OpenText Data Privacy and Protection Foundation

Comprehensive data-centric security for the evolving data-driven landscape

Benefits

- Format-preserving protection for all data states
- GDPR, CCPA, HIPAA, and PCI DSS regulations compliance
- Innovative key management and data security solutions
- Flexible integration with major cloud services, databases, and applications

The rapid growth of data, GenAI adoption, and cyberattacks has undermined consumer trust in companies' data protection. The Ponemon Institute's 2024 study shows a 10-percent spike in breach costs to $4.88M, the highest since the pandemic. Given that 40 percent of breaches involve multi-environment data, and public cloud breaches average $5.17M, security teams must prioritize hybrid and public cloud environments and implement robust encryption strategies.[1]

Format-preserving data protection for all data states

OpenText™ Data Privacy and Protection Foundation (Voltage SecureData Enterprise) offers comprehensive, end-to-end data protection across its entire lifecycle, from capture to movement within the enterprise, without exposing live data to high-risk environments. It protects sensitive data at rest, in motion, and in use, scaling to meet any requirement on premises and in multi-cloud hybrid IT. De-identifying data renders it useless to attackers while maintaining usability and integrity, effectively neutralizing data breaches.

[1] Ponemon Institute, *Cost of a Data Breach Report 2024*, July 2024

> “We are fully compliant with the latest financial services regulations and thanks to OpenText Data Privacy and Protection [Foundation] we achieved this in a minimally invasive manner, without having to change our existing infrastructure. We protect our sensitive data very cost effectively in a complex and distributed environment.”

Christian Stork
Head Strategic Projects, SIX

Read the full success story ›

OpenText Data Privacy and Protection Foundation is a unique, proven data-centric approach to protection—where the access policy travels with the data itself—by permitting data protection without changes to data format or integrity and eliminating the cost and complexity of issuing and managing certificates and keys. As a result, leading companies in financial services, insurance, retail, healthcare, energy, transportation, telecoms, and other industries have achieved end-to-end data protection across the extended enterprise with success in as little as 60 to 90 days, due to the minimum—in most cases zero—impact to applications and database schemas.

GDPR, CCPA, HIPAA, and PCI DSS regulations compliance

OpenText Data Privacy and Protection Foundation protects information in compliance with PCI DSS, HIPAA, GLBA, and global data privacy regulations, including the GDPR, CCPA/CPRA, KVKK, and POPI. OpenText™ It is also compatible with PCI DSS requirements on point-to-point-encryption (P2PE), enabling accelerated compliance and reduction in scope, time, and cost for PCI audits.

OpenText leads the industry as the patent holder and licensor of NIST’s AES FF1 Format-Preserving Encryption standard, a proven method for data-centric encryption used globally. OpenText ensures regulatory compliance and data breach protection, validated by FIPS 140-2 and Common Criteria. Our work with NIST, ANSI, IEEE, IETF, and security specialists solidifies our leadership and trusted advisor status across major industries.

Innovative key management and data security solutions

Stateless key management: Transparent, dynamic

Stateless key management securely derives keys on the fly as needed, once applications and users are authenticated and authorized against a centrally managed policy. This approach reduces IT costs and administrative burdens by eliminating the need for a key database and associated hardware, software, and processes. It automates supervisory or legal e-discovery requirements through simple application APIs and maximizes the reuse of access policy infrastructure by integrating with identity and access management frameworks.

Encryption and tokenization

Traditional encryption methods, such as AES 256, significantly alter data formats, requiring database schema changes. OpenText FPE, using NIST-standard FF1 mode, preserves the original format of sensitive data without sacrificing encryption strength, avoiding database and application changes. Tools for bulk encryption facilitate rapid de-identification of large data sets, protecting systems quickly and cost-effectively. OpenText Data Privacy and Protection Foundation supports high-volume needs of big data, cloud analytics, and IoT, and offers cryptographic and non-cryptographic tokenization methods.

