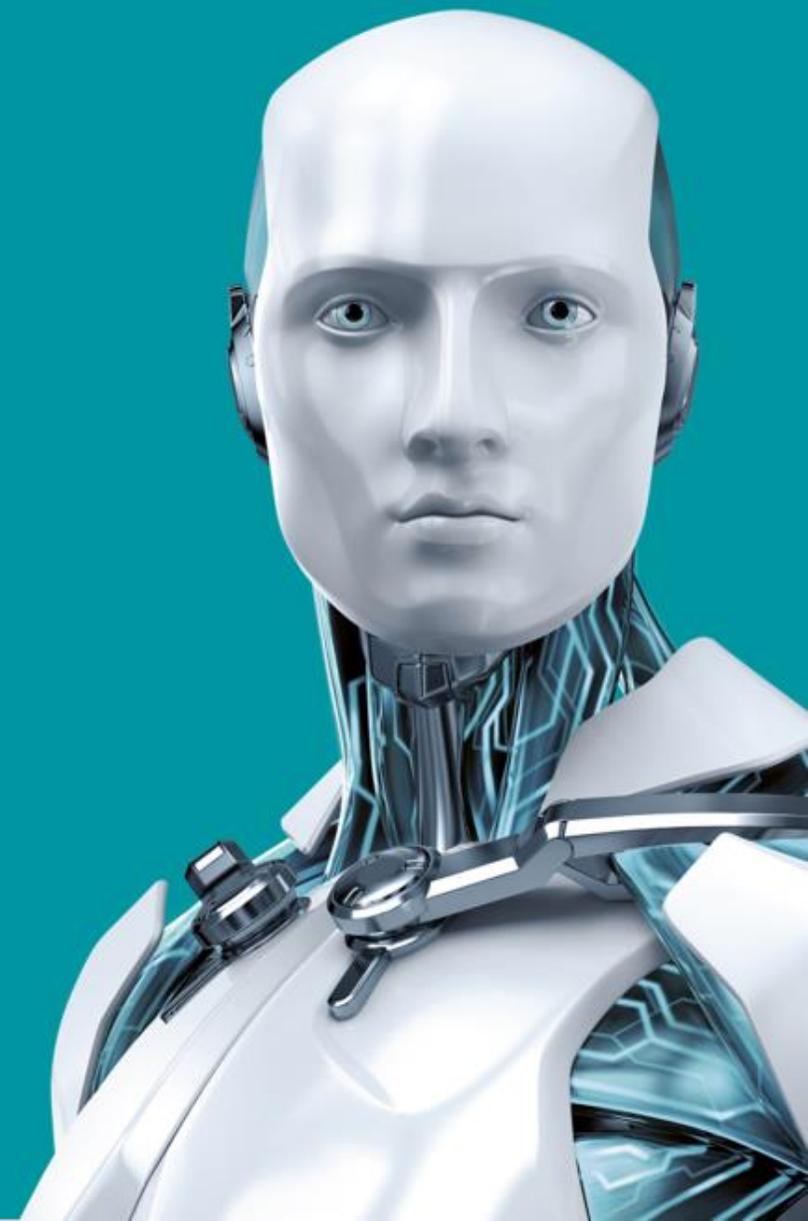


30 30 YEARS OF  
CONTINUOUS  
IT SECURITY  
INNOVATION

# ESET ENDPOINT SOLUTIONS FOR BUSINESS

**eset** ENJOY SAFER TECHNOLOGY™



# Index

01 회사 소개

02 Why ESET?

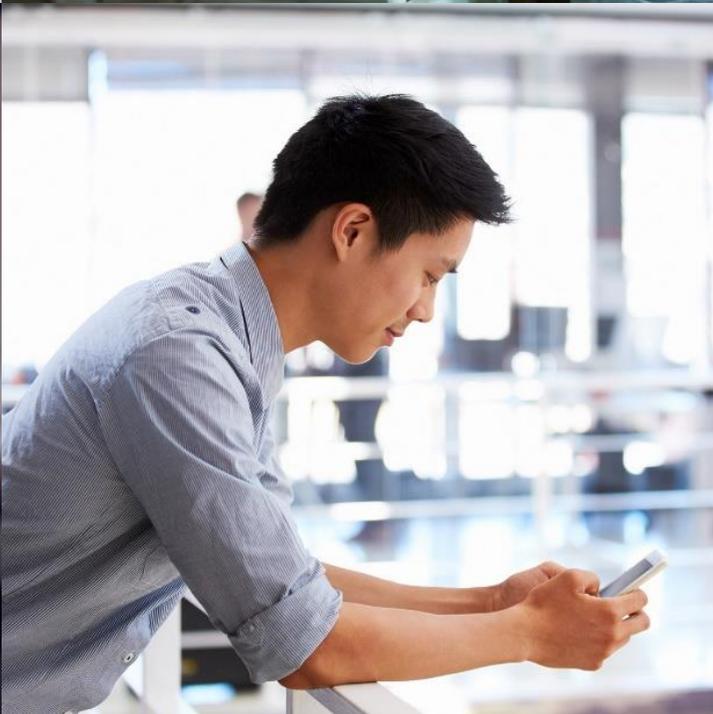
03 ESET Solution 제품 소개

04 기술지원

05 Appendix



ENJOY SAFER  
TECHNOLOGY™



# 회사소개

ESET은 34년 이상의 경험을 바탕으로 다양한 장치, 데이터, 사용자를 보호하기 위한 서비스를 제공하는 글로벌 보안 소프트웨어 기업입니다.

전 세계 1억 이상의 사용자들을 다양한 악성 위협으로부터 보호하고 있으며, VB100, AV-Comparatives와 같은 공신력 있는 인증기관에 최상위 인증을 받은 최고의 제품입니다.

# 회사 소개

- Why ESET?
- 제품 소개
- 기술 지원
- Appendix

<b>본사</b>	슬로바키아 (브라티슬라바)
<b>설립</b>	1987년(설립)
<b>직원</b>	1,500명(R&D인원 : 1,000명)
<b>공급 국가</b>	전세계 202여 개국
<b>매출</b>	9,000억(2020년 기준)
<b>사용자</b>	전세계 1.4억명 이상(2020년 기준)
<b>점유율</b>	전세계 개인, 기업 통합 14% 이상(2020년 기준)



**30** 30 YEARS OF CONTINUOUS IT SECURITY INNOVATION



## WHY ESET?

ESET은 여러 안티바이러스들 중 가장 낮은 리소스 점유율로 최고의 퍼포먼스를 보실 수 있는 유일한 제품입니다.

이러한 기술력은 여러 공신력 있는 인증기관을 통해서 입증되었으며, 이를 바탕으로 Google Chrome Clean Up에 ESET 엔진 탑재, 전세계 유료 백신 점유율 1위 등 안티바이러스 업계의 선두주자로 자리매김 하였습니다.

# 기존 백신 소프트웨어 운영 시 발생한 이슈사항

회사 소개

Why ESET? ◀

제품 소개

기술 지원

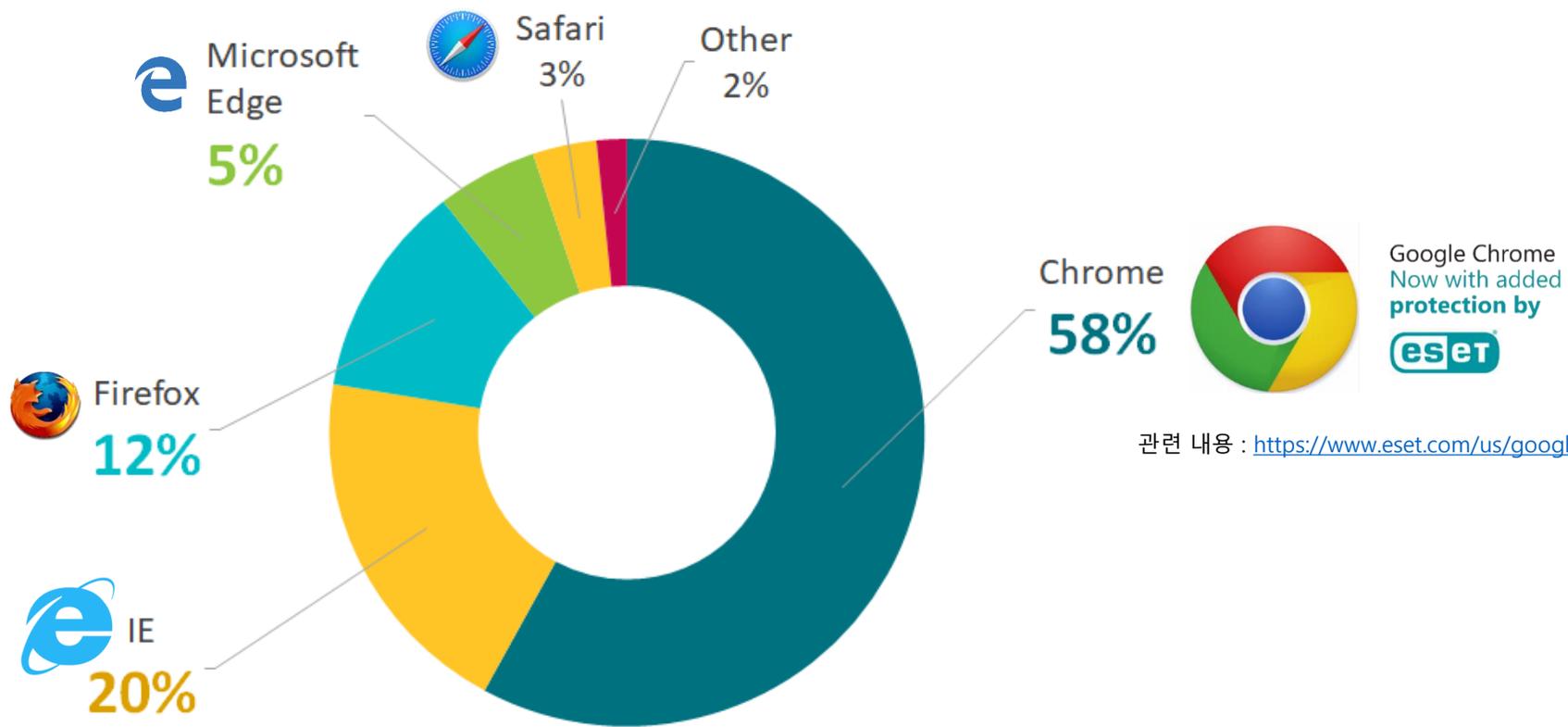
Appendix



# ESET은 Google과 협력하여 유해 애플리케이션 설치를 방지합니다.

ESET 엔진이 구글 크롬 브라우저의 새로운 악성코드 검사 및 삭제 도구인 크롬 클린업에 탑재 되었습니다.

전세계 시가총액 1060조 기업 IT 4위 (참고: 삼성전자 376조)



관련 내용 : <https://www.eset.com/us/google-chrome/>

세계 데스크톱 브라우저 시장 점유율 (2017년 기준)

Source : [http://www.zdnet.co.kr/news/news\\_view.asp?artice\\_id=20170203150802](http://www.zdnet.co.kr/news/news_view.asp?artice_id=20170203150802)

# ESET은 Google Play Store에서 모바일 앱을 능동적으로 보호합니다.

회사 소개

Why ESET?

제품 소개

기술 지원

Appendix

ESET은 Google App Defense Alliance의 창립 멤버가 되어, Google Play Store에 등록되는 모든 App에 대하여 악성코드를 검사합니다.

Google Security Blog  
The latest news and insights from Google on security and safety on the Internet

The App Defense Alliance: Bringing the security industry together to fight bad apps  
November 6, 2019

Posted by Dave Kleidermacher, VP, Android Security & Privacy

Fighting against bad actors in the ecosystem is a top priority for Google, but we know there are others doing great work to find and protect against attacks. Our research partners in the mobile security world have built successful teams and technology, helping us in the fight. Today, we're excited to take this collaboration to the next level, announcing a partnership between Google, **ESET, Lookout, and Zimperium**. It's called the App Defense Alliance and together, we're working to stop bad apps before they reach users' devices.

## App Defense Alliance

The App Defense Alliance is a collaboration between Google, ESET, Lookout, and Zimperium. The App Defense Alliance was created to ensure the safety of the Google Play Store. Together with our partners we aim to quickly find Potentially Harmful Applications (PHAs) and take the appropriate action to protect users.

Partners of the App Defense Alliance can send a request to the Google Play Protect scanner service to have an app analyzed. The GPP scanner service then sends back the scan results directly to the partner. This direct communication also allows GPP to send requests to partner's scanner services and receive results from the partner's scanning engines. This will generate new app risk intelligence as apps are being queued to publish. Partners will analyze that dataset and act as another, vital set of eyes prior to an app going live on the Play Store.

### Our Partners

All of our partners work in the world of endpoint protection, and offer specific products to protect mobile devices and the mobile ecosystem. They use a combination of machine learning and static/dynamic analysis to detect bad apps in the wild. Then, they analyze these apps to understand what makes them harmful to users, and ultimately protect individuals and organizations against those threats.

