Modernizing data protection in the AI era

EY-Zscaler Alliance

May 2026

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Disclaimer

- The views expressed by the presenters are their own and not necessarily those of Ernst & Young LLP or other members of the global EY organization. Moreover, they should be seen in the context of the time they were made.
- Neither Ernst & Young LLP nor any member firm thereof shall bear any responsibility for the content, accuracy or security of any third-party websites that are linked (by way of hyperlink or otherwise) in this presentation.
- These slides are for educational purposes only and are not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

Contents

1

The data protection imperative

The expansion of the attack surface and the evolution of data protection

Data protection is more complex than ever. What once was a castle-and-mote approach to protect on-premise data stores is now dispersed across on-premise, cloud, SaaS and artificial intelligence (AI). This evolution demands a new approach to securing sensitive data — an integrated, intelligence-led data protection capability within Zero Trust and other modern security architectures.

Rapidly expanding and fragmented regulatory environment

The current global data protection landscape is more complex than at any point in history:

- 144 countries enforce national data privacy laws.
- The absence of a federal U.S privacy law has resulted in state-by-state patchwork with varying thresholds, requirements and definitions for sensitive data.

This fractured landscape increases cost, operational complexity and the risk of non-compliance.

Hybrid workforces have expanded the attack surface

Employees increasingly access sensitive data from remote locations and unmanaged devices, expanding the organization's exposure.

As information flows across users, Software as a Service (SaaS) platforms, cloud environments and AI tools, traditional security controls lose visibility and effectiveness.

This broader and more complex attack surface elevates the risk of data leakage, misuse and unauthorized access, while making consistent policy enforcement and monitoring significantly more challenging.

Escalating cyber and AI-driven risk exposure

Threat actors and new technologies are driving a surge in data protection risk.

AI-powered cyber attacks and sophisticated ransomware campaigns continue to escalate, increasingly targeting critical infrastructure and global supply chains.

Meanwhile, AI governance is becoming a mandatory requirement as the EU AI Act enters phased enforcement, tightly linking AI oversight with privacy and data loss prevention (DLP) expectations.

Potential data loss scenarios impacting your organization

Accidental ← Data loss continuum → **Intentional**

Unintentional actions by employees that can result in data loss

- Emailing sensitive data to wrong recipient
- Uploading files to unauthorized cloud apps
- Sensitive information is included in a generative AI (GenAI) prompt
- Accidental backup of data to personal storage

