

RMS Chooses Sonrai Dig to Reduce Risk, Increase Security, and Maximize Efficiency



Risk Management Solutions, Inc. (RMS) is a leading technology company that focuses on delivering catastrophe risk modeling to help insurers, financial markets, corporations, and public agencies evaluate and manage risk. Insurers, reinsurers, trading companies, and other financial institutions trust RMS to better understand and manage the risks of natural and humanmade catastrophes, including hurricanes, earthquakes, floods, terrorism, and pandemics.



The Problem

RMS wanted greater visibility into the total number of cloud accounts across AWS and Azure and whether these accounts were configured appropriately. More importantly, they wanted greater insights into how data could be accessed across these public cloud environments by the large number of active compute instances. As a subsidiary of Daily Mail General Trust, RMS adheres to comprehensive compliance checks and mandates since they hold data for many companies across the globe. Tracking data movement and access is critical for mandates like GDPR.



“Sonrai Security provides us with complete visibility of platform, identity, and data risks across our large AWS and Azure cloud infrastructure. The platform has become the cornerstone of the RMS public cloud risk management and security program.”

Kyle Watson
Security Architect of RMS



The Goals

Initial deployment of the Sonrai platform highlighted 3 key areas of concern. First, there were tactical issues and platform configurations that needed remediation. Second, there were some unmanaged legacy cloud accounts that were interacting with RMS core cloud accounts. Lastly, there were gaps in security best practices that needed to be addressed at the development level. These issues included key rotation issues, open network groups, and identities that were too over-permissioned.

Maximize Efficiency

RMS understands the complexity of managing roles and privileges in the cloud. Their goal was to quickly remediate tactical issues and platform configurations. With issues sent directly to the teams that are responsible for them as opposed to a centralized queue, the RMS teams can reduce alert fatigue and missed alerts but also enables the team to run its operations at the speed of the cloud.

Reduce Risk

The team needed to find unmanaged cloud legacy accounts including all data stored in the cloud that may be interacting with RMS core cloud accounts. Then the data and identities needed to be classified, including the baseline access patterns and any security deviations.

Increase Security

They wanted their cloud migration to be built off a foundation of strong operational security, and quickly realized traditional first-generation would fall short. An exploding number of roles and identities would add identity and access complexity which, combined with increasing alerts, would have raised the risk to an unacceptable level.



The Results

The Sonrai platform easily solved the issue of activity monitoring across the cloud by gaining visibility and trust relationships across all accounts. By understanding interactions and originating identities, RMS was able to identify and establish all trust relationships between accounts. Compliance and platform posture gaps were quickly addressed as Sonrai identified problems at their source. Finally, the Sonrai platform's continuous monitoring of identity, access, and least privilege ensures best practices are adopted across RMS DevOps teams.

“Sonrai Security helped us identify a number of legacy cloud accounts that we had believed were shut down, that were actually still active and in use.”

Kyle Watson | Security Architect

Want to see Sonrai Dig in action? [Request a demo today.](#)