

# Harness the Power of Data Security

Leveraging Daser's Capabilities to Address Enterprise Data Security and Governance Needs







# Harness the Power of Data Security

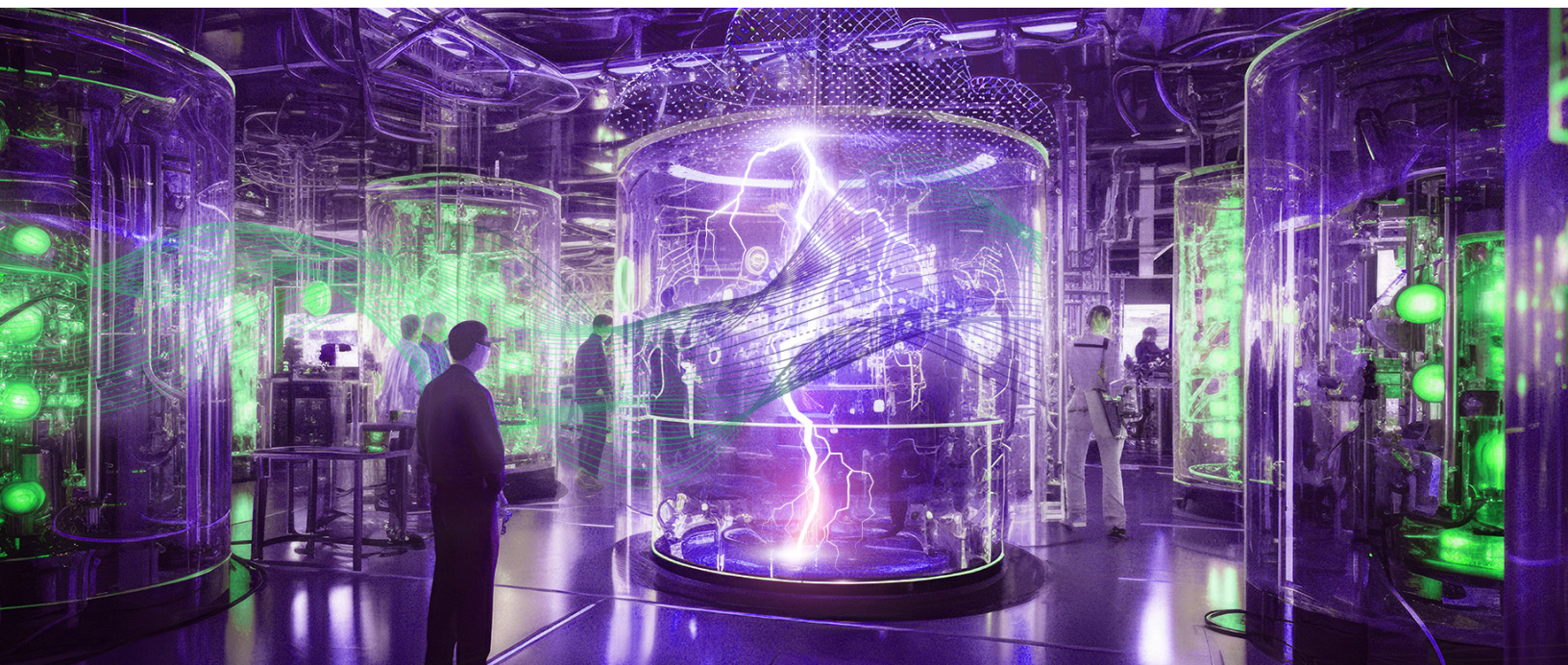
In the digital age, data is the beating heart of organizations, pulsing through every decision-making artery, fueling innovation, and propelling businesses to new growth frontiers. But as powerful as data is, it can also become the Achilles heel for organizations if not managed and safeguarded effectively. Data breaches, misconfigurations, and mishandling can bleed a company's financial resources and damage its reputation.

It's about protecting data and governing it with intelligence and precision. This calls for a solution that delivers end-to-end data security and governance.

## **Enter Dasera.**

More than a data security platform, Dasera is a powerhouse that equips businesses with comprehensive capabilities to ensure data visibility and accessibility across various data store types and platforms. It's not just about building walls around your data but about understanding its nature, movement, and vulnerabilities. With Dasera, you're not just reacting to threats but preemptively fortifying your data landscape.

