전세계 클라우드 · 가상화 · 서버 보안 1위의 트렌드마이크로

TREND MICRO™ 트렌드마이크로

클라우드 및 차세대 데이터센터 보안

Deep Security

클라우드 보안 / 가상화 보안 / 물리서버 보안

COMMON CRITERIA CERTIFIED EAL2+

클라우드 및 차세대 데이터센터 보안

Deep Security

하이브리드 클라우드 보안 솔루션 Deep Security

- **클라우드 보안**
  - 클라우드 플랫폼 API 통합
  - Auto-Scaling 지원
  - 호스트 기반의 IPS/IDS
  - 아마존 AWS, 마이크로소프트 AZURE, IBM SoftLayer, KT uCloud, 구글 Cloud, 오라클 Cloud
- **가상화 보안**
  - 가상화 서버 및 VDI 보안
  - 에이전트리스로 AV Storm 방지 및 성능최적화 (VMware)
  - VMware NSX 보안
  - VMware, 마이크로소프트 HIPER-V, 시트릭스 XEN, 레드햇 KVM
- **물리서버 보안**
  - 랜섬웨어 예방 및 대응
  - 보안 업데이트 적용 불가 시스템에 대한 취약점 가상 패치
  - 윈도우, 리눅스 (레드햇, SUSE, Ubuntu, Oracle, CentOS 등), Unix (HP-UX, IBM-AIX, 오라클 솔라리스)

모듈 별 SIEM 연동 및
Detail 로그 연동 (Syslog, API)

HP ArcSight, IBM Radar, splunk>

NSS Labs

Deep Security는 NSS Lab의
호스트침입방지시스템 (HIPS)
PCI 적합성테스트를 통과한
최초의 제품입니다.

PCI Security Standards Council

통합보안기능(모듈별 구성)

백신(Anti-Malware) : 바이러스, 웜, 트로이잔 등의 위협 탐지 및 차단,
Real-Time Scan, Manual Scan, Scheduled Scan 기능, Smart Scan 기능

웹 평판(Web Reputation) : 악의적인 URL에 대한 액세스 차단, 악성 사이트 차단 및 사이트 접속 차단/허용 관리, Security Level에 의한 차단 설정, 사이트 접속 허용/차단 관리, 차단 페이지 커스터마이징 기능 제공

방화벽(Firewall) : 양방향 스테이트 풀 방화벽, 인증 되지 않은 소스에 대한 패킷 차단, 표면적인 공격 감소 효과 (DoS 방어 & 포트스캔을 통한 탐지), 네트워크에 접속하는 application을 제어하고, 향상된 가시성 제공

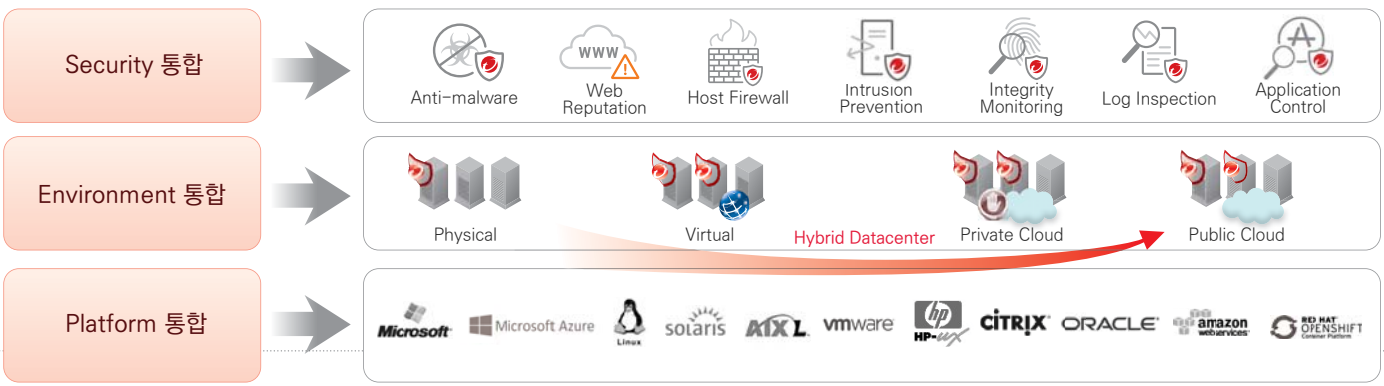
침입탐지 및 방지(IPS/IDS) : DPI 를 이용한 Virtual Patching 기능, 기본 룰 탑재와 서버 취약점 스캔을 통한 추천 룰 자동 적용 기능, 알려진 취약점이나 Zero-day 공격에 대한 탐지 및 차단, Web Application 취약점에 대한 방어

