WHITEPAPER

Fall of 2022

version 1.0.0

Endpoint Security Strategy & EDR

To Secure Visibility and Strengthen Security

NPCORE

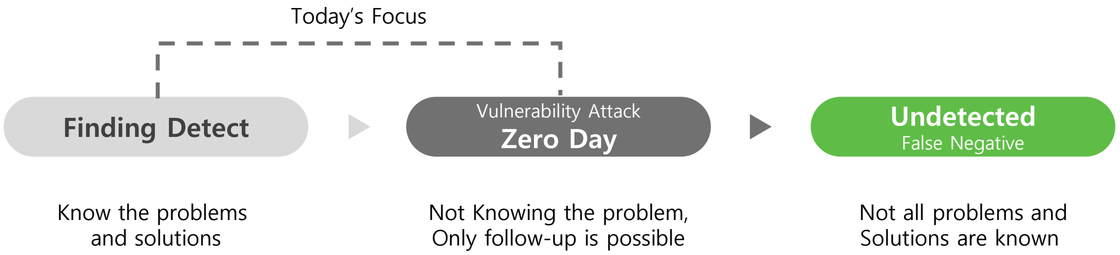
Table of contents

01 Introduction

“In the cybersecurity industry, we need to reshape our goals to be security, convenience and innovation.” said Rohit Galli, CEO of RSA, at RSA Conference 2022, which is called the world's largest cybersecurity conference and exhibition held this year. Always, technology is constantly changing and new technologies are being used. On the other hand, new types of vulnerabilities, malware, and exploits are also constantly being developed. Security should not be compromised for the sake of convenience and efficiency.

2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Real-world	BYOD	APT	BYOD	IoT	IoT	IoT	IoT	IoT	Data protection	Analytics
Real-time	Tablet	BYOD	IoT	Threat actors	Ransomware	Ransomware	GDPR	Access control	Insider Threats	Intelligence
Cloud-based	Apt	Security analytice	Security analytice	BYOD	Devops	GDPR	Blockchain	Threat management	Application security	Anti-Fraud
Third-party	Anti-virus	Mobile apps	Threat actors	Security analytice	Threat actors	IoT devices	Devops	Analytics	Simplify	C-Suite view
In-depth	MDM	Software-defined	Home depot	Kill chain	Kill chain	Devops	Devsecops	Intelligence	Bigdata	Cloud Security
High-profile	Ios	MDM	Snowden	Devops	GDPR	Blockchain	Ransomware	Human Element	Zero Trust	Cryptography
Real-life	Stuxnet	Ios	Software-defined	OPM	Blockchain	Equifax	Artificial intelligence	Global Threat	Endpoint Security	DevSec0ps
Epsilon	Flame	Stuxnet	Data science	Software-defined	Cyber insurance	Wannacry	Crypto-currency	Machine Learning	Hackers& Threats	Software Integrity
End-user	Mobile apps	Tablet	Devops	NIST CSF	Security analytics	Threat hunting	Digital transformation	GDPR	Risk Management	Human Element
Enterprise-wide	Advanced malware	Prism	Heartbleed	IoT Security	NIST CSF	Bitcoin	Women	Election Hacking	SIEM	Identity
Zero-day	Kill chain	Advanced malware	Kill chain	Anthem	Dark web	Deep learning	Containers	Compliance	DevSec0ps	Innovation
Cost-effective	Software-defined	Dropbox	Ransomware	Dark web	Bitcoin	Devsecops	Consumer privacy	Endpoint Security	Compliance	Machine Learning

Then, if we look at RSA's annual keyword history for intelligent and personalized security threats of all threats, machine learning has become the hottest keyword this year. Also, if we look at important keywords by year in more detail, APT, ransomware, endpoint security, etc. have always appeared as hot keywords, and it seems that the global security agenda has always changed, but the answer is apparently security reinforcement for undetected area which is so called, false negative.



