

Cloud Security for As-a-Service Offerings





Expert Protection for Enterprise Data

Cloud computing has revolutionized the way organizations manage their data. Customers want as-a-service offerings for Teradata Vantage™ while at the same time there may be anxiety about entrusting intellectual property and IT infrastructure to an external provider.

Teradata recognizes and respects these concerns. Teradata treats security as the number one priority for its as-a-service offerings. Industry best practices are overseen by a team of experts empowered to keep threats at bay.

As-a-Service Delivers Peace of Mind

With as-a-service delivery of Vantage, the Teradata Cloud Operations team manages performance, security, availability, and operations of a customer’s analytics infrastructure. Internal teams can focus on answers, not IT. Benefits include:

| | | |
|---------------------|---|--|
| Security |  | Provides peace of mind via encryption and audited compliance |
| Consistency |  | Uses the same Vantage software deployed everywhere |
| Scalability |  | Delivers the ability to quickly adjust performance and cost |
| Transparency |  | Simplifies budgeting via predictable prices and no hidden fees |

The Cloud Operations team does not have visibility or access to customer data—and data is never transferred across country borders.

Audited Compliance

The as-a-service delivery architecture for Vantage is designed to comply with rigorous international standards. The Information Security Management System (ISMS) receives regular third-party audits to verify compliance with:

- GDPR: General Data Protection Regulation
- PCI: Payment Card Industry
- HIPAA: Health Insurance Portability and Accountability Act
- ISO 27001: International Standards Organization
- SOC 1 and 2: Service Organization Control

Each customer is provisioned in a single-tenant environment separate from other as-a-service accounts.

Strict Access Control

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

- 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 approved encryption mechanisms, and Multi-Factor Authentication (MFA) is required for any remote administrative access.

Two-Tiered Defense Plan

As-a-service delivery of Vantage includes two layers of network security. The first layer consists of ingress and egress filtering control lists applied to internet border routers; these lists are configured as “deny-by-default” and limit connectivity. Enterprise-grade application firewalls make up the second layer of defense.

Teradata also configures network connections to terminate on cloud firewalls and sets Access Control Lists (ACL) to define which traffic may be transported across tunnels. Any traffic not matching an “approved traffic” ACL is blocked.

Strong Data Encryption

All customer data is encrypted both in motion and at rest. For data in motion, Teradata encrypts all data traveling over public networks using site-to-site Virtual Private Networks (VPNs) with IPsec. For extra protection, customers may also use Multiprotocol Label Switching (MPLS) or point-to-point circuits.

For data at rest, self-encrypting storage drives ensure security once customer data arrives at an as-a-service environment. There are also a variety of enhanced security options to allow Vantage database administrators to encrypt and control access to individual rows/columns.

Active Directory

Each as-a-service environment is Lightweight Directory Access Protocol (LDAP)-ready. Alternatively, customers may choose to use database authentication or use the Cloud Active Directory to authenticate sessions. When using any of the LDAP methods, users must still be created in Vantage with usernames that match directory usernames.

Vantage User Roles

Vantage and data stored in as-a-service systems are accessible only by individual user IDs that are assigned to each customer’s designated users. User IDs and Vantage security are the methods for securing customers’ data within the platform. Members of the Cloud Operations team do not have visibility or access to customer data.

Open Source Policies

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 Critical and High-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 all security-relevant events. Network devices such as border 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.

About Teradata

Teradata leverages all of the data, all of the time, so you can analyze anything, deploy anywhere, and deliver analytics that matter. By providing answers to the complexity, cost, and inadequacy of today’s analytics, Teradata is transforming how businesses work and people live. Get the answer at [Teradata.com](https://www.teradata.com).