Modernize Data Resilience

Wipro CyberTransform℠ and Zscaler Data Security Platform

As businesses accelerate their reliance on complex digital ecosystems, security has evolved from local enforcement to a global imperative for data governance. In today's hybrid world, organizations must secure data across on-premises and cloud environments while navigating increasingly complex AI environments and stringent regulatory standards. To maintain data integrity and prevent accidental or malicious exposure, a proactive data protection strategy is no longer optional; it is a foundational requirement for the modern enterprise.

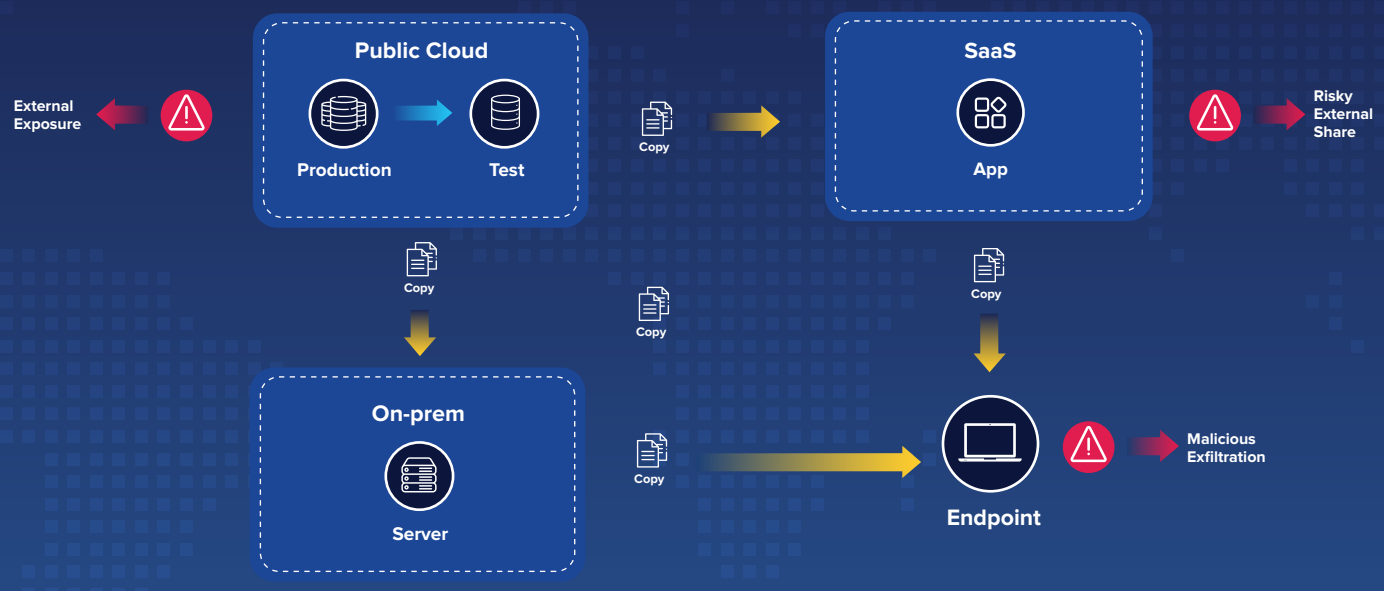


Fig: Modern Data Security Challenges

However, technology alone is not a silver bullet. Success requires a trusted partner who understands the nuances of the enterprise environment to evaluate, architect, and manage a platform tailored to specific business requirements and governance standards. This strategic oversight is especially vital as Generative AI tools enter the mainstream. While these tools foster unprecedented innovation and efficiency, they simultaneously escalate the risk of sensitive data exposure, making a robust security framework a foundational requirement.

Why Legacy Security is Failing

While the mandate for strategic data resilience is clear, legacy security models struggle to overcome fundamental challenges:

Limited visibility and control

Most legacy data security tools cannot connect to and discover sensitive data across all data sources - on-prem repositories, cloud infrastructure, SaaS applications, and data lakes. Without comprehensive discovery and classification of data at rest everywhere, organizations lack the foundational context needed to enforce granular controls and make informed security decisions.

