Deep Security

리눅스(Linux) 서버 보안

한국트렌드마이크로

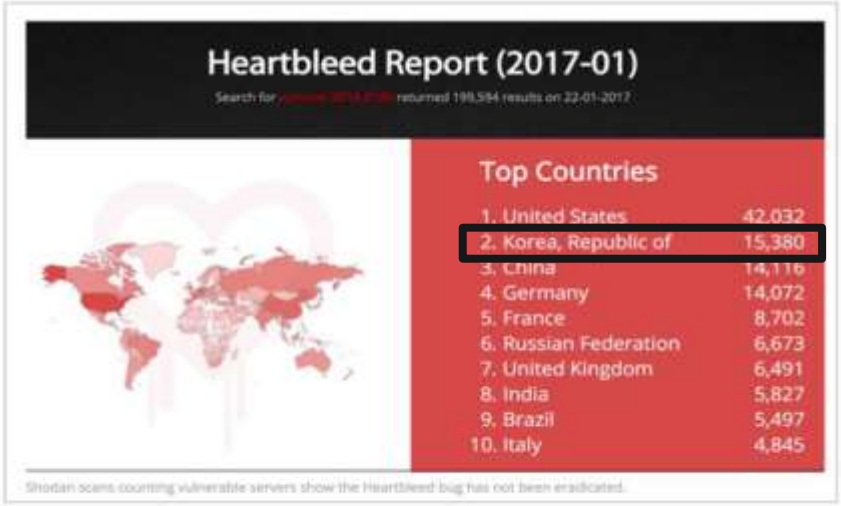
목차

- 리눅스 서버 위협 요소
- 리눅스 서버 위협 분석 시나리오
- 리눅스 서버 통합 보안 솔루션
- 리눅스 서버 보안 차별화

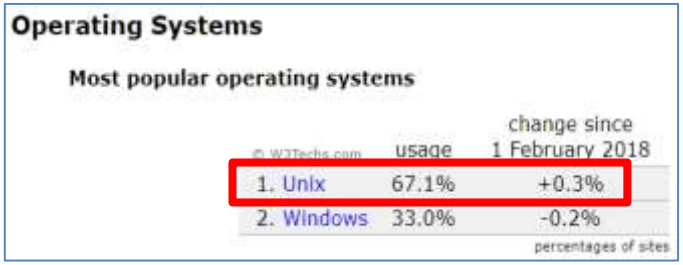
리눅스 서버 위협 요소

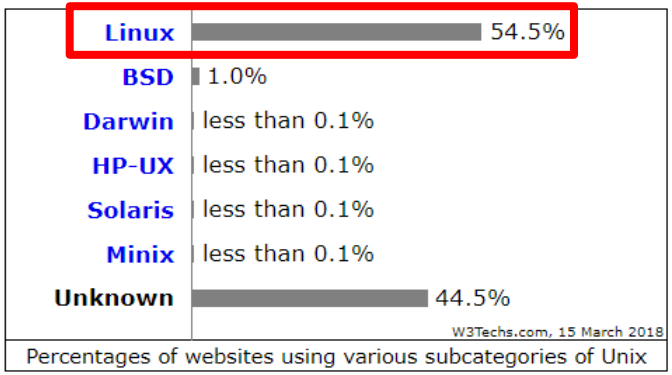
리눅스 서버 보안의 필요성

- 67.1%의 웹 서버가 유닉스/리눅스 서버(2018년 2월 1일 by W3Techs)
- 전체 유닉스 계열 서버 중 리눅스 서버가 절반 이상(2018년 2월 1일 by W3Techs)
- 현재 약 180,000 서버가 Heartbleed, Shellshock 취약점 보유

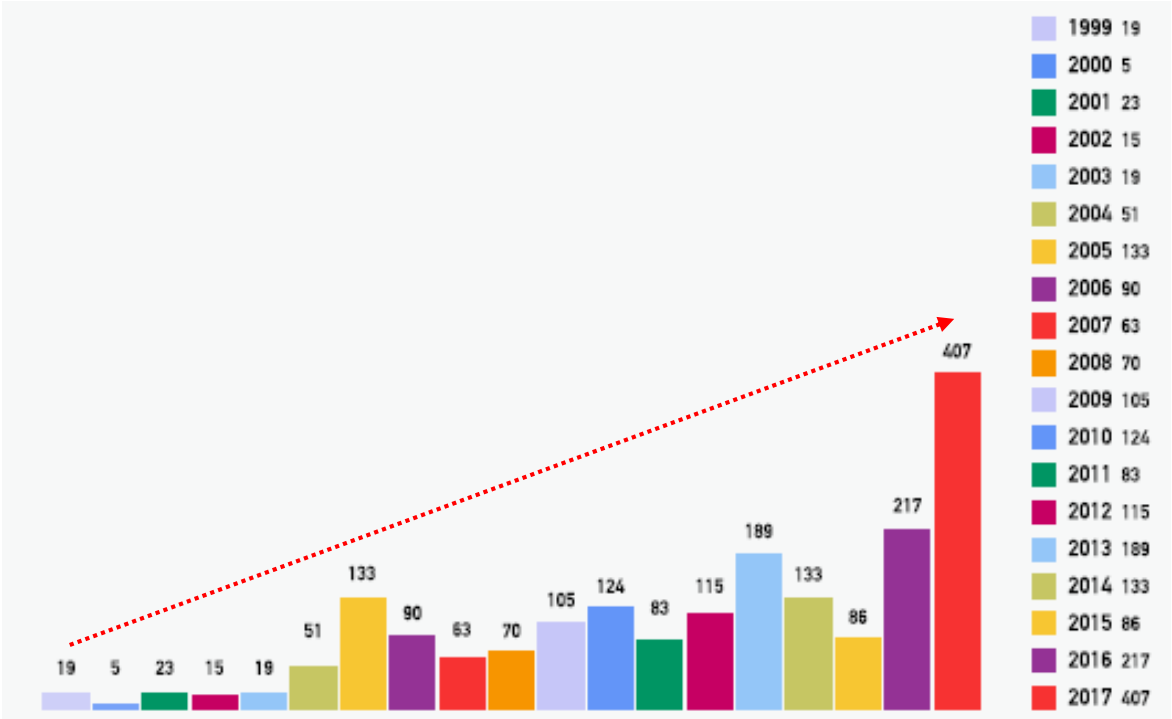


Source: Shodan, January 2017





리눅스 서버 취약점 증가



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

리눅스 서버 악성코드 동향

리눅스 악성코드 탐지

김인순 insoon@
보안 전문기자

몸값 13억원 지불한 6월부터 급증
지난해 악성코드 2만5895개 달해
취약점 늘어나도 제때 패치 안 돼
전용백신·호스트 방화벽 설치 필요

지난해 리눅스 운용체계(OS)를 노린 악성코드가 2만5000개가 넘게 발견됐다. 리눅스 OS 취약점이 계속 늘어나는데 패치는 제때 이뤄지지 않는다. 제2의 인터넷나야나나, 애플랜타시 마비 사태가 반복될 수 있어 대책 마련이 시급하다.

지난해 6월 10일 웹호스팅 기업 인터넷나야나는 해킹 후 리눅스 랜섬웨어에 감염돼 13억원이라는 막대한 몸값을 지불했다. 인터넷나야나가 호스팅하던 서버 153대가 랜섬웨어에 감염돼 5496개 홈페이지가 중단된 지 1년이 지났지만 국내 리눅스 보안은 여전히 초기 상태다.

