The CISO's Guide to Future-Proof Data Security with AI-powered DSPM

2025

EBOOK

zscaler™

Table of Contents

Navigating Through the Modern Data Security Landscape

The exponential growth and dispersion of data across multiple platforms have increased complexity, cost and risks for many organizations. Security leaders now face significant challenges in deeply understanding and controlling their critical data. Compounding this complexity is the rapid adoption of AI which further scatters data, leaving organizations more vulnerable to data and compliance risks.

To effectively mitigate security risks and ensure robust compliance, data security teams require innovative tools that offer real-time, comprehensive understanding of their entire data universe. Data Security Posture Management (DSPM) has emerged as the definitive modern approach, empowering data security leaders to achieve this continuous visibility and understanding using AI and automation.

This essential ebook dives into the transformative potential of DSPM, empowering security leaders and their teams to proactively safeguard sensitive data. Tailored specifically for senior security and risk professionals, it provides actionable insights to navigate the intricacies of the modern data security landscape. As your comprehensive guide to elevating organizational data security posture, this resource explores critical trends, addresses pressing challenges, and unveils innovative strategies, ultimately highlighting the indispensable role of DSPM in securing your data assets in the dynamic AI era.

The CISO's Imperative: Mastering Data Security in the AI Era

For Chief Information Security Officers (CISOs), the rapid adoption of AI and cloud technologies presents a profound dilemma. While offering unprecedented opportunities for cost savings, enhanced business outcomes, and remarkable productivity gains, this digital transformation simultaneously introduces a complex landscape of data security challenges.

The Exploding Data Landscape

The heart of this challenge lies in the explosion of enterprise data. Valuable and sensitive information is no longer confined; it's increasingly fragmented and spread across diverse environments: AI ecosystems, SaaS, PaaS, multicloud deployments, hybrid cloud architectures, and traditional on-premise infrastructure. This proliferation is staggering: IDC forecasts data growth at a compound annual rate of 21.2%, soaring to over 221,000 exabytes by 2026.

Navigating Complexity and Risk

This creates immense complexity for CISOs, who must now manage data security across an ever-expanding and ephemeral data environment. Data is constantly being created, shared, and stored across hundreds of diverse systems and applications throughout the enterprise, making comprehensive data protection incredibly difficult.

Key Data Security Risks in the AI Age:

- **Vulnerability and Compliance Risks:** Dispersed and fragmented data significantly heightens the risk of data breaches and regulatory non-compliance. Ensuring adherence to evolving data governance and privacy regulations (like GDPR, CCPA, etc.) becomes a monumental task.
- **The Menace of ROT Data:** The unchecked proliferation of shadow data (unknown or unauthorized data copies) and abandoned data (stale or forgotten data) creates critical vulnerabilities. These often lead to significant security oversights and expand the attack surface exponentially.
- **Generative AI (GenAI) & LLM Security Challenges:** The rise of generative AI and Large Language Models (LLMs) introduces a new wave of highly specialized risks. These include Shadow AI, data spillage (unintentional exposure of sensitive information), entitlement issues within AI systems, and novel avenues for regulatory infractions. Vigilant AI security and LLM data governance are paramount.

Addressing these multifaceted data security challenges requires a strategic and proactive approach from CISOs, focusing on robust data governance, advanced data protection solutions, and comprehensive AI security frameworks to safeguard sensitive information in this dynamic era.

Risk of Losing Valuable Data

With an ever-increasing cascade of targeted attacks and a dynamic regulatory landscape, it has become crucial for CISOs to prioritize the security of these environments. About 44% of businesses experienced a data breach in their cloud environment in the last 12 months.[1] A data breach can have serious consequences, including data loss, reputation damage, and financial losses. As the threat landscape for AI and cloud-related attacks becomes more treacherous, the CISO role becomes more critical.

To handle these risks and ensure adherence to

1. Infosecurity Magazine, **Cloud Breaches Impact Nearly Half of Organizations**, June 25, 2024.
2. **IBM's Cost of a Data Breach Report 2025**

US$4.44M

The global average cost of a data breach in 2025[2]

regulations, security leaders must thoroughly comprehend their data environments. Often, however, the volume, variety, and velocity of data make it challenging to secure. Leaders frequently lack answers to these questions:

- Where is the data?
- Which data stores contain valuable or sensitive data?
- Who, what or which AI tools have access to those stores?
- How is the data accessed/accessible or shared with AI tools?
- How valuable is the data?
- How is the data handled and what is the impact on compliance posture?

