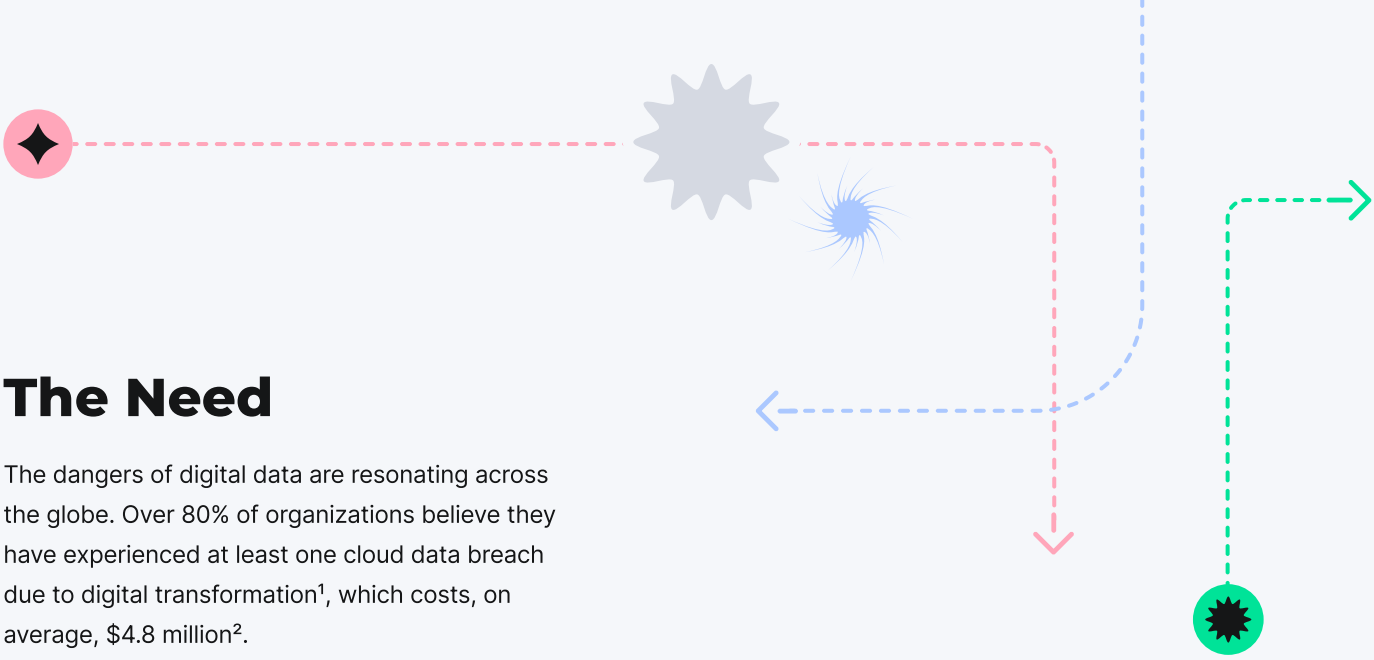
Dig for Cloud DLP

Apply an agentless, cloud-native DLP solution to prevent data leakage across myriad services

Dig Security



The Need

The dangers of digital data are resonating across the globe. Over 80% of organizations believe they have experienced at least one cloud data breach due to digital transformation[1], which costs, on average, $4.8 million[2].

Why the fear? Data democratization, the use of cloud technologies such as microservices, and constant sharing of data in and outside of the organization have generated a huge data sprawl. This leaves security leaders with poor visibility as to where sensitive data resides, how it moves across different clouds, and who is accessing it. That explains why, without an effective solution, it takes 277 days, on average, to identify and contain a data breach[3]. And if that's not enough, industry and compliance regulations involving data privacy, data sovereignty, and data security are on the rise.

Unfortunately, existing solutions are not doing the trick. On the one hand, traditional, agent-based data leakage prevention (DLP) solutions cannot scale to protect cloud data. They rely on the network or the endpoints, neither of which is involved in most cloud data breaches. On the other, cloud provider solutions also fall short of the mark. Despite offering DLP capabilities, they cover only a fraction of all available services, do not trace the lineage of data when it travels beyond the cloud, and fail to provide a centralized view of data.

