LOGIQAL HEALTHCHECK PRO

CYBER SECURITY DATASHEET

Does Logiqal Healthcheck Pro compromise server security?

Logiqal Healthceck Pro is a cloud-based monitoring software allowing users of Secure Logiq server hardware to easily monitor key components of all the machines they have deployed in the field. For the Healthcheck monitoring and alerting solution to work the server must have a connection to the internet and be running the Healthcheck service. The functionality has raised the question of cyber security and rightly so. Below are a series of bullet points in which I will deliver more detail on throughout the document.

- Deployed server hardware connects back to the datacentre
- Unique hash key for each company as well as unique serial number per machine
- Remote server & browser connections use SSL encryption for all data
- Multiple user levels restricting functionality
- Future implementation of two stage authentication

Deployed server hardware connects back to the datacentre

The benefit of having Healthcheck Pro connecting back to our data centre rather than having the datacentre server connect into the remote machine offers significant security as well as making configuration and setup much easier.

Working in this manner means you do not need to know the public IP address of the server, there is no port forwarding or other router configuration to be done. All incoming connection ports could in theory be blocked whilst allowing just port 443 as an outgoing connection and Healthcheck would be able to establish communication with the datacentre.

In summary Healthcheck does not accept any incoming connections meaning you don't need any additional ports open to the outside world which can increase the risk of external cyber threats. It also makes setup and configuration of Healthcheck Pro extremely simple.

Unique hash key for each company as well as unique serial number per machine.

During the installation process of Healthcheck Pro it requires the randomly generated hash key for the company in which the server will be assigned as well as the unique serial number of the machine. Without both of these being correct and matching up with our internal database of customers and serial numbers of built machines the installation will fail, or the connection will not be authorised.

This makes the connections coming into our data centre limited to only machines that are supported by Secure Logiq and prevents any malicious connections accessing our cloud server.

The installation of Healthcheck Pro is done in house during the manufacture process for new machines and will require remote access from one of Secure Logiq's support staff for installation on any legacy machine.

The installation package is not publicly available which limits deconstruction of our software for potentially malicious purposes.

Remote server & browser connection use SSL encryption for all data.

SSL encryption is the standard for online banking as well as large ecommerce sites and prevents your data from being intercepted by a third party when performing transactions. For this reason, the deployed servers communicate through an SSL encrypted connection back to the data centre. SSL certificates must be purchased and licensed on a yearly basis, so they remain valid.

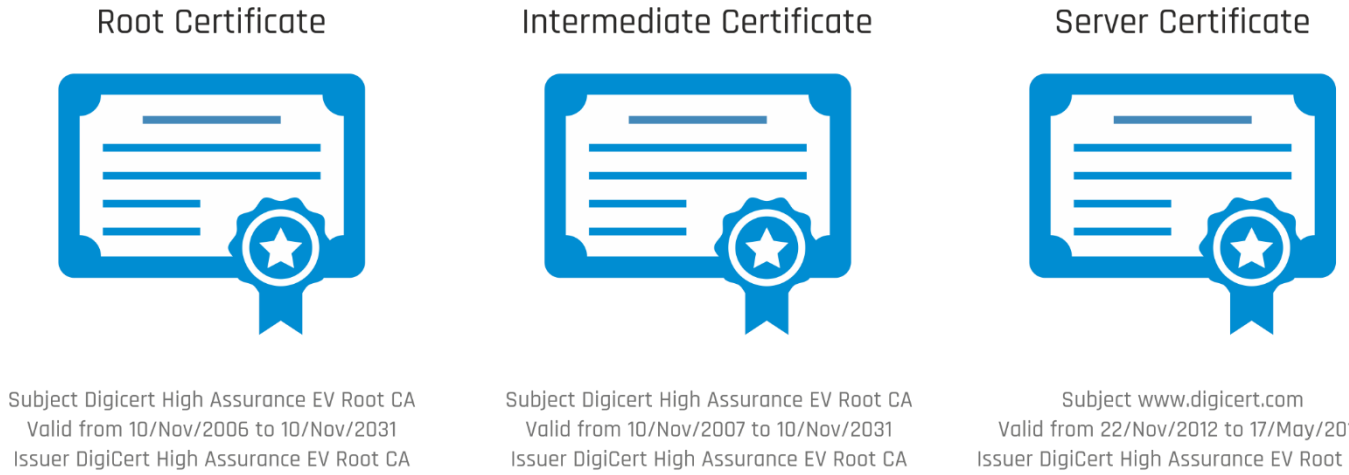
Remote servers deployed in the field connect back to the datacentre using SSL encrypted connections as well as the browser session for viewing and monitoring the hardware.

