HUNNA

Version 1.9.1

The Hunna USB Sanitization System Whitepaper

hunna.eu

Contents

Contents ... 2

1. Purpose of the Hunna USB Sanitization System ... 3

2. System Overview ... 4

2.1 The USB Sanitization Terminal ... 4

2.2 Import of software updates and security patches ... 9

2.3 Built-in Security ... 9

2.4 The USB Sanitization Update Server System ... 10

3. Roles and Administration ... 12

3.1 The User ... 12

3.2 The Daily Operator ... 12

3.3 The Administrator ... 13

1. Purpose of the Hunna USB Sanitization System

The Hunna USB Sanitization system has been developed to meet 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.

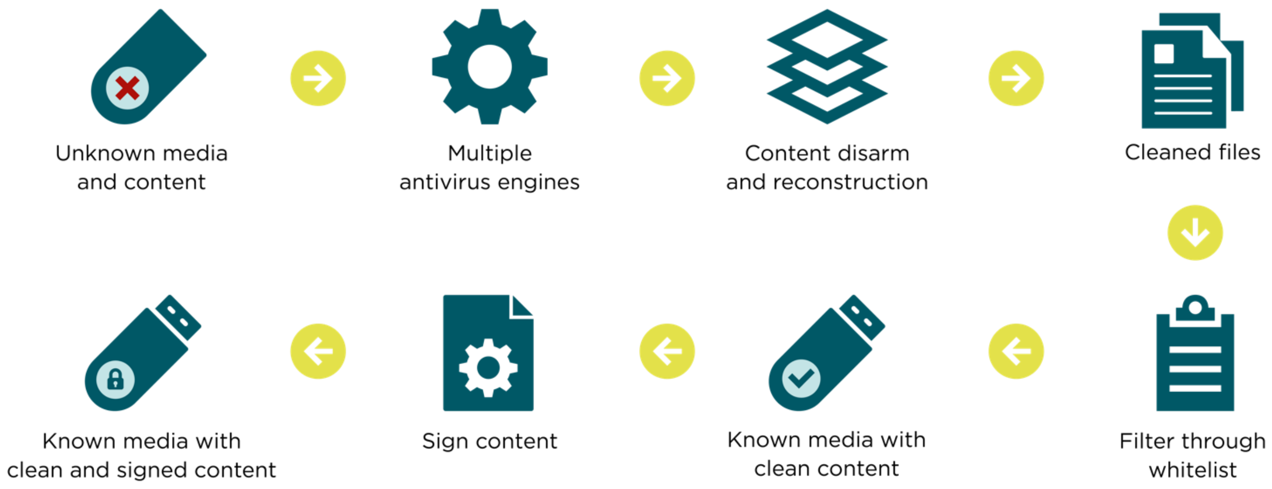
4. To be impossible/extremely difficult to manipulate through built-in security features, including high-assurance security components.

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

6. To enable the 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 customer’s 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 system is used correctly.

2. System Overview


Unknown media and content
Multiple antivirus engines
Content disarm and reconstruction
Cleaned files
Filter through whitelist
Known media with clean content
Sign content
Known media with clean and signed content

2.1 The USB Sanitization Terminal

The terminal is a security platform which can run almost any type of security function. It also includes a number of security features pre-configured into the platform, including Anti-Virus engines, Content Disarm and Reconstruction (CDR) and whitelist.

There are at the moment different models of terminals, however the basic functionality is the same.

2.1.1 Basic overview

The basic function of the terminal is to copy files from the Source media to the Target media, passing through a number of security functions on the way.

Any files that contain malware can be copied to the Quarantine media[1]. Those files will not be copied to the Target media.

Logs are stored on Target media and on Quarantine media[1].

[1] *If the terminal type has a quarantine port.*

The terminal initiates scanning once media is connected to the Source 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[1].

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.

2.1.2 Start-up process

Some terminal types have 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 of disrupting 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.

2.1.3 Scan process

When an unknown media is connected to the terminal, once the start-up process is completed, the system immediately begins copying files contained on the media into RAM and scanning the files for malware, then rebuilding the files using CDR.

2.1.4 Anti-Virus (AV) checks

The first security control that will be performed uses the embedded AV engines. The terminal will run at least one AV engine. Depending on terminal type more than one AV engine can run simultaneous and in parallel.

Current supported AV engines are:

- ClamAV
- Microsoft Defender for Endpoint
- Trend Micro
- F-Secure
- ESET

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 system permits the use of such AV signatures through a separate process.

Such AV definitions are only visible to the organisation's Administrator.