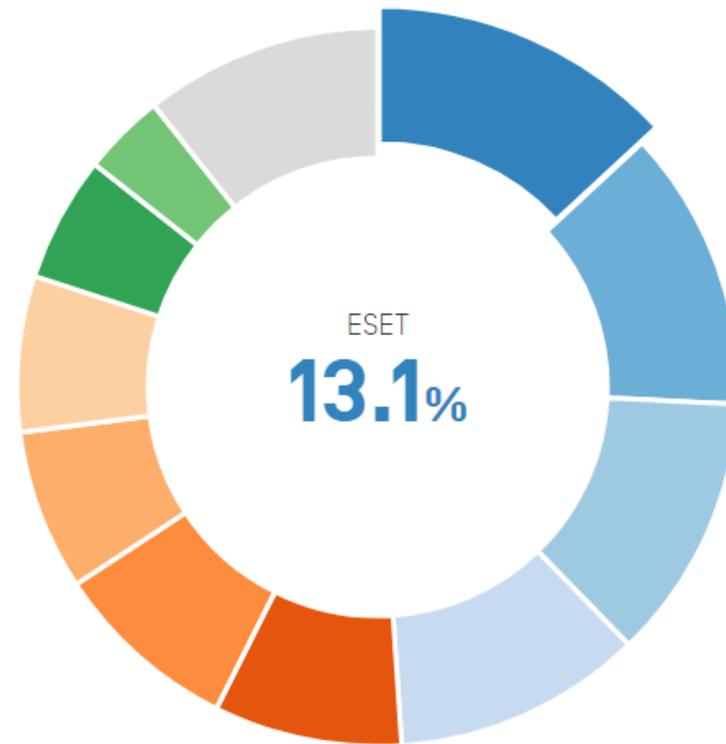
Source : <https://developers.google.com/android/play-protect/app-defense-alliance>

Source : <https://security.googleblog.com/2019/11/the-app-defense-alliance-bringing.html>

## 전세계 백신 점유율 1위

OPSWAT의 간소화된 시장 점유율 보고서는 주요 맬웨어 방지 공급 업체 및 제품의 시장 점유율에 대한 월별 업데이트를 제공합니다.

	<b>ESET</b>	13.1%
	McAfee, Inc.	12.66%
	Symantec Corporation	11.98%
	Bitdefender	11.2%
	Kaspersky Lab	8.44%
	AVAST Software a.s.	8.37%
	Cylance Inc.	7.23%
	Malwarebytes	7.01%
	Webroot Software, Inc.	5.65%
	Sophos Limited	3.7%
	Other	10.66%



백신 점유율 (2019년 9월 기준)

Source : <https://metadefender.opswat.com/reports/anti-malware-market-share?date=2019-09-30&lang=en>

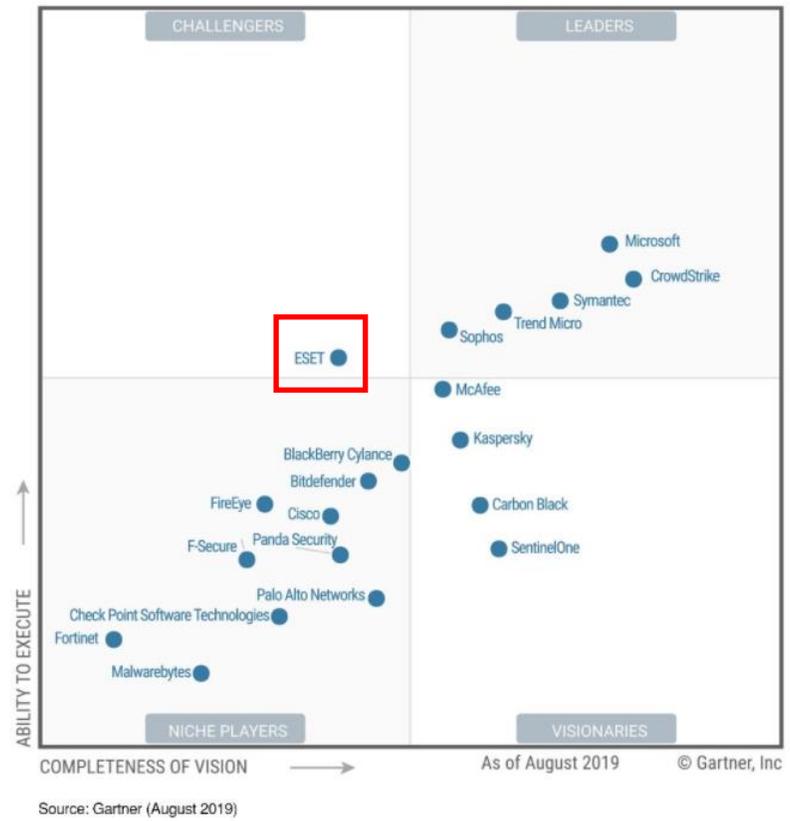
# Gartner Magic Quadrant EPP 부문 유일한 "챌린저" 선정

- 회사 소개
- Why ESET? ◀
- 제품 소개
- 기술 지원
- Appendix

ESET은 2년 연속(2018~2019년) Gartner Magic Quadrant Endpoint Protection Platform 부문에서 유일한 챌린저(Challenger)로 선정되었습니다.



가트너의 매직 쿼드런트는 각 분야별 비전과 실행능력, 기술 완성도 등을 평가해서 작성되는 보고서입니다.  
 이 보고서에 등재되는 것만으로도 글로벌 시장 속에서 해당 솔루션의 기술력을 객관적인 지표로 인정 받은 것입니다.  
**챌린저 (Challenger)**로 선정되었다는 것은 우수한 실행 능력을 보여주는 벤더라는 것을 의미합니다.  
 이는 ESET이 기업의 엔드포인트 보호 기능을 제공하는 것에 지속적으로 발전했다는 신호입니다.



Source: <https://blog.eset.co.kr/7/>, <https://blog.eset.co.kr/93/>

## ESET, ESCO로부터 'Cybersecurity made in Europe' 수상

ESET은 유럽 사이버 보안 기구 ECSCO(European Cyber Security Organization)로부터 'Cybersecurity Made in Europe'라벨을 수상했습니다.



ECSCO의 'Cybersecurity Made in Europe' 레이블을 획득하려면 기업은 다음을 입증해야 합니다.

- 본사는 유럽에 위치해야 합니다.
- 직원의 대부분은 유럽에서 근무하고 있어야 합니다.
- ENISA(유럽 네트워크 정보 보호원/European Union Agency for Cybersecurity)에서 지정한 10가지 기본 보안 요구사항을 준수해야 합니다. 이는 정보 통신 기술에서 제품 및 서비스가 안전한 것으로 간주되기 위한 필수 사항입니다.



## 세계 1위 – VB100 최다 인증 123회. 업계 최초 “100 VB100 어워드” 수상

영국의 바이러스 연구 기관인 Virus Bulletin(www.virusbtn.com)에서 수여하는 VB100 인증은 전 세계에서 수집된 최신의 악성코드 샘플(Wild List)을 대상으로 오진 없이 100% 진단이 가능해야만 주어지는 인증입니다.

**ESET은 안티바이러스 제품 중 세계 최초로 100회 수상을 받아 검증된 세계 최고의 제품입니다.**  
[\(ESET 안티바이러스 세계최초 VB100인증 100회 수상 영상\)](#)

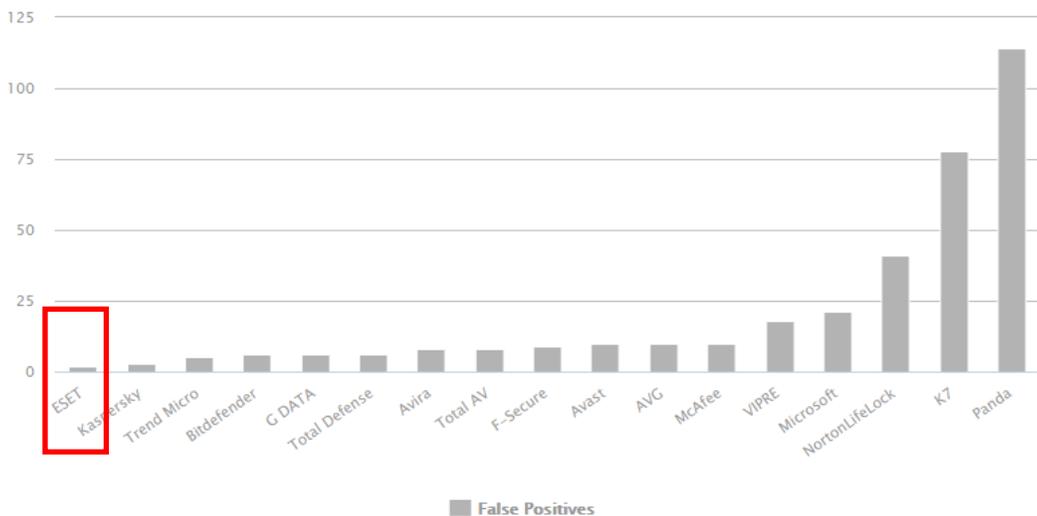
※ 2개월 마다(매년 총 6회) 엄격하게 테스트하는 비영리 기관으로 높은 공신력을 자랑합니다.

ESET은 타 백신 대비하여 높은 통과율을 보이고 있습니다.

구분	제조사	전체 테스트 횟수 (1998년 1월 ~ 2020년 12월)	통과 횟수	통과율(%)
해외	ESET	 134 	123	92%
	K사		105	78%
	S사		57	43%
국내	A사		40	31%
	E사		41	31%
	H사		7	5%

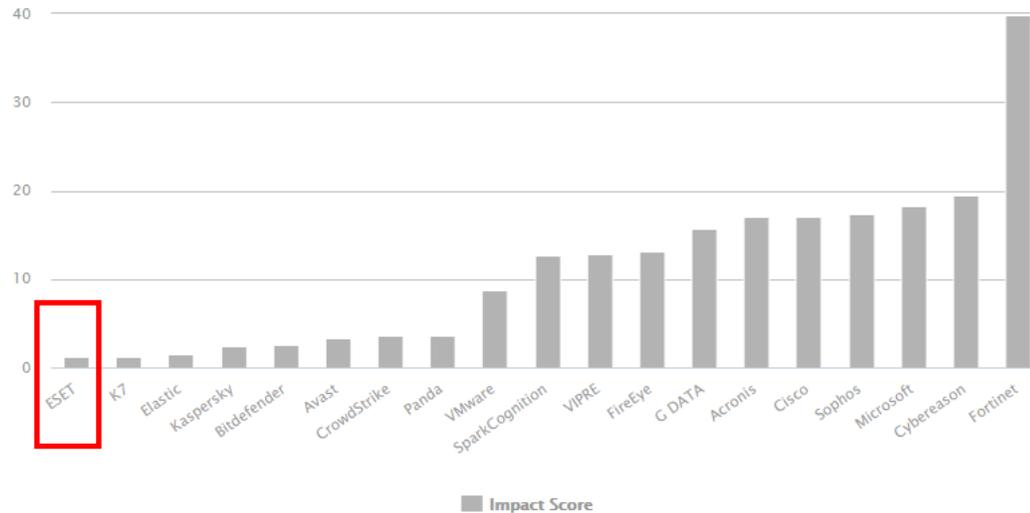
2020년 12월 기준 Source : [www.virusbtn.com](http://www.virusbtn.com)

오스트리아의 보안 소프트웨어 연구 기관인 AV-comparatives ([www.av-comparatives.org](http://www.av-comparatives.org))에서 시행하는 테스트로, 오진률 및 시스템 점유율(퍼포먼스) 부분에서 ESET이 1위를 기록하고 있습니다.



오진을 포함한 오작동 여부를 검사하는 것으로 낮을수록 성능이 우수하다고 볼 수 있습니다.

[2020년 10월 기준]



백신 설치 후 시스템에 미치는 영향을 측정한 수치이며, 경쟁사 대비 탁월한 동작 성능을 보여주고 있습니다.

[2020년 11월 기준]

Source : <http://www.av-comparatives.org>

# 리눅스 백신 GS 인증 획득 및 조달 등록되었습니다.

ESET File Security for Linux 제품이 GS인증 1등급을 획득하고 리눅스 서버 방역 제품으로는 최초로 조달 등록이 되었습니다.

- 회사 소개
- Why ESET?**
- 제품 소개
- 기술 지원
- Appendix



**나라장터**  
국가종합전자조달



세부품명 : 보안소프트웨어 (4323320501)  
 회사명 : 주식회사 유엔정보 [중소기업]  
 식별번호 : 23295408 3자단가계약  
 규격 : 보안소프트웨어, 이에스티씨, 이셋 리눅스 파일 시큐리티 V4.5, 라이선스  
 [원산지 : 대한민국]  
 [계약종료일 : 2022/02/06] [납품기한 : 30일(납품요구일로부터)]  
[납품장소도] [전지역]  
 우선구매대상 : 해당 없음  
 의무구매대상 : 해당 없음

440,000 원

조

# ESET은 글로벌 R&D 센터를 운영하고 있습니다. (대륙별 악성코드 대응센터 운영)

보안 위협의 99%가 해외로부터 유입되는 것이 현실입니다. 이제, 글로벌 방역 시스템 확보는 선택이 아닌 필수입니다.

- 회사 소개
- Why ESET? ◀
- 제품 소개
- 기술 지원
- Appendix





# 제품 소개

ESET은 전세계 1억명 이상의 사용자들이 선택한 제품으로 그 성능과 안정성을 인정받은 안티바이러스입니다.

Windows, Mac, Linux, Android까지 다양한 제품군을 바탕으로 안전한 업무 환경을 제공해드립니다.

