Zscaler Data Security Posture Management (DSPM)

Solution Brief

Overview: Securing Data in the Cloud-Centric World

The challenges of securing vast amounts of business data in multicloud environments include managing the complexity and scale of data protection; dealing with insider threats, data breaches, third party and vendor access, and supply chain risks; and complying with data regulations. Organizations struggle to inventory, classify, control, and protect critical data assets while securing them from various threats. Compounding this complexity is a multitude of fragmented data locations, roles, and permissions across different environments.

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 were not designed for dynamic multicloud environments. At the same time, point DSPM vendors are delivering siloed approaches that do not integrate seamlessly into existing data protection programs. Organizations need a new, unified approach to securing their cloud data.

Zscaler solves these data security challenges in multicloud 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

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 other solutions in an organization's security 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 enables organizations to proactively address the risk of data exposure. In doing so, DSPM helps them strengthen 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?

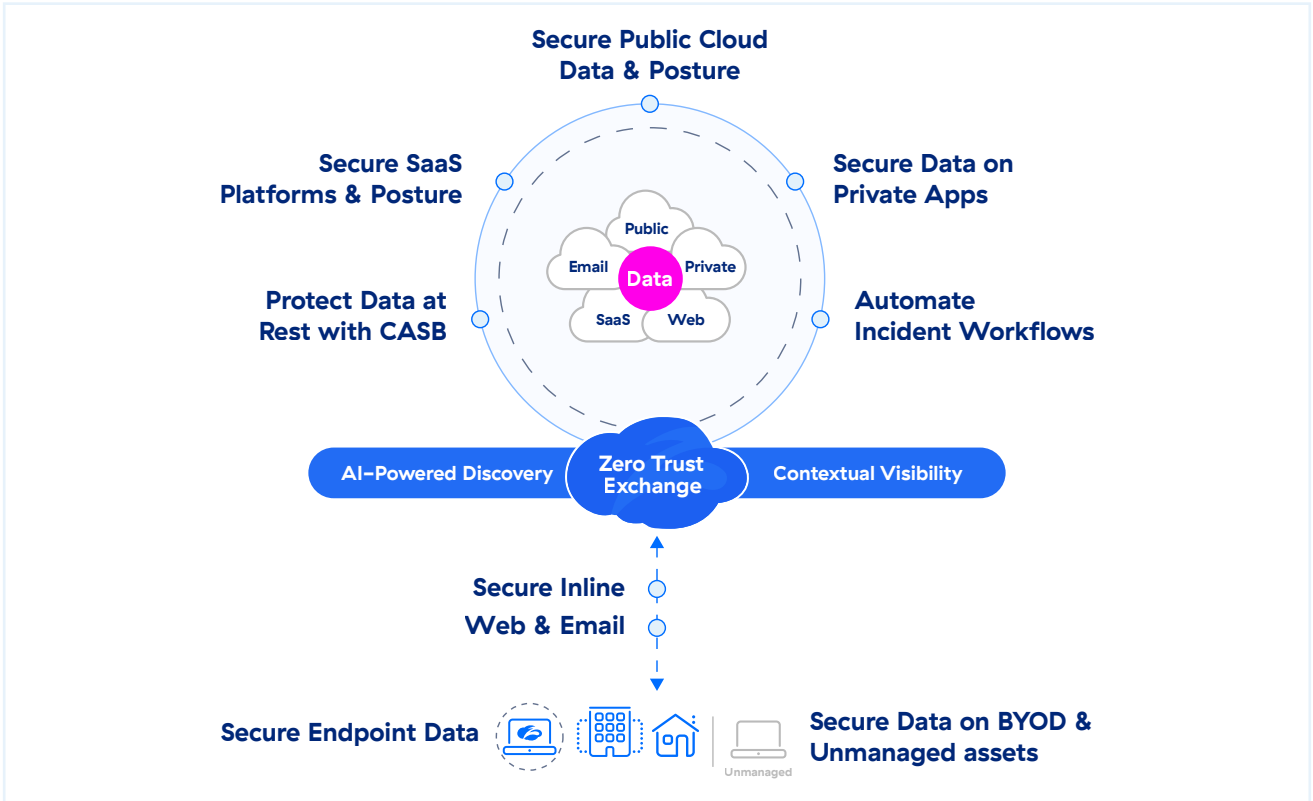
The main focus of DSPM tools is to evaluate and handle the security status of an organization's data environment by finding weaknesses, monitoring security settings, and identifying potential threats to sensitive data. DSPM goes beyond policy alone to look at the actual data itself.

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.

