보안 프레임워크
클라우드 환경에서의 스마트한 보안 방법

박형근 차장
한국IBM 보안 기술영업 리더

© 2011 IBM Corporation

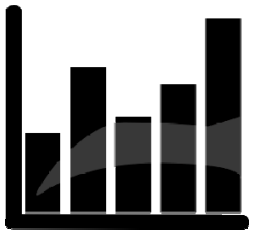
성명	박 형 근	소속	한국 IBM
주요 경력	• 1997 국군기무사령부 사령관 표창 수상(제111호) - 국군기무사령부 전산 보안 체계의 취약점 발굴 보고 • 2004 CISSP(Certified Information Systems Security Professional) 자격 획득 • 2006 CISA(Certified Information Systems Auditor) 자격 획득 • 2006 국가공인 정보시스템 감리원 자격 획득 (서울체신청) • 2008 CGEIT(Certified in the Governance of Enterprise IT) 자격 획득 • 現 방송통신위원회 미래전략 IT 자문 위원 역임 • 現 한국IBM IBM Security 보안팀 기술 리더 • 現 정보보안 전문 커뮤니티 시큐리티플러스 대표 운영자 • 現 국제 정보보안 포럼, Open Group, OASIS, TCG, ISC2, ISACA 정회원	E메일	phk@kr.ibm.com
		저서	• 2010 OASIS 웹서비스 품질 요소 표준 중 웹서비스 보안 품질 분야 표준 저술 (OASIS) • 2010 '경영자, 보안 담당자, 개발자, 감사자가 반드시 알아야 하는 정보 보안 취약점과 지침' 기획, 감수 및 출간 (시큐리티플러스) • 2011 개인정보보호 실천 가이드 공저 (인포더)
		SNS	• 트위터: http://twitter.com/#!/securityinsight • 페이스북: http://www.facebook.com/hyungkeun.park • Linkedin: http://kr.linkedin.com/pub/hyung-keun-park/1/890/113 • 링크나우: http://securityplus.linknow.kr/ • 미투데이: http://me2day.net/mirrk

Get ready to break free.

© 2011 IBM Corporation

클라우드 컴퓨팅이란?

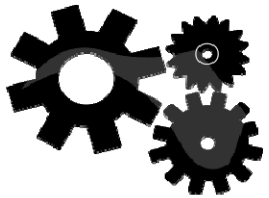
Self Service



Standardized

Virtualized

Flexible
Pay & Metered

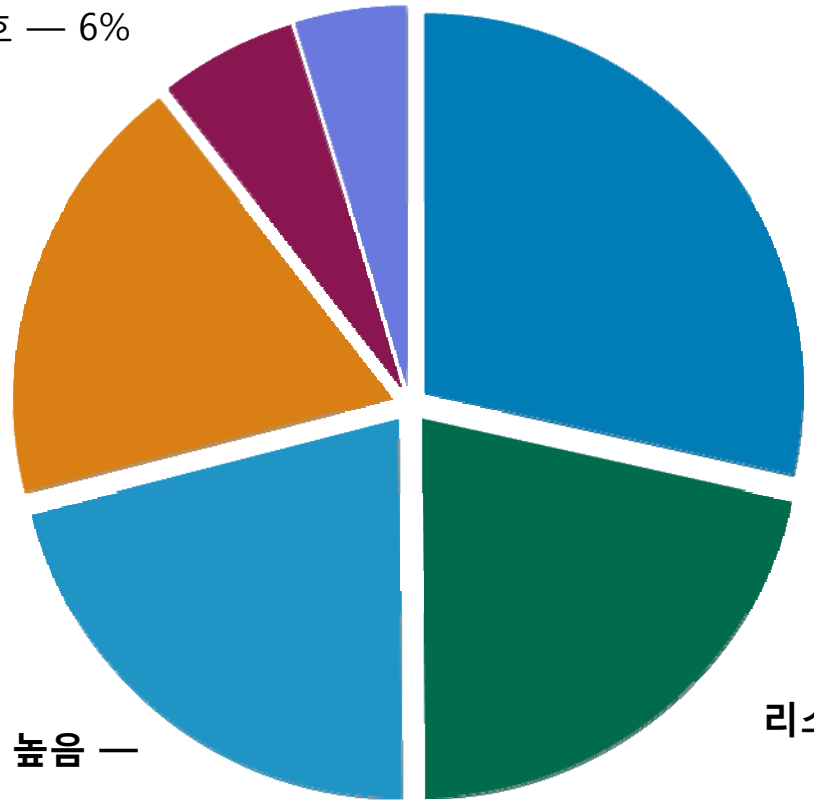


Automated

Get ready to break free.

© 2011 IBM Corporation

리스크 관리 또는 비즈니스 복원 계획에서의 클라우드 컴퓨팅 역할

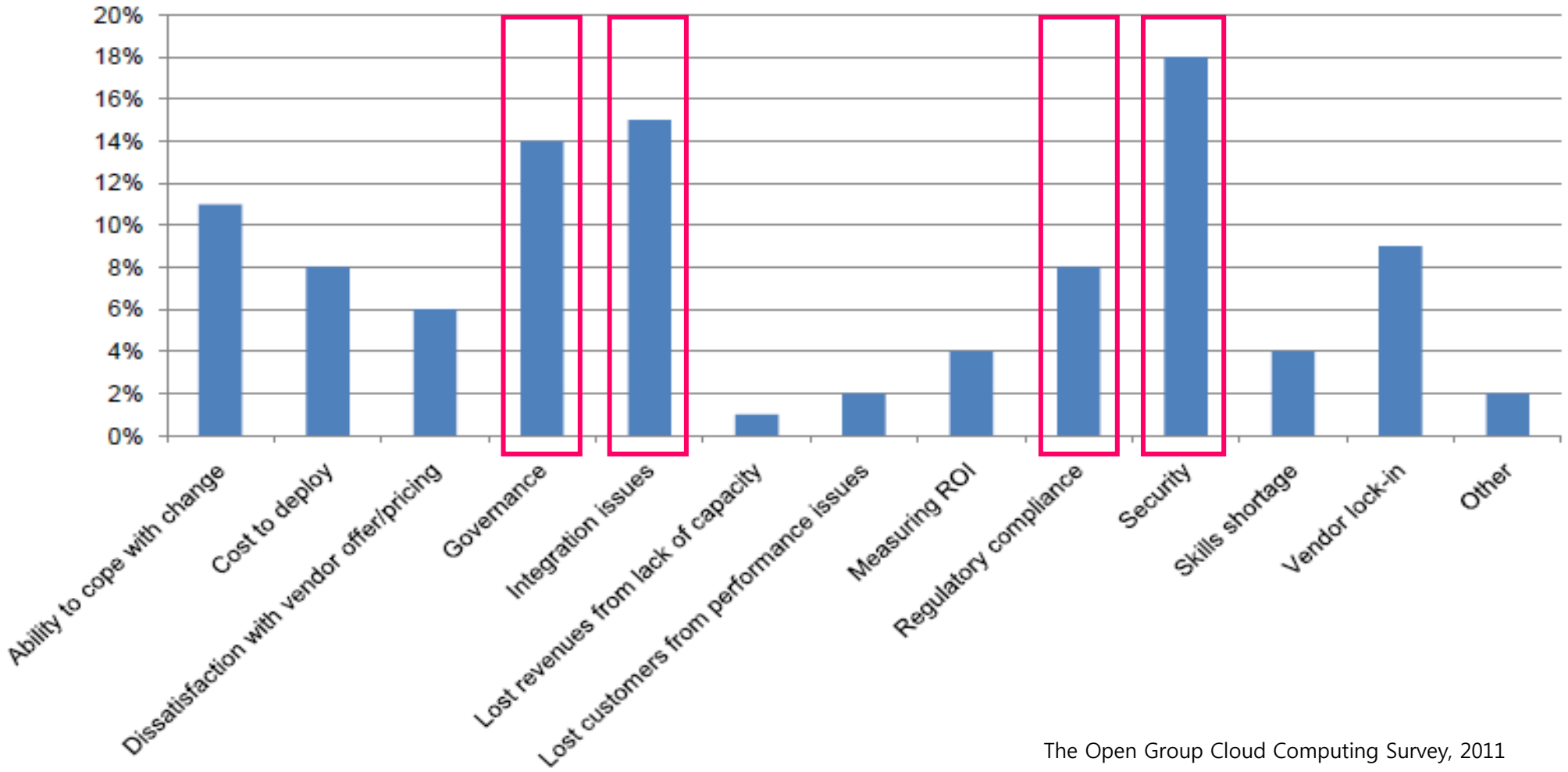


2011 IBM Global Business Resilience and Risk Study 결과

Get ready to break free.

