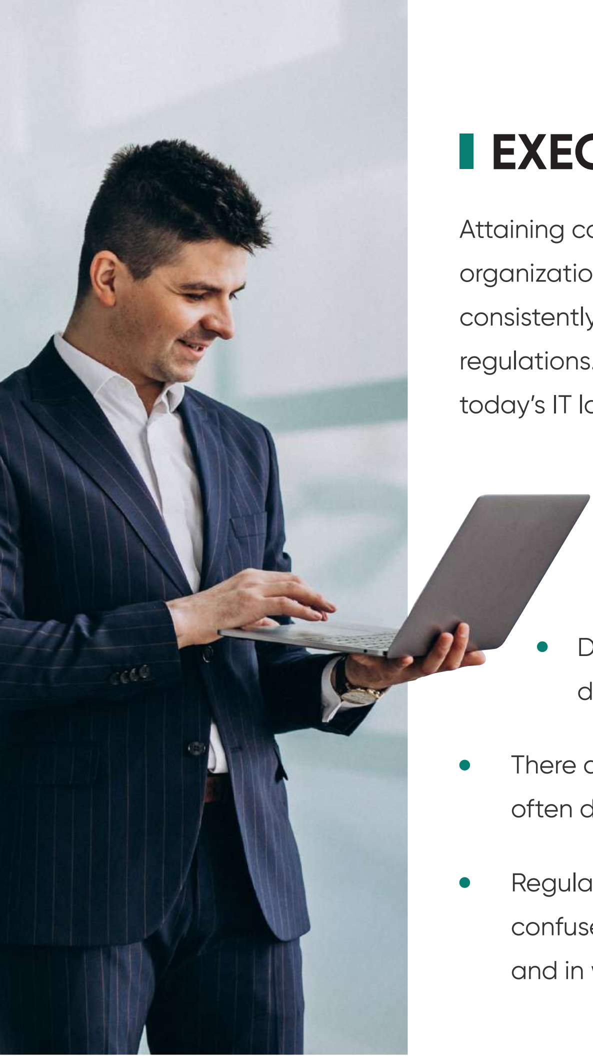
DRUVSTAR®

CLOSING THE DATA VISIBILITY GAPS IN YOUR COMPLEX, DISTRIBUTED ENVIRONMENT

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Attaining comprehensive data visibility is mission-critical if organizations want to secure their most sensitive data, consistently apply data governance policies, and comply with regulations. Several factors combine to hamper data visibility in today's IT landscape:

- Large volumes of data move across systems with high speed and frequency.
- Data gets stored in disparate locations across a distributed environment and in many different formats.
- There are many different data sources, and sensitive data is often duplicated across different sources.
- Regulatory oversight pertaining to specific types of data can confuse organizations about what controls to put in place and in what context.

This lack of visibility poses serious risks to data security, governance, and compliance. The only way to adequately protect sensitive data is to know where it is and who is accessing it. Often a gap emerges between the permission granted to data and the level of data access actually needed.

This sensitive data comes in a variety of forms:

- Protected Health Information (PHI) and Personally Identifiable Information (PII)
- Credit/Bank card information belonging to customers that transact with an organization
- Biometric data on both customers and employees
- Customer behavior data

Not only are organizations storing a large variety of sensitive data, but each data type has its own associated data protection guidelines. For instance, a healthcare provider needs to comply with HIPAA, which protects PHI for patients, and PCI DSS, which protects cardholder data for patients who pay for services using their credit or debit cards.

Furthermore, each data type often has its own associated data protection guidelines. For instance, a healthcare provider needs to comply with HIPAA, which protects PHI for patients, and PCI DSS, which protects cardholder data for patients who pay for services using their credit or debit cards.

Closing the data visibility gap requires the combination of strategies and solutions to fully catalog and visualize data, classify what's sensitive, enforce governance consistently, and monitor data access for anomalous behavior.

Organizations that take these necessary steps to meet the inevitable data visibility challenge are better placed to responsibly use data as a driver of business success while protecting their most sensitive data assets against leaks, breaches, and cyberattacks.

WHY IS DATA VISIBILITY GETTING HARDER?

- Increased Data Complexity
- Higher Volumes of Data
- Distributed IT Environments
- Increased Regulatory Oversight

You can't protect what you can't see. Visibility into data sources and how people are accessing that information is central to compliance and data protection. Data visibility gaps expose organizations to financial, legal, and reputational risks that can add up to severely impacting the bottom line. Here are some of the key factors behind the widening data visibility gaps in today's IT landscape.

Increased Data Complexity

Increased data complexity results in organizations struggling to identify the full scope and sensitivity of data collected and stored in disparate systems. A big driver of this complexity is unstructured data, which does not have a pre-defined data model or fit into relational databases with pre-defined structures. Unstructured data accounts for approximately 80 percent (Source) of modern business data.

