



News Release

Teradata Introduces New Privacy, Security, and Resiliency Capabilities as AI Forces Change in Enterprise Data Protection

2026-10-20

New capabilities protect the sensitive data and intelligence behind enterprise AI while keeping mission-critical operations available and recoverable

SAN DIEGO, Oct. 20, 2026 /PRNewswire/ -- **Teradata** (NYSE: **TDC**) today announced new privacy, security, and resiliency capabilities designed to address one of the defining challenges of enterprise AI: how sensitive data is protected, who and what can access it, and whether it remains available and recoverable when something goes wrong. Teradata addresses all three through an integrated approach that reduces raw identity exposure, enforces protection closer to the data, and keeps the intelligence powering AI available and recoverable. In practice, that means protecting the intelligence behind AI without diminishing what makes it valuable.

Key Capabilities

- Poly-Anonymization®: reduces raw identity exposure while preserving the relationships and utility AI and analytics require
- Format-preserving encryption: protects sensitive values without changing their format or breaking downstream systems
- Post-quantum security and readiness: strengthens protection against emerging quantum-era threats through Anonomatic PII Vault® and TLS 1.3 hybrid-key exchange for data in transit
- Immutable backup protection: prevents recovery points from being modified or deleted, strengthening cyber-recovery readiness
- Database-level high availability: an additional availability layer for mission-critical workloads, distinct from disaster recovery

Why It Matters Now

As AI becomes mission-critical, it expands both the value and the vulnerability of enterprise data. Sensitive information now moves among users, applications, models, and agents, making it harder to secure at the boundary alone. AI is designed to combine disparate information to find patterns and make decisions, which means data that isn't individually identifiable can become so when AI brings it together.

Executive Quote

"Privacy, security, and resiliency have historically been treated as separate problems with separate solutions. That approach doesn't hold up when AI is moving sensitive data across users, applications, models, and agents simultaneously. This announcement reflects how we think those capabilities need to work together, and it's the foundation for how we intend to extend that protection as AI environments grow more complex and the actors operating within them multiply."

-Sumeet Arora, Chief Product Officer, Teradata

Privacy Protection

Access control determines who can see sensitive data. Identity reduction changes how much identifying information needs to be present in the analytical environment in the first place. Teradata combines both, through an OEM partnership with **Anonomatic**, whose privacy capabilities are natively available to Teradata customers.

Poly-Anonymization replaces PII fields with a stable identifier while holding underlying identity separately within Anonomatic PII Vault, a post-quantum-secure environment built with multiple layers of overlapping security controls designed to protect sensitive identity information. Authorized users can restore identity when a legitimate use case requires it, but everyone else works with data that retains its analytical structure, its relationships, and its utility. The result is an analytical environment where sensitive data can be used for AI, analytics, testing, and approved collaboration without broadly exposing who the data is about.

Unlike approaches that rely solely on mathematically reversible encryption, PII Vault combines identity separation, Poly-Anonymization, access controls, and additional layered protections to reduce identity exposure while retaining the utility required for AI and analytics. Format-preserving encryption extends that protection to situations where a value's structure matters to downstream systems, protecting sensitive data without breaking the applications and workflows built around it.

Testing at large scale demonstrated that Teradata's Anonomatic-powered privacy-preserving controls can support enterprise analytical workloads without the performance tradeoffs organizations typically associate with data privacy. Multi-table join queries on protected data used fewer Teradata resources than equivalent queries on unprotected data, though results will vary by workload and configuration.

Partner Quote

"Enterprise AI creates a fundamentally different privacy challenge. Organizations need to use sensitive, individual-level data to build effective AI, but the traditional tools for protecting that data weren't designed to preserve what AI needs to work. Our partnership with Teradata makes it possible to reduce identity exposure at enterprise scale without forcing organizations to choose between protection and utility."

-Matt Fleck, Founder and CEO at Anonomatic, a data security software company focused on making PII data privacy secure, simple and cost effective

Native Data Security

Protection that follows the data requires controls enforced at the data layer, not just at the systems surrounding it. Teradata applies classification, policy enforcement, and access controls closer to the data itself. Together, these capabilities provide a governance-led foundation for protecting data and intelligence across users, applications, and workloads.

