

SAAS DATA RESIDENCY

DataStealth for Salesforce Marketing Cloud

Data residency compliance without compromise.

PLATFORM SALESFORCE MARKETING CLOUD

CAPABILITY TOKENIZATION IN TRANSIT

DRIVER DATA SOVEREIGNTY



01 · EXECUTIVE SUMMARY

The residency trade off, eliminated

Salesforce Marketing Cloud is a leading platform for digital marketing automation and analytics, and the preferred choice for organizations executing omnichannel campaigns. However, its limited data residency options create challenges for global organizations in jurisdictions with strict privacy and governance mandates. For many non United States enterprises, deploying SFMC without violating data sovereignty laws can be difficult, if not impossible.

The choice often comes down to abandoning SFMC in favour of less integrated alternatives, or assuming regulatory risk. DataStealth eliminates that trade off.

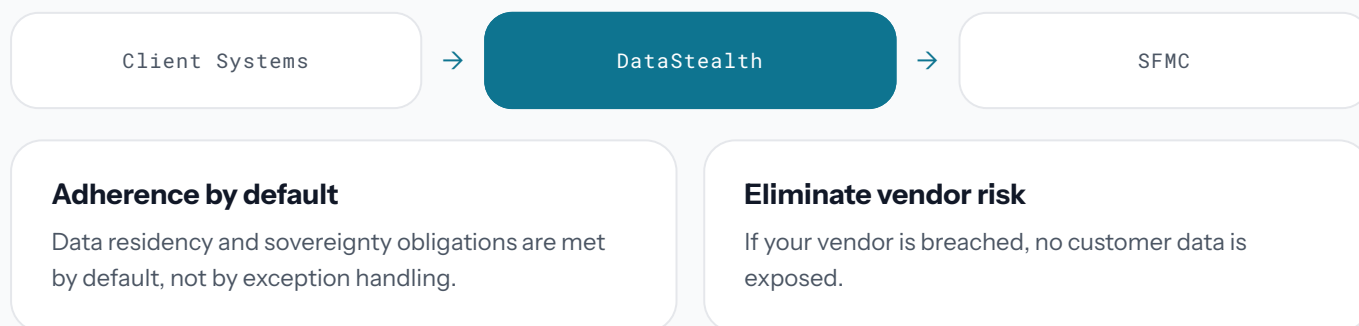
A PARADIGM SHIFT IN DATA SECURITY

When used with SFMC, DataStealth anonymizes personally identifiable information in transit and at rest. Sensitive data is tokenized or encrypted before reaching SFMC, ensuring Salesforce never receives or stores real sensitive data. Authorized users and systems can still access detokenized data; Salesforce, and any potential threat actors, cannot.

02 · HOW IT WORKS

Protected before it lands

The DataStealth Data Security Platform anonymizes and protects sensitive data in real time, without requiring changes to applications or infrastructure, working transparently at the network level so sensitive data is always protected before it lands in SFMC.



03 · DIFFERENTIATORS

Why DataStealth is different, and better

No application changes required

Works without modifying Salesforce or SFMC, with no APIs, no agents, and no custom development.

Data never leaves your region

In region tokenization maintains 100% data residency compliance.

Transparent to end users

All Salesforce features remain intact with no loss of functionality or performance.

Protection from credential breaches

Even if SFMC credentials are compromised, no usable data is exposed.

Q Day resistant

Unlike encryption, tokenization is not susceptible to quantum decryption threats like Harvest Now, Decrypt Later.

04 · CAPABILITIES

Inputs supported and outputs secured

Data inputs supported

Salesforce Sales and Service Clouds via Marketing Cloud Connect, with multi org and OAuth support. Direct file uploads, where SFTP endpoints tokenize in transit. Salesforce Marketing Cloud APIs, where HTTPS endpoints tokenize and detokenize dynamically.

Data outputs secured

Email, detokenized in flight, in region, and SPF and DKIM compliant. Web views, fully personalized without exposing real data. SFMC application access, where authorized users see detokenized data and others see redacted or tokenized content. Downloads, transparently detokenized.

NET EFFECT

The marketing team keeps the platform it wants and the functionality it expects. The compliance team gets a deployment where sensitive data never crosses the jurisdictional boundary in clear text.

Secure marketing, made the default

DataStealth transforms the way organizations can safely use Salesforce Marketing Cloud and other third-party tools, even in highly regulated industries and geographies, anonymizing sensitive data before it enters the SFMC ecosystem while maintaining full functionality.

- 100% data residency compliance
- No Salesforce or SFMC changes
- Full feature parity for users
- Quantum threat resistant

info@datastealth.io