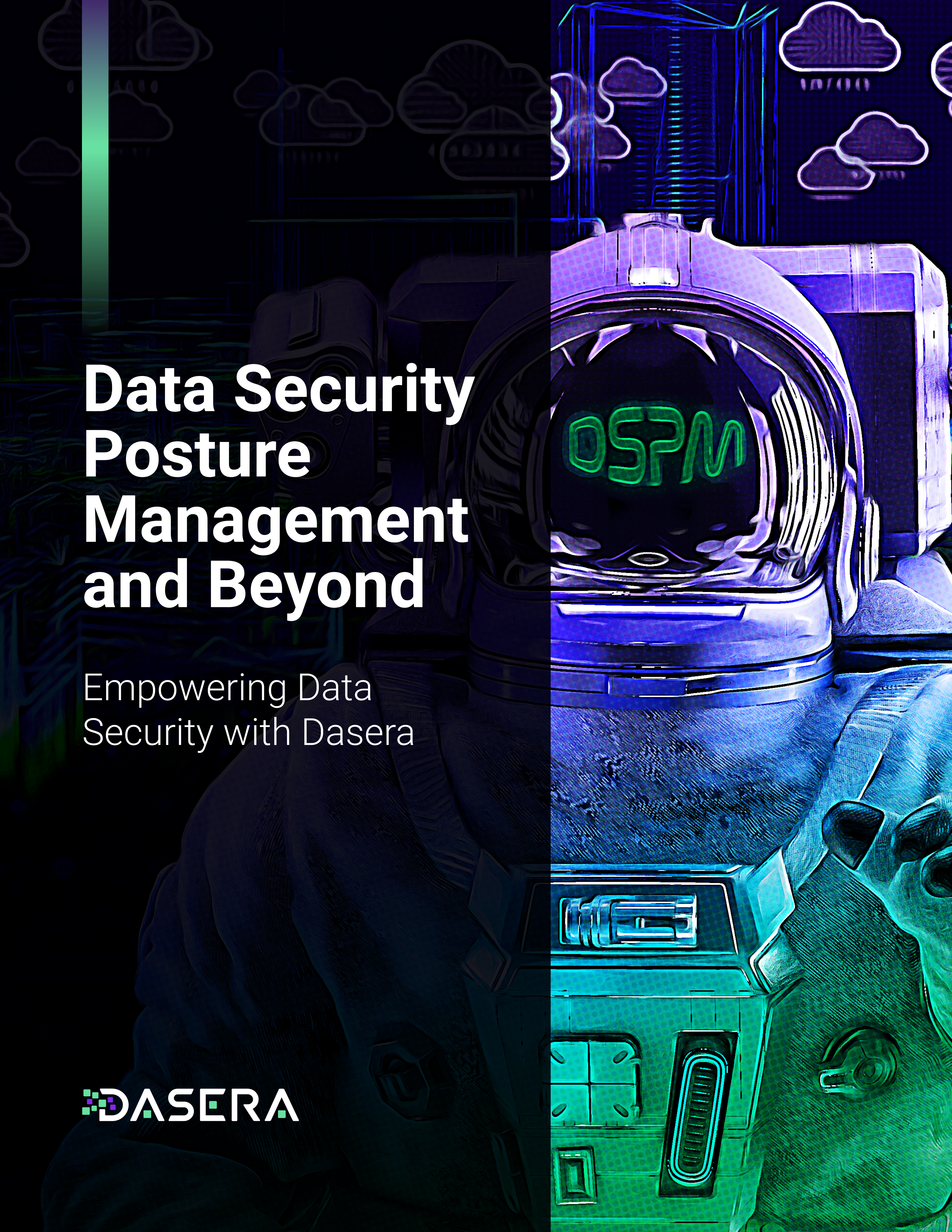


Data Security Posture Management and Beyond

Empowering Data Security with Dasera

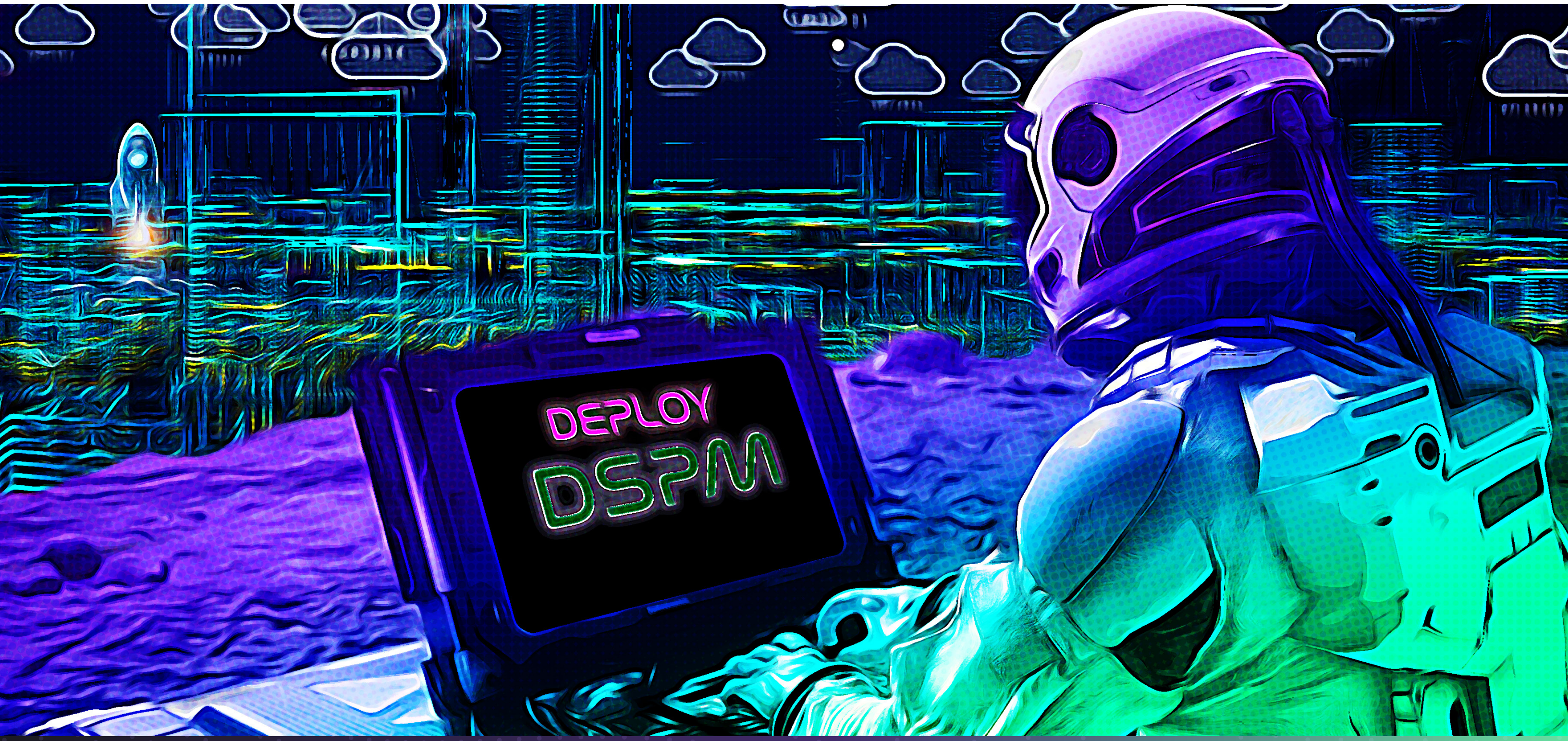
DASERA

What is Data Security Posture Management (DSPM)?

With the rapid proliferation of sensitive data in modern cloud environments, it can be challenging for organizations to know where all their data is and how it is secured. Data Security Posture Management (DSPM) solves this issue by providing a practical approach to securing cloud data and ensuring that sensitive and regulated data always has the correct data security posture, no matter where it is stored or moved.

DSPM has quickly become an emerging security trend and a crucial component of a defense-in-depth strategy. It helps organizations discover all their cloud data, classify it by data type and sensitivity level, detect and alert on data security policy violations, prioritize those alerts, and provide remediation playbooks.

This paper delves into the significance of DSPM in today's data-centric world, contrasting it with established methodologies. Furthermore, it sheds light on the advanced capabilities that customers need beyond standard DSPM tools. We will also elaborate on the mechanics of DSPM and pinpoint critical attributes to consider when selecting a DSPM solution. As our global landscape grows more reliant on data, adopting an effective strategy to protect sensitive information against unauthorized access, theft, or misuse becomes paramount.