© 2011 IBM Corporation

클라우드 컴퓨팅의 주요 이슈



The Open Group Cloud Computing Survey, 2011

Get ready to break free.

© 2011 IBM Corporation

클라우드 컴퓨팅의 주요 이슈

클라우드 컴퓨팅 환경이 전통적인 환경보다 더 안전할 수도 있다

- **특화된 워크로드 보안**
  - 일반적인 보안이 아니라 특화된 보안에 투자를 집중할 수 있다

- **보안 자원**
  - 믿음과 신뢰를 바탕으로 하는 비즈니스를 하는 조직에 의해 제공되는 보다 증가된 보안 능력으로부터 이점을 얻을 수 있다

- **보안 서비스**
  - 서비스로써의 보안이란 조직이 투자할 수 있는 비용 대비 최고의 제품을 사용할 수 있다는 것을 의미한다

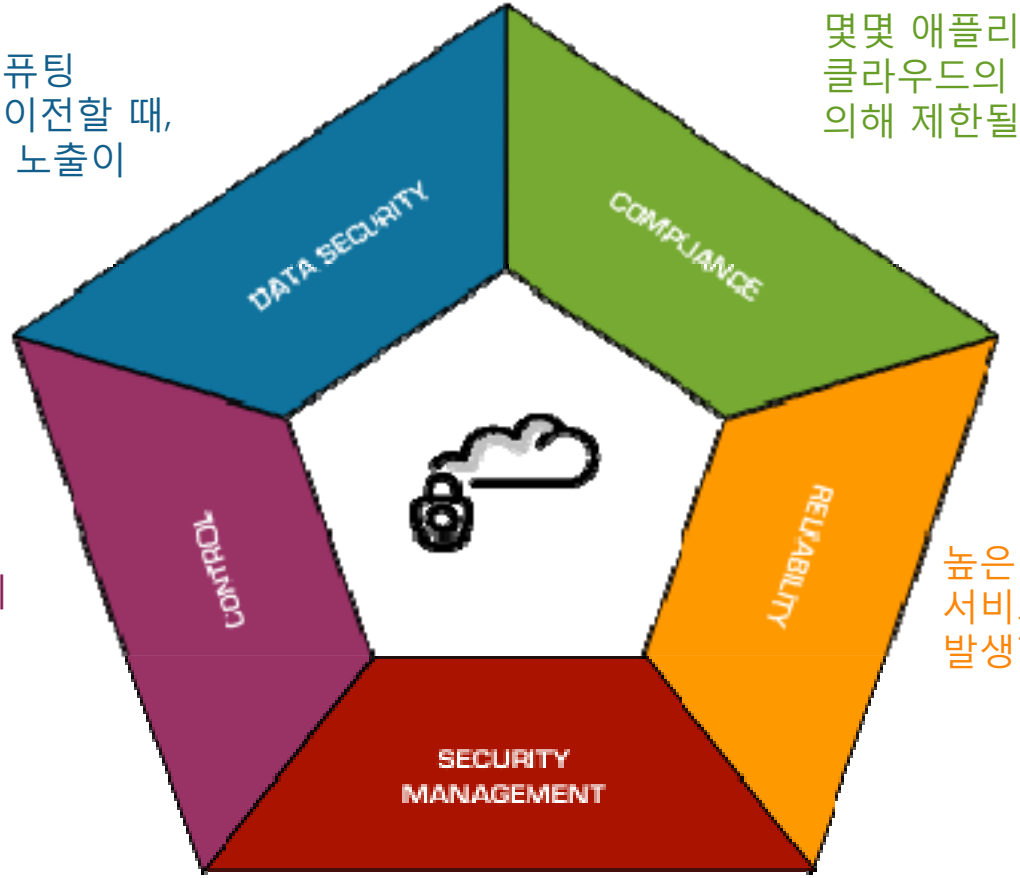
- **보안 기술**
  - 보안은 어렵다. 그러나 기술을 가진 보안 전문가를 찾기란 더더욱 어렵다

