Sponsored content | White paper

How to secure data without slowing AI innovation

CIO

Sponsored by zscaler™

Artificial intelligence (AI) is changing the pace and texture of everyday work. Employees now rely on AI assistants to summarize documents, automate workflows, analyze data, and generate content in seconds. At the same time, organizations are moving information across software-as-a-service (SaaS) platforms, cloud services, collaboration tools, and application programming interfaces (APIs) at unprecedented speed. Sensitive data is no longer confined to controlled repositories; it flows continuously through systems that were never designed to inspect or protect it.

This new reality exposes a fundamental challenge. Security teams once concentrated on safeguarding where data was stored. Now the greater risk lies in understanding where data travels, how it is used, and who can access it along the way.

According to Gartner, data security concerns remain one of the primary barriers to AI deployment, with the firm predicting that by 2027, 40% of AI data breaches will result from cross-border generative AI misuse. As AI adoption accelerates, organizations must protect sensitive information without restricting the productivity gains that AI enables.

Data exposure is expanding beyond traditional boundaries

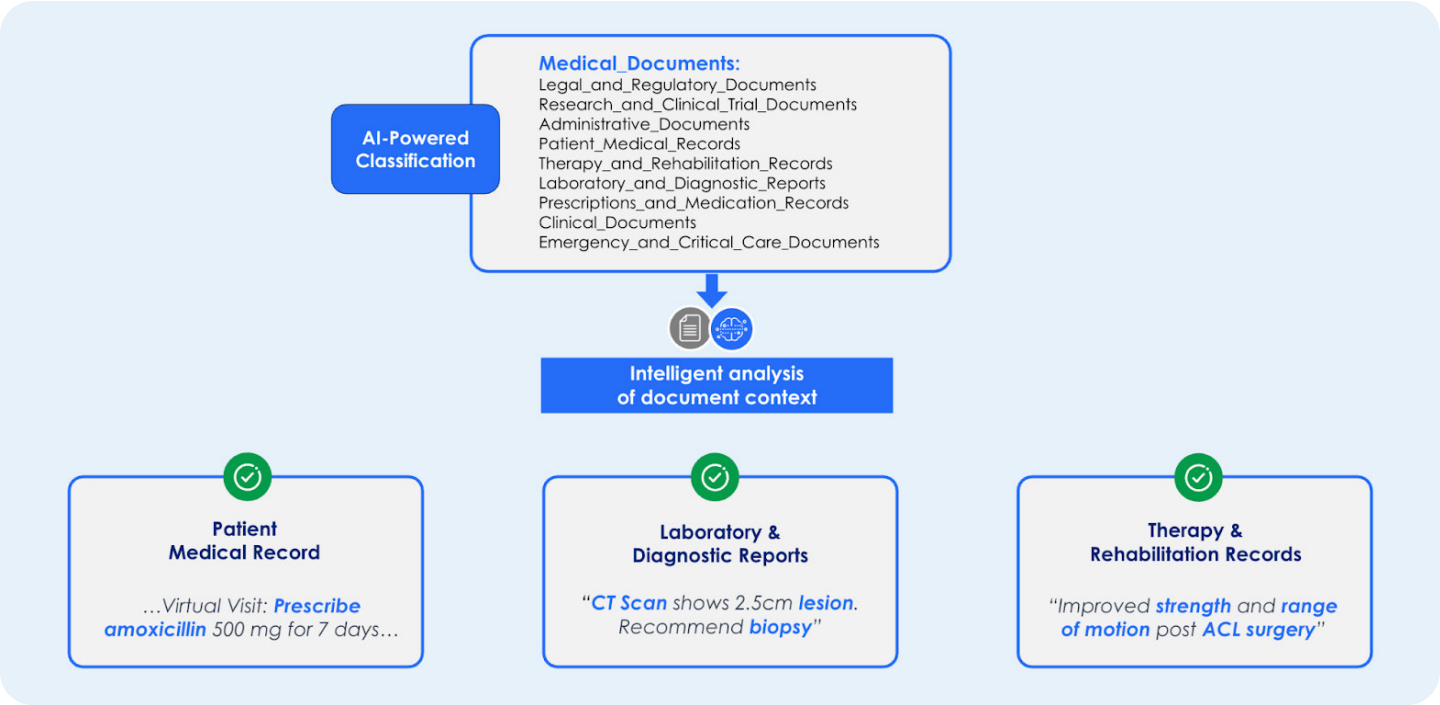
AI introduces new pathways for data exposure. Chatbots, copilots, and automation tools provide powerful interfaces for accessing and generating information. When permissions, data repositories, and collaboration environments are not tightly governed, AI systems can surface sensitive information at scale.

At the same time, cloud and SaaS ecosystems distribute data across environments while shadow data and oversharing increase exposure risk. Sensitive information can move from a cloud data store to a collaboration platform, on to an endpoint, and into an AI prompt within seconds. Organizations cannot protect data they cannot see.

