

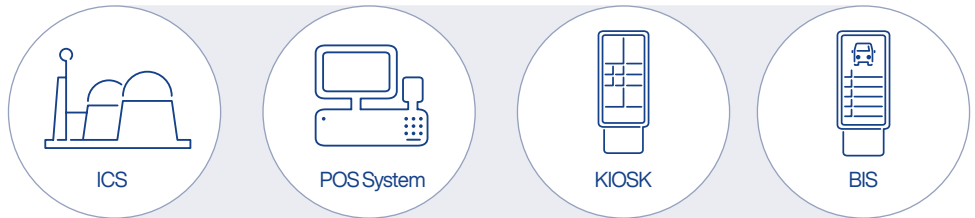
# AhnLab Xcanner

## OT Endpoint Malware Detection and Removal

Portable AV solution for OT systems unable to perform regular scan or engine updates

### Overview

AhnLab Xcanner is a portable antivirus tool that detects and removes malware in OT systems where it is unable to deploy normal security solutions. It enables users to set scan and repair options for each operating environment with minimal impact to the system. AhnLab Xcanner does not require installation as it can be mounted on a removable storage device.



- ✓ Supporting air-gapped systems
- ✓ Response to existing malware
- ✓ Supporting outdated OS
- ✓ No installation required
- ✓ Mounting on removable storage devices

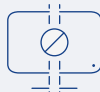
### OT-Dedicated Security

OT systems require high stability in operation and must use only authorized programs. Systems within air-gapped network face challenges in updating anti-malware engines to the latest versions, while still needing to address security issues. AhnLab Xcanner delivers optimal security measures dedicated to these unique security requirements.



OT Systems Unable to Install Security Solutions

- Critical systems where real-time scan and remediation are limited
- Systems using outdated operating systems
- Systems that may conflict with pre-installed security solutions
- When non-security experts should implement security measures






Air-Gapped Systems with Restricted Engine Updates

- Systems unable to update security engines to the latest version
- Cases of malware infection within air-gapped network
- Malware removal, memory scan, and stealth malware detection




## Strengths

AhnLab Xcanner supports not just security experts but also field workers and equipment managers in easily responding to malware.

|   |  |
|---|--|
| <br><b>Manual Scan for Detection and Clean</b> | <ul style="list-style-type: none"><li>· Minimal clash with pre-installed security agents</li><li>· Manual remediation option for compromised systems</li><li>· Full system scan prior to security agent installation for early prevention</li><li>· User-defined scan for reduced scan time</li></ul>  |
| <br><b>Various Operational Settings</b>        | <ul style="list-style-type: none"><li>· Various scan and remediation options for each environment</li><li>· Exception settings for targets that require no scan (folder, file, and extension)</li><li>· Features supporting environments where kernel driver cannot be operated</li><li>· Supporting GUI, CLI, and silent modes</li></ul> <p><i>* CLI and silent mode only for the Linux version</i></p> |
| <br><b>User Convenience</b>                    | <ul style="list-style-type: none"><li>· Manual remediation options after scan</li><li>· Quarantining infected programs in case of deletion and false positives</li><li>· Searching detection logs by period and saving files</li></ul>   |

## Key Features

AhnLab Xcanner offers the following features to enable powerful malware defense and efficient operation:

|   |  |
|---|--|
| <br><b>Scan</b>        | <ul style="list-style-type: none"><li>· Manual scan: Full scan, user-defined scan (folder and file)</li><li>· Potentially malicious &amp; unwanted program (PUP) scan</li><li>· Cloud detection</li><li>· Compressed file scan</li><li>· Search keyword lookup and selective remediation</li><li>· CPU usage setting</li></ul>   |
| <br><b>Remediation</b> | <ul style="list-style-type: none"><li>· Selecting scan method</li><li>· Auto remediation</li><li>· Deletion of irremediable file</li><li>· Cleaning or ignoring infected compressed file</li><li>· Remediation level</li><li>· Scan exception (folder, file, extension)</li><li>· Scan options</li></ul>   |
| <br><b>Setting</b>     | <p><b>Log management</b></p> <ul style="list-style-type: none"><li>· Event and detection logs</li><li>· Lookup scan results (by date)</li><li>· Storing log files</li></ul> <p><b>Quarantine</b></p> <ul style="list-style-type: none"><li>· Searching and exporting quarantine list</li><li>· Restoring quarantined file</li></ul> <p><b>Program Shut Down</b></p> <ul style="list-style-type: none"><li>· Shutting down executable programs only</li><li>· Deleting program (quarantine, log, and system setting data)</li></ul> |

