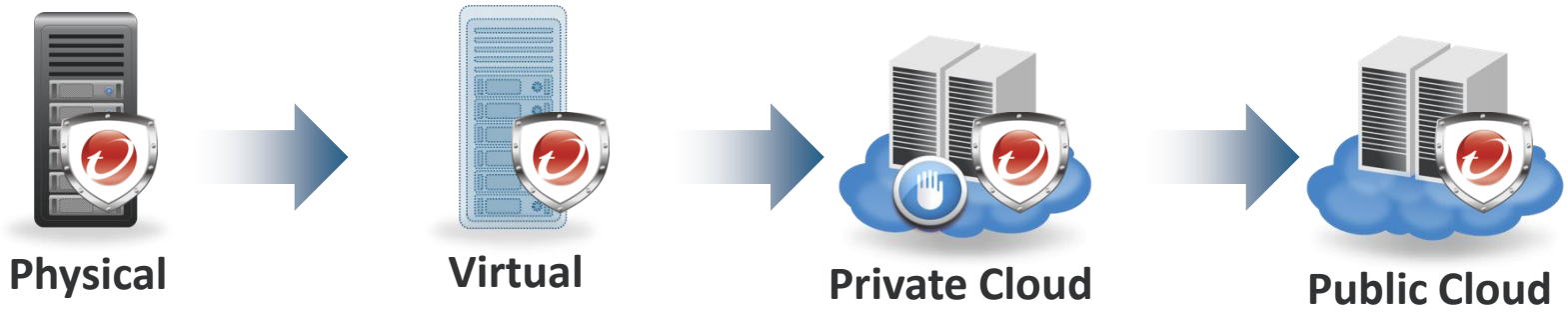
차세대 호스트 기반 보안 전략

김석주 팀장
클라우드 보안 사업부
04/24/2014



Data Center Ops

2016년 내로, **71%**의 서버 작업은 **가상화**로 전환 [1]

2015년 내로, **90%** 의 대기업과 정부기관 클라우드 사용[2]

1. Source: Gartner, Forecast Analysis: Data Center, May 2012
2. Source: Forrester Study, 2013

TREND MICRO

보안은 어떻게 처리할 것인가?

- 수 분내 서버 배포…
  보안은 몇 주
- 물리적 한계를 넘어선 가상 규모…
  보안의 벽
- 리소스 공유하는 서버…
  리소스 소비하는 보안

TREND MICRO

보안 원리/기술은 동일하다;
접근 방식에서의 보안은 변경 되어야 한다.

Static	**ADAPTIVE**	지능적인, 동적 정책 적용 특정 플랫폼에 자동 배포
Generic	**CONTEXT**	서비스 규모 및 종류 인지
Hardware	**SOFTWARE**	가상화 **&** 클라우드 인프라에 최적화
Many Tools	**PLATFORM**	서비스 형태의 보안

