opentext™

4 reasons why your sensitive data may be at greater risk than you think

With evolving compliance requirements and technology adding complexity, protecting sensitive data can be a headache.

Today's organizations face four main challenges when protecting their sensitive data.

1 Growing volume and types of sensitive data

With data regulations and standards continuously evolving, enterprises must protect an ever-increasing amount and variety of sensitive data to avoid punitive fines and reputational damage.

86% of enterprises manage multiple types of data and/or data related processes subject to privacy and security compliance requirements.[1]

86 percent

2 Vulnerable cloud environments

As organizations are increasingly moving to the cloud, it is paramount to ensure sensitive data is handled securely.

21 percent

21% of cloud files contain sensitive data.[2]

1,935

The average organization uses 1,935 unique cloud services. Most think they use about 30.[3]

3 Fragmented systems environments

With varying degrees of control, processing sensitive data across disparate cloud environments demands a unique approach for each individual system.

84% have a multi-cloud strategy.[4]

71% plan to process sensitive data in at least one type of cloud environment (SaaS, PaaS and/or IaaS).[5]

4 Rising data breaches

Two types of companies exist: Those at risk of breach and those protected against a breach.

60%

60% globally have been breached.[6]

30%

30% experienced a breach within the last year.[7]

The solution

Data tokenization

Data tokenization replaces individual data values, such as credit card numbers, with a surrogate value called a token. Tokens offer superior protection and usability over more traditional encryption. With tokens, sensitive data remains secure even if it ends up in the wrong hands.

Encryption	Tokenization
Uses algorithms that are mathematically connected to the original data	Replaces data with surrogate values not mathematically connected to the original data
Does not resemble the original data and requires changes to systems processing encrypted data	Retains the format and length of the original data and can be processed by existing systems
Protects unstructured data and/or large volumes of data, e.g., entire files, images, videos	Protects individual sensitive data values, e.g., credit cards,social security numbers, personal details

OpenText data tokenization solutions combine the security of the OpenText Cloud platform with OpenText tokenization experts to protect your sensitive data.

Learn more ›

opentext.com

[1] Aberdeen, *The State of Privacy and Security Compliance*, 2018. [2] McAfee, *Cloud Adoption and Risk Report*, 2019. [3] RightScale/Flexera, *State of the Cloud Report*, 2019. [4] McAfee, *Cloud Adoption and Risk Report*, 2019. [5] Thales/IDC, *2019 Thales Data Threat Report*, 2019. [6] Ibid. [7] Ibid.

Copyright © 2019 Open Text. All Rights Reserved. Trademarks owned by Open Text.
For more information, visit: https://www.opentext.com/about/copyright-information 09/2019I1322511EN