

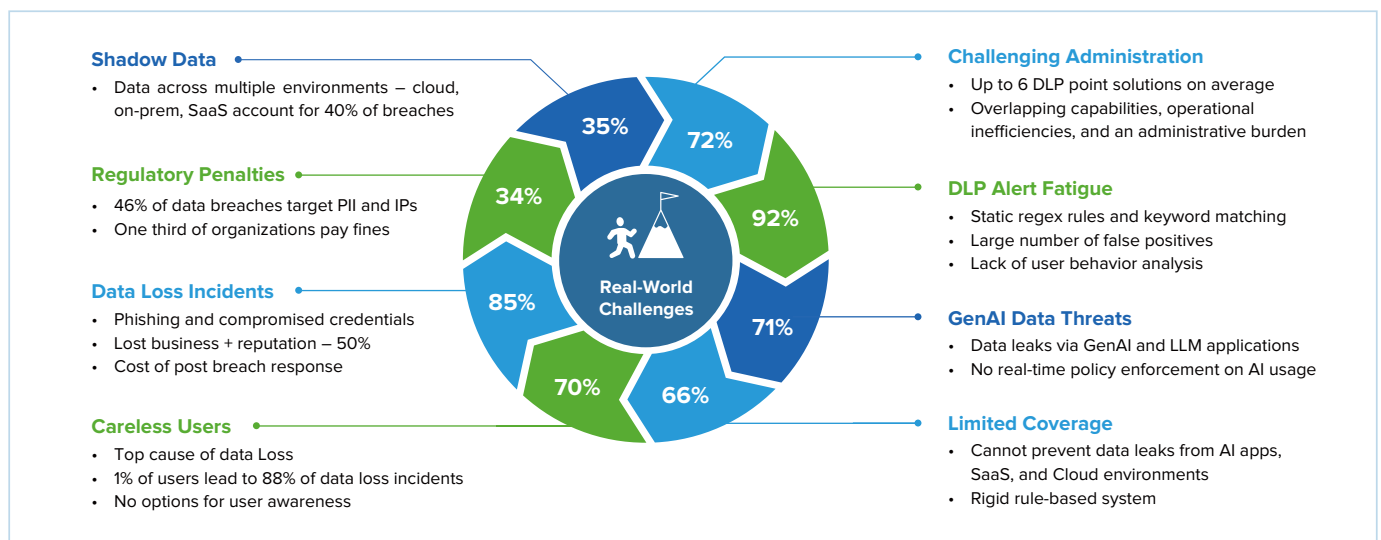
SANGFOR Zero Trust Data Protection

Effortless Data Defence: Powered by AI

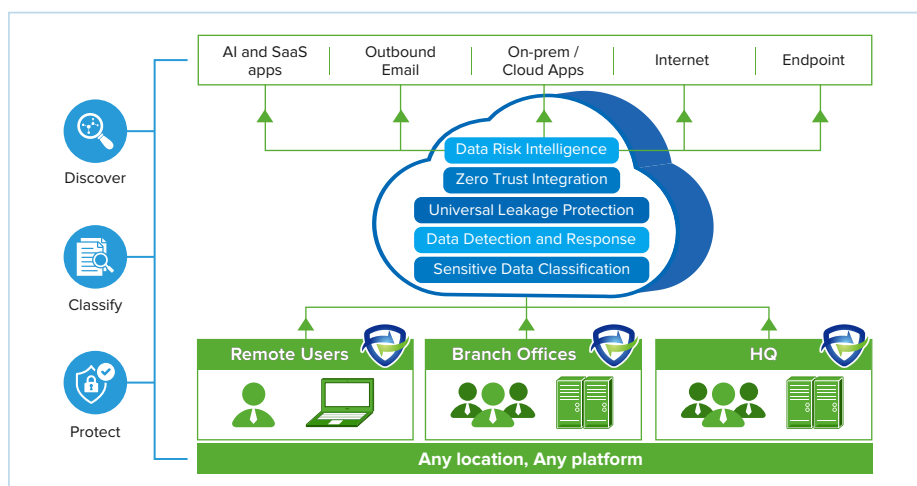


Modern Data Security Challenges

In today's digital landscape, data is a critical asset. As SaaS adoption, public cloud usage, and hybrid work models accelerate, sensitive information — like PII, financial records, and intellectual property (IP) — flows across users, applications, and devices. Legacy DLP solutions struggle to keep pace, making data discovery and protection increasingly complex.



