White Defender Products Lineup

WhiteDefender Lineup

Why WhiteDefender?

A) Do you have the technology to quickly analyze and respond to ransomware?

B) Can you immediately recover files attacked by ransomware?

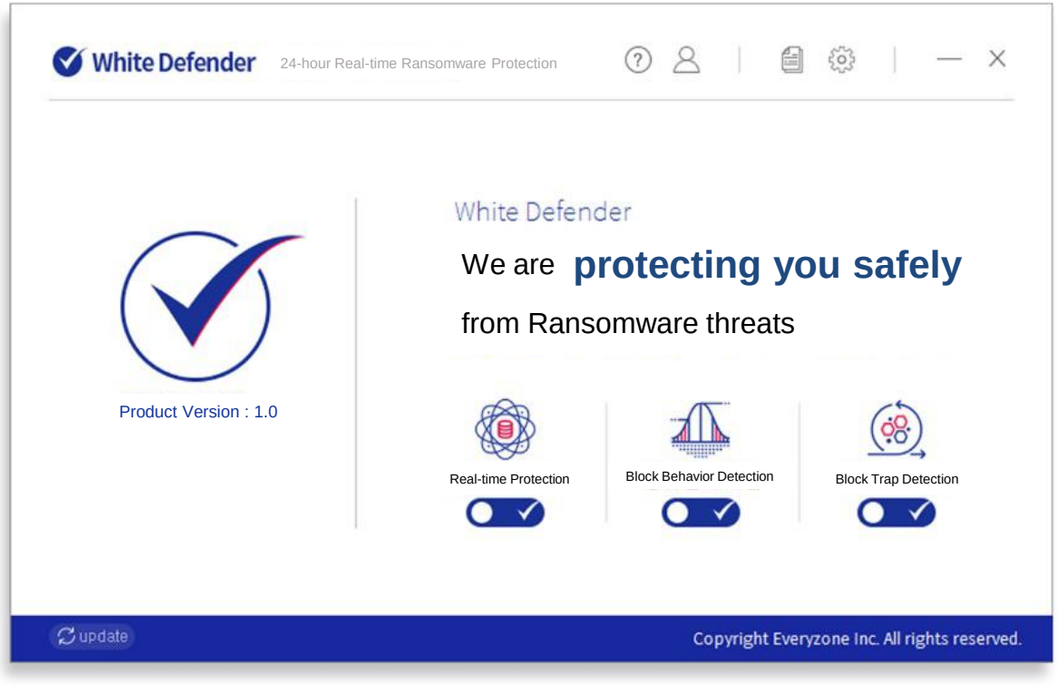
C) Are continuous SW updates and patches possible to keep up with ransomware evolution?

D) Is it possible to provide quick compatibility resolution support for the SW being used internally?

E) After PC installation, does it occupy a minimum cpu percentage of less than 2%?

White Defender!

It's an Anti-Ransomware solution which can answer **Yes!** to all these questions



