TREND MICRO

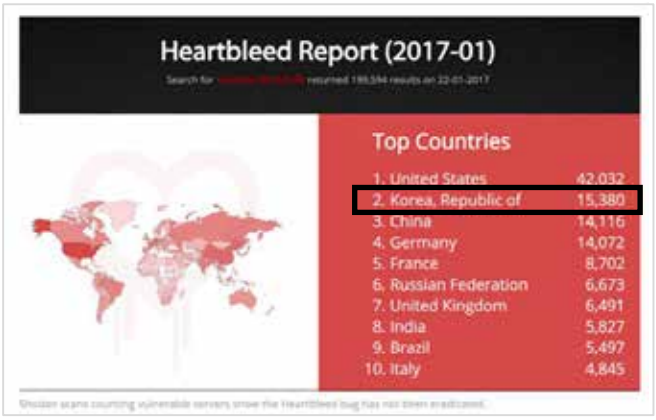
Linux Security?
Deep Security!

Trend Micro
리눅스서버 보안 솔루션

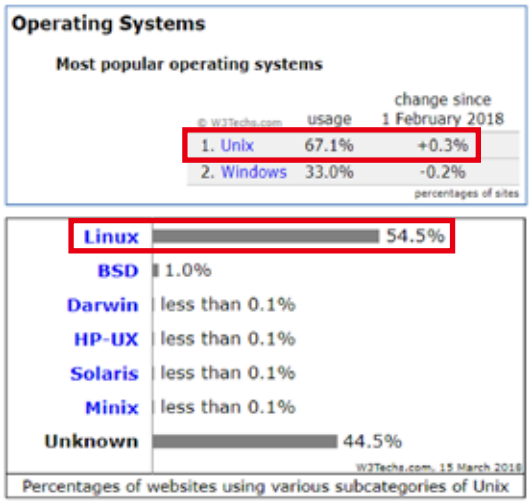
목차

1. 서버 보안

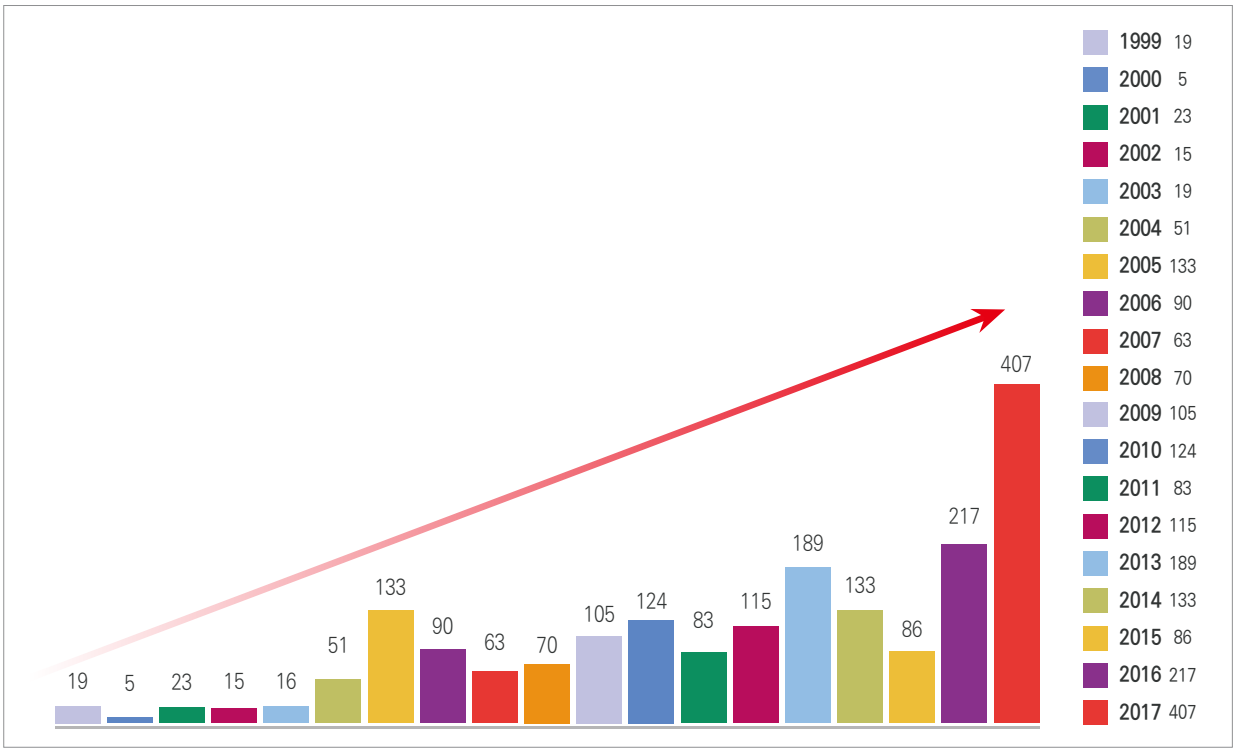
리눅스 서버를 가장 많이 사용하고 있는 곳은 고객과의 접점이 많은 웹 서버이며, 전 세계 웹 서버의 60% 이상이 리눅스 운영체제를 사용하고 있습니다. 이 서버들은 운영체제의 취약점(리눅스 커널 취약점) 및 사용하고 있는 각종 어플리케이션의 취약점이 공개되어 있음에도 2~3년 전의 취약점에 대한 공격 사례가 다양하게 나타나고 있습니다.



Source: Shodan, January 2017



[리눅스 서버의 취약점과 패치 필요성]



전 세계 리눅스 커널 취약점 현황 (*출처: CVE Detail, 2017.11)

1. 서버 보안

리눅스는 근본적으로 다양한 오픈 소스 기반이기 때문에 보안 홀이 파악하기 어려울 정도로 많이 존재합니다. 다만, 전 세계 커뮤니티의 도움을 받아 즉각 패치가 이뤄진다는 점에서 한편으론 폐쇄적인 운영체제에 비해 보안 강화가 쉽지만 이는 운영체제를 실시간으로 업데이트를 한다는 전제하에 논의되는 것이며 데이터 센터 안의 서버를 중단시킬 수 없는 현실 여건상 기업은 보안의 사각지대에 놓여 있다 해도 과언이 아닙니다. 윈도우용 공격 툴을 리눅스로 포팅하여 공격을 개시한 사례가 점차 증가하고 있습니다. (인터넷 나야나 사태, SAMSAM 등)

