sonraí SECURITY

De-Risk Your Public Cloud

Sonrai Security delivers an enterprise identity and data governance platform for AWS, Azure, Google Cloud, and Kubernetes. The Sonrai Dig platform is built on a sophisticated graph that identifies and monitors every possible relationship between identities and data that exists inside an organization's public cloud. Dig's Governance Automation Engine automates workflow, remediation, and prevention capabilities across cloud and security teams to ensure end-to-end security.

Eliminate all identity risks. Get to Least Privilege and stay there

This is critical in identity governance and the ephemeral nature of your cloud. It's extremely complex to keep track of what has access to what and if that permission is used. Dig maps every trust relationship, inherited permission, and policy for every entity. Identify all excessive privilege, escalation, and separation of duty risks across 1000's of roles, compute instances, and 100's of accounts.

Identity governance can reduce risk and strengthen security with insight to:

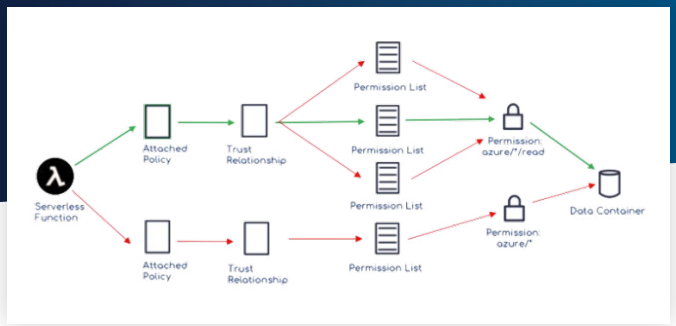
- Least Privilege
- Separation of Duties
- Toxic Combination
- Dormant Identities
- Who and What Has Access Rights?

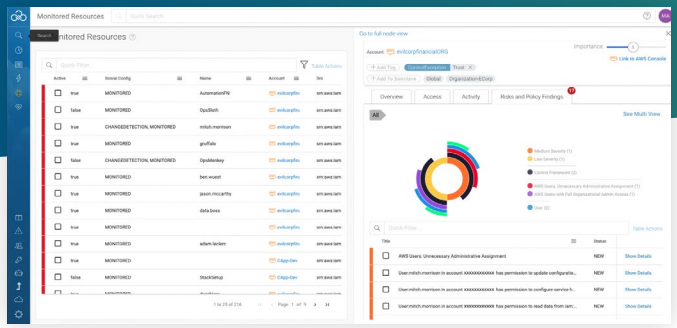
Discover, Classify, Lock Down, and Monitor "Crown-Jewel" Data

Sonrai Dig finds all stores and verifies rights. Not just what is accessing it, but everything that can potentially access it. If you have classified your data, Dig leverages that classification. But if you haven't, Dig classifies it for you. For structured and unstructured sources, Dig will learn about what's inside if it's PII. After we have found it, and classified it, Dig helps you lock it down.

Data governance provides control and maintains visibility to data through:

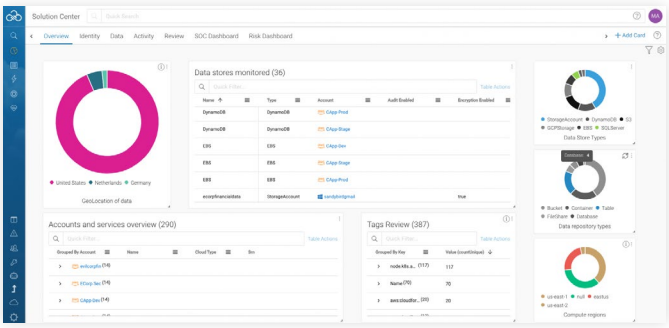
- Least Access
- Identify & Classify Data
- Track Data Movement
- Monitor Crown Jewels

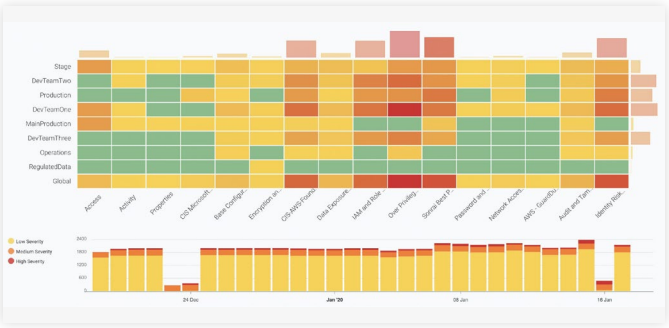




sonraisecurity.com | info@sonraisecurity.com | 646.389.2262

sonraí SECURITY





Unify Compliance and Platform Configuration Monitoring

Sonrai Dig delivers a platform for you that is the basis of a cloud security and risk operating model that spans cloud providers, container platforms, 3rd party data stores, and key stores. Data sovereignty, data movement, and identity relationships are all monitored and reported to ensure conformance to GDPR, HIPPA and other compliance mandates. Resolutions are coordinated with relevant DevOps teams.

Cloud Security Posture Management continuously manages cloud security risk for:

- Cloud Misconfiguration
- Compliance Enforcement
- Drift Detection

Governance Automation Engine Helps Companies Shift Left and Integrate Teams

Do you have too many alerts going to the wrong teams? Sonrai Dig's Governance Automation Engine organizes alerts and actions in the way you organize your cloud. The platform is API driven so it tightly integrates into your CI/CD pipeline. Dig also automatically dispatches prevention and remediation bots and provides safeguards in the form of code promotion blocks to help to ensure end-to-end security in public cloud platforms.

Governance Automation allows companies to shift left and integrate teams through:

- Automated Workflow to DevOps
- Automation Through APIs
- Remediation & Prevention
- Blocking Code Promotion

Ready to De-Risk Your Public Cloud?

Trust Sonrai Dig to govern identities and data across AWS, Azure, Google Cloud, and Kubernetes.

Request a demo.

sonraísecurity.com | info@sonraísecurity.com | 646.389.2262

sonraí SECURITY