Beyond Limits: Why Traditional Data Security Fails in the AI Era

The landscape of data security has fundamentally shifted. For many CISOs and their teams, the conventional response to escalating threats has been to accumulate a sprawling array of disparate security tools. However, these traditional data security tools are proving increasingly inadequate, failing to provide the crucial insights and protections truly needed in today's dynamic environment.

The Unmet Challenges of AI Security

A significant blind spot for legacy solutions lies in their inability to address the unique behaviors, novel failure modes, and specialized data governance requirements of emerging technologies. Specifically, they fall short when it comes to safeguarding LLM, generative AI agents, and other foundation models. These new AI risks demand a fundamentally different approach.

The Imperative for a New Security Paradigm

This emerging threat landscape necessitates not just new solutions, but a holistic and integrated approach to data governance and security in the AI era. We're talking about a paradigm shift where AI security isn't an afterthought, but a core component of your overall cybersecurity strategy.

Optimizing Investments Amidst Tighter Budgets

Compounding these challenges are increasingly tighter security budgets, forcing security leaders to critically evaluate and optimize investments. The focus is shifting decisively towards reducing operational complexity and minimizing costs, while simultaneously enhancing cybersecurity defenses and closing critical security gaps. Paradoxically, this strategic investment often includes leveraging sophisticated AI-driven security solutions themselves. These advanced tools aren't just a part of the problem; they are powerful enablers for enhanced visibility, accelerated risk detection, and more efficient incident response, ultimately strengthening your entire security posture against the threats of the AI age.

97%

of organizations that reported an AI-related breach lacked proper AI access controls[3]

3. IBM's Cost of a Data Breach Report 2025

Embracing DSPM: The Modern Imperative for AI Data Security

In the face of unprecedented AI risks and the acknowledged limitations of traditional cybersecurity tools, a truly modern approach to data security isn't just beneficial—it's essential. This is where Data Security Posture Management (DSPM) emerges as a pivotal, indispensable solution.

DSPM offers the requisite context and automation to adeptly navigate the intricacies of modern data landscapes. By embracing a forward-thinking methodology, CISOs can more proactively understand their data, ensure adherence to regulations, and reduce the risks associated with using AI.

4. Ibid.

US$1.9M

The average savings for organizations that use security AI and automation extensively[4]

How CISOs Can Improve Data Security Posture Using Integrated DSPM

Here are some of the ways CISOs can effectively utilize AI, ML and risk correlation to improve data security posture:

Address Shadow AI, Data and Abandoned Data Concerns

Shadow Data

Shadow data and abandoned data present substantial security risks, as they frequently operate beyond the scope of IT security protocols and data governance frameworks. Per IBM, 35% of data breaches involved shadow data, and breaches involving shadow data led to a 16% higher cost on average. Moreover, breaches involving shadow data took 26.2% longer to identify and 20.2% longer to contain[5]. Shadow data may be found in unstructured files, structured databases, cloud storage, or on personal devices without appropriate oversight, while abandoned data, without life cycle management, can become a liability.

DSPM solutions harness AI to perpetually discover data stores, enhancing the overall visibility of the data landscape. AI can help catalog dark and shadow data, increasing data visibility. It also alerts security teams about potential risks and minimizes breach risks. It can monitor for abnormalities in data access, patterns, detect anomalies, and predict potential security breaches.

