# What is DSPM, and why do you need it?

DSPM helps organizations discover, monitor, and reduce the risk associated with sensitive data in their cloud environments. By providing visibility into data assets and ensuring that proper security controls are in place, DSPM can help organizations maintain strong data security posture.

Watch Video

> "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

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

## What leads to data security challenges?

- **Complex environments**
- **Data volume**
- **Targeted, sophisticated attacks**
- **Overprivileged access**
- **Regulatory changes**

## Why do you need DSPM?

**99%**

of organizations store data in multicloud environments ›

### Complete visibility and control over data

Complex cloud environments, escalating volumes of data, and disparate tools lead to inconsistent visibility and control over sensitive data, complicating data discovery and security.

DSPM scans cloud data repositories, discovers and classifies sensitive data, and creates a map and inventory of data assets to help organizations understand where sensitive data is, who is accessing it, and where it's going.

### Continuous data risk assessment

Sophisticated targeted attacks that exploit vulnerabilities in data security measures pose significant risks to sensitive data. They can lead to data breaches, financial loss, and a severely damaged business reputation.

DSPM powers continuous monitoring and risk management with AI/ML and advanced threat correlation to secure expanding attack surfaces and data. By decoding weak signals, analyzing attack patterns, and uncovering hidden risk, DSPM accelerates incident response to help organizations effectively and accurately secure structured, unstructured, and shadow data.

**$4.45M**

global average cost of a data breach—a 10% year-over-year increase ›

**$1.94B**

in noncompliance fines issued—a 14% year-over-year increase ›

### Continuous regulatory compliance

Evolving data security regulations and standards like GDPR, CCPA, HIPAA, and SOC 2 challenge organizations to strike the right balance between compliance and cloud data security.

By enforcing policies based on relevant data protection laws and industry standards, DSPM helps organizations address compliance and cloud data security concerns to reduce their risk of costly fines or legal issues.

Learn More

### Risk prioritization and remediation

Cloud services and configurations change frequently, and it's essential to fix security gaps before bad actors can exploit them.

DSPM solutions aggregate security data and prioritize risk based on severity, coupled with step-by-step remediation guidance and configurable, near-real-time alerts and notifications. Putting risk in full context enables security teams to focus on what matters most to resolve potential risks or threats in progress.

**285DAYS**

to detect and contain a data breach

**145HRS.**

avg. to resolve a cloud security alert (~6 days)

**$1.02M**

avg. savings if a breach is contained within 200 days ›

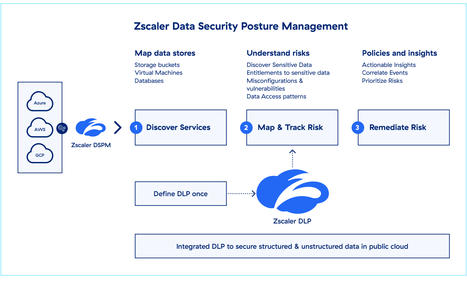
### Automated security workflows

Security teams need to focus on high-value priorities while helping avoid the costs of a breach. Traditional security tools create alerts without accounting for risk priority, increasing alert fatigue and the risk of more breaches.

DSPM leverages AI, ML, and advanced threat correlation capabilities to aggregate security data and effortlessly prioritize risk remediation that enables security teams to focus on what matters most. DSPM can be integrated with other enterprise security tools to improve data security posture in particular as well as threat detection, prevention, and response capabilities in general, increasing operational efficiency.

## How Zscaler DSPM can help

Zscaler DSPM extends best-in-class security for data in the public cloud. It provides granular visibility into cloud data, classifies and identifies data and access, and contextualizes data exposure and security posture, empowering organizations to prevent and remediate cloud data breaches at scale.




## Learn more about Zscaler DSPM

Visit our website | Download DSPM Guide | Schedule a data risk assessment | Talk to an expert

Experience your world, secured.


Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408 533 0288
www.zscaler.com