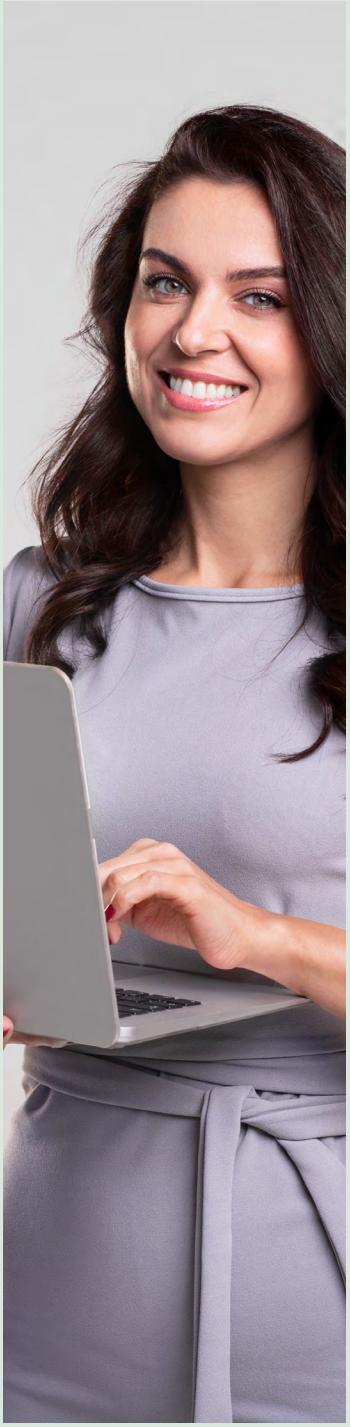
WHITE PAPER



DATA SECURITY POSTURE MANAGEMENT ACROSS CLOUD LANDSCAPE

Abstract

The fast-paced digital transformation has led to a widespread adoption of cloud technologies across the organizations. Cloud technologies have not only helped the organizations with a smooth transition to remote work environments, but also accelerated the speed of evolution with the ever-growing demands of customers. As a result, we have witnessed many small and large companies making a reluctant yet quick migration to the cloud over the past 20 years. However, it is only in recent few years that the organizations have realized the new and complex challenges of cloud. Growing rate of cyber-attacks, data proliferation across multi-cloud environment, and stringent data privacy regulations have further aggravated this problem. A strong security posture requires more than just performing vulnerability assessments, logging and monitoring system events & installing firewalls and anti-malware solutions. It requires in-depth visibility of data – where is the data, what is its purpose and who has access to it? This is where Data Security Posture Management (DSPM) comes into picture. This whitepaper will elaborate the need for Data Security Posture Management (DSPM), how it works and helps in establishing a strong cloud security posture management strategy.

Infosys®
Navigate your next

Overview and industry problem

With the increasing adoption of remote or hybrid work arrangements by organizations, cloud infrastructure has become essential in providing the necessary flexibility and productivity gains to satisfy the needs of employees, customers, and other stakeholders. Nevertheless, the widespread proliferation of data across multi-cloud and hybrid IT architectures has brought about significant data security and privacy risks.

As per Security Magazine article the danger is not merely hypothetical as evidenced by the reported 2,690 instances of ransomware attacks in 2021 92.7% increase from the year 2020. According to IBM Security, the typical cost of a data breach for enterprises was $4.35 million. Therefore, the primary objective of enhancing data security is to prevent data breaches from happening and minimize the risk of sensitive data exposure in the event of an attack.

Organizations face multiple challenges while securing their sensitive data, few of them are listed below:

- Cloud data assets, which comprises more than 50% of cloud deployed resources, are the main targets of cyber-attacks. Yet, there is no cloud-native or third-party security solution that provides visibility into the data residing on cloud workloads. In the absence of such tools, organizations do not have an automated solution to provide them complete visibility of all their data present in cloud.
- With increasing data security, privacy regulations and compliance requirements, organizations are bound to implement adequate security controls to protect data. This problem is further aggravated by the flexibility of data access, transfer, and modification available in modern cloud technologies.

- With most of the data residing outside the company IT premises, Shadow data has become the biggest threat to organizations. Organizations have a lack of visibility as well as control over this data which is being stored or transferred to cloud by users or applications.
- As there is lack of visibility of data, it is challenging for organizations to set up data-centric vulnerability management programs as well as monitoring to identify potential gaps and risks associated with data workloads. This results in poor security controls and increased risk of data exposure.