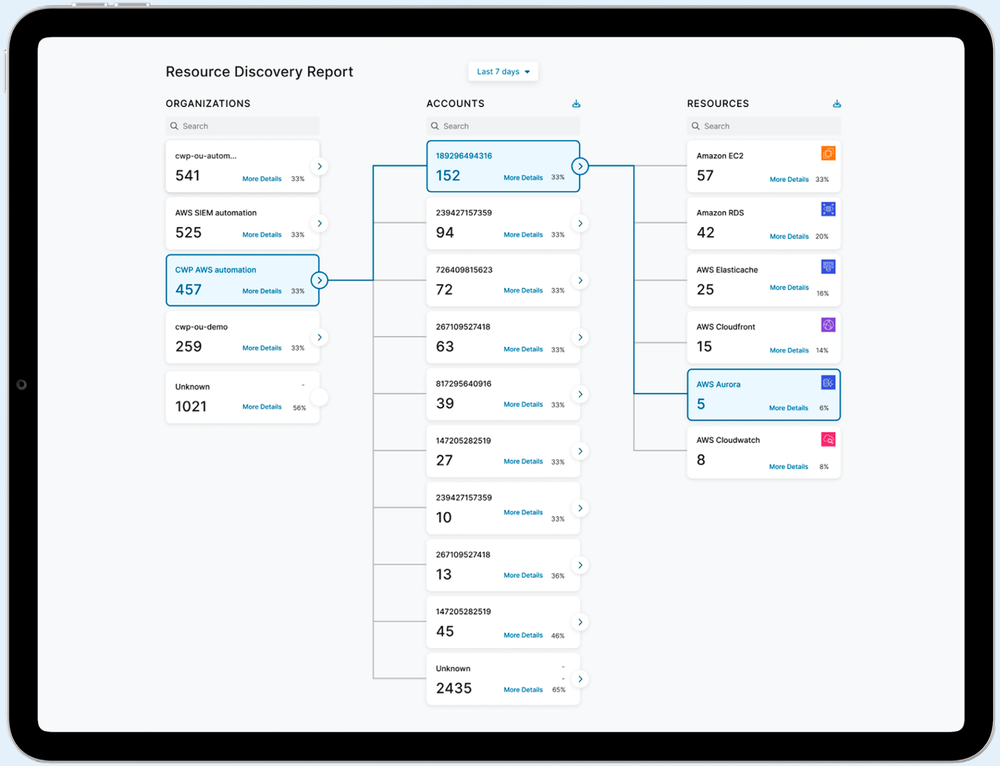
Shadow AI

Shadow AI, like shadow IT, mainly refers to use of unauthorized AI tools to interact with enterprise sensitive data that can have far-reaching consequences for data security and compliance. As these AI tools become more accessible and productive, employees are adopting them without IT oversight. While it may seem harmless, it can create cascading risks that traditional security frameworks can't address by simply banning AI tools.

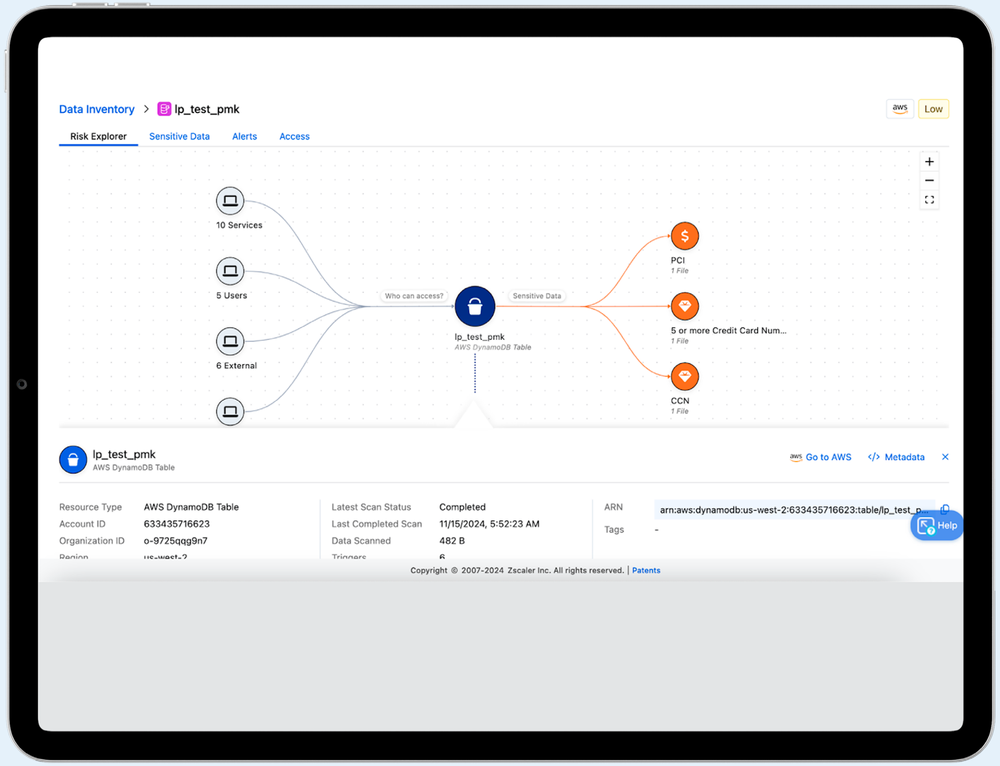
With DSPM organizations can reap the benefits of AI. Rather than blocking or banning AI tools, organizations can manage shadow AI risks with DSPM while leveraging AI's benefits. DSPM's built-in AI security capability helps teams get end-to-end visibility and control over data and AI models to proactively protect against AI risks. Its helps to

- Gain a 360-degree view of your AI models, agents, and services
- Identify and secure AI training data against data poisoning, misconfigurations, and exposure
- Align with new and emerging AI compliance frameworks

With DSPM security leaders can transform security chaos into controlled innovation, providing unified data discovery, contextual risk assessment, and automated governance across every AI interaction.



