Best Practices for Securing Cloud Resources

As your organization expands into the cloud, compliance becomes more complicated, and bad actors have more surface area to attack. The stakes are high: Fail to maintain compliance, and you face hefty fines. Expose data and provoke a leak, and you'll suffer severe reputational damage.

Avoid these issues by adopting the right cloud security strategy.

SECURING ALL 3 LAYERS OF CLOUD RESOURCES

1. **DATA**
2. **COMPUTE ENVIRONMENTS**
3. **SaaS APPLICATIONS**

Employ best practices to maximize security across these layers.

SECURING DATA

- Encrypt all data (at rest and in flight).
- Create a governance policy for data access.
- Anonymize data so that it's identified through a referential identifier, not PII.

SECURING COMPUTEENVIRONMENTS

- Understand that using a cloud service provider does not ensure compliance.
- Embrace a sha#d61e2a responsibility model, which often includes an SLA.
- Employ a zero-trust framework.

SECURING SaaS APPLICATIONS

- Prioritize identity and access management.
- Employ a Content Delivery Network (CDN) to decrease exposure.
- Use a Cloud Access Security Broker (CASB) to add an enforcement point between the user and the SaaS application.

Contact us today for help securing cloud resources.