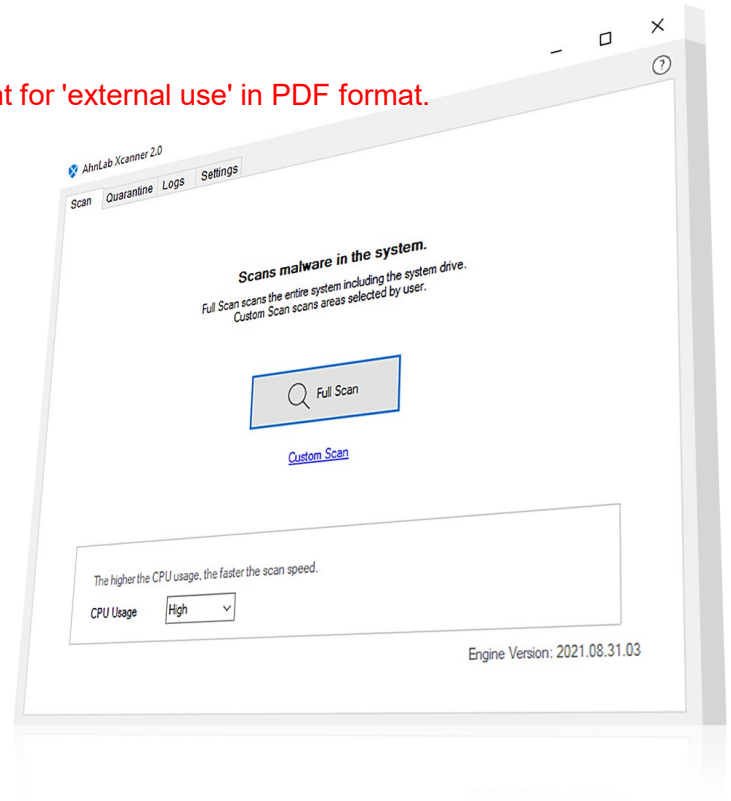
More security,
More freedom

AhnLab Xcanner

Malware Detection and Remediation for Fixed Function Systems

Standard Proposal

※ This document is for internal use only. For external use, please provide a document for 'external use' in PDF format.



AhnLab

Contents

Background

Air gapped networks where malware engine cannot be updated to the latest version, systems where expectations for stable operation are high, but only certain programs can be used, etc. Even in such special environments, there are security issues and demands for responses.

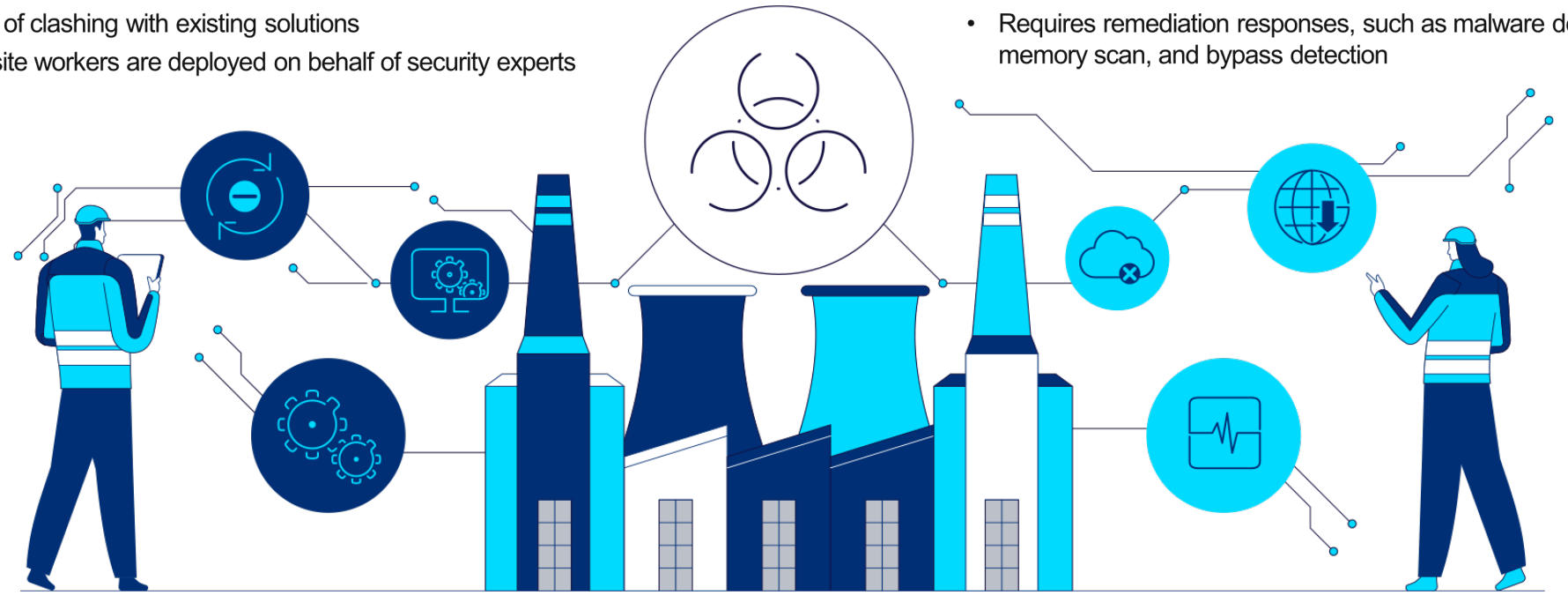
Need for Anti-malware Measures in Systems Where Real-time Response is not Possible

