SECURITY OVERVIEW

Authentication, Authorization, and Data Protection

UPDATED: JULY 20, 2021

hyperview

570-1122 Mainland Street
Vancouver, BC. V6B 5L1

SECURITY OVERVIEW

CONTENTS

Overview

This document describes authentication, authorization, and data protection techniques in the Hyperview cloud-based platform. Topics covered are:

- **Trusted Platform Foundation**
- **Types of Data**
- **Customer Data Isolation**
- **Authentication**
- **Authorization**
- **Stored Credentials Security**
- **Data at Rest Security**
- **Data in Transit Security**
- **Data Collector Security**

Trusted Platform Foundation

Hyperview is deployed on top of Microsoft Azure. It leverages the Azure application security services, continuous vulnerability scanning, and the work completed by Microsoft to certify their data centers for PCI, SOC and other certifications.

Hyperview, as a company, is also investing in its own SOC2 and ISO27001 certifications, which are planned for the 2020 and 2021 fiscal years.

Types of Data

There are four types of data stored in the platform:

User identification data. This is data used by the platform to authenticate a user and is limited to email, first and last name, password, and (optional) phone number. User identification data is owned by the user and is deleted if the user choses to terminate their relationship with Hyperview.

Customer application data. This is data created by the user, collected automatically by a Hyperview Data Collector, or generated while using the application. Examples include asset properties, data center floor layouts, sensor data, application usage log, and asset change logs. Customer application data is owned by the user and is deleted if the user choses to terminate their relationship with Hyperview.

Platform health data. This is data generated by Hyperview that is used to improve the application. Examples include latency data and application errors. Platform health data is owned by Hyperview and is used to improve the performance, stability, and usability of the platform.

Enrichment data. This is data provided by Hyperview to extend customer data. Examples include device attributes and software vulnerabilities. Enrichment data is owned by Hyperview and is used to enrich and improve user provided and collected data.

Customer Data Isolation

Customer application data is stored in two databases.

Time Series Big Data Store

This database keeps anonymized numeric sensor readings over time. For example, a reading would be a timestamp, sensor identifier (UUID), Sensor Type (e.g. Temperature), reading (e.g. 70).

Customer Data Store

All other customer data is kept in a dedicated database that is isolated and dedicated for customer use. This database keeps all Asset Information, Users, Layout, credentials etc.

Authentication

Hyperview customers can create their own dedicated user accounts in the platform or use an enterprise single sign-on with Azure AD/Microsoft 365.

Authorization

Hyperview has the following user roles:

- **Administrator**
- **Data Center Manager**
- **Power User**
- **Reporting User**
- **Read Only User**

User roles define what users can do in the application. In addition, an Administrator can define access controls on specific assets to limit what other users can see and interact with. For instance, a group of users can be restricted from viewing a certain location.

Stored Credentials Security

Hyperview users can add access credentials for managed devices. For example, Hyperview will use a configured SNMP community string to access sensors like current utilization from a managed Power Distribution Unit (PDU). Device credentials are stored in the Hyperview database and encrypted using the Advanced Encryption Standard (AES-256) with keys that are unique to the user. This data is always stored and transported encrypted even over HTTPS.

For data collection, it is recommended to use unprivileged or read-only user levels for device credentials.

Furthermore, the Hyperview roadmap includes offering users the ability to use asymmetric key encryption algorithms and third-party credentials management APIs.

Data at Rest Security

The application is installed in Microsoft Azure and uses the at-rest data protection capabilities of Azure Cloud.

The Data Collector is installed by the customer on a Windows physical or virtual machine. If at-rest data protection is required for Data Collectors, technologies like BitLocker can be employed.

Data in Transit Security

All interactions with the platform from a user (using a web browser) or from a Data Collector (as it communicated with the APIs) is secured with HTTPS.

Data Collector Security

The Hyperview Data Collector can be installed on one or more Windows Server 2016 instances on physical or virtual servers. It collects and relays data back to the Hyperview platform, which lets you monitor and perform operations against the collected data.

The Data Collector must be registered with the platform before it can relay information. Registration is a special handshake that creates a unique identifier to access the platform. The process can only be triggered from the machine that hosts the Data Collector and requires a unique key that is generated by the platform for that Data Collector.

Once registered, the Data Collector secures the key in a configuration file that is stored locally in a secure manner. It will then poll the platform for data collection jobs. Note that all communication between the Hyperview platform and the Data Collector must be initiated by the Data Collector.