	Tax ID 934-72-2356	**First name:** Gunther **Last name:** Robertson **SSN:** 934-72-2356 **DOB:** 08-07-1966
FPE AES-FF1 mode	**253-67**-2356	**First name:** Uywjlqo **Last name:** Muwruwwbp **SSN:** **253-67**-2356 **DOB:** 08-07-1966
Regular AES-CBC mode	8juYE%Uks&dDFa2345^WFLERG	lja&3k24kQotugDF2390^32 0OWioNu2(*872weW Oiuqwriuweuwr%olUOw1@

Deployment options

Extend your team

- On-premises software, managed by your organization or OpenText

Resources

Learn more about our data protection solutions

Visit our webpage ›

Tokens and tokenization

Read the flyer ›

Eliminate Security Gaps with Voltage SecureData Infographic

Read the infographic ›

Data anonymization with OpenText format-preserving hash

In use cases like click-stream analytics, recovering masked data may be unnecessary or undesired. Our Format-Preserving Hash (FPH) offers the same benefits as Format-Preserving Encryption (FPE)—preserving data format and referential integrity—while ensuring non-recovery of original data. This provides high-performance data usability in a non-disruptive and flexible manner, unlike traditional one-way transformations like SHA-256.

Flexible integration with major cloud services, databases, and applications

OpenText Data Privacy and Protection Integrations

Low-cost data storage, elastic computation, and diverse data analytics services are shifting big data deployments from on premises to the cloud, but this introduces additional security responsibilities. Under the shared responsibility model, cloud providers secure their services, while customers must secure their assets. OpenText™ Data Privacy and Protection Integrations ensures data is protected and usable by cloud applications, eliminating risks from misconfigured security controls, and enabling continuous data protection in multicloud environments without in-cloud decryption. Data must be protected throughout its lifecycle—at ingestion, at rest, and in use.

OpenText Data Privacy and Protection Sentry

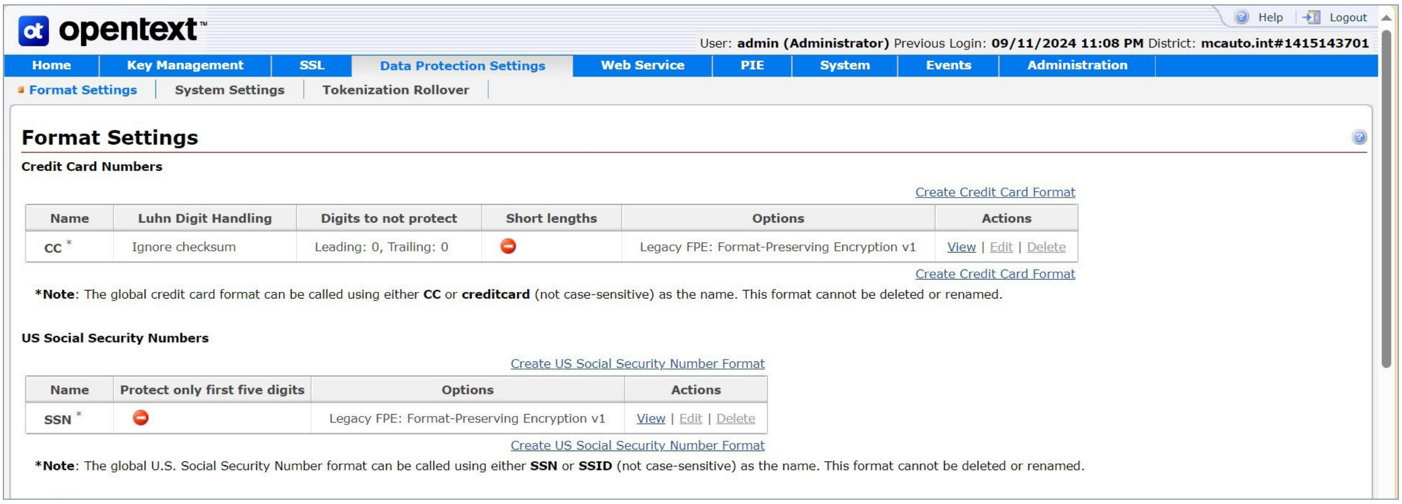
With migration to hybrid IT and an increasing reliance on SaaS applications, organizations may not have the accessibility or development resources for API-level integration. OpenText™ Data Privacy and Protection Sentry enables transparent data protection by intercepting sensitive data flowing through the network. It simplifies hybrid IT migration, accelerates time to value by quickly enabling security compliance, and offers consistency for end-to-end data protection, without having to break open applications and extensively re-qualify IT architectures.