Generative AI as a Data Loss Channel

Wipro implements specific Generative AI guardrails and governance protocols to ensure trade secrets are never ingested by external LLMs, going beyond simple 'blocking' to true IP governance. When organizations lack complete, accurate, and up-to-date discovery, classification, and labeling of their sensitive data, they cannot enforce controls that prevent that data from flowing into public LLMs. Many large language models use content from prompts as training data - making undiscovered, unclassified sensitive data an emerging and silent exfiltration risk.

Protection gaps

There are multiple DLP (Data Loss Prevention) and SWG (Secure Web Gateways) tools in the market and security monitoring platforms that only address specific aspects of data protection. Gaps between tools and teams lead to redundant processes, a lack of visibility, insufficient data exposure controls across environments, and bloated operational overhead.

User experience

Legacy security architectures use centralized appliances to divert traffic that can degrade performance, often resulting in poor user experience. Scaling such systems to accommodate the number of users as a business grows, causing challenges for IT & Information Security.

The Mandate for Strategic Data Resilience

Today, data is more fluid than ever, dispersed across cloud apps, unmanaged devices, and generative AI. These modern and diverse data environments need data protection solutions designed for performance and scalability across all data channels, ensuring users and systems can securely access data without impeding productivity. In distributed work environments these solutions can handle data protection across on-premises systems, private networks, and third-party applications.

To address these challenges, organisations can adopt zero trust principles, to secure data access based on context, such as user identity, device status, and application behavior before allowing any connection. Zero Trust approach mitigates risks by ensuring that only entities explicitly permitted by company policy based on identity can gain access to sensitive information.

A Unified Architecture for Global Data Governance

Wipro and Zscaler bring together complementary strengths to address global data governance. Zscaler's cloud-native Zero Trust platform enables inline data protection across web, SaaS, private applications, and endpoints, eliminating reliance on legacy appliances. Wipro complements this with deep expertise in data security transformation, helping organizations design, integrate, and operationalize security frameworks aligned to business and regulatory needs. Together, the joint solution enables a unified, scalable, and future-ready data security architecture.

Wipro CyberShield: Scaling Trust Across the Enterprise

Managed Data Visibility:

Wipro leverages AI-driven automation to discover and classify sensitive data across the hybrid landscape, establishing a foundation for zero-trust governance.

Active Posture Governance

Utilizing DSPM to proactively identify and remediate data risks, ensuring continuous compliance with global regulatory frameworks.

Intelligence-Driven Resilience

A "closed-loop" response strategy that bridges posture insights with real-time enforcement to adapt to evolving enterprise risk.

Strategic AI Guardrails:

Wipro governs the secure adoption of Generative AI, implementing inline protections and browser isolation to prevent sensitive data leakage into LLMs.

Zscaler's platform unifies data security into a single architecture built on three integrated layers:

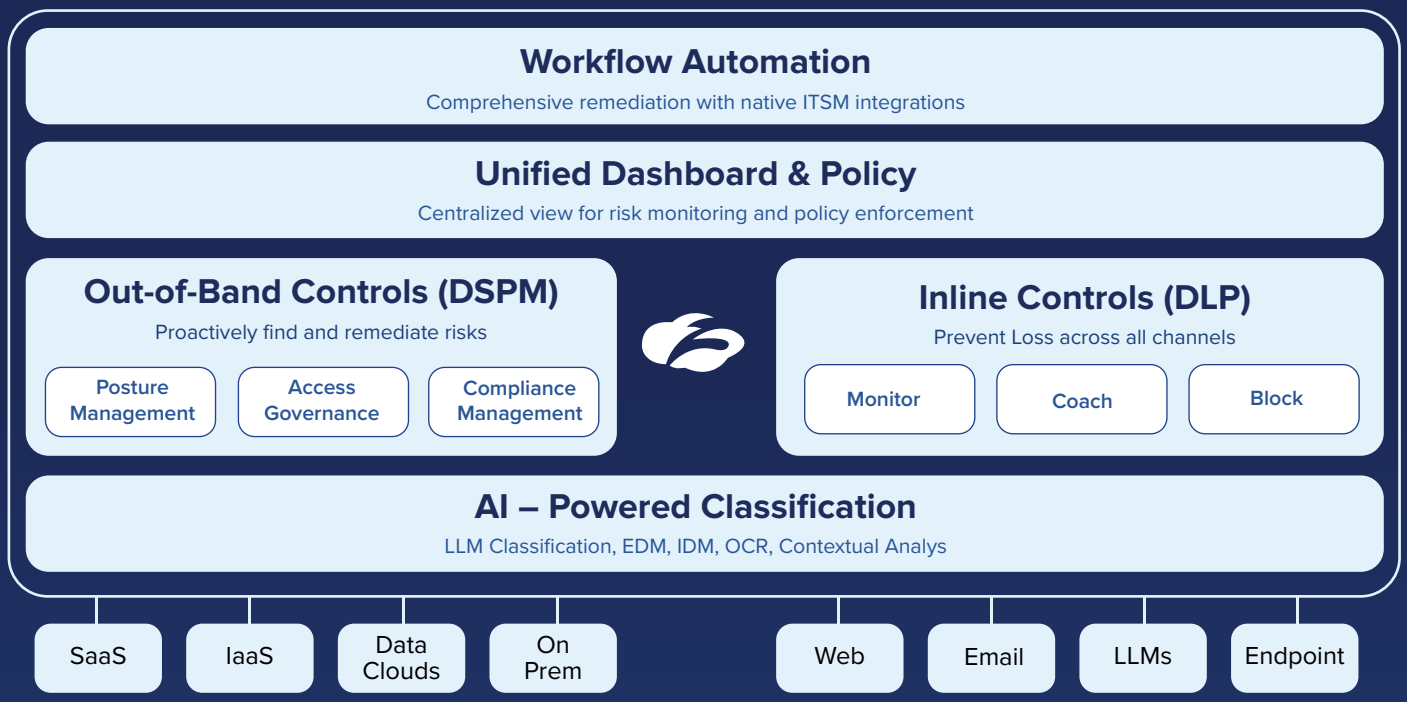


Fig: Zscaler Unified Data Security Platform

01 AI-Powered Classification (Foundation): A shared engine - leveraging AI classification, EDM, IDM, OCR, and contextual analysis - that classifies data both at rest and in motion, ensuring consistent visibility regardless of where data lives or moves.

02 Dual Control Modes

a. Out-of-Band (DSPM): Proactively discover, classify, govern access, assess risk, and remediate - across SaaS, IaaS, data clouds, and on-prem.

b. Inline (DLP): Prevent data loss in real time — detect, coach, block, and investigate - across web, email, LLMs, and endpoints.

03 Adaptive Data Defense (Intelligence Layer): Bridges DSPM and DLP through agentic workflows, dynamic policies, risk scoring & analytics, and unified data lineage — staying ahead of evolving risk and accelerating response.

Powerful Classification Everywhere

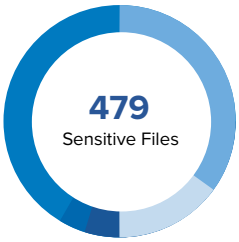
Data Sources:

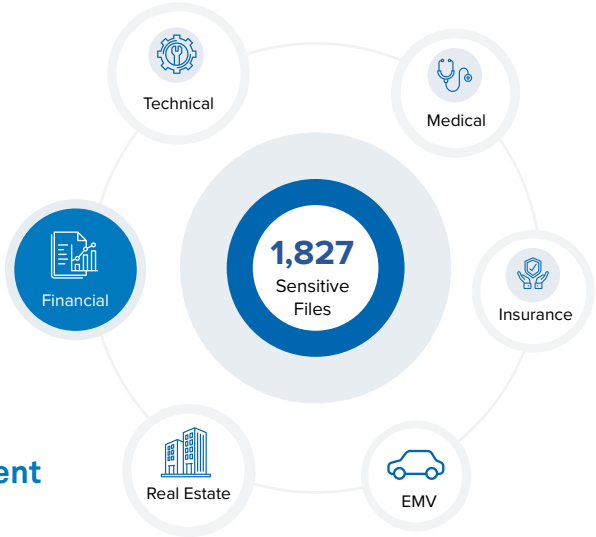
- SaaS
- IaaS
- Web
- Endpoint
- Email
- On Prem
- Data Clouds
- LLMs

LLM Classification

Reads language and understand intent

- The company will revise its capital allocation
- Initiatives to secure revenue streams





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

Agentic Policy & Workflow Automation

Zscaler Inline DLP
Data At Rest, Everywhere

Data Landscape Intelligence & Context

Zscaler Inline DLP
Data In Motion, All Channels

Data Signal & Evidence Sharing

The Benefits of Adaptive Data Defense

- Predict & Stop Insider Risk
- Get Visibility of Data Lineage
- Enable Alert Auto Tuning

Fig: Adaptive Data Defense: Automated Response to Changing Risk

By integrating Wipro's CyberShield framework with the Zscaler's Zero Trust platform, organizations can enforce consistent governance wherever data moves—ensuring visibility and control across even the most distributed environments. This joint offering eliminates traditional data silos, enabling enterprises to detect and classify sensitive information regardless of its format or location. From structured databases to unstructured cloud documents, the solution ensures that no data goes untracked, providing the strategic resilience required for the modern enterprise.