TREND MICRO

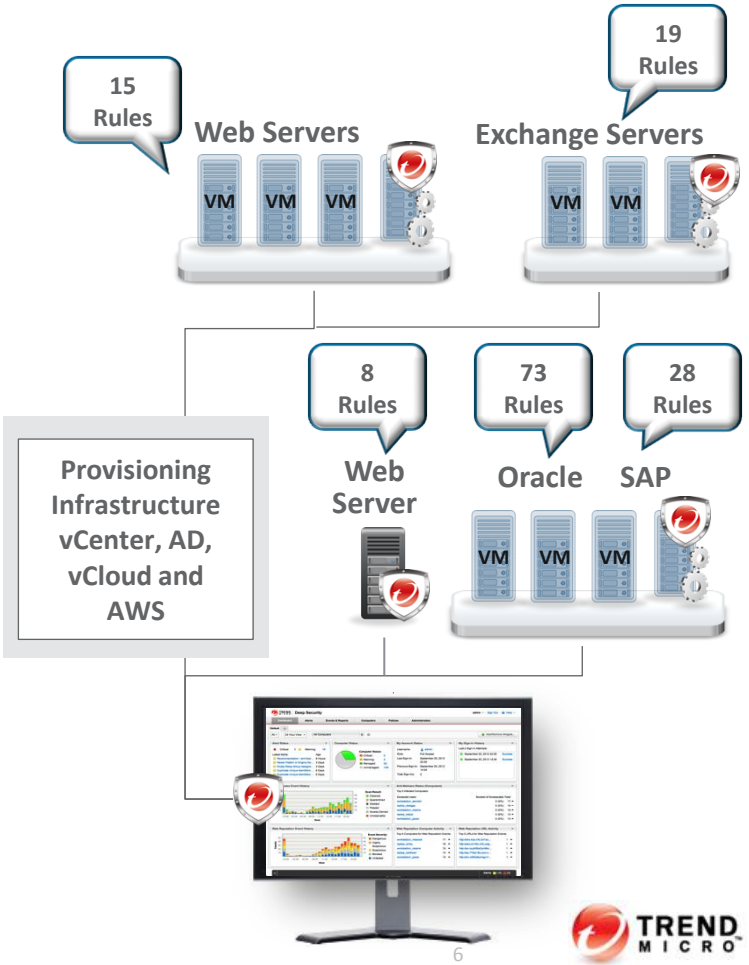
새로운 접근으로의 데이터센터 보안

- 보안 적용의 자동화 및 최적화
- 규모에 맞는 보안의 효율적 관리
- 보안 강화 및 모듈 통합

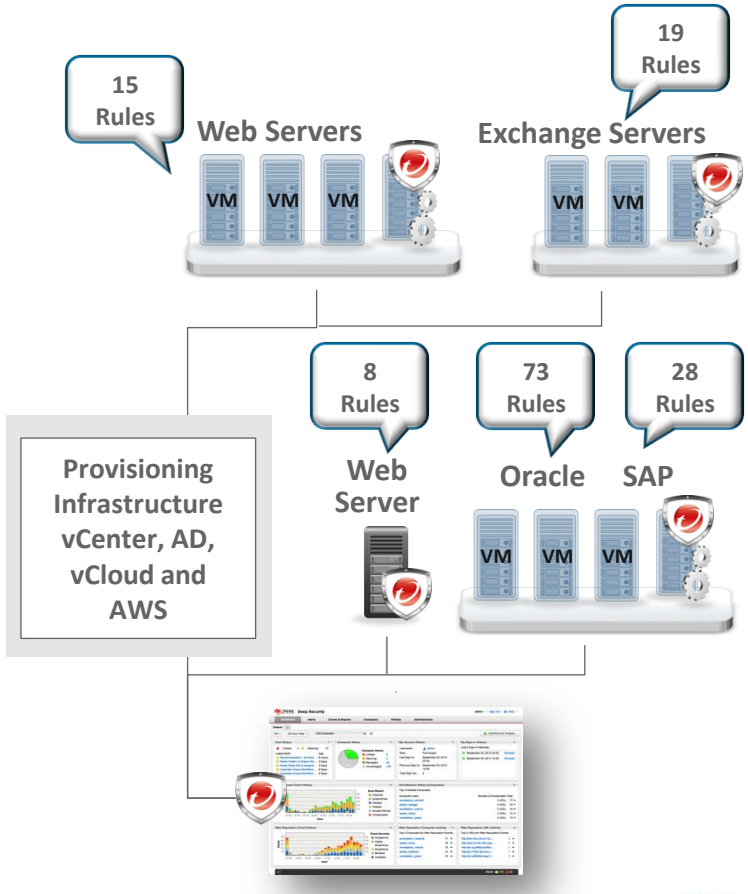
TREND MICRO

환경 특성에 맞는 자동 보안 적용

- Virtualization Mgmt., AD, LDAP등과 연동하여 가시성 확보
- 서비스, 플랫폼등에 따른 보안 정책 자동 권장 적용
- Auto-Scale UP/Down 발생시 – Security Hole 최소화

