TREND MICRO

Security
TRENDS 2018

하이브리드 클라우드 환경에서의 도커/컨테이너 보안 적용방안

트렌드마이크로
양희선 부장

요약

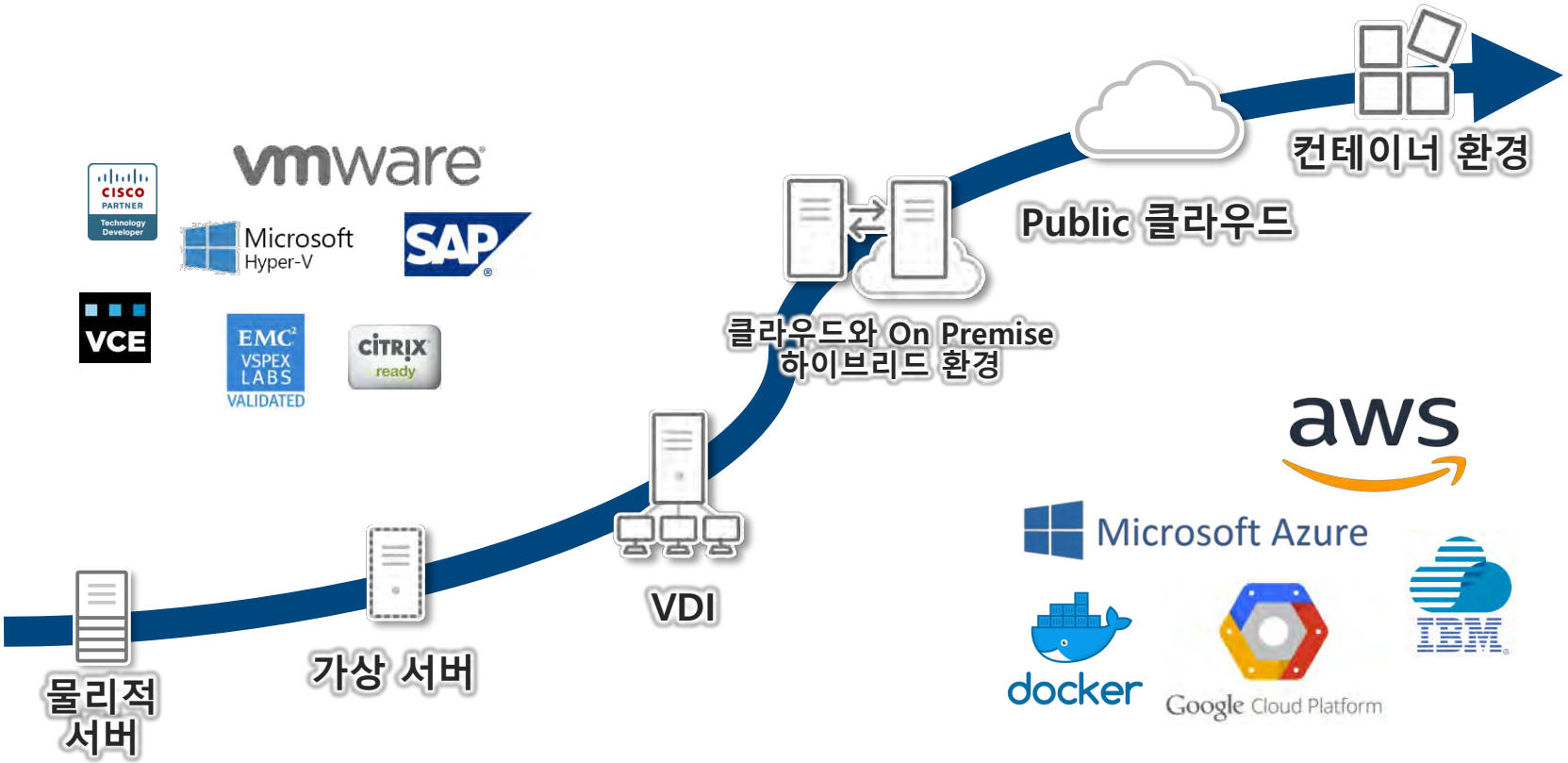
TREND MICRO | Security TRENDS 2018

하이브리드 클라우드 보안

- 하이브리드 클라우드 내 보안 접근은 기존의 보안 적용 방식과 많은 차이점이 있습니다.
  따라서 하이브리드 클라우드 워크로드(도커+컨테이너)에서는
  기존과 다른 차별화된 보안 적용이 매우 중요합니다.
- 본 내용에서는 하이브리드 클라우드 워크로드(도커+컨테이너)
  에서의 차별화된 보안 적용 필요성을 알아보고 트렌드마이크로의
  Deep Security 를 통한 최적의 보안 적용 방법을 살펴보겠습니다.

클라우드 보안이란?

환경의 변화


vmware
CISCO PARTNER Technology Developer
Microsoft Hyper-V
SAP
VCE
EMC² VSPEX LABS VALIDATED
CITRIX ready
컨테이너 환경
Public 클라우드
클라우드와 On Premise 하이브리드 환경
VDI
가상 서버
물리적 서버
aws
Microsoft Azure
docker
Google Cloud Platform
IBM

