AWS 보안을 위한
Trend Micro Deep Security 소개

한국트렌드마이크로
클라우드 보안팀

목차

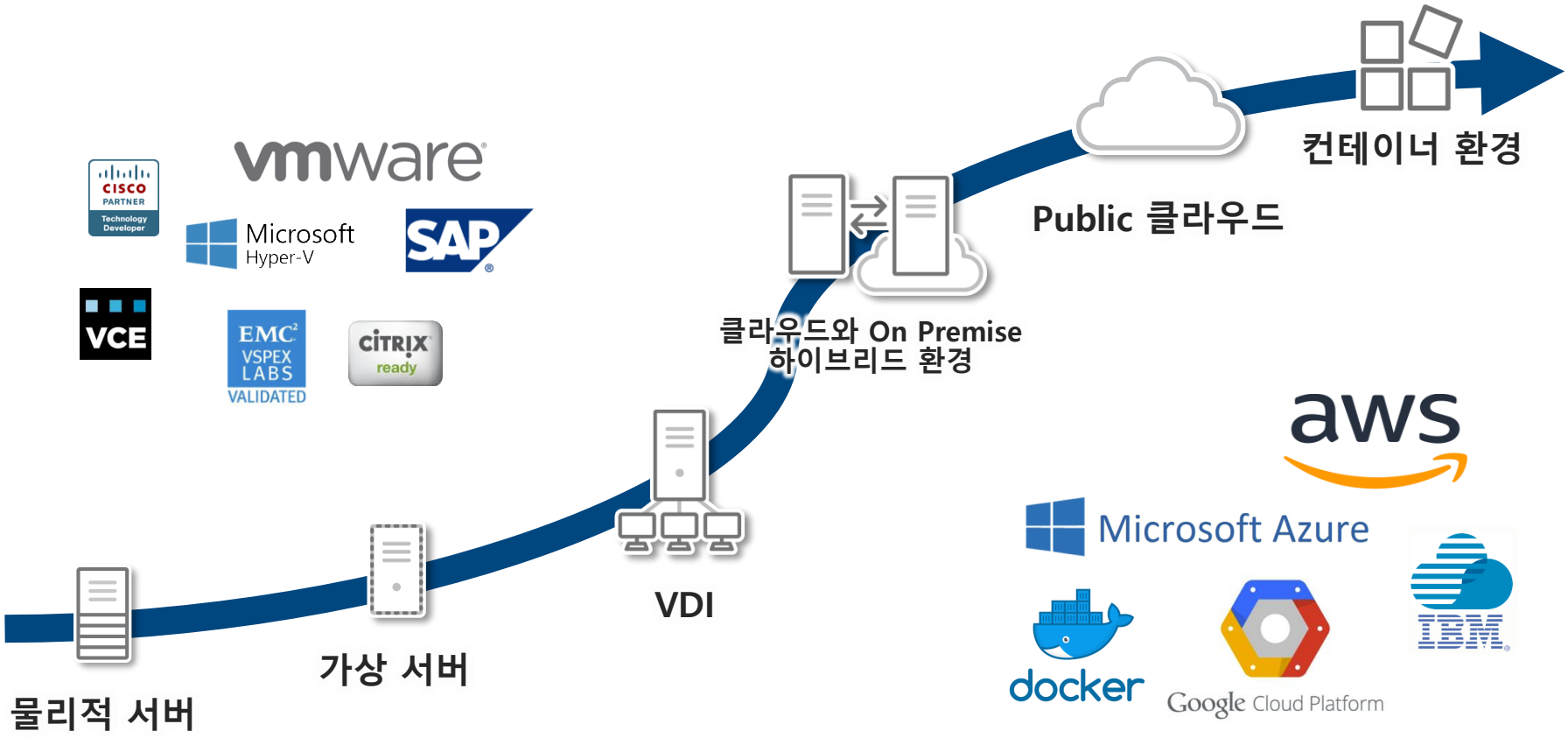
1. 클라우드 보안이란?
2. Deep Security 10.3
3. AWS 에서 Deep Security 장점
4. Deep Security 구성 방안
5. AWS 보안을 위한 DS 구성 추가 방안
6. Deep Security 추가 소개

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

클라우드 보안이란?

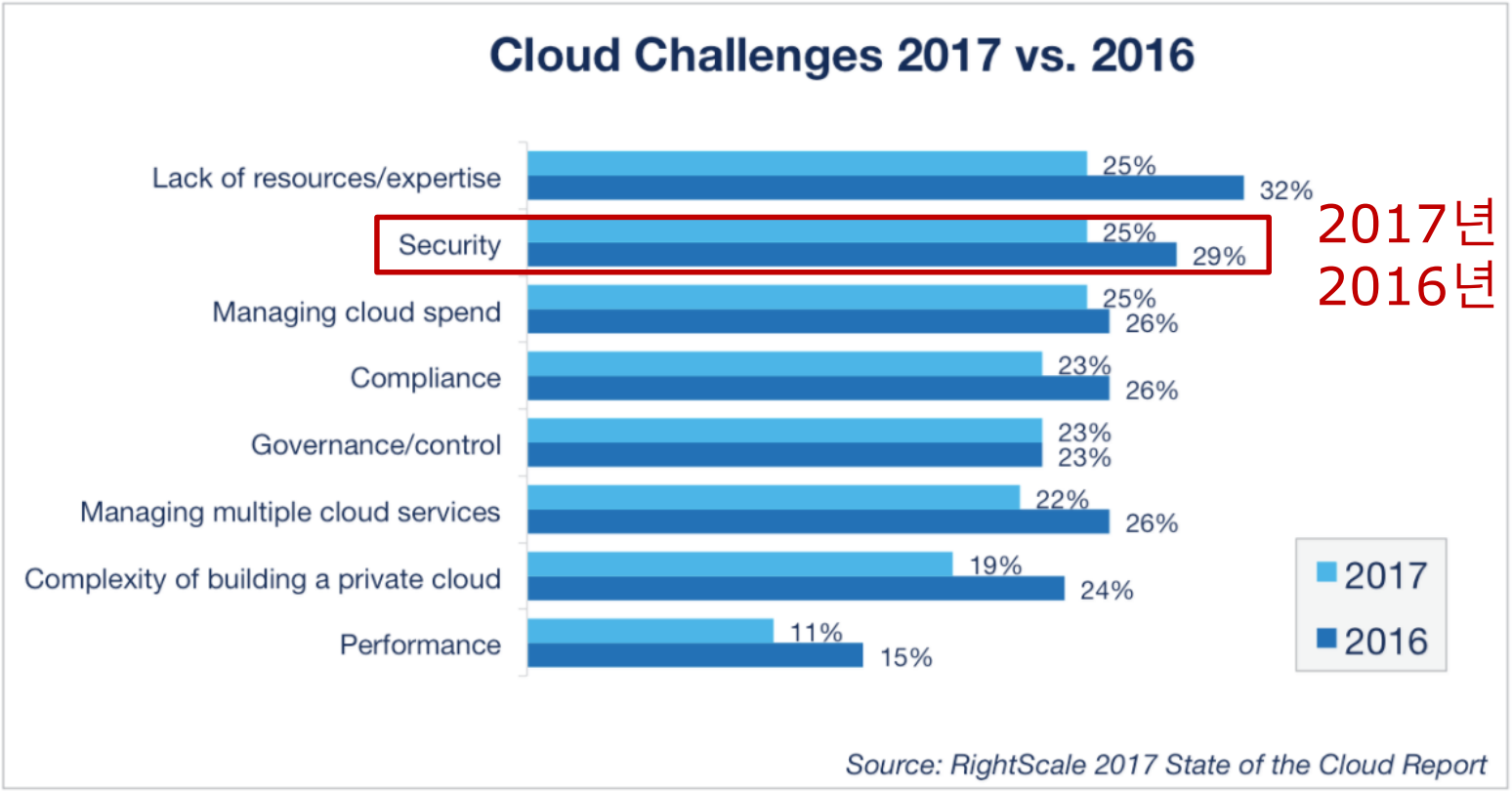
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

변화하는 서버를 둘러싸는 환경



Copyright 2017 Trend Micro Inc.

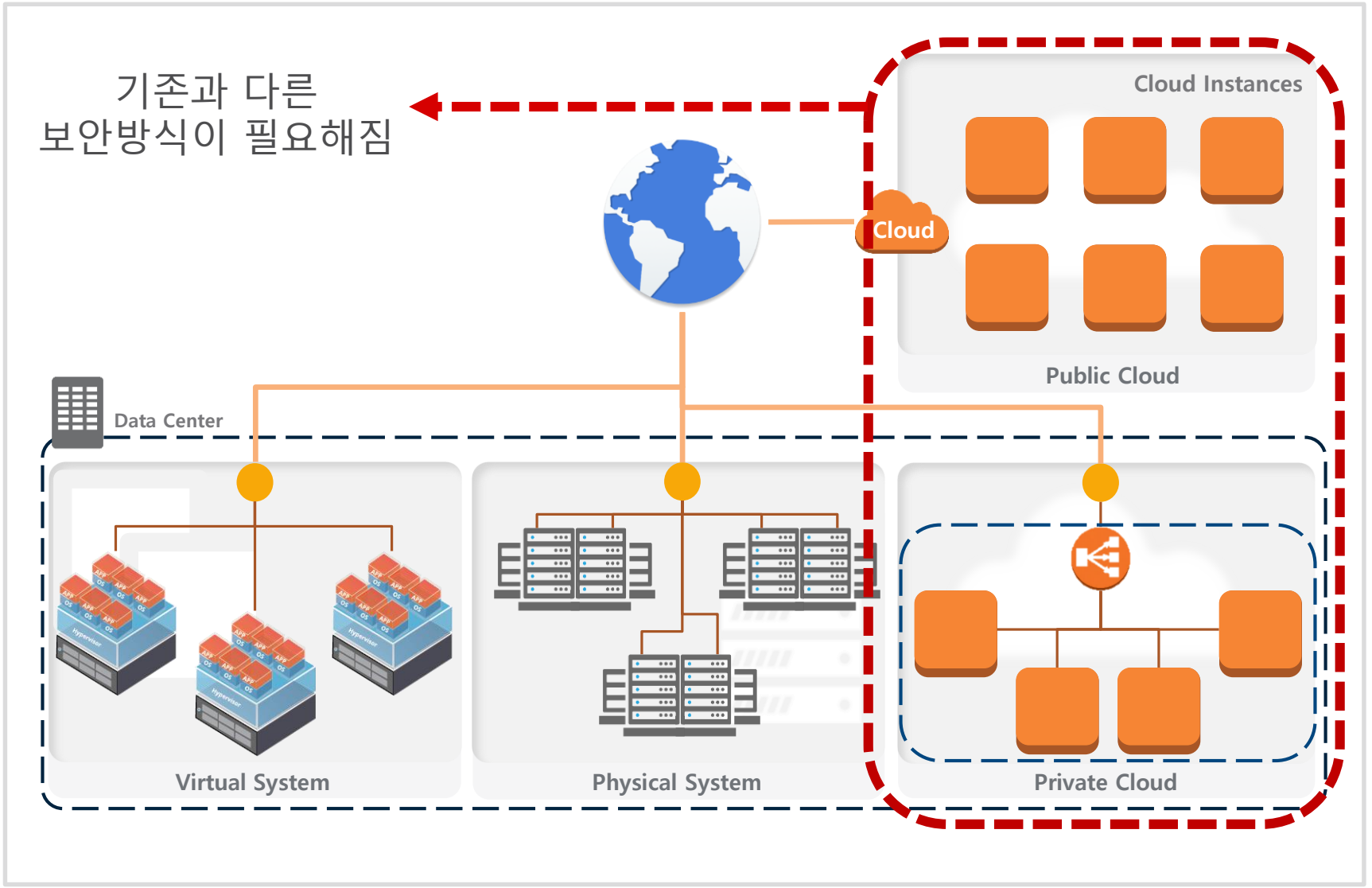
클라우드 도입 시 방해 요소



2017년 2위
2016년 2위

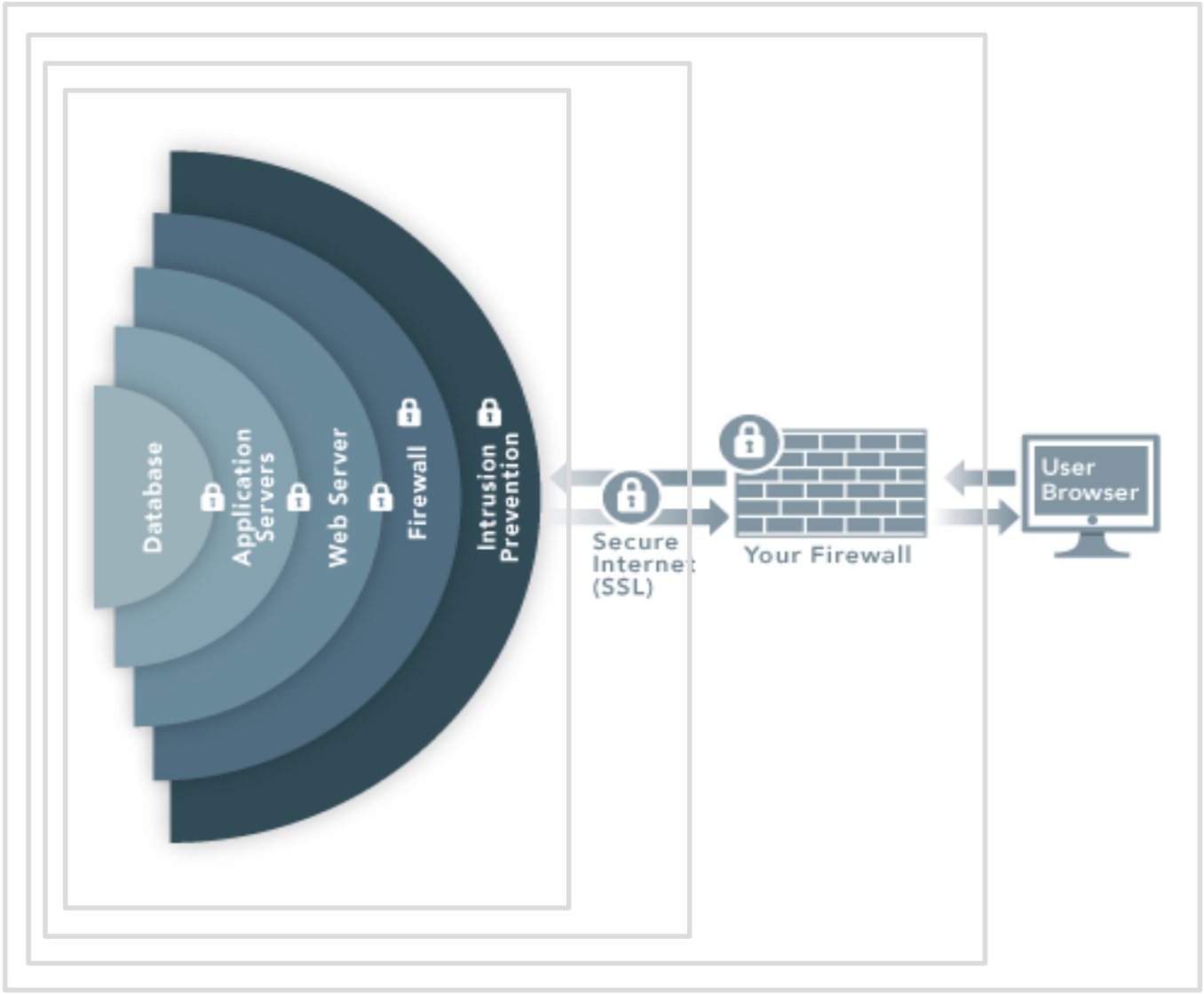
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

