전세계 서버 · 가상화 · 클라우드 보안 1위의 트렌드마이크로

TREND MICRO™ | 트렌드마이크로

클라우드 및 차세대 데이터센터 보안
Deep Security

트렌드마이크로
서울시 강남구 테헤란로 522
홍우빌딩 6층 (우 06181)
TEL. 02-561-0990
FAX. 02-561-0660
www.trendmicro.co.kr

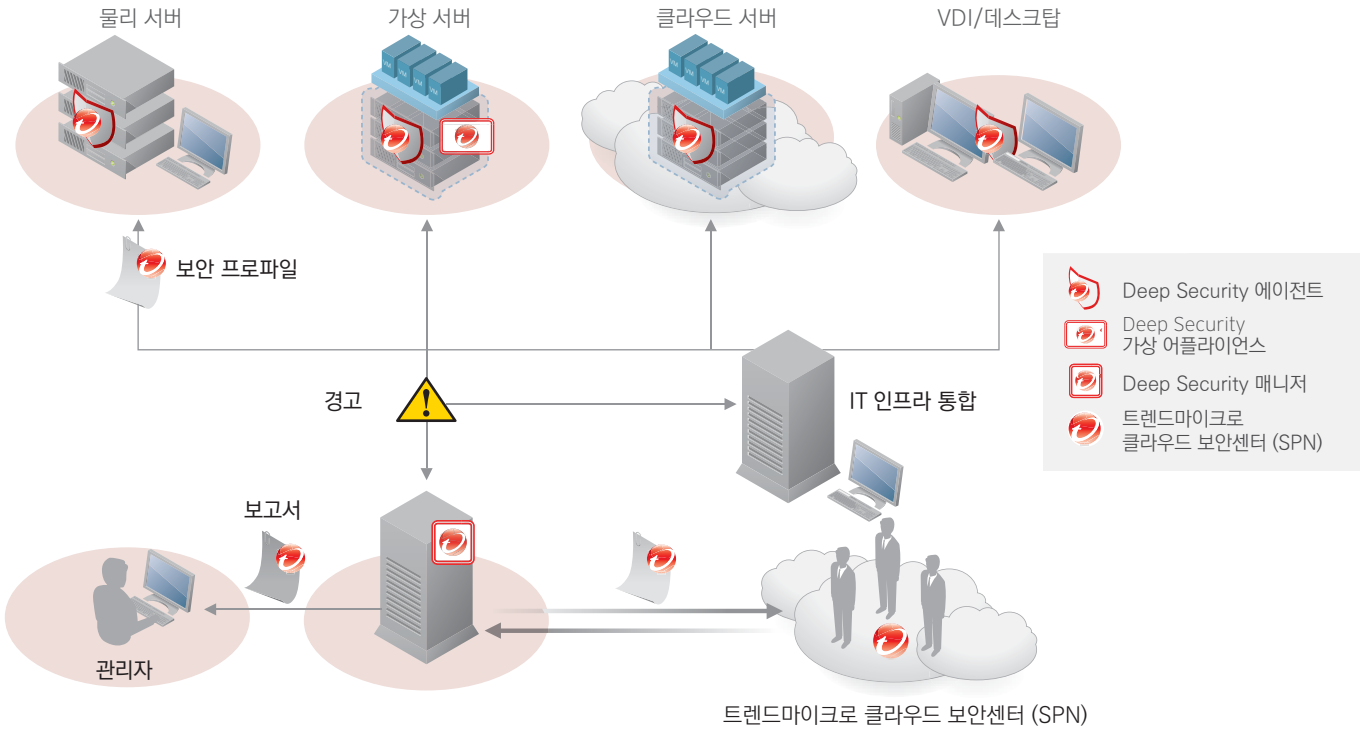
클라우드 및 차세대 데이터센터 보안

Deep Security

하이브리드 클라우드, 차세대 서버 환경의 데이타센터 통합 보안

- **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
- **클라우드 보안**
  - Auto-Scaling 지원
  - 호스트 기반의 IPS/IDS
  - 아마존 AWS, 마이크로소프트 AZURE, IBM SoftLayer, KT uCloud, 구글 Cloud, Rockspace
- **물리서버 보안**
  - 보안 업데이트 적용 불가 시스템에 대한 취약점 가상 패치
  - 윈도우, 리눅스 (레드햇, SUSE, Ubuntu, Oracle, CentOS 등), Unix (HP-UX, IBM-AIX, 오라클 솔라리스)