The need for a cloud-native, data-centric solution that adapts DLP principles to today's complex cloud environments is clearer than ever.

The Dig Solution

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

Combining full data security posture management (DSPM) capabilities with data detection and response (DDR), Dig provides a cloud DLP solution that prevents exposure of sensitive data. Dig performs cloud DLP operations by discovering and classifying all the data across the clouds, as well as 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 in real time.

1. Report: Digital Transformation is Increasing Cyber Risk
2. Cost of Data Breach Report 2022, IBM
3. Cost of Data Breach Report 2022, IBM

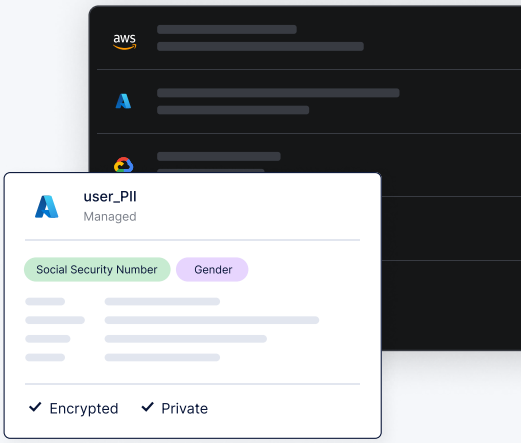
Dig in Action – Security Risk Scenarios

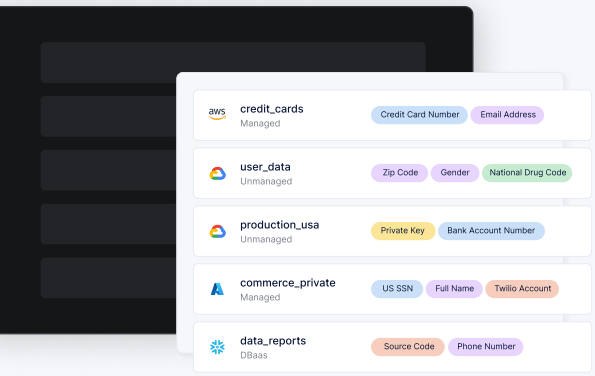
Scenario	Security Risk	Dig's Solution
Public Cloud Coverage	Traditional DLP solutions use agents to connect to various data stores such as databases and cloud storage solutions. This method cannot be achieved in PaaS and DBaaS environments where installing an agent is not feasible.	Dig's solution is agentless and works with all public cloud deployments, including PaaS, IaaS, and DBaaS. Onboarding Dig takes a few minutes, and you can gain visibility into all data assets – storage, database, analytics, cloud data (e.g. Snowflake), and virtualized environments – in just hours.
Deployment	With an agent-based approach, a security team must first connect to each storage location and database instance with its own credentials and then maintain the connection. Considering that most organizations run thousands of database instances daily, this approach is inefficient and costly.	Dig is an agentless platform that automatically discovers and classifies all data assets. Onboarding takes minutes, inventory display takes hours, and risk assessment takes one-to-two days.
Shadow Data	Developers can quickly spin up a new database in a virtual environment for testing and copying an entire set of data containing customer PII. After the test is completed, the data remains stale and "under the radar" of existing security controls, which represents perfect prey for attackers. Given that legacy solutions require defining connection strings, you need a tool that performs real discovery of what you don't know exists.	Dig solution automatically discovers all data assets on all cloud deployments without installing agents or providing connection data. This means that within hours, you can find all your shadow data that has fallen between the cracks.

