

NEVER MIND THE SECURITY



100% SIGNATURELESS ANTI-RANSOMWARE
THE ONLY ANTI-RANSOMWARE PROFESSIONAL SOLUTION THAT SOLVES RANSOMWARE
ADVANCE DETECTION, BLOCKING, AND AUTOMATIC RECOVERY AT ONCE

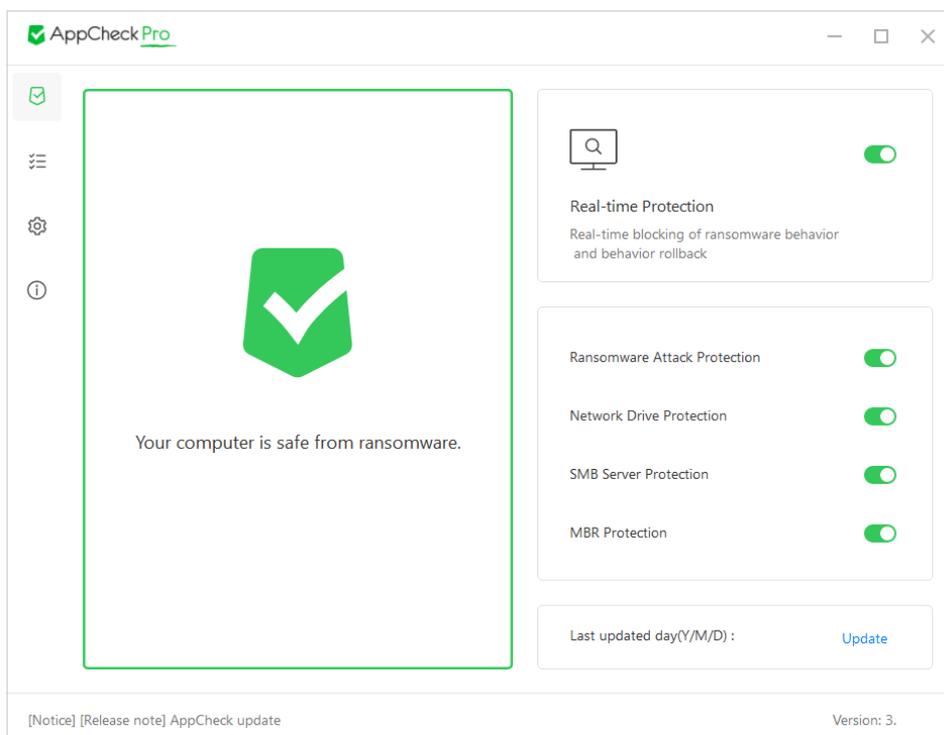


AppCheck Pro

AppCheck Pro for Windows Server

Patented 100% Signatureless Anti-Ransomware

The only anti-ransomware professional solution that solves ransomware advance detection, blocking, and automatic recovery at once



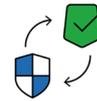
More powerful Anti-ransomware

New/variant ransomware advance defense, detection, blocking, data backup, and automatic recovery all at once!



Outstanding Server Protection

SMB server protection blocks the IP address of a remote PC during a ransomware attack.



Perfect Compatibility

It can be used with an antivirus without collisions and performance degradation.

More powerful ransomware behavior detection

- Detects more than 2,800 new/variant ransomware attacks with context-awareness-based ransomware behavior detection engine (CARB engine)
- Enhanced ransomware protection with advanced detection features (ghost detection, smart detection)
- Through the SMB server protection function, when ransomware executed on a remote PC attacks a shared folder in the server, the IP address of the remote PC is automatically blocked
- Blocks ransomware attacks inside/outside the server through a shared folder protection function considering the corporate environment
- Prevents incapacitation of Windows system restoration function by ransomware and malicious programs
- Pre-blocking safe mode boot execution for attack
- Automatic deletion of files created by ransomware when ransomware behavior is detected

Real-time detection and defense of vulnerability attacks (AppCheck Pro v3.0)

- Real-time detection and proactive defense of zero-day exploit attacks
- Protects the system from attacks on vulnerable Internet Explorer web browser vulnerabilities
- Choose which applications to protect can be applied

Temporary backup and restore to a safe haven

- Deletion of files damaged by the attack when ransomware is detected
- Real-time file backup and restoration in case of damage to protected files
- Disk capacity management through various shelter backup settings
- Provides a function to move the shelter route considering the disk capacity

Automatic backup with double protection against ransomware

- Supports data backup to other storage devices connected as local disks or network drives
- Supports periodic automatic data backup according to various schedule settings
- Maintaining and managing changed backup data files through file history