White Defender, a proprietary security technology for preemptive defense

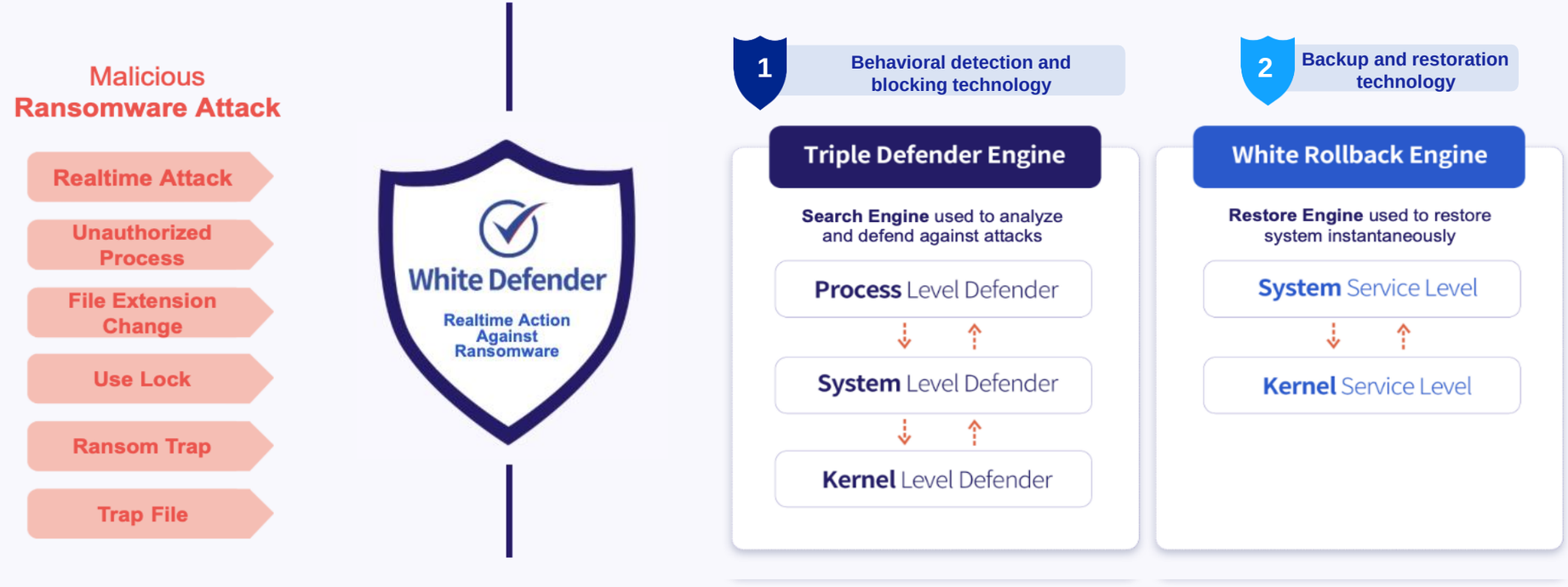
1 Behavioral detection and blocking technology

2 Backup and restoration technology

White Defender is a product launched by Everyzone based on over 25 years of turbo vaccine development and research.

This is a **next-generation anti-ransomware solution** that monitors and blocks ransomware in real time and defends against unknown ransomware through a **3-stage defense system (process level > service level > kernel level) developed with proprietary technology aimed at actively responding to ransomware.**