OpenText Data Privacy and Protection Foundation Integrations includes:

- 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®, IBM DataStage®, Ab Initio®, and others.
- Streaming platforms, such as Apache Kafka®, Apache NiFi®, Apache Storm®, StreamSets®, and cloud streaming services such as AWS Kinesis®, Azure Event Hubs®, 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®, Amazon Aurora®, Amazon DynamoDB®, Azure SQL Database®, Azure Cosmos DB®, Google Cloud SQL™, and others.

The OpenText Data Privacy and Protection Foundation platform offers unparalleled flexibility and scalability, ensuring high availability and performance across multicloud hybrid IT infrastructures. Whether deploying virtual appliances or cloud-native, containerized microservices within Kubernetes clusters, OpenText meets the most demanding enterprise requirements. This flexibility allows customers to tailor their data protection strategies to diverse environments, avoiding the costs and complexities of managing multiple products. OpenText stands out by providing a comprehensive, adaptable solution that addresses varied use cases efficiently and effectively.

Product capabilities	Description
Data protection	Safeguards data and information to preserve its confidentiality (privacy), integrity, and availability.
Format-preserving encryption	Encrypts structured data by integrating datatype-agnostic encryption into legacy business application frameworks without altering the data format.
Tokenization	Replaces sensitive data with unique identification symbols that retain all essential information about the data without compromising its security.
OpenText Format Preserving Hash (FPH)	Offers full data anonymization while maintaining the benefits of other OpenText tokenization technologies, such as structure, logic, partial field application, and usability for use cases like click-stream analytics.
Secure stateless tokenization	Delivers advanced data security without token databases, dramatically improving speed, scalability, security, and manageability over conventional, first-generation, and PCI DSS tokenization solutions.
OpenText Data Privacy and Protection Sentry	A cloud data protection gateway that addresses data protection for SaaS and commercial off-the-shelf (COTS) applications.
OpenText Data Privacy and Protection Integrations	Ensures persistent protection of sensitive data across multi-cloud, hybrid, and on-premises environments. By embedding data-centric security throughout hybrid IT, it reduces the risk to sensitive data and accelerates safe migration to cloud environments.
OpenText Structure Data Manager	For data management use cases, such as Test Data Management, application retirement, and data archiving.
Secure and compliant test data management	A single integrated platform to discover, extract, transform, protect, and make test data available for consumption.



User: **admin (Administrator)** Previous Login: **09/11/2024 11:08 PM** District: **mcauto.int#1415143701**

Format Settings

Credit Card Numbers

Create Credit Card Format

Name	Luhn Digit Handling	Digits to not protect	Short lengths	Options	Actions
CC *	Ignore checksum	Leading: 0, Trailing: 0	⛔	Legacy FPE: Format-Preserving Encryption v1	View | Edit | Delete

Create Credit Card Format

***Note**: The global credit card format can be called using either **CC** or **creditcard** (not case-sensitive) as the name. This format cannot be deleted or renamed.

US Social Security Numbers

Create US Social Security Number Format

Name	Protect only first five digits	Options	Actions
SSN *	⛔	Legacy FPE: Format-Preserving Encryption v1	View | Edit | Delete

Create US Social Security Number Format

***Note**: The global U.S. Social Security Number format can be called using either **SSN** or **SSID** (not case-sensitive) as the name. This format cannot be deleted or renamed.

OpenText Data Protection Settings for encrypting credit card and Social Security numbers with customizable options.