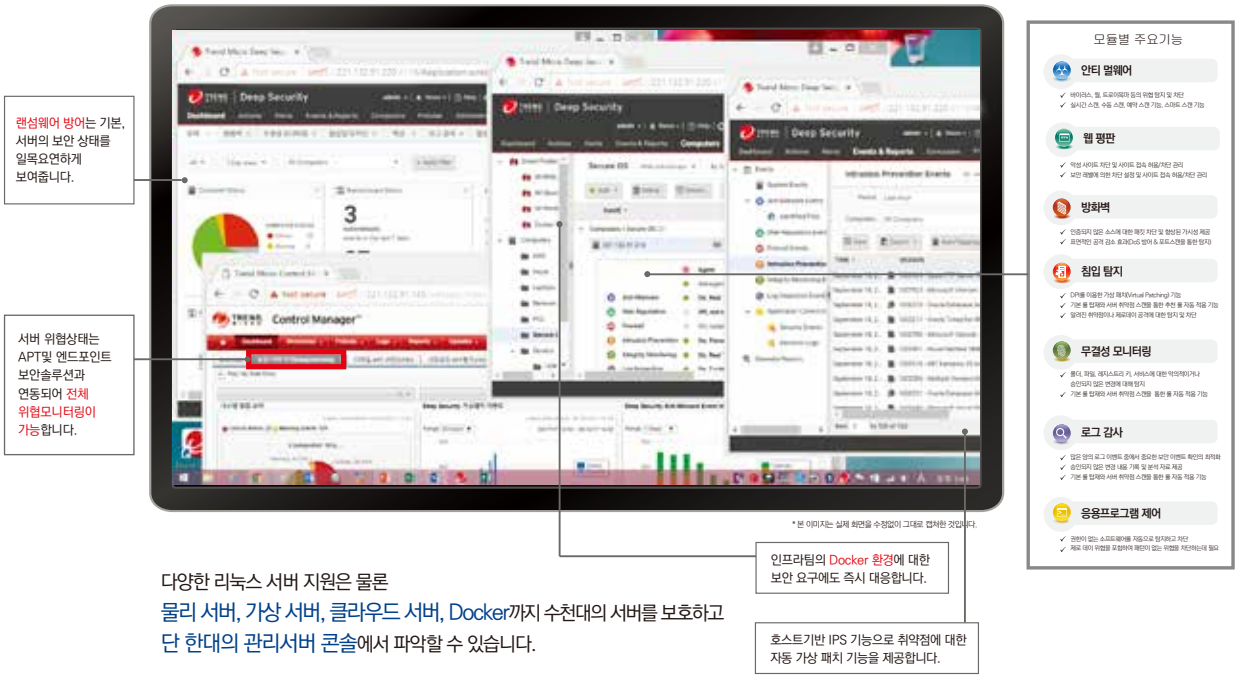
[리눅스 서버의 취약점과 패치 필요성]

리눅스 서버 보안 제품시 도입시 점검할 사항

- ☑ 리얼타임 바이러스 스캔이 되고 있는지?
- ☑ 글로벌 랜섬웨어 방어에 충분한 지?
- ☑ 호스트 서버별 별도의 보안 정책이 적용가능한지?
- ☑ 무결성 검증, 취약성 방어를 위한 가상패치가 가능한지?
- ☑ 특정 프로그램 작동만을 허용하는 화이트리스트 기능이 있는지?

이에 따라 리눅스 서버에 필수적으로 적용해야하는 실시간 백신과 각종 취약점 방어를 위한 가상패치 무결성 모니터링 및 응용 프로그램 제어를 통한 화이트리스트 기능 적용을 통해 다단계 방어가 필수적입니다.
Deep Security는 번거롭고 복잡한 리눅스 서버 보안 작업을 소프트웨어 방식으로 자동화하여 운영상의 편리함을 추가한 솔루션으로 2004년부터 각종의 리눅스 배포판과 커널을 지원하고

Deep Security 적용 화면



다양한 리눅스 서버 지원은 물론
물리 서버, 가상 서버, 클라우드 서버, Docker까지 수천대의 서버를 보호하고
단 한대의 관리서버 콘솔에서 파악할 수 있습니다.

리눅스 서버 보안 : Deep Security

- 가장 높은 탐지율과 다양한 리눅스 OS 종류를 지원
- 수많은 리눅스 및 커널에 대해 실시간 백신 지원

Amazon Linux
CentOS
CloudLinux
Debian
Oracle Linux
Red Hat Enterprise Linux
SuSE
Ubuntu

[수많은 리눅스 지원]

Linux Platform	32/64	Kernel Support Package
amazon2	64	KernelSupport-amzn2-11.0.0-262.x86_64.zip
amazon	64	KernelSupport-amzn1-11.0.0-263.x86_64.zip
centos6	32	KernelSupport-RedHat_EL6-11.0.0-282.i386.zip
centos6	64	KernelSupport-RedHat_EL6-11.0.0-283.x86_64.zip
centos7	64	KernelSupport-RedHat_EL7-11.0.0-288.x86_64.zip
cloud7	64	KernelSupport-CloudLinux_7-11.0.0-261.x86_64.zip
debian8	64	KernelSupport-Debian_8-11.0.0-232.x86_64.zip
oracle6	32	KernelSupport-Oracle_OL6-11.0.0-286.i386.zip
oracle6	64	KernelSupport-Oracle_OL6-11.0.0-287.x86_64.zip
oracle7	64	KernelSupport-Oracle_OL7-11.0.0-277.x86_64.zip
rhel6	32	KernelSupport-RedHat_EL6-11.0.0-282.i386.zip
rhel6	64	KernelSupport-RedHat_EL6-11.0.0-283.x86_64.zip
rhel7	64	KernelSupport-RedHat_EL7-11.0.0-288.x86_64.zip

