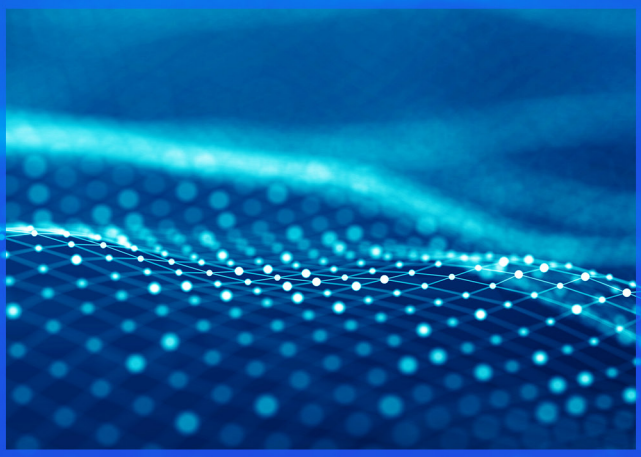
Zscaler Data Loss Prevention (DLP)

Empowering organizations to secure their data, reduce risk exposure, and strengthen stakeholder trust.



In today's digital ecosystem, data flows continuously across multiple cloud platforms, mobile devices, and enterprise applications. Sensitive data flowing throughout these platforms puts your organization at great risk of data loss, exposure, and unauthorized access.

As a result, more organizations are implementing a Data Loss Prevention (DLP) strategy, a proactive and unified approach that is essential to mitigating these risks and safeguarding the organization's most valuable digital assets by detecting, monitoring, and controlling sensitive data flows so critical information remains secure. Zscaler Data Loss Prevention (DLP), a subscription-based cybersecurity solution, is a critical component of any robust DLP strategy.

Zscaler's Zero Trust Exchange prevents lateral movement within your network, so users do not have access to the entire environment. Instead, it allows access only to areas allowed by their individual identity. To grant access, Zscaler is always verifying—through port verification, multifactor authentication, and device and location trust assessments—to help assure compliance.

By continuously computing a risk score—based on user posture, device behavior, and access conditions—Zscaler evaluates access request against the organization's security policies.

Zscaler capabilities for DLP

How it works: The user and server establish independent, encrypted sessions with the Zscaler cloud, which securely allows them to communicate. This approach reduce direct network connections, lowering the risk of attacks, preventing lateral movement, and enabling deep visibility and control over data in motion. During this protected session, Zscaler delivers a set of capabilities designed to protect sensitive data across communication channels and environments, such as:

- **SSL/TLS inspection:** Gives full visibility into encrypted traffic, uncovering concealed threats so encrypted data flows cannot be exploited.
- **Inline data inspection:** Performs real-time analysis of data in motion across web, email, and cloud applications, identifying and protecting sensitive information before it leaves the organization's environment.
- **Out-of-band inspection:** Enables security controls to data at rest, detecting threats without disrupting business operations or data access.
- **Granular policy enforcement:** Allows organizations to define rules based on user roles, data categories, and application contexts, aligning protection policies with business priorities and regulatory requirements.
- **AI-powered data discovery and classification:** Uses machine learning and artificial intelligence (AI) models to automatically identify sensitive data, detect anomalies, and reduce false positives.
- **Integration with cloud access security broker and endpoint protection:** Extends DLP coverage to cloud applications and endpoints, applying consistent security across digital assets.

The KPMG advantage

KPMG complements Zscaler's DLP by delivering strategic consulting, policy design, and integration services that align DLP with broader data governance, privacy, and compliance frameworks. Zscaler and KPMG help organizations secure sensitive data, meet regulatory requirements, and reduce operational and reputational risks through a unified, proactive data protection strategy.

Achieving a mature and effective DLP program requires a unified strategy that brings together people, processes, and technology across an organization. The KPMG framework methodology turns policies into actionable controls, leading to measurable risk reduction, and ultimately an environment where sensitive data is protected by design, not just enforcement.

How KPMG helps implement Zscaler DLP

By aligning Zscaler's advanced capabilities with an organization's governance, risk, and compliance framework, KPMG helps make data protection an integral component of its security and business strategy. The process involves a series of steps:

1

Current-state assessment

KPMG conducts a thorough evaluation of existing data flows, data protection tools, and security solutions used within the organization.

