kyndryl

Perspectives on sovereign cloud

Why organizations are turning to sovereign cloud

Data is the lifeblood of every modern economy and safeguarding it has become more important than ever. Because of this growing need, data protection, digital sovereignty, and data sovereignty are three rising areas of interest for organizations around the world.

Data protection refers to the control and safeguarding of data from unauthorized access. It encompasses sensitive data storage, access, retention, immutability, and security. Protecting data from falling into the wrong hands is paramount to most organizations. Not only do they want to ensure customers can trust their digital interactions, driving needs also include new governance and regulations and the potential embarrassment and financial impacts associated with reporting a data breach.

Since data privacy and protection have become so critical, the terms “digital sovereignty” and “data sovereignty” have gained momentum. Digital sovereignty refers to a country’s ability to exercise control and independence over its digital infrastructure, data, and technology-related policies. It is the concept of ensuring that a nation has the authority and capacity to govern its digital domain without undue influence or control from foreign entities, corporations, or governments. For example, in the United States (US), the CLOUD Act obligates cloud service providers to comply with a subpoena regardless of whether a communication, record, or other information is located in or outside of the US. The information requested can be critical to cyber investigations by authorities around the world.

Data sovereignty is a set of regional data security and residency requirements to control the access and transmission of data. In other words, it is the understanding that data stored outside of an organization’s host country is still subject to the laws in the country where the data is collected. In many cases, governments are passing laws that require businesses to store and transmit data only within their sovereign borders. This effort requires IT systems to control the physical location of the data and restrict access to individuals of specific citizenship or residency. Data sovereignty rules tend to vary by country, political region, and industry. These rules accompany a host of other regulatory or compliance requirements, as shown in the examples on the following page.

- **General Data Protection Regulation:** The European Union (EU) General Data Protection Regulation (GDPR) from 2018 regulates the collection and use of data about EU citizens and enforces security requirements for personal data, regardless of where it is stored.
- **Schrems II:** In July of 2020, the Schrems II decision further restricted personal data transfer from the EU to other countries that do not offer what the EU deemed an adequate level of data protection. This decision was the impetus for the invalidation of the 2016 EU-US Privacy Shield Framework. It also placed specific requirements on personal data stored in the cloud, including physical data storage locations and authorized access. The Schrems II ruling may have been motivated by the fact that the US Intelligence Community had disproportionate access to the data of EU residents without the possibility of judicial redress. Proportionality and judicial remedy are two of the EU's core principles.
- **European Commission adequacy decision:** On July 10, 2023, the European Commission adopted an adequacy decision for the EU-US Data Privacy Framework, which amends the privacy principles organizations adhered to under the EU-US Privacy Shield Framework, stating that the US ensures a level of data protection equivalent to that of the EU.
- **Act on the Protection of Personal Information:** Japan's Act on the Protection of Personal Information requires that organizations, including government agencies, businesses, and nonprofits, obtain an individual's consent before collecting, using, or sharing their personal information. It was originally passed in 2003 but underwent significant revisions in 2017 and 2022.
- **Personal Information Protection law:** China's Personal Information Protection law from 2021 regulates use of personal data by all companies operating in China and requires that personal data must be stored on servers within the country. Indonesia created a similar Personal Data Protection law in 2022.
- **Other country and industry regulations:** India and Malaysia have local regulations requiring consent before transferring personal data across borders. In Australia, data localization regulations apply to electronic health records and other personal data collected by specific industries. Electronic protected health information may be subject to additional data privacy controls, such as the HIPAA healthcare legislation in the US.
- **EU Data Act:** Proposed in February 2022, the EU Data Act aims to create new requirements governing the use of and access to data of connected products and related services. The Data Act invoked data-sharing obligations on private sector companies, which understandably raised concerns about protecting trade secrets and restricting contractual freedom. EU member states reached a common position on the proposed Data Act, enabling negotiations on the final version of the proposed legislation to begin among the Council of the European Union and European Parliament. The EU Data Act will contribute to creating a single market to allow data to flow freely within the EU and across sectors for the benefit of businesses, researchers, public administrations, and society at large. We will see an official announcement from the EU in the next few years.