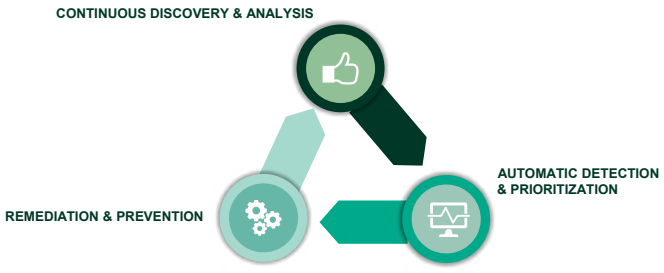
To mitigate these risks, organizations must take a proactive approach by deploying security strategies and solutions that specifically address these concerns. Organizations that neglect to do so and rely on outdated or on-premises security technology may face greater risks of data leakage and deployment complications.

Solution

Data Security Posture Management (DSPM) is an emerging security practice that solves data security concerns by automating data visibility and protection in cloud environment. Gartner defines DSPM as a process that 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."

DSPM focusses on securing the key asset of an organization – Data. It enables them to define their cyber security strategy with a data-centric lens by providing better visibility, control, and governance on data. An effective DSPM framework would be able to address the most critical concerns around data, such as:

- What sensitive data we have?
- Where does this sensitive data reside?
- Who has access to this data and what permissions they have?



- Where is this data being processed and/or transmitted?
- What are the security risks that can lead to data compromise?

Moreover, Data Security Posture Management across cloud landscape aligns seamlessly with information security frameworks and industry benchmarks and best practices to strengthen data security along with IT infrastructure, network, and applications.

Key Features | DSPM

Data Discovery & Classification

- Discovers cloud native structured and unstructured data stores
- Discovers cloud native block storage, such as EBS volumes & PaaS data stores such as Snowflake and Databricks.
- Classify data through automated classifier for PCI,PII,PHI,GDPR,CCPA etc
- Notify security team on discovery of new sensitive data

Access Governance

- Ensures that only authorized users are allowed to access specific data stores or types of data
- Discover issues related to abandoned databases & excessive privileges
- Identification of all users with access to cloud data stores
- Identify all roles & resources with access to those data stores
- Detect external users/roles with access to the data stores

Detect & Remediate Vulnerabilities and Misconfigurations

- Find potential attack paths that could lead to a breach of sensitive data
- Detects vulnerabilities affecting sensitive data, and insecure users with access to sensitive data
- Checks data against industry benchmarks and compliance standards
- Shows relationships across data stores, users, and cloud resources which helps in investigation and remediation

Compliance

- Automate mappings of your data to compliance benchmarks
- Provides coverage heatmap on data compliance gaps, such as misplaced (PII), shadow data, or abandoned data stores with sensitive data
- Dashboard and reports to track and manage data compliance

Data Security Posture Management solutions help address these complex data security challenges by:

- Identifying all the sensitive data in the cloud – from intellectual property to financial to PII/PCI/PHI – across IaaS, PaaS and DBaaS deployments. DSPM performs regular scanning of data to where and how sensitive data is stored, which also provides the basis for policy enforcement and monitoring.
- Classifying sensitive data to prioritize risk management for the most critical data assets. Automatic classification of data helps security teams to implement appropriate security controls and prioritize risk remediation as well as incident response in the context of data.
- Establishing what data is being shared with whom – internal users / groups or external third parties. Once sensitive data has been detected and classified, DSPM helps in enforcing granular access controls, permissions, and secure storage policies.
- Tracking data lineage as it moves across the environment. It ensures organizations can detect potential loopholes and risks, such as storing data in an insecure data center or location or sharing data with unauthorized users.
- Identifying risks associated with data, such as sensitive data not being shared in accordance with corporate security guidelines, access, or activity violations.
- Alerting security analysts upon policy violations or data exposure and providing actionable insights
- Remediating issues as they are happening, such as fixing access control issues and permissions or restricting third parties from further sharing of sensitive data or files.

How does DSPM differ from CSPM?

It is important to understand the differences between the data-centric and the infrastructure-centric solutions for security posture management. Cloud Security Posture Management (CSPM) technologies are designed to safeguard cloud infrastructures by identifying misconfigurations, vulnerabilities, and compliance violations across an organization's cloud infrastructure and alerting security teams to address and rectify them.

