WHITE PAPER

Logical Healthcheck Pro Cyber Security

Does Healthcheck Pro compromise server security?

www.securelogiq.com I info@securelogiq.com

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 which we 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 data centre

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

SSL encryption is the industry standard for secure online communication, used by online banking and major e-commerce platforms. It ensures that data transmitted between a client and server cannot be intercepted by third parties.

All Secure Logiq servers deployed in the field communicate with our data centre using SSL-encrypted connections. Similarly, browser sessions used to monitor and manage the hardware are also secured via SSL encryption.

How SSL Encryption Works

SSL certificates are based on a **public/private key pair**. These keys work together to establish an encrypted connection:

1. A **Certificate Signing Request (CSR)** is generated on the server, which creates a public and private key.
2. The **public key** is submitted to a Certificate Authority (CA), while the **private key** remains securely stored and never shared.
3. The CA uses the CSR to issue a signed SSL certificate that verifies the identity of the organisation or domain.

To establish full trust, the server must install:

- The **SSL certificate** (issued to the server),
- An **intermediate certificate** (issued by the CA),
- A **root certificate** (pre-trusted by browsers and operating systems).

Understanding the Certificate Chain

The certificate chain builds trust by linking your SSL certificate to a recognised, pre-installed root certificate via an intermediate authority. Here's an example structure:

Root Certificate

- Subject: DigiCert High Assurance EV Root CA
- Valid: 1 Nov 2006 – 1 Nov 2031
- Issuer: DigiCert High Assurance EV Root CA (self-signed)

Intermediate Certificate

- Subject: DigiCert Intermediate Certificate Authority
- Valid: 1 Nov 2007 – 1 Nov 2031
- Issuer: DigiCert High Assurance EV Root CA

Website Certificate (End-Entity Certificate)

- Subject: www.digicert.com
- Valid: 22 Nov 2012 – 17 May 2014
- Issuer: DigiCert Intermediate Certificate Authority

Each level in the chain adds credibility to the one below it. This structure ensures that a browser can trace the server's certificate back to a trusted root authority.

Why Trust Matters

Browsers only trust certificates signed by recognised Certificate Authorities (CAs) listed in their Trusted Root CA Store. To be listed, a CA must undergo strict security audits and comply with industry standards.

When you visit a secure site, your browser:

- Checks that the SSL certificate is valid and signed by a trusted CA,
- Confirms the identity of the organisation behind the website,
- Establishes a secure connection using a temporary session key, created during the SSL handshake.

This process is invisible to the user, but critical to secure communication.

How Does an SSL Certificate Create a Secure Connection?

When a browser attempts to access a website secured by SSL, it initiates a process called an SSL Handshake. This process is invisible to the user and happens almost instantaneously.

The handshake uses three types of keys to establish a secure connection:

- A **public key**
- A **private key**
- A **session key**

The public and private keys are used only during the handshake because encrypting with them is resource-intensive. Their purpose is to securely generate a symmetric session key, which is then used to encrypt all ongoing data transmission between the browser and the server.

The SSL Handshake Process:

1. The browser connects to a web server secured by SSL (https) and requests the server's identity.
2. The server responds by sending its SSL Certificate, which includes its public key.
3. The browser verifies the certificate by checking:
   - Whether it's signed by a trusted Certificate Authority (CA)
   - That it hasn't expired or been revoked
   - That the domain name matches
4. If the certificate is trusted, the browser creates a symmetric session key, encrypts it with the server's public key, and sends it back.
5. The server decrypts the session key using its private key and acknowledges the connection.
6. From this point forward, both server and browser encrypt all communication using the shared session key.

Multiple User Levels Restricting Functionality

Once a Healthcheck Pro account is set up, an admin-level user is assigned. This user can create additional accounts with restricted access, limiting what each user can see or modify. This access control helps maintain system integrity while ensuring users only interact with relevant features.

Future Implementation: Two-Stage Authentication

To further enhance security, Secure Logiq plans to implement optional two-stage authentication for Healthcheck Pro. This will provide extra protection against brute-force attacks on the web interface and ensure secure user logins.