Skillmine
Technology • Consulting • Services

infosec
Miners

Cloud Security

Making the switch from on-premises hardware to the cloud for your computing requirements can be the first step in setting up your company for success in the future. The cloud makes content management simpler, offers you access to additional applications, enhances data accessibility, and fosters better teamwork. Some consumers may be hesitant to transfer their data to the cloud due to security concerns, but a reputable cloud service provider (CSP) can remove your fears and keep your data extremely secure and safe using cloud services.

Cloud security, commonly referred to as cloud computing security, is a group of security controls intended to safeguard cloud-based applications, data, and infrastructure. These steps preserve data privacy, guarantee device and user authentication, and control access to data and resources. They also assist with the in-progress of regulatory data. Cloud security is used in cloud settings, to safeguard against distributed denial of service (DDoS) attacks, unauthorized user access and viruses.

Cloud Security and its Categories :

- Data security
- Data retention (DR) and Business continuity (BC) planning
- Legal compliance
- Identity and access management (IAM)
- Governance (policies on detection, threat prevention, and mitigation)

The cloud environments that are currently used :

- **Public cloud** environments are multi-tenant cloud services, like a coworking space or office building, where a client shares a provider's servers with other clients. To provide customers with access via the web (Internet), the supplier operates these third-party services.
- **Private in-house cloud** environments are single-tenant cloud service servers run from their own private data centre. In this instance, the cloud environment is managed by the company directly, allowing for complete element setup and configuration.
- **Private third-party cloud** gives clients the sole use of their own clouds, which are built on the use of cloud services. These single-tenant environments are often owned, controlled, and managed by a third-party provider offshore.
- **Hybrid cloud** environments consist of onsite private cloud data centres with one or more public clouds and use the private third-party cloud.
- **Multi-cloud** environments include the use of multi, that is two or more cloud services from separate providers. These can be any public and/or private cloud services.

CSP Customer Policies and Standards :

infosec Miners

IaC Security

- Infrastructure Security Scanner.
- Ensure compliance via policy as code.
- Prevent hazardous configurations and apply automated remediation.

Cloud Security Posture Management

- Monitor security and compliance posture.
- Prioritize and remediate cloud security issues.
- Keep track of the security status of your cloud, identify and tackle potential threats, and ensure compliance.

Cloud Infrastructure Entitlements Management

- Enforce least-privilege access.
- Insight into excessive permissions and entitlements.
- Obtain insight into excessive permissions and authorizations and enforce the principle of least privilege access.

Cloud Workload Protection

- Vulnerability management.
- Continuous compliance validation and threat detection.
- Secure containers, Kubernetes hosts, and serverless functions across the application lifecycle.

Kubernetes Network Segmentation

- Dynamic topology maps.
- Network security policy creation.
- Implement a Zero Trust approach for container network security.

Scope of Cloud Security Includes :

- **Data Storage:** Hard drives.
- **Data:** All the information is stored, modified, and accessed.
- **Operating Systems (OS):** A software program that manages computer hardware and software resources.
- **Physical Networks:** Electrical power, routers, climate controls, cabling.
- **Middleware:** Application Programming Interface (API) management.
- **Applications:** Traditional software services (email, productivity suites, tax software).
- **Data Servers:** Core network software and hardware.
- **Runtime Environments:** Execution and good conditioning of a running program.
- **End-user Hardware:** Computers, mobile devices, and Internet of Things (IoT) devices.
- **Computer Virtualization Frameworks:** Host machines, Virtual machine (VM) software, and guest machines.

Types of cloud services :

01 **Infrastructure as a Service (IaaS)**

02 **Platform as a Service (PaaS)**

03 **Software as a Service (SaaS)**

Benefits of Cloud Security :

- Lower upfront costs
- Centralized security
- Reduced ongoing operational and administrative expenses
- Greater ease of scaling
- Increased reliability and availability
- Improved DDoS protection

Things to consider while choosing a CSP :

For the protection of the data and the general security of the business, finding the appropriate CSP solution with secure cloud services is crucial.

Controls designed to prevent data leakage:

Seek providers with integrated security controls for cloud computing to aid with issues like unauthorised access, data theft, and unintentional data leaks. They should let you apply more exact security restrictions, including native security classifications, to your most important and sensitive data.

Data encryption:

Make sure it's possible to have all data encrypted both at rest and in transit. Data is encrypted using a symmetric key as it is written to storage. Data is encrypted in transit across wired networks or wireless by transporting the data over a secure channel using (TLS)Transport Layer Security.

Strong authentication:

Ensure that the CSP offers effective Multi-Factor Authentication (MFA) and strong password controls to grant appropriate access. The CSP should also allow single sign-on and MFA for internal and external users so users only need to log in once to access the tools they require.

Continuous compliance:

Look for content lifecycle management features including legal holds, eDiscovery, and document preservation and disposal. Ask if the service is independently accredited and audited to satisfy the strictest international requirements.

Visibility and threat detection:

Machine learning should be used by a secure supplier to recognise hazards, notify your staff, and track undesirable behaviour. Machine Learning (ML) algorithms examine usage to discover patterns of usual use. Administrators can observe all user activity and all shared content.

Integrated security:

Assess if the provider's tools can be seamlessly incorporated into your security framework by utilizing APIs. Comprehensive security coverage across all your applications while maintaining a seamless user experience is essential to integrate these tools into all of your applications.

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services
India | KSA | UK | USA

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

Follow us on