Important as they are, the global landscape of these data privacy regulations is not uniform, as you can see. Because these regulations comprise a complex patchwork, they can be difficult to navigate. The US, for instance, has hundreds of data privacy laws at the sector level but does not currently have a single, comprehensive federal law in place. Today, only 12 states—California, Colorado, Connecticut, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia—have passed comprehensive data privacy laws or have laws that will take effect on a predetermined date. We expect to see more states and countries pass laws in the next few years.

What is a sovereign cloud?

A sovereign cloud can be public or private. It is a cloud that operates in a particular country or region and meets a governing body's data privacy and jurisdictional standards. With a sovereign cloud, all data and metadata stay on sovereign soil, preventing other nations from accessing it. Sovereign clouds offer enhanced security measures, including encryption, access controls, zero trust, and network segmentation, which may be tailored to specific countries or regions.

Because data privacy and protection and digital and data sovereignty have become so critical, sovereign clouds are growing increasingly popular. According to IDC, 62% of customers state they need a cloud option that provides data sovereignty with complete jurisdictional control and authority over data.

A sovereign cloud introduces a new architectural approach toward addressing data and national independence concerns, enabling countries and organizations to be digitally self-sufficient.

Sovereign cloud drivers

In addition to the data privacy and security, digital sovereignty, and jurisdictional controls discussed above, geopolitical changes are also driving the demand for sovereign clouds. To be able to quickly comply with changes in local laws, it's imperative for organizations to stay abreast of geopolitical factors like growing trade disputes or friction between traditional allies, which have the potential to change policies and economies.

Sovereign clouds are implemented in multiple ways. Some enterprises choose private, on-premises sovereign clouds while others opt for public or regional clouds with additional security, compliance, and operational controls.

Data security and privacy

Geopolitical changes

Digital sovereignty

Jurisdictional controls

Figure 1: Sovereign cloud drivers

Why is data sovereignty important?

For businesses and organizations, protecting the personal and confidential information of employees and customers is critical. Failing to protect this data can result in lawsuits and government fines. GDPR and other privacy laws give people the right to seek compensation if they have suffered damages based on an organization not adhering to the law. Non-compliance with GDPR could also result in a fine of up to EUR €20 million or 4% of a company's total annual worldwide gross revenue. 12 of the biggest data fines and settlements to date financially impacted the affected companies with costs upwards of USD $4 billion.

Recent geopolitical tensions have spurred even more laws to tighten data security and limit data flow across borders. Cybercrime and cyber warfare have further heightened the urgency for businesses to put data sovereignty at the forefront of their cloud strategies.

Global interest in sovereign cloud

It is estimated that the sovereign cloud total addressable market will reach USD $60 billion by 2025, due to the rapid increase of data privacy laws around the world. According to the World Population Review, more than 120 countries have adopted international data privacy laws that regulate the movement of data, including how it is collected, how people are informed about the purpose of the data collection, and what rights a person has over their information once it is transferred. An IDC study states that 88% of large organizations say data sovereignty is very or extremely important, with 40% anticipating an increase in their sovereign solution investments over the next two years. This number rises to 53% over a longer term of three to five years. Data sovereignty is often cited as one of the most important factors driving cloud repatriation—the practice of migrating applications or workloads away from public clouds and moving them elsewhere, in many cases to a private cloud.

The key industries adopting sovereign clouds are financial services, healthcare, manufacturing, and public sector. While governments around the world are focusing on sovereign cloud initiatives, the EU is leading the charge.