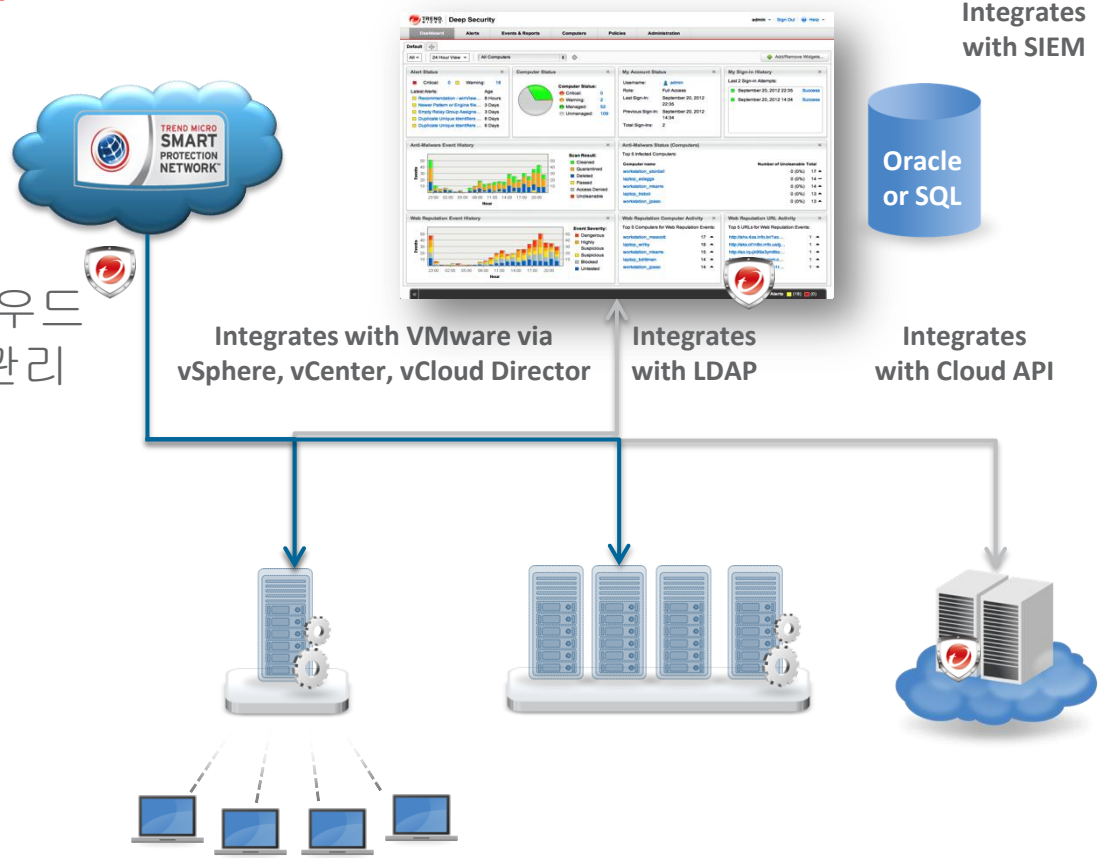


엔터프라이즈 표준과의 호환



호스트 기반 보안 권고

- 가상환경의 API를 사용하여 가상 보안 Appliance를 배포하고 가시성 제공
- 하나의 콘솔로 물리/가상/클라우드 환경에 정책, 룰, 이벤트, 작업 관리
- 정기 업데이트 방식을 넘어 실시간 업데이트 방식으로 신/변종 악성코드, Zero-day 공격에 빠른 대응
- 모든 탐지/차단, 관리 이벤트 SIEM 연동(Syslog, API)

