BLUE COAT®

Network
+ Security
+ Cloud

Cloud Data Protection Gateway Encryption

SOLUTION BRIEF

Protecting Data in the Cloud

Enterprises need to ensure corporate data remains private and secure. This is increasingly challenging, as more and more information traverses or is stored in environments, such as wireless networks and public clouds, that are outside of the direct control of the enterprise. To maintain the integrity and security of their data, enterprises can use encryption, which transforms plain text information into a non-readable form, so it cannot be understood if stolen or intercepted by an unauthorized user. As a result, enterprises can confidently support the access and storage of data in public networks, without putting the privacy or security of that data at risk.

Requirements for Effective Encryption

Encryption is an obfuscation approach that uses a cipher algorithm to mathematically transform plain text information into a non-readable form, called ciphertext. The reverse process, decryption, decodes the ciphertext back into plain text. To ensure only authorized users can read the content, the mathematical algorithm requires a secret value, called a key, in order to encrypt or decrypt the data properly. When selecting encryption, enterprises should consider the strength of the cryptography and their key management:

Encryption Strength

Enterprises have choices when it comes to the strength of their encryption solutions. In the U.S., one of the most rigorous standards is the federal government's FIPS 140-2. Many enterprises now follow this standard because of its maturity and strong level of encryption. To provide a "FIPS mode" that adheres to FIPS 140-2's multiple levels of security, a solution must be validated, which means it:

1. Uses an approved algorithm
2. Handles the encryption keys appropriately
3. Handles the data to be encrypted in a certain way – with a certain block size, a certain amount of padding, and some amount of randomness - so the ciphertext can't be searched

Unfortunately, many solutions are unable to deliver on the FIPS 140-2 standard, without disrupting the functionality of the cloud application or affecting the overall user's experience. Enterprises should look for solutions that offer a FIPS mode that doesn't impact the ability to search or sort data, so users can easily and securely do what they want to do within their cloud applications.

Key Control and Management

Another important consideration for enterprises looking to deploy encryption surrounds the ownership of the encryption keys. According to the Cloud Security Alliance it is important the enterprise retain control of encryption keys and maintain separation of duties between the enterprise and cloud provider who is hosting the data. This "provides the greatest protection, both against an external breach of the service provider, as well as an attack originating from a privileged user/employee of the provider. Additionally, this segregation of duties prevents the cloud provider from unauthorized disclosure of customer data, such as compliance with a

AT-A-GLANCE

PROBLEM

Protect the privacy and integrity of corporate data as it traverses or is stored in networks outside an enterprise's control

SOLUTION

The Blue Coat Data Protection Gateway's Encryption

BENEFITS

- **Strong Security** – supporting a variety of encryption standards, including FIPS 140-2.
- **Granular Control** – providing ensuring enterprises retain control over key management and dictate exactly how data will be transmitted and stored in the cloud
- **Seamless User Experience** – enabling users to do all they need to do, securely

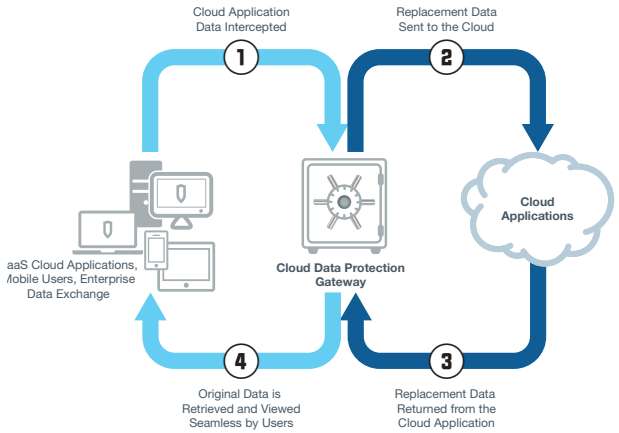
BLUE COAT

Network
+ Security
+ Cloud

SOLUTION BRIEF

subpoena, without the customer's knowledge or approval. The customer should retain complete control over their data and only they should be able to comply with disclosure requests."

Management of encryption keys can be a complex process. Key rotation involves changing keys periodically to reduce the amount of harm that can be done if a key is compromised. When working with keys, enterprises need to define related policies around how often should the keys be rotated? What should be done about data that was encrypted with an old key? Should it be decrypted and re-encrypted with a new key? Where should old keys be stored, and for how long? These sorts of questions need to be addressed and re-assessed on an ongoing basis when employing encryption on sensitive data.



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.

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 encryption and tokenization to meet their varied data protection needs.

Blue Coat Encryption – Cloud Data Protection Gateway

The Blue Coat Cloud Data Protection Gateway enables enterprises to define data protection policies that govern exactly how they want their sensitive data to be secured and protected when stored and processed in public, cloud applications. Blue Coat leverages a connector framework (Crypto Connectors) that supports a wide array of publicly available encryption modules, including those that are FIPS 140-2 certified. With Blue Coat, enterprises are assured the encryption they deploy meets their stringent security and regulatory requirements, while enabling them to maintain the overall functionality of the cloud applications they are using and deliver a satisfactory user experience.

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 - FIPS 140-2 Encryption

Blue Coat is the only cloud data protection vendor that provides a FIPS mode with validated FIPS 140-2 encryption modules that is able to preserve all the cloud application's functionality. By enabling the use of a validated FIPS 140-2 module to protect cloud data, Blue Coat eliminates the security, compliance and usability barriers that previously prevented enterprises and government agencies from moving to the cloud.

Granular Control over Data Protection

The Gateway gives enterprises complete flexibility and control over how their data is protected. Enterprises retain control over encryption keys. The Gateway also enables enterprises to select, on a field-by-field basis, whether to:

- allow it to remain in clear text
- encrypt it
- replace it with a token

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

Seamless User Experience

Because Blue Coat is algorithm-agnostic, the Gateway does not depend on any proprietary encryption schemes or "Searchable Encryption". As a result, the Gateway preserves all the cloud application's functionality, allowing users to seamlessly access, search and sort protected data from their favorite cloud services.

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

© 2016 Blue Coat Systems, Inc. All rights reserved. Blue Coat, the Blue Coat logo, BlueTouch, CacheFlow, CloudSOC, ContentIQ, Elastica, IntelligenceCenter, PacketShaper, Perspecsys, PolicyCenter, ProxyOne, ProxySG, StreamIQ, and WinProxy are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only. Blue Coat makes no warranties, express, implied, or statutory, as to the information in this document. Blue Coat products, technical services, and any other technical data referenced in this document are subject to U.S. export control and sanctions laws, regulations and requirements, and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws, regulations and requirements, and acknowledge that you have the responsibility to obtain any licenses, permits or other approvals that may be required in order to export, re-export, transfer in country or import after delivery to you. v.SB-CDPG-ENCRYPTION-EN-v1d-0816