한국트렌드마이크로에 따르면 지난해 보고된 리눅스 악성코드가 2만5895개에 달한다. 인터넷나야나 사태가 발생한 6월 리눅스 악성코드가 5721개로 급증한 후 대당 1000개가 넘게 발견됐다. 리눅스 OS 취약점도 계속 보고된다. 한국인터넷진흥원(KISA)이 내놓은 2018년 1분기 사이버 위협동향보고서에 따르면 리눅스 OS 취약점이 169개에 달한다. 취약점 발견은 늘어나는 데 패치가 되지 않아 사이버 위협에 그대로 노출됐다.

취약한 시스템을 검색하는 쇼단에 따르면 2014년 4월 발견된 최악의 보안 취약점 '하트블

리드(CVE-2014-0160)'를 패치하지 않은 톱 10위 국가 중 한국이 8위를 차지했다. 리눅스 서버는 취약점 발견이 많지만 가용성 문제로 업데이트가 제때 이뤄지지 않는다. 해커는 알려진 취약점만 이용해도 서버를 공격한 후 랜섬웨어를 감염시키고 몸값을 요구할 수 있다.

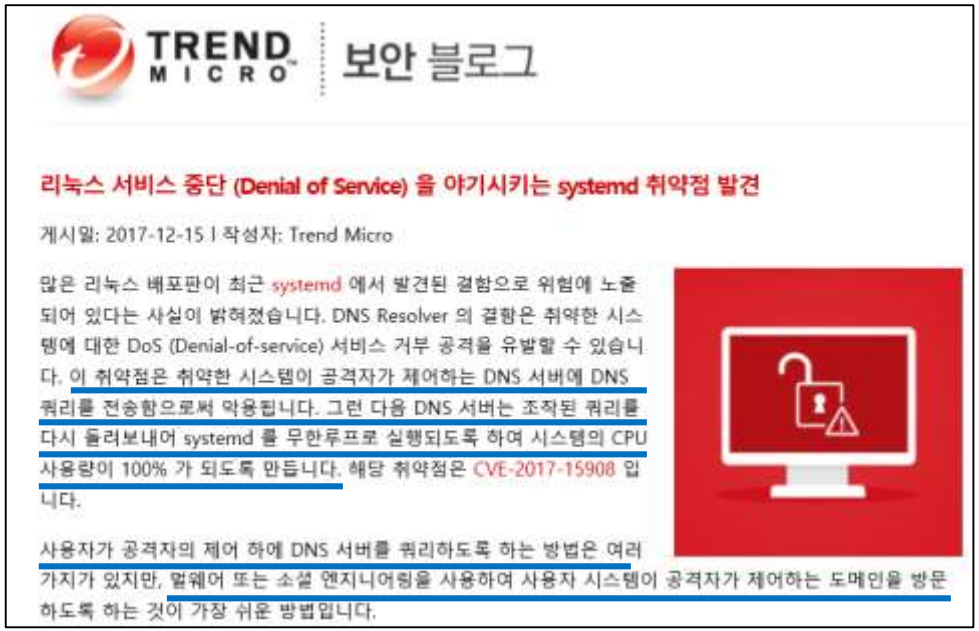
국내 기업과 기관은 운영비용이 적고 기술 적용 자유도가 높은 리눅스 도입을 늘렸다. 생산, 제조, 금융 등 각 분야에서 도입이 줄을 이었다. 사물인터넷(IoT), 인공지능(AI), 빅데이터, 클라우드 플랫폼으로 주목받으며 도입이 확대될 전망이다. 리눅스 채택이 늘면서 이를 표적한 사이버 공격도 함께 증가했다.

리눅스 악성코드는 계속 늘어나는데 리눅스 서버 전용 백신 사용이 미흡하거나 보안 패치가 제때 이뤄지지 않는다. 일부 기업과 공공기관은 오픈소스 백신을 리눅스 서버에 설치했다. 리눅스 서버 보안에 체계적 대응 없이 임시방편을 도입했다.

박상현 한국트렌드마이크로 대표는 "3월 미국 애틀랜타 도시를 마비시킨 샘샘 랜섬웨어 공격이 국내 지방자치단체에 발생할 수 있다"면서 "애틀랜타시처럼 일주일 이상 도시 업무가 마비돼 시민이 불편을 겪을 수 있다"고 설명했다.

이어 "대량의 리눅스 서버를 데이터센터 한 곳에서 관리할 때 외과 네트워크 보안에만 의존할 것이 아니라 전용 백신과 호스트 방화벽 등을 설치해야 제2의 나야나 사태를 막을 수 있다"면서 "서버 운영을 중단하지 않으면서 패치한 것과 같은 기능을 제공하는 가상패치 등도 제안한다"고 덧붙였다.

리눅스 시스템 대상 위협 사례



TREND MICRO 보안 블로그

리눅스 서비스 중단 (Denial of Service) 을 야기시키는 systemd 취약점 발견

게시일: 2017-12-15 | 작성자: Trend Micro

많은 리눅스 배포판이 최근 systemd 에서 발견된 결함으로 위험에 노출되어 있다는 사실이 밝혀졌습니다. DNS Resolver 의 결함은 취약한 시스템에 대한 DoS (Denial-of-service) 서비스 거부 공격을 유발할 수 있습니다. 이 취약점은 취약한 시스템이 공격자가 제어하는 DNS 서버에 DNS 쿼리를 전송함으로써 악용됩니다. 그런 다음 DNS 서버는 조작된 쿼리를 다시 돌려보내어 systemd 를 무한루프로 실행되도록 하여 시스템의 CPU 사용량이 100% 가 되도록 만듭니다. 해당 취약점은 CVE-2017-15908 입니다.

사용자가 공격자의 제어 하에 DNS 서버를 쿼리하도록 하는 방법은 여러 가지가 있지만, 멀웨어 또는 소셜 엔지니어링을 사용하여 사용자 시스템이 공격자가 제어하는 도메인을 방문하도록 하는 것이 가장 쉬운 방법입니다.

- **취약점 분석**
- RFC 4034에 정의된 NSEC (Next Secure) 레코드는 DNS Security Extensions (DNSSEC) 에 추가된 새로운 유형의 리소스 레코드 중 하나인데, NSEC bitmap에서 pseudo-type을 표현하는 비트를 처리하는 과정에서 발생

- **대응 방안**
- 들어오는 DNS 응답 트래픽을 모니터링하고 응답 섹션의 DNS RR 에 DNS 및 NSEC RR 을 정의하는 RFC 4034 Section 4에 지정된 타입의 레코드가 포함되어 있는지 검색
- 첨부된 bitmap 이 처리되고 pseudo-types 가 포함되어 있다면 차단

리눅스 시스템 대상 위협 사례

Cryptocurrency Miner Distributed via PHP Weathermap Vulnerability, Targets Linux Servers

'합법적 대규모 암호 화폐 채굴 운영업체는 악용 여부 구분없이 채굴에 사용되는 전자기기에 투자'
'Cacti's Network Weathermap plug-in의 오래된 PHP 취약점인 CVE-2013-2618을 이용해 Linux Web Server 대상으로 Shell 스크립트 다운로드 및 실행하여 몰래 채굴'

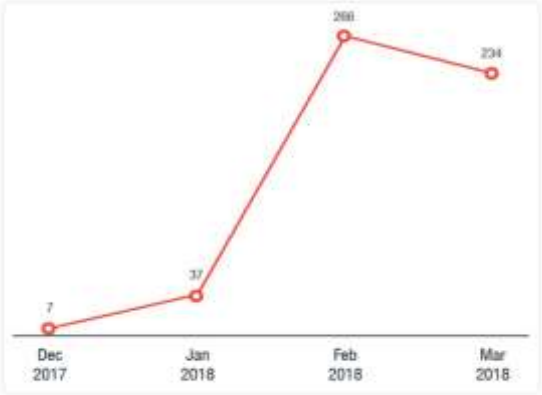


Figure 1. Network intrusion attempts observed from the cryptocurrency-mining campaign (December 2017 to mid-March 2018)

