IT-Security
Roadshow 2026

zscaler™

Datenschutz & GenAI-Sicherheit

Zscaler KI als Antwort auf die neuen Herausforderungen – effizient, kostensparend, schützend.

Mike Schumak
Partner Consulting Sales Engineer, Zscaler

3. März 2026 , München

Forward-Looking Statements

This presentation has been prepared by Zscaler, Inc. (“Zscaler”) for informational purposes only and not for any other purpose. Nothing contained in this presentation is, or should be construed as, a recommendation, promise or representation by the presenter or Zscaler or any officer, director, employee, agent or advisor of Zscaler. This presentation does not purport to be all-inclusive or to contain all of the information you may desire.

This presentation contains forward-looking statements. All statements other than statements of historical fact, including statements regarding our planned products and upgrades, business strategy and plans and objectives of management for future operations of Zscaler are forward-looking statements. These statements involve known and a significant number of unknown risks, uncertainties, assumptions and other factors that could cause results to differ materially from statements made in this message, including any performance or achievements expressed or implied by the forward-looking statements. Moreover, we operate in a very competitive and rapidly changing environment, and new risks may emerge from time to time. It is not possible for us to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results or outcomes to differ materially from those contained in any forward-looking statements we may make. Additional risks and uncertainties that could affect our financial and operating results are included in our most recent Quarterly Report on Form 10-Q filed with the Securities and Exchange Commission (“SEC”), which is available on our website at ir.zscaler.com and on the SEC's website at www.sec.gov.

In some cases, you can identify forward-looking statements by terms such as “anticipate,” “believe,” “continues,” “contemplate,” “could,” “estimate,” “expect,” “explore” “intend,” “likely,” “may,” “plan,” “potential,” “predict,” “project,” “should,” “target,” “will” or “would” or the negative of these terms or other similar words. Zscaler based these forward-looking statements largely on its current expectations and projections about future events that it believes may affect its business. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements. All forward-looking statements in this message are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

Plattform

Was macht Zscaler?

Secure Public AI with Shadow AI visibility, Data Protection and Guardrails

Generative AI:

Types of risks

- Access to risky AI apps
- AI misuse – sensitive topics, injection, prompt, harmful prompts
- Confidential data/PII leakage

Visibility & Governance

Shadow AI

AI apps used in env

Embedded AI

AI embedded in SaaS

Prompt Visibility

Capture and classify prompts

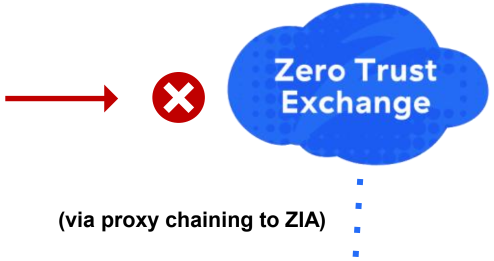
Protection

Data Loss Prevention

Detect/block PII, Confidential data

Browser Isolation

Prevent copy-paste of sensitive data



(via proxy chaining to ZIA)

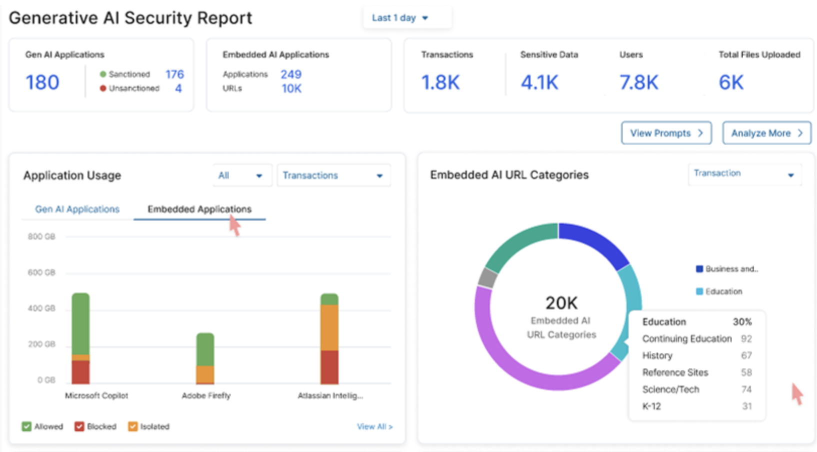
Guardrails (AI Guard)

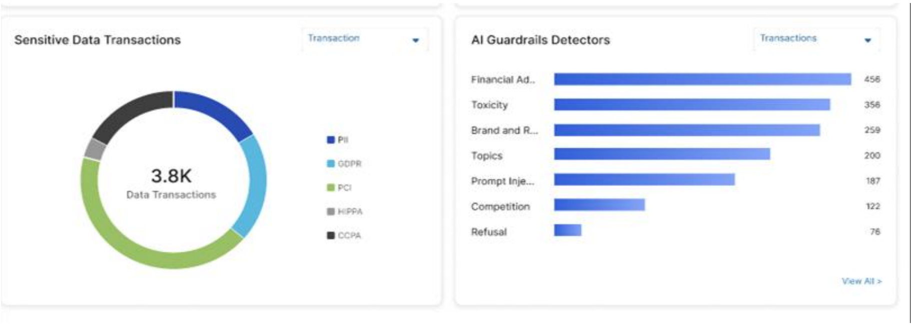
Responsible AI

(e.g. toxic or harmful prompts)

Intent Based Detection

(e.g. legal or financial advice, competition)