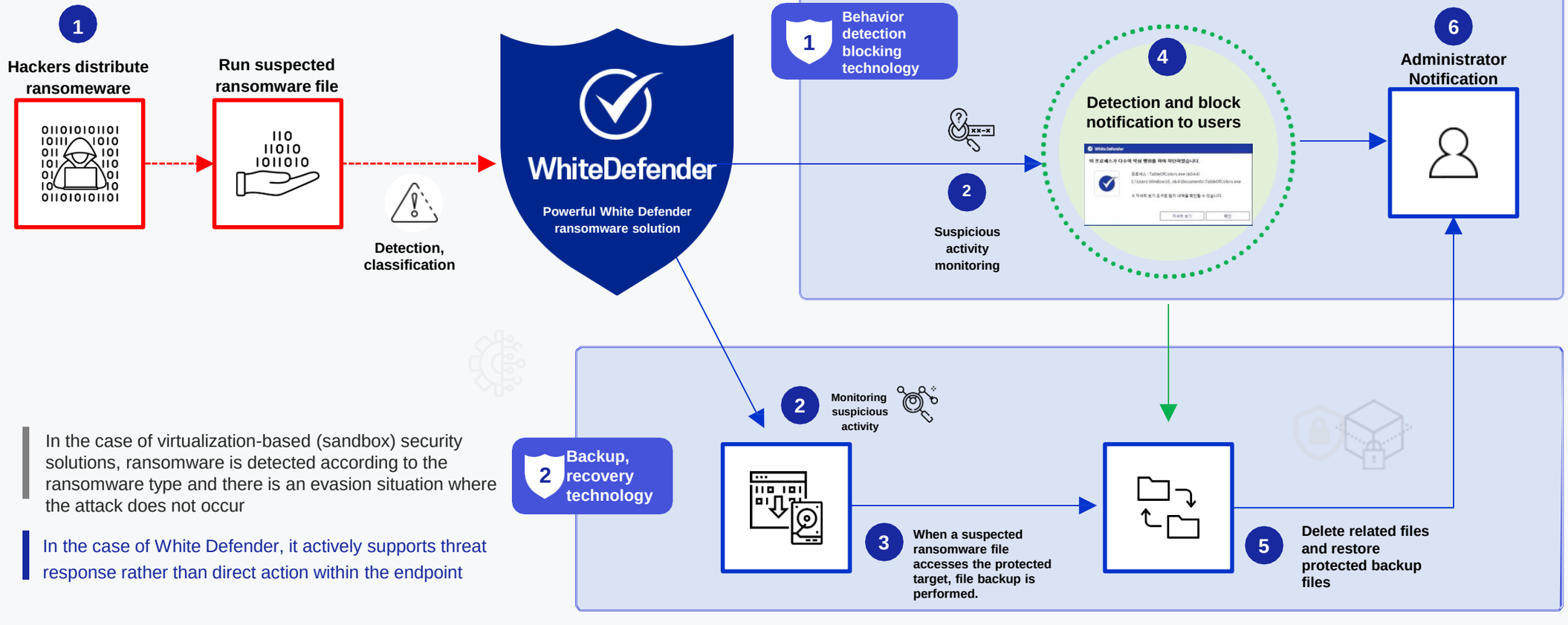
Two ransomware detection engines



Behavior-based ransomware blocking detection and restoration technology

Active response technology to threat situations by exchanging complex information during the operation process to support major detection and blocking/restoration

White Defender's behavior detection and blocking technology



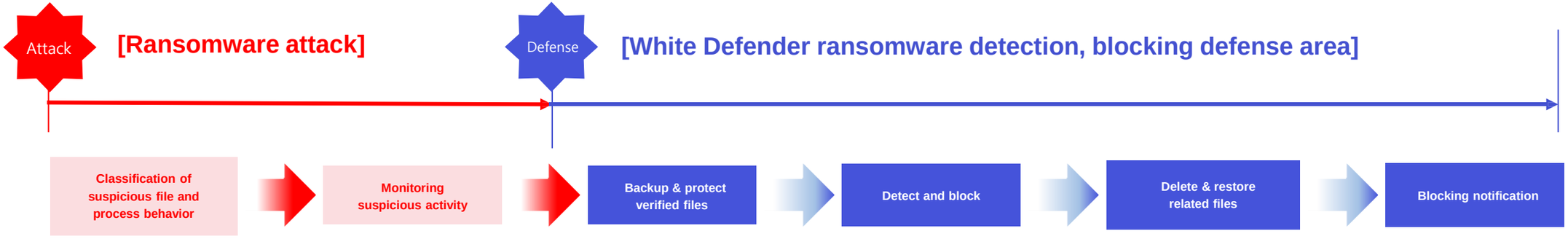
In the case of virtualization-based (sandbox) security solutions, ransomware is detected according to the ransomware type and there is an evasion situation where the attack does not occur

In the case of White Defender, it actively supports threat response rather than direct action within the endpoint

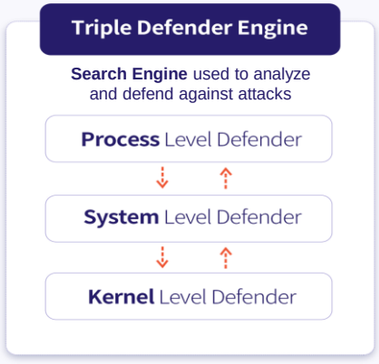
White Defender operation process for responding to ransomware

When a suspicious ransomware-related activity occurs on an endpoint system where the White Defender product line is installed,

the TD engine that performs detection and the WR engine that performs instantaneous backup and restoration of the protected files interact with each other to perform ransomware response detection and blocking.



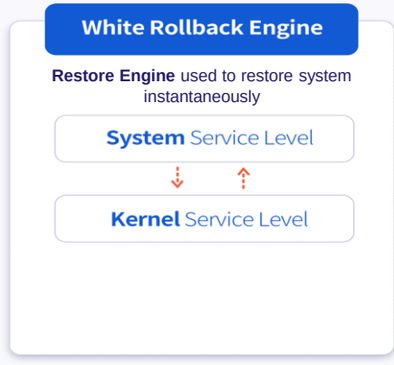
TD engine (Triple Defender Engine)



1 Behavior detection blocking

- A detection engine that monitors and analyzes various ransomware attacks in real time to defend against them
- When processes executed on the endpoint system and other processes injected into existing processes, and scripts executed are classified as suspicious behaviors, the White Defender service and driver interact with each other to monitor the suspicious behaviors and conduct analysis and judgment
- Once the final detection and blocking is completed, files that should be deleted due to suspected ransomware activity are deleted and moved to a recovery site

WR engine (White Rollback Engine)



2 Backup, restoration technology

- When a ransomware attack occurs, the protected files accessed by processes related to suspicious behavior are instantly backed up and sequentially restored as the detection and blocking process proceeds.
- Collected information on suspected ransomware activity is analyzed and restored by **the distinctive implemented core engine.**

White Defender, a proprietary security technology for preemptive defense

This section details White Defender's main detection and blocking/restoration actions in each major infection scenario where a suspected ransomware file is executed.