Local cloud service providers

Local cloud service providers (CSPs) play a pivotal role in realizing the sovereign cloud vision. By establishing data centers within a nation's borders and being resident business entities, they help ensure data sovereignty, security, and compliance with local regulations. With an in-depth understanding of the domestic landscape, local CSPs offer tailored services to meet the unique needs of businesses and government entities, fostering digital autonomy while enhancing data protection. The partnership between local CSPs and national stakeholders helps drive the evolution of a secure, self-reliant digital ecosystem for the countries.

However, local CSPs face a challenge. Because they lack economies of scale, their costs can be higher, and it becomes more difficult to deliver expert technical services and experience on par with leading public cloud providers in the market.

For local CSPs, the implementation of the EU Data Act could open the broader EU market beyond their country of origin, allowing them to scale operations to other EU countries. This shift would allow data to flow freely within the EU and across sectors for the benefit of businesses, researchers, public administrations, and society at large.

Global cloud service providers

Public cloud giants like Amazon Web Services, Microsoft Azure, and Google Cloud, with extensive infrastructure and global reach, enable governments and enterprises to establish localized, security-rich cloud environments while benefiting from economies of scale. These players offer the technological prowess and expertise required to create resilient and compliant sovereign cloud solutions. By partnering with public cloud leaders, nations can harness cutting-edge innovations to fortify their digital sovereignty and enhance data-management capabilities, thereby shaping a more secure and independent digital future

Many public CSPs have entered partnerships with local CSPs to allay government concerns about digital sovereignty and their high dependence on US companies for new-age technologies.

Private cloud service providers

There is a clear need for sovereign cloud solutions that have stronger security and adherence to local regulations; local CSPs are challenged by higher costs while larger public cloud players must overcome the foreign-owned label. It is imperative for organizations to look at private sovereign cloud solutions. Private sovereign cloud solutions can provide the required security, resiliency, scalability, ownership, and control while also controlling costs. In many cases, businesses may find it more efficient to adopt and implement a sovereign cloud framework on their existing infrastructure.

When it comes to sovereign cloud solutions, a universal approach is not feasible. It's essential that an organization's sovereign cloud strategy aligns with the overarching cloud strategy. Moreover, an integrated service delivery and management approach is crucial, because a sovereign cloud solution is likely to function as a specific component within the organization's larger IT estate.

Key business benefits

The benefits of adopting a sovereign cloud may vary based on an organization's specific country, cloud provider, individual needs, and regulatory requirements. Benefits include compliance with regulations and enhanced security but also extend to less-obvious outcomes like reduced latency.

- **Data residency and compliance:** These factors are particularly important for organizations handling sensitive or regulated data that must comply with specific data-protection and privacy laws.
- **Enhanced security and control:** By using cloud services that are managed and operated within their own country or region, organizations may have more confidence in data-protection mechanisms and regulatory compliance.
- **Mitigation of legal risks:** Adopting a sovereign cloud can help organizations minimize legal risks associated with the data access and surveillance laws of other countries. Storing sensitive data locally may help protect it from foreign government data access requests.
- **Reduced latency:** Locating cloud services closer to the end users or critical infrastructure can reduce data transfer latencies, resulting in better performance for applications and services.
- **Customization and tailored services:** Sovereign cloud providers may offer services and solutions tailored to specific industries or national requirements, which can be advantageous for organizations with specific needs.

In addition, sovereign clouds can serve a national economic benefit: governments often promote the use of sovereign clouds to support local technology companies, drive economic growth, and create jobs within their own borders.

The Kyndryl vision and value

Kyndryl's services for sovereign cloud are designed on the core principles of data sovereignty, localized data residency, digital sovereignty, and operational sovereignty. Our focus lies in helping our customers uphold stringent security protocols, adhere to local compliance standards, and deliver cost efficiency.

Our integrated approach flexibly caters to the unique requirements dictated by an organization's operational locale and can be customized for any local regulatory requirements.

An expansive global footprint ensures in-country delivery across numerous operational regions.

Deep collaboration with local CSPs and prominent security and cloud software figures allows us to seamlessly curate solutions that align with an organization's requirements while maintaining a cost-effective approach.