Hybrid Cloud 환경

Physical Servers

Virtual servers

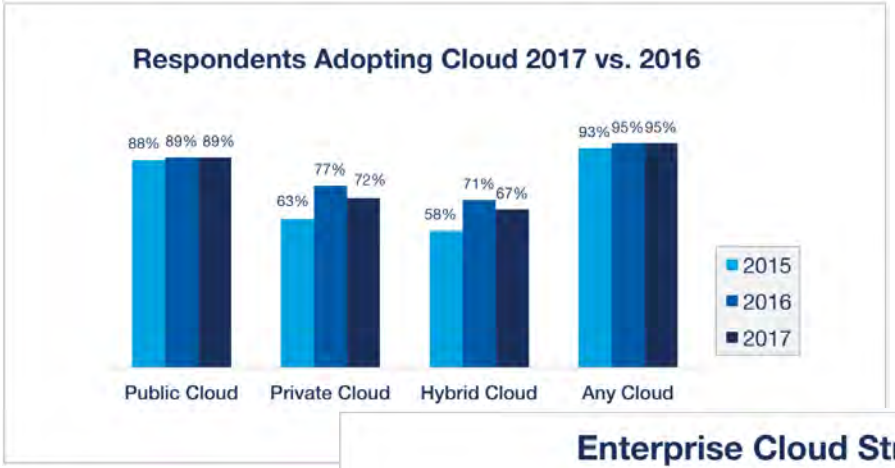
+

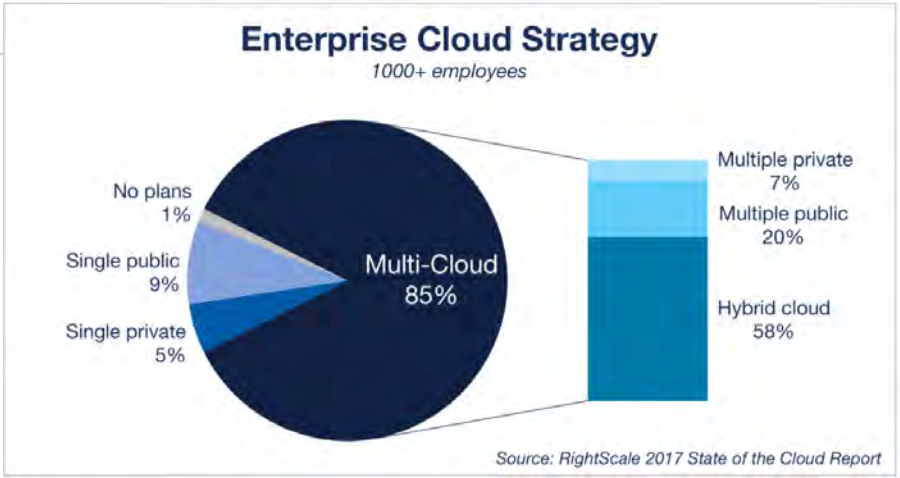
Public Cloud

+

Private Cloud

하이브리드 클라우드 도입

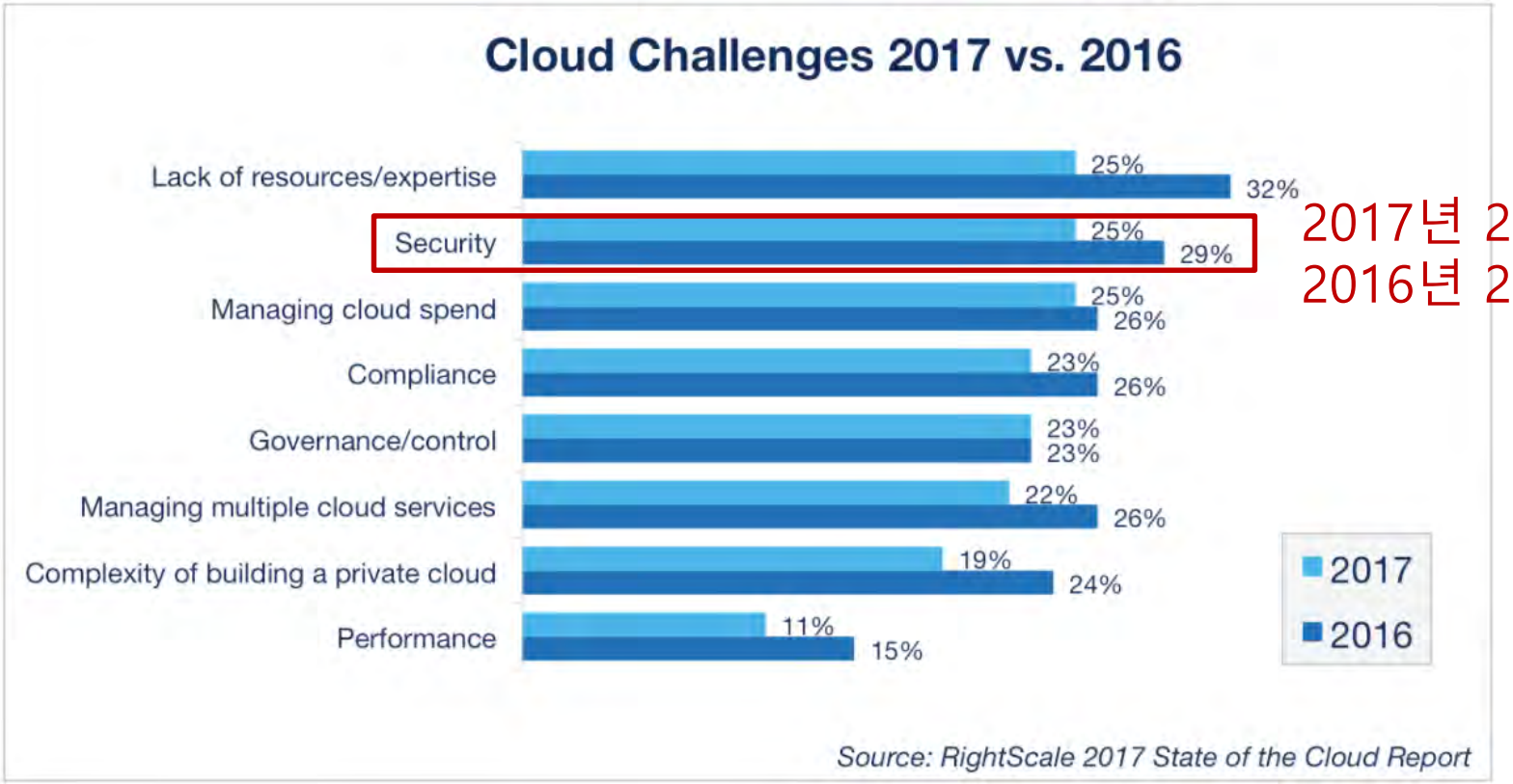




85%

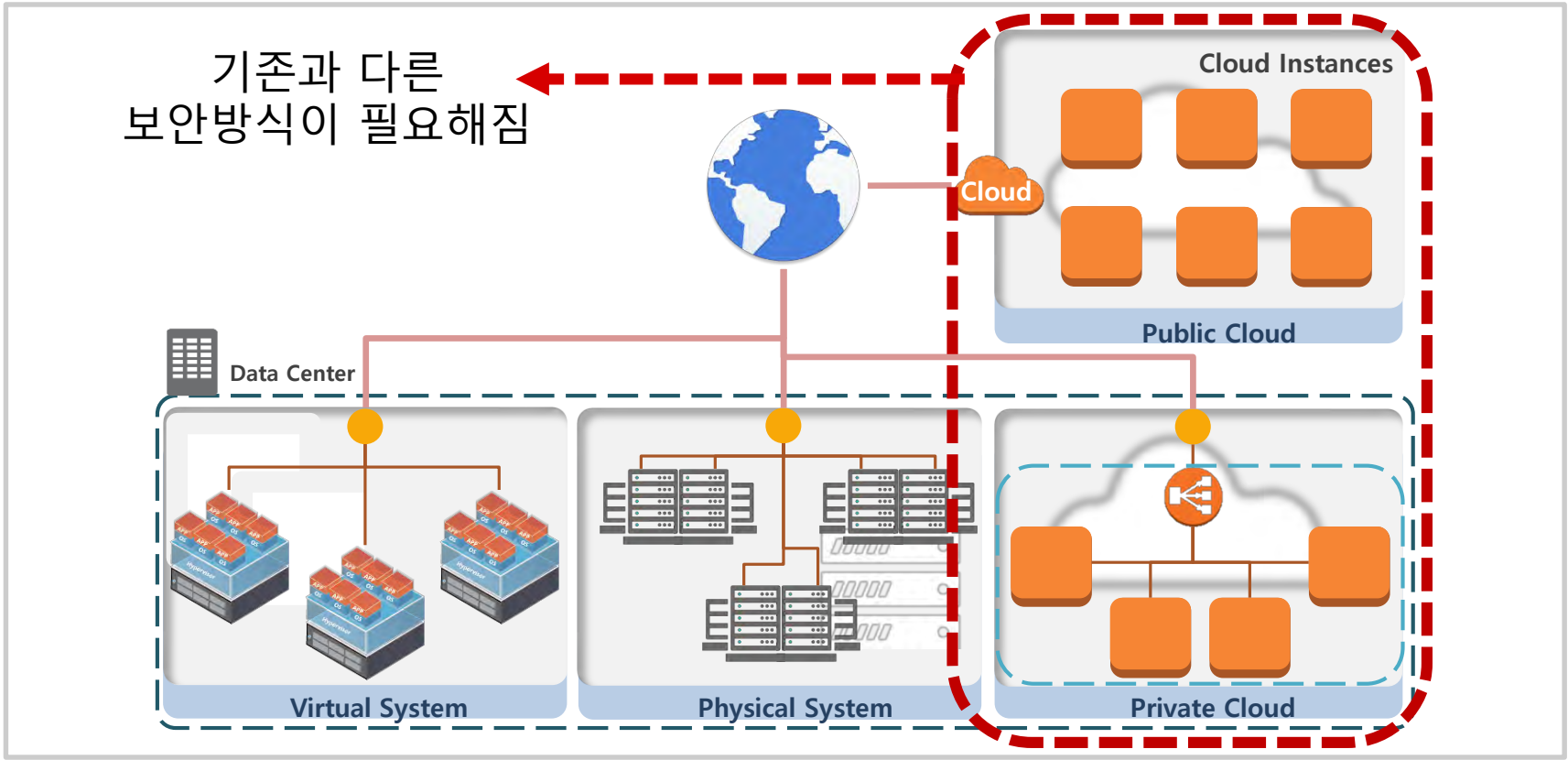
하이브리드 클라우드로 전환 계획을 가진 기업

클라우드 도입 시 방해 요소



2017년 2위
2016년 2위

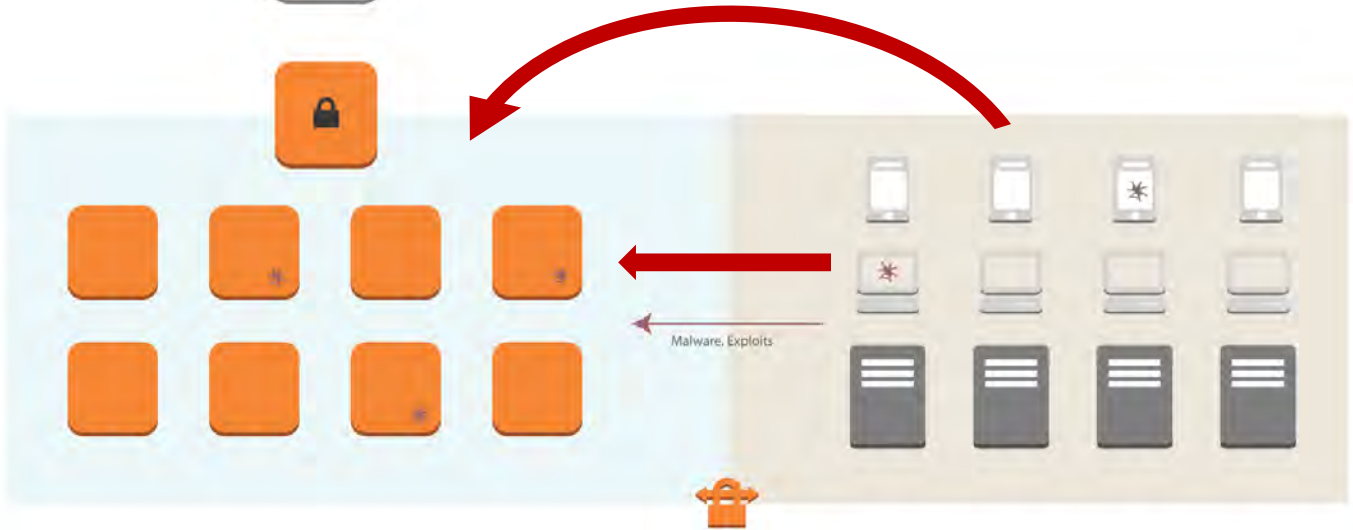
클라우드 보안 구현 방향


기존과 다른
보안방식이 필요해짐
Cloud Instances
Cloud
Public Cloud
Data Center
Virtual System
Physical System
