duo>key

10 Ways to Secure Your Data on Public Cloud in 2024

Best Practices for Cloud Security by DuoKey

Table of content

Introduction

The adoption of cloud computing has skyrocketed in the past few years, driven by its ability to enhance efficiency, scalability, and innovation for businesses across sectors. However, the benefits of cloud technology come with increased security challenges. As more data and operations move to the cloud, the threat of security breaches grows, making cloud security critical.

Effective cloud security is essential not just for protecting data but for ensuring that businesses can fully leverage cloud technology, while mitigating risks and minimising compromises. It involves a comprehensive approach, from managing access controls to encrypting sensitive information and educating team members about potential threats.

This guide outlines ten best practices for securing data in the cloud. Compiled from leading security organisations and cloud providers, these recommendations will help organisations mitigate risks of data breaches and maintain the integrity, confidentiality and sovereignty of their data. It seeks to provide the right strategies for organisations to continue to leverage the cloud's capabilities, while minimising compromises.

- Nagib Aouini, CEO at DuoKey

1.—Know Cloud Provider Responsibilities

31% of companies misunderstand the responsibility model for cloud security.

– 2019 Cloud Security Alliance (CSA)

Understand Cloud Provider Responsibilities

Familiarize yourself with the shared responsibility model of your cloud provider. Understand which security aspects are managed by the provider and which are your responsibility.

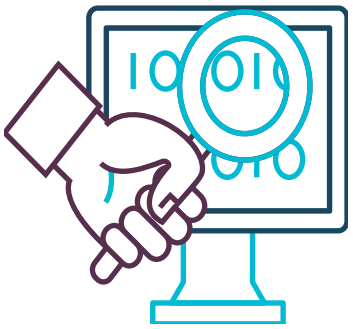
Why?

The shared responsibility model in cloud computing outlines the security responsibilities of the cloud provider and the user. Understanding this model is crucial to ensure that all aspects of cloud security are adequately covered.

DuoKey's Tips

- Clarify responsibilities for securing specific services and data with your cloud provider.
- Regularly revisit the shared responsibility model, especially when deploying new services or applications, to ensure all security bases are covered.

2.—Implement Strong Access Controls



61% of companies experienced an insider attack in 2020

– 2020 Insider Threat Report by Cybersecurity Insiders

Implement Strong Access Controls

Use identity and access management (IAM) systems to ensure that only authorized users can access specific cloud resources. Implement *least privilege access* and *identity-centric* principles, meaning users are given only the permissions necessary to perform their job functions. Multi-factor authentication (MFA) should also be mandatory for all users.

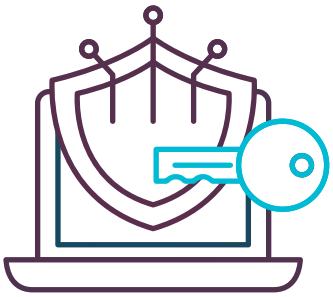
Why?

Access controls are fundamental to securing cloud environments. They ensure that only authorized users can access specific resources, minimizing the risk of unauthorized data access or manipulation.

DuoKey's Tips

- Regularly review and update access permissions to reflect changes in roles or employment status.
- Utilize groups or roles to manage permissions more efficiently rather than assigning permissions to individual users.
- Implement conditional access policies that consider the context of access requests, such as the user's location or device security status.

3.—Encrypt Data



93% of cloud environments are vulnerable to breaches due to misconfigurations

– 2020 Cloud Misconfigurations Report by DivvyCloud

Encrypt Data

Encrypt data both at rest and in transit. Use strong encryption standards and manage your encryption keys securely. Consider cloud services that offer built-in encryption capabilities to simplify this process.

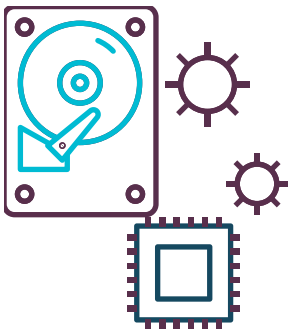
Why?

Encryption transforms readable data into a coded format that can only be decoded with the correct key, safeguarding data from unauthorized access, especially important in the cloud, where data is stored remotely. Encrypting data at rest and in transit ensures that even if data is intercepted or accessed by unauthorized parties, it remains unreadable and secure.