© 2011 IBM Corporation

클라우드 컴퓨팅의 위험

공유된 네트워크와 컴퓨팅 인프라에 워크로드를 이전할 때, 잠재적으로 권한 없는 노출이 증가할 수 있다

몇몇 애플리케이션에 대해 클라우드의 사용은 산업 규제에 의해 제한될 수 있다



주된 이슈는 정보가 어디에 저장되고 위치하는지, 누가 접근하고 백업하는지, 어떻게 모니터링되고 비상 대응을 포함하여 관리되고 있는지 등이다

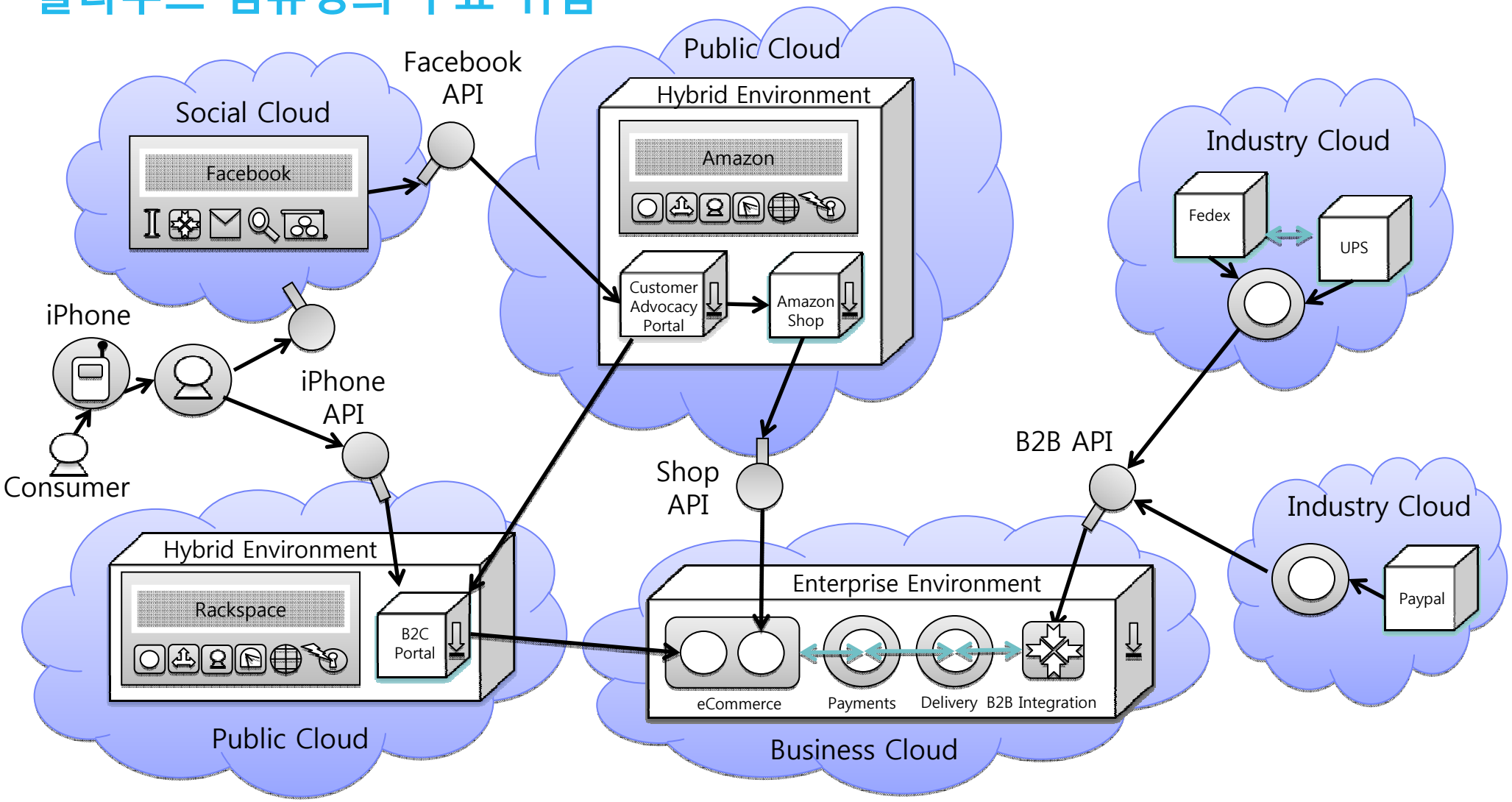
높은 가용성에 대한 관심과 서비스 손실과 사용 불능이 발생할 수 있다

클라우드 내 애플리케이션과 런타임 환경을 위한 방화벽을 관리하고, 보안을 설정하기 위한 통제가 필요하다

Get ready to break free.

© 2011 IBM Corporation

클라우드 컴퓨팅의 주요 위험



Get ready to break free.

© 2011 IBM Corporation

클라우드 보안 위험? 단지 우려만인가?

데일리시큐

인쇄 취소

뉴스
토픽

아마존 AWS 등 클라우드 아키텍쳐 취약점 발견

등록 : 11-11-07 21:59 , 박춘식 서울여자대학교 정보보호학과 교수

[박춘식 교수의 보안이야기] 독일 대학연구팀이 미국 Amazon.com의 클라우드 서비스 Amazon Web Services(AWS)에 시큐리티 결함이 있음을 발견했다고 외신이 보도했다.

이들 취약점은 "많은 클라우드 아키텍처에 존재하고 있으며, 공격자가 관리자 권한을 취득 이용자의 데이터에 접근하는 것을 가능하게 할 우려가 있다"는 견해를 나타냈다.

연구팀은 이들의 시큐리티 결함에 대해서 Amazon AWS부문에 통보했으며 AWS는 이들을 다. 단지 연구팀이 고안, 실증한 이들을 통한 공격 수법은 다른 클라우드 서비스에도 유효했다.

연구팀은 다양한 종류의 XML 시그니처 래핑 공격에 의해서 고객 계정에 대한 관리 접근여 그 고객 계정으로 신규 인스턴스를 작성해 이미지를 추가·삭제할 수 있는 것을 실제 증다.

또한 연구팀은 XSS(Cross Site Scripting) 공격을 오픈소스의 프라이빗 클라우드(Private반 소프트웨어 'Eucalyptus'에 대해서 실행할 수 있다는 것도 실증했다.

Dropbox

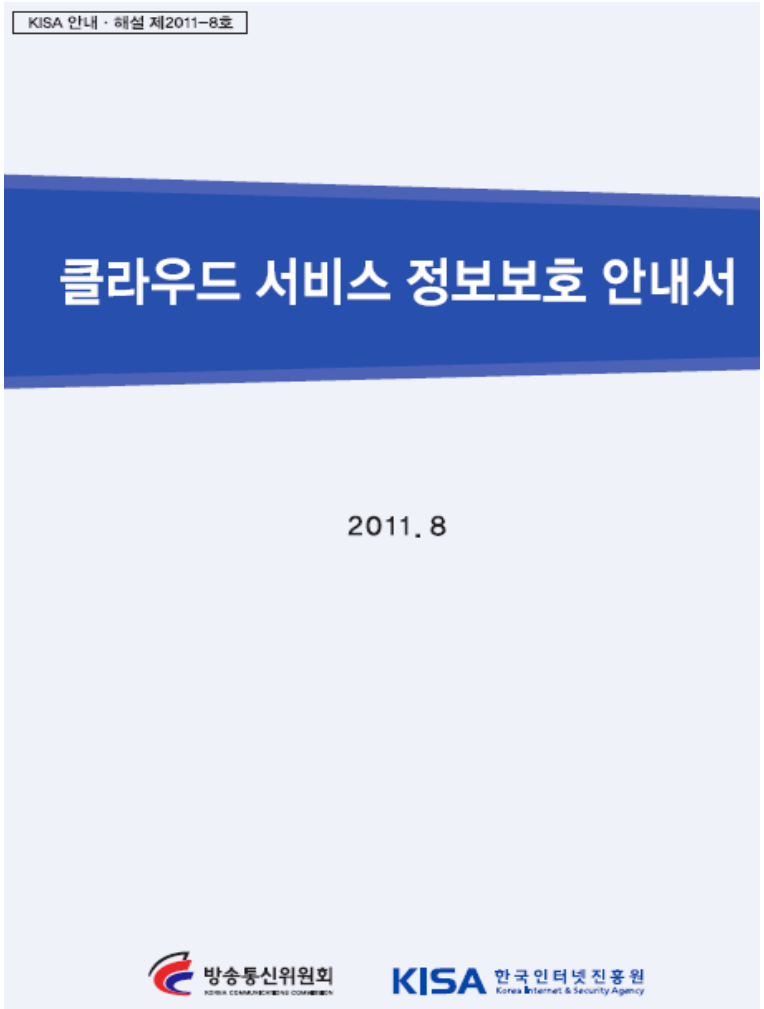
[박춘식 교수의 보안이야기] 지난 8월8일부터 12일까지 미국 샌프란시스코에서 개최된 USENIX Security Symposium에서 미국에서 가장 인기있는 클라우드 스토리지 서비스 Dropbox에 존재하는 취약성이 발표되었다.

이 취약성은 Dropbox에 의해 논문 발표 이전에 이미 수정 조치 되었다. 오스트리아 SBA Research 연구자들이 발표한 "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space" 논문에 의하면, Dropbox의 클라이언트 소프트 및 데이터 송수신 프로토콜에는 결함이 있어 정상적인 이용자가 Dropbox에 보존된 파일에 대해서 불법으로 접근하는 방법이 3가지 존재한다고 주장했다.

Get ready to break free.

© 2011 IBM Corporation

클라우드 서비스 관련 보안 가이드라인



[클라우드 서비스 정보보호 안내서 http://www.securityplus.or.kr/xe/?document_srl=3149996](http://www.securityplus.or.kr/xe/?document_srl=3149996)

[클라우드 SLA 가이드 및 개인정보 보호 수칙 http://www.securityplus.or.kr/xe/?document_srl=3239097](http://www.securityplus.or.kr/xe/?document_srl=3239097)

[Defined Categories of Service 2011 http://www.securityplus.or.kr/xe/?document_srl=3219939](http://www.securityplus.or.kr/xe/?document_srl=3219939)

[[NIST]Guidelines on Security and Privacy in Public Cloud Computing http://www.securityplus.or.kr/xe/?document_srl=43123](http://www.securityplus.or.kr/xe/?document_srl=43123)

Get ready to break free.

