opentext™

PRODUCT OVERVIEW

OpenText Protect

Protect sensitive data with tokenization to reduce the risk of data breaches and lower the cost of compliance

- Reduce the number of systems in scope of compliance audits by **up to 98%**
- Achieve average response times of fewer than **30 milliseconds** per tokenization request
- Maintain the length and format of original data with **format-preserving tokenization** to ensure interoperability with existing systems

Many enterprises process sensitive data, such as payment card information, personally identifiable information and personal health information, which needs to be protected to ensure compliance with applicable standards and regulations. Organizations must also effectively manage the reputational and monetary risks associated with potential data breaches.

Managing risks regarding sensitive data and maintaining compliance across the enterprise requires specialized skills and is often costly and time-consuming. OpenText™ Protect™ enables tokenizing any type of sensitive data, allowing companies to reduce the number of systems that process it in an unprotected format. This reduces the footprint of sensitive data in enterprise systems, lowering the risks associated with data breaches and the cost of compliance audits. In addition, making sensitive data safe to share across the organization introduces opportunities for data analytics without adding risk.

Tokenization replaces sensitive data with surrogate values

Tokenizing data means replacing field-level data values with surrogate values that, unlike encrypted data, have no mathematical connection to the original values. This means that the protection provided by tokenization cannot be broken without access to the separately held token-value pairs, rendering the tokenized data meaningless by itself. As a result, any data that is tokenized is not considered sensitive.

Reducing risk and cost of compliance

Due to the level of protection that tokenization provides, any system that processes sensitive data in tokenized format is not considered to be within the scope of compliance audits, such as PCI DSS. By reducing the number of systems that need auditing, Protect can significantly lower the costs of maintaining compliance and performing mandatory audits.

Flexible features for tokenizing various kinds of sensitive data

Protect provides a tremendous amount of flexibility in how data is tokenized, which supports a broad variety of use cases, from reducing the scope of compliance audits to making sensitive data safe for analytics purposes.

Format-preserving tokenization

Any data values that have a standard length (credit card numbers, social security numbers, account numbers) can be tokenized using format-preserving tokens that maintain the format and length of the original data values, meaning the existing back-end systems and analytics tools can process the tokens without need for system changes. Data values with variable length (names, addresses etc.) can be tokenized using randomized numeric, alphabetic or alphanumeric tokens that conform to the desired formatting rules.

Referential integrity of tokenized data

Protect enables 1:1 referential integrity between tokens and the original data, so that tokens that are unique to the original data values can be created and retained. For example, these kinds of tokens can be used as unique identifiers for customers or other entities in enterprise systems instead of credit card or account numbers, enabling companies to expand the use of this data for analytics and other purposes without adding risk. Data values where 1:1 referential integrity is not suitable (for example, names or salary information) are tokenized without this relationship.

Advanced integration capabilities

Protect leverages the OpenText Cloud platform's any-to-any integration capabilities and can therefore take in sensitive data from any source and pass it on as tokens to any application or system. This makes enterprise data processing highly flexible, as challenges related to sensitive data can be addressed as part of the integration workflow.

Secure sensitive data while maintaining its usability

The flexibility of Protect makes it ideal for protecting sensitive data while maintaining its usability for analytics and business processes. Most systems do not readily process encrypted data values without costly changes, while anonymizing the data by redacting or removing sensitive values leads to losing these insights altogether. With tokenization, sensitive data values are secure, while authorized parties can reconstruct the original data if needed.

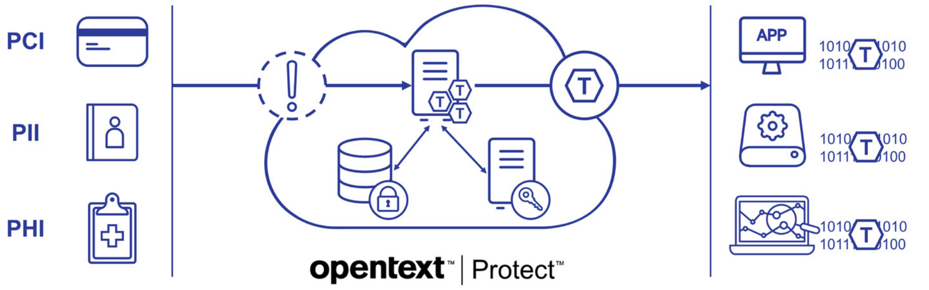
Leverage managed services for end-to-end solution delivery

OpenText provides Protect as a managed service, offering an end-to-end solution for protecting sensitive data. This includes everything from Professional Services expertise required to design and implement the solution to managing and maintaining the availability and performance of the day-to-day tokenization services on the OpenText Cloud Platform.

- Professional Services
- Managed Services

Keep up to date

Learn more



Protect can substitute any sensitive data values stored in an application with tokens and seamlessly integrate into existing business processes. It encrypts the original data value and stores the cipher text in a secure data vault, whereas the token is passed on and used as a surrogate for the real data.

OpenText Protect data tokenization features	
Vault-based tokenization	Leverages a highly-secure data vault for storing the token-value relationships, meaning that no mathematical connection exists between the two
Format-preserving tokens	Supports format-preserving tokenization that allows maintaining the length and format of the original data, enabling existing systems to process the tokens as if they were the original data values
1:1 referential integrity of tokenized values	Supports 1-to-1 referential integrity of field-level data, so that unique tokens can be created to represent the unique original data values, such as credit card, account or social security numbers, enabling the tokens to be used for analytics, identification and other purposes in place of the original sensitive data
Portability of tokens	Provides portability of the token-value pairs and enables importing tokens from other tokenization solutions, for example, in case of mergers and acquisitions
TTL (Time to Live) capabilities	Includes TTL (Time to Live) capabilities that auto-delete encrypted data and tokens after a predetermined amount of time
Key management	Provides centralized key lifecycle management for managing the encryption keys for the data vault
Secure web UI	Provides the option to leverage a secure web UI for revealing the original values behind tokens and where required, this highly controlled access to the original values enables authorized users to perform tasks, such as fraud prevention and investigation
High performance	Leverages best-of-breed NoSQL solutions for high-volume, high-speed handling of requests, achieving average response times of fewer than 30 milliseconds per request (not including network latency)
Compliance	Complies with multiple global industry and government data regulations (for example PCI DSS, HIPAA and SOC 2)

opentext.com/contact