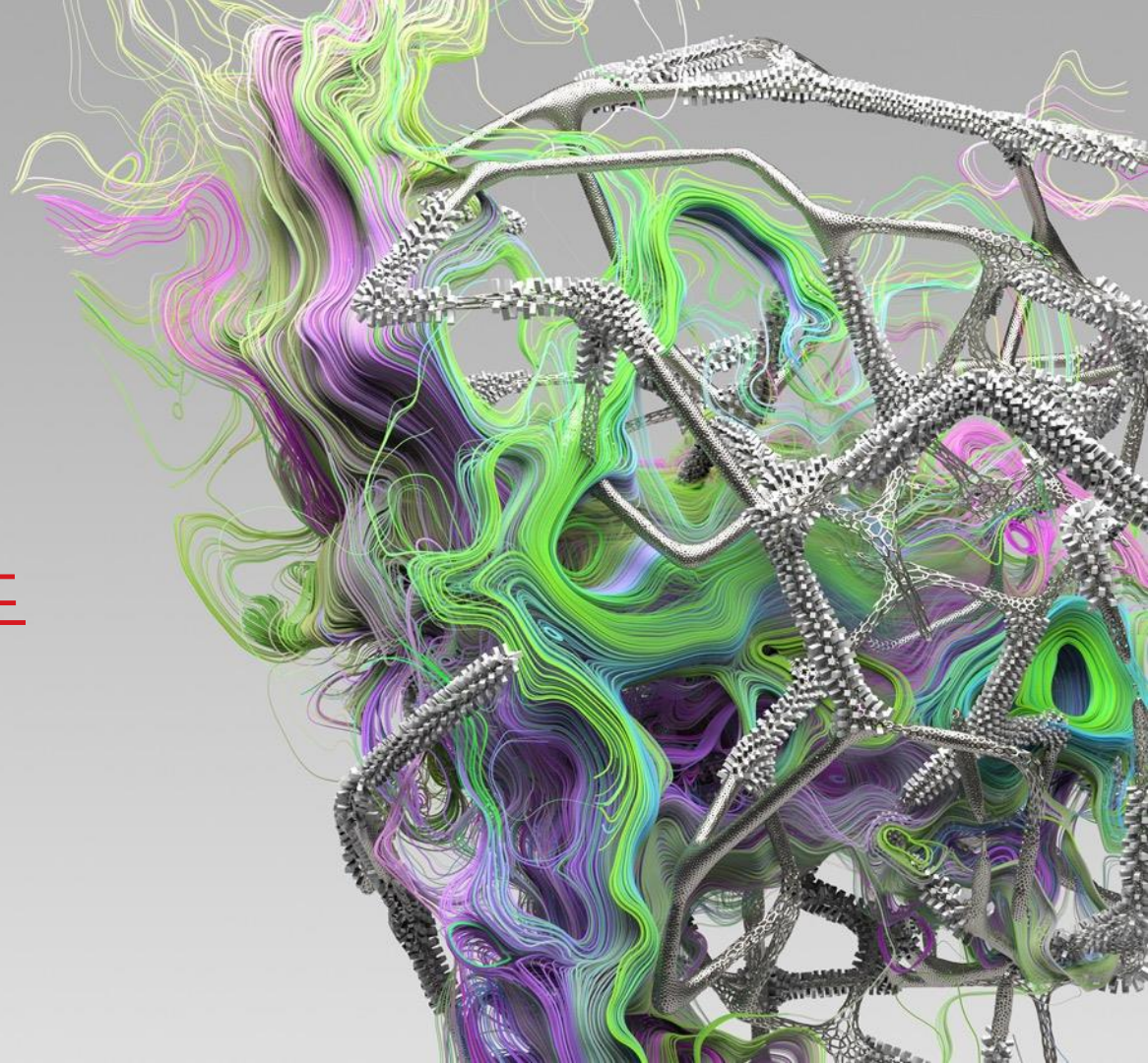