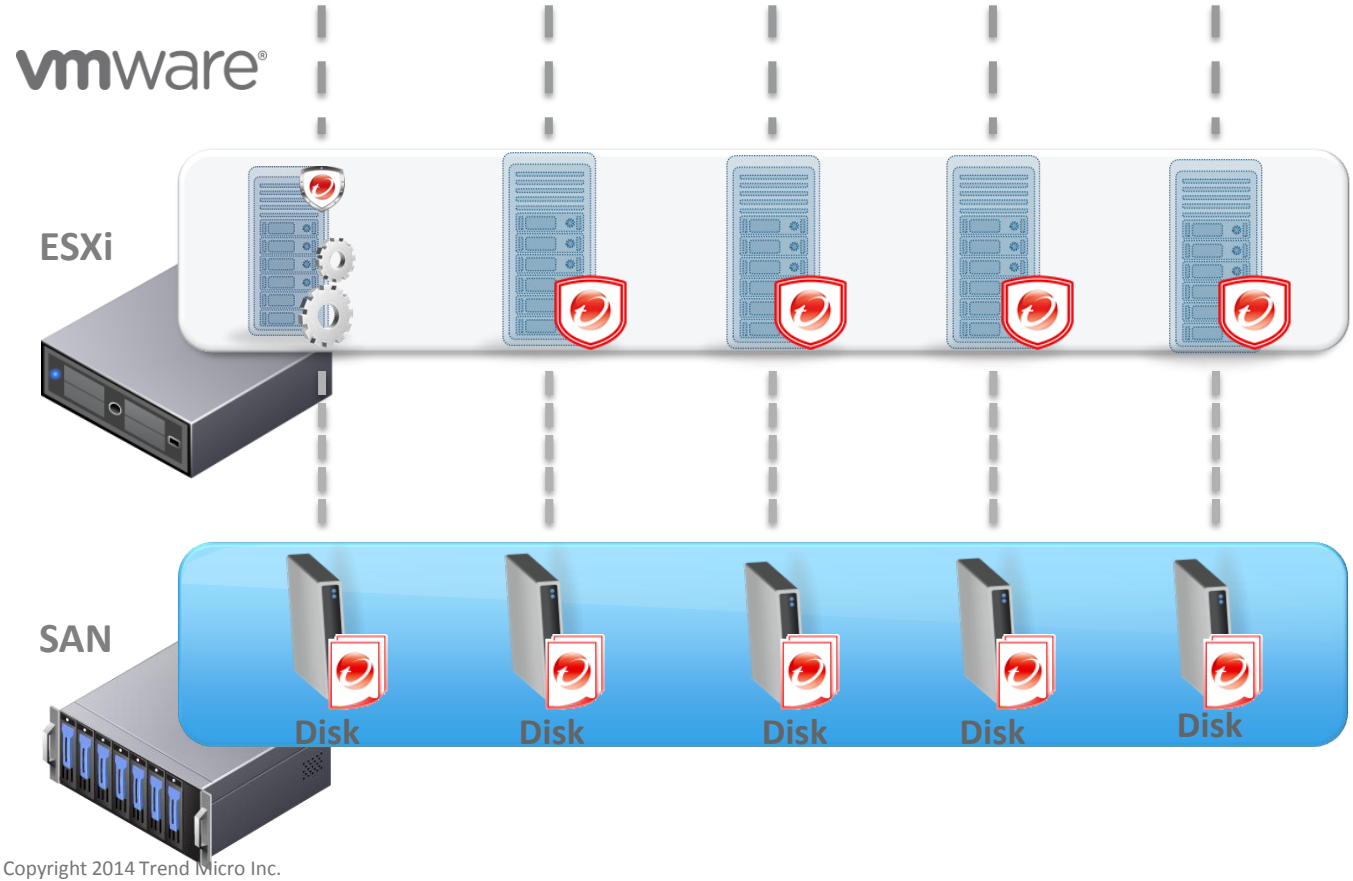


새로운 접근으로의 데이터센터 보안

- 보안 적용의 자동화 및 최적화
- 규모에 맞는 보안의 효율적 관리
- 보안 강화 및 모듈 통합

TREND MICRO

가상화 환경에 최적의 보안 모델



Network Usage

Scan Speed

CPU/Memory Usage

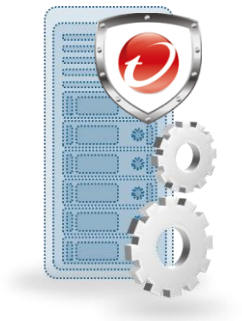
IOPS

Storage

TREND MICRO

중복 검사 회피로 성능 최적화

Scan Cache



Up to **20X** Faster*

Full Scans

Up to **5X** Faster

Realtime Scans

Up to **2X** Faster

VDI Login

*All results based on internal testing using VMware View simulators