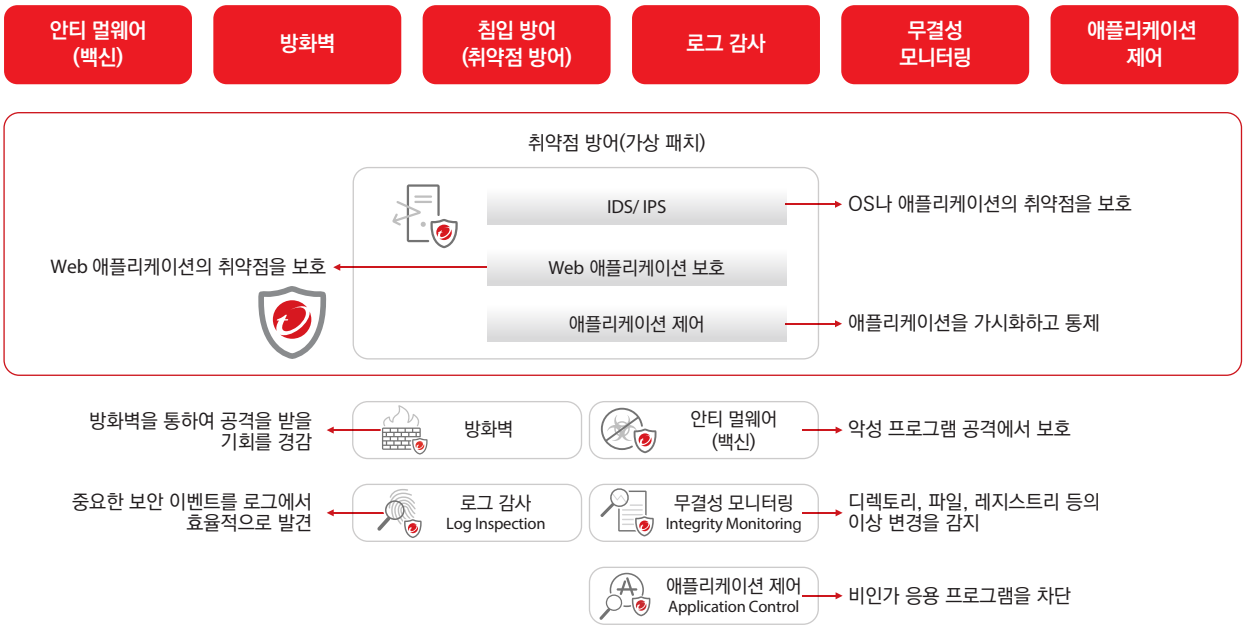
[수많은 리눅스 커널 지원]

3. Trend Micro Deep Security 개요

Trend Micro Deep Security는 서버를 다단계 방어하는 소프트웨어 입니다.
물리, 가상 , 클라우드 등 다양한 서버 환경에 대응하고, 각 서버들에 통합된 보안을 제공할 수 있습니다.
데이터 침해 및 무단 침입에 의한 업무의 혼란을 방지하고 PCI, DSS등 중요한 규정 및 표준 준수를 지원하여 구현 후 운영 비용을 줄이기 위해 도움이 됩니다.

- Anti-Malware (백신)
- Web Reputation (웹 평판)
- Firewall (방화벽)
- Intrusion Prevention (침입 탐지/차단)
- Integrity Monitoring (무결성 모니터링)
- Log Inspection (로그 감사)
- Application Control (응용프로그램 제어)

Deep Security 기능



4. Trend Micro Deep Security 도입 시 장점

서버 보안은 가상화, 클라우드 등 여러 복잡한 IT 아키텍처에 대응해야 하는 서버환경에서 Deep Security는 다음과 같은 장점을 제공합니다.

• 데이터 침해 및 외부 위협에 대응

- 서버에서 호스트 방식으로 보안을 적용하여 물리 환경, 가상화 환경, 클라우드 환경 지원
- Web 애플리케이션 및 기업 애플리케이션, OS의 알려진 또는 알려지지 않은 취약점에 대해 보호를 지원 하고 취약점을 이용한 시스템 공격을 탐지 차단
- 의심스러운 행동을 식별하고 예방하는 수단을 제공

• 컴플라이언스 준수에 대한 대응 · 지원

- PCI-DSS 컴플라이언스 요구사항 (파일 무결성 모니터링 서버 로그 수집 등) 대응
- 세부 감사에 대응되는 보고서를 생성, 외부/내부에서의 공격을 시각화하여 제공

• 도입 이후 운용 비용 절감

- 보안 패치 검증 및 취약점에 대응되는 IPS 규칙 “가상패치”로 취약점을 이용한 악성 공격으로부터 서버를 보호
- 관리 매니저를 통한 중앙 집중 관리 방식으로 각각의 서버에 통합 보호 제공 하여 여러 소프트웨어 사용하지 않아 비용 절감

