Public Cloud Security Principles

As Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) have exploded, the complexity of securing your data in public clouds has also exploded. While networking controls remain essential, these controls are insufficient in the new world of public cloud. Working with customers, Sonrai Security has developed the "Public Cloud Security Principles" to help guide your path for public cloud security.

1 Identities and data are the new perimeter for securing public cloud

Agile development, auto-scaling, continuous development, microservices based apps, serverless functions, and containers render network controls insufficient. Identity and data are the linchpin control points for cloud-native security.

2 Modeling trust relationships continuously is critical for assessing risk

Imagine, six thousand instances, three thousand containers, thousands of serverless functions, sixty agile teams, hundreds of cloud accounts and one hundred million data objects. In your ephemeral public cloud, you must continuously know what can access what and what is accessing what.

3 Effective segregation of duties is paramount to avoid catastrophe

Public cloud account owners have exceptional powers to circumvent controls, instantiate compute and delete vast swaths of your infrastructure. In the old-world admins cannot delete your data centers, but in public cloud, they can.

4 Over-privilege, insidious and difficult to discern, must be monitored daily

Excessive privilege and auto-escalation are not uncommon across a plethora of developer ID's and roles. Complicating matters, ACL's, group inline policies, user inline policies, role inline policies, assumed roles, switched roles, federation and managed policies determine rights.

5 Controlling access and encryption keys is of utmost importance

You should use a third-party key vault and ensure cloudprovider employees cannot see your keys. Given the limitation of network controls, maniacal vigilance is required to ensure keys are rotated and not stored across cloud accounts without stringent access policy.

Copyright © Sonraí Security 2019

6 DB and storage service monitoring mitigate the limited utility of network controls

You have expunged all internet gateways from your accounts and installed security groups. You think nothing in your cloud will communicate to the internet and nothing from the internet can get in. However, someone with an access key or console login can still access your storage or database services from a coffee shop, and make them public.

7 Effective tagging and classification is transformational

Public cloud resource tags are bloated and inconsistently used. Data classification is haphazard. However, effective tagging, classification, and tracking are possible to an extent inconceivable in old data-center worlds. Effectiveness here reimagines security.

8 Data exposure risks in S3 and Blob object stores are just the tip of an iceberg

Providers made creating public buckets harder, but developers still create public objects even though the bucket isn't. More concerning, crown-jewel data is now pouring into a plethora of databases and cloud services like RDS, CosmosDB, Atlas, MongoDB, CouchDB, Elasticache and many more.

9 Agnostic security platforms are foundational for security and risk control

Your public clouds contain third-party key management, database, and other middleware services. Your company will leverage multiple cloud platform providers. Cloud provider identity models are impenetrably complex and tooling disjointed, biased and ever-changing.

10 Being two-faced is a virtue in public cloud security

Security teams want dashboards, compliance mandates and incidents a SOAR platform will consume. DevOps teams need speed, APIs and Slack channels. Your new security program and underlying security platforms must satisfy both simultaneously.

Identity and Data Protection for AWS, Azure, and Google Cloud

Sonrai's public cloud security platform provides a complete risk model of all identity and data relationships, including activity and movement across cloud accounts, cloud providers, and 3rd party data stores. Identity and data access complexity are exploding in your public cloud. This is causing security holes you don't even know exist. First-generation security tools miss this as evidenced by so many breaches. Sonrai's platform finds these holes, helps you plug them, and makes sure they won't reappear.

Want to see Sonrai in action?

Request a Demo sonraisecurity.com/demo

sonraí SECURITY

Copyright © Sonraí Security 2019