Hero OUTBOUND

Technical Description

Hero Outbound Platform Security & Data Privacy

Version 1.14 July 2019

Table of Contents

1. Introduction

Success is built on trust. And trust starts with information.

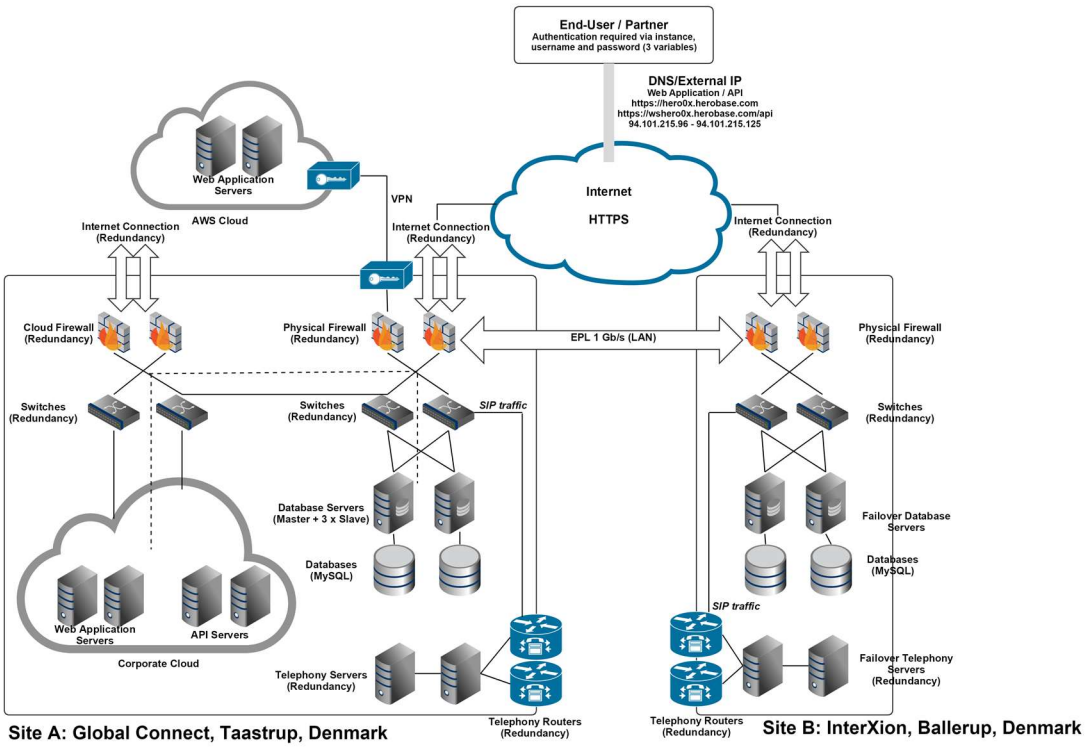
In this document you will read what platform security measures have been put in place by HeroBase A/S ("HeroBase") to provide our customers with best of breed telephone sales dialer. Specific information is available on request.

The following elements of Hero Outbound platform and service are described in this document:

- Platform Architecture
- Backup
- Security
- Privacy
- Data Centres

2. Hero Outbound platform architecture and protection

Hero Outbound platform is an intelligent hosted Software as a Service (SaaS) telephone sales solution designed to operate 24/ 7/ 365 with maximum availability superior to 99.8% and so with the full redundancy and multiple levels of backup.



With regards to network protection there is failover internet and redundancy. Failover internet and internet redundancy is achieved by multiple WAN CARP Firewalls connected by multiple third-party internet providers, which continuously provide redundant internet access.

There are perimeter firewalls that block unused protocols. The sensors throughout the internal network report events to a security event management system for logging, alerts and reports.

3. Hero Outbound Backup

All data are backed up at a daily basis. Data is continuously synchronized to backup servers, located on the premises.

Additional data backup sets are also created each night and uploaded to external servers, at a separate data center.

High availability is achived through the use of virtualization, thus utilizing ressources more effectively and providing a very robust and redundant infrastructure.

Within Site A (Global Connect, Taastrup, Denmark), one Master database and three Slave databases are running and kept synchronized via MySQL replication jobs. Within site B (InterXion, Ballerup, Denmark), two Slave databases are running and kept synchronized with the Master database via MySQL replication jobs.

