Best Practices for Secure Cloud Systems

(By Kavitha Bangalore)

1. Deploy multi-factor authentication

Adaptive MFA is crucial to helping businesses add an extra layer of security to their cloud-based environments while improving user experiences.

Passwords are no longer enough when it comes to protecting user accounts and sensitive business data. Along with stolen credentials, weak passwords are one of the easiest and most popular ways for hackers to gain unauthorized access to business systems: it's estimated that 80% of security breaches involve compromised passwords.

MFA requires employees, customers, and partners to verify their identity by providing a second piece of evidence—whether a one-time password or biometric verification—when attempting to access applications, devices, and systems. This process ensures businesses aren't relying solely on username and password combinations to authenticate users.

2. Go passwordless

Once you've established MFA, the next step for many companies will be detach from passwords altogether.
Passwordless authentication enables businesses to:

- Leverage session risk to enhance the authentication experience.
- Provide one-click or one-touch authentication across desktop and mobile.
- Reduce IT helpdesk and support costs associated with password management.
- Minimize the risk—and cost—of data breaches caused by stolen or compromised credentials.

3. Manage user access

Employees really only require access to the applications and resources they need to get their job done. And providing users with access levels beyond what they need can leave a business open to credential theft and insider threat attacks.
Organizations need to set appropriate levels of authorization to ensure that every employee is only able to view and access the applications and data they require. They can also set user access rights to prevent an employee from editing or deleting information they aren't authorized to and protect them from hackers stealing an employee's credentials.

4. Constantly monitor activity

Given the high threat level of cloud applications and systems, it's important to regularly and systematically scan for any irregular user activity. Businesses should carry out real-time analysis and monitoring to detect any actions that deviate from regular usage

patterns, such as a user logging in from a new IP address or accessing an application from a new device.

These irregularities can indicate a potential security breach, so real-time monitoring helps to stop a hacker before they can do any damage. And in the case where a user has accessed the system from a new device and triggered a benign alert, they can be quickly and easily verified through MFA.

Solutions that help businesses to monitor applications and systems in real time include endpoint detection and response, intrusion detection and response, and vulnerability scanning and remediation.

5. Automate onboarding and offboarding

When a new employee joins a company, they require access to the applications and systems they need to get up and running and do their job effectively. However, it's equally important that as soon as an employee leaves the organization their access to all data and resources is revoked.

Automating the onboarding and offboarding process ensures that no mistakes are made, there's no delay in deprovisioning user access, and takes the burden of account maintenance off of admins and IT teams.

6. Ongoing employee training

Having cloud computing security in place is important, but it's also vital to ensure that your employees understand the risks that they face. With password and credential theft so prevalent, employees are an organization's first line of defense against hackers.

Organizations need to provide regular training to keep security top of mind for employees. Teams should be trained to understand the signs of a phishing attack, what spoofing websites are, and the tactics hackers use to target victims.

Important Points:

❖ Build security while initial design process of application. Creating Cloud Native applications presents an opportunity to engage cloud-based security early.

❖ Deployment process to be integrated with security testing.

❖ Encryption key management to maintain controls of all private / public encryption keys. Departments should understand the new architectural options and services available in the cloud. The departments should update their standards and security policies to support them and shouldn't merely attempt to enforce existing standards entirely on model.

Best Practices for Secure Cloud Systems

(By Kavitha Bangalore)

❖ Segregation: Web facing application should be deployed in DMZ (De militarized) zone and the Database Server should be deployed in the secured zone while deploying the application on cloud.

❖ Use of Web Application Firewall for Web apps and online portals

❖ Application integration and information exchange to happen over secured API channels.

❖ Security controls for interfaces and API's

❖ Log and monitor API calls.

❖ Use software-defined security to automate security controls.

❖ Use event-driven security such Anti-virus, when available, to automate detection and remediation of security issues.

Below Figure compares the security between the On-premises and Central Location Cloud.

	On-premise/ Co-located DC	Cloud
Technical Expertise	Government Department's own team or an IT Managed Service Provider	Cloud Managed Service Provider
Security Technology Upgrade	Less frequent	More frequent
Physical DC Security	Government Department/ Co-location DC Provider	Cloud Service Provider
IT Infrastructure Security	Government Department/Co-location DC Provider	Cloud Service Provider
Vulnerability/ Security Patching	Depends on support levels and technical expertise of in-house team	More frequent and up to date
Certifications & Compliances	Government Department	Cloud Service Provider
Resiliency (Downtime)	Less Resilient with varying commitments on downtime	More Resilient and committed uptime and availability SLAs

Best Practices for Secure Cloud Systems

(By Kavitha Bangalore)

References: Cloud Security Basics, Best Practices & Implementation | GlobalDots