Today's Focus

Finding Detect

Know the problems and solutions

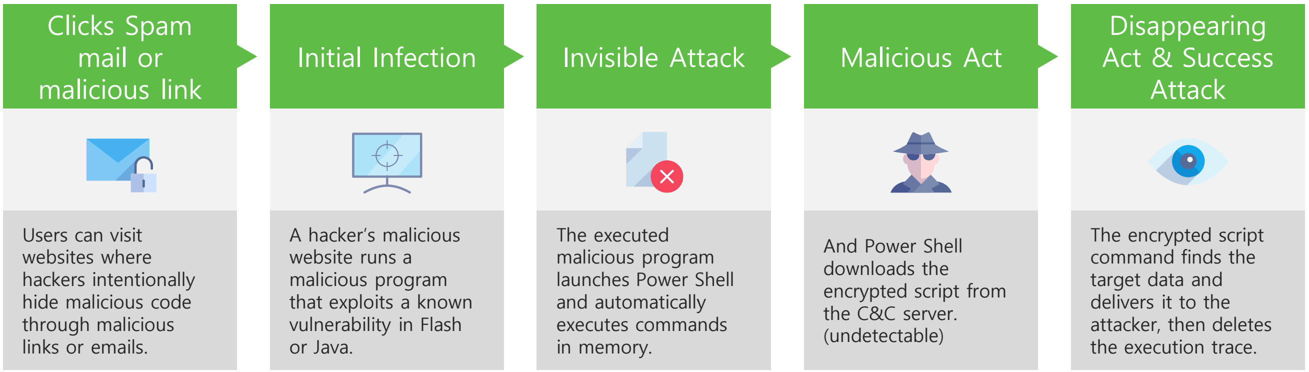
Vulnerability Attack
Zero Day

Not Knowing the problem, Only follow-up is possible

Undetected
False Negative

Not all problems and Solutions are known

So far today, if we focus on the facts that are known to be false (Findings) and the facts that are not known to be false (Zero-days), we must from now on be aware of the "false negatives". In other words, if the security focus from the past to the present has been detection and vulnerability attacks, the future security focus will be on how quickly to solve undetected areas (false negative).



Clicks Spam mail or malicious link

Users can visit websites where hackers intentionally hide malicious code through malicious links or emails.

Initial Infection

A hacker's malicious website runs a malicious program that exploits a known vulnerability in Flash or Java.

Invisible Attack

The executed malicious program launches Power Shell and automatically executes commands in memory.

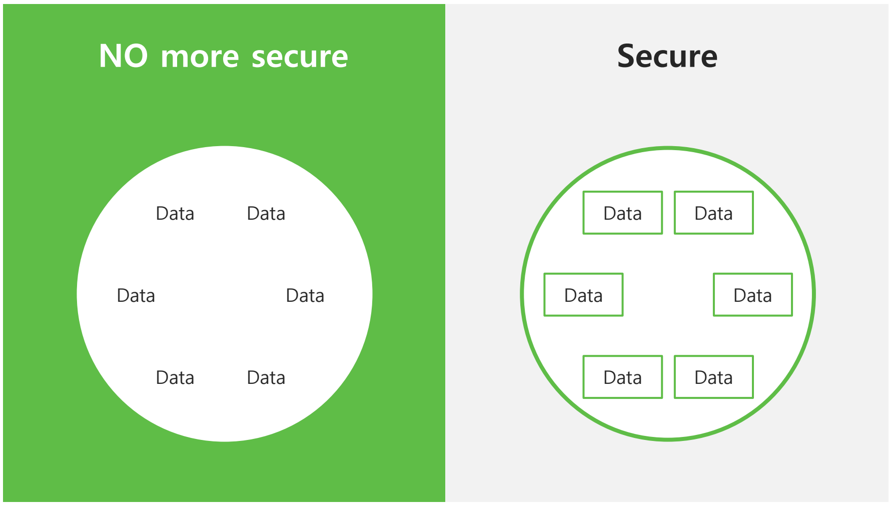
Malicious Act

And Power Shell downloads the encrypted script from the C&C server. (undetectable)