클라우드 보안 구현 방향



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

보안 적용 범위

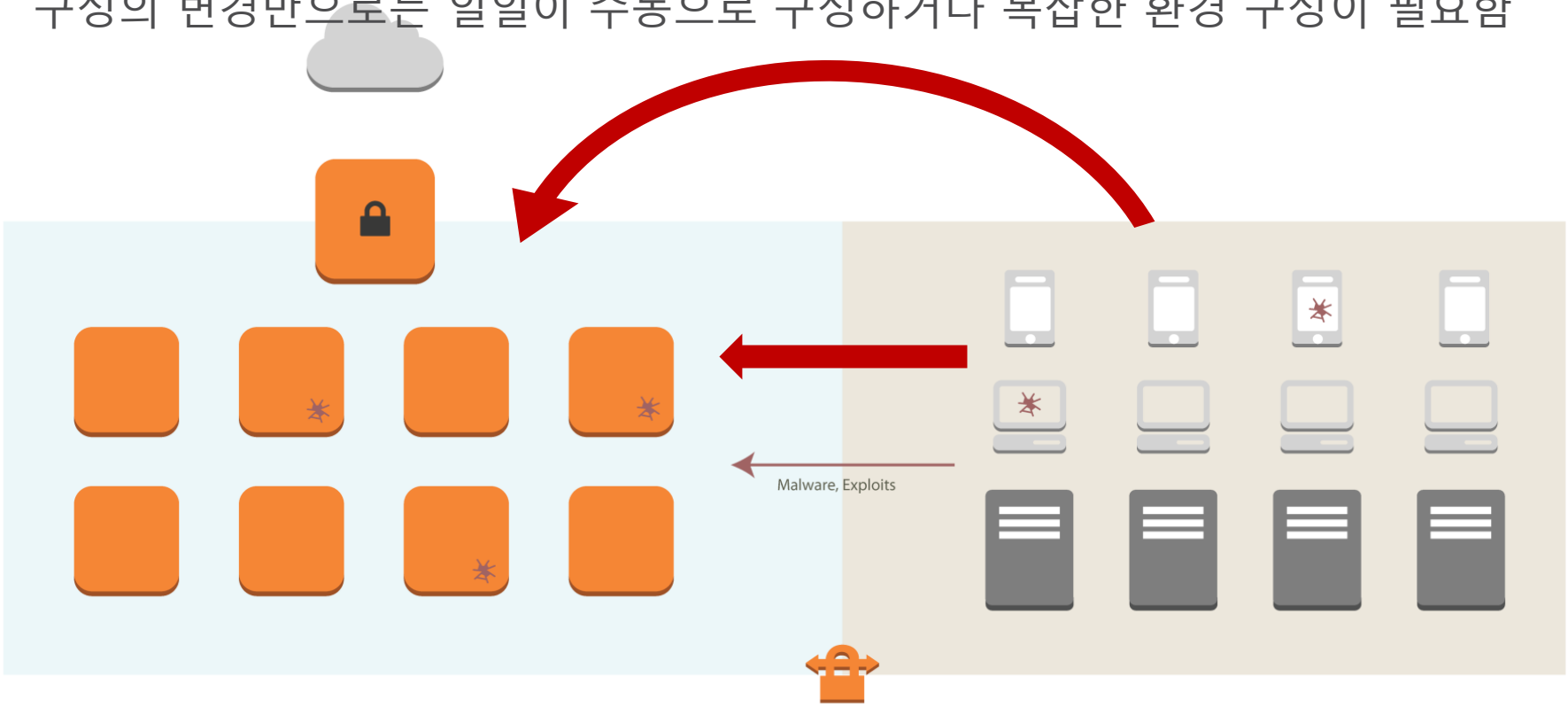


Copyright © 2016 Trend Micro Incorporated. All rights reserved.

클라우드 보안 구현 방향

기존의 물리적 보안 장비로는 내부 클라우드 자원과의 East-West 보안을 구현하기에는 어려움

기존의 보안 정책이 적용된 East-West 트래픽 보안을 구현하기 위해 네트워크 구성의 변경만으로는 일일이 수동으로 구성하거나 복잡한 환경 구성이 필요함



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 책임 공유 모델

고객 시스템

로그 | 콘텐츠

운영 체제 | 미들웨어 | 응용 프로그램

네트워크

고객의 책임 범위

TREND MICRO™ SMART PROTECTION NETWORK™

고객 책임 범위의
보안 대책을 도움

서버 | 스토리지 | 데이터베이스 | 네트워크

지역 | 가용성 존 | 에지 위치

AWS 글로벌 인프라

Cloud Service Provider **책임 범위**

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

TREND MICRO™

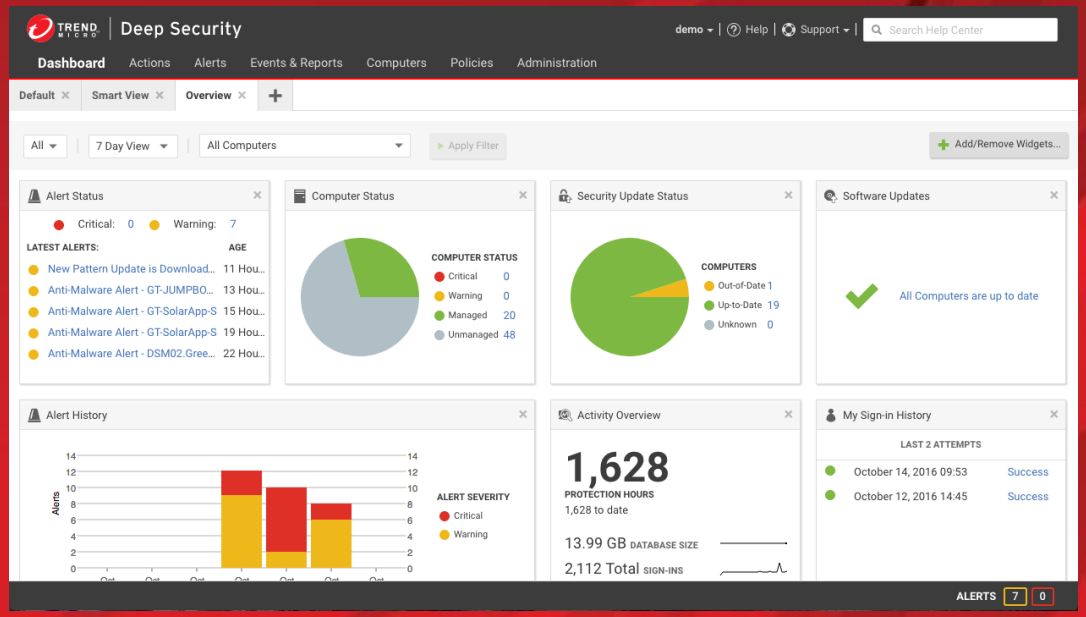
AWS 책임 공유 모델

			Deep Security	AWS
Cloud User Responsibility	Application Security	Access Control		
		Configuration		
		L4 Network Protection		some capabilities
		L7 Network Protection		
		Application Integrity		
		Log Security Intelligence		
		Security Alerts		
	Operating System Security	Access Control		
		Configuration		
		L4 Network Protection		some capabilities
		L7 Network Protection		
		Malicious File Protection		
		System Integrity		
		Log Security Intelligence		
		Security Alerts		
	Instance Configuration	Roles, Security Groups, Encrypted Volumes	AWS provides tools but is customer responsibility	
	Services Controls	Authentication and user authorization		
AWS Responsibility	Hypervisor Controls	Access control, configuration		AWS
	Network Infrastructure Controls	Router/switch access control, configuration		AWS
	Physical Infrastructure controls	Badge readers, alarm systems etc		AWS

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 사용시 고객의 의무

Copyright © 2016 Trend Micro Incorporated. All rights reserved.



Deep Security 10.3

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Deep Security란?

