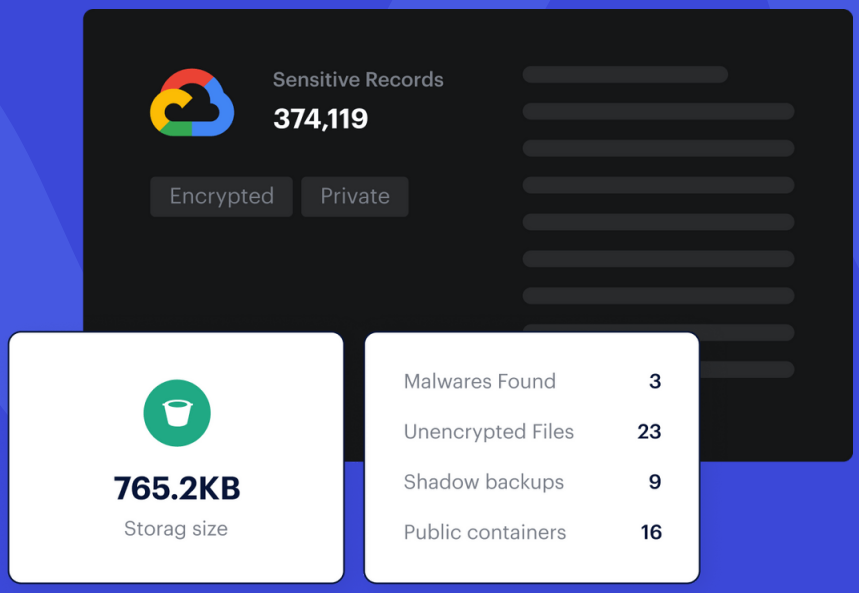


Dig for for Google Cloud Platform (GCP)

Protect your sensitive data
in BigQuery and beyond

Dig Security

The Need

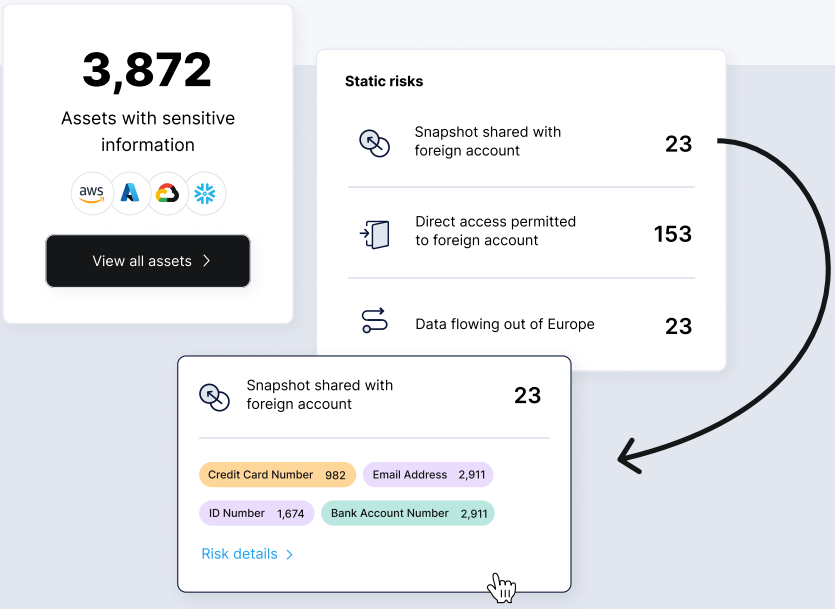
Today's enterprise data is typically spread across dozens of services and thousands of instances. Businesses are showing an increased appetite to adopt new cloud data technologies, often spanning multiple public clouds.

As one of the largest cloud service providers[2] (CSPs), Google Cloud offers a tightly-integrated ecosystem of analytics tools and business applications. BigQuery – a high-performance, high-scale cloud data warehouse that can handle virtually any workload – is often the main draw. Google makes it very easy for both business and technical users to move their data into BigQuery, especially if it is already residing in another Google service (such as its web analytics tools).

