ADVANCED ANALYTICS / DATASHEET

Teradata® IntelliCloud™ Security

Expert Protection for Your Data

Cloud computing has revolutionized the way organizations manage their data. Along with this accelerating trend comes questions about security. Executives want to leverage as-a-service offerings to take advantage of agility and on-demand consumption—and at the same time there may be anxiety about entrusting core elements of IT infrastructure to an external provider.

Relax, we've got you covered. Security is the number one priority for every facet of Teradata IntelliCloud™ services. Indeed, IntelliCloud security encompasses industry best practices and is overseen by a team of experts empowered to keep threats at bay. We take this responsibility very seriously.

IntelliCloud = As-a-service

Teradata IntelliCloud is our as-a-service offering for analytics at scale. We manage performance, security, availability, and operations of your data and analytics infrastructure so you can focus on delivering high-impact business outcomes.

IntelliCloud enables you to:

- Get the most value from your analytics investment
- Have peace of mind about security and compliance
- Enjoy higher uptime with greater business continuity
- Free up in-house resources to extract business-transforming answers from your data

Security Never Sleeps

The Teradata IntelliCloud service architecture is designed to comply with strict international standards:

- Cloud Security Alliance (CSA)
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- International Standards Organization (ISO) 27001
- Payment Card Industry (PCI)
- Service Organization Control (SOC) 1 and 2

We invest in recurring third-party audits of the IntelliCloud Information Security Management System to ensure compliance with these rigorous standards. Audit reports and the latest certifications are available upon request.

Access Control

As part of Teradata's access protection policy, we assign a risk designation to every Teradata Cloud Operations position and establish screening criteria for individuals who fill those posts. Our program makes sure signed agreements are in place before access is assigned.

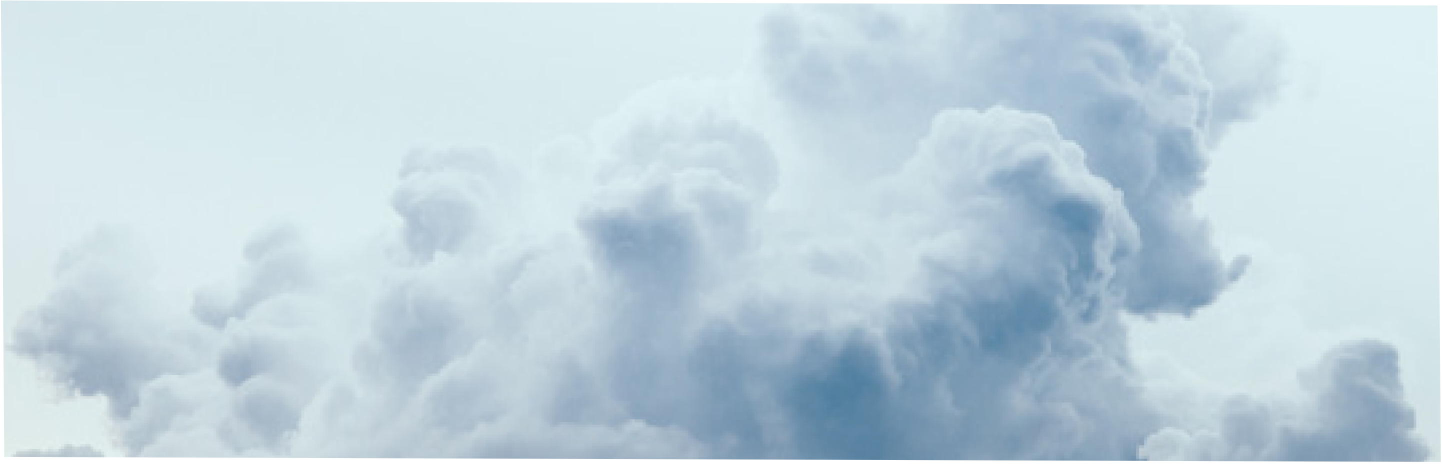
Specifics include:

- Access control systems
- Administrator logging
- Background checks
- Codes of conduct
- Confidentiality agreements
- Multifactor authentication

Teradata Cloud Operations also enforces password complexity, stores and transmits only encrypted password representations, and sets minimum and maximum lifetime restrictions on those passwords.

