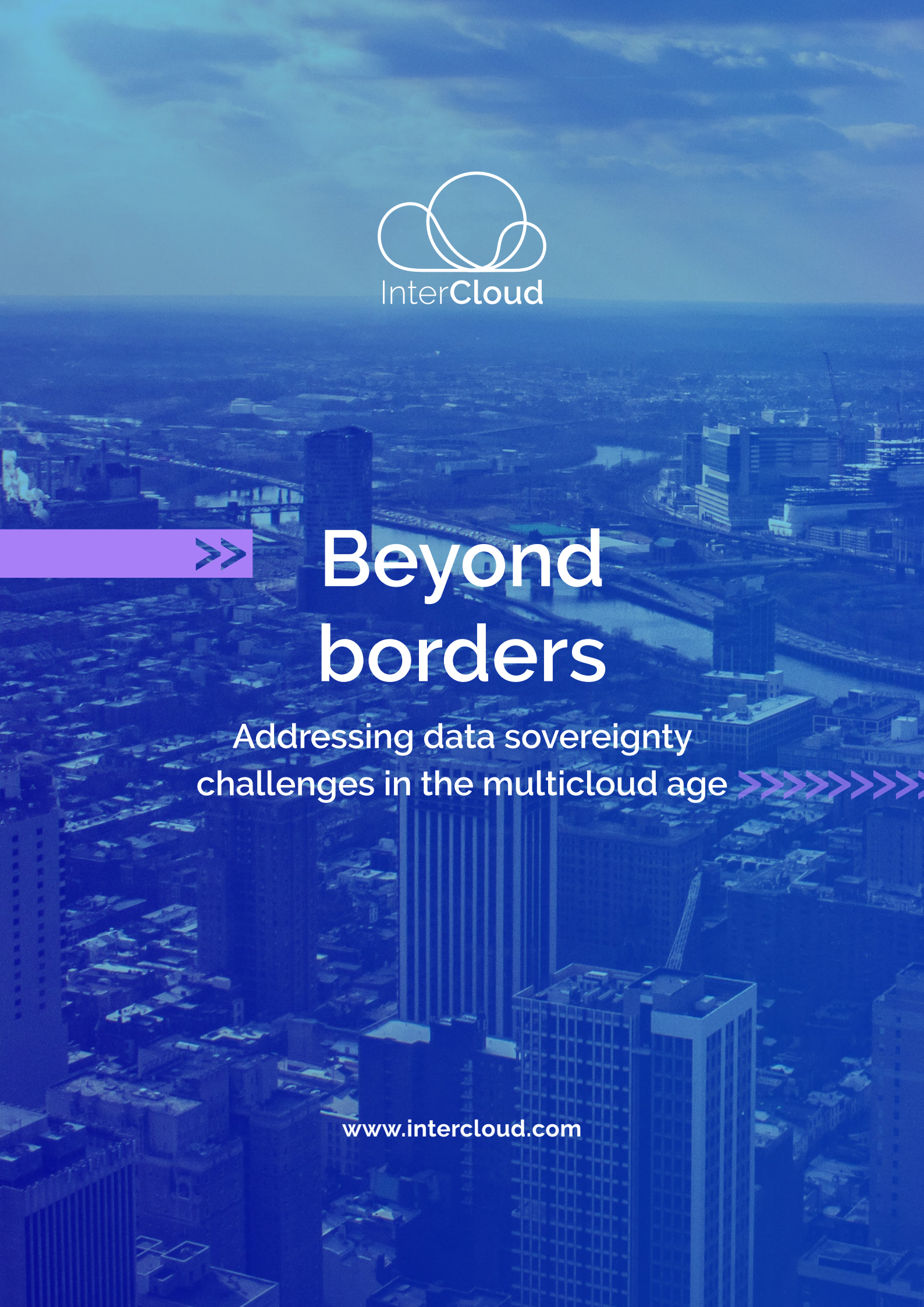
