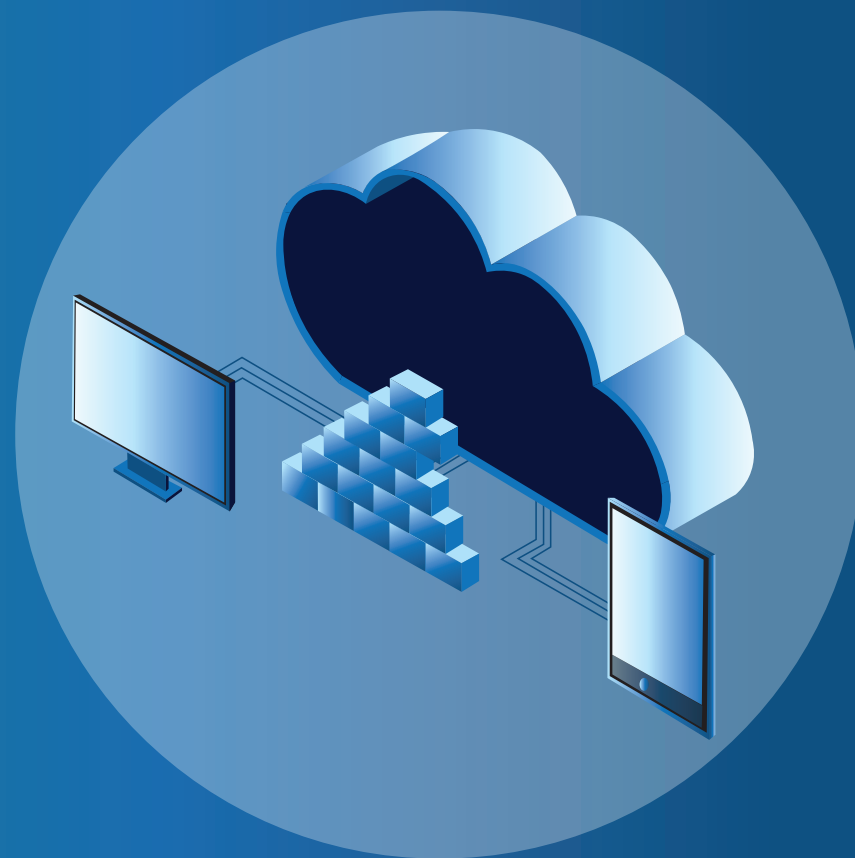


# Lock Down Crown Jewel Data

Not all data is created equal. Crown Jewel data is the most precious set of data in your Cloud system. It contains sensitive information, such as PII such as passwords, credit details, and key cyber assets that regulate your daily operations. Data breaches cost companies around the world millions of dollars and a fraction of your overall data represents three-quarters of your company's market value.

Adversarial threats can cause serious trouble for your organization if they've gained access to your crown jewel data. Unprotected data serve as vulnerabilities that are easily exploited by opportunistic agents. Hence, it is vital that organizations maintain optimal security of their data storage by prioritizing those files and locking them down.



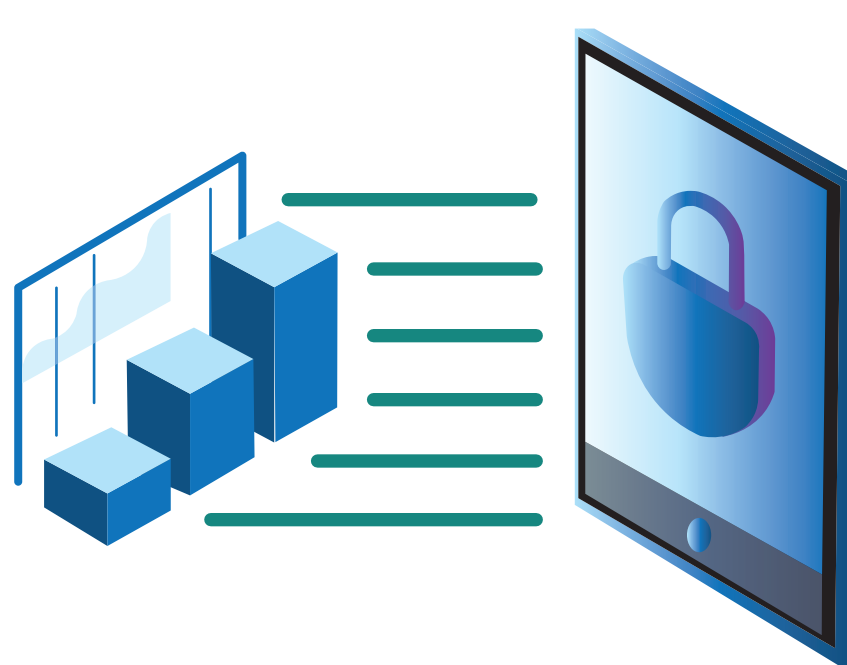
## Common Threats to Crown Jewel Data in Misconfigurations

The two risks are internal and external. Internal is insider threats, misconfigurations, confidential integrity, and the availability of data. Follow the security CIA of crown jewel data.

