Cloud Computing Security Best Practices for Protecting Your Data

TechRounder PDF Edition

Live article: https://www.techrounder.com/cloud/cloud-computing-security-best-practices-for-protecting-your-data/

By Vipin PG | Published March 27, 2025 | Updated March 9, 2026 | Format: Article | 5 min read

In brief

Over the past decade, businesses have become increasingly reliant on cloud computing for managing their data services. Goldman Sachs estimates that cloud computing sales will increase to $2 trillion by 2030.

Over the past decade, businesses have become increasingly reliant on cloud computing for managing their data services. Goldman Sachs estimates that cloud computing sales will increase to $2 trillion by 2030. Cloud computing offers unique benefits for businesses, such as cost savings, scalability, and ease of collaboration.

When sharing and storing information in the cloud, it is important to develop robust security measures that protect your sensitive data. Here are some of the best strategies for securing your cloud environment.

Understand Your Shared Responsibility Model

To ensure your cloud environment is protected, you need to understand your role in keeping your data safe and clearly explain these responsibilities to all users. Your business is responsible for securing applications, managing user access, and protecting sensitive data. By remaining diligent on your end, you minimize the risk of losing data in an attack.

While users handle security for smaller systems, providers are responsible for securing the entire cloud infrastructure. They maintain physical security for your cloud environment to ensure uptime throughout the organization.

Choose a Trusted Cloud Service Provider (CSP)

When selecting a CSP to partner with, make sure they are qualified to meet your specific business needs. A trusted CSP should have proper certifications, comply with industry standards, and enforce strong security protocols. Providers should always be transparent about their work and offer detailed security documentation to verify your information is properly protected.

Implement Strong Identity and Access Management

Businesses have recently turned to Zero Trust Security to fortify their cybersecurity strategy. This approach assumes that every user and device poses a threat to your environment and should not be trusted. Zero Trust policies ensure that your business is protected from threat actors by only allowing access to authorized users and devices.

Along with these policies, your business should implement policies like Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC). MFA requires users to verify their identity multiple times before being granted access to sensitive information. The most common example of this is putting in a password for an account and then verifying your identity by logging in with another device, such as a phone. RBAC, on the other hand, assigns users to specific roles that have corresponding access settings, like "Senior Engineer."

After establishing IAM policies, you should conduct regular audits and reviews of user permissions to ensure that only authorized users have access to confidential information. Continuous monitoring helps your business detect issues before they evolve into major incidents.

Data Encryption Best Practices

Encryption protects your data in transit and at rest by coding your information so authorized users can only unlock it with a digital key. Encrypting your data protects devices in your environment and improves compliance with cybersecurity standards, such as HIPAA and GDPR.

The strength of an encryption key directly impacts how effectively that system will protect a digital environment. Factors that determine key strength include length, randomness, and techniques used for key management. With key management, businesses should ensure that all active keys are securely stored, and inactive keys are retired.

You can also partner with a trusted Microsoft CSP and leverage their encryption tools to fortify your cybersecurity strategy. They will share industry knowledge and techniques to safeguard your data from an attack.

Regular Security Audits and Vulnerability Assessments

Your business should conduct routine vulnerability scans to monitor your environment for threats. This includes testing for spots that could be easily exploited, software that needs to be upgraded, and data misconfigurations. Identifying these vulnerabilities on the front end saves your business in remediation costs and minimizes organizational downtime.

Another way to test your current security infrastructure is by performing penetration testing. In a penetration test, a security professional simulates an attack on your environment to identify vulnerabilities. These tests allow businesses to examine and reevaluate their incident response plans while educating employees about the importance of cybersecurity policies.

For rapid response times, many organizations implement continuous monitoring with real-time alerts. Real-time alerts notify your security team as an issue occurs, allowing them to address the problem before the impact worsens.

Ensure Robust Backup and Disaster Recovery Plans

Even with advanced security measures in place, your business still faces the threat of a cyberattack. Establish a detailed disaster recovery plan to combat damages caused by a data breach.

Regular data backups are an important practice that protects your business from experiencing wide-scale information loss. The 3-2-1 Backup Rule has your business create three copies of each document, storing those copies in two different types of storage media and storing one copy in an offsite location. This reduces your chances of data loss by creating additional copies with different access points.

When establishing a disaster recovery plan, your organization should analyze and assess your current environment to understand business needs. Then, you can purchase the necessary infrastructure and software to protect your data.

Disaster Recovery is a continuous process, meaning it requires ongoing maintenance and testing to ensure its success. Regularly test your systems to make sure all your bases are covered in the event of an attack and all technology is up to date.

Employee Training and Security Awareness

According to Verizon's 2024 Data Breach Investigations Report, 68 percent of security breaches occurred as a result of human error. Phishing schemes, ransomware, and social engineering attacks continue to advance as AI technology evolves. Luckily, these threats can be significantly reduced with proper employee training.

Run fake email schemes to test your employees' abilities to identify potential threats. Regularly educate your team on your company's security protocols and ensure everyone adheres to these safety measures, including remote employees. Urge team members to create strong passwords and use multi-factor authentication to further protect their accounts. Following these steps will promote a culture of cybersecurity awareness throughout your organization, reducing the likelihood of an attack.

Staying Compliant with Data Protection Regulations

Many industries have developed regulations to protect sensitive data from being leaked. Compliance requirements like GDPR, HIPAA, and CCPA force companies to establish cybersecurity systems that effectively secure confidential information.

Non-compliance not only comes with legal and financial troubles, but it also damages a business's reputation. Failure to comply with regulations causes customers to lose trust and shift their loyalty to another organization. To combat this problem and maintain trust, conduct regular investigations that ensure your company is compliant with all required standards.

Conclusion

Securing your cloud environment is crucial for reliable, safe business operations. Implementing strategies like encryption and employee training ensures that your data remains protected from threat actors. For optimized security, establish proactive solutions that actively monitor your environment to stop incidents before they occur.

Stay educated on cybersecurity trends and watch out for evolving threats that could impact your organization. If you need help managing your cloud environment, consider partnering with a trusted Microsoft Cloud Solution Provider to optimize your business operations and safeguard your most critical assets.

References

1. goldmansachs.com - insights / articles - https://www.goldmansachs.com/insights/articles/cloud-revenues-poised-to-reach-2-trillion-by-2030-amid-ai-rollout

2. verizon.com - business / resources - https://www.verizon.com/business/resources/reports/dbir/

3. plow.net - microsoft-cloud-solution-provider - https://plow.net/microsoft-cloud-solution-provider/?utm_source=Blog&utm_medium=organic