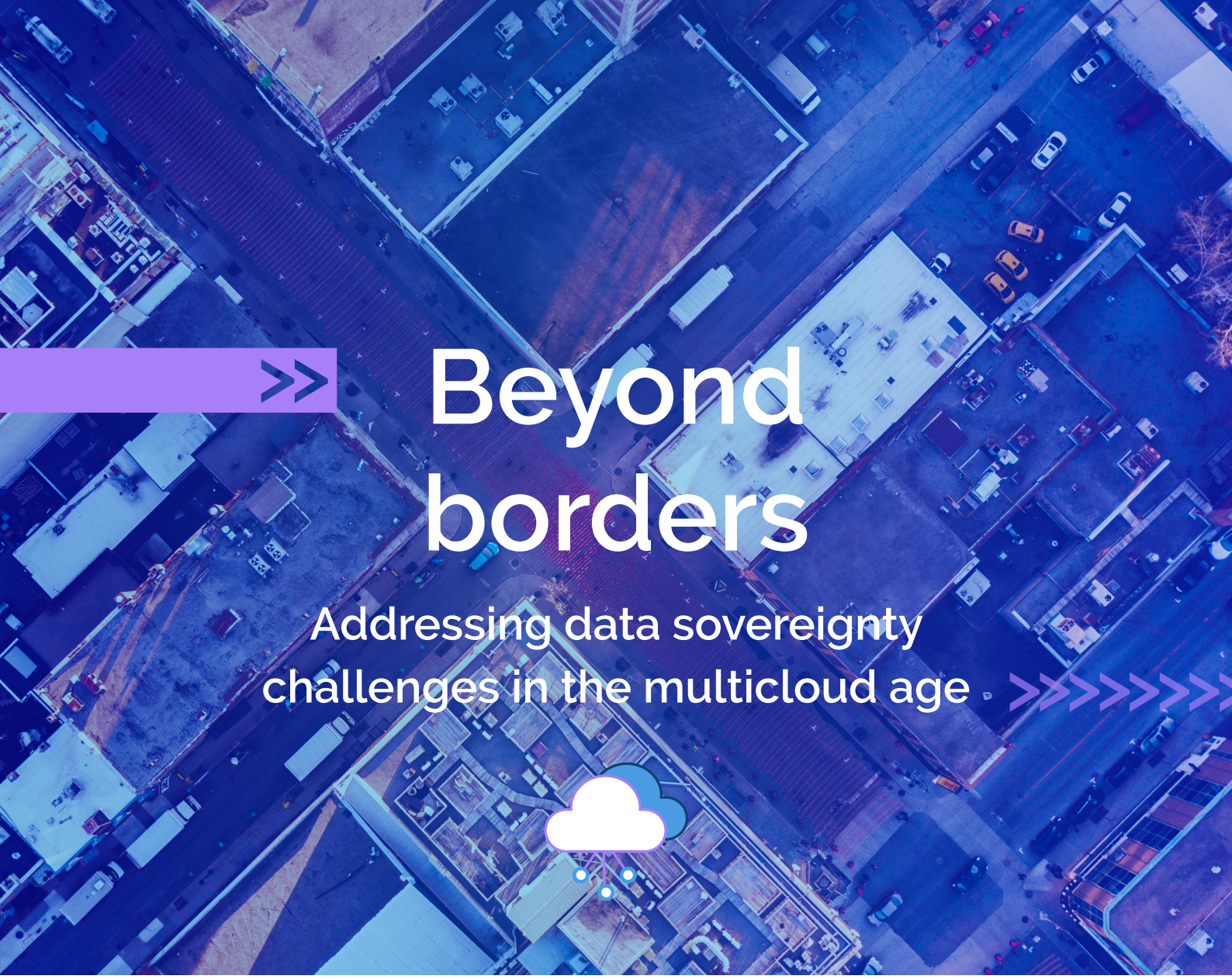