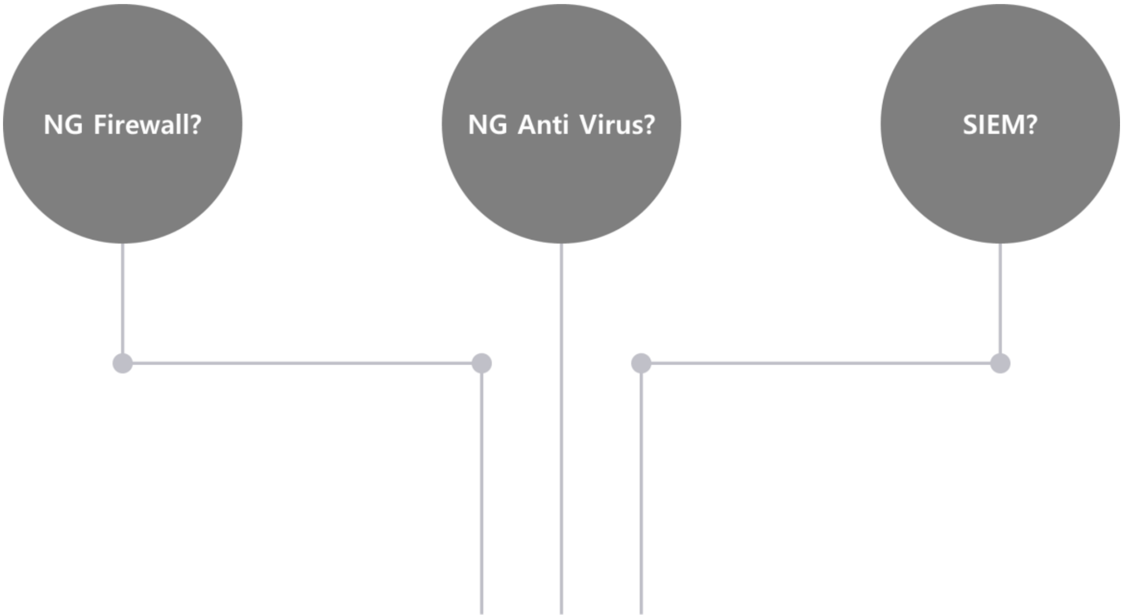
Disappearing Act & Success Attack

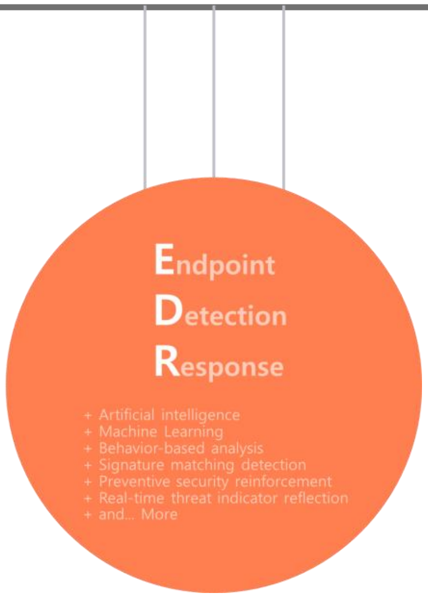
The encrypted script command finds the target data and delivers it to the attacker, then deletes the execution trace.

A typical example of "False Negative Attack" is Fileless attack. The figure above shows the sequence of typical fileless attacks. In summary, the malware is loaded into memory and executed instead of being installed on disk. Moreover, because it is loaded and executed in Powershell and WMI (Windows Management Instrumentation) installed in the Windows operating system, the antivirus unable to detect such fileless attack.

