

네트워크 가상화 기술을 접목한 차세대 VDI 구현전략

임관수 부장 / lims@vmware.com

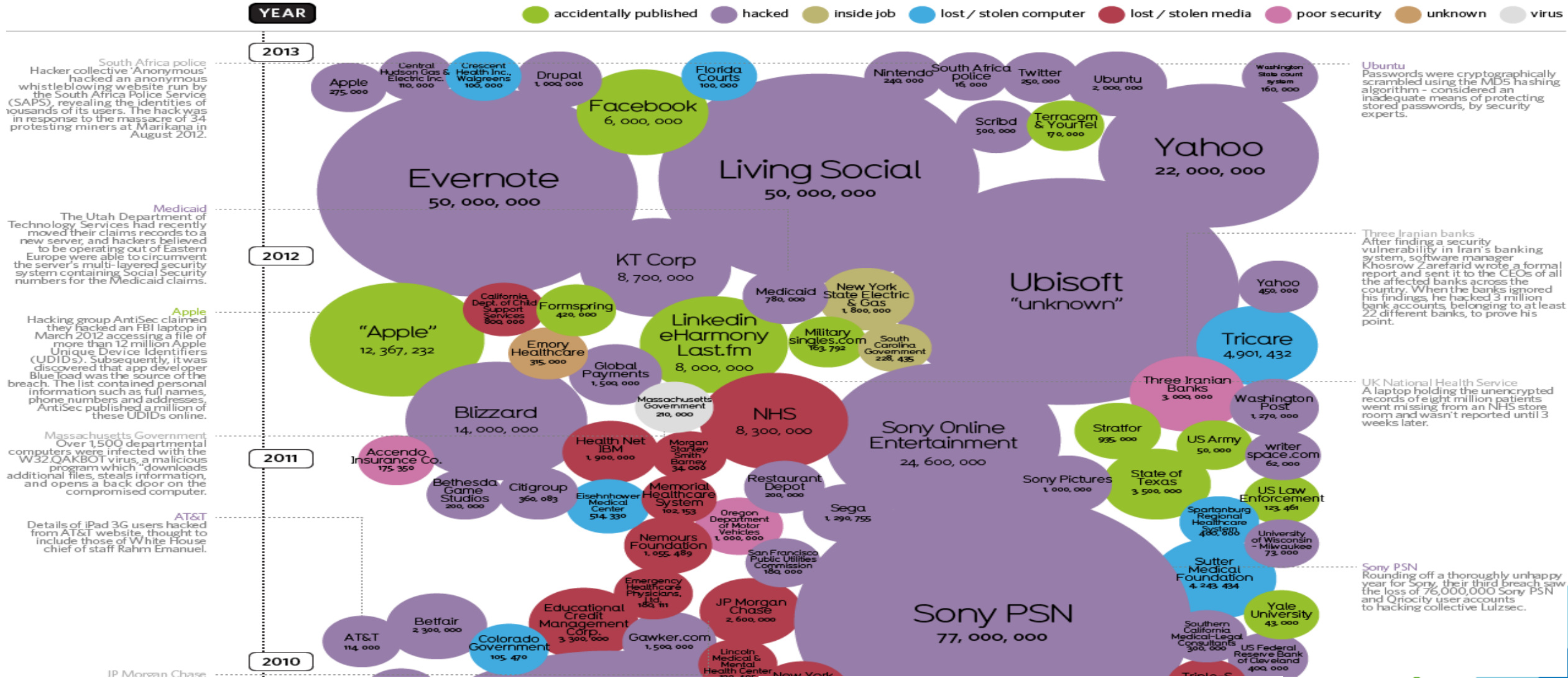
VMware Korea, EUC Specialist

vmware®

© 2014 VMware Inc. All rights reserved.

World's Biggest Data Breaches

Selected losses greater than 30,000 records



design & concept: David McCandless // v1.0 // July 23rd 2013
 research: Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson
 additional design: Fabio Bergamaschi
 InformationIsBeautiful.net

CISO가 직면한 중대한 문제

언론에 보도된 기업의 IT 보안 침해 사고

보안 사고 증가율: 연평균 **66%**

보안 침해 사고의 평균 비용: **590만** 달러

내부자 범죄의 **65%**는 전현직 직원이 주범임



Security and Compliance becoming the same thing
- PCI, HIPAA, GLB



"75% of CISOs who experience publicly disclosed security breaches and lack documented, tested response plans will be fired"

Employees the 'number one' cyber security threat facing businesses

Bosses see their employees as a bigger threat to their corporate data and computer systems than criminals or cyber attackers, according to a new international study.

IT Governance (ITG) polled 260 corporate executives, IT directors, and other technology professionals for its *Boardroom Cyber Watch 2013* survey. Fifty-three per cent of them ranked their own staff ahead of the risks from criminals (27 per cent), state-sponsored cyber attackers (12 per cent), and competitors (eight per cent).

ITG says its research also confirms the high level of cyber threat facing today's organisations, with 25 per cent of bosses saying they have received a "concerted attack" in the past 12 months. However, it adds that many board directors still appear

"inadequately informed" about cyber risks. While a majority of respondents say their board receives "regular" reports on the status of their organisation's IT security, 52 per cent say that such reports are only received, at best, annually.

Furthermore, despite threats potentially impacting many mission-critical business operations, only 30 per cent of respondents say an understanding of current IT security threats is a prerequisite for board-level job candidates.

ITG chief executive Alan Calder believes that while companies are not ignorant of the risks, the boardroom still appears "too removed from the action" for directors to meet their governance obligations. He adds that the best way for organisations to prove

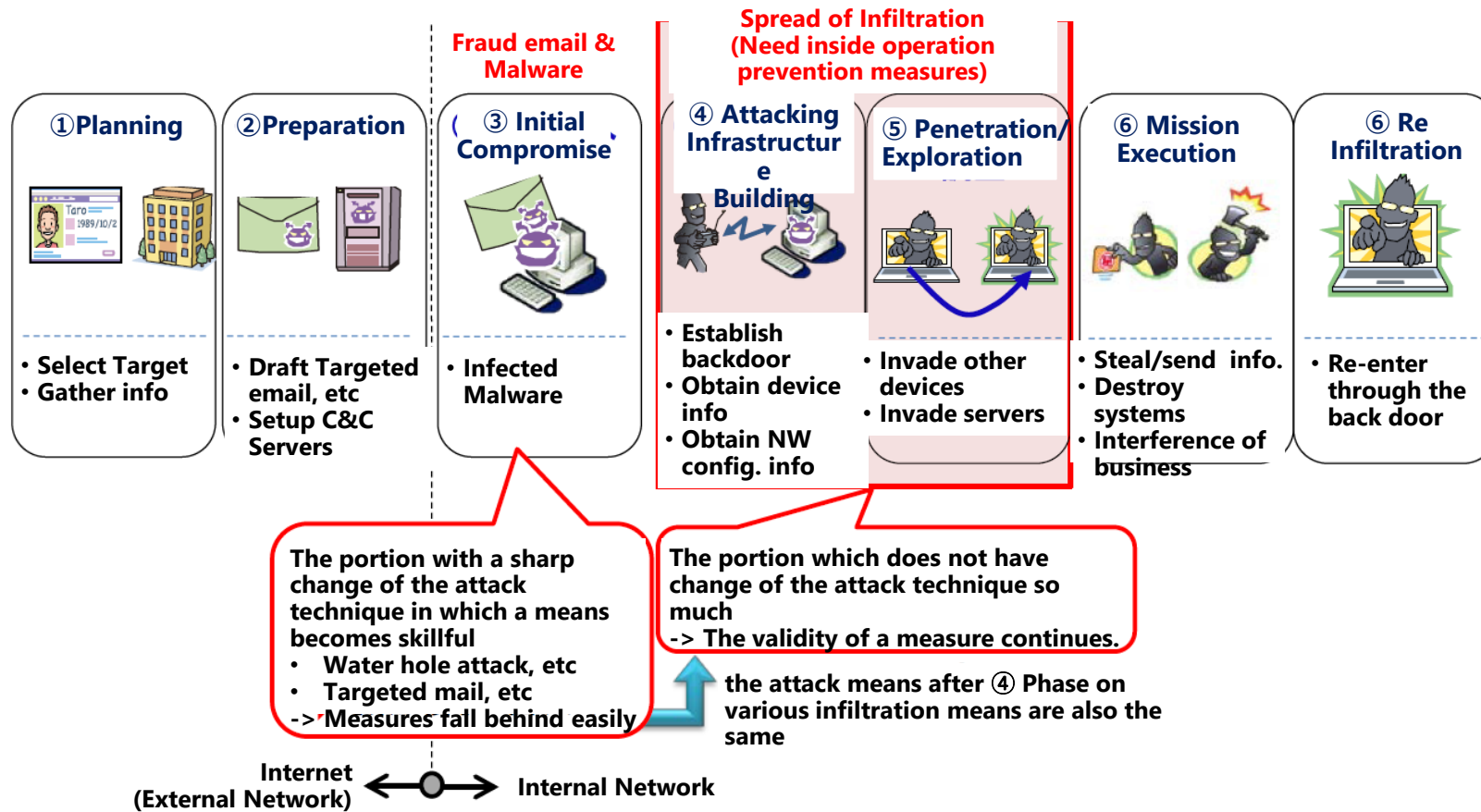


Alan Calder, IT Governance chief executive, says ISO 27001 certification is the "best way" for organisations to prove their cyber security credentials.

their cyber security credentials is to comply with, and be certificated against, ISO 27001, the global best practice standard for information security management.

