GUIDE

YUGABYTE PCI DSS COMPLIANCE GUIDE

yugabyteDB

Table of Contents

Purpose

YugabyteDB is an open source distributed SQL database used by enterprises to build systems of record and systems of engagement for mission critical applications. Yugabyte understands that its customers may leverage YugabyteDB as part of a Customer solution that processes and stores sensitive information. For our customers who are subject to **Payment Card Industry (PCI)** compliance requirements, this Yugabyte PCI Compliance Guide ("Guide") contains a set of recommendations for hardening and secure usage of YugabyteDB.

Scope

YugabyteDB Anywhere is a self-managed database-as-a-service (DBaaS) based on the open source YugabyteDB project. YugabyteDB Anywhere lets customers deploy YugabyteDB across many clouds anywhere in the world with a few clicks, simplifies day to day operations through automation, and provides the services needed to realize business outcomes. This Guide applies to all Yugabyte customers subject to PCI compliance and who are using YugabyteDB Anywhere as a fully customer-hosted solution to manage Yugabyte databases. This document does not apply to YugabyteDB Managed – customers should not use data subject to PCI in YugabyteDB Managed.

Disclaimer

This information is provided by Yugabyte, Inc. ("Yugabyte") and is for general informational purposes only. All information contained within this Guide is provided in good faith, however we make no representation or warranty of any kind, express, or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information contained within this Guide. Additionally, please note that the recommendations provided in this Guide are consistent with PCI DSS compliance requirements but not all PCI compliance requirements are listed; Yugabyte recommends you use this Guide in collaboration with PCI DSS subject matter experts.

How To Use This Guide

This Guide is based on PCI DSS Version 3.2.1. The PCI DSS standard is organized into 6 security domains, each domain with its own set of requirements, with a total of 12 requirements:

1. **Build and Maintain a Secure Network and Systems**
   - **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data.
   - **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters.

2. **Protect Cardholder Data**
   Requirement 3: Protect stored cardholder data.
   Requirement 4: Encrypt transmission of cardholder data across open, public networks.

3. **Maintain a Vulnerability Management Program**
   Requirement 5: Protect all systems against malware and regularly update anti-virus software programs.
   Requirement 6: Develop and maintain secure systems and applications

4. **Implement Strong Access Control Measures**
   Requirement 7: Restrict access to cardholder data by business need to know.
   Requirement 8: Identify and authenticate access to system components.
   Requirement 9: Restrict physical access to cardholder data.

5. **Regularly Monitor and Test Networks**
   Requirement 10: Track and monitor all access to network resources and cardholder data.
   Requirement 11: Regularly test security systems and processes.

6. **Maintain an Information Security Policy**
   Requirement 12: Maintain a policy that addresses information security for all personnel.

This Guide provides guidance on installing, configuring, and managing YugabyteDB Anywhere as part of your PCI DSS-compliant application.