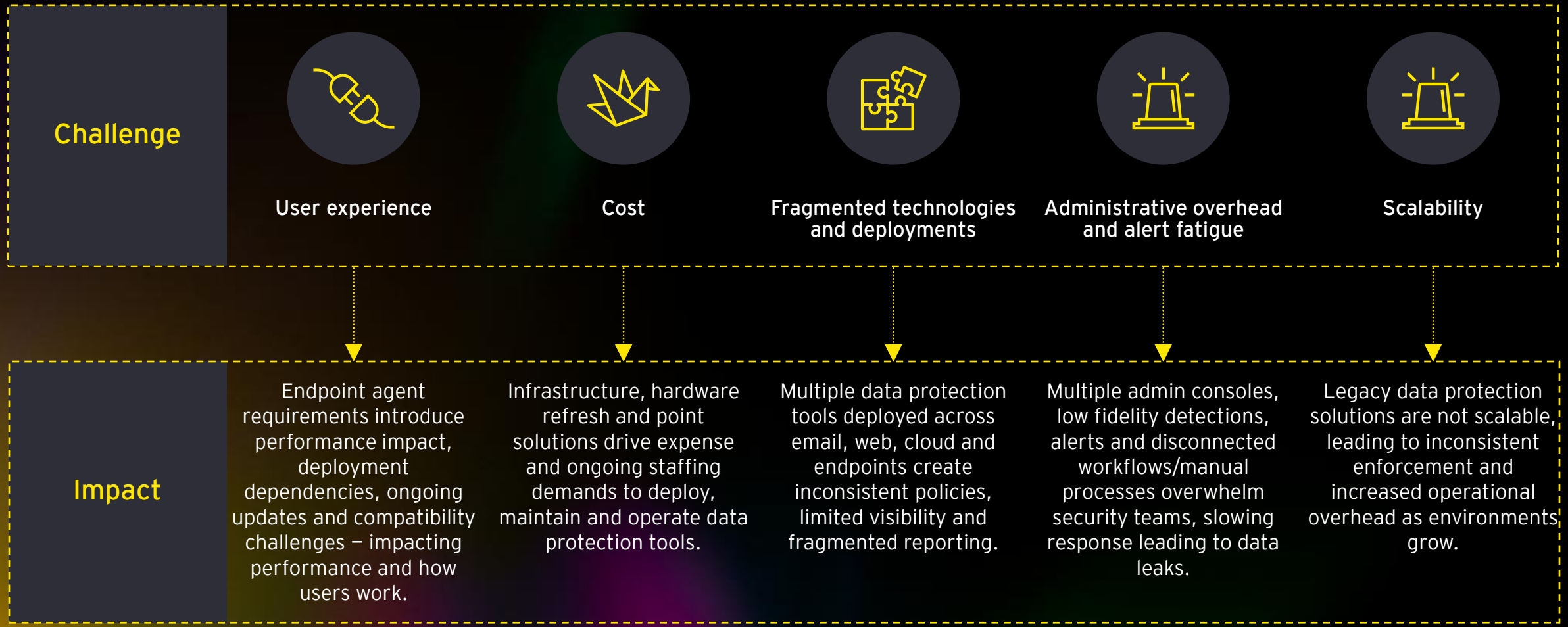
Next-gen data protection to address loss scenarios

Deliberate actions by insiders can compromise sensitive data

- Intentional exfiltration of data via email, removable storage, personal cloud storage, etc.
- Use of encryption to evade data exfiltration
- Use of unapproved data transfer methods
- Intentional misuse of a GenAI model to circumvent controls or extract sensitive information

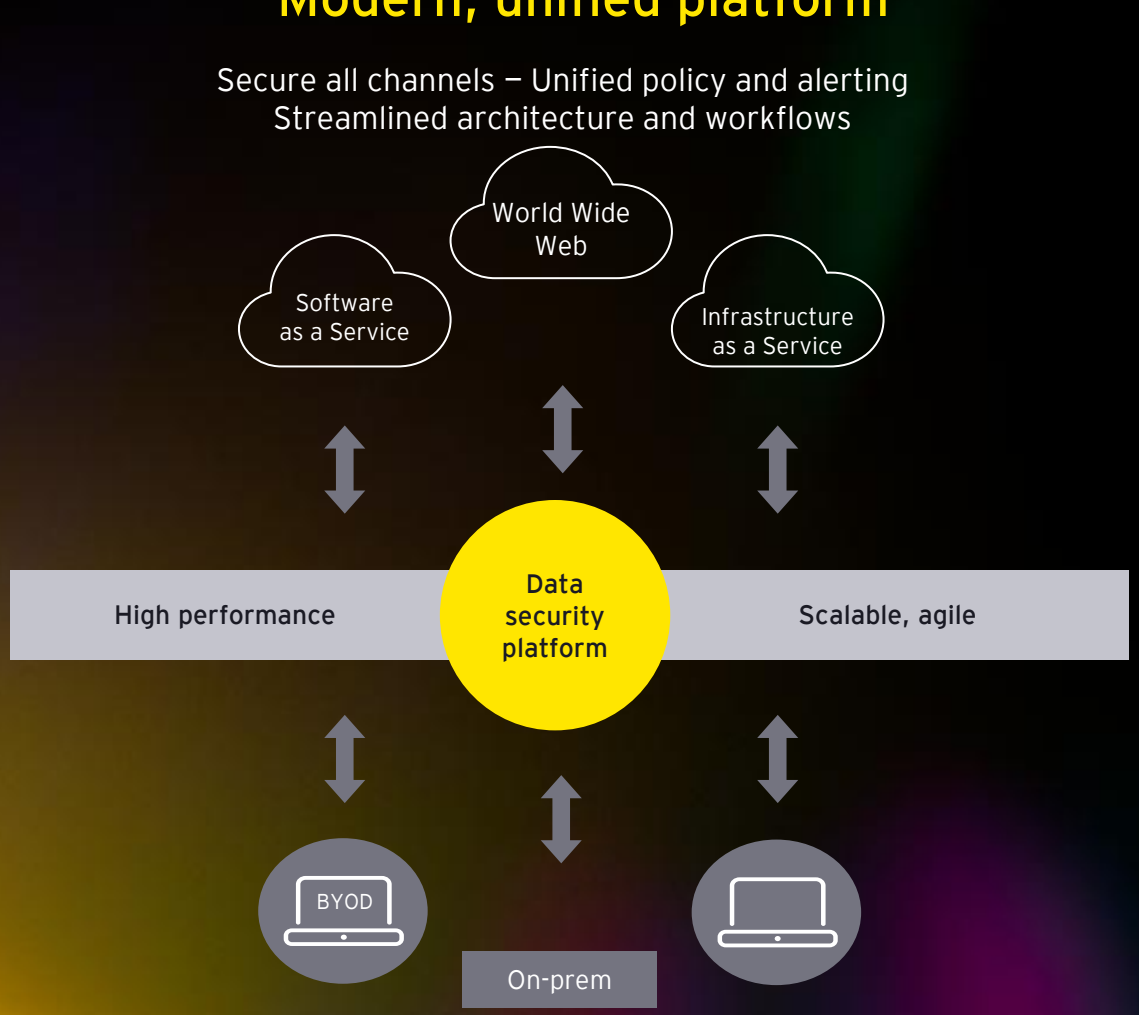
Legacy data protection challenges and impact

