



# Know More, Do More:

Strengthening Security & Governance  
With Data Classification

## Today's data ecosystems are large and complex.

Data is moving out of data centers to cloud and edge computing environments. All the while, cybercriminals are getting smarter and more targeted — and end users continue to unintentionally mishandle data, exposing security vulnerabilities.

As new platforms and users are introduced into already data-rich environments, security teams are being called on to find structure amid the chaos. Two common pitfalls make this challenging:



Siloed perspectives on data and data security



A lack of understanding around data usage at each stage of its lifecycle

From data creation to management, protection, archival, and removal, there's an entire lifecycle around data. With different processes across each stage, how can IT teams create a foundation for an effective security strategy that connects the data dots, achieves data governance, and keeps bad actors away?

The answer is committing to visibility — understanding your data environment through data discovery and data classification.

# The value of knowing what you have

What data exists within your organization? What platforms are you using to store that data? How is it handled by users across the business?

Data discovery and classification help you answer these questions, and many more.

Data discovery is the process of performing a complete scan of your IT environment to locate sources of both unstructured and structured data.

Data classification follows; using discovered data sources, teams are able to define the types of data they have based on keywords, patterns, or rules, and assign labels accordingly.

The benefits of data discovery and classification are numerous. With the right processes in place, organizations can:



Expose risks, vulnerabilities, and gaps within their current security programs.



Create a business case or encourage buy-in for new data security investments.



Build a more thoughtful data protection strategy by prioritizing security measures.



Drive efficiency and productivity by helping users find information faster.



Identify duplicate or out-of-date data that needn't be maintained.



Stay compliant with regulatory requirements (GDPR, HIPAA, PCI DSS, etc.).



Uncover opportunities to innovate and/or grow the business using data-driven strategies (Artificial Intelligence (AI), machine learning, edge technology, etc.).

## Gaining an edge

Data classification is an important part of a comprehensive security program — and it also plays a key role in innovation.

Today, just 13% of organizations are delivering on their data strategy.<sup>1</sup> By establishing a strong foundation of data management and architecture, this powerful minority will be able to “democratize” data and leverage AI and machine learning to maximize its value.

## Why classify?

Extending classification efforts to unstructured data is critical. This infographic highlights six reasons why.

[Check it out here](#)



## Keys to success

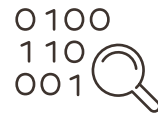
---

Performing comprehensive data discovery and classification is a massive undertaking. From defining the schema and controls aligned with each classification level, to building organizational awareness, there's a lot to consider. Here are several strategies.



### Work with tools and processes you can trust.

Projects of such magnitude require specific expertise and tool sets. Managers must be able to balance macro and micro perspectives, IT requirements, and business objectives. Accuracy is critical, and time can't be wasted using methodologies that don't produce quick and conclusive results.



### Make the process of data discovery and classification ongoing.

Data is constantly being created by existing and new end users. With today's IT environments in a constant state of change, businesses should have clear processes in place to regularly evaluate how data is being used and handled across users and platforms. This ensures the most up-to-date knowledge.

### Data in the cloud

There is still plenty of confusion as to how to manage and secure data in the cloud:

**93%** of IT security professionals worry that human error could accidentally expose data in a public cloud.

**37%** say that risk management capabilities in the cloud are at least somewhat worse than in other parts of the organization's infrastructure.

Only **22%** say their organization maintains continuous compliance with cloud security regulations and standards.<sup>2</sup>





## Commit to a holistic data management and security strategy.

IT and security teams need to oversee policies, controls, processes, end-user training, and governance across the environment. [Automation](#) can greatly support these efforts. And because unnecessary processes can expose your organization to security risks, process consolidation should be a priority.

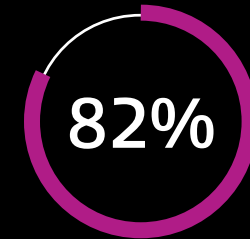
### Why is process consolidation critical?

In a recent Insight LinkedIn Live, Senior GRC Consultant Mansour Farani stressed the importance of taking a deeper dive into processes:

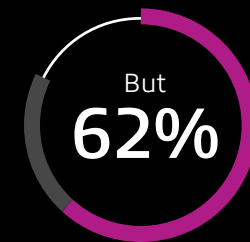
*"We worked with an organization to perform data discovery and classification, looking at all the channels that were handling sensitive information — and we identified 400 processes that were handling that sensitive data. We took a step back and identified those processes, mapped them, and then developed strategies around how to streamline processes, because each process created more risk for the organization. We eliminated some processes that were redundant and unnecessary. We did process consolidation and got rid of intermediary steps. And as a result, we made the organization leaner and more efficient."*

[Learn more by viewing the full LinkedIn Live session.](#) →

Identity and access management is also a critical focus area, particularly for businesses with remote and hybrid workforces. Traditional perimeter security strategies aren't effective when workers require access to business data off-site and from a variety of corporate-owned and personal devices. The most successful approaches are identity-based, in which users are only granted access to specific types of data.



of employees say their organization uses a data classification system.



of companies with a data classification policy provide employees access to more data than they need.