2.1.5 Administration of AV engines

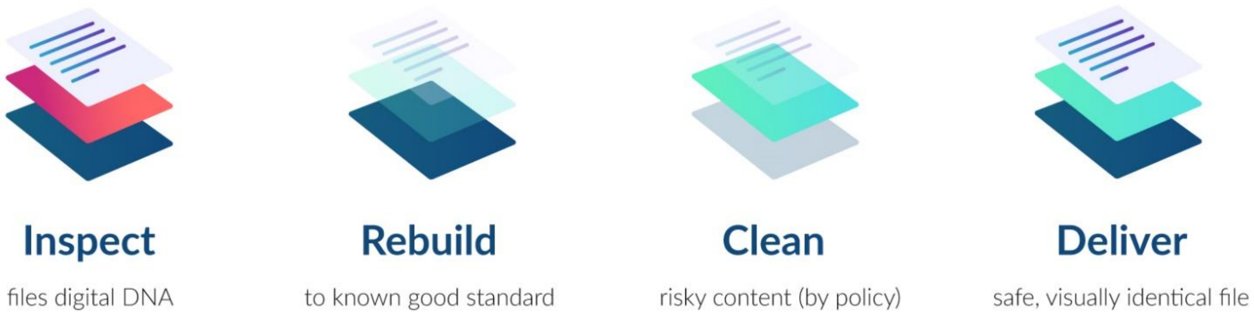
Through the custom tool delivered with the terminal, the AV engines can be configured in their completeness. This means that all configuration options available from the AV provider are available to the administrator.

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

2.1.6 CDR

After passing through the AV engines, each file is then processed by a CDR-filter. The CDR-filter instantly cleans and rebuild files to match their known good manufacturer's specification, stripping away anything that doesn't conform. This proactive approach automatically removes malware and exploits from the file.

The CDR-filter operates through four key processes:



1. Inspect: Most files entering organisations do not comply with their file specification. The CDR-filter inspects every incoming file's structure at the byte level and conducts thousands of conformance checks, identifying any deviation from the file's standard structure, as determined by its manufacturer (e.g., 3,500 checks for .pdf, 7,446 for .xlsx and 4,279 .docx).

2. Rebuild: Where there are deviations, The CDR-filter remediates the file, eliminating any possible structural threat the rebuilt file now matches it’s known good manufacturer's standard.

3. Clean: Non-structural threats in Active Content (e.g., Macros, JavaScript, embedded files, URLs and metadata) are neutralised by the sanitization function in the CDR-filter. Sanitization is set and refined through policy management.

4. Deliver: Upon completion of the process, the user receives a safe, identical file in its original format. The clean, threat-free file is compliant, standardised and free of risky Active Content, reducing risk while maintaining operational continuity.

This four-step process is completed in milliseconds, generating a new, structurally compliant and safe file that meets management policy without impacting or changing the content in any way whatsoever.

The CDR-filter does not require any ongoing patching or updates.

2.1.7 Whitelist check

The whitelist enables limitation of which files or types of files are permitted to be copied from source to target media.

For some terminal types a further whitelist feature enables the terminal to only accept media based on its vendor/PID or serial number. The Source/Target/Quarantine USB ports can be configured individually depending on the use case.

2.1.8 Quarantine list check[1]

Any malware found through the AV checks in the scan-process is copied to the Quarantine media. In addition, it is possible to configure the terminal to automatically route files with certain file-types or file names to the quarantine USB media, irrespective of if they contain malware or not.

For example, a certain system can be configured to only receive certain file types. The CDR-filter analyses the complete binary of the files with any unauthorised file types sent to the Quarantine media rather than the Target media.

[1] *If the terminal type has a quarantine port.*

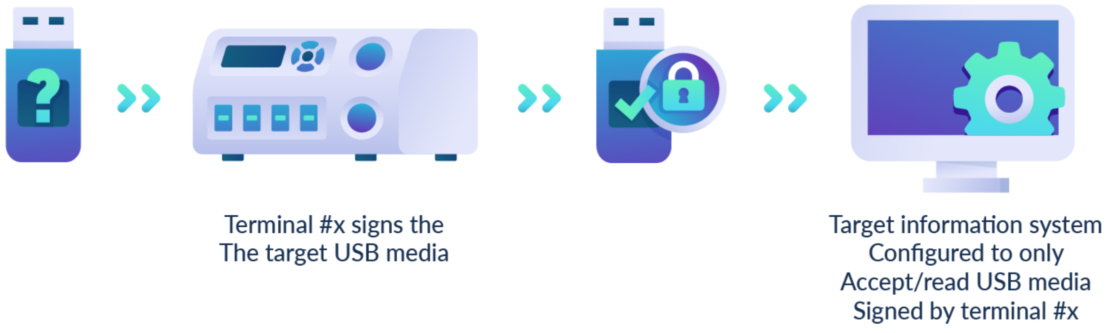
2.1.9 Copy process

The terminal 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 CDR-filter, the whitelist, the quarantine list before 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.

2.1.10 Sign process

The terminal transforms into a complete system when this function is adopted. The standard required function is that the receiving system will refuse to receive files that have not been checked by the relevant terminal(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 terminal(s), and that no files have been altered following having been controlled by this terminal.

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

2.2 Import of software updates and security patches

The terminal is compatible with PD Update to enable quality assured import of software updates, installation packages and security patches.