InterCloud
Beyond borders
Addressing data sovereignty challenges in the multicloud age
www.intercloud.com



Beyond borders

Addressing data sovereignty challenges in the multicloud age

Executive summary

By most current counts, there are more than 130 countries[1] with national data sovereignty laws. If your business is operating in any of these countries — or your company does business in a country with data sovereignty laws — data sovereignty should concern you.

Data sovereignty laws aren't purely a result of cloud computing, but the cloud has forced data sovereignty to center stage as its dispersed nature has broken down many of the traditional geopolitical barriers limiting the transfer of data across borders. The transformation to multicloud — where enterprises rely on not just one cloud service provider but potentially many — provides benefits to enterprises but also serves to increase the risk that data could extend — knowingly or not — into different regions with different data sovereignty laws.

Put simply, the challenge with the cloud model, particularly multitenant deployments, is that you, as a cloud service provider customer, don't know or control where your data is ultimately being stored or where replicated copies of the data are being pushed to. You could be breaking your data sovereignty and privacy obligations without even knowing it.

This InterCloud white paper identifies critical issues, discusses current solutions, and explains why a centralized approach to cloud connectivity management can effectively tackle data sovereignty challenges while ensuring seamless and secure operations in multicloud environments.

1. UNCTAD | Data Protection and Privacy Legislation Worldwide | 2023

The data sovereignty challenge

"Digital sovereignty will be a primary source of complex, dynamic and expanding compliance obligations for multinational enterprises." - Gartner [2]

The convergence of regulatory compliance and data protection laws has ushered in stricter requirements for cross-border data transfers. Navigating this intricate web of regulations becomes crucial for organizations seeking to ensure compliance and safeguard sensitive data. Additionally, the concept of data residency has gained prominence as enterprises strive to establish geographically distributed data centers to meet legal obligations and cater to the unique needs of local customers.

Moreover, customer expectations surrounding data privacy and security have evolved significantly. Modern consumers now demand increased transparency, control, and protection of their personal information. Consequently, organizations must exhibit unwavering commitment to safeguarding customer data, thereby introducing an additional layer of complexity to data sovereignty considerations.

In tandem with these developments, the accelerated adoption of cloud services as part of digital transformation initiatives has introduced new complexities. Enterprises are increasingly reliant on multicloud environments, leveraging services from multiple cloud providers to attain scalability, agility, and cost efficiencies. However, effectively managing data sovereignty in such intricate environments poses significant challenges.

Global enterprises encounter several business challenges when confronted with addressing data sovereignty within the realm of multicloud connectivity.

Data compliance across borders

The primary challenge lies in ensuring compliance with data protection and privacy regulations across multiple jurisdictions, a complex task in itself. Organizations must skillfully navigate a labyrinth of legal requirements, encompassing data localization directives, consent mechanisms, and frameworks facilitating lawful data transfers.

2. Gartner | What forces are driving digital geopolitics and where CIOs should focus | 28th February 2022

Ensuring data availability across multiple clouds

Data replication and synchronization across disparate multicloud environments present another challenge. Maintaining high levels of data availability and resilience becomes critical in geographically distributed environments to ensure uninterrupted operations and protect against data loss.