Sources of unstructured data commonly generated and collected in today's business world include:

- Email copy
- Slack, Teams and other intranet messaging channels
- Text or voice logs from customer service interactions

- Medical records, such as radiology images or physician notes
- Data from social media touchpoints, including private messages, images, and comments
- Business documents, such as memos and PowerPoint presentations

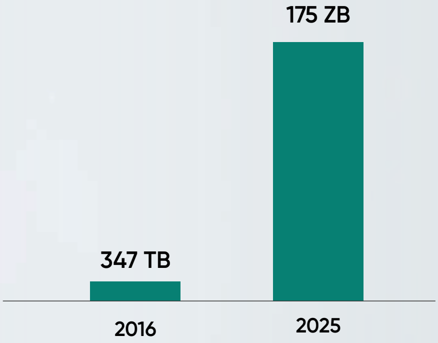
Sensitive information residing within all this unstructured data must be protected to avoid compliance issues and data breaches. The gap between the amount of data that needs to be protected and the amount of data that is actually protected is increasing.

The challenge organizations face is to identify all sources of structured and unstructured data and index or tag sensitive information within these data sources. In a real-time environment of near-constant data generation and user interaction with data, comprehensive visibility into data sources and users is a difficult challenge to meet without the right tools.

Higher Volumes of Data

The volume of data generated globally continues to rise at a startling rate. There will be 175 zettabytes (Source) of data worldwide by 2025, which amounts to a 61 percent compounded annual growth rate. Keeping up with this sheer volume of data growth poses a significant challenge to visibility for businesses of all sizes.

Even as far back as 2016, the average enterprise managed 347 terabytes of data and the average SMB managed 47 terabytes. It's safe to say these numbers have increased substantially since then.



Regulatory compliance demands that organizations track sensitive data, including where it's stored, how it's processed, and how it flows across the IT environment. With such large volumes of data generated daily, it's a formidable prospect to keep up with all this information and retain the necessary visibility.

Distributed IT Environments

Increased data volumes and complexity in the distributed nature of modern IT environments, compounds the data visibility gap. **Most businesses use a hybrid multi-cloud strategy combining traditional on-premise data centers with an average of 4.8 clouds** (Source). As data moves across this hybrid infrastructure and different users access it, many organizations struggle to maintain sufficient visibility.

It's not just the IT environment that is distributed—workforces are also distributed. Remote workers access company data from residential and public Internet connections. Knowing what data is being accessed, by whom, and at what times is critical. VPN connections lack the scalability needed to ensure visibility into the data access layer for a remote workforce.

Most businesses use a hybrid multi-cloud strategy combining traditional on-premise data centers with an average of 4.8 clouds

Increased Regulatory Oversight

High-profile data breaches exposing sensitive information, such as credit card details and healthcare records, have resulted in regulators demanding greater transparency about how organizations protect this data. Increased scrutiny from regulators comes in the form of more regular compliance audits, frequent legislative updates, and emerging new regulations.

Data protection laws require organizations to have granular visibility into sensitive data and its access across their IT environments. Often, a single organization needs to comply with several different regulations simultaneously, each with its own nuances. Almost 8 in 10 US businesses **have to comply with two or more privacy laws while 10 percent have to comply with up to 50 privacy laws simultaneously.**

Almost 8 in 10 US businesses have to comply with two or more privacy laws while 10 percent have to comply with up to 50 privacy laws simultaneously.

With increased regulatory oversight, compliance fatigue can set in as organizations trade off constant compliance demands for the ability to remain operational and conduct business as usual. As companies struggle to keep up with increased regulatory oversight, data visibility gaps naturally emerge. The scale of the problem is such that 51 percent of healthcare providers (Source) are still not HIPAA compliant.

THE RISKS OF INSUFFICIENT DATA VISIBILITY

- Exposed Sensitive Data
- Data Breaches
- Non-compliance

It's imperative for organizations to understand what sensitive data they have, where it resides, who can access it, who is accessing it, what is the access frequency, and detect abnormal access patterns. Without comprehensive data visibility, you can't adequately protect your most valuable and vulnerable information assets. Insufficient data visibility brings three key risks to your business.

Exposed Sensitive Data

83% (Source) of security professionals believe that employees have put customer PII and business-sensitive information at risk. This data exposure often arises due to data visibility gaps; employees don't know what is sensitive and what isn't because there is no clear inventory and classification of data. Sensitive data exposure can occur through email, file-sharing services, and collaboration tools.