Traditional data security involves multiple disconnected solutions, creating complexity and inefficiency.



Benefits of addressing legacy complexity with a modern unified platform

Modern, unified platform



Benefits

- Reduce cost and complexity with a cloud-delivered, unified DLP approach across all data channels.
- Improve user experience by removing agents and enabling seamless protection.
- AI-driven classification everywhere to fully understand and protect your data universe.
- Automate workflows to streamline operations and guide users with built-in education.
- Simplify technology management by reducing tool sprawl, easing administration and accelerating incident response.
- Effortlessly scale protection without major infrastructure changes or added licensing overhead.
- Integrate easily with key cloud applications for consistent policy enforcement.
- Strengthen regulatory compliance and audit readiness with consistent, defensible data protection controls across all channels.

2

Overview: Zscaler's data protection solutions

Zscaler's platform capabilities are customizable, fit for purpose and delivers unified data protection

Cloud-native platform that scales with your data universe

DLP

- Discover and protect sensitive data across web, SaaS, email, endpoints and cloud applications.
- Enforce consistent policies inline to prevent data loss through uploads, sharing and user actions.

Data Security Posture Management (DSPM)

- Continuously discover, classify and assess sensitive data stored across cloud services and repositories.
- Identify data exposure risks, and over-permissive access to reduce attack surface.
- Provide contextual insights to prioritize remediation and strengthen overall data security posture.

AI classification

- Automatically identify and classify sensitive data using AI-powered detection and contextual analysis.
- Enable scalable, consistent data classification across structured and unstructured data.

Bring your own device (BYOD)

- Protect your organization's data from exfiltration by contractor workforces and unmanaged devices.
- Block copy/paste, disable printing, restrict downloads/uploads, and apply watermarking to documents viewed on BYOD screen.