# AhnLab EPS Integration

By integrating AhnLab Xcanner with AhnLab EPS, users can achieve stronger and more precise malware defense. With EPS, Xcanner's scan and remediation logs are centralized and can be monitored through the management console. Additionally, Xcanner can be run without requiring the unlock settings of EPS, improving operational efficiency and reducing the risk of malware infection.



### Enhanced Detection

- Scan and clean PE and non-PE malware
- Auto-analysis of file in the cloud-based ASD server (not supporting air-gapped systems)
- Pre-checking memory and process
- Scan stealth malware



### Scan and Remediation in Lock Mode of EPS

- No need to disable Lock Mode of EPS
- Reducing the risk of malware infiltration when disabling Lock Mode
- \* Not supporting EPS Standalone
- \* Selective use recommended considering user systems



### Central Management from Admin Console

- Checking malware remediation results on the EPS console
- Downloading the latest version of Xcanner
- Managing the Xcanner license
- Monitoring product status and managing policies
- \* Linux version does not support the EPS integration

## System Requirements

### AhnLab Xcanner for Windows

|          |             | System Requirements   |
|----------|-------------|---|
| Hardware | CPU         | Intel CPUs  |
|          | MEM         | 128MB or more   |
|          | HDD         | 1GB or more   |
| OS       | Embedded OS | Windows XP Embedded<br>Windows Embedded Standard 2009<br>Windows Embedded Standard 7<br>Windows Embedded POSReady 2009<br>Windows Embedded POSReady 7<br>Windows Embedded 8.1 Industry (Pro, Enterprise)<br>Windows 10 IoT Enterprise   |
|          | Client OS   | Windows 2000 Professional<br>Windows XP (Professional)<br>Windows Vista (Enterprise, Ultimate)<br>Windows 7 (Enterprise, Professional, Ultimate)<br>Windows 8/8.1 (Enterprise, Pro)<br>Windows 10 (Enterprise, Pro)<br>Windows 11 (Enterprise, Pro)   |
|          | Server OS   | Windows 2000 (Server, Advanced Server)<br>Windows Server 2003 / 2003 R2 (Standard, Enterprise)<br>Windows Server 2008 / 2008 R2 (Standard, Enterprise)<br>Windows Server 2012 / 2012 R2 (Essentials, Standard)<br>Windows Server 2016 (Essentials, Standard)<br>Windows Server 2019 (Essentials, Standard)<br>Windows Server 2022 (Essential, Standard) |

\* Supporting both 32-bit and 64-bit versions for the OS above

## AhnLab Xscanner for Linux

|          |                          | System Requirements  |
|----------|--------------------------|--|
| Hardware | CPU                      | Intel CPUs   |
|          | MEM                      | 300MB or more  |
|          | HDD                      | 500MB or More  |
| OS       | Cent OS                  | Cent OS 3.3 ~ 3.9, 4, 5, 6, 7, 8                                     |
|          | Red Hat Enterprise Linux | RHEL 3.3 ~ 3.9, 4, 5, 6, 7, 8.0 ~ 8.1                                |
|          | AntiX Linux              | AntiX Linux 13.2, 16.2<br>AntiX Linux 15-1, 15-V<br>AntiX Linux 17.2 |
|          | Ubuntu                   | Ubuntu 10.04, 11.04, 11.10, 12.04, 14.04, 18.04                      |
|          | SUSE Linux               | SUSE Linux 9.2, 10.3   |
|          | Fedora                   | Fedora 8, 14   |
|          | Debian                   | Debian 8.9   |
|          | Redhat                   | Redhat 9   |
|          | Scientific Linux         | Scientific Linux 6.7   |
|          | Ruby Duck                | Ruby Duck 5.6, 5.6.5.x   |