Features & Benefits

Find data with sensitive information and understand your data's context and flow without impacting your production environment

- Discover and classify active and shadow data assets in AWS, Azure, GCP, and Snowflake to find PII, PHI, PCI, trade secrets, and other buried "crown jewels"
- Accelerate compliance readiness 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



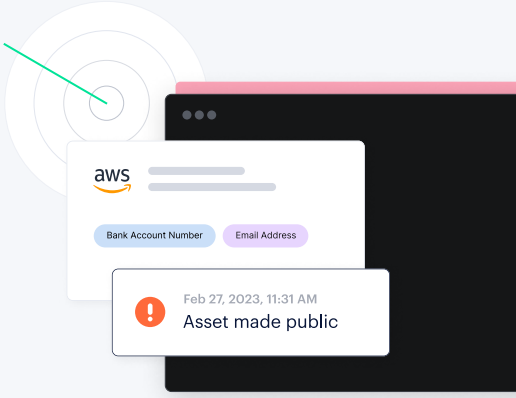


Strengthen your data security posture to reduce data exposure caused by public cloud environments

- Assess your data security posture across all data assets to tighten access permissions, fix data misconfigurations, and govern active identities
- Protect sensitive data against loss, theft, misuse, and unauthorized access

Apply an agentless cloud DLP with real-time data detection and response (DDR) capabilities to stop data exfiltration and reduce dramatically your MTTD/MTTR*

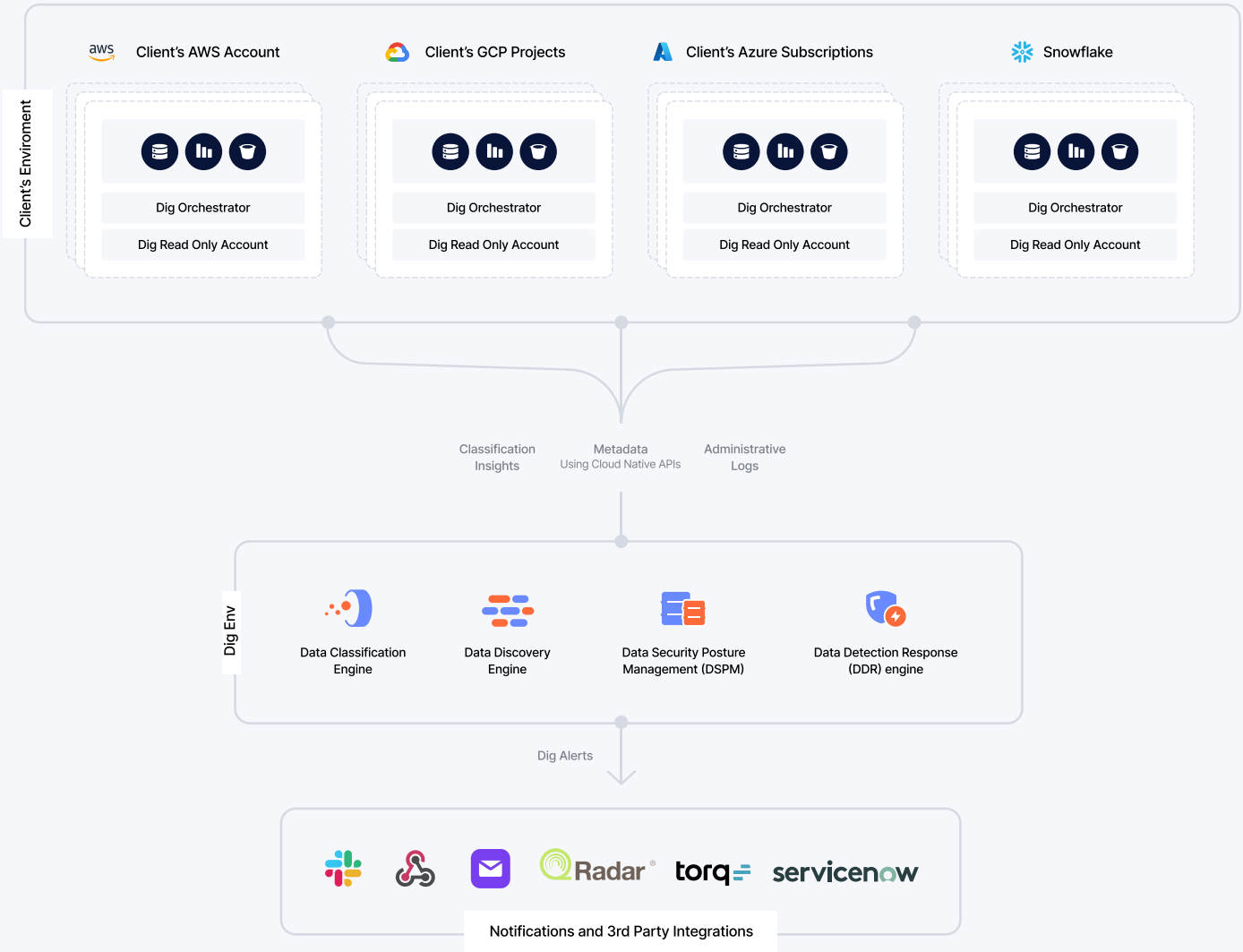
- Detect and respond to data security and compliance issues, including the creation of external data flows with sensitive information, as soon as they occur
- Integrate security alerts into your cyber operations teams to automate your response and increase your visibility
- Leverage a threat model built on a proprietary database of historical breaches to assess each event in real time and to determine data exfiltration potential