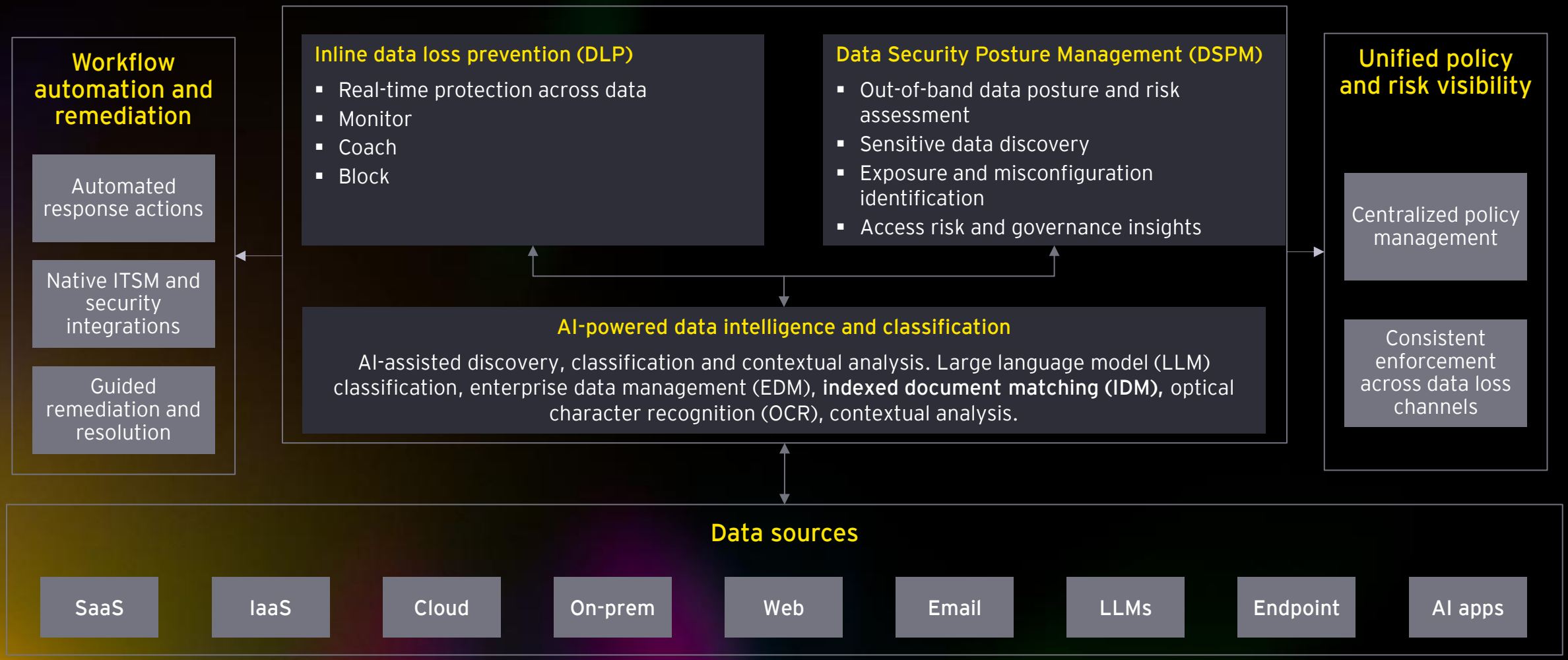
Securing AI usage

- Deep inspection and visibility into user input prompts sent to GenAI apps.
- Enforces policies to prevent the leakage of sensitive data through GenAI application inputs and outputs across web, endpoints and cloud.

Workflow automation

- Centralized incident management.
- Real-time coaching to provide instant feedback to users attempting risk actions.
- Automate DLP incident response.
- Facilitate resolution through automated incident escalation.

How Zscaler's Data Protection platform delivers unified data security with AI as the foundation



AI-powered classification: the foundation of data security

To protect data consistently, organizations must first understand what their data is, where it lives and how it is used. This slide illustrates how Zscaler applies multiple classification techniques to accurately identify sensitive data everywhere it exists.

