Zscaler Data Security Posture Management (DSPM) for Amazon Web Services (AWS)

Solution Brief

Overview: Securing Cloud Data in Amazon Web Services (AWS)

Considerations associated with securing vast loads of business data in AWS environments include managing the complexity and scale of data protection, dealing with insider threats, third party and vendor access, supply chain risks, and complying with data regulations. Organizations struggle to inventory, classify, control, and protect critical data assets while securing them from various risks. The complexity is further compounded by the multitude of fragmented data locations, roles, and permissions across different environments. The key challenges of securing data in AWS environments are numerous and involve several factors as below:

Complex environments	Data volume	Targeted, sophisticated attacks	Overprivileged access
82% of breaches involve data stored in the cloud[1]	175 ZB estimated data to be stored in the cloud by 2025[2]	USD 4.88M – The global average cost of a data breach in 2024[3]	80% of organizations have suffered identity-related breaches[4]

Unfortunately, legacy data protection solutions are not designed for dynamic AWS environments. All the while, point DSPM vendors are delivering siloed approaches that fail to integrate seamlessly into existing data protection programs. Organizations need a new, unified approach to securing their data in the AWS environment.

Zscaler solves these data security challenges in AWS environments with an agentless, fully integrated data security posture management (DSPM) solution.

What Is DSPM?

"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 stored or application is." — Gartner

First identified by industry analyst Gartner in its 2022 Hype Cycle for Data Security, DSPM is sometimes referred to as 'data first' security, inverting the protection model embraced by other cybersecurity technologies and practices. Instead of securing the devices, systems, and applications that house, move, or process data, DSPM focuses on protecting the data directly, while still complementing many of the other solutions in an organization's security technology stack.

Specifically, DSPM involves continuous monitoring, assessment, and optimization of security controls to protect sensitive data across multicloud platforms. By automating the identification of sensitive data as well as any potential vulnerabilities, configuration errors, or compliance violations, DSPM ensures that organizations can proactively address the risk of data exposure. In doing so, DSPM helps them strengthen their overall data security posture, minimize the risk of data breaches, and meet regulatory compliance requirements.

1. https://www.informationweek.com/cyber-resilience/data-breaches-just-keep-piling-up
2. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/
3. https://www.ibm.com/reports/data-breach
4. https://www.darkreading.com/cybersecurity-operations/identity-related-breaches-last-12-months

Why DSPM?

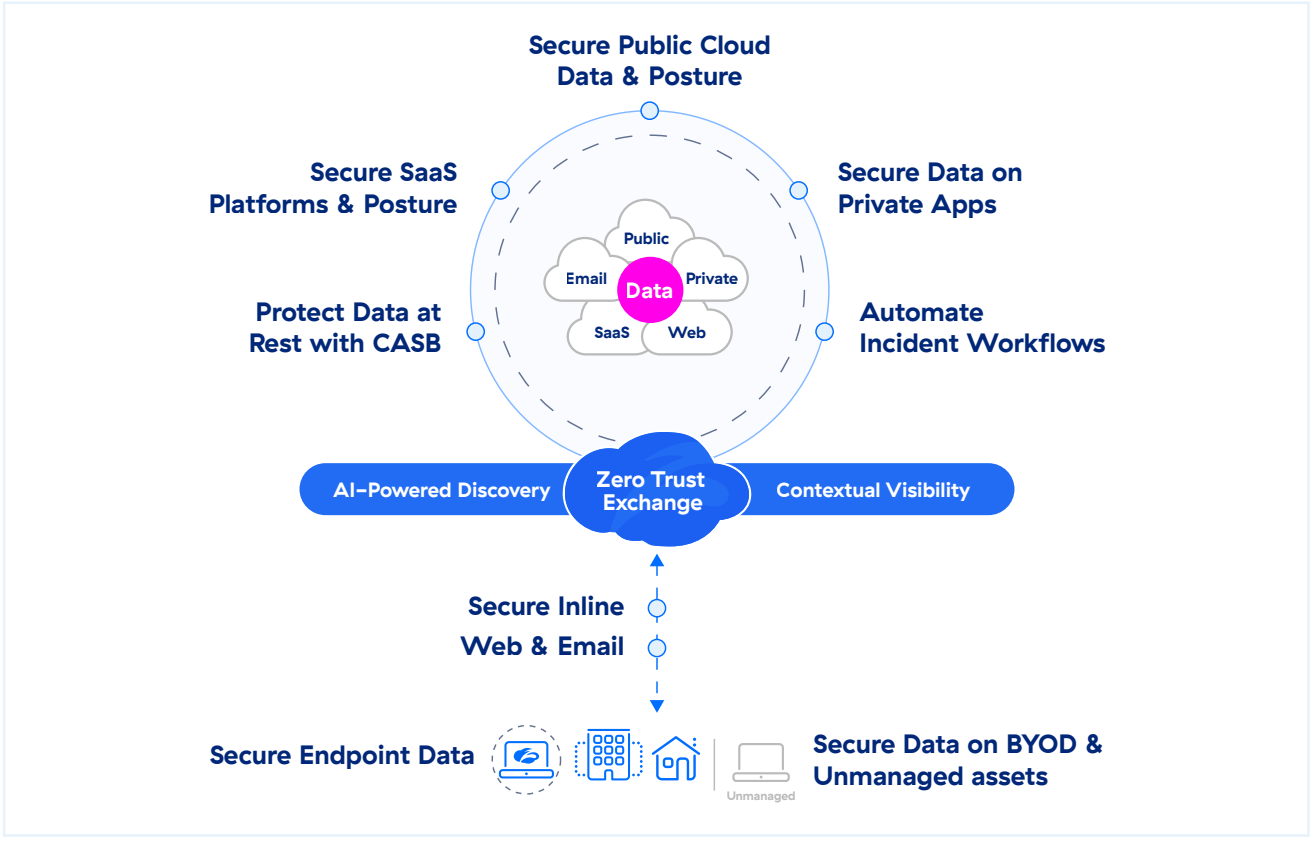
The main focus of DSPM tools is to evaluate and handle the security status of an organization's data environment by finding weaknesses, monitoring security settings, and identifying potential threats to sensitive data. DSPM goes beyond policy alone to look at the actual data itself. By scanning and categorizing data, it helps organizations fully understand where sensitive data is located and how it is being used. It also helps prioritize identified issues and prevents overwhelming alerts that could lead to such issues being overlooked.