Security concerns arise due to the ease of granting permissions (especially within Google Workspace), and the few-click possibilities to move data between BigQuery, Google Cloud Storage, and external services. Google makes its cloud data tools accessible to almost any user – and this can be a double-edged sword when sensitive data is at stake. Data flow between data stores and CSPs becomes difficult to manage, leading to shadow data assets, security vulnerabilities, and compliance violations.

Cybersecurity teams need to identify sensitive data movement in fluid cloud environments, prioritize datasets based on security and compliance concerns, and monitor risks in real time. They need a way to cut through the noise by understanding the content and context of the data. This is the data-centric approach to cloud security, which Dig is pioneering.

The cloud data landscape is far more diverse and fractured than traditional on-premise architectures. This requires a new approach to finding and protecting sensitive data in order to prevent costly cloud data breaches and ensure regulatory compliance.



The Dig Solution

Dig Security is the enterprise-grade security solution you need to map all the sensitive data that moves through your GCP environment, detect incidents in real-time, and respond to policy violations.

Dig is an agentless, multi-cloud data security platform tool that protects all your cloud data - at rest, in motion, or in use. By unifying static and real-time data protection, Dig will harden your security posture, improve compliance, and detect breaches in your GCP environment the moment they occur. Dig's industry-leading threat model is based on rigorous analysis of previous breach incidents, in GCP and other public clouds, and is continuously updated as new attack vectors are discovered.

Leveraging full data security posture management (DSPM) capabilities, Dig gives you the tools you need to prevent exposure of sensitive data. Within minutes of being deployed, the software discovers sensitive data assets on both managed and unmanaged data stores, highlights misconfigurations and over-permissive access, and alerts security teams to remediate the most urgent data exposure events.

The platform extends its DSPM capabilities to address threats in real time via data detection and response (DDR). Integrating with your existing security solutions and workflows, Dig provides immediate alerts for important data-related incidents – whether these are actions committed by malicious actors or insider threats.

- Unify data risk and protection across all data store types and multi-cloud deployments
- Increase data visibility by automating discovery and classification of sensitive data
- Reduce mean time to detect (MTTD) and mean time to respond (MTTR) for shadow data assets, data misuse, data exfiltration, data privacy and compliance violations, ransomware

Security Scenarios Dig solves for customers

Understand how Dig defuses common data security risks in GCP:

Overly-broad permissions granted through Google Workspace.

Security Risk

For companies that use Workspace, granting permissions to Google Cloud is a matter of just a few clicks. An admin gives a large group of users permissions for a specific project, then forgets to revoke it, giving dozens of principals in the organization access to PII.

Dig Security Solution

Dig identifies all the data stores that contain customer records (DSPM), and gives security teams the means to easily see who has access to them. They can see that a database with sensitive information has been shared with an entire group or organization in Workspace, and check whether these permissions are necessary.

Sensitive data copied outside of EU (data residency violation)

Security Risk

As part of a new technology evaluation, sensitive records relating to EU residents are exported from BigQuery and uploaded to a database running in a non-compliant region.

Dig Security Solution

Dig identifies the policy violation within minutes of the data being uploaded to the non-EU database, highlights the specific compliance frameworks it violates, and alerts security and compliance teams to the incident.

Data exfiltration

Security Risk

An orphaned snapshot of an unused database, which has not been accessed for a long time, is now being shared with an unfamiliar account.

Dig Security Solution

Dig identifies the breach in real time and alerts security teams, which can take steps to contain the attacker and prevent further data loss.

