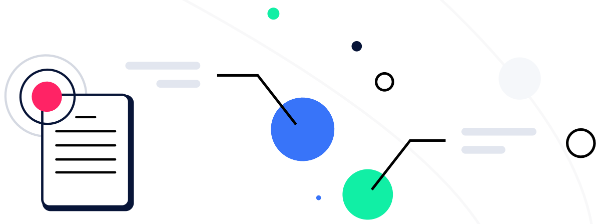
Dig Security Platform Datasheet

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

With cloud adoption strategies now the new normal, organizations are moving their data to a wide range of cloud data services. But this shift is exposing new vulnerabilities and increasing the risk of your sensitive data falling into the wrong hands.

Comprehensive, Beyond-the-Perimeter Solutions are Hard to Find

Existing offerings are hard-pressed to protect your data in the cloud. Data leakage prevention (DLP) solutions are ineffective beyond the organization perimeter. And cloud security posture management (CSPM) solutions focus on infrastructure and lack a data-centric view. Moreover, cloud-native solutions are limited to only a subset of the environments and data types. As such, they ultimately impact just one part of a much bigger picture and lead to more data fragmentation issues.



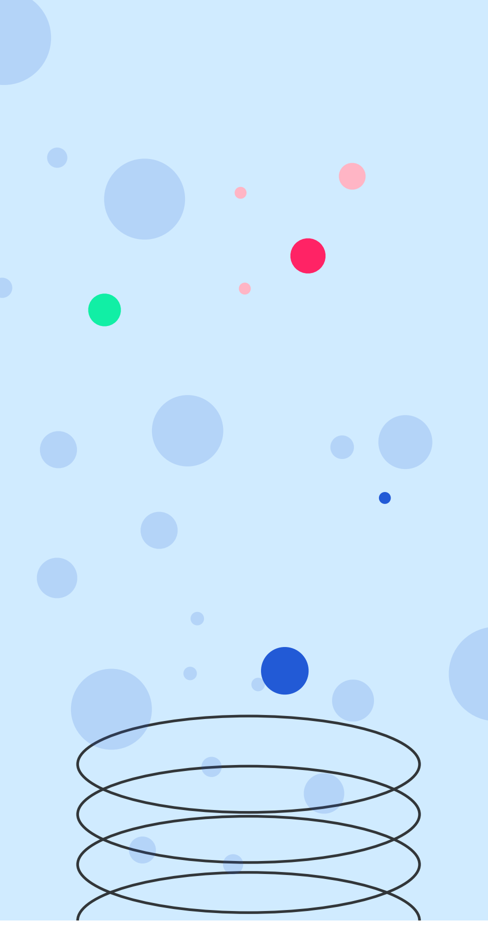
Highlights

- Cloud DLP solution that uses agentless technology to discover, classify, govern and protect your sensitive data assets across all major providers (i.e. AWS, Azure, GCP) and data platforms (e.g. Snowflake)
- Continuous data monitoring service across your cloud data that identifies data security and compliance incidents in real-time, and uses data context to prioritize findings to improve your course of action
- Cutting-edge platform that integrates seamlessly with your existing security workflows to ensure rapid resolution and increased resilience against data security and compliance issues

Detect and Respond to Risks in Real-Time

Dig Security offers an agentless multi-cloud data security platform that discovers, classifies, protects and governs sensitive data. Leveraging full data security posture management (**DSPM**) capabilities, Dig prevents exposure of sensitive data by highlighting data misconfigurations, access anomalies, shadow data and other data vulnerabilities that increase the risk of a data breach if not remediated.

Dig's platform extends its DSPM capabilities to address risk changes in real-time via data detection and response (**DDR**), enabling you to stop data exfiltration early in the kill chain. Integrating with your existing security solutions and workflows, Dig ensures immediate handling of incidents triggered by newly discovered data.