Practical DSPM use cases include:

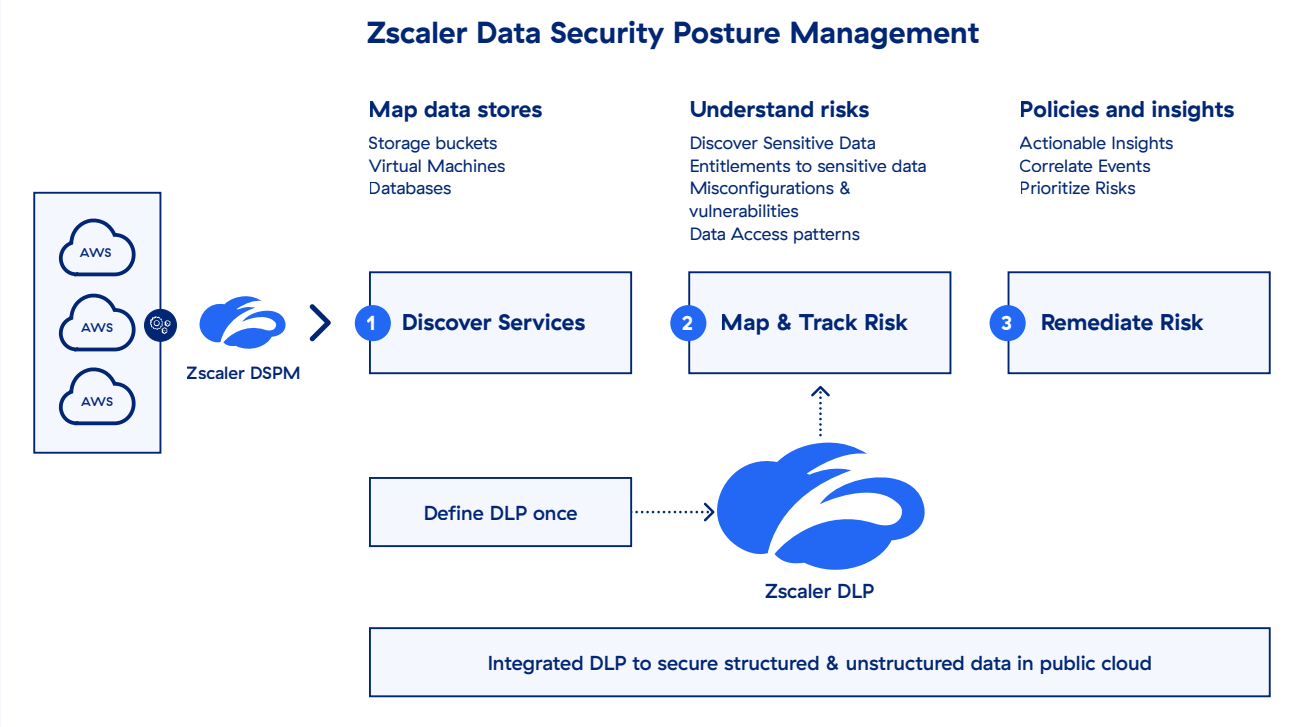
- Discover, classify, and inventory sensitive data, including shadow data
- Analyze hidden risks such as misconfiguration, excessive permissions, vulnerabilities, etc.
- Prioritize risk based on severity and easily fix issues with context–based guided remediation and easy integration with existing security ecosystem