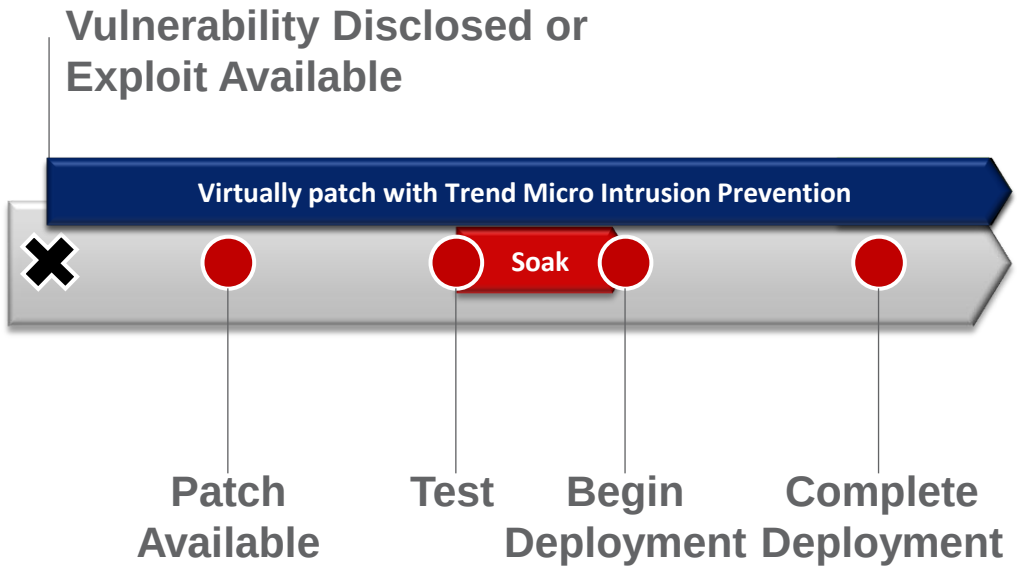
새로운 접근으로의 데이터센터 보안

- 보안 적용의 자동화 및 최적화
- 규모에 맞는 보안의 효율적 관리
- 보안 강화 및 모듈 통합

TREND MICRO

효과적인 취약점 관리/조치 – 패치 전

- 취약점 악용으로부터 노출 위험 제거
- 긴급 보안 패치 관리 비용 줄임
- 패치 관리의 편의성



위협 분석, 보안 정책준수 – Best Practice

Anti-malware with Web Reputation: 데이터 유출과 시스템 공격으로 사용되는 신종 악성코드에 대해 실시간 보호

Intrusion Prevention: 필요할때 필요한 서버에 필요한 보호를 하기위해 자동 보안 정책 업데이트로 패치되지 않은 취약점들의 노출로부터 방어

