BLUE COAT®

Network
+ Security
+ Cloud

TOP 5 QUESTIONS ANSWERED ON HOW TO BEST PROTECT YOUR DATA IN THE CLOUD

SOLUTION BRIEF

The number of successful cyber-crime attacks per year, per company has increased 46% over the last four years.[1] Given this backdrop, it's not surprising the overall market for security products and services is growing globally, with cloud-based security leading the charge.[2] As more and more organizations adopt cloud services, it is important a consistent level of security is maintained to keep data safe. While there is no silver bullet, there are some basic cloud security components that form the foundation of a successful plan. The following are the top five questions you should consider as you formulate your cloud data security strategy.

Question #1: When enterprises move from on-premises to cloud-based applications, what do we need to consider?

The Answer: Data Compliance

You need to understand how the adoption of cloud services can impact your ability to comply with relevant industry regulations and regional requirements around how sensitive data can be handled and stored. Depending on the industry, there are a host of regulations that cover how data must be protected, such as the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, the financial industry's Gramm-Leach-Biley Act (GLBA), the Payment Card Industry Data Security Standards (PCI DSS), manufacturing's International Traffic in Arms Regulations (ITAR), and the government's Federal Information Security Management Act (FISMA), Criminal Justice Information Services (CJIS) requirements. In addition, many countries have their own cloud data regulations and laws that may require you to retain data sovereignty and residency (i.e. regulated data cannot cross a country's physical border).

It is important to understand what data compliance regulations and standards you need to adhere to and identify the data-centric security tools you can use, which work both inside and outside of your firewall, to effectively protect regulated data. For example, encryption and tokenization are often used to enable organizations to safely adopt cloud services, while maintaining compliance with strict, complex data regulations.

Question #2: What is the first step we should be taking to secure cloud services?

The Answer: Cloud Access Security Broker (CASB)

Maintaining control over sensitive data can be difficult when you move to the cloud; a cloud access security brokers (CASB) can help you retain control and safely adopt cloud services to support your business. Gartner has defined CASB as "on-premises or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed[3]."

CASBs can take different forms, but a well-planned data privacy and protection program should always incorporate CASB capabilities. No matter what stage of cloud adoption your enterprise is in, you should vet the different CASBs available to ensure you can deploy the one that best meets your key security needs, which may include attaining visibility into cloud usage, adhering to regulatory requirements, achieving data residency or extending internal security best practices.

Question #3: What do you need to consider when regulations require you to maintain control over the location where regulated data and documents physically reside?

The Answer: Data Residency

Data residency (also called data sovereignty) refers to the physical location of where data actually resides. With the adoption of the

Network
+ Security
+ Cloud

cloud, the residency of data used and stored by the service is outside of your enterprise's domain; ultimately it is determined by the cloud service providers (CSPs), who may have data centers all over the world.

This means, you need to ensure regulated data is appropriately handled and stored to comply with data residency requirements, which may dictate data remain within a defined border (often within the country of origin). As you adopt cloud services, you need to consider the rules that cover the handling of data in each of the jurisdictions in which you operate. Restrictions around data residency may make it more challenging for you to adopt certain cloud applications; however, there are solutions (such as tokenization) that can be used to maintain data residency, despite the location of the CSP the enterprise selects.

Question #4: How can we protect the privacy of our data in the cloud?

The Answer: Encryption

Encryption can be used to protect information in transit and storage, within networks, the Internet and mobile and wireless systems. It uses an algorithmic scheme to transform plain text information into a non-readable form, called ciphertext. The reverse process, decryption, decodes the ciphertext back to plain text. To prevent unauthorized access to plain text data, the mathematical algorithm requires a secret value, called a key, to encrypt or decrypt the data properly.

In the cloud, encryption algorithms are used to protect outgoing data, so information is not vulnerable once it's left the enterprise's direct control. Data encryption is an essential cloud data security tool for organizations using popular SaaS applications; it is commonly used to achieve compliance with industry regulations, including the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standards (PCI DSS).

Question #5: How can we protect and maintain data residency when we use cloud applications?

The Answer: Tokenization

Tokenization is recognized as a best practice for securing sensitive data at rest, in transit and in the cloud; it enables enterprises to adhere to relevant data privacy and residency requirements. 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. Tokenization ensures organizations retain complete control over their information, keeping data local, while enabling tokens to be stored and processed in the cloud.

You may be wondering how tokenization differs from encryption. With tokenization, the original data is completely removed from the systems in which the tokens reside, while encryption maintains a link between the data it has obfuscated and its unencrypted form. Tokenization tends to be more flexible in its length and format, compared to traditional encryption techniques, allowing tokens to be generated that have no relationship to the length of the original value. Additionally, tokens cannot be returned to their corresponding clear text values without access to a secured "look-up" table that matches them to their original values.

Learn more about Blue Coat Cloud Data Protection.

[1] "2015 Ponemon Institute of Cyber Crime Study," Ponemon Institute, 2015, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/.

[2] ???

[3] http://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs

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