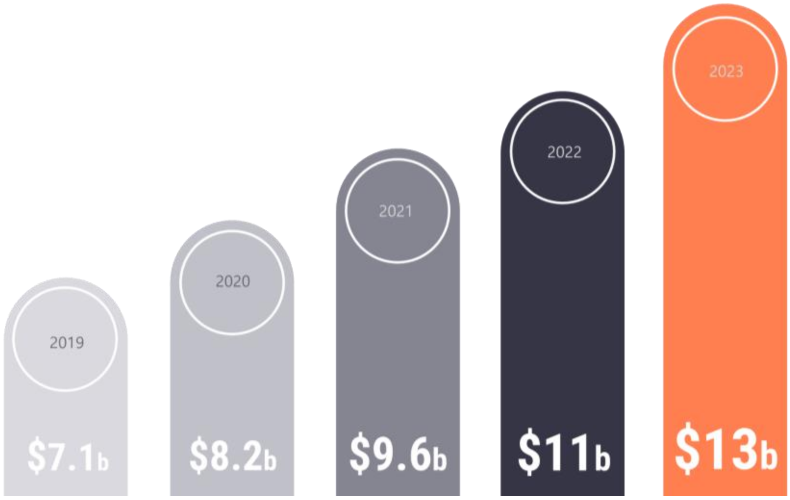


In order to prepare for malicious codes such as fileless attacks, each data must be individually encrypted and protected and managed as shown in the figure above.
So what are the best ways to defend against these false negatives? For now, we can think of next-generation firewalls, next-generation antivirus, and security devices such as SIEM (Security Information Even Management) as security devices that can respond to undetected attacks such as fileless attacks.




Endpoint
Detection
Response
+ Artificial intelligence
+ Machine Learning
+ Behavior-based analysis
+ Signature matching detection
+ Preventive security reinforcement
+ Real-time threat indicator reflection
+ and... More

Recently, the EDR (Endpoint Detection Response) system is attracting attention as the most advanced solution to these undetected areas. This is because, through the four-step analysis of EDR (signature/static analysis/dynamic analysis/reputation analysis, etc.), it is possible to overcome the parts or limitations that the conventional security devices listed previously cannot detect.



Forecast revenue from endpoint security market worldwide - statista.com

Then, let's look at why EDR is leading the global security trend from the market perspective. The growth rate of the EDR market is expected to increase from $7 billion in 2019 to $13 billion in 2023. This increasing trend is seen as EDR continues to replace the A/V market.

02 Endpoint Security Strategy and EDR

Prior to diving into endpoint security strategies and EDR in detail, let's first describe the definition and evolution of endpoint security.

An endpoint means any terminal or terminal device (laptop, desktop, workstation, smartphone, server, IoT sensor, etc.) connected to a wide network such as the Internet. And endpoint security is a strategy designed to protect the network perimeter and all terminal devices on that perimeter. To further explain, endpoints are important gateways that can affect the entire system. Therefore, endpoints are likely to be useful targets for cybercriminals (Hackers), and endpoint security aims to prevent these attackers from gaining access to systems and data.

To see the evolution of endpoint security, we can go back to 1971. It was around this time that Worm first appeared, and it was the beginning of AV (Antivirus Vaccine). The prototype “Creeper” of the worm developed by computer researchers Bob Thomas and Ray Tomlinson was developed, and a program called “Reaper” was developed by Tomlinson, which is a prototype of AV (Antivirus Vaccine) to delete the worm. The birth of the full-scale Antivirus Vaccine (AV) industry was achieved in the 1980s. After the first worm was developed, many developers began to test AV (Antivirus) programs in earnest, and the network was built almost independently. Until later network penetration increased, these programs were largely effective. In the 2000s, legacy AV (Antivirus Vaccine) is at a crossroads of change. In particular, the need for a next-generation vaccine (NGAV) has been further emphasized as cloud computing has been developed and the concept has been released to the public. However, most organizations are unfamiliar with Internet security practices, allowing hackers many attack opportunities. Entering the 2010s, the demand for EPP (Endpoint Protection Platform) / EDR (Endpoint Detection & Response) exploded. Networks have expanded rapidly as more and more organizations adopt cloud services. Therefore, there is an increased demand for solutions (EPP, EDR, etc.) that can dynamically protect and monitor a wide range of networks.