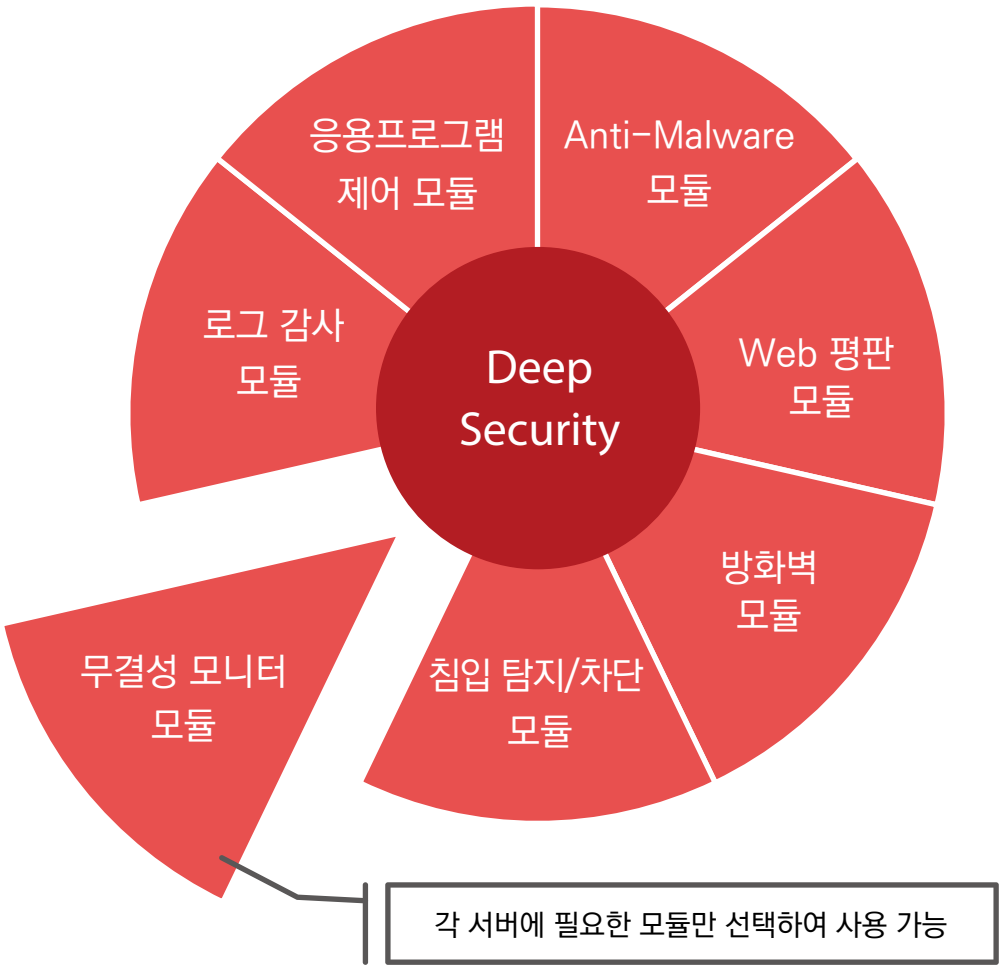
• 가상화 환경 클라우드 환경에 적합한 보안 구현을 실현

- VMware ESXi, VMware NSX와 연동하여 가상 환경에서 게스트 OS에 에이전트를 설치할 필요 없이 “에이전트리스 보안”을 적용하여, 업무 위주의 게스트 OS에 영향없이 보안 기능을 적용 가능
- 동적으로 인스턴스가 증감하는 클라우드 환경인 AWS 및 Microsoft Azure 등에서 Auto Scaling 기능을 통해 자동으로 증가하는 인스턴스에 맞게 Deep Security도 자동으로 적용하여 서버를 보호하고 보안 을 강화하여 담당 관리자가 매번 보안 에이전트를 수동으로

5. Trend Micro Deep Security 보안 모듈과 기능

Deep Security에서는 필요한 보호 기능만을 사용하여 변화하는 비즈니스 요구 사항에 맞게 적절한 보호 기능을 도입할 수 있으며 모든 기능을 사용하여 서버에 보안을 강화합니다.
모든 보안 모듈의 기능은 서버 또는 가상 머신에 단일 Deep Security Agent로 배포됩니다.
이 Agent는 Security Manager를 통해 중앙에서 통합 관리하게 됩니다.
또한 물리 · 가상 · 클라우드에 모두 대응할 수 있습니다.

Deep Security Agent **각 보안 모듈**



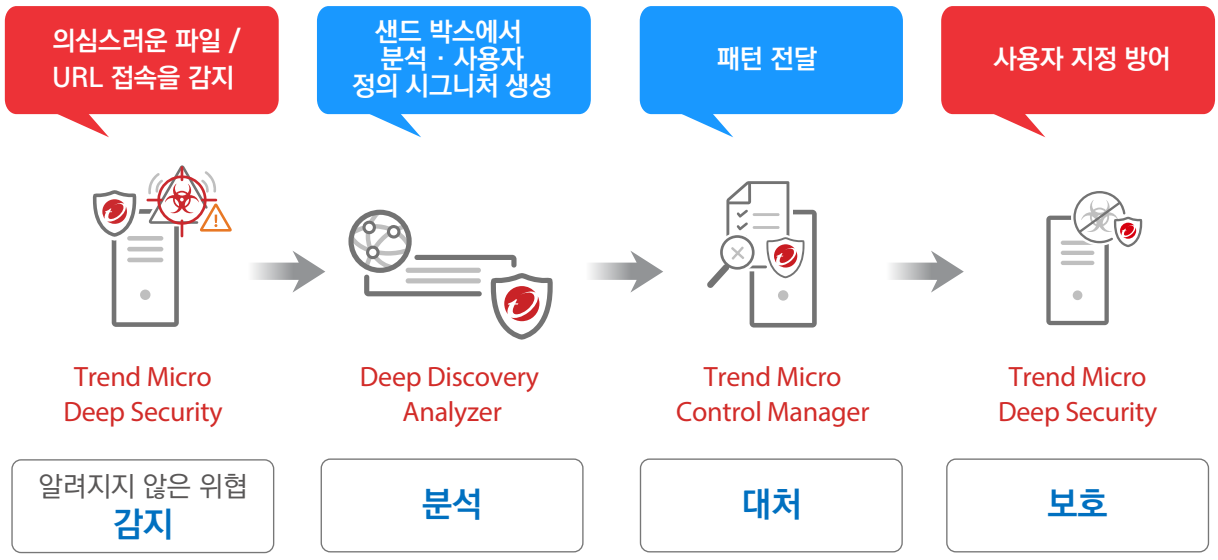
• Anti-Malware (백신)

서버에 악성 프로그램이 감염되는 것을 방지합니다.
악성 프로그램이 서버에 침입하려고 할 때 탐지하는 실시간 검색과 매주/매일 등 사전에 설정 한 시간에 검색하여 서버를 악성 프로그램 감염으로부터 보호합니다.

- 동작 모니터링 기능 : 알려지지 않은 악성 프로그램이 의심스러운 행동을 했을 때 이를 탐지하여 작동을 차단합니다. 예를 들어, 랜섬웨어가 파일 암호화를 시작했을 때 그 행동을 탐지하여 프로세스를 중지 할 수 있습니다. 또한 암호화되어 버린 파일을 복원 할 수

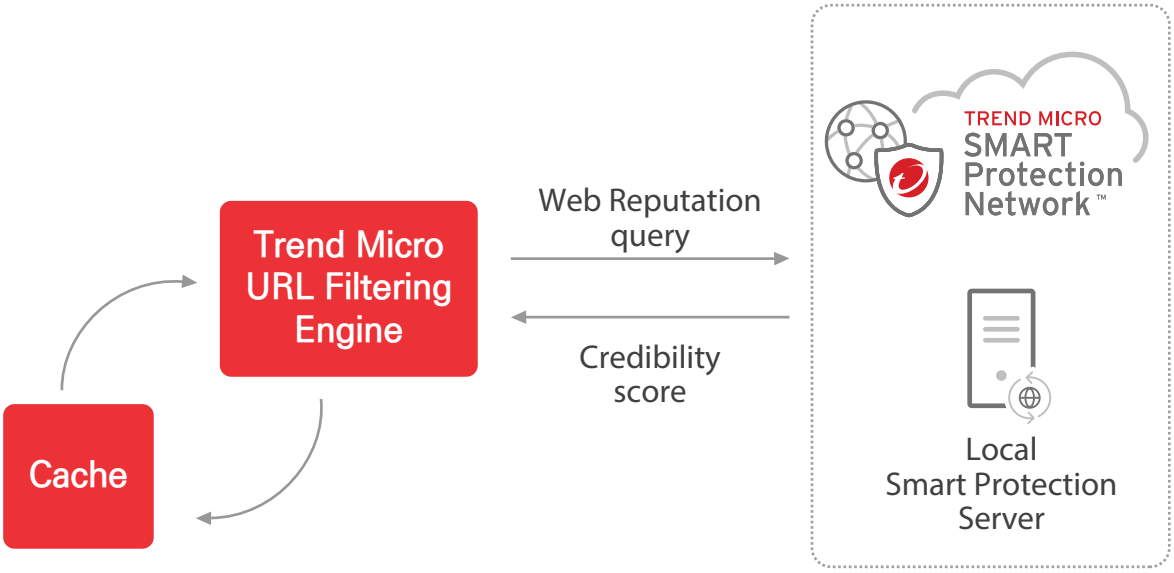
- 샌드 박스 연동 : 트렌드 마이크로의 다른 제품과 연동하여 알려지지 않은 위협을 발견 · 보호 할 수 있습니다.
  이 기능에서 찾아낸 의심스러운 파일을 Trend Micro 액티브 샌드 박스 제품 (Deep Dis-covery Analyzer)에 보내고 그 파일의 위험을 판정합니다. 위험이 높은 파일로 판명되면 통합 관리 도구 Trend Micro Control Manager를 통해 각 제품에 이 파일을 탐지 · 제거하기위한 사용자 정의 시그니처를 제공합니다.