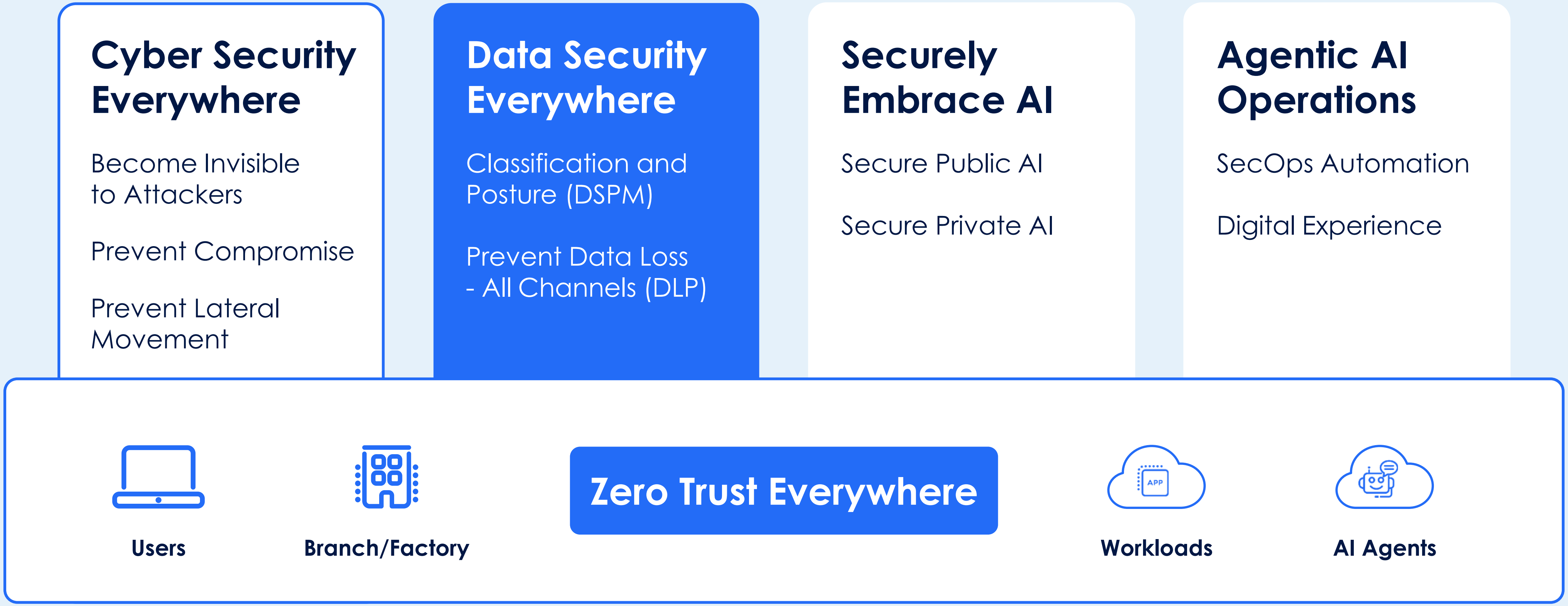
Best Practices on Approaching Gen AI Control

Block
Unsanctioned /
High Risk
AI Apps

Isolate
Questionable Gen
AI Apps to control
interactions

Monitor
Sanctioned AI
Apps with DLP controls

Data Security in the Zscaler Ecosystem



Cyber Security Everywhere

Become Invisible to Attackers

Prevent Compromise

Prevent Lateral Movement

Data Security Everywhere

Classification and Posture (DSPM)

Prevent Data Loss - All Channels (DLP)