What Problems Does DSPM Solve?

Businesses are moving towards cloud transformation initiatives and data democratization to meet the high expectations of their customers and employees. This transformation has made the data available to more people to harness its value better. But with the increased accessibility and data sharing comes a new set of challenges that require practical solutions to ensure data security and privacy.

The cloud transformation era is characterized by the sprawl of cloud data storage technologies across multiple cloud providers, the proliferation of data, the death of traditional perimeters, and a faster rate of change. The convergence of these factors has created a new kind of threat, which most organizations accept as the cost of doing business.

This is where DSPM comes in. DSPM provides organizations with a practical approach to securing cloud data by ensuring sensitive and regulated data always has the correct data security posture regardless of where it is stored or moved to. DSPMs must be able to discover all data, both in cloud and on-prem, classify it by data type and sensitivity level, detect and alert on data security policy violations, prioritize those alerts, and provide remediation playbooks.

By implementing a DSPM solution, companies can mitigate the risks associated with data democratization and cloud transformation initiatives, ensuring their sensitive data remains secure, regardless of the complexity of their cloud environment. Gartner predicts DSPM will become critical to data analytics initiatives, making it an essential component of any defense-in-depth strategy.

> **“By 2026, more than 20% of organizations will deploy DSPM technology, due to the urgent requirements to identify and locate previously unknown data repositories and to mitigate associated security and privacy risks.”**

What are the Benefits of DSPM?

DSPM solutions answer the most crucial question in cybersecurity - “Where is my data?” Before securing your data, you must know where it is, especially the critical business, customer, or regulated data. With the advent of the new era of agile, your data can be almost anywhere in the cloud, making it challenging to keep track of.

DSPM is a new prescriptive approach to securing your organization’s data on-prem or in your cloud environment. In the words of Gartner, “Data security posture management (DSPM) provides visibility as to where sensitive data is, who has access to that data, how it has been used, and what the security posture of the data store or application is.”

At its core, DSPM involves a three-step process: Find, Flag, and Fix.

Find

In the Find phase, DSPM locates your data, classifies its data type, and tags it for regulation and security standards. This phase is essential because data location and identification is a massive issue in DevOps and data-driven organizations, where an expanding amount of structured or unstructured data can be located anywhere, whether in the cloud or on-premises, and where access permissions are given much more liberally resulting in accelerated data manipulation and movement.

Flag

The Flag phase automatically identifies data security risks and helps prioritize the remediation order. These risks can come in various forms, including misconfigurations at the data store or field level, inappropriately located sensitive data, and user access permissions. The ability of a DSPM platform to comb through the vast amounts of data in the cloud to identify security risks is critical to ensure your data is secure and compliant.

Fix

In the Fix phase, DSPMs secure cloud data at risk by remediating the security risks found during the Discovery and Detection phases. This remediation comes in two flavors: (1) automated orchestration or (2) escalating tickets to stakeholders. The more powerful DSPMs can automate many issues automatically to enable your security team to be more efficient and agile. However, some issues need a decision made by a security professional, so DSPMs need to be able to alert as a remediation option.

DSPM is a holistic approach that acknowledges the complexity of modern hybrid cloud environments. It provides a comprehensive view of your data by offering visibility as to where sensitive data is, who has access to that data, how it has been used, and the security posture of the data store or application. With DSPM, you’ll better understand your data and how to secure it, making it less susceptible to data breaches, cyberattacks, and regulatory violations.

How Do You Use DSPM?

Here are the five key ways you can use DSPM to safeguard your data:

Data Discovery and Classification:

With DSPM, you can easily map your data landscape, identifying and classifying all known and unknown data, including shadow and abandoned data lurking in cloud accounts.

Policy Validation and Enforcement Automation:

DSPM can quickly find, prioritize, and fix policy violations for all your cloud data as it travels through the cloud, saving you time and effort.