Build And Maintain A Secure Network And Systems

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	• Install YugabyteDB and YugabyteDB Anywhere within the boundaries of your PCI compliant network. • Update your network diagrams to include YugabyteDB and YugabyteDB Anywhere components and corresponding connections.
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.	• Update your data flow diagrams to include data flows to/from YugabyteDB.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	• Update your business justification and approval documentation for firewall and router configuration to include YugabyteDB and YugabyteDB Anywhere components as applicable, including but not limited to protocols and ports allowed. Additional information related to protocols and ports in use by YugabyteDB Anywhere can be located in our online documentation: https://docs.yugabyte.com/latest/yugabyte-platform/security/customize-ports/
1.3 Prohibit direct public access between the internet and any system component in the cardholder data environment.	• Install the YugabyteDB and YugabyteDB Anywhere components within your PCI network boundary and ensure there is no access to any of the YugabyteDB and YugabyteDB Anywhere components from untrusted networks.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	• Install the YugabyteDB and YugabyteDB Anywhere components within your PCI network boundary and ensure there is no access to any of the YugabyteDB and YugabyteDB Anywhere components from untrusted networks.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.)	• YugabyteDB supports two query layers based on PostgreSQL and Apache Cassandra; for the PostgreSQL portion of YugabyteDB, called YSQL, the default account that ships with YugabyteDB is "yugabyte" and must be either disabled or have its password of "yugabyte" changed to a strong password. The default account that ships with the Cassandra portion of YugabyteDB, called YCQL, is "cassandra" and must be either disabled or have its password of "cassandra" changed to a strong password. Instructions for changing the YSQL and YCQL passwords are available here: https://docs.yugabyte.com/latest/secure/enable-authentication/ycql/. Please note, YugabyteDB Anywhere allows the users to both set strong passwords and optionally disable YSQL/YCQL during Yugabyte cluster creation time.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS) International Organization for Standardization (ISO) SysAdmin Audit Network Security (SANS) Institute National Institute of Standards Technology (NIST)	• Apply your documented hardening standards to assets that host the YugabyteDB and YugabyteDB Anywhere components.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	• Ensure that YugabyteDB and YugabyteDB Anywhere are installed on assets dedicated to each respective function. YugabyteDB and YugabyteDB Anywhere should not co-exist on the same host, nor should either of these components co-exist with any other service on the same virtual or physical host.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	• Disable all unnecessary services, protocols, daemons, etc. that are not necessary for the functioning of YugabyteDB and YugabyteDB Anywhere components on your hosts; remove any unnecessary software from the information systems that are hosting the YugabyteDB and YugabyteDB Anywhere components.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	• Disable any unnecessary functionality in YugabyteDB and remove any unnecessary plugins, scripts, drivers, features, subsystems, file systems, etc. • It is recommended to remove network access to unused ports via iptables following “deny-all” by default policy.
2.3 Encrypt all non-console administrative access using strong cryptography.	• Ensure that any YugabyteDB and YugabyteDB Anywhere administrative access traffic is encrypted using strong cryptography. To set encryption in transit see: https://docs.yugabyte.com/latest/yugabyte-platform/install-yugabyte-platform/install-software/default/
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	• Update your PCI inventory of system components to include all assets hosting the YugabyteDB and YugabyteDB Anywhere.

Protect Cardholder Data

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention	• Contact your compliance or security department to determine data retention requirements established for cardholder data, and apply your retention policies accordingly to any cardholder data that is stored in YugabyteDB. Data retention policy requirements could be enforced and managed using a multitude of techniques; establishing procedures or technical controls to enforce data retention policy requirements is beyond the scope of this Guide. • Secure deletion of data can be achieved using various techniques. The method used will largely depend on the architecture of your PCI-based solution, but typically in a cloud computing environment, cryptographic erasure is used to securely delete data in a cloud environment. Additional information on secure destruction techniques can be referenced through NIST Special Publication 800-88 [Guidelines for Media Sanitization]
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	• Ensure that full track/chip data is not stored in your YugabyteDB and YugabyteDB Anywhere instance(s). • Ensure that card validation codes or values are not stored in your YugabyteDB and YugabyteDB Anywhere instance(s). • Ensure that PIN data is not stored in your YugabyteDB and YugabyteDB Anywhere instance(s). ***Note:*** *Reference Appendix A: PCI Storage Guidance for additional cardholder data storage requirements.*

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	• YugabyteDB does not have data masking capabilities therefore you must leverage third party masking/tokenization services to apply data masking to the first six and last four digits of all PANs prior to storing them in YugabyteDB.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One-way hashes based on strong cryptography, (hash must be of the entire PAN) Truncation (hashing cannot be used to replace the truncated segment of PAN) Index tokens and pads (pads must be securely stored) Strong cryptography with associated key-management processes and procedures	• Rendering PAN data unreadable can be achieved via various techniques. The method used for rendering PAN data unreadable will largely depend upon the architecture of your YugabyteDB instance(s). Regardless of the approved method chosen, it is imperative that you ensure it applies to anywhere the PAN is stored (to include backup media, portable media and logs).
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	• Enable disk encryption for your YugabyteDB and YugabyteDB Anywhere installation.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	• Update your documentation to include how encryption keys used in YugabyteDB and YugabyteDB Anywhere are protected. See, for example: https://docs.yugabyte.com/latest/yugabyte-platform/security/create-kms-config/aws-kms/

