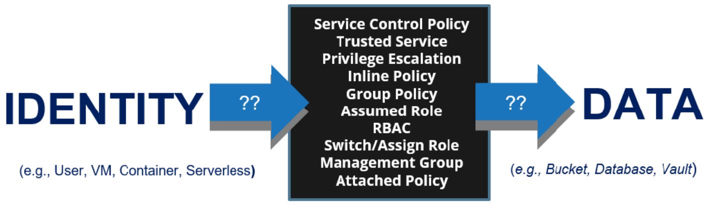
Unraveling Complex Identity and Data Relationships in Public Clouds

Organizations building applications in AWS, Azure, or GCP will quickly discover how complex these models actually are when extending to resource policies like S3 bucket policies, region restrictions, resource or management groups. And, more importantly, how a poor identity and access management (IAM) configuration will expose corporate data to breach by an external actor or an over permissioned insider. Sonrai Security's Critical Resource Monitor (part of our Cloud Data Control platform) helps organizations unravel the complexity in public cloud IAM architectures, helping to eliminate weak or accidental configurations that if left unchecked, will inevitably lead to a data breach.


IDENTITY

??

Service Control Policy
Trusted Service
Privilege Escalation
Inline Policy
Group Policy
Assumed Role
RBAC
Switch/Assign Role
Management Group
Attached Policy

??

DATA

(e.g., User, VM, Container, Serverless)

(e.g., Bucket, Database, Vault)

Figure1: Complex Identity and Data Relationships In a Public Cloud

The Power of The Sonrai Critical Resource Monitor

Central to Critical Resource Monitor is a unique capability – the Sonrai Security IAM/data graph model. Behind the scenes, the Sonrai platform is collecting IAM related data from a broad range of sources (e.g. APIs, logs, cloud analytics). This information is compiled into a normalized graph data model that can quickly surface complex IAM and data relationships across an entire public cloud deployment. Unlike many tools that only show singular IAM relationships (e.g. role with an EC2FullAccess or owner of a subscription), the Sonrai platform can connect the dots and show all relationships in a single picture. See an example of this below:

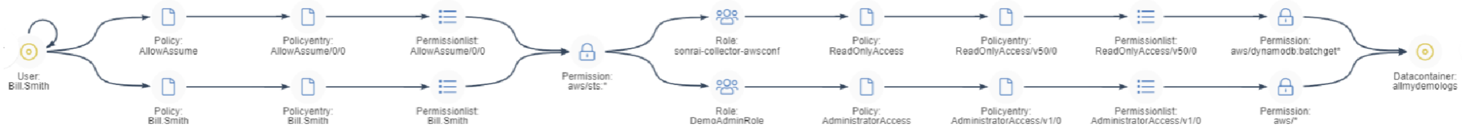
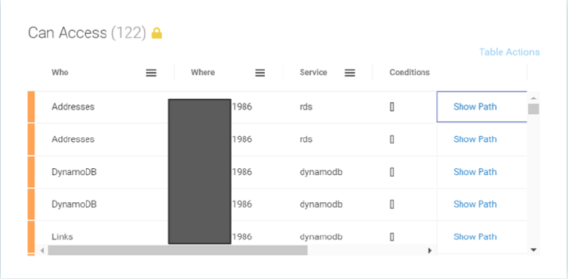

User: Bill.Smith
Policy: AllowAssume
Policyentry: AllowAssume/0/0
Permissionlist: AllowAssume/0/0
Policy: Bill.Smith
Policyentry: Bill.Smith
Permissionlist: Bill.Smith
Permission: aws/sts:*
Role: sonrai-collector-awsconf
Policy: ReadOnlyAccess
Policyentry: ReadOnlyAccess/v50/0
Permissionlist: ReadOnlyAccess/v50/0
Permission: aws/dynamodb:batchget*
Role: DemoAdminRole
Policy: AdministratorAccess
Policyentry: AdministratorAccess/v1/0
Permissionlist: AdministratorAccess/v1/0
Permission: aws/*
Datacontainer: allmydemologs

Figure 2: Sonrai IAM/Data Graph

Find Out What "Can Access" What

Assess Trust Relationships. Quickly assess, regardless of underlying complex IAM policy assignments, what identities "can access" what data and what it can do to the data, such as read vs. delete vs. reconfigure. This is nearly impossible to obtain without a normalized graph.

Automate Controls. Implement automated cloud security controls that notify of risky IAM policies that fall outside of corporate policy.