Hybrid IT ecosystems further increase the risk of data exposure in light of data visibility gaps. Organizations can unintentionally expose sensitive data in public cloud services because they lack visibility into where their sensitive data is stored. This sensitive data exposure can affect even the biggest companies.

For instance in 2020, Pfizer exposed sensitive patient information on a misconfigured Google Cloud storage bucket.

Data breaches cost businesses $4.24 million per breach incident, and a lack of data visibility dramatically increases the risk of a data breach. These breaches can happen when an outsider accesses exposed sensitive data. Cybercriminals regularly trawl the Internet for unsecured cloud storage buckets that can provide easy access to sensitive data.

Another common cause of a data breach starts when an insider has access to resources that they shouldn't have and they disclose sensitive data. **97 percent of IT leaders (Source) cite insider data breaches as a major concern.** Incomplete data visibility results in unmonitored data access.

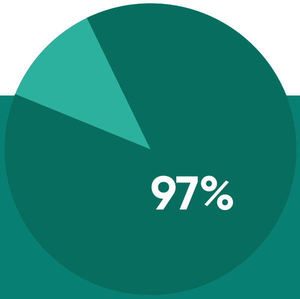
Generally, insider data breaches occur under the following three scenarios:

1. Users obtaining access to sensitive data through privilege escalation
2. Users getting access to more resources than they need to carry out their work
3. Users abusing the access they have and acting maliciously, such as by downloading large volumes of data

Data Breaches

A data breach occurs when the data for which your organization is responsible suffers a security incident resulting in an unauthorized disclosure. The consequences can be permanent and devastating for both individuals whose privacy has been violated as well as businesses who depend on their customers' trust in order to succeed. Data breaches can result in the following negative outcomes:

- The destruction of information
- Unauthorized use of confidential information
- Intellectual property theft
- Regulatory requirements to notify affected parties
- Compensation payments to customers, business partners, or other victims of the breach



97 percent of IT leaders (Source) cite insider data breaches as a major concern.

Non-compliance

Various regulations govern the protection and privacy of sensitive data. In the United States and Europe, these regulatory frameworks include CCPA, GDPR, HIPAA, PCI-DSS, and SOX. Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws. The right to data protection continues to be regulated in the form of increasingly strict and frequently updated regulations.

When you don't know where all your sensitive data is, you can't apply the controls, policies, and safeguards mandated by regulations.

Taking HIPAA as an example, violations of the regulation include:

- Unauthorized access to protected health information (PHI)
- Failure to implement safeguards to ensure the confidentiality, integrity, and availability of PHI
- Failure to provide patients with copies of their PHI on request
- Failure to implement access controls to limit who can view PHI
- Failure to terminate access rights to PHI when no longer required

Data visibility gaps are often the root cause behind these violations. When you don't know where all your sensitive data is, it's impossible to comply with data subject access requests, implement access controls, or safeguard data using encryption. Addressing these visibility gaps is key to reducing non-compliance risks.

Organizations failing to protect data in line with relevant regulations are at risk of non-compliance and the significant costs associated with that. The average cost of non-compliance currently stands at $14.82 million (Source). These costs of non-compliance include penalties, productivity losses, and business disruption.

STEPS TO CLOSE YOUR DATA VISIBILITY GAPS

- Build A Centralized Data Catalog
- Leverage Metadata for Context
- Classify and Control
- Manage Data Access

Build A Centralized Data Catalog

Full data visibility starts with building a centralized source of truth that properly catalogs all of your information assets, where they are stored, who owns the assets, who can access the data, and what governance or security measures currently protect that data. The visibility provided by a centralized data catalog informs organizations about where sensitive data exists across structured and unstructured data sources.

Organizations lacking a centralized repository that catalogs their information assets don't know where all their sensitive data is and if it's protected sufficiently for compliance. Furthermore, consistently applying governance policies across the full spectrum of your information assets isn't possible without this centralized inventory.

API-driven integrations with various asset scanning and asset inventory tools can help to build an accurate centralized data catalog that fully accounts for sensitive data across a complex, distributed IT environment. Machine learning techniques can find sensitive information lurking inside unstructured data sources, such as spreadsheets, marketing material, and reports.

Leverage Metadata for Context

Metadata helps to enrich data with additional contextual information that can make it easier to track, manage, and protect data. For sensitive data, metadata clarifies how PII, PHI, and other sensitive information is protected and governed.

Some examples of metadata that improves data visibility include:

- Who owns the data asset and who is the custodian
- The relationships between different data objects
- Tags that describe the purpose for processing sensitive data
- Retention policies that describe how long to retain particular data objects or attributes for regulatory compliance
- Data security controls, including encryption and anonymization
- Information about who can access the data

Leveraging metadata for added context can come from manual or automated approaches. The manual approach requires a data or security administrator to enrich the objects in a centralized data catalog. An automated approach uses connectors and APIs to extract metadata for each asset automatically. In practice, both approaches will be needed to get full context and visibility into sensitive data.

