클라우드 환경에 따른 보안 기술의 변화

- 오픈소스를 중심으로 -

김호중 부장
한국 레드햇

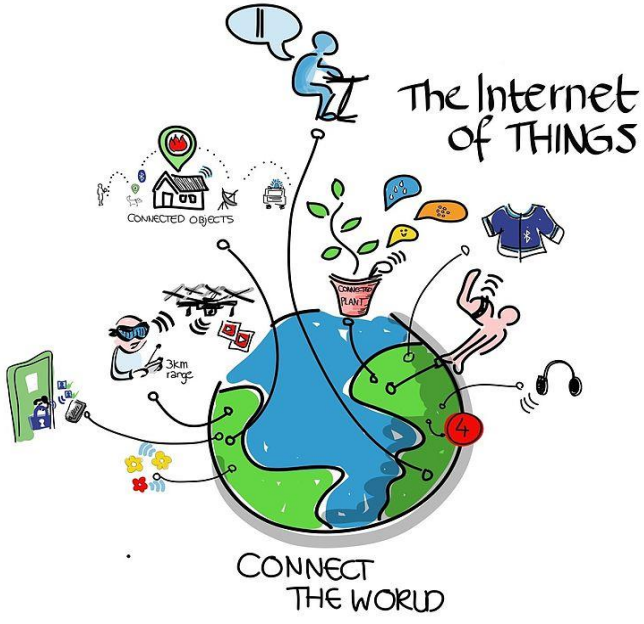

redhat.
IT트렌드
클라우드 컴퓨팅의 개념
클라우드 컴퓨팅 보안
레드햇 보안 정책
공개SW포털
OPEN SOURCE SOFTWARE

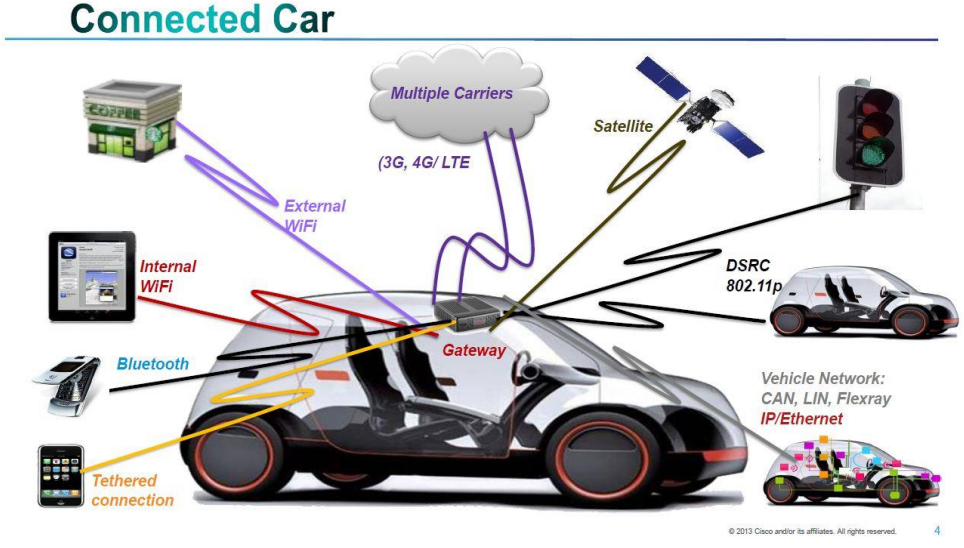
개방적인 소통과 협업의 창구로서의 SNS

사물인터넷(IoT/IoE)

- **애플워치, 갤럭시 기어 등 웨어러블 디바이스 컴퓨팅**
- **헬스케어, 화상진료 등** M2M**기술의 발전**
- **스마트자동차**(Connected Car), 무인자동차, 전기 자동차
- 2015 : 49**억개**, 2020 : 250**억개 연결 예상(가트너)**

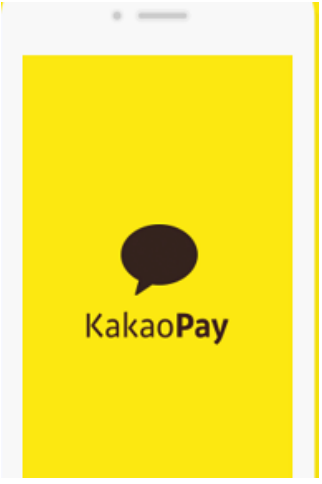
WATCH

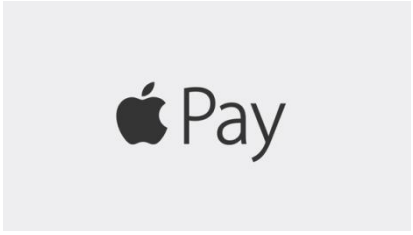




O2O(Online to Offline) 서비스

- 카카오택시 / 배달의 민족 / 얍(쿠폰+비콘)
- 핀테크(Finance + Technology)
- 스마트폰 또는 인터넷 간편결재 서비스
- 인터넷은행, 외환송금, 크라우디드펀딩, 비트코인, 자산운용, P2P 대출 등
- 카카오페이, 네이버페이, 알리페이, 페이팔 등



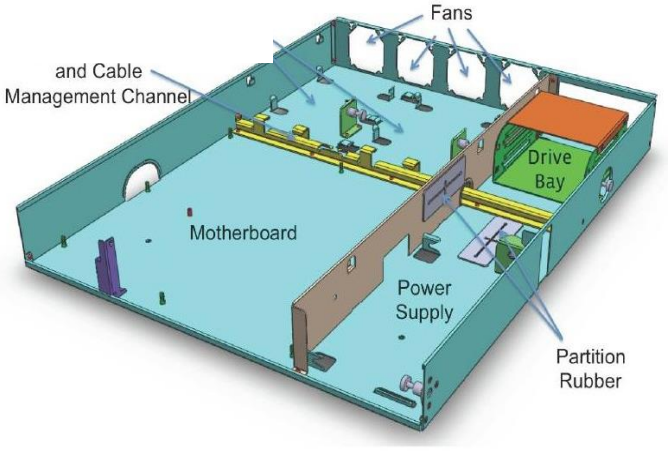


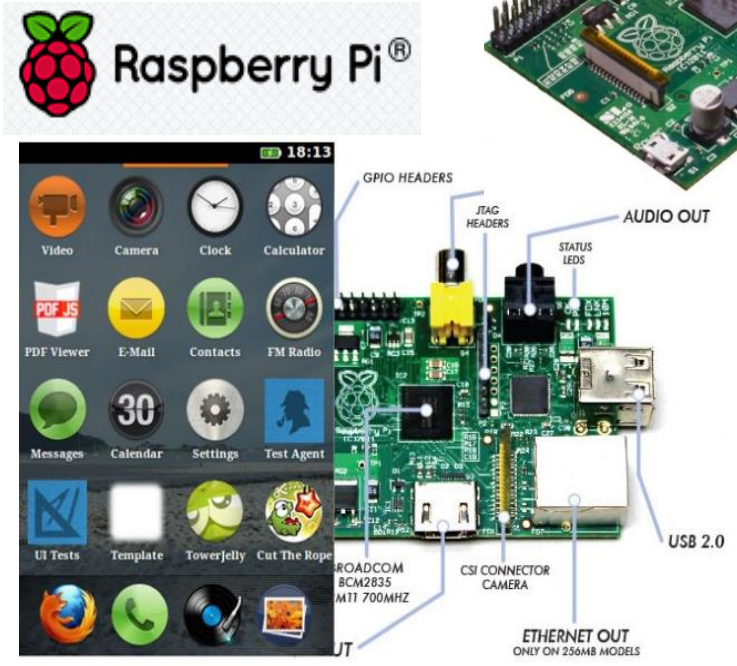
드론(Dron) & 로봇(Robot)

- 드론(DRON) : 무인항공기(UAV), 배송수단(아마존), 촬영, 취미생활 등
- 민간드론 시장 - 2015 : 2000억, 2023 : 2조2천억 예상
- 로봇 : 청소용, 산업용, 축구로봇 등

오픈 하드웨어

- 오픈컴퓨트 프로젝트 (opencompute.org) : Facebook 주도의 하드웨어 아키텍쳐 오픈
- 라즈베리 파이(raspberrypi.org) : 교육용 보드
- 아두이누(Arduino) : 마이크로 컨트롤러 내장 제어용 기판