PD Update process flow before USB device is connected to the terminal,

1. Unknown content
2. Source validation
3. Up to 8 AV Engines
4. Cleaned files
5. USB with Known content
6. Sign content
7. USB With Known Signed Content

PD Update process flow when USB device is connected to the terminal, three steps

1. USB With Known Signed Content
2. Signature and data Validation
3. USB with Known Signed Content and Validated Signature

2.2.1 The PD Update process

PD Update identifies packets through Scrapers and Connectors, a combination of specially designed and vendor-based applications. With information from the Scraper and Connectors PD Update downloads packets through a fetcher.

Sources are validated and downloaded packets and are validated and scanned. A manifest-file with metadata from the validation and scanning processes is created for traceability and recreation of the validation and scanning.

All steps are monitored to detect errors or inconsistencies.

PD Update is delivered through The USB Sanitization Update Server System or physically on an encrypted hard drive.

2.3 Built-in Security

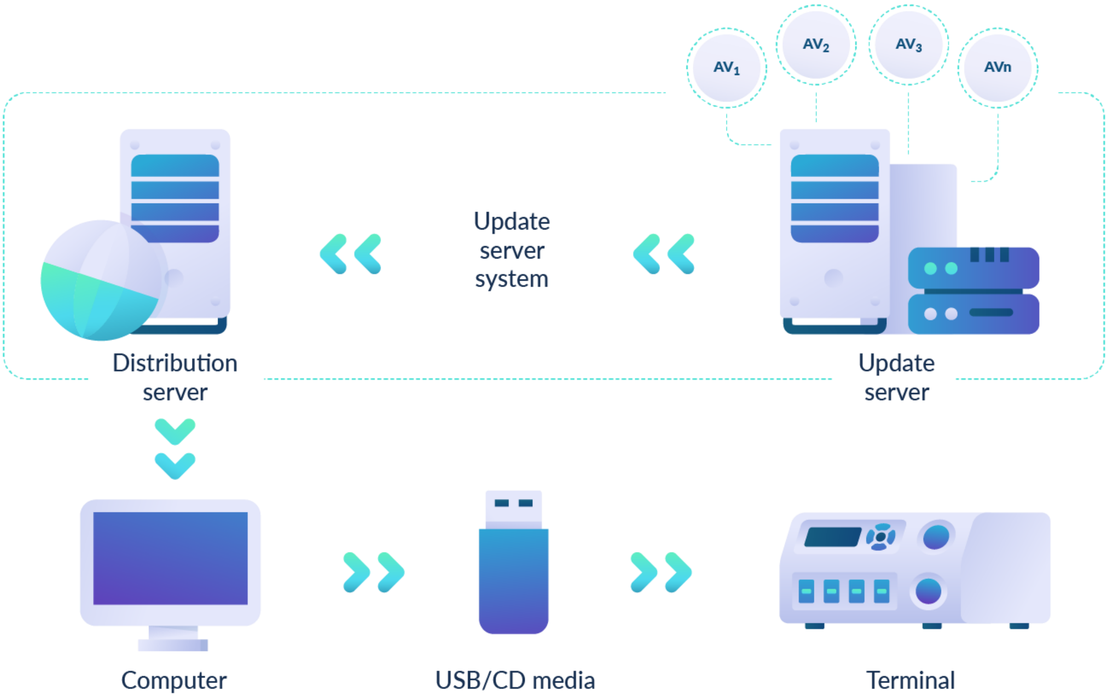
The terminal is a high-assurance system based on multiple security functions and principles. Such functions include:

- Linux-based, heavily stripped-down distribution to limit attack vectors.
- Virtualised in multiple instances.
- Firmware stored in physically write-protected lock-down drive[2].
- 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[2].

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

2.4 The USB Sanitization Update Server System

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



[2] *Applies only to some terminal types*

The purpose of the update system is to provide relevant terminals 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 terminal(s) if it is signed correctly and is encrypted correctly for that/those specific terminal(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 provided as full updates including all relevant AV definitions. No regular updates of the CDR-filter are required.

2.4.1 Internal or external update system

An internal update system refers to when an organization wants to have full control and have the update system located within their own organisation.

An external update system refers to when an organization has deemed it possible, from an information security standpoint, to receive updates remotely from the Hunna USB Sanitization update system located in Sweden.

3. Roles and Administration

There are three basic roles related to the terminal:

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.

3.1 The User

To the user, the 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 terminal is safe to connect to the critical information system, whereas it is only USB media from the Target port to which files have been copied are safe to connect to the relevant system.

3.2 The Daily Operator

The role of the daily operator is to update the terminal(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 terminal 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 terminal between Scan and Admin. Leaving the key in the terminal introduces a risk that a user alters the state at the wrong time, thus risking triggering 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.

3.3 The Administrator

The administrator can determine the functionality of the terminal. 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.

The Hunna USB Sanitization system is available in various designs and configurations. This means that final functionality depends on what is ordered and how these components are configured.