SEMI E187/E188 Compliance

Enhancing Threat Visibility in Isolated OT Systems with VaccineUSB3

SEMI E187 and E188

SEMI E187 and E188 are cybersecurity standards developed by SEMI, with leadership from TSMC, to strengthen the security of semiconductor manufacturing. These standards define responsibilities across the supply chain—from OEMs to fabs—to ensure equipment is secure by design and free from malware upon delivery. **VaccineUSB3** directly supports these requirements by enabling malware scans and generating compliance-ready reports.

SEMI E187 :

The responsibility to design new semiconductor equipment to be cyber-secure.

- **Equipment Manufacturers (OEM)**
- **Sub-component Suppliers**

SEMI E188 :

The responsibility to ensure any equipment integrated into the Fab is free of malware.

- **Fabs/Foundries**
- **System Integrators**
- **3rd Party Service Provider (Repair/Maintenance)**

Key Advantages of VaccineUSB3 in meeting SEMI E187/188 requirements :

Scan Any Asset, On the Spot.

The “Plug and Scan” approach allows agentless malware scan for any system, from legacy Windows to modern Linux.

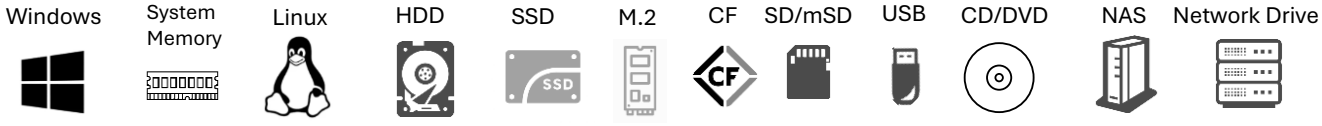
Eliminate Security Blind Spots.

Air-gapped environments and unpatchable legacy systems (Shadow OT) are often your most vulnerable points. Scan them physically with VaccineUSB3 to mitigate risk and gain asset visibility across your entire supply chain.

Automate Compliance Reporting

Instantly generate detailed reports that are SEMI E187/E188 compliant upon scan completion. Drastically reduce time-consuming tasks for audits and pre-shipment procedure.

From OS to Media—All Covered.



Directly Fulfills SEMI E817/E188 Requirements

SEMI standards	Requirement	VaccineUSB3
SEMI E187, 9.3 Malware Scanning [E187.00-RQ-00006-00]	Perform a malware scan before shipping and provide a report that includes tool name, version, scan scope, and date.	Allows OEMs to run a final scan on fully assembled equipment. Generates a detailed, tamper-proof log that fulfills compliance and audit documentation.
SEMI E188, 8.3 Malware Scanning [E188.00-RQ-00001-00]	Perform a malware scan and confirm no malware is present before shipping to the equipment user.	Enables reliable malware scanning at the integration stage. Acts as a physical tool to ensure and document malware-free status before delivery.
SEMI E188, 8.4 Malware Scanning Reporting [E188.00-RQ-00002-00]	Provide a report detailing scan configuration and results in electronic format.	Automatically generates a compliant report, stored on the secure partition or transferred electronically for recordkeeping and submission.

Capabilities

Portable	Allows operators to easily carry it for on-the-spot inspections.
Offline Operation	Enables offline scan with the latest malware definitions
Unlimited Scan	Allows unlimited scans on any devices during the license period, eliminating complex license management.
Agentless	Performs scans without requiring software installation.
Cross-Platform	Supports a wide range of systems—from legacy Windows to modern Linux.
Audit-Ready	Generates malware scan reports compliant with SEMI E187/188. Also suitable as general-purpose diagnostic records across industries.

Actionable Reporting & Workflow

Shadow OT Coverage	Performs malware scans on isolated, air-gapped, or outdated systems, while supporting asset discovery in hard-to-access environments.
SIEM-Compatible Data Format	Outputs scan reports in CSV format for easy manual management or integration with SIEM platforms.
Self Protection	Permanently write-protected at the firmware level to prevent tampering, ensuring the device cannot carry or spread malware.

HAGIWARA SYS-COM
23272 Mill Creek Drive, STE220 Laguna Hills, CA 92653 U.S.A.
Tel:(949) 328-9870 / sales@hsc-us.com
www.hsc-us.com