Meet Zscaler Data Security Posture Management (DSPM)

Zscaler AI Data Protection is the world's most comprehensive, fully integrated data protection platform. It secures both structured and unstructured data across web, SaaS–based services, public cloud environments, private applications, email, and endpoints.



As part of the Zscaler platform, Zscaler Data Security Posture Management (DSPM) extends robust, best-in-class security for your data into the AWS environment. It provides granular visibility into sensitive data, classifies and identifies data and access, and contextualizes data exposure and security posture, empowering organizations and security teams to prevent and remediate data breaches at scale.



It uses a single and unified DLP engine to deliver consistent data protection across all channels. By following all users across all locations, and governing data in-use and at-rest, it ensures sensitive data is seamlessly protected and compliance is achieved.

Zscaler DSPM Core Capabilities

Data Discovery, Classification, and Inventory
Traditional scanning methods are expensive and require efforts to yield the desired results. Zscaler DSPM, with minimal access to resources in AWS environments, scans data stores, discovers sensitive data, and accurately classifies data. It offers:

- **Comprehensive data discovery:** DSPM constantly monitors AWS environments to automatically discover new datastores as they are instantiated in ever-changing data environments to save time and eliminate data blind spots.
- **Precise data classification:** DSPM uses AI, ML, predefined DLP engines, and dictionaries for data classification. It offers visibility into what type of sensitive data is stored in AWS data stores, the region, the files containing sensitive data, the severity of risk associated with the sensitive data, etc. It also offers flexibility to organizations to create or replicate the existing policies that are available.

- **Accurate data inventory:** DSPM also creates an accurate map and inventory of data assets, helping security teams locate sensitive data and understand who has access to it and how it is being used.

DSPM provides security teams with greater visibility into data within the AWS infrastructure. This then makes it far easier to manage and improve the data security posture of AWS' environment, which encompasses complex layers of SaaS, PaaS, IaaS, and databases.

Map and Track Data Exposures

AWS services and configurations change frequently that might lead to data exposure. It is essential to fix these security gaps before bad actors can exploit them. DSPM detects publicly exposed resources along with the vulnerabilities or misconfigurations in the different components (network security group, load balancer, virtual network, etc.) that are associated with the data resource. Zscaler helps with:

- **Exposure analysis:** DSPM determines public exposure, misconfigurations, and vulnerabilities for data stores and services.
- **Risk assessment:** DSPM aggregates the overall risk level by combining the impact and likelihood. This Involves categorizing risks into critical, high, medium, or low levels.
- **Risk prioritization:** DSPM helps security teams filter out the noise and prioritize incidents based on risk and severity.
- **Advanced threat correlation:** DSPM leverages advanced threat correlation, threats, risk, and hidden attack path to minimize risk.
- **Adaptive access intelligence:** DSPM provides a granular, risk-based, user-centric view of all access paths to mission-critical data and configurations.

Risk Remediation

DSPM streamlines risk management with context-based guided remediation, enabling security teams to easily fix issues and violations at the source, preventing future disruptions. Capabilities include:

- **Effective investigation and response:** DSPM helps security teams quickly understand potential root causes during investigations of data security events.
- **In-depth guided remediation:** DSPM helps cross-functional teams with automated workflows and step-by-step guidance with complete context to address data security risk and remediate effectively.
- **Faster time-to-security:** DSPM allows to configure custom real-time alerts to keep pace with rapid change to data and its environment, speeding up investigation and response.
- **Seamless integration:** Easily integrate with the existing ITSM, SIEM, or chatops tools and platforms for alerts, remediation, guidance, and workflows.
- **MITRE Att&ck mapping:** Strengthen data security by aligning defenses with known adversary tactics and techniques.

Experience Zscaler DSPM

Request a Demo
See Zscaler DSPM in action with a guided demo.

Request a demo

Download the DSPM Buyer's Guide
Learn about the top 5 requirements to consider while selecting the right DSPM for your organization.

Download now

For more information, visit www.zscaler.com/products-and-solutions/data-security-posture-management-dspm

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com