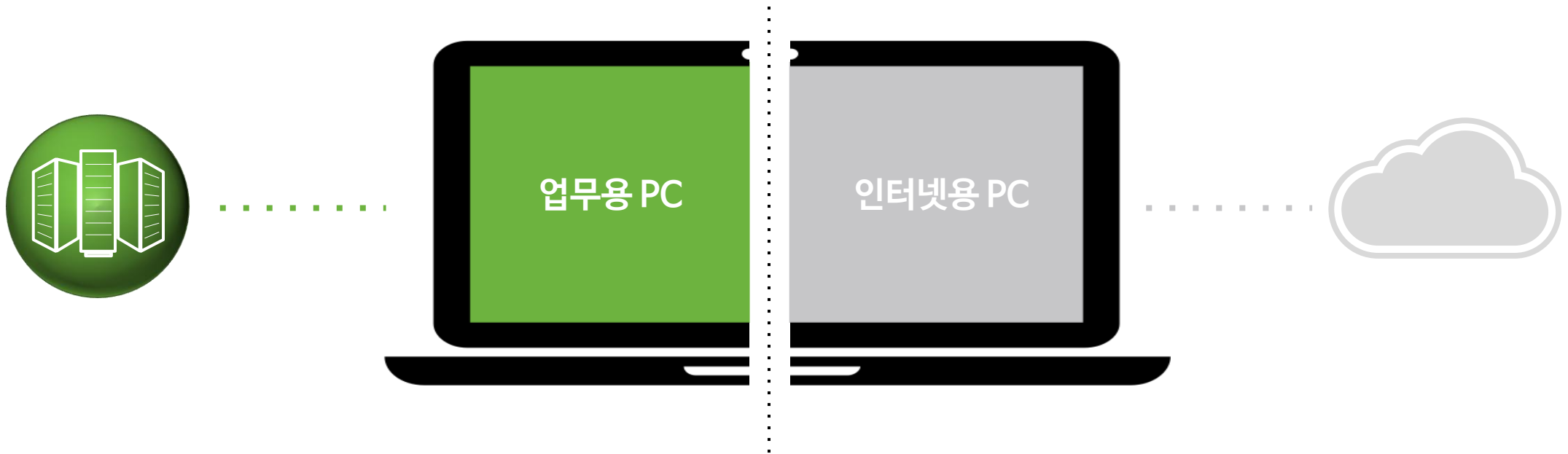
"This lets you signal to customers anywhere in the world that you have a robust method for addressing the entire range of risks associated with systems, people and technology," says Calder. ■

지능형 표적공격 (APT)

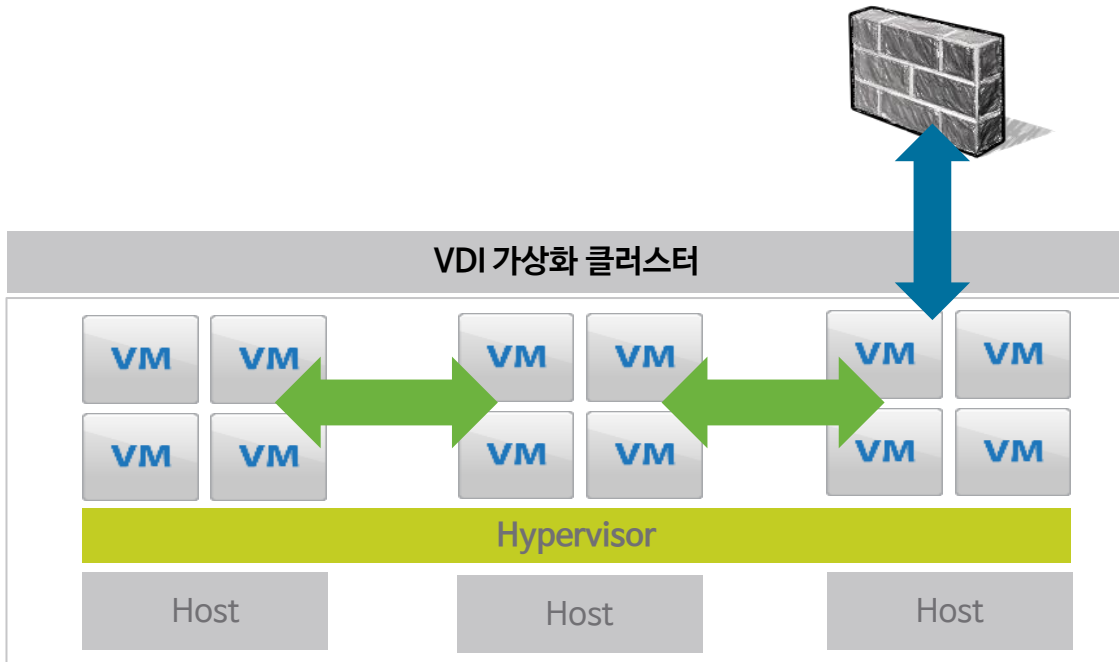


프라이빗 클라우드 기반의 VDI 인프라의 확대

- 공공 : 시범사업을 거쳐 2010년 이후 국가기관 및 산하기관까지 확대 적용중
- 금융 : 전산센터 망 분리는 '14년말 까지, 본점·영업점은 단계적으로 추진 (은행 '15년말, 그 외 금융사 '16년말 까지')
- 일반기업 : 전사 업무망 적용 사례 등 내부중요정보(R&D) 보호 등의 목적으로 도입 확대



가상화 환경의 Challenge

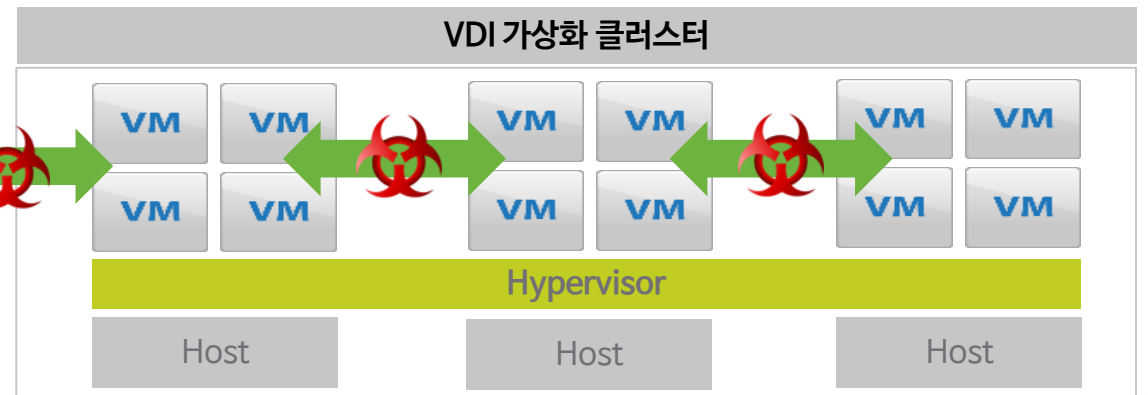
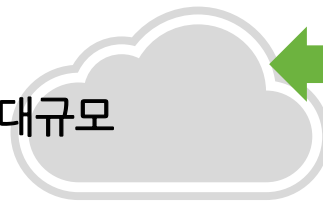


가상화 클러스터 내부의 자원에 대한 내부 통제가 어려움.

- East-West 트래픽 제어 힘들

가상화 클러스터 내부의 보안이슈 발생시 대규모 장애상화 발생가능성.

