Protect Cloud Data and Stop Breaches with Zscaler DSPM

Define once, apply everywhere with the world's most comprehensive, fully integrated data protection platform

Cloud data is the new target

82%

82% of data breaches have involved data stored in cloud environments

227

The average time to identify a data breach is 227 days

4.45M

The global average cost of a data breach is $4.45M

"STATE OF DATA GOVERNANCE AND EMPOWERMENT REPORT" ESG, 2022
"COST OF A DATA BREACH 2023 REPORT" IBM SECURITY - 2023

> "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."
>
> – 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.

Challenges of securing data in the cloud–centric world

Multicloud environments are intrinsically complex and resource–intensive. The sheer amount of data being pushed to the cloud combined with a high number of users accessing different cloud platforms, accounts, and services makes it difficult for organizations to understand and control what's happening in the cloud.

Security professionals face four main challenges when it comes to securing datain a multicloud environment:

01 THE CLOUD IS AGILE

Modern, agile cloud technology and services offer developers the flexibility to collaborate and share data with ease, which can result in losses of visibility and control over sensitive data.

02 THE CLOUD IS COMPLEX

It is estimated that the total amount of cloud data will increase from 33ZB today to 175ZB by 2025. With a data sprawl in multiple cloud platforms, accounts, and services, organizations struggle to understand which cloud services, regions, and accounts are consuming and storing data.

03 EXCESSIVE ENTITLEMENTS

On top of the challenges of discovering and classifying data, security teams also struggle to understand data access and simultaneously achieve and maintain compliance with data sovereignty requirements, rresulting in massive security gaps.

04 LACK OF DATA CONTEXT

Alert overload surrounding misconfigurations and vulnerabilities without prioritization based on context of sensitive data lead to greater resource fatigue and security breaches offer developers the flexibility to collaborate and share data with ease, which can result in losses of visibility and control over sensitive data.

What's driving the need for comprehensive DSPM?

Unfortunately, legacy data protection solutions have proven to not be designed for dynamic multicloud environments. All the while, point DSPM vendors are delivering siloed approaches that fail to seamlessly integrate into existing data protection programs. It's clear that organizations need a new, unified approach to securing their cloud data.

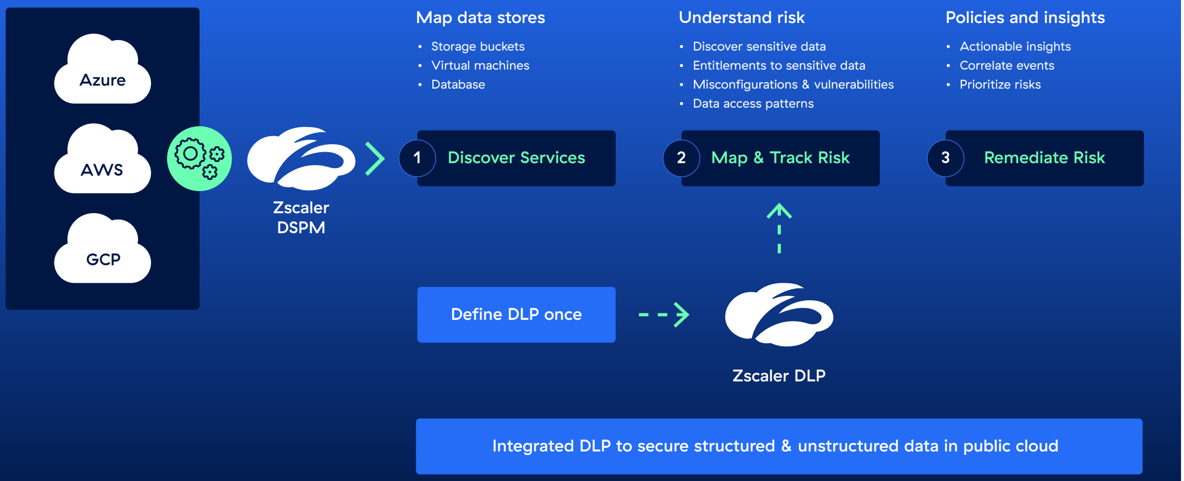
Meet Zscaler Data Security Posture Management (DSPM)

The Zscaler AI Data Protection is the world's most comprehensive fully integrated data protection platform that 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 Data Security Posture Management (DSPM) extends robust, best–in–class security for your data 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 organizations andsecurity teams to prevent and remediate cloud 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 DATA SECURITY POSTURE MANAGEMENT



Azure

AWS

GCP

Zscaler DSPM

Map data stores
- Storage buckets
- Virtual machines
- Database

Understand risk
- Discover sensitive data
- Entitlements to sensitive data
- Misconfigurations & vulnerabilities
- Data access patterns

Policies and insights
- Actionable insights
- Correlate events
- Prioritize risks

1 Discover Services

2 Map & Track Risk

3 Remediate Risk

Define DLP once

Zscaler DLP

Integrated DLP to secure structured & unstructured data in public cloud

Why Zscaler DSPM?