Powerful classification everywhere

Data sources:

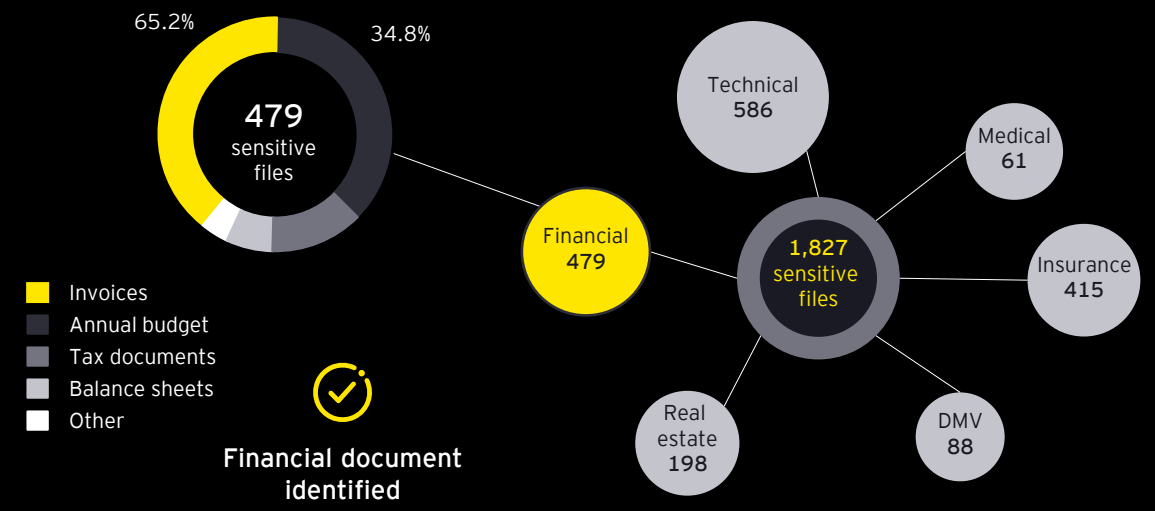
- SaaS
- IaaS
- Web
- Endpoint
- Email
- On-prem
- Data clouds
- LLMs

LLM classification

Reads language and understands intent

The company will revise its capital allocation strategy next quarter, prioritizing funding for high-performing business units while scaling back investments in weaker sectors. These changes are expected to improve EBITDA margin by 2%–3% and strengthen liquidity reserves to mitigate market risks.

In response to supply chain volatility and inflation, workforce expenditures are under review, with potential cuts in nonessential roles to safeguard financial health. Focus will shift to enhancing customer acquisition through digital platforms and loyalty initiatives to secure revenue streams and protect shareholder value.



Advanced classification

- **Exact data match (EDM)** — Structured custom data
- **IDM** — Custom docs and forms
- **OCR** — Screenshots and images

Regular expressions (regex), labeling and contextual

- **DLP dictionaries** — 100+ predefined and customizable
- **Data labeling** — Add or update missing data labels
- **90k+ shadow IT catalog** — Find risky apps across 75+ attributes

Enable AI while protecting data

This slide illustrates how Zscaler provides control to monitor AI usage, inspect prompts and responses in real time and enforce data protection policies consistently, enabling users to safely leverage AI without exposing sensitive information.

Key highlights

Discover and control use of AI:

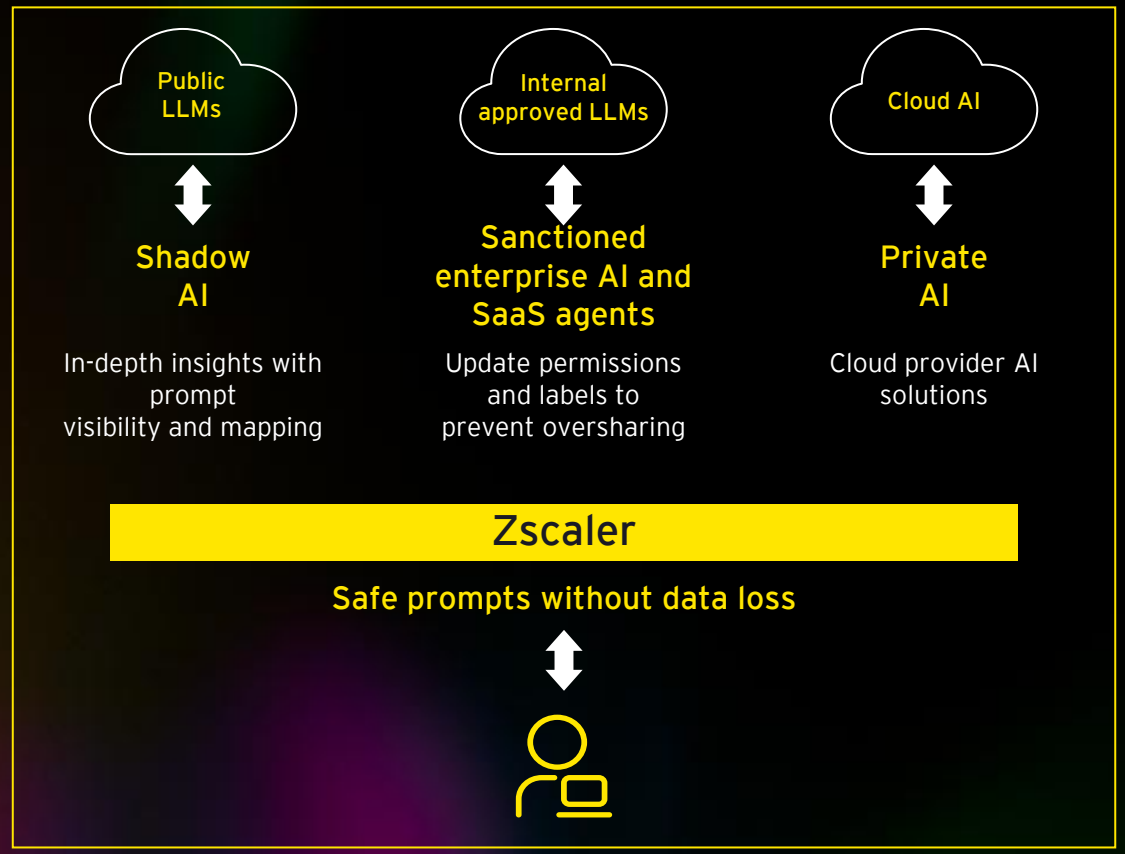
- Shadow AI and risk visibility
- Restrict content used in prompts

Safeguard data used for AI:

- Scan, classify and tag data
- Maintain proper access permissions

Govern AI systems (AI-SPM)*:

- Assess AI models and services
- Secure AI data pipelines



Benefits

Accelerate AI initiatives:

- Gain visibility and control to better scale AI strategies

Protect data:

- Empower users while controlling data risk

Spot AI trends:

- Gain usage insights to uncover new areas of need

Maintain compliance:

- Adhere to regulations across AI channels

* AI-security posture management (AI-SPM).

3

The EY-Zscaler Alliance

The EY–Zscaler Alliance| Data protection services alignment

The EY organization delivers end-to-end data protection services supported by Zscaler's technology to help clients discover, classify, protect and govern sensitive data. These services align to EY Strategy, Transform, and Operate cyber domains and support enterprise data protection, insider risk reduction and regulatory compliance initiatives.

Strategy and advisory

Define and align data protection strategy, architecture and use cases to business risk and regulatory requirements.

- Enterprise data protection maturity assessments
- Target-state data protection architecture design leveraging Zscaler Data Protection
- Data classification, labeling and policy strategy aligned to business risk and regulatory requirements
- Use case and value definition for data loss prevention, insider risk and cloud data protection
- Regulatory and risk alignment for sensitive data (PII, PCI, IP, regulated data types)