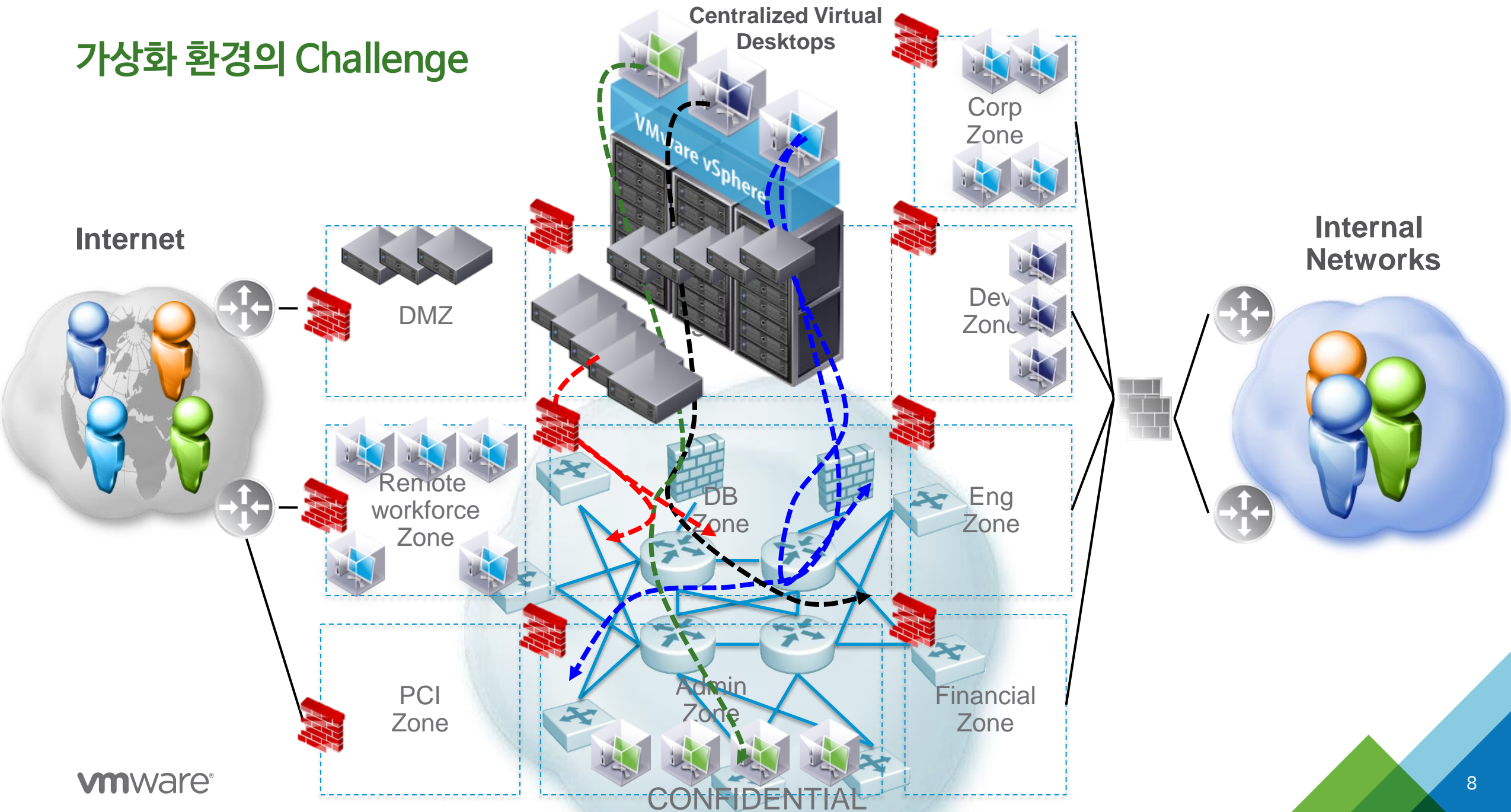
- Trust Security 모델



가상화 환경의 Challenge



가상화 환경의 Challenge



가상화 환경의 Challenge

Security Zones

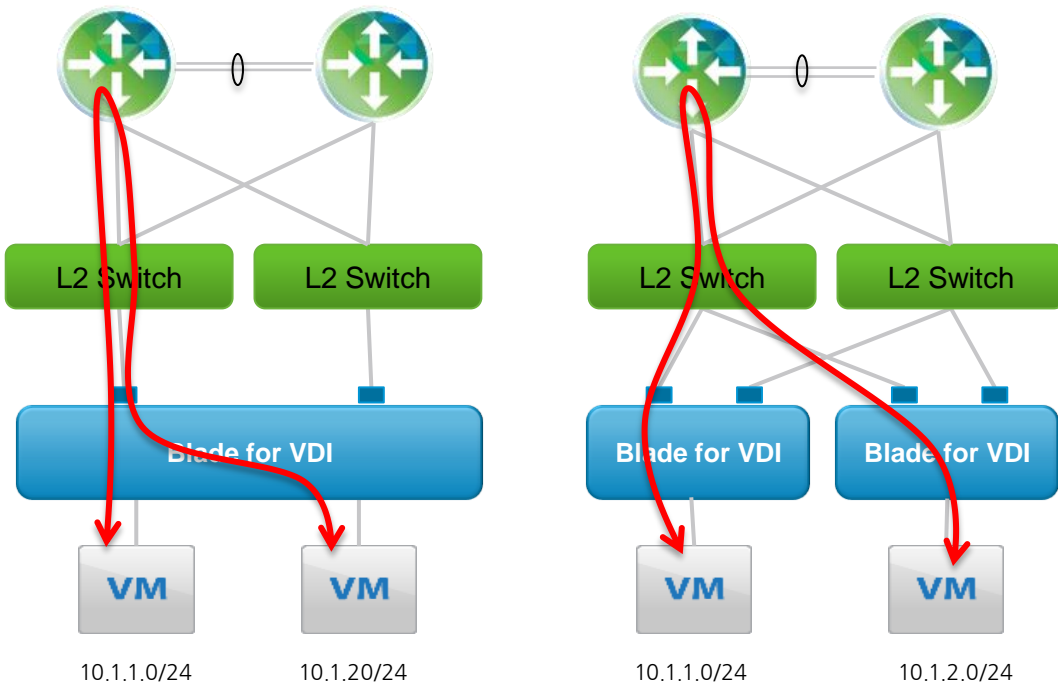
VLANS

192.168.10.4
192.168.10.12
192.168.20.6
192.168.20.11
...