Visibility must extend across structured, unstructured, and AI data flows

Traditional data governance focused primarily on structured databases, but AI changes the equation. Most enterprise data today is unstructured: documents, chat logs, transcripts, presentations, source code, and images. AI systems consume this unstructured content and combine it with structured data to generate responses. Effective protection requires visibility across data at rest and in motion, along with insight into how data connects to AI systems. Security teams need to understand what sensitive data exists, who can access it, where it resides geographically, and how it flows between systems.

Advanced classification technologies now improve accuracy by analyzing context across structured and unstructured data. This reduces false alerts while helping teams identify risk more precisely. Visibility is the foundation of effective data protection.



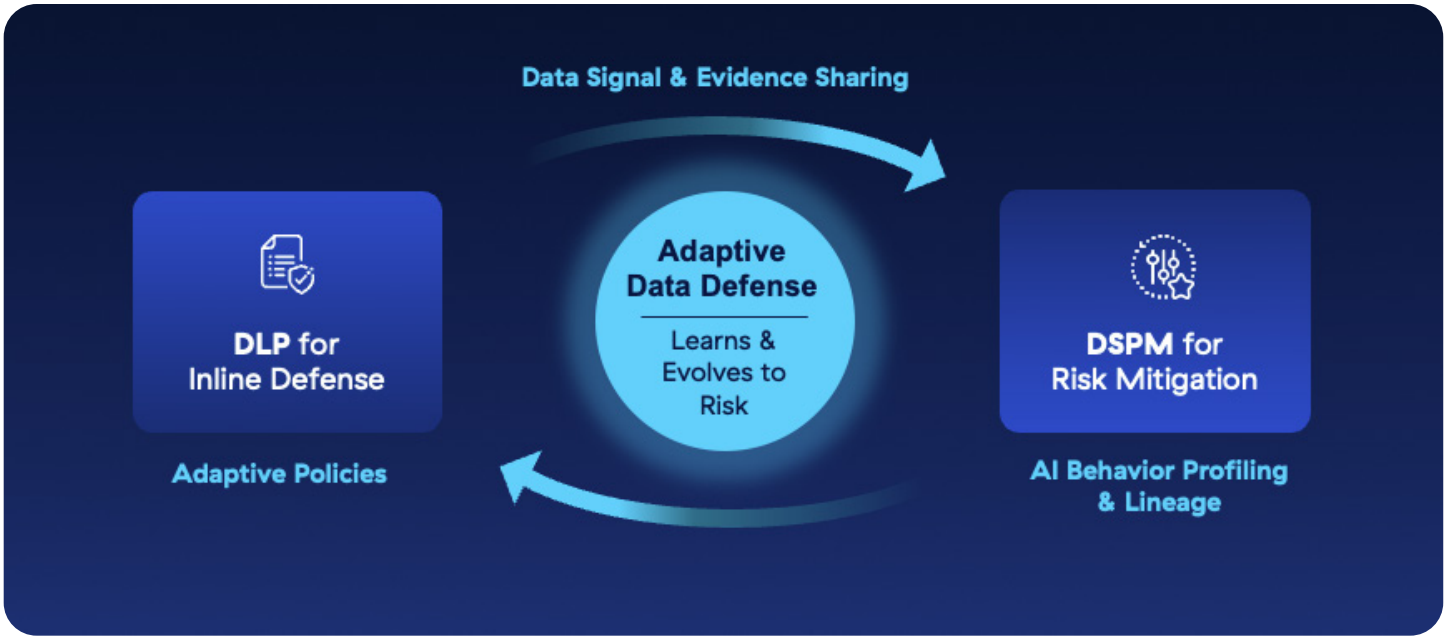
Finding new types of unstructured data with AI-powered classification

DSPM and DLP together reveal hidden risk

Data security posture management (DSPM) and data loss prevention (DLP) have traditionally operated in separate domains. DSPM analyzes data at rest, identifying sensitive data stores, access risks, and exposure issues across cloud and data environments. DLP enforces real-time policies to prevent sensitive information from leaving the organization through email, web traffic, endpoints, and collaboration tools. Together, they provide a more powerful defense.

DSPM delivers a comprehensive inventory of sensitive data, reveals overprivileged access, and highlights compliance gaps. Data lineage capabilities show how information flows across systems and AI workflows, revealing risk that would otherwise remain hidden.

DLP provides inline protection, enforcing policies in real time. When DSPM insights feed into DLP controls, organizations can dynamically adjust protections based on context. For example, if data originates from a sensitive customer database, policy enforcement can automatically prevent that data from being copied to removable media or shared externally.



Unifying DLP and DSPM for intelligent closed-loop data security

This combined approach also supports insider risk detection. Risk often stems not from malicious intent but from employees trying to be productive. Telemetry and behavioral signals can identify unusual activity patterns, enabling adaptive controls that strengthen protections when risk increases.

If DSPM is the security camera monitoring entrances and exits, DLP is the guard-and-gate system that prevents sensitive information from moving into unauthorized areas. Together, they create layered, contextual protection.