CTD(Connected Threat Defense) 동작 흐름



• Web 평판 (Web Reputation)

서버가 Web 사이트에 액세스하는 등의 통신이 발생하는 경우 Trend Micro Smart Protection Network에 자동으로 질의(Query)를 합니다.
연결할 도메인, Web 사이트, Web 페이지가 악성으로 판단된 경우에는 접근 자체를 차단하여 악성 프로그램 서버에 감염 정보 유출 등을 방지 할 수 있습니다.



• 방화벽 (Firewall)

적정한 서버 운영에 필요한 포트 및 프로토콜을 통해 통신을 가능하게 하고, 그 이외의 포트 및 프로토콜은 모두 차단하여 서버에 대한 무단 액세스의 위험을 줄일 수 있습니다.

- 미세한 필터링 : IP 주소, MAC 주소, 포트 등을 기반으로 방화벽 규칙을 설정하여 트래픽을 필터링합니다. 네트워크 인터페이스마다 다른 정책을 설정할 수 있습니다.
- TCP 프로토콜 대응 : 전체 패킷 캡처를 지원하여 쉽게 발생하는 TCP, UDP ICMP 등의 방화벽 이벤트를 분석 및 판단할 수 있는 유용한 정보를 제공합니다.
- IP 프로토콜에 대응 : 전체 패킷 캡처를 지원하여 문제를 간단하게 해결합니다.
- Reconnaissance(정찰) 탐지 : 포트 스캔 등의 활동을 탐지합니다. ARP 트래픽과 같은 비 IP 트래픽을 제한 할 수 있습니다.

• Anti-Malware (백신)

취약점에 대응하여 해당 IPS / IDS 룰 '가상 패치'를 통하여 취약점을 노린 공격으로부터 서버를 보호합니다.

지원하는 취약점 탐지/차단 룰은 Windows, Linux, Solaris 등 주요 서버 OS 와 Apache, WordPress, BIND, Microsoft SQL, Oracle 등 100 개 이상의 애플리케이션과 미들웨어를 보호 합니다.

또한 지속적으로 Windows 업데이트에 대해 대응하는 IPS 룰 “가상 패치”를 업데이트하여 최신 취약점을 이용한 공격으로부터 Windows를 보호 할 수 있습니다.

모든 규칙은 차단 모드 (패킷을 차단 하는 모드)로 탐지 모드(이벤트만 기록하고 트래픽은 통과시키는 모드)를 선택 적용 가능합니다.

Deep Security의 도입에 따라 정상적으로 패킷을 차단 하는 등의 오탐이 우려되는 경우, 처음에는 탐지 모드로 구축하고 응용 프로그램의 동작 및 서비스의 이상이 없음을 확인 된 후

- Web 응용 프로그램 보호 룰 : SQL 인젝션, 크로스 사이트 스크립트 (XSS) 등의 Web 어플리케이션의 취약점을 노린 공격으로부터 보호 할 수 있습니다.

- 응용 프로그램 제어 룰 : 네트워크에 액세스하는 애플리케이션의 가시성을 높이고 제어합니다.
  이 룰은 네트워크에 액세스하는 악성 소프트웨어를 식별 또는 서버 취약점 이용을 줄이기

- 응용 프로그램 제어 룰 : 네트워크에 액세스하는 애플리케이션의 가시성을 높이고 제어합니다.
  이 룰은 네트워크에 액세스하는 악성 소프트웨어를 식별 또는 서버 취약점 이용을 줄이기

NAME	APPLICATION TYPE	PRIORI...	SEVERI...	MODE	TYPE
1000552 - Generic Cross Site Scripting(XSS) Prevention	Web Application Common	1 - Low	Critical	Prevent	Smart
1000608 - Generic SQL Injection Prevention	Web Application Common	1 - Low	Critical	Prevent	Smart
1002433 - Mass SQL Injection Script Insertion Attack	Web Application Common	2 - Normal	Medium	Prevent	Exploit
1002651 - YouTube Blog Multiple Remote Vulnerabilities	Web Application Common	2 - Normal	Medium	Prevent	Exploit
1002684 - Mass Hack Script Insertion Attack	Web Application Common	2 - Normal	Medium	Prevent	Exploit
1002743 - Mass SQL Injection Script Insertion Attack 2	Web Application Common	2 - Normal	Medium	Prevent	Exploit

[수많은 리눅스 커널 지원]

• 무결성 모니터링 (Integrity Monitoring)

디렉토리, 레지스트리 키 및 파일 등 운영 체제와 응용 프로그램의 중요한 파일을 모니터링하여 그 변화를 감지합니다.

- 다양한 파일 속성 검사 : 파일과 디렉토리의 내용, 속성 (소유자, 권한, 크기 등), 날짜 및 시간 스탬프 변경을 모니터링 할 수 있습니다. Windows 레지스트리 키 및 값 액세스 제어 목록 로그 파일의 추가, 변경, 삭제를 모니터링하고 경고 할 수 있습니다.

