Ensuring Data Security Across the Automation Hero_ Platform

Table of Contents

Purpose and Scope

This document outlines and defines the security measures **Automation Hero** follows to maintain the safety and integrity of all data handled by our platform. These measures are designed to:

- minimize the exposure of sensitive data to unauthorized users
- prevent improper use of the platform
- protect the confidentiality of data, even in the case of loss or theft of physical devices

The document's scope is restricted in discussing the security measures of **Automation Hero,** the components of its platform, the data it processes and data it temporarily stores.

This document is intended for readers with a basic understanding of software systems, infrastructure and software security, thus the terminology used is technical in nature. On the next page, we provide a glossary of common acronyms and terms used throughout this document.

Glossary

API
Application Programming Interface

Clickbot
An automation which can record user operation and replay it later

Internet
The world wide web

internet
Interconnected computer networks providing a variety of information and communication facilities

LAN
Local Area Network

RAM
Random Access Memory

REST
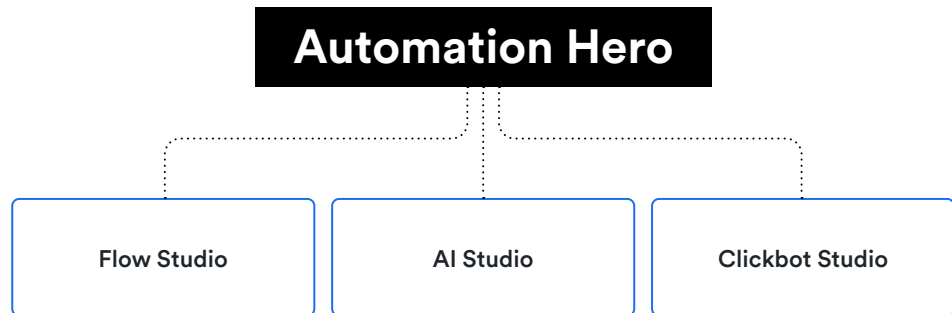Representational State Transfer

SSL
Secure Sockets Layer

TLS
Transport Layer Security

Components of Automation Hero Platform

The **Automation Hero** platform is comprised of several pieces of technology that come together to create our intelligent process automation platform. We refer to each of these separate technologies as components throughout this document. The suite of components include:

Hero_Flow:

This is the heart and brain of the whole platform; it's a scalable cluster built to process large amounts of data and automate busin ess processes. **Hero_Flow** includes three intuitive user interfaces, which allows organizations to build custom automations:

- Flow Studio
- AI Studio
- Clickbot Studio

It exposes important REST APIs that are used by other components of the platform.
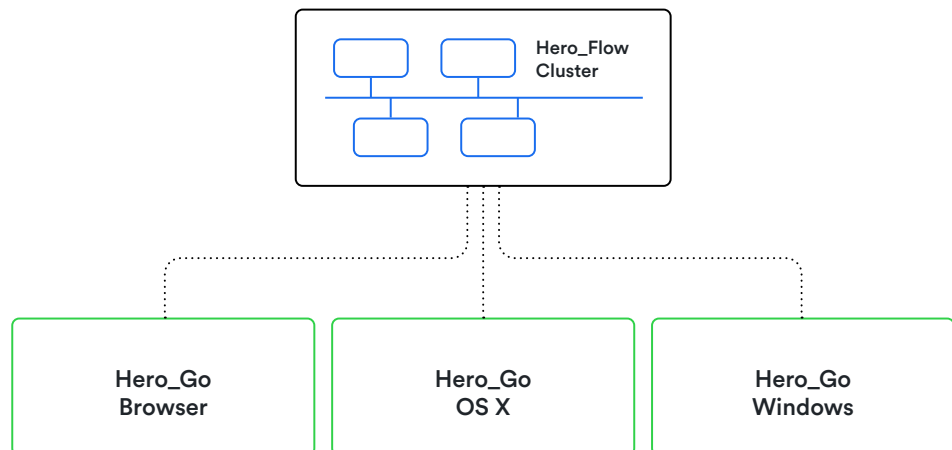
Hero_Go:

Clickbot automation that allows users to record desktop and web workflows as automations and distributes these to end users. This can run on native Windows desktop, OSX based platforms or as a Chrome extension to record web-based automations.

Network

All aspects of the platform are on the same network, enabling them to communicate with each other, which can be achieved through various network topologies.

The simplest is a LAN shared by all components of the platform, which allows complex systems to be connected. Hero Go/Native/Browser and the **Hero_Flow** cluster operate on different networks, but are connected through an internet.

The software doesn't need the Internet for the different components to communicate with each other, however Internet may be required for installation.

Several of the components in the network come with an easy-to-use, intuitive user interface. The components don't require complex configurations to be set up or to initiate communication over the network.

Apart from these network components, **Automation Hero** can communicate to the user via other channels, such as email. In this case, the platform needs to leverage the organization's email network.

Application Security

Automation Hero makes an effort to provide various security dimensions for our customers, all of which are transparent and enterprise-ready. **Automation Hero's** robust security protocol ensures customers can combat security threats and protect personally identifiable information (PII). Our authentication, authorization and encryption capabilities secure the system while keeping it in full compliance. We will discuss each dimension separately in its respective section.

