




# How Hero Platform\_ ensures data security with process automation technology

# 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**

Here, we'll discuss Automation Hero's security measures, the components of its platform, the data it processes, and the data it temporarily stores.

With more consumers adopting a digital-first approach to how they engage with businesses, there's more opportunity for data to be stolen. This danger is compounded by the rise of remote work, which requires employees to transmit sensitive information between their company's databases and their computers at home, co-working spaces, or coffee shops.

As a result of all this exposure, data breaches are becoming increasingly common. According to Symantec, [roughly 4,800 websites are compromised every month](#). The consequences are becoming increasingly severe, as well. As of 2021, [the average cost of a data breach \(including penalties, damages, and corrective actions\) is \\$4.24 million](#), up from \$3.86 million the previous year. Companies also suffer a tarnished reputation, which can have a substantial, though hard to quantify, impact on revenue.

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.

# Network Security

Hero Platform\_ is deployed in secured single-tenant environments in the cloud in AWS infrastructure.

## Glossary

### API

Application Programming Interface

### 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

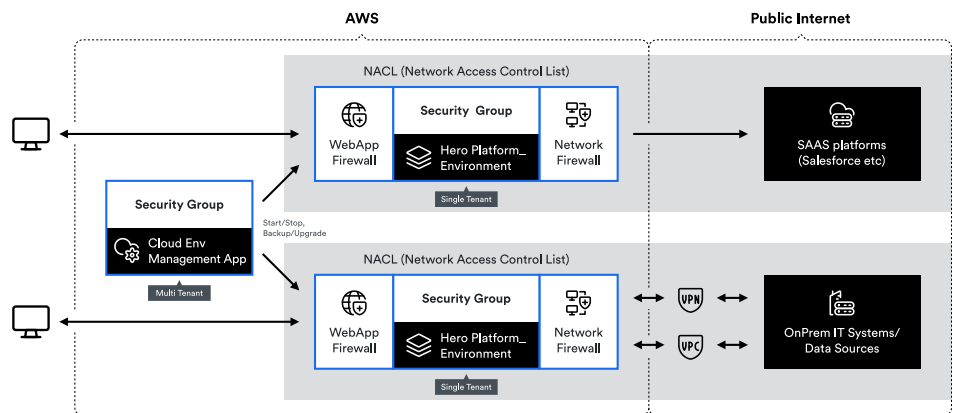
### TLS

Transport Layer Security

By default, access to the environment is restricted exclusively to the web interface which can be further locked down through a firewall configuration to selected host(s).

Connecting to data sources from the AWS ecosystems does not guarantee that the data will be traveling through AWS pipelines even if both Hero Platform\_ and customer AWS data sources are deployed in the same AWS region. This means that data between them could potentially travel through the open internet.

Through VPC peering, the Hero Platform\_ can be plugged into the customer's existing private networks ensuring all traffic between the deployments go through AWS wires and never travel through the open internet.



# 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

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



## Authorization

granting or denying access to a network resource

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 Document Extractors, HITL skills, Connectors, Inputs, and Outputs.

Furthermore, Administrators can customize access control in the application by defining custom roles and associating the necessary permissions for users. This flexibility allows tighter security controls if for example in your organization a group of users are only allowed to setup connections but not see anything else in the application.



## Encryption

translation of data into  
a secret code

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 organizations to manage their own encryption keys further ensuring they are the only ones able to decrypt the data and set up key rotation policies as needed.

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.

Hero Platform\_ allows granular configurations of individual security capabilities, including:

- Pluggable encryption algorithms and strength
- Encryption of data from input to data flow
- Encryption of data from data flow to input
- 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)



## 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, Input, Output
- 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.

**Disclaimer:** The information within these documents is confidential, privileged, and meant only to provide further knowledge to the intended recipient. The contents of this document may not be used, published, or redistributed without prior written consent from Automation Hero, Inc.

There is no single point of failure for the Automation Hero platform. A new node in the cluster 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 in order 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.

Despite all of these built-in resilience capabilities in the platform, the Hero Platform\_ performs snapshot backups of the current environment state automatically so the environment can be recovered in another region if complete failure in the primary region were to happen.

Furthermore, Administrators can have control over the frequency and schedule of these automatic snapshot backups and adjust them to better match business needs.

**To learn more about how Automation Hero protects customer data through process automation technology, schedule a free, personalized product demo.**

[Schedule a demo](#)