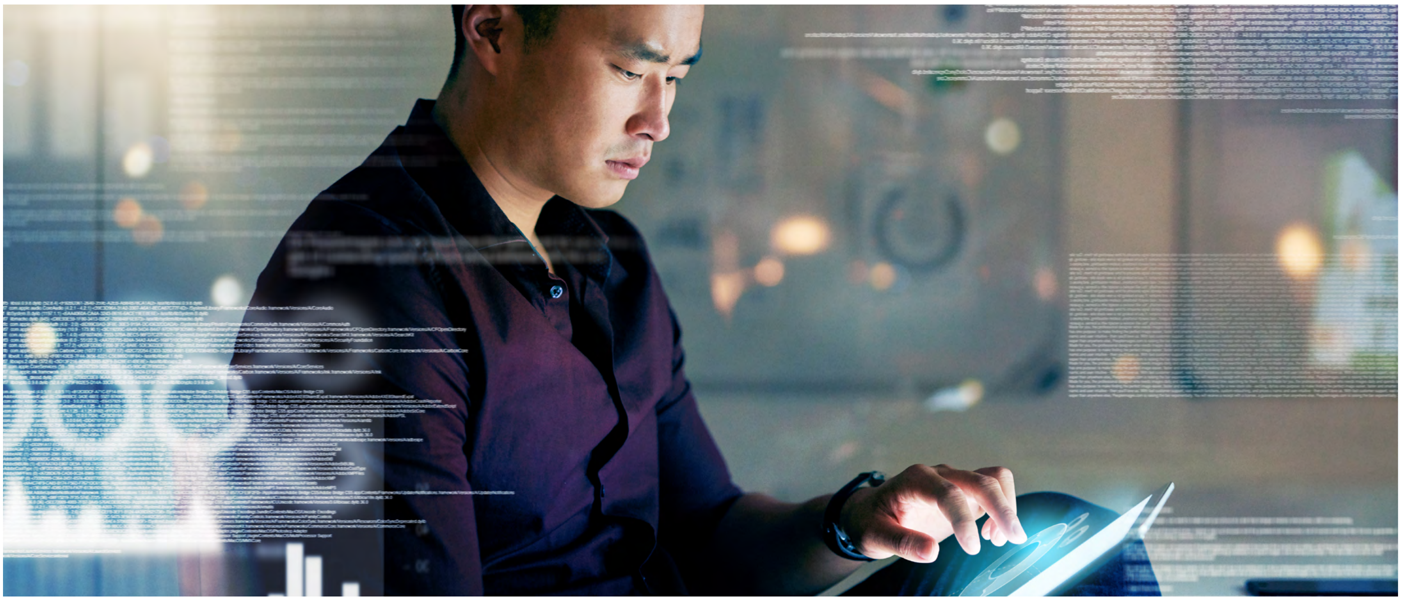
Ensure data trust for secure AI adoption

Establish and maintain trustworthy data to securely operationalize AI across your organization



Benefits

- Reduce data risk by ensuring visibility, governance, and privacy across AI data pipelines.
- Secure your AI data pipelines with consistent, data-centric controls across on-premises repositories, multicloud environments, and SaaS applications.

Artificial intelligence presents vast opportunities and is reshaping today's business landscape. Organizations are steadily adopting AI to unlock new competitive advantages, including uncovering new insight and driving operational efficiencies. Given the profound impact of AI investments, embracing this technology has become a strategic imperative for businesses to maintain competitiveness.

AI initiatives are only as good as the data they are built on, and the emerging need for AI is contributing to exponential data growth. According to Forrester, 27 percent of decision makers attribute data storage growth to new big data techniques, including generative AI.[1] Before organizations can safely scale and operationalize AI, they must address data sprawl and its impact on data quality, end-user productivity, operational costs, and security risk.

Trusted data throughout the data lifecycle forms the bedrock of successful AI implementation, directly influencing the accuracy, reliability, and integrity of your organization's AI initiatives. The OpenText™ data security platform equips you with comprehensive tools to responsibly curate high-quality data for AI systems.

[1] Forrester, *The State of Storage*, Global 2025, Figure 2, Page 4

Our leading data security platform delivers trusted AI by providing:

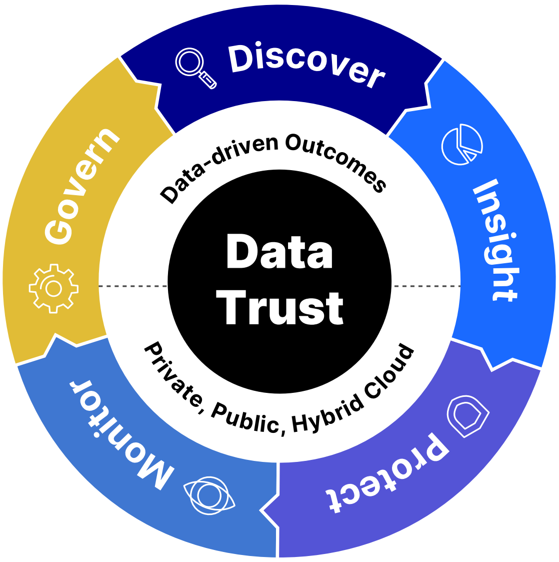
- **Enhanced data security**—Implementing rigorous data security practices reduces risks like data breaches, unauthorized access, and AI model poisoning, ensuring the integrity and reliability of data feeding AI systems.
- **Improved data governance**—Unified data lifecycle governance helps reduce data sprawl, optimize storage, and maintain compliance with regulations, reducing overall data risk.
- **Accurate data analysis**—AI-driven and context-aware pattern recognition models accurately identify and classify sensitive data with precision, enhancing privacy, compliance, and operational efficiency.
- **Comprehensive data protection**—Enable end-to-end, data-centric security across the entire data lifecycle. And remediate risk by using leading protection techniques—including de-identification—to protect your data from attackers, without disrupting applications, databases, or performance.
- **Proactive data monitoring**—Continuously monitor data access and usage to ensure only authorized users can access sensitive data, supporting IT modernization and audit readiness.

Reduce data risk for AI adoption

To establish trust in your AI data, it's essential to implement robust data security practices and curate high-quality data—because effective AI relies on exceptional data. As a critical foundation that empowers AI use cases, our data security platform provides significant advantages through its cloud architecture. The platform delivers unified set-up, discovery, classification, policy management, centralized analytics, and high scalability.

OpenText provides a unified data security platform that bridges visibility and context data privacy, and governance . We discover, analyze, and ensure the privacy of your most sensitive data. Additionally, integration with our innovative identity and access management capabilities empowers organizations to continuously monitor data usage—who has access to what—and govern data throughout its lifecycle.

By leveraging cutting-edge technologies, such as AI-driven PII detection, encryption, masking/anonymization, tokenization, and data minimization, you can meticulously curate data for safe and ethical use in LLMs and GenAI platforms. With this approach, organizations can confidently train and operate models, allowing them to unlock the full benefits of AI. Our platform helps you ensure that personal data is secure and handled ethically during use—even in data analytics contexts—safeguarding it from any harm.



Secure your AI data pipelines

Our unified data security platform helps you build a comprehensive foundation for your AI-related data security posture management with industry-leading capabilities across the pillars of data trust:

- Data analysis
- Data classification
- Data protection
- Data monitoring
- Data lifecycle governance

Data analysis

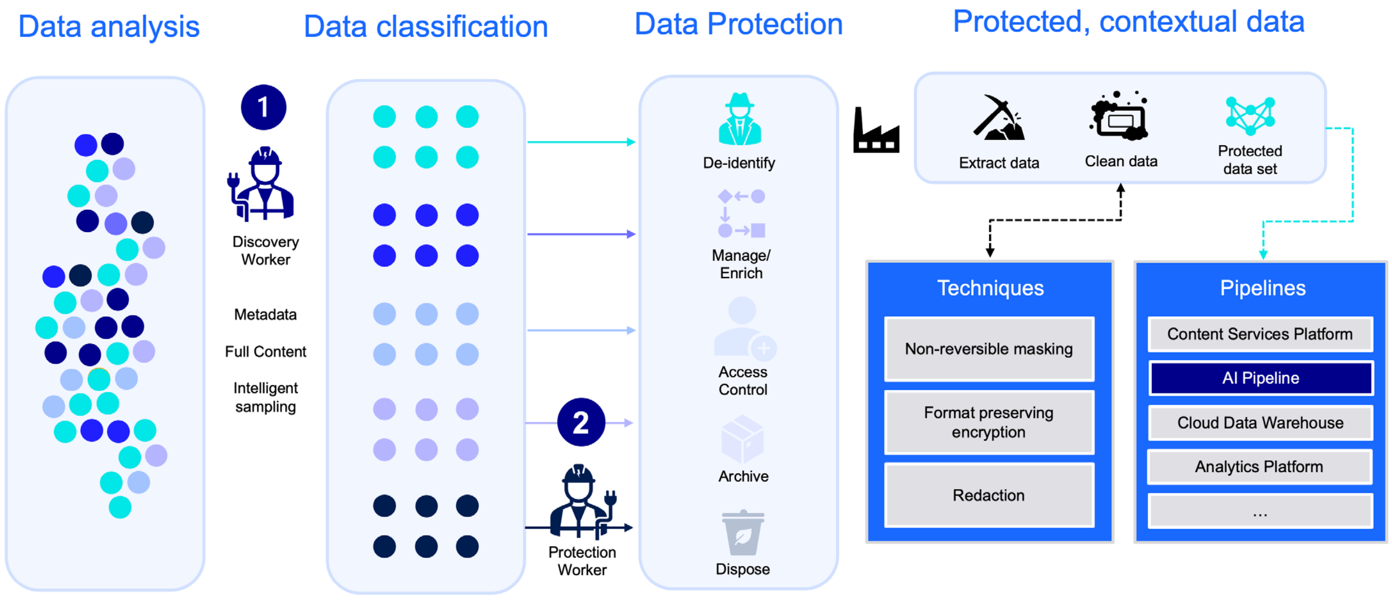
Secure data pipelines with OpenText's data security platform

To safeguard your AI data pipeline, it's crucial to first pinpoint the location of sensitive data. Our platform offers comprehensive data discovery through scanning, tagging, analytics, risk measurement, and personal data discovery across structured and unstructured repositories. This visibility ensures you can effectively protect your sensitive data.