Securely Embrace AI

Secure Public AI

Secure Private AI

Agentic AI Operations

SecOps Automation

Digital Experience

Zero Trust Everywhere

Users

Branch/Factory

Workloads

AI Agents

Securing Your Critical Data is Harder Than Ever

Data Sprawl

Data is the fastest growing resource

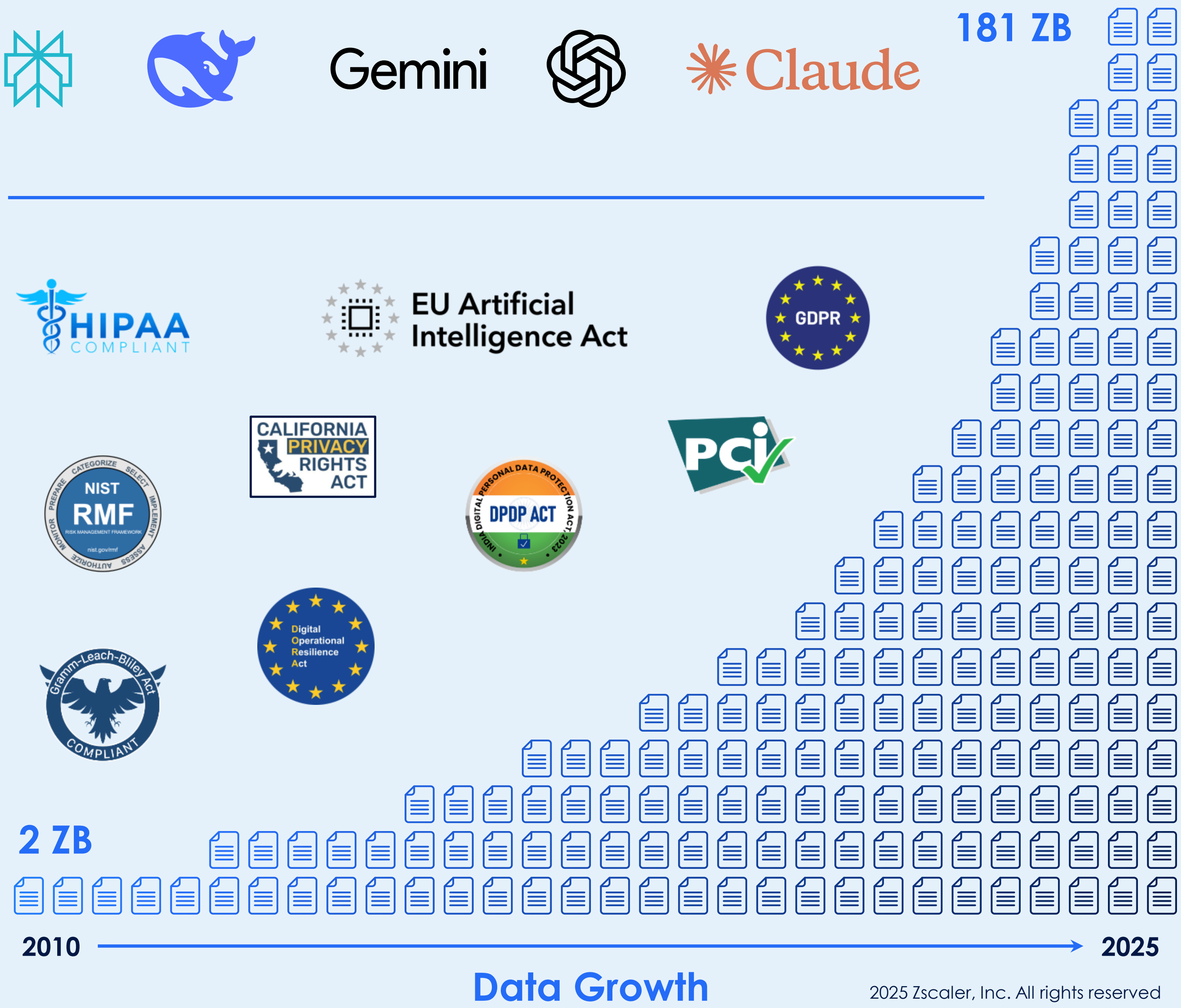
Regulatory Complexity

New regulations are constantly emerging

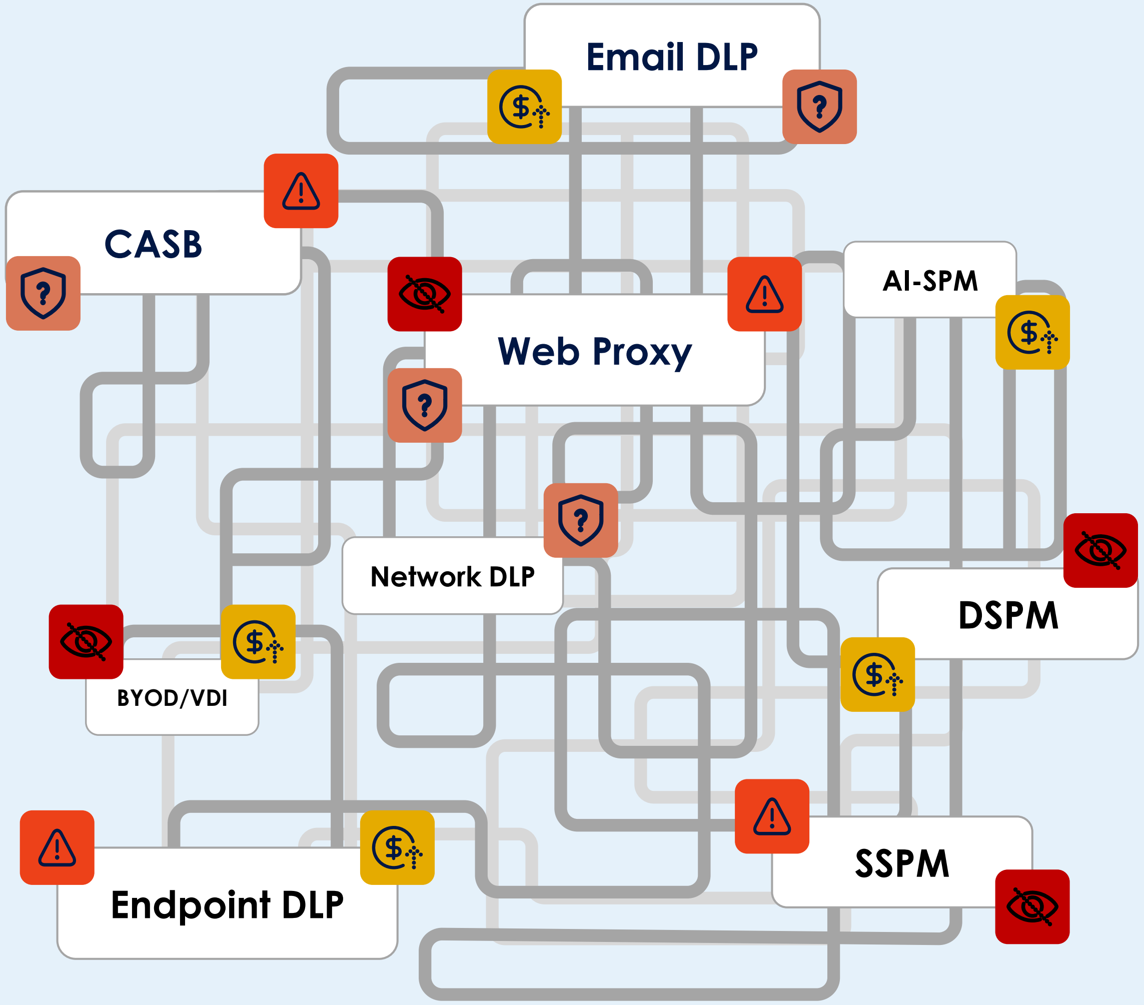
GenAI Emergence

Rapid adoption without data controls

Can you ensure compliance & prevent exposure?