For those of us living in the present, there is an increasing number of new threats in the 2022s, and a time has come when we need to change our security strategy. Because "Ransomware", a malicious code for financial and political purposes, has emerged and attack techniques of variant malware that cannot be detected by legacy AV are increasing. Not only security teams but also attackers (adversaries) are using artificial intelligence and machine learning, and more organizations. Furthermore, this is because the importance of endpoint / endpoint security is increasing with the introduction of big data and cloud services. Under this circumstance, it is expected that more advanced XDR (Extended Detection & Response) will be seriously reviewed and introduced EDR more common in the near future. Prior to suggesting the full nine endpoint detection strategies, let's take a look at some **endpoint threat types** in the table below.

Data Loss An attacker could use endpoint vulnerabilities to access datastores in public systems. Attacks using valuable local data with in the endpoint Are also possible.	Phishing It is a method used by attackers to obtain Financial information, ID, password, and personal information from users. Many users still suffer significant damage through Emails or malicious links.
Unpatched Vulnerabilities Unpatched Vulnerabilities in endpoints provide an Opportunity for attackers to exploit system privileges By exploiting the vulnerabilities stored in endpoints (terminal devices).	Malicious Code In order to infect the system, attackers advance the method of infecting endpoints with malware in various Ways, such as manually, via email, and infecting legitimate download files.

Nine endpoint threat detection strategies are suggested as follows:

1

Extensive Malware Sample Modeling - Fast, intelligent endpoint threat detection starts with the study of a valid and diverse sample. These studies allow us to correctly determine threats and harmless software environments. However, it should include malware samples with advanced evasion techniques to avoid creating overly simplistic models.

2

Applying a weighted scoring detection model - a scoring model is important because not all malicious indicators are created equal. Even smartly crafted malware eventually makes mistakes. It is impossible to keep all activities secret. A detection model should use as many metrics as possible to precisely measure a contextual detection threshold.

3

Studying normal software behavior - learning is necessary as much as possible about how normal processes work in order to advance advanced threat detection and find malicious behavior in processes more easily. By studying the behavior of normal processes, we can also expect a reduction in the generated noise level and false positives.

4

Mid-to-long-term data analysis - It is important to analyze data over a long period of time, as malware sometimes executes malicious actions over a long period of time and interval. Malware manufacturers are well aware that there are “temporary blind spots” in endpoint security products, and that delayed execution can be used to bypass even the most advanced threat detection systems.

5

Simultaneous use of static and dynamic analysis - Dynamic analysis is essential for detecting the behavior of malicious code with complex packers. However, code that bypasses traditional malware techniques (such as hooking) should be subjected to static analysis. For example, when analyzing memory, static file properties such as Signature and PE section structure are important for advanced threat detection.

6

Aggressive use of threat intelligence - Understanding the correlation between the technologies of new malware types and their numerous variants is critical to advanced threat analysis. It learns the traits of malicious code through machine learning, uses artificial intelligence to keep the accurate detection rate high, and keeps the false positive rate as low as possible, so applying threat intelligence is the most effective.

7

Gathering sufficient analytical data - The vast amount of data collected from a process during runtime may seem redundant at first, but having a thorough strategy and gathering enough data is critical when creating an advanced threat detection method. It also enables a more precise incident analysis by the incident response team in the event of an incident.

8

Memory analysis - Memory analysis requires a complex task because of high CPU utilization and careful handling due to the volatile nature of memory. However, given the vast amount of malware that cannot be detected by other means, memory analysis is essential for advanced threat detection.

