opentext™

WHITE PAPER

OpenText Data Privacy and Protection (Voltage) Cloud & Analytics

Securing sensitive data assets for cloud services

Contents

Enterprise security and risk professionals responding to cloud data security research confirm that more than 40% of their corporate data in the cloud is sensitive in nature and insufficiently secured.[1]

Introduction

Today's business challenges pressure enterprises to be agile and flexible, and to swiftly serve customers in new markets. While these factors are encouraging enterprises to adopt the cloud across their entire business, most often the main driving factors are the cost and complexity of maintaining on-premises data center hardware and software. Businesses that require increased capacity for growth or which experience seasonal bursts of activity have realized that it is more cost effective to take advantage of elastic cloud capacity when needed than to acquire, manage, and maintain data center hardware and software.

Enterprise security and risk professionals responding to cloud data security research confirm that more than 40 percent of their corporate data in the cloud is sensitive in nature and insufficiently secured.[1] Adding further complexity to the problem, the Ponemon Institute found that, on average, today's enterprises use 27 different Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) solutions to run their business.[2]

However, traditional security controls embedded throughout existing IT infrastructure are proving increasingly ineffective as data has become more pervasive, mobile, and cross-functional. Most organizations are now using multiple cloud providers, complicating efforts to protect sensitive data moving across hybrid IT. With the increasing number and complexity of privacy regulations, such as the GDPR and CCPA, and the upward trend in the number, scope, and scale of data breaches, more effective measures are required to protect sensitive data wherever it flows, whether on premises, in cloud infrastructure and applications, or in analytics platforms.

The combination of these strong business drivers and ineffective security controls has unfortunately already led to sensitive data being migrated into the cloud ahead of organizational readiness to secure it. Large-scale data breaches, typically associated with missing, ineffective, or misconfigured cloud-native data security capabilities, are increasing along with the penalties and fines being levied for the consequent non-compliance with data privacy regulations.

Apply data centric security to accelerate cloud migration

OpenText™ Data Privacy and Protection Cloud & Analytics (Voltage) protects sensitive data persistently across multi-cloud, hybrid, and on-premises environments. It embeds data-centric security across hybrid IT and, by reducing the risk to sensitive data, accelerates the safe migration to cloud environments.

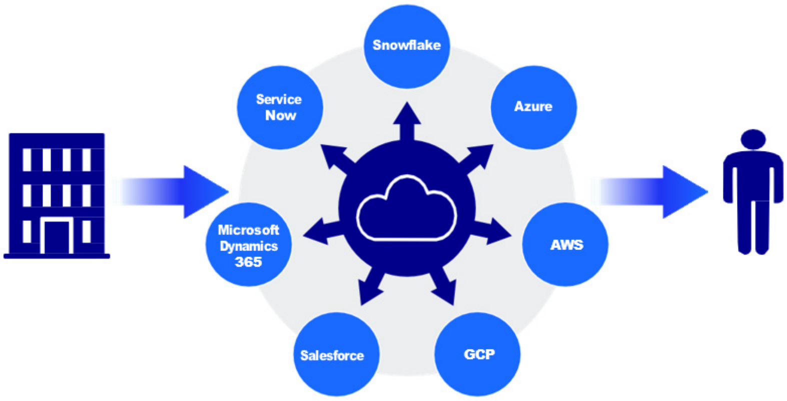
1 Enterprise Strategy Group, Trends in Cloud Data Security: The Data Perimeter of Hybrid Clouds, 2019

2 Ponemon Institute LLC, The 2018 Global Cloud Data Security Study, 2018

The tokenization technologies in OpenText Data Privacy and Protection Enterprise provide flexible implementation and protection for a virtually unlimited number of structured data types in any language and any region, with proven performance and scalability.

OpenText Data Privacy and Protection Cloud & Analytics provides security servers and clients that enable applications, data, and data stores to interoperate with on-premises and in-cloud services to provide end-to-end protection across the data lifecycle. OpenText Data Privacy and Protection Enterprise (Voltage) is FIPS 140-2 and Common Criteria validated and supports the industry’s broadest range of platforms and systems, from z/OS, and transactional systems such as Stratus VOS, to open systems such as Hadoop across distributions such as Cloudera and MapR, cloud services such as AWS EMR and Azure HDInsight, and high-performance analytics platforms such as OpenText Analytics Database (Vertica), Teradata, and Snowflake.