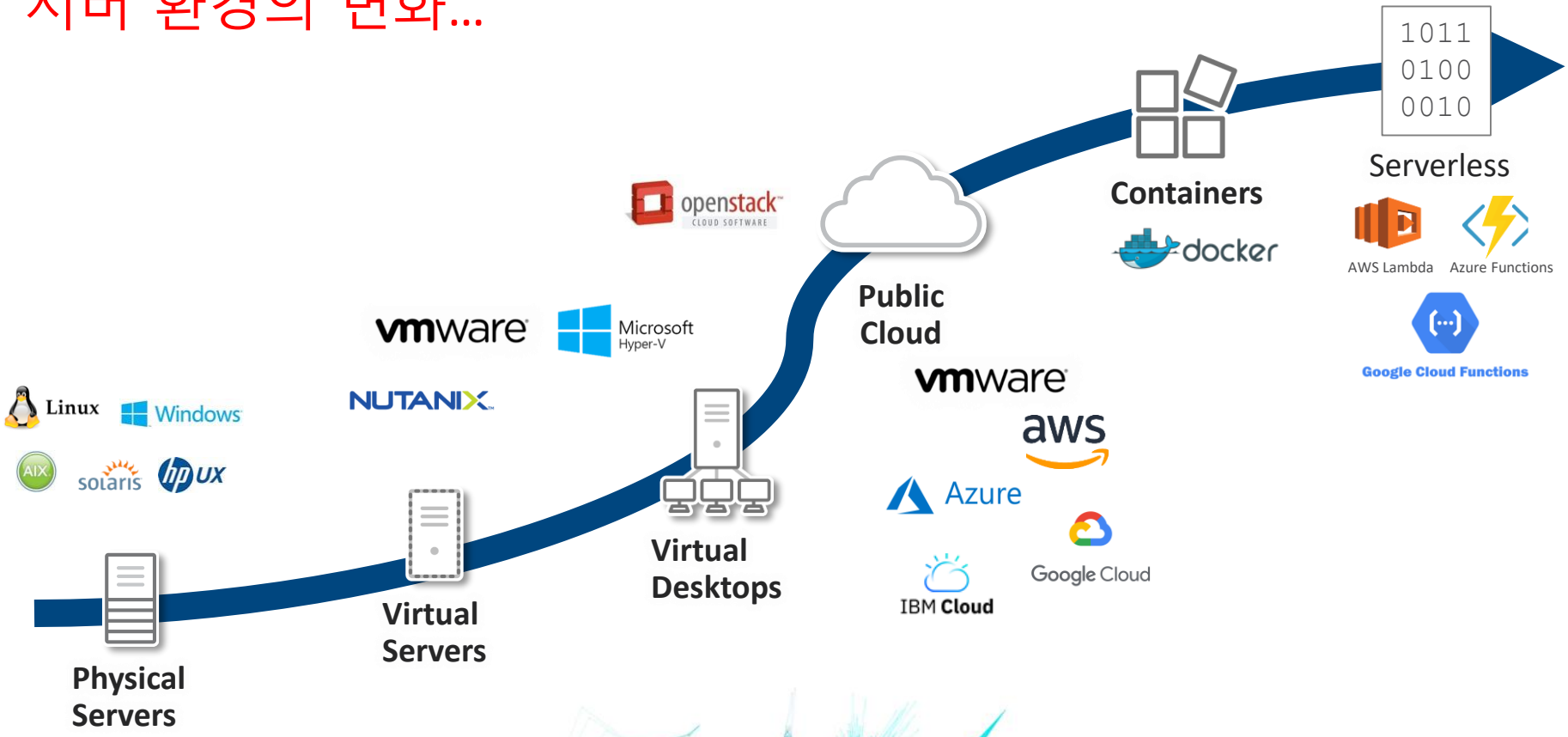