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	• Ensure that cryptographic keys used in YugabyteDB and YugabyteDB Anywhere are kept in a secure location and that only those with an approved business need have access to that location.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: Encrypted with a key-encrypting key that is at least as strong as the data- encrypting key, and that is stored separately from the data-encrypting key Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) As at least two full-length key components or key shares,in accordance with an industry-accepted method	• Ensure that cryptographic keys used in YugabyteDB and YugabyteDB Anywhere are kept in a secure location and that they are also encrypted via an approved method. See, for example: https://docs.yugabyte.com/latest/yugabyte-platform/security/create-kms-config/aws-kms/
3.5.4 Store cryptographic keys in the fewest possible locations.	• Store cryptographic keys used in YugabyteDB and YugabyteDB Anywhere in the absolute minimum number of locations possible, and that those keys themselves are encrypted. • We recommend to leverage external key management providers supported by Yugabyte. https://docs.yugabyte.com/latest/yugabyte-platform/security/create-kms-config/aws-kms/
3.6.1 Generation of strong cryptographic keys.	• Generate certificates and encryption keys for YugabyteDB and YugabyteDB Anywhere using directions found here: https://docs.yugabyte.com/latest/secure/tls-encryption/server-certificates/

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.	• Develop a procedure to retire and/or replace your cryptographic keys used in YugabyteDB and YugabyteDB Anywhere when they have reached expiration age or when an employee with knowledge of a clear text component of that key departs. https://docs.yugabyte.com/latest/yugabyte-platform/security/enable-encryption-at-rest/#rotate-the-universe-keys-used-for-encryption-at-rest
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	• Yugabyte recommends keys be configured using the following instructions: https://docs.yugabyte.com/latest/secure/tls-encryption/ and https://docs.yugabyte.com/latest/secure/encryption-at-rest/

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	• YugabyteDB supports Transport Layer Security (TLS) encryption based on OpenSSL (v. 1.0.2u or later). Instructions to set up server to server or Client server encryption can be found here: https://docs.yugabyte.com/latest/secure/tls-encryption/ and here: https://docs.yugabyte.com/latest/yugabyte-platform/security/enable-encryption-in-transit/#enforc-ing-tls-versions

Maintain A Vulnerability Management Program

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)	• Install and configure antivirus software on all YugabyteDB and YugabyteDB Anywhere systems in your YugabyteDB and YugabyteDB Anywhere and CDE. • In the case of cloud installation we recommend to use OS images with anti-virus software preinstalled.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	• Reference Yugabyte Guide details in Section 5.1 above.
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7	• Configure anti-virus software to update automatically ensuring that signatures and DAT files are kept up to date for all systems within your CDE including the assets hosting the YugabyteDB and YugabyteDB Anywhere. • Configure anti-virus software on systems hosting the YugabyteDB and YugabyteDB Anywhere and any other systems in your CDE to run regularly scheduled periodic scans and that logs from those scans are created and retained.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	• Use technical controls such as anti-virus application system passwords to prevent your users from uninstalling or otherwise disabling anti-virus software running in your YugabyteDB and YugabyteDB Anywhere and CDE.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	• Run regularly scheduled vulnerability scans against all systems hosting the YugabyteDB and YugabyteDB Anywhere as well as any other system that is part of the CDE. Assign a risk rating for each vulnerability discovered using reputable sources such as CVSS base score and vendor recommendations. Reference the PCI DSS specification for additional details surrounding this requirement.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release.	• Develop and maintain a system and application patch management process that ensures that all systems used for hosting the YugabyteDB and YugabyteDB Anywhere in your CDE as well as any other system within your CDE are patched on a regular cadence and that cadence meets PCI requirements.
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	• Yugabyte is based on PostgreSQL and Cassandra; for the PostgreSQL portion of YugabyteDB, the default account that ships with YugabyteDB is “yugabyte” and must be either disabled or have its password of “yugabyte” changed to a strong password. The default account that ships with the Cassandra portion of YugabyteDB is “cassandra” and must be either disabled or have its password of “cassandra” changed to a strong password. The password can be changed using the following instructions: https://docs.yugabyte.com/latest/secure/enable-authentication/ycql/

