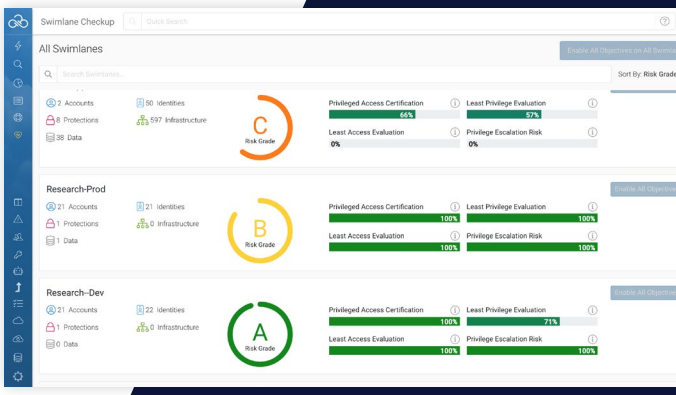
sonraí SECURITY

Sonraí Dig on Microsoft Azure

Who Can and Has Accessed Azure Resident Data, Resources, and Infrastructure?

Organizations building applications on Azure quickly discover how important identity and access management (IAM) is to securing data resident in public cloud. A poor Azure AD configuration can expose corporate data to potential breaches by an external actor or an over-permissioned insider. Sonrai Dig, our identity and data governance platform, helps organizations understand and monitor Azure AD to eliminate weak or accidental configurations that if left unchecked, will inevitably lead to a disaster.



Available on **Microsoft Azure Marketplace**

Increase Visibility into Azure Workloads

- Cross-subscription configuration checks for possible data exposure from poor usage of configuration and trust relationships
- Automated alerts for over-privileged identities and compute
- Timely notification of high risk workloads, network, and resource configurations

Address Identity and Data Governance Concerns

- Who has accessed sensitive resources and data?
- Who can access Azure workload data and their components?
- Does the Azure AD configuration properly protect data if a credential is stolen or misused?

Secure Azure Data Stores & Support More Services

- Data stores including Storage Accounts, Microsoft SQL, and more
- Compute including VM, Azure Functions, and more
- Other services including Azure Key Vault, networks, load balancers, firewalls, and more

Assess Azure Policy Change Risk Auto-remediation

- Continually monitor configuration drift against an approved baseline
- Integrated use of Azure resource tags to align risk with-workload classifications
- Strong audit capabilities of changes to configuration and data access

Ready to graph, identify, and monitor identities and data inside your Azure? Request a demo today.

sonraísecurity.com | azureteam@sonraísecurity.com | 646.389.2262

sonraí SECURITY