- 유연한 모니터링 지정 : 특정 사용자 환경에 맞게 감시 활동을 최적화 할 수 있는 유연성과 제어를 제공합니다. 여기에는 매개 변수 파일의 포함 / 제외, 파일 이름의 와일드 카드 지정 하위 디렉토리 포함 / 제외 지정 등이 있습니다.
  또한 자신의 요구 사항에 맞게 사용자 정의 규칙을 만들 수 있는 유연성도 있습니다.

• 로그 감사 (Log Inspection)

운영 체제 및 응용 프로그램 로그에서 보안 이벤트를 수집하고 분석하는 기능을 제공합니다.
보안 로그 모니터링 규칙을 설정하여 여러 로그 항목에 묻혀있는 중요한 보안 이벤트의 식별합니다.
이러한 이벤트는 SIEM 또는 중앙 집중화 된 로그 서버로 전송하여 관련 보고서를 작성하고 보관할 수 있습니다.

- 의심스러운 동작 탐지(로그 발생) : 사용하는 서버에서 발생했을 가능성이 있는 의심스러운 동작을 확인할 수 있습니다.
  Microsoft Windows, Linux, Solaris의 각 플랫폼 전체의 이벤트와 Web 서버, 메일 서버, SSHD, Samba, Microsoft FTP 등 응용 프로그램 이벤트 또한 사용자 지정 응용 프로그램 로그 이벤트를 수집하고 연결할 수 있습니다.

- **응용 프로그램 제어 (Application Control)**

서버에 설치된 응용 프로그램 검색하여 화이트리스트 방식으로 허용되지 않은 프로그램이 실행되었을 때 감지 · 차단하는 기능입니다.
알려지지 않은 악성 프로그램의 실행을 방지하고 서버의 용도를 제한하고 싶은 경우 등에 유용합니다.

- 유지 관리 모드 : 서버에 새 응용 프로그램을 추가하거나 이미 실행중인 응용 프로그램의 버전 업을 할 때 Deep Security 관리 콘솔에서 응용 프로그램 제어를 '유지 관리 모드' 로 변경하고 그 사이에 추가 변경 된 응용 프로그램을 허용하여 룰 세트에 포함 할 수 있습니다.

- API 연계 : 유지 보수 모드로 할 때, Deep Security Manager의 관리 콘솔에 로그인하지 않고도 API를 사용하여 유지 관리 모드로 적용 할 수 있습니다.
응용 프로그램이 수시로 변경 되는 경우 보안 담당자의 부담 감소를 목표로 설계가 가능합니다.

6. Trend Micro Deep Security 각 구성요소

- **Deep Security Manager (소프트웨어)**

Deep Security Manager(DSM)은 Web 기반의 강력한 중앙 관리 시스템입니다.
DSM은 데이터베이스를 사용하고 있으며, 보안 관리자가 수행하는 종합적인 보안 정책 생성 및 관리, 기록 (로그)을 집중적으로 관리합니다. 또한 상황을 파악하기 위한 대시 보드 및 보고서 작성, 서버에 대한 작업 적용 등 Deep Security Agent 의 모든 관리 작업을 수행합니다.

- **Deep Security Relay (소프트웨어)**

Deep Security 는 새로운 위협에 대응하기 위해 Deep Security 소프트웨어와 악성 프로그램의 패턴 파일 IPS 규칙 등을 매일 업데이트 해야합니다. Deep Security 시스템에서 구성 요소 패턴 파일 업데이트를 실행하는 것이 Relay 서버입니다. Relay 서버는 인터넷에서 최신 구성 요소 패턴 파일을 다운로드하고 Deep Security Agent 및 Deep Security VirtualAppliance 최신 구성 요소를 제공합니다. 따라서 Relay 서버는 반드시 하나를 설치 해야합니다. 또한 IPS 규칙은 Deep Security Manager 에서 제공됩니다.

- **Deep Security Agent (소프트웨어)**

Deep Security Agent (DSA)는 최소한의 자원으로 최대한의 보안을 제공하는 소프트웨어로 서버에 직접 설치되어 작동합니다.
Deep Security Agent는 네트워크 레이어에서 실행되는 방화벽 및 IPS / IDS (침입 방지) 엔진과 OS의 보호를 제공하는 변경 모니터 및 보안 로그 모니터링 기능은 지금까지 개별적으로 제공되고 있던 보안 기능을 일괄적으로 제공할 수 있습니다.