© 2011 IBM Corporation

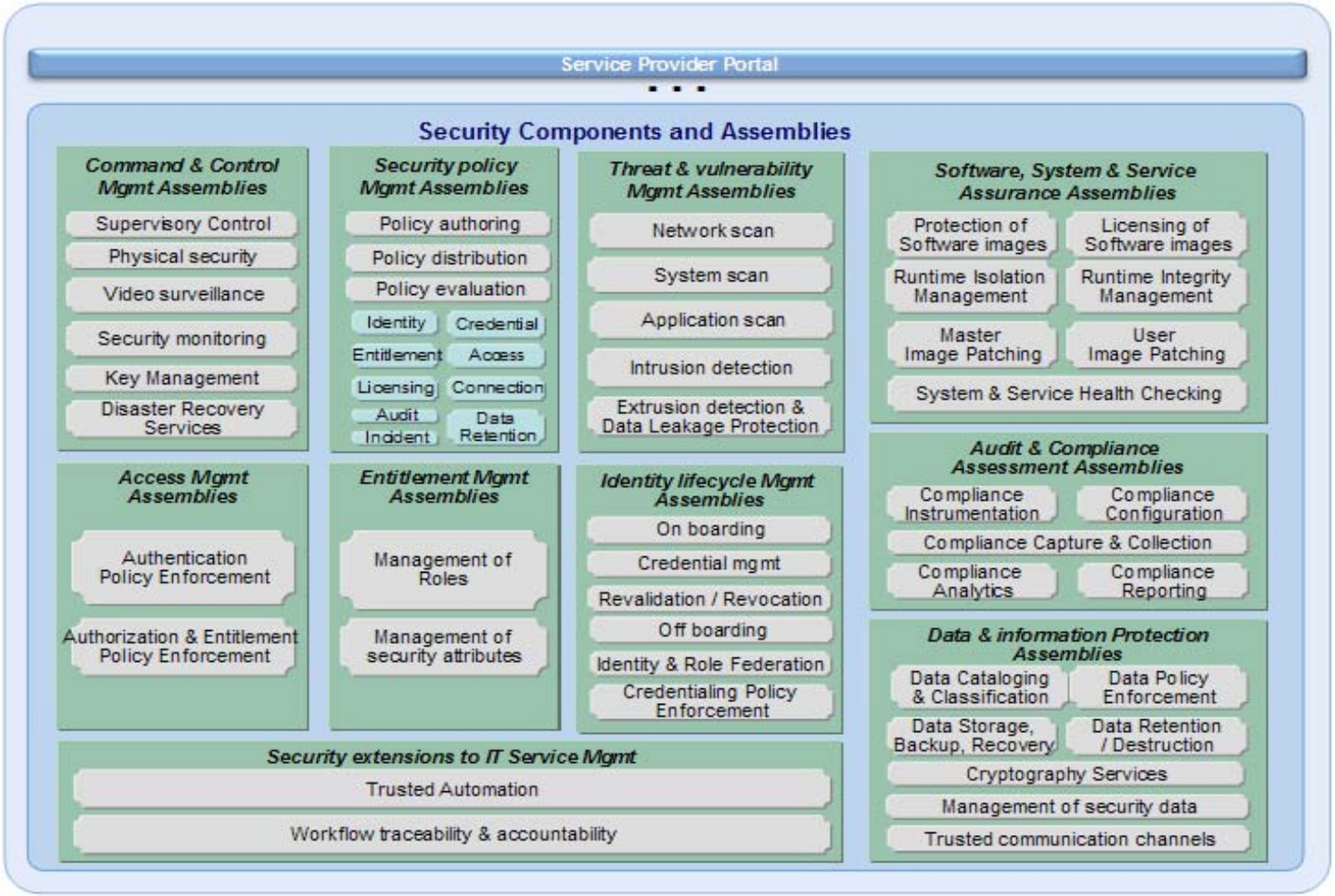
IBM의 클라우드 컴퓨팅 보안 아키텍처 원칙

One Size Does not Fit All!

Get ready to break free.

© 2011 IBM Corporation

IBM 클라우드 컴퓨팅 보안 참조 아키텍처

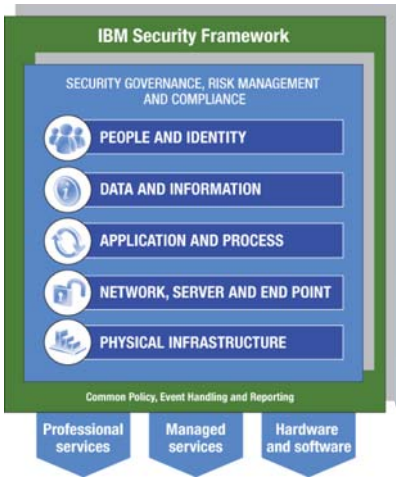


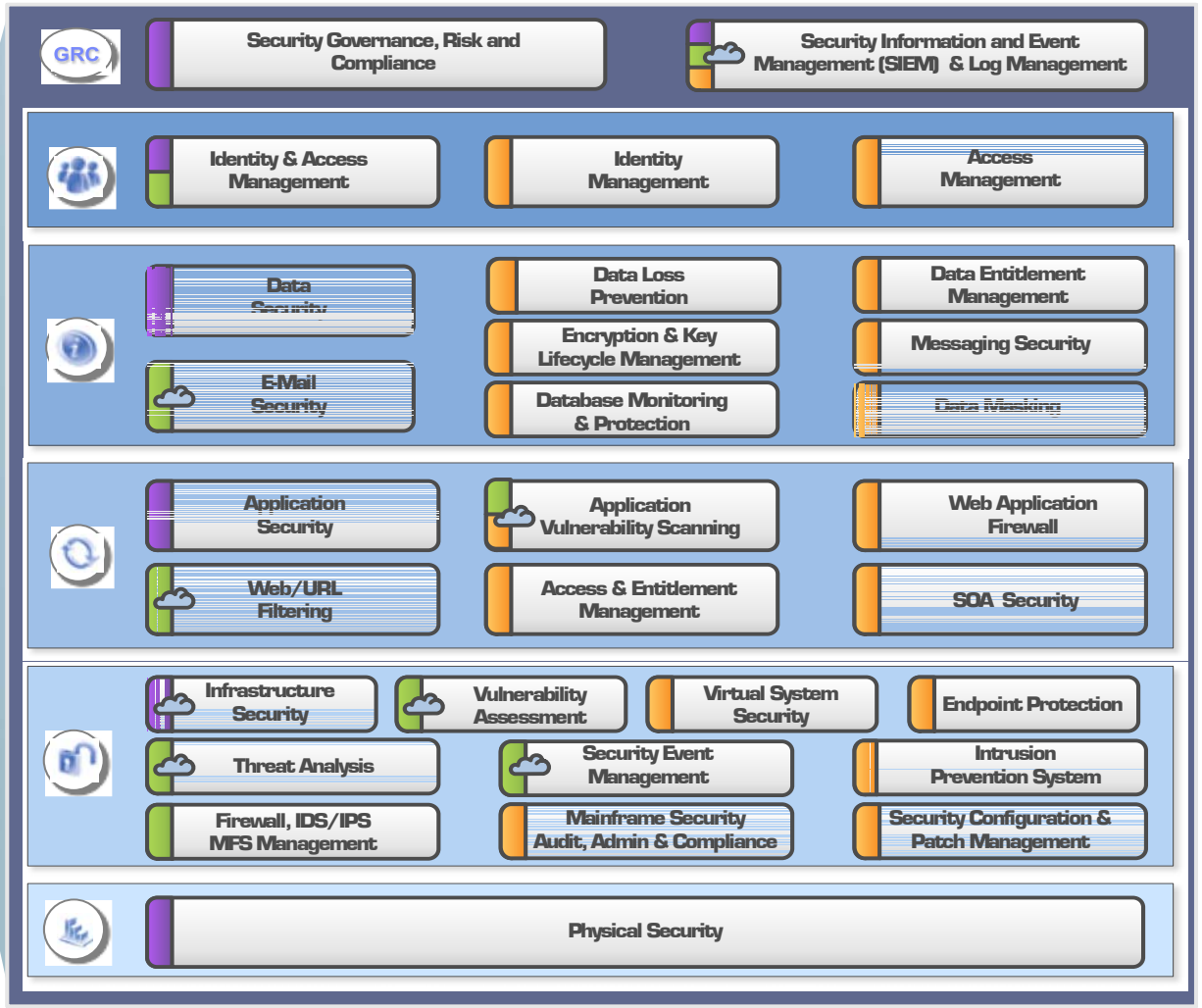
Get ready to break free.