Private Cloud

하이브리드 환경 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



Shared Responsibility : Cloud

Cloud	You
Physical	Operating System
Infrastructure	Applications
Network	Data
Virtualization	Service Configuration

Shared Responsibility

Operating System

Applications

Data

Service Configuration

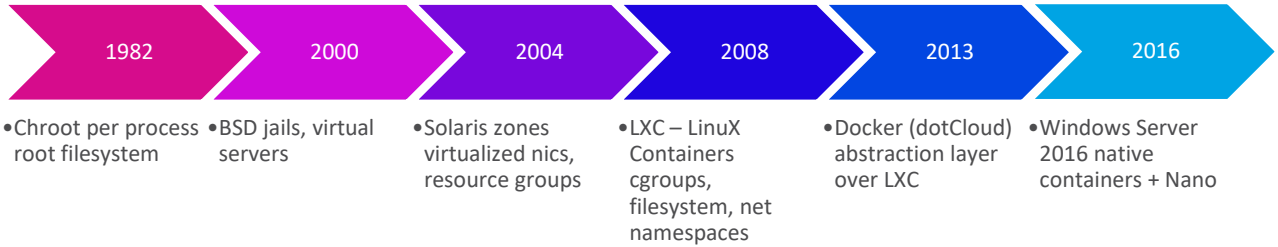
+

Security Solution

Docker 보안

Container 역사

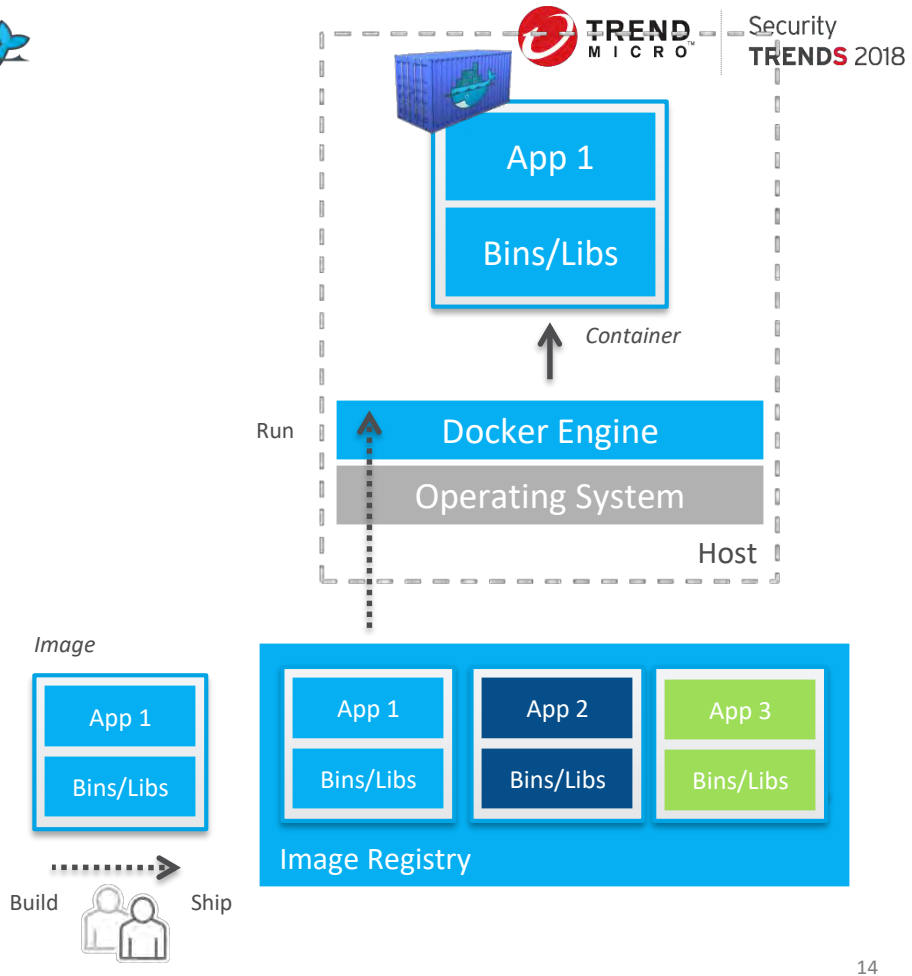
- 많은 컨테이너에서 Docker와 동의어로 사용
- 기반 기술은 시간이 지나면서 발전