Features & Benefits

01 Data Security Posture Management (DSPM) solution that identifies and protects sensitive data wherever it lives. No snapshots left behind

- Get a full, up to date inventory of all the sensitive data your business manages across GCP data stores (including Google BigQuery, Cloud Storage, and Firebase); unmanaged databases running as virtual machines; or 3rd party services such as Snowflake. Classify sensitive data to understand the level of risk it poses to your organization, e.g.: PII, PCI, or credit card details.
- Standardize and enforce the same policies across any number of cloud data stores and environments.
- Prioritize risks based on data context and sensitive data assets. Identify data exposure and opportunities to improve your security posture.
- Understand how data flows between services: Find shadow backups, shadow databases, and snapshots you didn't know existed, and get them under the umbrella of your cloud security strategy.

02 Respond to breaches in real time with data detection and response (DDR) technology

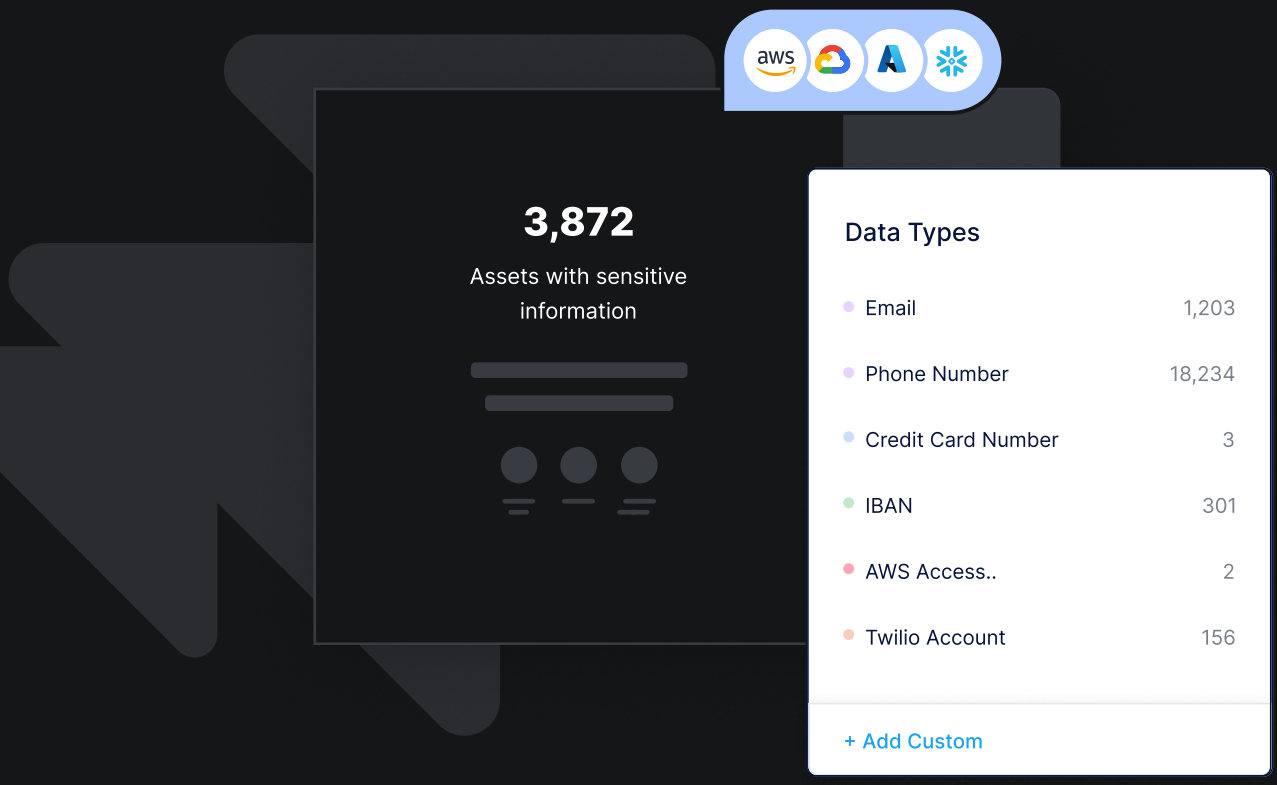
- Dig's DDR allows you to go beyond posture management. Add a layer of dynamic monitoring to identify breaches or severe risk incidents as they happen, rather than when the damage is already done.
- Dig provides out-of-the-box DDR policies that are regularly updated, based on expert analysis of the latest known vulnerabilities and data breach incidents.
- Get alerts when sensitive data is being illegitimately copied or exfiltrated from your GCP account - even by an authorized actor.
- Apply a unified threat model across hybrid and multi-cloud environments, without duplicating your efforts.
- Dig's threat detection is frequently fine-tuned to only surface alerts that pose a true risk to your organization - preventing overwhelm and notification overload.