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



트렌드마이크로 클라우드 보안센터 (SPN)

가상화 보안 문제의 해결

문제점	해결 방안
• AV-Storm 문제	Deep Security는 가상화 환경에서 에이전트리스 방식의 구성으로 원천적으로 AV-Storm을 해결할 수 있으며 또한 Agent 방식에 있어서도 Virus Scan Cache와 Lightweight 디자인으로 다양한 보안 기능 제공에도 리소스 사용을 최소화 함
• OS/Application 취약점	Deep Security의 DPI(IDS/IPS, WAP) 기능으로 시스템에 영향 없이(보안패치, 재부팅, 시스템 리소스) Zero-day / Exploit 공격에 대한 방어가 가능
• 관리의 복잡성	에이전트리스 방식(Agent 미설치)으로 각 호스트에 Virtual Appliance(DSVA)를 통한 모든 Virtual Machine을 보호
• VM간 공격시 무방비	기존 네트워크 레벨에서 IPS/IDS, WAF로는 가상환경내에서의 VM간 악성코드/통신 탐지가 불가함으로 Deep Security가 제공하는 Host-base의 IPS/IDS, WAF로 가상환경내의 네트워크 모니터링 필요

클라우드에서는 호스트기반의 보안

유연성, 확장성, 관리효율성 보장

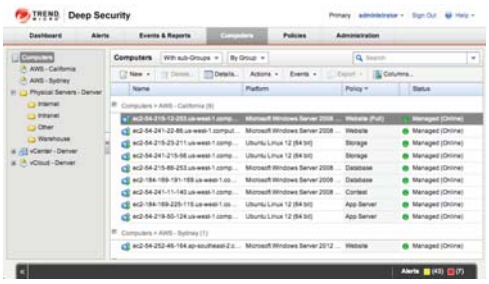
비교항목	네트워크 기반	호스트(SW)기반 (Deep Security)
구성방식	Hardware Appliance (Inline / Tap)	Software Agent (Inline/Tap)
Inter-VM 웹 트래픽 모니터링/탐지/차단	불가능	가능
VM 취약점 스캔	불가능	각 VM 에 대한 웹, OS 취약점 스캔기능 제공
가상패칭 (Virtual Patching)	불가능	각 VM에 대한 웹, OS 취약점 가상 패칭 기능 제공
통합관리	다수장비 통합관리	장비 및 VM통합보안관리로 서버 및 애플리케이션 가시성제공
맞춤형 룰 설정	모든 서버에 동일한 정책	서버의 용도,OS,App에 따라 맞춤형 설정
성능	네트워크 레이어에서 트래픽 분석하여 모든 서버들에 포함되는 탐지 룰 적용으로 성능이슈 발생	각 서버 레이어별 트래픽을 분산분석및 필수탐지룰 적용으로 성능 최적화
오탐의 영향	오탐이 발생할 경우 모든 서버들에 발생할 수 있음	오탐이 발생하더라도 적용된 서버에만 조치
장애 대처	보안기능 장애 발생시 전체 트래픽에 영향	해당 서버만 조치하여 타 서버들에 영향 없음
Auto Scaling	불가능 또는 수량 제한적	무제한 확장 가능

Deep Packet Inspection (DPI 모듈)