Difficult to deploy normal security solutions:
Fixed Function Systems

- Impossible for remediation immediately after real-time detection
- OS that are no longer supported by the provider
- Risk of clashing with existing solutions
- On-site workers are deployed on behalf of security experts

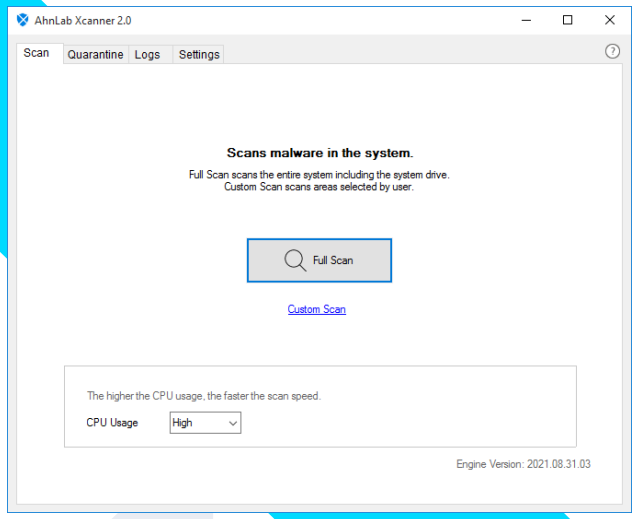
Impossible to perform regular engine/mass updates:
Air Gapped/Low Bandwidth Networks

- Regular updates for security engine is impossible
- Known and unknown malware infects air gapped networks
- Requires remediation responses, such as malware deletion, memory scan, and bypass detection



AhnLab Xcanner

AhnLab Xcanner is a manual scan-based malware detection & remediation program developed to detect and delete malware in Windows-based systems. This program, however, does not replace anti-malware programs. This is a program optimized to support security administrators and users when dealing with infected systems.



AhnLab Xcanner

Manual, Scan-based Detection & Remediation

- Minimizes clash in programs by not deleting existing security agents
- Remediates compromised systems after detection
- Scans all systems for early prevention before installing any security agents
- Supports user-defined scan for reduced scan time

Various Operational Settings

- Supports various scan/remediation options optimized for each specific case
- Allows the security administrator to set exceptions for targets that require no scan (folder, file, extension)
- Provides various features for environments where kernel driver cannot be operated
- Supports GUI, CLI, and Silent modes

User Friendly, Easy to Manage

- Offers option of immediate remediation after the scan
- Provides quarantine feature to respond to deletion of infected key program and false-positives
- Records event and detection log by period, looks up search keyword, and saved files

※ For real-time protection with automatic updates, AhnLab V3 or AhnLab EPS is recommended.

Key Features

AhnLab Xcanner provides the following features:

Malware Response

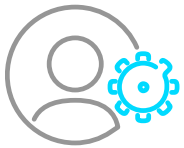
Malware Scan

- Manual (Detailed) Scan: Full scan, user-defined scan (folder, file)
- Potentially malicious program & unwanted program (PUP) scan
- Search keyword lookup and remediate selected
- Cloud detection
- Zipped file scan
- CPU usage setting

System Settings

- Remediation Methods
  - Auto remediation setting
  - Delete irremediable file setting
  - Remediate/ignore infected zipped file setting
  - Remediation level setting
- Scan Exception Setting
  - Folder, file, extension
- Scan options

Administrators



Log Management

- Event log, detection log
- Lookup by date & scan results
- Save log files

Quarantine

- Lookup quarantine list and export
- Restore quarantine file

Program Exit

- End executable programs only
- Delete program (delete quarantine, log, and preference data)

EPS Integration Features

- Detect and remediate from EPS Lock Mode (not supported in EPS standalone)
- Lookup integrated Xcanner event log and detection log from AhnLab EPS server
- Manage and renew Xcanner license from AhnLab EPS server
- Download Xcanner mounted with the latest engine daily from AhnLab EPS server

(EPS Client for Windows, EPS Standalone)

Advantages (1)

AhnLab Xcanner does not require installation; it can be run by being mounted on a removable storage device.

