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.

We recognize and respect these concerns. In fact, we treat security as the #1 priority for all Teradata offerings, especially Teradata VantageCloud. We employ industry best practices and empower an experienced team of cloud, security, and database experts to keep threats at bay. Our data protection options not only can ensure data is protected at rest, in motion, and in use, but can also provide data sovereignty, trusted data pipelines, and impenetrable protection of sensitive data.

As-a-service delivery

The Teradata cloud operations team manages performance, security, availability, and operations of customers' VantageCloud 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 VantageCloud software deployed everywhere

Scalability: Delivers the ability to quickly adjust performance and cost as needed

Transparency: Simplified budgeting via predictable prices and no hidden fees

Strict access control

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. Multifactor authentication (MFA) is required for any remote administrative access. Teradata also does not manage or have access to cloud storage encryption keys controlled by the customer.

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 multifactor authentication (MFA) and Bring Your Own Identity Provider (IdP), or a cloud-based identity and access management system (e.g., Microsoft Entra ID) for secure user authentication. When using LDAP, usernames matching those in the customer's domain must be created in the VantageCloud database or can be managed automatically with Teradata's automated provisioning solution.

Teradata cloud operations does not have visibility or access to customer data, nor is customer data ever transferred across country borders.

Lastly, Teradata offers backup as a service (BaaS) that provides an immutable backup solution to protect user data and remove the onerous task from the customer. Coming soon, our BaaS service will also include an air-gapped functionality that will protection customer backups from attacks like ransomware.

VantageCloud user roles

The VantageCloud platform 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. VantageCloud also provides fine-grained access using built-in row- and column-level security, trusted sessions, and IP filters.

Multilayered 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 privileged access service (PAS) event-based access (EBA) together with ServiceNow™. These systems are secured with multiple defenses, including web application firewalls, NACLs, MFA TLS 1.2 encrypted web traffic, Secure Shell (SSH), and OS-based privileged access checking.

Strong data de-identification protection

All customer data is encrypted at rest on storage array drives using FDE and/or transparent encryption and cloud object stores. For data in motion, Teradata can enable encryption for all network and client/server connectivity. Enhanced security options allow column-level encryption or tokenization to protect data in use for sensitive confidential data like PII and PHI. In addition, Teradata offers data protection modernization via poly-anonymization for sensitive data that will never enter the cloud but still provides full access for analytics and data science as if it were in the cloud. This renders any lost or stolen data harmless.

Open-source security policy

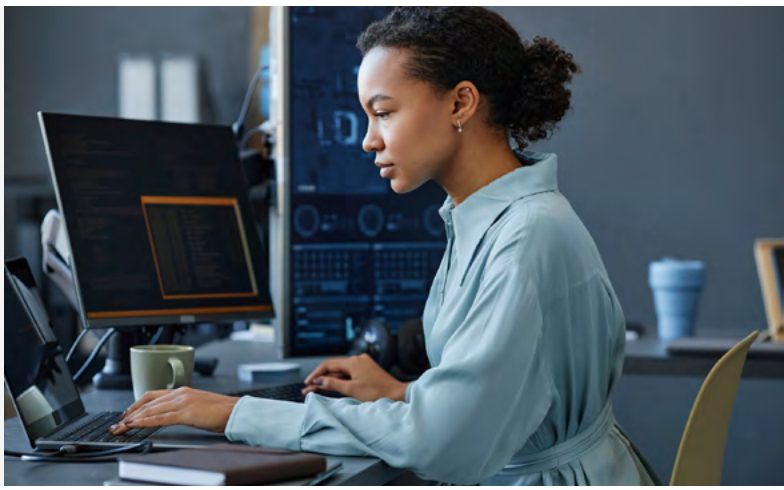
Teradata cloud operations maintains an open-source security policy that is reviewed annually. A list of all code libraries required for execution is identified and a report of all entries in the National Vulnerability Database (NVD) for the software is provided. The availability of patches for all moderate-, 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, application security, and policy violations, the security monitoring process intelligently scans for vulnerabilities and 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.

VantageCloud Enterprise uses single-tenant subscription

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



Audited compliance for peace of mind

The delivery architecture for VantageCloud is designed to comply with rigorous multinational standards. These offers are audited periodically for compliance with important standards, including:

HIPAA: Requires U.S. healthcare providers and organizations to protect patient health information from unauthorized use and disclosure

ISO/IEC 27001: International Organization for Standardization/International Electrochemical Commission

PCI DSS: PCI Security Standards Council

SOC 1 and 2: System and Organizational Controls designed by Association of International Certified Professional Accountants

HITRUST: Healthcare data security certification

These audits help customers meet their associated privacy responsibilities, such as the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), New York's SHIELD Act, the General Data Protection Regulation (GDPR), GxP guidelines, and FISC security guidelines.

About Teradata

At Teradata, we believe that people thrive when empowered with trusted information. We offer the most complete cloud analytics and data platform for AI. By delivering harmonized data and Trusted AI, we enable more confident decision-making, unlock faster innovation, and drive the impactful business results organizations need most. **See how at Teradata.com.**

17095 Via Del Campo, San Diego, CA 92127 Teradata.com

teradata.