하이브리드 클라우드 보안을 위한 Deep Security

Trend Micro

서버 환경의 변화...



보안요구사항 for 하이브리드 클라우드

강력한 보안

악성코드방어 뿐만 아니라 **취약점 방어**, 허가되지 않은 **접근 제어**

일관된 보안 관리

다양한 환경에 동일한 보안정책관리, 하나의 보안관리 시점 제공

자동화된 보안관리

DevOps 파이프라인에 부담이 되지않는 **자동화된 보안**

하이브리드 클라우드를 위한 보안 적용범위

Build Pipeline

Image Scanning

Vulnerability Scanning

Malware Detection

Sweeping & Hunting

Runtime

Network Security

Intrusion Prevention

Firewall

Vulnerability Scanning

System Security

Application Control

Integrity Monitoring

Log Inspection

Malware Prevention

Anti-Malware

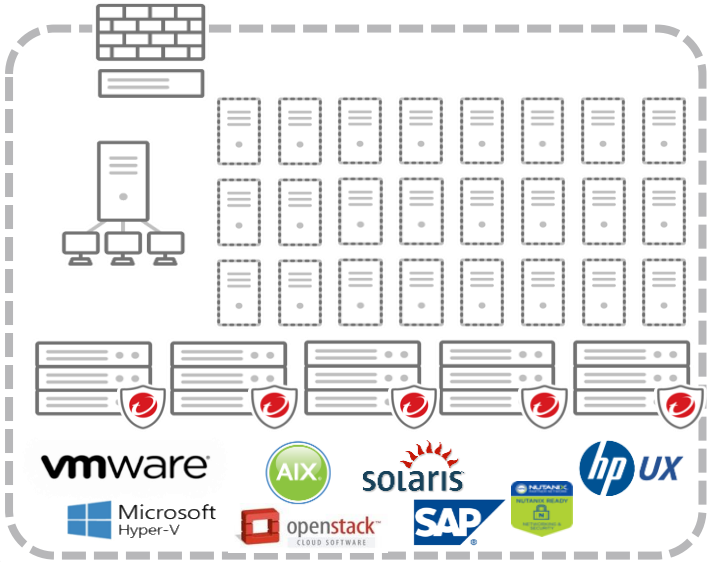
Behavioral Analysis Machine Learning

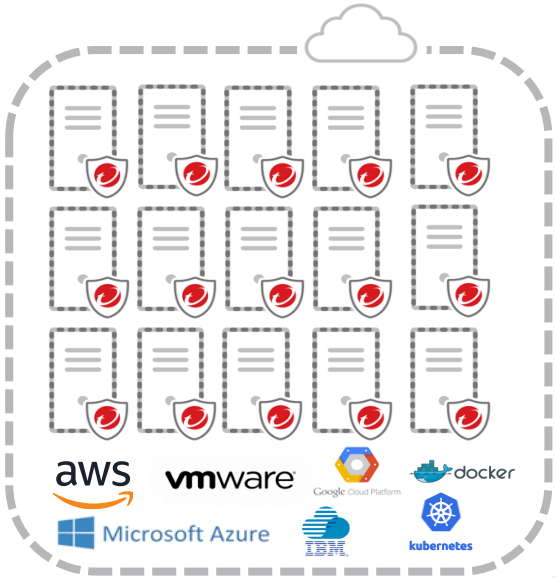
Sandbox Analysis

보안 요구사항 for 하이브리드 클라우드

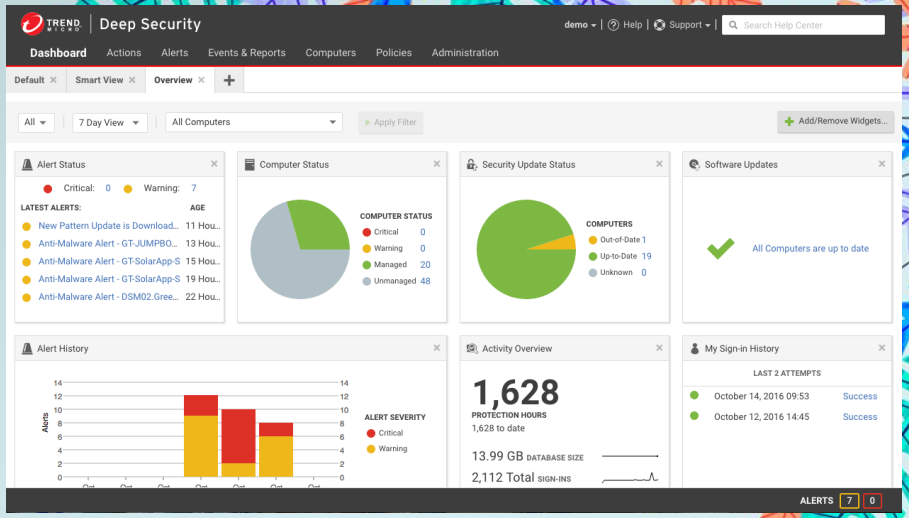
Hybrid Cloud Security

물리, 가상, 클라우드 및
컨테이너 배포에 대한
완전한 가시성을 갖춘
단일 보안 관리 콘솔



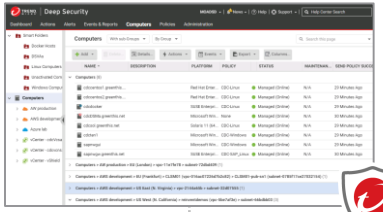


TREND MICRO



Deep Security 12

Deep Security - 클라우드 네이티브 보안솔루션



Deep Security

Data Center

vmware