Legacy Point Products Don’t Work



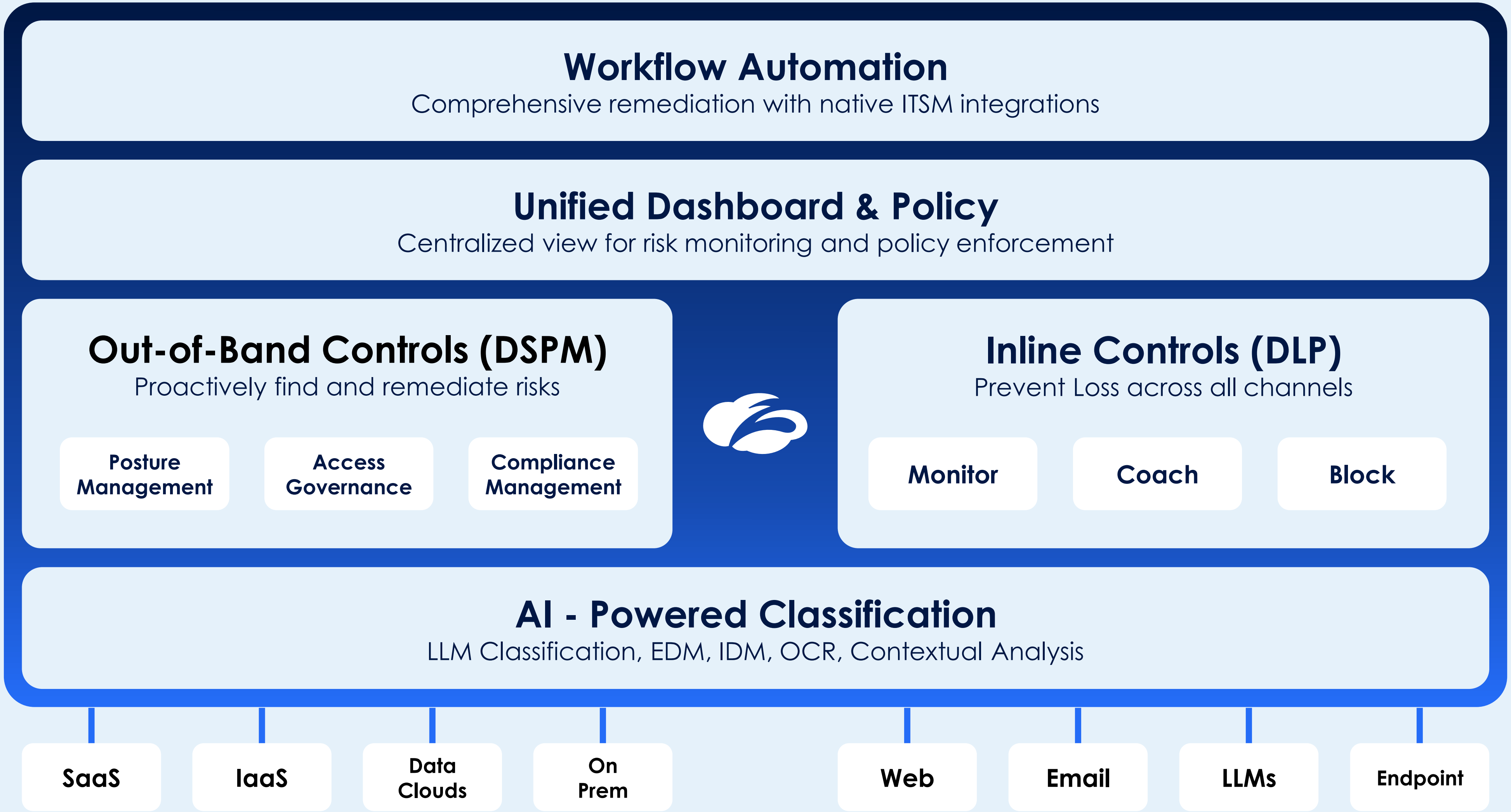
Lack of Visibility
Disjointed tools leave sensitive data blind spots

Excessive Alerting
Excessive false positives and alerts increase OpEx

Inefficient Operations
Inflexible workflows from multiple DLP policies

Costly & Complex
Lack of agility from disjointed approaches

Zscaler's Platform Provides Unified Data Security



Workflow Automation
Comprehensive remediation with native ITSM integrations

Unified Dashboard & Policy
Centralized view for risk monitoring and policy enforcement

Out-of-Band Controls (DSPM)
Proactively find and remediate risks

- Posture Management
- Access Governance
- Compliance Management

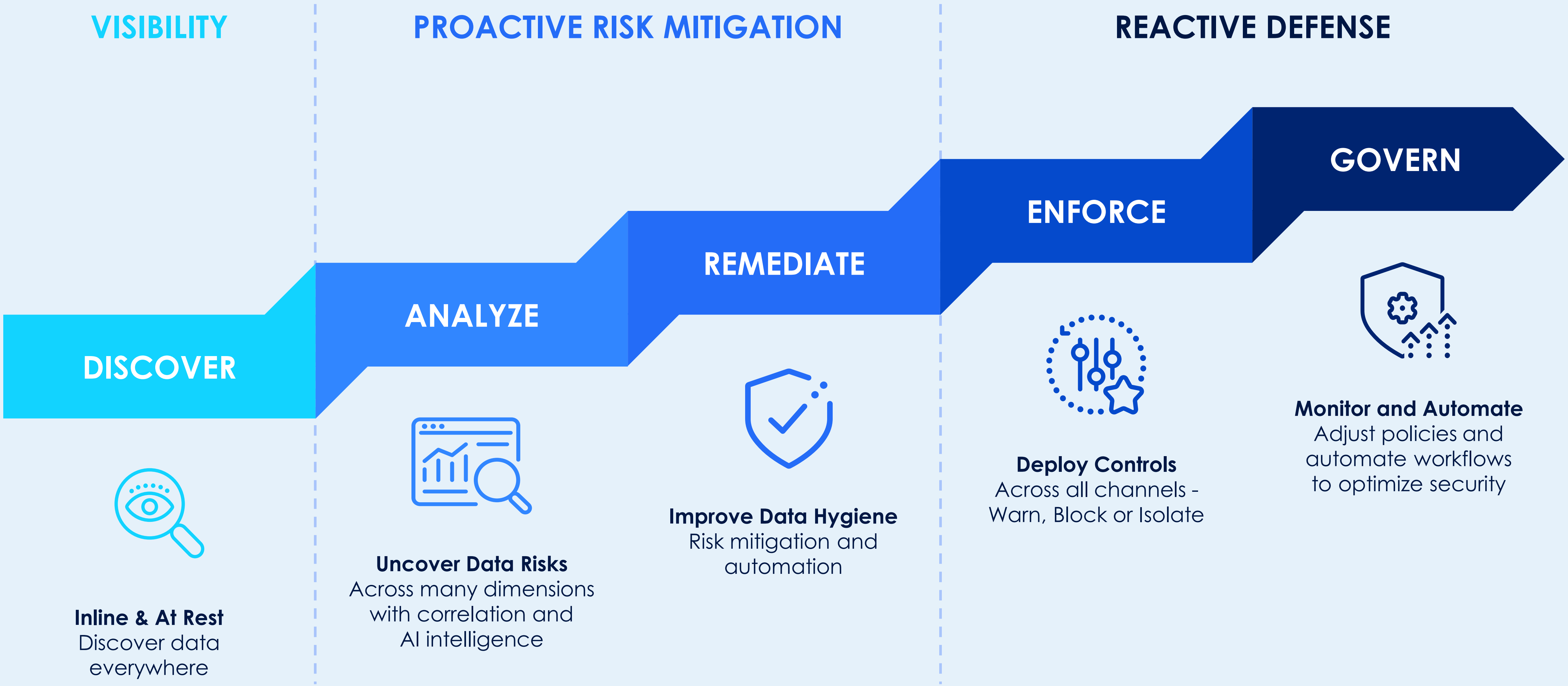
Inline Controls (DLP)
Prevent Loss across all channels

