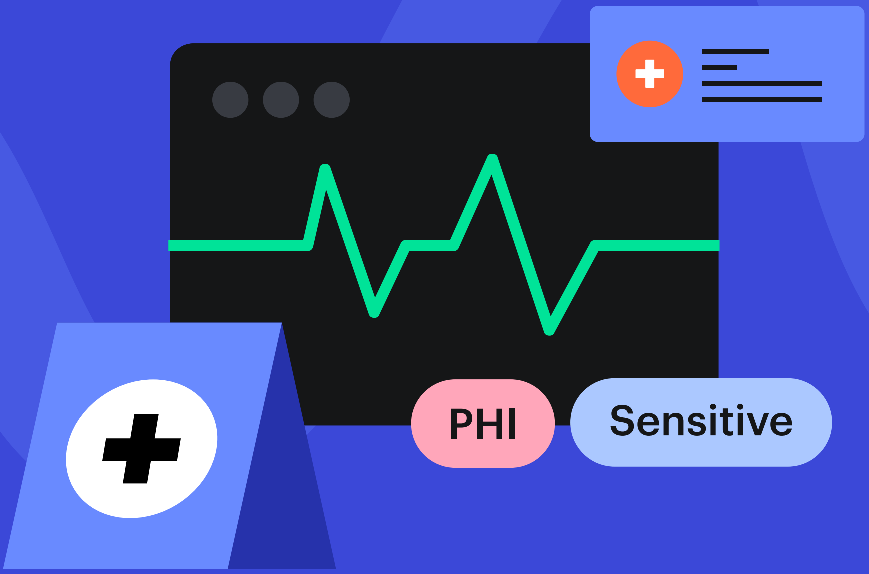


Dig for Healthcare

Protect patient information in cloud environments

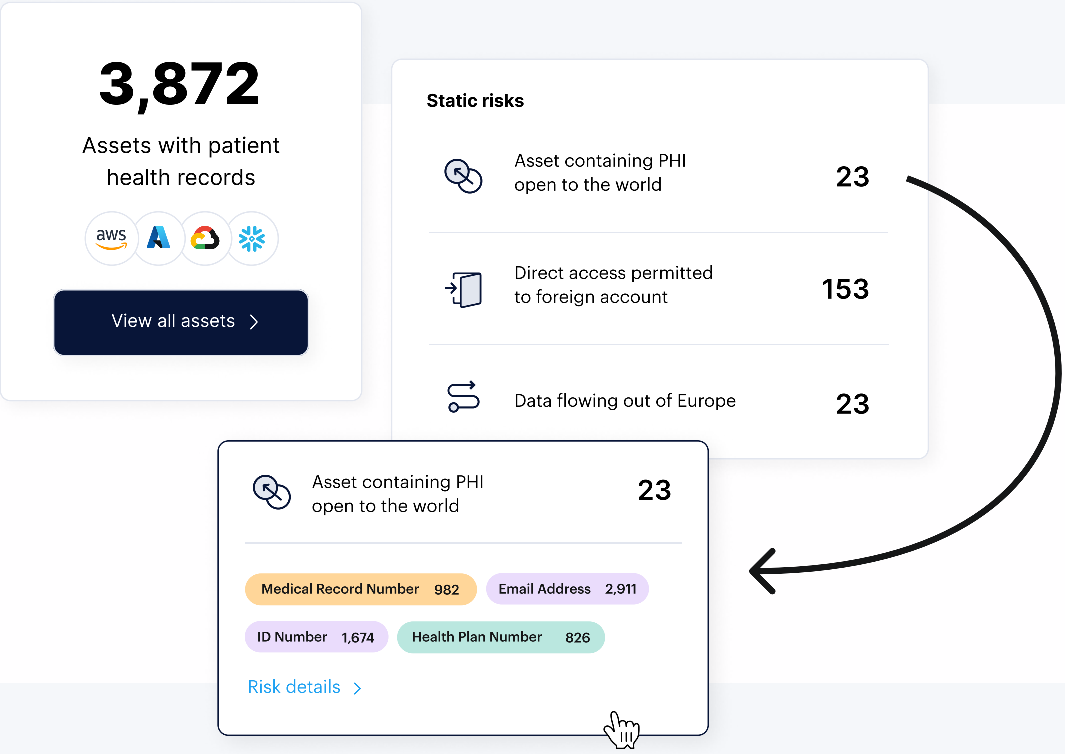
Dig Security

The Need

Modern healthcare organizations are feeling the impact of unprotected patient data – directly in their pocket. The cost of a data breach in the industry tops $9 million[1]. The average ransomware payout is over $211,000[2]. And each healthcare organization pays, on average, nearly $2 million in HIPAA penalties[3].