데이터 누적량

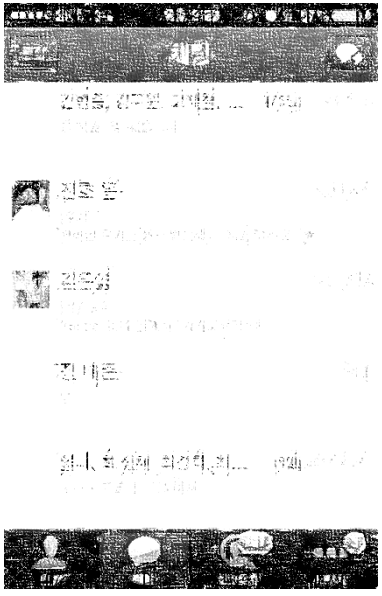
1분

2억 개의 이메일이 발송

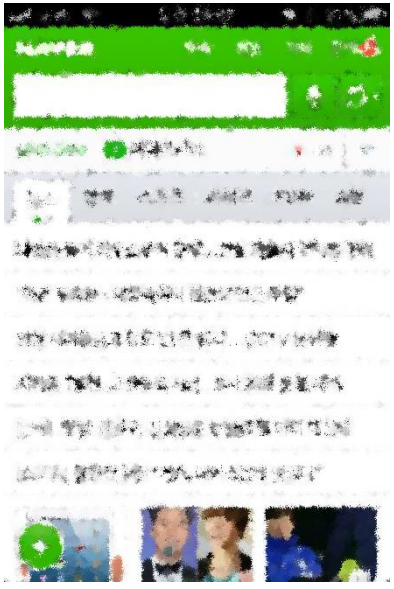
10만개의 트윗 메시지

293,000개의 상태 업데이트
20G 이상의 로그 데이터

1일



일 10억건 발송
즉, 초당 11,574건 메시지



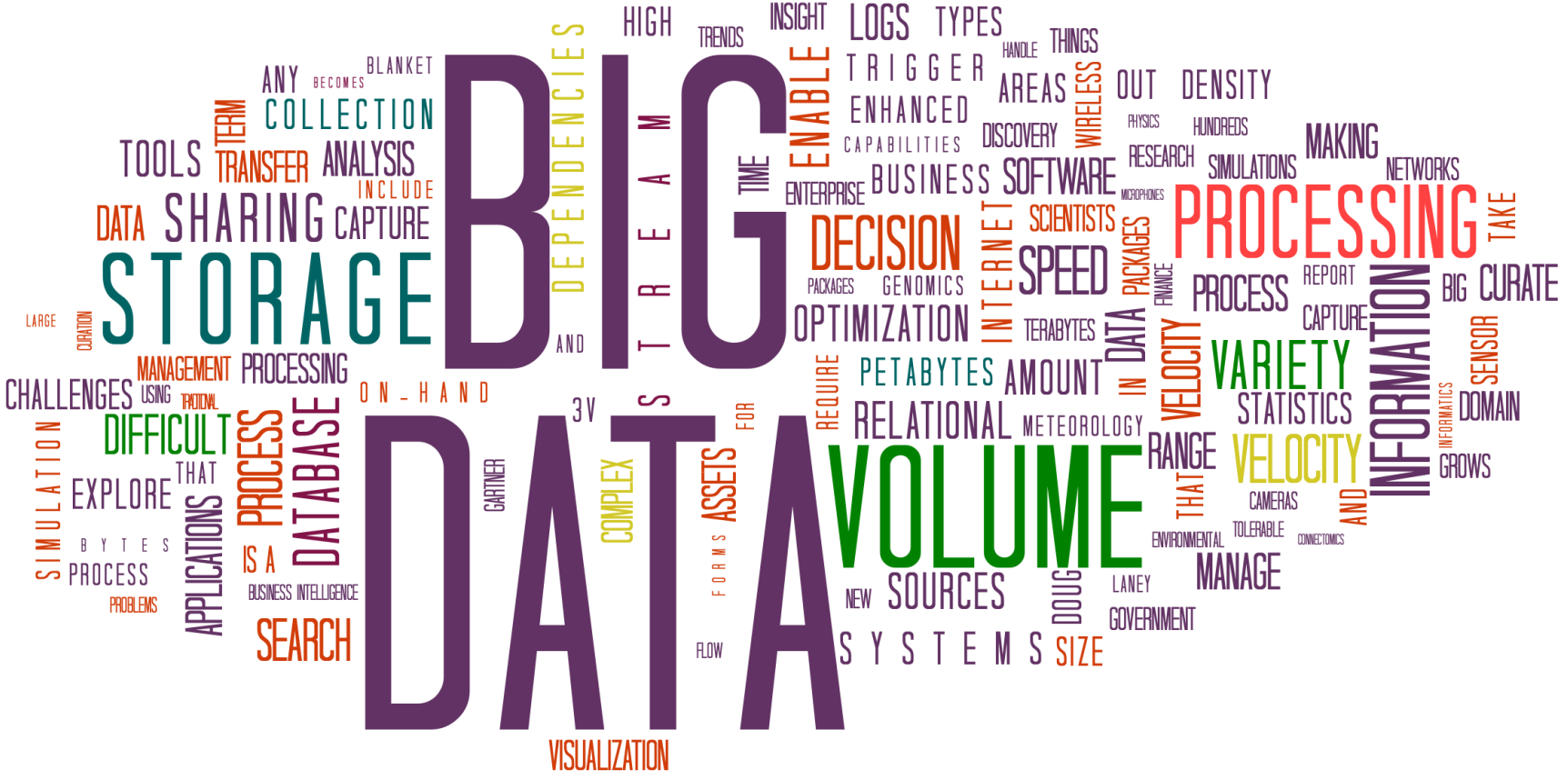
일 12억 페이지 뷰,
일 1.3억 건 검색,
3 테라 바이트 Log

일 3억개의 이미지 업로드,
일 5억개의 콘텐츠 공유

일 26억 건 검색 (글로벌)

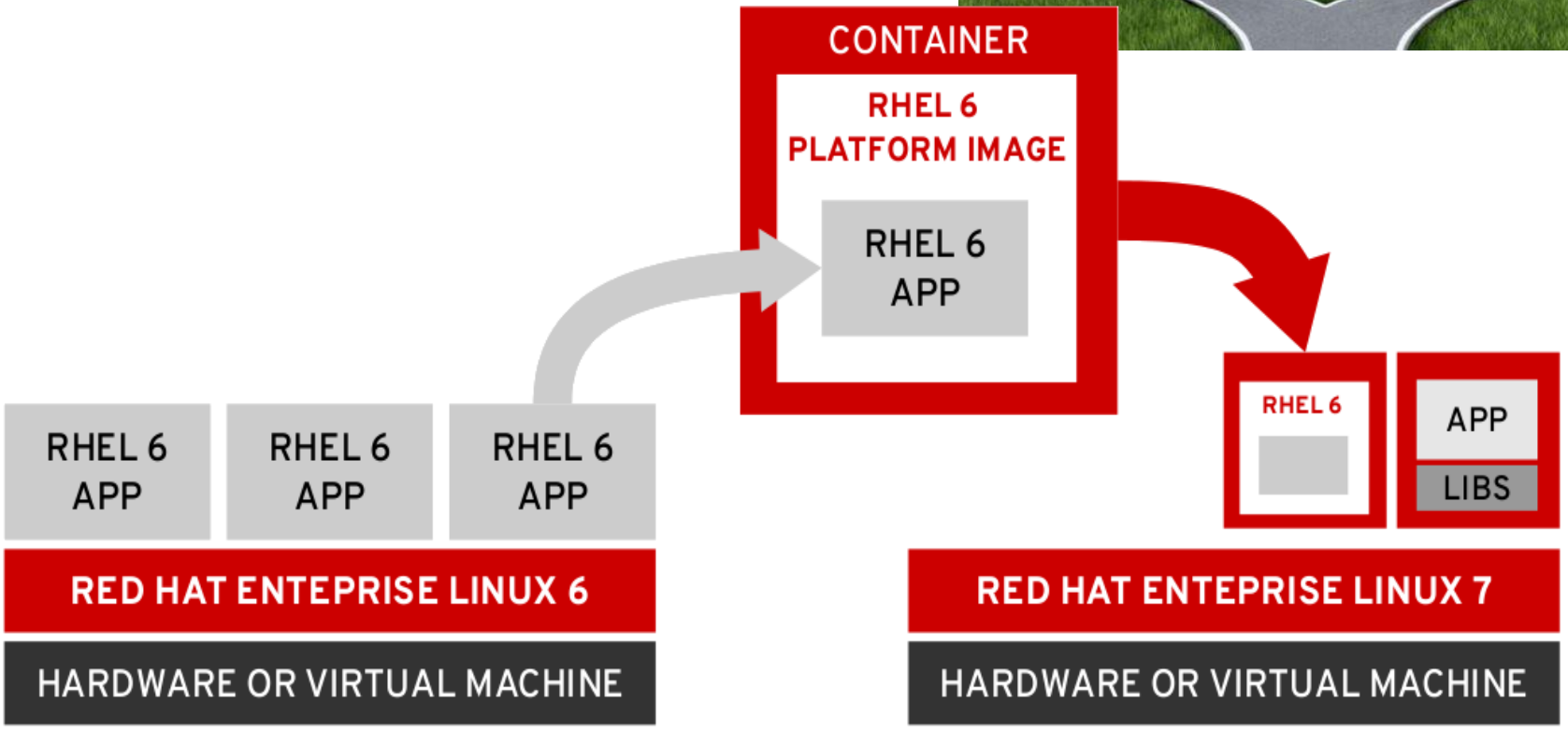
빅데이터

- **매년 50%이상의 데이터 증가율(모바일 매년 78%성장)**
- **데이터 생성, 수집, 분석 기술의 고도화 요구**
- 3V(Volume, Velocity, Variety)