Can Access (122)

Who	Where	Service	Conditions	
Addresses	[redacted]1986	rds	▯	Show Path
Addresses	[redacted]1986	rds	▯	Show Path
DynamoDB	[redacted]1986	dynamodb	▯	Show Path
DynamoDB	[redacted]1986	dynamodb	▯	Show Path
Links	[redacted]1986	dynamodb	▯	Show Path

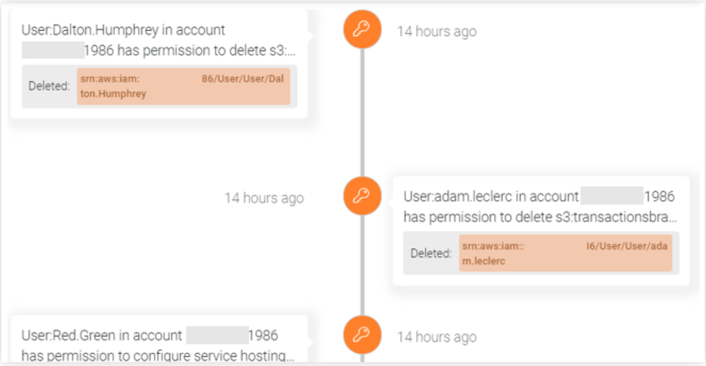
Figure 3: Sonrai What "Can Access" What Summary View

Find Out “What Trust Relationships Have Changed” After A Locked Baseline

Baseline Trust Relationships. Establish an IAM trust relationships baseline that represents IAM policy and the associated use of permissions accepted by the appropriate team members (e.g. cloud security architecture team).

Monitor IAM Changes. Monitor deviations from the accepted baseline, flagging any changes that might introduce risky activity or that could be malicious that the security team may be unaware.

Investigate Change. Receive a time series trace of changes to the configuration baseline, helping reduce the potential window of exposure from oversight or poor configuration change.



User:Dalton.Humphrey in account [redacted]1986 has permission to delete s3:...

Deleted: srn:aws:iam: [redacted] 86/User/User/Dalton.Humphrey

14 hours ago

14 hours ago

User:adam.leclerc in account [redacted]1986 has permission to delete s3:transactionsbra...

Deleted: srn:aws:iam:: [redacted] 16/User/User/adam.leclerc

User:Red.Green in account [redacted]1986 has permission to configure service hosting...

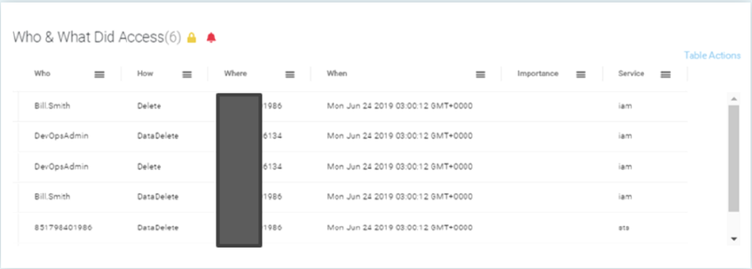
14 hours ago

Figure 4: Sonrai Monitored Change View

Find Out “What Has” Accessed a Resource

Monitor Data Access. Understand what “Identities” (e.g. user, VMs, containers, serverless) have accessed what data (e.g. buckets, database, vault) to effectively report on fine grain access patterns to data resources.

Normalized Results. All access views are normalized to simple action statements (e.g., read, configure, write, delete, audit, etc.) from 1000’s of potential API/actions.



Who & What Did Access(6)

Who	How	Where	When	Importance	Service
Bill.Smith	Delete	[redacted]1986	Mon Jun 24 2019 03:00:12 GMT+0000		iam
DevOpsAdmin	DataDelete	[redacted]6134	Mon Jun 24 2019 03:00:12 GMT+0000		iam
DevOpsAdmin	Delete	[redacted]6134	Mon Jun 24 2019 03:00:12 GMT+0000		iam
Bill.Smith	DataDelete	[redacted]1986	Mon Jun 24 2019 03:00:12 GMT+0000		iam
851798401986	DataDelete	[redacted]1986	Mon Jun 24 2019 03:00:12 GMT+0000		sts

Figure 5: Sonrai “What Has” Accessed View

Sonrai Security

Sonrai Security provides a Cloud Data Control service that delivers a complete risk model of all identity and data relationships, including activity and movement across cloud accounts, cloud providers and third-party party data stores. Our Cloud Data Control platform helps security and DevOps leaders stop data security threats, ensure compliance, and increase DevOps efficiency.

Want to see Sonrai CDC in action?

Request a Demo sonraisecurity.com/request-a-demo

sonraí SECURITY