

Most Enterprises Think Their Data is Protected. It's Not. Teradata Can Help.

Expert Protection for Enterprise Data

The cloud has revolutionized how organizations gather, store, process, manage, and get value from their data. Enterprises want cloud-native as-a-service offerings, yet executives may also have anxiety about entrusting IT resources and administration to a partner.

Relax. Teradata is on top of it. We recognize and respect these concerns. In fact, we treat security as the number one priority for all Teradata Vantage in the Cloud offerings. We employ industry best practices and empower an experienced team of cloud, security, and database experts to keep threats at bay.

As-a-Service Delivery

The Teradata Cloud Operations team manages performance, security, availability, and operations of customers' Vantage in the Cloud environments. The primary benefit for customers is that internal teams can focus on answers, not IT. Attributes include:

Security		Provides peace of mind via encryption, audited compliance and other robust security controls
Consistency		Uses the same Vantage software deployed everywhere
Scalability		Delivers the ability to quickly adjust performance and cost as needed
Transparency		Simplifies budgeting via predictable prices and no hidden fees

Teradata Cloud Operations does not have visibility or access to customer data – nor is customer data ever transferred across country borders.

Strict Access Control

As part of our strict access control policy, Teradata assigns a risk designation to every Cloud Operations position and establishes screening criteria for individuals. They include:

- Administrator logging
- Background checks
- Codes of conduct
- Confidentiality agreements

The Cloud Operations team also enforces password complexity, stores and transmits only encrypted password representations, and sets minimum and maximum lifetime restrictions on those passwords. All remote access is encrypted using FIPS 140-2 validated cryptographic modules. Multi-Factor Authentication (MFA) is required for any remote administrative access.

Active Directory Authentication

Each VantageCloud advanced analytics database environment is Lightweight Directory Access Protocol (LDAP)-ready. Alternatively, customers may choose Kerberos single sign-on (SSO), Federated SSO configurable with MFA and Bring Your Own Identity Provider (IdP), or the Cloud Active Directory for secure user authentication. When using LDAP, usernames matching those in the customer's domain must be created in the VantageCloud database.

Vantage in the Cloud Uses Single-Tenant Subscription

- Cloud resources are not shared with other customers
- Helps with security, performance, and reliability

Vantage User Roles

VantageCloud platforms and data are accessible only by individual user IDs assigned to each customer's designated users. User IDs and Role Based Access Control (RBAC) or role membership are two key methods for securing customer data within the platform. Vantage also provides fine-grained access using built-in Teradata Secure Zones and Row/Column Level Security.

Multi-Tiered Defense Plan

VantageCloud includes multiple layers of network security. Ingress and egress filtering network access control lists (NACLs) are applied to internet border gateway routers. These NACLs are configured as "deny-by default" and strictly limit connectivity to whitelisted IPs. Enterprise-grade application firewalls together with Network Security Groups comprise additional layers of defense.

Teradata also configures private network connections to terminate at cloud firewalls and sets Access Control Lists (ACLs) to define which traffic may be transported across tunnels, which may be encrypted. Traffic not matching an "approved" ACL is blocked. Further, Teradata Cloud Operations administrative and service access is secured using Site Gateways, Vantage Console and Centrify PAS Event Based Access (EBA) together with ServiceNow™. These systems are secured with multiple defenses including Web Application Firewalls, NACLs, Multi-factor Authentication (MFA) TLSv1.2 encrypted web traffic, Secure Shell (SSH) and OS based privileged access checking.

Strong Data Encryption

All customer data is encrypted at rest on storage array drives and cloud object stores. For data in motion, Teradata can enable encryption for all network and client/server connectivity. Enhanced security options allow row and column encryption.

Open-Source Security Policy

Teradata Cloud Operations maintains an Open-Source Security Policy that is reviewed annually. A list of all code libraries required for execution is identified and a report of all entries in the National Vulnerability Database (NVD) for the software is provided. The availability of patches for all Moderate, High and Critical Risk vulnerabilities identified in the NVD report is documented, and these patches are applied to the software.

Vigilant Security Monitoring

To facilitate detection of cyberattacks and policy violations, the security monitoring process intelligently scans for, collects, and correlates relevant security events. Network devices such as border gateway routers and firewalls send intrusion events to the Security Information and Event Monitoring (SIEM) system, which is calibrated to respond according to the type of event detected.

Audited Compliance for Peace of Mind

The delivery architecture for Vantage in the Cloud is designed to comply with rigorous multi-national standards. These offers are audited periodically for compliance with important standards, including:



HIPAA: Health Insurance Portability and Accountability Act



ISO/IEC 27001: International Standards Organization Information Security Management System (ISMS)



PCI: Payment Card Industry



SOC 1 and 2: Service Organization Controls

Such audits help customers meet their associated privacy responsibilities such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR).

About Teradata

Teradata is the connected multi-cloud data platform for enterprise analytics, solving data challenges from start to scale. Our industry-leading platform helps organizations turn data into their greatest asset, unlocking value and effectively delivering business outcomes. See how at [Teradata.com](https://www.teradata.com).

17095 Via Del Campo, San Diego, CA 92127 [Teradata.com](https://www.teradata.com)

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. Teradata continually improves products as new technologies and components become available. Teradata, therefore, reserves the right to change specifications without prior notice. All features, functions and operations described herein may not be marketed in all parts of the world. Consult your Teradata representative or [Teradata.com](https://www.teradata.com) for more information.

© 2023 Teradata Corporation All Rights Reserved. Produced in U.S.A. 02.23



teradata.