Through Kyndryl Consult, we can assist organizations in their adoption of sovereign cloud solutions with rapid assessments and deep expertise in infrastructure, security, network, and data management solutions.

The Kyndryl solution

Kyndryl sovereign cloud services provide an architectural and operational framework to help our customers implement sovereign cloud attributes, including the assessment, build, and management of on-premises private cloud infrastructures. The framework includes in-depth, layered security principles, such as data localization, zero trust, encryption, converged identity controls, and endpoint security—all delivered through a modular approach by trained and certified security professionals. With Kyndryl sovereign cloud services deployment, data remains subject to the jurisdictional control and authority of the governmental bodies within sovereign borders, and the complete ownership of the data and metadata lies with the business.

Bringing together multiple Kyndryl practices—Kyndryl Private Cloud, Kyndryl Security and Resiliency, and Kyndryl Network and Edge—along with Kyndryl Consult, we deliver sovereign cloud offerings and services through advanced technologies, methods, skills, and governance.

Kyndryl's depth of service offerings can help our customers through all the steps of the sovereign cloud journey, from feasibility and cost analyses to design and implementation to a full set of management services.

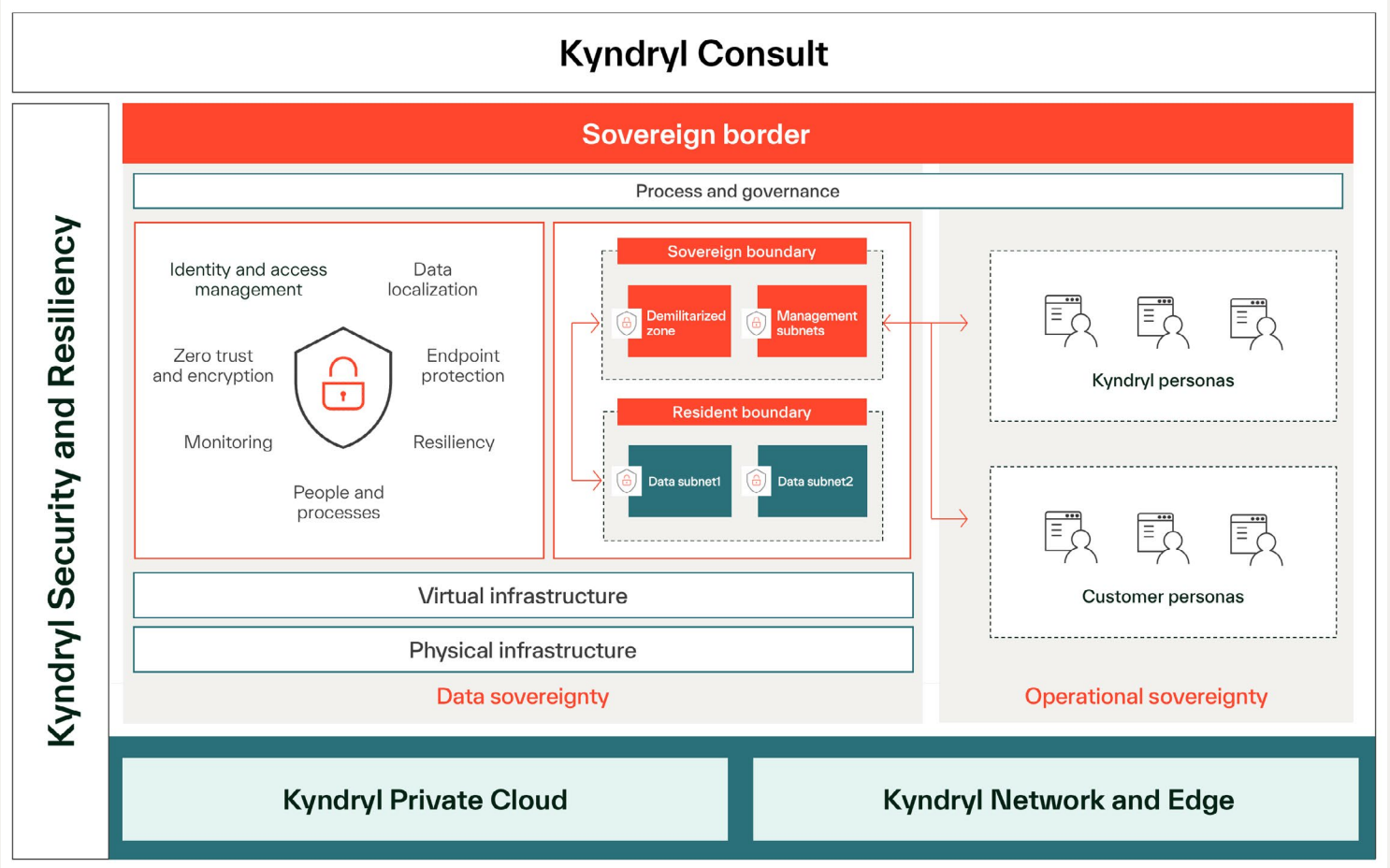

Figure 2: Kyndryl sovereign cloud services high-level architecture

The sovereign cloud journey starts with Kyndryl Consult. Our team will analyze the required local data privacy and protection regulations, the current environment, and all the organization's specific requirements to formulate a high-level solution design. Along with the solution design, our customers receive a cost analysis that includes implementation, migration, and operational costs, as well as the total cost of ownership.

From there, the Kyndryl Consult team can provide services to help build a sovereign cloud infrastructure on-premises or with a local infrastructure provider. Finally, the Kyndryl Managed Services team can step in to manage and operate the sovereign cloud with the highest standards required to meet the necessary service-level objectives and agreements.

Our approach leverages a set of assets based on our years of experience in designing and managing customers' mission-critical environments around the world. These assets provide cost analysis, design, and architectural decision templates for specific sovereign cloud solutions that can be customized to address very specific customer requirements during the consulting or design phase.