SSL certificates have a key pair: a public and a private key. These keys work together to establish an encrypted connection. The certificate also contains what is called the "subject," which is the identity of the certificate/website owner.

To get a certificate, you must create a Certificate Signing Request (CSR) on your server. This process creates a private key and public key on your server. The CSR data file that you send to the SSL Certificate issuer (called a Certificate Authority or CA) contains the public key. The CA uses the CSR data file to create a data structure to match your private key without compromising the key itself. The CA never sees the private key.

Once you receive the SSL certificate, you install it on your server. You also install an intermediate certificate that establishes the credibility of your SSL Certificate by tying it to your CA's root certificate.

In the image below, you can see what is called the certificate chain. It connects your server certificate to your CA's (in this case DigiCert's) root certificate through an intermediate certificate.



The most important part of an SSL certificate is that it is digitally signed by a trusted CA, like DigiCert. Anyone can create a certificate, but browsers only trust certificates that come from an organization on their list of trusted CAs. Browsers come with a pre-installed list of trusted CAs, known as the Trusted Root CA store. In order to be added to the Trusted Root CA store and thus become a Certificate Authority, a company must comply with and be audited against security and authentication standards established by the browsers.

An SSL Certificate issued by a CA to an organization and its domain/website verifies that a trusted third party has authenticated that organization's identity. Since the browser trusts the CA, the browser now trusts

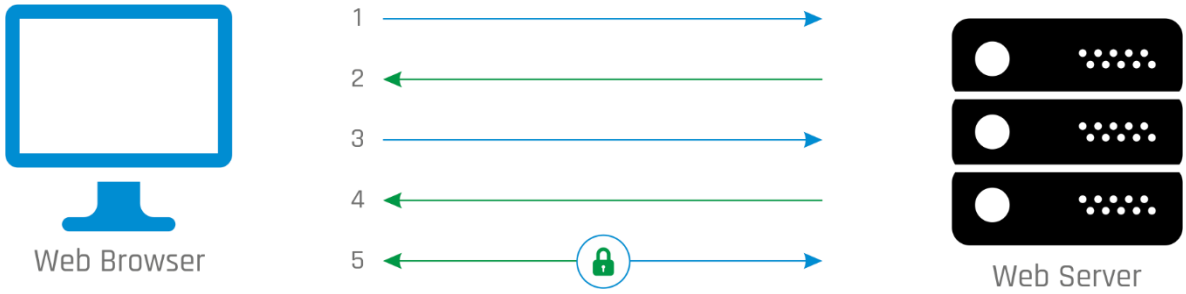
that organization's identity too. The browser lets the user know that the website is secure, and the user can feel safe browsing the site and even entering their confidential information.

How Does the SSL Certificate Create a Secure Connection?

When a browser attempts to access a website that is secured by SSL, the browser and the web server establish an SSL connection using a process called an "SSL Handshake" (see diagram below). Note that the SSL Handshake is invisible to the user and happens instantaneously.

Essentially, three keys are used to set up the SSL connection: the public, private, and session keys. Anything encrypted with the public key can only be decrypted with the private key, and vice versa.

Because encrypting and decrypting with private and public key takes a lot of processing power, they are only used during the SSL Handshake to create a symmetric session key. After the secure connection is made, the session key is used to encrypt all transmitted data.



Browser connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.

Server sends a copy of its SSL Certificate, including the server's public key.

Browser checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.

Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.

Server and Browser now encrypt all transmitted data with the session key.

Multiple user levels restricting functionality

Once a request to setup a Healthcheck Pro account has been made an admin account will be provided. The user of this admin account has the ability to create different levels of users, restricting what they can change and see within the software. Whilst there are no settings available that could compromise security of the security system being able to remove a user if required is fast and easy for an admin.

Future implementation of two stage authentication

For added security from user login side to the system, there are plans to add the option to enable two stage authentication for users. This removes any potential for brute force password cracking of the web interface.