- 서버 취약점을 이용한 Exploit 공격은 Application / OS에 전달되기전 Deep Security의 DPI Shield로 사전 차단
- DPI는 자동 업데이트 되는 약 6,000개의 시그니처룰을 보유하고 있으며, 일반적 공격 패턴에 대해서는 사용자가 패턴 수정이 가능하고, 또한 사용자 정의 룰을 생성하여 폭 넓은 모니터링이 가능
- 가상패치: 보안 패치 이전에 취약점 보호, 긴급 보안 패치 관리 비용 줄임, 패치 관리의 편리

하나의 콘솔로 모든 위협구간 모니터링

- 다중 보안 통제를 통한 포괄적 대시보드 활용
- 통합 보고 및 경고 기능 사용
- 지속적인 서버와 어플리케이션 모니터링
- 웹 콘솔 또는 API를 통한 관리
- Public cloud & Private cloud & Physical server 통합 모니터링



모듈별 기능

1 안티 악성코드

Deep Security의 안티악성코드(백신)의 가장 큰 특징은 각각의 가상머신에 백신을 설치하지 않아도 백신이 설치된 것과 동일한 기능을 수행합니다. 이와 같은 방식을 통해 AV Storm과 같은 리소스 경합 문제를 해결하였습니다.

- ✓ ESL 레벨 캐싱과 중복방지를 이용한 성능 향상
- ✓ Manager에서 스캔방식 설정 및 상속기능
- ✓ Deep Security Manager에서 안티멀웨어 패턴 업데이트 진행
- ✓ 가상 어플라이언스에 룰 업데이트 및 패턴 정보 저장
- ✓ 스캔 및 치료 방식을 프로파일로 생성 가능
- ✓ 각각의 OS맞게 스캔방식 설정 가능
- ✓ 격리된 악성코드 다운로드 기능 제공

2 무결성 검사

Deep Security 의 무결성 검사 모듈 시스템은 중요 파일이나 폴더, 프로세스 그리고 레지스트리, 권한, Owner 등이 변경 되었을 경우 관리자에 알려주는 기능을 제공합니다. MS, Linux 뿐만 아니라 UNIX에 대해서도 전체적인 지원이 가능하며 SHA-1 및 SHA-256으로 해쉬를 지원합니다. 기본적으로 지원되는 템플릿 외에도 추가적인 룰 추가가 가능합니다.

- ✓ 인텔 TPM/TXT를 활용하여 하이퍼바이저 통합 모니터링
- ✓ 파일, 디렉토리, 권한, 프로세스
- ✓ 서비스, 레지스트리 등 변경에 대한 모니터링
- ✓ 100여 개 무결성 감사 템플릿 제공
- ✓ 룰 추가 기능 제공
- ✓ 추천 검사 기능 제공 (관리 편리성 제공)
- ✓ OS 및 애플리케이션 무결성 대상 추천
- ✓ 수동(자동) 무결성 감사

3 로그 감사

Log Inspection 모듈은 시스템의 OS나 애플리케이션에서 발생하는 무수한 로그들을 효과적으로 모니터링하고 중요한 이벤트를 쉽게 찾아낼 수 있도록 지원합니다. 시스템의 중요한 Log Inspection 부분에 대해서 관리자에게 알려주는 기능을 지원하여 로그에 대한 관리 편의성을 제공합니다. 추가적으로 중요한 이벤트에 대해서 위험도별로 분류하여 관리자가 중요한 로그를 보다 빨리 확인 할 수 있도록 지원합니다.

- ✓ 지능형 감사 대상 설정 가능
- ✓ 해당 시스템의 취약점 알림 서비스
- ✓ 100여 개 무결성 감사 템플릿 제공
- ✓ 룰 추가 기능 제공
- ✓ 추천 검사 기능 제공 (관리 편리성 제공)
- ✓ OS 및 애플리케이션 무결성 대상 추천
- ✓ 수동(자동) 로그 감사

4 침입 탐지 및 방지(IDS/IPS)

각각의 IDS/IPS, WAP, IM, LI 와 같은 보안제품을 통합보안 솔루션으로 제공하며 DPI(Deep Packet Inspection) 모듈의 경우, IDS/IPS 와 애플리케이션 컨트롤 및 WAP 기능을 제공하여 외부로 부터 들어오는 내부 시스템의 취약점에 대한 공격으로 부터 효과적인 대응이 가능하도록 지원합니다.

