VERISTOR

DON'T ASSUME YOUR DATA IN THE CLOUD IS ALWAYS SAFE

(it just ain't so)

Many businesses continue to turn to public, private and hybrid cloud providers to scale and augment the IT services they provision from their on-premises servers. Yet when businesses send data to the cloud for processing, the cloud provider secures the data only within certain boundaries. While many businesses don't realize this, end-to-end security is still their responsibility.

This is a bit ironic since security is one of the most popular reasons why businesses turn to the cloud. There's the perception that cloud providers must be extremely diligent, comprehensive and up-to-date with their security measures. In reality, only a third of sensitive data stored in cloud-based applications is encrypted.[2] And despite their increasing reliance on the cloud for processing, many companies do not adopt appropriate governance and security measures when it comes to these workloads.

Sixty Percent of Business and Tech Decision-Makers Say the Cloud Is a High or Critical Priority.[1]

The Ponemon Institute report—The 2016 Global Cloud Data Security—cites a survey of IT practitioners in which 54 percent said their companies do not take a proactive approach in managing security and complying with privacy and data protection regulations in their cloud environments. This is despite the fact that 65 percent say their organizations are committed to protecting confidential or sensitive information in the cloud.

Why cloud environments are not always secure

Cloud environments are not the safe haven many think they are for a variety of reasons. The vast amount of data stored on cloud servers makes them an attractive target for cybercriminals. Data breaches and other attacks frequently succeed from the result of weak authentication protocols and ineffective passwords.

In addition, many cloud providers rely on APIs, which are open to exposure from hackers because they're usually accessible from the Internet. And when an exploitable bug gets into a multi-tenancy cloud environment, it can quickly spread to the other customers who share the infrastructure.

While rare, malicious hackers have also been known to permanently delete cloud data. Unless the data is backed up to another data center, it's gone forever. Cloud data centers are also just as vulnerable to natural disasters as any facility. Without redundancy and failover capabilities, operations can't be restored.

How to protect your data in the cloud

To ensure your organization's data is protected at all times—as sensitive data is uploaded to, stored in and downloaded from your cloud environments—Veristor recommends several cloud security measures. Our team of experts has worked together with numerous businesses to develop these measures to help you solve your cloud security challenges.

Some of the measures involve actions you can take internally while others require verifying the policies and standards of your cloud provider. Doing so will give you confidence that your sensitive data is compliant and secure:

- **End-to-End Visibility and Control:** Ideally, you should be able to view the status of all your enterprise assets in the cloud via a single console view. This gives you quick and easy visibility into your platform provider's performance and enables you to analyze security control reports. Access control policies should enforce cloud authentication to eliminate the threat from insiders and ensure access is available only to authorized users.
- **Regulatory Compliance:** Many compliance regulations impact data security and handling in the cloud. Make a list of your government and industry regulatory requirements, identify your critical data and then ensure your cloud platform complies.
- **Policy Enforcement:** The same security policies you enforce on-premises should also be in play across your cloud environments—especially as you add new workloads to the cloud. Document these policies and evaluate your cloud platform accordingly.
- **Right to Audit:** Ensure that the SLA with your cloud provider gives you the right to audit their security measures and that the provider agrees to comply with auditing standards, such as SSAE 16.
- **Data Classification:** Use a standard to classify data and then provide that classification to your cloud provider so they can properly protect the data. A good data classification schema specifies which data should be protected in transit, at rest and in use. The method of protection will more likely be a platform-specific decision using a centralized policy-driven approach that supports multiple data-protection options. Data that will be protected should be defined in your organization's data security policy according to industry or regulatory compliance mandates.
- **Data Encryption/Tokenization:** Include encryption in your SLA and clarify where it will be used—for data at rest, in transit or preferably both. Also note who will maintain the encryption keys and how they can be accessed when necessary. Another standard to apply is tokenization, which allows you to set boundaries and policies that manage strict data residency requirements while also preventing sensitive data from being exported across geographical lines

- **Immediate Protection for New Workloads:** A new cloud workload can be deployed in a matter of seconds. If they are not protected as soon as they are created, you are left vulnerable to breaches and leaks.
- **Shadow IT Detection and Elimination:** Given the ease at which employees can stand up cloud workloads, and the lack of security governance when they do, it's imperative to discover shadow IT initiatives and remediate them as they are found.
- **Employee Training:** Despite the measures you apply, employees who are unaware of potential threats can open your cloud environment to attacks. Create security awareness among your employees on how to recognize and handle malicious emails and website links, and keep them informed about the security risks of shadow IT.
- **Breach Protocol:** Security breaches are always a possibility, and cloud-based services are often viewed as soft targets by hackers. Document in your contract both the support that will be provided and protocols that will be used by the cloud provider in case a security breach occurs. And don't forget to specify if and how much you will be compensated should a breach occur. It's a good idea to include this information in your Cyber Incident Response Plan
- **Business Continuity:** Ask to see the business continuity plan that guarantees the continuation of services in case the cloud provider's data center is hit by a disaster. Ideally, your location, the cloud provider's main data center, and their back-up data center should not be too closely located to ensure all three locations can't be hit by the same disaster.
- **Dedicated Servers:** Another key factor in protecting your data is to designate in your cloud provider SLA that you want dedicated servers to host your data and applications—rather than shared servers that also store other customer applications and data. While you may pay more for disk space, processing power and band-width, dedicated servers give you the security and privacy you need.
- **Due Diligence:** Before you sign a contract, check your service provider's track record. Also ask to talk with current customers. Make sure the provider is not likely to temporarily or permanently shut down. And to protect yourself in case they do need to shut-down, verify the process for returning data and workloads to you in their original format and permanently eliminating the data from their environment.

It's still worth banking on the cloud computing model

These protective measures should not discourage you from taking advantage of all the benefits that the cloud has to offer. As long as you do your homework and make sure you and your cloud provider have all the security bases covered, you can successfully leverage the cloud to improve business agility and accelerate new service roll-outs—while also controlling your IT costs and paying only for the compute resources you consume.

To learn more about protecting your data in the cloud, visit **veristor.com.**

1. "Market Overview: Cloud Workload Security Management Solutions — Automate Or Die," Forrester Research, 2 June 2015.
2. "Cloud security data still pose challenge for many companies: study," Deccan Chronicle, 26 July 2016.