Sangfor Zero Trust Data Protection – Solution Overview

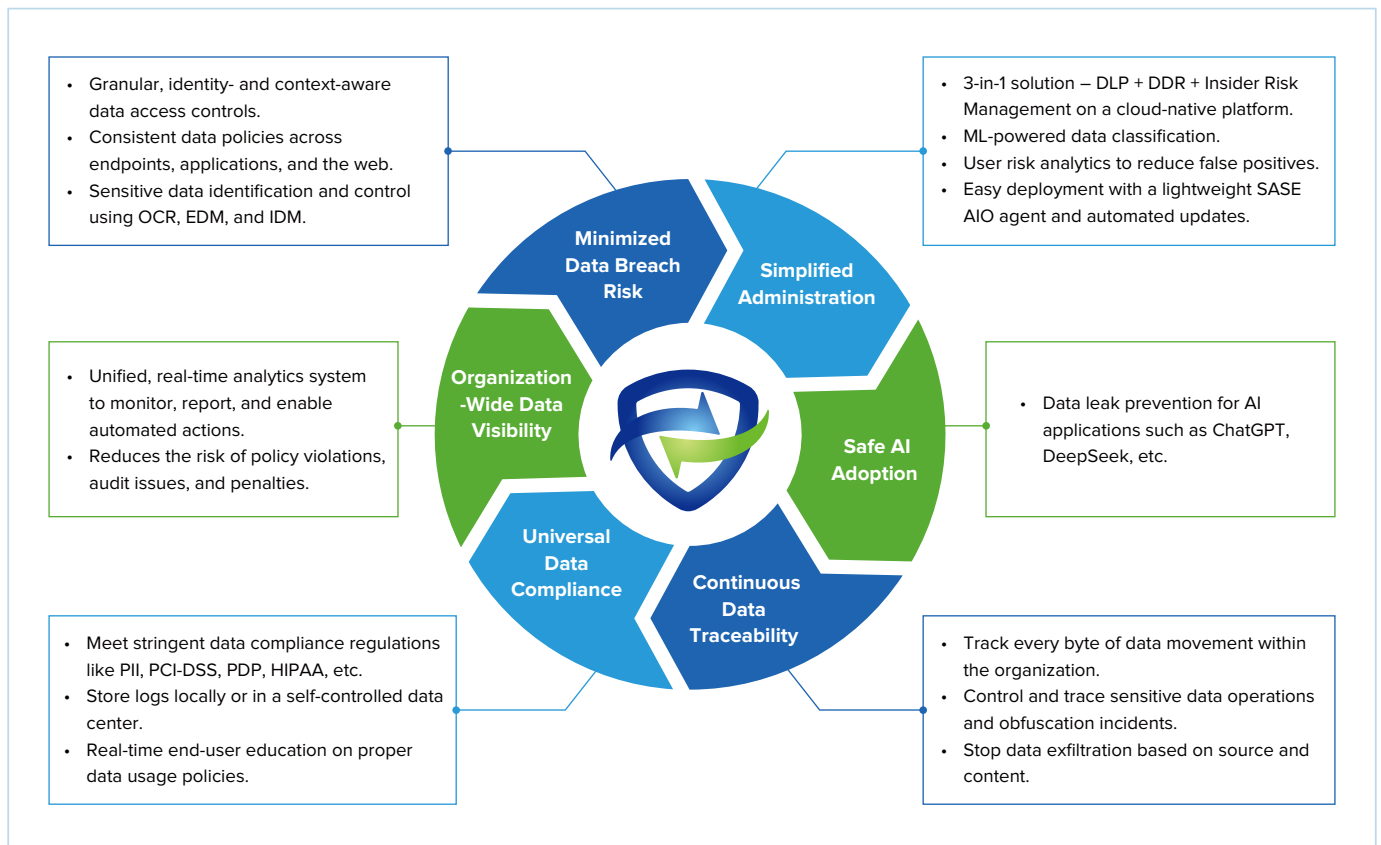


Natively integrated with Sangfor Athena SASE, Sangfor Zero Trust Data Protection (ZTDP) offers a 3-in-1 solution to address modern data security challenges. It seamlessly integrates advanced Data Loss Prevention (DLP), real-time Data Detection and Response (DDR), and user-centric, risk-based data security techniques to enhance the protection of an organization's data.



Protect What Matters Most — Your Data, Your Reputation, Your Growth

Sangfor ZTDP delivers comprehensive data protection across every environment—whether data is at rest, in motion, or in use. Centrally managed through a cloud-native console, it proactively prevents leakage, loss, and misuse while maintaining compliance. With multi-vector protection, Sangfor ZTDP stops breaches before they happen and empowers security teams with advanced Detection & Response (DDR), streamlined Data Loss Prevention (DLP), and robust Insider Threat Mitigation.



Sangfor ZTDP Use Cases

<p>Prevent Sensitive Data Exfiltration</p>	<p>Insider Threat Mitigation</p>	<p>Achieve Compliance</p>
<p>Prevent the exfiltration of source code, product roadmaps, M&A documents, and trade secrets. Use EDM, OCR, and IDM to secure proprietary formats and structured data.</p>	<p>Detect and prevent unauthorized sharing, printing, or uploading of confidential data. Monitor user risk scores based on anomalous behavior, such as bulk downloads or off-hours access.</p>	<p>Enforce policies aligned with GDPR, HIPAA, PCI-DSS, and regional data sovereignty regulations. Automate incident logging and reporting to maintain audit trails and reduce manual overhead.</p>

