dig.security

360° Cloud Data Security with Dig Security & Okta Identity Platform

Gain visibility into your cloud data, understand how it's being used and leverage your Okta IdP to protect it from cyber attacks

Modern organizations today are experiencing an explosion of data on their public cloud environments. With the shift to cloud data services, more data resides on cloud than on premises and in more services than ever before.

The growing spread of micro services leads to data fragmentation, with multiple teams maintaining their own data sets, containing customer information and other organization crown jewels.

All this results with an extended data attack surface that can lead to a breach as well as failure to comply with regulations.

To ensure your data is secure you need full visibility into how data flows through your cloud deployments, who has access to sensitive and critical information and how it is being used.

This requires a solution that focuses on all public cloud environments and deployment types, including AWS, Azure, GCP and Snowflake with a data-centric approach. A solution that discovers and classifies all data assets running in the cloud, finding forgotten dark data, misplaced access permissions and compromised identities with sensitive data access. Moreover, when suspicious behavior is detected, it issues real-time alerts so you can stop data exfiltration.

Dig Security solution extends Okta Identity Platform to protect data beyond managing access policies and with the knowledge of the data in mind.

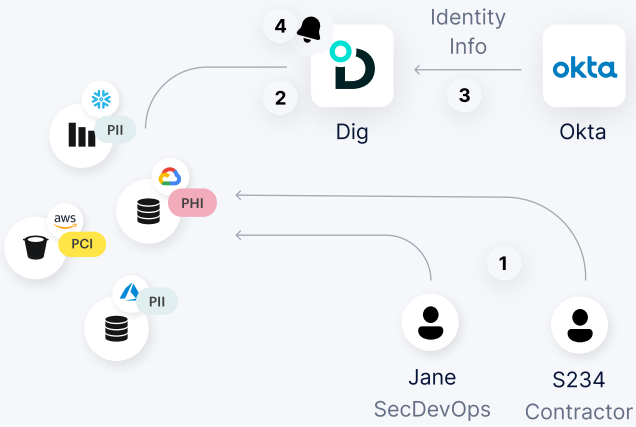
By discovering and classifying your entire data on public clouds, you can answer questions such as “where does sensitive data reside across my cloud environments”, “who has access to sensitive data and what they are doing with their access”. Furthermore, with the Dig Security platform you can apply a single policy across your many cloud data services that detects violations of data security in real time and will allow a streamlined process to respond to such events and prevent further data exposure.

> 92% (organizations) that have already experienced a data breach believe they will experience another breach of cloud data in the next 12 months.
>
> — SC MEDIA

Dig Security ↔ okta Integration Use Cases

Gain a data centric view to access policies

Dig discovers and classifies all cloud data, providing full context for each data asset, including personal information (PII), credit cards information (PCI) and other data types, as well as the active identities and their usage patterns. Know who has been accessing your organization's critical assets and if access policies should be changed.

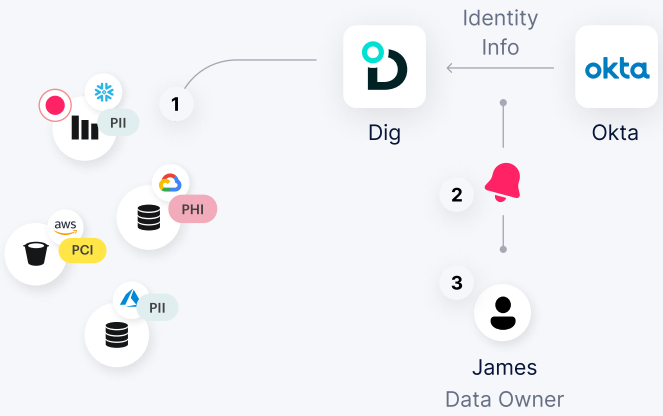


(1) Contractor initiates access to sensitive information (2) Dig identifies the user activity

(3) Dig enriches user profile using Okta's centralized identity platform (4) Dig issues notification on access sensitive information

Obtain Data Security Posture Management (DSPM) through data ownership

Dig performs a static risk analysis across your cloud data, identifying shadow data assets that lead to data exposure and data misuse. Resolving static risk through data ownership utilizes the business units in the data governance effort.

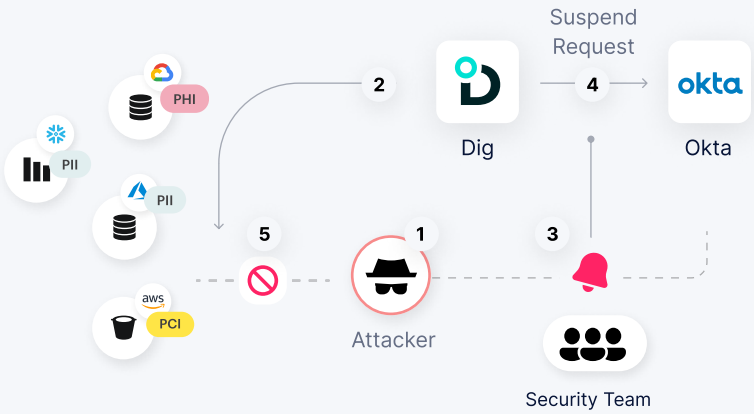


(1) Dig identifies sensitive shadow backups residing in an unencrypted cloud asset

(2) Dig issues a notification and retrieves the data ownership from Okta (3) Risk is resolved by the data owner

Detect and respond to data threats in real-time

Dig detects suspicious events such as mass download of data to external sources. If a data risk is detected, the attacking identity can be immediately suspended using Dig and Okta integration



(1) Attacker is downloading sensitive data to a personal machine

(2) Dig detects the exfiltration in real-time (3) Secrutiy team is notified and remediates by suspending the identity

(4) Dig sends a 'suspend session token' request to Okta (5) Attacker loses federated identity access