BLUE COAT®

Network
+ Security
+ Cloud

Cloud Data Protection Gateway Tokenization

SOLUTION BRIEF

Maintaining Control over Data in the Cloud

Regional and industry regulations are designed to ensure organizations are taking appropriate precautions when handling and storing sensitive data and personally identifiable information (PII). These regulations typically require organizations to maintain control over the data at all times and, in the case of regional mandates, store that data within a defined border. As organizations look to adopt cloud platforms and services, which are managed by a cloud provider, with data centers around the world that are outside of the enterprise's direct control, they must consider how to retain data sovereignty and residency to adhere to relevant regulatory requirements. Enterprises can use tokenization, which replaces data with a surrogate value, so that it has no extrinsic meaning if that data is stolen or intercepted. As a result, organizations can maintain control over their sensitive data when using cloud services.

Requirements for Effective Tokenization

Tokenization substitutes a sensitive plain text data field with a surrogate value, called a token, which has no extrinsic meaning. The reverse process, de-tokenization, replaces the token with its associated plain text information. Transmitting, storing and processing tokens in the cloud, instead of the original data, ensure sensitive information never leaves the organization's domain and control.

Tokenization is recognized as a best practice for securing data, helping organizations adhere to industry regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Biley Act (GLBA), the Payment Card Industry Data Security Standards (PCI DSS), manufacturing's International Traffic in Arms Regulations (ITAR), and the Criminal Justice Information Services (CJIS) requirements.

When selecting tokenization, organizations should look for solutions that are truly secure and have been validated by independent, third parties. Some "masking" systems tokenize only part of a string, which significantly weakens the security they provide; organizations need tokenization technologies that replace the entire data string with randomly generated values that cannot be traced to the original data. They should also look for solutions that offer granular controls to ensure the capabilities meet the unique needs of the organization and don't impact the experience of the end-user to maximize the benefits that can be derived from cloud services.

The Difference between Encryption and Tokenization

While encryption can be used to obfuscate a value, a link back to its plain text form still exists, tokenization, on the other hand, completely removes the original data from the systems in which the tokens reside. Encryption is typically used by enterprises to protect the privacy of data, while tokenization is often deployed to address compliance or policy requirements that impose strict guidelines on data sovereignty and residency. The Blue Coat Cloud Data Protection Gateway gives enterprises the flexibility to use both tokenization and encryption to meet their varied data protection needs.

AT-A-GLANCE

PROBLEM

Maintaining control over data when it traverses or is stored in the cloud to adhere to regulatory data residency requirements

SOLUTION

The Blue Coat Data Protection Gateway's Tokenization

BENEFITS

- **Strong Security** – offering tokenization that has been validated by a third-party for compliance with regulatory requirements
- **Granular Control** –allowing organizations to dictate exactly how data will be transmitted and stored in the cloud
- **Seamless User Experience** – enabling users to do all they need to do in the cloud, securely

BLUE COAT

Network
+ Security
+ Cloud

SOLUTION BRIEF

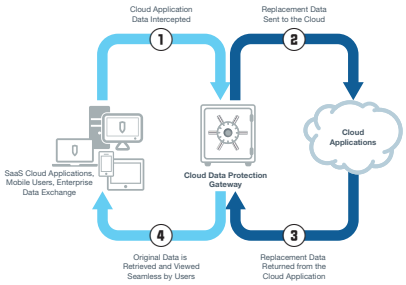
Blue Coat Tokenization – Cloud Data Protection Gateway

The Blue Coat Cloud Data Protection Gateway enables organizations to define data protection policies that govern exactly how they want their sensitive data to be secured and protected when stored in cloud applications. Blue Coat tokenization ensures organizations retain complete control over their information to address data residency requirements, keeping data local, while enabling tokens to be stored and processed in the cloud.

The Cloud Data Protection Gateway gives enterprises the ability to monitor and discover how cloud applications are being used within the organization and take steps to protect and secure sensitive data, ensuring it never leaves an enterprise's control.

Strong Security

Blue Coat tokens are randomly generated strings of characters, with no mathematical or logical associations to the clear text data they replace. As randomly-generated and arbitrarily assigned values, knowing the clear text value of a single token would provide an adversary no insight to the value of any other token.



The Cloud Data Protection Gateway gives enterprises the ability to monitor and discover how cloud applications are being used within the organization and take steps to protect and secure sensitive data, ensuring it never leaves an enterprise's control.

Blue Coat generates and assigns a new token for each unique piece of data that it receives within a defined token space, based on a sequence. In the case of long text data type fields, Blue Coat generates a single token for the entire string, not a token for each unique word in the string, ensuring there are no links to the original data. As a result, Blue Coat tokens cannot be returned to their corresponding clear text values, without access to the original "look-up" table that matches them to their original values. These tables are typically kept in a database in a secure location inside an organization's firewall.

3rd Party Assessment and Validation

The Blue Coat Cloud Data Protection Gateway's tokenization has been assessed by Coalfire™, a 3rd Party PCI DSS QSA and FedRamp 3PAO, for compliance with the PCI DSS tokenization standards. Key findings from the report include:

- Blue Coat tokens were observed to have no relation to the data for which the token was generated. Tokenization conforms to the PCI SSC Tokenization Guidelines.
- All tokenization components were located on secure internal networks that are isolated from any untrusted and out-of-scope networks.
- Only trusted communications were permitted in and out of the tokenization system environment.
- The tokenization solution enforced strong cryptography and security protocols to safeguard cardholder data when stored and during transmission over open, public networks.
- The tokenization solution implemented strong access controls and authentication measures in accordance with PCI DSS Requirements 7 and 8.
- The tokenization system components are designed to strict configuration standards and are protected from vulnerabilities.
- The tokenization solution supports a mechanism for secure deletion of data as required by a data-retention policy.
- The tokenization solution implements logging, monitoring, and alerting as appropriate to identify any suspicious activity and initiate response procedures.

Granular Control Over Data Protection

The Gateway gives organizations complete flexibility and control over how their data is protected. The Gateway allows organizations to select, on a field-by-field basis, whether to:

- allow data to remain in clear text
- encrypt data
- replace data with a token, so sensitive data never leaves the organization's control

In this way, enterprises can be confident they have the protection capabilities in place to safely adopt cloud services.

Seamless User Experience

The Blue Coat Cloud Data Protection Gateway preserves all the cloud application's functionality, allowing users to seamlessly access, search and sort protected data from their favorite cloud services. End users can still perform operations on data that has been tokenized in the cloud, due to the innovative capabilities of the platform.

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000