5. Ibid.



AI-Powered Data Classification

Effective data classification is the fundamental aspect of robust data security. Proactively mapping sensitive data to associated risks is essential for avoiding potential exposure caused by misconfigurations or unsafe practices. Conventional approaches, often reliant on manual procedures or simplistic pattern recognition, are susceptible to elevated false-positive outcomes and suboptimal allocation of security resources. Often, organizations rely heavily on regex-based solutions—a rigid and burden by false positives approach, proved brittle and inefficient. Even current point-product approaches fail to integrate classification within a centralized, unified platform leading to inconsistent alerts and siloed visibility, especially as data moves across an organization's ecosystem.

Security leaders can leverage DSPM with the AI-Powered LLM classification that augments operation around traditional regex workflows, bringing incredible visibility and flexibility empowering them to secure both known and unknown sensitive data like never before. Unlike keyword-dependent techniques, LLM classification enables deeper content identification. It uses advanced language processing for data classification to understand the intent and context of content, without needing any predefined patterns or keywords. This allows organizations to not only enhance their existing practices but also uncover and secure new types of sensitive data previously overlooked or undiscoverable.

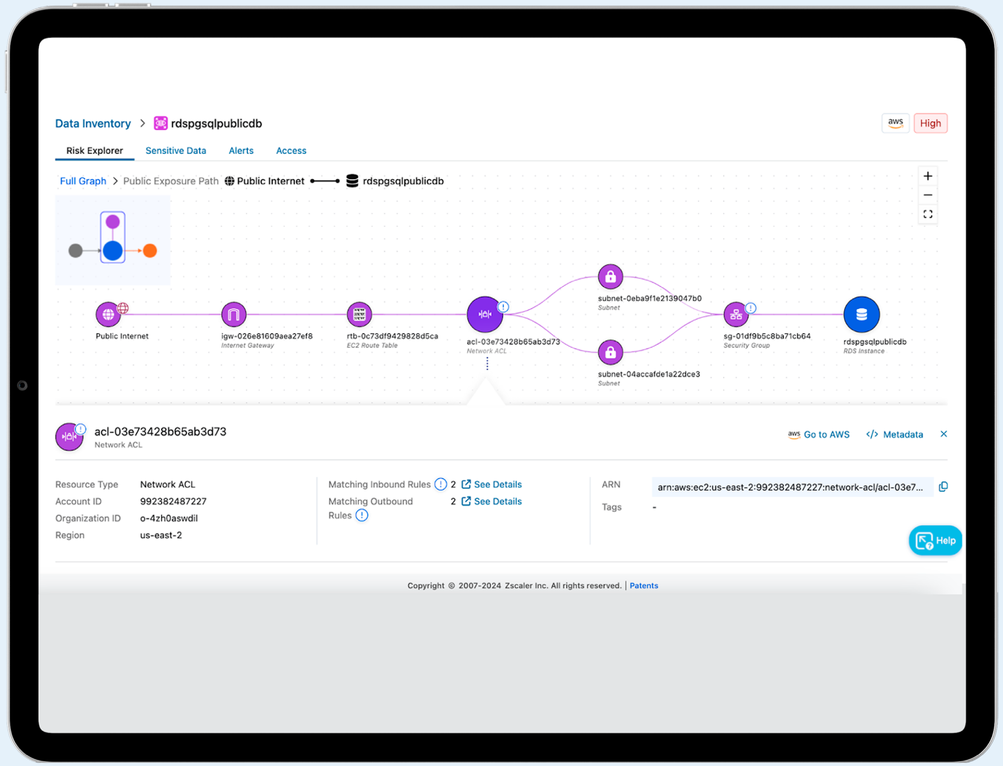
Proactive Risk Management

To effectively control security risk and ensure compliance, security leaders need a proactive way to manage their data security posture. One of the most exciting applications of AI in data security is proactive security approach and predictive analytics. By analyzing and correlating data, AI algorithms can predict potential security risks. This proactive approach enables organizations to stay one step ahead of threats and critical risk.

DSPM leverages AI and advanced correlation techniques that helps identify patterns and trends in data that may indicate impending security incidents. Furthermore, it can prioritize data stores based on their value (risk severity), thus ensuring that security efforts are directed to the most critical assets. Moreover, by automating numerous security processes, it lessens the workload on security professionals, enables a proactive security approach, and enhances overall operational efficiency.

