PROTECTING YOUR DATA IN THE CLOUD

People are routinely abandoning traditional file storage systems for modern, cloud-based systems. Cloud adoption has accelerated IT modernization thanks to:

- Simplified scalability
- Reduced costs
- The flexibility to transform IT models based on evolving business requirements

It's not all good news. Cloud adoption has disrupted traditional security models, which were designed to secure data and apps operating via on-premises servers. Protecting your data stored in the cloud—that's an entirely different situation.

With the worldwide increase in remote work, organizations have come to rely on cloud vendors even more heavily. This uptick in cloud computing and cloud storage has also opened myriad opportunities for cyber criminals and bad actors to attempt to access and corrupt our data.

The users of cloud, though? We're a little in the dark.

Customers tend to assume that vendors are doing everything necessary to keep their data safe in the cloud, and they are—to a point. Unfortunately, the nature of keeping data in the cloud means that information is more susceptible to breaches, no matter how tight the security is on the vendor's end.

Customers are directly responsible to ensure that their own data is always available, protected, and recoverable. Just like when you use an external hard drive, you may trust the manufacturer, but you

still put your own measures in place to prevent the hard drive from being damaged, lost, or stolen.

How to protect cloud data

An effective data security protection program for cloud environments can include the following strategies and best practices:

Plan for security

Define the unique security profile for various cloud environments deployed or proposed for your organization. The process may begin from defining the scope and boundaries of the infrastructure requirements, leading to the definition of an Information Security Management Systems (ISMS) policy for anything cloud-bound:

- Data assets
- Applications
- Processes

Understand the various deployment models in context of your risk tolerance, security, and compliance considerations as well as potential risk exposure to data, apps, processes and end-users. Map the data flows between your organization, cloud environments, and end-users to determine the appropriate security protocols and control frameworks for each workload. This information will enable IT to support the diverse security needs of multiple data sets, services, and tools required to protect sensitive data. Further management approval would also be required to account for the residual risk that may appear despite the security controls in place.

For different cloud solutions, it's important to work with the vendors to understand the true requirements of the shared security responsibility model.

Mitigate vulnerabilities

For dynamic cloud architecture models, the perimeter of security controls may deviate and require organizations to take additional measures in protecting their assets in the cloud. It is important to understand that cloud networks are not physically separated and isolated like the traditional on-premises network infrastructure. Organizations must build security from the ground up, extending security across all layers of the network that may evolve over time.

The following controls and best practices can help mitigate risk associated with the cloud-bound assets:

- **Encrypt the data at rest, in process, and in transition between the networks.** Encrypting at each point of contact helps to reduce the opportunities for a breach. Healthcare, defense, and governmental institutions should enforce stringent encryption requirements for data security in cloud environments, as they deal with particularly sensitive information.
- **To protect data at rest, manage access privileges to limit access to confidential information.** Employ the principle of least privilege that allows users the bare minimum controls over the data as necessary. Extend these controls to prevent data integrity compromise, through resource permissions, data integrity checks, backup, replication, and versioning.
- **Infuse redundancy into the system and regularly backup data offline** so that data can be

replicated at the application level and remain accessible as required. In addition to protection against data disclosure and modification, organizations must also ensure the communication channels are equally protected against identity spoofing and man-in-the-middle attacks.

- **Establish trust controls across federated cloud environments between multiple vendors and delivery models.** This means that organizations will be required to manage identity and access, authentication, audits and API security across multiple cloud vendors and infrastructure. Understand how these controls can be standardized, prioritized, and automated across the hybrid cloud environments through a DevOps approach. For controls that cannot be automated, organizations must train their workforce to follow the necessary standardized procedures.

Consider a combination of storage tiers

Files across an organization can have a variety of accessibility, security, and storage needs. Fortunately, there are different tiers that allow files to be stored safely and thoughtfully. It would be wise to utilize multiple tiers in order to cover all bases.

bmc	Hot storage	Warm storage	Cold storage
Location	Close to the moment of computation	On a remote server or private network, usually a step away from users	In cloud services
Defining Characteristic	Very fast access	Medium speeds	Different pricing tiers for hot and cold options
Examples	Personal hard drives, SSDs, flash drives	Larger, cheaper, spinning drives	Cloud drives, AWS, Google Cloud Storage

Comparison of data storage types

- **Hot storage** is when files are stored locally on desktops, laptops, mobile phones, etc. Files in hot storage are easily accessible at a moment's notice. They require no extra download time and are available without internet connection. When data exists on the edge, it's not as accessible to other parties in the organization and if anything happens to that local storage location, it can be lost. (On the other hand, edge computing reduces the number of instances where data is touched by other humans, servers, and databases, thus reducing the chance of a breach.)
- **Warm storage** is when data stored on the edge is made easily accessible to the network via a gateway. This is a common way to replace traditional file servers in offices and cut down on hardware storage restraints. These gateways make data more accessible for remote users and enables collaboration and productivity.
- **Cold storage** refers to files stored on the cloud. This is best for files that are not used too regularly, need to be stored securely, and perhaps require a larger storage capacity. Cold storage is great for long-term archival and allows files to be seen and identified before downloaded. When cold storage is connected to hot storage via a gateway, all the data remains accessible, but everything has the security, capacity, and availability best suited for the type of file it is.

Security-enhancing tools

Of course, there are some third-party apps or programs that can be utilized to help keep your data secure.

- **Cloud storage gateways.** As mentioned above, a cloud storage gateway bridges the gap between files in local hot storage, and files stored in cold storage on the cloud. A good gateway can reduce latency, security risks, and bandwidth concerns. It will ensure the retention of edge-generated data, allow access across data tiers, and maintain security.
- **Cloud security posture management.** CSPM is a class of security tools that identify and remediate potential security issues, providing a means of reducing the attack opportunities. The processes are automated, and they continuously monitor cloud systems to identify any gaps in the armor and they will alert the customer if something is out of sync.
- **Security incident event management.** SIEM utilizes analytics and AI to determine what internal and external behaviors could generate potential threats. SIEM updates its threat awareness in real time and is able to adequately respond to security events as they pop up.

Consider the vendor, too

Of course, when shopping for a cloud provider, it is vital to consider the vendor's security and risk management practices, financial stability, transparency toward compliance, long term strategy, and past track record in relevant contextual situations. Also, make sure that what the vendor provides aligns with your business needs, including the cost of storing and retrieving data.

Even with the most reliable vendor, it is important that any organization also shoulder the responsibility of keeping their data safe from potential loss or corruption.

Related reading

- BMC Multi-Cloud Blog
- BMC Security & Compliance Blog
- The Cloud Today: Growth, Trends, Market Share & Outlook
- Common Roles in Cloud Computing
- Risk Management: A Complete Introduction To Managing Enterprise Risk
- What Is Threat Remediation? Best Practices for Remediating Threats