# ESET Protect (EP)

ESET Protect(EP)는 중앙에서 사내에 위치한 다양한 클라이언트 워크스테이션 및 서버를 비롯한 네트워크 환경의 ESET 제품을 관리 할 수 있는 중앙관리 솔루션 입니다. 통합적인 관리를 통해 사내에 발생하는 다양한 보안 위협에 대해 신속 하게 대응 할 수 있습니다.

- 회사 소개
- Why ESET?
- 제품 소개**
- 기술 지원
- Appendix

The screenshot displays the ESET PROTECT dashboard with the following data:

- Dashboard Overview:**
  - 총 장치 수 (Total Devices): 26 (Confirmed: 24)
  - 주의 요망 (Attention Required): 0
  - 보안 위협 (Security Threats): 2
- 장치 상태 (Device Status):**
  - 데스크톱 (Desktop): 21 (Confirmed: 21, Attention: 0, Threats: 2)
  - 합계 (Total): 23
- 연결 상태 (Connection Status):**
  - 26 devices connected (1 day)
- 제품 버전 상태 (Product Version Status):**
  - 에이전트 (Agents): 100% latest version
  - Endpoint: 100% latest version
  - 서버 (Servers): 50% latest version, 50% outdated version
  - 모바일 (Mobile): 0%
- 관리 상태 (Management Status):**
  - 25 관리 및 보호되는 장치 수 (Managed & Protected Devices)
  - 26 관리됨 (Managed)
  - 0 등록 취소됨 (Unregistered)
  - 60 Rogue
- RSS 피드 (RSS Feed):**
  - ESET Support News**
  - ESET Full Disk Encryption for macOS version 1.2.0.8 have been released**
  - THU DEC 10 2020 02:00:00 GMT+0900 (대한민국 표준시)
  - <https://support.eset.com/news7762>
  - On December 8, 2020 ESET Full Disk Encryption (EFDE) for macOS version 1.2.0.8 has been released and is

## ESET Protect (EP)

ESET Protect를 통해 중앙 집중 관리, S/W 및 H/W 현황 관리, 로그 및 리포트 생성이 가능합니다.

주요 기능	기능 소개
중앙 집중식 관리	ESET의 모든 제품을 하나의 관리서버로 통합적인 관리가 가능합니다. Windows, Linux, Mac, Android 등의 모든 제품을 하나로 관리 가능합니다.
웹 브라우저 콘솔	사내 어디서든 웹 브라우저가 있는 PC에서 사내 보안 이슈 파악 및 관리할 수 있는 웹 기반의 콘솔을 지원합니다.
S/W, H/W 현황 관리	PC에 설치되어 있는 소프트웨어(어플리케이션), 하드웨어(CPU, 메모리 등) 현황을 보여줍니다. 소프트웨어 현황에서 원격으로 제거할 수 있는 어플리케이션을 보여주고 삭제가 가능하며, 소프트웨어의 라이선스를 할당하여 라이선스 관리를 할 수 있습니다.
로그 및 리포트	사내 네트워크에서 발생하는 다양한 보안 이슈 및 세부 내역들을 확인할 수 있도록 이벤트 로그 및 리포트를 실시간으로 제공합니다.
동적 그룹화	운영체제, IP, 대역, 호스트 네임 등의 다양한 조건을 기반으로 동적 그룹 설정이 가능합니다. 동적 그룹 설정을 통해 관리자는 클라이언트 현황에 대한 빠른 파악 및 관리가 가능합니다.
권한 기반 관리	ESET Protect(이하 EP)는 자체적으로 계정을 생성 및 관리합니다. 다수의 관리자가 보안을 관리하는 경우 각각의 역할에 맞도록 권한을 지정하여 효율적인 관리가 가능합니다.
원격 배포 기능	EP에 연결된 클라이언트는 원격으로 ESET 제품을 자유롭게 원격 배포하여 설치가 가능합니다. ESET 제품이 아닌 다른 설치 패키지도 원격 배포가 가능합니다. (MSI 파일일 경우)
기능 제어	특정 클라이언트에 대한 기능을 임시적으로 비 활성화가 필요한 경우 ERA를 통해 클릭 한번으로 제어가 가능합니다. 원하는 시간을 설정해 지정한 시간 동안만 비 활성화 되도록 설정이 가능합니다.
다양한 운영체제 지원	Windows 플랫폼의 운영체제 외에도 리눅스, 가상화 환경의 플랫폼을 지원하여 다양한 환경에서의 구축을 지원합니다.

# ESET Protect (EP)

ESET Protect(EP)를 통해 S/W 현황 파악이 가능합니다.

- 회사 소개
- Why ESET?
- 제품 소개**
- 기술 지원
- Appendix

The screenshot shows the ESET Protect console interface. The left sidebar contains navigation options: 대시보드, 컴퓨터, 위협, 보고서, 작업, 설치 관리자, 정책, 알림, 상태 개요, and 자세히. The main area displays a list of installed applications with columns for Name, Supplier, Version, Size (MB), Agent removal support, Latest version, and Update status. The '설치된 애플리케이션' (Installed Applications) menu item is selected in the left sidebar.

이름	공급업체	버전	크기[MB]	에이전트가 제거를 지원	최신 애플리	버전 검사 상태
Bandizip	Bandisoft.com	7.20		아니오		
Beyond Compare 4.4.0	Scooter Softwar...	4.4.0.25886	48	아니오		
BlueStacks 5	BlueStack Syste...	5.3.110.1002	2047	아니오		
Chrome	Google LLC	94.0.4606.81		아니오		
Dropbox	Dropbox, Inc.	134.3.4102		아니오		
EditPlus (64 bit)	ES-Computing			아니오		
ESET Endpoint Security	ESET, spol. s r.o.	8.1.2037.2	212	예	8.1.2037.2	최신 버전
ESET Management Agent	ESET, spol. s r.o.	8.1.1223.0	166	예	8.1.1223.0	최신 버전
FileZilla Client 3.56.0	Tim Kosse	3.56.0	40	아니오		
Honeycam	Bandisoft.com	3.45		아니오		
Intel(R) Chipset Device Software	Intel(R) Corpora...	10.1.18634.82...	2	아니오		
Intel(R) Management Engine Componen...	Intel Corporatio...	2101.15.0.208...	105	아니오		
Internet Download Manager	Tonec Inc.	6.39.2		아니오		
LAV Filters 0.75.1	Hendrik Leppke...	0.75.1	44	아니오		
Microsoft Edge	Microsoft Corp...	94.0.992.47		아니오		
Microsoft Edge Update		1.3.153.47		아니오		
Microsoft Edge WebView2 런타임	Microsoft Corp...	94.0.992.47		아니오		
Microsoft OneDrive	Microsoft Corp...	21.180.0905.0...	165	아니오		
Microsoft Visual C++ 2013 Redistributa...	Microsoft Corp...	12.0.21005.1	17	아니오		

# ESET Protect (EP)

ESET Protect(EP)를 통해 동적그룹을 생성하여 사용하는 S/W를 관리할 수 있습니다.  
설치된 소프트웨어를 쉽게 파악할 수 있습니다.

- 회사 소개
- Why ESET?
- 제품 소개**
- 기술 지원
- Appendix

그룹	컴퓨터 이름	발견된 문제점	IP 주소	원격 호스트
모두 (23)	컴퓨터 이름	ESET Dynamic Threat Defens...		
01. Tech (7)		제품이 활성화되지 않음		
02. Sales (5)		장치를 다시 시작해야 함		
03. Marketing (3)		Enterprise Inspector 서버에 ...		
04. Planning (2)		Enterprise Inspector 서버에 ...		
05. Business Support (2)		장치를 다시 시작해야 함		
06. Server (3)		Enterprise Inspector 서버에 ...		
발견된 컴퓨터 (1)		Enterprise Inspector 서버에 ...		
새 정적 그룹 (0)				
Windows 컴퓨터				
Windows(데스크탑)		Enterprise Inspector 서버에 ...		
관리 가능한 암호화 제품이 없음		장치를 다시 시작해야 함		
Windows(서버)		장치를 다시 시작해야 함		
관리 가능한 보안 제품이 없음		장치를 다시 시작해야 함		
비즈니스용 Microsoft 365		Enterprise Inspector 서버에 ...		
192.168.20.x				
카카오톡				
Linux 컴퓨터				
Mac 컴퓨터				

카카오톡 Kakao Corp. 3.3.3.2911

# ESET Protect (EP)

ESET Protect(EP)를 통해 동적그룹을 생성하여 사용하는 H/W를 관리할 수 있습니다.  
사용하고 있는 H/W를 쉽게 파악할 수 있습니다.

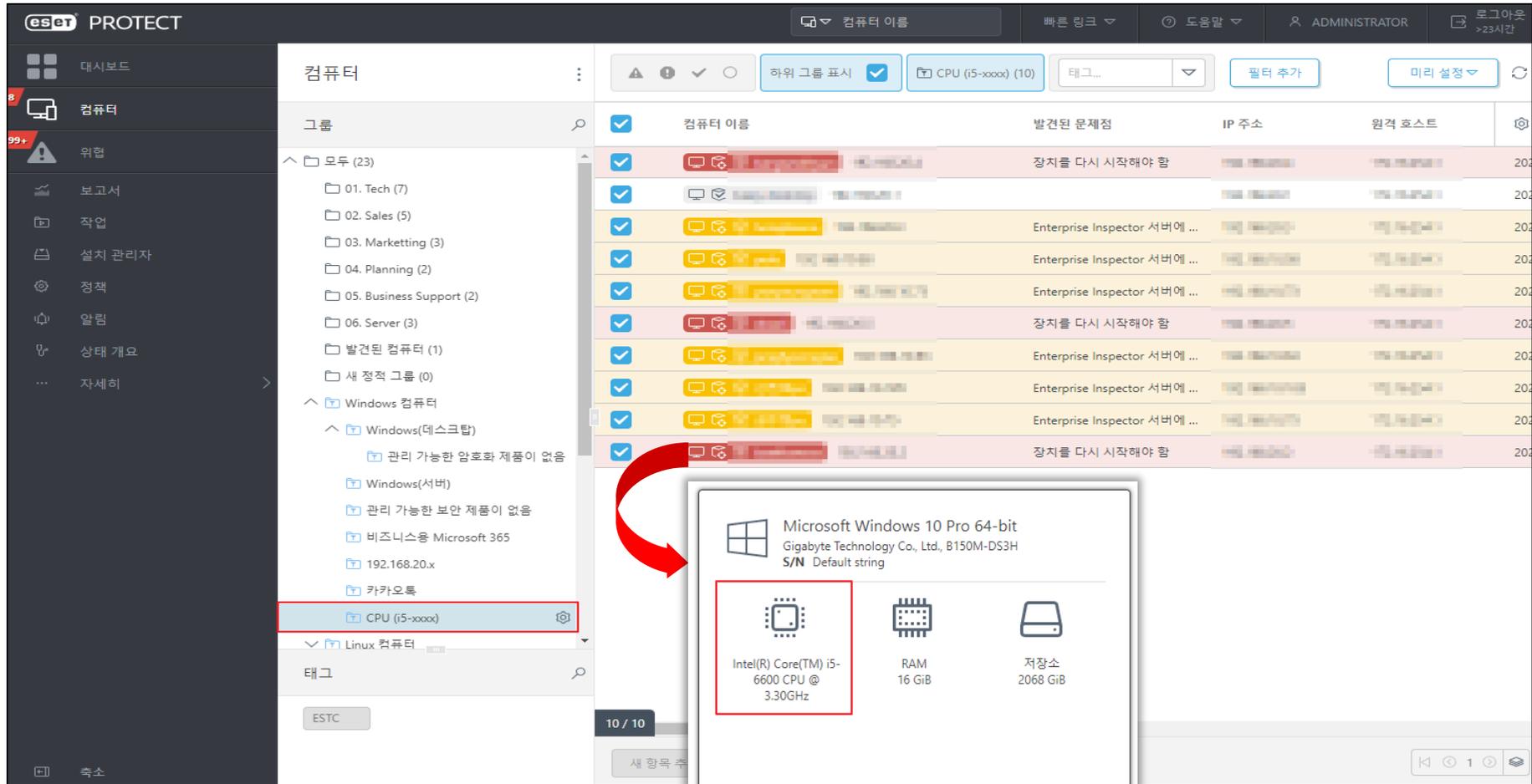
## 제품 소개

회사 소개

Why ESET?

기술 지원

Appendix



# ESET Protect (EP)

ESET Protect(EP)는 IP대역별로 동적그룹 생성이 가능합니다.

- 회사 소개
- Why ESET?
- 제품 소개**
- 기술 지원
- Appendix

The screenshot shows the ESET Protect management console. On the left, a navigation pane shows a tree view of computer groups. The group '192.168.20.x' is selected and highlighted with a red box. The main area displays a table of computers within this group. The table has columns for '컴퓨터 이름' (Computer Name), '발견된 문제점' (Detected Issues), 'IP 주소' (IP Address), and '원격 호스트' (Remote Host). The IP address column is also highlighted with a red box. The table lists several computers with their respective IP addresses and detected issues.

