3 Steps to Effective Cloud Security for Business

According to a recent report from Symantec Corporation, business organizations have transferred over half of their workload to the cloud. With huge benefits in terms of scalability and collaboration, the move makes good business sense. But those benefits come with risks. Business leaders must take a proactive approach to achieve effective cloud security that protects critical business assets.

Complex Environment Creates Unique Challenges

While the vast majority of organizations operate in the cloud to some degree, the nature of that cloud usage varies widely. Some businesses access specific software applications in the cloud while storing data on-premises. Other organizations move entire networking and storage functions to the cloud. Many businesses use multiple clouds, some public and some private.

At the same time, employees frequently use cloud apps for business purposes without the knowledge of their employers. These "shadow IT" practices complicate the landscape by making it difficult to monitor the location and security of sensitive information. In addition, they add to the significant problem of employees sharing files inappropriately.

Unfortunately, organizational security strategies have not kept pace with cloud usage. As businesses take advantage of new opportunities in the cloud, the chain of responsibility for cloud security grows more complicated. At the same time, hackers benefit from a larger attack surface and increasingly sophisticated tools.

1. Share Responsibility

An important first step to keeping data safe in the cloud involves understanding the shared responsibility model of cloud security. The cloud vendor provides physical security and, to varying degrees, secures the infrastructure, network and applications. But the burden of data protection ultimately rests on the cloud customer.

When implementing cloud services, examine service level agreements and contracts carefully. Ask detailed questions to understand the data protection strategies of your cloud services providers.

In addition, work with your cloud providers to develop an incident response plan well in advance of a breach. Determine communication plans and know what roles the organization and the vendor will each play. Outline a plan to ensure availability of crucial information during the remediation process.

2. Update Security Policies to Match Current Reality

Security policies that worked last year may no longer provide the effective cloud security you need in a rapidly evolving environment. For instance, utilizing the cloud holds significant implications for regulatory compliance. Privacy regulations may mandate, for example, that you include certain language in contracts with cloud vendors.

In addition to regulatory compliance, another key area of concern involves acceptable use of cloud resources. Maintain a "safe" list of approved applications and detail best practices for storing and sharing information online. Communicate these policies clearly to all employees and automate them where possible.

3. Implement Key Components of Effective Cloud Security

In addition to understanding the shared responsibility model and updating existing security policies, bolster data protection in terms of several crucial areas.

- Access management – Begin with multi-factor identification. Additionally, define role-based privileges, restricting access by job description.
- Encryption – Do not rely on the cloud vendor's encryption to secure sensitive data. Maintain full encryption at the file-level, ensuring the safety of data in transit, as well as at rest.
- Artificial intelligence (AI) and machine learning – Increase security by incorporating solutions that monitor for behavioral anomalies and automatically take action to secure data.
- Robust multi-layer security – The cloud environment places additional burdens on all levels of security, from firewalls and anti-malware to threat analytics. Choose solutions built for the cloud environment and apply patches in a timely fashion.
- Regular audits – Perform security audits and penetration testing on a regular basis. In addition to revealing vulnerabilities, you need to keep an updated view of the flow of information through your environment.

Operating in the cloud presents new levels of complexity for organizations as they strive to prevent data loss and achieve compliance. Fortunately, the above three-step process to achieve effective cloud security helps to mitigate the risk. The cloud security experts at eMazzanti guide organizations to safely navigate the complexity and implement comprehensive, custom cloud security solutions.