Best Practices for Optimizing Cloud Security

Devolutions

FORBES REPORTED IN 2018 THAT 2.5 QUINTILLION BYTES OF DATA ARE CREATED EVERY DAY!

Companies are migrating business functions to the cloud with increasing regularity. This means the security of consumer and operational data is paramount. Business leaders and IT professionals have a vested interest in implementing processes that keep online data secure. Due to the sheer quantity of data being stored in the cloud, this is not an easy task.

So, just how much data is being stored in the cloud? Forbes reported **in 2018 that [2.5 quintillion bytes of data] are created every day**. This is due, in no small part, to the recent proliferation of smart devices and cloud applications. To put this into perspective, Forbes also noted that 90 percent of the world's data was created in the previous two years alone.

It's safe to say that given the recent explosion of cloud-based platforms (the global cloud computing market is expected to grow to more than $600 billion by 2023), more and more organizations are investing in cloud infrastructure in order to streamline business operations. The software-as-a-service (SaaS) industry, in particular, is thriving as a result of the mass cloud migration. Modern cloud offerings like enterprise applications suites can accumulate a massive quantity of business-critical data, from high-level financial projections to marketing automation metrics.

Cloud-based tools like these help connect disparate business systems end-to-end and drive cross-functional insights. Because applications generate so much sensitive data, security protocols are crucial. **Here are just a few tips businesses can implement to keep data secure in the cloud.**

Institute and Maintain Proper Permissions

Cloud-based applications import data from a myriad of aggregate sources. At any given time, various **employees at an organization will need access to these accounts in order to carry out day-to-day job functions**.

For example, a digital marketing team might need access to Facebook engagement data for a report. Companies can use tools like an encrypted password manager to manage, modify, and share passwords among stakeholders. System administrators can view and edit permission levels as employees move teams or leave a company.

Provide Comprehensive User Training

One of the most crucial tasks for any IT professional is training the individuals who will be using a given software platform. From onboarding to routine training sessions, end-user training helps maximize the ROI of a business's investment in a cloud ecosystem.

Cybersecurity experts have found that ongoing awareness training (e.g., ones that include realistic simulations of phishing emails) are more successful at driving down instances of human error. Untrained users click on an estimated 90 percent of email links from external organizations, leading to more than 10,000 malware infections per year. This equates to **more than $1 million in lost productivity**. Conversely, organizations that instituted two to three security awareness training sessions saw a reduction in failure rate to just 3 percent. The value of proper security training is incalculable when it comes to maintaining productivity, as well as preventing an inadvertent data breach.

Develop a Data Recovery Plan

According to Gartner, **the cost of IT downtime is $5,600 per minute**. Although this figure is reflected in the compliance regulations and databases of major corporations, it's also a sign that downtime as a result of a system breach is incredibly costly for businesses of all sizes.

It's not all about malicious breaches. Loss of access to a network as a result of natural disaster or other circumstances is a factor businesses must contend with. It's crucial to develop an airtight, iterative recovery plan that involves frequent backups, the use of data recovery software, and expert guidance. Testing a recovery process across variables is especially important, as companies should be confident they won't lose valuable data because of an unplanned circumstance. If an IT infrastructure is hosted by a cloud provider, it's a lot simpler to back data up over a network connection and retrieve data if an interruption occurs. This requires less maintenance than on-premises hardware and is easier to train end users on.

The cloud provides numerous benefits to companies looking to better organize and streamline their data collection and analysis. Proper governance will ensure data stored in the cloud will remain available and secure.