DuoKey's Tips

- Use built-in encryption features offered by cloud providers and manage your own encryption keys when possible for greater control using solutions like DuoKey Key Management System (KMS).
- Implement a Key Management System (KMS) for better overview of your encryption keys lifecycle.
- Regularly rotate encryption keys and use robust key management practices to enhance security.
- Ensure that encryption protocols are up to date and comply with industry standards.

4.—Implement Robust Data Backup & Recovery Strategies



150% increase of ransomware attacks in 2021

– 2021 Statista report on ransomware attacks

Implement Robust Data Backup & Recovery Strategies

Ensure that your data is regularly backed up in secure, geographically separate online and offline locations. This not only protects against data loss due to cyberattacks but also natural disasters.

Why?

Regular backups protect against data loss from cyberattacks, accidental deletions, or other disasters. Storing backups in separate online and offline locations from the primary data adds an extra layer of security, ensuring that you can restore data quickly and efficiently without significant downtime.

DuoKey's Tips

- Automate backup processes to ensure they occur regularly without manual intervention.
- Make sure to test backup restoration processes regularly to ensure that data can be effectively recovered when necessary.
- Use encryption for backups to protect data privacy and security even in storage.
- Follow the 3-2-1 rule: back up your data at least three times, in two different locations, with one copy stored off-site

5.—Secure APIs

40% of companies experienced an API security incident in 2020

– 2020 State of API Security Report by Salt Security

Secure APIs

APIs are used to interact with cloud services. Secure your APIs by implementing strong authentication, encryption, and monitoring for any abnormal activities that could indicate a security breach.

Why?

APIs are critical for integrating services and data in cloud environments but can also be vulnerabilities if not properly secured. Securing APIs involves implementing strong authentication, ensuring encryption, regularly updating and patching API-related software, and monitoring API traffic for suspicious activities.

DuoKey's Tips

- Use OAuth or similar secure authentication standards for APIs.
- Throttle API requests to prevent abuse or denial-of-service attacks (DDoS).
- Regularly audit and review API access logs for unusual or unauthorized access patterns.

6.—Monitor and Log Activities

206 days is the time required on average to identify a data breach

– 2021 Cost of a Data Breach Report by IBM Security

Monitor and Log Activities

Use cloud monitoring tools to track user activities and resource configurations in real-time. Log management helps in the detection and analysis of potential security incidents.

Why?

Continuous monitoring of cloud environments and logging of access and activities help in detecting and responding to potential security threats promptly. It involves using tools to track real-time activities and maintaining logs for forensic analysis and compliance purposes.

DuoKey's Tips

- Implement a centralised logging solution (SIEM, SOC) to aggregate logs from various sources for easier analysis.
- Set up alerts for unusual activities or access patterns to enable quick response to potential threats.
- Ensure effective triage of alerts with up-to-date and thoroughly tested playbooks.
- Regularly review and analyse logs to identify security trends or recurring vulnerabilities.

7.—Secure Perimeter

2.5X increase in Distributed Denial of Service (DDoS) attacks in 2020

– 2020 Kaspersky DDoS Protection Report

Secure Perimeter

Use firewalls, intrusion detection/prevention systems (IDPS), and other network security tools to protect your cloud resources. Segmentation and isolation of cloud resources can also reduce the risk of lateral movement in case of a breach.

Why?

Network security measures protect cloud resources from unauthorized access and attacks. This includes using firewalls, intrusion detection and prevention systems, and network segmentation to control traffic and reduce the attack surface.

DuoKey's Tips

- Use virtual private networks (VPNs) or private connectivity options offered by cloud providers for secure access.
- Regularly update and patch network security devices and software to address known vulnerabilities.
- Implement microsegmentation to isolate workloads and minimize lateral movement in case of a breach.
- Install WAFs and firewalls IDS/IPS to easily stop and prevent DDoS attacks.

8.—Secure Endpoints

70% of breaches start on endpoint devices

– 2019 Data Breach Investigations Report by Verizon

Secure Endpoints

Ensure that devices accessing the cloud are secured and up-to-date with the latest security patches. Endpoint protection solutions can help detect and mitigate threats

Why?

Endpoint security is critical as devices accessing the cloud can be entry points for threats. Securing endpoints involves using antivirus software, firewalls, and regular patching to protect devices against malware and other attacks.

DuoKey's Tips

- Implement a mobile device management (MDM) solution to manage and secure mobile devices accessing the cloud.
- Use endpoint detection and response (EDR) tools for advanced threat detection and response capabilities.
- Ensure all devices follow a strict update and patch management policy to keep security features current.