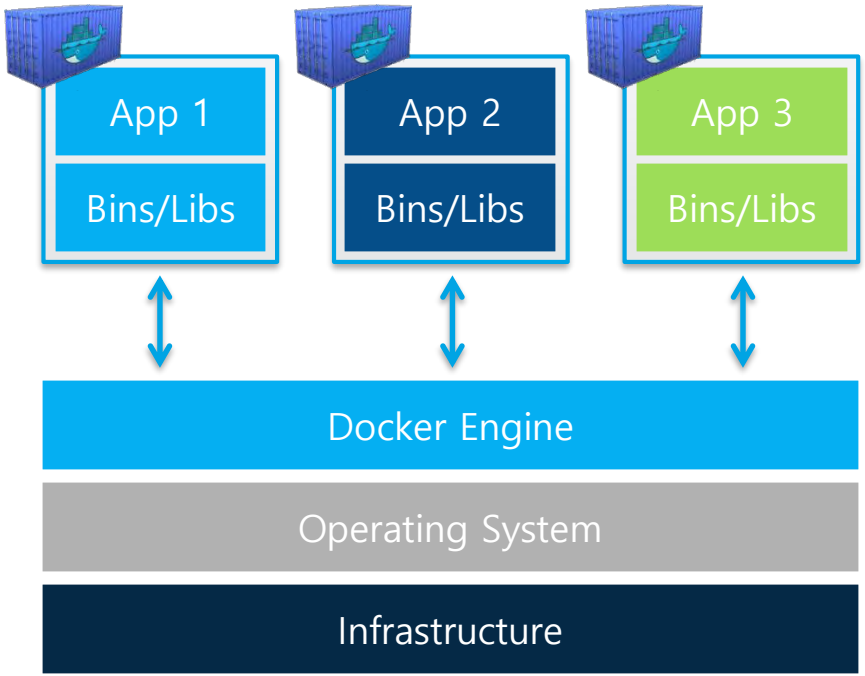
- 기타 컨테이너 기술
  - LXC (Linux Containers), rkt (CoreOS), Warden/Garden (Cloud Foundry), Solaris Zones…

Build, Ship, Run…

- **Build**
  - 빌드 프로세스가 이미지를 생성합니다.
  - 이미지에는 응용 프로그램 및 종속성이 포함됩니다.
  - 그러나 기본 O/S가 아닙니다.
- **Ship**
  - 이미지가 레지스트리에 푸시.
- **Run**
  - Docker Engine을 사용하여 등록된 이미지를 가져온 다음 Docker호스트의 이미지에서 컨테이너 생성 및 실행

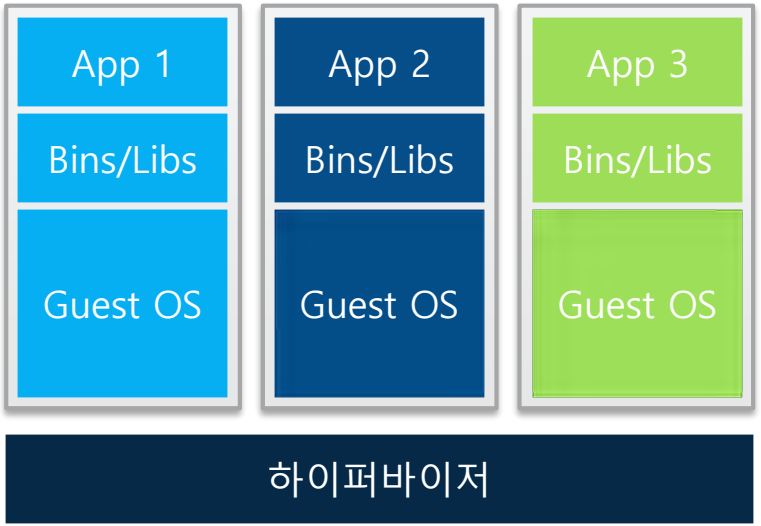


Docker + Container



컨테이너

- 개발자는 Docker+Container 선호!!!
  - VM보다 가벼운 Container(효율적인 리소스 관리)
  - 간편한 빌드, 배포



가상 머신

기존 워크로드 vs. Container 워크로드

기존 워크 로드	컨테이너 워크 로드
OS 포함	공통 호스트 OS 공유
단일 애플리케이션	마이크로 서비스
Long-lived	Short-lived 또는 임시
릴리스로 제공	CI / CD
제한적인 이식성	호환 엔진을 가진 모든 플랫폼

기존 어플리케이션을 호스트 OS및 컨테이너용 애플리케이션에 적용할 수 있지만, 컨테이너 워크로드를 위해서는 이미지를 새로 만들거나 완전히 새로운 방식으로 구축/적용해야 합니다.

Docker를 주목하는 이유

가상 머신보다 가벼운 컨테이너

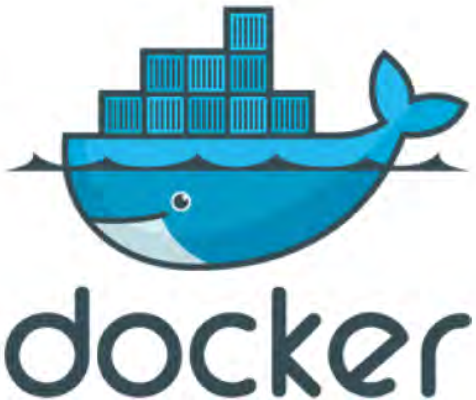
→ 효율적인 리스스 공유

이미지 빌드, 이미지 배포, 이미지 롤백

→ 서비스의 상태를 관리

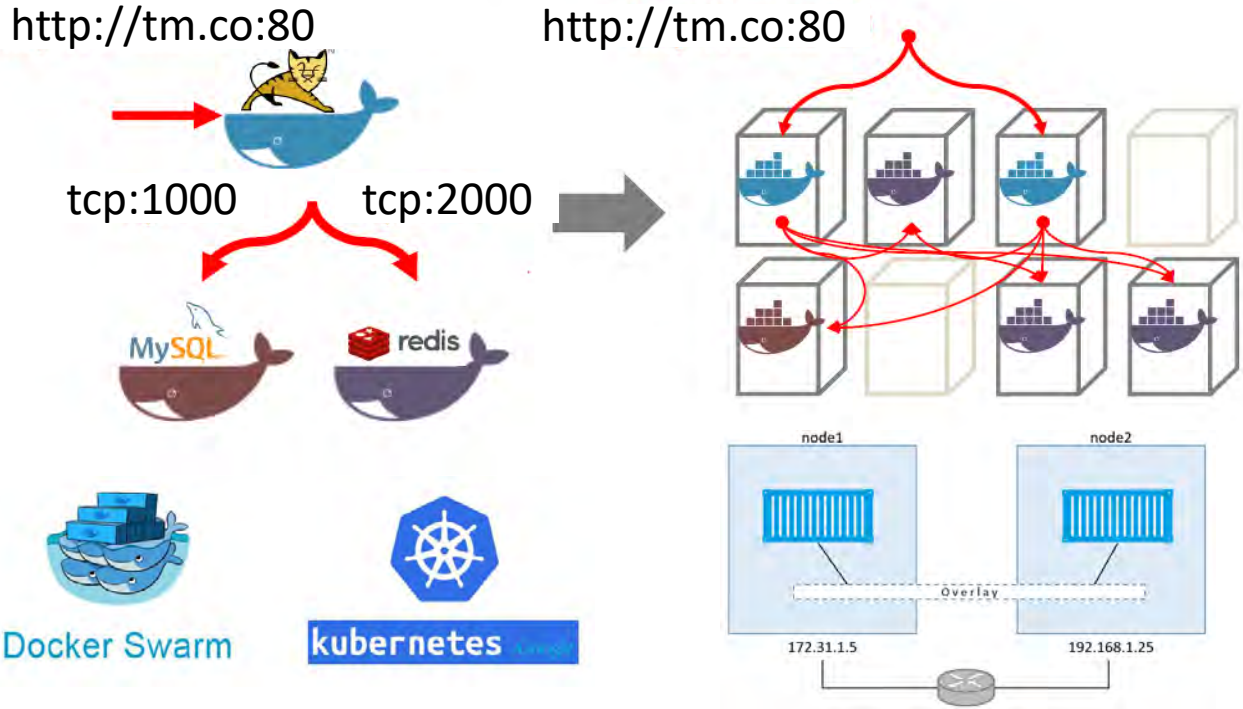
“Write Once, Run Anywhere”