Attack **Ransomware infection by situation**

Running phishing email attachments

User executes malicious file via attachment or link within phishing email

Attacks via compromised websites

Visits to compromised websites, searches, downloads, etc for illegal materials, are executed and infected through vulnerabilities

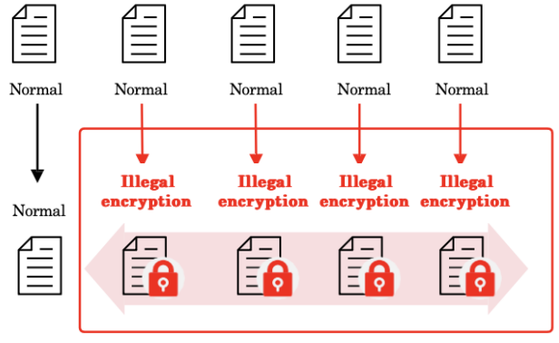
Security vulnerability exploitation attack

Visits to compromised websites, searches, downloads, etc for illegal materials, are executed and infected through vulnerabilities

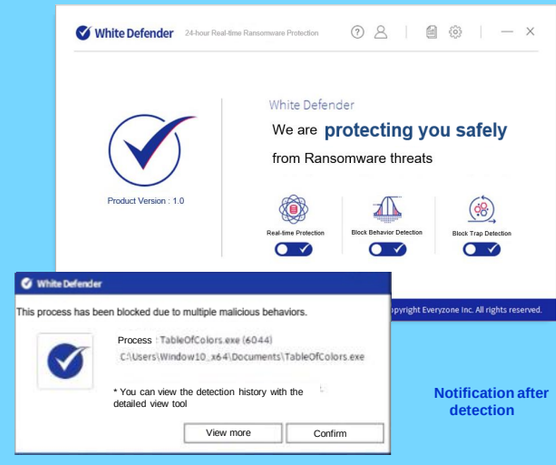
Attack **Ransomware attack execution**

Encryption attack proceeds according to ransomware characteristics

Monitoring and real-time backup of protected files in case of suspected ransomware in the system



Defense **Ransomware detection defense notification**



If it is determined that there is an illegal encryption situation due to a suspicious process, the ransomware process is stopped, the expected damaged files are restored, and then the user is notified.

White Defender optimal system utilization

The White Defender product line provides maximum protection against basic operational slowdown of installed endpoint systems with low system resource utilization levels.

White Defender's excellent performance

System resource utilization measurement results

Classification	Normal Condition	Upon detection	Remark
CPU	About 1%	About 3%	When ransomware is detected, there is no slowdown in system operation
Memory	Approx. 40 MB	Approx. 40 MB	No change
Ransomware detection time	0 sec	3.4 sec	The duration to backup and restore after detecting ransomware based on the behavior

Even when behavior detection blocking is in progress, security and system performance is maintained at its best.

White Defender's main features and key features

White Defender safely protects important data on your PC by operating protection mechanisms such as pre-detection, trap detection, behavior detection, automatic backup/restoration, and protected folders to provide strong response to ransomware.

Classification	White Defender
Detection features	1. Has its own engine that protects against ransomware and blocks file corruption and rolls back damage 2. Minimize false positives for suspicious situations through forensic verification of the behavior detection engine 3. Using a ransomware target pre-detection database
Security threat response form	1. Simultaneous tracking and monitoring of suspicious processes related to user files 2. Do a real-time backup and monitor changes when suspicious situation occurs 3. When file corruption is detected by a suspicious process, driver linkage is used to obtain maximum information related to the changes and restoration is performed.
Personality of the behavior	✓ Proactive based on behavioral engine detection ✓ Security features + ransomware specific efficiency ✓ Provides high pre-detection capabilities and security features at the same time

Excellent Performance

GS quality certificate grade 1

Anti-Ransomware Real-Time Protection

White Defender PC Products

Monitor ransomware threats in real-time and defend against even unknown and emerging ransomware.

1/ Real-time monitoring
Real-Time Ransomware Protection

Ransomware risks require real-time, 24/7 defense. It provides real-time defense against a wide range of security risks, including ransomware attacks.