Unfortunately, current data security offerings fall short when it comes to protecting patient health records in the cloud. On the one hand, traditional 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 identifying exactly where your PHI data resides across various public cloud environments, you can not only keep your most sensitive data secure, but also avoid penalties and ensure HIPAA compliance.



3,872

Assets with patient health records

Static risks

Asset containing PHI open to the world	23
Direct access permitted to foreign account	153
Data flowing out of Europe	23

Asset containing PHI open to the world	23
Medical Record Number	982
Email Address	2,911
ID Number	1,674
Health Plan Number	826

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

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

[3] https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

The Dig Solution

Dig Security offers an agentless, multi-cloud data security platform that discovers and classifies your patient data and medical records, including those from third-party suppliers. Dig's advanced solution ensures compliance requirements and protects your healthcare data from ransomware and other cyber attacks across all cloud services, including AWS, Azure, GCP, and Snowflake.

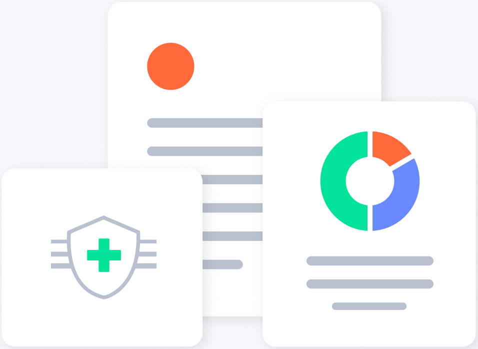
Leveraging full data security posture management (DSPM) capabilities, Dig prevents exposure of sensitive data by highlighting data misconfigurations, access anomalies, and data vulnerabilities that increase the risk of a data breach if not remediated.

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.

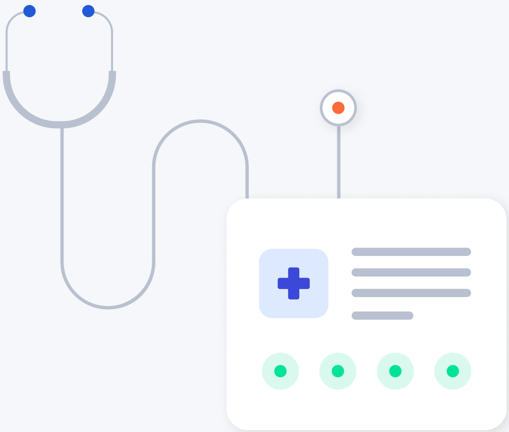
- Combines DLP, DSPM, and DDR capabilities to provide the highest level of data protection
- Applies threat modeling in a single policy across multiple deployments to create a unified view of all cloud data exposure issues
- Protects any data asset on any cloud with a single consolidated policy engine

Features & Benefits

01 / Maintain round-the-clock HIPAA compliance readiness



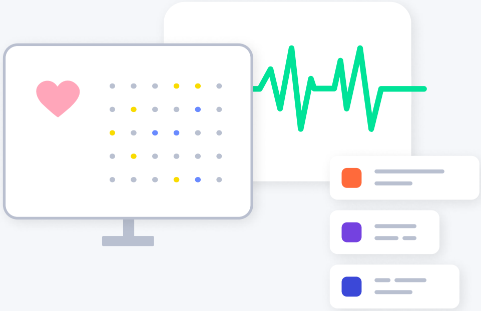
- Gain full visibility into all PHI and medical records located within your cloud services
- Apply a single-policy engine to track data movement changes and avoid unnecessary penalties
- Receive real-time notifications of newly detected risks to ensure proper remediation control



02 / Prevent data leakage by strengthening your data security posture

- Assess the security posture of sensitive data to tighten your access policies
- Prioritize remediation with a data-first approach to improve your loosely configured access permissions on your most sensitive data assets
- Monitor data-threat model changes and issue real-time alerts when new risks are detected