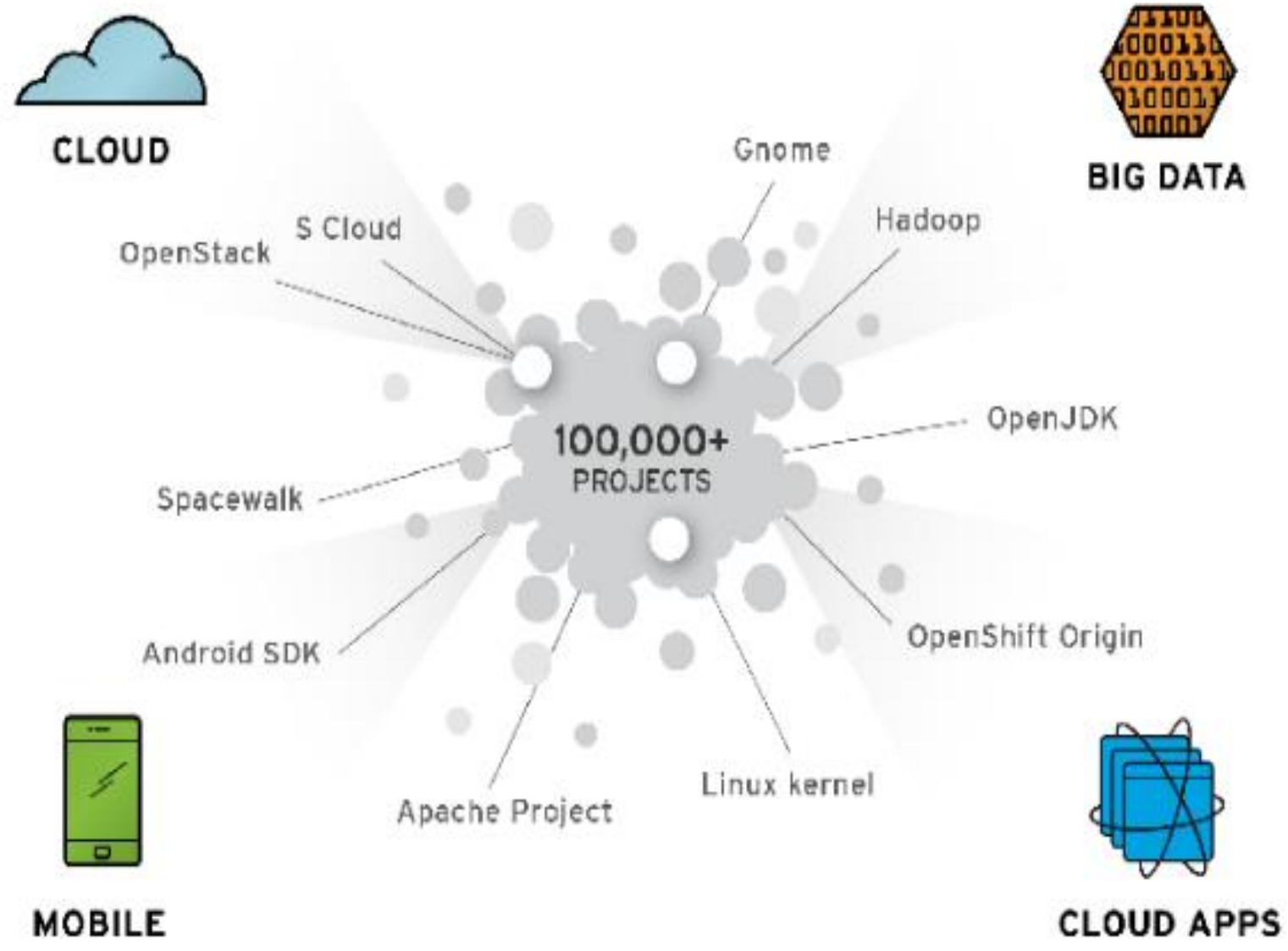


SW중심의 IT

- From Hardware to Software
- From Scale-up to Scale-out
- Container 기술(Docker) 등장
- Micro-Service Architecture 등



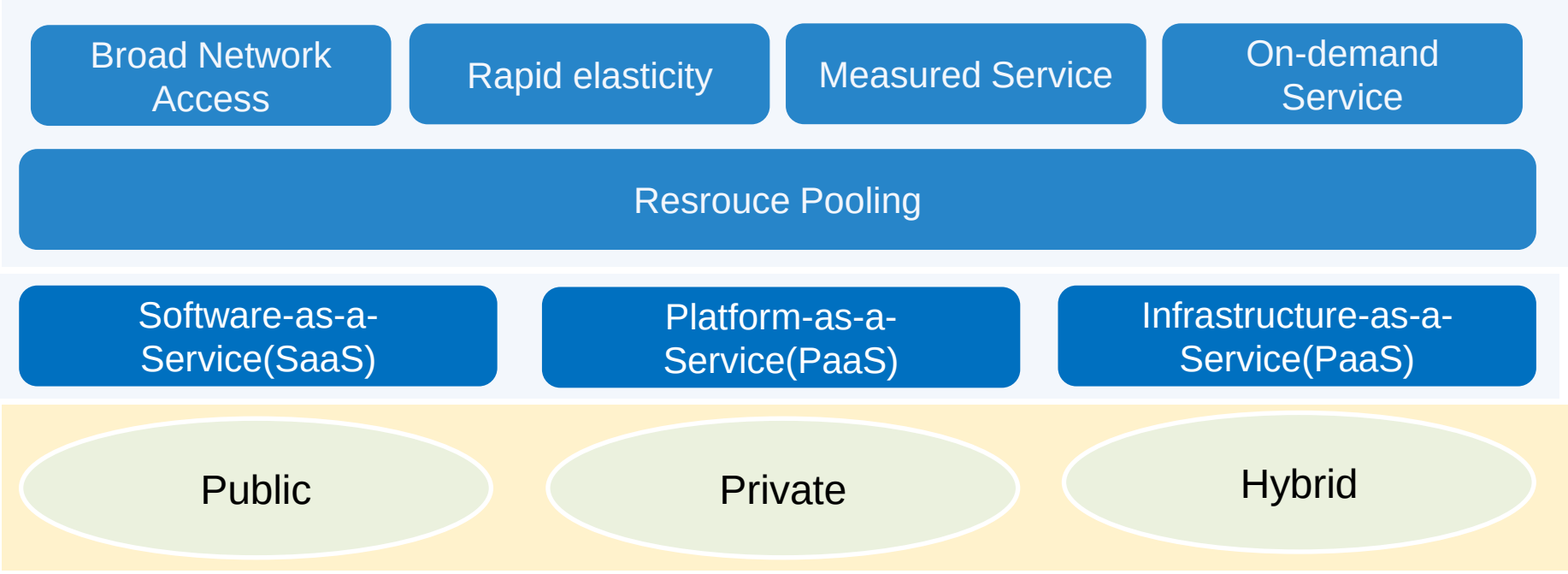
미래를 만드는 오픈 혁신


CLOUD
BIG DATA
Gnome
S Cloud
OpenStack
Hadoop
OpenJDK
100,000+
PROJECTS
Spacewalk
Android SDK
OpenShift Origin
Apache Project
Linux kernel
MOBILE
CLOUD APPS


redhat.
IT트렌드
클라우드 컴퓨팅
클라우드 컴퓨팅 보안
레드햇 보안 정책
공개SW포털
OPEN SOURCE SOFTWARE

클라우드 컴퓨팅

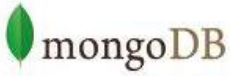
- 애플리케이션 자동 확장 구조의 아키텍처 기반
- Public, Private, Hybrid 클라우드 컴퓨팅
- IaaS-PaaS-SaaS 형태의 클라우드 컴퓨팅 기술
- Google, Amazon, Red Hat, Salesforce 등