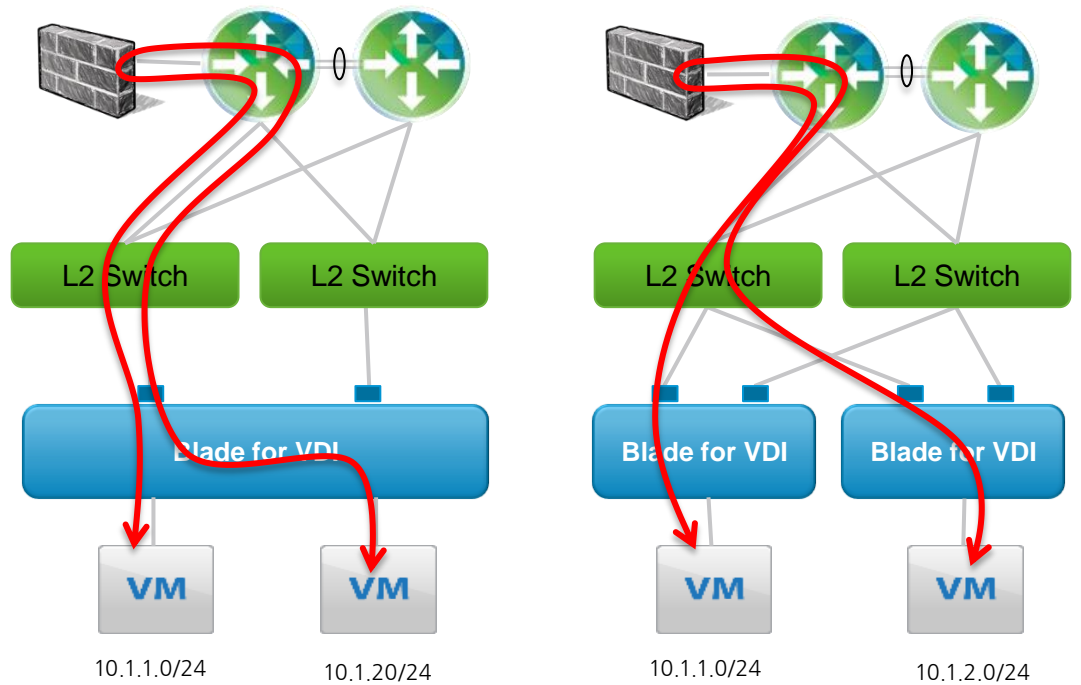


가상화 환경의 Challenge

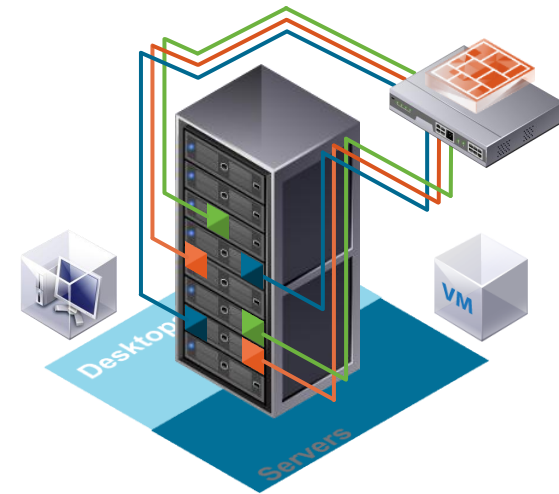
East-West Layer 3



East-West Firewall



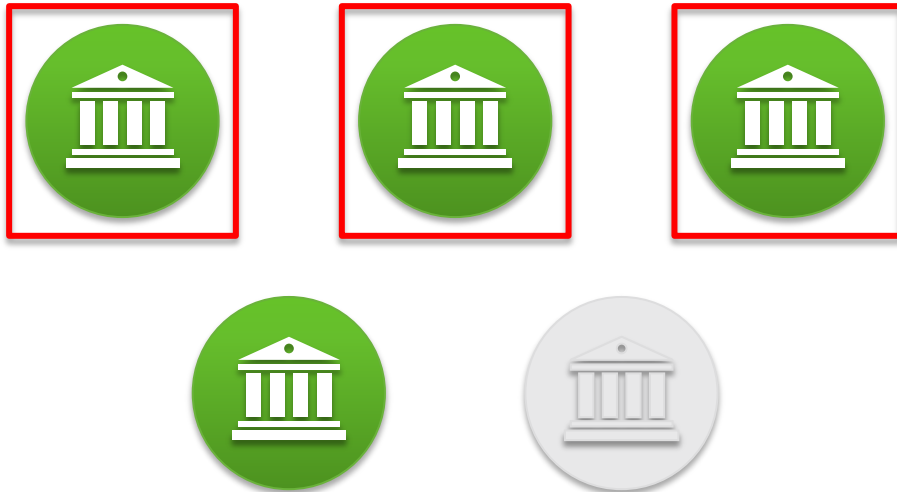
네트워크 가상화기술 (VMware NSX)을 적용한 VDI 인프라 구현



VMware NSX Momentum

4 of 5

top investment banks

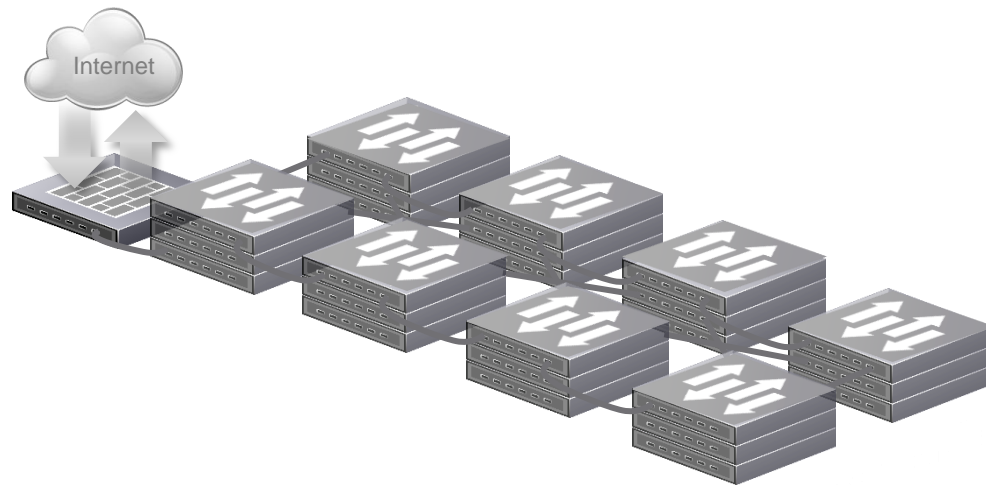


Leading global

enterprises & service providers



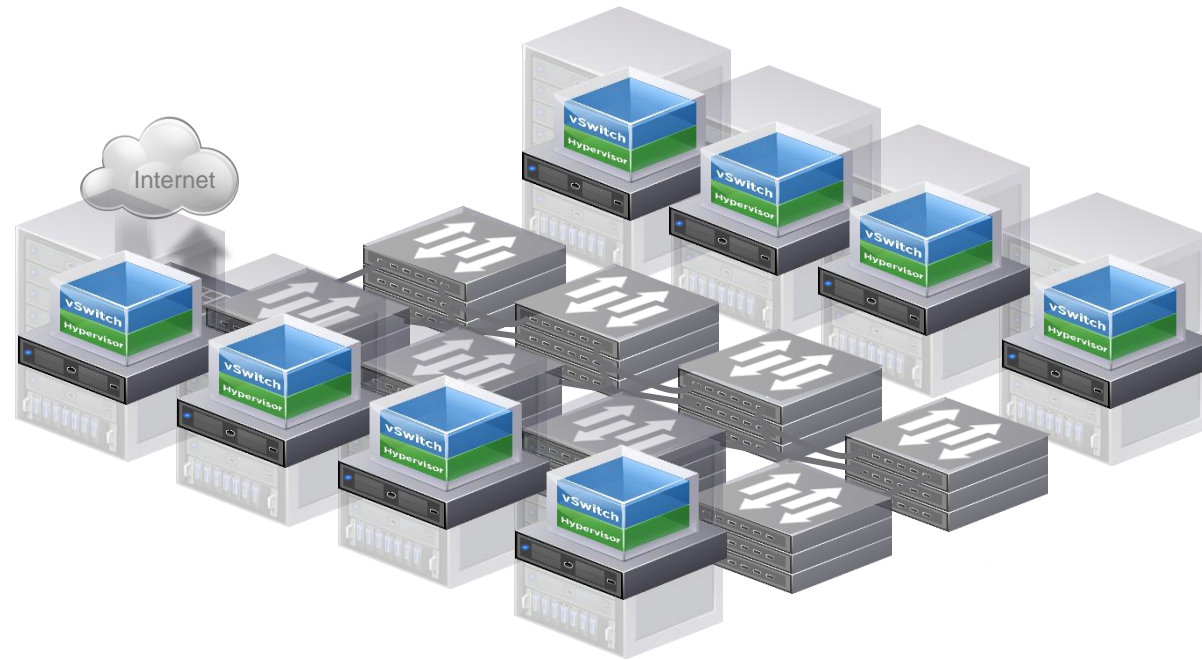
네트워크 인프라 ...



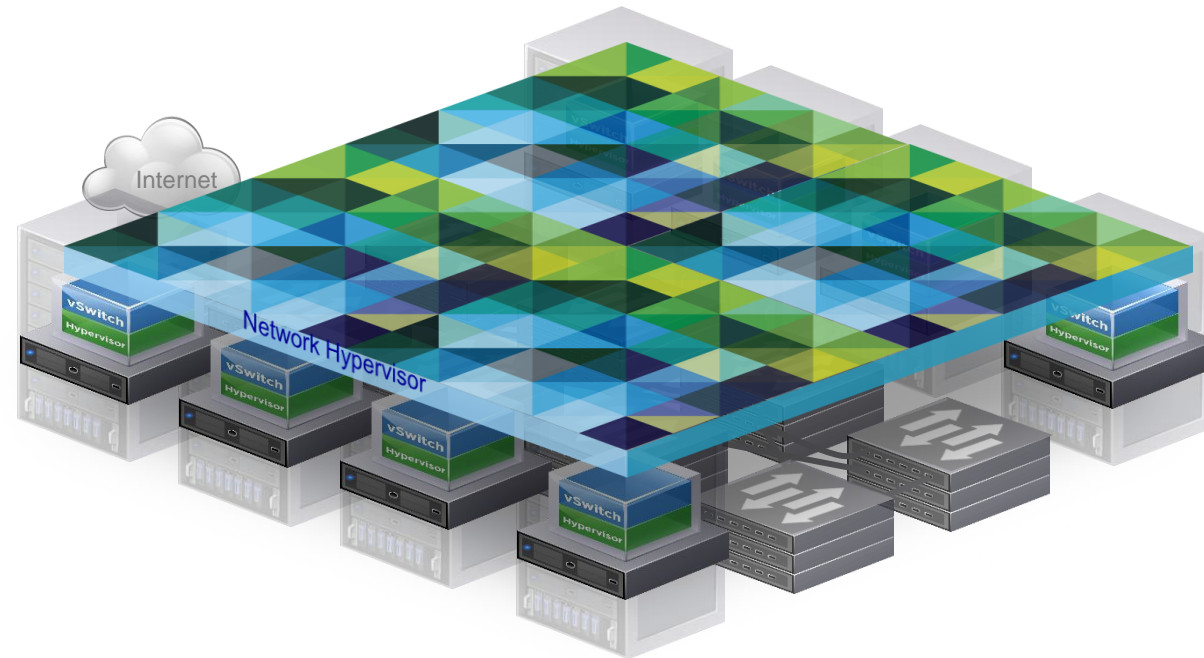
컴퓨터 인프라 ...



