Cloud Security Fundamentals Guide

Cloud computing changes the security model but does not eliminate security responsibilities. The shared responsibility model means the cloud provider secures the infrastructure while you secure your data, access, and configurations. Misunderstanding this boundary is the root cause of most cloud breaches.

Key Points

- ✓ Understand the shared responsibility model: IaaS vs PaaS vs SaaS responsibilities differ
- ✓ Identity is the new perimeter — secure IAM with MFA, least privilege, and conditional access
- ✓ Encrypt data at rest and in transit — use provider-managed or customer-managed keys
- ✓ Enable cloud-native logging: CloudTrail (AWS), Activity Log (Azure), Audit Logs (GCP)
- ✓ Regularly audit storage permissions — public S3 buckets and storage accounts cause breaches
- ✓ Use infrastructure as code (IaC) to enforce consistent, auditable configurations
- ✓ Implement cloud security posture management (CSPM) for continuous compliance monitoring

Action Items

1. Review your cloud IAM policies and remove overly permissive roles
2. Enable MFA for all cloud console access, especially root/global admin accounts
3. Audit all storage buckets and containers for public access settings
4. Enable cloud provider security recommendations (AWS Security Hub, Azure Defender, GCP SCC)
5. Implement tagging policies for cost and security visibility

Quick Reference

Shared Responsibility:
IaaS — You manage: OS, apps, data, access. Provider manages: physical, network, hypervisor.
PaaS — You manage: apps, data, access. Provider manages: OS, runtime, infrastructure.
SaaS — You manage: data, access. Provider manages: everything else.
Top Cloud Risks (OWASP): Misconfigured access, insecure APIs, overprivileged identities, lack of logging, unencrypted data.