The platform's cloud-based data discovery spans file systems, databases, and cloud data warehouses. Leveraging fast and intelligent scanning capabilities, OpenText swiftly identifies at-risk data repositories in days rather than weeks, streamlining your discovery process.

OCR capabilities enhance detection of sensitive data in scanned images and media files, ensuring thorough identification of organizational information. Beyond sensitive data, the platform identifies redundant, obsolete, and trivial data, optimizing storage and reducing security risks.

Discovery and de-identification are essential elements of any data security and AI strategy



Data classification

Determining the importance and value of your data is critical to mitigating risk and operationalizing privacy and data insight for AI adoption. The OpenText data security platform applies powerful analytics to identify sensitive data entities that need to be protected.

Our core grammar sets focus on:

Data classification	Description
PII	Personally identifiable information, including 13 categories of entities across 38 different countries.
PHI	Protected health information, normally associated with the North American health industry.
PCI	Payment Card Industry data such as credit card and primary account numbers.
IP	Intellectual property, can be customized to your business.

Context is king and accuracy is essential. Powered by OpenText™ Knowledge Data Discovery analytics, our cloud platform provides curated and optimized grammars built to assist today's global data privacy challenges—supporting entity extraction for 38+ country languages, data formats, and economic regions:

- Our grammars also use context and "landmarks" to generate a risk score that we use to deliver more accurate results and filter out false positives.
- Accuracy and risk score is based on proximity to the identified entity extracted or matched combined with sophisticated probabilistic modeling and natural language processing algorithms used to determine the strength of the relationship and augment the score.
- Extended language support in grammars also helps with context in determining the sensitivity or even presence of PII.
- Multiple grammars can be combined to target entities more broadly but can result in higher compute costs and slower processing times.
- Customizable risk scoring and weighting of categories provides greater flexibility in how you choose to implement and configure grammars to meet your needs.

Data privacy

OpenText enables you to ensure data privacy across the entire data lifecycle—from the point your data is captured and throughout its movement across your extended enterprise—all without exposing live information to elevated risk, high-threat environments. That's the essence of data-centric protection.

With our data privacy technologies, you'll gain control of your sensitive data at rest, in motion, and in use. Whether you implement one use case or hundreds, our technology can scale to meet any data privacy requirement on premises and in multicloud hybrid IT. Our solution de-identifies data, rendering it useless to attackers, while maintaining its usability, usefulness, and referential integrity for data processes, applications, and services. With OpenText, you can neutralize data breach threats by making your protected data worthless to an attacker, whether it is in production, analytic systems, test/development systems, or shared externally.

Resources

Navigating the intersection of AI and financial risk: A proactive approach

Read the blog ›

3 steps to decoding data risk

View the infographic ›

OpenText's guide to data security and mitigating financial risk

Watch the video ›

Our unique, proven data-centric approach to data privacy—where the access policy travels with the data itself—permits data privacy without changes to data format or integrity and eliminates the cost and complexity of issuing and managing certificates and keys. As a result, our customers across industries have achieved end-to-end data protection across the extended enterprise in as little as 60 to 90 days. This success is due to the minimum, in most cases zero, impact on applications and database schemas.

Data monitoring

Our data access governance capabilities will enable your organization to ensure that only authorized users with specific roles can access your AI data pipelines and other privileged data. You'll gain comprehensive features, including change notifications, lifecycle management, security lockdown, and security fencing. And the granular reporting capabilities make it easy to identify data that requires movement, security, or retirement.

OpenText™ Database Activity Monitoring actively monitors databases in real time and promptly generates alerts for policy violations, covering a wide range of activities, such as data manipulation, schema modifications, access control changes, and transaction control. You can use this information to identify databases for retirement and gain insights into applications interacting with sensitive data, preventing or minimizing outages, enhancing privacy posture, supporting IT modernization efforts, and promoting green IT and sustainability initiatives.

Data governance

Data and application sprawl have constantly led to a bloat of redundant data (duplication, and convenience copies of data spread out across the enterprise and in cloud repositories). The same is true for outdated, stale data (data that has not been accessed for extended periods of time) or low-value data that simply takes up storage space and resources to manage (data like vacation photos or DLL or EXE files).

A well-structured data management strategy for your AI governance and general business practices include data lifecycle actions—such as data deletion, records declaration, and archiving—which are essential for maintaining compliance with various regulations, minimizing data risk, and reducing data storage costs. By carefully implementing defensible data deletion practices, you can apply remediation actions to control access and securely manage high-value data.

Next steps

People in your organization are likely already using AI tools like LLMs. But to adopt these tools optimally and securely across your organization takes a serious commitment to data trust—including analysis, classification, protection, monitoring, and governance. We're ready to help you gain an advantage over your competition with tools that help you do all of the above.

Learn more about our products

opentext™