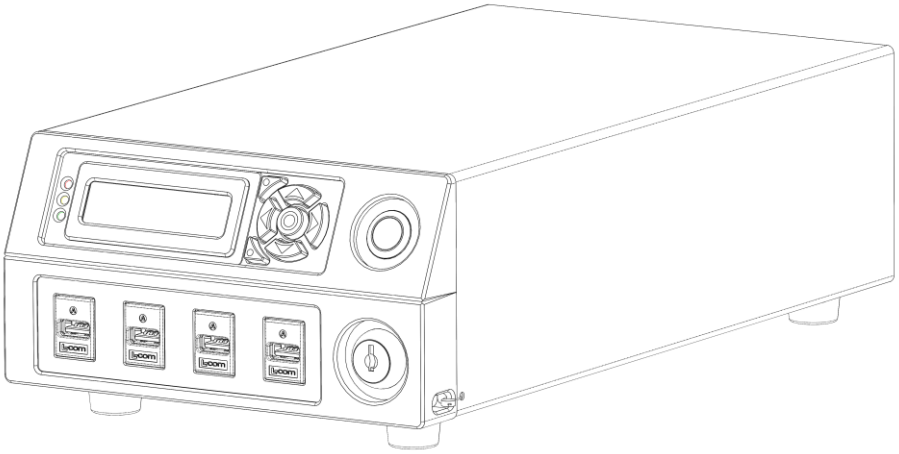
The Hunna system - whitepaper

Version 1.4

Document nr WSL190201



Contents

1 PURPOSE OF THE HUNNA SYSTEM

The Hunna system has arisen from the following requirements:

1. To enable import of information into critical air-gapped information systems, without the risk of malware infection.

2. To enable import of information on commonly used media, such as USB-media, CD/DVD and other media that may be connected through a reader that is connected to a USB-port.

3. To act as an external device that becomes the first surface of attack, thus protecting the critical information system.

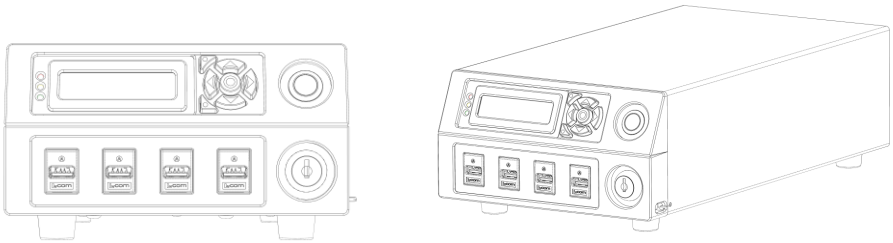
4. To be impossible/extremely difficult to manipulate through built-in security features, including high-assurance security components.

5. To guarantee that no forensic traces of scanned information remain in the device between scan cycles, as this would otherwise provide a risk in itself through concentration of sensitive information in digital forensic form. The Hunna system thereby avoids the scanning system becoming “contaminated” with sensitive information.

6. To enable the Hunna system to become digitally connected with the information system it protects through certificates, enabling a function for the receiving information system to only accept media that has come from the customers specific device(s), thus eliminating the risk of human error to inadvertently (or purposely) connect potentially infected media to the critical information system.

7. The system shall perform standard operational functions automatically, i.e. without the user having to enter information or perform certain functions. Ease of use is a key parameter to ensure that the Hunna system is used correctly.

2 TECHNICAL SPECIFICATIONS



Measurements	The device	Device incl packaging
Height	104 mm	188 mm
Width	180 mm	502 mm
Depth	328 mm	400 mm
Weight	3,5 kg	7,5 kg

Energy requirements: The Hunna device is powered by an electrical adapter with the output of 19 V 4.74 A.

3 SYSTEM OVERVIEW

3.1 The Hunna device

The Hunna system is a security platform which can run almost any type of security function, and also includes a number of security features already configured into the platform, including multiple Anti-Virus functions, whitelist and quarantine list.

Certain functions, such as the fully customisable Optional security process, can be configured to replace or complement other security processes.

3.1.1 Basic overview

The basic function is that the device copies files from the Source-media to the Target-media, and passes through a number of security functions on the way.

Any files that contain malware will be copied to the Quarantine-media, and those files will not be copied to the Target-media.

Logs are stored on Target-media and on Quarantine-media.

The system initiates scanning once media is connected to the Scan-port. If media is to be copied for entering into a critical information system, media needs to be connected to the Target-port, and that media then connected to the critical information system following the scan-copy process. If malware is found, this can be received for analysis by entering USB-media to the Quarantine-port.