01 A UNIFIED DATA SECURITY PLATFORM

Zscaler DSPM seamlessly integrates with the Zscaler AI Data Protection platform, purpose-built around a centralized DLP engine that allows security teams to get best-in-class data security for web, SaaS, on-prem applications, endpoints, BYOD devices, and public cloud.

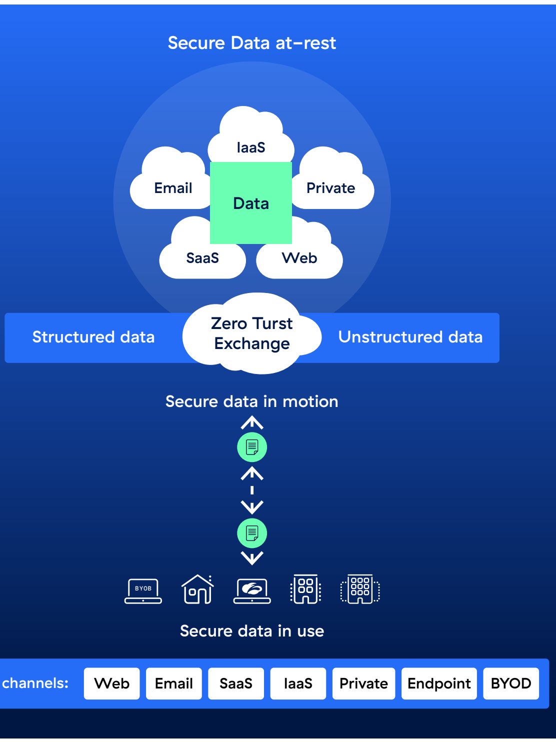
02 AI AUTO DATA DISCOVERY

Our agentless approach automatically discovers, classifies, and identifies data without any configuration while drastically accelerating deployment and operations.

03 EMPOWERED TEAMS AND SIMPLIFIED OPERATIONS

Significantly reduce alert overloads with powerful threat correlation that uncover hidden risk and critical attack paths, allowing your team to focus on the risks that matters most.

POWERFUL CLASSIFICATION: ALL DATA TYPES, LOCATIONS & CHANNELS



Secure Data at-rest

IaaS

Email

Data

Private

SaaS

Web

Structured data

Zero Turst Exchange

Unstructured data

Secure data in motion

Secure data in use

All channels: Web | Email | SaaS | IaaS | Private | Endpoint | BYOD

DSPM Use Cases

FEATURE	ADVANTAGE	BENEFITS
Discover and classify data	Scan and discover sensitive data across various cloud platforms and services in real-time or near-real-time. Accurately categorize, label, and inventory sensitive data based on predefined or custom policies. Get precise, AI-based data classification backed up Zscaler platform that monitors billions of transactions daily.	Gain exclusive visibility into cloud data sprawl anddiscover sensitive data—even where you didn't know you had it.
Map and track exposure	Get a unified view of security, inventory, and compliance for sensitive data in your multicloud environmentGet a granular, risk-based, user-centric view over all access paths to mission critical data assets and its configuration. Analyze hidden risk such as misconfiguration, excessive permissions, vulnerabilities.	Understand the data blast radius of compromised data assets, access, hidden attack paths, and sophisticated threats underway.
Remediate risk	Prioritize risk based on severity. Easily fix issues and violations at the source with context-based guided remediation.	Minimize the risk of data exposure and breaches.
Maintain a consistent posture	Enforce consistent, best-in-class data security everywhere, from endpoint, email, SaaS, public cloud, etc.	Improve overall security posture and outpace threats.
Maintain continuous compliance	Continuously map posture against regulatory benchmarks to identify and remediate compliance violations. Leverage a comprehensive compliance dashboard that simplifies security collaboration between cross-functional teams.	Control violations, simplify audits, and prevent financial and reputational loss.
Integrate workflows	Seamlessly integrate with your existing security ecosystem, third-party services, native tools for risk prioritization, and team collaboration applications.	Minimize the cost and complexity of securing sensitive data.

Zscaler DSPM key components

Data discover	Discovers structured and unstructured data stores	Included in DSPM SKU
Data classification	Automatically detects and classifies sensitive data with out-of-box detection and custom rules	Included in DSPM SKU
Data access control	Maps and tracks access to data resources	Included in DSPM SKU
Risk assessment	Detects and prioritizes risk based on severity and impact using AI, ML, and advanced threat correlation	Included in DSPM SKU
Risk remediation	Offers step-by-step guided remediation with complete context	Included in DSPM SKU
Compliance management	Automatically maps data security posture against industry benchmarks and compliance standards such as GDPR*, CIS, NIST, and PCI DSS*	Included in DSPM SKU

*PRODUCT ROADMAP CAPABILITIES

Experience Zscaler DPSM

Schedule a demo

Experience the power of Zscaler DSPM platform with a guided demo.

REQUEST A DEMO

Watch the launch event

Explore how DSPM eliminates complexity and delivers better data protection against today's sophisticated attacks and threats, allowing security teams to maximize efficiency.

WATCH THE LAUNCH EVENT

For more information, visit:
www.zscaler.com/dspm

zscaler™