

Data Residency

Your guide to securing data and documents in the Cloud

HPE ProLiant servers running Datex DataStealth software is a paradigm shifting solution that protects your data and documents on the way to the Cloud. Together, this bundled solution addresses regulatory compliance requirements according to PCI-DSS, GDPR, HIPAA, and others, enabling simplified and cost efficient use of Cloud storage and applications.

Data residency challenge

Many companies collect and process vast quantities of customer data, and much of it contains highly sensitive personal information such as dates of birth, social insurance numbers, payment card information, bank account details, online banking credentials, or credit scores. Collected data increases in sensitivity over time when details are combined and related to generate an accurate and complete picture or profile for individual clients. As a result, adhering to a variety of data security and compliance requirements, along with multi-jurisdictional privacy legislation, are of critical importance.

Most companies take privacy and data security responsibilities very seriously and work to remain in agreement and compliance with all applicable and ever changing rules of the game, but when expanding a product or service offering which was developed for one jurisdiction into another, organizations can face privacy challenges from integrating different and overlapping privacy or data protection rules and regulations.

Regions and regulations

Canada: Canadian companies are subject to a combination of Canadian privacy and residency laws such as The Privacy Act, PIPEDA, FOIPPA, and the recently approved Digital Privacy Act (DPA).

USA: Laws such as FISA and the USA PATRIOT Act are applicable to companies operating within the United States that wish to store data and documents in the Cloud. This restrictive legislation has caused some companies to abandon a Cloud based strategy all together.

European Union: Within the EU, privacy laws are even more restrictive. The General Data Protection Regulation (GDPR) is a law coming into effect in May 2018 by which European Parliament, the European Council and the European Commission collectively designed policy to return control of personal data to citizens, and significantly restricts the export of personal data outside the EU.

Solution Brief

Easy to deploy

- Plug and Play
- No application development
- No desktop agent/API/Plugin
- No key management
- Transparent to users and technology

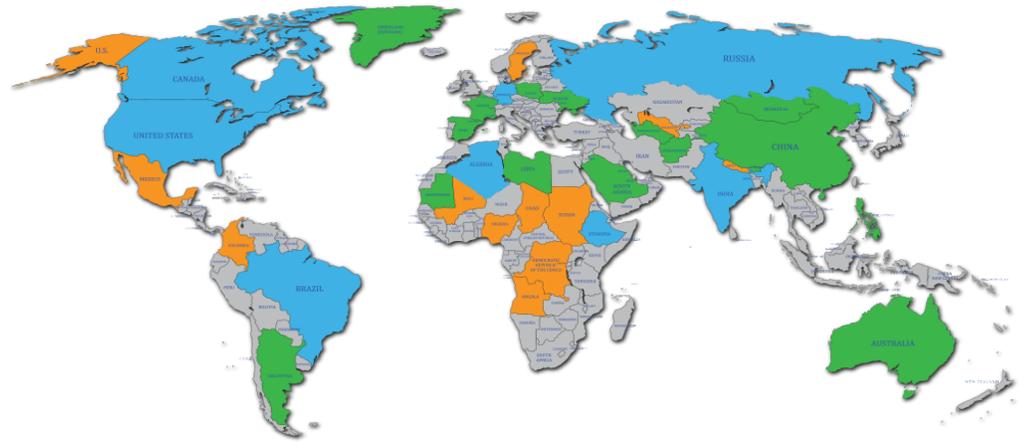
Highly available

- Clustering support
- Multi-site resiliency
- Built-in replication

HPE and Datex

Datex is a software company focused on protecting Enterprise data and documents. HPE is a global technology company that helps customers make IT more efficient, more productive, and more secure.

For many years, Datex and HPE have worked together to design and deliver comprehensive and cost-effective solutions that comply with the highest security standards.



DataStealth Solution

Patented paradigm shifting technology

In response to such complex data residency regulations, a generally accepted principle has emerged and states that if data has been anonymized to such extent that it is indecipherable in transit and at rest, either by way of tokenization or de-identification, said data can be precluded from most if not all residency restrictions. To this end, Datex has developed a revolutionary new approach that solves the dilemma by keeping organizations compliant using a simple plug and play solution. We call it DataStealth.

At a high level, the DataStealth solution is placed at the egress point of your infrastructure and inspects every element of your data on the way out, identifying and extracting private sensitive and/or confidential data discovered in the stream. On the return trip, at the ingress point to your infrastructure, the data passes through the DataStealth solution again, and the original data is reinserted into the stream prior to presentation to the end user, but only for authorized users, and only for authorized use cases.

What makes DataStealth so revolutionary is that DataStealth is plug and play, and is transparent to both end users and to Cloud providers. No app development is required. No code changes are required. No plugins (no API, desktop app, or browser plugin) need to be installed. No software or databases need to be installed and managed.

The Result

DataStealth is the enabling technology you have been looking for.

DataStealth allows enterprises to define their data protection and data residency policies to ensure their sensitive data is appropriately secured and protected while they remain in control of data residency. Private, sensitive and / or confidential information never leaves their environment without explicit consent and full control over where it goes, how it is protected, and when it can be reconstituted. NEVER.

Authorized data security administrators can select whether to allow a data going to the cloud should remain in clear text, be encrypted, or to be replaced with a token on a field-by-field basis. When using surrogate token values, sensitive data never leaves the organization's control in any format – making it particularly useful for organizations that need to adhere with Canadian Privacy Laws. Data in the Cloud is either tokenized or encrypted, or both, so it is meaningless when viewed within the cloud and organizations can be confident that their sensitive data is within their full control at all times.

Learn more at
www.datex.ca/datastealth