Easy to Use via Removable Storage Device

Establish Security Policy for Removable Storage Device

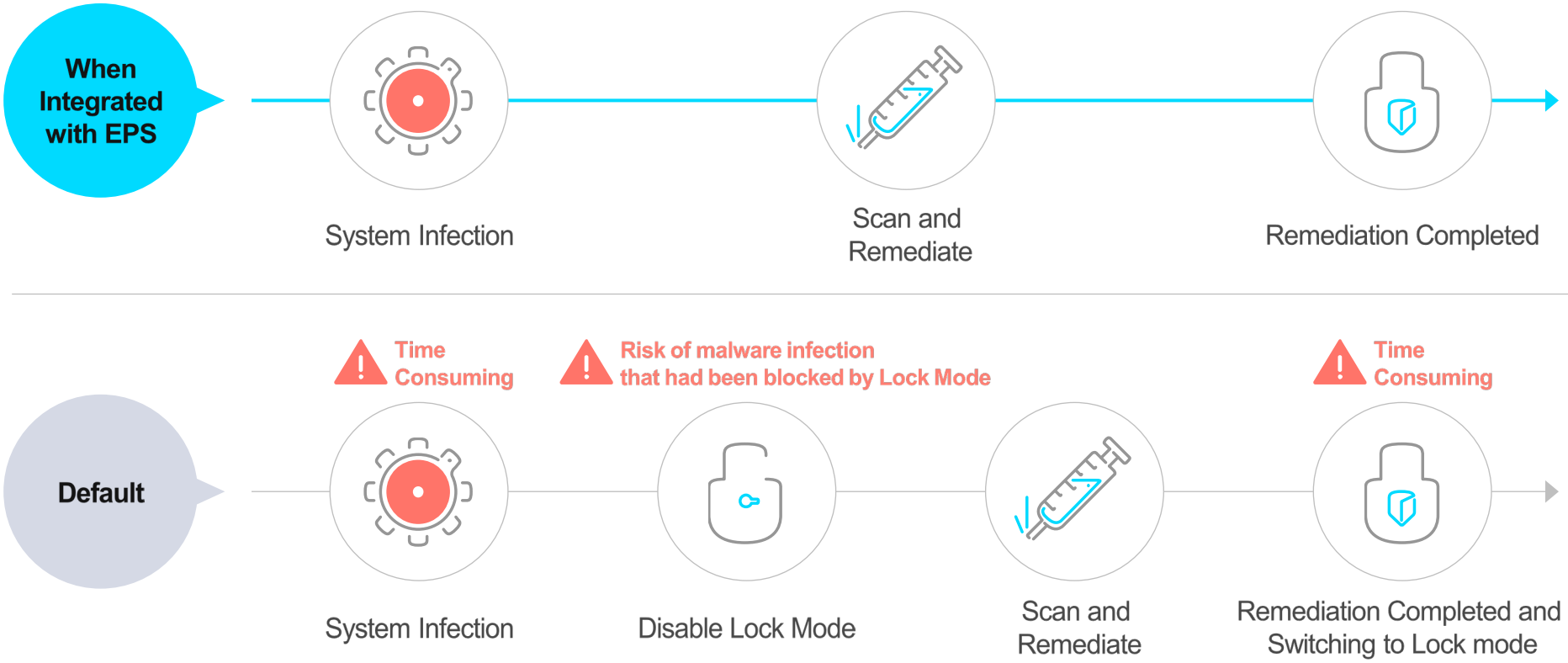
Mount Xcanner on Authorized Removable Storage Device

Run Xcanner

Advantages (2)

When integrated with EPS, AhnLab Xcanner can be used even in Lock Mode.
It saves time and removes risk of malware infection due to disabling Lock Mode for malware scan and remediation.

Available in Lock Mode with EPS Integration



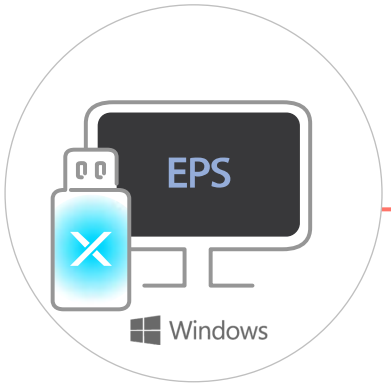
※ EPS Standalone not supported.
※ Malware scan and remediation is also possible after disabling Lock Mode due to limitations in system availability

Advantages (3)

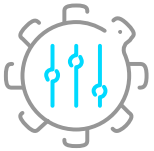
Using EPS with AhnLab Xcanner allows system administrators to centralize scan and remediation logs and monitor them from the management console. AhnLab Xcanner can also respond to PE malware as well as non-PE malware, allowing more precise prevention.