하이브리드에 각종 구성에 대응. 서버/클라이언트 보호에 필요한 보안 기능을 제공하는 All in One의 보안 제품

물리환경

에이전트방식의 소프트웨어에 의한 **서버단위** 보호

가상환경

Virtual Appliance 에 의한 **ESXi단위**로 보호

vSphere환경과 연계가능

클라우드 환경

에이전트 방식 또는 Virtual Appliance 로 보호

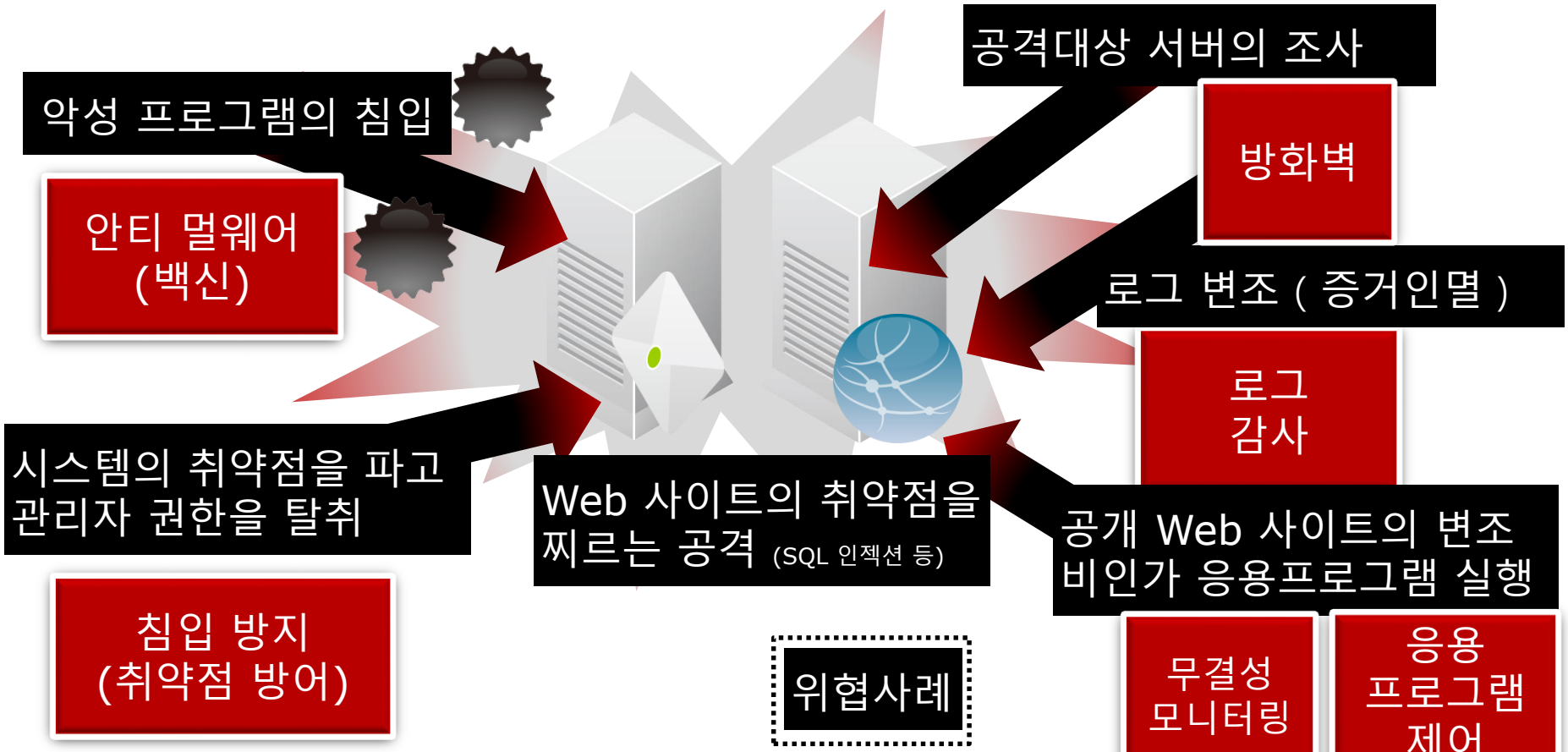
vCloud Director, vCloud Air、AWS와 연계 가능

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

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

서버를 둘러싼 위협과 Deep Security

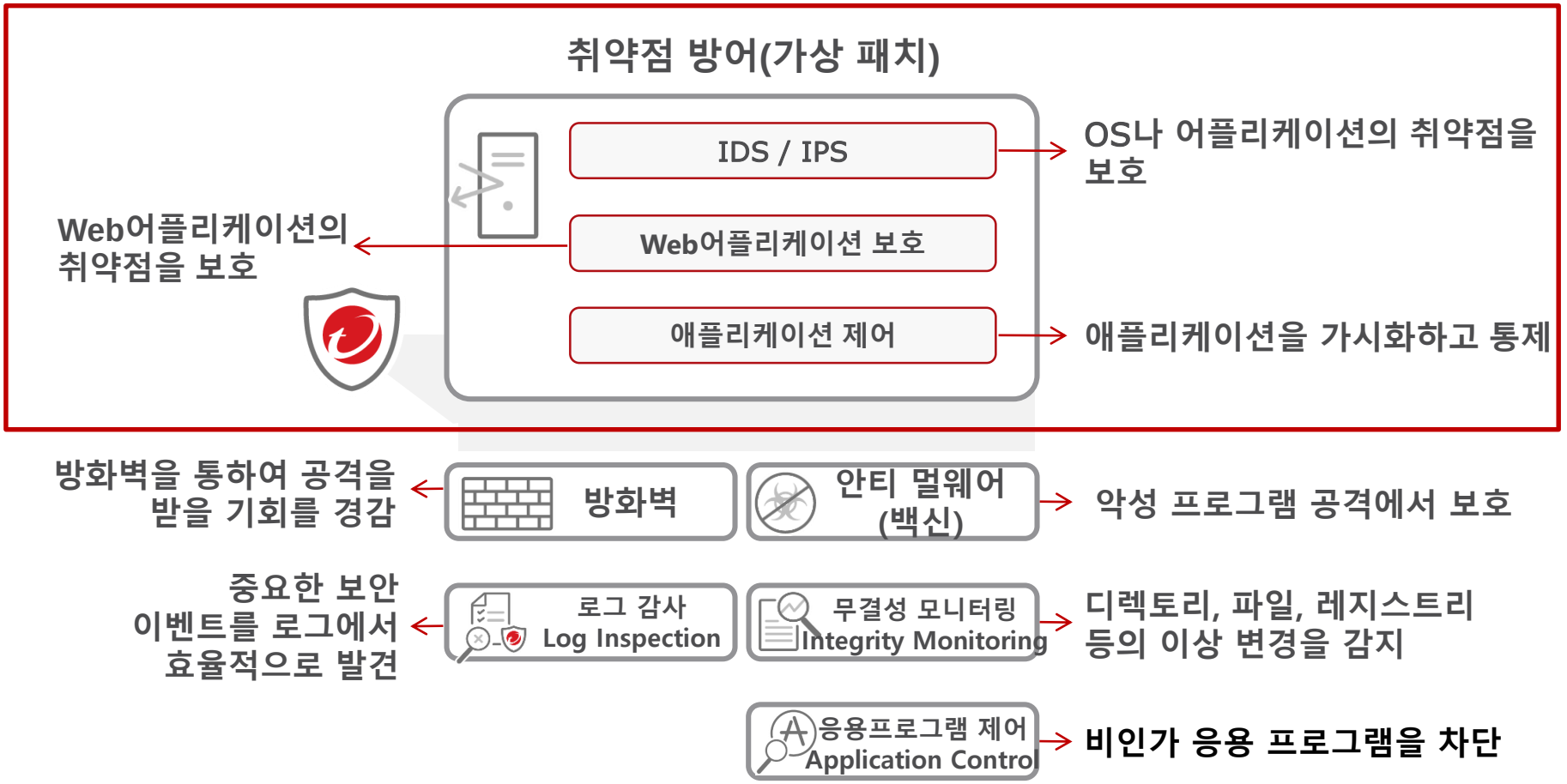
서버를 둘러싼 위협은 악성 프로그램 (바이러스)뿐만 아닙니다. 사이버 공격의 공격자는 다양한 방법으로 서버를 노립니다. Deep Security는 이러한 위협에서 중요한 서버를 보호합니다.



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Deep Security 기능

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



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

안티 멀웨어(백신)

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

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 별 기능 제한
(자세한 내용은 시스템 요구 사항에 기재)
예약 검색, 수동 검색, 실시간 검색

Deep Security 10

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

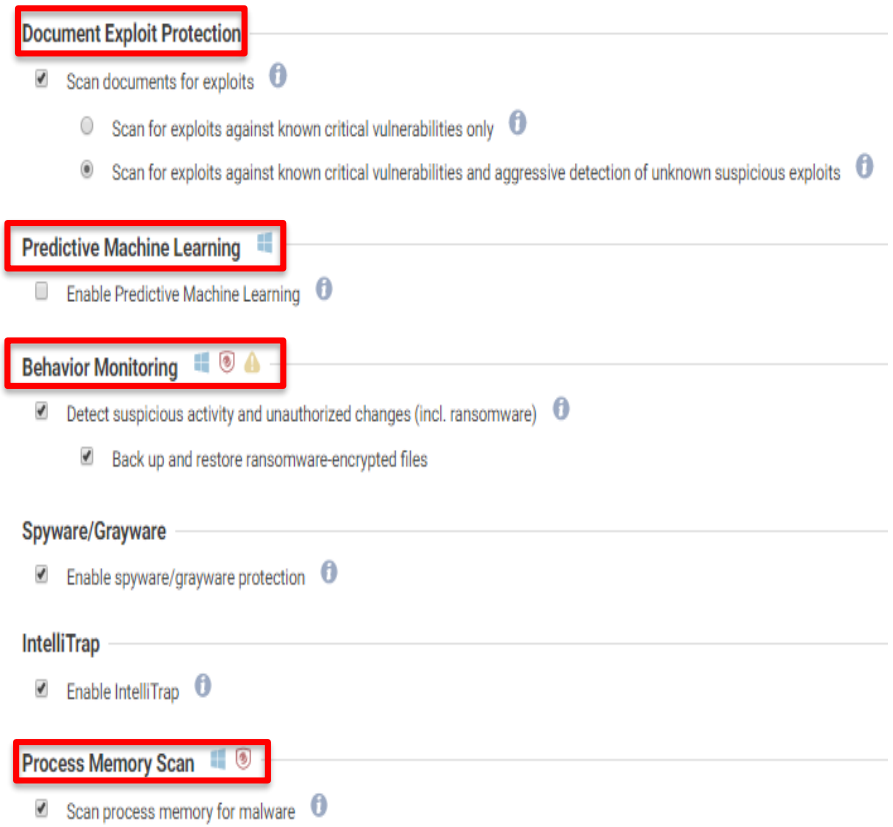
- 검색 제외 설정, 격리된 악성코드 복원 및 다운로드, 수동/예약 검색 시 CPU사용량 제한, 압축파일 검색 레벨 등 다양한 백신 정책을 설정

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

안티 멀웨어(백신)

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

안티 멀웨어 (백신)



