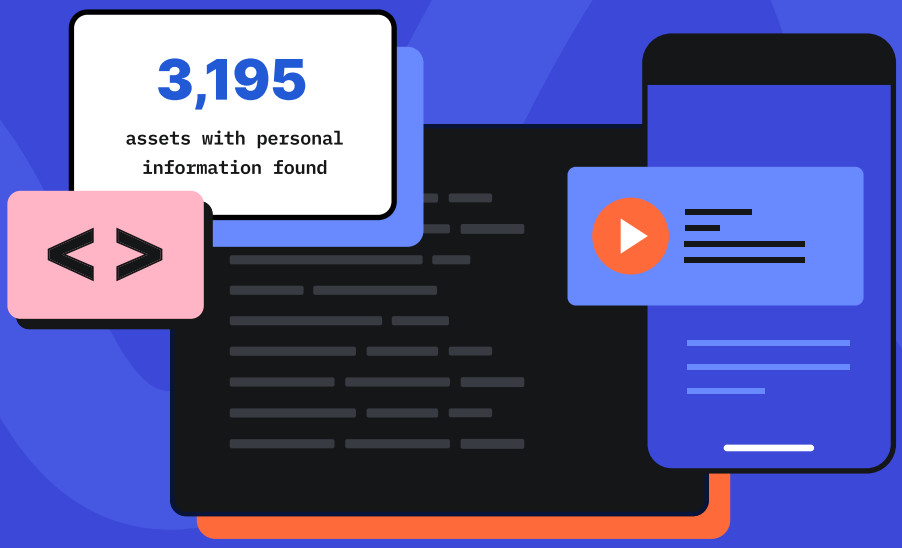


Dig for Tech Companies

Protect customer information in the cloud

Dig Security

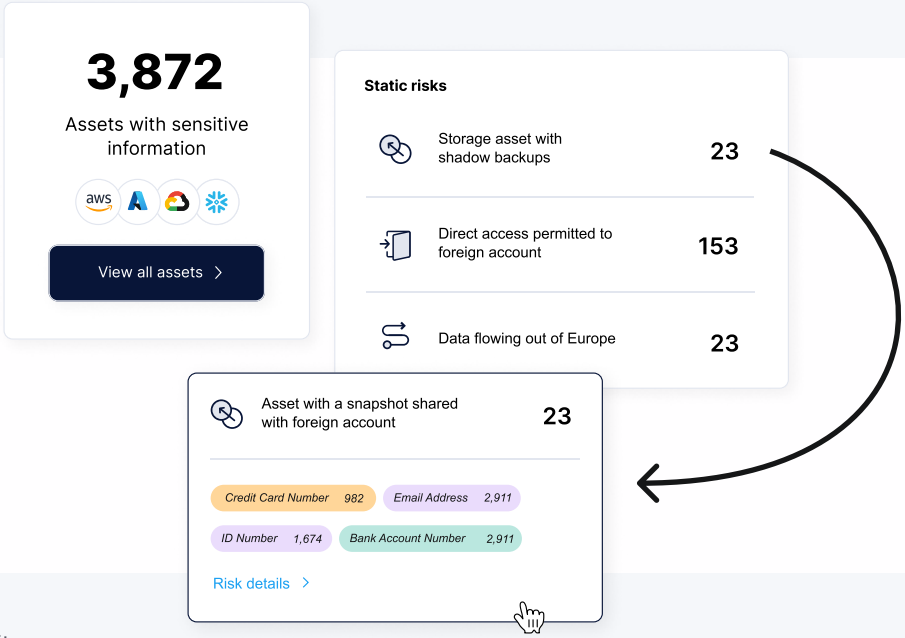
The Need

High-tech organizations are renowned as one of the earliest adopters of cloud services. Given its long and proven track record, the industry is also continuously exposed to new, unprecedented risks – risks that extend the attack surface and make tech companies vulnerable to data exfiltration and cyberattacks. According to IBM[1], the average cost of a data breach in the industry is $4.9 million, and the average cost of a breach at organizations with 1,000-5,000 employees is $4.1 million. Meanwhile, the average cost to recover from a ransomware attack is $1.85 million, according to Gartner[2].