© 2011 IBM Corporation

클라우드를 위한 IBM 보안 솔루션 포트폴리오

- Professional Services
- Managed Services
- Products
- Cloud Delivered



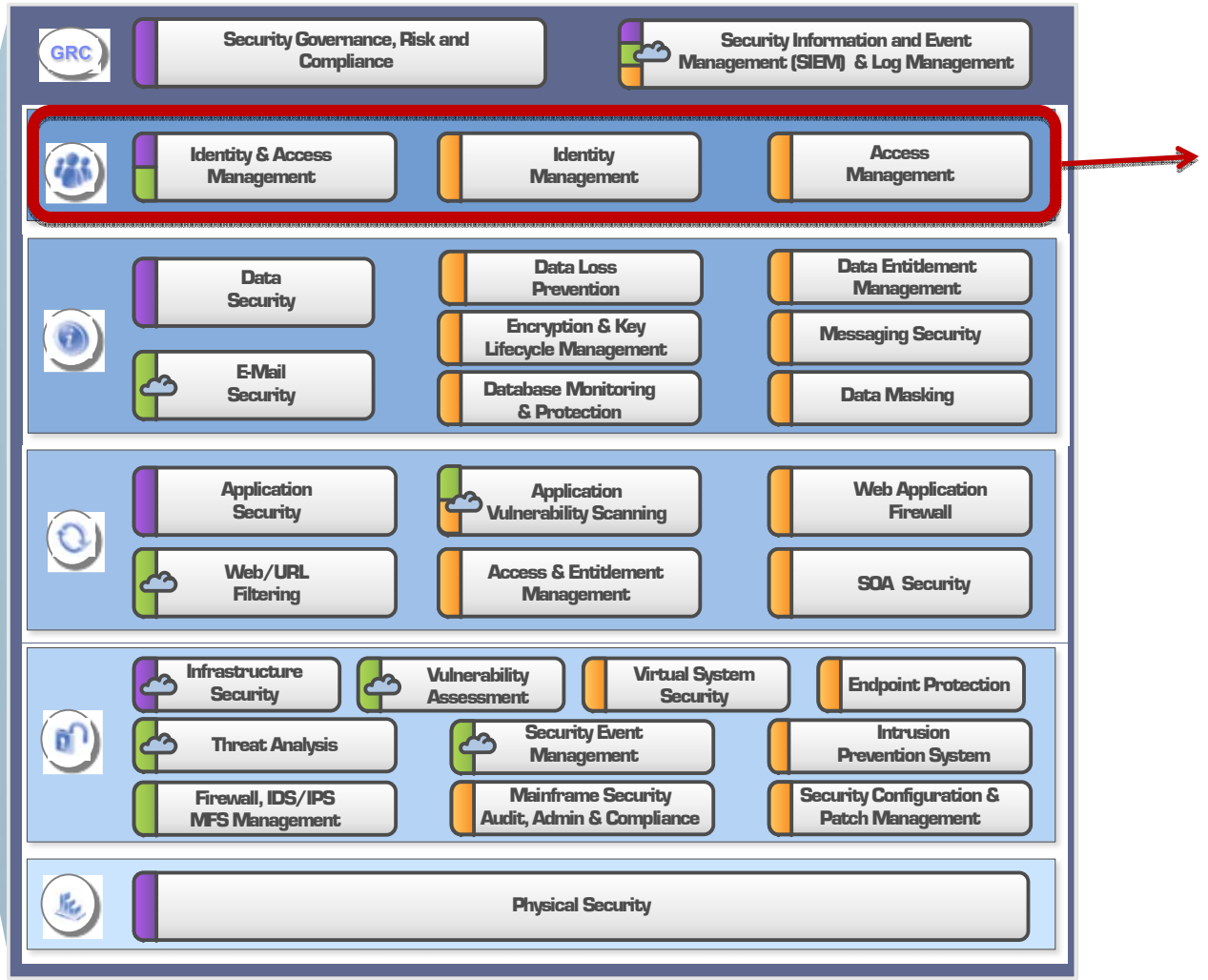


Get ready to break free.

© 2011 IBM Corporation

클라우드를 위한 IBM 보안 솔루션 포트폴리오

- Professional Services
- Managed Services
- Products
- Cloud Delivered

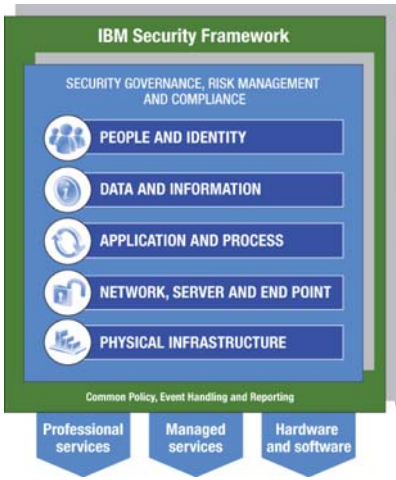


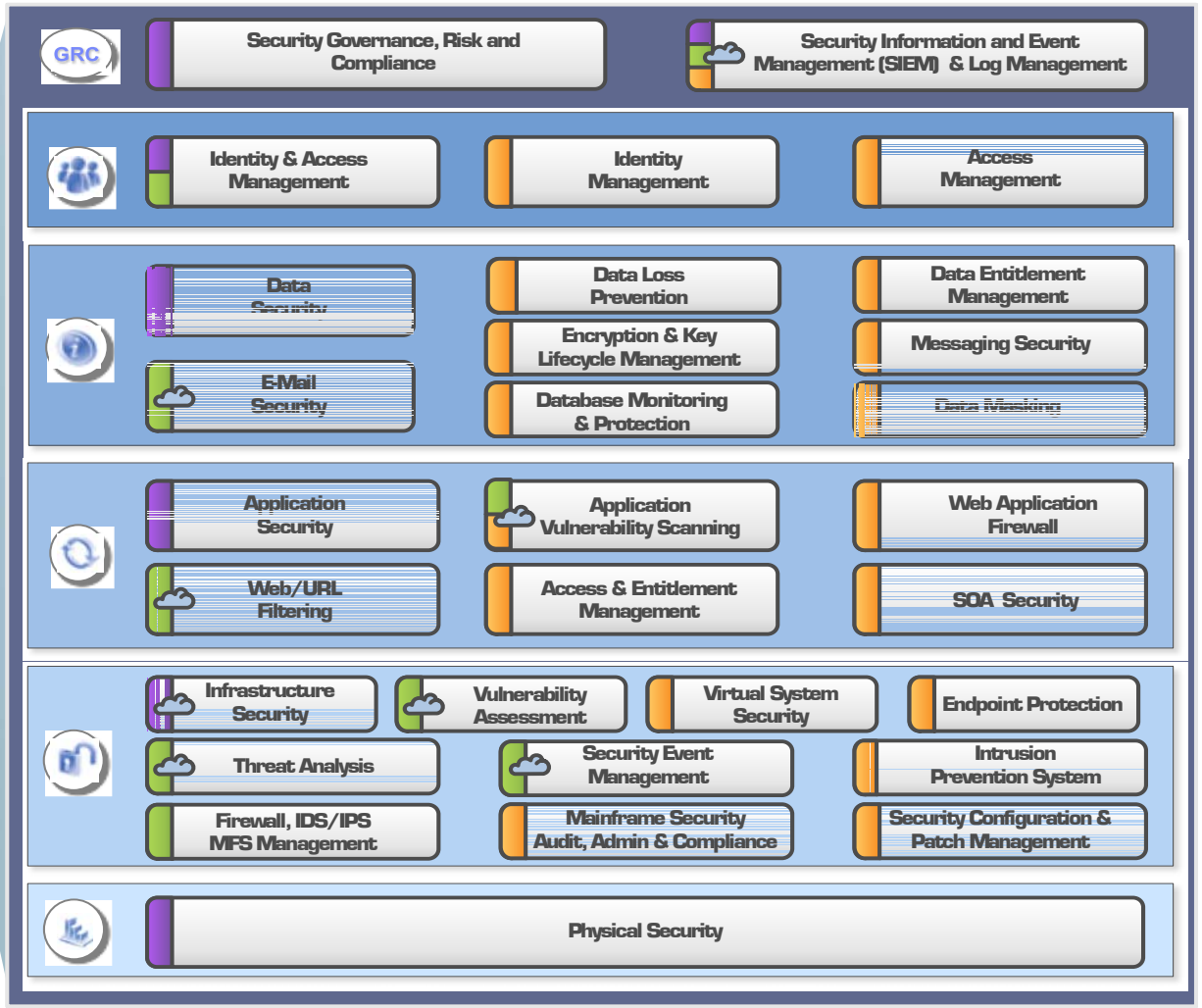
Get ready to break free.