- ✓ DPI (Deep Packet Inspection)기능을 이용
- ✓ Manager로 부터 룰 주기적인 업데이트
- ✓ 6000여 개의 시그니처 보유
- ✓ 시스템 및 애플리케이션 취약점 점검
- ✓ 간편한 패치 적용 기능 제공 (가상패치)
- ✓ 가상패치 수동, 자동 적용 설정 가능
- ✓ 취약점 알림 서비스
- ✓ Detection / Prevention 모드 지원

5 Stateful Inspection 방화벽

방화벽의 경우 Virtual Appliance 형태나 에이전트 (호스트기반)의 형태로 보안 적용이 가능합니다. Stateful Inspection 기반의 F/W로서 중앙에서 룰 관리가 가능하고 룰에 대한 상속, 정책 상속 및 추가가 가능합니다.

- ✓ Stateful Inspection F/W 기능 제공
- ✓ 80여 개의 샘플 F/W 룰 제공
- ✓ Manager로 부터 룰 상속 가능
- ✓ 각 OS에 맞게 룰 추가 삭제 가능
- ✓ 상세한 Rule Sorting 기능 제공
- ✓ OS별 / 애플리케이션별 최적화된 룰 제공

Compliance 대응, PCI-DSS

PCI	책임
• 카드회원 데이터를 보호하기 위한 방화벽 도입, 최적의 설정 유지	공동
• 벤더가 제공하는 디폴트 시스템 패스워드 및 기타 보안 매개변수 값 사용금지	공동
• 저장된 카드회원 데이터를 안전하게 보호	공동
• 카드회원 데이터 암호화 전송	사용자
• 바이러스 백신소프트웨어 사용 및 정기 업데이트	사용자
• 안전한 시스템과 애플리케이션 개발 및 유지보수	공동
• 카드회원 데이터에 대한 접근을 업무상 필요한 범위 내로 제한	공동
• 컴퓨터에 접근하는 사용자마다 개별 ID 할당	공동
• 카드회원 데이터에 대한 물리적 접근 제한	클라우드 제공자
• 네트워크 자원과 카드회원 데이터에 대한 모든 접근 추적 및 모니터링	공동
• 보안 시스템 및 관리 절차를 정기적으로 테스트	공동
• 정보보호 정책 유지관리	공동

NSS Labs

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

PCI Security Standards Council

Deep Security 특장점

- 클라우드 플랫폼 API 통합
- 엔터프라이즈의 AWS 보안 표준, 국내 최다 사용
- 호스트 기반의 보안으로 클라우드에 적합
- VMware vCloud 및 NSX 보안
- 하이브리드 클라우드 보안 통합 (클라우드,가상화,물리환경)
- 보안 솔루션 통합 (AV, IPS/IDS, F/W, LI, IM)
- 플랫폼 통합(Linux, Windows, Unix)
- 가상패치로 취약점 사전 방지
- 각종 보안 컴플라이언스 만족(PCI-DSS, HIPPA, HITECH)
- 국제CC 최고 등급, EAL2+, (구EAL4+)

COMMON CRITERIA
CERTIFIED
EAL2+

지원 플랫폼

amazon web services
Microsoft Azure
Google Cloud Platform
IBM
kt ucloud
vmware
CITRIX ready
Microsoft Hyper-V
KVM
rackspace HOSTING
Windows
redhat READY
Linux
solaris
hp UX
IBM AIX
VCE
CISCO PARTNER Technology Developer
EMC² VSPEX LABS VALIDATED
NUTANIX READY
SAP

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

hp ArcSight
IBM Radar
splunk>