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
6.4.5 Change control procedures must include the following: • Documentation of impact • Documented change approval by authorized parties • Functionality testing to verify that the change does not adversely impact the security of the system • Back-out procedures	• Create and maintain a formal change control process for changes to YugabyteDB, YugabyteDB Anywhere, as well as with any other system(s) that are part of your CDE.
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up- to-date secure coding techniques, including how to avoid common coding vulnerabilities • Develop applications based on secure coding guidelines	• Ensure that the front end application(s) you are using with YugabyteDB and YugabyteDB Anywhere have addressed common coding vulnerabilities found (such as the OWASP Top 10) e.g., XSS, SQL injection, Buffer overflow, direct object reference, CSRF attack.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Installing an automated technical solution that detects and prevents web- based attacks (for example, a web- application firewall) in front of public- facing web applications, to continually check all traffic	• If you provide a front end for YugabyteDB and YugabyteDB Anywhere as a public facing web application you should: • At least annually review the web application(s) for vulnerabilities via an automated or manual vulnerability assessment (PEN test) by an organization that specializes in application security. • Install and configure a web application firewall in front of the web application

Implement Strong Access Control Measures

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources	• Create formal documentation that outlines (by role) the levels of access to your YugabyteDB and YugabyteDB Anywhere system components and the CDE contained within. Then assign each user account to a role. • We recommend leveraging YugabyteDB functionality for that as set forth here: https://docs.yugabyte.com/latest/yugabyte-platform/security/authorization-platform/
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	• Do not give Admins access to PCI data within YugabyteDB unless it is needed to perform their job functions.
7.1.3 Assign access based on individual personnel's job classification and function.	• Ensure that access to YugabyteDB and YugabyteDB Anywhere system components and cardholder data is granted via roles and not directly by user accounts. User accounts are to be assigned to roles based upon job classification and function.
7.2 Establish an access control system(s) for system components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components Assignment of privileges to individuals based on job classification and function Default "deny-all" setting	• YugabyteDB has both PostgreSQL and Cassandra APIs; for the PostgreSQL portion of YugabyteDB and to restrict access based upon role see: https://docs.yugabyte.com/latest/secure/authorization/ • Ensure that all access is denied unless specifically granted.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	• Do not create generic and/or shared accounts within or in support of the YugabyteDB and YugabyteDB Anywhere. Each user accessing the cardholder data environment must have a unique user ID.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
8.1.3 Immediately revoke access for any terminated users.	• Develop a process for disabling terminated user's accounts as quickly as possible after their termination.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	• Automatically disconnect sessions after 15 minutes of inactivity.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/ phrases) unreadable during transmission and storage on all system components.	• Yugabyte by default ships with the MD5 setting for passwords. At a minimum this must be changed to SCRAM-SHA-256 whos configuration can be found at: https://docs.yugabyte.com/latest/secure/authentication/password-authentication/. • For additional authentication methods available for use in your environment please see: https://docs.yugabyte.com/latest/secure/authentication/
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least • seven characters • Contain both numeric and alphabetic characters • Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above	• All user passwords used in your YugabyteDB and YugabyteDB Anywhere should be at least seven characters long, have numeric and upper and lower case alphabetic characters.
8.2.4 Change user passwords/passphrases at least once every 90 days.	• All user passwords/passphrases should be changed every 90 days or sooner.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	• Make sure all administrative access to all the systems in PCI scope require multi-factor authentication.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	• Configure your remote access tools authentication mechanisms used to access your YugabyteDB and YugabyteDB Anywhere to require multi-factor authentication for all administrative access into the CDE.
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised	• Train all your users: to create strong passwords and not to reuse previously used passwords.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed • Shared user IDs do not exist for system administration and other critical functions • Shared and generic user IDs are not used to administer any system components	• Ensure that all accounts used to access YugabyteDB and YugabyteDB Anywhere systems are assigned to an actual person (authorized personnel). • Each person accessing the Yugabyte cardholder system(s) must only use the user account assigned to them. • Users must be prohibited from sharing their authentication credentials with any other person.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	• Do not create generic and/or shared credentials within or in support of the YugabyteDB and YugabyteDB Anywhere. Each user accessing the cardholder environment must have a unique user ID.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	• Develop and implement strict access control to any area that contains or could contain cardholder data and to monitor that access to ensure that only authorized individuals have accessed those areas.
9.5 Physically secure all media.	• All systems in the CDE and media containing cardholder data must be secured when unattended.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	• Create a detailed list of all CDE Systems within PCI scope.

