BLUE COAT

Network
+ Security
+ Cloud

DON'T GET LOST IN THE CLOUD

10 Tips for Protecting Data in the Cloud

SOLUTION BRIEF

With information flowing more freely than ever before in today's digital economy, tracking sensitive data has become increasingly difficult. In fact, findings show more than half of IT professionals admit they do not have a complete picture of where their sensitive data lives.

As organizations adopt cloud services, putting more and more of their data in the hands of outside, third-party cloud service providers, the challenges associated with maintaining visibility and control over their sensitive and regulated data is only going to expand exponentially. Within outsourced environments, such as SaaS cloud applications, organizations have little to no control over how their information is stored or moved within the cloud provider's data centers or how it flows to the systems of the cloud provider's partners.

It is due to concerns around privacy and security that organizations are hesitant to use the cloud as much as they may want. Despite spending projections (IDC forecasts that public IT cloud services will account for more than half of global software, server and storage spending growth by 2018), organizations have been holding back, limiting the true transformational benefits the cloud could bring.

Relying on a cloud service provider for data compliance and protection is not enough. On the flip side, writing off cloud services because of security skepticism is unnecessarily limiting and harms the business. Enterprises need to consider encrypting or tokenizing any sensitive data before it goes to the cloud, so they retain full control of their information while it is in-transit, stored (at-rest) and in-use (being processed) in the cloud.

10 tips to maintain control over your data in the cloud

1. Ask cloud providers and developers, who are configuring the virtual networks on cloud platforms, how the **network is designed**, so you can gain assurance that your data isn't just being thrown willy-nilly into a "cloud," according to Forrester.
2. Get familiar with data-centric security tools that work both inside and outside your company's walls, in particular **cloud data encryption**.
3. When it comes to the encryption of data at rest in a cloud environment, pay attention to **who owns the keys** and where the keys physically reside. Retaining the keys enables you to retain control over the security of the data.
4. Develop a security platform that allows you to implement a consistent policy across **multiple cloud services**, preferably one that does not involve complex key management.
5. Don't forget data in-use. **Data in use** is the data that has been loaded into a process and is in the memory of the running program. In general, this data is in the clear while it's being processed, which typically means it is not protected by any cloud-based encryption provided by the cloud service provider. Make sure you own the entire encryption process of this data.

SOLUTION BRIEF

6 Consider **tokenization** as a means of protecting cloud data. Tokens replace original plain text data with surrogate values before it leaves your organization, so the sensitive information always remains within your domain or control. The replacement values have no mathematical relationship to the original clear text, so the token can't be reversed to reveal the original data if it is intercepted or stolen. The only place you can translate a secure token back to its original value is within a secure token vault, which is always under the enterprise's full control.

7 Control the **mobile data flow**. Don't forget to protect the data that is accessed by your employees' mobile devices (BYOD). Often, this data bypasses desktops and is processed and stored exclusively on these mobile devices or in the cloud. You need to take measures to ensure your enterprise data on these devices and in the cloud isn't "over-exposed."

8 **Preserve cloud application functionality.** When choosing a cloud security solution, be sure to select one that doesn't compromise user functionality. You want to be able to maximize the benefits you can derive from the cloud/SaaS offering, while still maintaining the strongest possible security and data control.

9 Understand what **legal and regulatory data compliance** requirements exist for the types of data being stored in the cloud. Understand whose responsibility it is to ensure relevant legal and regulatory data compliance and privacy laws are addressed.

10 Look at your business **contracts**, how you share data with your business customers, and the types of information exchanged. There may be requirements to treat sensitive information and intellectual property in certain ways, especially in cloud/SaaS environments. In addition, if you are in a regulated industry, such as banking and healthcare, you need to adhere to the restrictions and protections that undoubtedly apply.

Learn more about Blue Coat Cloud Data Protection.

BLUE COAT®

Network + Security + Cloud

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