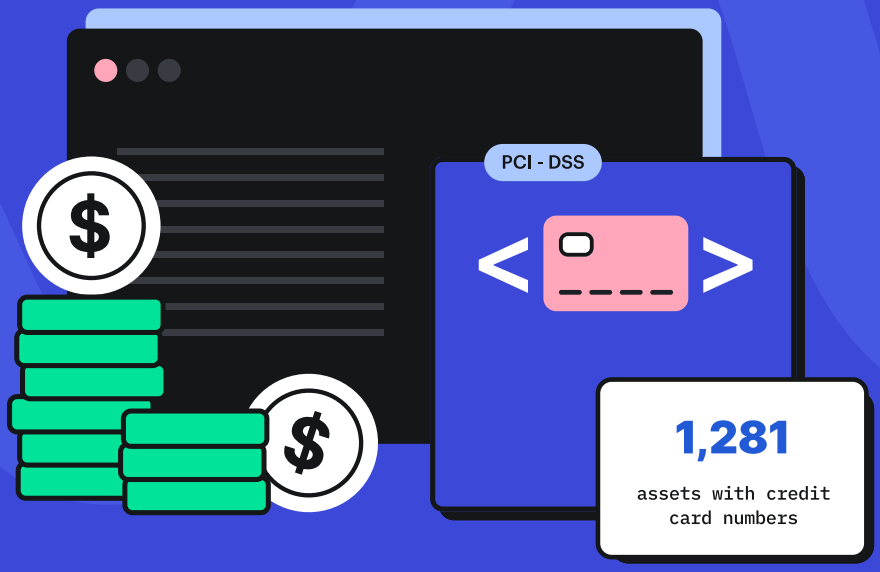


Dig for Financial Services

Protect financial data in multi-cloud environments

Dig Security

The Need

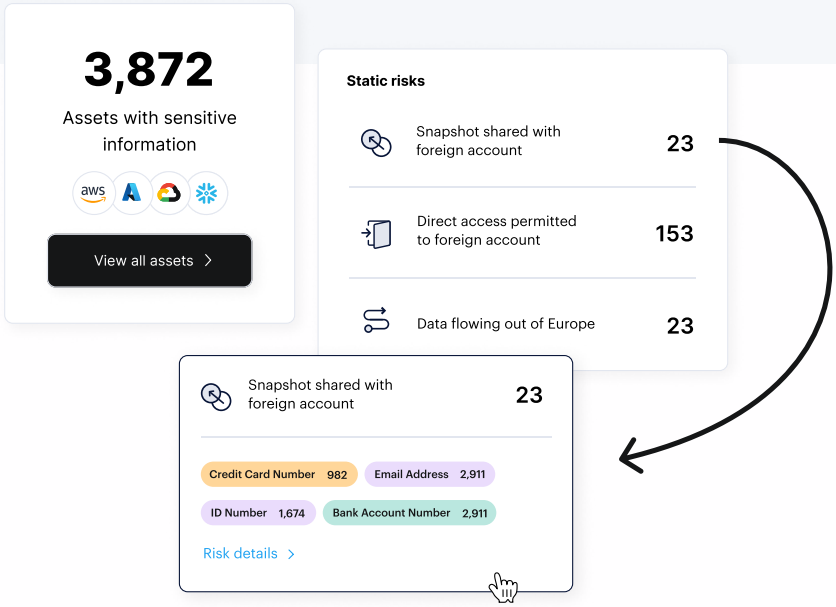
It is no surprise that the financial services industry is a leading and tempting target for cyber criminals. The average cost of a breach in the industry is over $5.7 million, and the average cost of a ransomware breach is more than $4.6 million.[1] Meanwhile, the average cost to recover from a ransomware attack is $1.85 million.[2]

At the same time, organizations must comply with an increasing number of ongoing and stringent industry regulations, such as GLBA, SOX, SOC-2, and GDPR.

Current data security offerings fall short when it comes to protecting data in the cloud. On the one hand, data leakage prevention (DLP) solutions are ineffective beyond the organization perimeter. On the other hand, cloud security posture management (CSPM) solutions focus on infrastructure and lack a data-centric view.

Moreover, cloud-native solutions lead to more data fragmentation issues, with each solution impacting only one part of a much bigger picture.

By reducing the overall risk of data exposure in the cloud, securing your financial data, and responding to breaches in real time, you will reduce your mean time to detect (MTTD) new incidents, avoid financial losses, and ensure compliance with industry regulations.