Regularly Monitor And Test Networks

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
10.2 Implement automated audit trails for all system components to reconstruct the following events: • All individual user accesses to cardholder data • All actions taken by any individual with root or administrative privileges • Access to all audit trails • Invalid logical access attempts • Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges • Initialization, stopping, or pausing of the audit logs • Creation and deletion of system- level objects	• Implement a SIEM to collect and correlate logs/audit trails from YugabyteDB and YugabyteDB Anywhere and other CDE system components. Logging can be enabled and configured by following instructions found at https://docs.yugabyte.com/latest/secure/audit-logging/ • Please see your vendor documentation for other CDE system components for instructions for enabling audit trails and logging.
10.3 Record at least the following audit trail entries for all system components for each event: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected • data, system component, or resource	• Implement a SIEM to collect and correlate logs/audit trails from all YugabyteDB and YugabyteDB Anywheres and other CDE system components. Logging can be enabled/configured by following instructions found at https://docs.yugabyte.com/latest/secure/audit-logging/ • Please see your vendor documentation for other CDE system components for instructions for enabling audit trails/ logging.
10.4.1 Critical systems have the correct and consistent time.	• Ensure that all critical systems within the YugabyteDB and YugabyteDB Anywhere and your CDE have their system times synced with an industry-accepted time source.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
10.4.3 Time settings are received from industry-accepted time sources.	• Ensure that all YugabyteDB and YugabyteDB Anywhere systems have their system times synced with an industry-accepted time source.
10.5.1 Limit viewing of audit trails to those with a job-related need.	• Ensure that access to Yugabyte system/application logs as well as other PCI-related systems/applications is limited to only those who have a job related need.
10.5.2 Protect audit trail files from unauthorized modifications.	• Lock down the directory where audit trails (logs) are being stored within the system and ship copies of those logs to a SIEM in near real time. See: https://docs.yugabyte.com/latest/secure/audit-logging/
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	• Implement a SIEM or other central log server for all external facing systems.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	• Ensure that File-Integrity-Monitoring (or other change detection software) is configured to alert upon modification of log data within your SIEM solution.
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	• Implement a SIEM to collect and correlate logs and alerts from your Security monitoring systems as well as production systems.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
10.6.3 Follow up exceptions and anomalies identified during the review process.	• Investigate exceptions and anomalies found in your CDE to determine if any findings result in a security incident.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	• Yugabyte recommends implementing a SIEM to collect and correlate logs and alerts from your Security monitoring systems as well as production systems. Have sufficient storage on your SEIM to hold the last three months of log and audit trail history then store a year's worth of log and audit trail history in online or offline storage.
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	• Schedule and conduct (at least quarterly) an internal authenticated vulnerability scan against the YugabyteDB and YugabyteDB Anywhere and any other systems that are part of the CDE.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor(ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	• Schedule and conduct (at least quarterly) an external unauthenticated vulnerability scan against the YugabyteDB and YugabyteDB Anywhere and any other systems that are part of the CDE.
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	• Schedule and conduct vulnerability internal/external rescans of your YugabyteDB and YugabyteDB Anywhere to verify the effectiveness of corrective actions and/or whenever there is a significant change to the CDE.
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	• Schedule and conduct an annual external penetration tests for your YugabyteDB and YugabyteDB Anywhere and entire CDE on at least an annual basis and/or whenever there is a significant change to the CDE.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	• Schedule and conduct an annual internal penetration tests for your YugabyteDB and YugabyteDB Anywhere and entire CDE on at least an annual basis and/or whenever there is a significant change to the CDE.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	• Correct exploitable vulnerabilities found during your penetration tests as soon as possible after discovery and verify the effectiveness of the corrective action with a repeat of the penetration test.
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	• Implement an intrusion-detection and/or intrusion-prevention tool to monitor the perimeter of YugabyteDB and YugabyteDB Anywhere and at key points within CDE.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparison at least weekly.	• Implement file integrity monitoring tools for your YugabyteDB and YugabyteDB Anywhere and configure that software to alert on any unauthorized modifications to critical system configuration or content files.
11.5.1 Implement a process to respond to any alerts generated by the change- detection solution.	• Create play books/run books for each type of alert generated.