Sensitive Data Protection:

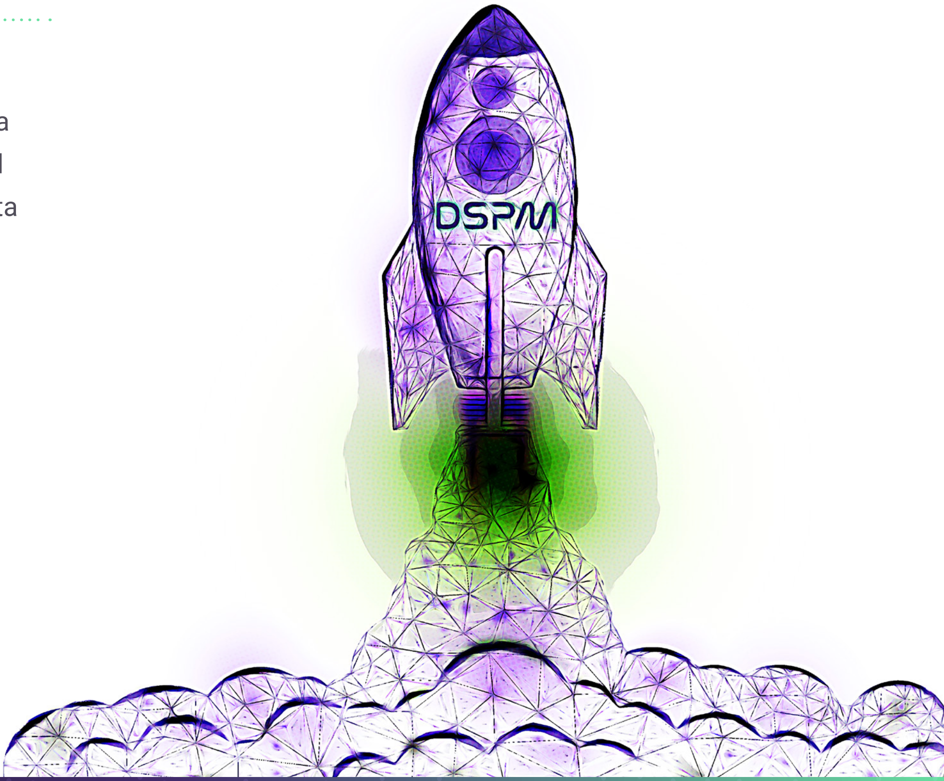
DSPM can pinpoint all your exposed sensitive data and remediate any misplaced data, misconfigured controls, or overexposed access, keeping your data secure from public exposure.

Ensure Data Regulation Compliance:

With DSPM, you can detect and create alerts when sensitive and regulated data violates data policies, ensuring you comply with regulations.

Environment Segmentation:

DSPM can help you segment your environment based on data privacy requirements (e.g., PCI DSS, HIPAA) and business needs, enabling you to enforce environment segmentation and data privacy.