Firewall: 필요한 프로토콜과 포트만을 제한하고 각 서버간 통신을 방화벽으로 모니터링하여 내부간 공격으로부터 보호

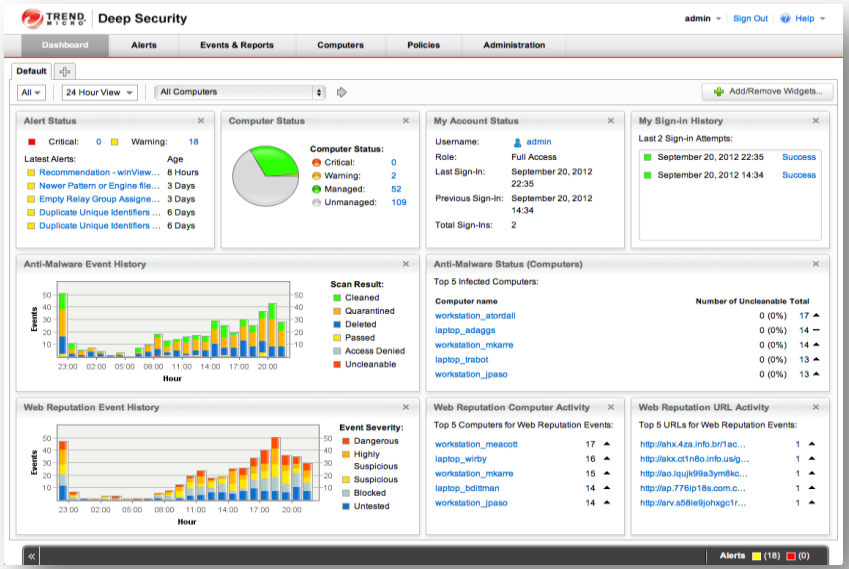
Integrity Monitoring: 무결성 정책에 벗어난 시스템 변경을 탐지하고 리포팅함으로써 보안 감사 요구사항 활용

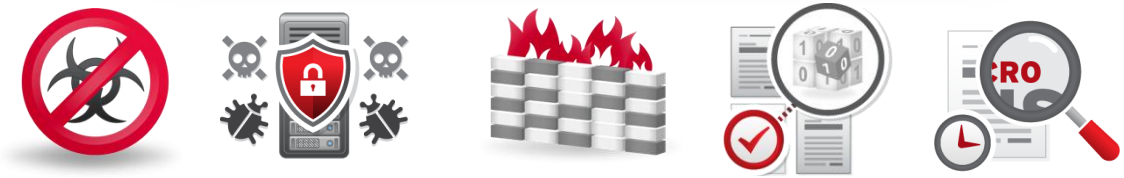
Log Inspection: 시스템 로그에서 보안 관련 이벤트를 추출하여 보안 감사 요구사항에 위배됨을 빠르게 인지