Maintain An Information Security Policy

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
12.1 Establish, publish, maintain, and disseminate a security policy.	• Update your security policy and ensure that all of your staff and contractors are trained on that policy.
12.3 Develop usage policies for critical technologies and define proper use of these technologies.	• Update your usage policies for YugabyteDB and YugabyteDB Anywhere.
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).	• Update your documentation and labels for all systems hosting YugabyteDB and YugabyteDB Anywhere to include system owner, contact information and purpose of the system.
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	• YugabyteDB and YugabyteDB Anywhere do not provide remote access capabilities. Remote access to the Yugabyte cardholder data environment must be obtained via a third party technology. Only use remote access technologies that allow for prohibition of copying, moving and storage of cardholder data onto local hard drives and or removable media.
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	• Implement a SIEM to collect and correlate logs and alerts from your security monitoring systems as well as production systems.
12.5.5 Monitor and control all access to data.	• Limit access to cardholder data to those who need it to perform their job duties and to monitor all such access when it occurs.

PCI DSS REQUIREMENT REFERENCE	YUGABYTE GUIDANCE
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity • procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical • system components • Reference or inclusion of incident response procedures from the payment brands.	• Apply your documented incident response plan to your YugabyteDB and YugabyteDB Anywhere components in the event of a system breach.
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	• Either have qualified members of your staff be on call in such a way as to provide 24/7 ability to respond to security alerts or delegate the 24/7 monitoring to a Managed Security Service Provider (MSSP).
12.10.5 Include Alerts From Security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	• Implement a SIEM to collect and correlate logs and alerts from your security monitoring systems as well as your Yugabye solution and CDE production systems.

Appendix A: PCI Storage Guidance

DATA CATEGORY	DATA ELEMENT	STORAGE PERMITTED	RENDER STORED DATA UNREADABLE
Card Holder Data	Primary Account Number (PAN)	Yes	Yes
Card Holder Data	Cardholder Name	Yes	No
Card Holder Data	Service Code	Yes	No
Card Holder Data	Expiration Date	Yes	No
Sensitive Authentication Data	Full Track/Chip Data	No	Cannot Store
Sensitive Authentication Data	CAV2/CVC2/CVV2/ CID	No	Cannot Store
Sensitive Authentication Data	PIN/PIN Block	No	Cannot Store

Appendix B: Definitions

YugabyteDB Anywhere is a Yugabyte product offering that gives you the simplicity and support to deliver a private database-as-a-service (DBaaS) at scale. Use YugabyteDB Anywhere to deploy YugabyteDB across any cloud anywhere in the world with a few clicks, simplify day 2 operations through automation, and get the services needed to realize business outcomes with the database.

YugabyteDB is a high-performance distributed SQL database for powering global, internet-scale applications. Built using a unique combination of a high-performance document store, per-shard distributed consensus replication and multi-shard ACID transactions (inspired by Google Spanner), YugabyteDB serves both scale-out RDBMS and internet-scale OLTP workloads with low query latency, extreme resilience against failures, and global data distribution. As a cloud native database, it can be deployed across public and private clouds as well as in Kubernetes environments with ease.

YugabyteDB and YugabyteDB Anywhere is the suite of proprietary and open-source Yugabyte products.

Cardholder Data Environment (CDE) – The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.