In this paper, we will explore the powerful capabilities that Dasera brings to the table and illuminate how it can solve the complex pain points of enterprise data governance. In the data security era, data security and governance are synonymous with business resilience and growth.





# Dasera's Comprehensive Suite of Capabilities

In the vast and often convoluted landscape of enterprise data security, Dasera stands out as a powerful sherpa, equipping businesses with powerful capabilities to navigate and conquer the complex terrains of data security and governance. Whether you're struggling with data visibility or dealing with intricate configuration challenges, or you need to discern who has access to what data or how your data is being used – Dasera has a solution tailored for you.

Dasera offers key capabilities, including Data Store Auto-Discovery, Configuration Analysis, Privilege Analysis, Classification, and Data-in-Use Monitoring. These capabilities help organizations discover and analyze their data stores, monitor usage, and maintain robust data security and governance.

## Auto-Discovery

Discovering data is the foundational step in data governance and security. Given today's businesses' diverse and complex architecture, it can take time to identify all the data stores effectively. Dasera's Auto-Discovery capability automates this process, ensuring that every data store across AWS, Google Cloud, and Microsoft Azure are identified and accounted for. This automated detection reduces the risk of leaving out any data stores, thus ensuring complete data visibility.

This capability is particularly crucial for organizations dealing with substantial volumes of data across various platforms. It frees up time and resources by eliminating manual tracking of data stores, and it ensures that no

data repository goes unnoticed or unprotected. This comprehensive view facilitates better decision-making and planning in data security and governance.

Consider the use case of a rapidly expanding enterprise that has seen a series of mergers and acquisitions. With each integration, new data stores are added to the mix, and in the rush of business, some of these may get sidelined or forgotten. Without a systematic approach to discovering these stores, they could become 'orphaned' and open to data security risks. Here, Dasera's Auto-Discovery capability can be a game-changer, detecting these orphaned data stores and ensuring they're included in the governance loop.

Similarly, in highly decentralized organizations where individual departments or teams may have autonomously set up their data stores, Dasera's Auto-Discovery ensures these data stores are brought to light and effectively governed. This promotes data security consistency and prevents data silos that could negatively impact business intelligence and decision-making.

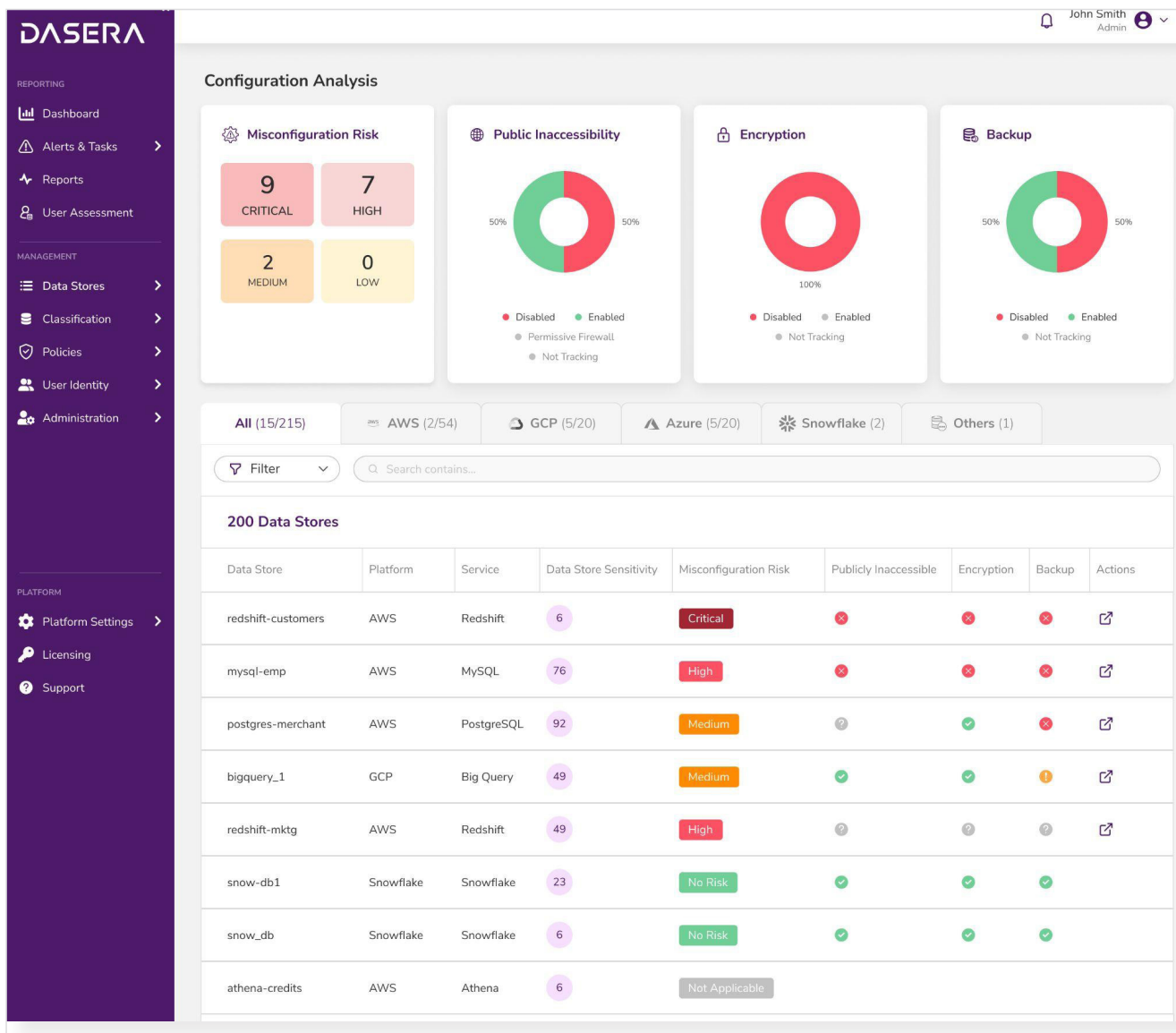
Dasera's Auto-Discovery capability is a vigilant sentinel, automating the data discovery process, eliminating manual tracking errors, and unmasking shadow data. It guarantees complete data visibility, enabling your business to implement comprehensive and effective data security and governance. Trust Dasera to shine the light on your data landscape, illuminating the shadows and empowering your business to make data-driven decisions confidently and securely.