- Monitor
- Coach
- Block

AI - Powered Classification
LLM Classification, EDM, IDM, OCR, Contextual Analysis

SaaS · IaaS · Data Clouds · On Prem · Web · Email · LLMs · Endpoint

The Ideal Data Security Journey



VISIBILITY

DISCOVER

Inline & At Rest
Discover data everywhere

PROACTIVE RISK MITIGATION

ANALYZE

Uncover Data Risks
Across many dimensions with correlation and AI intelligence

REMEDIATE

Improve Data Hygiene
Risk mitigation and automation

REACTIVE DEFENSE

ENFORCE

Deploy Controls
Across all channels - Warn, Block or Isolate

GOVERN

Monitor and Automate
Adjust policies and automate workflows to optimize security

AI-Powered Classification: The Foundation of Data Security

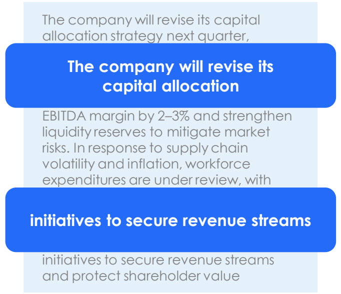
Powerful Classification Everywhere

Data Sources:

- SaaS
- IaaS
- Web
- Endpoint
- Email
- On Prem
- Data Clouds
- LLMs

LLM Classification

Reads language and understand intent



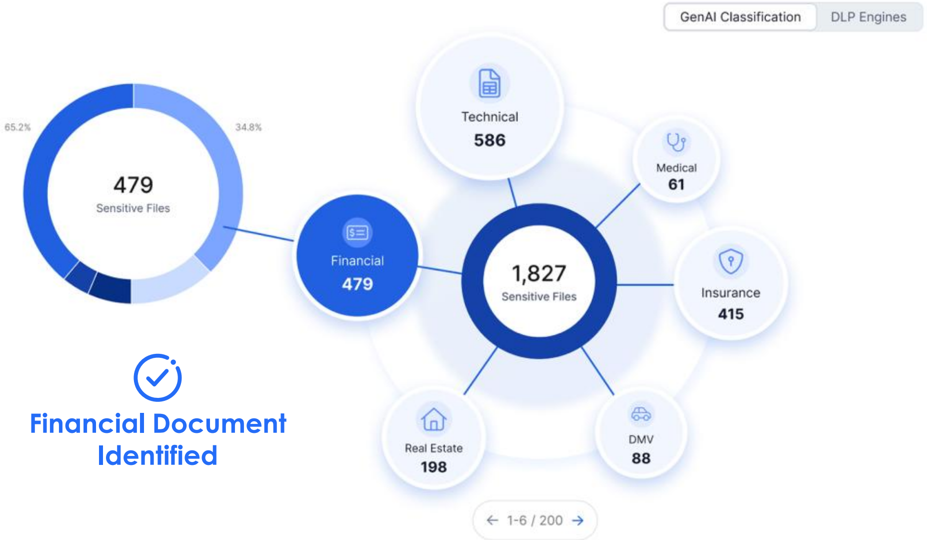
The company will revise its capital allocation strategy next quarter,

The company will revise its capital allocation

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

initiatives to secure revenue streams

initiatives to secure revenue streams and protect shareholder value



Financial Document Identified

Advanced Classification

Exact Data Match (EDM)
Structured custom data

Indexed Document Matching (IDM)
Custom docs & forms

Optical Character Recognition (OCR)
Screenshots & images

Regex, Labeling and Contextual

DLP Dictionaries
100+ pre-defined and customizable

Microsoft Purview Labeling
Update missing sensitivity labels

90k+ Shadow IT Catalog
Find risky apps across 75+ attributes

Proactively Discover & Mitigate Data Risks

Key Highlights

AI-Powered Classification

- Improved accuracy and simplicity
- Unified across all channels

Posture Management

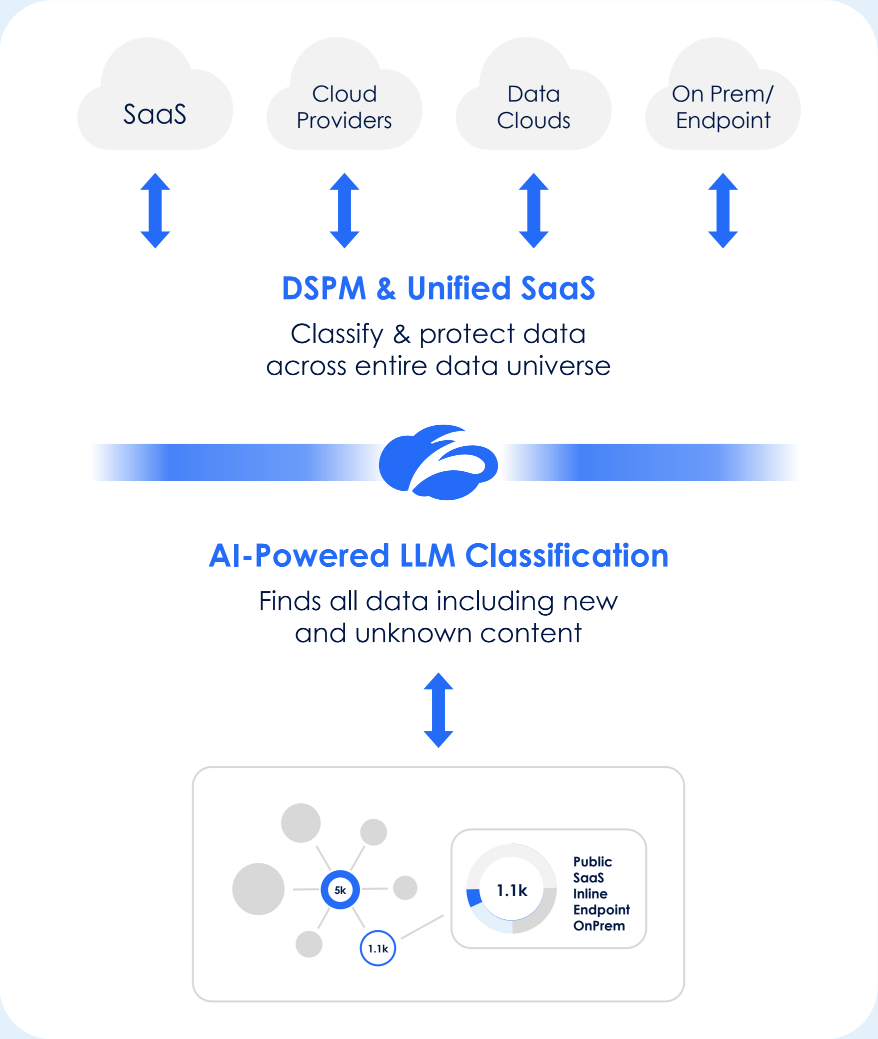
- Track posture & supply chain risks
- Prioritize and guide remediation

