데스크탑 클라우드를 위한 보안

IBM Software

Pulse2010

Pulse Comes to You

Optimizing the World's Infrastructure

April 29 Seoul, Korea

데스크탑 = 서버?

Quad Core,
4GB,
1TB…
DVD recorder
1GB Lan..

영업사원

S/W 개발자

기업담당자

고성능 데스크탑은 애물단지?

백신프로그램?
-> 감지되지 않으면, 막을 수 없다!

접근제어?
-> 누군가는 접근해야 한다

케이블?서약서? DRM?
-> 사용자의 부주의/고의적 행위는 훈련되지 않음

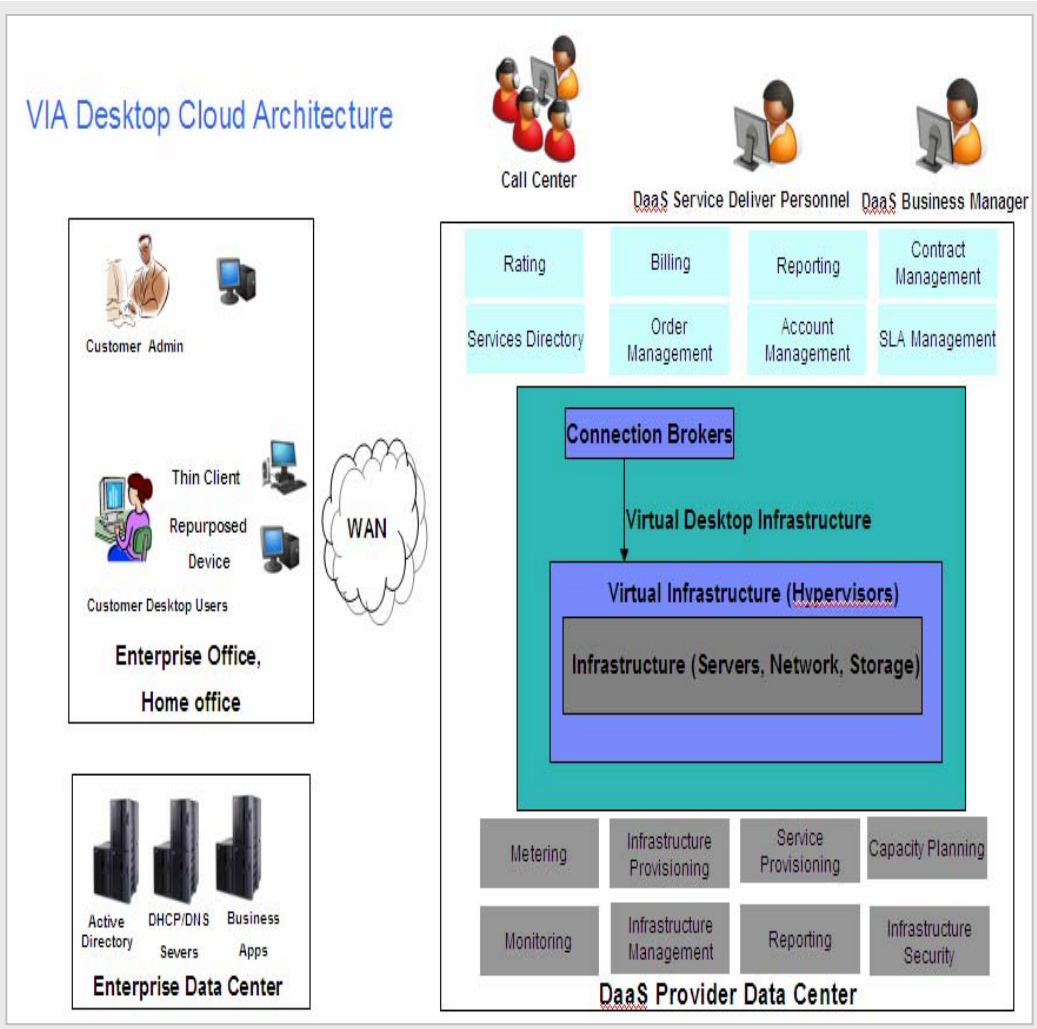
매체 파기?
-> 협력업체, 대리점에 있는 PC는 어떻게?