컴퓨터 이름	발견된 문제점	IP 주소	원격 호스트
컴퓨터 이름	ESET Dynamic Threat Defens...	192.168.20.80	원격 호스트
컴퓨터 이름		192.168.20.212	원격 호스트
컴퓨터 이름	제품이 활성화되지 않음	192.168.20.6	원격 호스트
컴퓨터 이름	장치를 다시 시작해야 함	192.168.20.2	원격 호스트
컴퓨터 이름	장치를 다시 시작해야 함	192.168.20.4	원격 호스트
컴퓨터 이름		192.168.20.1	원격 호스트
컴퓨터 이름	Enterprise Inspector 서버에 ...	192.168.20.3	원격 호스트
컴퓨터 이름	장치를 다시 시작해야 함	192.168.20.5	원격 호스트

## ESET ENDPOINT ANTIVIRUS

ESET ENDPOINT ANTIVIRUS 는 30년간 안티바이러스 산업의 기술혁신을 기반으로 기업 내 네트워크를 보호하는 강력한 안티바이러스 솔루션입니다. 엔드포인트 보호 기능을 통해 갈수록 증가하는 악성 개체로 부터 기업 내 사용자 및 데이터를 보호합니다.

주요 기능	기능 소개
컴퓨터보호	안티스텔스 기술을 사용한 안티바이러스, 안티스파이웨어를 통해 바이러스, 루트킷, 스파이웨어 등의 악성 코드에 대한 위협으로 사내 네트워크를 보호하고 ThreatSense 엔진을 사용하여 알려지지 않은 신종 악성 코드에 대해 강화된 보안을 제공합니다.
호스트 기반 침입 방지 시스템(HIPS)	클라이언트에 악의적인 영향을 끼치는 악성 코드에 대한 감시를 통해 실행 중인 프로세스, 파일 및 레지스트리 값을 수정하려 하는 동작을 차단하며 악성 위협을 감지 및 처리합니다.
접근 제어 (장치제어)	사내 네트워크 보호 및 데이터 유출을 방지하기 위해 웹 사이트 필터링 및 외부 장치에(디스크 저장소, USB프린터, FireWire 저장소, Bluetooth 장치, 카드리더, 이미징 장치, 모뎀, LPT/COM포트, 휴대용 장치) 대한 제어가 가능합니다. 읽기/쓰기, 차단, 읽기허용, 경고의 동작을 설정할 수 있습니다. Windows PC/Server, MAC, Linux Desktop OS에서 해당 기능을 지원합니다.
랜섬웨어 보호 차세대 클라우드	랜섬웨어 보호 기능과 LiveGrid® 평판시스템을 통해 랜섬웨어를 예방합니다. ESET Live Grid는 평판을 기반으로 신규 위협에 대해 클라이언트를 보호하는 차세대 클라우드 시스템입니다. 전 세계 ESET 사용자들의 평판을 통해 알려지지 않은 신규 위협으로 부터 빠른 대응이 가능합니다.
웹 및 이메일보호	네트워크 트래픽을 감지하여 웹 사이트 접속 및 이메일의 위협을 판단하여 클라이언트를 보호합니다. 필터링 기능을 사용하여 원하는 IP 및 URL에 대해 제외 처리도 가능합니다.
시스템 속도저하 방지	ESET만의 시스템 최적화 기술력을 통해 최소한의 리소스만을 사용하여 사용자 업무에 영향을 끼치지 않도록 시스템을 보호합니다.
ESET SYSINSPECTOR	ESET SYSINSPECTOR는 프로세스, 서비스, 애플리케이션, 레지스트리 등의 시스템 구성 요소에 대한 자세한 정보를 파악할 수 있는 툴을 제공하여 별도의 시스템 툴 없이 현재 시스템 현황을 파악 및 분석하는데 사용할 수 있습니다.

# ESET ENDPOINT ANTIVIRUS

회사 소개

Why ESET?

제품 소개

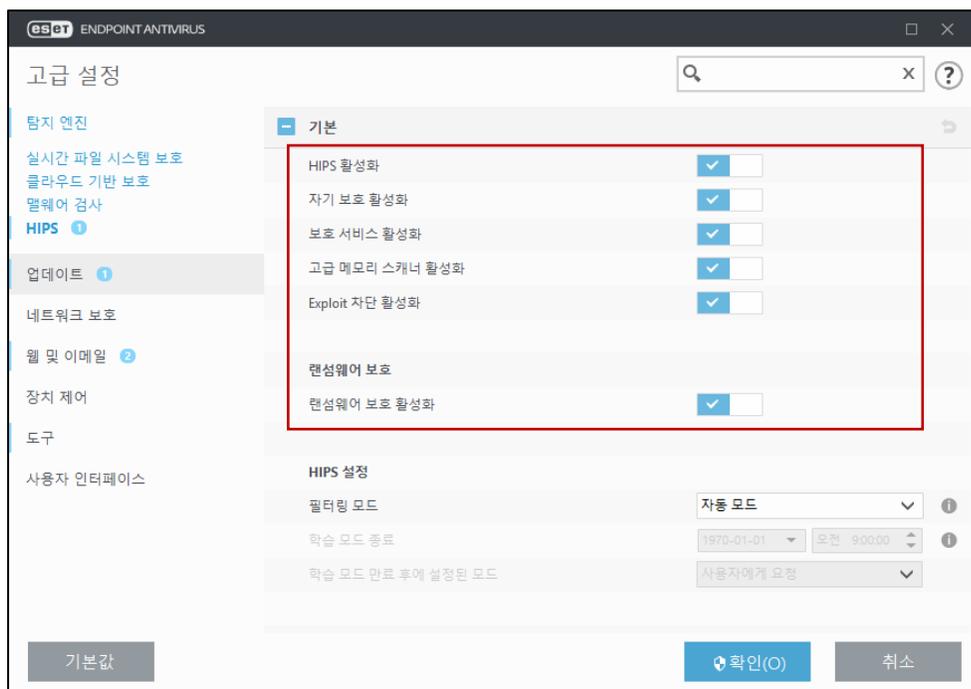
기술 지원

Appendix

ESET ENDPOINT SOLUTION으로 랜섬웨어를 예방할 수 있습니다.

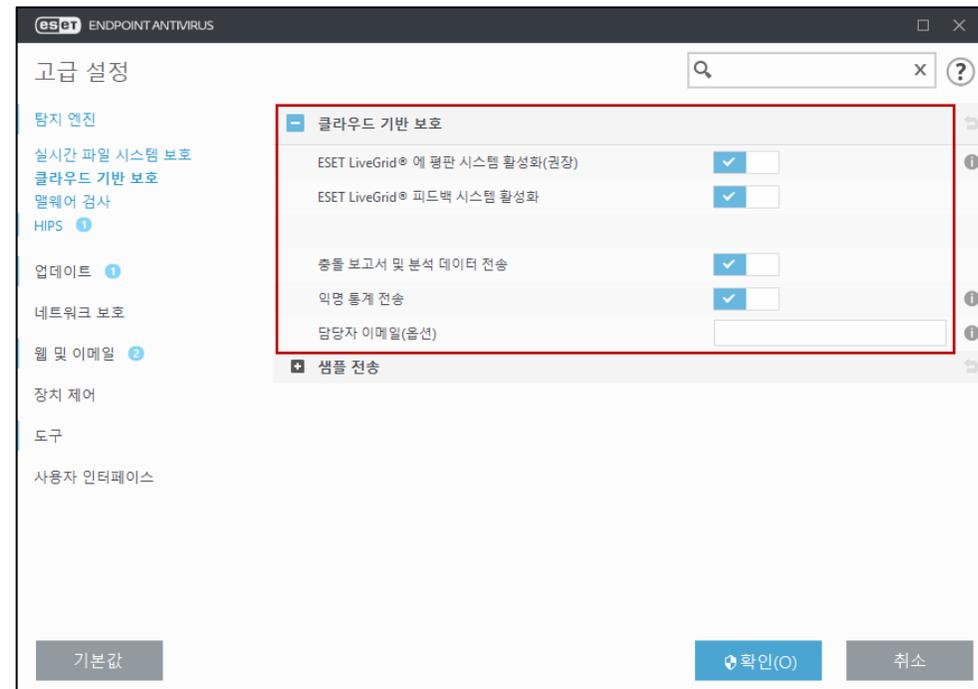
## HIPS, 고급 메모리 스캐너, Exploit 차단, 랜섬웨어 보호

ESET Endpoint Solution은 컴퓨터에 부정적인 영향을 주려고 시도하는 맬웨어 또는 원치 않는 활동으로부터 시스템을 보호합니다. HIPS는 네트워크 필터링의 검출 기능과 고급 동작 분석 기능을 함께 사용하여 실행 중인 프로세스, 파일 및 레지스트리 키를 보호합니다. 랜섬웨어 보호 기능과 LiveGrid® 평판시스템을 통해 랜섬웨어를 예방합니다.



## ESET LiveGrid® 평판 시스템 활성화

ESET Endpoint Solution은 여러 클라우드 기반 기술로 구성된 고급 조기 경보 시스템으로, 최근 발생한 위협을 감지하고 허용 목록을 통해 검사 성능을 향상시킵니다. 새 위협 정보는 클라우드로 실시간으로 스트리밍되기 때문에 ESET 맬웨어 연구소에서 적절한 조치와 일관된 보호를 항상 제공할 수 있습니다.



# ESET ENDPOINT ANTIVIRUS

회사 소개

Why ESET?

제품 소개

기술 지원

Appendix

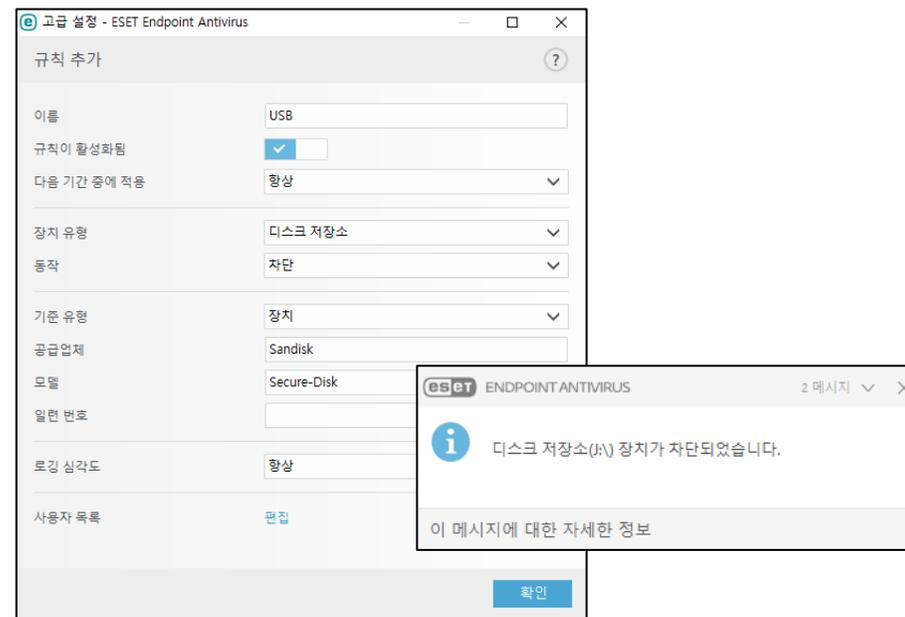
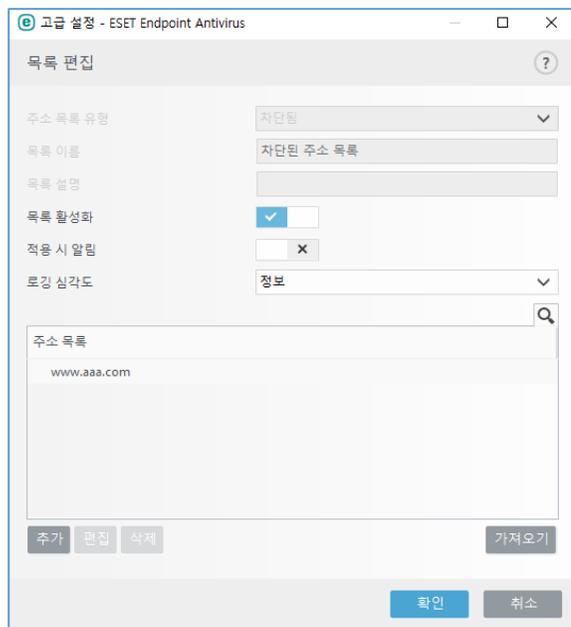
ESET ENDPOINT SOLUTION으로 랜섬웨어를 예방할 수 있습니다.

## 매체제어 (장치제어)

외부로 장치로부터 악성 개체 인입 및 데이터 유출을 차단하기 위해 장치 제어 기능을 제공합니다. 이동식 드라이브, Bluetooth, CD/DVD 등의 다양한 장치를 제어할 수 있습니다. 제어 설정 시 읽기/쓰기, 차단, 읽기허용, 경고의 동작을 적용하여 환경에 적합하게 제어가 가능합니다. 또한 특정 USB(공급업체, 모델, 일련번호)만 허용이 가능합니다.

Windows PC/Server, MAC, Linux Desktop 모두 지원합니다.

직원들의 업무 집중을 위해 접근을 차단해야 되는 웹 사이트가 있는 경우 URL, IP 형식으로 등록하여 웹 사이트 접근 제어가 가능합니다.