Access Governance

- Identify access risk to data
- Automate with ITSMs

Compliance Assessment

- NIST, GDPR, PCI & other frameworks
- Audit, report, and remediate gaps



DSPM & Unified SaaS

Classify & protect data across entire data universe

AI-Powered LLM Classification

Finds all data including new and unknown content

Benefits

Platform Approach

Unifies DSPM and Inline DLP for a complete solution

Comprehensive Visibility

See all data without additional tools

Proactive Risk Mitigation

Close dangerous gaps before data loss occurs

Governance & Compliance

Prioritize and mitigate risk against common frameworks

Safely Embrace AI While Protecting Data

Key Highlights

Control Use of AI (Gen-AI)

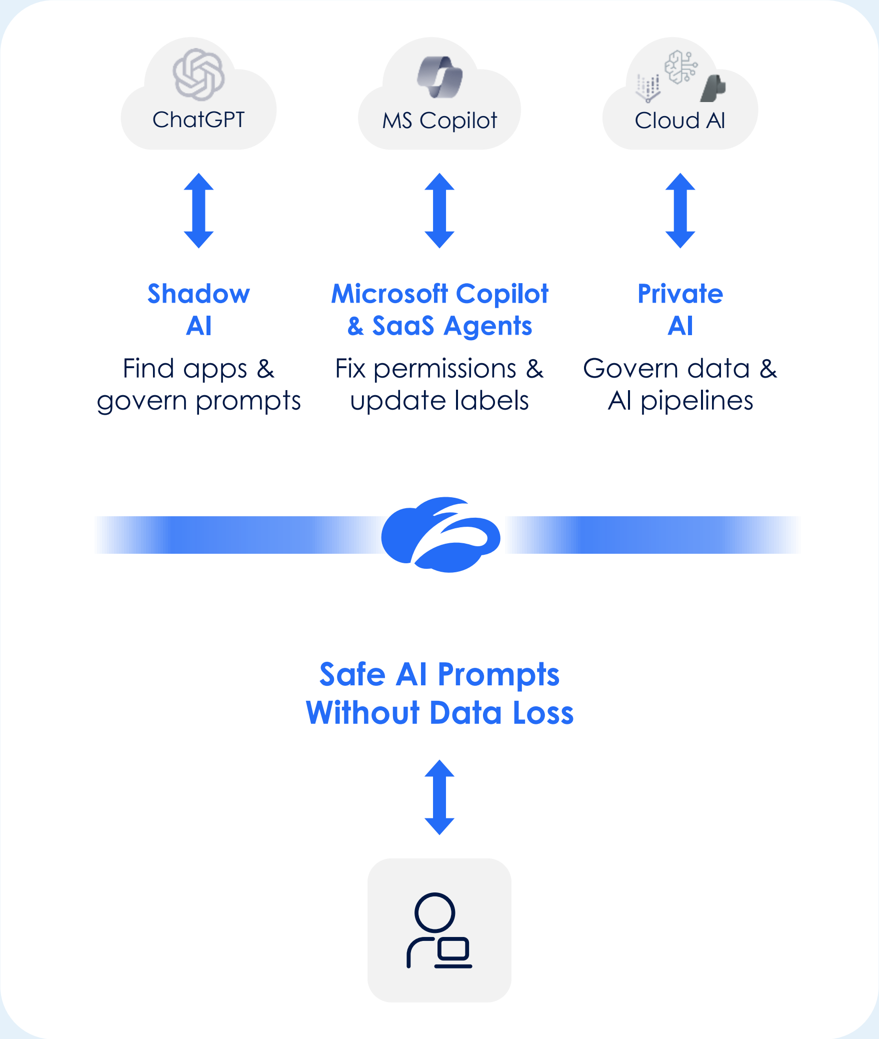
- Shadow AI & risk visibility
- Prompt visibility & controls

Protect Data Used for AI (DSPM)

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

Govern AI Systems (AI-SPM)

- Assess AI models & services
- Secure AI data pipelines


ChatGPT
MS Copilot
Cloud AI
Shadow AI
Find apps & govern prompts
Microsoft Copilot & SaaS Agents
Fix permissions & update labels
Private AI
Govern data & AI pipelines
Safe AI Prompts Without Data Loss