새로운 대안?

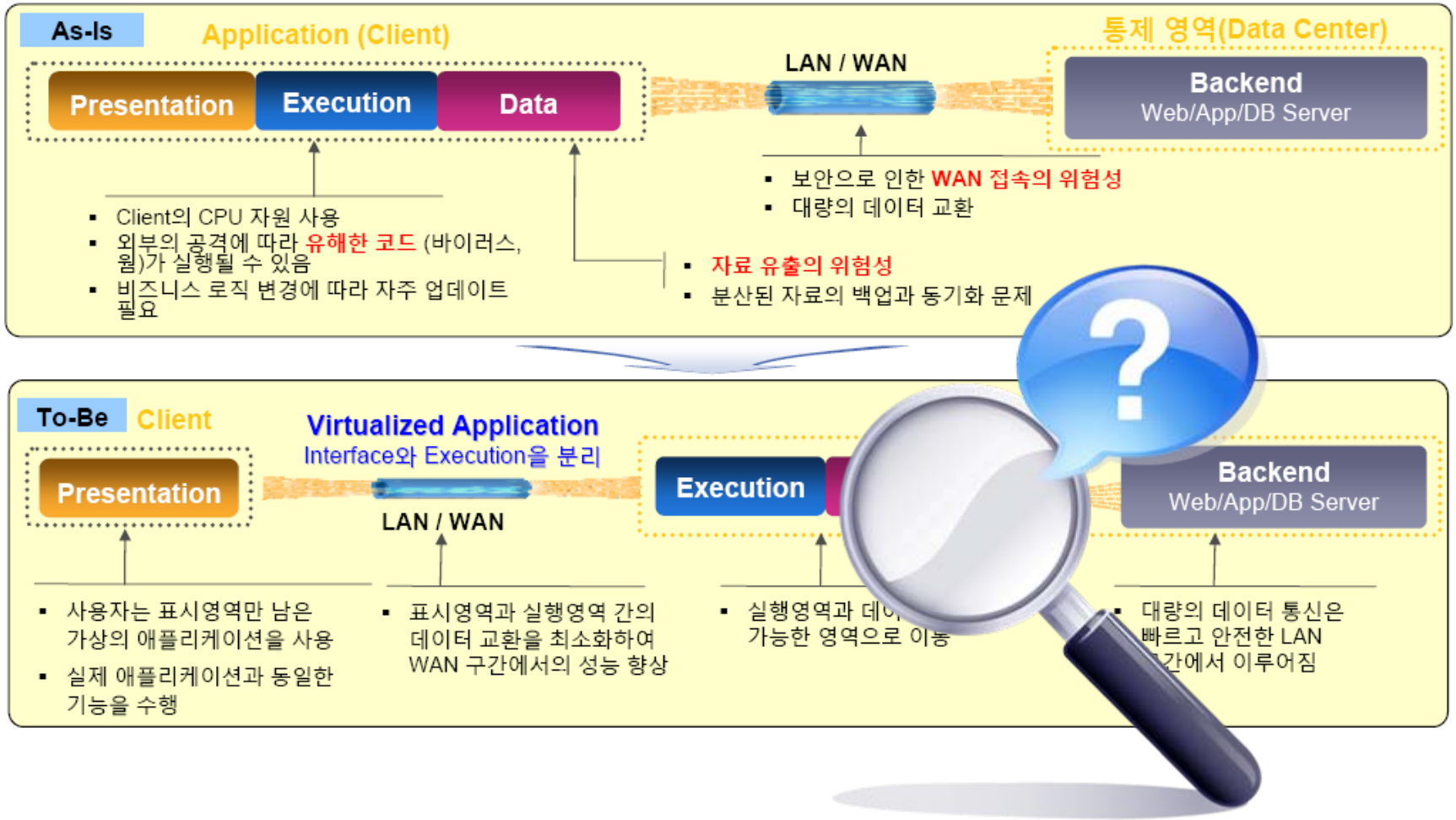
데스크탑 클라우드, DaaS

주요 특징 및 기대효과

- 서버기반컴퓨팅의 확장으로 사용자들이 가상화된 데스크탑을 사용하고, 사용하는 만큼 비용을 지불하게 됨
- Public Cloud / Private Cloud로 모두 구현 가능
- 서비스 특성
  - **표준화된 데스크탑 기능 제공**
  - 중앙 집중형 데스크탑 관리
  - 가용성 향상
  - **리소스에 대한 유연한 접근**
  - 100% 호스팅 서비스
  - 미리 구현된 패키지 형태의 서비스 (고정비용)
- **기대효과**
  - 업무 공간 대체
  - 데스크탑 관리 비용 절감