Document Exploit Protection

- 문서 취약점을 가진 문서 파일 탐지
- 문서 취약점이 탐지된 문서파일을 Deep Discovery Analyzer(DDAN)로 전송

Predictive Machine Learning

- 머신러닝 기능으로 신종 악성코드 탐지 & 차단

동작 모니터링 - 랜섬웨어 대응

- 랜섬웨어의 암호화 행위 탐지
- 암호화 행위를 시도하는 프로세스를 강제 종료

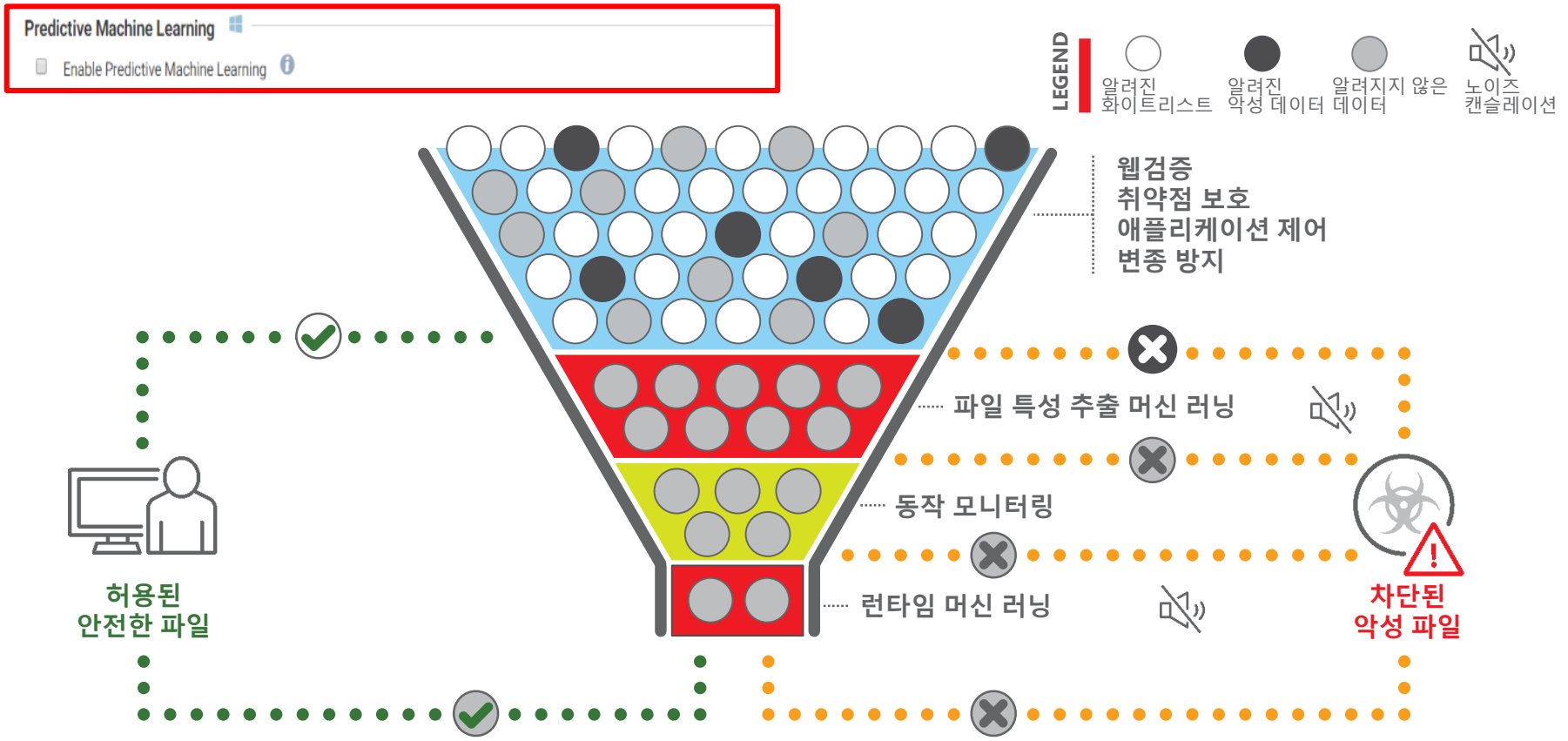
실시간 메모리 검색

- 메모리 공간에서 실행되는 의심스러운 프로세스를 차단

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

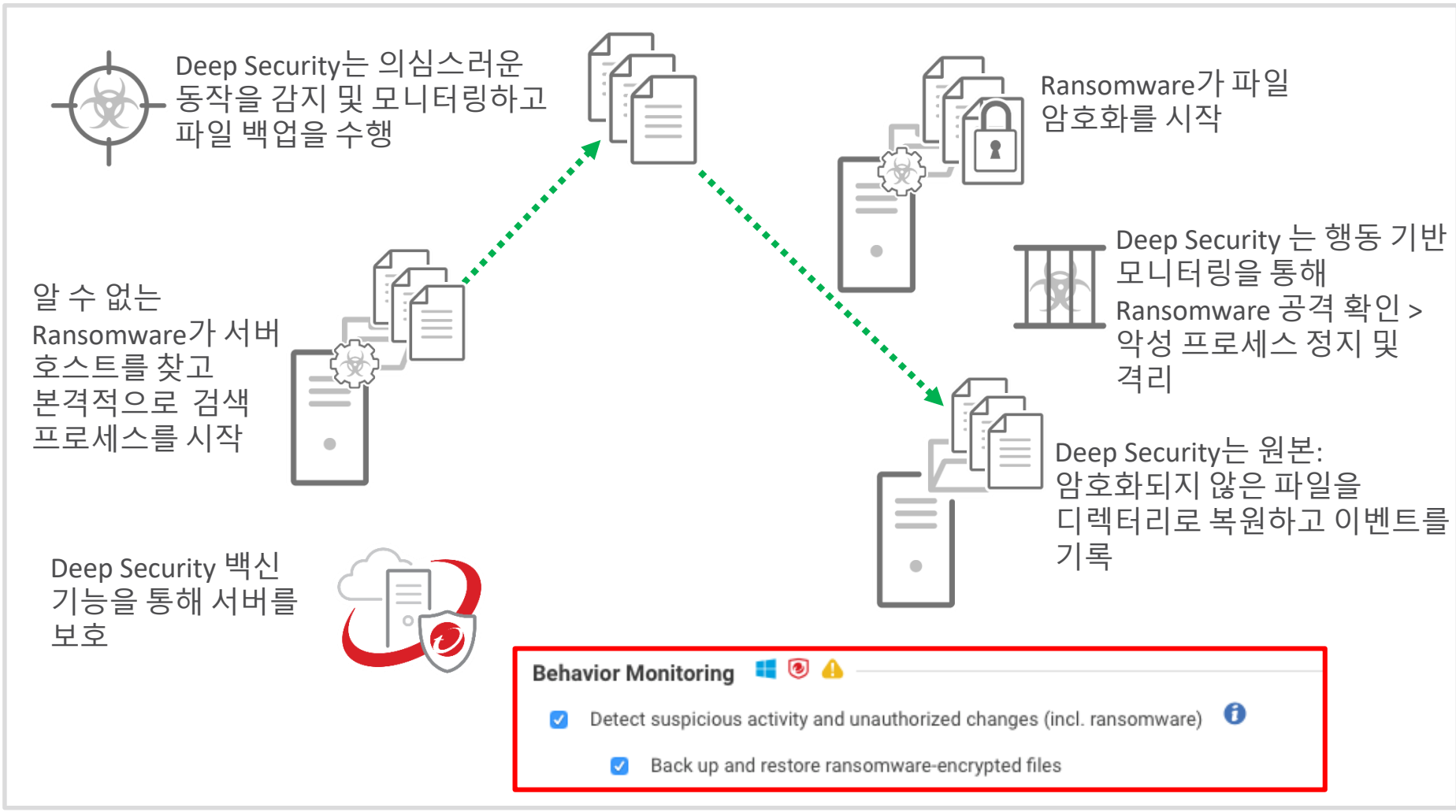
안티 멀웨어(백신) - 머신러닝

- 매일 100TB의 방대한 데이터를 처리하는 클라우드 보안센터의 학습데이터를 이용
- 머신러닝 기능으로 신종 악성코드 탐지 & 차단



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

안티 멀웨어(백신) Ransomware 대응

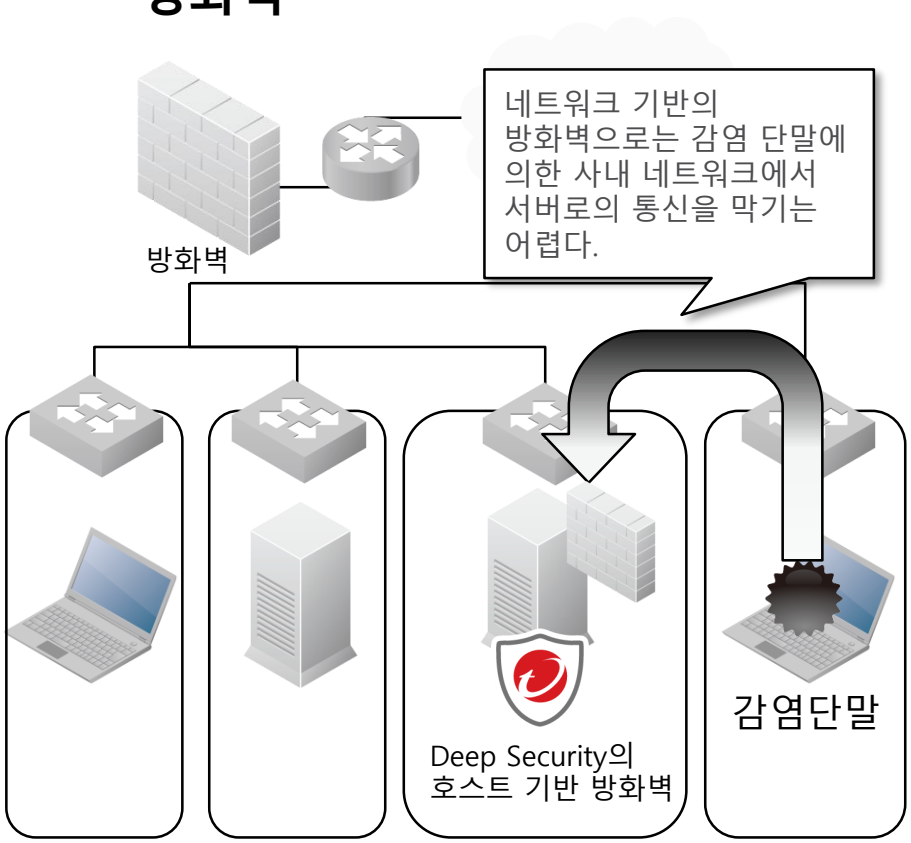


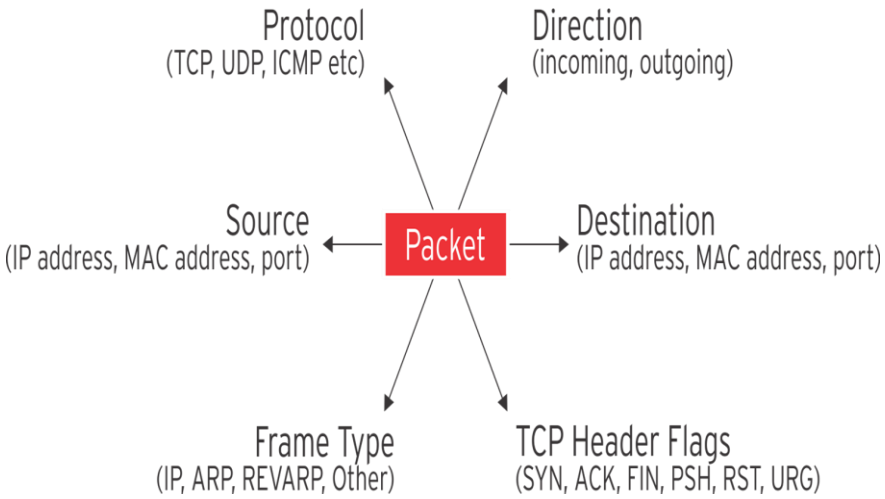
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

방화벽

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

방화벽





Copyright © 2016 Trend Micro Incorporated. All rights reserved.

침입방지 (가상패치 기능)

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

- OS 나 응용 프로그램의 취약점 (보안 취약점)을 통한 공격 패킷을 탐지하고 방어하는 기능 (**가상패치**)
- 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.

트렌드 마이크로로부터 제공되는 침입 차단 규칙 외 커스텀 규칙을 작성할 수도 있습니다.

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

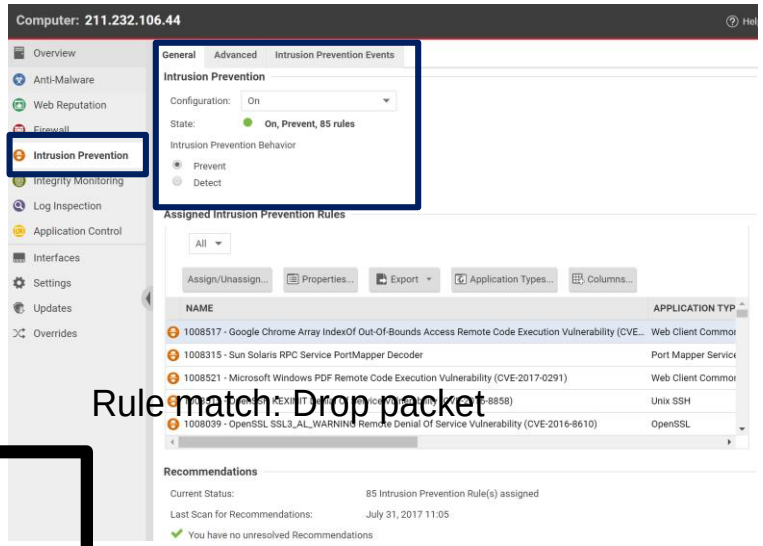
가상 패치는 일시적 보호를 목적으로 한 것으로,
근본적인 해결을 위해서는 보안 패치를 설치할 필요가 있습니다.

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

침입방지 (가상패치 기능)

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

- **침입 방지 동작 방식**
- Application Control (패킷 기반)
- IDS / IPS
- Web Application Protection



DPI engine

DPI rule
Shellcode:do_something_bad

Rule match: Drop packet

Network → Reassembly process → Packet:**do_something_bad** → Fragmentation process → Application

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

권장 스캔 : 룰 자동 선별, 자동 적용

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

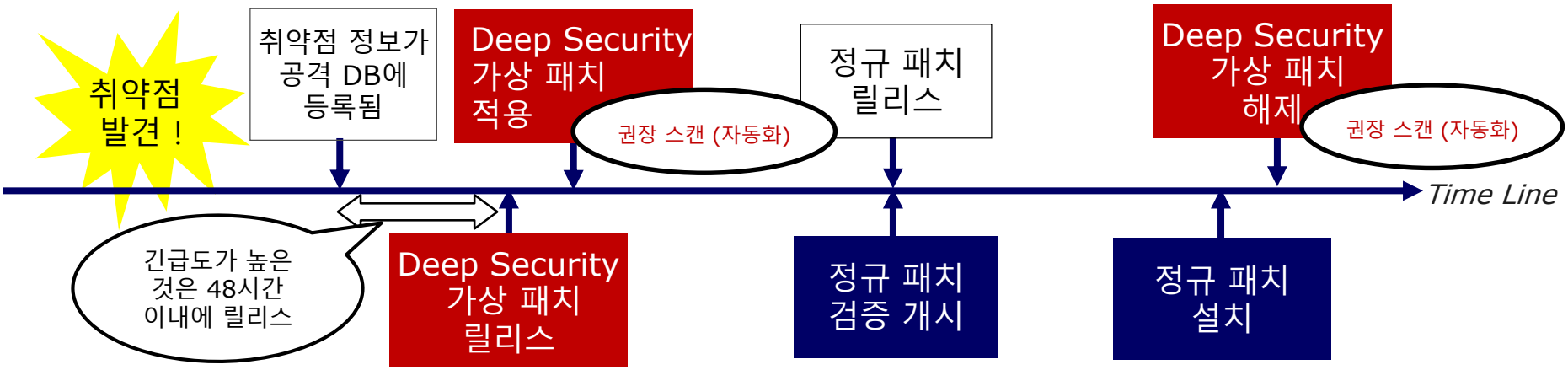
권장하는 룰의 선별 자동 적용

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

권장 스캔 : 룰 자동 선별, 자동 적용

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

권장 스캔을 이용한 패치 관리

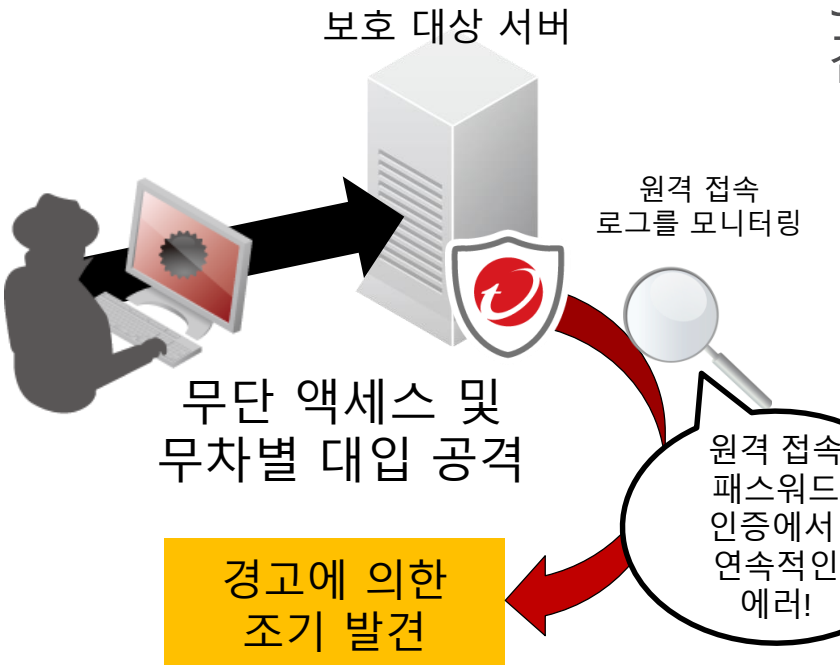


Copyright © 2016 Trend Micro Incorporated. All rights reserved.

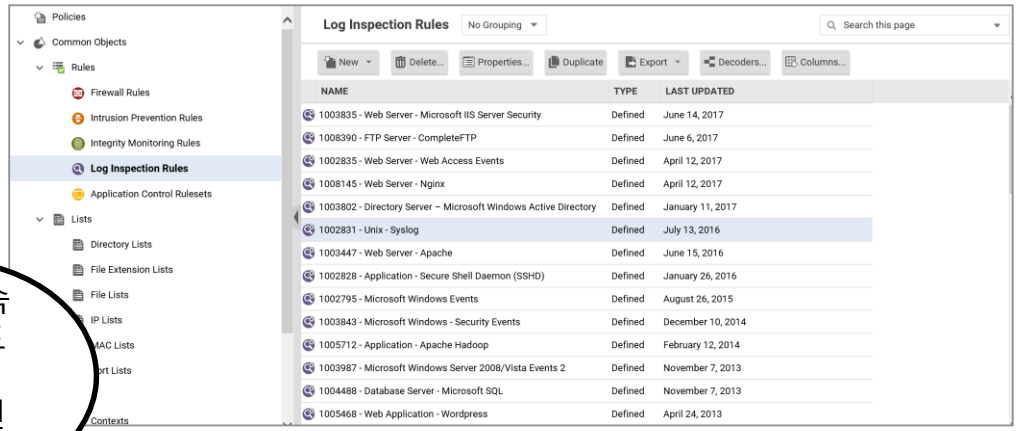
로그 감사

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

로그 감사 (예)



주요 OS, DB, Application에 대한 54개의 로그 프로파일을 이용한 로그 감사 설정 기능 제공



OS 이벤트 로그, Syslog 외에 Web 서버나 DB 등의 로그를 모니터링 할 수 있습니다.