Real-Time Ransomware Protection

2/ Unknown new species
Ransomware Behavior Detection

Proactively detect malicious ransomware behaviors and behaviorally defend and respond to emerging and lesser-known ransomware.

Behavioral detection

3/ Respond to file corruption
Ransomware backup/recovery

Defend against falling into sophisticated ransomware traps. It provides defenses to help clients stay ahead of persistent security threats.

Automatic backup/recovery

Product features for PC

Self-Protection

- Self-protection against corrupted processes, folders, and registries

Shadow copy protection

- Block accesses to information used in restoration, and at the time of the restoration point

Non-signature process execution notification/blocking

- When unsigned files are executed, alerts will appear with options of Allow, block, or exception

Block file writes

- Prevents ransomware infections with my PC & network File write protection

Blocking risky script behavior

- Block dangerous files being created by scripters

Deleting a saved file for restoration

- Stores detected restore files that are set for a set period, then the data afterwards are automatically deleted

Behavioral detection restoration save file

- Ability to exclude saving a behavior detection restore file if it's larger than the file that has been set (up to 100 MB)

Recommended products specifications for PC

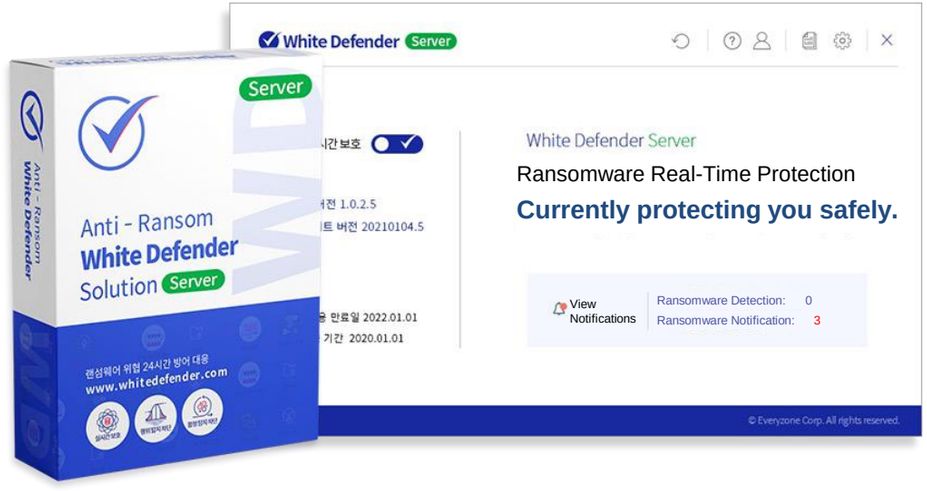
Category	Specification
Operating systems	Windows 7 and higher recommended
CPU	Intel Pentium i3 2.6 GHz or faster
Memory	2GB or more
Storage space	100 MB or more for installation / 5 GB or more for operation

※ If the program's default network is blocked by a firewall, normal updates may not work.

Real-time monitoring of ransomware on servers

White Defender **Server Products**

Build a reliable enterprise security environment with a server-specific anti-ransomware solution optimized for Windows servers.



1 Windows Server Only
Ransomware Real-Time Protection

Provides real-time defense against ransomware attacks across multiple security risks

Server Real time Protection

2 Unknown
Ransomware Behavioral Detection

Proactively detects ransomware's behavior and responds with behavior-based defenses against emerging ransomware

Behavioral detection

3 Responds to file corruption
Ransomware backup/recovery

Stay safe with instant backups, ransomware protection, and file recovery in case of the file being compromised

Automatic backup/recovery

Product features for White Defender Server

Self-protection

- Self-protection against corrupted processes, folders, and registries

Shadow copy protection

- Block accesses to information used in restoration, and at the time of the restoration point

Non-Signature Process Execution notification/blocking

- When unsigned files are executed, alerts will appear with options of Allow, block, or exception

Block file writes

- Prevents ransomware infections with My PC & Network File Write protection

Blocking risky script behavior

- Block dangerous files being created by scripters

Deleting a saved file for restoration

- Stores detected restore files that is set for a set period, after which the data is automatically deleted

Behavioral detection restoration save file

- Ability to exclude saving a behavior detection restore file if it's larger than the file that has been set (up to 100 MB)