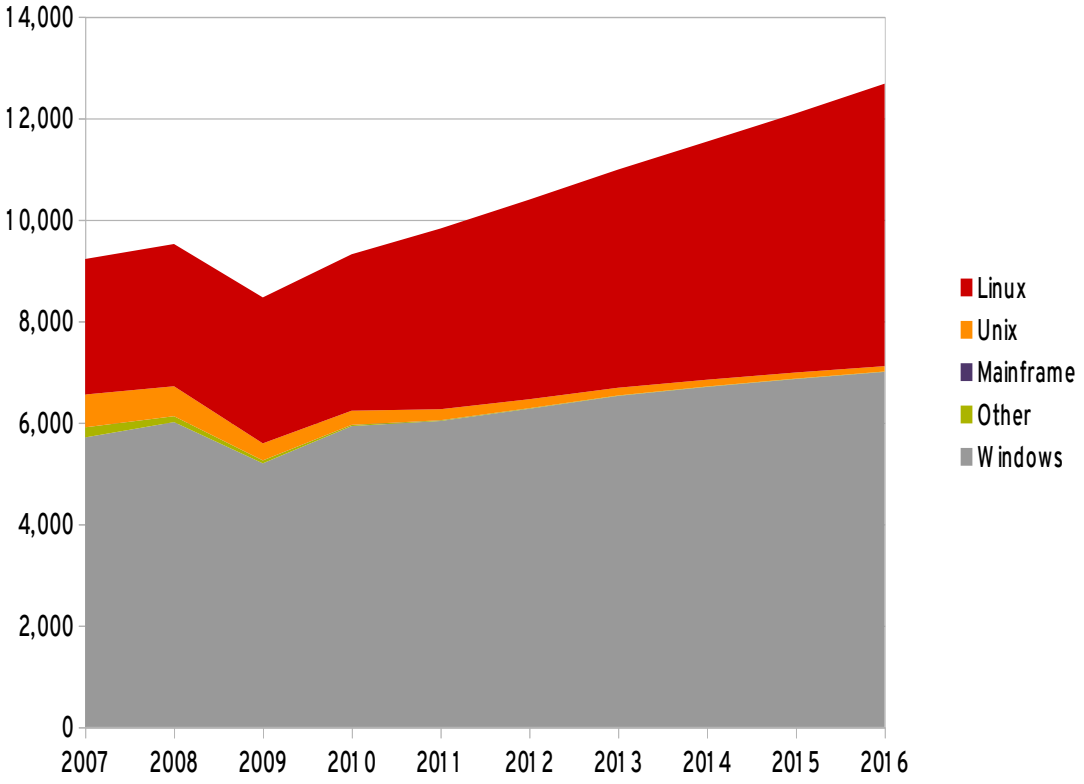
오픈소스 기반의 클라우드 환경

클라우드 컴퓨팅


빅데이타

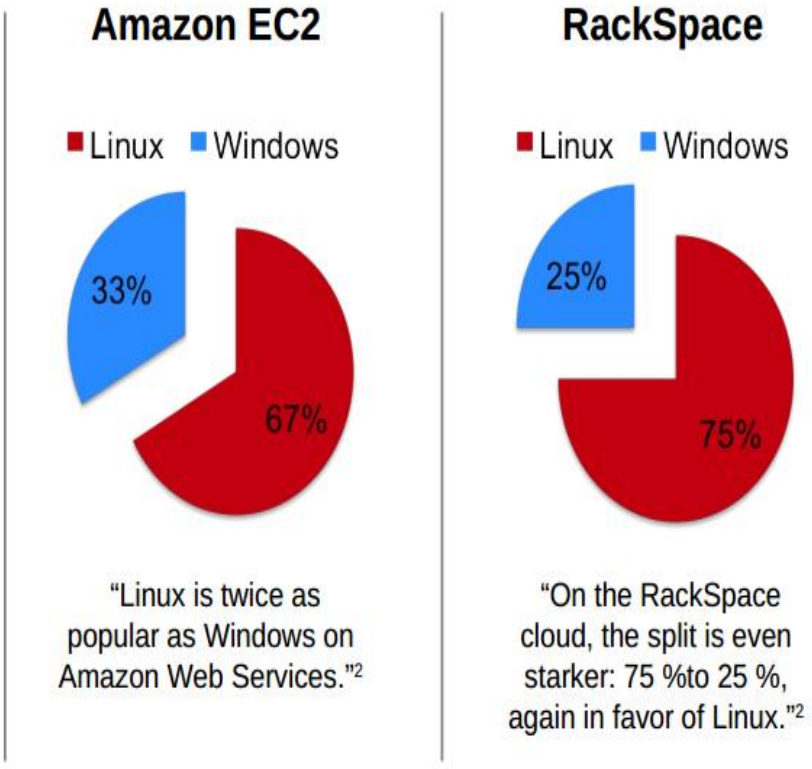




클라우드 환경에서의 리눅스 점유율

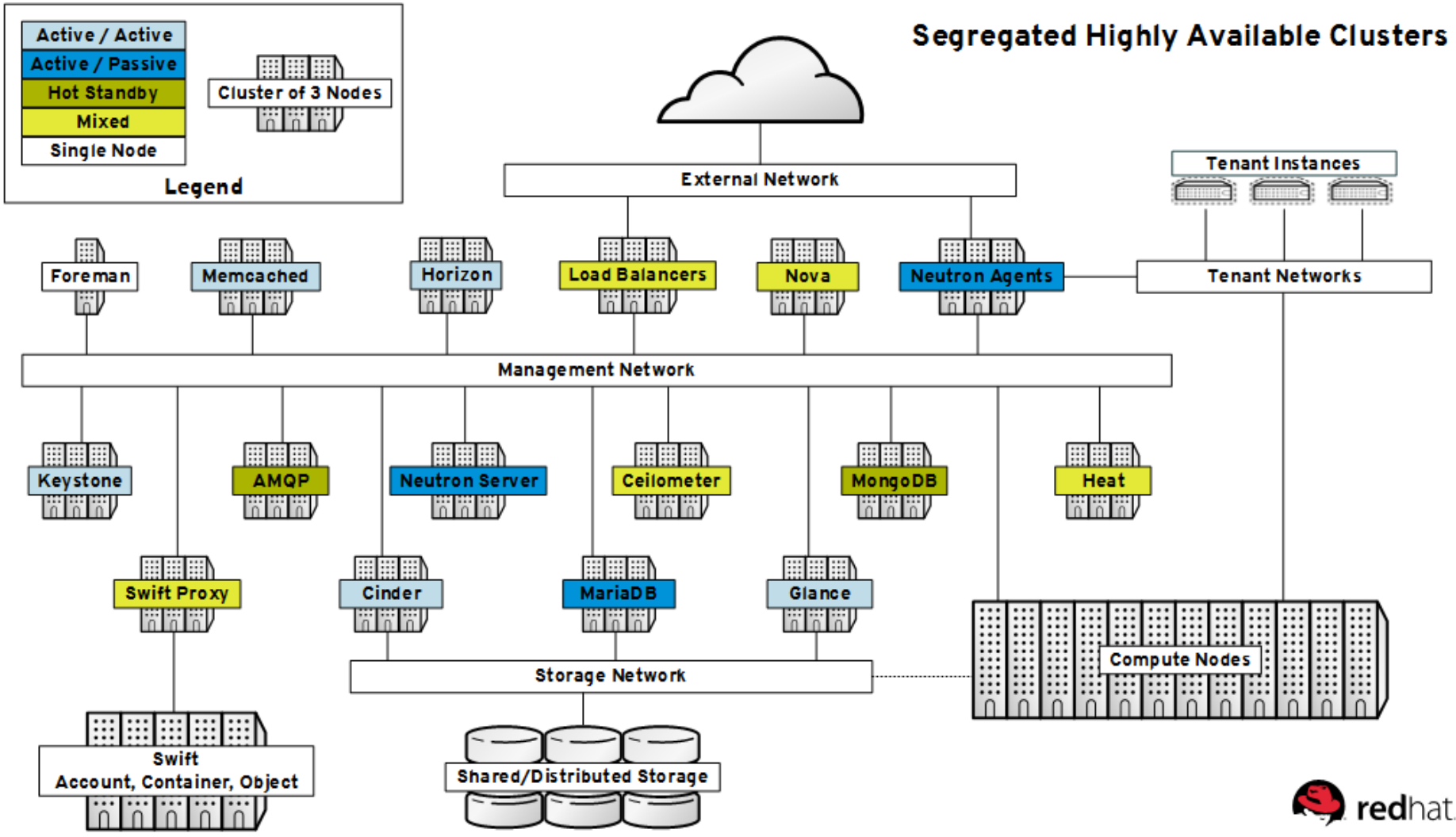


Analyze the Future

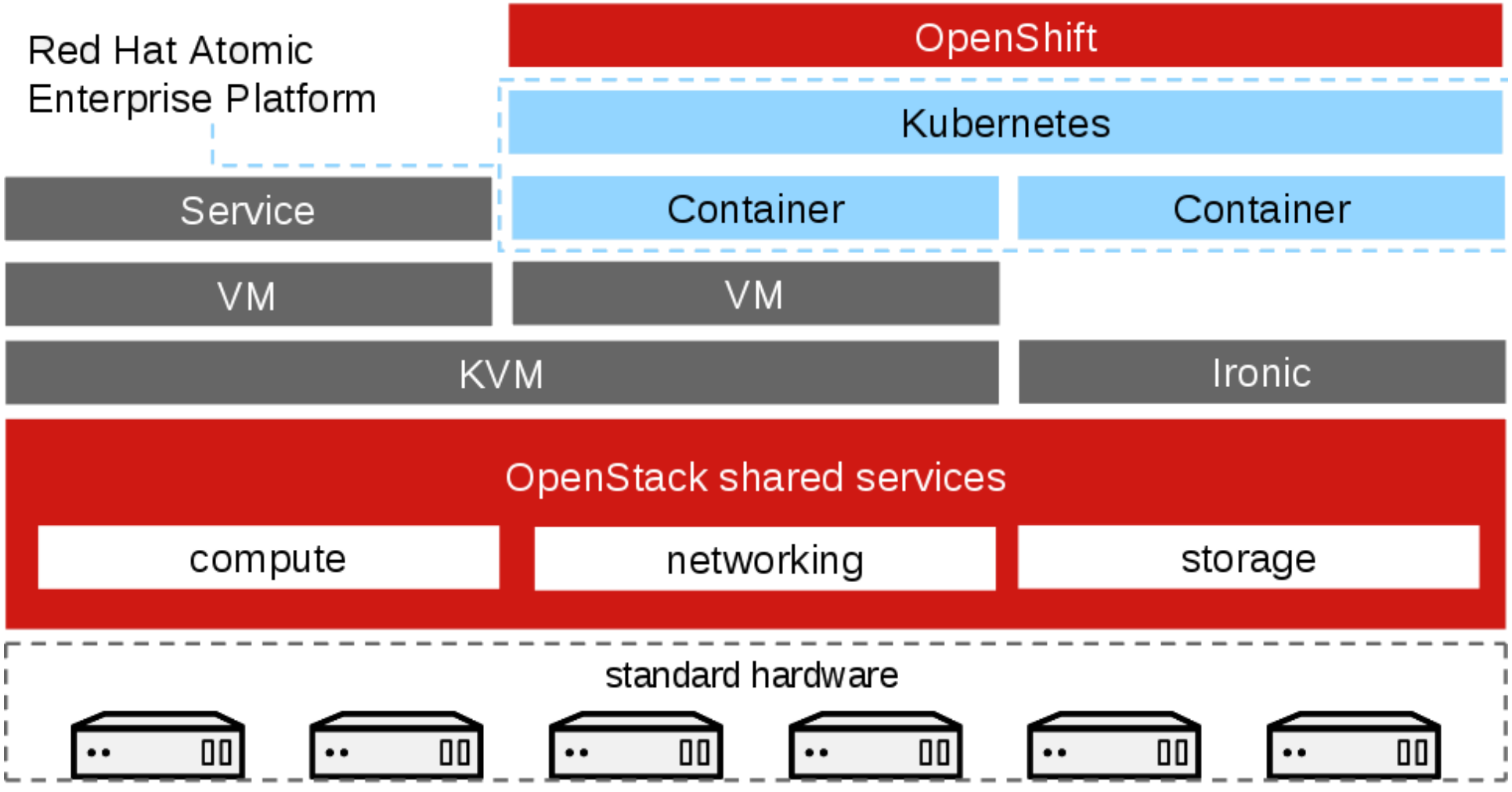
Source: Worldwide Client and Server Operating Environments Market Analysis and 2012-2016 Forecast and 2011 Vendor Shares: The Changing Dynamics and Demographics (IDC #236428, August 2012).



오픈스택 아키텍처