## 웹사이트 차단

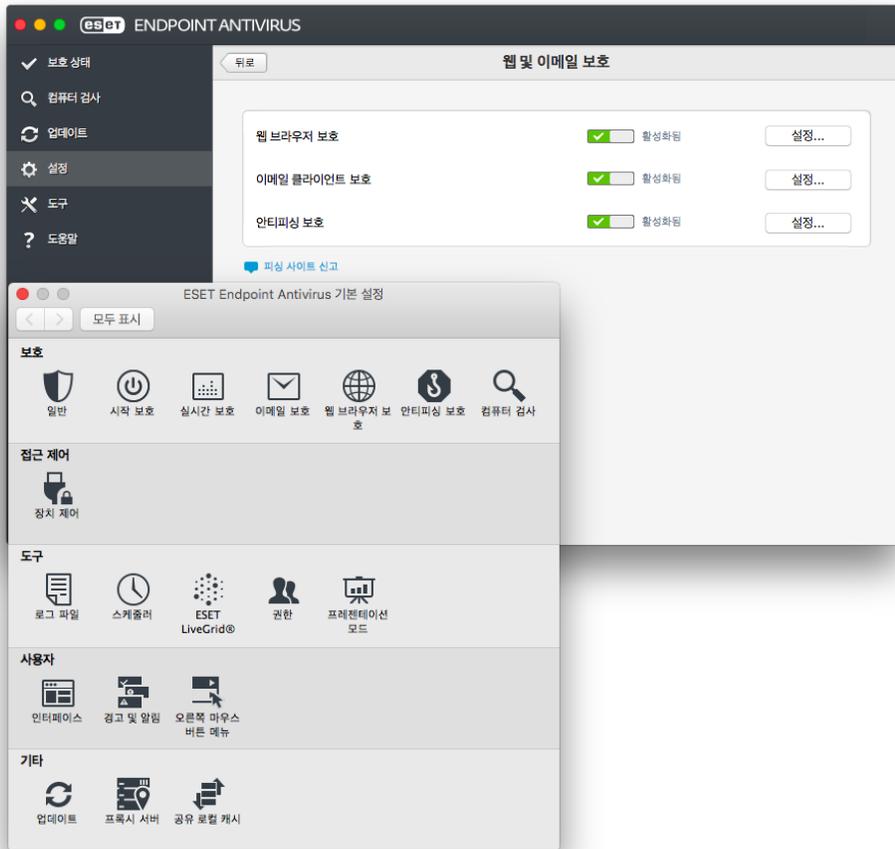
특정 URL에 대하여 차단 및 허용을 설정합니다.  
클라이언트에서 브라우저를 통해 설정된 URL 접속 시 차단합니다.

## ESET ENDPOINT ANTIVIRUS for OS X (MAC)

주요 기능	기능 소개
컴퓨터보호	안티스텔스 기술을 사용한 안티바이러스, 안티스파이웨어를 통해 바이러스, 루트킷, 스파이웨어 등의 악성 코드에 대한 위협으로 사내 네트워크를 보호하고 ThreatSense 엔진을 사용하여 알려지지 않은 신종 악성 코드에 대해 강화된 보안을 제공합니다.
접근 제어 (장치제어)	사내 네트워크 보호 및 데이터 유출을 방지하기 위해 웹 사이트 필터링 및 외부 장치에(디스크 저장소, USB프린터, FireWire 저장소, Bluetooth 장치, 카드리더, 이미징 장치, 모뎀, LPT/COM포트, 휴대용 장치) 대한 제어가 가능합니다. 읽기/쓰기, 차단, 읽기허용, 경고의 동작을 설정할 수 있습니다. Windows PC/Server, MAC, Linux Desktop OS에서 해당 기능을 지원합니다.
랜섬웨어 보호 차세대 클라우드	랜섬웨어 보호 기능과 LiveGrid® 평판시스템을 통해 랜섬웨어를 예방합니다. ESET Live Grid는 평판을 기반으로 신규 위협에 대해 클라이언트를 보호하는 차세대 클라우드 시스템입니다. 전 세계 ESET 사용자들의 평판을 통해 알려지지 않은 신규 위협으로 부터 빠른 대응이 가능합니다.
웹 및 이메일보호	네트워크 트래픽을 감지하여 웹 사이트 접속 및 이메일의 위협을 판단하여 클라이언트를 보호합니다. 필터링 기능을 사용하여 원하는 IP 및 URL에 대해 제외 처리도 가능합니다.
시스템 속도저하 방지	ESET만의 시스템 최적화 기술력을 통해 최소한의 리소스만을 사용하여 사용자 업무에 영향을 끼치지 않도록 시스템을 보호합니다.

## ESET ENDPOINT ANTIVIRUS for OS X (MAC)

많은 사람들이 애플의 맥은 악성코드로부터 안전하다고 생각하지만 맥 악성코드는 악성코드 초기부터 존재했으며 지금도 꾸준히 발견되고 있습니다. ESET Endpoint Antivirus를 통해 안전하게 보호하시기 바랍니다.



- 실시간 파일 시스템 보호
- 이메일 감시(POP3, IMAP 프로토콜)
- 웹 브라우저 감시
- 안티피싱 기능 및 신고
- 컴퓨터 검사 (전체검사, 빠른검사)

- 장치 제어 (이동식 미디어 차단 설정)

- 로그 관리
- 스케줄러 관리 (컴퓨터 검사, 업데이트)
- Live Grid 조기 경고 시스템 (클라우드 기반 평판 정보)
- ESET 실행 권한 관리
- 프레젠테이션 시 알림 설정

- 인터페이스 관리
- 경고 및 알림 관리
- 마우스 버튼 메뉴 관리

- 업데이트 관리
- 공유 로컬 캐시를 통한 검사 속도 향상 (가상화 환경)

# ESET ENDPOINT ANTIVIRUS for OS X (MAC)

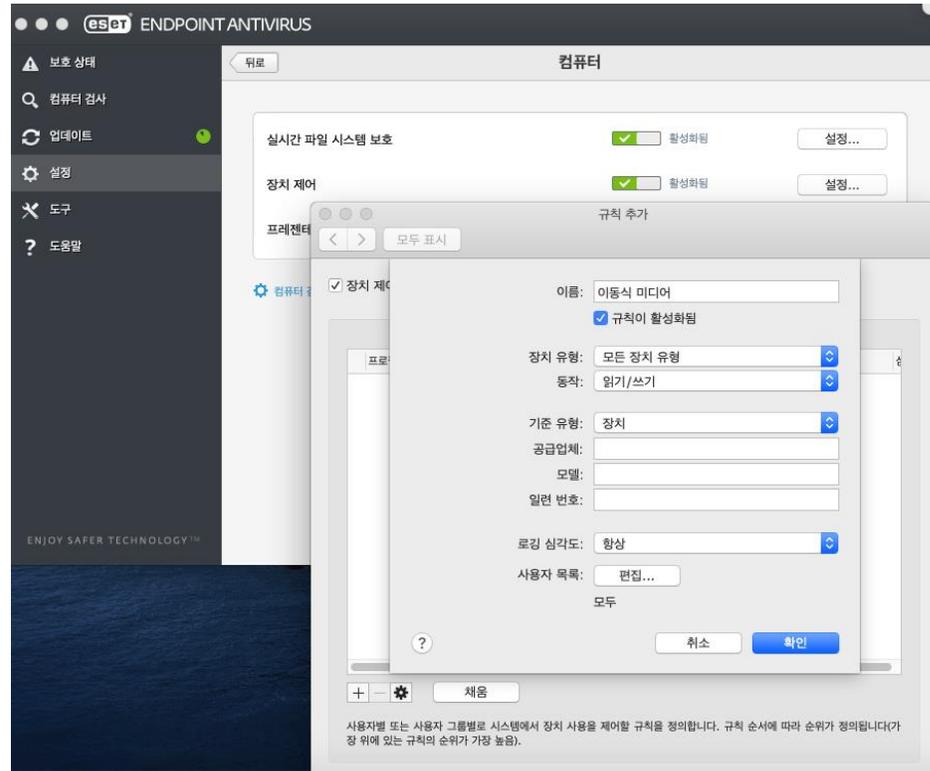
회사 소개

Why ESET?

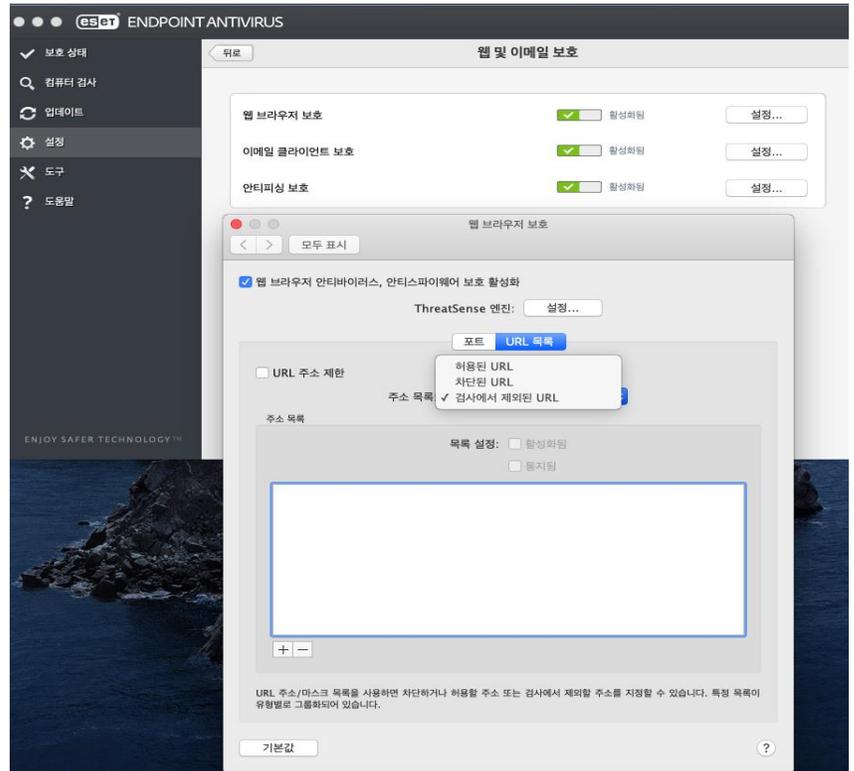
제품 소개

기술 지원

Appendix



**장치 제어 (이동식 미디어 차단 설정)**  
- 차단/허용 할 미디어 장치 설정



**웹 브라우저 보호**  
- 특정 URL 허용/차단 설정  
- 검사에서 제외 URL 설정

# ESET ENDPOINT ANTIVIRUS for OS X (MAC)

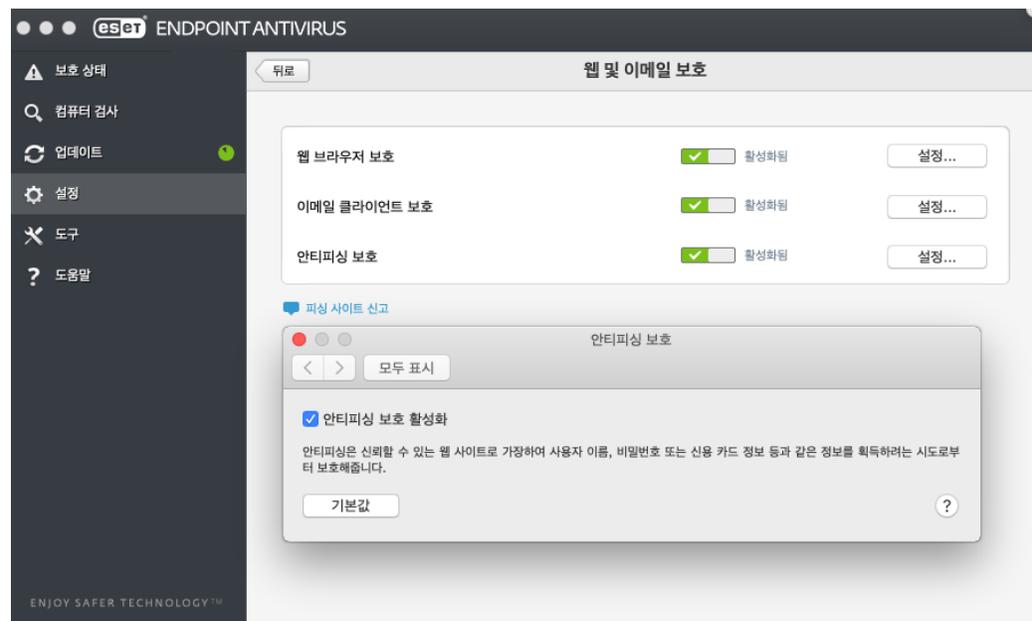
회사 소개

Why ESET?

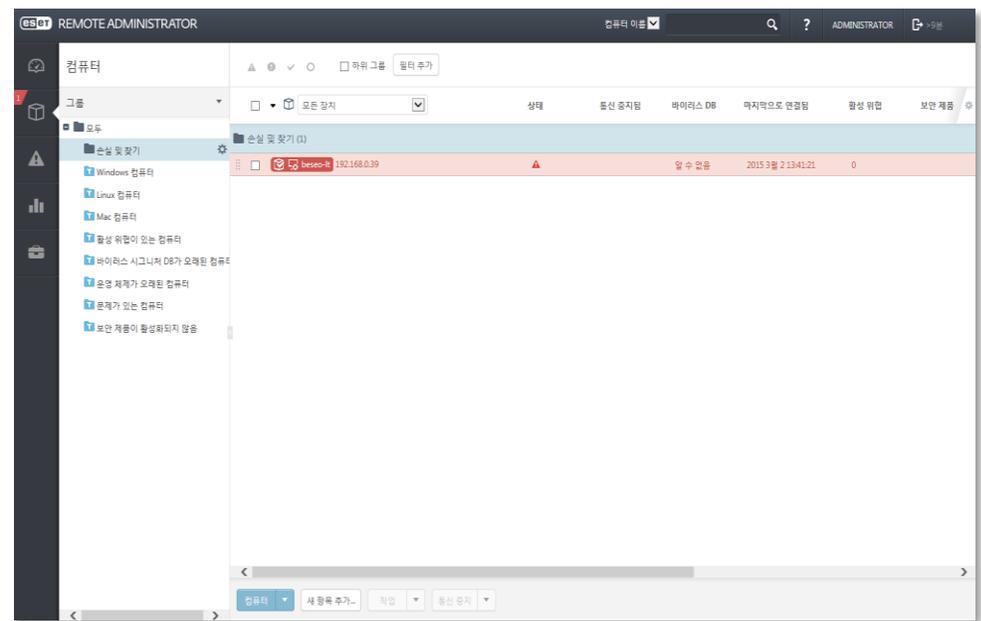
제품 소개

기술 지원

Appendix



**안티피싱 보호**  
- 안티피싱 보호 활성화로 피싱 사이트로부터 방어



**중앙관리툴을 이용한 통합 관리**

## ESET SERVER SECURITY for MS Windows Server

ESET SERVER SECURITY는 기업 내 중요한 서버를 보호하도록 제작된 강력한 안티바이러스 제품입니다. ESET만의 고유 기술을 통해 시스템 리소스를 최소화하면서 강력한 보호를 제공하여 기업의 자산을 안전하게 보호합니다.