무결성 모니터링(Integrity Monitoring) : 폴더, 파일, 레지스트리 키 그리고 서비스에 대한 악의적이거나 승인되지 않은 변경에 대해 탐지, 기본 룰 탑재와 서버 취약점 스캔을 통한 룰 자동 적용 기능

로그 감사(Log Inspection) : 많은 양의 로그이벤트 중에서 중요한 보안 이벤트 확인의 최적화, 승인되지 않은 변경내용 기록, 최적화된 로그 정보, 효과적인 감사를 위한 분석 자료 제공, 기본 룰 탑재와 서버 취약점 스캔을 통한 룰 자동 적용 기능

응용프로그램 제어(Application Control) : Windows 및 Linux 서버에서 권한이 없는 소프트웨어를 자동으로 탐지하고 차단, 인벤토리가 생성되면 시스템을 잠그고 새로운 응용 프로그램이 허용 목록없이 실행되는 것을 방지, 제로 데이 위협을 포함하여 패턴이 없는 위협을 차단하는데 필요

Deep Security 특징



퍼블릭 클라우드 보안

클라우드에서 Deep Security의 장점

모듈형 통합 보안 기능에 의한 인스턴스의 다단계 방어

서버 보호에 필요한 IDS / IPS, 안티 바이러스, 변경 감시, F/W, 로그 관리 기능을 하나의 에이전트로 구현

Host 기반의 보안 구성으로 클라우드의 장점 최대화

게이트웨이 방식의 보안은 클라우드의 장점 저해 요소, 호스트 기반의 보안 구성이 솔루션

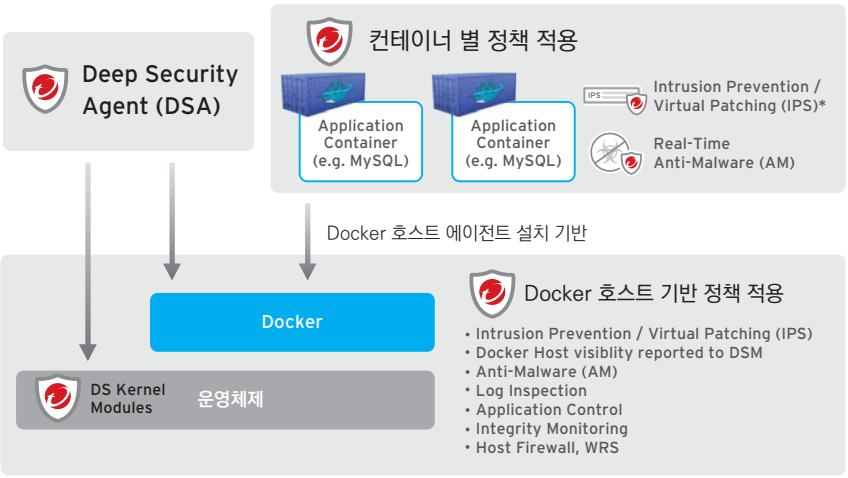
Auto Scaling 기능에 대응 한 자동 보안 기능

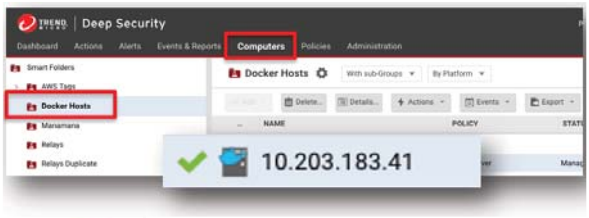
Auto Scaling 기능을 통해 증분된 인스턴스에 대해 자동으로 에이전트를 설치하여 즉각적인 보호