Additionally, we offer a stringent security re-approval process that includes:

- Creating, enabling, modifying, disabling, and removing Teradata IntelliCloud Directory accounts in accordance with account management procedures
- Reviewing and approving all account management actions



- Monitoring account management operations for any unauthorized actions
- Disabling appropriate Teradata IntelliCloud directory accounts whenever an individual is terminated or transferred
- Modifying role-based access whenever an individual's system usage or need-to-know requirements change
- Automatically disabling inactive accounts after 90 days

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

Two-Tiered Defense Plan

Teradata IntelliCloud includes two layers of network security. The first layer consists of ingress and egress filtering control lists applied to our Internet border routers; these lists have been configured as "deny-by-default" and limit connectivity. Robust application firewalls make up the second layer of defense.

Teradata also configures customer site-to-site Virtual Private Networks (VPNs) to terminate on the cloud firewalls, and we set Access Control Lists (ACLs) to define which traffic may be transported across tunnels. Any traffic not matching an "approved traffic" ACL is blocked. For internal traffic between Amazon Web Services Virtual Private Clouds (VPCs) or Microsoft Azure Virtual Networks (VNets), data is private and not exposed publicly.

Data Encryption

IntelliCloud protects customers' data in motion and data at rest. For data in motion, Teradata encrypts all data traveling over public networks using site-to-site VPNs by using the IPsec protocol. For extra protection, you can also choose to use Multiprotocol Label Switching (MPLS) or point-to-point (P2P) circuits to connect to Teradata IntelliCloud.

Once your data arrives at an IntelliCloud environment, self-encrypting storage drives ensure security for data at rest. There is also an enhanced security option to allow a database administrator to encrypt and control access to individual rows/columns within the database if so desired.

Active Directory

The IntelliCloud environment is Lightweight Directory Access Protocol (LDAP) ready. Alternatively, you may choose to use database authentication (TD2 in Teradata) or use the Teradata IntelliCloud Active Directory to authenticate database sessions. When using any of the LDAP methods, users must still be created in the database with usernames that match directory usernames.

Teradata Vantage User Roles

Teradata Vantage and data stored in the IntelliCloud service are accessible only by individual user-IDs that are assigned to each of the customer's designated users. User-IDs and Teradata Vantage security are the method for securing your data within the Teradata environment.

User types DBC (superuser), SYSDBA (database management), and SECADM (security administration) are provided with TD2 authentication and default passwords, which should be changed after initial use.

Monitoring

To make it easier for customers to proactively detect cyberattacks and policy violations, the IntelliCloud security monitoring process intelligently collects and correlates all security-relevant events. Network devices such as border routers and firewalls send intrusion events to our Security Information and Event Monitoring (SIEM) system. When the SIEM detects an intrusion attempt, it responds appropriately based on the type of event detected.

Physical Security

When it comes to physical protection of Teradata Cloud infrastructure, we offer comprehensive support. Teradata data center facilities are staffed 24x7x365 and offer complete video surveillance with best-in-class monitoring and fire safety controls.

In addition to ensuring that every system component entering or exiting our data center facilities has been authorized, documented, monitored, and controlled, each facility meets or exceeds applicable requirements for emergency power, emergency power shutoff, emergency lighting, fire protection, temperature and humidity controls, and water damage protection.

We log and monitor all physical access to the environment to detect and prevent potential security incidents. We also regularly review access logs to pinpoint any suspected unauthorized access and then document such events and coordinate review and investigation with Teradata Corporate Security.

Storage Device Decommissioning

The only storage media used in Teradata Cloud environments are hard disk drives and the primary memory used in the Teradata Cloud infrastructure—and the storage media that customers supply for loading data. These media are stored in locked cabinets within the physically-controlled data center. All media is sent to the data centers via secure courier or by another delivery method that can be accurately tracked.

As part of our decommissioning support, the Teradata Cloud Operations team performs the following actions:

- Sanitizes all digital media prior to disposal, using mechanisms commensurate with the security classification of the information
- Shreds and destroys non-digital data prior to disposal
- Maintains inventory logs of all media and conducts media inventories at least annually

Why Trust Teradata?

Teradata understands the intricacies and importance of network security, access, management, monitoring, and control to protect your data. Our unique combination of industry knowledge, consulting expertise, and best-in-class software offers everything needed for you to assess and maintain the protection you need while enjoying the most effective cloud analytics environment available.

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**.

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

teradata.