© 2011 IBM Corporation

클라우드를 위한 IBM 보안 솔루션 포트폴리오

- Professional Services
- Managed Services
- Products
- Cloud Delivered



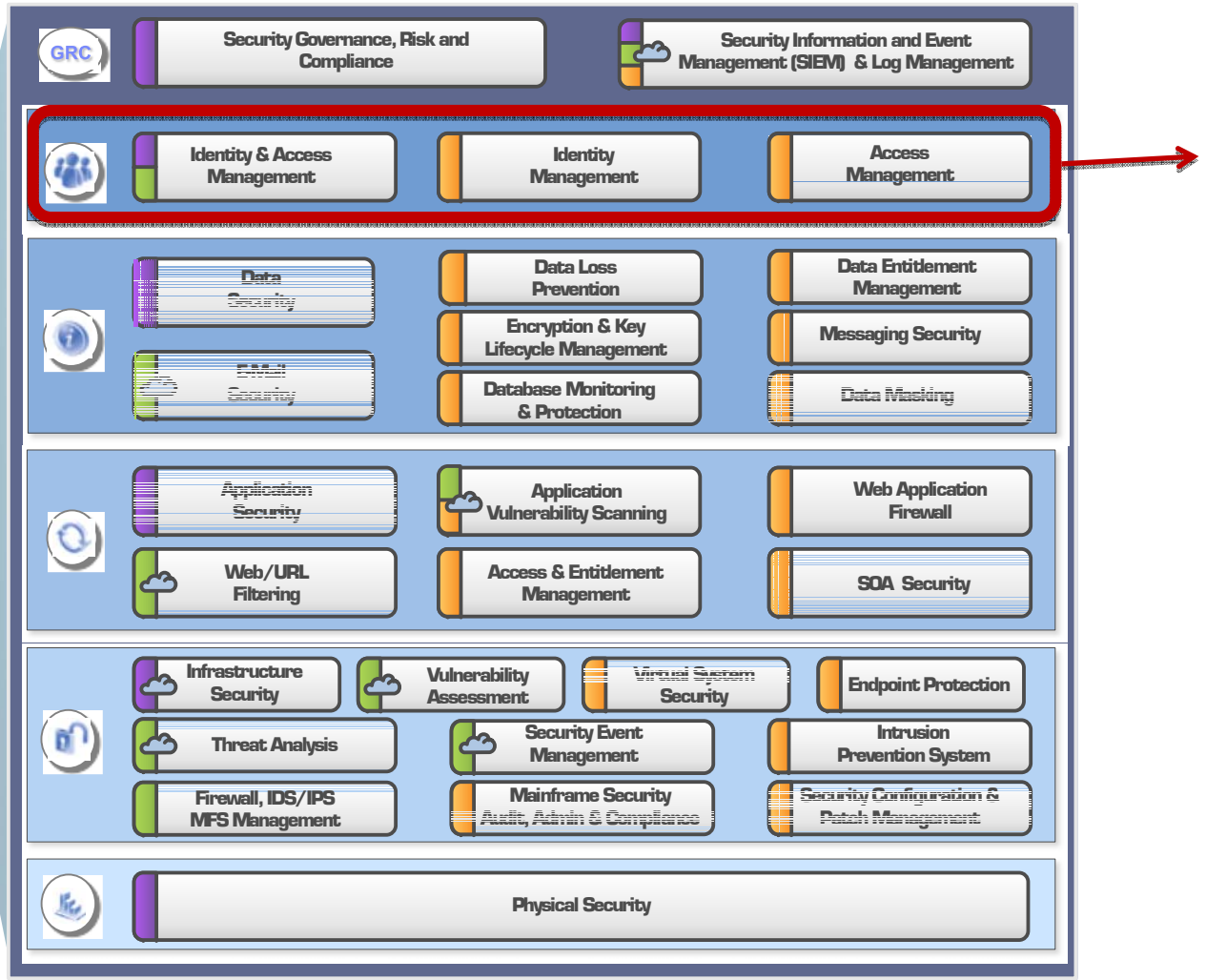


Get ready to break free.

© 2011 IBM Corporation

클라우드를 위한 IBM 보안 솔루션 포트폴리오

- Professional Services
- Managed Services
- Products
- Cloud Delivered



Get ready to break free.

© 2011 IBM Corporation

Identity and Access Management as a Services

Lighthouse Gateway™
Identity and Access Management in the Cloud

Identity Management

- User Provisioning
- Identity Lifecycle Automation
- User Self-Service
- Role Governance & Compliance
- and more...

Web Access Management

- Web Single Sign-on
- Centralized Access Control Policy
- Two-Factor Authentication
- and more...

Federated Identity & Access Management

- SSO for SaaS Applications
- Business-to-Business Federation
- and more...