Such companies are

**2.5X** more likely to experience a data breach compared to companies with a data classification policy and restricted data access.<sup>3</sup>

## Don't go it alone.

The process of data discovery and classification has many moving parts and can be complex. A trusted solutions and services provider can help simplify the process. Here's what to look for in a partner:



**Proven experience, methodology, and tools** for collecting and aggregating data to drive decision-making



**Agnostic expertise** that brings together the best technologies and tools from industry leaders wherever appropriate



**Success beyond data discovery and classification** — the ideal partner will have end-to-end expertise with strategically integrating IT modernization initiatives for total synergy and transformation

### Start with an assessment from Insight

As a frontrunner in the data space, Insight has deep expertise in discovery and classification, migration, consolidation, hybrid cloud, managed services, and beyond. With decades of experience and proven, proprietary discovery tools like [SnapStart](#), we accelerate time to value and help you deliver on your promise to the business.

To start your journey with confidence, learn about our [Data Protection Assessment here](#).

#### Explore these resources for more information:

##### BLOG:

[The Value of an Experienced Data Migration Partner](#)

##### VIDEO:

[Why Store Data? Here Are 4 Reasons.](#)

##### VIDEO:

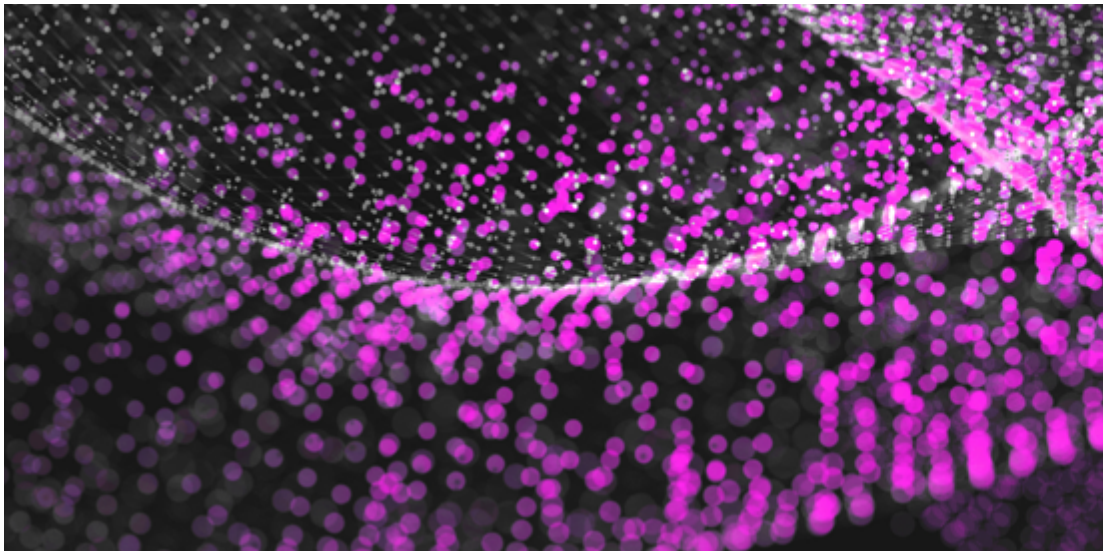
[Why Understanding Your IT Estate Is Critical — Plus 3 Reasons Why It's a Challenge](#)

##### VIDEO:

[SnapStart data discovery engine](#)

##### SOLUTION BRIEF:

[Data Protection Assessment](#)



## Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.



[solutions.insight.com](https://solutions.insight.com) | [insight.com](https://insight.com)

### Sources:

<sup>1</sup> Wiggers, K. (2021, April 15). Only 13% of organizations are delivering on their data strategy, survey finds. VentureBeat.

<sup>2</sup> Lapena, R. (2020, Aug. 12). Survey: 76% of IT Pros Say It's Difficult to Maintain Security Configs in the Cloud. Tripwire.

<sup>3</sup> Capers, Z. and Maria, G. (2020, Oct. 5). GetApp's 2020 State of Data Security Report – 10 Trends to Watch. GetApp.