Prescriptive reference design artifacts, implementation guides, automations, and operational runbooks help us design, implement, and manage a quality-proven and cost-effective sovereign cloud solution customized for an organization's specific needs.

Consulting services

Advisory
- Advisory services
- Business case

Assessment
- Sovereign cloud adoption readiness assessments

Strategy
- Strategy and architecture

Migration
- Migration to sovereign cloud

Design and build services

Infrastructure
- On-premises sovereign private cloud

Security and Resiliency
- Data-at-rest/in-transit encryption
- Key management system
- Endpoint security
- Identity and access management
- Threat detection and intrusion prevention
- Backup and disaster recovery

Network and Edge
- Microsegmentation and data-classified network segments
- Firewall rules and validation

Manage services

Infrastructure
- Management of sovereign private cloud infrastructure and hosted workloads
- Service integration and management
- Deployment and management of data and operational sovereignty

Security and Resiliency
- Management of security and resilience components

Network and Edge
- Management of network components

Governance, risk management, and compliance

Figure 3: Kyndryl sovereign cloud services capabilities

Kyndryl can help create a sovereign cloud for four major scenarios:

01

Company sovereign cloud: Build and manage a sovereign private cloud exclusively dedicated to a specific company—for example, banks, insurance companies, and healthcare organizations operating with extremely sensitive data.

02

Multi-tenant sovereign cloud: Build a multi-tenant sovereign private cloud, hosting data and applications from multiple customers and companies on a shared in-country infrastructure, with management services to come at a later stage.

03

Government sovereign cloud: Build a sovereign private cloud, hosting sensitive or classified data and applications from one or multiple government agencies running on a dedicated infrastructure or as isolated tenants on the same infrastructure, with management services to come at a later stage.

04

Sovereign disaster recovery cloud: Build and manage a sovereign private cloud that can be used to recover sensitive data and applications from government entities or regulated companies in case of a catastrophic event.