Transformation and implementation

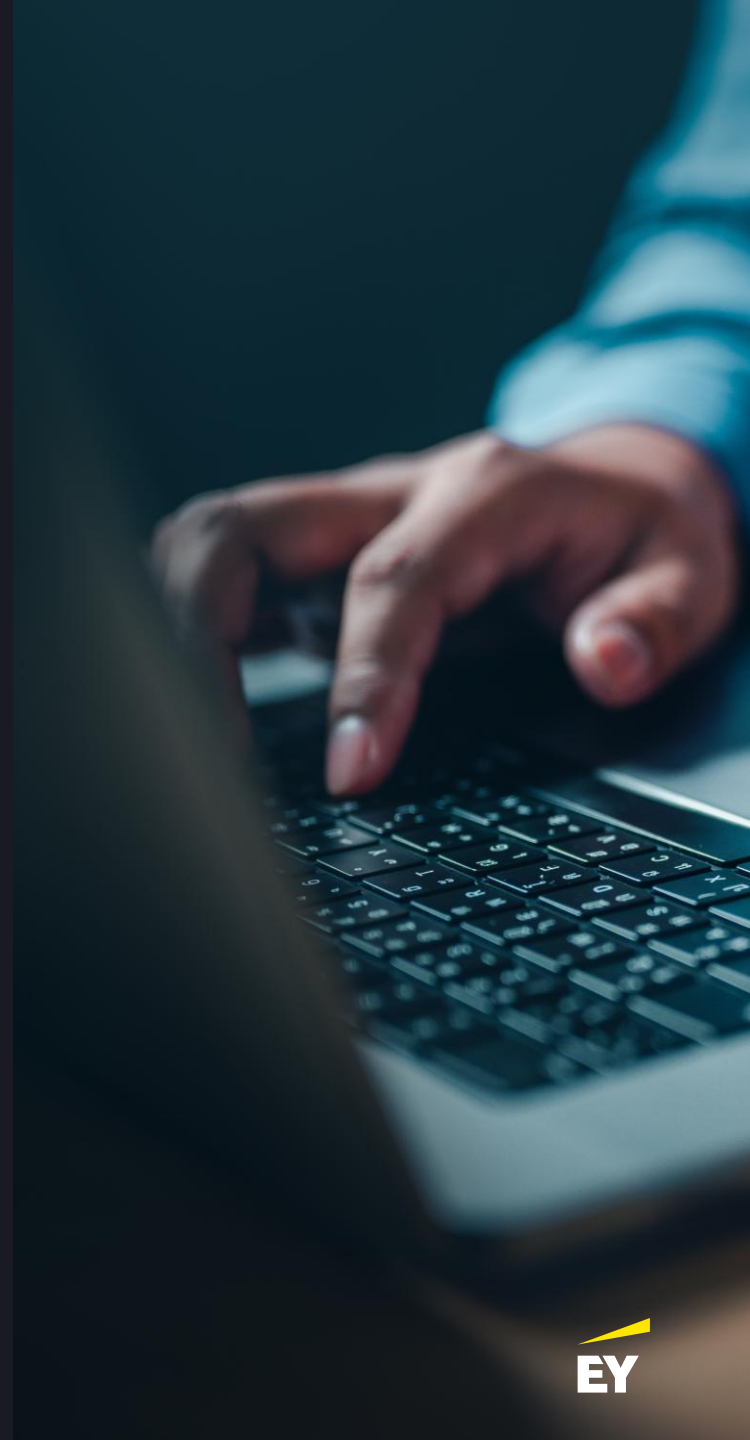
Deploy, integrate and operationalize cloud-native, Zero Trust data protection capabilities.

- Deployment and configuration of Zscaler Data Protection capabilities
- Integration with identity platforms, data classification tools and security operations center (SOC) workflows
- Policy design and tuning aligned to data sensitivity, user context and business processes
- Migration from legacy DLP and perimeter-based controls to cloud-native, Zero Trust data protection
- Operationalization of data protection use cases, including data exfiltration prevention and SaaS data governance

Operate and managed services

Run, optimize and evolve data protection controls through ongoing monitoring, incident support and alignment to changing business and regulatory needs.