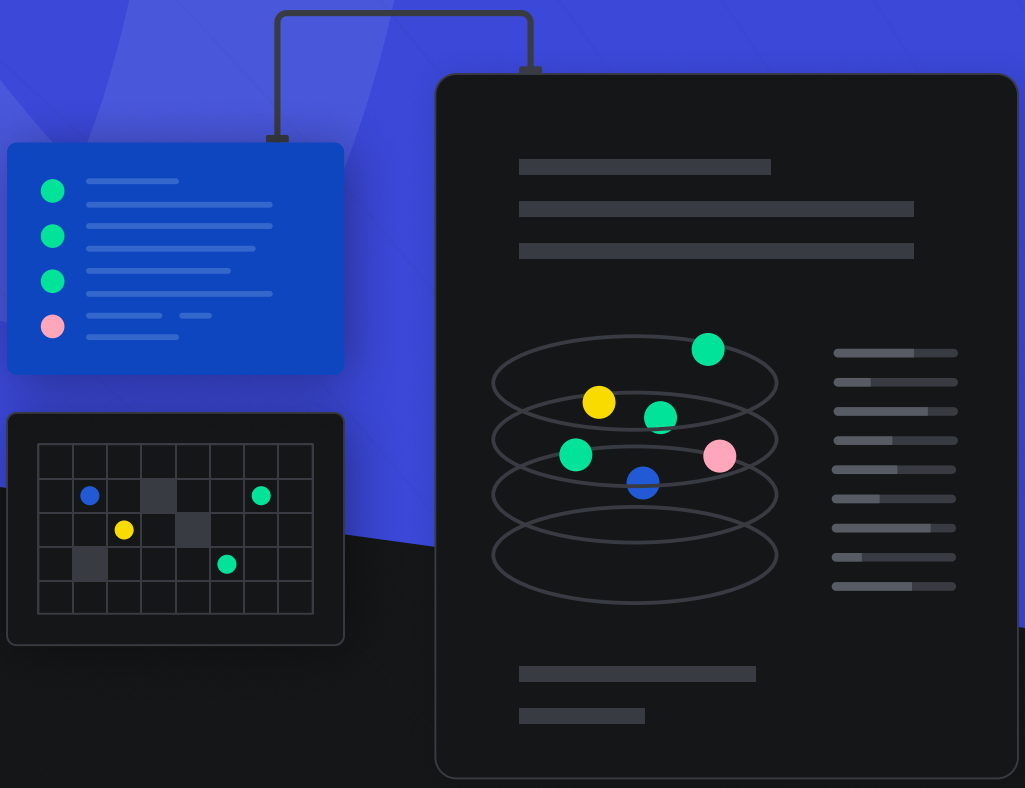


1. MTTD = mean time to detect
2. MTTR = mean time to respond

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





About Dig Security

Dig Security helps organizations discover, classify, protect, and govern their cloud data.

With organizations shifting to complex environments with dozens of database types across clouds, monitoring and detecting data exfiltration and policy violations has become a complex problem with limited fragmented solutions. Dig's cloud-native, completely agentless approach reinvents cloud DLP with data detection and response (DDR) 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, CrowdStrike, CyberArk, SignalFire, Okta Ventures, and others.

Dig Security