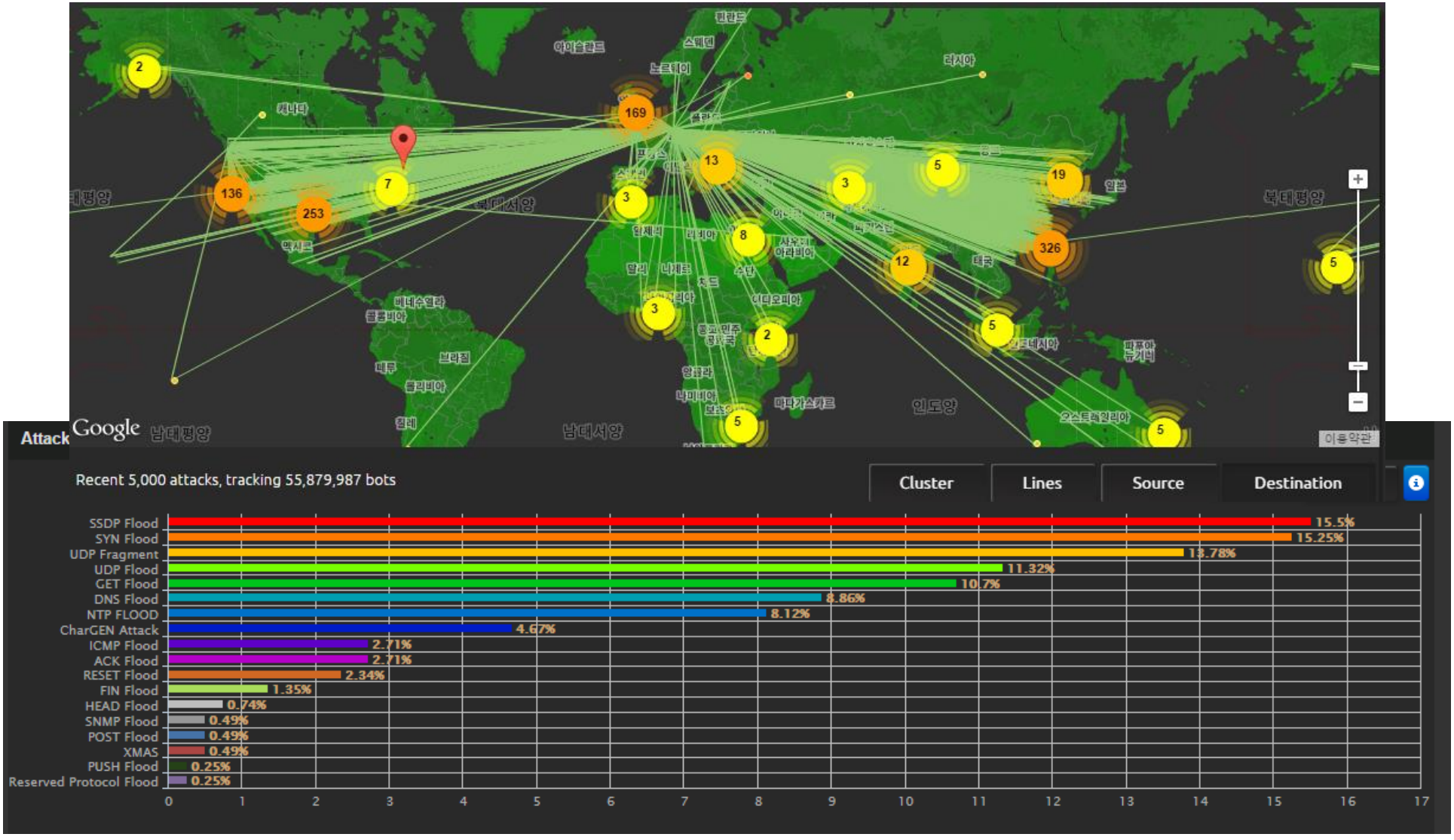

Active / Active
Active / Passive
Hot Standby
Mixed
Single Node
Legend
Cluster of 3 Nodes
Segregated Highly Available Clusters
External Network
Tenant Instances
Foreman
Memcached
Horizon
Load Balancers
Nova
Neutron Agents
Tenant Networks
Management Network
Keystone
AMQP
Neutron Server
Ceilometer
MongoDB
Heat
Swift Proxy
Cinder
MariaDB
Glance
Compute Nodes
Storage Network
Swift
Account, Container, Object
Shared/Distributed Storage
redhat.