- Ongoing monitoring, policy optimization and alert triage for data protection events
- Incident response support for data loss and insider risk scenarios
- Managed data protection operations, including reporting, compliance support and continuous improvement
- Alignment of data protection controls to evolving business and regulatory requirements



Deployment: illustrative team structure

Zscaler account sponsor

Zscaler DLP subject-matter resource (SMR)

EY core delivery team

EY engagement partner

EY operations lead

EY execution team

EY onshore team

- Engagement manager
- DLP compliance specialist

EY offshore team

- DLP solution architect
- DLP operations SMR
- DLP operation analyst

Client executive sponsor

Client DLP operations leads

EY pillar leads (cloud, AppSec, data protection, etc.)

4

Case study

Use case: Financial services client

Client: Financial company
Service: DLP
Industry: Financial services

Business drivers:

- The EY team was engaged by the client to make impactful and tangible improvements to their DLP program and enhance its current capabilities, the desire was to protect the information crown jewels and the data protection drivers to maintain control of personal data.
- The program enabled rapid assessment and developed policies and procedures to support the client's DLP program to identify and secure sensitive data (PCI and PII) and track National IDs.
- The client needed to prioritize DLP action plans and implement enhanced capabilities and plan for future improvements and identify automation opportunities to reduce manual task.

EY services:

- Created rules and policies to discover sensitive data like PCI, PII, etc.
- Created regex to identify the National IDs.
- Created Exact Data Matching (EDM) and Indexed Document Matching (IDM) fingerprinting policies to overcome difficulties to track source code data.
- Created watermarking policy to detect the sensitive-marked document.
- Performed incident triaging of the incidents generated.
- Performed business impact analysis (BIA) of the incidents.
- Reduced the false positive incidents from 85% to 3% and enabled block mode for high-severity incident to prevent the data loss.

Value delivered:

- Enabled the discovery of sensitive data in client's environment.
- Implemented DLP policies and rules to protect payment card information (PCI) and PII data, such as National IDs, which was the key concern of the client.
- Enabled DLP blocking policies to prevent high-severity/crown jewel data from leaving organization boundaries.
- Enabled tracking of client's source code data.
- The sensitive documents, which were labeled or marked as not to be sent out of the organization were successfully detected.
- Reduced work and time spent by the security operations center (SOC) team by reducing false positives.
- Created tailored policies for employees exiting organization.

Use case: Large pharmaceutical client

Client: Large multinational pharmaceutical company, Fortune 500
Service: Zscaler accelerate engagement
Industry: Healthcare

Business drivers:

- A global pharmaceutical company, having already implemented Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), was seeking to enhance their data protection strategy by integrating Zscaler DLP solutions to achieve more comprehensive coverage and improved compliance.

EY services:

- The EY team was engaged by the client to provide execution support for their global program based on its proven methodology, demonstrable implementation skills and comprehensive Zscaler implementation experience:
  - Supported the integration of Zscaler DLP with ZIA and ZPA, providing a unified security posture and centralized management for policy configuration.
  - Drafted an architecture blueprint to enable the client to leverage Zscaler's DLP for endpoint data protection.
  - Conducted policy review and identified risk areas and created granular policies tailored to specific data types and user roles for precise data control.
  - Worked with clients in achieving compliance with data protection regulations and helped implement monitoring solution.

Value delivered:

- Performed gap analyses on DLP controls and supported clients in applying risk-based proactive approaches.
- Supported the seamless integration of the Zscaler DLP solution with client's existing Zscaler Zero Trust environment.
- Implemented ongoing monitoring to evaluate the effectiveness of the DLP policies and the performance of Zscaler, enabling real-time adjustments.

5

EY contacts

EY contacts for an initial data protection discussion

Nick Granack

Managing Director, Cybersecurity
Ernst & Young LLP

nick.granack@ey.com

Kendra Hodge

Senior Manager, Cybersecurity
Ernst & Young LLP

kendra.l.hodge@ey.com

Belle Chu

Senior Manager, Cybersecurity
Ernst & Young LLP

belle.chu@ey.com

Hasaan Shah

Senior, Cybersecurity
Ernst & Young LLP

hasaan.shah@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

2602-10747-CS
ED None

ey.com