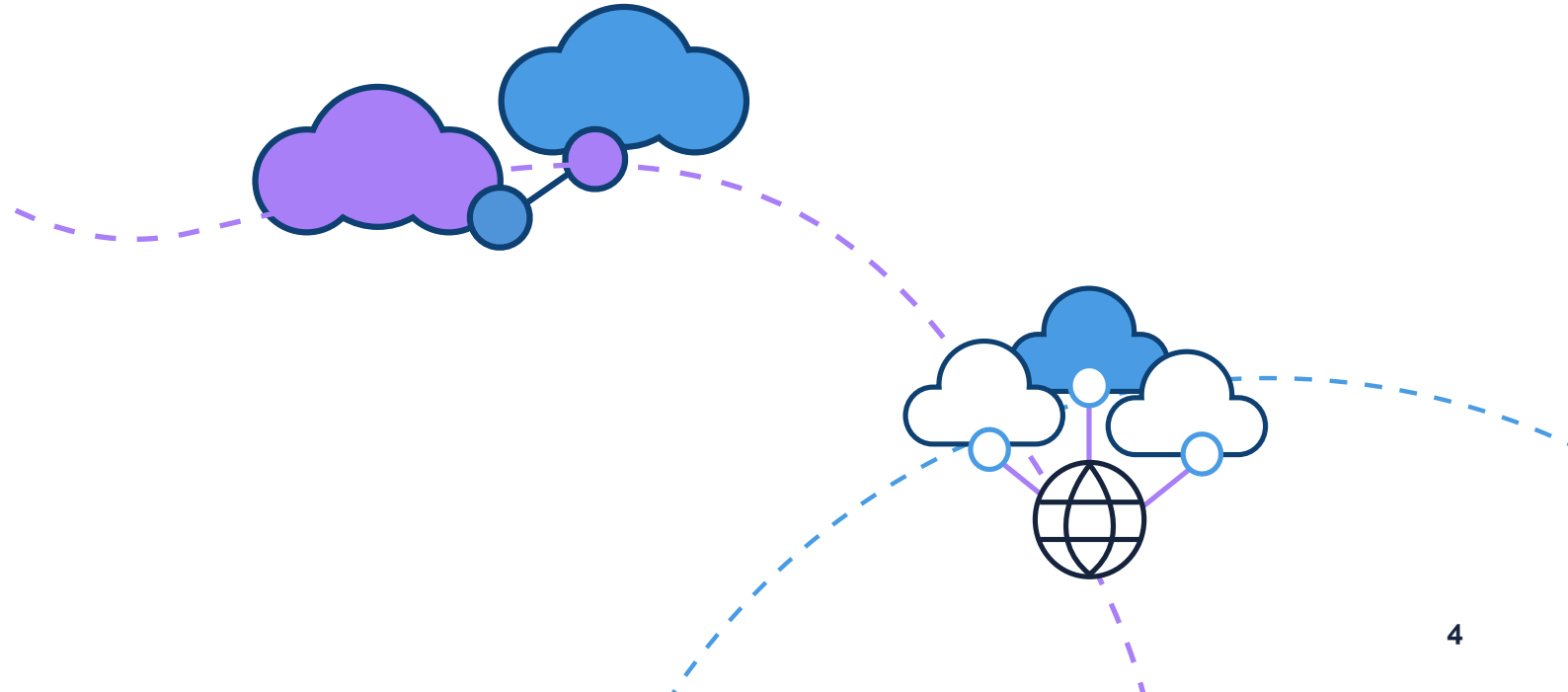
Complexities of inter-cloud connectivity

The complexities of network connectivity and inter-cloud communication add further obstacles. Organizations must establish reliable and secure connections between different cloud environments while addressing latency, bandwidth, and performance requirements.

Protecting data within a globalized landscape

Security concerns are paramount in data sovereignty considerations. Protecting sensitive data in transit and at rest requires robust security measures. Enterprises must address threats such as unauthorized access, interception, and data breaches to maintain sovereignty and protect customer trust.

These challenges highlight the need for a comprehensive and managed approach to cloud connectivity that specifically addresses data sovereignty concerns. Traditional cloud connectivity approaches fall short in meeting these requirements, necessitating a shift towards centralized managed connectivity solutions.



Challenges and limitations of traditional cloud connectivity approaches

Traditional cloud connectivity approaches, such as using the public internet, VPNs, dedicated network connections, or hybrid cloud connectivity, often struggle to effectively address data sovereignty concerns. Here are some of the key challenges and limitations:

Lack of data localization and control

Traditional approaches may not provide the level of control and localization required to address data sovereignty concerns. Without the ability to deploy cloud infrastructure in specific geographic regions or data centers, organizations may find it challenging to comply with regulations and keep sensitive data within desired boundaries.