  - **중앙 집중형 서비스를 통한 데이터 보안**
  - 데스크탑 복구의 위험 줄어듦
  - Green, Mobility 등의 기업 전략과

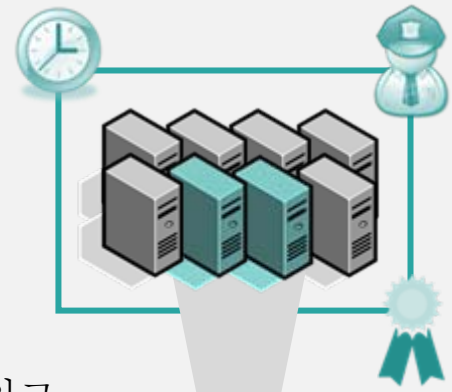


데스크탑 클라우드의 보안 이점, 그러나...



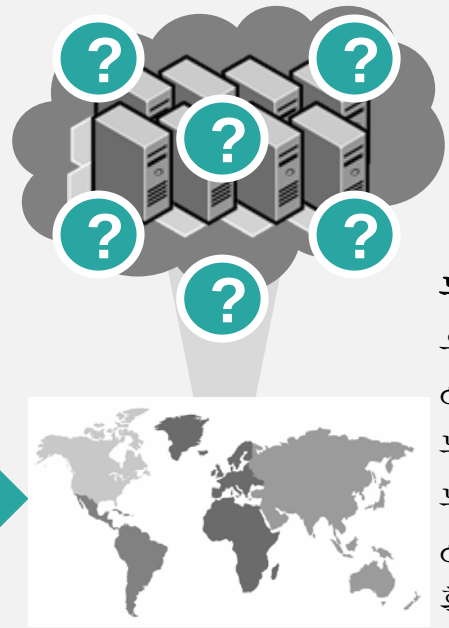
클라우드 환경에서의 새로운 보안 위협

현재의 전산 센터



통제할 수 있다.
자산들은 특정 위치에 있고.
서버의 수량과 종류를 알고 있다.
주기적인 백업과 관리자에 의해
접근 통제를 수행한다.
가동 시간은 충분하며,
보안팀을 운영하고,
정해진 기간에 감사를 받는다.