## Configuration Analysis

Misconfigured data stores can leave your data exposed and susceptible to breaches. With Daser's Configuration Analysis, businesses can efficiently mitigate these risks. Daser systematically inspects configurations across various data store types, confirming that they conform to best practices. This includes verifying encryption settings, data backups, and public accessibility, firewall configurations, access controls, and other security features that help secure your data from unauthorized access.

The importance of accurate configuration analysis must be considered. Misconfigurations can create inadvertent entry points for malicious attackers, leading to data breaches. By continuously and automatically reviewing the configurations, Daser helps businesses promptly identify and rectify any misconfigurations, reducing the window of opportunity for potential cyber threats.



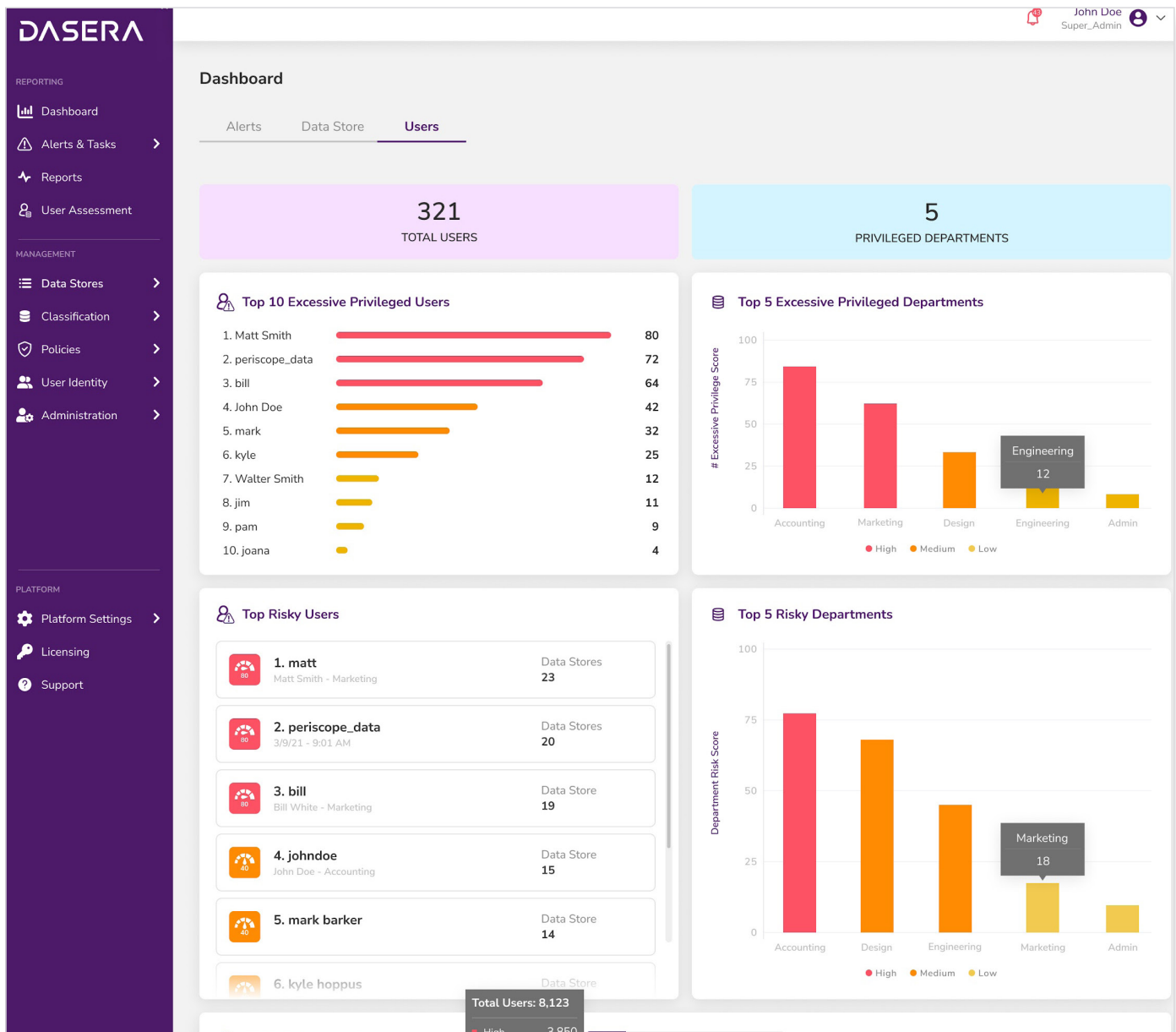


## Privileges

Understanding who has access to what data is central to a robust data governance strategy. Dasea's Privileges Analysis capability retrieves detailed user and role information from databases and information about object-level access. This data is critical for maintaining tight control over who can access, modify, or delete data in your organization.

With this capability, you can ensure that the principle of least privilege (PoLP) is effectively implemented,

reducing the risk of data breaches caused by excessive access rights. Furthermore, Dasea's granular Privileges Analysis supports several platforms and data store types, meaning that businesses of all kinds can reap the benefits of stringent access control, no matter their preferred data environment. Dasea's Privilege Analysis goes much deeper than others in data security, ensuring you have granular visibility into who should and should not have access to data stores.





## Classification and Data Tagging

Accurate data classification is critical to effective data governance. By classifying data according to its sensitivity and business value, you can implement appropriate protective measures, such as encryption for highly sensitive data. Moreover, data tagging helps businesses identify data subject to regulation and comply with regulatory frameworks like GDPR and CCPA that mandate certain protections for specific data types.