- **Deep Security Virtual Appliance (가상 어플라이언스)**

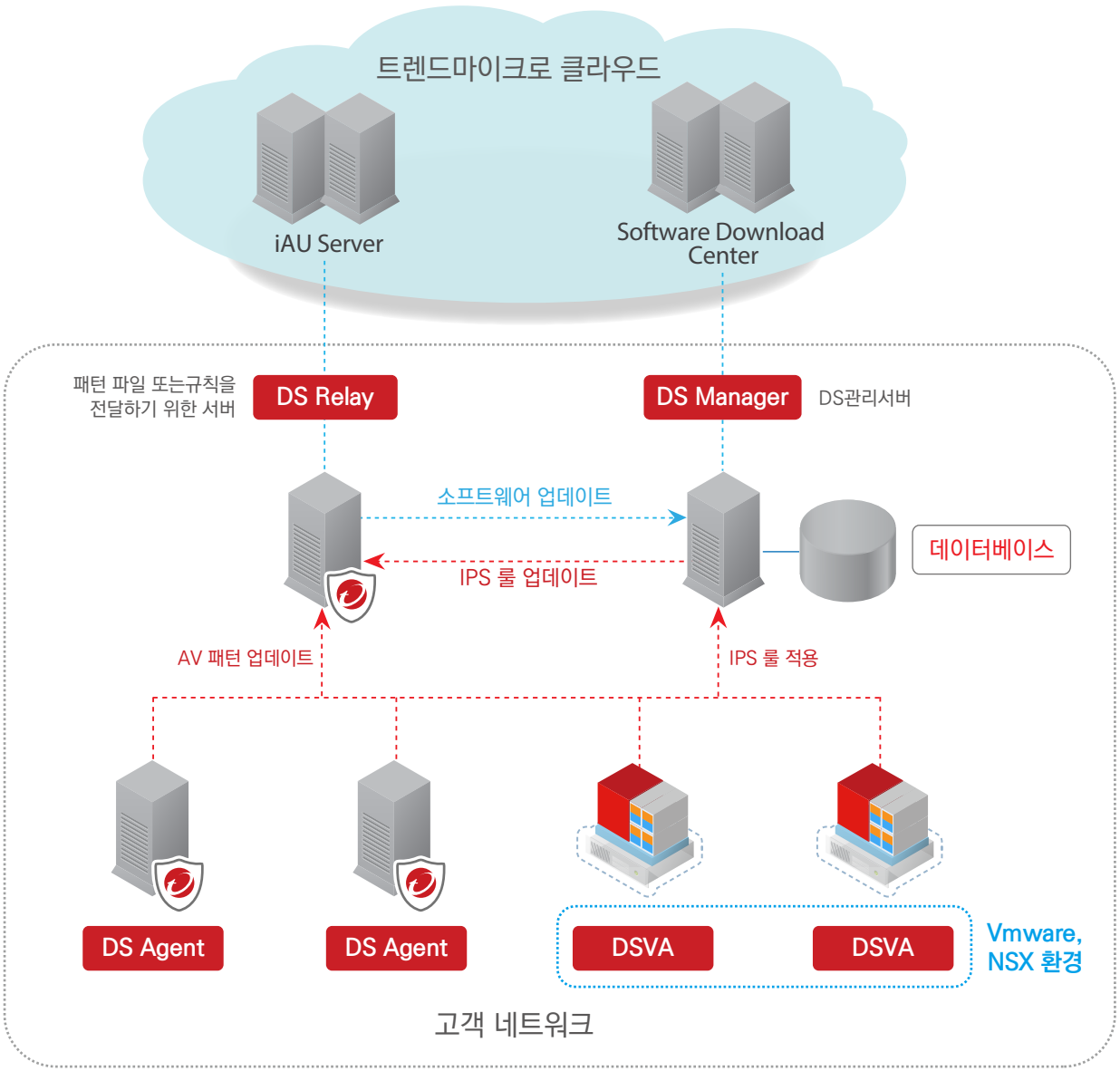
Deep Security Virtual Appliance (DSVA)는 가상화 환경에서 실행되는 보안 구성 요소입니다.
Agent가 직접 서버 OS에 설치되는 반면 Deep Security Virtual Appliance는 ESXi에서 실행되는
가상 머신으로 동작하고 게스트 OS에 소프트웨어를 설치할 수 없고, Deep Security의 보안 기능을 에이전트리스로 볼 수 있기 때문에 게스트 OS의 자원을 소비하지 않고 게스트 OS를 보호 할 수 있습니다.
또한 가상화 된 게스트 OS를 일괄로 보호 할 수 있는 장점도 있습니다. 또한 Web 평판, IPS / IDS, 방화벽, 변경 모니터링 에이전트없이 구현하려면 VMware NSX가 필요합니다.

- **Deep Security Agent (소프트웨어)**

Deep Security Agent (DSA)는 최소한의 자원으로 최대한의 보안을 제공하는 소프트웨어로 서버에 직접 설치되어 작동합니다.

Deep Security Agent는 네트워크 레이어에서 실행되는 방화벽 및 IPS / IDS (침입 방지) 엔진과 OS의 보호를 제공하는 변경 모니터 및 보안 로그 모니터링 기능은 지금까지 개별적으로 제공되고 있던 보안 기능을 일괄적으로 제공할 수 있습니다.

Deep Security 세부 구성 현황



7. Trend Micro Deep Security 설치 구성

Deep Security Manager를 설치하기 위한 다음과 같은 권장 하드웨어가 필요합니다.

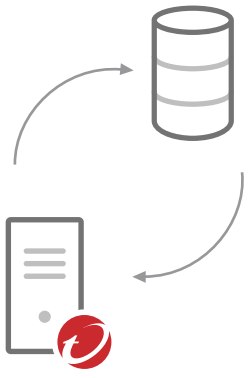
Deep Security Manager와 Relay Server는 Database가 필요합니다.

- Microsoft SQL Express 버전 구성은 테스트 용으로만 사용 가능합니다.(에이전트 10대 미만)

Deep Security Manager 설치 권장사양

- Quad core
- 1.5 GB (최소 사양)
  5 GB (권고 사양)
- 8 GB
- Internet
- Windows Server 2008, 2012, 2016
- Red Hat Enterprise Linux 6/7

Deep Security Manager 설치 권장사양



- Deep Security Manager 외 별도 구성 필요

- Quad core
  (Deep Security Manager 보다 사양이 같거나 더 고 사양 필요)
- 8-16 GB
- ORACLE 11g, 12C
- Microsoft SQL Server 2008, 2012, 2014

Deep Security Agent는 설치 모듈에 따라 권장 하드웨어가 필요합니다.

Deep Security Agent가 설치된 동일 Agent에 Relay 서버를 설치할 경우는 추가로 하드디스크 30GB가 필요합니다.

Deep Security Agent 설치 권장사양

최소구성	안티멀웨어 모듈 & DPI 모듈	Relay 서버 구성 시
128 MB	512 MB	추가 HDD 30GB
500 MB	1GB	

Deep Security Agent 지원 리눅스, 유닉스 플랫폼

Linux

- Red Hat Enterprise for Linux 5 (32-bit and 64-bit)
- Red Hat Enterprise for Linux 6 (32-bit and 64-bit)
- Red Hat Enterprise for Linux 7 (64-bit)
- Oracle Linux 5 (32-bit and 64-bit)
- Oracle Linux 6 (32-bit and 64-bit)
- Oracle Linux 7 (64-bit)
- CentOS 5 (32-bit and 64-bit)
- CentOS 6 (32-bit and 64-bit)
- CentOS 7 (64-bit)
- Debian 7 (64-bit)
- SUSE Linux Enterprise Server 11 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 12 (64-bit)
- CloudLinux 6 (32-bit and 64-bit)
- CloudLinux 7 (64-bit)
- Ubuntu 14 LTS (64-bit)
- Ubuntu 16 LTS (64-bit)
- With Relay functionality enabled: All 64-bit Linux versions above

Linux

Solaris

- Solaris 10 Update 1/13 Sparc
- Solaris 10 Update 1/13 x86 64bit
- Solaris 11.2/ 11.3 Sparc
- Solaris 11.2/ 11.3 x86 64bit

Solaris

Deep Security 설치 구성 단계

Trend Micro Deep Security 지원 정보 확인

Deep Security Agent 지원 정보 확인 – Linux 커널 정보

- 지원 커널 버전 정보 (주기적으로 업데이트 확인)
- 지원 커널 정보는 계속 변경(최신 커널 지원 등으로)되므로 제공된 사이트에서 조회

https://help.deepsecurity.trendmicro.com/11_0/on-premise/Get-Started/linux-kernel-support.html?redirected=true