Benefits

Accelerate AI Initiatives

Gain visibility & 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

Retire Legacy DLP Complexity with a Modern, Unified Platform

Key Highlights

Unified Classification

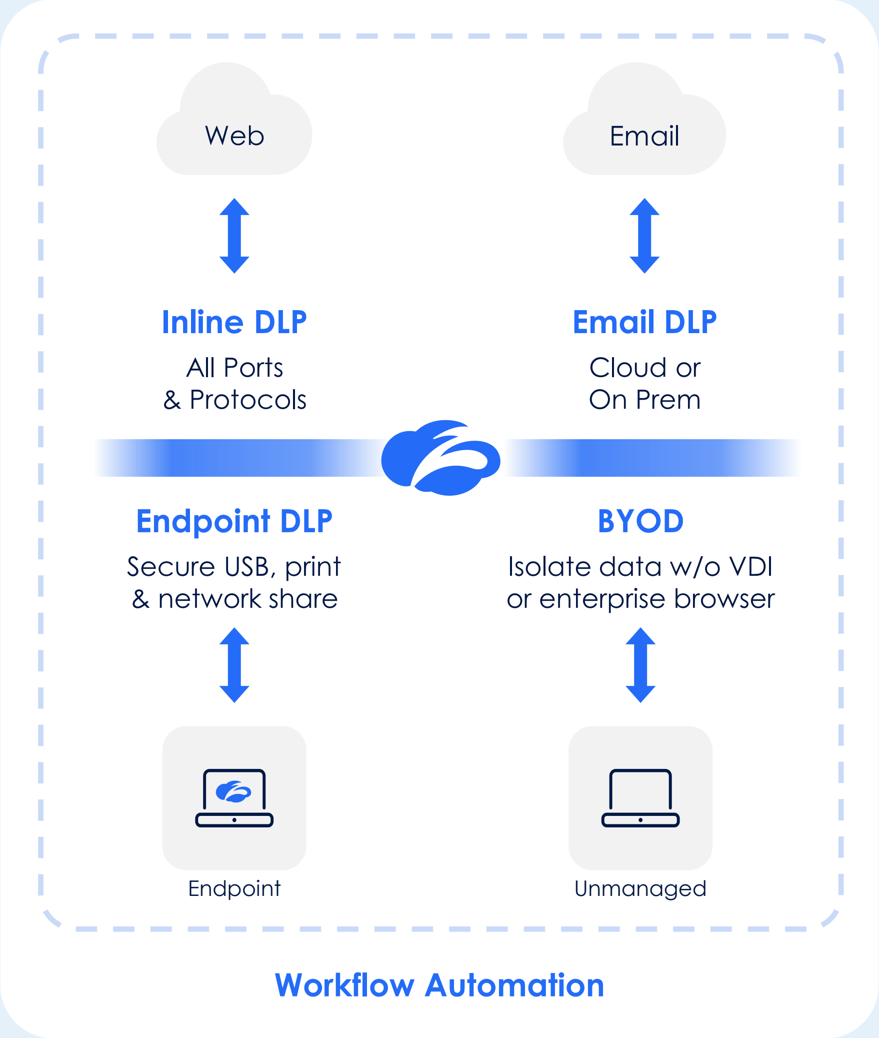
- All channels: In Motion & At Rest
- AI-Powered: LLM Classification
- Adv. Classification: EDM, IDM, OCR
- PII, PCI, PHI, 100+ more
- Regex, Proximity, & ML-based

Contextual Analysis

- File type, cloud app, tenancy
- Adaptive Risk Profiling & UEBA

Workflow Integration

- Microsoft tag enforcement (MIP)
- Unified Incident Management
- Workflow integrations with ITSMs



Inline DLP
All Ports
& Protocols

Email DLP
Cloud or
On Prem

Endpoint DLP
Secure USB, print
& network share

BYOD
Isolate data w/o VDI
or enterprise browser

Workflow Automation

Benefits

Cut Costs & Simplify

Cloud-delivered approach for consistent DLP across channels

Simplify the Endpoint

Eliminate agents and deliver a seamless user experience

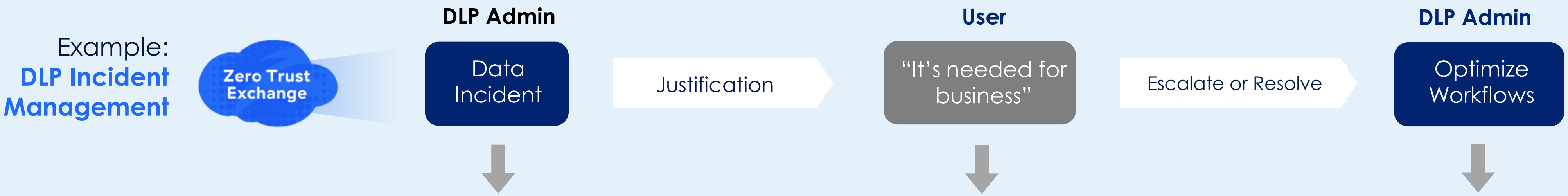
Boost Performance

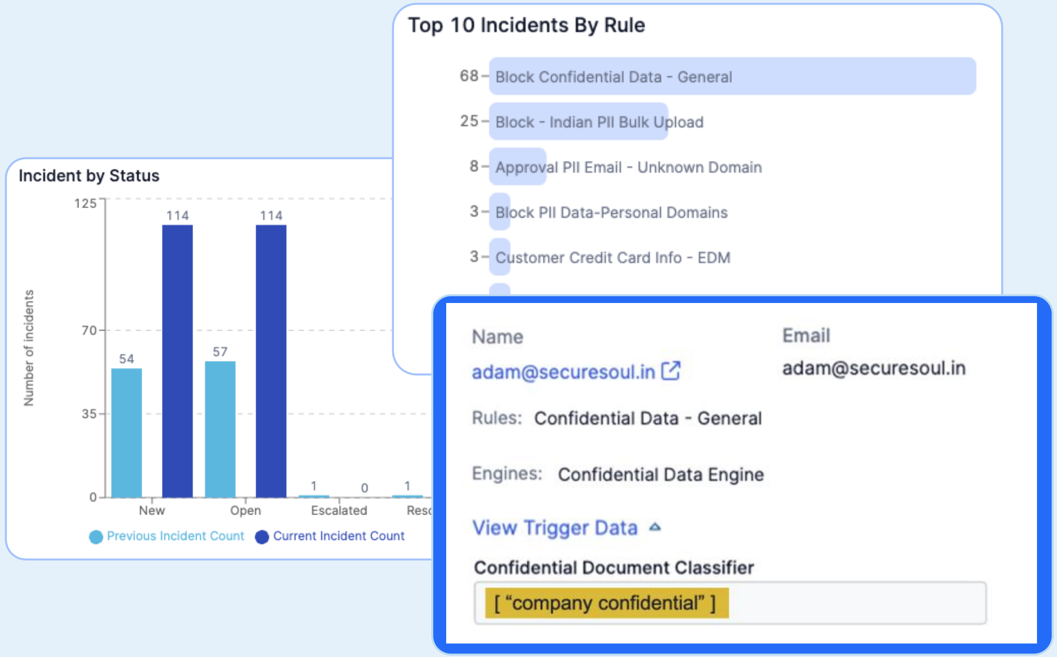
Proven SSL proxy inspection without patching requirements

