DataStealth

DataStealth for Salesforce Marketing Cloud

Data Residency Compliance without Compromise

datastealth.io | info@datastealth.io

Executive Summary

Salesforce Marketing Cloud (SFMC) is a leading platform for digital marketing automation and analytics. Its seamless integration with Salesforce Sales Cloud and Service Cloud makes it the preferred choice for organizations looking to execute omnichannel campaigns and customer engagement strategies.

However, SFMC's limited data residency options create challenges for global organizations, particularly those in jurisdictions with strict privacy, compliance, and data governance mandates. For many non-U.S. enterprises, deploying SFMC without violating data sovereignty laws can be difficult, if not impossible. In some cases, companies must exclude certain customer segments to remain compliant, resulting in fragmented marketing programs, limited reach, and increased operational costs.

The choice often comes down to abandoning SFMC in favor of less integrated alternatives or assuming regulatory risk.

DataStealth eliminates that trade-off.

DataStealth: A Paradigm Shift in Data Security

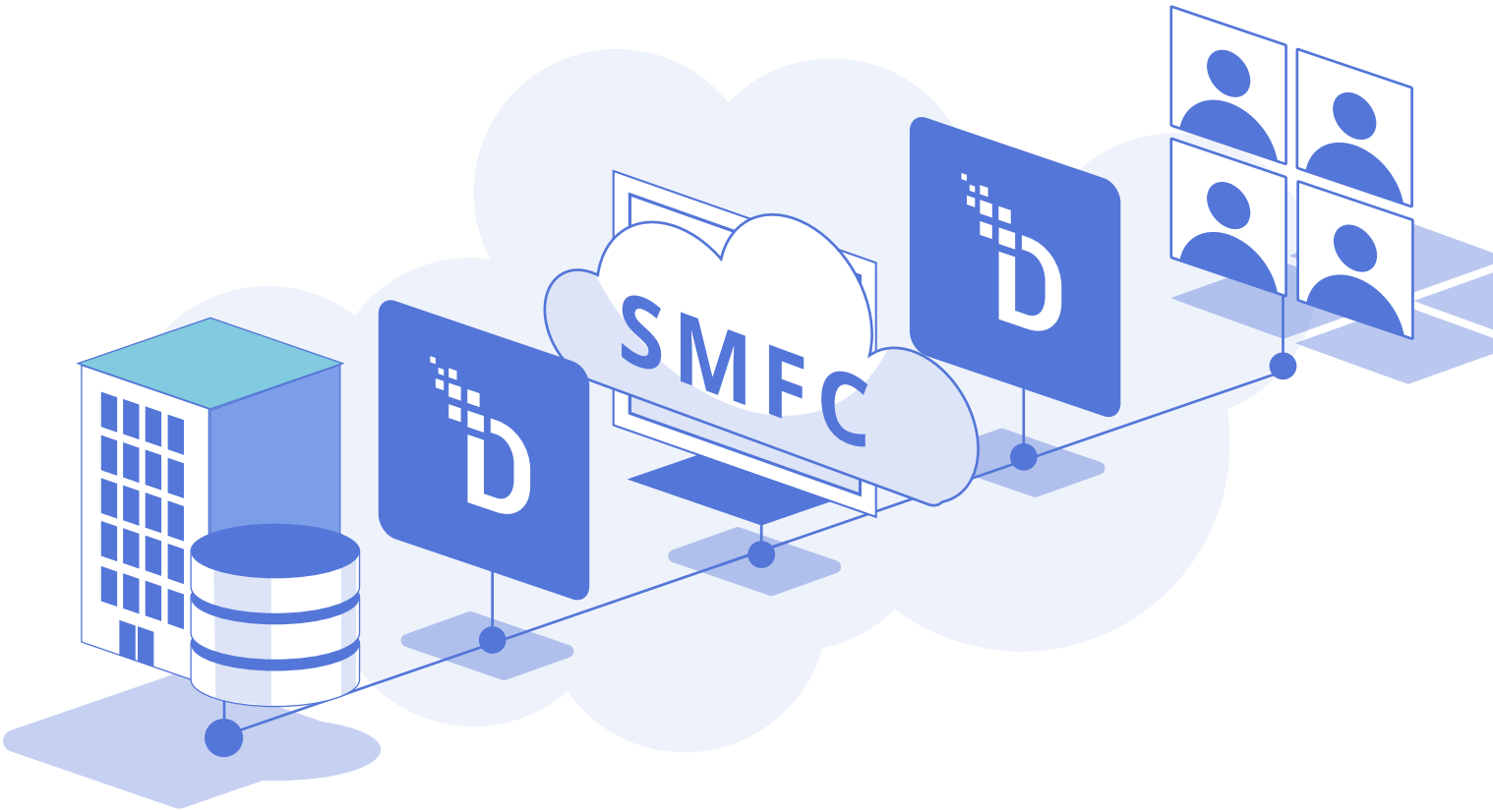
When used with Salesforce Marketing Cloud, DataStealth anonymizes personally identifiable information (PII) in transit and at rest. Sensitive data is tokenized or encrypted before reaching SFMC, ensuring that Salesforce never receives or stores real sensitive data. Authorized users and systems can still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