For instance, Zscaler DSPM advanced correlation can proactively connect dots and detect hidden risk, allowing for the prioritization of security efforts on the most critical data.

6. **IBM's Cost of a Data Breach Report 2025**



49%

of organizations investing in security post breach[6]

Streamline Compliance With Real-Time Governance

Maintaining compliance with evolving regulations and internal security protocols is a cornerstone of AI and data security, from the GDPR to the SEC. Today organizations must navigate not only established regulations, such as GDPR and HIPAA, but also emerging frameworks specifically targeting AI, including the EU AI Act, NIST AI 600 and more. Security and compliance risk share an unbreakable bond, profoundly influencing one another and shaping an organization's trajectory. Breaches can trigger non-compliance sanctions, leading to severe repercussions, substantial fines and tarnishing an organization's reputation. Conversely, embracing regulations can serve as a shield, fortifying AI and data against security vulnerabilities and threats.

Many regulations break down to knowing AI and sensitive data, limiting who can access it, and continuously monitoring risk. Although that may sound simple, but the complexity of AI and data environments can make it challenging. Also, regulations are constantly evolving, driven by new technologies, changing privacy concerns, and the increasing interconnectedness of the global economy. This ever-shifting regulatory terrain demands constant vigilance and adaptation from organizations that wish to remain compliant. Traditional compliance approaches with fragmented views, manual assessments and reactive response struggle to provide clarity and efficiency.

DSPM can streamline compliance processes with real-time data compliance and governance capabilities. The DSPM solution provides organizations with a broad view of data compliance status, comprehensive analytics, benchmarking, remediation, and reporting to act swiftly on their compliance gaps. This is especially important in heavily regulated sectors, where a clear understanding of data status and risk mitigation is essential. From guided remediation steps to automated workflows, the compliance dashboard empowers security teams to act quickly and effectively. The application of AI in data governance ensures that organizations can meet regulatory demands while upholding robust security measures.

63%

of organizations lack AI governance policies[7]

7. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Achieve Least-Privileged Access

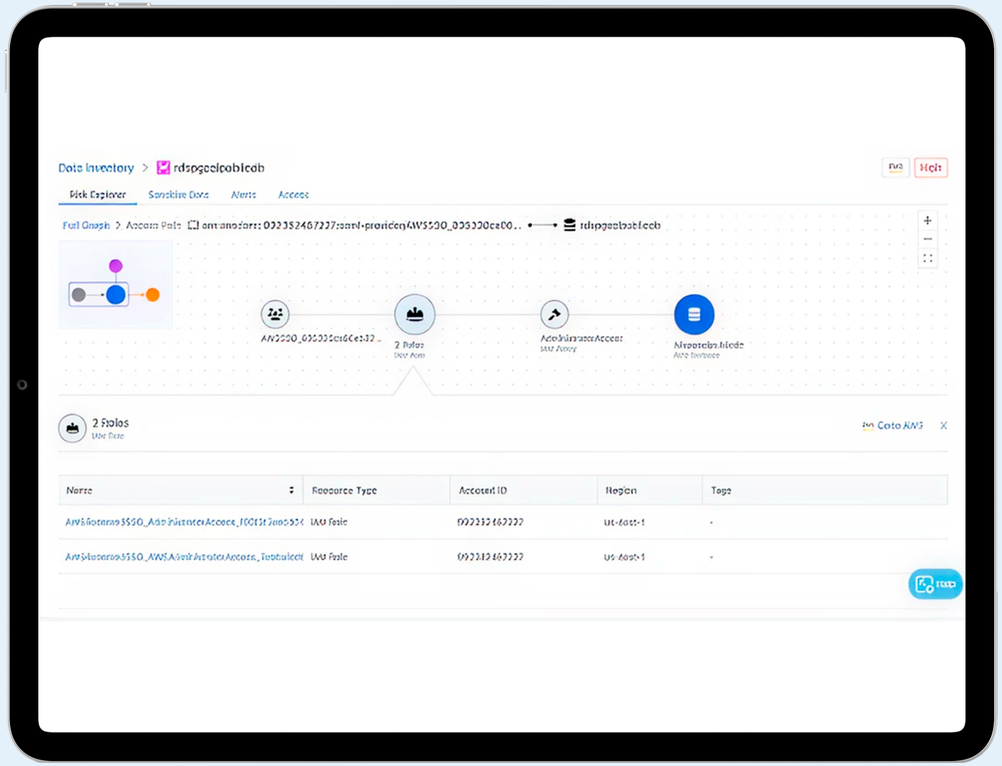
With the sheer volume of users, applications, and resources, data environments harbor significant risk of improper access controls, identity sprawl, and orphaned stores. Approximately 90% of organizations suffered identity related breach, resulting in costly security incidents.