Hybrid IT: Platform-agnostic data-centric security



OpenText data protection preserves data usability

The tokenization technologies in OpenText Data Privacy and Protection Enterprise provide flexible implementation and protection for a virtually unlimited number of structured data types in any language, and any region, with proven performance and scalability. OpenText Format-Preserving Encryption (FPE), OpenText Format-Preserving Hash (FPH) and OpenText Secure Stateless Tokenization (SST) enable enterprises to de-identify sensitive information in ways that neutralize the effects of a data breach, but permit continued use of the data in its protected state in applications and analytics platforms.

OpenText tokenization technologies maintain the context and meaning of the data—such as its referential relationships, logic, and business intent—in its protected form, ensuring that businesses can minimize requirements to decrypt. The preservation of referential integrity also enables protected data to be reliably referenced and joined for cross-cloud analytics, providing key insights through identifiers, such as phone numbers or IDs, common across disparate data sets.

OpenText Format-Preserving Hash (FPH) offers full data anonymization but with the same benefits of other OpenText tokenization technologies regarding structure, logic, partial field application, and usability for some use cases, such as click-stream analytics.

Data pseudonymization with OpenText

OpenText FPE, a mode of the Advanced Encryption Standard (AES), is a fundamental innovation, which enables OpenText Data Privacy and Protection Cloud to provide high-strength, robust data encryption, while maintaining flexibility for use. An implementation of the FF1 method as presented in NIST SP 800-38G3, OpenText FPE is a cryptographic standard that provides the pseudonymization necessary to enable compliance with data privacy regulations at data field and sub-field levels, while simultaneously enabling organizations to run business processes and analytics on protected data sets.

OpenText Secure Stateless Tokenization (SST) is an advanced, patented, data security solution that helps assure protection for payment card data on premises or in the cloud. OpenText SST eliminates the token database and removes the need for storage of cardholder or other sensitive data, enabling a vast reduction in the scope of a PCI-DSS compliance audit, for example. By using a set of static, pre-generated tables to consistently produce a unique, random token for each data value, such as a Primary Account Number (PAN), the speed, scalability, security, and manageability of the tokenization process is optimized.

Data anonymization with OpenText

In specific use cases, such as enabling secure and compliant test data management, the ability to recover data may present an unnecessary risk or be explicitly undesired. OpenText Format-Preserving Hash (FPH) offers full data anonymization but with the same benefits of other OpenText tokenization technologies regarding structure, logic, partial field application, and usability for some use cases, such as click-stream analytics. OpenText FPH employs a non-disruptive and more flexible one-way, irreversible transformation that enables high-performance data usability, unlike traditional anonymization techniques such as SHA-256.

OpenText Stateless Key Management

OpenText Stateless Key Management is the cornerstone of OpenText simplicity and scalability. Keys are derived dynamically as required, with no key database to store, protect, back-up, or to integrate with traditional key management solutions. Enterprises do not need to manage keys, certificates, or databases, eliminating the hardware, software, and IT and personnel processes and costs required to continuously protect key databases on-premises, in off-site back-ups, or even in the cloud. OpenText Stateless Key Management maintains an organization's complete control over their encryption keys while enabling low-cost, high-performance, highly available data protection that scales to protect the sensitive data of the world's largest financial services companies, telcos, payment processors, and other global enterprises and government agencies.

[3] National Institute of Standards and Technology (2016) Special Publication 800-38G, Recommendation for Block Cipher Modes of Operation: Methods for Format- Preserving Encryption

> **OpenText Data Privacy and Protection Cloud & Analytics not only eliminates the risk of data breaches introduced through missing or misconfigured security controls but also enables the adoption of a continuous data protection model in multicloud environments through removing the need for in-cloud decryption.**

Evolution of hardware security modules to cloud environments

Where OpenText Data Privacy and Protection Enterprise is used to migrate storage and workloads to cloud-based environments, an HSM-based root of trust in the cloud may be important. nShield as a Service from nCipher Security, a certified OpenText alliance partner, supports OpenText Stateless Key Management, and is a subscription-based, FIPS 140-2-certified nShield HSM solution for generating, accessing, and protecting cryptographic key material separately from sensitive data. This cloud-hosted model gives organizations the option to supplement or replace HSMs in their data centers.

Protecting data and enabling analytics in the cloud

Low-cost data storage combined with elastic computation and an ever-increasing range of data analytics services is succeeding in shifting the balance of big data deployments from on premises to the cloud. But the external hosting of sensitive data carries additional security responsibilities and serious risks. Under the shared responsibility model, cloud providers will ensure that the hardware and software services they offer are secure, but customers are responsible for the security of their own assets.

