Dig Security

Multi-Cloud Data Security Platform with Real Time Data Detection and Response (DDR)

Discover sensitive data assets across cloud deployments (IaaS PaaS and DBaaS), boost your data security posture and stop early attempts of data exfiltration that could lead to a breach

Data is fueling today's economy.
Decision makers at all levels of the business leverage data to drive their company's growth and success. Meanwhile, data continues to sprawl from the organization to cloud deployments, spreading beyond the reach of existing data security solutions. While the business is pushing forward, the onus lies with the data security team to protect the organization from the threat of a breach and maintain compliance, all while not interfering with the ongoing business processes.

What you need is a solution that discovers, classifies and protects sensitive data assets across cloud data platforms, one that detects all the suspicious incidents related to data in real time and which can integrate with your security workflows for rapid resolution - **you need Dig Security.**
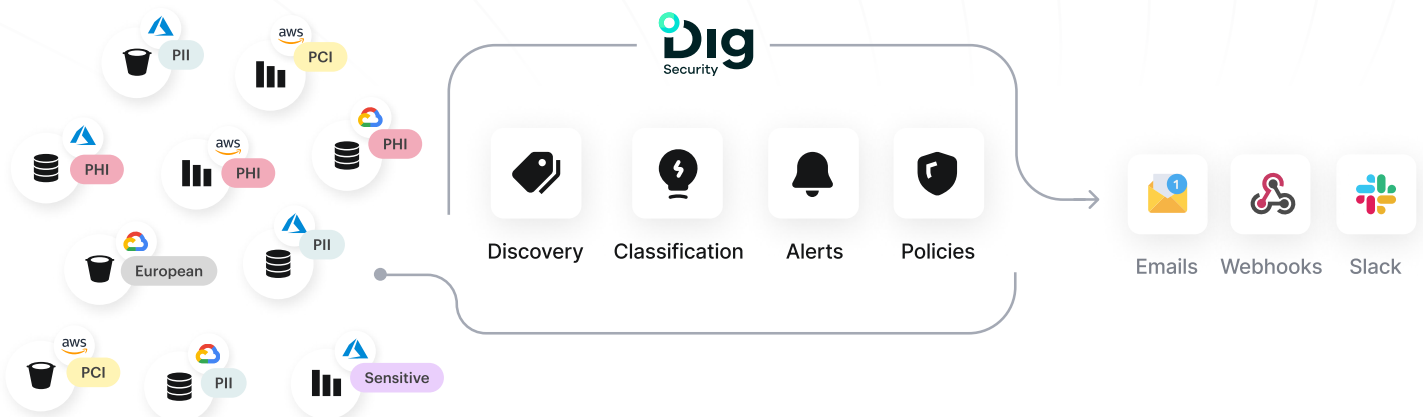
> " This is a type of visibility we just simply don't have today. Looking at this from a data-first view is a game changer for us "

CISO, Financial Services Corp

MARKETECTURE

Dig Security

Discovery · Classification · Alerts · Policies

Emails · Webhooks · Slack

Why Dig Security?

The only data security platform that combined all capabilities into one single solution:

Data Security Posture Management (DSPM) - highlights data misconfigurations, access anomalies and data vulnerabilities

Data Leak Prevention (DLP) - prevents data exfiltration early in the kill chain

Data detection and response (DDR) - a real time engine that issues alerts as soon as a suspicious activity has occurred

Want to see how we Dig?
Request a demo at dig.security

Features & Benefits

> Automated discovery of data assets in public clouds including AWS, Azure, GCP and Snowflake to gain visibility into where data resides and reduce data sprawl

> Data classification with automated classifiers for PCI, PII, PHI, FTC, GDPR, CCPA and others to locate where sensitive data resides and ensure compliance with latest security and privacy regulations

> Data detection and response (DDR) through continuous monitoring to evaluate attacks in real time and immediately respond to cyber threats

> Prioritization of data security posture issues based on context to reduce the amount of "noise" that leads to "alerts fatigue"

> Improved compliance assurance and risk management through reports for data teams and data owners

Watch a demo

About Dig Security

Dig Security helps organizations discover, classify, protect and govern their cloud data.
Dig's cloud-native and completely agentless approach re-invents cloud DLP with DDR (Data Detection & Response) capabilities to help organizations better cope with the cloud's data sprawl. Dig is founded by 3 cyber security veterans from Microsoft and Google, and is backed by Team8, SignalFire, Felicis, Crowdstrike, Okta Ventures, CyberArk Ventures, and Merlin Ventures.

Dig
Security