클라우드 Management 연계를 통한 효율적인 관리

클라우드 Management Console 및 Deep Security 관리서버의 연계를 통해 인스턴스 정보를 공유하고 원활한 보안 관리

Docker + Container 환경 보안

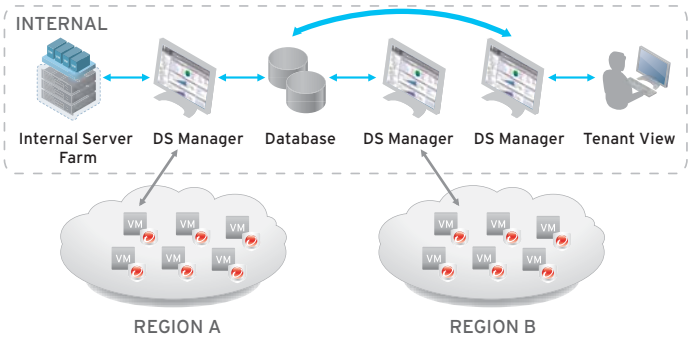




docker kubernetes Amazon ECS RANCHER

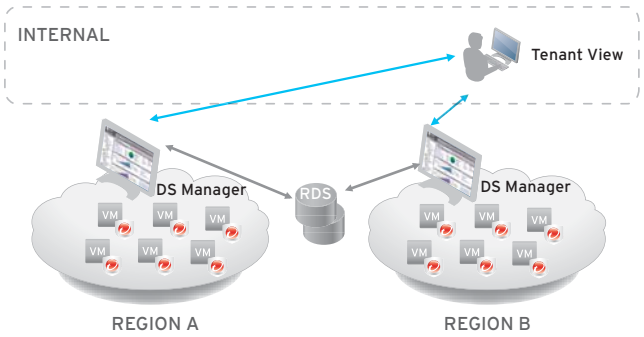
클라우드상에서 Deep Security 구성 방안 (Case1)

- Deep Security On-Premise
- DSM & DB를 관리자 환경에 위치시키는 경우



클라우드상에서 Deep Security 구성 방안 (Case2)

- Deep Security On-Premise
- DSM & DB를 instance에 올리는 경우

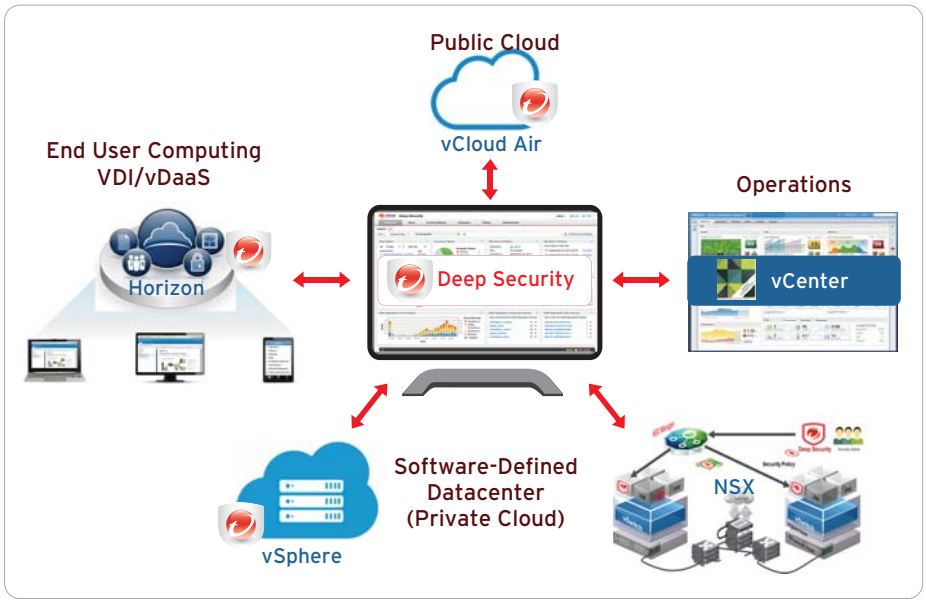


지원 플랫폼

amazon web services · Microsoft Azure · kt ucloud · IBM · Google Cloud Platform · ORACLE CLOUD
vmware · Microsoft Hyper-V · CITRIX ready · KVM · RED HAT OPENSHIFT Container Platform · docker
redhat · ubuntu · Windows · solaris · hp UX · IBM AIX
VCE · CISCO PARTNER Technology Developer · EMC VSPEX LABS VALIDATED · NUTANIX READY · SAP · rackspace HOSTING