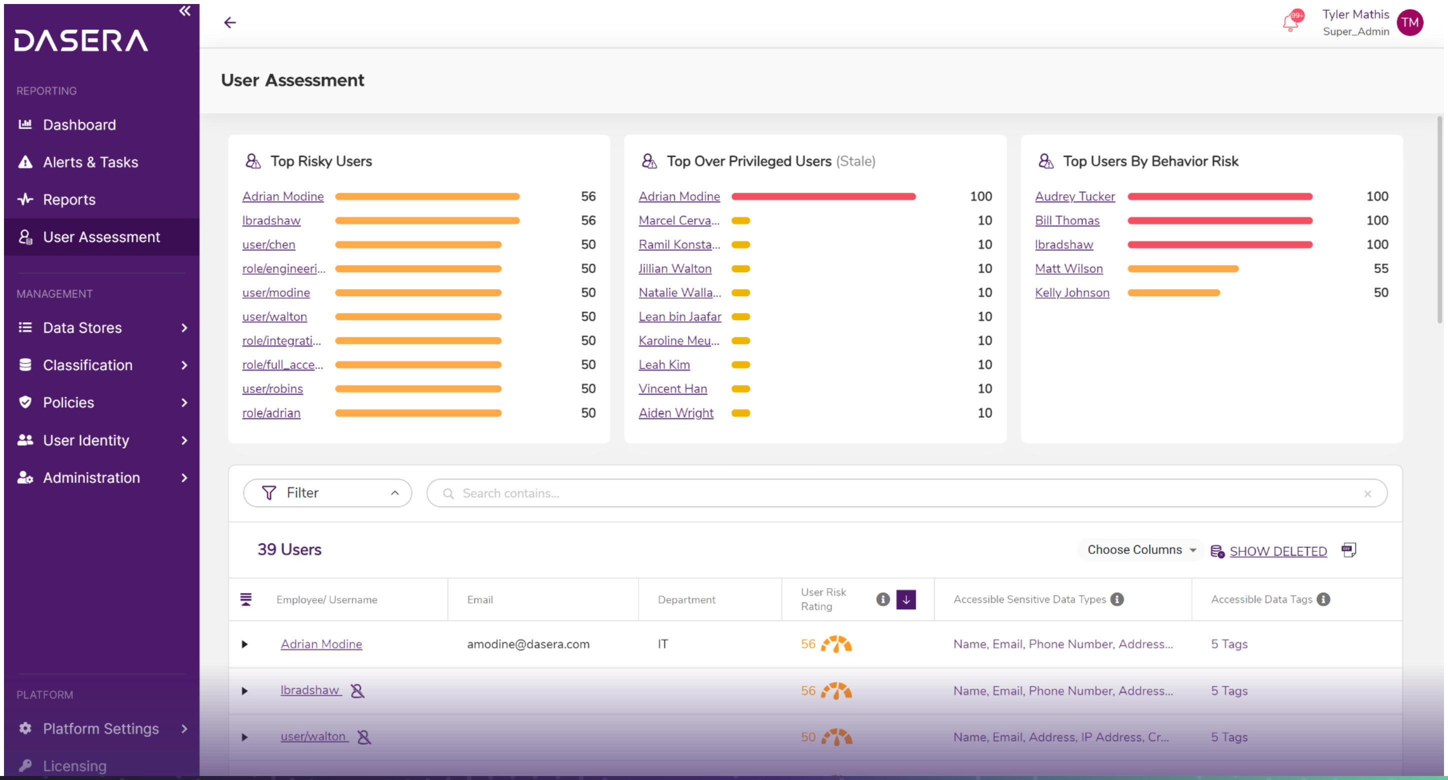


Enhancing DSPM with Real-Time Data Usage Monitoring and Query Analysis

While DSPM is an essential and powerful tool for securing cloud data, it has some things that need to be addressed to achieve a more comprehensive data security approach. One of the primary challenges with traditional DSPMs is their focus on data at rest, leaving a critical gap in monitoring data usage or data-in-use. This limitation means that DSPMs may not provide real-time visibility into how data is being accessed, used, or modified, which can lead to potential security blind spots.

To overcome these shortcomings, advanced data security platforms like Dasera go beyond traditional DSPMs by introducing data usage and data-in-use monitoring capabilities. Dasera's platform offers a holistic approach to data security by providing real-time insights into data access patterns and usage. By continuously monitoring data activities, Dasera ensures that any data misuse or access risks are immediately detected and flagged, enabling prompt remediation actions.

Incorporating data usage and data-in-use monitoring, along with sophisticated query analysis, enhances the effectiveness of DSPM solutions. Organizations can now have a complete view of their data security landscape, encompassing data at rest and in use. By closing these gaps, Dasera enables businesses to create a robust data security posture, effectively protecting sensitive information and maintaining compliance with data regulations.



User Assessment

Top Risky Users

Adrian Modine	56
lbradshaw	56
user/chen	50
role/engineeri...	50
user/modine	50
user/walton	50
role/integrati...	50
role/full_acce...	50
user/robins	50
role/adrian	50

Top Over Privileged Users (Stale)

Adrian Modine	100
Marcel Cerva...	10
Ramil Konsta...	10
Jillian Walton	10
Natalie Walla...	10
Lean bin Jaafar	10
Karoline Meu...	10
Leah Kim	10
Vincent Han	10
Aiden Wright	10