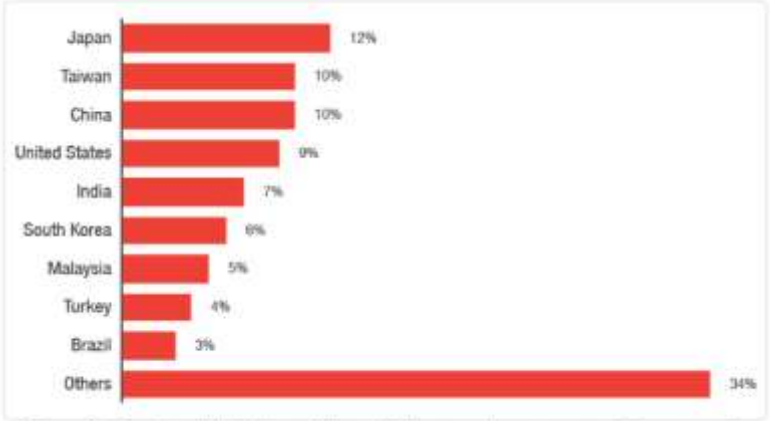


Figure 2. Country distribution of the malicious cryptocurrency-mining campaign

2017’ Major Player (랜섬웨어)

WannaCry

- 약 US$4 billion 피해

Petya

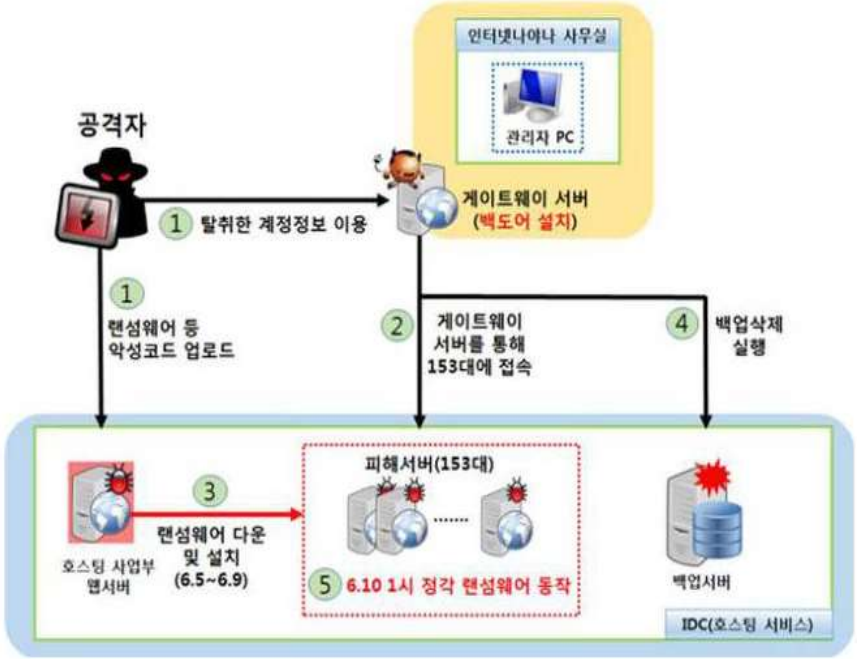
- 약 US$300 million 피해

Bad Rabbit

- 러시아 및 동유럽의 미디어 기업들과 인프라 서비스 중단 피해

리눅스 시스템 대상 위협 사례

EREBUS 랜섬웨어



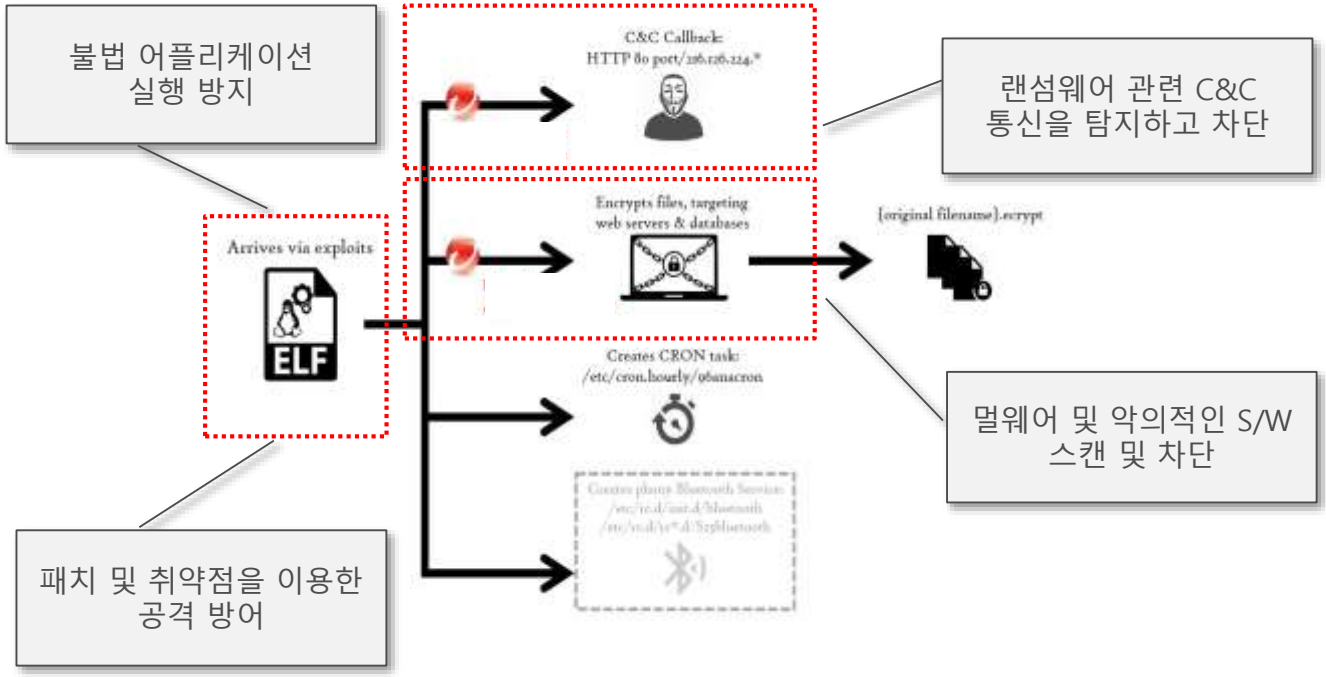
- 153 리눅스 서버 감염
- 3400 고객 웹사이트 감염
- 433개의 파일 타입 암호화
- 13억 비트코인 요구
- 2016년 9월 악성 광고에 처음 등장한 랜섬웨어 사용
- 2017년 초에 리눅스 용 악성코드 발견