Moreover, AI models and LLM-powered tools introduce additional risks around unauthorized data access. Key risks include unintentional or unauthorized sensitive data disclosures, data exfiltration—where sensitive data is stolen via AI outputs —and sophisticated attacks, where compromised identities exploit AI systems to gain unauthorized access.

That's why ensuring least-privileged access to data stores is a foundational principle of data security. Data access governance is more challenging because of data sprawl, permissions sprawl, and complex AI and multicloud architectures. Still, it remains an essential component of data security, since unauthorized exposure of sensitive data is typically the first step of a sophisticated attack.

DSPM delivers a unified approach to data access governance with continuous monitoring of data security posture and user behavior. DSPM scrutinizes identity and data access management roles, permissions, and related attributes to swiftly identify risky access paths to data stores. DSPM supports structured, unstructured, and data across on prem, multicloud and SaaS environments, enabling organizations to consistently identify and address access risks and enforce access policies across diverse data estate and AI ecosystem. By providing detailed insights into access patterns and potential vulnerabilities, data security teams can enforce least-privileged access more effectively. This approach reduces the risk of unauthorized access and enhances the overall security of the data environment.

8. Security Today, Study: **90 Percent of Organizations Experienced an Identity-Related Incident in Last Year**, June 5, 2024.



90%

of organizations have suffered an identity-related incident[8]

Optimize Storage and Consumption Costs

Data teams need to optimize storage and consumption costs by identifying duplicate or neglected data repositories that can be eliminated or transferred to more cost-effective storage solutions. Conventional methods frequently fall short in identifying and managing this data, resulting in superfluous storage expenses.

DSPM solutions can confront this issue by furnishing insights into duplicate, or abandoned data stores, enabling organizations to take appropriate measures. Like Zscaler DSPM provides a comprehensive view of duplicate or abandoned data stores, enabling teams to identify data that can be safely deleted or migrated.

With AI-driven insights, organizations can curtail excess storage expenses and ensure the proper management and protection of sensitive information.

Enforce Unified Policies Across All Data Environments

With traditional methods, the challenge of maintaining consistent data security policies across diverse environments is formidable. DSPM solutions can surmount this by offering a unified approach to data security in multicloud settings, enabling organizations to enforce uniform policies across all data environments.

Zscaler DSPM presents a unified strategy for data security. It empowers organizations to establish uniform policies across all data landscapes, ensuring comprehensive surveillance over cloud data and streamlining the process of risk identification and resolution. By using AI/ML insights, organizations can reduce the risk of data breaches and better follow data protection rules.

