Study on Improving Endpoint Security Technology★

Seung Jae Yoo*

ABSTRACT

Endpoint security is a method of ensuring network security by thoroughly protecting multiple individual devices connected to the network. In this study, we survey the functions and features of various commercial products of endpoint security. Also we emphasizes the importance of endpoint security to respond to the increasingly intelligent and sophisticated security threats against the cloud, mobile, artificial intelligence, and IoT based sur-connection era. and as a way to improve endpoint security, we suggest the ways to improve the life cycle of information security such as preemptive security policy implementation, real-time detection and filtering, detection and modification.

엔드포인트 공격대응을 위한 보안기법 연구

유 승 재*

요 약

엔드포인트 보안은 네트워크에 연결된 여러 개별 장치를 철저하게 보호함으로써 네트워크 보안을 보장하는 방법입니다. 본 연구에서는 엔드포인트 보안의 다양한 상용제품의 기능과 특・장점을 살펴본다. 그리고 클라우드, 모바일, 인공지능, 그리고 사물인터넷 기반의 초연결시대를 대비하여 날로 지능화되고 고도화되는 보안위협에 대응하기 위한 엔드포인트 보안의 중요성을 강조하고, 그 개선방안으로서 선제적인 보안 정책 구현, 실시간 탐지 및 필터링, 탐지 및 수정 등의 정보보안의 생명주기의 개선방안을 제시한다.

Key words : Endpoint Security, Network Security, Security Policy

접수일(2018년 8월 31일), 수정일(1차 : 2018년 9월 23일)
게재확정일(2018년 9월 29일)

* 중부대학교 정보보호학과

★ This paper was supported by Joongbu University Research & Development Fund, in 2018.

1. Introduction

According to market researcher Erricson, the penetration rate of IoT devices will reach 16 billion in 2021 from about 4.6 billion in 2015, with annual market growth of 23%. However, since IoT devices, which are the foundation of the connection society, are generally characterized by utilizing open source, there is a threat that security vulnerability is high and vulnerability is easily exposed.[4]

Until a few years ago, the concept of PC security was satisfied with the installation and operation of antivirus and network firewalls on individual terminals. However, in terms of its operation and efficiency, it has come to require linked and integrated services rather than individual ones. Especially, the need for and the importance of endpoint security has already been proven by the 2003 Slammer worm, which has caused massive damage to networked systems.

Endpoint security is an approach to ensure network security by thoroughly securing individual devices such as computers, laptops, smart phones, tablets, and smart cameras which are connected to the network. Endpoint security differs from simple home computer protection measures, such as firewall or antivirus software installation, by centrally managing security tools installed on endpoints. That is, there are software 'agents' running in the endpoint background, and there is a centralized endpoint security management system that monitors and manages these agents. Endpoint security products are basically based on roles such as anti-virus and network firewall. In addition, the endpoint security products are based on roles such as application control, port control, browser sandbox / isolation, deception technology, endpoint detection response(EDR), data loss prevention (DLP), and the like.[7]

The endpoint serves as a terminal for analyzing and filtering the encrypted network traffic. Endpoints provide a very rich set of secure remote measurements, and the new endpoint security suite includes EDR functionality, so endpoint security can act as a new link for security analysis

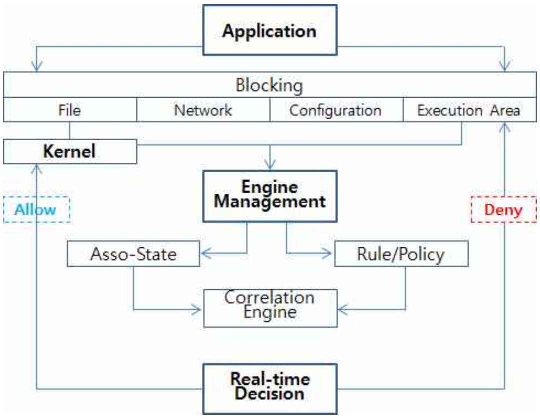
Therefore, the huge amount of data that is produced and delivered in mobile and IoT environments now requires centralized command and control, distributed execution. And then this role will be handled by endpoint security solutions, and endpoints are expected to play a central role in the security world. In this paper, we look over the functions and performance of several commercial products, and study the current status, limitations, and development of endpoint security.