Together, these layers deliver four outcomes: **make data AI-ready, prevent data loss, reduce data exposure, and ensure compliance.**

Operational Simplicity with Zero Trust

The hallmark of this solution is simplicity. While traditional classification tools require elaborate integrations and constant rule refinement, this solution applies Zero Trust principles to automatically enforce policies.

By leveraging AI/ML this solution can analyze vast amounts of data to detect anomalies, identify vulnerabilities, and predict potential security incidents before they occur. By automating threat detection and response, AI and ML help organizations stay ahead of increasingly sophisticated cyberattacks.

Further, this solution allows creating and enforcing policies around the generative AI tools enterprise users can access and how they can interact, directly or via browser isolation, to protect sensitive data.

CyberTransform: Strategic Implementation and Managed Outcomes

As organizations adopt AI at scale, governance becomes central to data security. Regulatory frameworks such as the EU AI Act and NIST AI RMF emphasize risk-based classification, transparency, accountability, and continuous monitoring.

The joint Wipro–Zscaler solution enables organizations to operationalize these principles and embed governance controls directly into the security fabric. This ensures that AI adoption is not only secure but also auditable and compliant with global regulatory expectations.

While Zscaler provides the cloud-native platform, Wipro ensures successful enterprise transformation and adoption to ensure data security scales effectively across geographies and environments:

Assessment
Understanding the data landscape, risks, and compliance requirements.

Implementation
Deployment and integration of Zero Trust data protection architectures.

Managed Services
Continuous monitoring, policy optimization, and incident response.

Leveraging a global delivery footprint, an extensive talent pool, and strong ecosystem alliances, Wipro delivers the following strategic business outcomes:

Risk & Compliance:

Significantly reduces the probability of a data breach and the associated legal or financial liabilities.

Operational Efficiency:

Delivers a major reduction in Mean Time to Respond (MTTR) through automated incident management. Using workflow automation, admins can review and remediate data security incidents globally from a single, closed-loop location.

TCO Optimization

Minimizes the cost of legacy appliance stacks and isolated point solutions, with potential annual security benefits reaching hundreds of thousands of dollars.

Safe Innovation

Enables the enterprise to adopt Generative AI safely by ensuring sensitive data is never leaked into public LLMs.

User Experience

Improves employee productivity by unifying AI-powered root cause analysis with deep telemetry. IT teams can quickly detect and resolve issues across the entire network path, ensuring a seamless experience from any device or location.

Driving Strategic Resilience: The Path Forward

The path to comprehensive data resilience isn't just about finding data, it's about governing it with confidence. By unifying Wipro's CyberTransform℠ methodology with the Zscaler AI-powered platform, organizations no longer have to choose between speed and security. We deliver a unified, CyberShield-managed architecture that automates the complex task of data discovery and classification, while aligning every action to specific business and regulatory requirements. Together, Wipro and Zscaler empower organizations to eliminate data silos, mitigate risk, and accelerate digital transformation with a security-first mindset.

Call to Action

Ready to transform your data approach? Discover how Wipro and Zscaler can help your organization secure data across hybrid environments, enable responsible AI adoption, and build a resilient, Zero Trust–driven security posture for the future. Learn more today.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading AI-powered technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our consulting-led approach and the Wipro Intelligence™ unified suite of AI-powered platforms, solutions, and transformative offerings, we help clients realize their boldest ambitions to build intelligent and sustainable businesses.

The Wipro Innovation Network – part of the Wipro Intelligence™ suite – underpins our commitment to client-centric co-innovation and co-creation by bringing together capabilities from the innovation labs and partner labs, academia, and global tech communities. With over 240,000 employees and business partners across 65 countries, we deliver on the promise of helping our customers, colleagues, and communities thrive in an ever-changing world.

For additional information, visit us at www.wipro.com