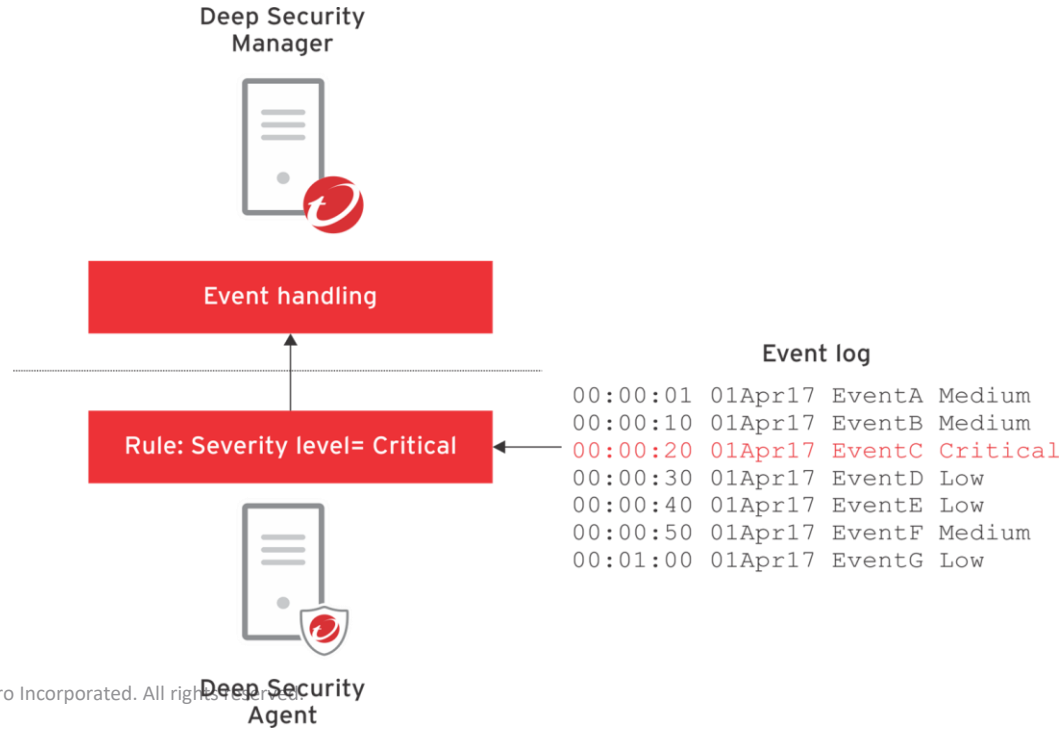
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

로그 감사

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

Deep Security가 탐지하지 못한 시스템/App 로그까지 모니터링 하여 서버에 접근한 공격에 대해 모니터링 제공

서버나 애플리케이션에서 발생하는 로그를 모니터링 하는 기능으로 위협이 될만한 의심스러운 이벤트/메시지 발생시 이를 탐지하여 경고

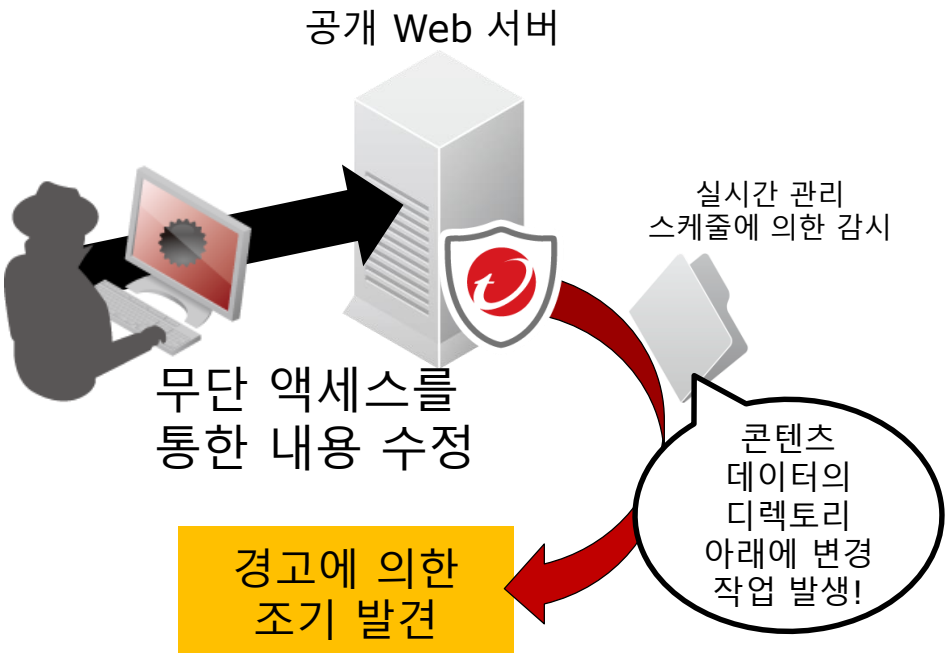


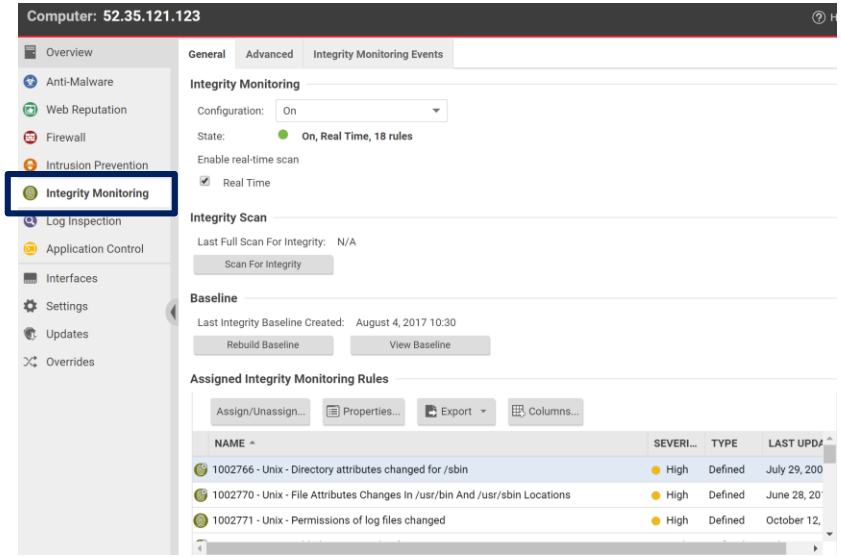
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

무결성 모니터링

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

무결성 모니터링 (예)



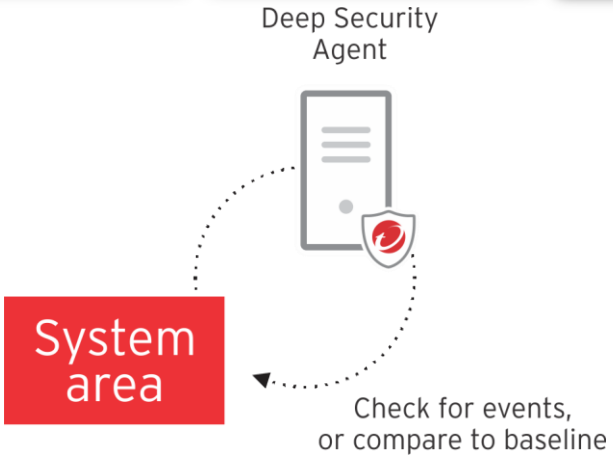


파일 (파일 속성 포함), 디렉토리, 레지스트리, 프로세스 등의 변화를 감지 할 수 있습니다.

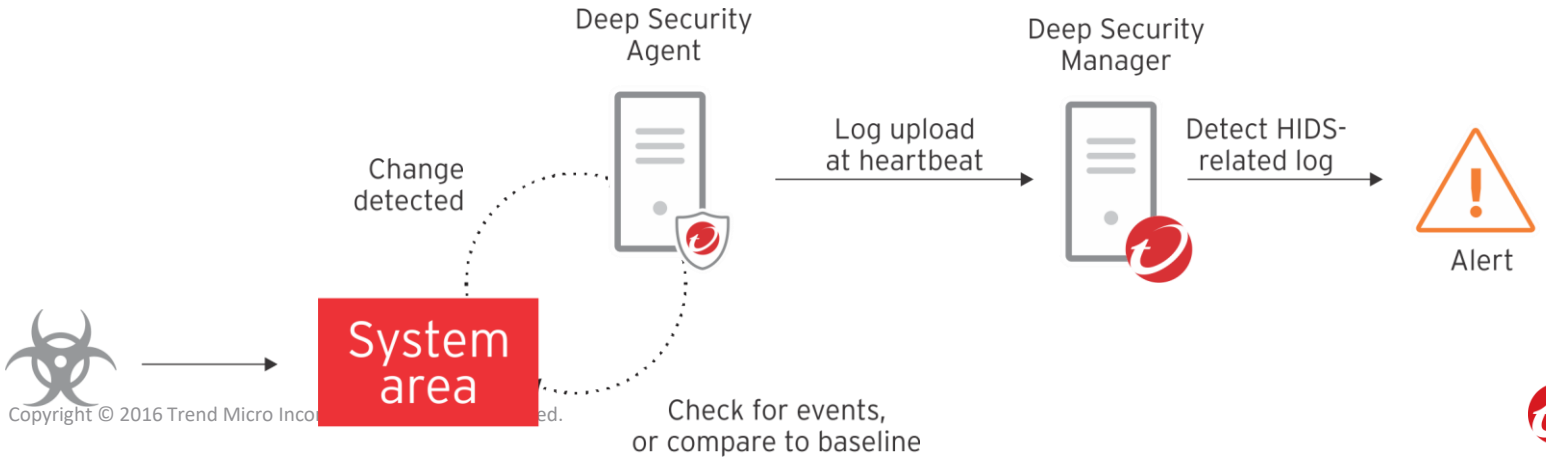
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

무결성 모니터링

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



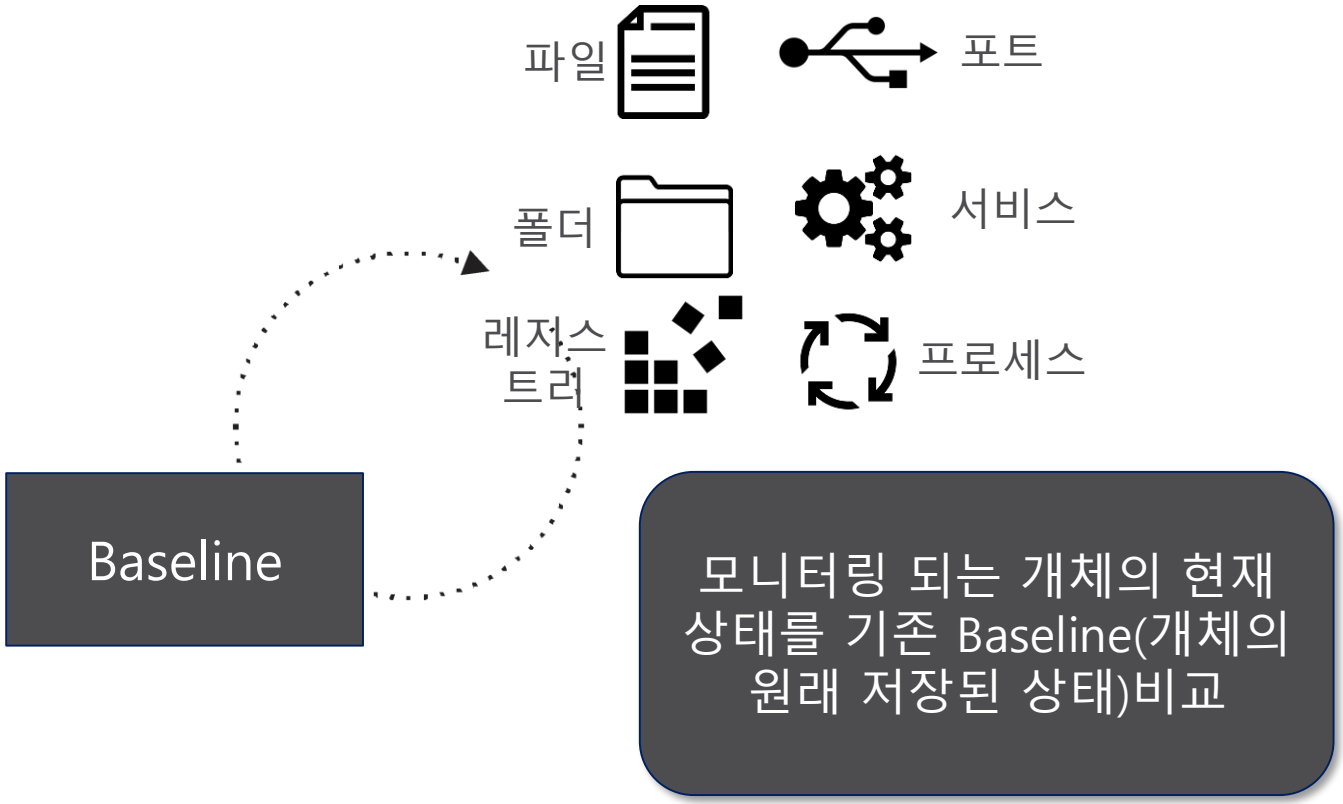
- Windows 레지스트리와 같은 파일 및 중요 시스템 영역에 대한 변경 사항을 탐지
- 이전에 기록한 기준과 비교하여 탐지 수행
- 사전 정의된 무결성 모니터링 규칙 및 새로운 규칙을 DSA 로 적용



Copyright © 2016 Trend Micro Incor ed.

무결성 모니터링

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

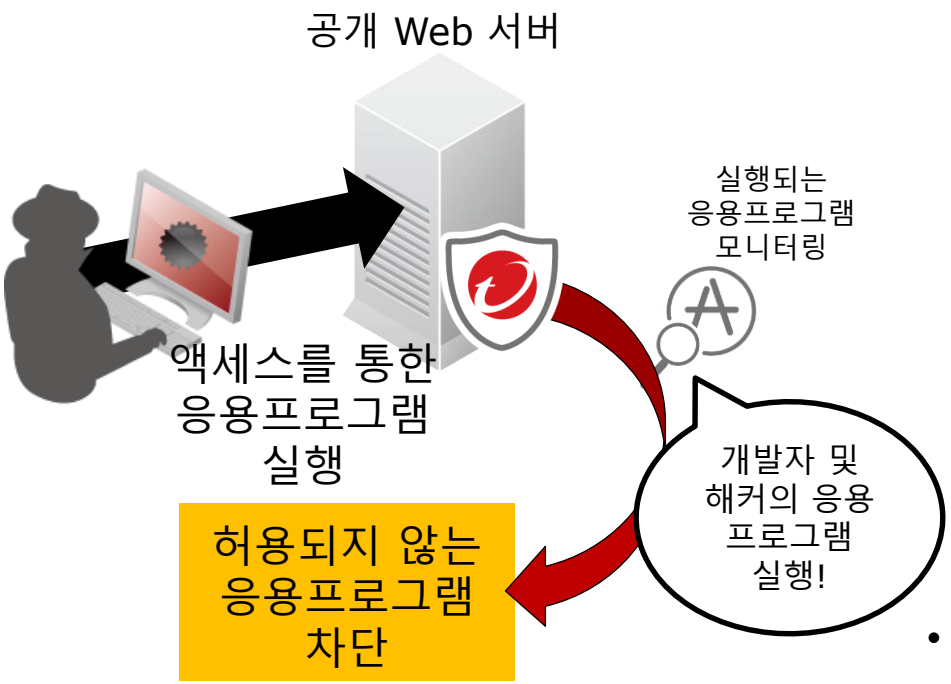


Copyright © 2016 Trend Micro Incorporated. All rights reserved.