가상화 서버 및 VDI 보안

VMware 구성요소들에 포괄적 보안 제공



기존 네트워크 운용 부담 경감

- 네트워크 스위치에 의한 엑세스 제어는 불필요
- 물리적 네트워크의 추가/변경에 영향을 받지 않음

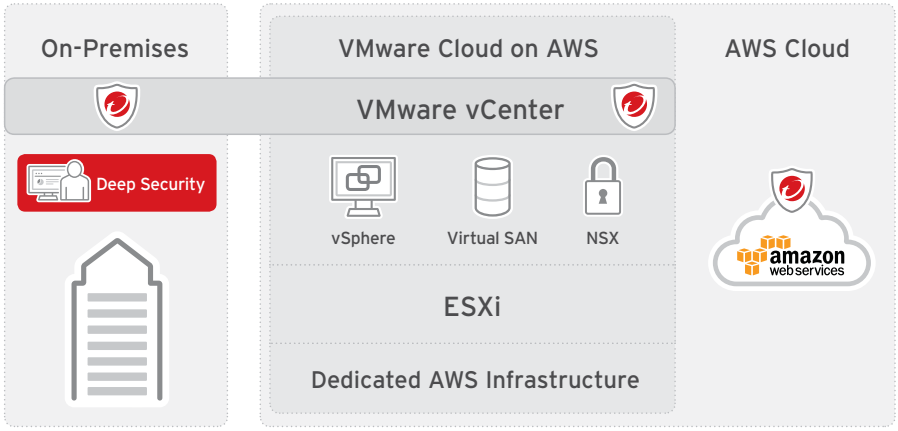
마이크로 세그먼테이션

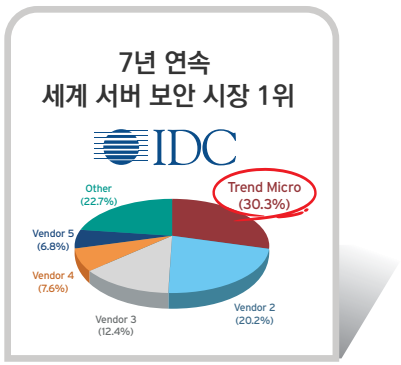
- 네트워크 세그먼트 및 보안 세그먼트를 분리
- 가상머신 마다 네트워크 방화벽을 구현하여 보안 세그먼트 최소화
- 필요없는 경로를 모두 차단
- 가상 머신 레벨에서의 보안 위반을 추적
- 동적 보안 관리

차단/격리에 의한 자동 검역 기반 보안

- 악성 코드/바이러스를 감지하고 즉시 기존 네트워크에서 자동 격리하여 보안 수준 증가

VMware on AWS





- IDC, 서버 보안: 가상화 및 클라우드 보안 솔루션 2016년 1월

물리적 서버 보안

서버를 위한 랜섬웨어 예방 및 대응

- 취약점 사전 차단(가상패치)으로 서버 보호
- 침입 방지 기능을 통하여 내부 확산 탐지 및 예방
- 의심스러운 동작을 감지 및 모니터링하고 파일 백업수행
- 허가되지 않은 응용프로그램 실행 차단
- 행동 기반 모니터링을 통해 Ransomware 공격 확인 및 악성 프로세스 정지 및 격리
- 랜섬웨어의 C&C 통신 탐지 및 경고
- 감염된 클라이언트들이 네트워크를 경유하는 의심스러운 파일 변경 활동의 감지

가상패치는?

취약점을 수정하는 보안 패치를 설치하는 대신 취약점을 악용하는 공격을 차단하고 가상 패치의 역할을 제공합니다.

- OS 및 애플리케이션의 취약점을 노린 공격을 네트워크 레벨에서 차단
- 취약점 발견 후 정식 패치까지 보안 홀 방지
- 리부팅 또는 업데이트 불가 시스템