9.—Conduct Regular Security Assessments

Only 5% of companies' folders are properly protected

– 2019 Global Data Risk Report by Varonis

Conduct Regular Security Assessments

Perform vulnerability assessments and penetration testing to identify and address security weaknesses in your cloud environment. This should be part of a regular security review process.

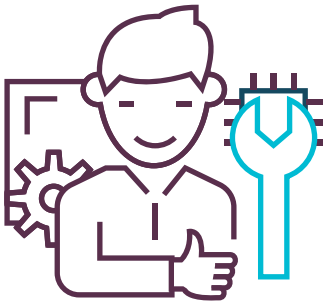
Why?

Regular security assessments, including vulnerability scans and penetration testing, help identify and address security weaknesses in cloud environments. These assessments provide insights into potential vulnerabilities and the effectiveness of existing security measures.

DuoKey's Tips

- Schedule regular penetration testing by external experts to get an unbiased assessment of security postures.
- Use automated tools for continuous vulnerability scanning and remediation.
- Include compliance checks in security assessments to ensure adherence to relevant laws and regulations.

10.—Educate Your Team



95% of cybersecurity breaches are caused by human error

– 2019 Cyber Security Breaches Survey

Educate Your Team

Provide regular security training for your team. Educate them on the latest security threats and best practices for securely using cloud services.

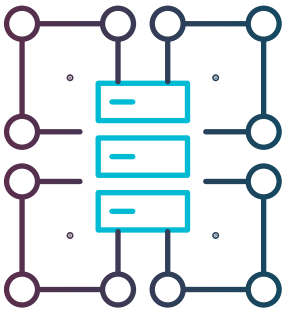
Why?

Human error is a significant factor in many security breaches. Educating your team about security best practices, the latest threats, and safe online behaviors is crucial for strengthening your organization's overall security posture. Regular training can significantly reduce the risk of breaches caused by phishing attacks, poor password practices, or accidental data exposure.

DuoKey's Tips

- Develop a regular training schedule that includes updates on the latest security threats and trends.
- Use engaging content formats like videos, quizzes, and interactive modules to enhance learning and retention.
- Encourage employees to report suspicious activities and providing them with the tools and knowledge to recognize potential threats.
- Implement phishing simulation exercises to teach employees how to recognize and react to phishing attempts.

Bonus: Monitor Configuration & Compliance



80% of non-compliant organizations suffer financial losses of an average $4.13 million per breach

Monitor Configuration & Compliance

Regular monitoring of cloud configurations and compliance with security benchmarks ensures that your cloud environment adheres to industry standards and regulatory requirements. This helps prevent breaches and ensures operational integrity by detecting misconfigurations and deviations early.

Why?

Monitoring and maintaining compliance to benchmarks helps maintain a secure, compliant, and reliable cloud environment, reducing the risk of legal or security issues.

DuoKey's Tips

- Use automation tools to continuously assess compliance with frameworks like CIS or ISO.
- Embed compliance checks in your development pipelines to identify issues early.
- Keep your benchmarks current with evolving security practices and regulations.
- Utilise tools provided by cloud services for efficient monitoring and compliance checks.

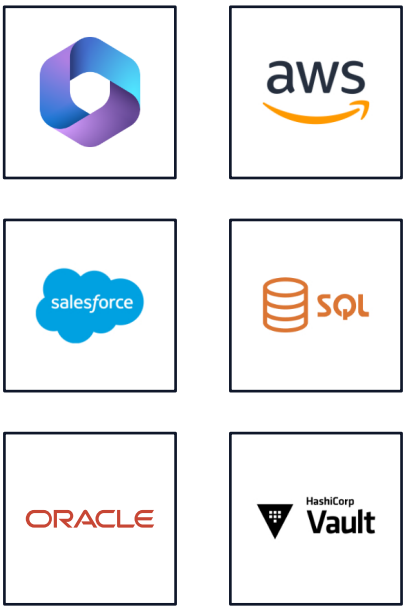
Keep your data safe with true peace of mind

DuoKey is a cloud security leader that specialises in robust key management and advanced encryption for enterprise cloud.

Leveraging secure Multi-Party Computation (MPC), DuoKey offers:

- Seamless integration with your technology stack, without disruption.
- Unified control panel for key management.
- Enhanced security for your critical data.

Learn more at: **duokey.com**



duokey

duokey.com