Classify and Control

Not all data requires the same level of protection. Organizations need to classify their data based on sensitivity levels, the potential for harm in the event of an unintentional disclosure, and the risks to particular data sources. These classifications can be as simple as “restricted, confidential, private, and public.” The data classification should ideally keep pace with real-time as organizations constantly generate and collect new data.

The point here is to simplify the process of protecting sensitive data at rest, in motion, and while in use with the appropriate policy-based controls. Dynamic classification is a key enabler in ensuring sensitive data is protected and handled appropriately.

Manage Data Access

Data visibility doesn’t just relate to where an organization’s data is—it’s also about knowing how data is being used and by whom. It’s imperative to implement access controls that selectively restrict who can access sensitive information based on job function, data sensitivity, and contextual factors such as user location. Compliance and effective data governance begin when an organization restricts data access to only the information assets strictly necessary for an employee to carry out their job duties and only in the approved contexts based on policies.

Controlling access on its own is not enough for data visibility. Organizations need to monitor access to IT assets to ensure consistent policy enforcement over how sensitive data is being used. User activity monitoring or other types of activity logs can help to provide insight into how data access is being used.

WHAT TO LOOK FOR IN A COMPREHENSIVE DATA VISIBILITY SOLUTION

- Intuitive Cross-Environment Visualization
- Policy Enforcement
- Automation (Discovery, Classification, and Users)
- Threat Detection

Intuitive Cross-Environment Visualization

A key requirement of a comprehensive data visibility solution is to intuitively visualize data assets, where those assets reside, and how users access those assets through applications and services. Visualization should extend to data classification so that organizations can easily view and secure their most sensitive assets.

Data visibility solutions must operate across all types of modern IT architectures. Whether an organization runs on-premise only, fully cloud-based, or a hybrid architecture, it's critical to be able to discover and visualize data across all types of IT environments.

Automation (Discovery, Classification, and Users)

Organizations constantly generate and store new data. Any data visibility solution needs to incorporate as much automation as possible to keep pace with the explosive levels of data growth in today's business landscape. The ability to automate should cover the most fundamental aspects of data visibility, including:

- Automated discovery of data assets, including structured and unstructured data across a multi-cloud hybrid IT environment

- The ability to automatically apply classification tags to structured and unstructured data based on context, risk, and sensitivity levels
- Automated user discovery so that organizations can easily track who has access to sensitive dat

Time is of the essence when it comes to data discovery and stopping data breaches. Automation reduces the time it takes to discover and classify sensitive data from months to hours.

Policy Enforcement

Effective governance ensures that sensitive data is handled with appropriate care based on an organization's policies while also helping to comply with regulations. However, merely having governance policies and procedures for data is not enough to protect data—consistent policy enforcement across the IT environment is what matters.

A comprehensive data visibility solution should provide the ability to monitor the environment for policy violations via a central dashboard. This policy enforcement should be capable of providing rapid alerts based on anomalous user behavior or data access. The ability to quickly investigate and act on policy violations protects sensitive information and reduces the risk of data breaches.

Threat Detection

Threat actors constantly probe IT environments looking for weaknesses that can provide access to the crown jewels—sensitive data. Modern data visibility solutions should extend beyond data discovery to sophisticated threat detection, including:

- Detecting and alerting about unauthorized data access
- Using AI-driven anomaly detection to stay ahead of threat actors
- Track expired access and de-provision access for users who no longer need it

Product

DruvStar Data Vision™

Visibility

360-degree visibility into your data sources and users

Classification

A comprehensive data security map and data classification

Monitoring

Policy-based data protection and monitoring

Detection

The ability to track data access and detect anomalies, regardless of source

Contact Druvstar today to find out how we can help you close your data visibility gaps, secure your most sensitive information assets, and help your data work for you rather than against you.

Schedule a demo now

info@druvstar.com druvstar.com

Secure your business with Druvstar's trusted cybersecurity products and services

Services

Cybersecurity Protection

- 24/7 Security Operations Center (SOC).
- Managed Detection And Response (MDR).
- Security Incident And Event Management (SIEM)
- Threat Intelligence
- Incident Response
- Root Cause Analysis

Cybersecurity Assessment

- Penetration Testing
- Internal Vulnerability Scan
- D-SWAT
- Product Security Verification
- Mobile Application Security Testing
- Web Application Security Testing
- Security Readiness Assessment

Cybersecurity Training

- OWASP Top10
- Security Awareness
- Incident Handling
- Ethical Hacking and Countermeasures