Top Users By Behavior Risk

Audrey Tucker	100
Bill Thomas	100
lbradshaw	100
Matt Wilson	55
Kelly Johnson	50

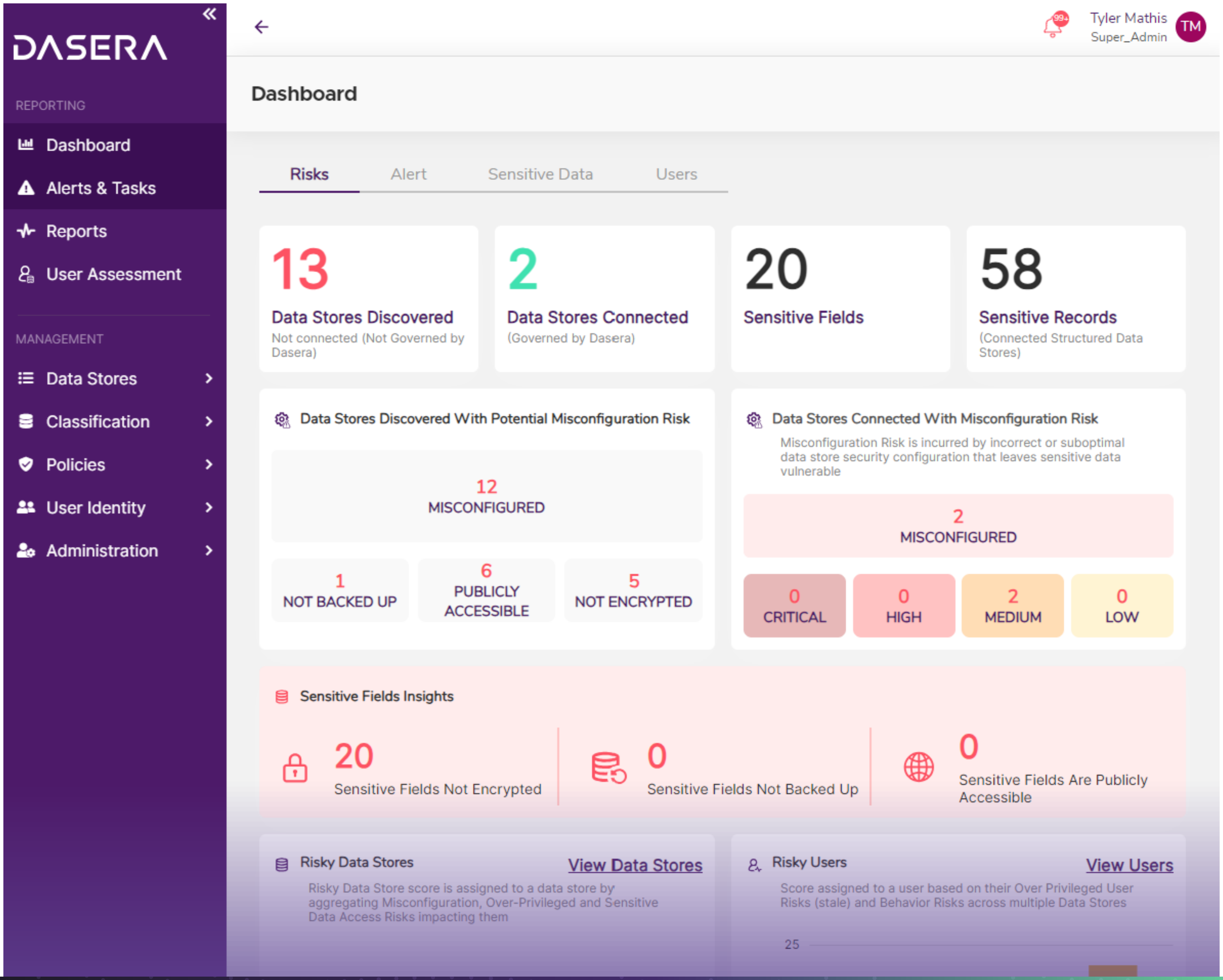
39 Users

Employee/ Username	Email	Department	User Risk Rating	Accessible Sensitive Data Types	Accessible Data Tags
Adrian Modine	amodine@dasera.com	IT	56	Name, Email, Phone Number, Address...	5 Tags
lbradshaw			56	Name, Email, Phone Number, Address...	5 Tags
user/walton			50	Name, Email, Address, IP Address, Cr...	5 Tags

Securing the Future: Empowering Data Protection with Advanced DSPM Capabilities

DSPM has emerged as a critical component of modern data security and a vital tool in the fight against cyber threats. With the rapid growth of sensitive data in cloud environments, organizations must take a practical approach to securing their data and ensuring compliance with data regulations. DSPM provides a three-step process of Find, Flag, and Fix, enabling businesses to gain real-time visibility into their data and respond promptly to potential breaches.