데이터센터 가상화 레이어

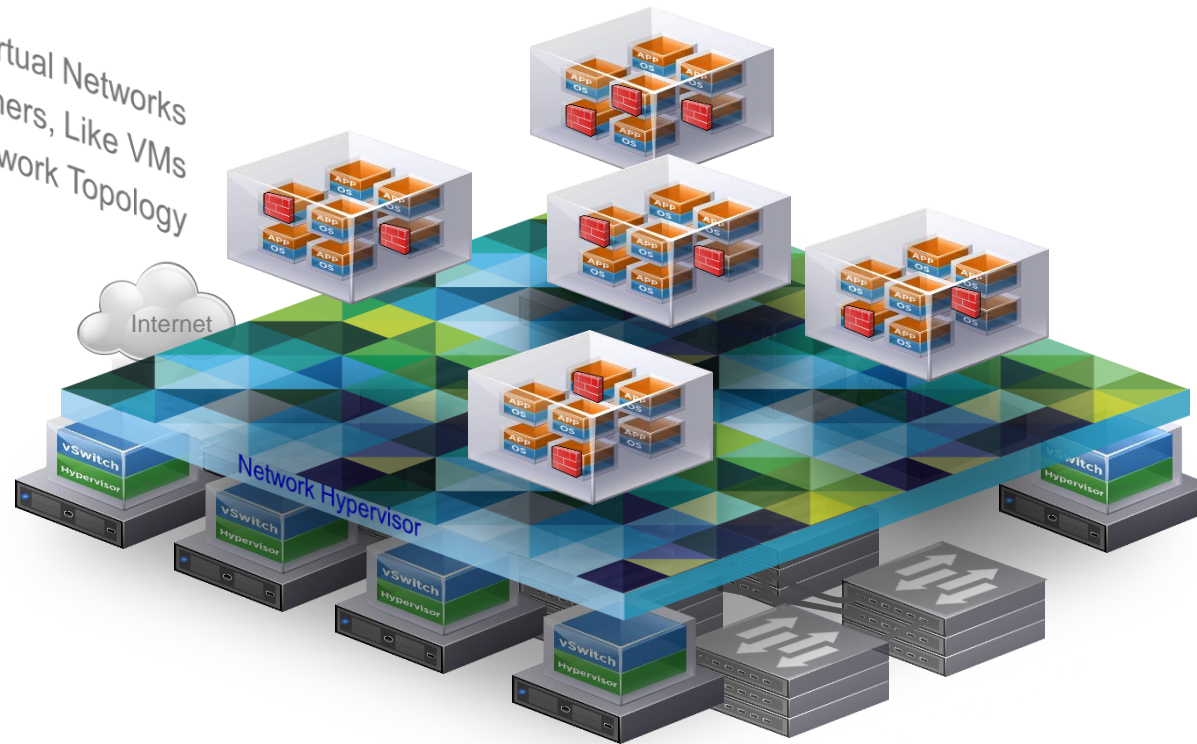


네트워크 하이퍼바이저



가상 서버들을 위한 네트워킹 운영 모델

Virtual Networks
Software Containers, Like VMs
Virtual Network Topology



VMware NSX 구성요소

Orchestration



vCloud® Automation Center™
OpenStack, etc

VMware NSX Manager™ with vCenter

Management Plane



Virtual Appliance

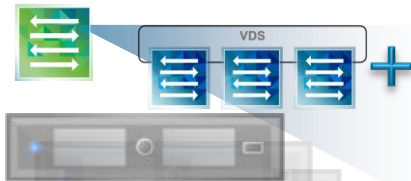
VMware NSX Controller™

Control Plane

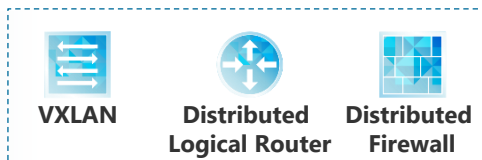


Virtual Appliance

Distributed Services



VMware ESXi™



Hypervisor Extension Modules

VMware NSX Edge™



Logical Router



Logical FW



Logical Load Balancer



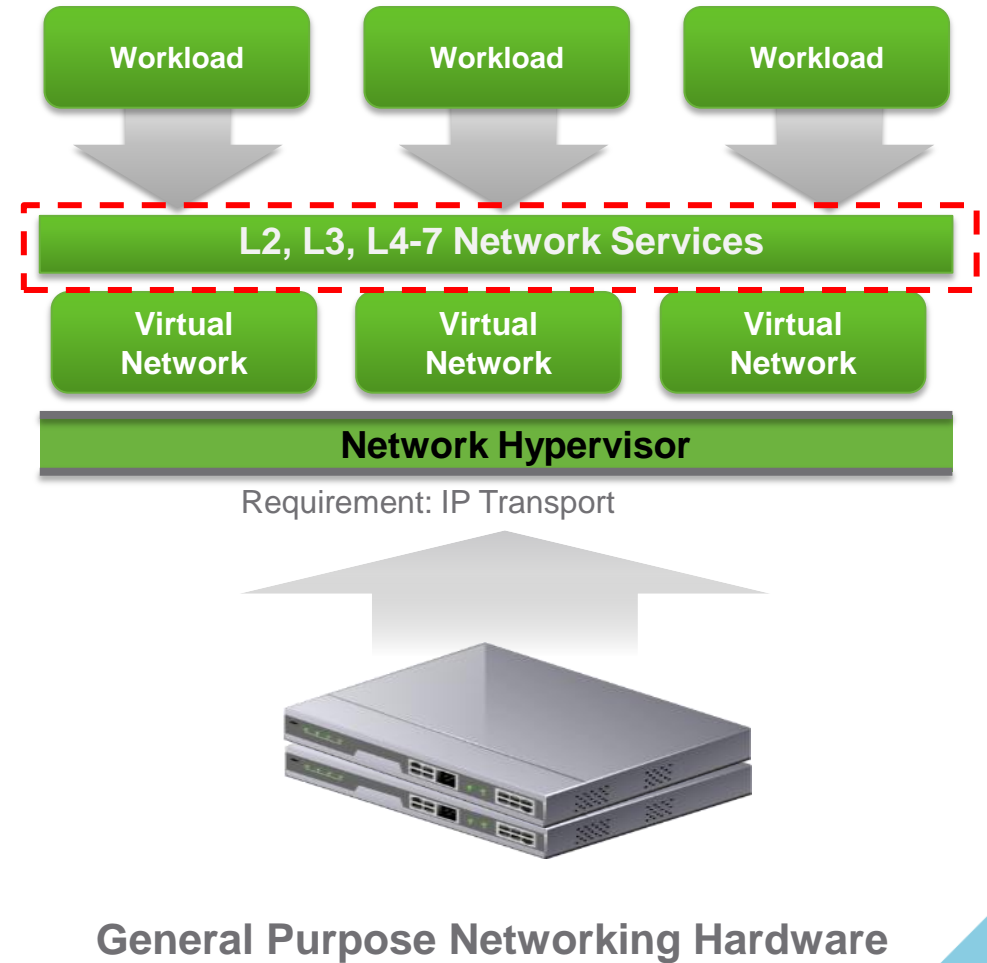
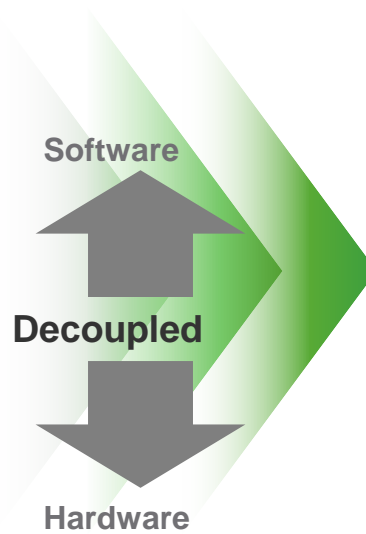
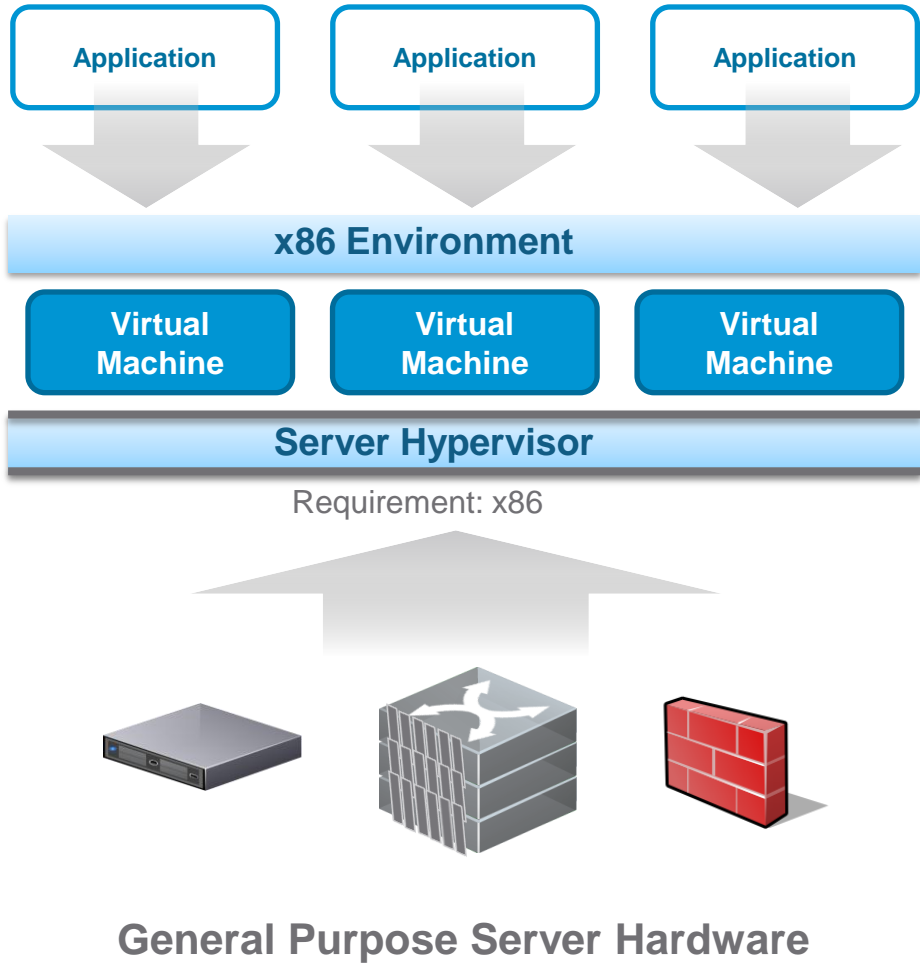
Logical Connectivity VPN