Rapid Incident Response

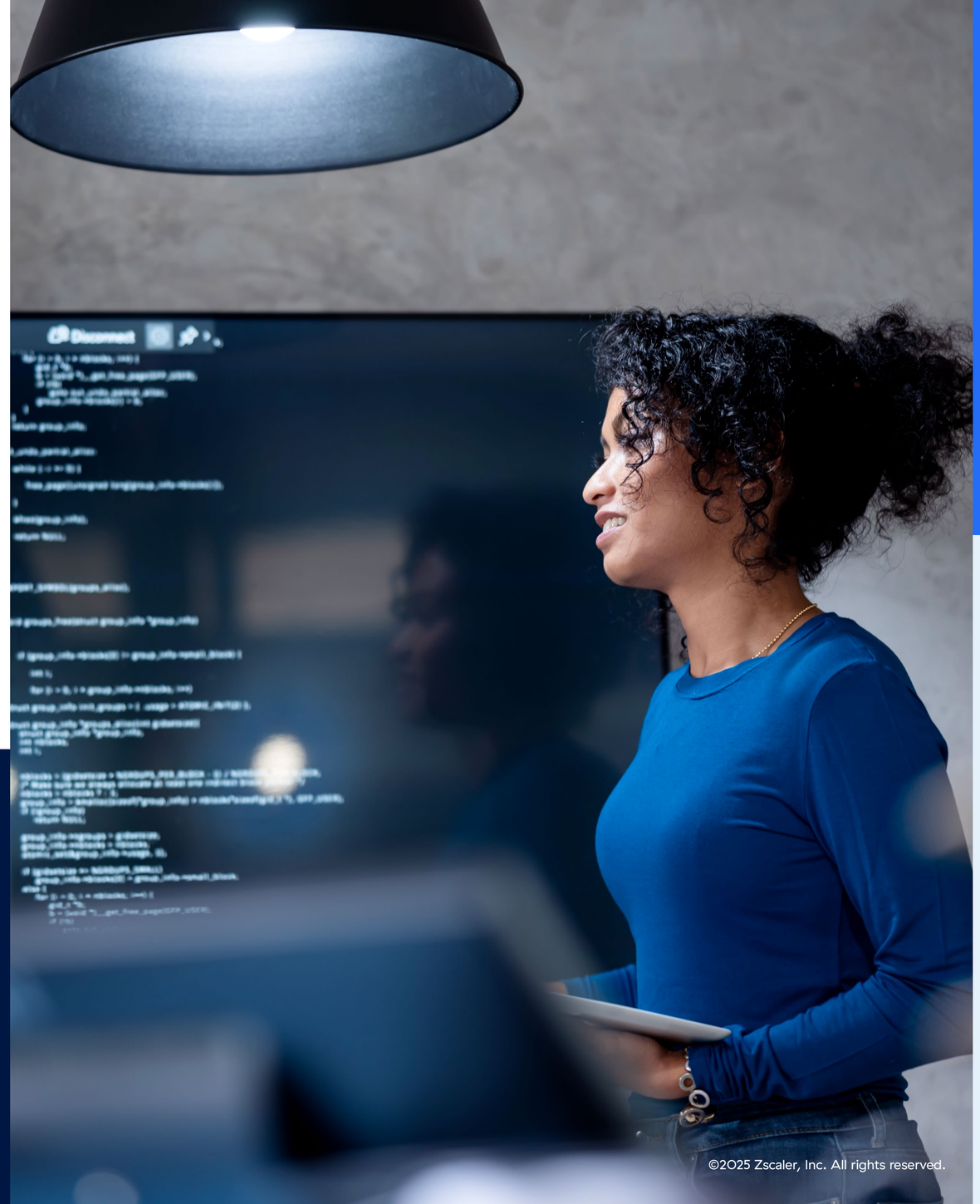
Identifying and mitigating risks are fundamental tasks for data security professionals. The speed at which threats evolve necessitates real-time responses. However, conventional methodologies may falter in the face of a dynamic AI driven threat environment. AI-driven security automation is the answer to this challenge.

DSPM can continuously monitor data, detect anomalies, and help respond to threats. DSPM solutions bolster risk mitigation by offering sophisticated risk correlation and adaptive access intelligence. Some of the DSPM solutions, like Zscaler DSPM, incorporate threat intelligence from Zscaler ThreatLabz, meticulous guided remediation, and expedited security implementation. Through sophisticated AI-driven threat correlation, organizations can unveil latent risks and pivotal attack vectors, enabling a concentrated effort on the most critical risks.

9. Statista, **Mean time to identify and contain data breaches worldwide from 2017 to 2024**, accessed December 9, 2024.

194 days

The average time to identify a data breach[9]



Enhanced AI Security

Organizations are adopting AI applications at a breakneck pace. Unfortunately, AI applications like generative AI (GenAI) and large language models (LLMs) have introduced significant data breach and noncompliance risks. A recent report stated that 13% of organizations reported breaches of AI models or applications[10], highlighting that AI is becoming a high-value target.

Organizations that integrate GenAI across their operations must take measures to prevent inadvertent use of sensitive data within these models. Security teams must prioritize flagging, tagging, and classifying data to ensure that cross-functional teams are leveraging GenAI responsibly.

DSPM can enhance the control and protection of data in GenAI environments with integrated AI-SPM capabilities. By meticulously identifying and categorizing data, DSPM can prevent sensitive information from being fed to LLMs, reducing risk of both data breaches and noncompliance. DSPM takes a "data-first" approach, focusing on securing the information that fuels AI rather than only the infrastructure. By continuously discovering, classifying, and monitoring data throughout its lifecycle, DSPM helps mitigate unique AI security risks like data poisoning, sensitive data exposure, and model theft.

Adopting DSPM that has in-built AI-SPM capabilities can empower organizations to instill trust in their AI applications. In doing so, they not only protect their important data, but also make AI applications more reliable and secure.

10. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Harnessing DSPM to Secure Diverse Data Landscape

Strategic use of DSPM is paramount in the pursuit of more robust data security. These technologies offer the requisite context and automation to effectively manage the intricacies of modern data environments. Through a proactive stance, security leaders can more effectively safeguard sensitive data, ensure compliance, and mitigate the risks associated with progressive technologies like GenAI.

