aws | intel

Meeting Your Data Residency Requirements With AWS

Legal, regulatory, contractual or policy requirements mean many organizations must keep data in a particular location. Data residency requirements are paramount to staying compliant in world of digital data privacy. AWS provides edge infrastructure and services that move data processing and analysis as close to the end point as necessary. Whatever your data residency need, it's covered by AWS at the Edge, including our hybrid solution, AWS Outposts.

Here are three areas we'll cover...

1. What data residency is and common situations where it applies
2. Guidance on defining your data residency requirements and meeting your security demands
3. How AWS Outposts enables organizations to meet data residency requirements

What drives the need for data residency?

Data residency is the requirement to store or process data in a specific geographical location. There are three main drivers.

Regulatory requirements

Some businesses and public sector bodies must store or process data in a particular geographical location, to comply with legislative or regulatory demands.

Contractual requirements

Organizations may have contractual agreements with their customers that require data to be stored or processed in a specific geographical location.

Corporate policies

Businesses or government organizations might specify that certain data must be stored or processed in a specified location as part of their license agreements.

Meet your data residency needs with AWS Outposts

AWS Outposts extends AWS infrastructure, services, APIs and tools into your own data center, colocation space or on-premises facility, as a managed service. In essence, it's an extension of the AWS Cloud, running on dedicated AWS infrastructure in a location you specify.

Outposts enables you to meet your data residency requirements, while benefitting from AWS services, even where there's no AWS Region. For example, you can use Amazon EC2 instances, and If you're already running applications on Intel® Xeon® Scalable servers on-premises and benefitting from the software optimizations, you'll enjoy those same benefits on Outposts.

Outposts also unlocks many other advantages, including:

Reduced maintenance and management costs, compared to running your own technology

AWS-grade security controls, including continuous monitoring and protection with AWS Nitro, plus encryption

Consistent experience for developers and operations teams across cloud and on-premises

Process workloads locally and keep your sensitive customer data on premises

How to define your data residency requirements

How do you determine which (if any) of your data assets must be stored in a particular geographical location? Every organization's obligations are different, so there's no 'one size fits all' checklist. But broadly speaking, data that may have data residency requirements associated with it will typically fall into one of two groupings:

Personal information

Personally identifiable information, such as data about users and their behaviors. This could include anything from someone's financial transactions to their medical records.

National security

Nationally sensitive data, such as information about critical infrastructure or resources. Examples include data about the operation of transportation and utility networks, geospatial information and military data.

Analyze your data against applicable legal, regulatory, contractual and policy requirements, to identify whether data residency needs exist, and their specific details. This will typically involve close collaboration with your legal, compliance, business and technical stakeholders.

The outcomes will give you a clear picture of what data needs to be stored where, and why.

Meet your security demands without imposing data residency requirements

Analysts at both Gartner[2] and IDC[3] concluded that the security posture of major cloud providers is equal to or better than the best enterprise data centers, and that security should no longer be considered a primary inhibitor to the adoption of cloud services. You can read more about this in our AWS Data Residency paper.

Some organizations cite better security as a reason for imposing data residency restrictions. In reality, the physical location of data doesn't protect against most attacks, since many are carried out over the internet.[4]

AWS has a robust set of security infrastructure and services that enable organizations to safeguard their data in the cloud. This means businesses and the public sector can typically meet their security needs without imposing data residency requirements.

76%

of countries have existing or draft legislation in place to secure individuals' private data.[5]

AWS Outposts security features

- Protected by the same global network security procedures that protect AWS infrastructure in the Region
- Cabinet has tamper detection and lockable door for additional security
- **Data-at-rest:** Data is encrypted at rest by default on EBS volumes, and S3 objects on Outposts. Intel® AES-NI encryption instruction set improves upon the Advanced Encryption Standard (AES) algorithm to provide faster data protection and greater security. All current generation EC2 instances support this processor feature
- **Data-in-transit:** Data is encrypted in transit between Outposts and the AWS Region
- **Deleting data:** All data is deleted when instances are terminated in the same way as in the AWS Region
- Outposts' Data is encrypted by default and protected by a purpose-built security key that cryptographically shreds data if server security is compromised

Use cases where data residency matters

Healthcare

Driven by regulatory requirements, including those resulting from the Health Insurance Portability and Accountability Act (HIPAA), healthcare providers must safeguard the large amounts of protected health information (PHI) they hold. Data residency requirements here can stem from the need to provide strict physical controls on access to the facilities where data is stored, to guard against unauthorized intrusion.

Financial services

Banking, payment-processing and risk-management services are frequently required to store customers' personally identifiable data in a specific country, for compliance purposes. US legislation such as the Gramm-Leach-Bliley Act (Financial Modernization Act) requires that financial institutions are able to explain how they keep, protect and share customers' private information.

iGaming

iGaming, or online gambling, is a rapidly growing sector, operating in an evolving regulatory landscape. Data residency needs here are driven by authorities' requirements to locally store the personally identifiable data of those participating.

Public sector & critical national infrastructure

Local and national governments process enormous amounts of sensitive data about individuals. From taxpayers' financial information on their tax returns, to nationality details, criminal records and other data collected through people's use of public services, authorities typically need to keep this information within their own jurisdiction. Programs like FedRAMP provide a cyber security risk management program for the purchase and use of cloud products and services by organizations that work with U.S. federal government agencies. AWS Outposts is certified as compliant for FedRAMP.

Data associated with the operation of critical infrastructure, including utilities, transportation, security and defense, is sensitive. Storing this within their own jurisdiction will be desirable or even essential for many authorities.

Oil, gas and mining

Companies extracting resources from the ground perform significant amounts of geomapping to monitor seismic activity . The data this produces is national intelligence, and many authorities require that it remains in-country.