4. Hero Outbound Security

4.1 Security statement

Hero Outbound utilizes some of the most advanced technology for Internet security available today. When you access our service using industry standard Secure Socket Layer (SSL) technology, your information is protected using both server authentication and data encryption, ensuring that your data is safe, secure, and available only to registered users in your organization. Your data will be completely inaccessible to any other users or 3rd parties.

Hero Outbound provides each user in your organization with a unique user name and password that must be entered each time a user logs on.

In addition, Hero Outbound is hosted in a secure server environment that uses a firewall and other advanced technologies to prevent interference or access from outside intruders.

Fail2Ban mechanisms are in place in front of publicly exposed services, meaning that IP addresses are banned at firewall level when multiple logon attempts using incorrect credentials are detected.

Upon request, HeroBase can establish an IP based whitelist-only logon procedure at customer (corporate) level, meaning that logins will only be authenticated given that they origin from a list of IP addresses agreed on (and maintained) with the end-customer.

4.2 Secure transmission and sessions

Connection to the Hero Outbound environment is via SSL, using certificates, ensuring that our users have a secure connection from their browser to our service.

Individual user sessions are identified and re-verified with each transaction, using a unique session ID created at login.

4.3 Security monitoring

Our Information Security department monitors notification from various sources and alerts from internal systems (including, but not limited to, Fail2Ban services mentioned in section 4.1) to identify and manage threats and handle incident- and management.

5. Hero Outbound Data Privacy

5.1 Data privacy objective

The privacy and security of our customers' data is at the paramount of importance for HeroBase. We believe that protecting the privacy of our customers' data is integral to our mission of earning and maintaining the trust of each of our customers. We seek to lead the industry as a trusted service for premium telemarketing sales productivity tool through a privacy program and provide a secure infrastructure and flexible tools that help enable our customers to comply with global privacy and data protection regulations.

5.2 Data privacy statement

5.2.1 Information collected

When you request additional information or register on herobase.com, we ask you to provide basic contact information.

HeroBase uses common Internet technologies, such as cookies to keep track of interactions with HeroBase website and emails.

5.2.2 Use of information

HeroBase uses information collected to provide you with the services and the assistance you request and need.

HeroBase may use information collected to provide you with additional information about HeroBase company’s services, partners, promotions, and events.

HeroBase may use information collected to improve HeroBase website and services.

HeroBase does not share, sell, rent, or trade personally identifiable information with third parties for their promotional purposes.

For non-customers, i.e. unknown users/potential customers visiting our websites and submitting their contact information (up to and including name, company name, e-mail address and telephone number), information is stored for 6 months, after which it will be deleted. For customers, i.e. potential customers getting a test account for our software and eventually signing a contract with us, by which point he/she is converted into an actual customer, the information is stored and used (according to the descriptions in this document section) throughout the customer relationship and maximum 6 yeas after this has come to an end, due to laws about storing documentation for economic transactions.

5.2.3 Customer data

HeroBase users may electronically submit data or information to the Hero Outbound platform.

HeroBase will not review, share, distribute, or reference any such customer data except as provided in the HeroBase agreement or as may be required by law. In accordance with the HeroBase agreement, HeroBase may access customer data only for the purposes of providing the services, preventing or addressing technical problems, at customer's request in connection with customer support cases, or as may be required by law.

As part of standard procedure between HeroBase and the customer, a Data Processing Agreement will be prepared, stating clearly responsibility and task ownership distributed between the customer (the Data Controller) and HeroBase (the Data Processor). HeroBase happily provides our standard Data Processing Agreement to the customer for their review and signing, but also happily receives the customer's version of a Data Processing Agreement for our review. It is however an ultimate requirement that the Data Processing Agreement clearly defines Obligations of the Data Processor, has a clear description of processes related to Transfer of data to other data processors and third parties, and has a clear description of processes related to the unlikely event of Data Leak.

As the Data Processing Agreement states, HeroBase acts as data processor on behalf of the customer, who acts as data controller, and will as such act on instructions only. The boundaries of the instructions are the services to be delivered as described in the contract between the customer and HeroBase. HeroBase and any personnel of HeroBase will never access, read, export, modify or delete any of the customer's data unless clearly requested by the customer as part of delivering the services described in the contract – e.g. support. If HeroBase personnel is to access, read or export data, instructions must be provided by an approved contact person of the customer in talking or writing. If HeroBase personnel is to modify or delete any data, instructions must be provided on the same premises, but in writing. If HeroBase personnel accesses and/or exports data following instructions provided by the customer, the HeroBase employee must do so via a safe mechinasm exclusively for HeroBase personnel, meaning the customer does not need to share login and password. Afterwards, the HeroBase employee must log out safely. Data must not be saved/stored locally in any ways by the HeroBase employee, who must, if this has been necessary temporarily to filful the customer's request, delete all data stored locally immediately.