Through ensuring that data is simultaneously protected and useable by cloud applications and services in its protected form, OpenText Data Privacy and Protection Cloud & Analytics not only eliminates the risk of data breaches introduced through missing or misconfigured security controls but also enables the adoption of a continuous data protection model in multicloud environments through removing the need for in-cloud decryption. While data is being moved to the cloud, it needs to be persistently protected across its lifecycle, at ingestion, at rest, and while in use.

OpenText Data Privacy and Protection Cloud & Analytics can be integrated with:

- Cloud ETL services, such as AWS Glue, Azure Data Factory, and Google Data Fusion, as well as other COTS ETL tools such as Informatica, Talend, DataStage, Ab Initio, and others.
- Streaming platforms, such as Kafka, NiFi, Storm, Streamsets, and Cloud streaming services such as AWS Kinesis, Azure EventHubs, Google Dataflow, and others.
- Data lake services, such as AWS Simple Storage Service (S3), Azure Blob storage, Google Cloud Storage, AWS RedShift, Azure Databricks, Azure SQL Data Warehouse/Synapse Analytics, Google BigQuery, AWS EMR, Azure HDInsight, Google Dataproc, Snowflake, and others.
- SQL and NoSQL database services, such as AWS RDS, Aurora, and DynamoDB, Azure SQL Database, Cosmos DB, Google Cloud SQL, and others.

Additional capabilities include:

- OpenText transformation on serverless compute services or Functions as a Service (FaaS), such as AWS Lambda, Azure Functions, and Google Cloud Functions, AWS Macie, AWS API Gateway, Google Data Catalog, Google Apigee, Azure Data Catalog, API Management, and others.

In a multi-cloud enterprise landscape, OpenText Data Privacy and Protection Enterprise removes the security gaps between different CDWs, cloud services, query tools, business intelligence platforms, SaaS applications, and cloud service providers.

OpenText Data Privacy and Protection for Cloud data warehouses

The integration of OpenText Data Privacy and Protection Enterprise with cloud data warehouses (CDWs), such as Snowflake, Amazon Redshift, Google BigQuery, and Azure Synapse, enables OpenText customers to conduct high-scale secure analytics and data science in the cloud using format-preserved, tokenized data that mitigates the risk of compromising business-sensitive information while adhering to privacy regulations.

In addition, OpenText Data Privacy and Protection Enterprise's advanced tokenization technologies that permit the pseudonymization and anonymization of any structured data type, in any quantity required, across all languages, promote data sharing and mobility without requiring the data to be unprotected and reprotected at each technology border crossing. In a multi-cloud enterprise landscape, OpenText Data Privacy and Protection Enterprise removes the security gaps between different CDWs, cloud services, query tools, business intelligence platforms, SaaS applications, and cloud service providers.

These powerful, cloud-native integrations add to OpenText Data Privacy and Protection Enterprise's existing deep capabilities for data privacy and protection across databases, data warehouses, and big data environments both on-premises and in the cloud. PII, PHI, PCI, and other categories of sensitive data such as intellectual property can be protected on premises prior to uploading to the cloud, or protected as it lands in the cloud, such as into AWS S3 buckets or Snowflake external stages.

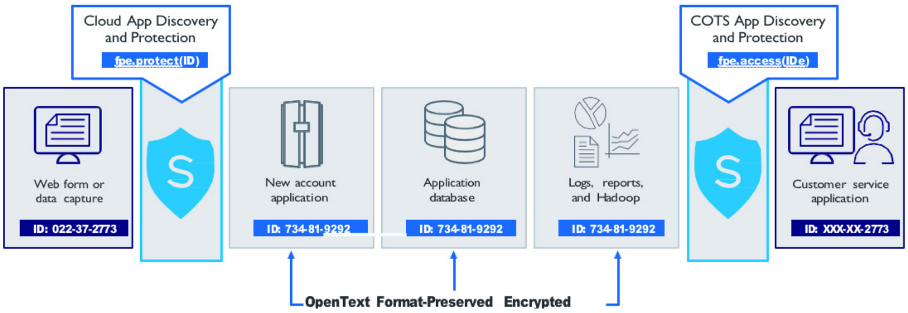
OpenText Data Privacy and Protection Enterprise's CDW solutions permit direct control of the protection and unprotection of data in these environments, giving you control over which sensitive result sets, if any, are exposed to your data scientists or analytics partners. And by working with native role-based access policies in CDWs, OpenText Data Privacy and Protection Enterprise permits transparent access to protected data with no need for code changes or knowledge of OpenText APIs.