→ 빌드/배포를 단순하게



Docker 오케스트레이션(Orchestration)

여러 개의 컨테이너로 하나의 서비스를 구성하는 것



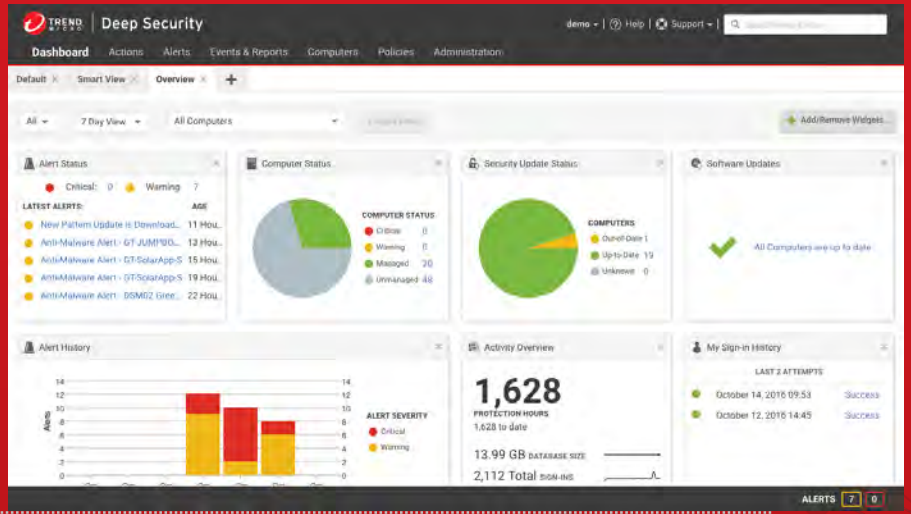
Docker Orchestration

Source: https://containerd.io/

Container 플랫폼들

Kubernetes	Swarm	Mesosphere	Amazon ECS	Cloud Foundry
• Google Container Engine • CoreOS Tektonic • Openshift (Redhat) • Azure	• Docker Datacenter • Azure • DIY	• Azure • DCOS		• IBM Bluemix • Pivotal CF

Deep Security



Deep Security 기능

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

취약점 방어(가상 패치)

Web어플리케이션의 취약점을 보호

OS나 어플리케이션의 취약점을 보호

애플리케이션을 가시화하고 통제

방화벽을 통하여 공격을 받을 기회를 경감

방화벽

안티 멀웨어 (백신)