For data in transit, Teradata introduces post-quantum protection via TLS 1.3 hybrid-key exchange, which combines classical and post-quantum cryptographic algorithms in a single handshake. As quantum computing advances make current encryption standards increasingly vulnerable, organizations that establish cryptographic readiness now will be better positioned for what's ahead.

New native capabilities including dynamic data masking, data classification and tagging, column-level encryption, and global identity extend that protection across the data layer. Through a partnership with **Immuta**, a data authorization platform between identity and enterprise data, dynamic ABAC brings identity-aware, attribute-driven access control that enforces policy consistently across users and AI workloads without duplicating data or rewriting governance rules.

Teradata's security architecture is designed to extend as AI environments evolve, with ongoing investment in controls that govern how AI agents access and act on enterprise data within policy boundaries.

Enterprise Data Protection

For enterprises running AI at scale, a cyberattack is a threat to the data, context, and operational knowledge that AI depends on to function. Teradata Enterprise Data Protection addresses that reality through a workload-aligned approach that lets organizations match protection levels to business criticality rather than applying the same resiliency architecture to every workload. The objective is not simply to restore data, but to restore the trusted context AI needs to resume mission-critical operations.

Database-level high availability via real-time replication introduces an additional availability layer designed for continuous synchronization and low recovery objectives.

Immutable backup protection strengthens cyber-recovery readiness by ensuring recovery points cannot be modified, encrypted, or deleted, even by privileged administrators. As ransomware increasingly targets backup data specifically, protected recovery points have become as critical as the protection strategies built around them. Teradata's resiliency architecture is designed to extend as cyber threats and recovery requirements evolve.

Additional capabilities including backup and recovery, scheduled data synchronization, and disaster recovery round out a more consistent Enterprise Data Protection experience.

Availability

- Privacy capabilities, powered by Anonomatic and delivered by Teradata, are available now for Teradata Cloud on AWS, Azure, and Google Cloud.
- Native data security capabilities including dynamic data masking, data classification and tagging, and column-level encryption are available on Teradata Cloud across AWS, Azure, and Google Cloud. Dynamic data masking, data classification and tagging are available for Teradata Factory and on-premises deployment options.
- Teradata Enterprise Data Protection including immutable backup protection is available now on Teradata Cloud across AWS, Azure, and Google Cloud with availability on Teradata Customer Cloud planned in the coming months.

About Teradata

Teradata empowers enterprises to turn intelligence into autonomous action, grounding AI agents in deep business context and trusted data. As AI agents multiply, Teradata is the context foundation, governance layer, and performance backbone that companies need now. The Teradata Autonomous Knowledge Platform puts AI into production across cloud, on-premises, and hybrid environments.

Forward-Looking Statements

This press release contains "forward-looking statements" about the expectations, beliefs, plans, and intentions relating to Teradata's privacy, security, and resiliency capabilities. Such statements include statements regarding future product availability, capabilities, and offerings, and expected benefits to Teradata customers. Forward-looking statements are subject to known and unknown risks and uncertainties and are based on potentially inaccurate assumptions that could cause actual results to differ materially from those expected or implied by the forward-looking statements. If any such risks or uncertainties materialize or if any of the assumptions prove incorrect, Teradata's results could differ materially from the results expressed or implied by the forward-looking statements made. Teradata undertakes no obligation, and does not intend to update the forward-looking statements. Factors that may cause actual results to differ materially from those in any forward-looking statements

include: (i) delays and unexpected difficulties and expenses in executing the planned product capabilities and offerings, (ii) changes in the regulatory landscape related to AI and (iii) uncertainty as to whether customer adoption will justify the investments in the product capabilities and offerings. Further information on factors that could affect Teradata's financial and other results is included in the filings Teradata makes with the Securities and Exchange Commission from time to time.

The Teradata logo is a trademark, and Teradata is a registered trademark of Teradata Corporation and/or its affiliates in the U.S. and worldwide.

Poly-Anonymization and PII Vault are registered trademarks of Anonomatic, Inc.

MEDIA CONTACT

Jennifer Donahue

Jennifer.Donahue@Teradata.com

View original content:**<https://www.prnewswire.com/news-releases/teradata-introduces-new-privacy-security-and-resiliency-capabilities-as-ai-forces-change-in-enterprise-data-protection-302913579.html>**

SOURCE Teradata