컨테이너 (on Open Stack) 아키텍처




redhat.
IT트렌드
클라우드 컴퓨팅
클라우드 컴퓨팅의 보안
레드햇 보안 정책
공개SW포털
OPEN SOURCE SOFTWARE

전세계 DDoS 현황 (2015.9.11.기준)



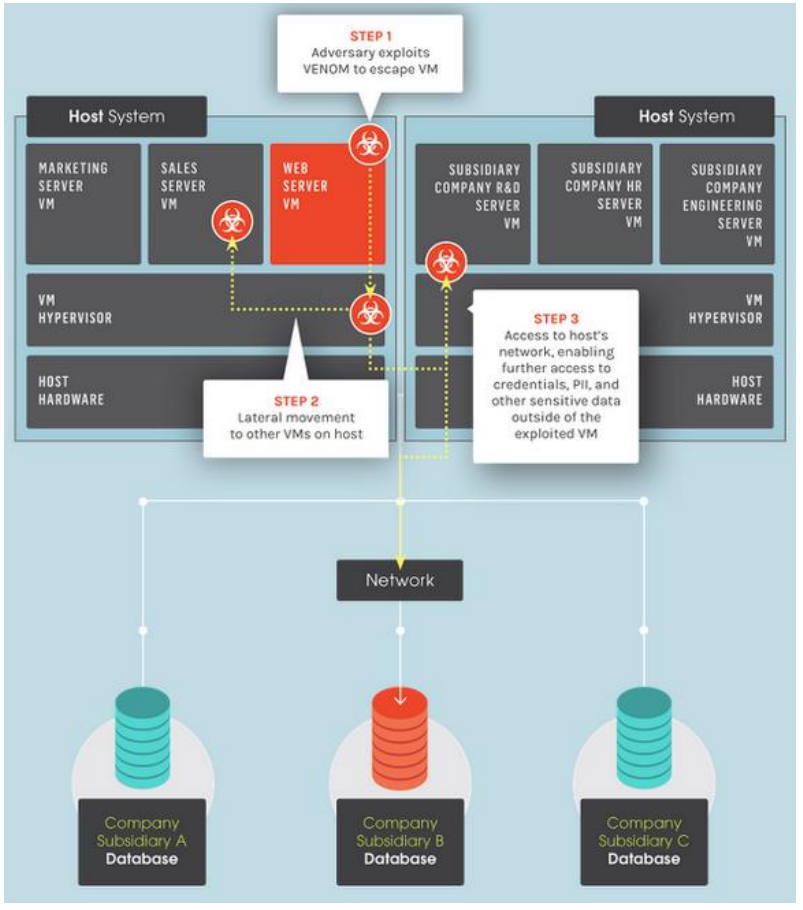
- 출처 : https://www.stateoftheinternet.com/trends-visualizations-security-real-time-global-ddos-attack-sources-types-and-targets.html

이제는 안심할 수 없는 스마트폰

- 이탈리아 '해킹팀'의 스마트폰 해킹솔루션 RCS(Remote Control System)
- 이탈리아 '해킹팀' 내부자료 Wikileaks에서 자료 공개로 우리나라 국가기관의 감청프로그램 구입 노출(2015.7.6)
- 방법 : 이메일에 특정 URL 클릭 또는 이메일 첨부 문서를 통한 스파이 프로그램 설치
- 대상 : 안드로이드, (탈옥)아이폰
- 전화통화 모니터링 및 녹음, 문자 모니터링, 잠금해제, SNS(라인, 페이스북, 텔레그램 등) 감시, 사진 및 동영상 모니터링 등

하이퍼바이저 취약점

- VENOM 취약점 (CVE-2015-3456)
- KVM/QEMU, XEN 하이퍼바이저의 플로피 디스크 관련 '버퍼오버플로우' 취약점'
- 영향도 : 상기의 하이퍼바이저를 사용하는 가상화 리눅스 솔루션
- 해결방법
- 취약성 점검 : VENOM: QEMU Vulnerability Detector
- 패치
- 세부 관련 정보 : https://securityblog.redhat.com/2015/05/13/venom-dont-get-bitten/



- 출처 : http://venom.crowdstrike.com/

Bash Shell 취약점

- Bash Code Injection – Shellshock
- Bash 환경변수와 관련된 취약점으로 Code Injection 을 통해 공격자는 시스템 내 제한을 회피하고, 인증되지 않은 권한을 획득
- 영향
- 1989~ 2014(15년) 동안 취약점 존재
- Unix, Linux, MacOS, Android Mobile 등
- 전세계 51% 의 서버 및 device 들이 본 취약점에 노출되어 있었던 것으로 추정됨 CVE
- CVE
- CVE-20140-6271, CVE-2014-7169, CVE-20140-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278
- 2번의 패치로 6개의 CVE 가 패치됨

OpenSSL Heartbleed

- TSL/DTSL 프로토콜을 OpenSSL 에 적용하면서 발생한 취약점 (2011년)으로 공격자는 packet 조작하여 다른 사용자에 대한 정보 등 중요한 정보를 얻을 수 있음
- 전세계 **2/3**의 웹서버가 **OpenSSL**을 사용하기 때문에 영향도는 민감하고 큰 문제로 판단
- 영향:

- OS와 관계없이 취약 버전의 **"OpenSSL"**을 이용하는 모든 소프트웨어 및 디바이스에 영향을 미치며, **OS, SW, Mobile Phone, SSL VPN**장비 및 취약 버전의 **OpenSSL**버전이 적용된 **Web Site** 등

- CVE

- CVE-2014-0224


CVE-ID

CVE-2014-0160 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://heartbleed.com/
- CONFIRM:http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=96db9023b881d7cd9f379b0c154650d6c108e9a3
- CONFIRM:http://www.openssl.org/news/secadv_20140407.txt
- CONFIRM:https://bugzilla.redhat.com/show_bug.cgi?id=1084875

Date Entry Created

20131203 Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20131203)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

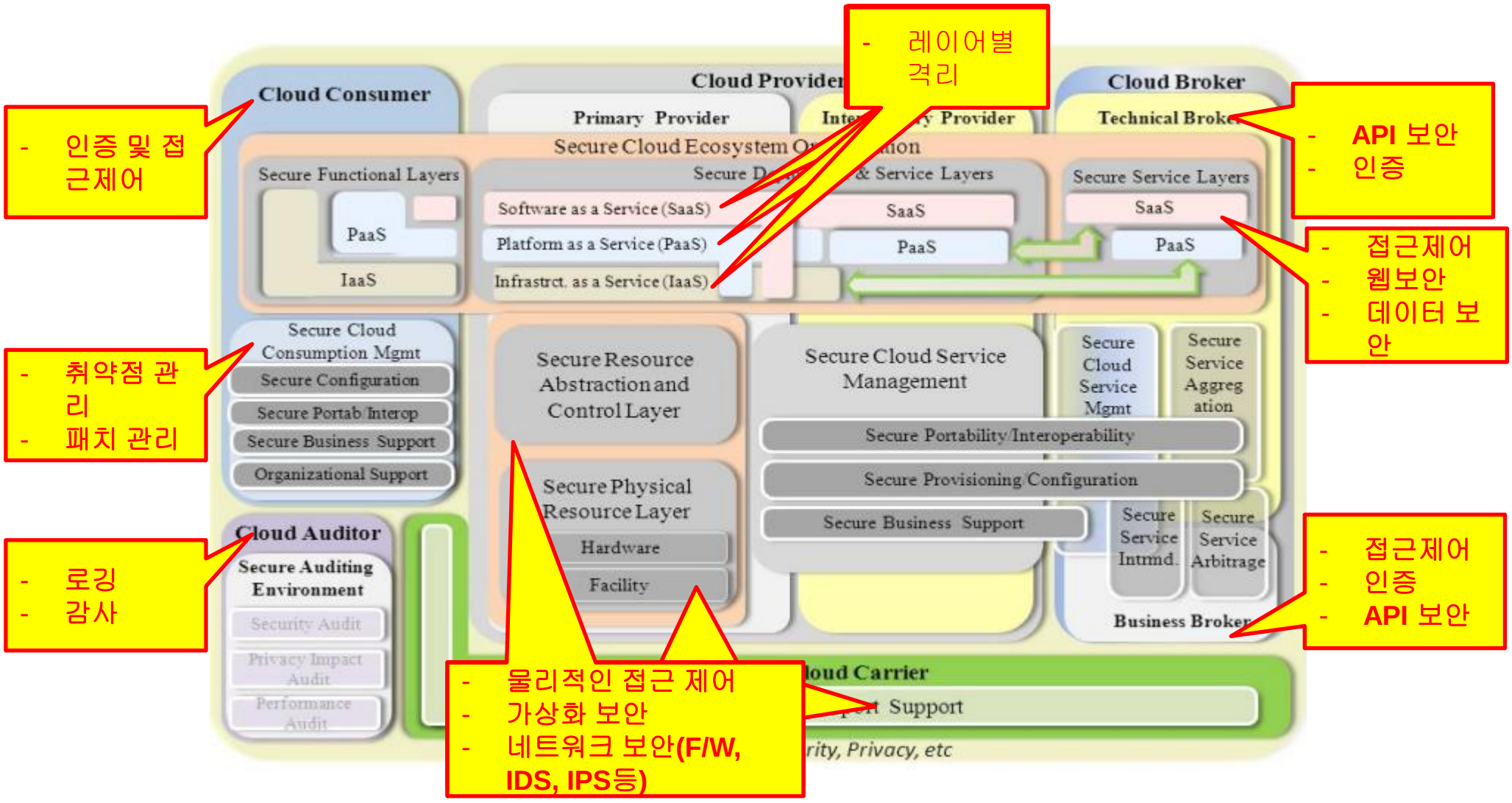
SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