2. Endpoint Security Trends and Limitations

2.1 Endpoint Security Commercial Products

In this section, we will look at the performance and characteristics of some of the latest commercial products.

Cisco Security Agent software is an action-based endpoint security tool that prevents intrusions by blocking threats.



[Fig.1]Cisco security agent INCORE procedure[11]

As in [Fig.1], prior to running the application, the execution structure first intercepts the system request and drives the interrelated system engine to correlate the action with the rule / policy, and then proceeds through the INCORE process to determine whether to "allow" or "deny" the interrelated system requests with a set of rules of behavior.

The endpoint security agent can perform the following detection functions by adding functions;

- Type of application installed on a single / workgroup computer,
- Type of application used on the network,
- All IP addresses that communicate with the server or desktop computer,
- Application state on a remote system, specific user installation information,
- Execution information of unwanted applications, etc

Endpoint Security agents act as part of a self-defending network strategy.

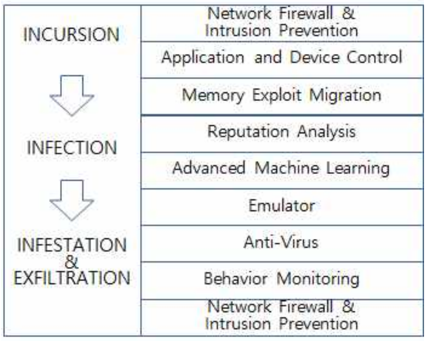
In fact, in addition to the fact that it provides the first real-time intrusion prevention feature, it can also obtain state information that is not available at the network edge by being present on the endpoint.

[Table1] Next-generation Endpoint Protection Technologies[2]

Technologies
Understanding Machine Learning
Preventing Exploits
Monitoring Behavior
Examining Intrusion Prevention and Firewalls
Considering File Reputation
Comprehending Emulation
Eyeing Application and Device Control
Reducing Costs and Complexity with a Single
Agent Architecture
Extending Endpoint Protection to Cloud Workloads

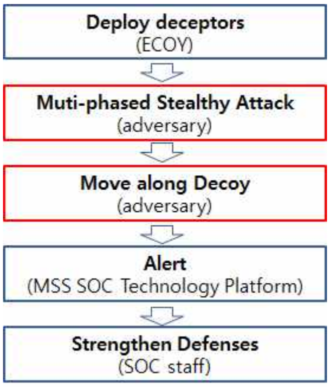
As in [Table1], Symantec emphasizes the need to change endpoint security and presents the following technologies that must be specifically considered for next-generation endpoint protection.[1]

It is characterized by protecting end points regardless of where an attacker attacks in an attack chain as show in [Fig.2].[9]


INCURSION
INFECTION
INFESTATION & EXFILTRATION
Network Firewall & Intrusion Prevention
Application and Device Control
Memory Exploit Migration
Reputation Analysis
Advanced Machine Learning
Emulator
Anti-Virus
Behavior Monitoring
Network Firewall & Intrusion Prevention

[Fig.2] SEP Protection Procedure

It also has a deception feature that targets the post-incursion stages of the attack cycle And so it plants deceptors to expose hidden adversaries and reveal attacker intent and tactics via early visibility, so that the information can be used to enhance security posture as show in [Fig.3].[9]


Deploy deceptors (ECOY)
Muti-phased Stealthy Attack (adversary)
Move along Decoy (adversary)
Alert (MSS SOC Technology Platform)
Strengthen Defenses (SOC staff)

[Fig.3] SEP Deception Work

Further an overview of some typical endpoint security solutions is shown in [Table2] below.