Limited security and connectivity options

Traditional cloud connectivity approaches might not offer robust security features or dedicated connections needed to ensure secure and private communication. This limitation can result in potential data exposure or interception, undermining efforts to maintain data sovereignty.

Inflexibility and scalability challenges

Traditional approaches may lack the flexibility to scale and adapt to changing data sovereignty requirements. Without the ability to easily expand or contract cloud footprints across different regions, organizations may find it difficult to align their network infrastructure with evolving compliance needs.

Inadequate compliance tools and auditing capabilities

Compliance and auditing requirements play a crucial role in data sovereignty. Traditional cloud connectivity approaches may not provide the necessary tools and capabilities to monitor, track, and demonstrate compliance with data sovereignty regulations. This limitation can hinder organizations' ability to meet the legal and regulatory obligations of their specific geographic locations.

Limited integration with cloud providers

Traditional cloud connectivity approaches may be tied to specific cloud providers, making it challenging to integrate multiple cloud environments seamlessly. This lack of neutrality restricts organizations from fully leveraging the benefits of a multicloud strategy and hampers their ability to maintain data sovereignty across different cloud platforms.

These challenges highlight the need for a centralized managed connectivity solution that specifically addresses data sovereignty concerns in a comprehensive and efficient manner.

The benefits of a centralized managed connectivity approach

A centralized managed connectivity approach that delivers end to end managed serviced offers several key benefits when it comes to addressing data sovereignty concerns:

Enhanced data control

With a centralized managed connectivity approach, organizations have better control over their data. They can ensure that data remains within specific legal boundaries and meets data residency requirements. This level of control allows businesses to comply with regulations and maintain control over how and where traffic moves across the network, reducing the risk of unauthorized access or data breaches.

Compliance management

Data sovereignty often involves compliance with complex regulatory frameworks and regional data privacy laws. A centralized managed connectivity approach provides tools and capabilities to help organizations manage compliance effectively. It enables businesses to track and audit data flows, monitor access controls, and ensure that data is handled in accordance with relevant regulations. This helps organizations avoid penalties and maintain trust with their customers.

Geographic flexibility

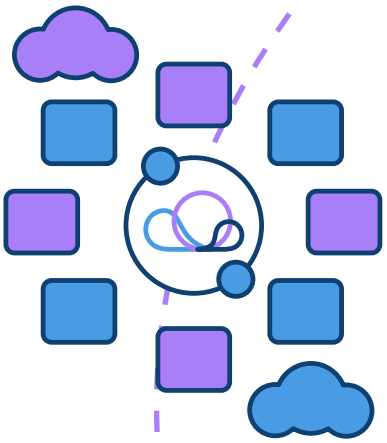
A centralized managed connectivity approach offers geographic flexibility, allowing organizations to choose the location of their data centers or cloud providers strategically. This flexibility enables businesses to align their data storage and processing with specific jurisdictions, ensuring compliance with local data protection laws. By having control over the connectivity paths, organizations can navigate the complexities of data sovereignty and tailor their approach to different regions.

Secure and encrypted connectivity

Managed connectivity solutions prioritize security and encryption to protect data in transit. These solutions establish secure tunnels and encrypted connections, ensuring the confidentiality and integrity of data as it moves between different locations or cloud environments. By leveraging robust security measures, organizations can mitigate the risks associated with unauthorized access or interception, reinforcing data sovereignty requirements.

Seamless integration with multiple cloud providers

A centralized managed connectivity approach facilitates seamless integration with multiple cloud providers. It enables organizations to choose and integrate different cloud services while maintaining a consistent security posture. This flexibility empowers businesses to select the most suitable cloud providers based on their data sovereignty requirements and specific needs. By streamlining the connectivity between multiple clouds, organizations can achieve a cohesive and efficient multicloud strategy while ensuring data sovereignty compliance.