While CSPM solutions are highly effective at protecting cloud infrastructure, they lack data context. CSPM do not recognize the significance of the data or the potential risks to the data stored within data repositories. As a result, while a CSPM may identify a critical vulnerability in an S3 storage bucket, it may not be aware of whether the bucket contains sensitive data, the loss of which could have significant implications for the organization. Meanwhile, the CSPM may overlook a less severe vulnerability that could affect data stores containing sensitive financial information such as credit card data.

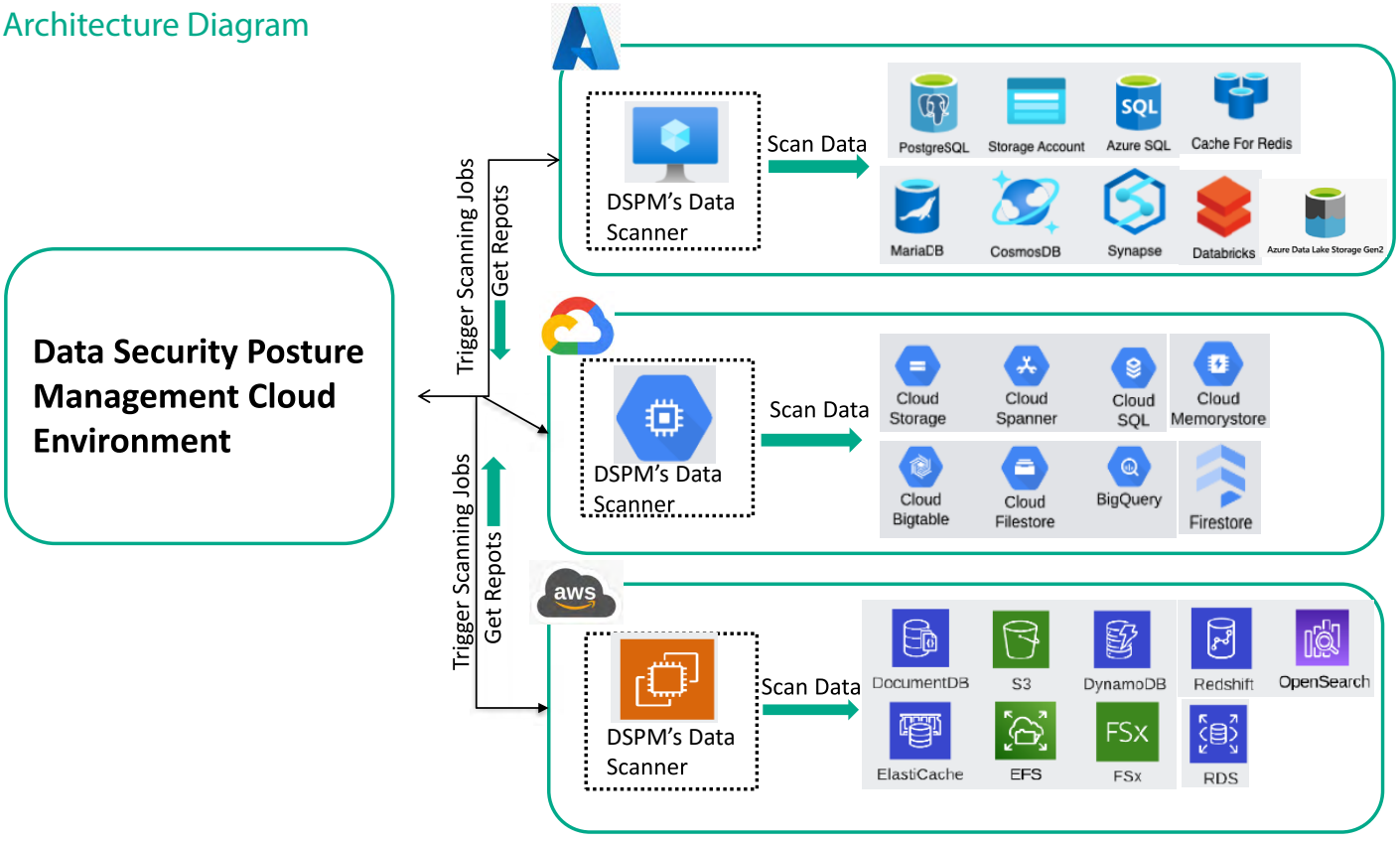
Benefits of DSPM

Embedding DSPM in the cyber security strategy will help organizations implement adequate controls and monitoring around their sensitive data and thereby reduce the risk of data breach.