Additional file protections

- Extra protection in case of corruption of protected extension files larger than 100 MB

Centralized management integration

- Centralized management of primary server operational functions with exception integration for business continuity

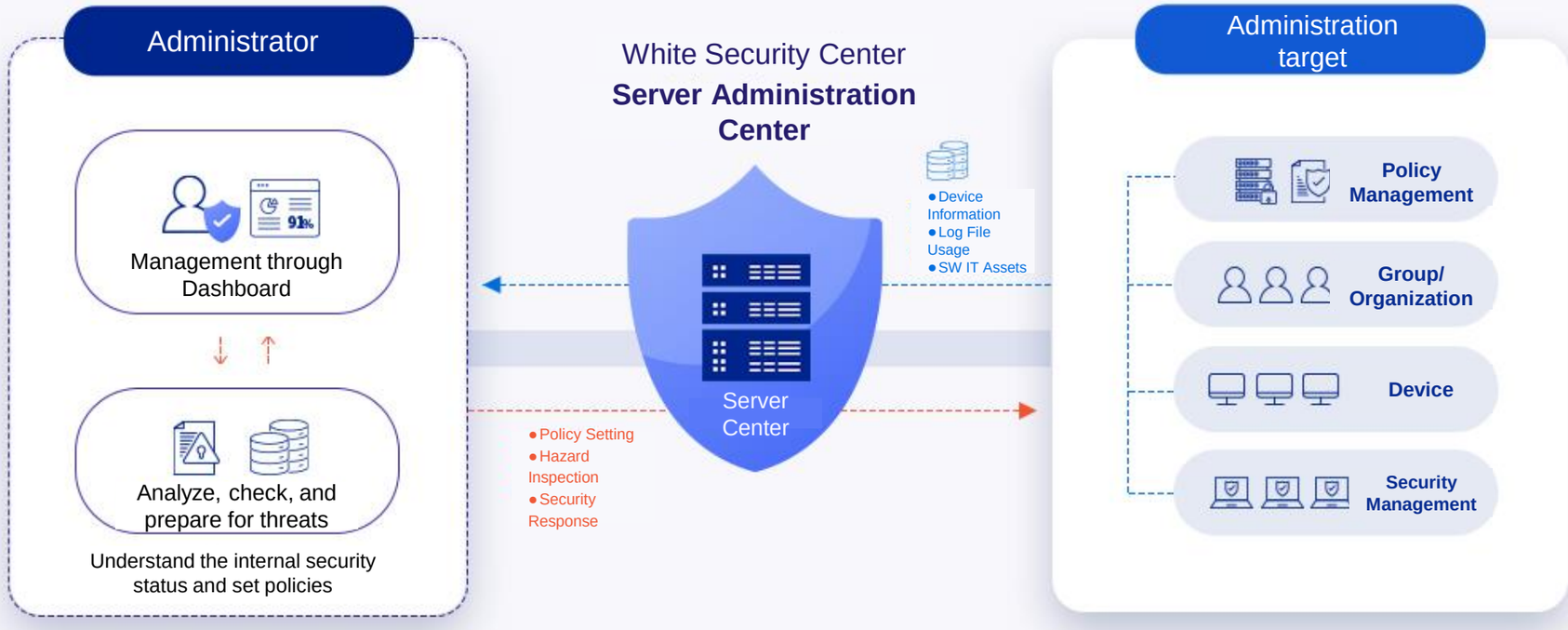
Recommended server specifications

Category	Specification
Operating systems	Windows Server 2008 R2 or higher recommended (64-bit)
CPU	Intel Xeon Dual Core or higher
Memory	Recommended memory 4 GB or more
Storage space	100 MB or more free hard drive space for installation / 10 GB or more free hard drive space recommended
Network	IPv4, IPv6 network environment recommended/ *WSC server integration for centralized management recommended

※ If the program's default network is blocked by a firewall, normal updates may not work.