- 인가된 관리자 PC 해킹을 통한 서버계정정보 이용

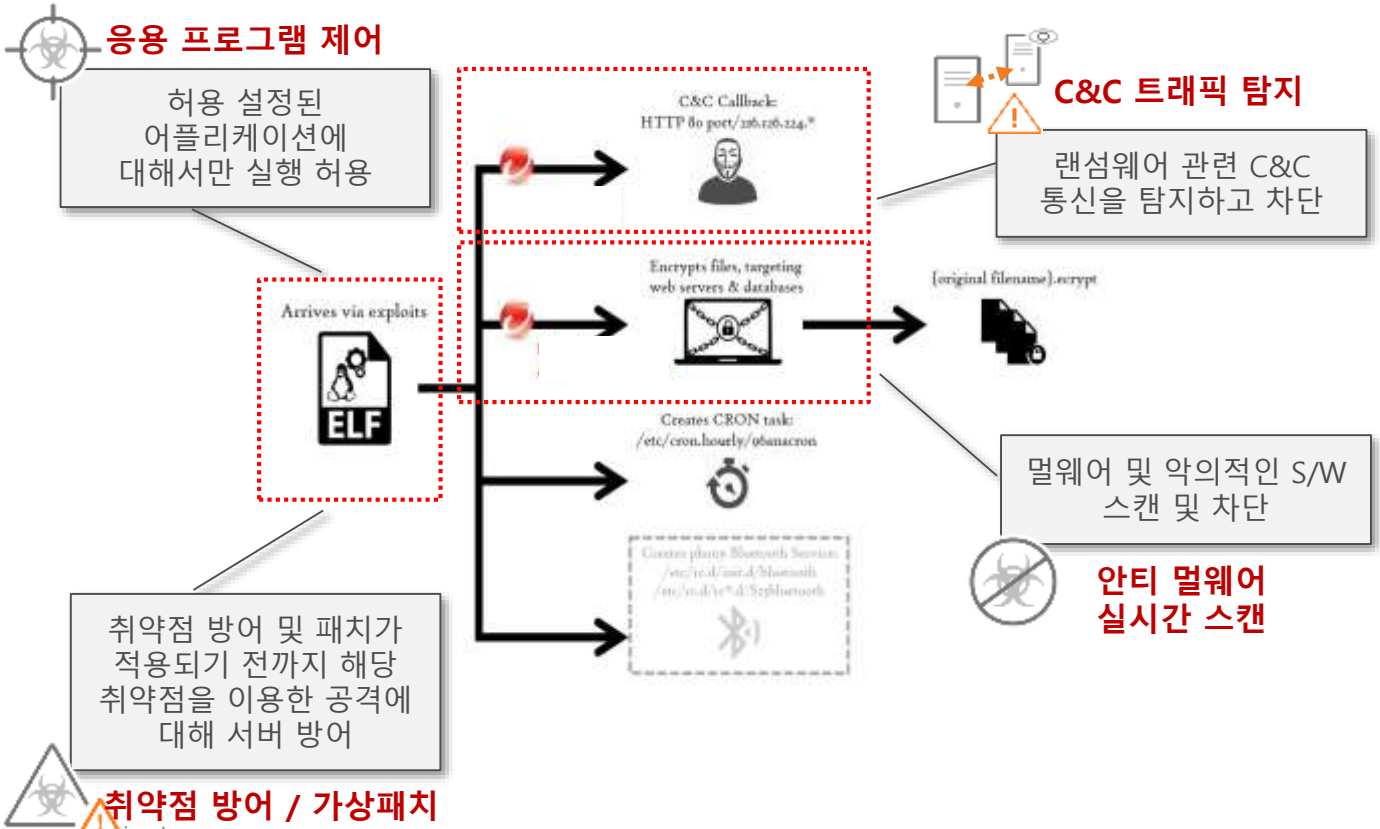
리눅스 서버 위협 분석 시나리오

리눅스 보안 기능 필요성

EREBUS 랜섬웨어



리눅스 보안 기능 필요성



리눅스 보안 기능 필요성

리눅스 서버 보안 제품 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?

리눅스 서버 통합 보안 솔루션

리눅스 서버 보안 주요 기능 필요성

1. 실시간 리눅스 백신 (랜섬웨어, 악성 URL 방어)

2. 취약점 방어를 위한 가상 패치

3. 무결성 모니터링, 응용 프로그램 제어

1. 실시간 리눅스 백신 (랜섬웨어, 악성 URL 방어)

안티멀웨어

알려진 멀웨어
탐지 및 차단

멀웨어와 표적 공격 차단

행위분석 머신러닝

의심스러운 파일 및
행위 탐지

랜섬웨어 탐지 및 차단(ex: WCRY)

Zero-day 공격 방어

웹 평판

악성 URL로부터 서버를
보호 하기 위해 웹
사이트 평판 탐지, 차단

악성 URL 및 C&C 로 부터 서버 보호

TREND MICRO

1. 실시간 리눅스 백신 (랜섬웨어, 악성 URL 방어)

안티 멀웨어 (백신)

실시간 검색
예약 검색
수동 검색
동작 감지 기능에 의한 자기 방어 기능

[Web 평판(Reputation) 서비스]

Web 평판은?
Web에서 위협의 출처 인 악성 URL에 대한 액세스를 미연에 차단합니다.
트렌드 마이크로의 노하우가 담긴 'Smart Protection Network "기능의 하나입니다.

Linux 버전 실시간 백신 지원
(자세한 버전 확인은 트렌드마이크로 문의)
예약 검색, 수동 검색, 실시간 검색 지원

백신 기능

- 악성코드와 스파이웨어/그레이웨어를 탐지하고 치료
- 운영체제에 따라서 지원 기능이 다름

클라우드 패턴 사용

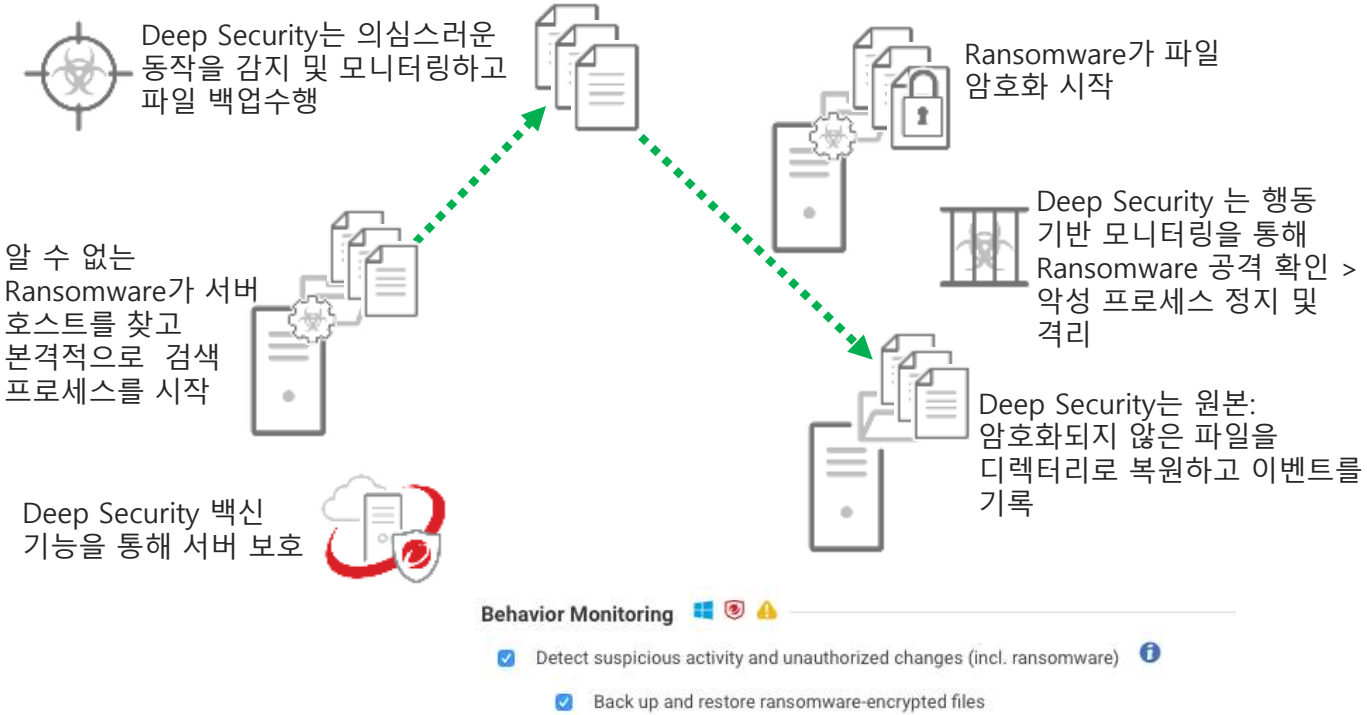
- 파일 평판 조회(WRS)와 웹 평판 조회(WRS)에 클라우드 패턴 방식을 사용

