Datex | DataStealth

Solution Overview

DataStealth

A paradigm-shifting approach to data and document protection

“Intruders Cannot Steal What Is Not There!”

The Cybersecurity Challenge

Cybersecurity has become the leading concern for organizations worldwide. Organizations that have suffered a network breach, and have had their data and documents stolen, have seen their loyal customers leave, their revenues eroded, and their share prices fall, not to mention the actual hard and soft costs of the breach.

In today’s electronic world, the theft of data and documents has become a pandemic; from payment merchants to healthcare providers, corporations of all sizes, and even the military and government. The responsibility for ensuring that an organization is not breached has worked its way up to the CEO office and to the Board of Directors, and executives are being held to the highest standard. For many companies, protecting the rights of customers is no longer just the right thing to do. In many jurisdictions, it is becoming be a legal requirement, with stiff penalties for non-compliance.

The Traditional Approach

Traditional data protection solutions that are commonly adopted by organizations today typically fall into two groups;
• Perimeter protection solutions designed to stop intruders from gaining access to an environment through the network perimeter. “Building bigger walls to keep the bad guys out”.
• Alert and monitor solutions, that are designed to inform organizations “if and when” an intruder gains unauthorized access to a network. This is reactive in nature and does not ensure data protection.

Organizations using these traditional methodologies to protect their networks are being breached at an alarming rate, as evidenced by the almost daily reports in mainstream media reporting on the latest victim of hackers. Despite this, these organizations tend to rely on the same traditional methodologies to protect their digital assets.

“Doing the same thing over and over, and expecting a different result, is the definition of insanity”. - Albert Einstein

It was clear that somebody needed to come up with a revolutionary and innovative way to protect an organization’s most valuable assets; their data and documents. Thus, DataStealth was born.

Solution Overview

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

About Datex

Datex is a software company focused on protecting Enterprise data and documents.

How DataStealth Works

DataStealth starts by combining an organization's privacy, regulatory, compliance and other standards and requirements, with DataStealth's suite of tokenization, deidentification and encryption options, to create a DataStealth Data Protection Policy. This policy is then applied to all network traffic passing through DataStealth.

When any network traffic matches any one of the active Data Protection Policies, DataStealth springs into action and applies the Data Protection Policy to the network traffic. This application happens in real-time, on the wire, as traffic passes through.

- **INSPECT** - Inspect all network traffic, data, and documents.

- **EXTRACT** – Remove private, confidential, regulated, and sensitive information (PCI, PII, PHI, etc.)

- **REPLACE** – Replace extracted data elements with substitute values.

- **SECURE** – Secure the original data elements. (With an algorithm that is computationally infeasible to breach)

In the event of a breach, whether external or internal in nature, there is no private or confidential data in the network. With DataStealth, intruders cannot steal what is not there.

What Makes DataStealth Unique

DataStealth is Simple! DataStealth is a plug- and-play solution that does not need to be integrated with any downstream technology. There is no requirement for application changes, no software, databases, agents, APIs, or browser plugins to install, and no key management solution required. We can also configure multiple customer Use Cases on a single appliance!

DataStealth is Agnostic! DataStealth works at the network layer, and supports a very large number of payloads and protocols. It also works with all network devices, server hardware, operating systems, applications, and devices.

DataStealth is Flexible! DataStealth can be deployed as physical or virtual hardware, deployed on-premise, hosted or in the Cloud, and can be run as a managed service or self-managed.

DataStealth is Secure! DataStealth uses an advanced storage methodology that is computationally infeasible to breach.

Solution Overview

DataStealth Customer Use Cases

We haven't experienced a customer Use Case that we haven't been able to address with DataStealth. Here are some of the ways customers are leveraging the unique value of DataStealth.

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

Data Residency (GDPR/PIPEDA/Patriot Act): DataStealth controls what data and documents can leave a geo-location, and controls when and where the actual data and documents can be viewed. Salesforce is a common Use Case.

CASB (Cloud Access Service Broker): DataStealth enables the use of Cloud Apps and Cloud Storage without exposing any private/confidential/regulated information beyond your organization's IT perimeter. Only obfuscated information is sent to Cloud providers such as AWS and Azure.

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.

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

Access and Entitlements: 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.)

Learn more at
www.datex.ca/datastealth
info@datex.ca
+1-855-55-DATEX

Datex | DataStealth