HAGIWARA Solutions

■ For offline terminals in production sites and control systems
■ For outgoing inspection of industrial equipment

Vaccine USB3 Installation-free malware scanning tool

Install-less malware checking! Equipped with Trellix (formerly McAfee) anti-malware engine. A USB memory-based tool for malware detection, quarantine, and removal

Vaccine USB3

Powered by Trellix

Target

> Production Equipment > Research and Inspection Equipment
> Medical Equipment > Offline business terminals
> Outgoing inspection of products
> Inspection of products returned for repair

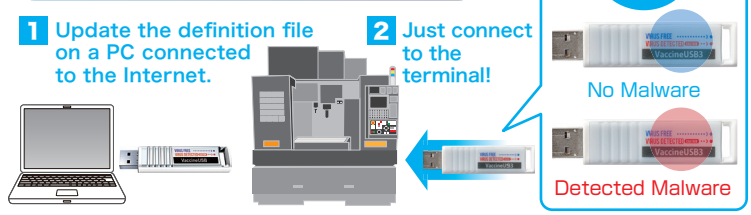
Common difficulties combating Malware

- Isolated from the network
- Unable to install software
- System resources are limited

Solution we provide

1 Update the definition file on a PC connected to the Internet.

2 Just connect to the terminal!



Semiconductor manufacturing equipment and processes

Security standard for semiconductor manufacturing: the 'malware diagnostic report' generation function defined in SEMI E187/188 has been implemented!

Available from 1 unit!

Easily scan target devices for malware by simply connecting the USB. You can choose how to scan and how to save the logs.

1. Extended target OS and environment.

Supports not only Windows but also Linux.
Malware checking on older operating systems is now possible.

Extended functionality in Linux environments!

- Supports malware quarantine.
- Support for asset information collection
- Equipped with high-speed scan mode

USB boot scanning is now supported!

When Vaccine USB3 is connected and the terminal is booted, its built-in operating system automatically starts and begins scanning.

2. Various scan setting for various use case

- Reduced scanning time: fast scan, differential scan, selection of scan targets
- Change operation settings: scan only, scan + quarantine/delete
- Timer scan

3. No dedicated PC required.

Update definition files on any internet-connected PC — no dedicated PC or software required. Designed to prevent malware infection when updating definition files.

4. Scan results and terminal asset information can be securely stored as log data.

Malware check results and terminal asset information are stored as log data in a special memory area in the product itself.
Preventing data tampering or malware infection.

Log information (malware check results & asset information of connected terminals)

- Information on checked terminals
- Information on detected malware
- Vaccine USB3 information
- Scan settings ● Scan results
- Software information installed on the checked device

5. Multiple terminals can be scanned with a single unit.

There is no limit to the number of terminals to be checked for malware; a single Vaccine USB3 can be used to check any number of terminals for malware.

Vaccine USB3 Video on how to use Vaccine USB3

Windows
https://youtu.be/-vJ5exPb680

Linux
https://youtu.be/AMyVWgP_o4U

Detect endpoint vulnerabilities and visualise patch status.

All-in-One: From Vulnerability Assessment to Reporting

Severity Classification (4-Level Rating Based on CVSS v3.1)

Critical (Critical)	9.0 - 10.0	A severe vulnerability requiring immediate action
High (Important)	7.0 - 8.9	A vulnerability that should be prioritized
Medium (Warning)	4.0 - 6.9	A vulnerability to be addressed as planned
Low (Caution)	0.1 - 3.9	Low risk, but should still be recognized

■Severity classification by CVSS score
Detected vulnerabilities are automatically classified into four levels based on their CVSS v3.1 score: Critical, High, Medium, and Low. This makes it easy to see response priorities at a glance.

■Visualisation of patch application status
Installed Windows updates (KBs) on each endpoint are compared with security update information.
Missing patches are identified, and the patch application rate is displayed for each endpoint.

■Vulnerability assessment report output
Assessment results can be output as a PDF report.
The report provides a list of detected CVE numbers, CVSS scores, and more, and can be used as evidence for security audits and compliance requirements.

Anti-malware USB flash drive to prevent malware infections.

Combined use of a security USB memory stick with anti-malware functionality to prevent malware from being brought in or spreading.
Can also be used as a simple malware check.

- Password lock and automatic encryption for information leakage prevention.
- Malware checker for running processes
- INFO BANKER support

Powered by Trellix

Lineup

Product Name	Summary	Licence	Model Number	Remarks
Vaccine USB3	Virus Checking Tool for Offline Terminals Virus Scan Engine by Trellix (formerly McAfee)	1 year Licence	ULD-VAU31A	
		3 year Licence	ULD-VAU33A	
		5 year Licence	ULD-VAU35A	
License Renewal	1-Year Extension Pack Hardware warranty also extended by 1 year. The maximum license period for the same device is 5 years.	1 year Licence extension	ULD-VAU31LRA	1 pack
			ULD-VAU310LR	10 packs

Specification

Item	Element
Virus scanning engine	Virus Scan Engine by Trellix (formerly McAfee)
Connector type	USB3.0 (Type A)
Support model	DOS/V devices equipped with a standard USB interface Physical free memory capacity of 512MB or more Page cache should be enabled (recommended) CD-ROM drive must be recognized Autorun via CD-ROM should be executable (recommended)
Supported User Accounts	Computer Administrator / Restricted User In a restricted user environment, viruses detected outside the following folders cannot be deleted or quarantined: Documents and Settings¥[Logged-in Username]¥[Below Foldes]
Operating temperature	0～50℃
Dimensions	Length 79.0mm×Width 18.0mm×Height 9.4mm ※Including cap

Supported OS

Windows 7 / 8 / 8.1 / 10 / 11
Windows Server 2008 SP2 / 2008 R2 / 2012 / 2012 R2
2016 / 2019 / 2022 / 2025
Windows Storage Server 2008 / 2012 / 2016
Windows Embedded Standard 7 / Embedded POSReady 7
Windows 7 for Embedded Systems
Windows Embedded 8.1 Industry Pro
Windows10 Enterprise LTSB,LTSC / IoT Enterprise LTSB,LTSC
Windows11 Enterprise LTSB,LTSC / IoT Enterprise LTSB,LTSC

Red Hat Enterprise Linux 6(32-bit/64-bit) 7 / 8 / 9(64-bit)
CentOS 5 / 6(32-bit/64-bit) 7 / 8(64-bit)
AlmaLinux OS 8 / 9(64-bit)
MARACLE LINUX 8 / 9(64-bit)
Rocky Linux 8 / 9(64-bit)
Debian 10 / 11 / 12(32-bit/64-bit)
Ubuntu Linux 14 ～ 18(32-bit/64-bit) 19 ～ 24 (64-bit)

※This software is compatible with Intel architecture CPUs.
(Not compatible with ARM environments)
※Language setting will automatically switch to English in non-Japanese environments.

HAGIWARA Solutions

Hagiwara Solutions Europe GmbH (Elecom Group)

Adress: Fritz-Vomfelde-Str. 34, 40547 Dusseldorf, Germany
Landline: +49 (0) 211 53883 311
Email: hagiwara_europe@hagisol.co.jp
Websaite: https://www.hagisol.com/
Linkedin: https://www.linkedin.com/company/hagiwara-solutions/

2026.8 HSXS24106-A07