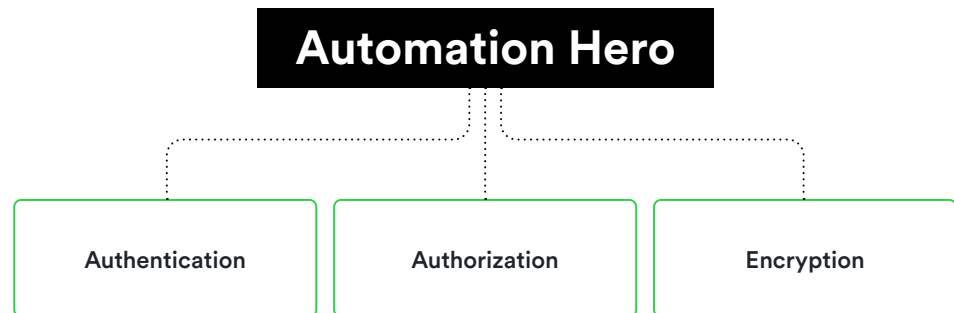**Authentication**
the process of identifying an individual

Authorization
granting or denying access to a network resource

Encryption
translation of data into a secret code

Automation Hero

Authentication	Authorization	Encryption

Authentication

Each component of **Automation Hero** supports multiple authentication mechanisms to ensure a user's identity while interacting with the platform. It also supports various pluggable authentication frameworks, such as:

- OAuth 2.0
- LDAP/AD
- SAML
- Plain Database User ID/Password
- Kerberos

Authorization

Automation Hero provides role-based access with delegation, reserving certain actions for super-user/admin only. Artifacts created by a user remain under their control until they are shared at the group level. This applies to Flows, AI Models, Connectors, Sources, Sinks and Clickbots.

Hero_Flow allows granular configurations of individual security capabilities, including:

✓ Pluggable encryption algorithms and strength

✓ Encryption of data from source to data flow

✓ Encryption of data from data flow to sink

✓ Encryption of any temporary written data (e.g. when data needs to be cached for a reduce-side join)

✓ Encryption of all communication between the node if configured

✓ Https access for the web-based admin console

✓ Integration into authentication providers such as OAuth, OAuth2, LDAP or Microsoft Active Directory

✓ Audit and access logs

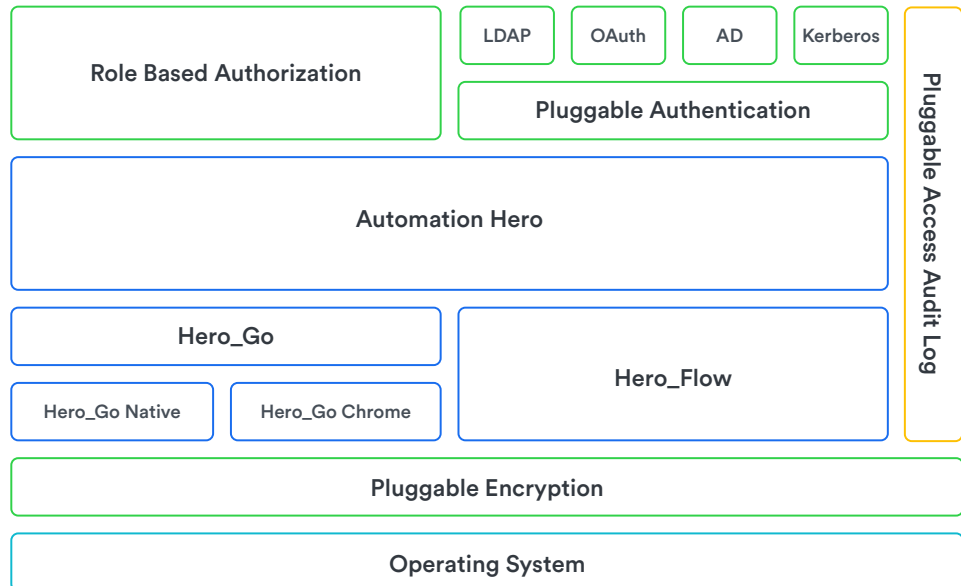✓ Encryption key rotation (on request)

Encryption

Automation Hero ensures that all data, in any condition, is encrypted when interacting with our system, other than when it is processed in the primary memory (RAM and register). The data is encrypted both as it is transmitted over the wire and when it is stored on a disk (even if only temporarily).

The platform is responsible for the encryption of stored data while it is under the control of the platform. Any data that is pulled from, or written to, external endpoints (such as a database) aren't controlled by **Automation Hero**. The platform provides a plug-in approach for data stored on a disk, which uses a symmetric encryption algorithm. Organizations can customize which encryption algorithm to use for data storage. Further, the platform allows the facility of key rotation based on different configurable policies.

The platform uses SSL (TLS) to ensure network communication is also encrypted and prevents potential attackers from viewing the communication channels.

Web Security

Automation Hero supports secured HTTP for the web-based admin console of **Hero_Flow** as well as the REST APIs exposed by the system.

Centralised Access Audit Logs

The audit logger is a pluggable module that allows administrators to choose a logger based on the location of the log destination. This can be on a flat file, database or other destination.

This can be used on any operation which includes access to a protected resource, like:

- Accessing a Connection, Source, Sink, Flow, Clickbot
- User authentication request
- Access of secured web pages

Backup Strategy

Data backup is one way the platform combats potential disaster recovery. Disasters could be as simple as a hardware failure or as serious as a complete collapse of the system.

There is no single point of failure for the **Automation Hero** platform. A new cluster in the node adds new processing power without adding a system failure point. In case of failure due to a bad hardware component or if a node has failed, the system can recover by removing the node from the cluster. A new node can then be started to replace the failed node. **Automation Hero** doesn't require storage or backup of the running system to recover from such a disaster.

Should a disk/system failure occur, the internal data and metadata written by the **Automation Hero** platform is stored on a shared file system using a fault tolerant and distributed file system with replication enabled.