미래의 클라우드 컴퓨팅 환경

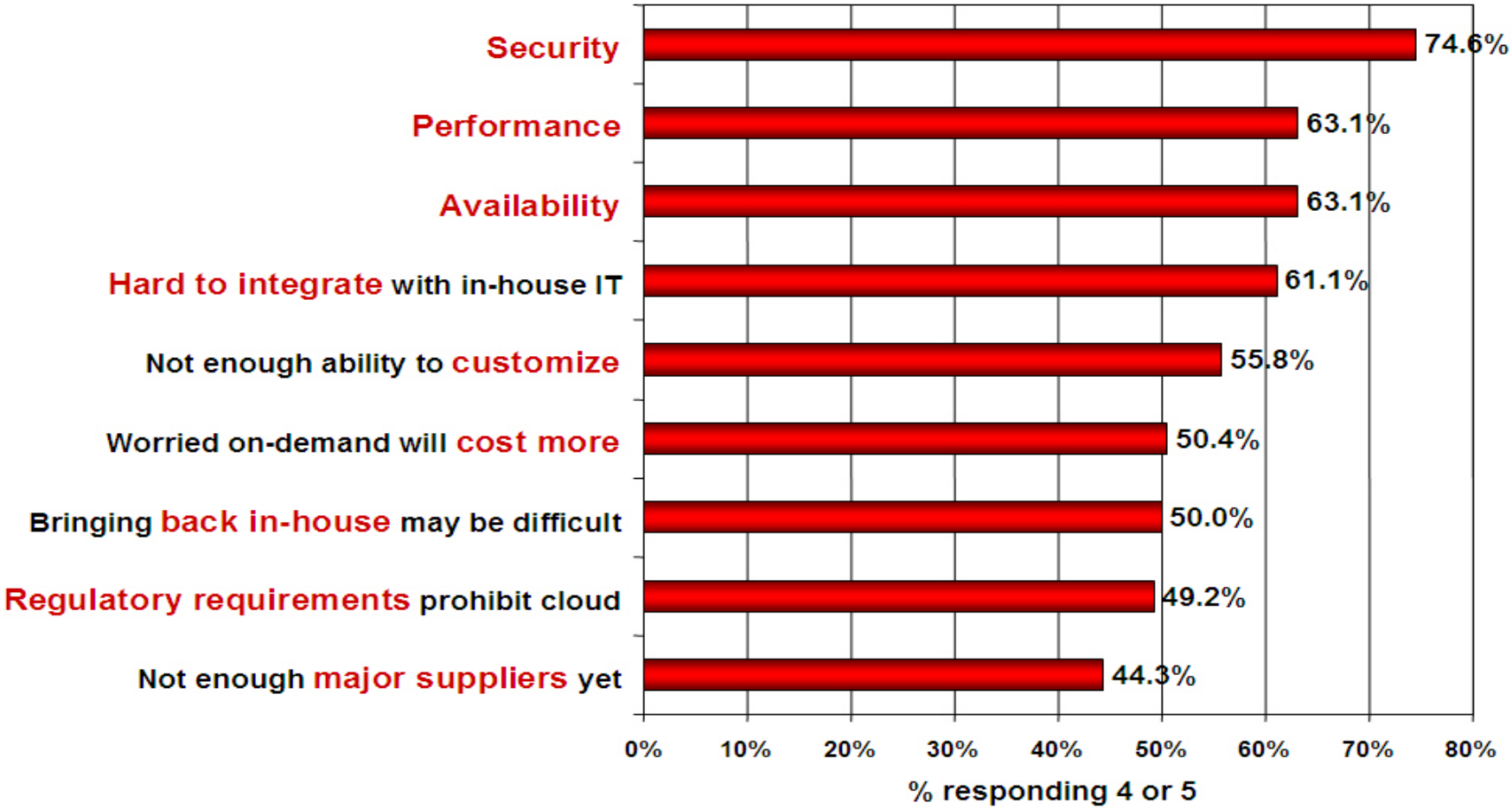


누가 통제하는가?
우리의 정보가 어디에 있고?
어디에 저장되며?
누가 백업하고?
누가 접근하며?
어떻게 서비스 지속성을
확보하고?
어떻게 감사하며?
어떻게 우리 보안팀이
관여할 것인가?

클라우드 컴퓨팅의 이슈

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

가상화 = 새로운 복잡성

- 새로운 복잡성
  - VM(가상머신)의 동적 재설정
  - 관리와 보호를 위한 인프라스트럭처 레이어의 증가
  - 다양한 O/S 및 애플리케이션
  - 시스템간 물리적 구분의 제거
  - 소프트웨어와 VM구성에 대한 수동 추적
  - 가상 이미지의 유지보수
  - 백업/재난 복구
  - 이미지와 데이터의 지리적 위치