주요 기능	기능 소개
접근 제어 (장치제어)	사내 네트워크 보호 및 데이터 유출을 방지하기 위해 웹 사이트 필터링 및 외부 장치에(디스크 저장소, USB프린터, FireWire 저장소, Bluetooth 장치, 카드리더, 이미징 장치, 모뎀, LPT/COM포트, 휴대용 장치) 대한 제어가 가능합니다. 읽기/쓰기, 차단, 읽기허용, 경고의 동작을 설정할 수 있습니다. Windows PC/Server, MAC, Linux Desktop OS에서 해당 기능을 지원합니다.
컴퓨터보호	안티스텔스 기술을 사용한 안티바이러스, 안티스파이웨어를 통해 바이러스, 루트킷, 스파이웨어 등의 악성 코드에 대한 위협으로 사내 네트워크를 보호하고 ThreatSense 엔진을 사용하여 알려지지 않은 신종 악성 코드에 대해 강화된 보안을 제공합니다.
코어 모드 지원	GUI형식이 아닌 CORE 플랫폼의 서버에서도 시스템 보호가 가능합니다. eshell 방식의 명령어를 통해 다양한 작업이 가능합니다.
시스템 업데이트	취약점을 통해 발생하는 위협을 방지하기 위해 Windows 보안 업데이트 및 서드파티 애플리케이션의 업데이트 유무를 체크합니다.
ThreatSense.net 조기 경보 시스템	알려지지 않은 새로운 위협으로부터 보호하기 위해 시스템에 감염이 의심되는 개체가 발견되는 경우 해당 샘플을 자동 전송하여 분석 후 처리 됩니다.
웹 및 이메일보호	네트워크 트래픽을 감지하여 웹 사이트 접속 및 이메일의 위협을 판단하여 클라이언트를 보호합니다. 필터링 기능을 사용하여 원하는 IP 및 URL에 대해 제외 처리도 가능합니다.
시스템 속도저하 방지	ESET만의 시스템 최적화 기술력을 통해 최소한의 리소스만을 사용하여 사용자 업무에 영향을 끼치지 않도록 시스템을 보호합니다.
ESET SYSINSPECTOR	ESET SYSINSPECTOR는 프로세스, 서비스, 애플리케이션, 레지스트리 등의 시스템 구성 요소에 대한 자세한 정보를 파악할 수 있는 툴을 제공하여 별도의 시스템 툴 없이 현재 시스템 현황을 파악 및 분석하는데 사용할 수 있습니다.

# ESET SERVER SECURITY for MS Windows Server

회사 소개

Why ESET?

## 제품 소개

기술 지원

Appendix

ESET SERVER SECURITY는 기업 내 중요한 서버를 보호하도록 제작된 강력한 안티바이러스 제품입니다. ESET만의 고유 기술을 통해 시스템 리소스를 최소화하면서 강력한 보호를 제공하여 기업의 자산을 안전하게 보호합니다.

### 보호 기능

안티바이러스, 안티스텔스 기능을 통해 악성 위협으로 부터 보호하며 서버의 부하를 줄이기 위해 실시간 감시 레벨을 다양한 방법으로 설정할 수 있습니다.

외부 장치를 통해 유입되는 위협으로 보호하기 위해 외부 장치 제어 연결 시 차단 설정이 가능합니다. 예외 처리를 통해 지정된 장치만 등록하여 연결도 가능합니다.

서버 운영상의 장애를 방지하기 위해 시스템 중요 개체의 경우 자동 제외 등록하여 원활한 서버 운영이 가능합니다.

### 웹 및 이메일 보호

사용자가 웹 사이트 접근 시 지정된 프로토콜을 감시하여 해당 웹 사이트의 위험 요소를 파악하여 사용자에게 안전한 웹 사이트 접근을 지원합니다.

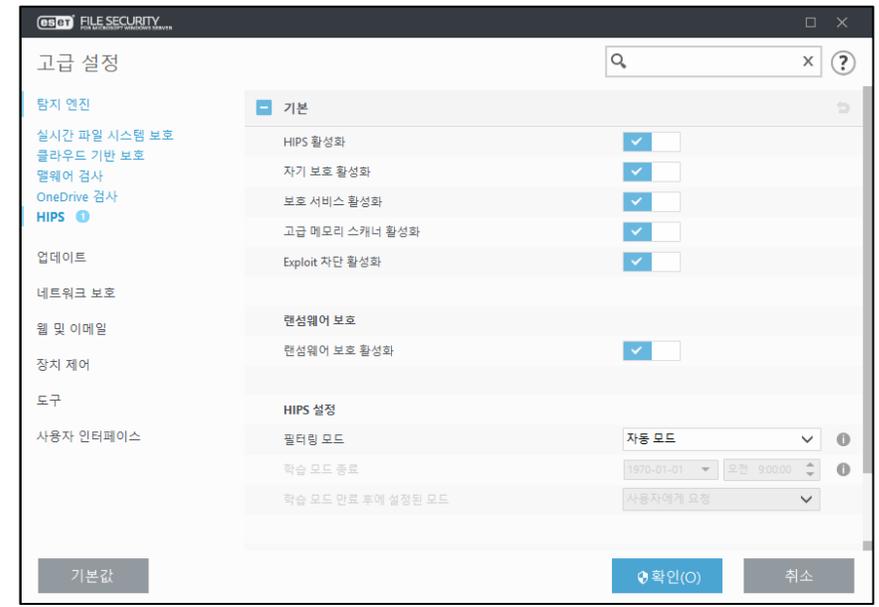
네트워크 접근 시 검사할 포트를 지정합니다. 기본적으로 http, https 프로토콜을 지원하며 기본 포트 외에도 지정 포트를 설정하여 검사가 가능합니다.

이메일 수신에 사용되는 Microsoft Outlook, Windows Mail, Mozilla Thunderbird 등의 이메일 클라이언트와 연동하여 이메일 보호를 진행합니다. 이메일 보호도 웹 보호와 동일하게 감시 프로토콜을 지정 가능합니다.

### 사전 방역

다중 위협 검출 방법으로 구현된 ThreatSense 기술을 사용하여 사전 예방 방식으로 검사를 수행합니다. 알려지지 않은 악성 개체에 대한 조기 보호를 제공하며 코드, 분석, 코드 에뮬레이션을 통해 악성 개체 유무를 판단하여 처리합니다.

ThreatSense.net 조기 경고 시스템을 사용하여 감염이 의심되는 개체를 발견 시 자동으로 ESET 연구소로 전송합니다. 해당 부분에 대한 피드백이 필요한 경우 이메일을 등록하여 회신을 받을 수 있습니다.



# ESET SERVER SECURITY for Linux

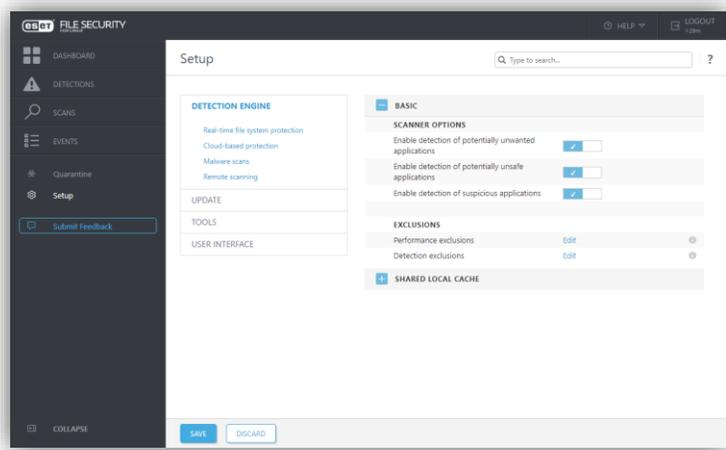
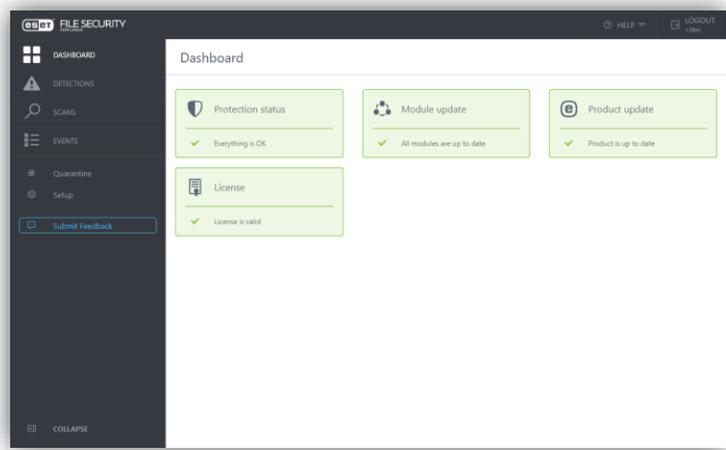
회사 소개

Why ESET?

제품 소개

기술 지원

Appendix



## 주요 기능

안티바이러스 및  
안티스파이웨어

크로스플랫폼 보호

낮은 리소스 점유율

원격 관리

다양한 리눅스  
배포판 지원

Linux 셸 명령어 지원

## 기능 소개

- 바이러스, 루트킷, 웜 및 스파이웨어를 포함한 모든 유형의 위협 제거
- ESET만의 차별화된 랜섬웨어 대응
- 서버에 저장된 데이터의 실시간 보호
- 클라우드 기반 평판 분석 시스템 LiveGrid

- 파일 공유 등을 통한 다른 플랫폼으로의 악성코드 확산 방지
- 윈도우, 맥 및 리눅스 운영 체제를 포함하는 모든 플랫폼을 대상으로 제작된 악성코드 탐지/제거

- 전 세계적으로 성능이 입증된 최고의 보호 기능을 제공하면서도 최소한의 리소스만을 사용함으로써 중요한 업무나 서비스에 더 많은 시스템 리소스 제공

- ESET Protect를 이용한 중앙 집중 원격 관리
- 전용 웹 인터페이스를 통한 개별 관리 (Linux 전용 WebUI 제공)
- 수동 검사, 이벤트 처리 및 보안 관리 작업의 예약 지원
- 상세한 로그와 사용자 정의가 가능한 보고서 및 알림을 통해 기업의 보안 정책 준수 여부를 모니터링

- RedHat, CentOS, Ubuntu, Devian, SUSE, Oracle, Amazon 등 다양한 리눅스 배포판 지원
- 단일 설치 프로그램을 이용한 간편한 설치 - 별도의 컴파일/빌드 과정 불필요

- 셸 명령어를 통한 검사, 환경설정, 라이선스 관리, 업데이트, 검사, 스케줄러 등 모든 기능 지원

## 제품별 지원 플랫폼

### ESET Protect(중앙관리)

#### 운영체제

Windows 10(x64)  
Windows Server 2012 R2, 2016, 2019  
Linux CentOS 7.7-1908

※ 중앙관리는 서버급 장비 설치/운영을 권장합니다.