How it works:

DataStealth's Data Security Platform (DSP) anonymizes and protects sensitive data in real time, without requiring changes to applications or infrastructure. Unlike traditional security tools that rely on perimeter defense or in-app modifications, DataStealth works transparently at the network level, ensuring sensitive data is always protected before it lands in SaaS applications, systems, databases, and applications.

When used in conjunction with third-party tools like SFMC, the results are immeasurable:

- Adherence to data residency and sovereignty obligations by default
- Eliminate risk - if your vendor is breached, no customer data is exposed



Why DataStealth is Different - and Better

No Application Changes Required:

DataStealth works without modifying Salesforce or SFMC. No APIs, no agents, and no custom development needed.

Protection from Credential Breaches:

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

Data Never Leaves Your Region:

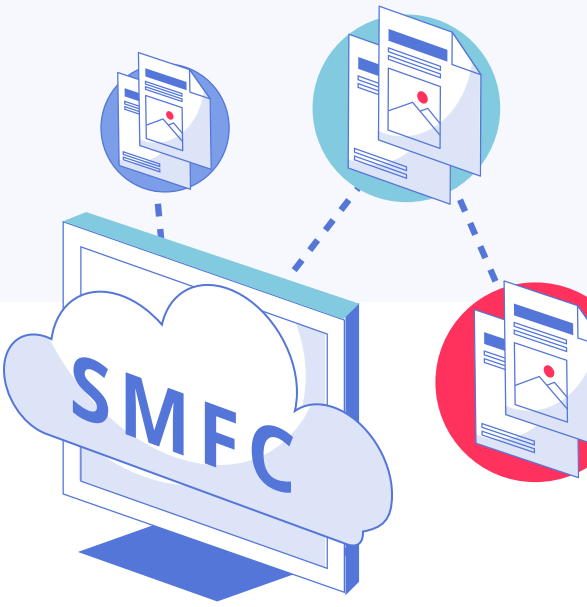
With in-region tokenization, organizations can maintain 100% data residency compliance.

Q-Day Resistant:

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

Transparent to End Users:

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



Key Capabilities for Salesforce Marketing Cloud

Data Inputs Supported:

- **Salesforce Sales & Service Clouds (via Marketing Cloud Connect):** Tokenized data is transferred using standard MC Connect functionality, with support for multi-org and OAuth-based user management.
- **Direct File Uploads:** SFTP endpoints intercept and tokenize data in transit without disrupting existing Salesforce user credentials.
- **Salesforce Marketing Cloud APIs:** HTTPS endpoints tokenize and detokenize data dynamically at the API level with minimal configuration.

Data Outputs Secured:

- **Email:** Personalized email content is detokenized in-flight, in-region, and all links, bounce-backs, and tracking are routed through DataStealth. SPF/DKIM compliance ensures deliverability.
- **Web Views:** Fully personalized and branded views are generated without exposing real data. Detokenization occurs only in-region.
- **SFMC Application Access:** Authorized users see detokenized data; unauthorized users see redacted or tokenized content based on the DataStealth policy.
- **Downloads**: All file downloads and API interactions are transparently detokenized without the need for downstream application changes.

Conclusion

DataStealth transforms the way organizations can safely use Salesforce Marketing Cloud and other Third Party tools, even in highly regulated industries and geographies. By anonymizing sensitive data before it enters the SFMC ecosystem, DataStealth empowers businesses to maintain full functionality while achieving compliance with privacy, regulatory, and contractual obligations.

DataStealth doesn't just enable secure marketing.

It makes secure marketing the default.