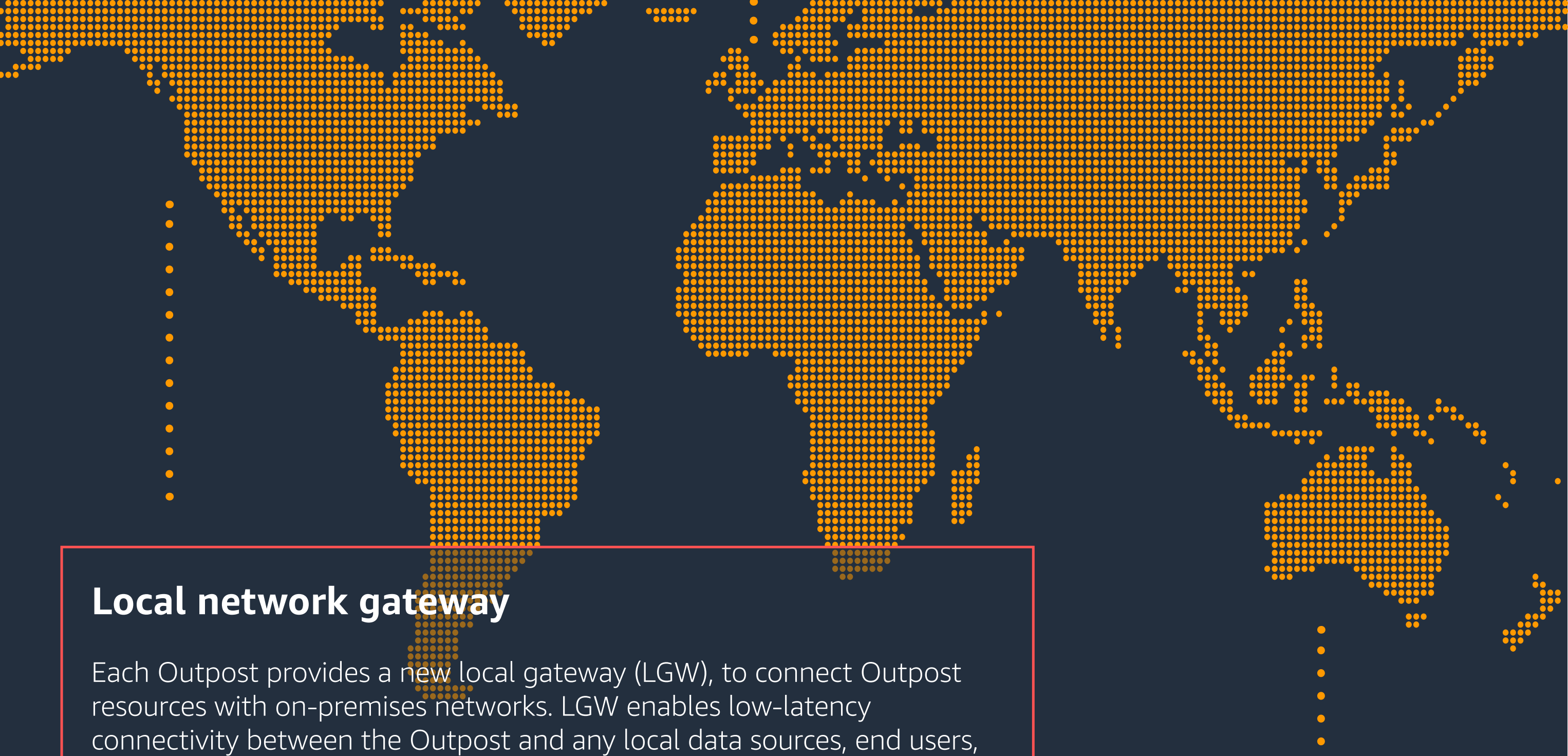
How AWS Outposts addresses your local compute, storage and network needs

Local compute

The AWS Outposts catalog includes options supporting the latest-generation Intel® Xeon® Scalable-powered EC2 instance types, with or without local instance storage. Choose from general-purpose instances, or those optimized for compute, memory, graphics or I/O, to enable the same compute in a customer's data center as in the Region.

Local storage

As well as local instance storage, your organization can store data using either Amazon EBS or S3 within an Outposts environment, giving you the ability to choose where you want data to be kept.



Local network gateway

Each Outpost provides a new local gateway (LGW), to connect Outpost resources with on-premises networks. LGW enables low-latency connectivity between the Outpost and any local data sources, end users, local machinery and equipment, or local databases — so there's no need to go via the Region.

Support from AWS and partners

AWS or our partners can help architect and configure customer workloads on Outposts, to ensure they meet their data residency requirements.

Other AWS services on Outposts

Containers: Amazon ECS and EKS
Databases: Amazon RDS
Data analytics: Amazon EMR
Plus: Access AWS services available in the local AWS Region

Get started with AWS Outposts in three easy steps

1. Engage
Reach out to your account team or fill out our online form: https://aws.amazon.com/contact-us
Alternatively, go into the AWS Management Console.

2. Choose
Select your size and then order the Outpost rack configuration that best suits. Custom configuration is available.

3. Install and Launch
AWS will install and deliver your configuration. Use standard AWS APIs or Management Console to launch and run AWS resources locally.

Learn more today

Discover more about AWS Outposts, including available services, specifications and pricing, on the Outposts website. You'll also find a library of resources, such as white papers, videos, on-demand webinars and training material, to accelerate your journey.

Learn more
https://aws.amazon.com/outposts

---

[1] ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[2] http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
[3] Pete Lindstrom, "Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment," International Data Corporation (July 2015).
[4] https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf
[5] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Intel® Xeon®
Scalable processors