NUTANIX

Microsoft Hyper-V

Public Cloud

aws

Azure

Google Cloud

Containers

docker

kubernetes

RED HAT OPENSHIFT

TREND MICRO

Deep Security for 하이브리드 클라우드 보안

Smart Check

Pre-deployment

Image Scanning

Vulnerability Scanning

Malware Detection

Sweeping & Hunting

Continuous image scanning for malware & vulnerabilities

Deep Security

Network Security

Intrusion Prevention

Firewall

Vulnerability Scanning

Stop network attacks, shield vulnerable applications & servers

Runtime / Deployed

System Security

Application Control

Integrity Monitoring

Log Inspection

Lock down systems & detect suspicious activity

Malware Prevention

Anti-Malware

Behavioral Analysis & Machine Learning

Sandbox Analysis

Stop malware & targeted attacks

Environments

Containers

Virtual Server

Data Center

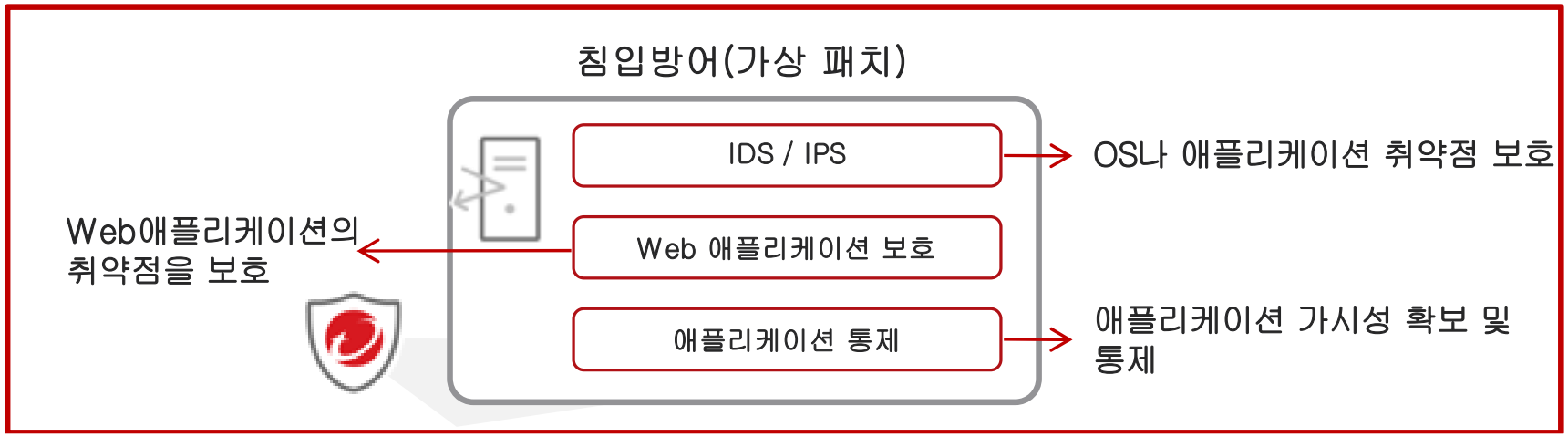
Cloud

Platforms

API & Integrations

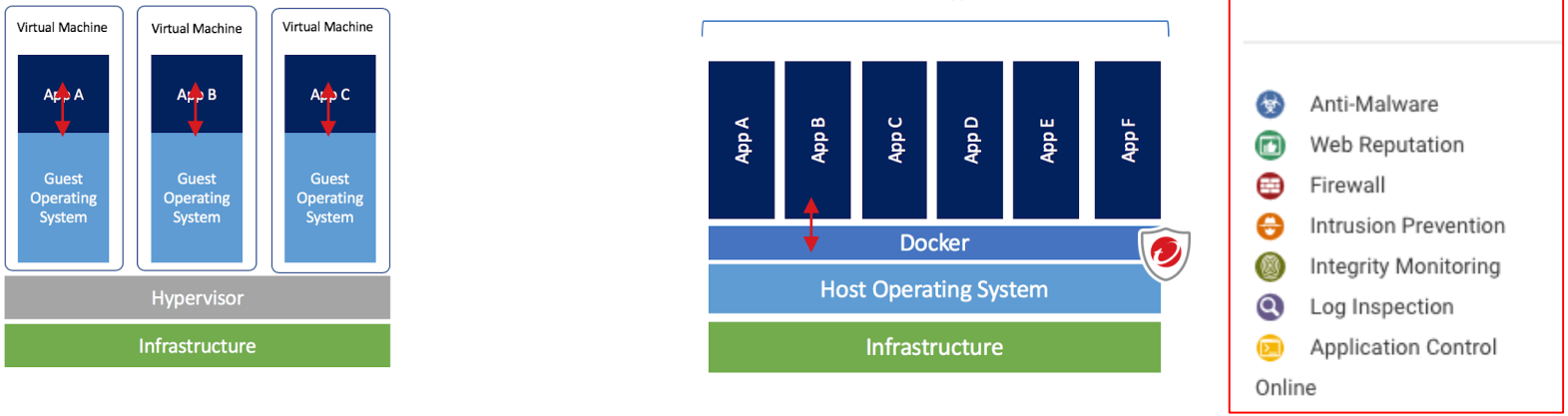
Deep Security – 통합서버보안솔루션(Runtime Protection)