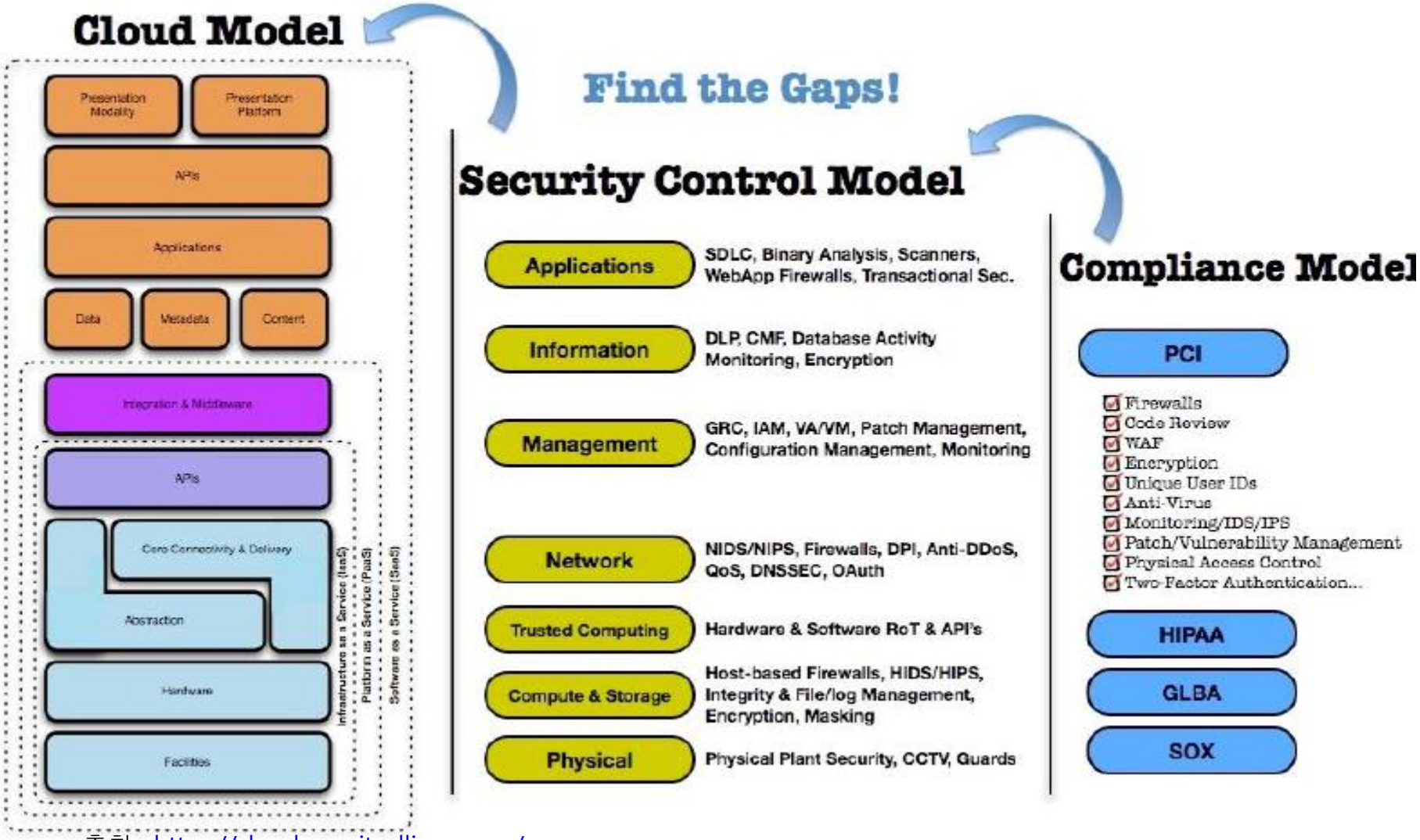
Source : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