다양한 백신 옵션 설정

- 검색 제외 설정, 격리된 악성코드 복원 및 다운로드, 수동/예약 검색 시 CPU사용량 제한, 압축파일 검색 레벨 등 다양한 백신 정책을 설정

1. 실시간 리눅스 백신 (랜섬웨어, 악성 URL 방어)

- 랜섬웨어 지능형 대응



1. 실시간 리눅스 백신 (랜섬웨어, 악성 URL 방어)

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

Platforms

- Windows (10.3 Agents)
- Red Hat Enterprise Linux (10.3 Agents)
- CentOS (10.3 Agents)
- Oracle Linux (10.3 Agents)
- SUSE Linux (10.3 Agents)
- Ubuntu (10.3 Agent)
- Debian (10.3 Agent)
- Cloud Linux (10.3 Agent)
- Amazon (10.3 Agents)
- Azure (10.3 Agents)
- Agentless (NSX) (10.3 Agents)

Anti-Malware Enabled

PLATFORM	STATUS	POLICY
Ubuntu Linux 16 (64 bit)	Managed (Online)	None
Ubuntu Linux 16 (64 bit)	Managed (Online)	None
Ubuntu Linux 16 (64 bit)	Managed (Online)	None
Red Hat Enterprise 7 (64 bit)	Managed (Online)	None
Ubuntu Linux 16 (64 bit)	Managed (Online)	None
Red Hat Enterprise 6 (64 bit)	Managed (Online)	None

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

2. 취약점 방어를 위한 가상 패치

침입방지

네트워크와
어플리케이션에
대한 위협 방어

취약점 스캔

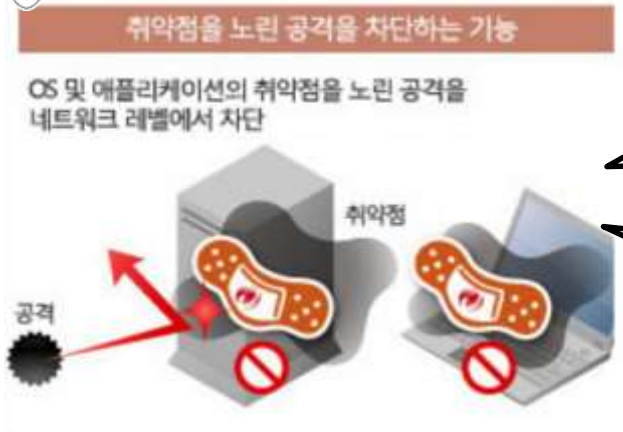
자동화된 취약점 감사
및 방어 룰 적용

- OS와 어플리케이션에 대한 취약점 방어
  (ex: Struts 2, Shellshock)
- 랜섬웨어 탐지 및 차단 (ex: WCRY)
- 긴급 패치에 대한 요구 감소
- EOS 시스템과 어플리케이션 방어

2. 취약점 방어를 위한 가상 패치

- OS 나 응용 프로그램의 취약점 (보안 취약점)을 통한 공격 패킷을 탐지하고 방어하는 기능 (**가상 패치**)
- SQL 인젝션과 크로스 사이트 스크립팅(XSS) 등의 Web 어플리케이션의 취약점을 통한 공격 패킷을 탐지하고 방어하는 기능 (**IPS 룰 기반**)

가상패치는?	취약성을 수정하는 보안 패치를 설치하는 대신 취약성을 악용하는 공격을 차단하고 가상 패치의 역할을 제공합니다.



포인트 1 :
소프트웨어 코드
레벨에서의 수정을
실시하지 않기 때문에
실행중인 시스템에
영향이 적다.

포인트 2:
Windows와 Linux 같은
OS뿐 아니라 다양한
애플리케이션의 가상패치가
트렌드 마이크로로부터
제공된다.

	Vulnerabilities Covered in and after 2014 (approx.)	Before 2014 (approx.)	Total
and Core Services	80	230	310
	114	472	586
Application Servers	255	319	574
Web Console/Management Interfaces	113	453	566
Database Servers	10	218	228
DHCP, FTP, DNS servers	9	82	91

Deep Security 취약점 대응
(CVE기준)

2. 취약점 방어를 위한 가상 패치

수집하는 정보

- 설치 프로그램 정보
- 파일 정보
- 실행되는 프로세스
- 환경 변수
- 열려있는 포트
- 레지스트리 (Windows 만 해당)
- 서비스 (Windows만 해당)

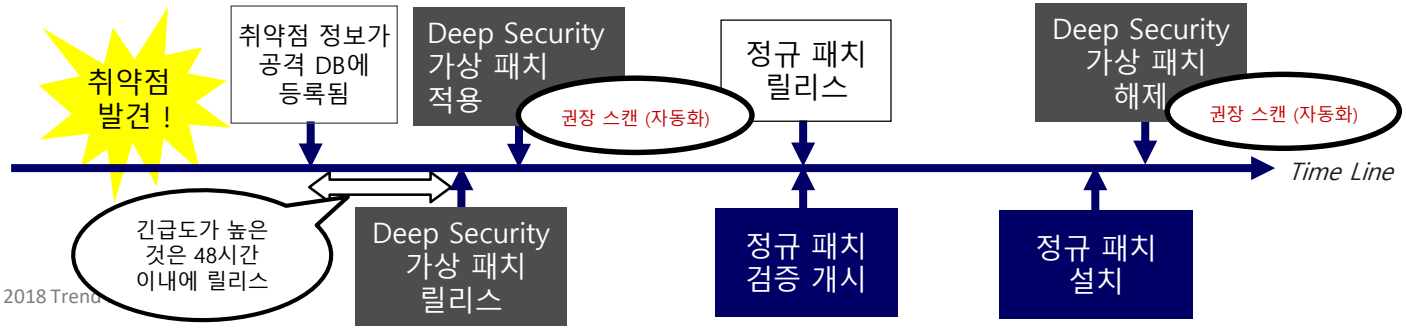
응용 프로그램 버전 / 보안 패치의 적용 상황

권장하는 룰의 선별 자동 적용

2. 취약점 방어를 위한 가상 패치

권장 스캔	서버에 설치된 Deep Security Agent가 서버에 설치된 애플리케이션의 정보를 수집하고 필요한 가상 패치를 자동 선택/적용

권장 스캔을 이용한 패치 관리



3. 무결성 검증, 응용 프로그램 제어

어플리케이션
컨트롤

서버에서의 변경
방지 및 Lock down
(whitelisting)