6. Data Centres

6.1 Introduction

HeroBase understands that the confidentiality, integrity and availability of our customers' information are of extreme importance to their business operations. We use a multi-layered approach to protect customer data information, constantly monitoring and improving our application, systems and processes to meet the growing demands and challenges of security.

At HeroBase we believe in using a standardized approach to operations and security, which is why we have chosen to implement ISO 27001 as the foundation for our ISMS, and are relying on elements from the ITIL framework in order to provide our customers with high service availability.

6.2 Data locations & sub-data processors

Our service is collocated at (a) Global Connect, Taastrup, Denmark; (b) Interxion, Ballerup, Denmark; and (c) AWS (Amazon Web Services), services within the Dublin and Frankfurt locations, i.e. AWS region = EU (Ireland) and AWS region = EU (Frankfurt).

All data centres are driven based on international standards ensuring that strict requirements to service level and security are followed. Standards include (and are not limited to) the ISAE 3402 type 2 standard certified by BFIH. This includes, among other things, that access is restricted to a few trusted employees; that each person who may access the sites only can do this using key, chip and password; and that eye scanning or fingerprint detection takes place as part of entering the server locations. Furthermore the sites are protected by guards, double fence, electronic locks etc.

Sub-data processors in use by HeroBase A/S are always published and listed on HeroBase's website – link to the particular subpage displaying sub-data processors for all solutions is the following: https://herobase.com/sub-data-processors/

6.2.1 Climate control

For optimum performances, all equipment is maintained and continuously monitored in a climate-controlled environment. The average room temperature is controlled between 22°C ± 2°C and a humidity level of 50% ± 10%. Multiple air conditioning units provide redundant capacity.

6.2.2 Water detection

Water detection systems are installed in all areas that may be susceptible to leakage. The water detection alarms are relayed directly to the Global Connect or Interxion main Support centre.

6.2.3 Security

Interxion and Global Connect data centre buildings are designed as "buildings within buildings," and are protected around the clock by security guards and monitored video

surveillance cameras. No one enters or leaves without proof of identity, and all visitors are checked against customer-defined access lists. All building areas are secured by an alarm system, and an external security firm patrols the area, both inside and outside.

For security purposes, the exact location of the AWS data centres in Dublin and Frankfurt is not publically known.

Ahead of initializing cooperation with our data centres as sub-data processors, the vendors have been evaluated and requirements have been put through to them, making sure that the same security level as described between HeroBase and our customers, is in place between HeroBase and subcontractors. Measurements include (and are not limited to) collecting and reviewing an ISAE 3402 type 2 (or similar) at a yearly basis, according to our ISMS.

6.2.4 Power & Cabling

230V AC and 400V AC, UPS, -48V DC with battery backup providing continual power. All data centres are backed up by N+1 diesel driven generators with 24 hours fuel storage.

Power cabling is laid under raised anti-static computer flooring. Data cabling is usually in trays overhead, and can also be laid beneath the flooring.

6.2.5 Fire protection and suppression

Fire-retardant walls, early warning laser smoke detectors (underneath and above the flooring), direct lines to fire stations, and automatic gas-based fire suppression systems provide world-class protection against fire.

6.2.6 Systems monitoring

HeroBase internal operations team makes use of a state-of-the-art monitoring tool that watches over servers, operating systems, network devices and web sites - 24 hours a day, 365 days a year. A wide range of parameters are monitored against pre-defined thresholds.
The solution helps us to identify problems BEFORE they occur, and thus perform pre-emptive actions in order to avoid service disruptions.

7. Data Flows Examples

With reference to section 2 and 4, the Hero Outbound architecture allows end-users and (subject to written approval by the customer and creation of unique, secure accounts) partners/certified third-parties to interact with customer data via the Hero Outbound webapplication user interface or the Hero Outbound API, the latter using the REST protocol also over HTTPS.

Based on the diagram in section 2, the below figure illustrates how, and through which network points, data will flow when accessed by end-users or partners/certified third-parties through the user interface or the API. The grey bars illustrate how data flows (principally, simplified).