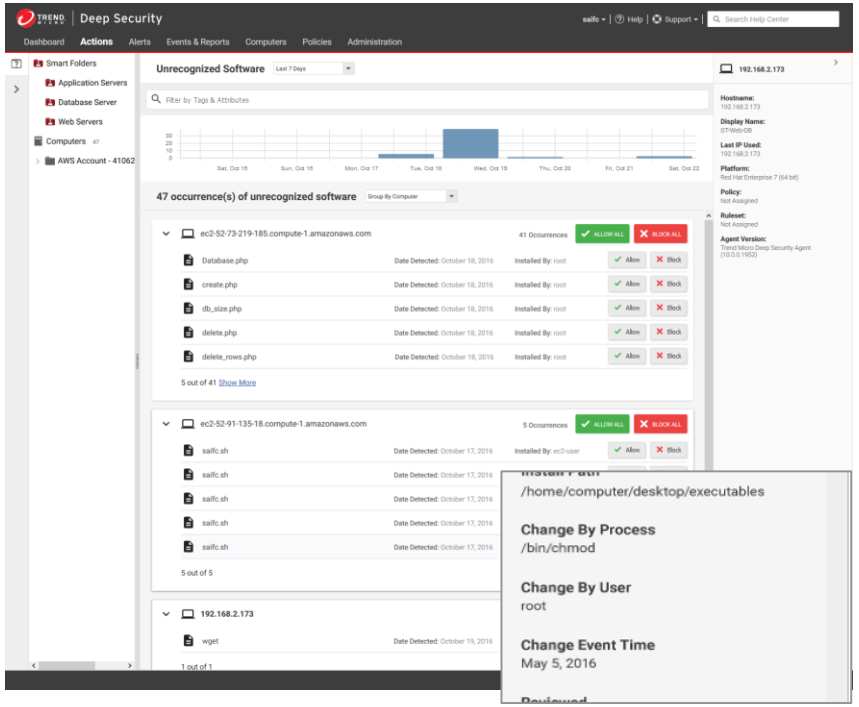
응용 프로그램 제어

안티 멀웨어 (백신) | 방화벽 | 침입 방어 (취약점 방어) | 로그 감사 | 무결성 모니터링 | **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
  - 탐지(로그) 또는 블록 선택 가능

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

응용 프로그램 제어

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

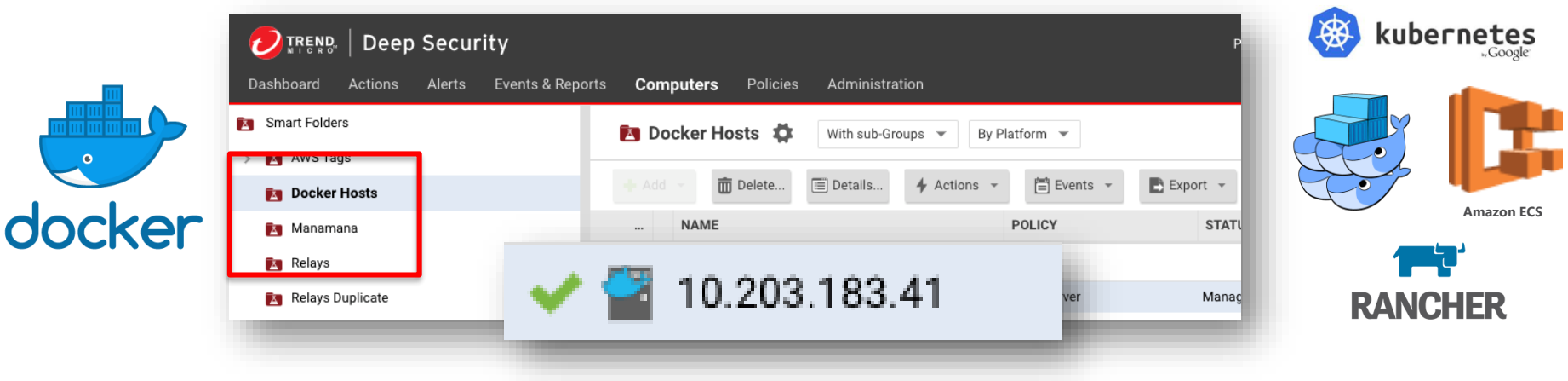
- **응용프로그램 제어 동작 방법**

- DSA 에서 변경사항을 지속적으로 모니터링
  - 기준 인벤토리 : ac.db 파일
- Deep Security Agent는 소프트웨어에 대한 쓰기 작업 검색
- 인벤토리에 있는 원본 파일의 해시를 새 파일 및 변경된 파일의 해시 비교

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Docker 보호

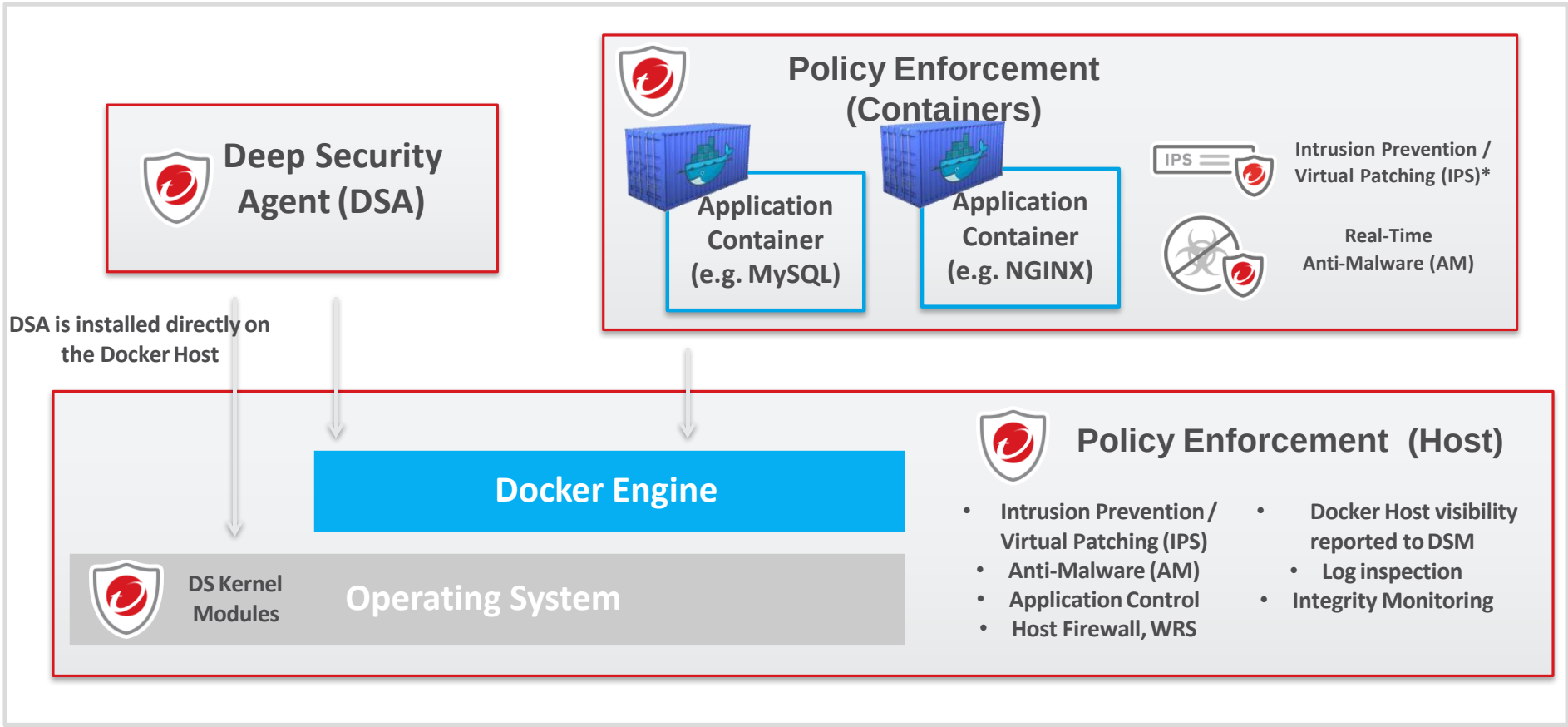
- 호스트와 Docker 컨테이너를 안전하게 보호
- 모든 워크로드에서 일관된 보안 유지
- Deep Security 서버 보호 기술을 Docker 컨테이너로 확장 적용
- 런타임 보호를 통해 마이크로 서비스 아키텍처를 보호