The InterCloud approach

In today's multicloud landscape, enterprises face a paramount challenge of ensuring data security and sovereignty as they navigate a complex network of cloud services. To address this challenge, organizations require a robust solution that delivers end to end managed connectivity services that not only tackle security concerns but also bring support and expertise to align with regulatory obligations.

With its focus on security, sovereignty, and the advantages of neutrality, agility, and simplicity, InterCloud's centralized managed cloud connectivity platform offers a compelling solution for organizations seeking to tackle data sovereignty challenges in the cloud.

Managed services and SDCI platform

By enabling third-party providers to adopt enterprise security policies and offering a centralized control layer, InterCloud empowers businesses to confront the growing threats head-on. With the ability to segment traffic and ensure robust network security, it delivers enhanced security measures that meet the escalating demand. Moreover, InterCloud recognizes the significance of data sovereignty compliance across global operations and allows traffic segmentation based on an organization's specific business requirements, ensuring adherence to sovereignty regulations. With specialized expertise in impacted regions and a steadfast commitment to meeting data sovereignty requirements, it becomes the ideal choice for enterprises seeking to conquer the data sovereignty challenges in a multicloud world effectively.

Benefits

Neutrality:
InterCloud's solution offers neutrality in terms of connectivity, allowing customers to benefit from the best connectivity route rather than being limited to one underlay option. Traditional telco organizations usually provide their own infrastructure, which can lead to vendor lock-in. InterCloud's neutrality provides flexibility and avoids dependency on a single provider.

Agility:
InterCloud recognizes that connectivity requirements vary across global operations. Their unique ability to provide custom connectors to specific cloud providers and deliver the first mile connection to customer premises allows for enhanced agility. This capability is essential for large enterprises that need to outsource end-to-end cloud connectivity effectively.

Simplicity:
Many enterprises prioritize certainty and surety when it comes to connectivity. InterCloud offers an end-to-end Service Level Agreement (SLA) where they take care of data from the customer premises to the clouds. This managed service approach provides peace of mind to customers, eliminating the need for them to have a specific view on how connectivity should be delivered.

Conclusion

While its benefits have been innumerable for IT deployments, the cloud itself poses data sovereignty issues due to the dispersed nature of its infrastructure. If organizations aren't careful, their cloud deployments could extend into different regions with different data sovereignty laws. On the other hand, complying with certain data sovereignty strictures may limit their choices when it comes to the cloud services they make available.

Traditional cloud connectivity approaches often fall short in addressing data sovereignty concerns, lacking data localization, security options, scalability, and compliance tools. In contrast, a centralized managed connectivity approach offers several benefits, including enhanced data control, compliance management, geographic flexibility, secure connectivity, and seamless integration with multiple cloud providers.

With its focus on security, sovereignty, and the advantages of neutrality, agility, and simplicity, InterCloud's approach offers a compelling managed connectivity solution for organizations seeking to tackle data sovereignty challenges in the cloud.

To take action and learn more about how InterCloud can help address data sovereignty challenges in your organization, contact us today to discover how InterCloud can empower your organization to overcome data sovereignty challenges and leverage the benefits of the cloud with confidence.

Together, we can navigate the complexities of data sovereignty and build a robust and secure multicloud infrastructure that meets your specific business needs.

About InterCloud

InterCloud's end-to-end global connectivity platform eliminates the complexity in deploying the cloud, giving businesses full control over the security, sovereignty, and performance of their critical data traffic with complete peace of mind.

Working with organisations to help them transform global connectivity, reduce network complexity, and accelerate growth and innovation, InterCloud is a trusted advisor to some of the world's leading brands when it comes to leveraging the cloud for future success.

With offices across Europe, the company's platform is underpinned by its team of cloud experts who guide customers to implement effective strategies to leverage the power of the cloud across their organization – making global connectivity a driver for business performance.

www.intercloud.com