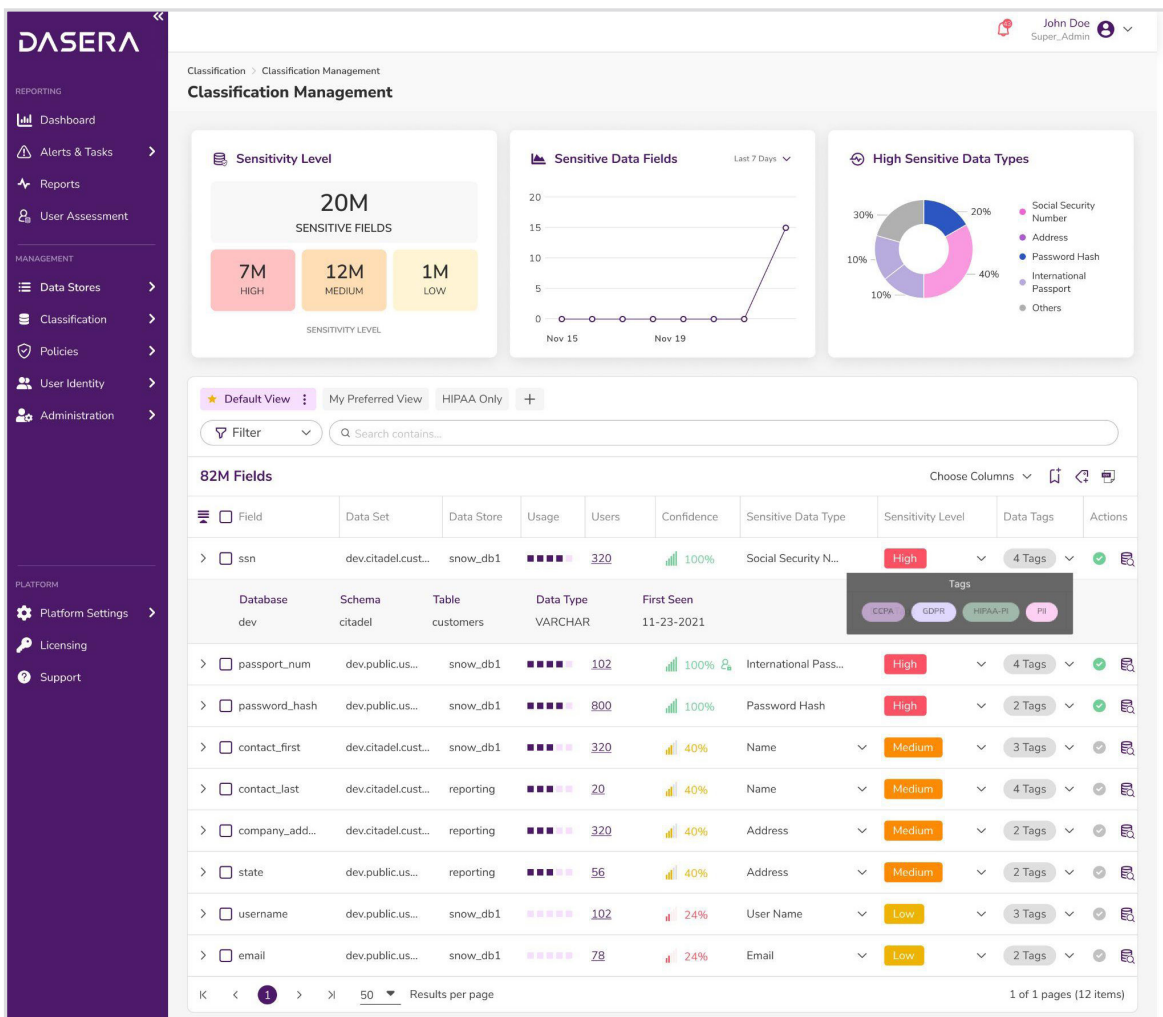
Dasera classifies sensitive data across all your infrastructure - structured or unstructured, cloud or on-premise.

### Structured data in:

- Data warehouses (e.g., Redshift)
- Cloud-managed or self-managed Relational Databases (e.g., MySQL, PostgreSQL)
- Cloud Data Platforms (e.g., Snowflake, Databricks)
- NoSQL Databases (e.g., MariaDB, DocumentDB)

### Unstructured data in:

- All Text and Image based unstructured data in data lakes (e.g., AWS S3)





## Data-in-Use Monitoring

Data-in-Use Monitoring is an essential component of a comprehensive data security approach. It allows businesses to track how their data is accessed and used, enabling them to spot suspicious or anomalous activity. Dasera's data-in-use monitoring capability uses not only native query logs but also custom ones, ensuring businesses have a complete understanding of their data usage patterns.

This functionality is crucial in identifying potential insider threats, policy violations, and other security risks. By providing a clear data usage overview, Dasera empowers businesses to take quick action when anomalies are detected, mitigating potential damage. This proactive approach to data security significantly reduces the risk of data breaches and helps maintain the integrity of your business's data.