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Docker 보호

- 백신(안티 멀웨어), 응용프로그램 제어,
  IPS 및 무결성 모니터링을 활용하여 컨테이너 보안 적용



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 에서 Deep Security 장점

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 보안을 위한 **4가지 장점**

1. All-in-One 보안

2. 호스트 기반

3. Auto Scaling 대응

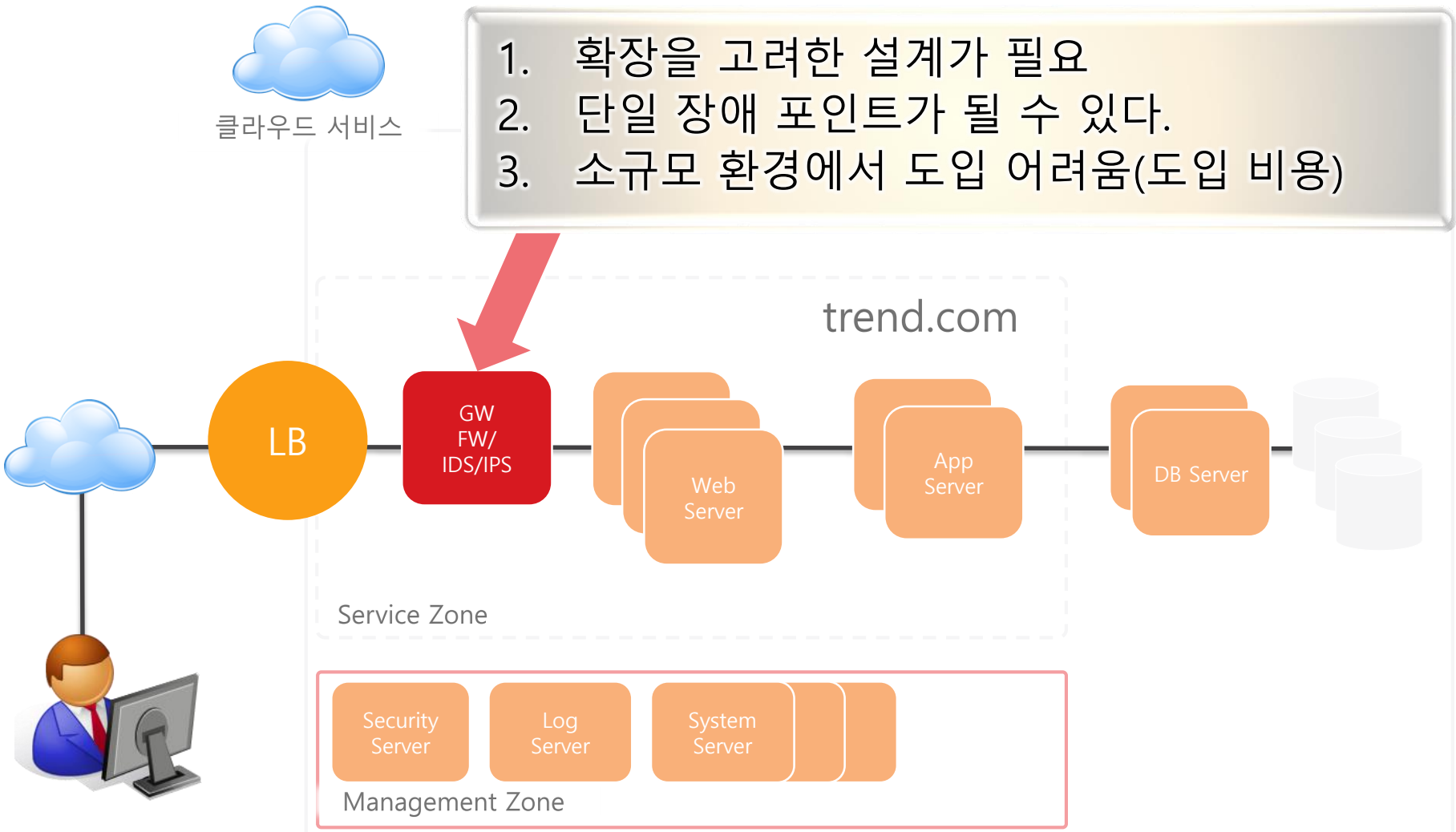
4. AWS 관리 콘솔과 연계

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

1. 6 가지 모듈을 통한 통합 방어

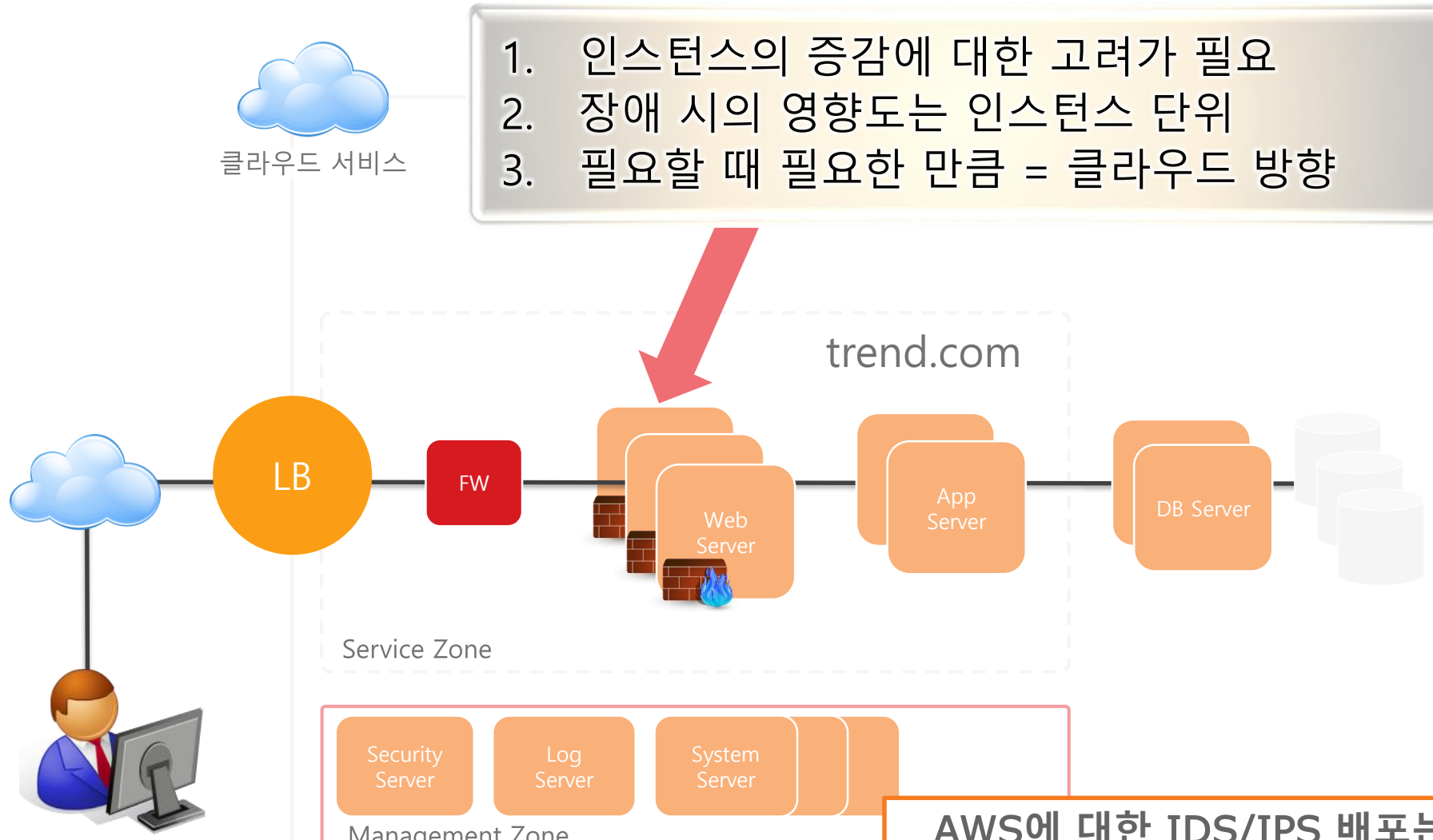
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

2. G/W 기반 장비의 경우



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

2. Host 기반 장비의 경우



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

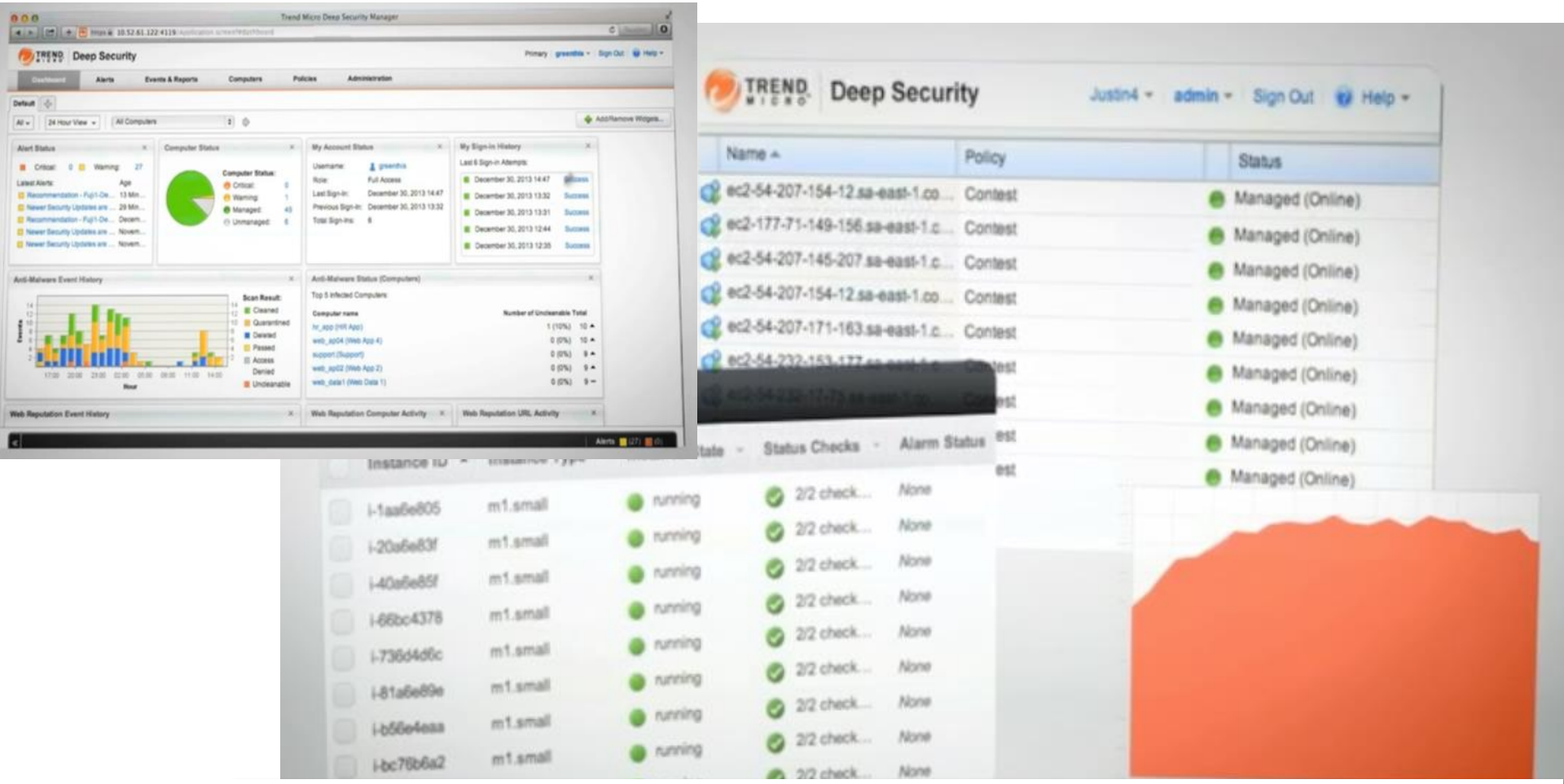
3. Auto Scaling 대응

- 동적으로 늘어나는 인스턴스를 자동으로 보호
- 운영 관리자가 일일이 설정 불필요
- 일시적인 증가에 관해서는 라이센스 무료

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

3. Auto Scaling 대응

- Auto scaling에 따른 보안 자동 배포 (데모)



http://www.trendmicro.com/us/boxes/videos/20141105083504.html

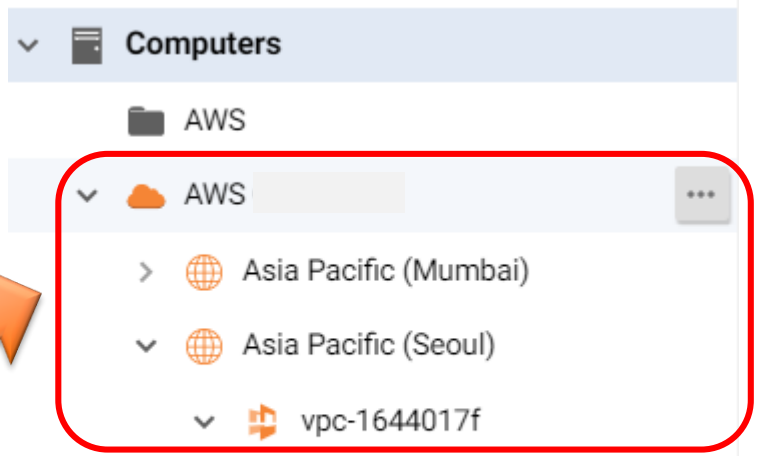
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

4. AWS 관리 콘솔과 연계

- Amazon Management Console와 연계하여 인스턴스 정보를 실시간으로 동기화
- 보안 적용 전·후 가시성 증가

Cloud Connecter로 접속

Deep Security 관리 매니저



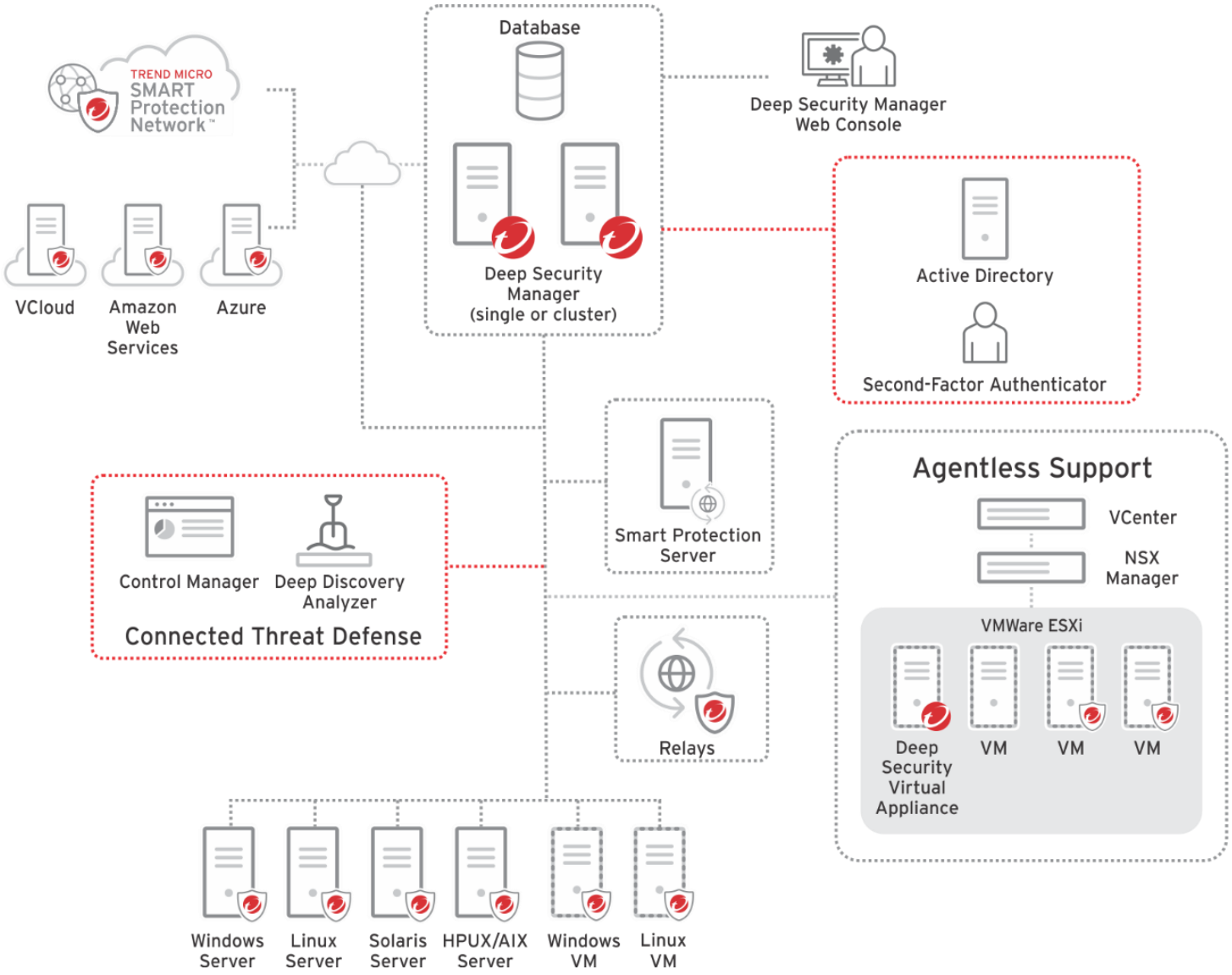
인스턴스 정보가 Deep Security 매니저에 동기화 (WorkSpaces 포함)