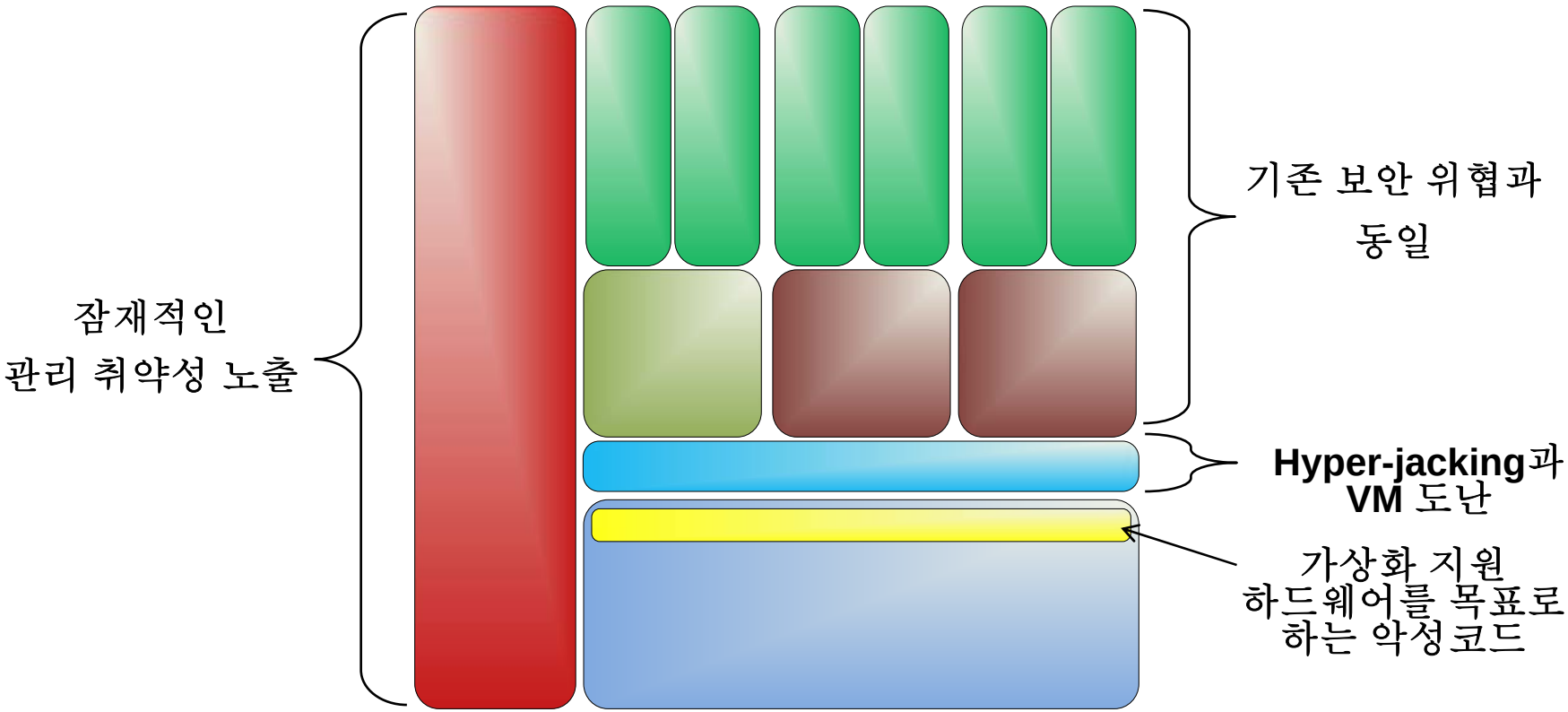
가상화 이전

- 서버 당 OS와 애플리케이션의 1:1 비율

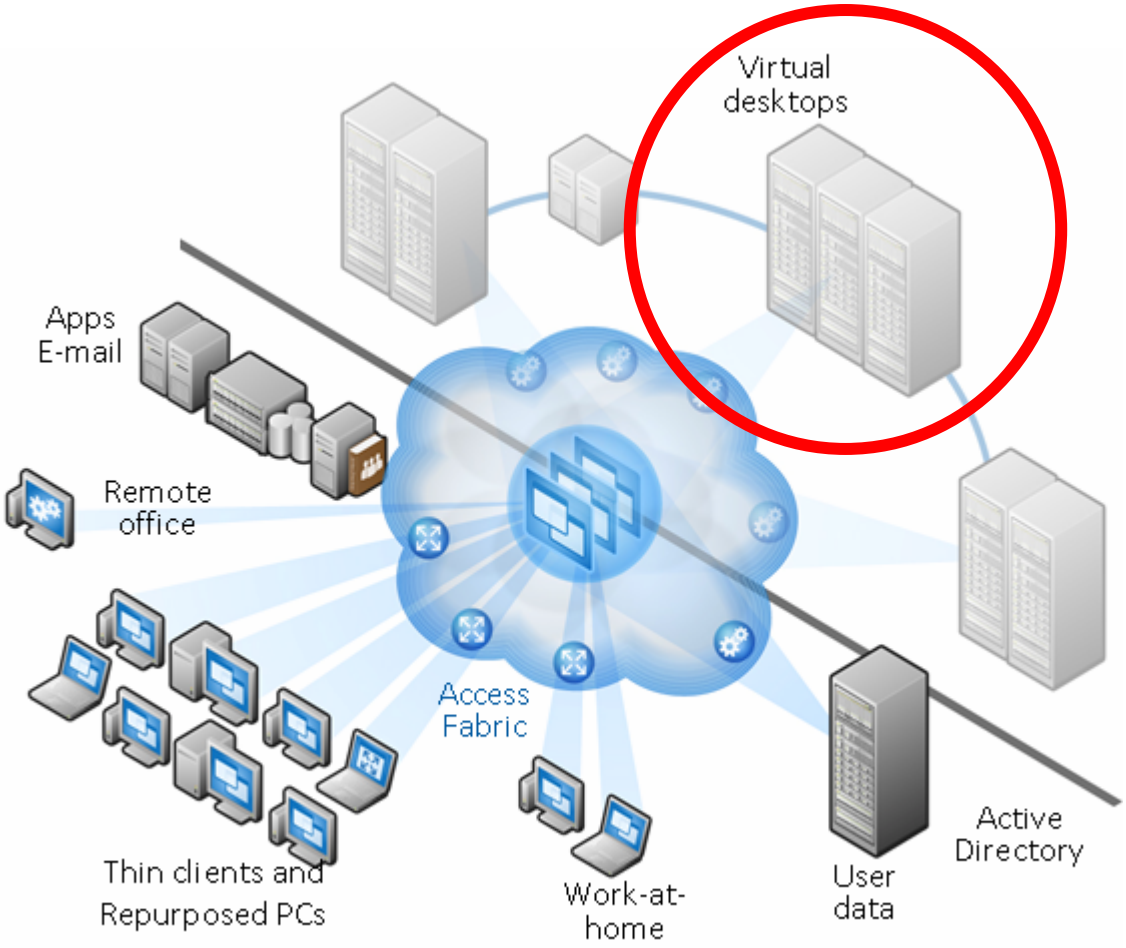
가상화 이후

- 서버당 OS와 애플리케이션의 1:M 비율
- 관리와 보안을 위한 레이어의 추가

가상 환경에서의 보안 위협 요소



클라우드 데스크탑의 위협 요소



표준 데스크탑 이미지의 보호

데스크탑 이미지에 대한 라이센스

Runtime 무결성 관리

마스터 이미지의 패치

사용자 이미지 패치

시스템/서비스의 **Health Check**

관리자/사용자 계정 도용.....

가상화 환경에 대한 Legacy 보안의 한계

	안전하게 보이지만..	... 충분히 안전하지 않음
네트워크 IPS	경계선에 대한 위협과 공격에 대한 방어만 수행	경계선 뿐만 아니라 VMs간의 위협에 대해 보호해야 함
서버 보호	단일 Agent를 통하여 개별 물리적 서버를 보호하고 보고함	물리적 서버의 보호 뿐만 아니라 각 VM을 보호해야 함
시스템 패치	개별 서버와 네트워크에 대해서 중요한 취약점을 패치 해야 함	VM에 대해 추적 및 패치를 수행할 필요가 있으며 VM전개를 통제해야 함
보안 정책	정책은 각 네트워크 세그먼트와 서버내의 핵심 애플리케이션에 대해 정의됨	정책이 더 많은 부분을 포함해야 하며(Web, 데이터, OS, 데이터베이스) VMs에 적용될 수 있도록 변경해야 함

