Dig Security

Essential Elements for Cloud Data Protection

WHITEPAPER

Executive Summary

Despite the acceleration of cloud adoption, companies are still only scratching the surface of the cloud's vast potential – making it hard to predict its true limits. Even though we are still far from the cloud's full capacity, recently, we've observed the number and variety of data assets per organization explode. At a time when businesses had a choice to adapt to the new way of work or falter, the cloud made successful operations possible.

Moving away from slower, more rigid on-premises infrastructure has been good for the pace of development. Simultaneously, it has thrown a wrench into the already difficult jobs of Security teams. While multiple cloud solutions can drive agility, they also create issues. These range from securing data, maintaining control, meeting regulatory and compliance requirements, and ensuring that security doesn't hamper data accessibility.

To thrive in the multi-cloud world, organizations now need complete data observability and the tools to:

- Reduce their attack surface
- Discover shadow data
- Detect and respond to threats against data in real time
- Reinstate control over data

And this is especially true for sensitive data or "crown jewels."

Multi-cloud security platforms are coming to market to solve these issues, but each has a unique take on solving the puzzle of securing data. This white paper helps security leaders start from the foundation to understand the essential elements for protecting cloud data as it proliferates in the hands of developers and users.

Data in the Cloud is Fueling Today's Economy

2022 made history as the first year where enterprises stored more data in the cloud than on premises. And the margin of difference is significant — 60% of enterprise data, including sensitive data like PII, PHI, and PCI is now stored in the cloud.[1] This new world where organizations entrust the majority of data to the cloud is only the beginning. As more businesses transition to multi-cloud operations we will continue to see the amount of data and associated complexity of securing it all grow.

> **By 2025, more than half of enterprise IT spending in key market segments will shift to the Cloud - Gartner** [2]

The change is a more significant opportunity than moving data to a more agile, scalable home. It also allows organizations to implement security specifically designed to provide control over their data security posture. With new technologies on the rise, security leaders will no longer have to shoehorn in on-premises security solutions to the complexity of the cloud. Nor will they have to stitch together complementary data security controls that can leave behind hidden gaps.

> **In a 2021 survey, a staggering 98% of the companies experienced at least one cloud data breach in the past 18 months – a significant increase from 79% in the previous survey.**

1 https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/

2 https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending

The Shortcomings of Old Solutions for a New Problem

Data is the thread that ties together organizations – providing insights and the content and context which fuel decisions. Being so dynamic, it can also multiply fast. Without the security stamp of approval, users and groups have free range to access public cloud platforms. At the same time, developers can move and copy data to new applications as they spearhead projects. Now imagine that at the scale of petabytes of data across a myriad of types, and you've reached the true looming challenge for today's organizations.

If we piece that together with the rise in cloud data breaches, we can see that there is not only risk, but risk that is difficult to identify. If we could visualize every anomalous data interaction and had control, we could suppress breaches.

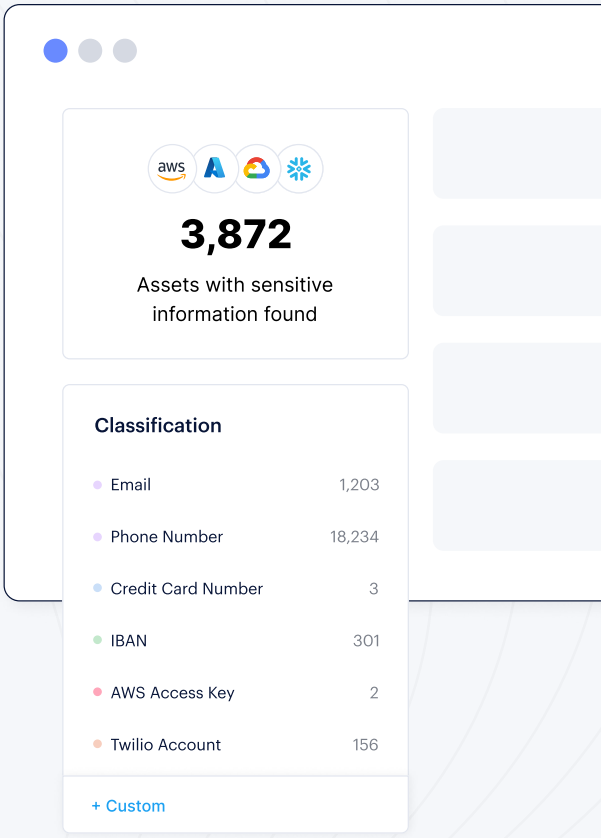
Incomplete data security controls create problems that lead to security incidents. These problems include:

Lack of Visibility Into Data Stored Across Multi-Cloud Environments

The vast majority of enterprises deploy a multi-cloud architecture with their data distributed across multiple clouds. In addition, data is stored across different types of cloud services including IaaS, SaaS, PaaS and DBaaS, making it difficult to discover where sensitive data is stored and understanding what data is at risk.