Key sovereign cloud elements

- A complete software-defined data center infrastructure stack set up in highly available data centers within an operating region
- An autonomous legal entity with jurisdictional sovereignty that owns the infrastructure and operations personnel
- Prescriptive security and resiliency controls to ensure infrastructure, data, and workload protection as per the sovereign cloud requirements
- Continuous compliance enforcement for the required country-specific and/or industry-specific regulations
- Data sovereignty and data integrity
- A flexible architecture to avoid vendor lock-in
- Comprehensive, publicly available guidance and documentation

The Kyndryl approach to implementing a sovereign cloud based on the above elements starts with the consolidated consult, design, build, and manage service offerings for a private cloud. Based on the required country regulations, this approach adds specific security and resiliency controls and policies for data storage, encryption, transmission, zero trust, and more, as required by a sovereign cloud solution.

Kyndryl offerings for building and managing private clouds allow us to set up private cloud hardware infrastructure on a customer's premises, in a highly available service provider, or a co-located environment within the country boundaries and owned by legal entities within the country—all based on an operating-expense model for infrastructure consumption.

Kyndryl Private Cloud services provide maximum flexibility, allowing our customers to choose from multiple hyperconverged infrastructure, enterprise storage, and infrastructure virtualization technology providers, such as VMware, Red Hat, Nutanix, and Microsoft.

On top of that flexibility, Kyndryl can also layer containerization platforms through a self-service portal powered by development, security operations, and automated workflows.

Kyndryl management services for private cloud provide monitoring, operations, and management of infrastructure, data, and applications, using personnel from autonomous in-country Kyndryl subsidiaries and based on years of experience outsourcing and managing these assets for thousands of customers around the world.

While Kyndryl's build and manage services for private cloud already implement a strong security posture, there are stringent sovereign cloud requirements with specific technology needs that call for a highly specialized team.

To implement these specialized sovereign requirements, we use a suite of security offerings that augment the standard private cloud elements.

- Data classification, encryption, protection, and access restriction at various levels
- Advanced identity management controls based on multiple techniques, such as multifactor authentication, single sign-on, role-based access control, biometrics, and geolocation
- Zero trust and network perimeter protection services
- Security and compliance monitoring and enforcement based on the requested country-specific and industry-specific regulations
- Cyber resilience embedded into operational processes to prevent data leakage and unauthorized data access and to anticipate, protect, and recover from adverse cybersecurity attacks

However, when we're talking about critical or sensitive data, security is not enough. The Kyndryl resiliency offering provides build and manage resiliency services to help:

- Back up and restore critical data in redundant copies in multiple data centers to protect and recover data in the event of a ransomware attack
- Implement a disaster recovery solution for critical data, leveraging Kyndryl IP automation and orchestration tools to minimize recovery point objective (RPO) and recovery time objective (RTO)

Finally, Kyndryl can help businesses with migration and modernization services to move applications across heterogeneous private, public, and sovereign clouds as needed to avoid vendor lock-in.

Why Kyndryl?

When you choose Kyndryl, you unlock the strength, experience, expertise, and reliability of a recognized global IT security and privacy leader. Trust is foundational to all we do, and we are committed to protecting the privacy and confidentiality of your personal information. See our Kyndryl Data Privacy Principles to read about our underlying security beliefs.

With our deep engineering roots and thousands of skilled professionals, Kyndryl has risen to be the world's largest IT infrastructure provider. Our global base of customers includes 60% of Fortune 100 companies. With thousands of skilled professionals globally, we are committed to the success of our customers and the health and continuous improvement of their vital systems. With our partners and customers, we co-create solutions to help enterprises reach their peak digital performance.

Kyndryl can simplify your adoption of sovereign cloud. Our Kyndryl Consult team can help you design and build your sovereign cloud strategy through a modular, scalable, vendor-neutral approach. We can even help you rework your existing infrastructure to operate in a sovereign environment.