**Threats to Crown Jewel data may be divided into two categories:**



Accidental threats, due to the configuration negligence of Cloud users within the company



Data theft and exploitation

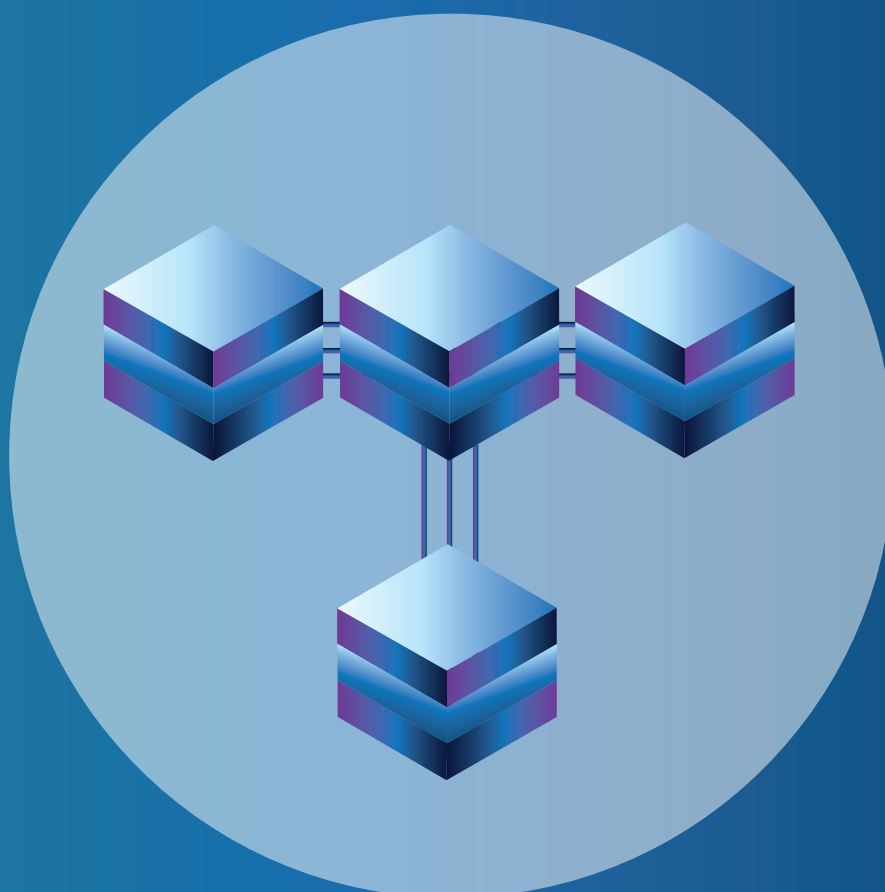
## The Sonrai Security Solution

Sonrai's Dig is an advanced cloud governance solution that ensures your crown jewel data are verified and locked down for maximum protection. Our solution is built upon the latest developments in identity governance and critical data monitoring. We cannot stress enough that your Crown Jewel data are business-critical information that must never fall into the wrong hands. As such, we de-risk your Cloud giving users peace of mind through:



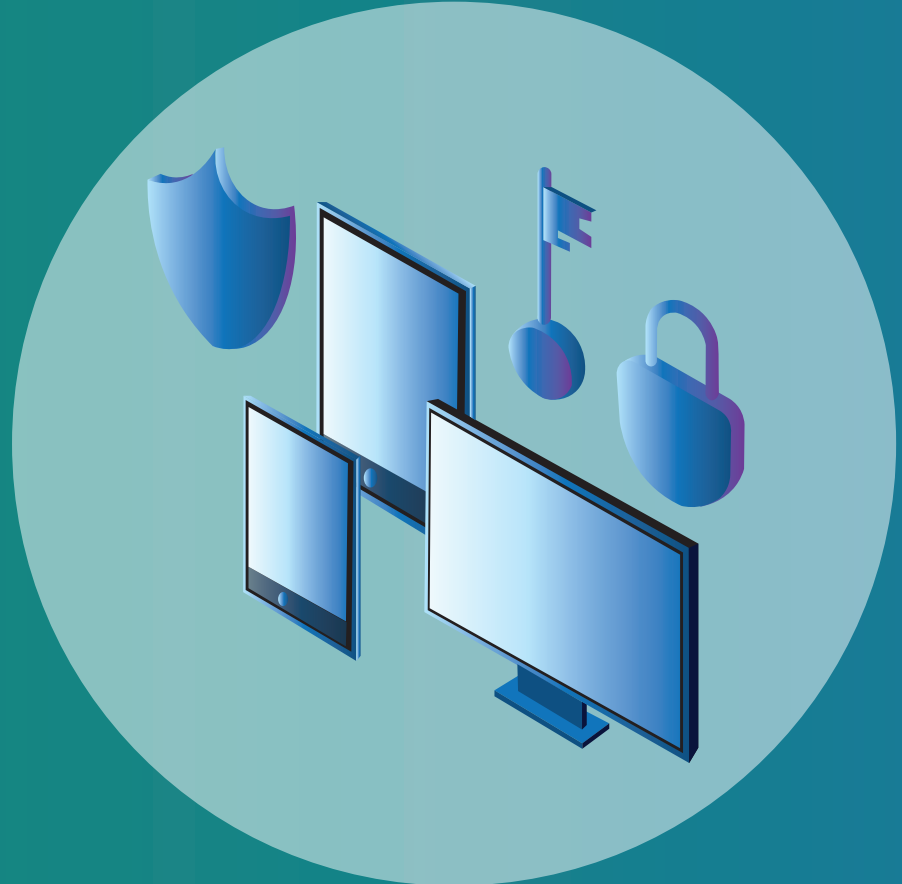
### Identity Governance

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.



### Data Governance

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.



### Cloud Security Posture Management

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, HIPAA and other compliance mandates. Resolutions are coordinated with relevant DevOps teams.



### Governance Automation

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.

Security is your trusted solution in advanced Cloud security solutions. Speak with one of our experts today to receive a of your workplace systems.