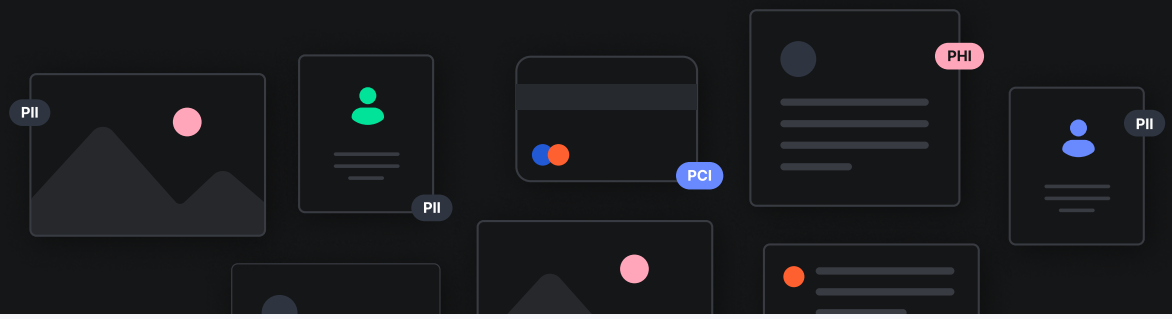
Why You Need DSPM
(Data Security Posture Management)



The Explosion of Data on Public Cloud

Organizations today are seeing an explosion of the number and variety of data assets in public clouds due to the following:

- The use of multi-cloud architectures which increase the size and variety of data assets by at least **4 times** than before
- The total number of data assets grew to at least **20** different types which span hundreds, if not thousands, of instances
- **Microservices:** gone are the days of the big, monolithic databases. Today we are seeing smaller services, each with their own data asset assigned to it

In addition, there are business drivers that require more data scrutiny and the ability to assess the risk of handling sensitive and critical data due to the following reasons:

- **Mergers and acquisitions**
- **Compliance**
- **Cost efficiencies**

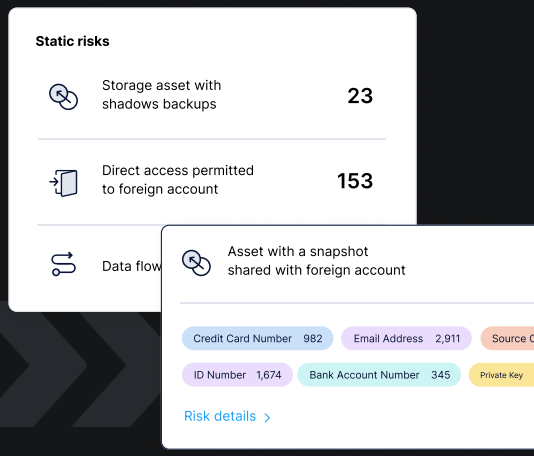
Migrating to the cloud holds many benefits, but it comes with the consequence of surrendering visibility & control over who's doing what with the data.

- Organizations need to know where all their data is, who is accessing it and how they can protect as if it was in their own data center.
- Need to perform threat analysis and view their data from the mindset of attackers.
- Cloud data stores are persistently attacked due to their monetary value.
- Protecting data assets in public clouds is the only area that lacks a dedicated solution. (until now)

New threats

Data breaches in the cloud are very different than on prem. Attack vectors are different, the cloud is more complex and current strategies have proven to be ineffective.

- 91% of all cloud data breaches never hit the endpoint
- No one is tracking data usage after permissions have been given



Legacy solutions are not sufficient

- **DLP** is for on-prem only and does not scale in the cloud
- **Cloud provider native solutions** do not support multi-cloud environments and are limited in coverage and functionality
- **CASB** only supports SAAS applications but does not support IAAS, PAAS or DBAAS
- **CSPM** solutions focus on cloud infrastructure only and lack a data centric view

Why DSPM

Discovery & Classification

Provides the necessary **discovery and classification** of the data to help understand where sensitive data is located, who is accessing the data, and where it is going

Static Risk Identification

Performs **static risk analysis** to identify data that is not fully protected: is it encrypted? Is logging enabled? So data is not misused

Real Time DDR

Data Detection and Response.
alert and automate actions on any data threat

Data is the missing context layer for proper risk analysis

DSPM prevents shadow data assets, ransomware, data exfiltration, data misuse and compliance breaches.

Additional Reading: The Importance of DSPM to Cloud Data Security

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.