DataStealth

DataStealth

Common Use Cases

vJanuary 2018

Tokenization

DataStealth decreases the scope of an annual PCI Compliance audit by up to 95% by removing all payment card information from data and documents BEFORE it enters a network. Tokenization options include random, repeatable, sequential, order preserving, format preserving and more.)

CASB (Cloud Access Service Broker)

DataStealth enables the use of Cloud Apps and Cloud Storage without ever exposing any private/confidential/regulated information beyond your organization's IT perimeter. Only obfuscated information is sent to the Cloud.

TDM (Test Data Management)

When moving data from a production environment to a development environment, DataStealth removes regulated and/or restricted information, in real time, as the data flows across the network. Developers, analysts, and researchers are able to work with fully obfuscated data, which may be re-identified later if required, but only by authorized users and for authorized use cases.

DLP (Data Loss Prevention)

DataStealth allows connections to sanctioned Cloud services, for authorized users, and limits or blocks the use of unknown or unsanctioned Cloud services. This keeps your data under your control, at all times.

Information Privacy (Data Masking)

DataStealth applies policy driven data masking to data and documents in real-time, on the way to an endpoint or to a user. Data Masking options include full and partial masking, suppression, rounding, offset, shuffling and more.

Data Residency (GDPR/PIPEDA)

DataStealth controls what data and documents leave a geo-location, and controls when and where the data and documents can be viewed.

Identity/Authentication/Entitlement Management

DataStealth decreases the risk of stolen credentials and phishing attacks by adding MFA/MSA/2FA to any application, website, or file server. This forces users to authenticate not only with something they know (username and password), but also with something they have (mobile phone, etc.).