**Alerts & Tasks**

**Alert Status**

38  
TOTAL OPEN ALERTS

10 CRITICAL | 14 HIGH | 8 MEDIUM | 6 LOW  
ALERTS BY SEVERITY LEVEL

**Alerts by Policy Types**

- Data Exfiltration
- Privacy Violation
- Field Classified
- Data Modified
- Others (2)

**Top Policies By Alerts**

- New SSN Field: 86
- Exfiltration <1,000 medium: 75
- SOX Compliance: 62
- Highly Sensitive Data Loss: 58
- New SSN Field: 45
- New SSN Field: 31
- SOX Compliance: 17
- SOX Compliance: 9
- Exfiltration <1,000 medium: 5

Filter	Date/Time	Policy Name	Policy Type	Employee	Severity	Status
	3/10/21 9:01 AM	Privacy violation on PII	Privacy Violation	Darrell Steward	Critical	Open
Alert ID: 123		Who was Notified: <a href="#">Setup Workflows</a>	Query: /*Query generated by Periscope Data ["chart_name"=user_growth_monthly"...	Rows Produced: 800	<a href="#">View Fields Impacted</a>	
Data Store Name: Snowflake_db1		Employee: Bob Williams	12 Other Policies Triggered by this Query			
	3/10/21 9:01 AM	High Sensitive Data Classified	Classification	Theresa Webb	Critical	Open
	3/10/21 9:01 AM	Ghost Users With Access to Sensi...	Data Access	Eleanor Pena	Critical	Open
	3/10/21 9:01 AM	Large Volume of Highly Sensi...	Data Exfiltration	Dianne Russell	High	Open
	3/10/21 9:01 AM	Highly Sensitive Data Loss	Data Exfiltration	Jane Cooper	High	Open
	3/10/21 9:01 AM	Privacy violation on HIPAA	Privacy Violation	Wade Warren	Medium	Open
	3/10/21 9:01 AM	Privacy violation on GDPR	Privacy Violation	Courtney Henry	Medium	Open
	3/10/21 9:01 AM	Regulated Data Accessed - Exfiltrati...	Data Exfiltration	Esther Howard	Low	Open

1 of 1 pages (12 items)



# The Daser-Snowflake Advantage

Snowflake is a popular choice among enterprises for its robust data warehousing capabilities. But when Daser complements Snowflake's power, the results are nothing short of transformative.

Daser adds a critical layer of intelligent data security and governance to Snowflake. With Daser's ability to analyze configurations, retrieve privileges, classify data, and monitor data-in-use in Snowflake, organizations can secure their data and optimize their data management practices.

Daser also provides a 360-degree advantage to Snowflake customers by triggering downstream Snowflake dynamic masking and access control workflows and policies. Daser's in-depth monitoring of data-in-use within Snowflake also provides valuable insights into data access patterns, helping identify potential security risks or policy violations.

## Data-in-Use Risk Assessment

Analyzes **Snowflake's** query logs to monitor interactions with data using its premium query analysis engine to surface security and compliance risks.

## Privilege Risk Assessment

Highlights and alerts on over privileged users and data stores so you can't restrict access using **Snowflake**.

## X-Functional Workflows

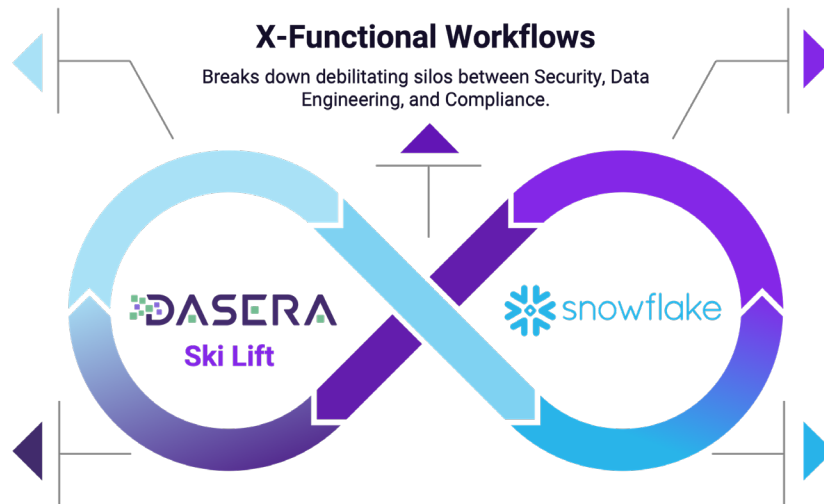
Breaks down debilitating silos between Security, Data Engineering, and Compliance.

