5 essential cloud security questions

Cloud-based data and apps are outside the traditional enterprise perimeter and require new methods of protection. Make sure your provider has everything you need.

Identity and access management

1. Can your cloud platform integrate my company's identity management system—or provide a trustworthy alternative?

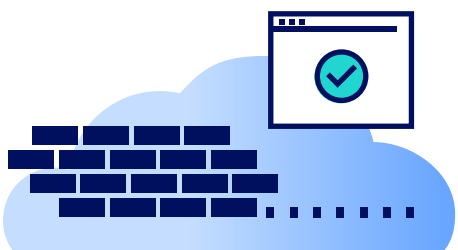
Any interaction with a cloud platform starts with verifying who or what is doing the interacting—an administrator, a user or even a service. Look for providers that offer a consistent way to:

- Identify and authenticate users that access the cloud platform
- Identify and authenticate end users of apps hosted in the cloud
- Authenticate an identity for API access and service calls
- Integrate your existing identity access management (IAM) system into the cloud platform

Developers on IBM Cloud™ can use **App ID** to build automatic authentication into their mobile and web apps.

Secure infrastructure

2. Does your cloud platform offer well-integrated firewalls, trusted compute hosts and options for micro-segmentation based on workload?



- **Security groups and firewalls**—Network firewalls are essential to protect the perimeter and to create network security groups for instance-level access.
- **Micro-segmentation**—Developing applications cloud-natively as a set of small services provides a security advantage: you can isolate them using network segments.
- **Trusted compute hosts**—Hardware-based host security with measure-verify-launch protocols offers excellent protection for running your workloads.

Deploy virtualized workloads on a trusted platform with **IBM Cloud Secure Virtualization** and container apps that use **IBM Cloud trusted containers.**

Data encryption and key management

3. Does your platform support bring-your-own-keys?

A bring-your-own-keys (BYOK) model allows you to manage encryption keys in a central place, ensures that root keys never leave the boundaries of the key management system and enables you to audit the key management lifecycle.

IBM Cloud enables BYOK support for data encryption with the **IBM Cloud Key Protect** service.

Application security

4. How often and to what extent will my containerized apps be scanned for vulnerabilities?

DevOps teams need automated security checks. Ask for integrated tools that continuously scan for potential vulnerabilities in your registry images and running containers.

IBM Cloud Container Service offers a **Vulnerability Advisor** to provide both static and live container image scanning.

Visibility and intelligence

5. Do your security logs and reports reflect multiple points of visibility and integrate with customer SIEMs?

A built-in cloud activity tracker can automatically log and track all access to the platform and services, including API, web and mobile access. Your organization should be able to integrate these logs into your security intelligence and event monitoring (SIEM) system to give you a 360-degree view of your environment.

IBM® QRadar® is a comprehensive SIEM offering that provides a set of AI-empowered security intelligence solutions that can grow with your organization's needs.

Need more answers to cloud security questions? Visit **ibm.com**/cloud/security

39013839-USEN-00