방화벽 | 안티멀웨어 | 로그감사 | 무결성 모니터링 | 애플리케이션 제어



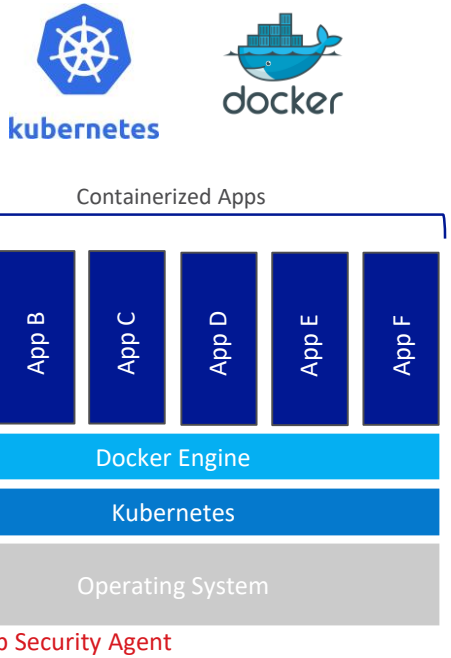
Deep Security – 도커 호스트 보호

- Docker에서 실행되는 컨테이너 애플리케이션은 호스트 커널 공유
- 도커 호스트가 손상되면 모든 컨테이너 공격 가능



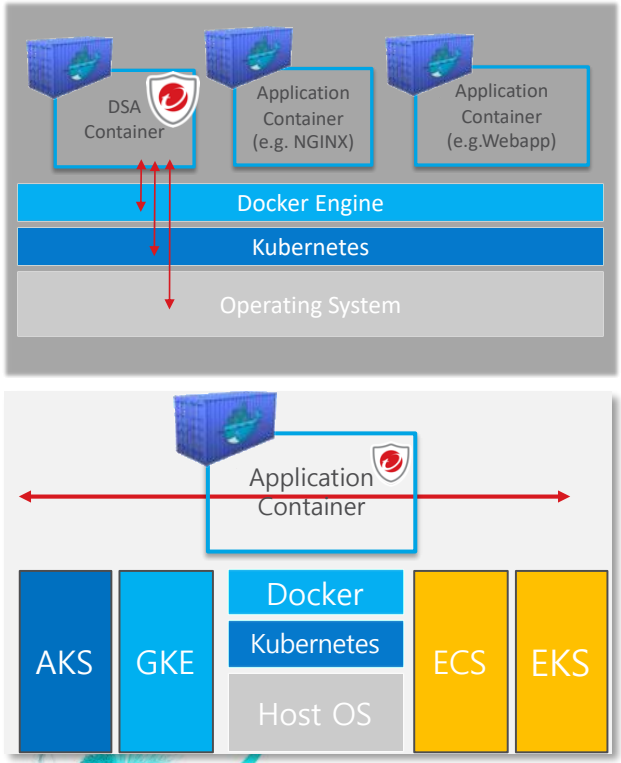
Deep Security – 쿠버네티스 및 도커 보호

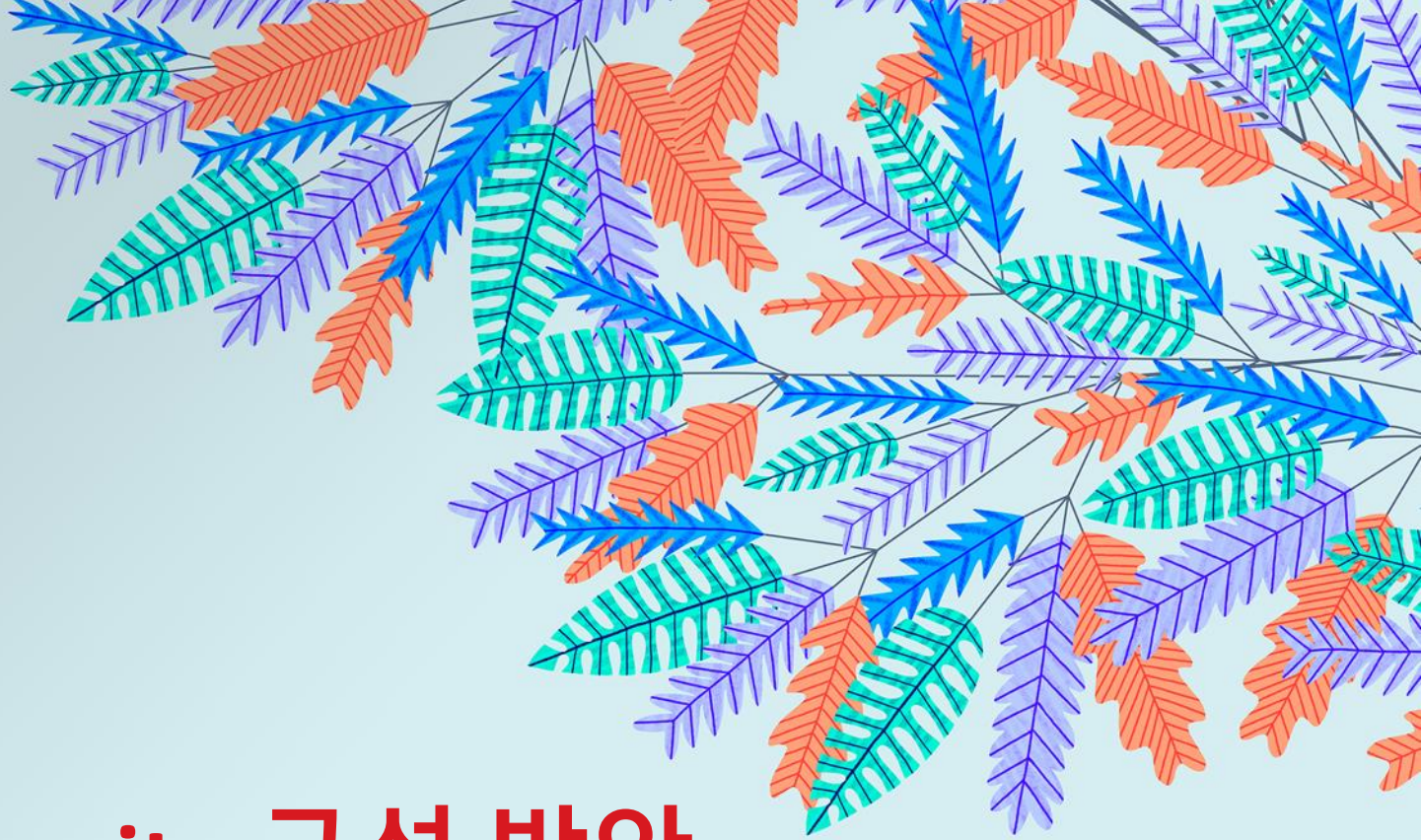
- 도커 & 쿠버네티스 주요 오브젝트 모니터링
  - 도커, 쿠버네티스 자동 감지
  - 소프트웨어 업/다운 그레이드, 삭제
  - 실행파일 속성 변경
  - 실행중인 프로세스, 데몬
    - etcd, Kubelet, Kube-apiserver
  - 주요 설정 파일
    - Config, certs, keys, yaml files
  - Iptables 룰
  - 주요 디렉토리 접근 권한



