zscaler

5 Steps to Successful DSPM Implementation

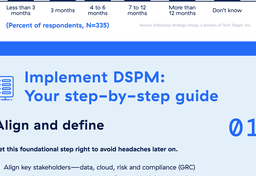
Data Security Posture Management (DSPM) solutions continuously monitor and assess an organization's data security controls across all infrastructure, including on-premises data centers and public cloud environments. While DSPM tools are typically faster to deploy compared to other security technologies, successful implementation requires thoughtful alignment across people, processes, and technology.

By following best practices, security teams can streamline the deployment process, reduce complexity, and ensure that DSPM becomes a cornerstone of their data protection strategy.

of organizations report they are currently using or plan to deploy DSPM.[1]

Data Breach Prevention is a top driver (20%) among organizations deploying DSPM.[2]

The average DSPM deployment time is 4 to 6 months.[3]



Implement DSPM: Your step-by-step guide

Align and define 01

Get this foundational step right to avoid headaches later on.

- Align key stakeholders—data, cloud, risk and compliance (GRC) and security teams—on goals, benefits, and individual roles in the DSPM initiative.
- Clearly define sensitive data, establish data classification standards, and establish success metrics.
- Secure executive buy-in by showing DSPM's role in risk mitigation, compliance, and business support to guarantee resources and prioritization.

Know your data 02

You can't protect what you can't see.

DSPM discovers and classifies sensitive data—including shadow data—across cloud, SaaS, on-prem, IaaS, and PaaS environments. This gives you a complete, real-time picture of your data landscape for smarter security decisions.

Why it matters:

- Accurate classification = faster deployment
- AI-powered classification provide granular, out-of-the-box results
- Custom policies align with your data sensitivity and business value
- Tuning time is nearly zero when you're already using trusted classification (e.g., Web DLP)

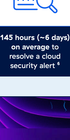
of security professionals are concerned about shadow data.[3]

of organizations have unstructured data.[4]

Streamline risk management 03

Cloud environments are dynamic, and with constant changes in services and configurations, the risk of data exposure is high. DSPM leverages AI and ML to deliver a granular, risk-based view of access paths to mission-critical data. It detects and flags exposed resources, vulnerabilities, and misconfigurations, then aggregates risk levels across your environment.

By prioritizing incidents based on likelihood and impact, DSPM helps teams focus on what matters most. With guided, context-aware remediation, security and cross-functional teams can quickly fix issues at the source, minimizing disruption and reducing long-term risk.



of data breaches involve a non-malicious human element, such as a social engineering attack or an error.[4]

Train teams and define ownership 04

Without clear roles and rule awareness, DSPM can fall short, no matter how good the tech is.

- Assign specific ownership for data security policies and provide thorough training to all relevant teams.
- Assign data security ownership, train teams, and implement structured governance to maintain order and ensure long-term success.

of data breaches in 2024 were tied to human error.[4]

of teams faced a security breach resulting from manual compliance practices.[4]

Stay compliant and proactive 05

Ongoing vigilance is the best way to ensure lasting data security and the continued success of your DSPM deployment.

- Set up real-time alerts to keep pace with rapid changes to data and its environment, speeding up investigation and response.
- DSPM ensures compliance with evolving data security industry regulations (e.g., PCI DSS, GDPR, HIPAA). Security teams can leverage DSPM to automate compliance monitoring, audits, and reporting.

Deploy DSPM with confidence

There's a critical difference between simply installing—and effectively implementing—a DSPM solution. Every organization is different, and the order and exact elements of the above steps will vary depending on your organization. Given that DSPM touches on multiple organizational functions within the enterprise including security, IT, and data governance, it's essential to start with clear objectives, a strong project plan, and the right stakeholder alignment. With the right foundation, you can accelerate deployment and maximize your success. Ready to deploy DSPM with confidence? Learn how Zscaler can accelerate your journey here.

Schedule a demo

Watch the webinar

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 is the company's cloud-native platform that 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, Zscaler's SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. It powers all four categories of Zscaler services, including Zscaler Internet Access, which secures connections to the internet and SaaS applications and protects against cyberthreats; Zscaler Private Access, which provides zero trust access to internal applications in the cloud and data center without a VPN; Zscaler Cloud Protection, which secures workloads using microsegmentation and by identifying cloud misconfigurations; and Zscaler Digital Experience, which provides end-to-end monitoring and troubleshooting for users' digital experience performance issues. Zscaler has been a Leader in the Gartner Magic Quadrant for Secure Web Gateways every year since 2011 and was 2020's only Leader.

With more than 10 years of experience developing, operating, and scaling the cloud, Zscaler serves thousands of enterprise customers around the world, including 500 of the Forbes Global 2000 organizations. In addition to protecting customers from damaging threats, such as ransomware and data exfiltration, it helps them slash costs, reduce complexity, and improve the user experience by eliminating stacks of latency-creating gateway appliances.

Zscaler was founded in 2007 with a mission to make the cloud a safe place to do business and a more enjoyable experience for enterprise users. Zscaler's purpose-built security platform puts a company's defenses and controls where the connections occur—the internet—so that every connection is fast and secure, no matter how or where users connect or where their applications and workloads reside.

Vision statement

Zscaler exists to create a world in which the exchange of information is always secure and seamless.

Mission statement

To anticipate, secure, and simplify the experience of doing business, transforming today and tomorrow.

[1] Data Resilience Emerges: The Collision of Data Discovery, Protection, Security, and Governance, Enterprise Strategy Group, Feb 2024.

[2] Streamlining Data Security Posture Management Implementations, Enterprise Strategy Group, Sept. 2024

[3] Gartner Innovation Insights: Data Security Posture Management, Gartner, March 2023

[4] 2024 Data Breach Investigations Report, Verizon Business, Verizon

[5] 85% of Data Breaches Tied to Human Error in 2024, Infosecurity Magazine, March 2025.

[6] Drata's 2023 Compliance Trends Report, Drata

[7] GDPR Fines and Data Breach Survey, DLA Piper, January 2024

[8] Cost of a Data Breach Report 2024, IBM.

© 2025 Zscaler, Inc. All rights reserved.