악성 프로그램 공격에서 보호

중요한 보안 이벤트를 로그에서 효율적으로 발견

로그 감사 Log Inspection

무결성 모니터링 Integrity Monitoring

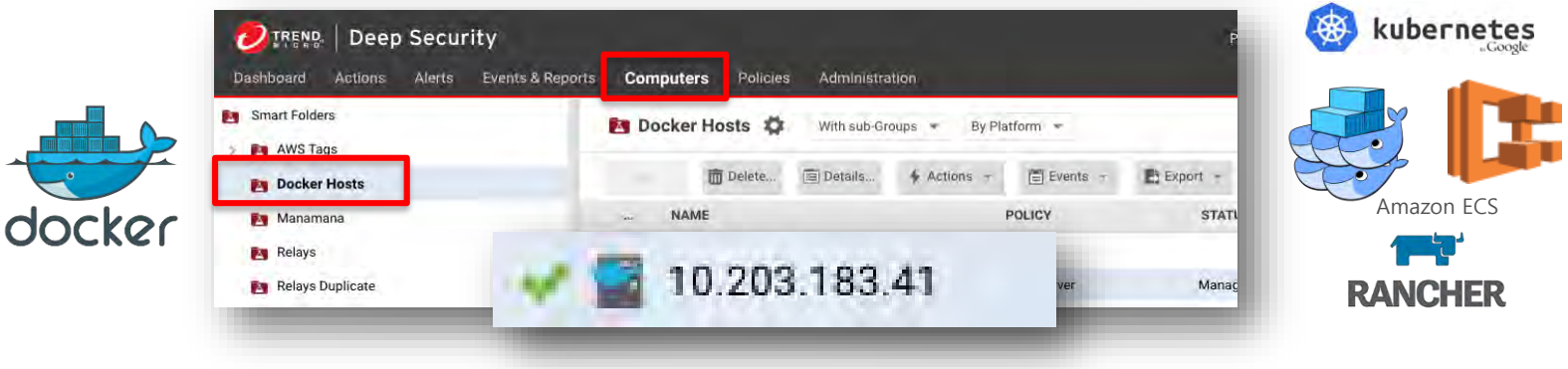
디렉토리, 파일, 레지스트리 등의 이상 변경을 감지

응용프로그램 제어 Application Control

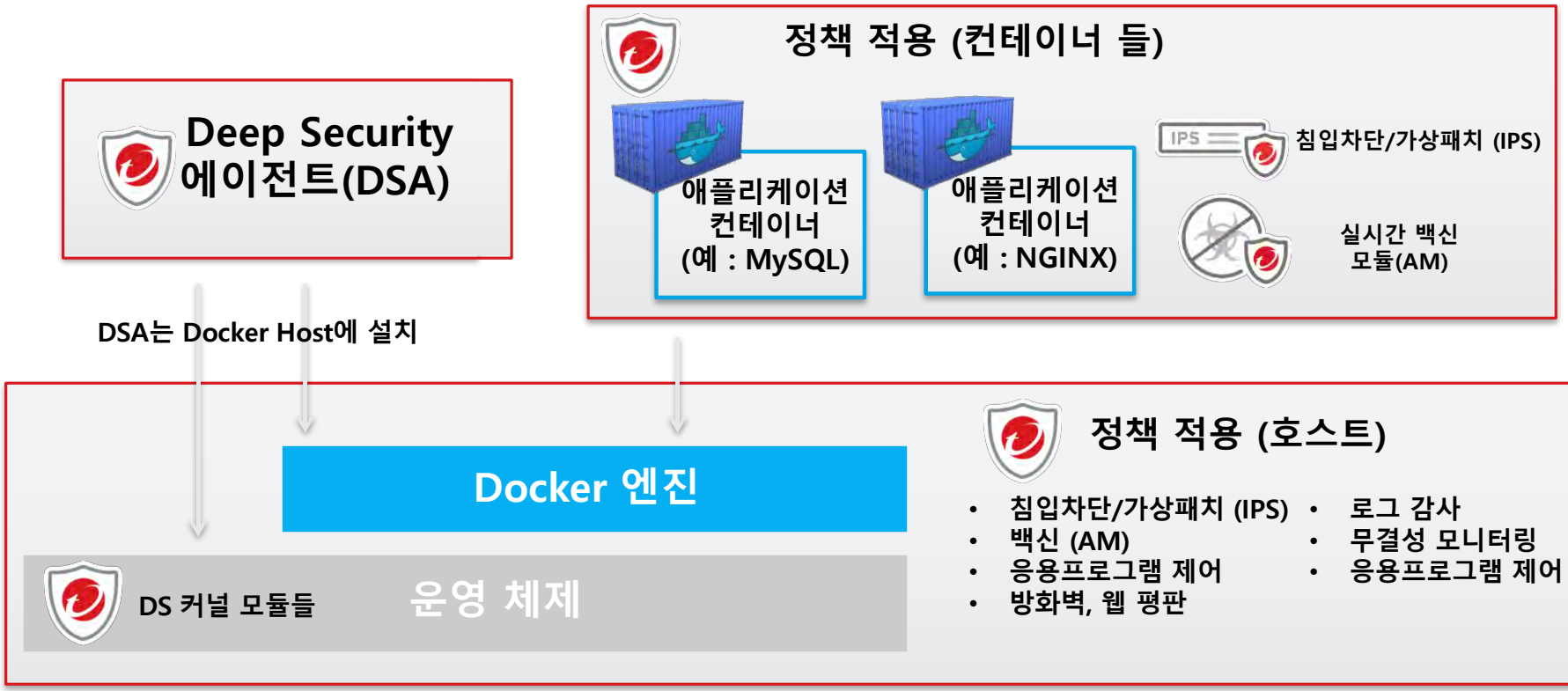
비인가 응용 프로그램을 차단

Docker 보안

- 호스트와 Docker 컨테이너를 안전하게 보호
- 모든 워크로드에서 일관된 보안 유지



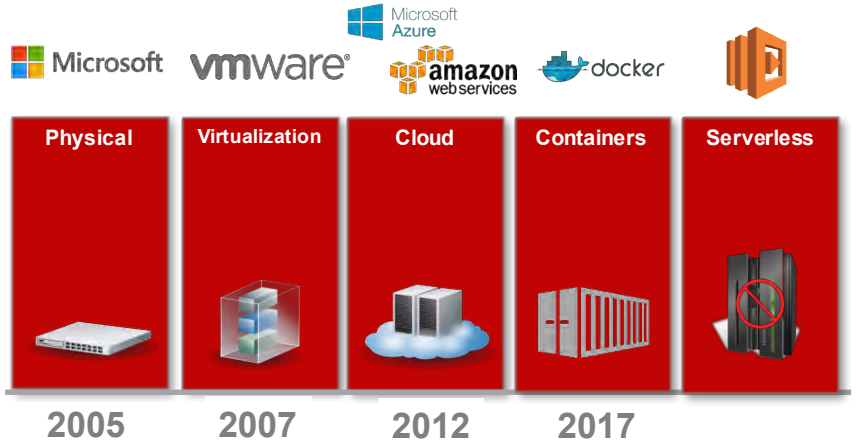
Docker 보안


Deep Security
에이전트(DSA)
정책 적용 (컨테이너 들)
애플리케이션
컨테이너
(예 : MySQL)
애플리케이션
컨테이너
(예 : NGINX)
IPS
침입차단/가상패치 (IPS)
실시간 백신
모듈(AM)
DSA는 Docker Host에 설치
Docker 엔진
DS 커널 모듈들
운영 체제
정책 적용 (호스트)
• 침입차단/가상패치 (IPS)
• 백신 (AM)
• 응용프로그램 제어
• 방화벽, 웹 평판
• 로그 감사
• 무결성 모니터링
• 응용프로그램 제어

Docker 보안

다양한 컨테이너 플랫폼 지원

- DS 는 물리, 가상 서버 및 클라우드에서 지원 되는 보안 기능을 Docker 컨테이너에 대한 부분도 지원
- DS 는 Amazon ECS, Docker Datacenter, Kubernetes, Docker Swarm, Rancher 등과 같은 다양한 오케스트레이션 컨테이너 플랫폼에서 사용

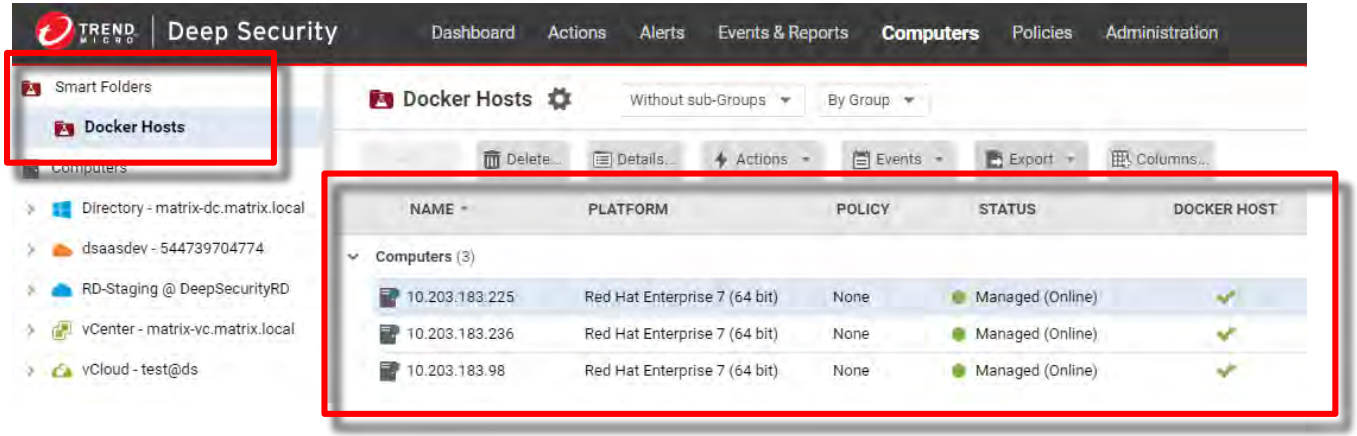


Swarm kubernetes Amazon ECS RANCHER

Docker 보안

설치된 Docker 호스트에 대한 가시성 제공

Docker 서비스를 하는 서버들은 DSM (Deep Security Manager)에서 스마트 폴더로 구성하여 쉽게 찾고 적용 할 수 있습니다.