IBM의 가상화 보안

가상화 워크로드의 보호에 검증된

- IBM Security Server Intrusion Prevention System (IPS)
- IBM Security Network IPS
- IBM Security Network Mail Security Systems
- Data Loss Prevention

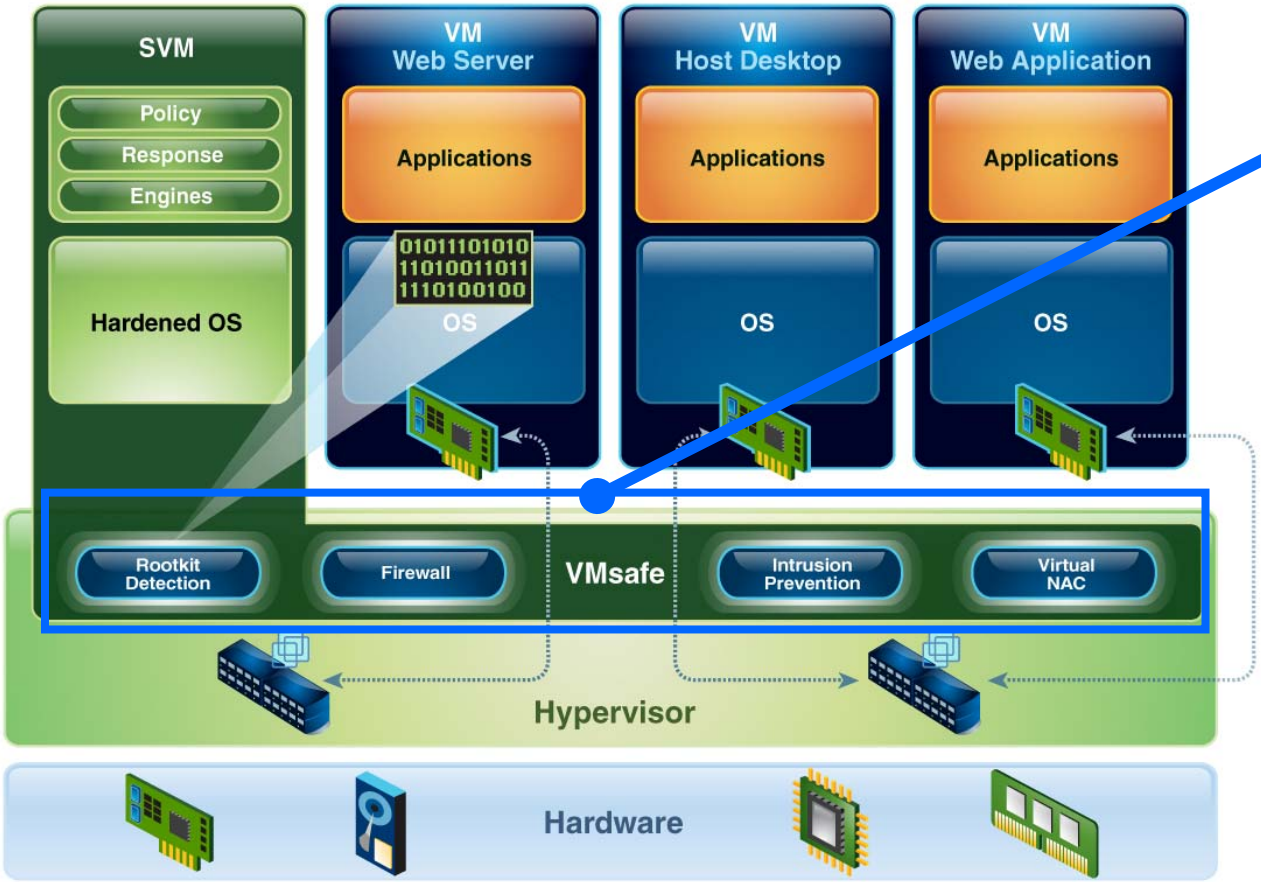
가상화된 폼-팩터 내에 위협에 대한 보호를

- IBM Security Virtualized Network Security Platform
- IBM Security Network Mail

통합된 가상화 환경- 위협에 대한 보호를

IBM Virtual Server Security for VMware®

IBM Virtual Server Security for VMware



IBM Virtual Server Security for VMware

- VMsafe Integration
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- Virtual Network Access Control