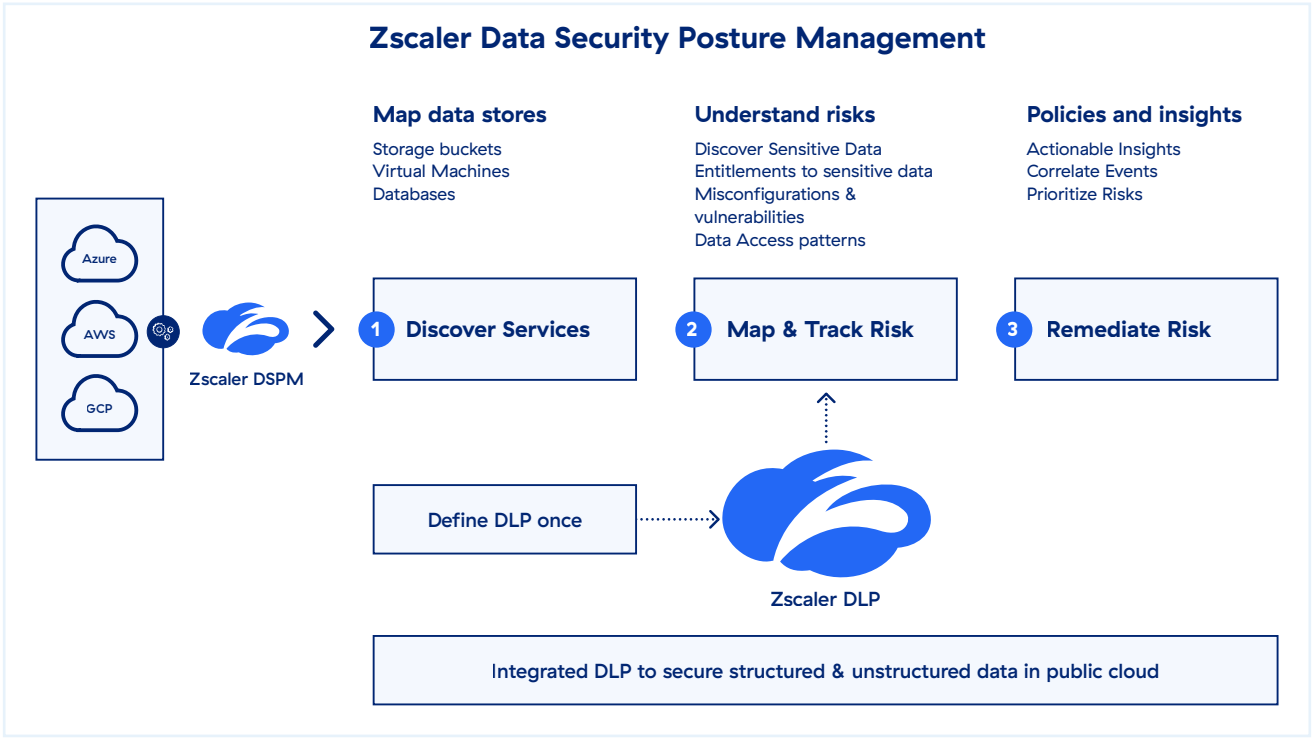
Practical DSPM use cases include detecting security vulnerabilities (such as encryption) in cloud environments, enforcing access policies, and providing alerts and investigation capabilities for incident management.

Meet Zscaler 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 (AWS, Azure, GCP), private applications, email, and endpoints.



As part of the Zscaler platform, Zscaler DSPM extends robust, best–in–class data security into the public cloud. It provides granular visibility into cloud data, classifies and identifies data and access, and contextualizes data exposure and security posture, empowering security teams to prevent and remediate cloud data breaches at scale.



Using a single, unified DLP engine, Zscaler DSPM delivers consistent data protection across all channels. By following all users across all locations, and governing data both 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 significant effort to yield useful results. Zscaler DSPM, with minimal access to resources in cloud environments (AWS, Azure, and GCP), scans data stores, discovers sensitive data, and accurately classifies data. It helps with:

- **Comprehensive data discovery:** Zscaler DSPM constantly monitors cloud 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:** Zscaler DSPM uses predefined DLP engines and dictionaries for data classification. It offers visibility into what type of sensitive data is stored in cloud resources, 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:** Zscaler DSPM 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.

With Zscaler DSPM, security teams gain greater visibility into data within cloud infrastructure. This makes it much easier to manage and improve the data security posture of multicloud environments, encompassing complex layers of SaaS, PaaS, IaaS, and databases.

Map and Track Data Exposures

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

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

Risk Remediation

Zscaler 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** to help security teams quickly understand potential root causes during investigations of data security events.
- **In-depth guided remediation** to help 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**, allowing teams to configure custom real-time alerts to keep pace with rapid change to data and its environment, speeding up investigation and response.
- **Seamless integration** for easy integration with existing ITSM, SIEM, or ChatOps tools and platforms for alerts, remediation, guidance, and workflows.

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 zscaler.com/dp/dspm.

Appendix

Glossary of terms

- Data Security Posture Management (DSPM)
- Cloud Native Application Protection Platform (CNAPP)
- Cloud Security Posture Management (CSPM)
- Cloud Infrastructure Entitlement Management (CIEM)

Further reading

Scan QR code to access DSPM resources

On-demand Sessions

- Keynote: Zenith Live '24 session, Zscaler DSPM: Secure Cloud Data with a Fully Integrated Platform —Learn about Inter&Co's DSPM journey.
- Webinar: 'Why Does DSPM Belong In Your Data Protection Strategy?'

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