Deep Security Agent 버전 별 다운로드 사이트

http://downloadcenter.trendmicro.com/

Deep Security Agent 플랫폼 별 기능 지원 리스트

https://help.deepsecurity.trendmicro.com/supported-features-by-platform.html

8. Trend Micro Deep Security 기능 비교

- Deep Security 타사 비교

Capabilities		Deep Security	Legacy Security		AV Niche Players		Network
			S사	M사	SP사	K사	P사
Security Capabilities	Anti-Malware	★★★	★★★	★★★	★★★	★★★	☆☆
	Application Visibility and Control	☆	☆☆	☆☆			
	IDS/IPS	★★★	☆	☆		☆	★★★
	Firewall	☆☆	☆☆	☆☆		☆	★★★
	File Integrity Monitoring	☆☆	☆☆	☆☆			
	Event Monitoring	☆☆	☆☆	☆☆			
	Vulnerability Assessment	☆		☆☆			★★★
Management & Deployment	Programmability & Automation	★★★	☆☆	☆☆			★★★
	Hybrid Environment Support	★★★	☆	☆			
	Multi-tenant (Service Provider)	★★★					
	Agent Protection Architecture	★★★	★★★	★★★	★★★	★★★	
	Security Management API	★★★				★★★	
	Agentless (Virtual Appliance) Option	★★★	☆☆	☆☆			
	VMware vRealize Operations Integration	★★★					
Virtual Platform Support	VMsafe - Network	★★★				★★★	
	Vshield - Host	★★★		☆☆		★★★	
	NSX	★★★					
	Hyper-V (Agent-based)	★★★	☆☆	☆☆	☆☆	☆☆	

9. Deep Security 를 통한 Compliance 대응

- Compliance 대응 (PCI-DSS)

PCI	Responsibility
Install and maintain a firewall configuration to protect cardholder data	Shared
Do not use vendor-supplied defaults for passwords or other security parameters	Shared
Protect stored cardholder data	Shared
Encrypt transmission of cardholder data	User
use and regularly update anti-virus software	User
Develop and maintain secure systems and applications	Shared
Restrict access to cardholder data by business need to know	Shared
Assign a unique ID to each person with computer access	Shared
Restrict physical access to cardholder data	Cloud Provider
Track and monitor all access to network resources and cardholder data	Shared
Regularly test security systems and processes	Shared
Maintain a policy that addresses info security for all personnel	Shared

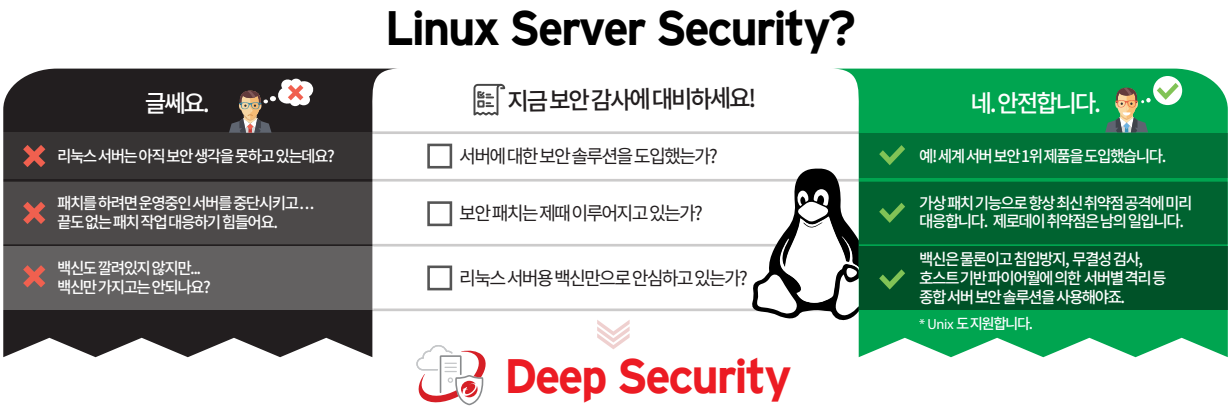
10. Trend Micro Deep Security 리눅스 AV 기능 비교

- Deep Security AV (Linux) 비교

기능	Trend Micro Deep Security	Clam AV (오픈 소스)
검색 지원 범위 및 구성요소		
안티 바이러스 & 안티 스파이웨어	O	O
웹 검증 기능 및 URL필터링 (WRS)	O	X
동작 모니터링 및 치료 기능(Clean) – 운영체제 또는 어플리케이션에 대한 비정상적인 수정의 행위	O	X 치료 기능 없음
웹 기반 콘솔	O	X
S/W구성 요소	관리서버 + 에이전트	Stand-Alone
클라우드 방식 검색		
클라우드 기반 패턴 지원(Smart Scan)	O	X
백신 프로그램 설치, 구성		
관리 서버 운영	O	X
Stand-Alone 구성(에이전트 만 구성)	O	X
관리 서버 1대당 관리 가능한 에이전트 수	약 5,000대	–
백신 프로그램 관리		
중앙에서 실시간/수동/예약 검색 설정	O	X
위젯 형태의 대시보드	O	X
중앙에서 업데이트 상태, 백신 서비스 상태 등의 확인	O	X
바이러스 패턴 및 엔진 업데이트/업그레이드		
중앙서버에서 자동으로 패턴/엔진 배포 기능	O	X
업데이트 에이전트(DSR)를 통하여 중앙관리 서버의 업데이트 부하를 분산	O	X
바이러스 검색 및 치료, 예방		
격리된 악성코드를 중앙관리 콘솔에서 복원	O	X
랜섬웨어가 파일을 암호화하는 행위를 탐지 및 중지	O	X
기타		
리눅스 패턴 탐지 개수	2017년 리눅스 악성코드 26,000개 이상 탐지 (트렌드마이크로 자료)	–
바이러스, 운영, 로그 등 운영 (로그 관리)	O	X
리눅스, 유닉스 지원	다양한 리눅스 버전 지원 솔라리스 수동 백신	한정적인 리눅스 버전 지원 솔라리스 만 지원

리눅스 서버 보안? Deep Security!

리눅스 보안에 최적화된 솔루션 – Deep Security



Deep Security 지원 리눅스 플랫폼 (업계 최대 플랫폼 지원)

TREND MICRO™ 트렌드마이크로

트렌드마이크로
(우 06176) 서울특별시 강남구 영동대로 416 KT&G타워 3층
TEL. 02-561-0990
FAX. 02-561-0660
sales@trendmicro.co.kr