In addition, DevOps teams and data scientists require full access to data to ensure innovation velocity. That's why high-tech companies must implement security measures that protect their data while not impeding the pace of innovation.

Finally, high-tech organizations must comply with more and increasingly stringent privacy regulations such as EU GDPR, US CCPA, and FTC.
Unfortunately, current 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, 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 locating and identifying your client data across multiple cloud environments, you can not only secure your customer data, but also ensure compliance.



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.

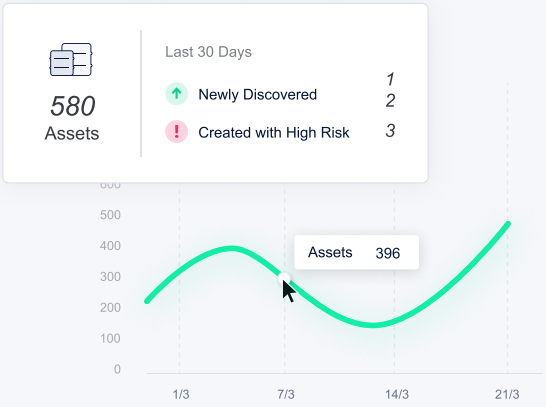
In addition, the platform extends its DSPM capabilities to address risk changes in real time via data detection and response (DDR). Integrating with your existing security solutions and workflows, Dig ensures immediate handling of incidents triggered by newly discovered data.

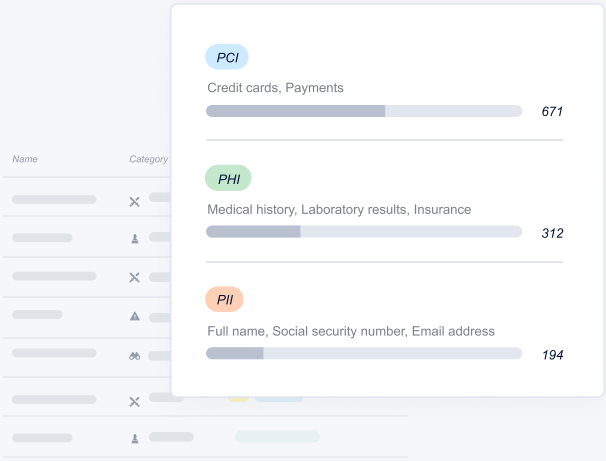
- Combines DLP, DSPM, and DDR capabilities to provide the highest level of data protection
- Applies threat modeling in a single policy across multiple deployments to create a single view of all cloud data exposure issues
- Protects any data asset on any cloud with a single consolidated policy engine

Features & Benefits

01 / Protect customer information and reduce your data attack vector

- Gain visibility across all of your data, and find shadow data such as old backups and snapshots no longer in use
- Discover sensitive data, including secrets, IP, and other “crown jewels” on AWS, Azure, GCP, and Snowflake
- Ensure that your data remains within allowed services