“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, Innovation Insight: Data Security Posture Management,
Brian Lowans, Joerg Fritsch, Andrew Bales,
28 March 2023

Zscaler DSPM

Zscaler DSPM is the world's most comprehensive integrated data protection platform for securing structured and unstructured data across, SaaS–, public cloud environments (AWS, Azure, GCP), on–prem, and endpoints.

Zscaler DSPM provides granular visibility into cloud data, classifies and identifies data and access, and contextualizes data exposure and security posture, empowering organizations and security teams to prevent and remediate cloud data breaches at scale.

Zscaler DSPM takes an AI–powered, unified approach to ensure strong data hygiene across all data stores, including IaaS, SaaS, on–premises, endpoint, and more. Natively integrated with the Zscaler Data Security Platform, it enables you to fully understand and control all your data on a single platform.

Zscaler Data Security Platform uses a single and unified DLP engine to deliver consistent, best–in–class data protection across all channels. By following all users across all locations, and governing data in motion and at rest, it ensures sensitive data is seamlessly protected and compliance is achieved

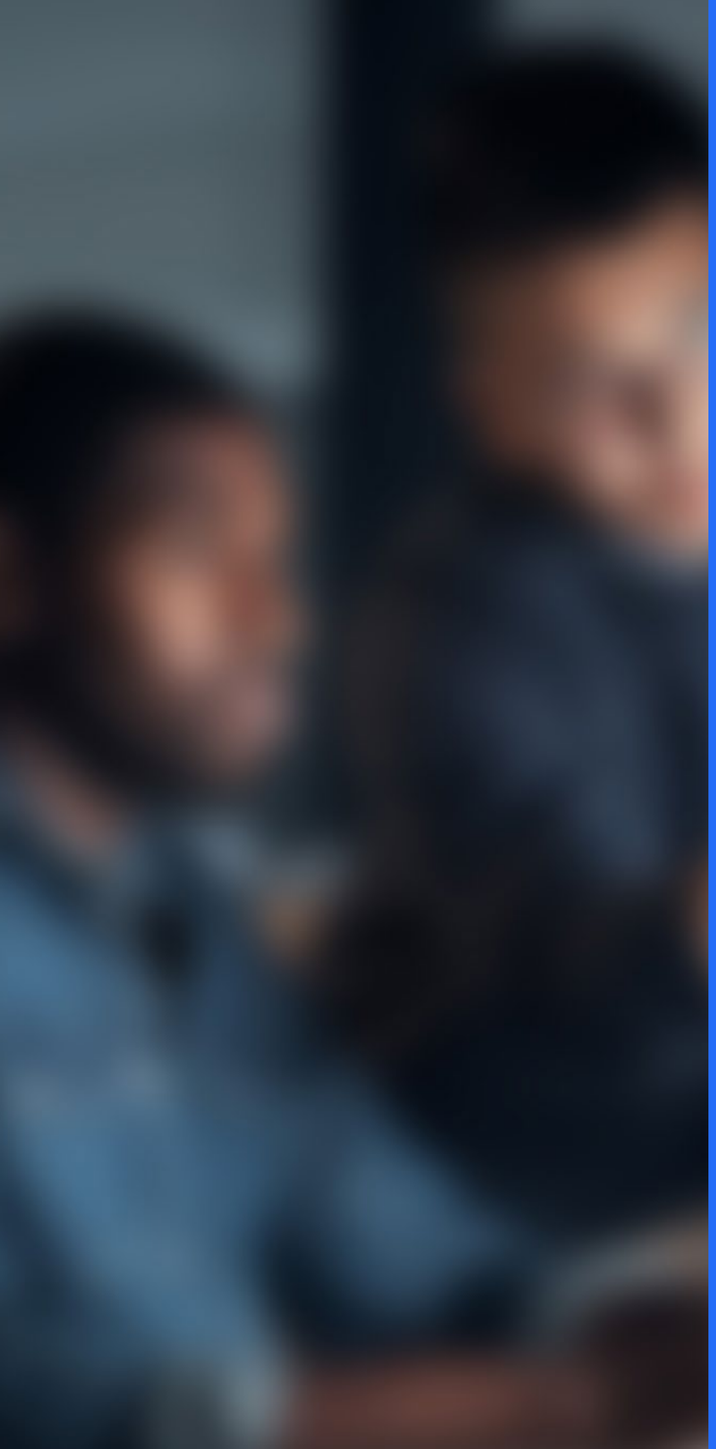
For more info, visit zscaler.com/dp/dspm.

Explore DSPM interactive product tour

Why Does DSPM Belong In Your Data Protection Strategy?

Watch the on–demand webinar ⟶

Scan the QR code to access helpful DSPM resources:



zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 in-line 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**