[Table2] List of other major ESS

Vender	Platform	Advantages
Digital Guardian	Threat Aware Data Protection Platform	On premises or service method Customized automation
enSilo	enSilo Platform	Threat detection traps; Lock to Threat
Minerva	Anti-Evasion Platform	Environmentally friendly new malware targets
promisec	Promisec EndpointManager	Support for compliance automation Continuous monitoring
Ahnlab	Ahnlab EDR	Continuous monitoring Visibility-based threat response

The following [Table3] is a list of security products and companies awarded at Gartner's Endpoint Protection Platforms Customer Choice Awards 2017. An Endpoint Protection Platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts.

[Table3] Endpoint Protection Platforms Customer Choice Awards 2017[10]

Awards	Product(s)	Vendor
Platinum	Endpoint Security for Business	Kaspersky
Gold	Symantec Endpoint Protection	Symantec
Silver	PROTECT	Cylance
Bronze	ESET Endpoint Security	ESET
Honorable Mention	Intercept X/Sophos Endpoint Protection	Sophos
	Windows Defender	Microsoft
	Trend Micro OfficeScan	Trend Micro
	Malwarebytes Endpoint Protection	Malware-bytes
	⋮	⋮

As in [Table4], in order to compare the performance of endpoint security solutions, Global C-company, a leader in endpoint security solution(ESS), presents the check items such as detection, prevention, response, architecture, threat information and integration and compares the performance.[10]

[Table4] Check items for ESS

Detection
Number of Integrated Detection Technologies Continuous analysis and retrospective, detection Device track Detection action, Dynamic file analysis File Analysis Distribution Model API support, file orbit
Architecture
Operating System Support Deployment model Offline support Closed loop detection, Integration with other platforms
Prevention
White-list / Black-list SW vulnerability Integrated advanced attack prevention Sandbox-aware malware
Threat Intelligence
Daily unique malware sample Threats blocked / day Number of emails scanned per day Well requests monitored daily URLs processed per day Automation Intelligence Feed Share Threat Intelligence
Response
Malware treatment Determining malware gateway Custom detection Retrieving and importing files Vulnerable application visibility
Integrated
Integrated

2.2 Limitations of Endpoint Security

It is well-known that cloud service users want to receive services through wired / wireless networks using various terminal devices. At this time, there is a threat of information leakage due to the security threats of the terminal and the vulnerability of the public wireless network environment.[5] Also endpoint security technology in IoT environment requires a security protocol for a strong password based key management system, and it needs to protect privacy by protecting large channel data generated by multiple channels.[6]

Agent-based endpoint security solutions are still limited in terms of overall network security. Endpoint DLP not only controls the outflow of personal information through printouts or external storage media, but also controls the use of external Internet networks and the sending of files over an encrypted channel. However, it is structurally impossible to secure the network using an agent-based approach that is an endpoint DLP installation. The reasons are as follows;[12]

- If the agent is not installed on the PC, or if the PC user arbitrarily turns off the agent, it is not secure. In addition, the end point DLP agent has a limitation that it can not simultaneously cover different OS-based devices.
- The risk of zero-day attacks during new malware detection and patching and timely agent updates is still exposed.
- It shows the disadvantage that the logs can not be analyzed collectively because the logs are accumulated on individual PCs.

Therefore, in the recent DLP market, it is centered on enterprise DLP that can control both endpoints and data leaks over the network. Here, 'Enterprise DLP' is a system that can centrally control the leakage of personal information from endpoint to network through complex detection and response technology that can protect important data of organization.[12]

3. Improving endpoint security

In response to the increasingly intelligent and sophisticated trends of security threats, new directions for functions and technologies that endpoint security solutions must have are being researched and developed.

In the background, in conjunction with the issue of the Fourth Industrial Revolution era, the following are analyzed as key elements.

