PCI Shared Responsibility Matrix

Chronicle Security

Introduction

Chronicle was designed with security as a core design component. Chronicle uses a variety of technologies and processes to secure information stored on Chronicle's (Google) servers. Chronicle has performed independent validation of Payment Card Industry Data Security Standard (PCI DSS) requirements that apply to Chronicle technologies and infrastructure managed by Chronicle. Chronicle does not control security on the operating system, packages or applications that are deployed by customers in their environments. It is the customer's responsibility to comply with the requirements of PCI DSS that relate to operating systems, packages and applications deployed by customers, or to customer's configurations outside the Chronicle boundary.

Chronicle adheres to the PCI DSS requirements set forth for a level 1 Service Provider. This document outlines each component of the application that customers are solely responsible for or have a shared responsibility for along with Chronicle.

We recommend that customers reference the responsibility matrix in this document as they pursue PCI compliance and find it a useful tool when conducting their own PCI audits.

Definitions

Terms	Description
Chronicle	The Service Provider
Chronicle responsibility	The scope in question is the responsibility of and implemented by Chronicle. A Qualified Security Assessor has assessed and validated this scope and found Chronicle to be compliant with PCI-DSS v3.2.1. This scope, which support the Customer's PCI-DSS efforts but the Customer cannot manage directly, are the sole responsibility of Chronicle
Customer responsibility	The scope in question is the responsibility of and implemented by the customer. Managing this scope is not applicable to Chronicle. Customers of Chronicle bear sole responsibility to meet their own PCI DSS compliance for this scope.
Shared responsibility	Both the customer and Chronicle are responsible for implementing parts of this scope. A Qualified Security Assessor has assessed and validated these specific scope and found Chronicle to be compliant with PCI-DSS v3.2.1. However, Customers of Chronicle share some responsibility and must take action in order to meet their own PCI DSS compliance for this scope.
Service Provider	The Service Provider, as defined by PCI-DSS requirement, is Chronicle
Agreement	Agreement signed between Chronicle and Chronicle's Customer
POS	Point of Sale
PCI DSS	Payment Card Industry Data Security Standard

PCI DSS Responsibility Matrix

Software

- **Forwarder:** Chronicle is responsible for the secure development for the forwarder; however, the Chronicle customer is responsible for the appropriate deployment and management of the forwarder.

Organization and Administration Controls

- **[Req. 12.1]** Customers are responsible for ensuring their information security requirements are considered in the deployment, configuration, and modification of their instance of the Chronicle Services
- **[Req. 12.1]** Customers are responsible for reviewing their information security policies and the security capabilities of the Chronicle Services to determine their applicability to modify or add policies as appropriate
- **[Req. 12.1.1]** Customers are responsible for establishing, documenting, and reviewing policies and procedures addressing transfer and sharing of information within their organization and with Chronicle
- **[Req. 12.1]** Customers are responsible for ensuring that end-users are trained to use the Chronicle Services consistent with their Agreement with Chronicle
- **[Req. 12.1]** Customers are responsible for ensuring that only security telemetry data and no customer cardholder data; together with what is consistent in the Agreement and with the Customer's internal policies are uploaded to the Chronicle Services
- **[Req. 12.1]** Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to the Chronicle Services
- **[Req. 12.1]** Customers are responsible for defining, documenting, and making available to users operating procedures for the operation of their instance of the Chronicle Services

Logical Access Controls

- **[Req. 7.1.a]** Customers are responsible for establishing, documenting, and reviewing policies and procedures addressing the Customer's administration of access to the Chronicle Services
- **[Req. 7.1.1]** Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Chronicle Services consistent with organizational policies
- **[Req. 7.1.2]** Customers are responsible for provisioning, maintaining, and disabling users' access in accordance with their internal access management policies
- **[Req. 8.2]** Customers are responsible for implementing secure log-on procedures to access the Chronicle Services consistent with their access policies
- **[Req. 8.2.2]** Customers are responsible for reviewing users' access rights periodically, consistent with organizational policies
- **[Req. 8.3]** Customers are responsible for enforcing the use of two-step verification on all accounts
- **[Req. 8.1.3]** Customers are responsible for removing users' access rights consistent with organizational policies
- Customers are responsible for establishing procedures to allocate the initial password to access Chronicle Services to end-users when Google password authentication is used
- **[Req. 8.2]** Customers are responsible for training users on the use and disclosure of passwords used to authenticate to Chronicle Services
- **[Req. 8.2]** Customers are responsible for assigning responsibilities for the operation and

monitoring of Chronicle Services
- **[Req. 8.2]** Customers are responsible for configuring domain settings related to integration with Chronicle Services consistent with customer policies
- **[Req. 8.2]** Customer should work with the Chronicle Team to ensure they are configured for the compliant authentication server

Change Management Controls

- **[Req. 6.3]** Customers are responsible for ensuring that individuals creating and/or updating profiles or accessing the Chronicle Services have the proper authorization
- **[Req. 6.3]** Customers are responsible for reviewing and testing, as appropriate, feature and product releases and evaluating their impact consistent with their organization's needs
- **[Req. 6.3]** Customers are responsible for periodically reviewing the configuration of the Chronicle Services to ensure it is consistent with their policies and procedures

Physical Security Controls

- **[Req. 9.1]** Customers are responsible for ensuring the appropriate physical security controls of all devices that access Chronicle Services

Incident Management Controls

- **[Req. 11.1]** Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Chronicle Services
- **[Req. 12.1]** Customers should train administrators and end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Chronicle Services
- **[Req. 11.1]** Customers should contact Chronicle if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account comprise of data and security events

Availability Controls

- **[Req. 12.1]** Customers are responsible for maintaining business continuity plans, including disaster recovery and backup procedures pertaining to the use of Chronicle Service