The right DSPM solution can provide various benefits such as:

- Strong Data Governance: DSPM provides data visibility & context through automated discovery and classification, thereby, helping security teams implement security controls and policy enforcement – where should the data be stored, how should it be stored and who can access the data along with what permissions.
- Continuous Assessment of Cloud security posture in context of data: DSPM continuously assesses cloud environment for any misconfigurations, unauthorized access, excessive permissions, and other vulnerabilities that could lead to data exposure. Thus, helping the security teams identify and fix gaps in a timely manner before it could be exploited.
- Improved Efficiency and Cost Optimization: Through automated monitoring and remediation workflows, DSPM helps in identifying potential risks and prioritize remediation of high-value data assets and hence avoiding costs of a breach.
- Compliance and Customer Trust: DSPM audits the configuration of data assets against data protection laws and regulations (HIPAA, GDPR, CCPA) and hence helps the organizations to comply with the regulatory requirements as well as provides an assurance to the customers that their data is secure.

Architecture Diagram



Best Practices for Data Security Protection Management Implementation:

Define Data Security Objectives:

Security objective outlines the purpose of having a data security strategy in place. It is based on the organization's commitment to secure its data against breach, build customer trust and/or comply with regulatory or compliance requirements. This forms the basis of establishing the scope of DSPM and helps organizations to assess various DSPM solutions that fulfils the defined objectives.

Define Scope for DSPM:

With the understanding of the existing data landscape, organizations should define the scope of DSPM solution. It is dependent on where company's sensitive data is being stored, processed, and used, such as company network, private cloud, public cloud or SaaS applications. Scope determines which type of DSPM solution would be most effective in achieving the security objectives.

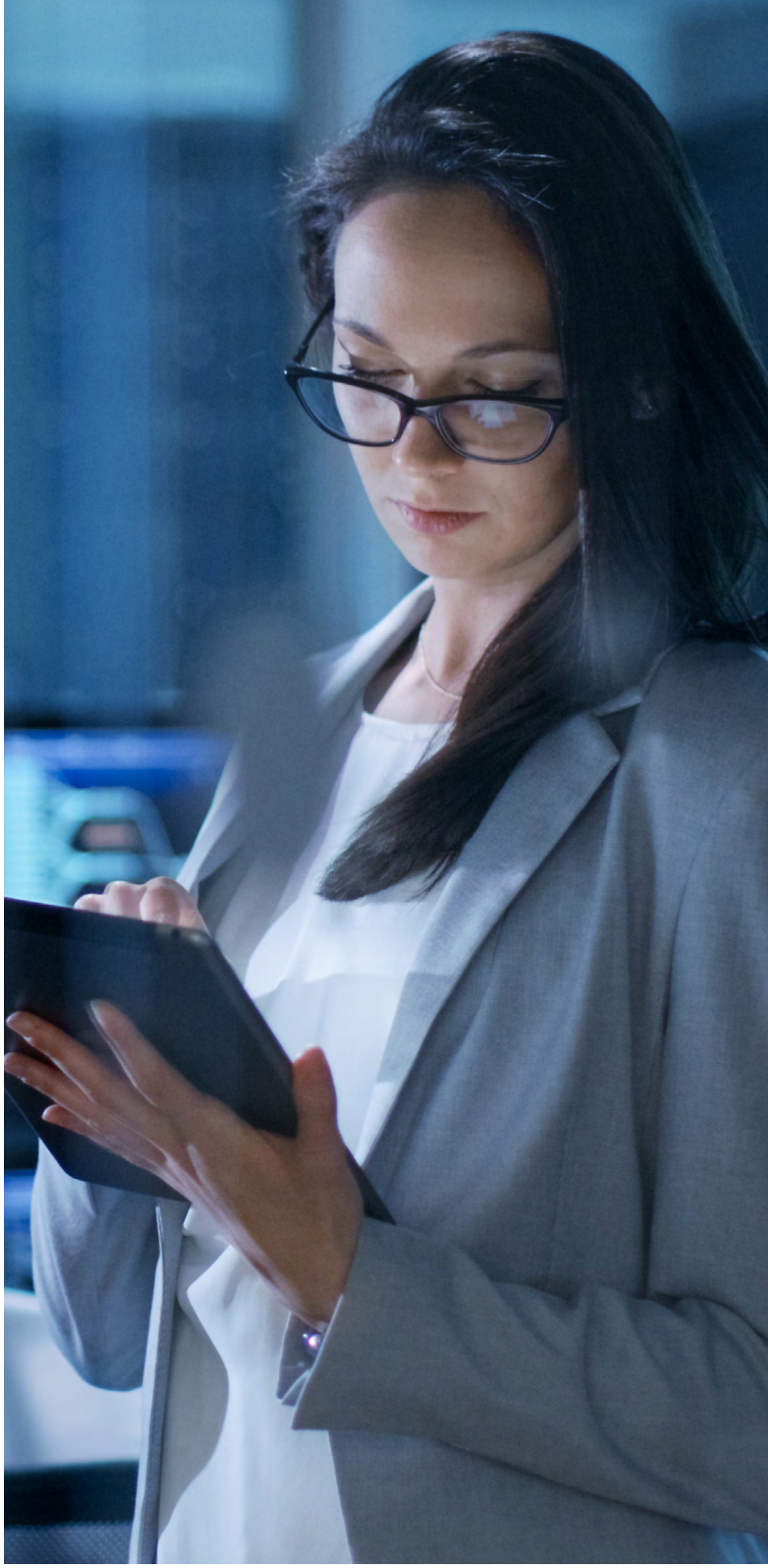
Deploy and Configure DSPM:

Establish processes and security controls to be configured in DSPM solution, such as data discovery, data classification, access control and permissions for data workloads, security compliances and standards for posture management and monitoring through incident detection and response. Once the solution is deployed with initial security policies, it can learn the environment and fine-tune the policies.

Integrate DSPM with existing processes and solutions:

Integrating DSPM with the existing processes and tools provides a holistic approach to data security. DSPM solution is effective when used along with solutions such as:

- Security Information and Event Management (SIEM) solution generates security alerts based on correlation of logs and events across all the devices in the environment. DSPM adds context to these security alerts and helps security team to prioritize response and remediation.
- Data Loss Prevention (DLP) tools can be fine-tuned through DSPM which provides visibility of sensitive data and its movement across the environment.
- Antivirus solutions conducts real-time monitoring of security threats such as virus or malware on the endpoints. Integration with DSPM helps prioritizing remedial actions on critical assets with sensitive information.
- Integration with Identity and Access Management (IAM) tools helps enforce access control and permission policies defined in DSPM for the users who need to access sensitive data.



Continuous Monitoring and Optimization:

Once implemented, DSPM should be continuously fine-tuned and updated with the changing data environments and evolving threats. As new data stores are created and changes happen in data flow, it is essential to perform regular assessments as well as monitoring of network traffic, system logs and user behavior to update security policies and configurations in DSPM.

Conclusion:

As data becomes the new oil for many organizations, there is a need to shift cyber security posture management approach from system-centric to data-centric.

DSPM is an evolving solution to manage data security posture of an organization. It provides insights into where sensitive data resides, who has access to that data and how it is being utilized. It also helps in classifying this data and implementing appropriate controls to restrict unauthorized access or misuse. Additionally, it offers capabilities to monitor data flows and configure alerting mechanism to notify security violations or non-compliance.

Multiple DSPM solutions have emerged in the market which caters to the need of organization's data security. It is important to define the security objectives of the organization and prudently choose the best DSPM solution that fits into their environment with existing tools, technologies, and processes. Security team should be trained to manage and fine-tune the solution with the dynamically changing environment. DSPM should be an on-going effort to improve the security posture of organization and staying ahead of the malicious actors.

References

- https://laminarsecurity.com/blog/data-security-posture-management-dspm-find-and-secure-cloud-data/
- https://www.ibm.com/reports/data-breach
- https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021
- https://www.flowsecurity.com/
- https://cloudsecurityalliance.org/blog/2023/03/31/the-big-guide-to-data-security-posture-management-dspm/
- https://www.zscaler.com/zpedia/what-is-data-security-posture-management

Author

Saurabh Sharma

Saurabh works as a Data Privacy & Protection consultant with Infosys Cyber Innovation Strategy and Excellence team which dwells into next generation cyber security solutions and strategies. He has 13 years of experience in consulting, assessment & implementation of data protection and building data privacy solutions. He has extensive knowledge and experience in infrastructure and cloud security domains as well.

For more information, contact askus@infosys.com

Navigate your next