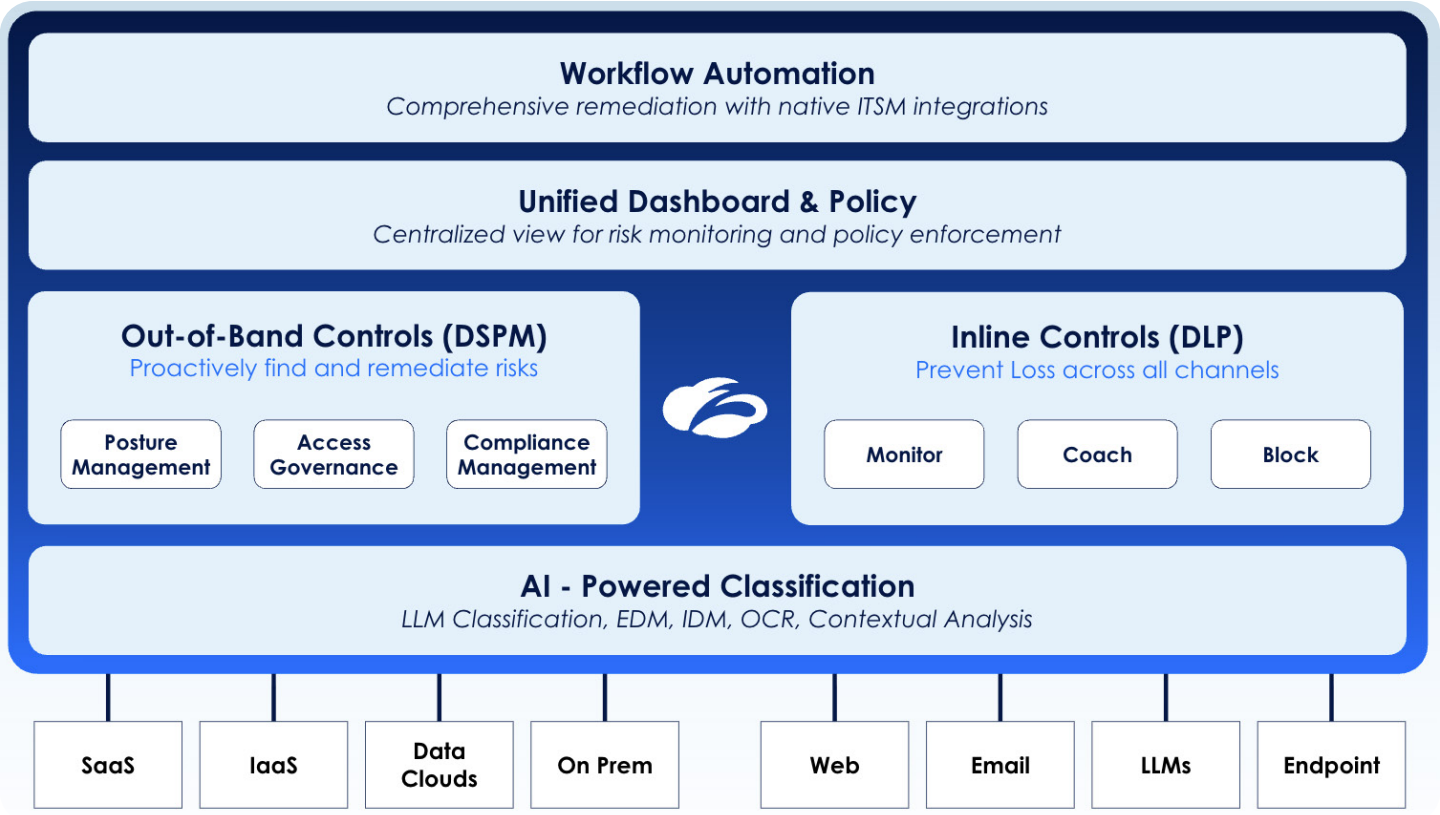
Inline protection enables safe data use without slowing work

Security controls must operate where data moves, not where networks once ended. Inline protection enables organizations to safeguard data across web traffic, email, endpoints, SaaS applications, and AI tools without disrupting workflows.

Inline inspection can prevent sensitive data from being used to train AI models and can also detect sensitive information in AI responses and block unintended data exposure in real time. Unified policy enforcement ensures consistent protection across channels while enabling employees to collaborate and innovate. Protection must travel with the data, not depend on network location.

Unified data security supports AI innovation and compliance

Fragmented security tools create gaps, complexity, and inconsistent enforcement. A unified approach provides a common classification engine, centralized policy enforcement, and consistent visibility across environments.



How Zscaler unifies all data security into one comprehensive platform

This approach reduces operational complexity, improves accuracy, and helps organizations maintain regulatory compliance while accelerating AI adoption. It also supports business agility by enabling teams to use data confidently and responsibly.

AI-driven productivity depends on trusted access to data. By prioritizing visibility, contextual risk insight, and consistent inline protection, organizations can reduce risk while enabling secure AI innovation.

Modern data security is not about restricting access. It is about ensuring that data can be used safely, intelligently, and at the speed today's businesses demand.

Visit Zscaler Data Security today to learn how a unified, zero trust-based approach to data protection can help your organization secure sensitive data while enabling safe AI adoption.