#### 권장 하드웨어 사양

CPU 4 core 이상, RAM 8GB 이상, 200GB 이상의 디스크 여유 공간

### ESET SERVER SECURITY FOR WINDOWS SERVER

#### 운영체제

Windows Server 2003 (2022년 2월까지 지원)  
Windows Server 2008 SP2(x86 and x64), 2008 R2 SP1, 2012, 2012 R2, 2016, 2019  
Windows Storage Server 2008 R2 Essentials SP1, 2012, 2012 R2  
Windows Small Business Server 2003 (x86), 2003 R2 (x86), 2008 (x64), 2011 (x64)  
Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials  
MultiPoint Server 2010, 2011, 2012

#### 하드웨어 사양

Intel Pentium, AMD 호환 프로세서  
RAM 4GB 이상, 하드디스크 2GB 이상의 디스크 여유 공간

### ESET ENDPOINT ANTIVIRUS

#### 운영체제

Windows XP SP3 (2022년 2월까지 지원), Windows Vista(x86, x64),  
Windows 7(x86, x64), Windows 8(x86, x64), Windows 8.1(x86, x64), Windows 10  
**MAC OS X, Linux Desktop**

#### 하드웨어 사양

Intel or AMD x86-x64 이상, RAM 4GB 이상, 2GB 이상의 디스크 여유 공간

### ESET SERVER SECURITY FOR LINUX/BSD

#### 운영체제

커널후킹 전체 실시간 감시  
리눅스 커널 버전 2.6.32 이상, glibc 2.12 이상의 CentOS 6이상, Red Hat 6이상,  
SuSE 12이상, Ubuntu 16.04 이상, Debian 9이상 등

#### 하드웨어 사양

프로세서 Intel®/AMD® x86/x64 이상  
RAM 4GB 이상, 4GB 이상의 디스크 여유 공간

# 레퍼런스 - 국내

구분	고객사명	수량	고객사명	수량
제조사	삼성전자	OOO Linux SVR	엘오티베콤	OOO PC / OO SVR / EDTD
	상신브레이크	OOO PC / OO SVR	현대종합금속	OOO PC / OO SVR
	현대상선	OOO PC / OO SVR	양지사	OOO PC / OO SVR
	파크랜드	OOOO PC / OO SVR	삼표	OOOO PC / OO SVR
	쿠쿠전자	OOOO PC / OO SVR	한국알박	OOO PC / OO SVR
	뉴옵틱스	OOOO PC / OO SVR	코리아써킷	OOOO PC / OO SVR
	대선조선	OOO PC / OO SVR / EDTD	아모텍	OOOO PC / OO SVR
	이건창호	OOO PC / OO SVR	서울반도체	OOOO PC
	솔브레인	OOOO PC, EDTD	호전실업	OOOO PC / OO SVR
	웰크론	OOO PC / OO SVR	덕우전자	OOO PC / EDTD
언론사 방송사	스포츠조선	OOO PC / OO SVR	세계일보	OOO PC / OO SVR
	경향신문	OOO PC / OO SVR	아프리카TV	OOO PC
	KBS미디어	OOO PC / OO Win SVR / O Linux SVR	EBS	OOO PC
	국악방송	OOO PC / O SVR	지방 MBC	OOO PC / OO SVR
IT 게임사	네시삼십삼분	OOO PC / OOO SVR	알서포트	OOO PC / OOO MAC / OOO SVR
	데브시스터즈	OOO PC / OOO MAC	해외 지마켓(지오시스)	OOO SVR
	조이시티	OOO PC / OO SVR	뉴딘콘텐츠	OOOO PC / OO SVR
	에스케이텔레시스	OOO PC / OO SVR	바른손이앤에이	OOO PC / OO SVR
	원스토어	OOO PC / OOO MAC / OOO SVR	마크애니	OOO PC / OO Win SVR / OO Linux SVR
교육	윤선생영어교실	OOOO PC / OOO SVR	대전외국인학교	OOO PC
	재능이아카데미	OO Win SVR / OO Linux SVR	파고다아카데미	OOO PC / OO SVR
종교	지구촌교회	OOO PC / OO SVR	연세중앙교회	OOO PC / O SVR
	온누리교회	OOO PC / O SVR	한국에스지아이	OOO PC / OO SVR

회사 소개

Why ESET?

제품 소개

기술 지원

Appendix

# 레퍼런스 - 국내

구분	고객사명	수량	고객사명	수량
건설/건축	라인건설	OOO PC / O SVR	시공테크	OOO PC / OO SVR
	디자인캠프문박디엠피	OOO PC / OO SVR	무영씨엠건축사무소	OOO PC / O SVR
금융	KB자산운용	OOO PC / OO SVR	코리안리재보험	OO WinSVR / OO LinuxSVR
	이지스자산운용	OOO PC / OO SVR	한국디지털자산거래소	OOO PC / OO SVR
	에이앤디신용정보	O000 PC / OO SVR	서울손해사정	OOO PC / O Linux SVR
병원 제약	아이디병원	OOO PC / OO SVR	경인양행	OOO PC / OO SVR
	김안과병원	OOO PC / O SVR	환인제약	OOO PC / OO SVR
	척병원	OOO PC / OO SVR	휴온스글로벌	O000 PC / OO WinSVR / OO LinuxSVR
	청주성모병원	OOO PC / OO SVR	고려은단	OOO PC / OO SVR
	유유제약	OOO PC / OO SVR / EDTD	유한화학	OOO PC / OO SVR
	신풍제약	OOO PC / O SVR	녹십자셀	OOO PC / OO SVR
공공	동해시청	OO Linux SVR	대한장애인체육회	OO Win SVR / O Linux SVR
	한국기초과학지원연구원	OO Linux SVR	한국해운조합	OOO PC / OO WinSVR / O LinuxSVR
	국가핵융합연구소	OOO PC / OO SVR	국방전직교육원	OOO PC / O Win SVR / O Linux SVR
	한국기계전기전자시험연구원	OOO PC / OO SVR / EDTD	서울교통공사 열차정보관리센터	OO PC / OOO SVR
기타	홈플러스	O0000 PC (POS) / O000 SVR	현대성우캐스팅	OOO PC / OO WinSVR / O LinuxSVR
	한독모터스(BMW)	OOO PC / OO SVR	KBK특허법률사무소	OOO PC / OO SVR
	스타자동차	OOO PC / OO WinSVR / O LinuxSVR	리앤목특허법인	OOO PC / OO SVR
	도서출판길벗	OOO PC / O SVR	애틀미	OOO PC / EDTD
	미래엔	OOO PC / OO SVR	한국시세이도	OOO PC / OO SVR
	한국피자헛	O000 PC (POS) / OO SVR	아웃백스테이크하우스	OOO PC / OO WinSVR / O LinuxSVR
	베스킨라빈스31, 빠리바게뜨	O000 PC (POS)	할리스에프앤비	OOO PC / O SVR
	탐앤탐스	OOO PC	삼천리	O000 PC / OO SVR

회사 소개

Why ESET?

제품 소개

기술 지원

Appendix

## 레퍼런스 - 해외

구분	고객사명	수량	고객사명	수량
제조	TOYOTA	25,000 Nodes	HONDA	23,000 Nodes
	Canon	29,000 Nodes	Panasonic	15,000 Nodes
	TOSHIBA	10,000 Nodes	Fuji Electric	1,400 Nodes
	TSINGTAO	7,000 Nodes		
서비스	TKC Corporation	300,000 Nodes	Recruit Holdings	33,079 Nodes
교육 공공	Harvard University	7,000 Nodes	HongKong Poly University	25,000 Nodes
	University of Auckland	16,500 Nodes	IWATE Medical University	7,750 Nodes
	Junsei Educational Institution	17,200 Nodes	University Sains Malaysia	10,000 Nodes
	公安 Police	40,000 Nodes	Directorate of Taxation	35,880 Nodes
	Courts of Justic	12,500 Nodes	Kagoshima University	10,000 Nodes
IT	CHINA TELECOM	3,000 Nodes	NTT DOCOMO, INC	65,000 Nodes
금융	Commercial Bank of Ceylon PLC	6,600 Nodes	Jilin Bank	6,000 Nodes

회사 소개

Why ESET?

제품 소개

기술 지원

Appendix



## 기술 지원

이셋코리아에서는 25년 이상 경력의 엔지니어들이 방문 정기점검 등 지속적인 기술지원을 제공합니다.

간단한 장애 해결부터 기업 내 IT 자원을 보호하는 테크니컬한 지원까지, 세계 백신 점유율 1위 업체다운 기술력을 바탕으로 고객분들께 안정적인 사용 환경을 약속합니다.

# ESET GLOBAL TECHNICAL PROCESS

회사 소개

Why ESET?

제품 소개

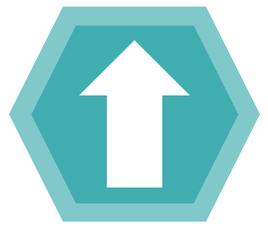
기술 지원

Appendix



## ESET 샘플 입수

- 1년 365일 24시간 내내 바이러스 샘플을 입수합니다.  
업무 시간 중에는 [support@estc.co.kr](mailto:support@estc.co.kr) 또는 기타 경로(원격)로 샘플을 입수합니다.  
업무 시간 외에는 [samples@eset.sk](mailto:samples@eset.sk) 로 샘플을 입수합니다.



## Virus 여부 판단

- 테스트 환경에서 실제 바이러스 여부 확인 및 ESET 백신에서 이미 탐지하고 있는가를 판단합니다.
- 24시간 ESET Global Virus-Lab에서 전세계의 바이러스 발생 현황을 확인하실 수 있습니다.



## 본사 분석

- 신고된 바이러스 샘플을 테스트 랩에서 1차 분석을 진행합니다.  
- 실제 바이러스 여부 및 2차 분석 작업 선별을 진행합니다.
- 한국지사에서 바이러스 여부 통지 및 예상 진단명을 통지합니다.
- 2차 정밀 분석을 통해 바이러스 시그니처를 생성합니다.
- 증가분 DB를 작성한 후 3차 테스트 랩으로 전달합니다.



## 업데이트 서버 업로드

- 분석된 바이러스 시그니처를 전세계 모든 ESET 업데이트 서버에 업로드합니다.
- 한시간 단위 데이터베이스 업데이트를 진행합니다.



## ESET TECHNICAL SUPPORT



### 전문 엔지니어를 통한 완벽한 기술지원

- 이셋코리아에서는 25년 이상 경력의 엔지니어들이 방문 정기점검등 지속적인 기술지원을 제공합니다.



### 신종 악성코드에 대한 빠른 업데이트

- 전세계 사용자들에게 실시간으로 수집된 악성코드를 본사 엔지니어가 빠르게 분석하여 업데이트합니다.



### 적극적이고 신속한 기술지원

- 문제가 발생할 경우 한국지사 엔지니어가 신속하게 원격지원을 해드리며 원격으로도 해결이 되지 않을 경우 직접 방문하여 원인 분석 및 기술지원을 제공합니다.



### 글로벌한 기술 대응

- 전세계 사용자들 또는 각 나라별 지사에서 알려지지 않은 바이러스 샘플 취득시 본사측에 샘플을 전달하여 분석 후 즉각 업데이트를 진행합니다.





# Appendix

## ESET Dynamic Threat Defense (EDTD) – WHY EDTD?

회사 소개

Why ESET?

제품 소개

기술 지원

Appendix

### 필요성

### EDTD



최신 악성파일에 대한 방어



샌드박스를 통한 최신 악성파일 발견



AI 머신러닝 등 최신 기술 필요



AI 머신러닝 탑재, 제로데이 위협 탐지



보안/전산 인력 부족



ESET 중앙관리를 통한 통합 관리



고가의 APT 제품



클라우드 샌드박스를 이용한 낮은 비용

# ESET Dynamic Threat Defense (EDTD) – WHY EDTD?

- 회사 소개
- Why ESET?
- 제품 소개
- 기술 지원

## Appendix

High End Solution  
(EDR, 장비형태)

- 높은 비용
- 전담 엔지니어(분석가) 필요
- 차단을 위한 추가 솔루션 필요
- 추가 에이전트 설치
- 장비에 대한 유지보수 필요

클라우드 기반 샌드박스 기술을 이용한  
APT 서비스 ESET Dynamic Threat Defense



- AI Machine Learning
- Ransomware Protection
- Zero-day Threats Detection
- Automatic Protection
- High End 솔루션보다 낮은 비용
- 백신에 포함되어 있어 추가 에이전트 설치 불필요



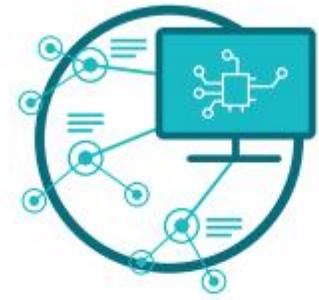
## ESET Dynamic Threat Defense (EDTD)

- ✓ ESET 제품과 연동 가능
- ✓ 머신러닝 기능 탑재
- ✓ 랜섬웨어 보호
- ✓ 제로데이 위협 탐지
- ✓ 모든 엔드포인트 대상 즉시 보호 기능
- ✓ 분석 결과에 대한 상세 리포트 전달



### ESET LIVEGRID®

Whenever a zero-day threat such as ransomware is seen, the file is sent to our cloud-based malware protection system – LiveGrid®, where the threat is detonated and behavior is monitored. Results of this system are provided to all endpoints globally within minutes without requiring any updates.



### MACHINE LEARNING

Uses the combined power of neural networks and handpicked algorithms to correctly label incoming samples as clean, potentially unwanted or malicious.



### HUMAN EXPERTISE

World-class security researchers sharing elite know-how and intelligence to ensure the best round-the-clock threat intelligence.



