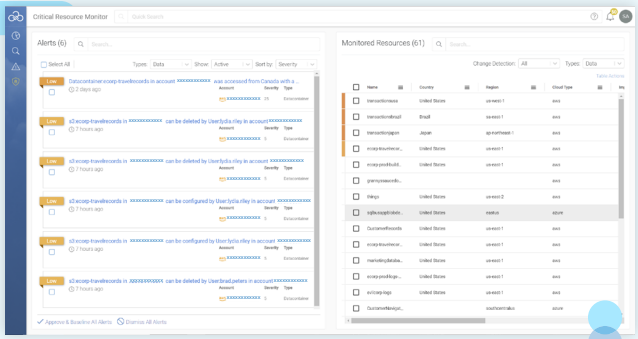
sonraí SECURITY

# Securing Identities & Data

## Data Security, Governance and Access

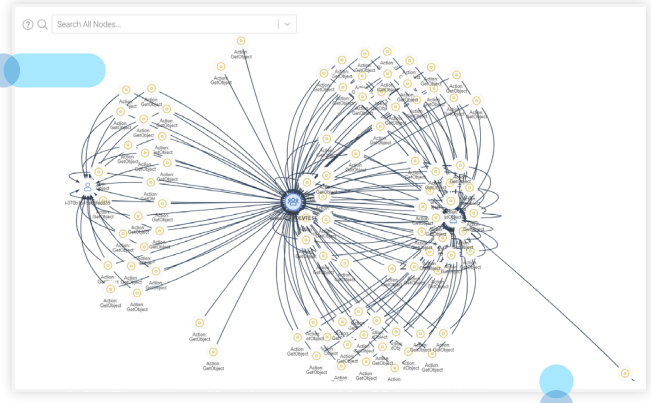


### Continuous monitoring of data access rights:

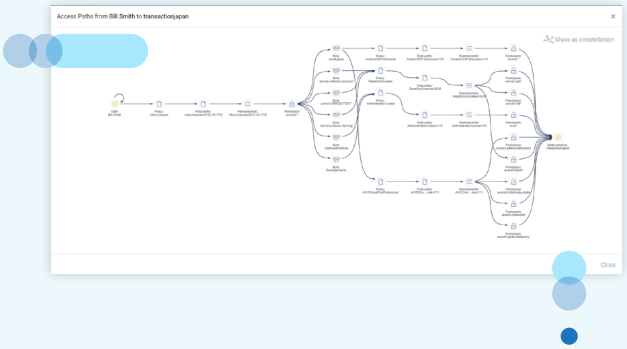
- Validate or re-validate all identities and systems which have access to sensitive data.
- Detect changes in access rights to any sensitive data.
- Monitor 3rd party account roles with access to sensitive data.
- Object level policy analysis. Both AWS and Azure allow for ACLs and public exposure of object level data. This is sometimes overlooked as people focus on the RBAC and Bucket Policies.
- Monitor access, permission, and lifecycle of encryption keys, secrets and certificates.
- Monitor public or account wide exposure of data.

### Continuous monitoring of data access activity:

- Monitor access from cloud identities and resources to sensitive data.
- Detect an anomalous change of access patterns to sensitive data or cloud resources.
- Monitor cross-geo movement of data.
- Identify mixed data classification based on resource relationships. For example, classified data should not be accessible on a network tagged for development or QA environments.
- Validate environment separation. Production workloads and data should not exist in the same boundaries as development.



# Identity Security, Governance and Permissions

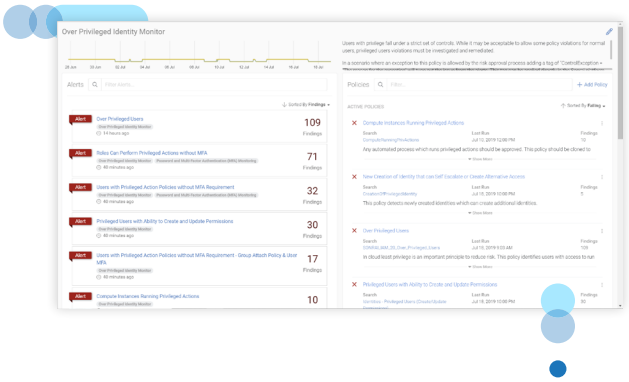


## Continuous Monitoring of Identity Privileges and Permissions:

- Validation or re-validation of all privileged identities per account, environment and based on tags.
- Identify over privileged identities which do not use privileged permissions they have been granted. Find identities that can self escalate their permissions using complex combinations of permissions from groups, roles, assumpts etc.
- Identify user, roles, compute, serverless that have permission to create alternative access or identities.
- Identify compute/serverless instances with permission to run privileged actions.
- Identify IAM or RBAC policies which could allow separation of duties violations in production.
- Detect separation of duties violations in production environments.
- Privileged users with control violations such as MFA requirements, access keys rotations.
- Validate separation of identities. Ensure that roles are not shared between production and development environments.

## Continuous Monitoring of Identity Activity:

- Anomalous activity from recently terminated users.
- Baseline identities that perform configuration changes to production and alert to changes.
- Detect identities which have created or changed an identity or policy that creates privileged access to sensitive resources.
- Monitoring of unapproved changes to any environment (requires integration with workflow).
- Identification of users creating service-based accounts with privilege as an alternative identity.
- Monitor automated workload or service accounts for changes in behavior




## Want to see Sonrai CDC in action?

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

sonraí SECURITY