Automate Workflows

Streamline ops with automated workflows and user coaching

Operationalize Data Security with Workflow Automation





Top 10 Incidents By Rule

68 – Block Confidential Data - General

25 – Block - Indian PII Bulk Upload

8 – Approval PII Email - Unknown Domain

3 – Block PII Data-Personal Domains

3 – Customer Credit Card Info - EDM

Name	Email
adam@securesoul.in	adam@securesoul.in

Rules: Confidential Data - General

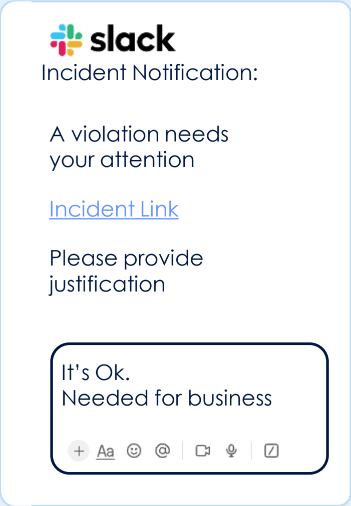
Engines: Confidential Data Engine

View Trigger Data

Confidential Document Classifier

["company confidential"]

See Incidents, Triggers and Response Trends



slack

Incident Notification:

A violation needs your attention

Incident Link

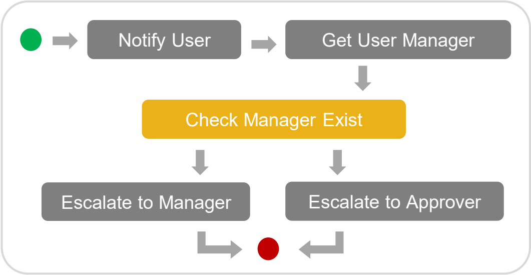
Please provide justification

It's Ok.
Needed for business

Engage & coach users

(Slack, Teams or Email)

✓ **Accelerate response with Automation**



✓ **Assign for User Training**

✓ **Assign for Policy Exception**

✓ **Integrate with ITSM Workflows**

Customers Worldwide are seeing Zscaler Data Protection Value

3x
faster deployment than previous approaches
AutoNation

92%
of encrypted traffic inspected
JOHN HOLLAND

250k
risks blocked each month
MGM RESORTS

25›95%
improvement in resolving cases
ciena

$875m
cost savings from product consolidation
STATE OF OKLAHOMA

513.2m
policy violations prevented in just 90 days
CUSHMAN & WAKEFIELD

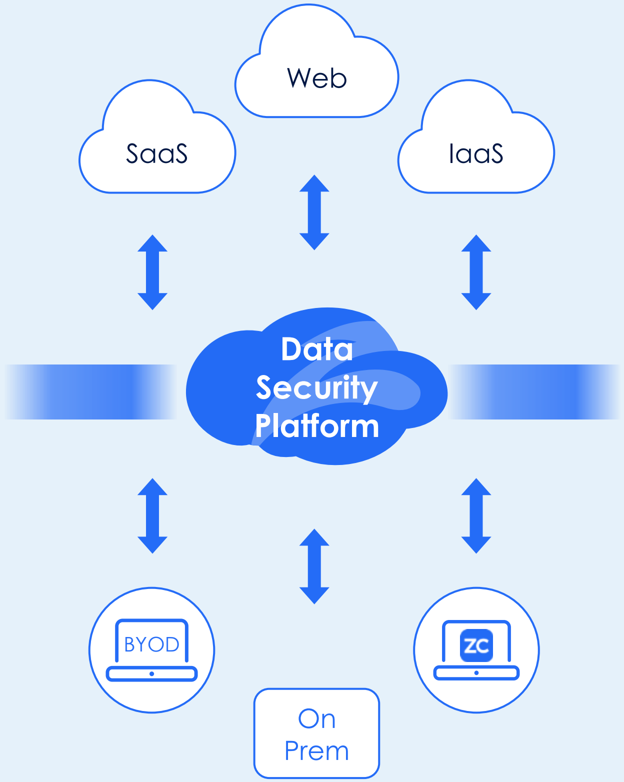
210TB
of encrypted traffic inspected in one quarter
SICK Sensor Intelligence.

100%
of organization protected
MERCURY FINANCIAL

62%
improvement in issue resolution
careem

90%
reduction in infrastructure complexity
CSC Commonwealth Superannuation Corporation

What Makes Zscaler Data Security Unique?



DSPM + DLP + AI-Powered Classification

Everything you need in one unified platform

Secure All Data Channels

Scale protection everywhere - data in motion and at rest

Automate Workflows & Operations

Integrated workflow automation to accelerate incident response

Proven Inline Proxy

Over 4,000 customers inline with real-time data protection

GenAI Security Risk Assessment

Gear up and learn if you're AI-battle ready.
Sign up for our GenAI risk assessment.

Benefits of the Assessment:

- **Shadow AI:** Uncover which apps, users and data are being used.
- **Sensitive Data:** In depth analysis that identifies sensitive data shared with GenAI.
- **Prompt Analysis:** Capture prompts to understand how users are leveraging GenAI.

Come to out both and sign up for you GenAI Security Risk Assessment

Your Zscaler Channel Team

Nicolai Stößer

Michael Schumak

IT-Security
Roadshow 2026

Danke für Ihre Aufmerksamkeit.