9

Applying optimized machine learning algorithms - Machine learning has greatly advanced the detection of threats that could not be detected based on the existing rules (Rule-Based) due to the vast variations and dependencies of malicious code. However, machine learning algorithms cannot be standalone tools, and the models must be manually reviewed and continuously improved by researchers with specialized security knowledge

03 ZombieZERO EDR and Expected Results

In this chapter, the main features and configuration of the ZombieZERO EDR product proposed by NPCore in accordance with the endpoint security strategy as previously suggested will be presented. In addition, the expected effects of the introduction of ZombieZERO EDR will be briefly proposed.

Advanced malware detection and blocking

- Analyze and detect advanced malware threats, and detects real-time threats based on global breach indicators.
- The evolution of EDR solutions! Block unknown malware with legacy AV + EDR function.
- Prepare fully for diversified malicious codes by supporting a total of 70 analyzable file formats.
- National Cyber Safety Center / Education Cyber Safety Center Executes static analysis of malicious code using YARA Rule pattern.

Virtual machine sandbox for dynamic analysis system

- Provide analysis function in a closed network environment through the virtual machine sandbox dynamic analysis system.
- Support manual update function and manual analysis of suspicious files in Internet blocking environment.
- Provide precise detection and blocking functions for virtual machine sandbox bypass malware.
- Support creation of sandboxes for various Windows OS versions, and up to 60 sandboxes can be created.

03 ZombieZERO EDR and Expected Results

Global threat of IOC (Indicators of Compromise) and reputation analysis

- Detect and block malicious behaviors reflecting the domestic and international intrusion threat indicators (IOC) in real time.
- Cross-checking malicious codes by utilizing overseas famous malware reputation analysis engines (Virus Total, McAfee).
- Update frequently patterns related to new types of malware based on the reliability of NPCore's Cyber Security Center (NSOC).
- To realize the zero threat of malicious code compromise, a four-step malware analysis system, Zero Trust Shield, is applied.

Providing user-centric convenience

- Provide analysis reports in various formats (DOC / EXCEL / PDF) that are easy to edit and understand.
- Provide protection computer asset security level, malicious file analysis status, security event status, etc. through the integrated dashboard.
- Provide E-mail and SMS alarms of security events depending on the characteristics of the institution when they occur.
- Provide Syslog linkage function for interworking with integrated security control system and heterogeneous security solutions.

03 ZombieZERO EDR and Expected Results

Technology-intensive design and proven stability

- Block fundamentally the possibility of malicious code infection with the function of pending the execution of the first executable file and analyzing it.
- Provide different application of security policies by organization and group. (Provide whitelist-based operation function)
- Minimize user PC resource usage and provides a function to prevent conflicts between different solution execution processes.

By adopting ZombieZERO EDR that meets the endpoint security strategy, security is strengthened by securing endpoint visibility, and organizations can secure the stability of the cyber security system and maintain business continuity.