Once the process is performed the system will request that all USB-media is disconnected. Removing all media will prompt the system to reboot and prepare for a new scan-cycle.

3.1.2 Start-up process

The Hunna device has security processes and hardware that ensures that the system is not physically available through USB-ports until the boot process is complete, thus eliminating the possibility to disrupt the boot-process. USB-ports will therefore become available only once relevant firmware has been loaded into RAM, and the system indicates that it is ready.

3.1.3 Scan process

When an unknown media is connected to the Hunna device, the system immediately (once the start-up process is completed) starts copying files contained on the media into RAM and scanning the files for malware through the security processes.

3.1.4 Anti-Virus (AV) checks

The first security control that will be performed is against the present AV-engines. There is no limitation to how many AV-engines can be included, although adding non-present AV-engines requires company development, normally at cost.

Due to their construction, there are some AV-engines that are more costly and/or less practical to deploy within the Hunna system.

The Hunna device can be set to check against all AV-engines (currently expanding from two to five as standard), or to randomly choose two AV-engines to check against. As the AV-scan process is the most time-consuming element in the whole system, expanding scans to include more AV-engines will affect overall performance.

3.1.4.1 Customer-specific AV-definitions

Some customers may have access to confidential non-public AV-definitions, that may have been obtained through signals intelligence, etc. The Hunna system permits the use of such AV-signatures through a separate process.

Such AV-definitions are only visible to the organisation (administrator level) deploying them.

3.1.4.2 Administration of AV-engines

Through the custom tool delivered with the Hunna device, the AV-engines can be configured in their completeness. This means that all configuration options available from the AV-provider are available to the administrator.

St Hunna provides a tool for configuration, and all configurables can be obtained from each respective AV-provider.

3.1.5 Optional security process

The Hunna system includes an area where custom security functions can be entered. Such functions can include whatever the customer requires, and can be internally developed functions, third-party functions, or functions developed by St Hunna.

Examples of functions that could potentially be implemented:

- Format conversion to eliminate/make it extremely difficult to enter a zero-day attack
- Sandbox functions
- Meta-data controls, for example to verify/limit import of information that has a certain information level class

The optional security process can be configured to be performed before, after or in parallel with other security functions, or replace one or more of them altogether.

Such security processes are only visible to the organisation (administrator level) deploying them, for the purpose of enabling confidential security functions to be included.

3.1.6 Whitelist check

The whitelist enables limitation of which files or types of files are permitted to be copied from source to target media. *File format verification through Magic Numbers is being implemented*.

3.1.7 Quarantine list check

Any malware found through the scan-process is copied to the "Quarantine"-media. In addition, it is possible to configure the Hunna device to automatically route files with required file-types or file names to the quarantine USB-media, irrespective of if it contains malware or not.

For example; a certain system should maybe only receive certain file types. If a specific file type is entered through the Hunna device protecting that critical information system, it may be required to analyse the complete binary to ascertain the reason for such a file type to be present in that environment.

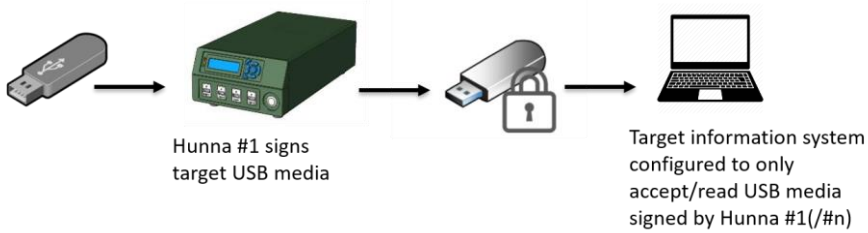
3.1.8 Copy process

The Hunna device copies files from Source to Target. It will only copy files that fulfil all requirements against set rules. This means that the file will need to pass the AV-engines, the whitelist, the quarantine list, and/or optionally the custom security check prior to being copied onto the Target USB-media.

Copying will, as a process in itself, reduce attack vectors somewhat by not copying malware that may reside in the boot sector of unknown USB-media.

3.1.9 Sign process

The Hunna device transforms into a complete system when this function is adopted. The required function is normally that the receiving system will refuse to receive files that have not been checked by the relevant Hunna device(s), thus avoiding such types of attacks or mistakes.



Once files have been copied to the Target USB-media, the files are signed, and a hash is added.

The receiving system can be configured to verify that the USB-media has come from the correct Hunna device(s), and that no files have been altered following having been controlled by this Hunna device.

Files can be signed with either X.509-type certificates, or with OpenPGP.