03 Technical integrations

- Works natively with all major public cloud providers – GCP, Amazon Web Services, Azure, and Snowflake.
- Real-time notifications and alerts can be delivered via email or Slack. Dig integrates with SOAR, SIEM, and SOC solutions to enable consolidated response.
- Connects with your existing IdP to provide a rich view of active identities for each data asset, adding a context layer for making access decisions on sensitive data

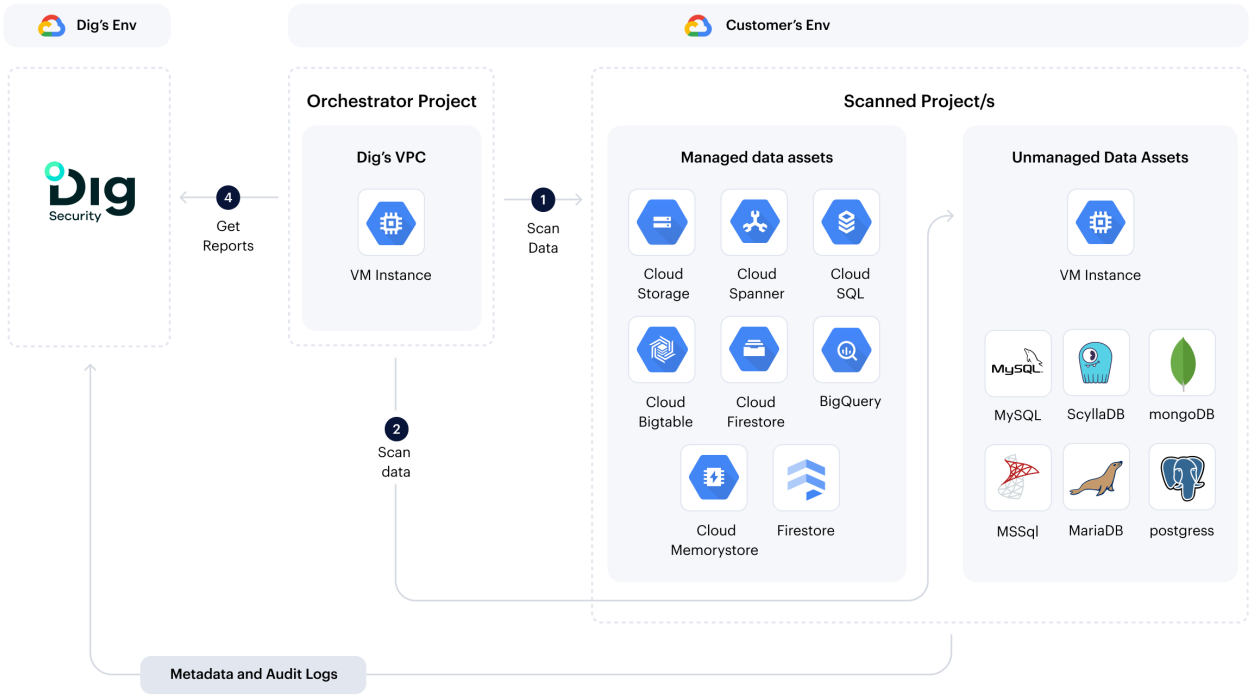
04 Security (learn more)

- Dig is ISO27001 certified and compliant with SOC 2 Type || requirements.
- All sensitive data discovered, scanned and classified by Dig's resources stays segregated in the client's environment.
- All sensitive data discovered, scanned and classified by Dig's resources stays segregated in the client's environment.