무결성
모니터링

의심스럽거나
인가되지 않은 변경
탐지 – 파일, 포트,
레지스트리 등

랜섬웨어와 같은 악성 공격 차단

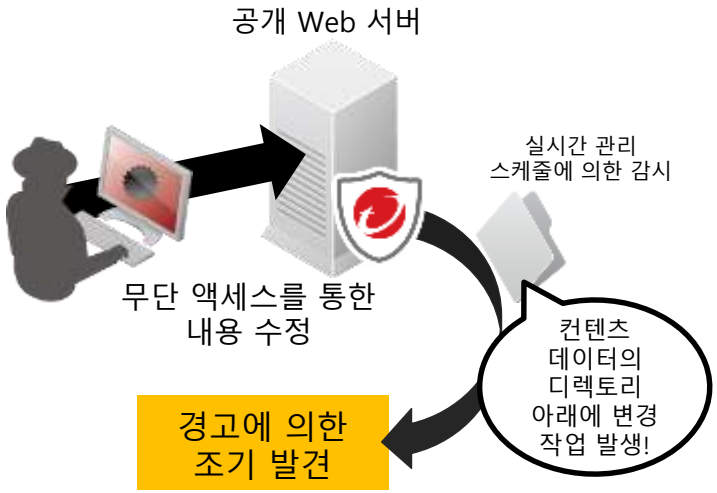
DevOps 와 CI/CD Pipeline 연계

공격 포인트 감소

IOCs (indicators of compromise)
탐지 및 알림

3. 무결성 검증, 응용 프로그램 제어

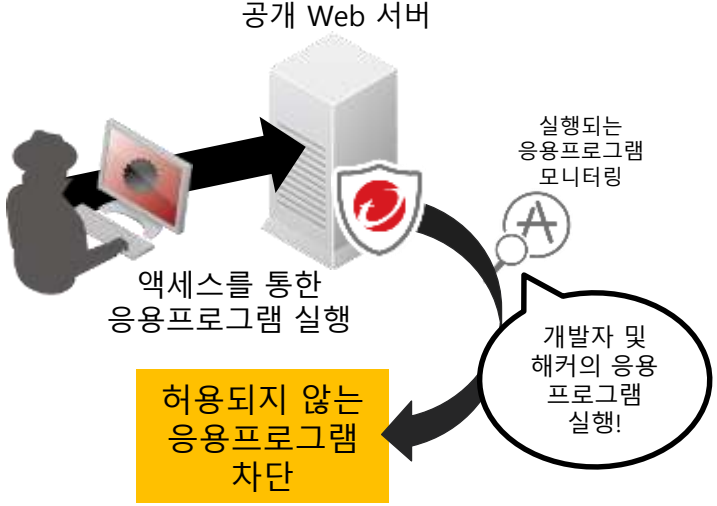
무결성 모니터링 (예)



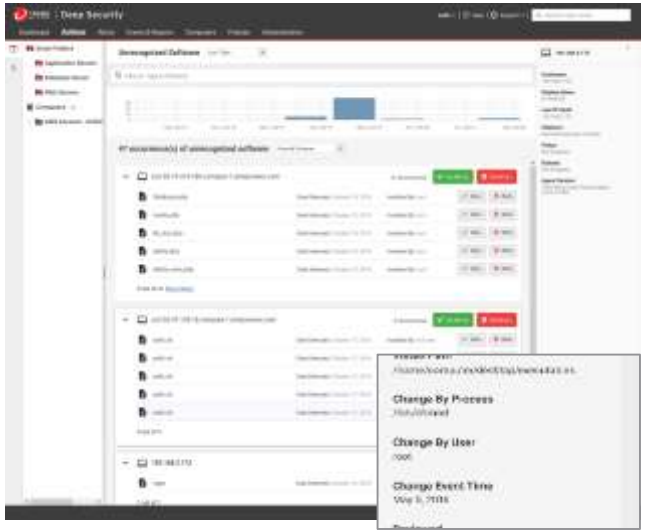
파일 (파일 속성 포함), 디렉토리, 레지스트리, 프로세스 등의 변화를 감지 할 수 있습니다.

3. 무결성 검증, 응용 프로그램 제어

응용프로그램 제어(예)



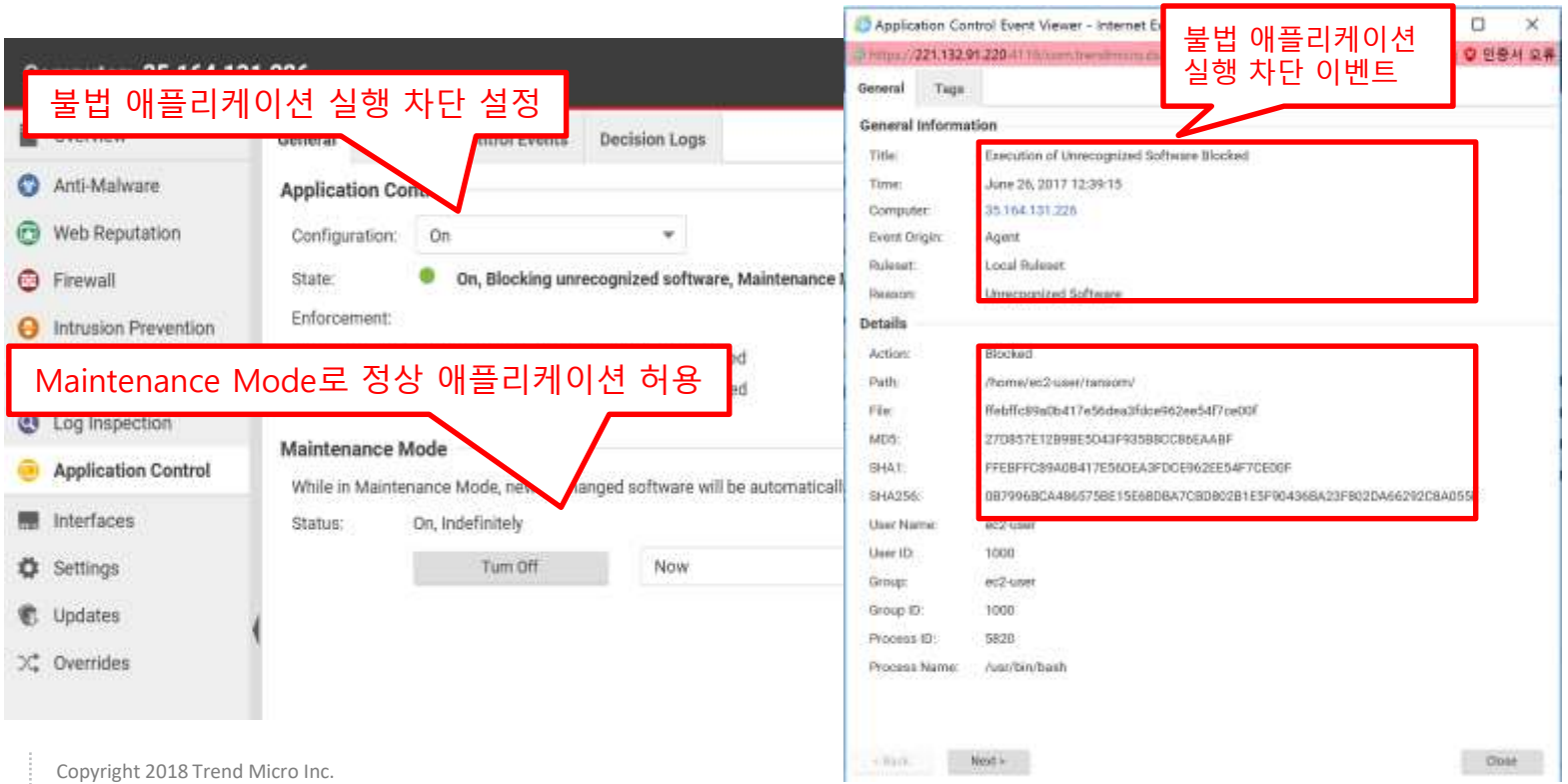
- 일반 실행 파일의 바이너리와 라이브러리 외에 Java, PHP, Python 등 주요 Web 어플리케이션 프레임 워크에도 대응