Application Scanning: 취약점을 자동으로 검사하여 찾아내어 사전 보호

Encryption: 클라우드 환경에서 보안 준수와 기밀성 유지를 위해 동적(SSL)/정적 데이터 암호화

하나의 콘솔로 모든 위협 구간 모니터링

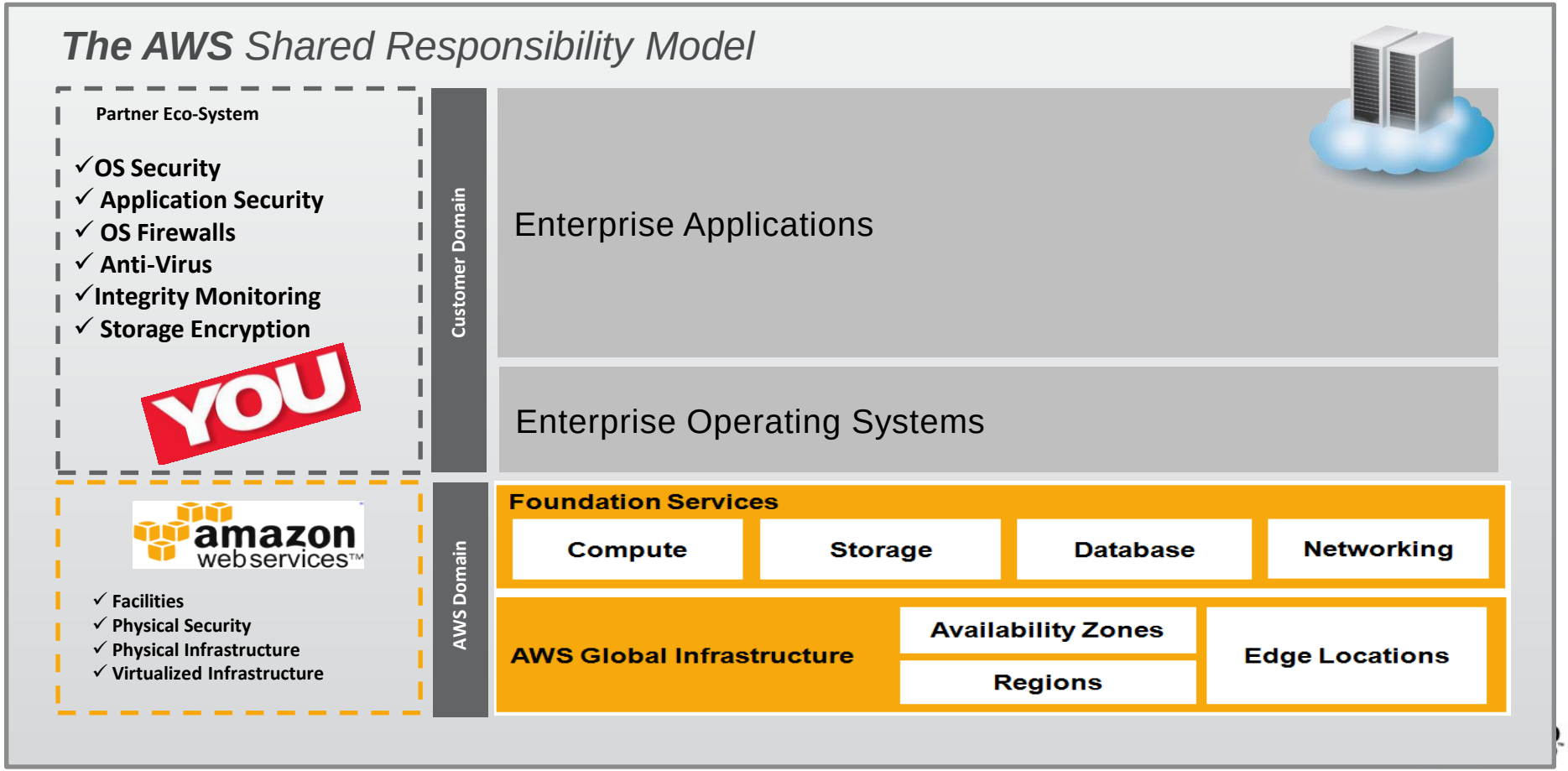




차세대 호스트 기반 클라우드 보안

TREND MICRO

Cloud Security is a Shared Responsibility



Cloud Security Checklist, p1

- 취약점 탐지를 위한 지속적 웹 어플리케이션 검사
- 외부 키 관리로 키 보관과 데이터 보호를 위한 부트 / 데이터 볼륨 암호화
- SSL 인증서를 통해 암호화된 동적 데이터 보호
- 보안패치 이전에 취약점들로부터 보호하기 위한 IDS/IPS를 통한 가상패치
- 호스트기반 양방향 모니터링 방화벽은 인가 받지 않은 외부 통신을 차단 – 로깅 및 알람으로 좀 더 쉬운 관리
- 파일 무결성 검사는 인가 받지 않은 시스템 컴포넌트 변경 탐지
- 웹 평판이 내재된 안티바이러스는 악성코드 및 악성 URLs로부터 보호