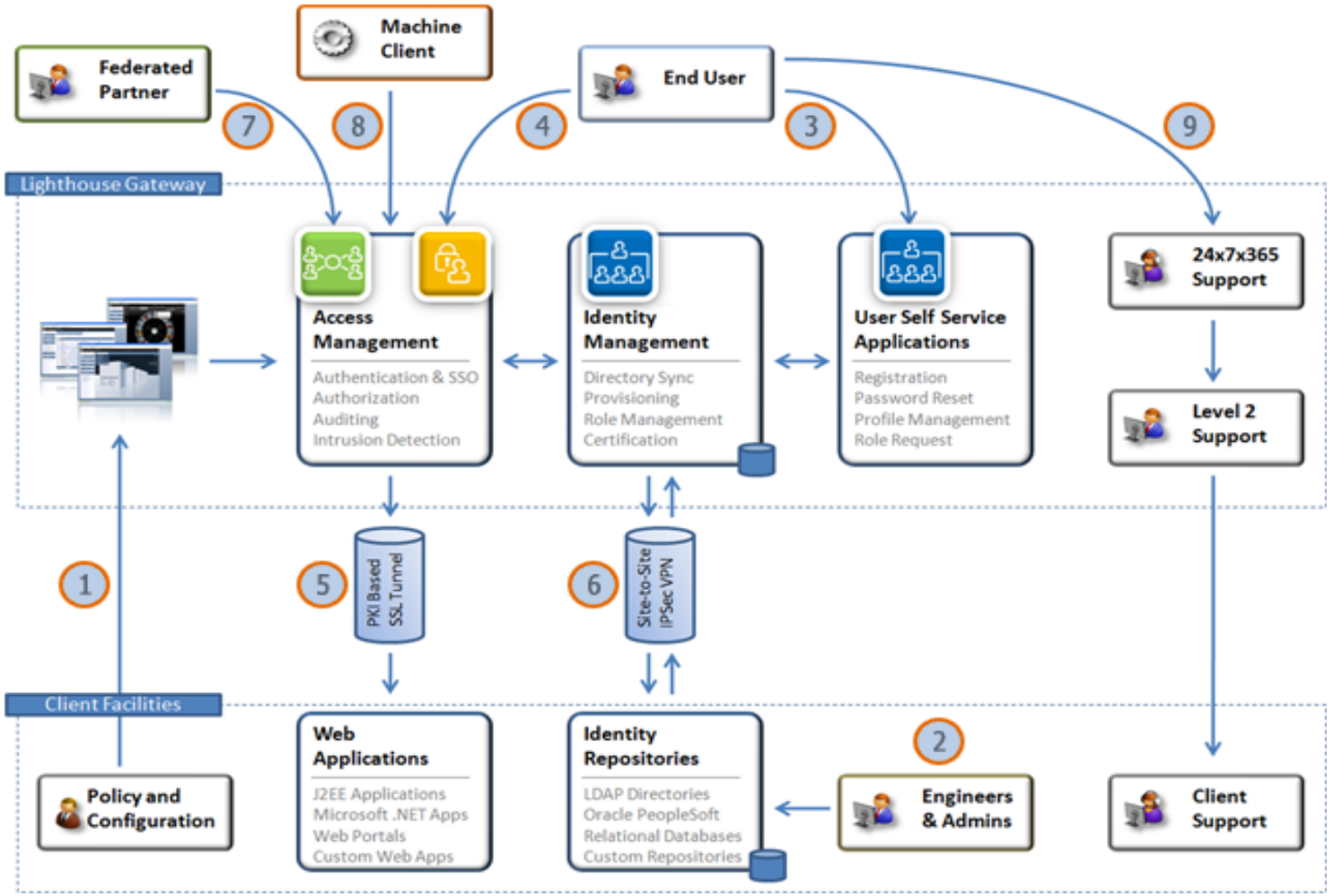
Get ready to **break free.**

© 2011 IBM Corporation

Identity and Access Management as a Services

Lighthouse Gateway™
Identity and Access Management in the Cloud

IBM Tivoli software



Get ready to break free.

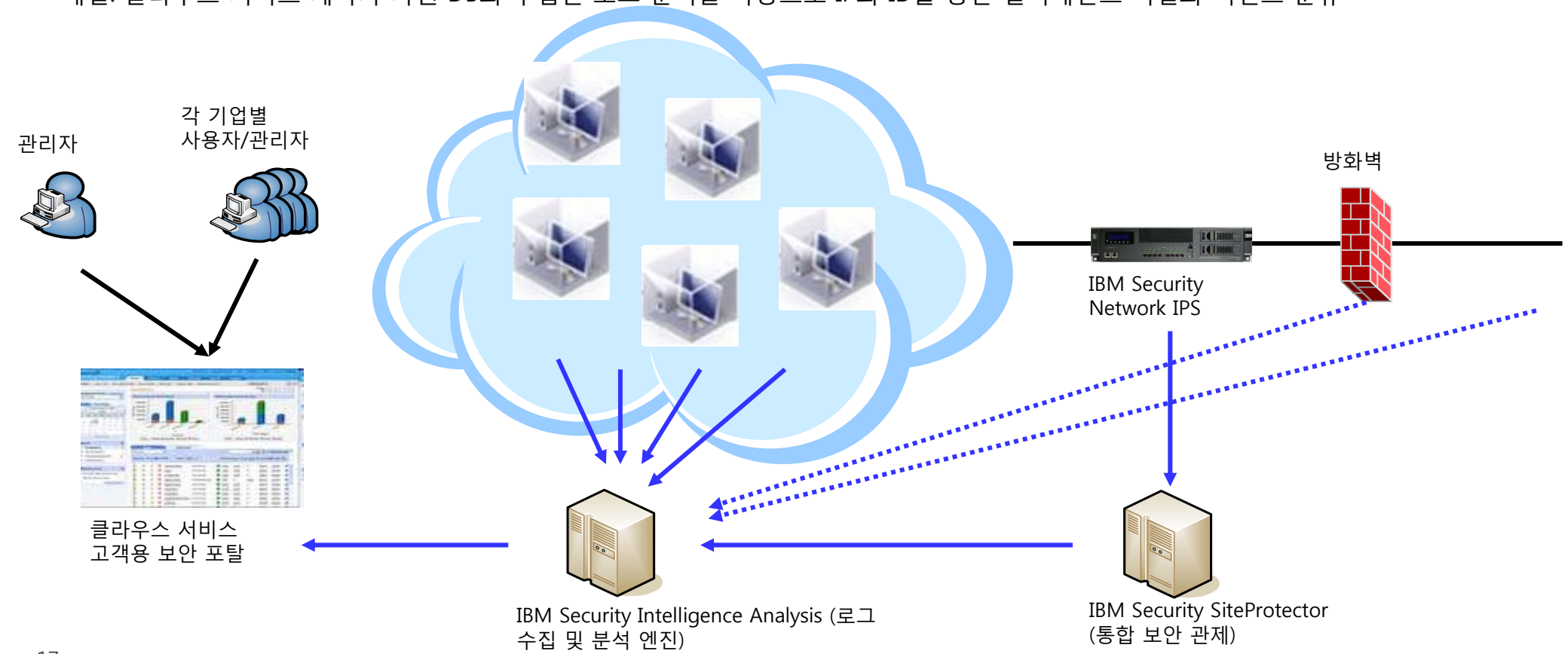
© 2011 IBM Corporation

Case Study: IBM Cloud Security Real Story

비즈니스 요구사항: 클라우드 환경 하에서 보안이 잘 이뤄지고 있음을 보여줄 수 있어야 한다

기술적 이슈: 각 클라우드 서비스 사용자 및 관리자, 즉 멀티테넌트들에 대한 식별과 그에 따른 이벤트 분류

해결: 클라우드 서비스 계약자 자원 DB와 수집된 로그 분석을 바탕으로 IP와 ID를 통한 멀티테넌트 식별과 이벤트 분류



Get ready to break free.

© 2011 IBM Corporation

Case Study: IBM Cloud Security Real Story

SAML 웹서비스 인증 센터

IBM Tivoli Federated Identity Manager &
IBM Tivoli Identity Manger

각 기업별
사용자/관리자

관리자

클라우스 서비스
고객용 보안 포탈

IBM Security Intelligence Analysis (로그 수집 및 분석 엔진)

VPN

방화벽

IBM Security Network IPS

IBM Security SiteProtector (통합 보안 관제)

비즈니스 요구사항: 클라우드 환경 하에서 대내외(구글, 세일즈포스닷컴 등) 각 서비스 별 인증의 문제가 없어야 하며, 사용자와 서비스 간 안전한 채널 확보가 필요하다.