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Deep Security 구성 방안

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Deep Security 주요 컴포넌트 구성



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Deep Security 주요 컴포넌트 구성

설치 단계

정책 적용 및 운영 단계

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 보안을 위한 DS 구성 추가 방안

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 보안을 위한 **추가 방안**

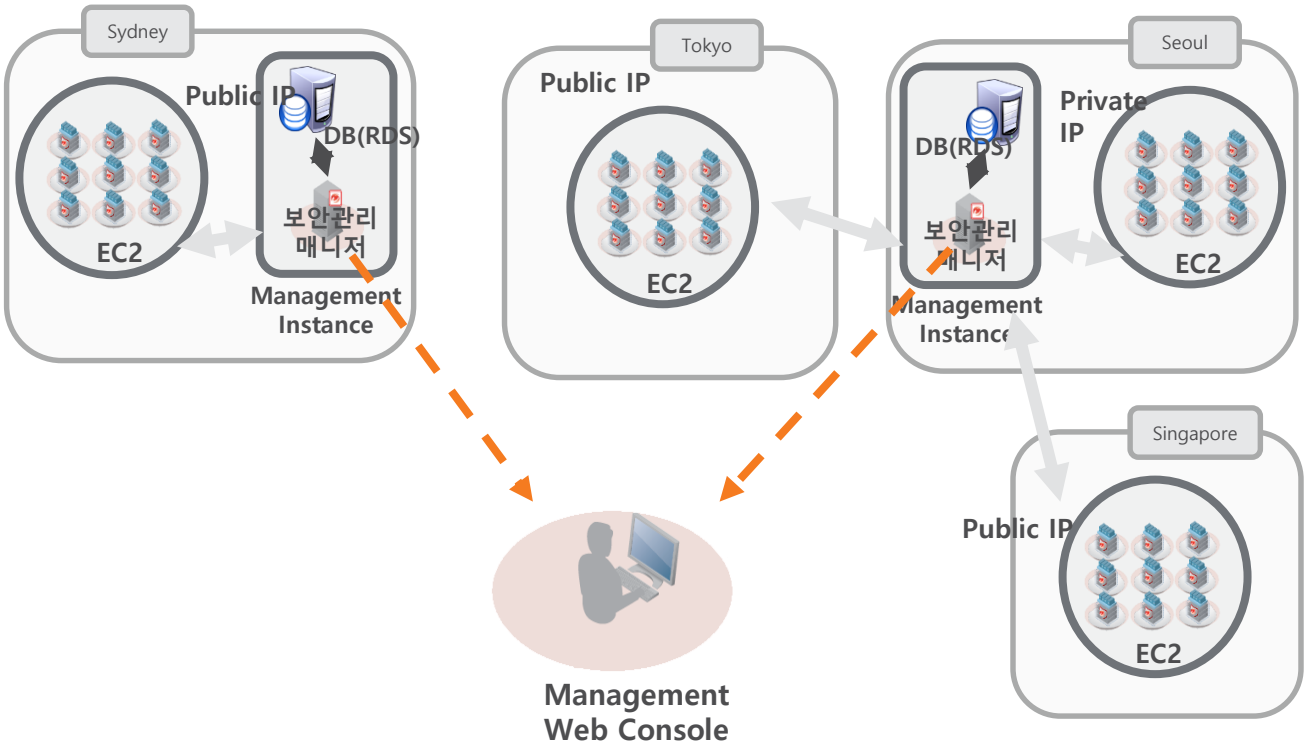
1. AWS 환경에서의 DS 구성 방안

2. AWS 환경에서의 DS 보안 관제 방안

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 환경에서의 DS 구성 방안

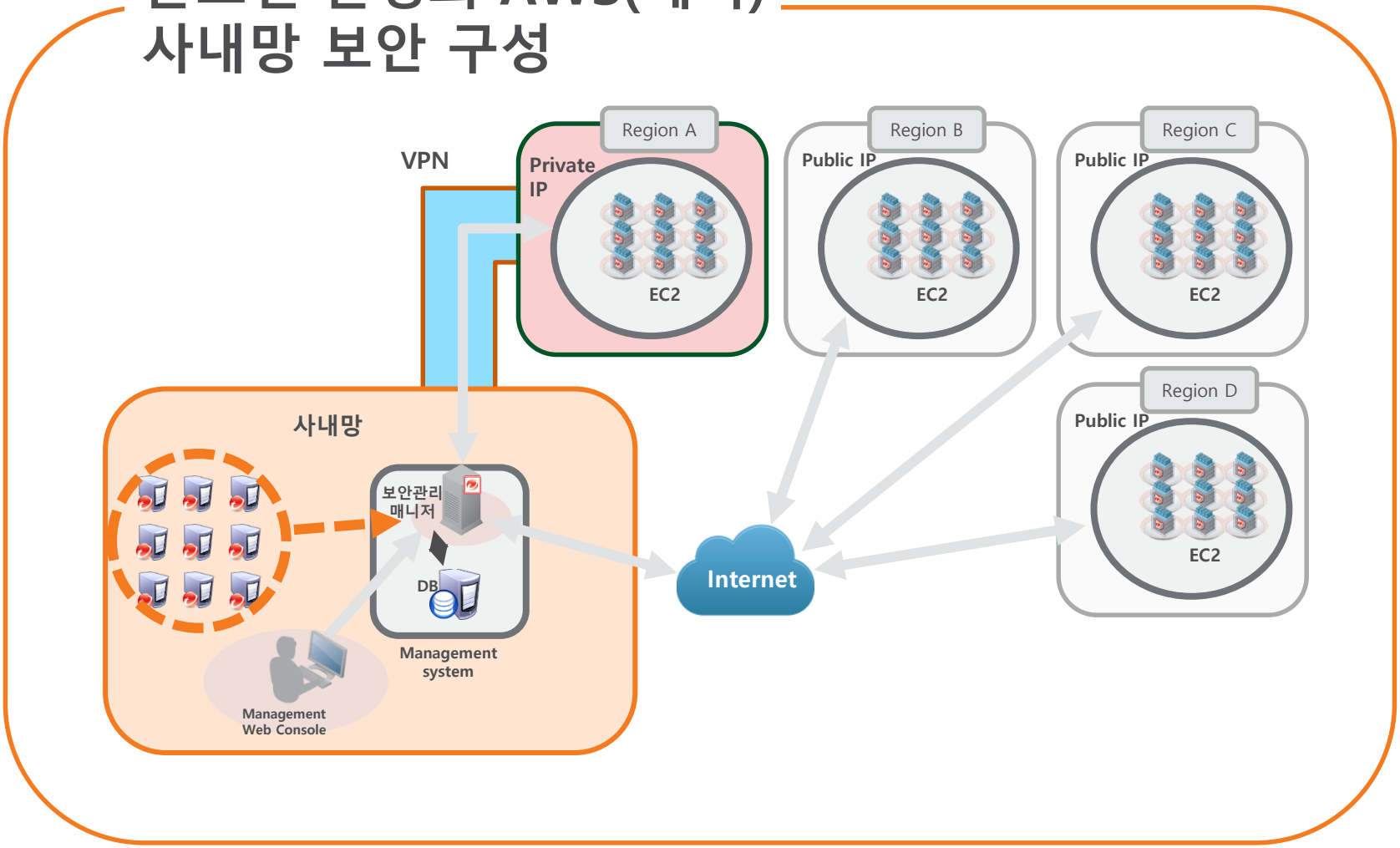
글로벌 환경의 AWS(예시) 리전 별 연결 보안 구성



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

AWS 환경에서의 DS 구성 방안

글로벌 환경의 AWS(예시) 사내망 보안 구성



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Deep Security 추가 소개

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

Compliance 대응 (PCI-DSS)

PCI DSS Requirement	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

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

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)

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

서버 보안 7년 연속 세계 1위

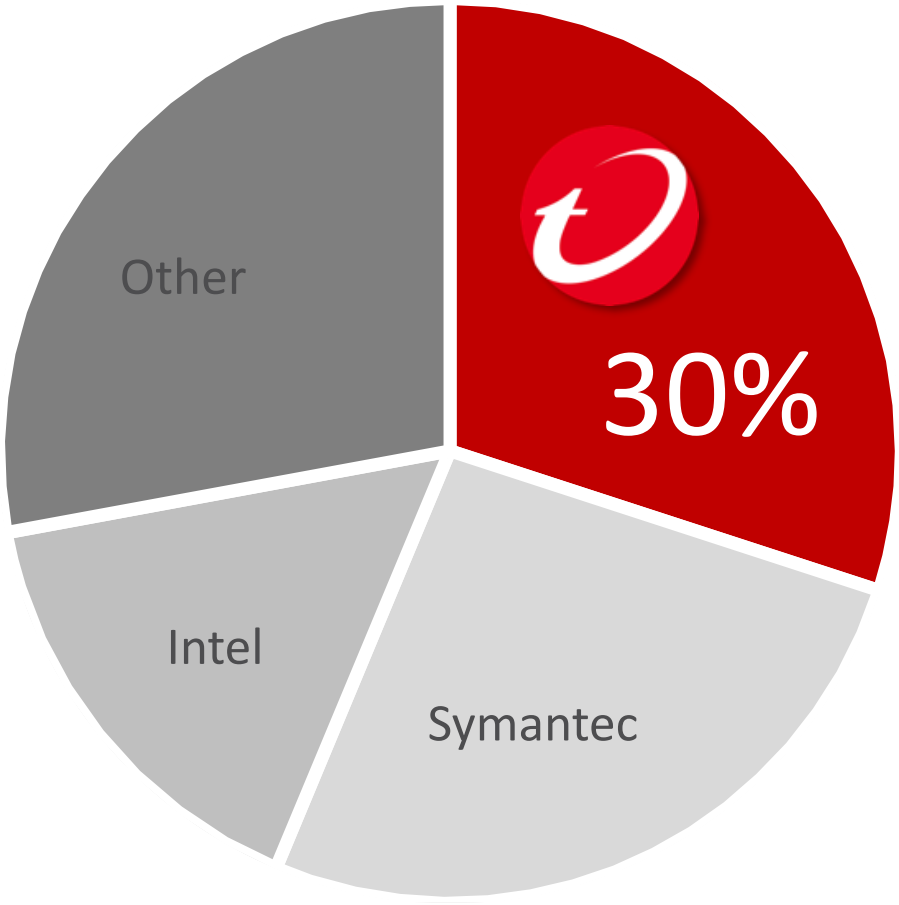
The MARKET LEADER

in server security for

7 straight years

IDC

Analyze the Future

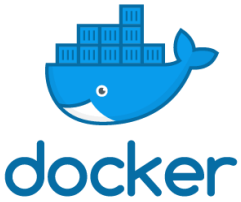


Source: IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

TREND MICRO

클라우드 서비스에서 입증된 기능



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

참고 (Gartner Best Practices)

Best Practices for Securing Workloads in Amazon Web Services

http://bit.ly/1pxaFTL

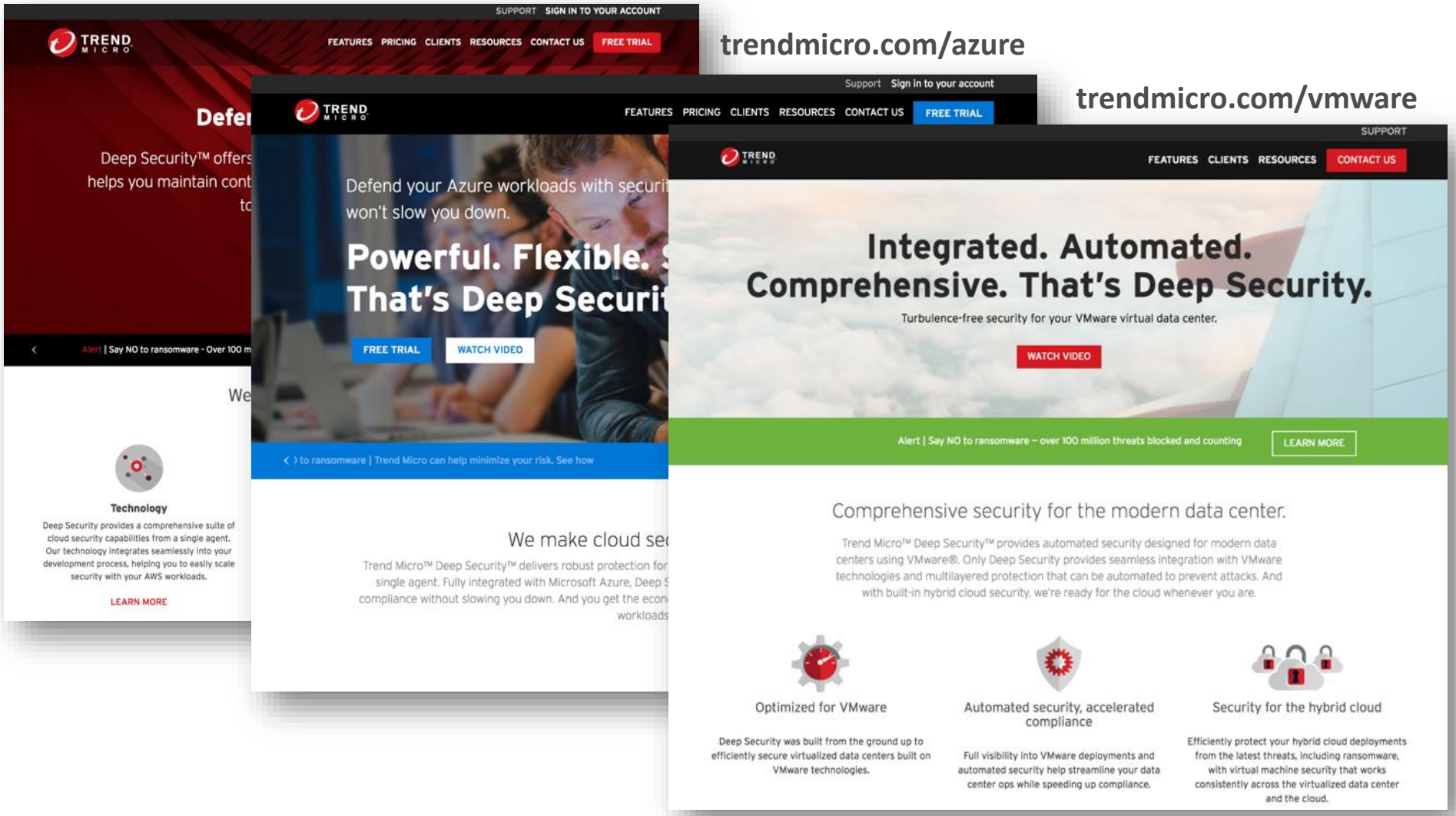
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

참고 (cloud)

trendmicro.com/aws

trendmicro.com/azure

trendmicro.com/vmware



Copyright © 2016 Trend Micro Incorporated. All rights reserved.

감사합니다!