## Custom classification and auto tagging

Allows you to extend **Snowflake's** classification with the **Daser's** built-in custom classifiers and automatic tagging.

## X-Platform Automation

Ingests **Snowflake's** data to automate policies that orchestrate cross platform tasks to enforce business controls (e.g. applying **Snowflake's** masking policy).



### Snowflake:

Modern cloud-based data storage and analytics service which improves access and usability to data.

### Daser Ski Lift for Snowflake Users:

Automated end to end platform for data security and governance across entire data infrastructure, data lifecycle, data users, data access & data storage.





## Dasera and Data Catalogs

Data catalogs serve as a structured inventory of a company's data assets, improving visibility and accessibility. Integrating Dasera with data catalogs brings another level of sophistication and security to data governance. Tags, labels, and classification results can be shared across Dasera and catalogs to enrich data and analytics efforts.

Dasera enriches data catalogs by automating data classification and privacy risk identification. It makes sensitive data easily identifiable and helps implement appropriate access control policies. Further, by continuously monitoring data-in-use, Dasera provides unique insights into how the cataloged data is being used and by whom, identifying any anomalous activities or potential policy violations.

## On-Prem Capabilities: A Significant Dasera Differentiator

In an era where cloud adoption is booming, Dasera remembers the critical data assets that still reside on-premises. Its capabilities extend not only to include the cloud but also to self-managed platforms like Microsoft SQL Server, Oracle, and PostgreSQL.

While these on-prem data stores can be somewhat of a blind spot for some data security solutions, Dasera's comprehensive suite of capabilities ensures they're just as protected and governed as their cloud counterparts. Dasera leaves no stone unturned in safeguarding these traditional data stores from auto-discovery to data-in-use monitoring.

Moreover, this ability to offer end-to-end data security and governance across cloud and on-premises environments is a significant differentiator for Dasera. It means businesses can benefit from consistent, comprehensive data security and governance regardless of where their data resides. This consistent approach not only simplifies data governance but also ensures no data store is left unprotected, reinforcing overall data security. Dasera truly presents a single pane of glass to view all data and risks both on-prem and in the cloud.



# Addressing Pain Points with Daser

Daser's capabilities are comprehensive and flexible, able to adapt to various data store types and platforms. This versatility is invaluable to businesses juggling diverse and constantly evolving data environments.

For instance, enterprises leveraging AWS can take advantage of Daser's full capabilities with AWS Redshift, while those using Google Cloud Platform can enjoy comprehensive support with BigQuery. Microsoft Azure users also benefit from extensive capabilities

when using Azure Synapse Analytics or Azure SQL Database. This extensive platform coverage ensures that Daser can help secure and manage your data no matter where it resides.

Moreover, Daser recognizes and adapts to the unique challenges of different data store types. From SQL databases like MySQL, PostgreSQL, and SQL Server to NoSQL databases like DynamoDB and MongoDB Atlas, Daser provides relevant solutions to secure and govern your data effectively.





# The Data Security Era

Navigating the complexities of the modern data landscape can feel like sailing in uncharted waters. The rules change rapidly; the threats grow more sophisticated, and the stakes increase. Amid these shifting sands, enterprises need more than just a solution; they need a trusted ally that can keep pace with their evolving needs, an ally that is as forward-thinking and adaptable as they are. Dasera is that ally.

Dasera is not just a tool; it's a paradigm shift in how enterprises approach data security and governance. It transcends the boundaries of traditional data protection solutions with its holistic capabilities, expansive platform coverage, and innate flexibility. But the magic of Dasera lies not just in its power-packed features but also in its vision. This vision sees data security and governance as protective measures and strategic enablers.

By ensuring robust data security and intelligent governance, Dasera allows businesses to unlock the true potential of their data without being held back by fear of breaches or compliance woes. It empowers organizations to use data confidently and responsibly to drive decision-making, fuel innovation, and enhance customer experiences.

With Dasera, you're not just safeguarding your data; you're protecting your business objectives, reputation, and future. Embrace Dasera and steer your enterprise into a new era where data security isn't a challenge to overcome but a strength to leverage. Data security is a journey, not a destination. **Request a demo today**, and let's navigate this path successfully together.

Don't wait any longer – **contact our data security experts at Dasera** to learn how we can help you navigate the complexities of data management and security and unlock your business's full potential.