- Applying machine learning and artificial intelligence technology for layered and automated response technology
- SaaS-based solutions for efficient organization and management
- Applying agent function for security management of many IoT devices
- Integration of distributed endpoint software agents

Due to the constantly evolving nature of the IT environment, attackers are attempting to penetrate the network with more sophisticated attack techniques, and endpoints are the last line of defense against such attacks.

As confirmed in the WannaCry and Petya incidents, the Ransomware attacks are becoming more aggravated, raising concerns about cyber damage and downtime. In addition, fileless and covert attacks are becoming more prevalent due to the open source impact of leveraging general purpose IT tools, and so the confidentiality, integrity and availability of endpoint assets are seriously threatened.[9] The lack of complete and regular software patches, blanking of application blocks, and the ongoing occurrence of shadow IT are the causes of endpoint security gaps and vulnerabilities.[8]

As the defense boundaries change over time, there is a need for a layered defense-in-depth strategy to protect networks and data. In conjunction with network security control functions, a hierarchical defense strategy is required for the endpoint itself. Therefore, a reliable solution with the following major security control functions has been required.[3]

- Advanced authentication technologies beyond basic cryptographic techniques
- Strong encryption for sensitive data regardless of the endpoint being stored
- Active preventive malware solution rather than passive

Users will be able to successfully secure new defense boundaries, while satisfying increasing compliance requirements as they do so. A software solution that is installed on commercial PCs solves the problems of the above three areas, thereby providing the most secure commercial PCs. The tight integration between the security software and the hardware on which the software is running is an absolute necessity to ensure that the authentication credentials and the proper maintenance of the encryption key and the integrity of the system are reliable. For the reliability of these solutions, verification of independent third parties such as FIPS or the Common Criteria is also essential.

4. Conclusions

A survey of endpoint protection platforms (EPP) by Gartner in 2014 found that 35 percent of all responding companies were affected by malware.[2]

Most companies that rely on reactive security technologies, such as firewalls and antivirus software, are not protecting their devices from malware. In fact, the target attacker creates and tests a payload before distributing the malicious code in order to disable the anti-virus antivirus system.

Therefore, successful endpoint security requires a preemptive information security system to develope and operate the management tools for endpoint security of various OS-based devices and mobile devices rather than a reactive approach. And the information security lifecycle needs to be improved for 'Policy' to configure a preemptive endpoint, 'Real-time protection' technology to detect and filter malware, 'Detection' to confirm the occurrence of abnormal symptoms or threats, and 'Remeditation' for dealing with and recovering from actual damage.

References

[1] Naveen Palavalli, Advanced Endpoint Security, for Dummies, 2018.

[2] Magic Quadrant for Endpoint Protection Platforms, Gartner, 2018.

[3] “엔드포인트 보안의 한계와 과제” IDG Tech Focus, 2015.

[4] 송근혜, 이승민, “4차 산업혁명과 보안 패러다임 변화”, ETIR주간기술동향보고서, 2018.5.

[5] 양환석, 이병천, 유승재, “클라우드 컴퓨팅 환경을 위한 침입탐지시스템 특징 분석”, 융합보안논문지, 제12권 제3호. pp.59-65, 2012.

[6] 노시춘, 김점구, “디바이스 센싱 단계의 IoT 네트워크 보안 기술 프레임워크 구성” 융합보안논문지, 제15권 제4호 pp. 41~47, 2015

[7] Jon Oltsic, “규모와 범위 모두 성장하고 있는 새로운 엔드포인트 보안시장이 펼쳐진다.”, http://www.itworld.co.kr/

[8] David Geer, “커지는 위협에도 여전히 부족한 엔드포인트 보안” http://www.itworld.co.kr/

[9] https://www.symantec.com/ko/kr/products/endpoint-protection

[10] https://www.cisco.com/c/m/ko_kr/products/security/advanced-malware-protection/competitive-comparison.html

[11] https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series -home.html

[12] http://www.dailysecu.com/?mod=news&act=articleView&idxno=36956

〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교
정보보호학과 교수
email : sjyoo@joongbu.ac.kr