Deep Security – 애플리케이션과 동일하게 컨테이너 기반

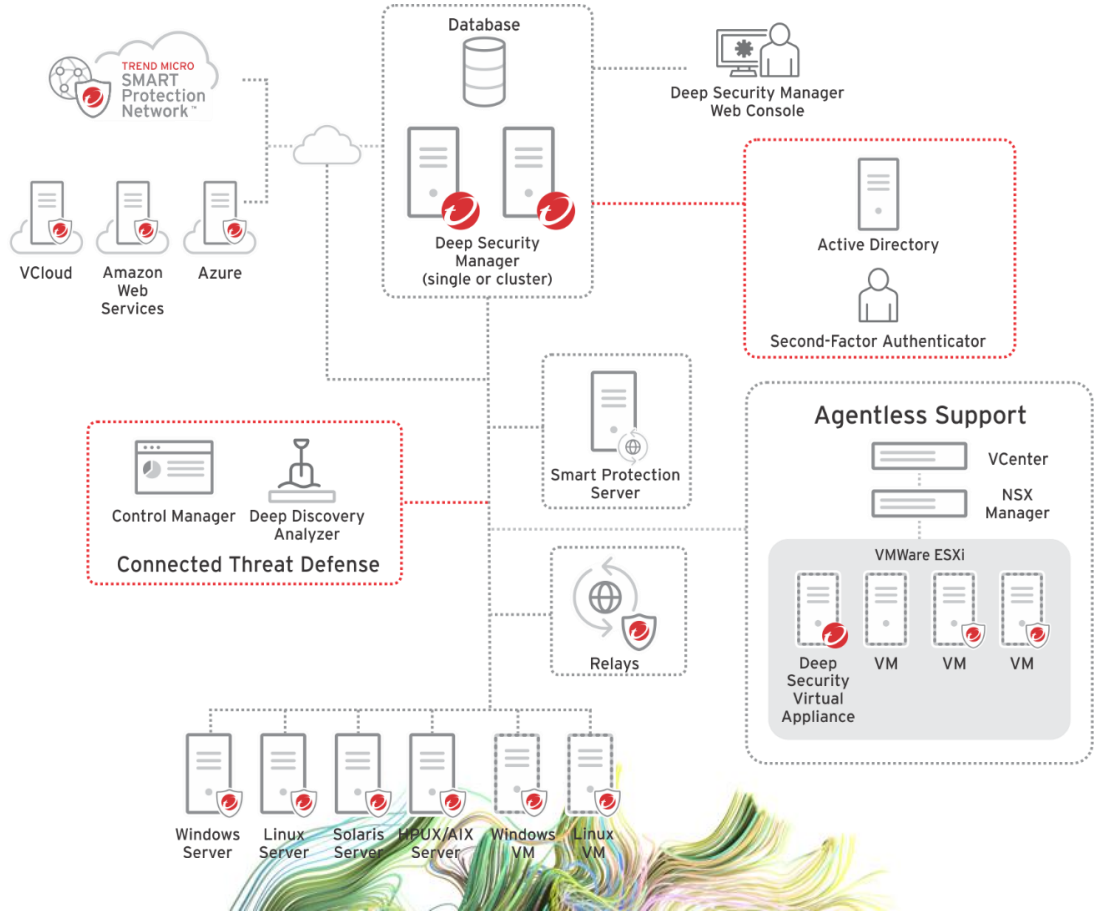
- 컨터이너로 Deep Security Agent실행
- K8S Cluster에 단일 에이전트 컨테이너
- IPS기능과 AM기능 제공
- 컨테이너 간 트래픽 검사
- 쉽게 배포 가능한 보안 컨테이너
- 다양한 K8S환경 지원



