Best Practice For Public Cloud Threats

Data Breaches

✓ Encrypt sensitive data at rest and in transit.

✓ Implement strong access controls and authentication mechanisms.

✓ Regularly audit and monitor access to identify suspicious activities.

→

Insecure Interfaces/ APIs

- ✓ Thoroughly review and secure cloud interface and API access.
- ✓ Use identity and access management (IAM) solutions for robust access control.
- ✓ Employ API security best practices, such as rate limiting and input validation.

Shared Resources

- ✓ Isolate workloads and resources to prevent performance interference.
- ✓ Use Virtual Private Cloud (VPC) or Virtual Networks for better network segmentation.
- ✓ Monitor resource utilization and adjust as needed.

Compliance Challenges

- ✓ Understand relevant compliance standards and ensure cloud configurations align with requirements.
- ✓ Use cloud compliance tools and services to help meet compliance obligations.
- ✓ Regularly audit and document compliance efforts.

Limited Control

- ✓ Leverage cloud security services and features provided by the cloud provider.

- ✓ Implement network security controls, such as firewalls and security groups.

- ✓ Use Infrastructure as Code (IaC) for automation and consistent security policy enforcement.

Confidence in the Cloud : Briskinfosec by Your Side

Secure your public cloud with our expertise

BRISK INFOSEC

CYBER TRUST & ASSURANCE

CONTACT US TODAY !

☎ 7305979769 www.briskinfosec.com ✉ contact@briskinfosec.com