2

Policy design and tuning

KPMG then develops and refines Zscaler's DLP policies to align with business needs, helping ensure protection for sensitive data while maintaining productivity.

3

Integration services

KPMG connects Zscaler ZTE with existing SIEM and SOAR platforms, enabling centralized monitoring and streamlined incident responses.

4

Pilot deployments

KPMG configures Zscaler solutions in controlled environments for selected high-risk use cases to validate performance and gather detailed feedback. Pilot deployments allow for adjustments and greater optimization based on real-world analytics and threat intelligence.

5

Rollout and optimization

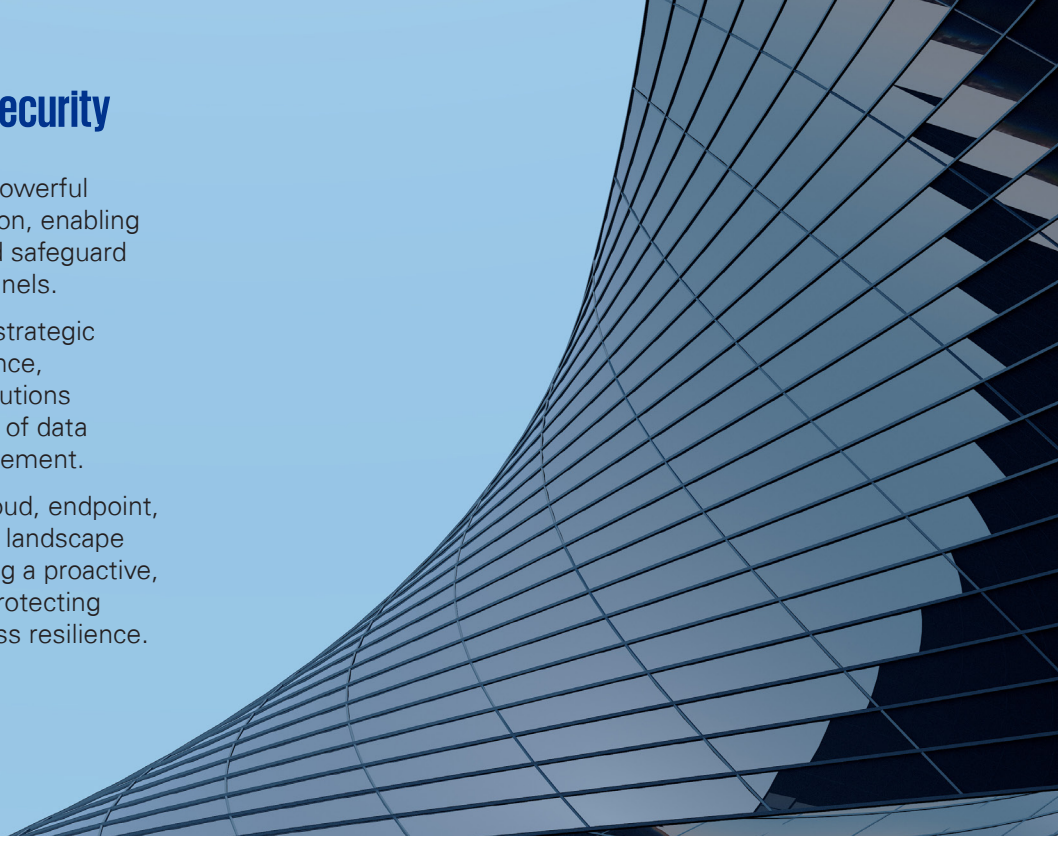
KPMG scales the deployment of Zscaler's ZTE across the enterprise, helping ensure thorough coverage and robust integration with existing security operations. KPMG will further establish key performance indicators and dashboards to monitor performance and policy compliance, driving ongoing enhancement through continuous analytics and refinement.

Gain control of your security

Zscaler's DLP capabilities create a powerful foundation for modern data protection, enabling organizations to detect, classify, and safeguard sensitive information across all channels.

KPMG amplifies this value through strategic consulting, implementation experience, and complementary governance solutions that address the broader challenges of data compliance, privacy, and risk management.

As data continues to flow across cloud, endpoint, and hybrid environments, the threat landscape continues to evolve as well. Adopting a proactive, integrated DLP approach is key to protecting digital assets and sustaining business resilience.



Contact us

Sai Gadia
Partner, KPMG LLP
E: sgadia@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**