3.2 Built-in security

The Hunna device is a high-assurance system based on multiple security functions and principles. Such functions include:

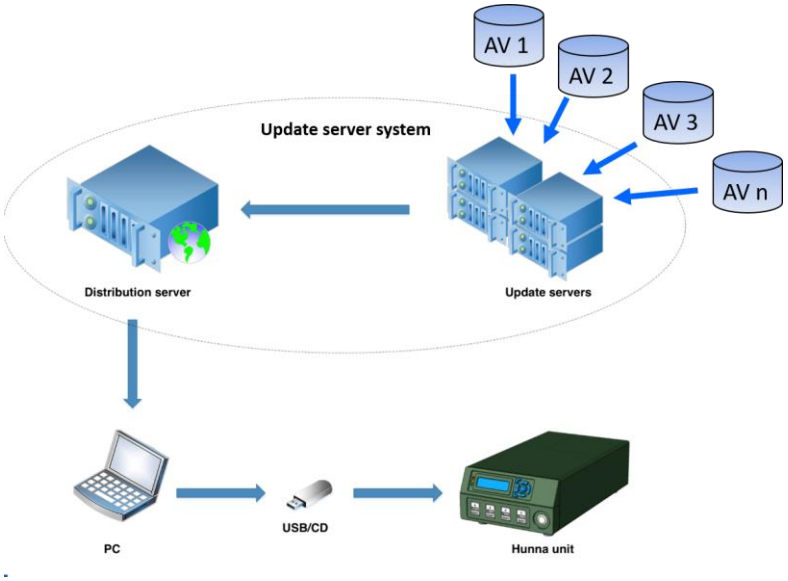
- Linux-based, heavily stripped-down distribution to limit attack vectors.
- Virtualised in multiple instances.
- Firmware stored in physically write-protected lock-down drive (custom-built high-assurance device).
- All operation is performed in RAM, rebooting between each Scan-cycle to clear operating memory.
- Ports protected by physical high-assurance component, ensuring that only relevant ports are electrically active when required and when the system is ready.

The system is used to protect information systems up to and including TOP SECRET within government functions.

Further details can be provided to NCSA interested in in evaluating the product.

3.3 The Hunna update server system

The Hunna update server system is in itself a high-assurance system, consisting of multiple servers, physically separated, with key servers protected by data diodes.



The purpose of the update system is to provide relevant Hunna devices with updates, consisting of:

- AV-definitions
- Firmware updates
- Optional non-public AV-definitions
- Optional updates to non-public security functions

The system is designed to collect AV-definitions from AV-vendors, and, through a specific process, package, encrypt and sign this BLOB and make it available to one or more distribution point(s).

The system is designed so that these BLOBs will only be accepted by one or more Hunna device(s) if it is signed correctly and is encrypted correctly for that/those specific Hunna device(s).

With this setup, it is possible to distribute BLOBs over an internal network or over the Internet, thus enabling use in remote locations.

AV-updates are normally provided as either full updates including all relevant AV-definitions, or incremental updates. BLOBs with incremental updates are specifically relevant to, for example, military units located overseas with limited bandwidth.

3.3.1 Internal or external update system

For organisations with highly sensitive systems, we would normally envisage that a Hunna update system is located within the organisation.

For organisations with few Hunna devices, or where it is deemed possible from an information security standpoint, it is possible to receive updates remotely from the St Hunna update system located in Sweden.

4 ROLES AND ADMINISTRATION

There are three basic roles related to the Hunna device:

1. The user
2. The daily operator
3. The administrator

The following roles may be divided between staff, or combined, as the organisation sees fit.

4.1 The user

To the user, the Hunna system is a simple and automatic system that performs its task automatically.

However, it is important that users receive a short basic training on how the system is used, to avoid a number of mistakes and risks.

For example, non-trained users may believe that any USB-media connected to the Hunna device is safe to connect to the critical information system, whereas it is only USB-media connected to the Target-port, to which files have been copied, that is safe to connect to the relevant system.

4.2 The daily operator

The role of the daily operator is to update the Hunna device(s) with the latest updates (AV-definitions, etc), that are obtained from the relevant distribution point within the update server system, via a closed network or via the Internet.

Updates are collected on USB-media, and each relevant Hunna device is thereafter updated in line with the update process.

The daily operator should be in control of the physical key used to alter the state of the Hunna device between Scan and Admin. Leaving the key in the Hunna device introduces a risk that a user alters the state at the wrong time, thus risking to trigger certain critical security functions.

The physical key is not a security feature as such, but a function to ensure that admin operations are performed correctly.

4.3 The administrator

The administrator can determine the functionality of the Hunna device. This includes:

Setting digital keys and determining which key can be used for which operation.

Configuring AV-engines, the whitelist and the quarantine list, as well as other potential custom security functions.