The lack of automatic discovery of data assets across multiple clouds and cloud services in traditional data security solutions makes understanding the full range of data assets unknown. This makes it nearly impossible to properly protect enterprise data in the cloud.

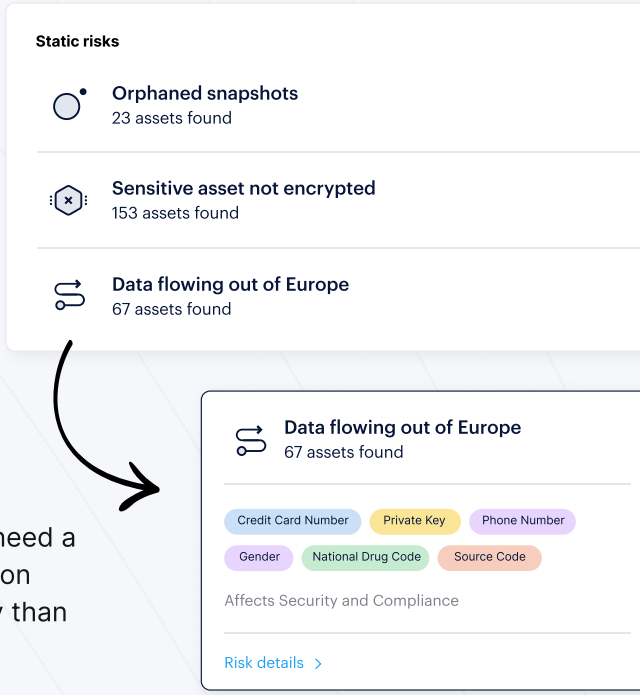
Case in point: when Twitter whistleblower, Peiter Zatko, testified before the U.S. Senate Judiciary Committee, he said Twitter does not "know what data they have, where it lives, or where it came from, and so unsurprisingly, they can't protect it." [3]



[3] https://whistleblowersblog.org/corporate-whistleblowers/a-company-driven-by-crises-twitter-whistleblower-peiter-zatko-testifies-before-senate-committee/amp/

Inconsistent Data Classification Across Deployment Methods

Cloud sprawl isn't only an IT problem, it has major implications for security because of the management complexity it creates. Data in the cloud is not static. It is constantly moved and copied by developers, data owners and engineers, across different cloud services. This means that security controls put in place at the origin of the data are no longer effective to monitor and protect the asset. New controls have to be put in place that require classification and context.



As data continues to grow and move, it is impossible to manually update each of those controls. Security teams need a way to continuously and automatically update classification and context to ensure sensitive data is treated differently than all the other data sitting in the same cloud.

Complex Security Policy Management Across Multi-Cloud

The complexity of multi-cloud makes it difficult to not only discover data assets, but to also implement and enforce a consistent data security policy. This includes controlling how data is being used, who is accessing the data, and enforcing policies around suspicious behavior and unauthorized access or use.

Piecing together disparate technologies to manage data security policies across different cloud providers is labor intensive, unrealistic, and risky. It also makes it nearly impossible to have a consistent set of policies to protect data. IT Security teams need a way to understand the different threat vectors to cloud data and apply a consistent policy across all cloud services.

> **Until 2022, there weren't solutions specifically designed to protect cloud data. Instead, organizations were stuck using multiple tools that still did not fully discover, classify, protect and govern their cloud data.**

Solutions and their shortcomings for protecting data in multi-cloud environments include:

- **Cloud Security Posture Management (CSPM)**
  Focuses on infrastructure and lacks a data-centric view. Only scans environments every 24 hours, taking a snapshot of a single moment. This does nothing to prevent an attacker from stealing data, covering their tracks, and disappearing before the next scan.

- **Data Risk Management solutions**
  Helps identify the data threats and vulnerabilities, but only works on-premises

- **Cloud-native solutions**
  Leads to more data fragmentation issues, with each solution impacting only one part of a much bigger picture (e.g. cloud-native solutions for discovery like Macie, for AWS, only support buckets)

- **Data Leakage Prevention (DLP)**
  Ineffective beyond the organization perimeter

Cloud providers are focused on what is best for their operations, not necessarily what is favorable for your security.