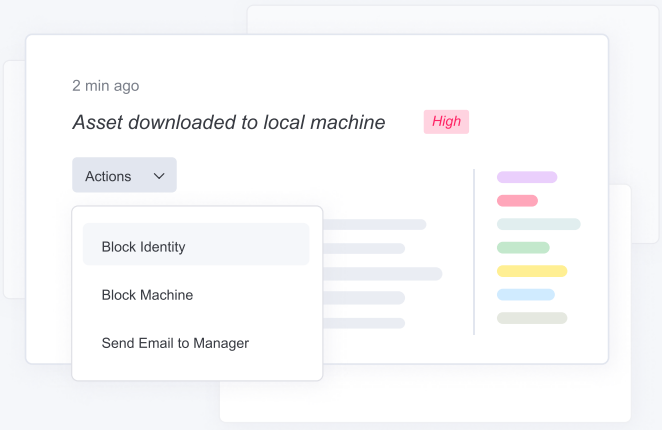


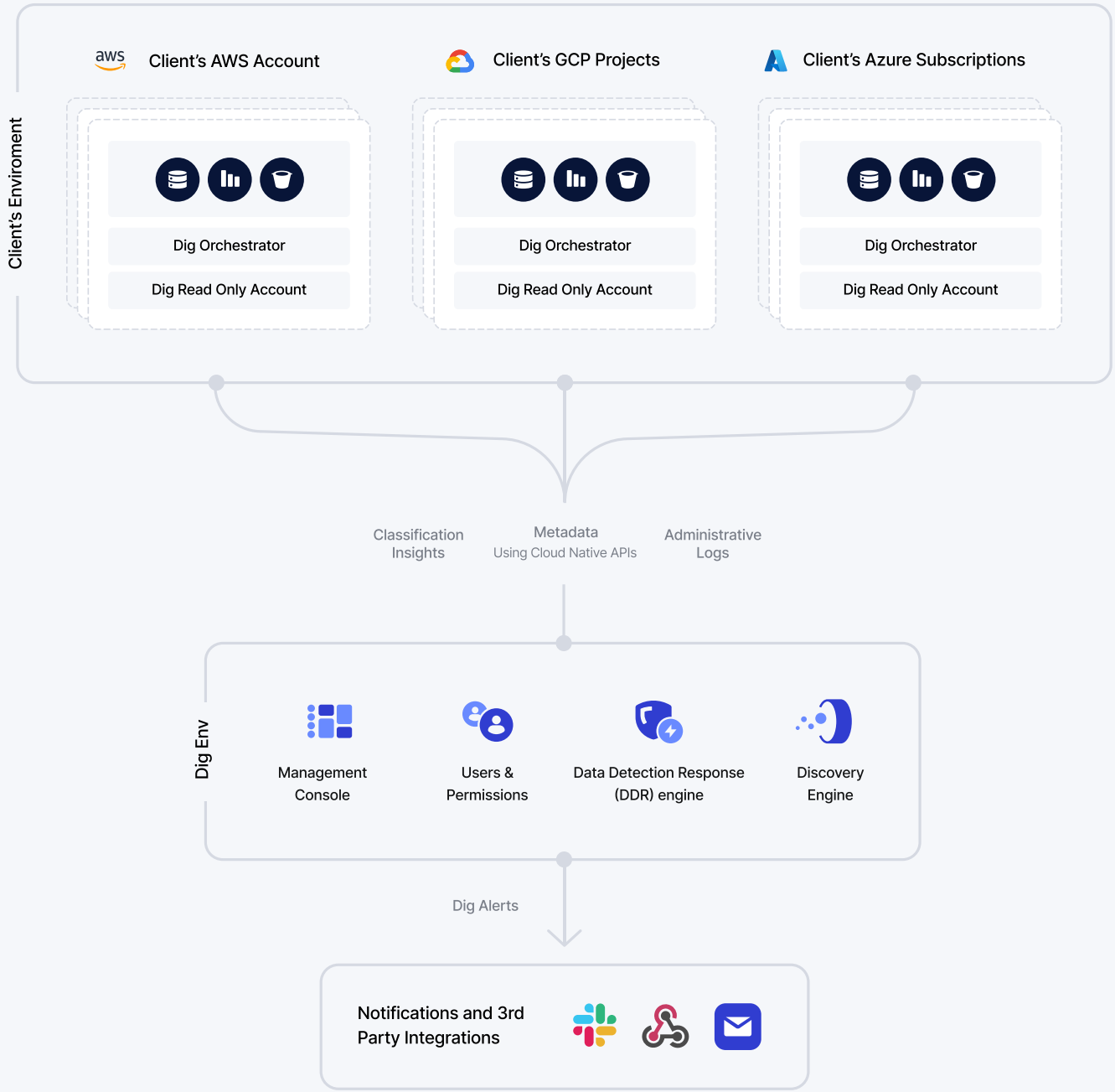
02 / Ensure that your data remains within allowed services

- Assess the security posture of sensitive data across multiple cloud solutions to tighten your internal policies
- Prioritize remediation with a data-first approach to improve your loosely configured access permissions on your most sensitive data assets

03 / Ensure innovation velocity while avoiding breaches

- Monitor data-threat model changes and issue real time alerts when new risks are detected to enable immediate reaction to breaches
- Consolidate your data response with your security operations team to avoid duplicating efforts
- Consolidate your data response with your security operations team to avoid duplicating efforts



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