OpenText Data Privacy and Protection Sentry for SaaS, COTS, and in-house applications

OpenText Data Privacy and Protection Sentry (Voltage) specializes in data protection for cloud software services as well as for on-premises applications. It extends the reach of OpenText data protection technologies to SaaS applications, such as Salesforce, ServiceNow, OpenText Software Delivery Management, and Microsoft Dynamics 365, as well as to commercial off-the-shelf (COTS) applications. Moreover, through additional innovations, such as secure local indices supporting partial and wildcard search terms, and secure email address formatting for SMTP relaying, OpenText Data Privacy and Protection Sentry preserves application functionality that is impacted by competing solutions. OpenText uses dataflow interception techniques to protect sensitive data flowing through the network, ensuring organizations remain in control of the security of their data used in SaaS and COTS applications that cannot be directly integrated with OpenText Data Privacy and Protection Enterprise.

OpenText Data Privacy and Protection Sentry uses dataflow interception techniques to protect sensitive data flowing through the network, ensuring organizations remain in control of the security of their data used in SaaS and COTS applications that cannot be directly integrated with OpenText Data Privacy and Protection.

OpenText Data Privacy and Protection with Sentry



With migration to hybrid IT and an increasing reliance on SaaS applications, organizations may not have the accessibility or development resources for API-level integration of their self-developed applications. The same technology can be used to accelerate the protection of these in-house applications, providing an alternative to API integration that avoids the need for programming. OpenText Data Privacy and Protection simplifies hybrid IT migration, accelerates time to value by enabling privacy compliance, and offers consistency for end-to-end data protection.

Organizations can deploy OpenText Data Privacy and Protection on premises and in the cloud. OpenText Data Privacy and Protection Sentry communicates with ICAP (Internet Content Adaptation Protocol) capable network infrastructure, such as HTTP proxies and load balancers, to apply security policies to data traveling to and from the cloud, and it intercepts JDBC (Java Database Connectivity) and ODBC (Open Database Connectivity) API calls to apply security policies to data traveling to and from the database. Wherever it is deployed, the enterprise retains complete control over the infrastructure, without the need to share encryption keys or token vaults with any other party, and OpenText Data Privacy and Protection Sentry's inspection mode ensures that security policies can be targeted at the specific data fields and file attachments that contain sensitive information.

Key benefits

High scalability and agility with enterprise data protection and privacy

By applying data-centric security, OpenText Data Privacy and Protection Cloud & Analytics and OpenText Data Privacy and Protection Sentry protect the data itself and address the main security challenges in the cloud. They mitigate the risk of cloud adoption across the spectrum of cloud services that enterprises operate, providing consistent data security for hybrid IT.

OpenText Data Privacy and Protection Cloud & Analytics and OpenText Data Privacy and Protection Sentry simplify deployment of a trusted IT architecture where data, applications and workflows can run On premises and in the cloud. They accelerate implementing new business models and achieving cost and competitive efficiencies, while protecting the data that matters most.

OpenText Data Privacy and Protection Cloud & Analytics and OpenText Data Privacy and Protection Sentry enable organizations to:

- Accelerate cloud migration with proven data-centric security for safe deployment of applications, data, and workloads.
- Enable data privacy compliance in cloud-based analytics, applications, and business processes.
- Conduct high-scale secure analytics and data science in cloud data warehouse systems.
- Manage data protection consistently across hybrid IT, IaaS, SaaS, or PaaS cloud services, as platform agnostic solutions for greater flexibility to scale with multi-cloud ecosystems.
- Reduce the risk of cloud-based data breach and insider attack in a shared environment.
- Neutralize data breach impacts by rendering data unusable by attackers.
- Remove the requirement for breach notification of affected consumers under regulations such as the GDPR where personal data has been protected.
- Consistently protect data regardless of where it is stored or processed, across the data lifecycle.

Consistent data-centric security for cloud migration

The key to safe enterprise migration to the cloud is to embed data security consistently, persistently, and seamlessly to span hybrid IT, allowing data to flow securely across environments. OpenText Data Privacy and Protection Cloud & Analytics and OpenText Data Privacy and Protection Sentry simplify deployment of a trusted IT architecture where data, applications and workflows can run on-premises and in the cloud. They accelerate implementing new business models and achieving cost and competitive efficiencies, while protecting the data that matters most.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.