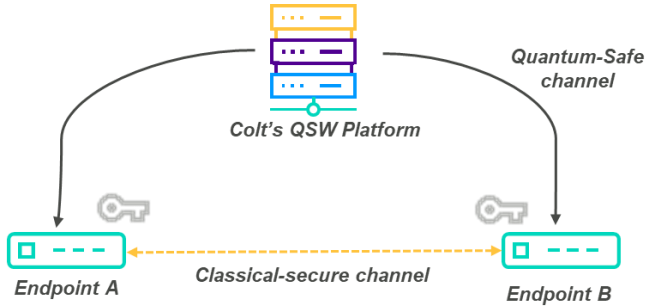
Field trial Partners

NOKIA ciena Adtran

Optical technology partners

IDQ Honeywell TOSHIBA

Quantum technology enablers



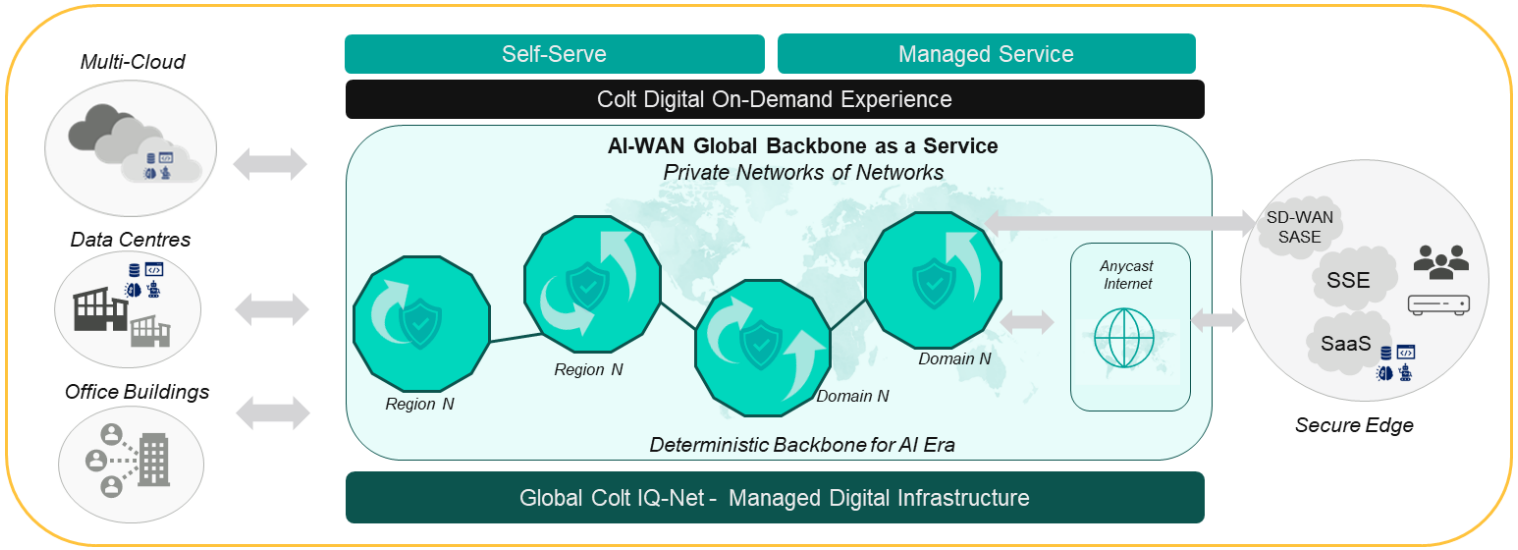
INTRODUCING AI-WAN – UNIFIED BACKBONE FOR THE AI AGE

Smart Network Fabric
An **intent-driven Layer-3** fabric prioritising AI and business-critical applications.

Sovereign Controls
Control where data travels and how it is handled across global jurisdictions.

Built-in Security
Integrated **security protecting AI workloads, applications and the network**, with **post-quantum** readiness.

Global Reach & Connectivity
Native connectivity across **multi-clouds, data centres and sites** at global scale.



Underlay for SASE SD-WAN
A **deterministic underlay** delivering predictable end-to-end performance.

Marketplace-Network/Security Service
Add **new capabilities** and services on demand as needs evolve.

Open Edge Choice
Integrate with existing **SASE/SD-WAN and SSE**– works with partner of choice

Simplified On-Demand Experience
A **rapid** setup, elastic **scaling**, and commercial **flexibility**.

Smart Operations
Self-monitoring and **self-healing operations** with minimal human intervention.

COLT SOVEREIGN OFFERINGS VS NATIONAL COUNTRY-CENTRIC INCUMBENTS

colt

colt	NATIONAL INCUMBENT OPERATORS
» Pan-European coverage with unified compliance	» Focused on national sovereignty only
» Data Protection: the only company with both UK & EU BCR’s	» Limited to domestic backbone
» End-to-end secure, sovereign connectivity across borders	» Fragmented compliance across countries
» Single provider for multi-country sovereignty needs	» Mainly long-distance connectivity via 3rd parties

Q&A
Q&A
Q&A
Q&A

ANALYST DAY
2026

colt | ANALYST DAY 2026

THANK YOU