How it Works?

Dig's agentless solution continuously monitors GCP logs and dozens of APIs in order to detect misconfigurations and suspicious activity around sensitive data. Production is never disrupted, and sensitive data never leaves your account.



01 / Fully automated

Deployment is quick and painless: Dig requires minimal permissions and no manual tuning or configuration.

02 / Completes in minutes

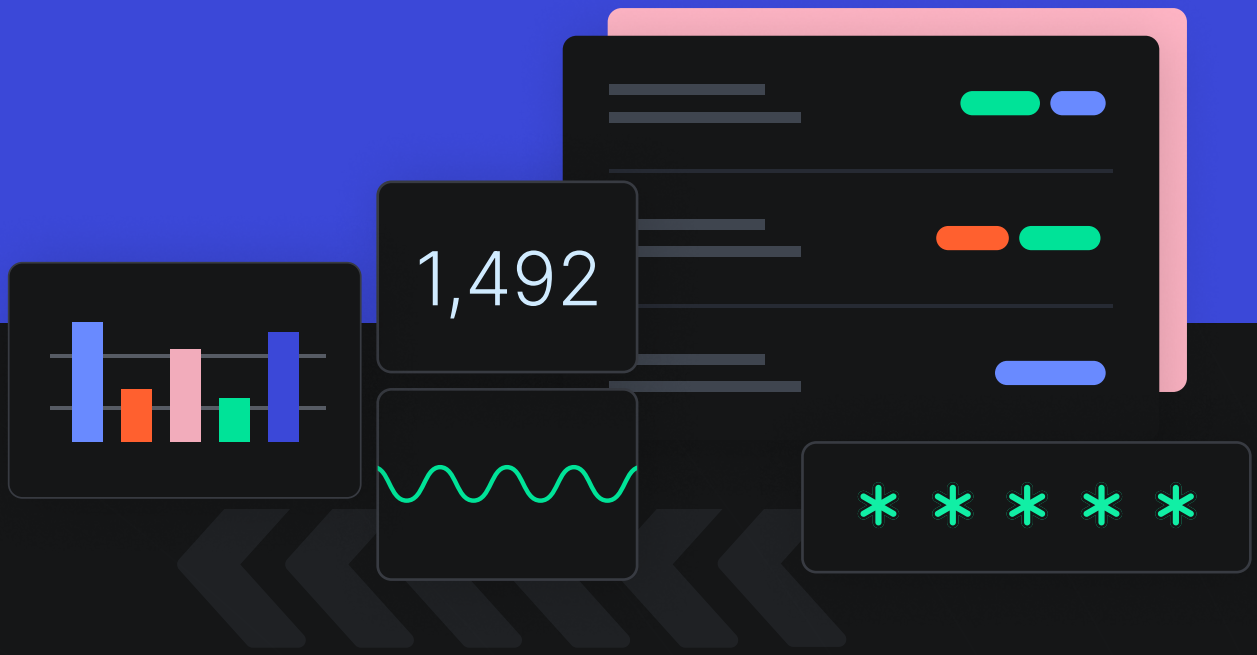
Get straight to work with immediate visibility into your data security posture and prioritized action items.

03 / All scanning is out of band

Dig does not require a live DB connection. No impact on production or other workloads.

04 / Sensitive data never leaves your GCP account

To provide dynamic monitoring capabilities, Dig parses and analyzes AWS logs (via CloudTrail), then applies its proprietary detection engine for data detection and response (DDR). Alerts are surfaced within minutes of an incident occurring.



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