Because of this you will find that cloud-native tools have inconsistent ways of managing data security across the cloud providers you use, making it complex to protect.

What Cloud Data Protection Can Fix

One benefit of ineffective tooling for keeping data secure in the cloud is that it has provided clear targets. The security gaps that remain dictate how to improve and decrease the number of data breaches over time. **Now we know – and can fix – these issues:**

Shadow Data

Security teams are constantly trailing Development teams as they make changes, spin up new data storage assets, and move files around the cloud. The result is shadow data that security teams don't know exist and aren't protected by current data governance and frameworks. Examples of shadow data include database snapshots and backups which can be left behind unprotected, often containing sensitive data.

Compliance Violations

Strict regulations paired with the flexibility of the cloud makes it more difficult to stay compliant – and be able to prove it to auditors. Compliance teams need an easier way to classify data under regulations like GDPR, PCI, and HIPAA to ensure it is handled accordingly and visualize the nuances. Only then can organizations ensure and prove the data is handled safely or intervene if a violation is detected.

Data Exfiltration/Theft

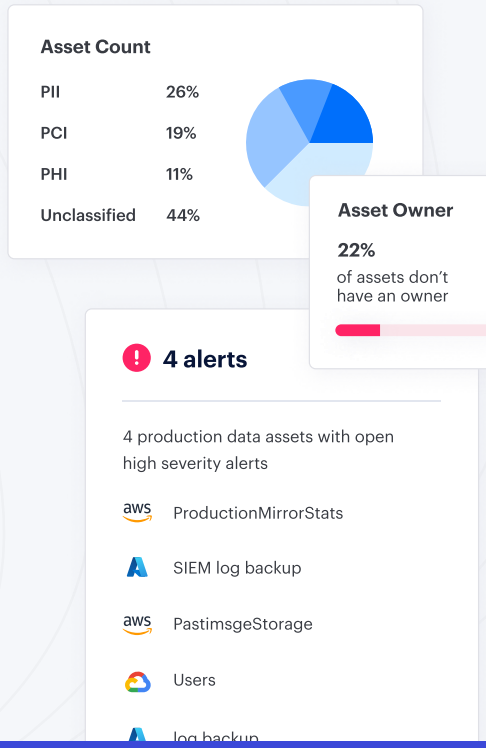
Cyber criminals' techniques used to steal data are becoming more sophisticated and can bypass many of the current data protection solutions. Without the ability to easily understand exposure at the data element layer, and how to limit access, there is no way to cut off access to adversaries. This often leads to open doors where data is siphoned for unspecified amounts of time.

Ransomware

Ransomware needs no introduction. It's one of the toughest threats to manage because the Security team is often left dealing with it after the fact. Once the data is leaked, even if you pay the ransom, there is no guarantee the adversaries won't do it again. Without visibility, real-time detection, and control of cloud data, stopping attacks early in the kill chain is impossible.

Data Misuse

Data misuse, while typically not malicious, can lead to unintentional data compromise. If there is no way to validate or enforce security policies across multi-cloud architectures, then users and developers can copy files or store data in places they aren't supposed to. And it can go on, undetected for long periods of time.



Mending the DevOps-SecOps Relationship

The relationship between the Development and Security teams has long been a troubled tale, but it doesn't have to be. Instead, we can make everyones' jobs easier by adopting a cloud data-centric security model. This approach maintains visibility and control over data, while simultaneously allowing developers to move as fast as they please.

Best Practices for Protecting Cloud Data

Protecting your most valuable data in multi-cloud environments is hard, but the new data-centric approach is redefining what's possible. To effectively manage and secure data across the expanding and complex environment.

01 / Discovery

You need to be able to see data to secure it. While this isn't a mind-blowing best practice, it is a necessary foundation for effective data security. To secure and govern across data stores and multi-cloud, you should first eliminate all blind spots and uncover shadow data. Only then can you see what data you have, who owns and accesses it, and where it resides.

02 / Classify

Once you gain visibility into your cloud data inventory and identify different types of data assets on IaaS/PaaS, you should then use data classification techniques to label sensitive data (PII, PCI, PHI, etc.) as well as the organization's crown jewels.

03 / Identify Risk

To strengthen your data security posture, you should highlight data misconfigurations, access anomalies, and data vulnerabilities that increase the risk of a data breach if not mitigated. This should also include the ability to properly prioritize a remediation plan for identified risks.