VPN

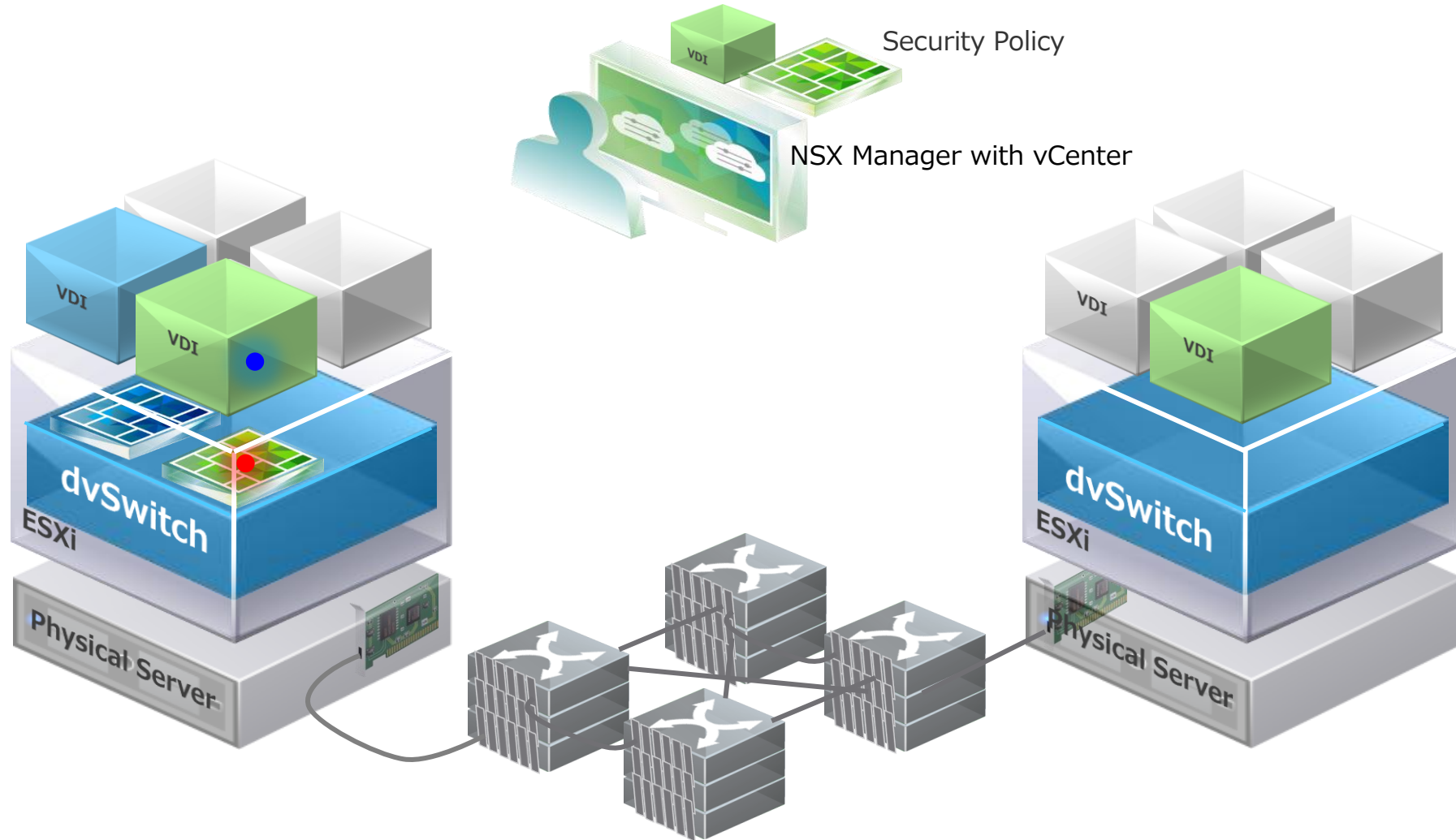
Virtual Appliance



네트워크가상화와 서버가상화의 유사점



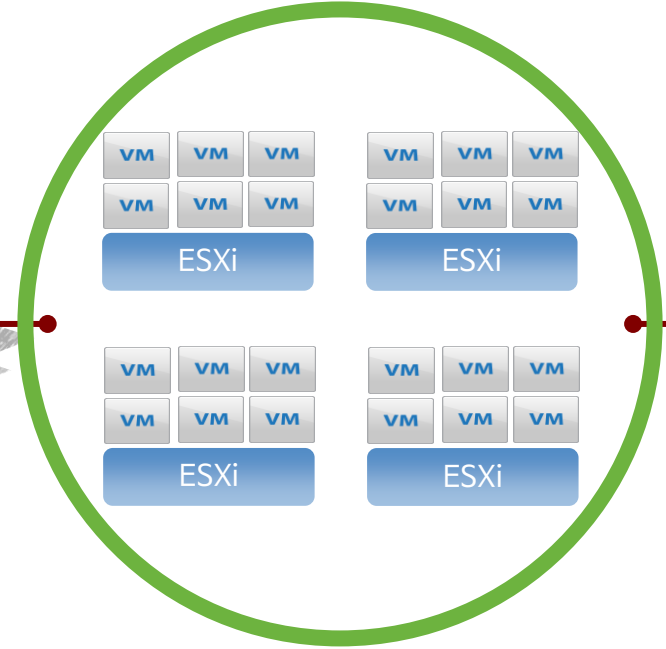
하이퍼바이저 기반의 분산방화벽



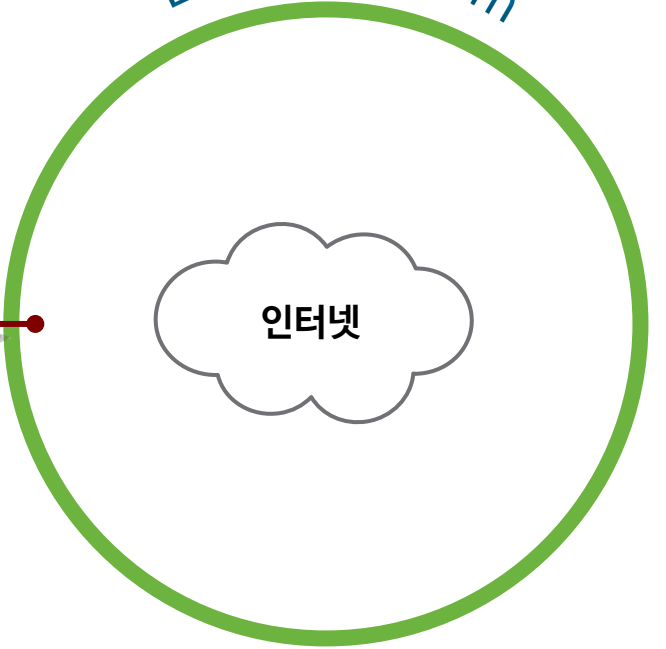
Server Farm