As-is

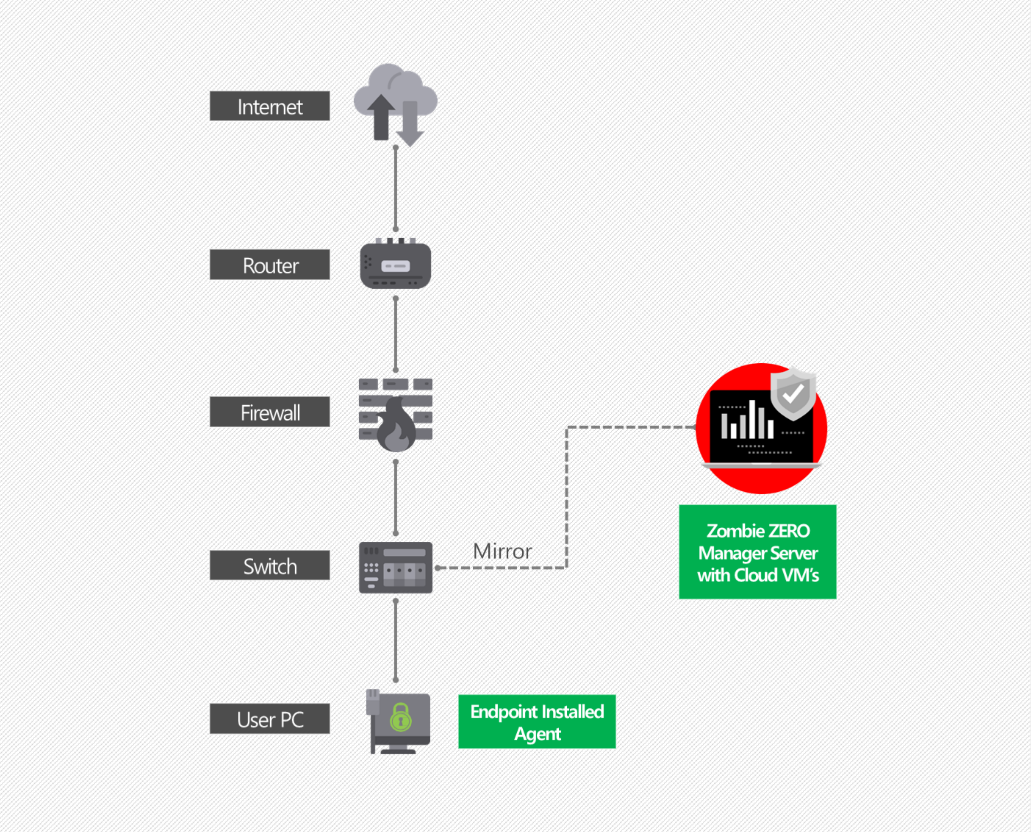
AV signature-based detection	• Signature-based blacklist method • Unable to detect new malicious codes and advanced continuous attacks-Multiple AV avoidance techniques exist
Persistent cyber threats	• Increasing cyber threats targeting organizations • Latent/hidden malicious behavior • Software and Web Vulnerability Attacks
Difficulties from a security manager's perspective	• Limitations on the existence of malicious file and the status of damage • Limitations on damage status reports, requests, and responses from higher authorities • Difficulty in monitoring and responding to malicious attacks

To-be

Advanced detection and blocking of new/variant malware	• Detection of known/unknown as behavior-based detection • Attack detection through the most vulnerable user terminal • Securing endpoint threat visibility (providing detailed information such as threat types, router, and attack targets)
User-friendly convenient system	• Real-time monitoring of analysis/detection results • Easy management of external inflow/outflow of files • Integrated management of Agents installed on each PC and comprehensive policy establishment
Creating a safe information security environment	• Establish a response strategy for potential threats • Prevention of loss of important data and reactive response through backup and recovery functions • Maximize the effectiveness of security management by linking with an integrated control system in the future

04 Configuration of ZombieZERO EDR

The following is a configuration of ZombieZERO EDR which is typically proposed on the ordinary network setting of the organization.



ZombieZERO Manager Server

- ✓ Endpoint agent management
- ✓ Security policy management and distribution
- ✓ Malicious executable file collection and detailed analysis
- ✓ Create/Manage Virtual Machine for Sandbox
- ✓ Yara Rule Update Management
- ✓ Collection of indicators of compromise of cyber threats

ZombieZERO PC Agent Software

- ✓ Real-time monitoring of user PC malicious process
- ✓ Detect and block malicious executable files
- ✓ File backup/restore in preparation for file corruption(Ransomware)
- ✓ User PC security threat control by manager server policy
- ✓ Real-time collection of other malware-related artifacts

WHITEPAPER

ISBiz Tower 1001, 26, Yangpyeong-ro 21-gil,
Yeongdeungpo-gu, Seoul, Korea
Email: sales@npcore.com

We Protect your Brand Reputation

NPCORE