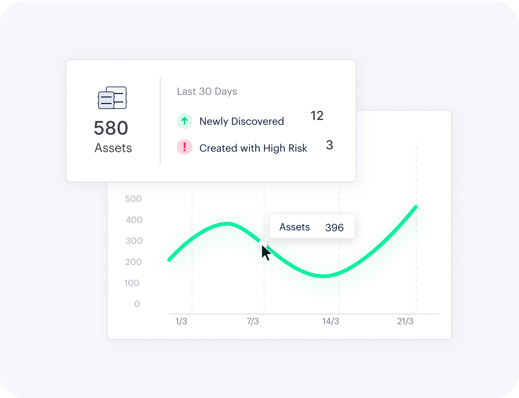


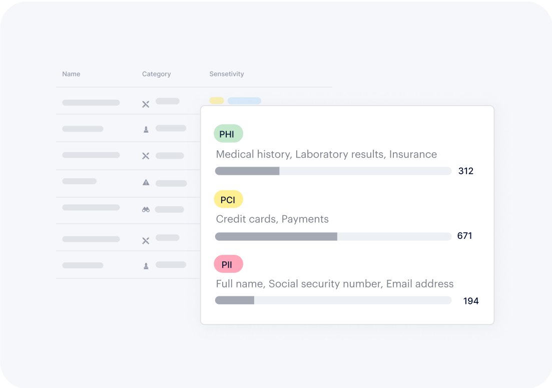
Data-Centric Platform

The Dig Data Security Platform provides a centralized view of all data assets, enabling you to apply a single policy engine for multi-cloud environments. Here's how it works.

Discover managed and unmanaged data stores and data analytics

Dig discovers and collects information on data from myriad cloud deployments, including managed data stores such as buckets, file storage, and databases, as well as unmanaged data stores such as MongoDB and MySQL servers running on virtual machines. The platform also discovers data analytic environments (DBaaS), such as Snowflake, to offer you a complete data landscape view.



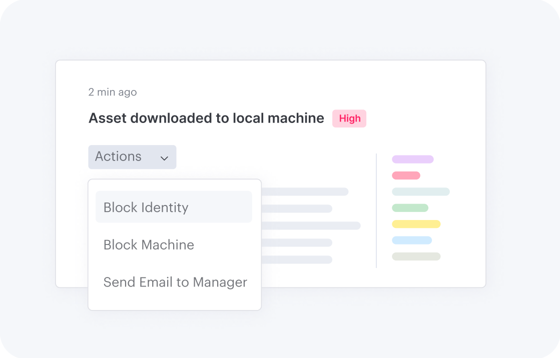

Name
Category
Sensetivity
PHI
Medical history, Laboratory results, Insurance
312
PCI
Credit cards, Payments
671
PII
Full name, Social security number, Email address
194

Classify and analyze content

After discovering a new data asset, Dig uses automated classifiers to classify and analyze the content. The platform automatically tags sensitive information types such as personal identifier information (PII), credit card numbers, and other categories, as well as leverages custom-defined classifiers to help find your IP and other "crown jewels."

Carry out DSPM and DDR in real-time

Dig offers DSPM capabilities, by highlighting data misconfigurations, access anomalies, and data vulnerabilities that increase the risk of a data breach if not mitigated. The platform also provides real-time data detection and response (DDR) to thwart potential data breaches early in the kill chain.



2 min ago

Asset downloaded to local machine High

Use Cases

Data Discovery

Know where sensitive data resides on PaaS/IaaS/DBaaS

- Gain a single view of your data across all clouds
- Locate your data assets by region to visually spot data residency violations
- Detect shadow data and newly adopted services

DSPM

Prioritize your data assets' most critical configurations, risks, and usage

- Fix data misconfigurations to lower overall risk of attack
- Tighten access permissions to reduce data exposure
- Involve data owners in data access decisions

Data Classification

Reduce the risk of sensitive data exposure in the cloud

- Identify personal information (PII), regulated data (PHI, PCI, SOX) and corporate secrets defined in structured, semi and unstructured data in the cloud
- Prioritize your security measures by content type
- Address your compliance requirements and avoid penalties

Real-Time DDR

Detect and respond to any policy violating data activity, block data exfiltration and eliminate data breaches

- Apply real-time data protection policies across your cloud services
- Continuously monitor and alert on malicious activity around your data
- Detect and evaluate actions according to MITRE, SOC-2, ISO27001 and other cyber threat frameworks

Benefits and Business Outcomes

Cut costs

Reduce costs by consolidating multiple data security solutions, while tightening security and extending coverage across all your cloud data assets

Reduce attack surface

Eliminate the data threat vector by identifying, highlighting, and prioritizing misconfigurations associated with your sensitive data

Respond rapidly

Identify risks and reduce your response time to changes via real-time detection and resolution capabilities and seamless business process integration

Unique Advantages

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

Technical Integrations

- Works with major public cloud providers including AWS Azure GCP and Snowflake
- Enables real-time notifications and alerts (DDR) via email, Slack, and Webhooks so security operations can carry out consolidated actions such as SOAR/ SIEM/SOC solutions
- Connects with an existing IdP to provide a rich view of active identities on each data asset in order to add a context layer for making access decisions on sensitive data