White Security Center (WSC) Configuration

[WSC General Configuration Form]



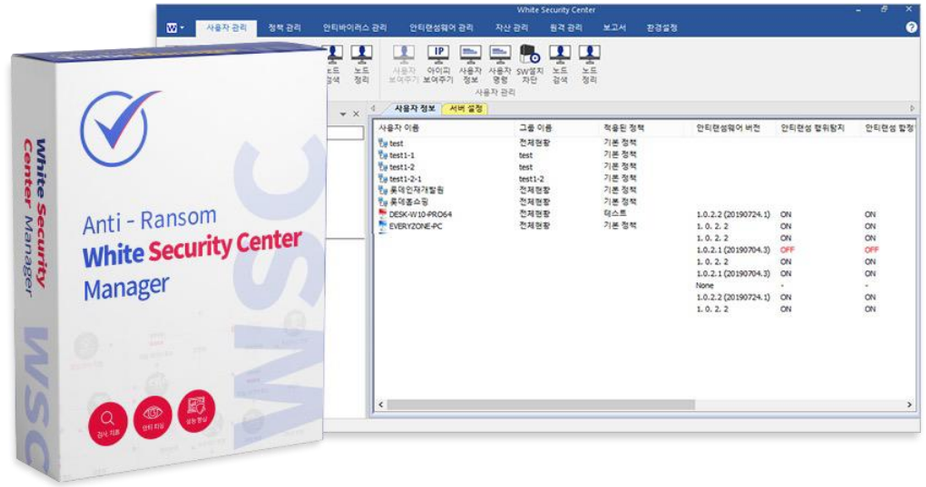
[Operating system]	WSC Server ▶ Linux CentOS 7.2 + PostgreSQL 9.5.4 or later version recommended | WSC Console & WSC Agent ▶ Windows 7 or higher
[Hardwares]	WSC Server ▶ CPU - Intel CPU with clock speed of 2.4GHz or faster | Memory - 8GB or more | DISK - 200 GB or more free space (SSD is recommended over HDD)
	WSC Console & Agent ▶ CPU - Intel i3 2.6 GHz or faster | Memory - 4 GB or more | DISK - 5 GB or more free space (SSD is recommended over HDD)

White Defender Centralized Administrator Solution

White Security Center WSC

White Security Center manages ransomware threats by collecting and monitoring ransomware threat data inside the enterprise.

Provides dashboards for administrators to view the organization's security status at a glance.



1/ Centralized management
Easy and fast usage

Manage installed White Defender, real-time usage status, and PC security status

Centralized management

2/ Policy Creation Management
Sustainable Management

By group and user
Create, delete, modify, and enforce policies in real time

Policy Creation Management

3/ Dashboard
Administrator convenience

View/print report on White Defender operation status and ransomware detection and mitigation status

Convenient dashboards

2-4. White Defender Central Administrator Product

White Security Center Features

Manages ransomware threats by collecting and monitoring ransomware threat data inside the organization.

Provides dashboards for administrators to view the organization's security status at a glance.

Dashboard

- Quickly understands the state of the internal security and take action as soon as possible when needed

Manage internal security

- Set and manage the security level of agent PCs or groups

Collect/manage internal assets

- Select agent PCs or groups to collect/manage S/W, H/W information

Management reports

- Reports to stay informed about the current state of internal security

Manage policy settings

- Set the H/W security level of agent PCs or groups

Manage remote control

- Select Agent PCs or groups to control remotely

White Security Center Configuration a web-based management console available to administrators, a central server, and agents.

Category	Specification
Product configuration environment	Server Management + Console Management + Agent
Server	Linux Centos 7.X, PostgreSQL DB
Console	Windows 7 or higher, 1 GB or more system memory, 150 MB or more storage space
Agent	Windows 7 or higher, 1 GB or more system memory, 1 GB or more storage & operating recommended

※ The server on which the White Security Center is installed may vary depending on the client's environment.

White Security Center (WSC) server configuration system recommended specifications

* Requires IPv4, IPv6 internet network environment to support latest updates

OS	Linux CentOS version 7.2 is recommended (operationally stable and the latest 7.6 version is also supported)
CPU	Intel CPU with a clock speed of 2.4 GHz or faster → Minimum 2 cores or higher / recommended 4 cores or higher
RAM	Requires at least 8 GB of free system memory → At least 8GB of free memory required (16GB or more of installed memory recommended)
HDD	200GB or more of free space on an SSD type hard drive is recommended : Install and operate on WSC Server module and PostgreSQL version 9.5.4 / save logs → SSD with faster processing speed than regular HDD is recommended

Minimum requirements for installing the White Security Center (WSC) Management Console

OS	Microsoft Windows 7 | 8 | 8.1 | 10 - (32bit/64bit)
CPU	Intel Pentium Core i3 2.6GHz or more is recommended
RAM	4 GB or more is recommended
HDD	100 MB or more free space for installation