04 / Detect and Respond

When data is exposed or is handled by bad-intentioned actors, the situation must be dealt with in real time to minimize the fallout. Cloud data protection should actively monitor all types of data-interactions that could potentially lead to a breach. With policies that alert to threats when it's time to take a remediation action, rather than any outlier, Security teams can avoid the dreaded alert fatigue.

Additionally, for any action that can lead to data exfiltration or compliance violations, the Security team should be able to quickly understand the progression and severity of the threat with categories such as reconnaissance, first move, attack, compliance, or asset at risk so there is no guessing games around the cloud data security event.
Within minutes of suspicious actions, Security teams should have clearly prioritized alerts and the ability to act on events using SIEM/SOAR integrations to dig deeper into logs and complete remediation efforts without interrupting data flows.

Imagine a world where Security teams don't have to be gatekeepers who restrict access and prevent unauthorized use of data.

Where Development teams don't have toslow their work. ...Or create shadow data because they've moved too quickly and haven't allowed Security teams to ask important questions and implement policies to protect the data.

Cloud data protection turns dreams into reality.

Assess Compliance to Industry Mandates

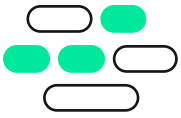
Visibility is great, but being able to report with a single version of truth on activity without endless spreadsheets is even better. Cloud data protection should include out-of-the-box reports with a consistent set of data for key stakeholders (e.g., Executives/Board of Directors, Security, Governance, data owners, and compliance groups) and external auditors to demonstrate compliance.

> **Solutions that leverage security models like MITRE ATT&CK, ISO27001, and SOC2 help ensure data security is always in line with compliance and privacy regulations.**

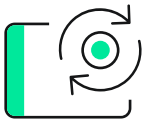
Dig Security for Proactive Cloud Data Security

As cloud security spend increases along with the rate and intensity of attacks, organizations need a way to spend smarter. Working cloud data security into your budget instead of piecing together CSPM, DLP, and other existing solutions that weren't designed for the specifics of cloud data gives you an advantage in the world of cloud complexity.

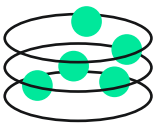
Dig Security is the only solution that combines all three capabilities to achieve the best practices needed to keep data secure and available for digital transformation efforts:



Data Security Posture Management (DSPM) highlights data misconfigurations, access anomalies, and data vulnerabilities. By accelerating assessments of how data security posture is enforced, it reduces business risk despite the speed, complexity, scale, and dynamics of multi-cloud.



Cloud DLP prevents sensitive data from leaving an organization by monitoring and stopping exfiltration early in the kill chain.



Real-Time Data Detection and Response (DDR) policy engine provides real-time detection and response to indicators of an active threat.

Dig's agentless multi-cloud solution discovers, classifies and protects sensitive data.

Using our data classification engine, you can quickly locate your most critical data and organizational "crown jewels" in both structured and unstructured data assets.

- Discovers and protects all data assets in public clouds. Dig discovers and classifies all your data assets anywhere on public clouds including storage (S3, RDS, EFS), virtualization environments and data analytics platforms so you never miss an asset containing critical or sensitive data, ever.
- Reduces the data attack surface. Dig classifies all your data assets on different cloud deployments, including structured and unstructured data. Our classification engine runs with built-in classifiers that detect PCI, PII, PHI and many other sensitive data types. Dig also allows you to use custom unique classifiers to identify all your organization's crown jewels.
- Responds to risk changes in real time in accordance with business processes. Dig's unique DDR solution monitors and processes all events to detect and respond to data related threats in real time – setting the business security workflows in motion. By significantly reducing MTTD and taking immediate action to involve data owners, incidents can be quickly mitigated.

To see how we would keep your data secure, visit dig.security to book a demo.

Your clouds and services all protected

Dig partners with leading cloud providers so we can work seamlessly and consistently in your environments including IaaS, PaaS, and DBaaS:

Amazon Web Services • Databricks

Microsoft Azure • Google Cloud Platform

Oracle Cloud Infrastructure • Snowflake

In five days or less from deployment you will:

- ✓ Increase visibility into multi-cloud data
- ✓ Identify sensitive data and "crown jewels"

In 30 days or less you will:

- ✓ Reduce MTTR
- ✓ Reduce MTTD
- ✓ Reduce impact of data breach
- ✓ Improve data privacy and GRC compliance