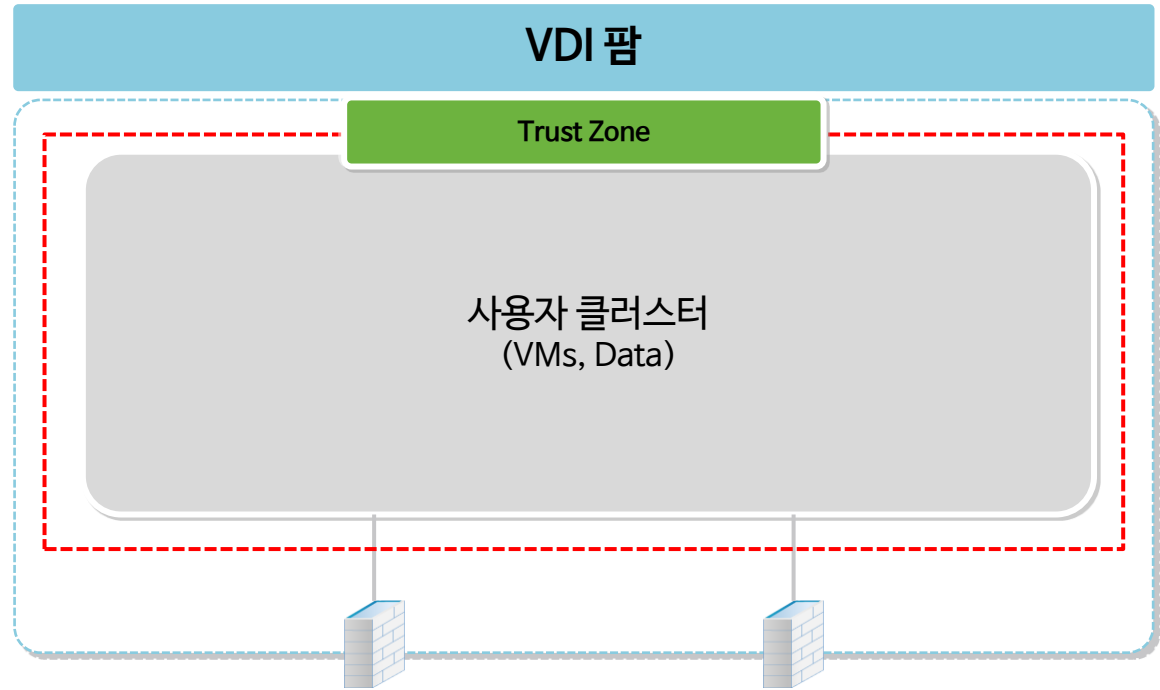
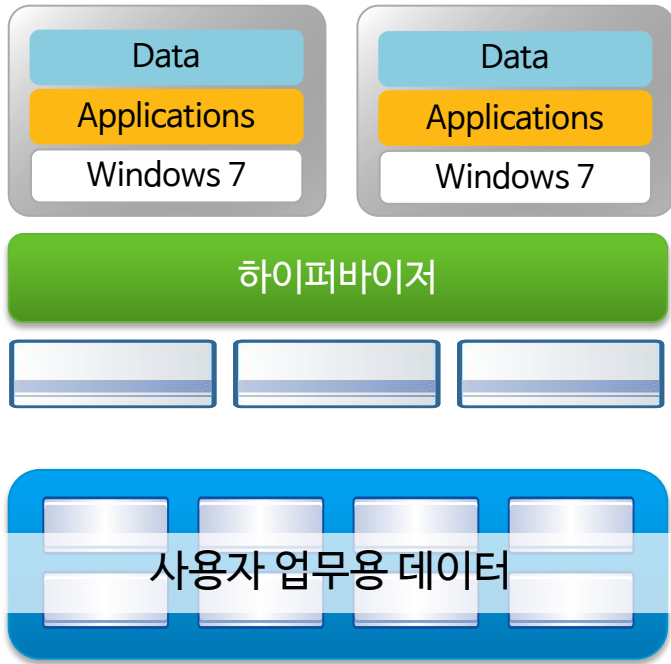
VDI Farm



인터넷 접속 Farm



Use Case #1 : Micro-Segmentation

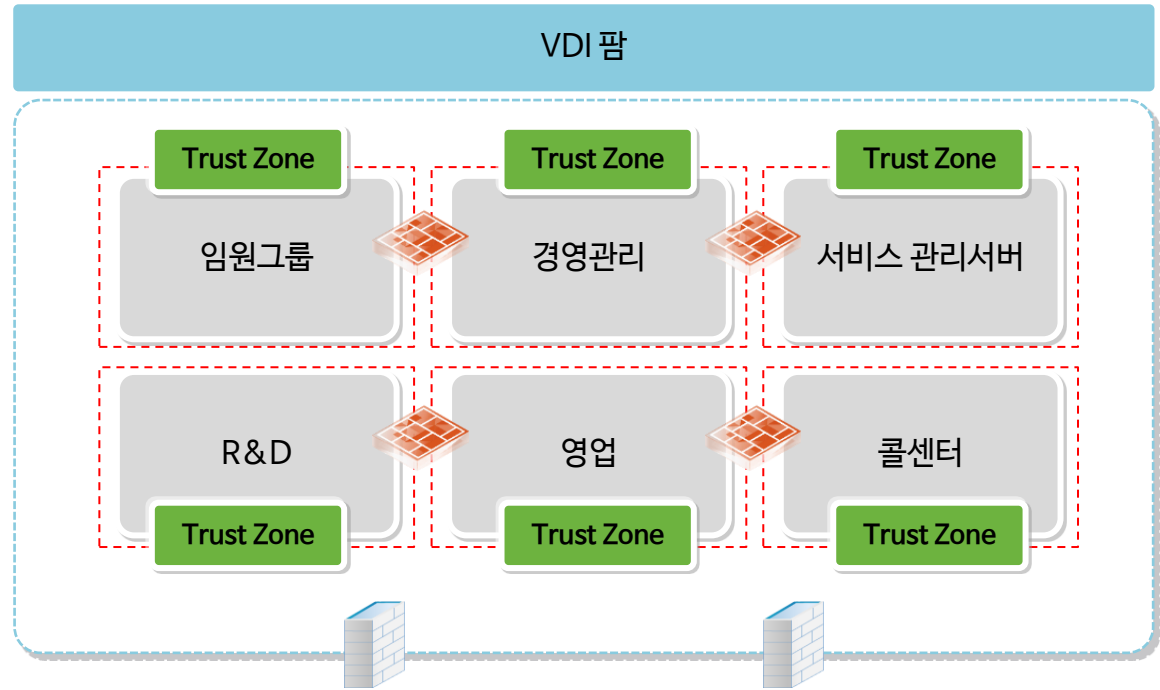
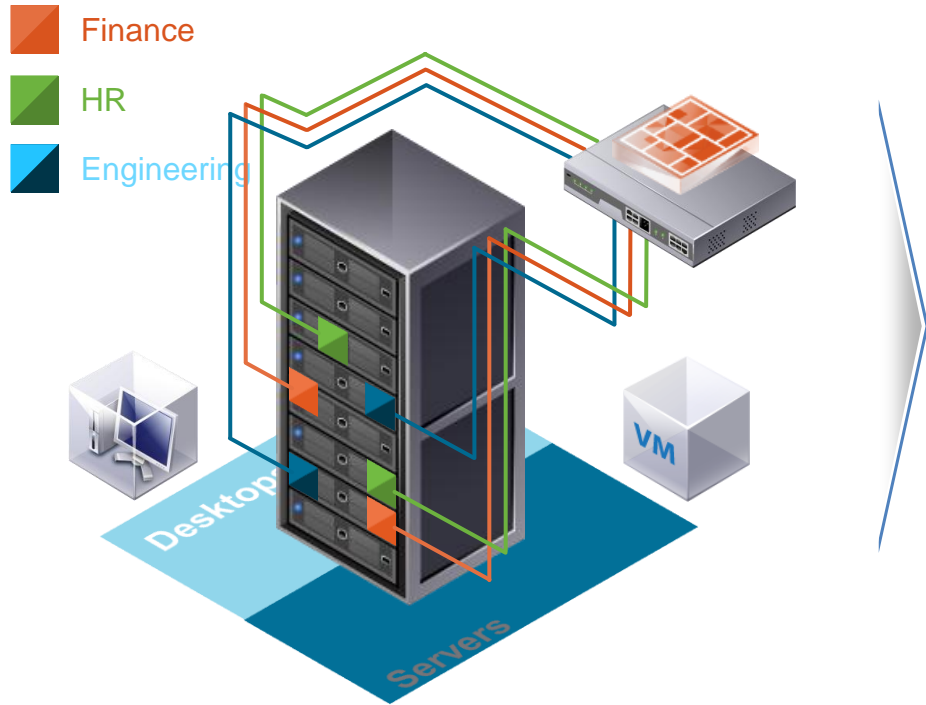