While DSPM offers substantial benefits, it is crucial to recognize its limitations, particularly in monitoring data usage and data in use. To achieve a more comprehensive data security approach, companies must consider advanced platforms like Dasera. By incorporating real-time data usage monitoring and sophisticated query analysis, Dasera addresses the shortcomings of traditional DSPMs, offering a holistic view of data security.



DASERA

REPORTING

- Dashboard
- Alerts & Tasks
- Reports
- User Assessment

MANAGEMENT

- Data Stores
- Classification
- Policies
- User Identity
- Administration

99+ Tyler Mathis Super_Admin TM

Dashboard

Risks | Alert | Sensitive Data | Users

13 Data Stores Discovered
Not connected (Not Governed by Dasera)

2 Data Stores Connected
(Governed by Dasera)

20 Sensitive Fields

58 Sensitive Records
(Connected Structured Data Stores)

Data Stores Discovered With Potential Misconfiguration Risk

12 MISCONFIGURED

1 NOT BACKED UP | 6 PUBLICLY ACCESSIBLE | 5 NOT ENCRYPTED

Data Stores Connected With Misconfiguration Risk

Misconfiguration Risk is incurred by incorrect or suboptimal data store security configuration that leaves sensitive data vulnerable

2 MISCONFIGURED

0 CRITICAL | 0 HIGH | 2 MEDIUM | 0 LOW

Sensitive Fields Insights

20 Sensitive Fields Not Encrypted

0 Sensitive Fields Not Backed Up

0 Sensitive Fields Are Publicly Accessible

Risky Data Stores — View Data Stores

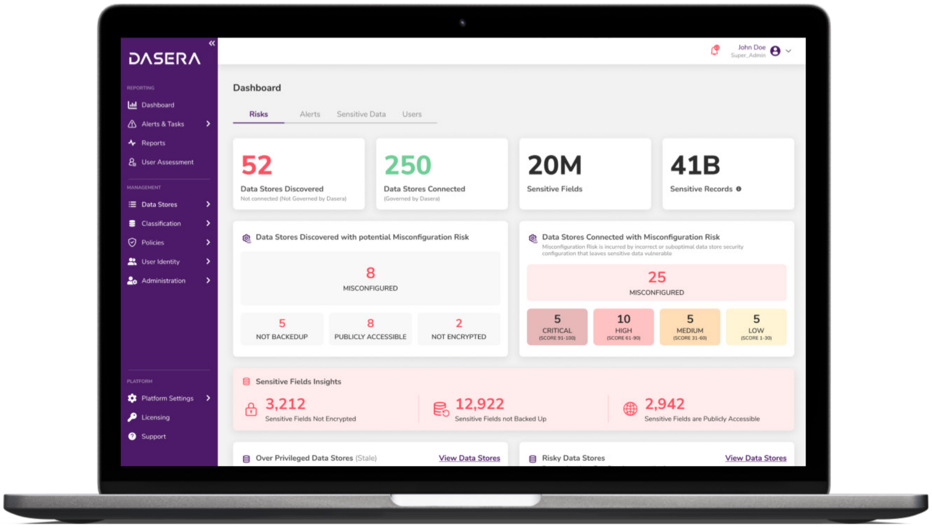
Risky Data Store score is assigned to a data store by aggregating Misconfiguration, Over-Privileged and Sensitive Data Access Risks impacting them

Risky Users — View Users

Score assigned to a user based on their Over Privileged User Risks (stale) and Behavior Risks across multiple Data Stores

The Dasera Advantage

With Dasera's platform, organizations can proactively detect unauthorized access and potential data misuse, minimizing the impact of data breaches. As the world becomes increasingly data-driven, investing in security partnerships with innovative companies like Dasera is essential for safeguarding sensitive information, building customer trust, and ensuring a secure digital future. We can fortify our data environments and stand resilient against evolving cyber threats.



Misconfiguration Risk is incurred by incorrect or suboptimal data store security configuration that leaves sensitive data vulnerable

Interested in learning more?

Visit **Dasera.com** or reach out for a demo of the platform at **Dasera.com/demo**.

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.

DASERA

DATA SECURITY ERA