**Module 5 Glossary: Cloud Security, Monitoring, Case Studies, & Jobs**

| **Term** | **Definition** |
| --- | --- |
| **Access group** | A group of users and service IDs is created so that the same access can be assigned to all entities within the group with one or more access policies |
| **Administrative users** | Create, update, and delete application and service instances, and need insight into their team members’ activities |
| **API keys** | Unique identifiers are passed into an API to identify calling application or user |
| **Application Performance Monitoring** **(APM)** | Measures application availability and performance, providing tools needed to troubleshoot issues in an application's environment |
| **Application users** | Users of the cloud-hosted applications |
| **AppSec** | Application Security |
| **Audit and compliance** | A critical service within identity and access framework used to validate implemented controls against policies |
| **Authentication** | Also known as identity service, it enables applications deployed to the cloud to authenticate users at an application level |
| **BYOK** | Bring Your Own Keys |
| **Client-side encryption** | Occurs before data is sent to cloud storage |
| **Cloud directory services** | Used to securely manage user profiles and associated credentials inside a cloud environment |
| **Cloud encryption** | Also known as the last line of defense, it encrypts data and provides robust data access control, key management, and certificate management |
| **Cloud monitoring solutions** | Assess data, application, and infrastructure behaviors for performance, resource allocation, network availability, compliance, and security risks and threats |
| **Cloud security** | Policies, technological procedures, services, and solutions designed to secure the enterprise applications and data on the cloud against insider threats, data breaches, compliance issues, and organized security threats |
| **Database monitoring tools** | Help track processes, queries, and availability of services to ensure the accuracy and reliability of database management systems |
| **Decryption key** | Defines how the encrypted data will be transformed back to legible data |
| **Developer users** | Authorized to read sensitive information and to create, update, and delete applications |
| **Encryption** | Scrambling data to make it illegible |
| **Encryption algorithm** | Defines the rules by which data will be transformed so that it becomes illegible |
| **Encryption at rest** | Protecting data while it is stored |
| **Encryption in transit** | Protecting data while it is transmitted from one location to another |
| **Encryption in use** | Protecting data when it is in use in memory |
| **Identity and access management** | Also known as access control, it helps authenticate and authorize users and provides user-specific access to cloud resources, services, and applications |
| **Infrastructure monitoring tools** | Identify minor and large-scale hardware failures and security gaps so that developers and administrators can take corrective action before problems affect user experience |
| **Key management services** | Help perform life cycle management for encryption keys that are used in cloud services or customer-build apps |
| **KYOK** | Keep Your Own Keys |
| **Multifactor authentication** | Adds an additional layer or authentication for application users |
| **Reporting** | Provides a user-centric view of access to resources |
| **Server-side encryption** | Occurs after cloud storage receives your data but before the data is written to disk and stored |
| **SSL** | Secure Sockets Layer |
| **TLS** | Transport Layer Security |
| **User and service access management capability** | Enables cloud application and service owners to provision and de-provision user profiles with minimal human interaction |