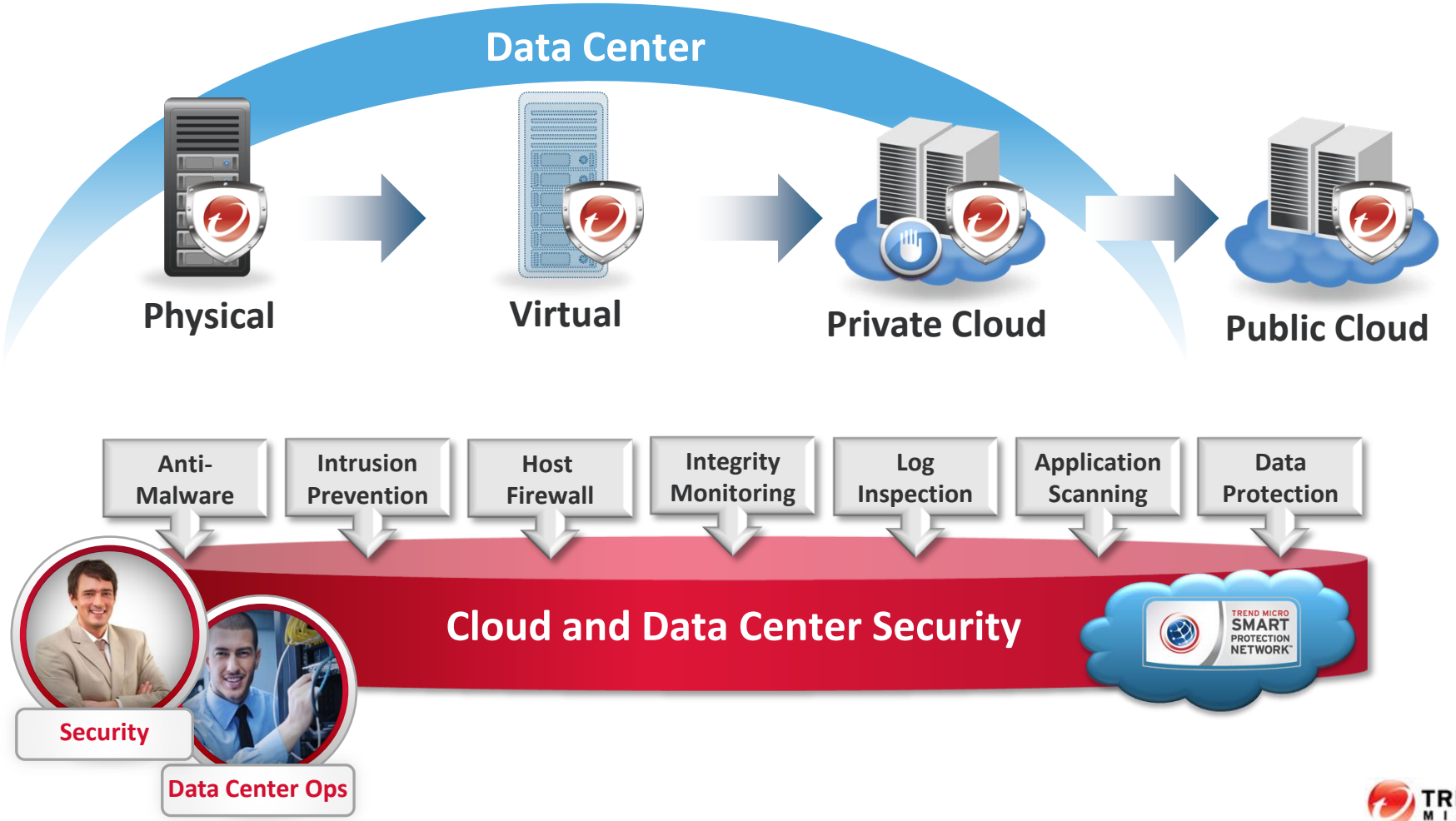
TREND MICRO

Cloud Security Checklist, p2

- 자동화된 권장 룰 적용 방식은 클라우드 인스턴스에 보안 정책을 배포하는 작업량 경감
- 하이브리드 환경에 중복적인 보안 정책 필터
- 클라우드 인스턴스의 Active / Standby 상태에도 지속적 보안 정책 유지
- 사용자 인스턴스에 필요한 보안 정책 스캔을 자동 적용
- 대표적 클라우드 관리 툴인 Chef, Puppet, AWS OpsWorks 의 운영 프로세스에 보안 서비스 추가 연동 지원
- 대시보드, 리포트, 알람은 사용자의 클라우드 환경에 실시간 가시성을 제공하고, 위험/중요도를 구분/인지 할 수 있도록 편의성 제공
- 사용자의 배포 / 운영 선호에 맞게 유연한 구성 옵션(software or service)과 비용 지불과 관련한 클라우드에서의 구매 모델을 제공(upfront, pay-as-you-go)

TREND MICRO

예제 데모 – 자동 배포 및 중앙집중식 관리



Thank you!

Email: anthony_kim@trendmicro.co.kr

Refer: deepsecurity.trendmicro.com