Through strategic consulting and services capabilities, we'll empower you to choose the right cost-optimized sovereign cloud solutions and design successful modern architectures.

For more information

To learn more about Kyndryl sovereign cloud services or to request an engagement, reach out to our Kyndryl Consult team.

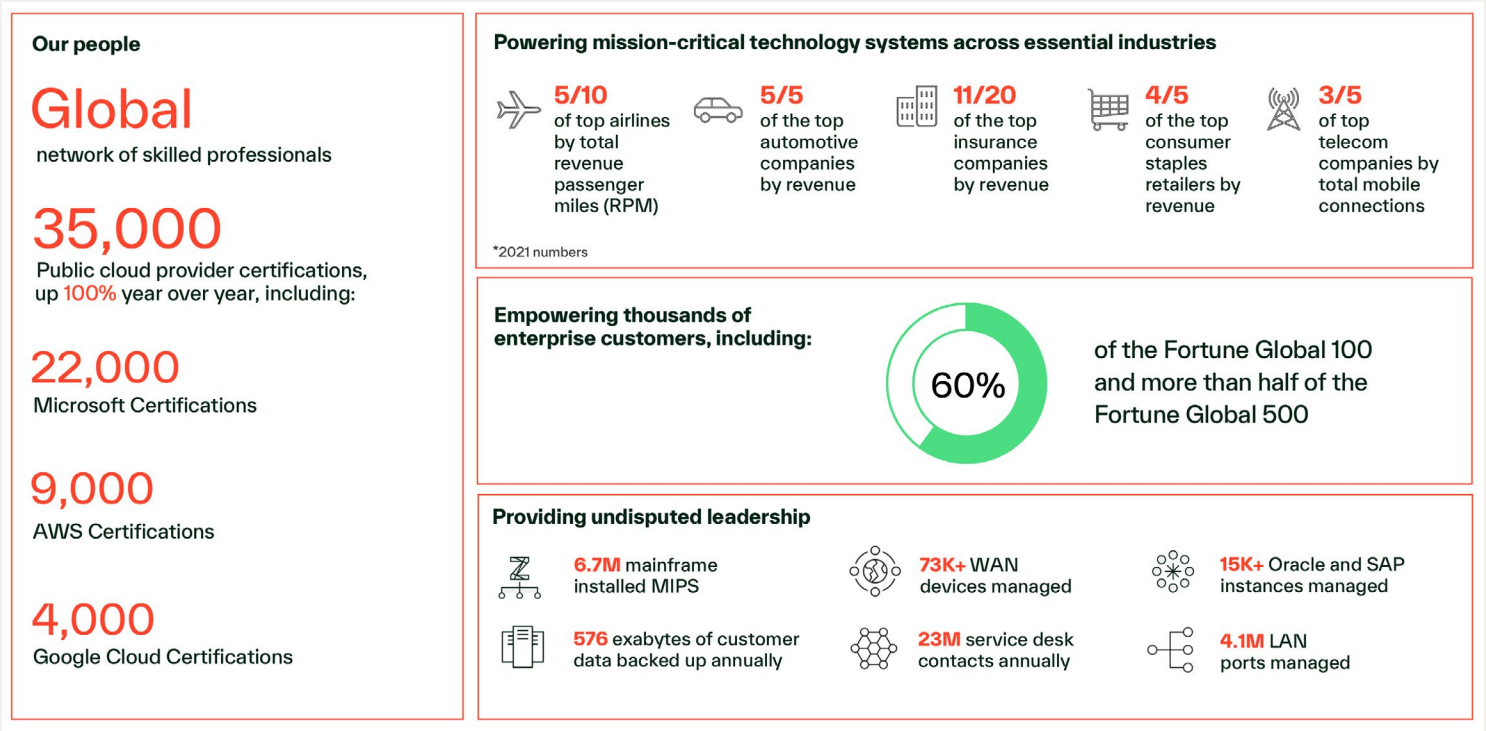

Figure 4: Kyndryl at a glance

kyndryl