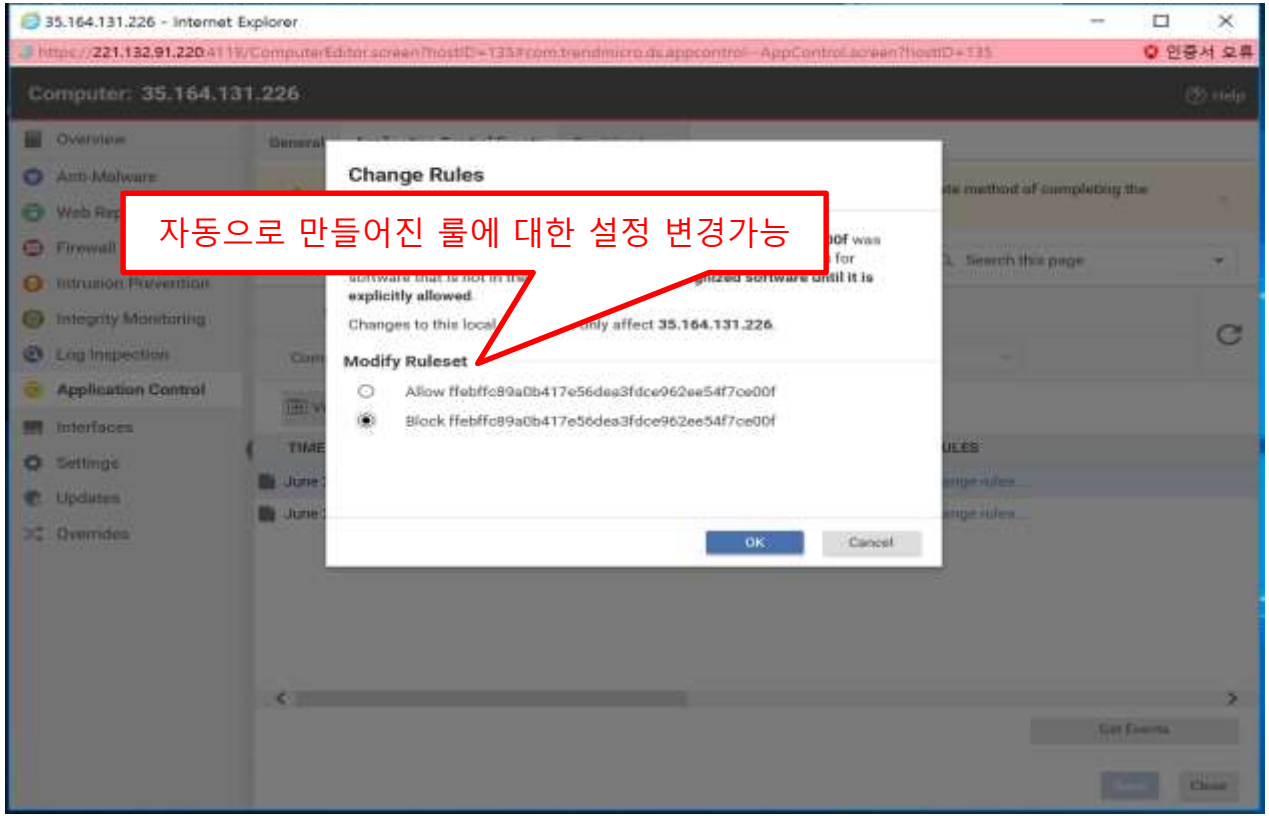
- DSA 호스트에서 실행되는 응용 프로그램을 모니터링
  - 화이트리스트 / 블랙리스트 방식 운영 가능
  - 감지(로그) 또는 블록 선택 가능