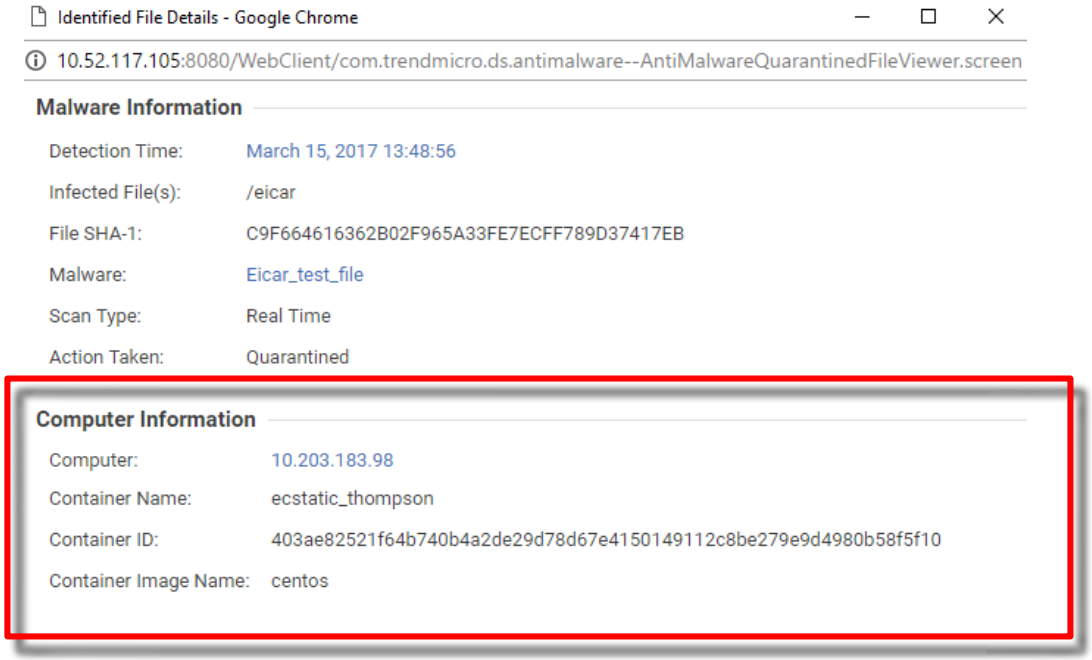


Docker 보안

TREND MICRO | Security TRENDS 2018

컨테이너 세부 정보 제공(악성코드 탐지/차단 시)

- 컨테이너에서 탐지/삭제된 악성파일 이벤트의 경우 Deep Security에서 세부정보 제공
  - Container ID
  - Container 이름
  - Container 이미지 이름
- 컨테이너 정보는 외부에 전달 가능
  - 이벤트 전달 (Syslog 및 AWS SNS)
  - REST API



Docker 보안

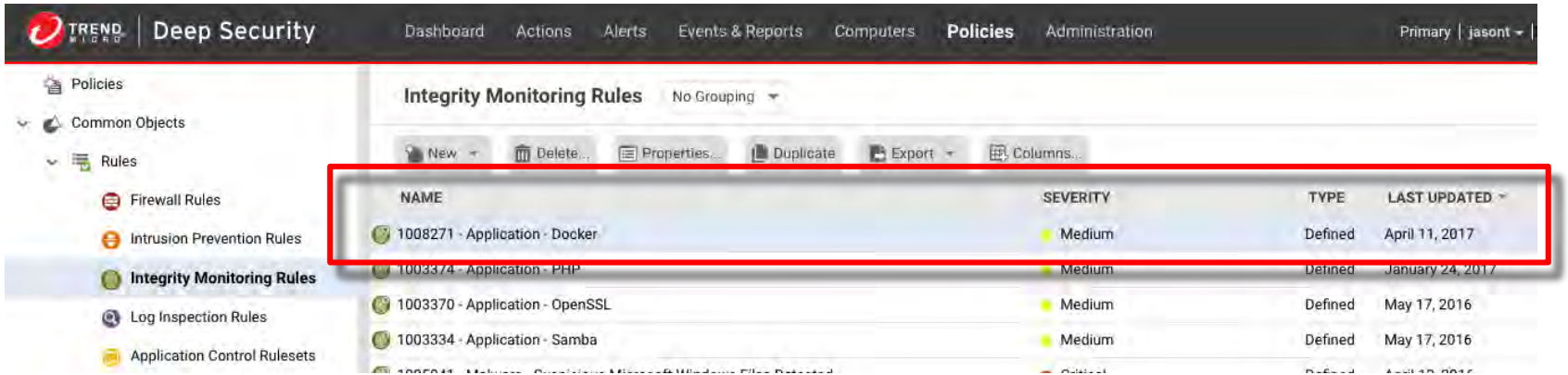
무결성 기능 룰(Rule) 제공

TREND MICRO | Security TRENDS 2018

docker

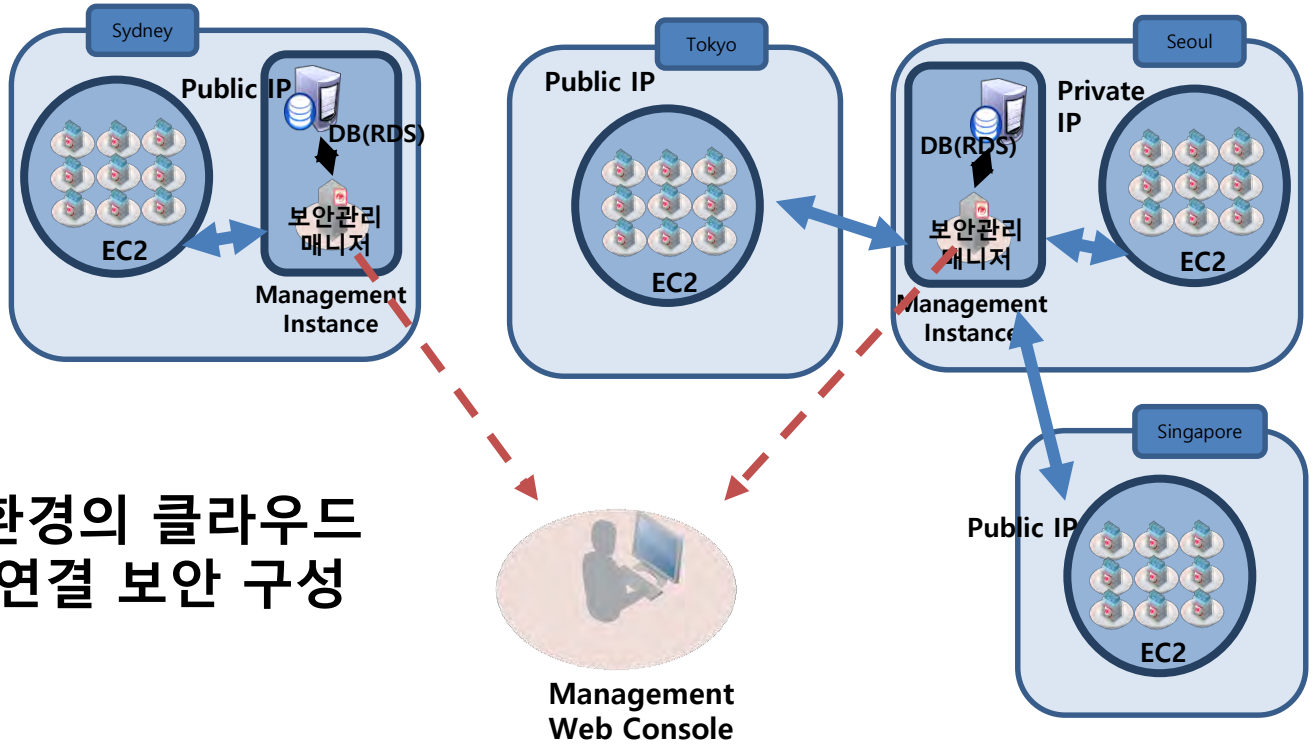
호스트 서버의 무결성 기능을 사용하여 Docker에 대한 설정 및 관리를 위한 무결성 기능 설정이 가능합니다.