# ESET Dynamic Threat Defense (EDTD)

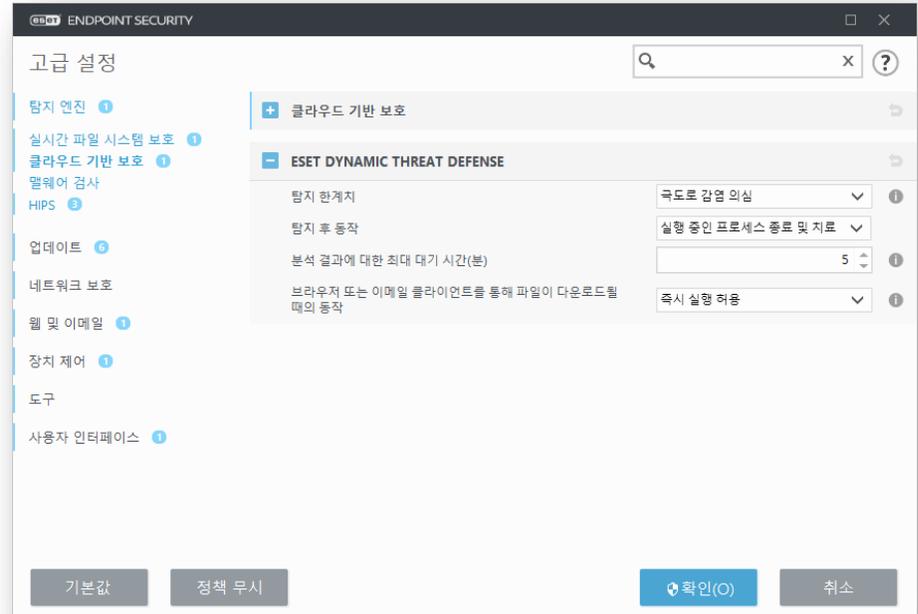
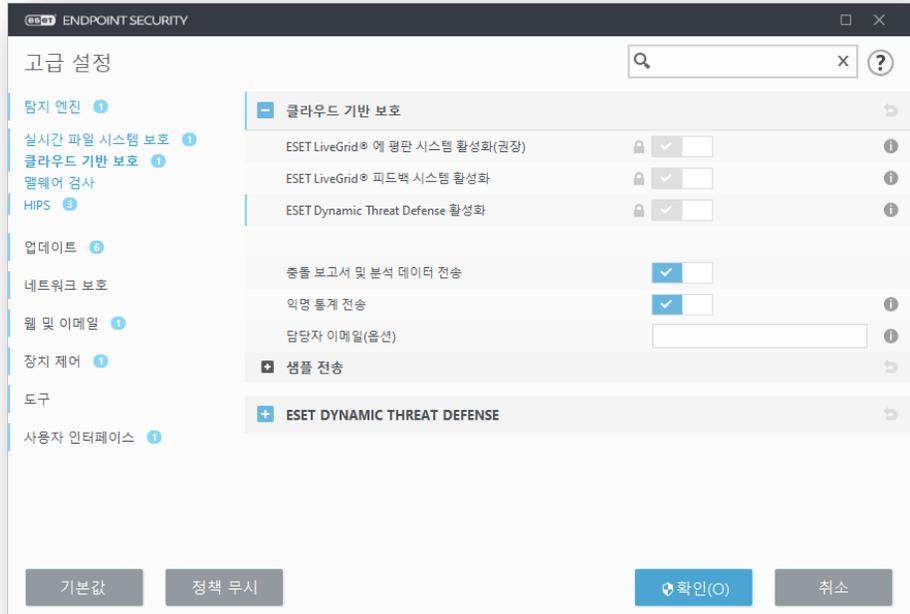
회사 소개

Why ESET?

제품 소개

기술 지원

## Appendix



**NEW** 클라우드 기반 샌드박스

ESET 클라우드 서버에서 머신러닝, 샌드박스 실행

**NEW** 제로데이 위협 탐지

DB에 없는, 알려지지 않은 신종 위협의 신속한 탐지 및 제거

**NEW** EP(중앙관리) 통합

EP(중앙관리)에서 분석된 개체 정보 및 보고서 확인

**NEW** ESET 제품 연동

EEA/EES/EFSW/EMSX 가 이미 설치된 시스템에서 바로 활성화

**NEW** 로밍 엔드포인트 지원

회사 네트워크에서 분리된 엔드포인트 호스트도 EDTD 이용에 제약이 없음



# ESET Dynamic Threat Defense (EDTD) – 중앙관리 및 보고서

회사 소개

Why ESET?

제품 소개

기술 지원

## Appendix

The screenshot shows the ESET Security Management Center interface. The main window displays a file action report for a file named 'file://C:/User...PLAYERSETUP.EXE'. The report is titled '극도로 감염 의심' (Highly Suspected of Infection) and shows the following details:

- 상태 (Status):** 극도로 감염 의심 (Highly Suspected of Infection)
- 상태 (Status):** 마침 (Completed)
- 전송된 날짜 (Date Transmitted):** 2019 12월 28 10:04:57
- 마지막으로 처리한 날짜 (Last Processed Date):** 2019 12월 27 20:35:17
- 동작 (Action):** 동작 보기 (View Action)

The '분석' (Analysis) section shows:

- 상태 (Status):** 극도로 감염 의심 (Highly Suspected of Infection)
- 상태 (Status):** 마침 (Completed)
- 전송된 날짜 (Date Transmitted):** 2019 12월 27 20:35:17
- 마지막으로 처리한 날짜 (Last Processed Date):** 2019 12월 28 10:04:57

The '원본' (Original) section shows:

- 컴퓨터 (Computer):** polo
- 사용자 (User):** NT AUTHORITY\SYSTEM
- 사용 (Usage):** 자동 (Automatic)
- 보낸 곳 (Sent From):** Dynamic Threat Defense

The '파일' (File) section shows:

- 해시 (Hash):** 95500A43D2480E836127821558C8CF155289A117
- 파일 이름 (File Name):** file://C:/Users/POLO/AppData/Local/Temp/GOM/PLAYERSETUP.EXE
- 크기 (Size):** 284KB (27 520 520 bytes)
- 방주 (Signature):** 실패 없음 (No Failure)

The screenshot shows a detailed file action report titled '파일 동작 보고서' (File Action Report). The report includes the following information:

- 상태 (Status):** 극도로 감염 의심 (Highly Suspected of Infection)
- SHA-1:** 95500A43D2480E836127821558C8CF155289A117
- 크기 (Size):** 275205208
- 방주 (Signature):** 실패 없음 (No Failure)

The '검색된 동작' (Searched Action) section lists the following details:

- 동작 (Action):** 행태어가 실행되지 않고 탐지됨 (Behavior not executed and detected)
- 설명 (Description):** 샘플이 실행되지 않고 악의적인 것으로 집계되었습니다. (Sample not executed and classified as malicious.)
- 일반적 행위 (General Behavior):** 정상적인 애플리케이션은 이러한 통신을 수행하지 않습니다. (Normal applications do not perform this communication.)
- 악의적 행위 (Malicious Behavior):** ESET 검사 엔진을 통해 실행 코드가 감지되었습니다. (Execution code detected by ESET engine.)

The '네트워크 통신' (Network Communication) section lists the following details:

- 동작 (Action):** 네트워크 통신 (Network communication)
- 설명 (Description):** 샘플이 네트워크를 통해 다른 컴퓨터에 연결하거나 다른 컴퓨터의 연결을 수신 대기하려고 시도했습니다. (Sample attempted to connect to other computers or receive connections.)
- 일반적 행위 (General Behavior):** 정상적인 애플리케이션은 이러한 통신을 수행하지 않습니다. (Normal applications do not perform this communication.)
- 악의적 행위 (Malicious Behavior):** 샘플이 추가 부분을 다운로드하거나 악성 서버와 통신하려고 시도했습니다. (Sample attempted to download additional parts or communicate with a malicious server.)

The '마신 러닝 탐지' (Machine Learning Detection) section lists the following details:

- 동작 (Action):** 마신 러닝 탐지 (Machine learning detection)
- 설명 (Description):** 샘플 자체가 알려진 행위어와 매우 유사합니다. (Sample is very similar to known behavior.)
- 일반적 행위 (General Behavior):** 정상적인 애플리케이션은 이러한 통신을 수행하지 않습니다. (Normal applications do not perform this communication.)
- 악의적 행위 (Malicious Behavior):** 신경망 마신 러닝에 의해 감지되었습니다. (Detected by neural network machine learning.)

# ISL Online (원격제어 솔루션) – 제품군

회사 소개

Why ESET?

제품 소개

기술 지원

Appendix

## SaaS(클라우드)

- 경제적인 도입 비용
- 99.99% 연속성 보장
- 최적의 성능, 속도, 신뢰성
- 글로벌 원격 지원
- 임대 기간 설정(1,2,3년)
- 자동 업그레이드



## On-Premise(구축형)

- 고객사 보안 정책 준수
- 영구 라이선스 사용
- 내외부망 지원
- 서버 1대로 최대 1만 단말기 연결 지원



## MPC(관리형 사설 클라우드)

- 다수의 고객사에서 사용
- 자체 구축형과 클라우드 방식의 장점만으로 서비스 구축
- 관리의 리스크 해소
- 사설 서버 구축으로 보안 보장
- OEM 커스터 마이징
- ITMS, CRM, ERP등 서비스 연동



# ISL Online (원격제어 솔루션) – 재택 근무형

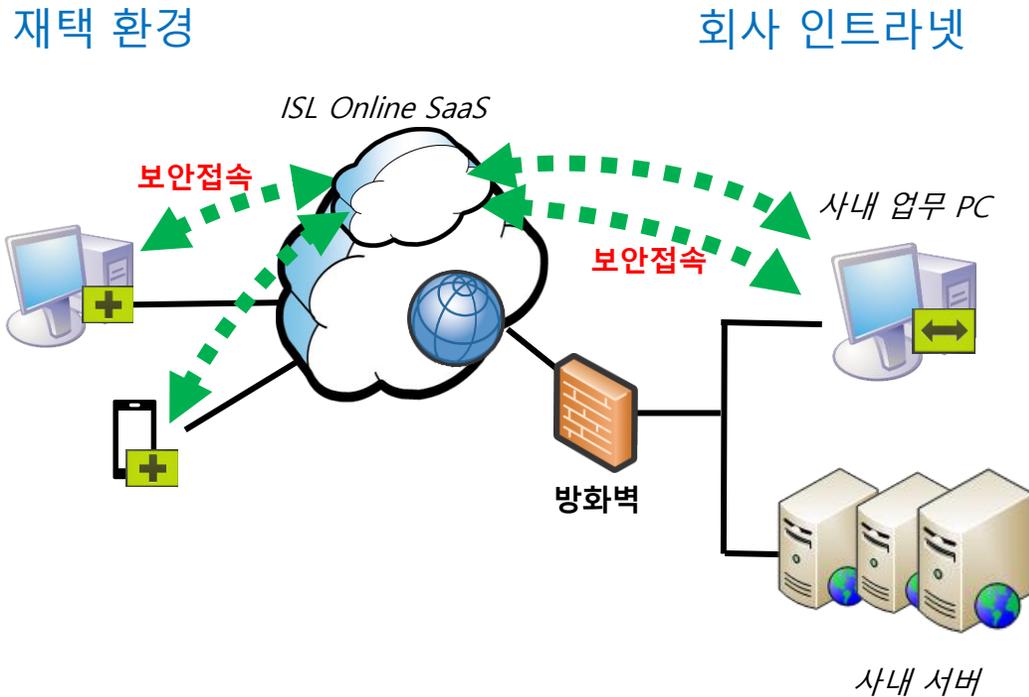
회사 소개

Why ESET?

제품 소개

기술 지원

## Appendix



사내 업무 PC를 집(원격지)의 PC에서 접속  
사내 업무 PC에서 수행하던 모든 작업을 집(원격지)에서 수행  
5분으로 원격 업무 환경 완성

### 절차

- 계정 만들기(1분)
- 회사 PC에 원격 제어 프로그램 설치(2분)
- 집/외근 지역에서 원격 프로그램 실행(또는 설치)(1분)
- 로그인하여 회사에 있는 PC에 접속하여 업무 진행(1분)

# ISL Online (원격제어 솔루션) – 타사 비교자료

회사 소개

Why ESET?

제품 소개

기술 지원

## Appendix

기능 비교	ISL light	R사	A사	T사	H사
공통 기능	마우스, 키보드 제어 / 채팅 / 그리기 / 다중모니터 지원 / 시스템 정보 확인 / 코드 사인 / 관리자 기능 / 접속화면 커스터마이징 등				
상담원 화면 전송	○	상품군별 구분	상품군 별 구분	○	▲(화면제어 제한)
파일 송수신 용량 제한	무제한	상품군별 구분(300M, 1G)	상품군별 구분(3GB, 무제한)	무제한	무제한
Wake on LAN 지원	○	별도 제품(RemoteWOL)	미지원	○	미지원
음성/화상채팅	○	상품군별 구분	▲(화상채팅 미지원)	○	미지원
안전모드 원격 지원	○	상품군별 구분	○	○	X
원격재부팅 자동 접속	○	상품군별 구분	○	○	○
화면 녹화	○	상품군별 구분	○	○	○
모바일 지원	○	별도 제품	별도 제품(Premium)	○	X
원격제어(무인 접속)	○	별도 제품(Remote View)	별도 제품(PCAnyPro)	○	X
웹 컨퍼런스(화상회의)	○	별도 제품(RemoteMeeting)	별도 제품(UCTogether)	○	X
상담 일지	○	상품군별 구분	상품군별 구분	○	▲
라이브 채팅	○	-	별도 제품(Liveweb)	-	X
보안 & 암호화	RSA 2048/4096-Bit AES 256-Bit	RSA 2048-Bit AES 256-Bit	AES 256-Bit	RSA 2048-Bit AES 256-Bit	AES 128-Bit

# 감사합니다.

- ESET -

세상에서 가장 가볍고 빠르고 정확한 백신!!  
관리가 쉽고 간단합니다.

ESET KOREA operated by ESTC

Address : 서울시 강남구 논현로 406 요경빌딩 4층

Tel : 1899-8352

Fax : 02)573-0040

구매 문의 : [sales@estc.co.kr](mailto:sales@estc.co.kr)

기술 문의 : [tech@estc.co.kr](mailto:tech@estc.co.kr)

웹 사이트 : [www.estc.co.kr](http://www.estc.co.kr)