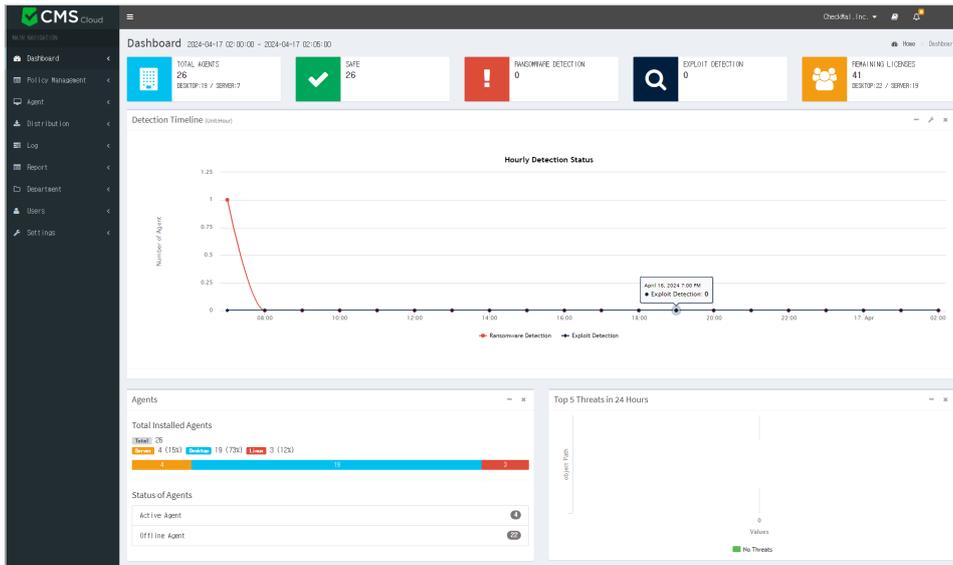
Appcheck that can be used more safely and lightly

- Block remote PC IP in case of ransomware attack from remote PC to server
- Concentrate ransomware attack detection function tailored to stable server operating system
- Compatibility with common antivirus products without crashing or compromising performance
- Maintain lightweight resource usage that does not impact server operation
- Korean / English / Japanese automatic language support according to the operating system

CMS Centralized Management

Endpoint central management solution that can easily manage security solution products

A central management solution that efficiently supports infection information and AppCheck detection logs, policy and agent management



Convenient management

- Agent management through department management considering corporate environment
- Efficient agent management by adding new policies in addition to individual policies
- Provides management convenience with live policy updates for modified policies

Management console with convenient unattended install/uninstall

- Unattended installation function that does not interfere with the user's work (provided by corporate users)
- Distributed via E-mail and PMS (Patch Management System)
- CMS Cloud that does not require separate server construction
- CMS Business that can be maintained even in a closed network environment

Detection notification for administrators

- Specify the date and use various filters to output a report consisting of only the necessary information
- Various information can be checked by providing detailed information for each agent
- Administrator e-mail notification function when ransomware is detected

Web-based interface for mobile, PC and tablet

- It operates on a web-based console composed of HTML5, allowing administrators to control all functions with only a web browser
- Responsive web, compatible with mobile web browsers, manages all functions
- Monitor the current situation at a glance on the dashboard

Convenient and Complete AppCheck Operation Process

Equipped with a patented situational awareness-based detection engine
Blocks new/variant ransomware
100% signatureless anti-ransomware solution



System Requirements

System Requirements	AppCheck Pro	AppCheck Pro for Windows Serve	CMS
Operating System	Microsoft Windows 7 SP1 (KB4490628, KB4474419) / 8 / 8.1 / 10 / 11 (32/64bit)	Windows Server 2008 R2 SP1(KB4490628, KB4474419) or higher	CentOS 7.0 or higher
CPU	Intel 6th generation Core i5 or higher AMD Ryzen 1000 series or higher	Intel Xeon Dual Core	Intel Xeon 3.0GHz or higher
Memory	4GB or higher	8GB or higher	4GB or higher
HDD	30GB or higher	64GB or higher	200GB or higher
Web Browser	MS Edge / Chrome / Firefox	MS Edge / Chrome / Firefox	MS Edge / Chrome / Firefox

Certification and Patent



▲ GS Certified



▲ Security function verification



▲ Copyright Registration



▲ Patent Certificate



(16827) A Bldg #1308, U-Tower A, 767, Sinsu-ro, Suji-gu, Yongin-si, Gyeonggi-do, Republic of Korea

Homepage <https://www.checkmal.com>

Tel +82-70-7770-5548

Email contact@checkmal.com

The information published in this document can be changed without prior notice.

© CheckMAL Inc.