[1]Cost of a Data Breach Report 2022, IBM Security

[2]Ransomware is Changing – Are You Ready, Gartner 2022

The Dig Solution

Dig Security offers an agentless, multi-cloud data security platform that discovers and classifies your client information to protect it from ransomware on all cloud services, including AWS, Azure, GCP, and Snowflake.

Leveraging full data security posture management (DSPM) capabilities, Dig prevents exposure of sensitive data by highlighting data misconfigurations, access anomalies, and data vulnerabilities that increase the risk of a data breach if not remediated.

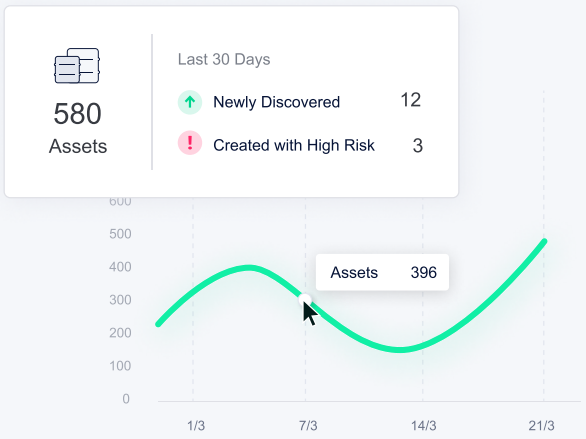
In addition, the platform extends its DSPM capabilities to address risk changes in real time via data detection and response (DDR). Integrating with your existing security solutions and workflows, Dig ensures immediate handling of incidents triggered by newly discovered data.

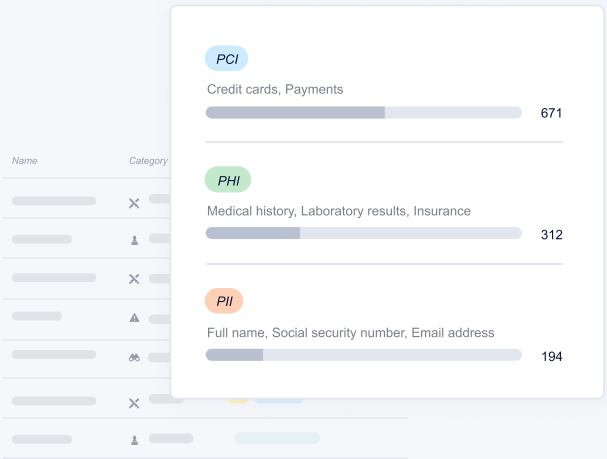
- Combines DLP, DSPM, and DDR capabilities to provide the highest level of data protection
- Applies threat modeling in a single policy across multiple deployments to create a unified view of all cloud data exposure issues
- Protects any data asset on any cloud with a single consolidated policy engine

Features & Benefits

01 / Reduce data exposure risk with deep visibility into structured and unstructured data sets

- Discover financial data assets on AWS, Azure, GCP, and Snowflake
- Identify security blind spots such as database backups that contain financial information
- Save time with automated classifiers for all major regulations, including FTC, GLBA, and SOX
- Define custom classifiers to find sensitive information across managed and unmanaged data assets