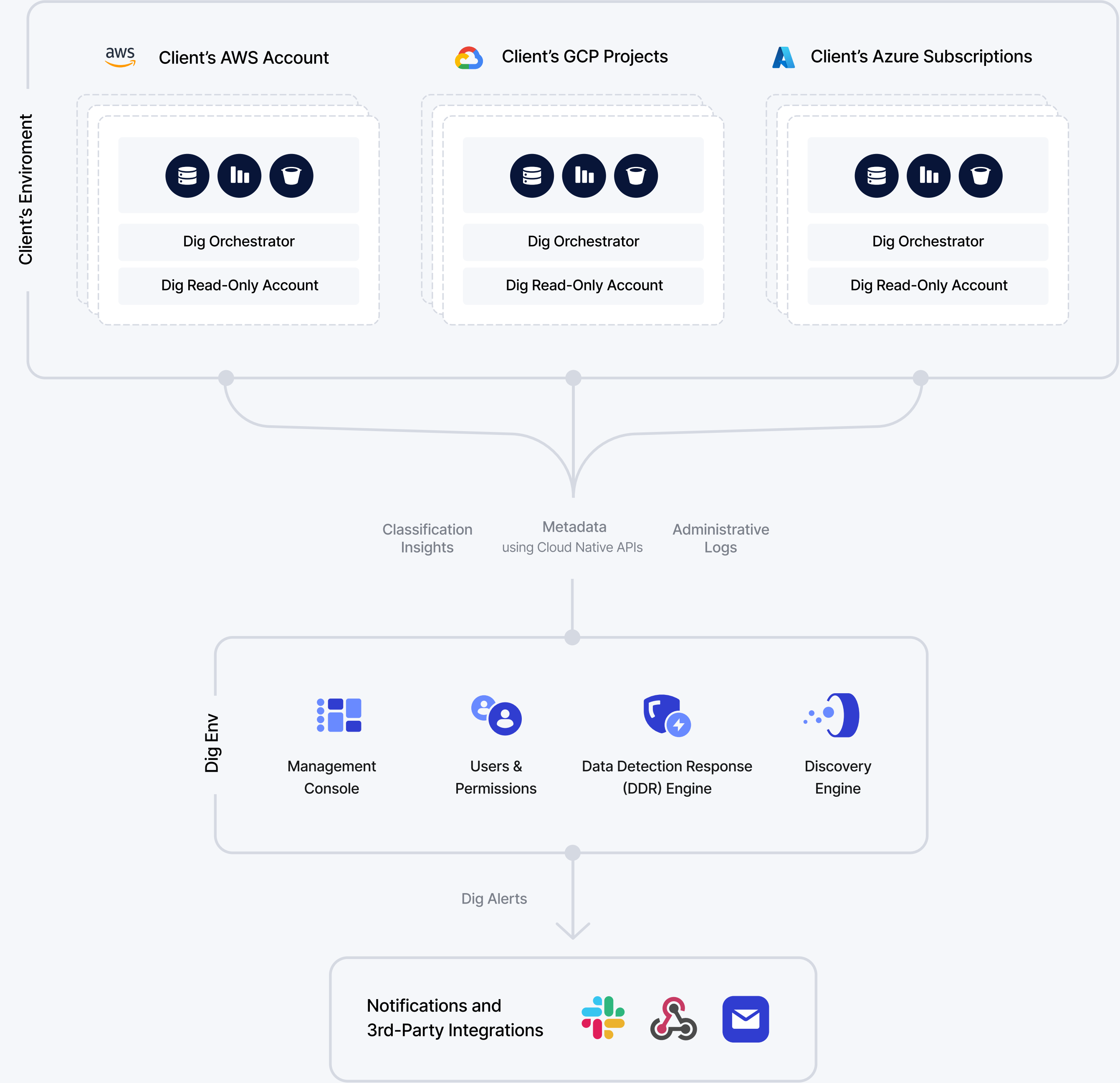
03 / Protect patient data and medical records from ransomware



- Find PHI and other sensitive data on AWS, Azure, GCP, and Snowflake
- Ensure that data remains within allowed services

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


Client's Enviroment
Client's AWS Account
Client's GCP Projects
Client's Azure Subscriptions
Dig Orchestrator
Dig Read-Only Account
Dig Orchestrator
Dig Read-Only Account
Dig Orchestrator
Dig Read-Only Account
Classification Insights
Metadata using Cloud Native APIs
Administrative Logs
Dig Env
Management Console
Users & Permissions
Data Detection Response (DDR) Engine
Discovery Engine
Dig Alerts
Notifications and 3rd-Party Integrations