3. 무결성 검증, 응용 프로그램 제어

- 불법 애플리케이션 실행을 차단(Default)하고 이벤트를 발생하여 허가여부를 결정



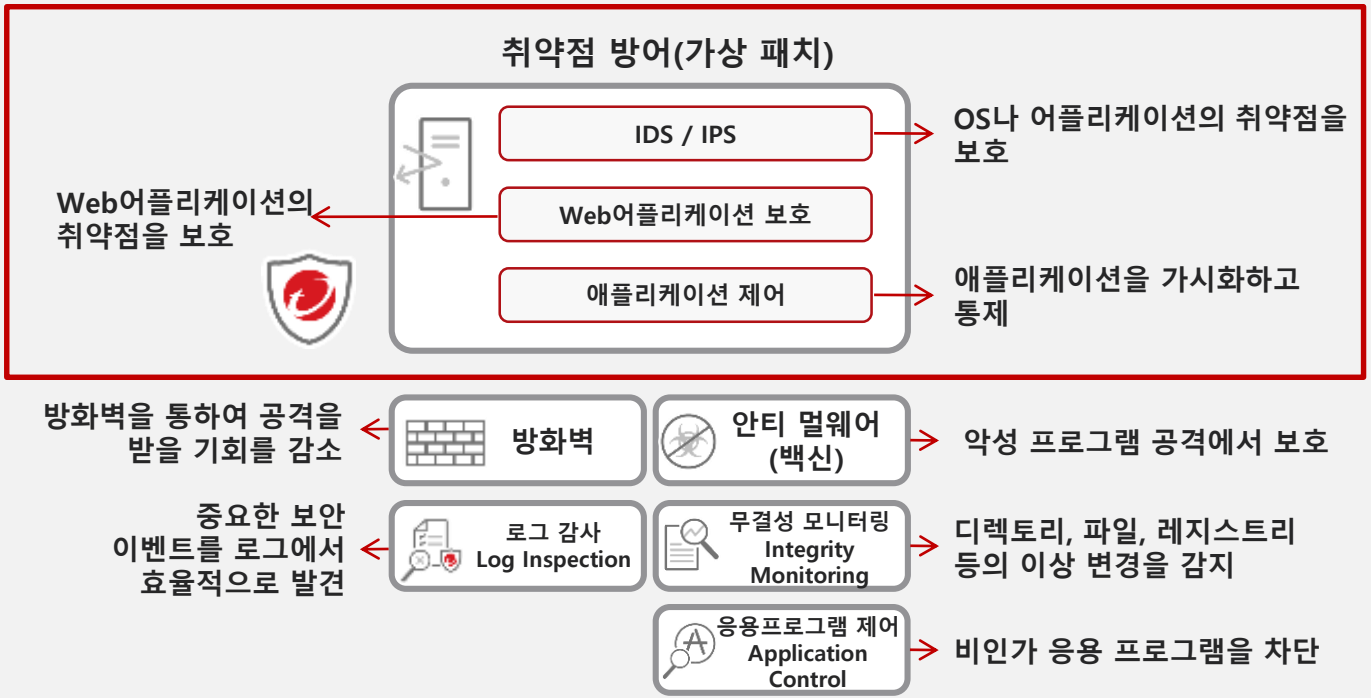
3. 무결성 검증, 응용 프로그램 제어



리눅스 서버 통합 보안 솔루션

리눅스 서버 통합 보안 솔루션

안티 멀웨어 (백신) | 방화벽 | 침입 방어 (취약점 방어) | 로그 감사 | 무결성 모니터링 | 응용 프로그램 제어

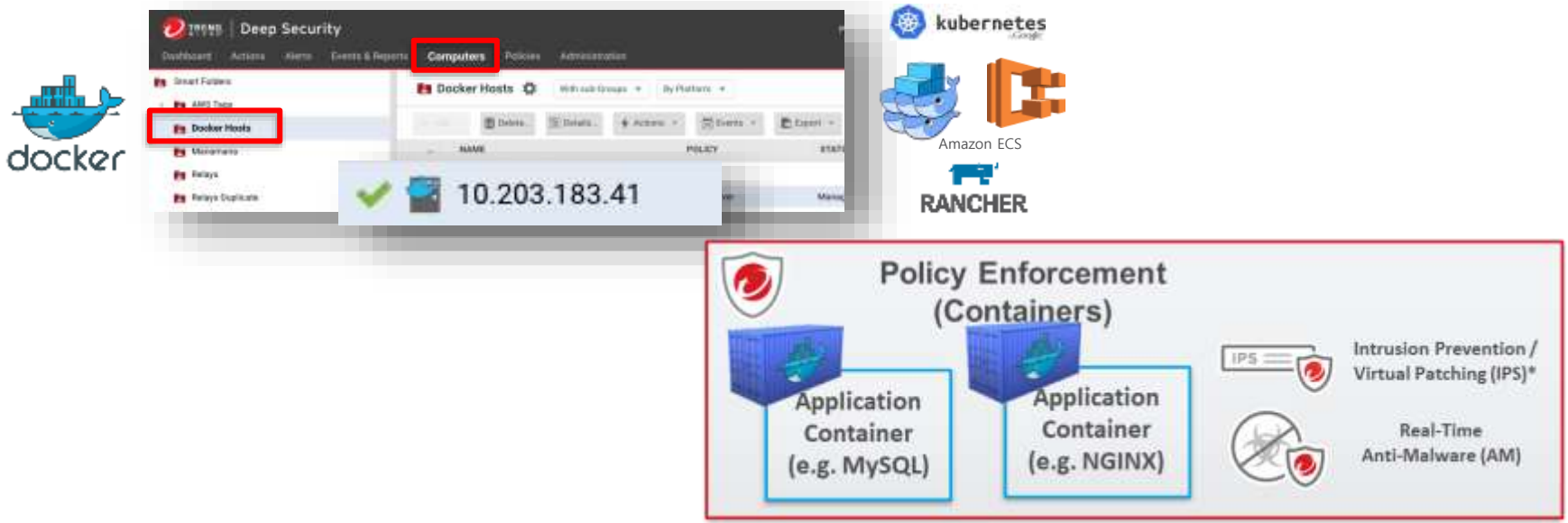


TREND MICRO

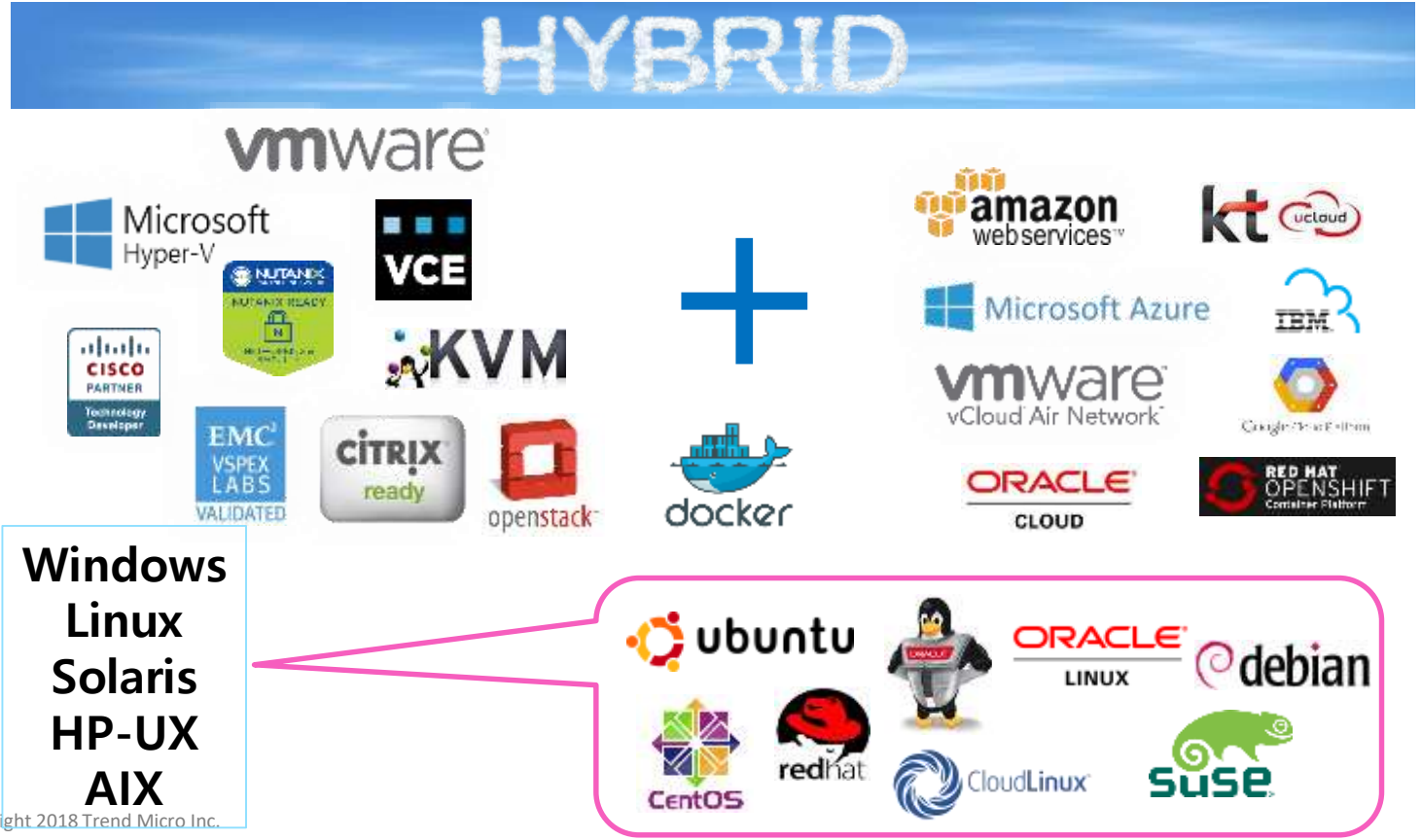
리눅스 서버 보안 차별화

Docker + Container 보안기능 확장

- 호스트와 Docker+Container를 안전하게 보호
- 안티 멀웨어(백신), 응용프로그램 제어,
  IPS 및 무결성 모니터링을 활용하여 컨테이너 보안 적용



Deep Security 지원 플랫폼



Endpoint 세계 1위

Gartner Magic Quadrant for Endpoint Protection Platforms
January 2017

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from

https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html

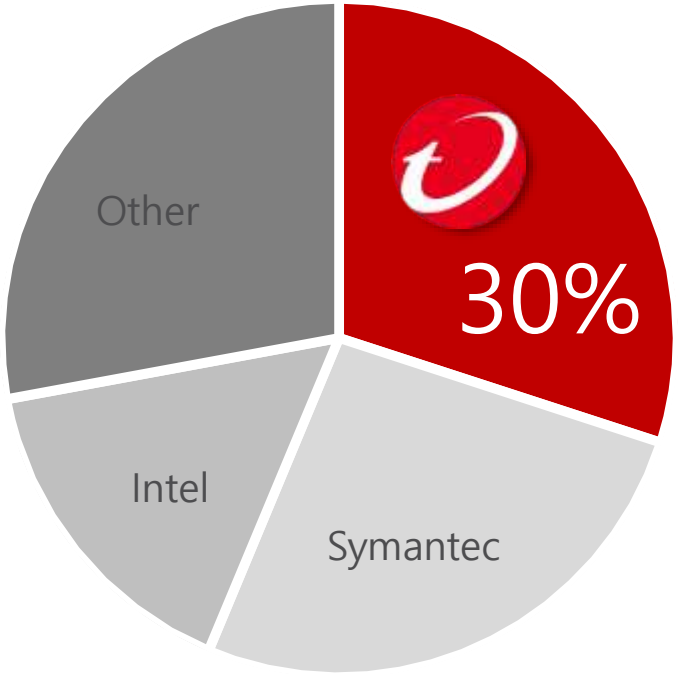
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Source: Gartner (January 2017)

서버 보안 7년 연속 세계 1위

The MARKET LEADER
in server security for 7 straight years

IDC
Analyze the Future



Source: IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116

TREND MICRO

Deep Security !

감사합니다!