해결: 웹서비스 인증 기반 SAML 인증 서비스 센터와 VPN(Site to Site) 구축

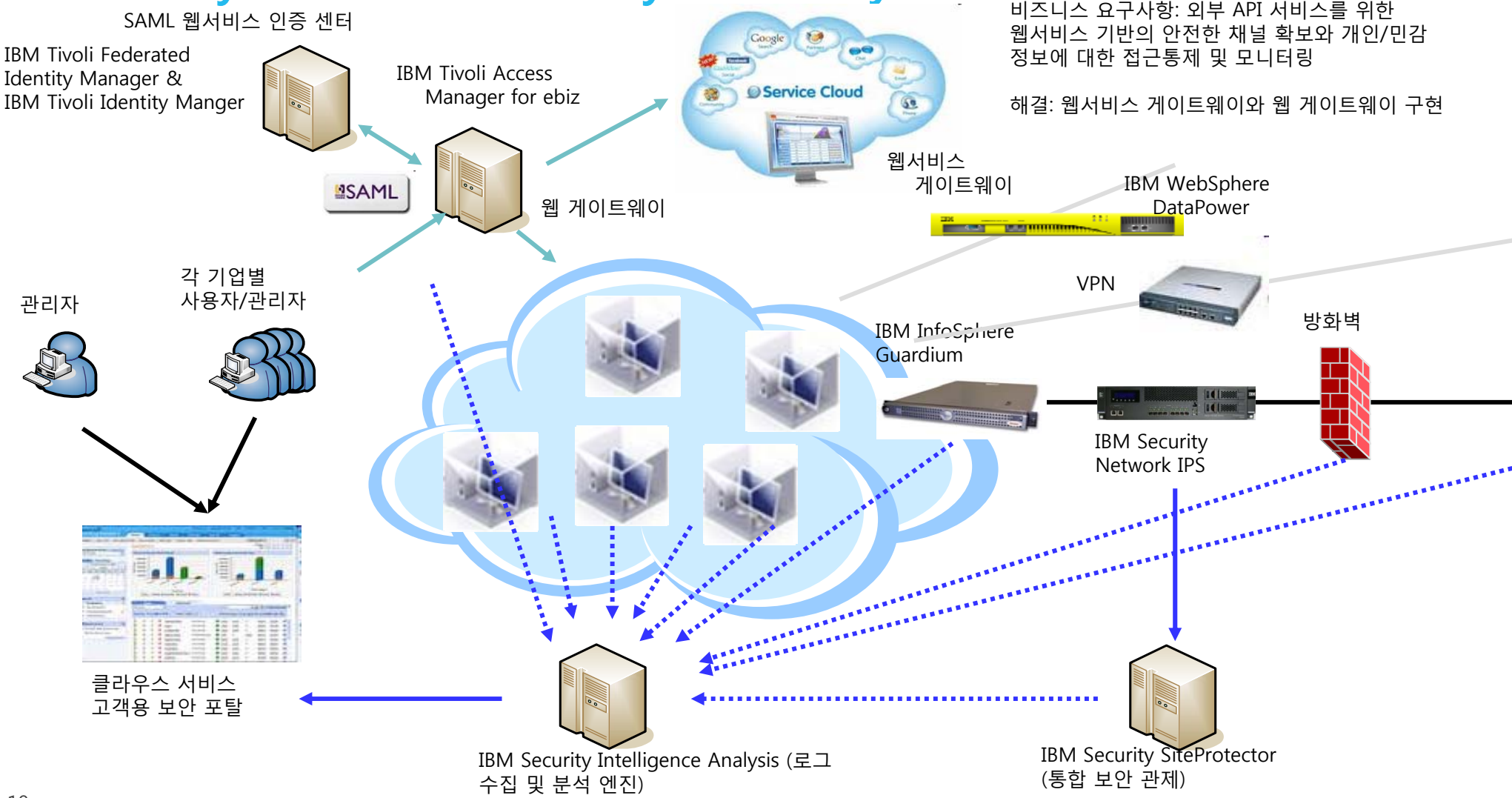
Get ready to break free.

© 2011 IBM Corporation

Case Study: IBM Cloud Security Real Story

비즈니스 요구사항: 외부 API 서비스를 위한 웹서비스 기반의 안전한 채널 확보와 개인/민감 정보에 대한 접근통제 및 모니터링

해결: 웹서비스 게이트웨이와 웹 게이트웨이 구현



Get ready to break free.

© 2011 IBM Corporation

Case Study: IBM Cloud Security Real Story

SAML 웹서비스 인증 센터

IBM Tivoli Federated Identity Manager & IBM Tivoli Identity Manger

IBM Tivoli Access Manager for ebiz

SAML

웹 게이트웨이

Service Cloud

웹서비스 게이트웨이

IBM WebSphere DataPower

비즈니스 요구사항: 개스트 OS의 보안성 및 통합 보안 관제 고도화
해결: 호스트 침입 탐지 및 가상화 보안 전문 솔루션 배치. 지능형 보안 분석 범위 확대.

관리자

각 기업별 사용자/관리자

IBM Security (Virtual) Server Protection

VPN

IBM InfoSphere Guardium

방화벽

IBM Security Network IPS

클라우스 서비스 고객용 보안 포탈

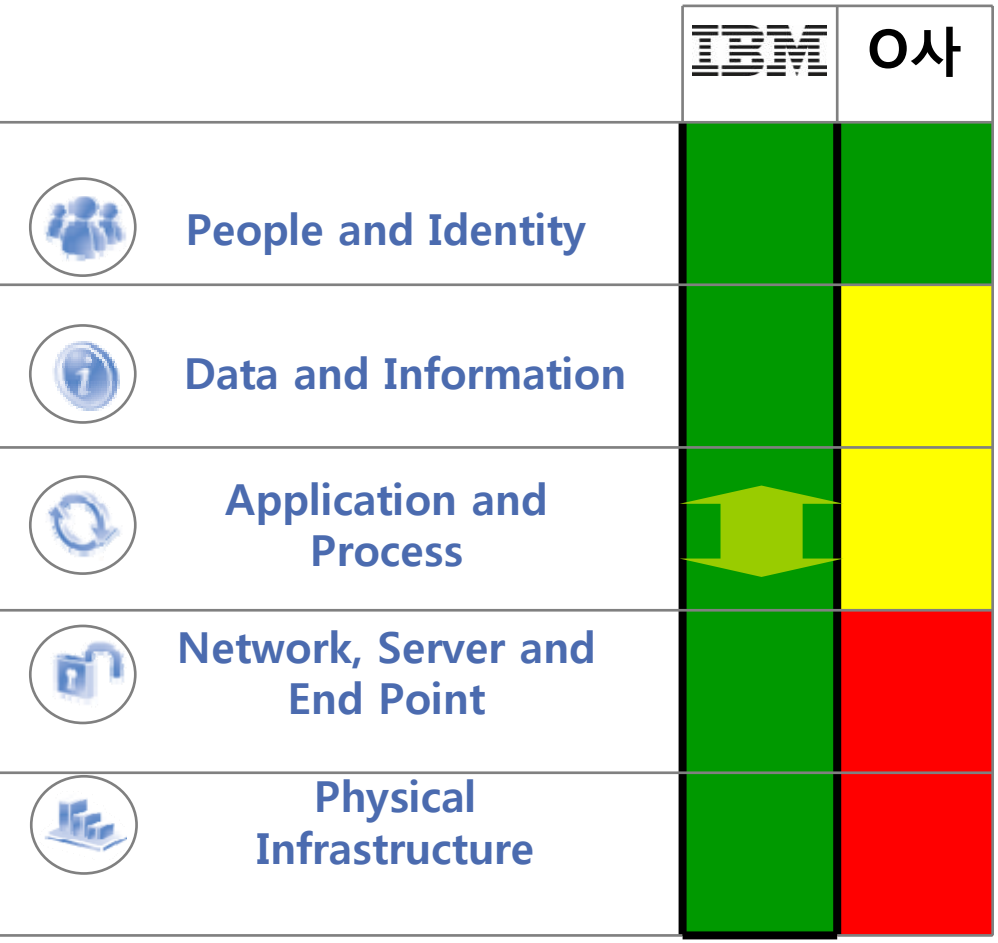
IBM Security Intelligence Analysis (로그 수집 및 분석 엔진)

IBM Security SiteProtector (통합 보안 관제)

Get ready to break free.

© 2011 IBM Corporation

Cloud Security에 대한 타사 대비 IBM의 가치



SC MAGAZINE AWARDS 2010 WINNER Honored in the U.S.

IBM Best Security Company

가트너, 세계 보안 소프트웨어 시장 점유율(2009년~2010년)

(단위 : 백만 달러)

회사명	2010 매출	2010 시장 점유율(%)	2009 매출	2009-2010 성장률(%)
시만텍	3,121.6	18.9	2,949.5	5.8
맥아피	1,711.8	10.4	1,595.6	7.3
트렌드 마이크로	1,036.9	6.3	981.4	5.7
IBM	**814.7**	**4.9**	**759.6**	**7.3**
EMC	626.6	3.8	498.8	25.6
기타	9,188.8	55.7	7,928.6	15.9
Total	**16,500.4**	**100.0**	**14,713.5**	**12.0**

Get ready to break free.

© 2011 IBM Corporation

클라우드 보안에 대해 고민하고 있다면,
비즈니스와 IT, 그리고 클라우드 컴퓨팅에 대한 깊은 이해를 갖고 있는
보안 전문 회사인 IBM과 지금 바로 상담하시기 바랍니다!

Get ready to break free.

© 2011 IBM Corporation

감사합니다!

Get ready to break free.

© 2011 IBM Corporation