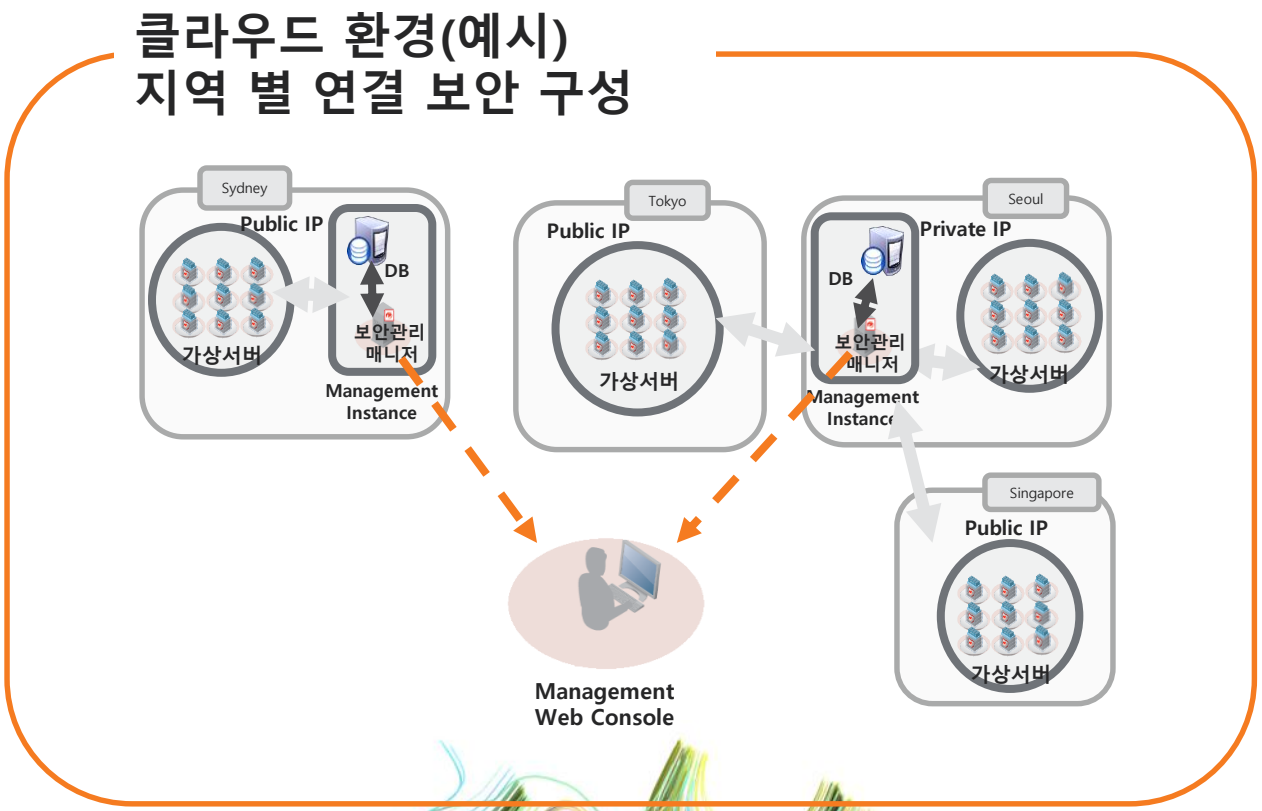


Deep Security 구성 방안

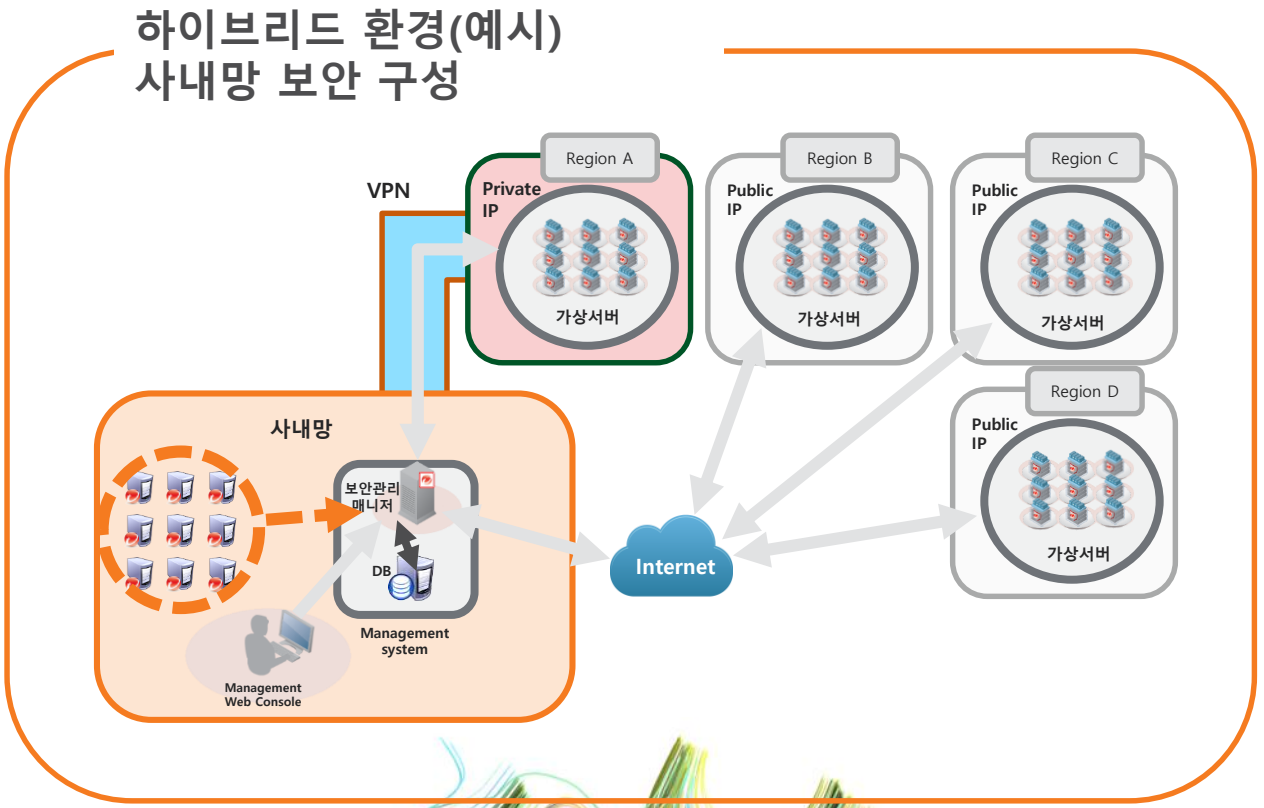
Deep Security 주요 컴포넌트 구성



클라우드 환경에서의 DS 구성 방안



하이브리드 환경에서의 DS 구성 방안

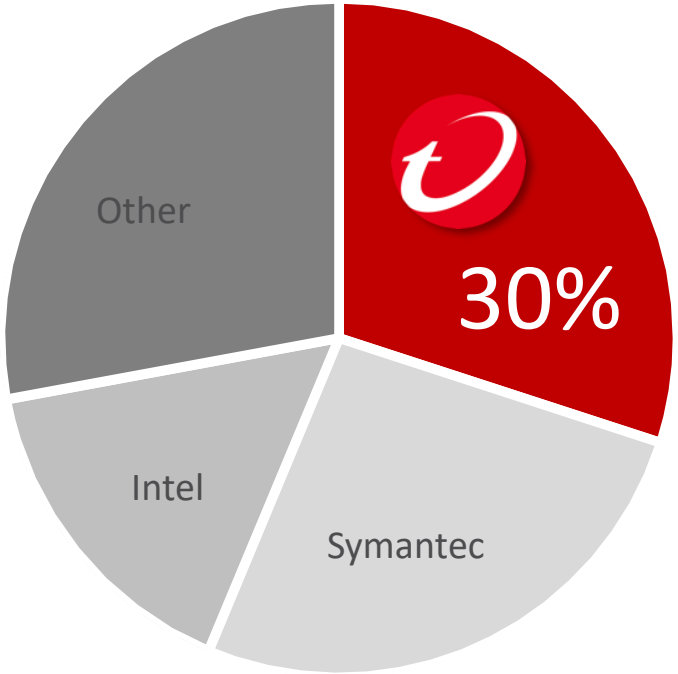



Gartner
2018
Market Guide for
Cloud Workload
Protection Platforms
23 of 26
capabilities &
considerations
Trend Micro delivers the
most cloud security
controls of all security
vendors evaluated

서버 보안 8년 연속 세계 1위

The MARKET LEADER
in server security for 8
straight years

IDC
Analyze the Future



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

TREND MICRO


TREND MICRO
THE ART OF CYBERSECURITY
Automated hybrid cloud workload protection via calls to Trend Micro APIs. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.**