IBM 가상화 보안 솔루션의 특장점

쉬운 구현, 쉬운 보안의 유지

- 개별 **VM**의 온라인 시 자동 보호 수행
  - 자동 발견
  - 자동화된 취약점 진단 및 평가
  - IBM Virtual Patch® technology
- 비 관입**(Non-intrusive)**
  - 가상화 네트워크의 재구성 없음
  - Guest OS내에 제공되지 않음
    - 향상된 안정성
    - 워크로드에 대해 더 많은 CPU/memory을 할당
    - 공격 요소의 감소
- **Guest OS** 종류에 상관 없는 보호
  - 다양한 OS들을 위한 보안 agent의 감소
- **Guest OS**내에 존재하지 않음
  - 더 많은 CPU/memory를 워크로드에 부여
  - 공격 요소를 감소
- 중복되는 처리 작업을 제거하여 관리 부담을 경감시킴
  - 물리적 서버 당 한 개의 보안 가상화 머신(SVM)
  - 1:다수의 VM보호 비율
  - Guest OS로부터 CPU에 의존적인 프로세스를 제거하여 SVM에 독립화
- 중앙집중화 된 관리
  - IBM Security Management SiteProtector™ system

IBM 가상화 보안 솔루션의 특장점

1. *최신의 가상화 보안 전문가의 조언, 프로세스, 기술을 적용하여 비용을 줄임*
2. *최신의 보안 위협과 취약점을 경감하고, 모니터하고 관리함*
3. *규제 준수에 대한 위험을 식별하고 경감함*
4. *VMs에 대한 내부 엑세스의 제한 및 민감한 정보의 외부 유출 방지를 위한 비용을 줄임*
5. *IAM (Identity and access management)의 비용을 줄임*
6. *애플리케이션 레벨의 취약점으로부터 야기될 수 있는 위험을 경감시킴*

IBM의 가상화 보안 스펙트럼


최종 사용자


엔터프라이즈 관리자


IT 감사자(내부통제자)


애플리케이션 관리자


클라우드 제공자

Privileged User Access
centralized access and audit policies, directories

Identity Management
single sign-on, identity provisioning technologies

Privileged Account Management
change control processes for privileged users

Trusted Identity
protecting their identities as constituents, employees, and consumers

People and Identity

Data Segregation
encryption, network segmentation, Hardware / OS / App / Database isolation

Data Recovery
centralized backups, remote storage

Data Reduction and Termination
secure removal processes for customer data and metadata

Data Leakage Prevention
DLP technologies for data in motion and data at rest

Data and Information

Compliance and Auditing
audit policy creation, log generation and management

Investigative Support
audit retention, search, and correlation

Policy Management
unified security, governance, and policy enforcement

Secure Provisioning
image management, hardening, cohabitation policies

Application Testing
vulnerability assessment, fuzzing, app scanning, automated code reviews

Application and Process

Server Security
trusted computing, auditing, access control

Network Security
Firewall, IPS, VLAN

Virtualization Security
VM Segmentation, Virtual Appliances, Integrated Hypervisor Security

Browser Security
ssl, memory protection, multi-level security, anti-malware

Patch Management
assessment, prioritization, scheduling, and application

Network, Server, and Endpoint

Data Location
cloud data centers

Disaster Recovery
highly resilient clouds

Cloud Availability
multiple cloud centers

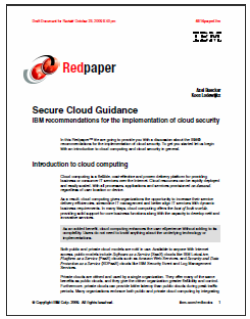
Physical Infrastructure

Why IBM?

IBM Security Framework

보안에 대한 비즈니스적 접근

IBM Cloud Security Guidance



보안에 대한 기술적 접근

IBM Capabilities & Offerings to Help

보안에 대한 제품, 솔루션,서비스

Coarse grained ***Fine grained***

감사합니다

IBM Software

Pulse2010

Pulse Comes to You