- DSRU17-015에서 무결성 모니터링 규칙 (1008271)
- Docker 배포 시 컨테이너를 보호하기 위한 추가 규칙을 제공 예정



추가 내용

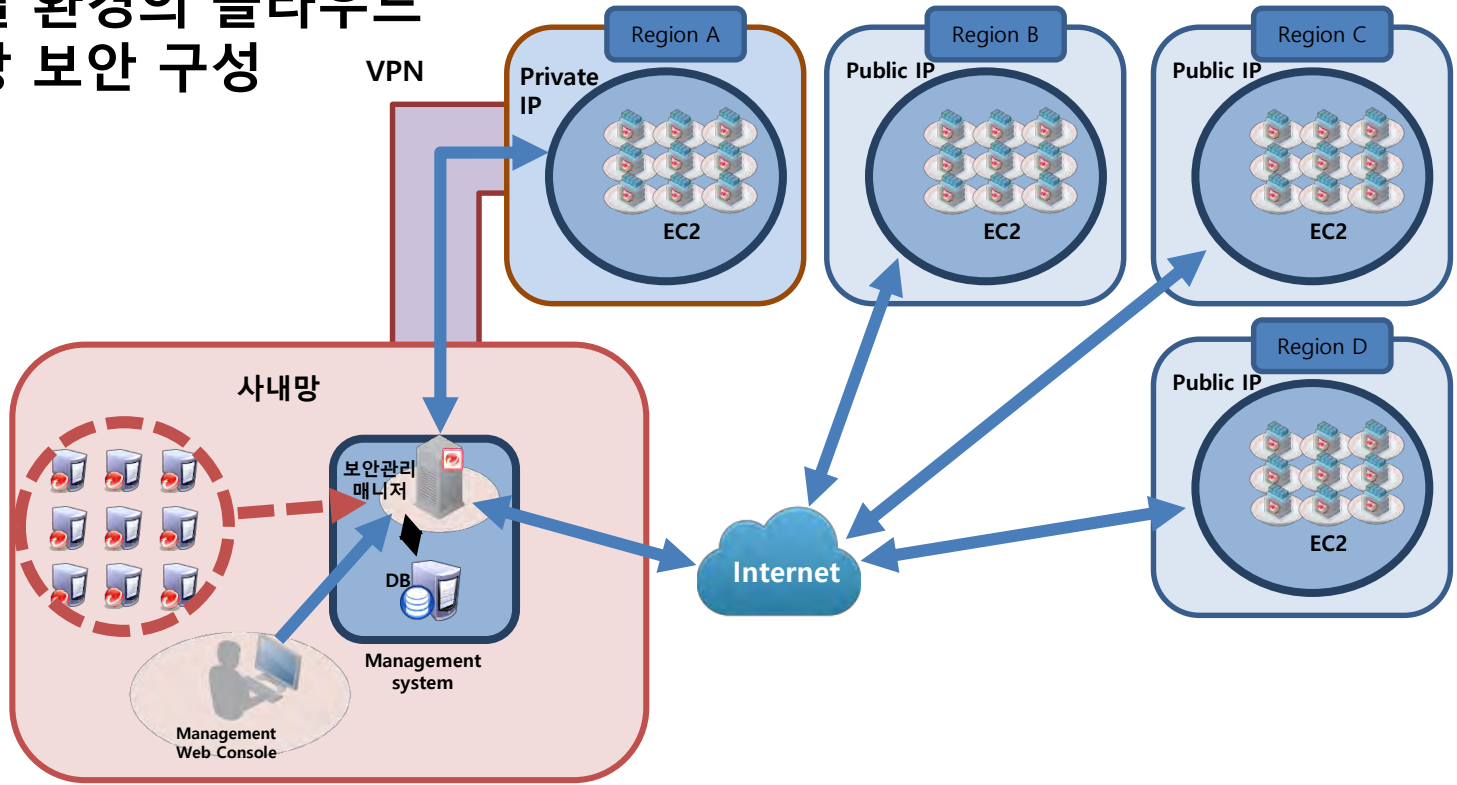
클라우드 환경에서의 구성 방안



글로벌 환경의 클라우드 리전 별 연결 보안 구성

클라우드 환경에서의 구성 방안

글로벌 환경의 클라우드 사내망 보안 구성

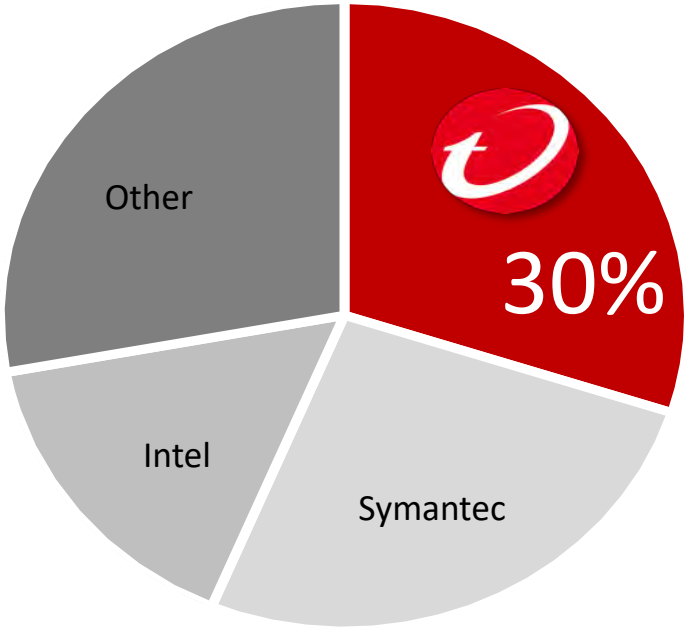


서버 보안 7년 연속 세계 1위

TREND MICRO | Security TRENDS 2018

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

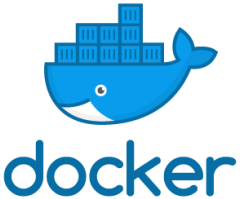
Compliance 대응 (PCI-DSS)

TREND MICRO | Security TRENDS 2018

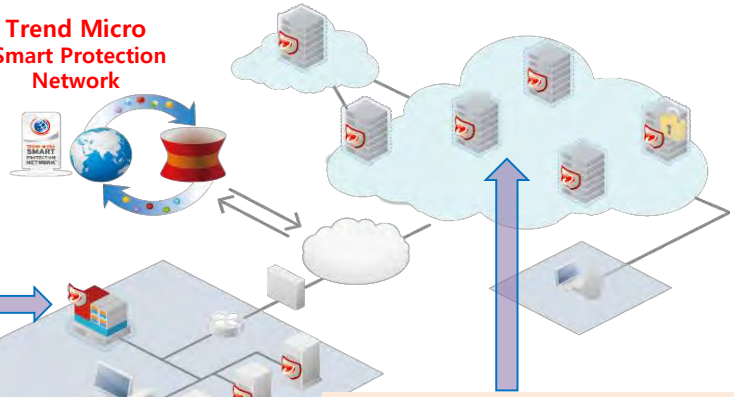
PCI

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

클라우드 서비스에서 입증된 기능



다양한 환경에 통합 보안 적용 및 관리



서버 가상화 환경

VMware ESXi

가상 머신 All in One 솔루션 보호

Deep Security Virtual Appliance

※ 환경에 따라 다양한 구성

VDI 환경

VMware Horizon View

VDI 환경에 적합함
에이전트리스 기반 보안 적용

Deep Security Virtual Appliance

퍼블릭/프라이빗 클라우드 환경

AWS, Azure, Google Cloud

퍼블릭 클라우드 환경에서
통합보안 제공

Deep Security Agent

물리서버 환경

Windows, RHEL, Ubuntu..

물리서버 환경에서 통합보안 제공

Deep Security Agent

TREND MICRO

Security
TRENDS 2018

THANK YOU!

클라우드 보안팀
양희선 부장