VDI 팜내 보안통제 없음

모든 VM간 연결 및 데이터 접근가능

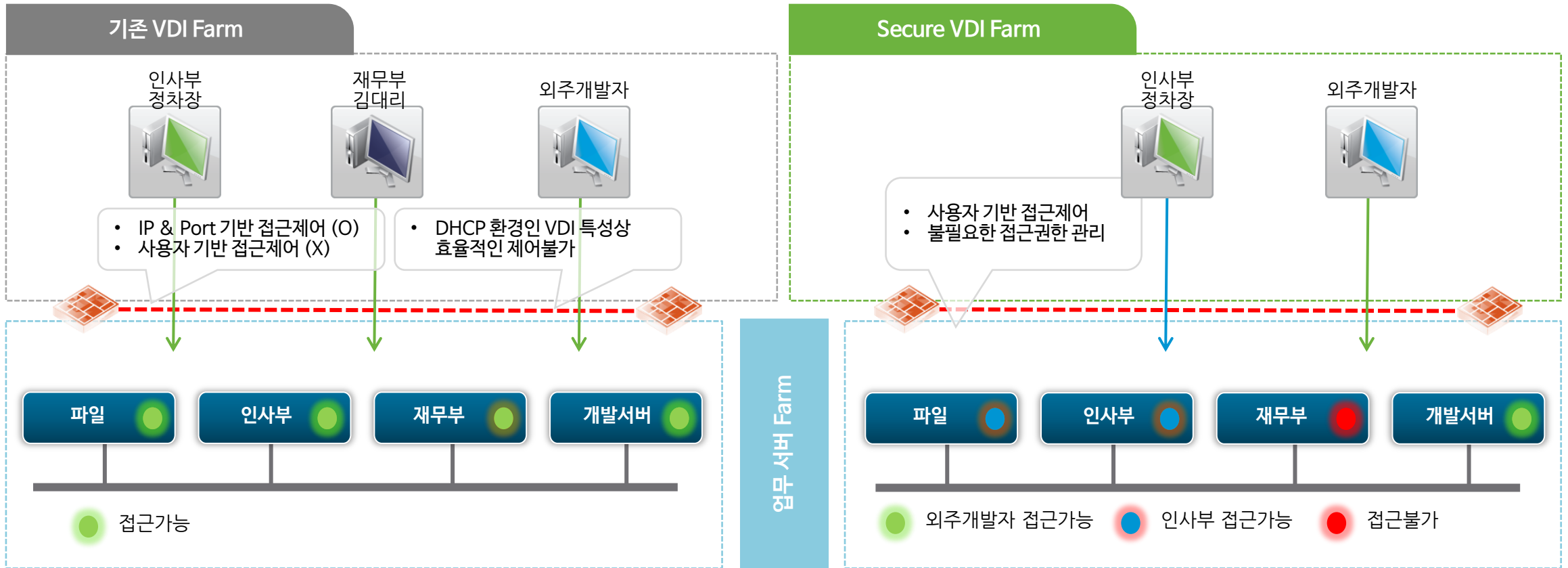
특정 VM 보안이슈 발생시 모든 VM 영향/확산 가능성

Use Case #1 : Micro-Segmentation



Micro Segmentation
- Zero Trust, Zone Security -

Use Case #2 : Access Control - 사용자 기반



Use Case #3 : 감염단말 자동격리

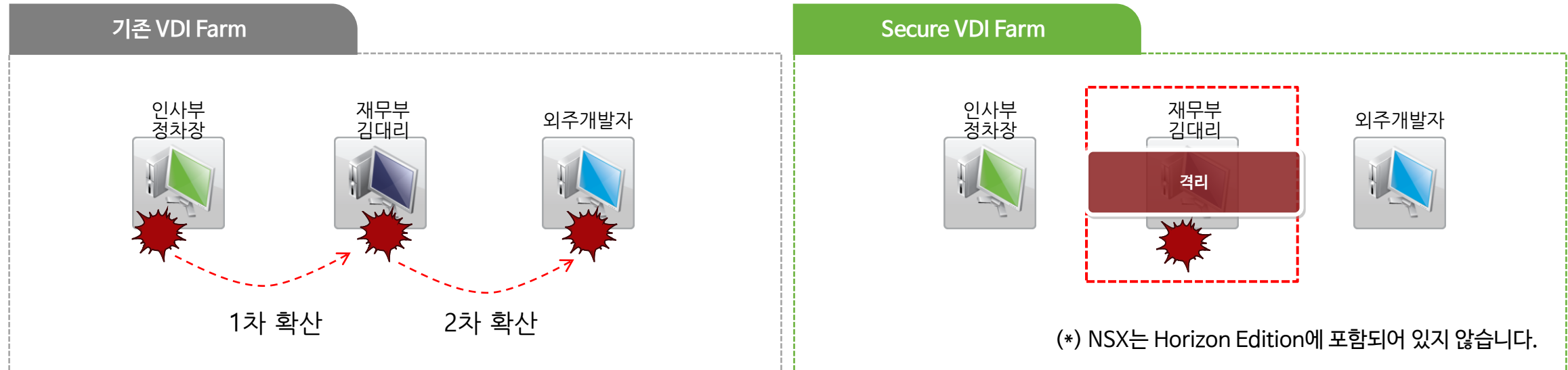
Security Group = **Quarantine Zone**
Member = {Tag = 'ANTI_VIRUS.VirusFound', L2 Isolated Network}

Security Group = **VDI**
Member = {Tag = VDI}



Use Case #3 : 감염단말 격리

Horizon View는 전문 APT(표적공격) 대응 솔루션과 연동하여 VDI Farm내의 의심/감염 시스템을 능동적으로 감지 및 자동 격리조치 할 수 있습니다.



(* NSX는 Horizon Edition에 포함되어 있지 않습니다.)

AS-IS

- VDI팜내 악성코드 유입시 확산방지 불가능
- VDI팜내 트래픽에 대한 이상감지 불가능
- VM별 백신SW에 절대적 의존

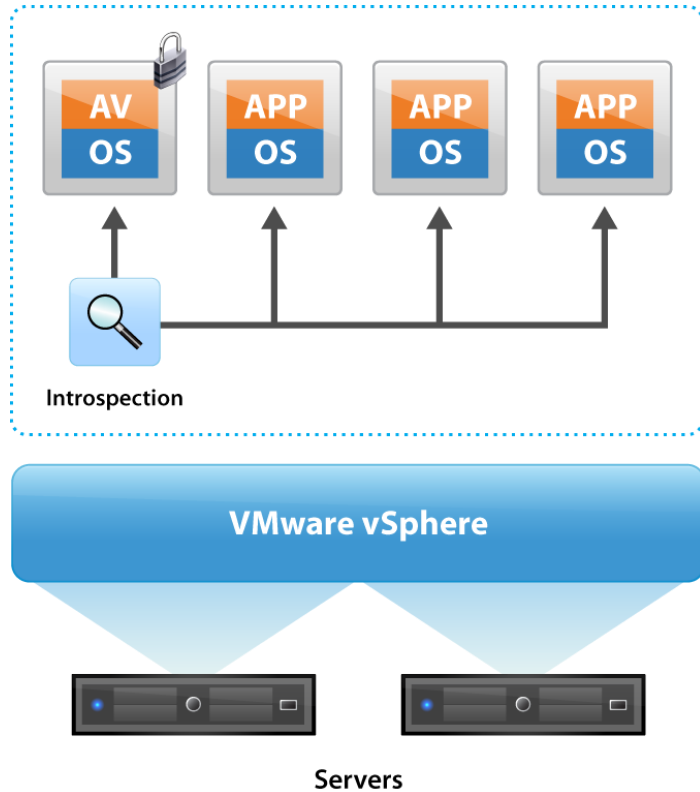
TO-BE

- 차세대 방화벽 및 백신SW 연동을 통해 VM간 트래픽 감시
- Agentless 백신SW 연동을 통해 VM간 악성코드 전이 감시
- 감염 의심 VM에 대한 자동격리



Use Case #4 : 효율적인 보안솔루션 운영

Horizon View는 하이퍼바이저 레벨에서의 백신솔루션과의 연동을 통해 안정적인 VDI 및 백신솔루션 운영을 보장합니다.



백신 솔루션의 동작방식의 혁신을 통한 가상호스트 성능개선

오프로드 방식 백신기능 :하이퍼바이저(vSphere)와 백신솔루션 연동을 통해 Agentless 백신기능 구현

주요기능

- ❑ 파일 액세스에 대한 보안검사를 Security VM이 담당
- ❑ 악성코드 조치(삭제, 격리 등)는 VM의 드라이버(VM tool)을 통해 처리
- ❑ API를 통해 보안파트너사 솔루션과 연동(트렌드마이크로, 시만텍, 맥아피)
- ❑ API(REST)를 통한 정책관리
- ❑ 로깅기능 제공

Summary

빠르고 간편한
VDI 네트워킹



자동화된
정책관리



확장 가능한 역할
기반 보안

감사합니다.