Centralized Scan and Remediation Log, Allows Monitoring vis Management Console

Integrates with Xcanner to Enhance Detection

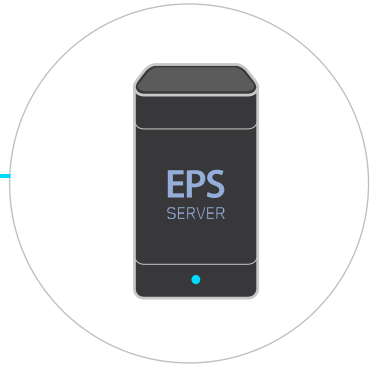


Administrator Responds and Applies Security Policies



Sends Scan and Remediation Result Logs to EPS server

Uses Administrator Web Console to Look up Xcanner Status and Logs



- Detects and remediates PE malware and non-PE malware
- Automatically analyzes file safety in cloud-based ASD server (Air Gapped Network Not Supported)
- Pre-checks memory and process
- Scans for stealth malware

- Looks up Xcanner detection and remediation result
- Provides download page for the latest Xcanner version
- Manages Xcanner license
- Monitors Xcanner status and manages policies

Advantages (4)

Because AhnLab Xcanner's engine is updated daily, it can respond to the latest malware. System administrators can download Xcanner with the latest engine through AhnLab.com and EPS server as needed.

Regular Update for Effective Malware Response

AhnLab Security Tower

AhnLab updates Xcanner engine daily to keep it up-to-date.

If you are a client of Xcanner, you are provided with the latest version of Xcanner executable in AhnLab.com even if you do not use AhnLab EPS.

If EPS Agent is installed on your device, you can download Xcanner directly from the EPS server.

※ If using EPS standalone, you can access the download page in the network environment connected with the EPS server to download Xcanner executable file.

System Requirements

AhnLab Xcanner is supported in the following environments.

		System Requirements
Hardware	CPU	Minimum OS Requirement (Supports Intel CPU)
	MEM	Minimum OS System Requirement (Recommended: 128MB or more)
	HDD	1GB or more available space
OS	Embedded OS	• Windows XP Embedded • Windows Embedded Standard 2009 • Windows Embedded Standard 7 • Windows Embedded POSReady 2009 • Windows Embedded POSReady 7 • Windows Embedded 8.1 Industry (Pro, Enterprise) • Windows 10 IoT Enterprise
	Client OS	• Windows 2000 Professional • Windows XP (Professional) • Windows Vista (Enterprise, Ultimate) • Windows 7 (Enterprise, Professional, Ultimate) • Windows 8/8.1 (Enterprise, Pro) • Windows 10 (Enterprise, Pro)
	Server OS	• Windows 2000 (Server, Advanced Server) • Windows Server 2003 / 2003 R2 (Standard, Enterprise) • Windows Server 2008 / 2008 R2 (Standard, Enterprise) • Windows Server 2012 / 2012 R2 (Essentials, Standard) • Windows Server 2016 (Essentials, Standard) • Windows Server 2019 (Essentials, Standard)

※ Supports both 32-bit and 64-bit for the OS above

Feature Comparison with AhnScan

		AhnScan	Xcanner
System Requirements	User Interface	Command Line	Graphic User Interface, Command Line
	Minimum Supported OS	Windows 2000 or later	Windows 2000 or later
	Supported Language	-	Korean, English, Simplified Chinese
Malware Response	Malware Scan	Full Scan	Full Scan, Advanced Scan (folder, file)
	Remediation	Full Remediation	Check scan result from UI and remediate all or selected results
	Preference	Command-line individual settings	Change settings from UI
Administrator Features	Log Management	Save log file	Save log file, lookup and search log from UI, export as CSV
	Quarantine	X	Provided
	Exit program	Exit program	Exit program, choose to save deleted or reused data

More security,
More freedom

© AhnLab, Inc. (Headquarter)
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do 13493, Korea
Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | Business Inquiries: global.sales@ahnlab.com | www.ahnlab.com

AhnLab Xcanner

AhnLab

www.ahnlab.com
www.linkedin.com/company/ahnlab-inc.
www.youtube.com/user/OfficialAhnLab