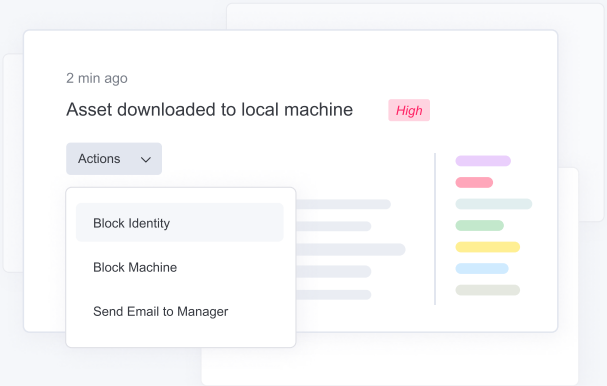


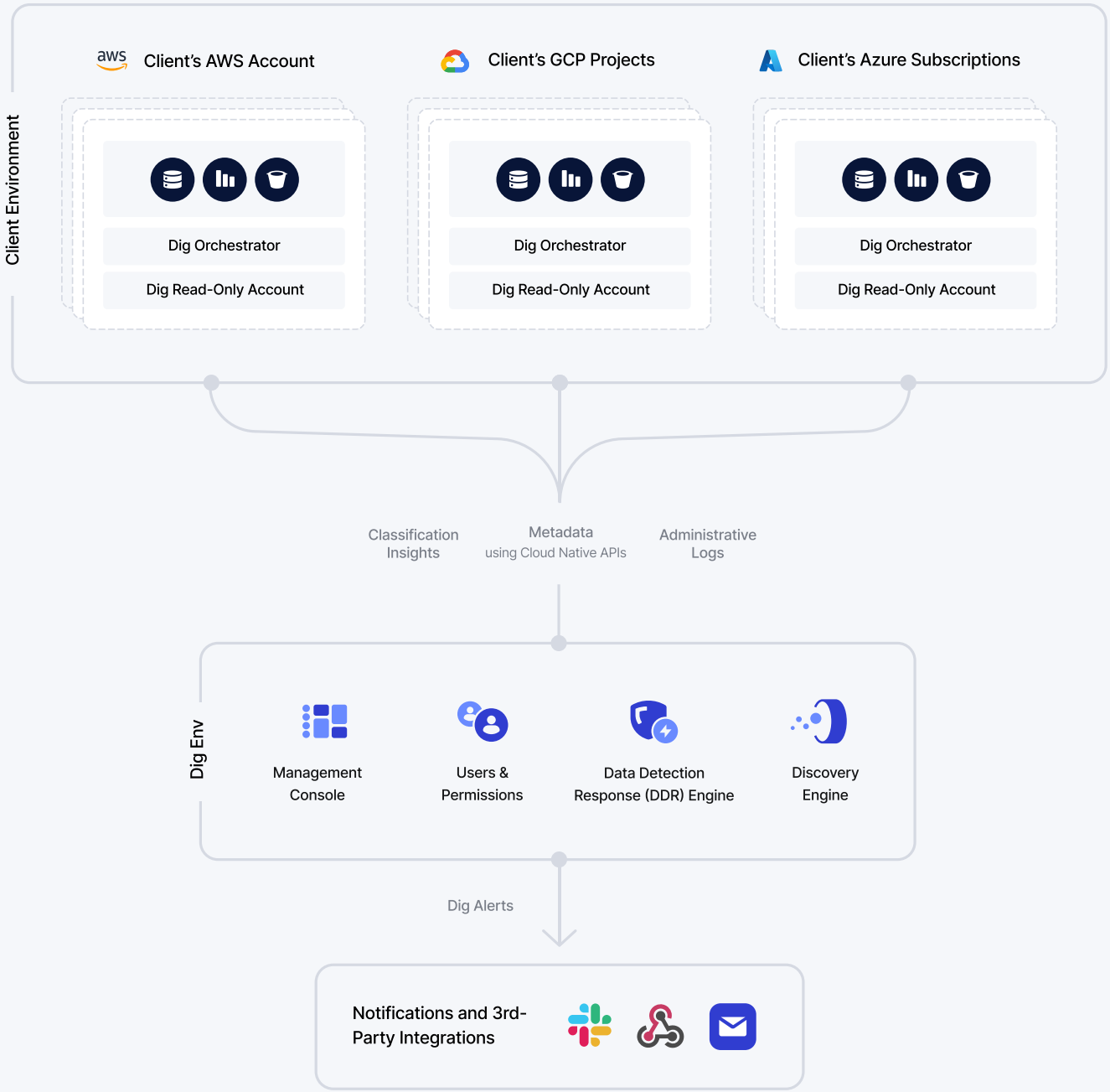
02 / Secure financial data by reducing the risk associated with misconfigured data

- Assess your data security posture across all data assets, including access permissions, data misconfigurations, and active identities
- Prioritize remediation with a data-first approach to improve your loosely configured access permissions on your most sensitive data assets

03 / Save money and mitigate incidents by responding to data breaches in real time

- Monitor data-threat model changes and issue real-time alerts when new risks are detected
- Ensure the entire DDR cycle by seamlessly integrating with IAM and SOC solutions



04 / Technical Integrations

- Works with major public cloud providers, including AWS, Azure, GCP, and Snowflake
- Allows for real-time alert notifications (DDR) by email, Slack, and Webhooks, enabling security operations to take consolidated actions (e.g. SOAR, SIEM, and SOC solutions)
- Connects with an existing IdP to provide a rich view of active identities for each data asset in order to add a context layer for making access decisions on sensitive data