클라우드 보안 참조 아키텍처 : NIST



- 출처 : http://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf

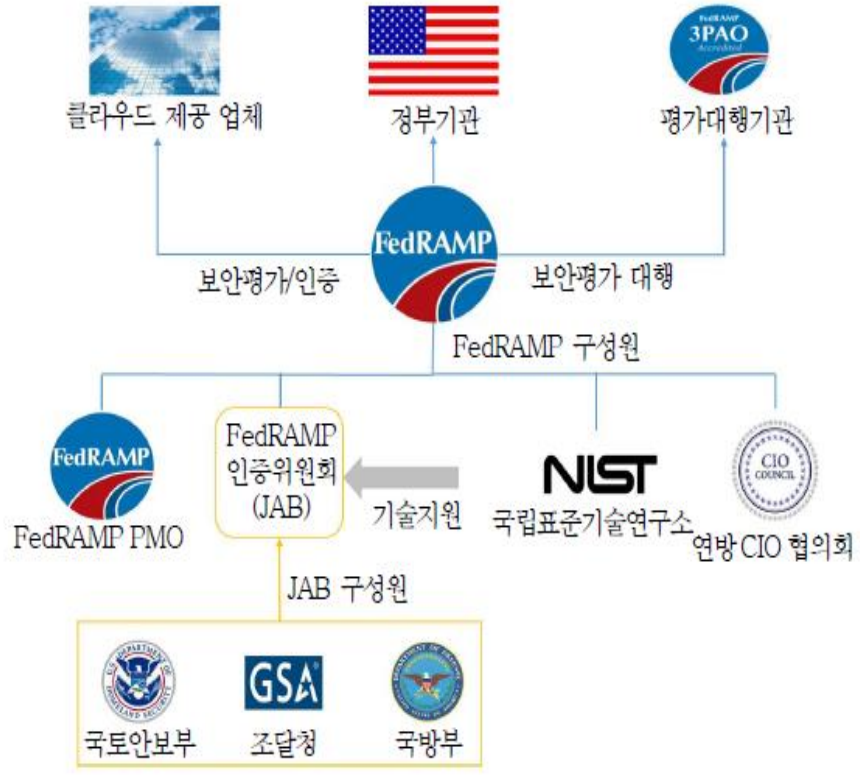
클라우드 보안 참조 모델 : Cloud Security Alliance



- 출처 : https://cloudsecurityalliance.org/

정책 및 절차적 보안 : FedRAMP

- 미 정부기관이 이용하려는 클라우드 제품 및 서비스에 대한 보안 평가, 인증 및 사후관리를 위해 도입한 프로그램

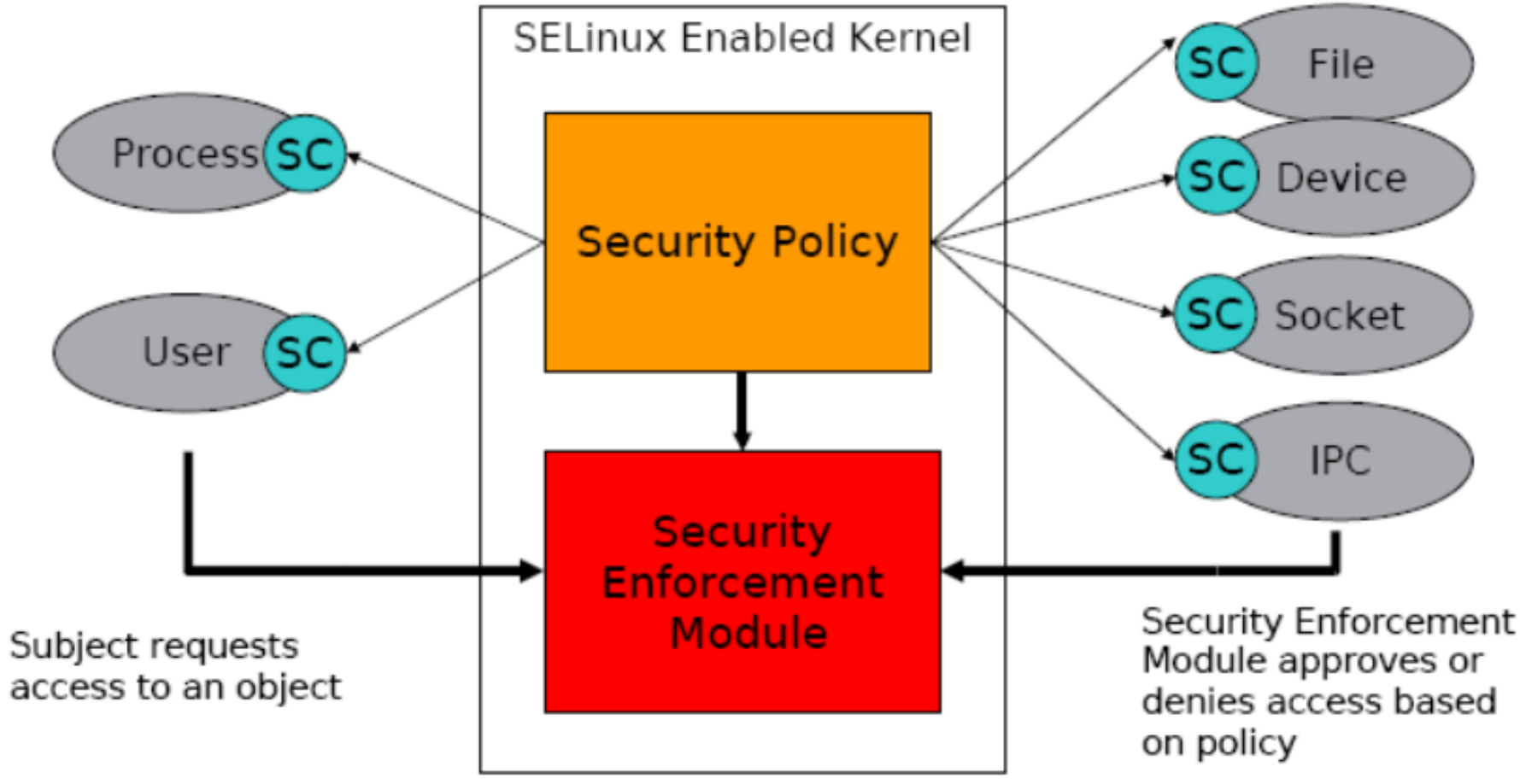


美 FedRAMP	국내 정보보호시스템 공통평가기준
접근통제	접근통제 정책, 기능
인식 및 교육	정보보호 교육 및 훈련
감사 및 책임	보안 감사는 있지만 책임 여부는 없음
인증, 보안 평가	식별 및 인증만 존재, 보안 평가 요소는 없음
구성 관리	n/a
비상 계획	n/a
식별 및 인증	식별 및 인증
사고대응	보안사고 관리
유지 보수	n/a
매체 보호	암호 지원
물리적 환경 보호	TSF 의 물리적 보호만 존재
계획	n/a
인사 보안	n/a
리스크 평가	n/a
시스템 및 서비스 취득	TSF 보호, TOE 접근
시스템 및 통신 보호	통신 보호만 존재
시스템 또는 정보의 무결성	TSF 보호, 사용자 데이터 보호

- 출처 : 美 클라우드 보안인증체계(FedRAMP) 동향 및 국내 정보보호시스템 공통평가기준의 비교 분석(대전대 박기웅,박준형)

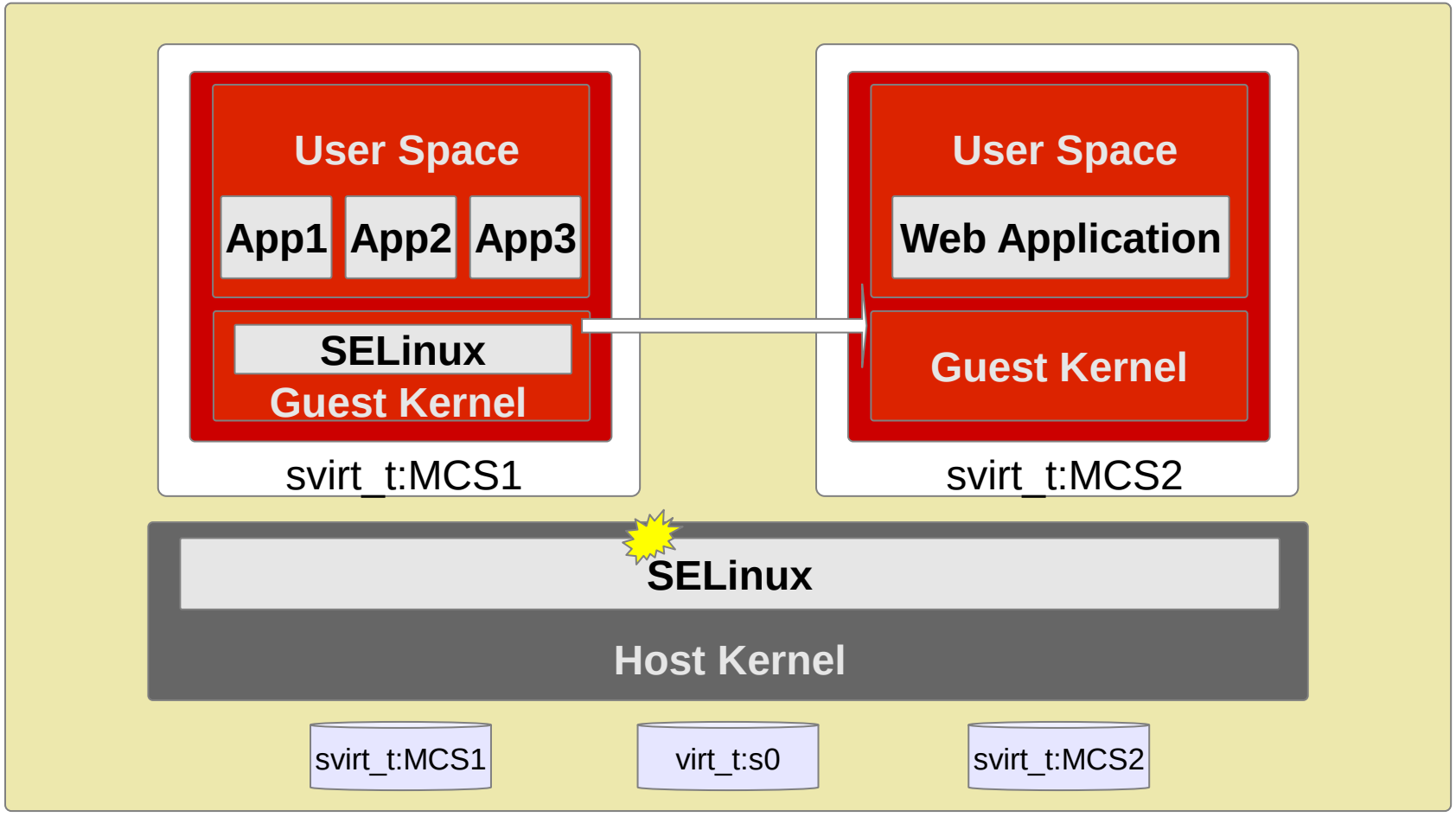
호스트 / VM OS 보안

- SELinux를 이용한 프로세스, 유저, 파일, 디바이스 등의 역할접근제어 정책 적용



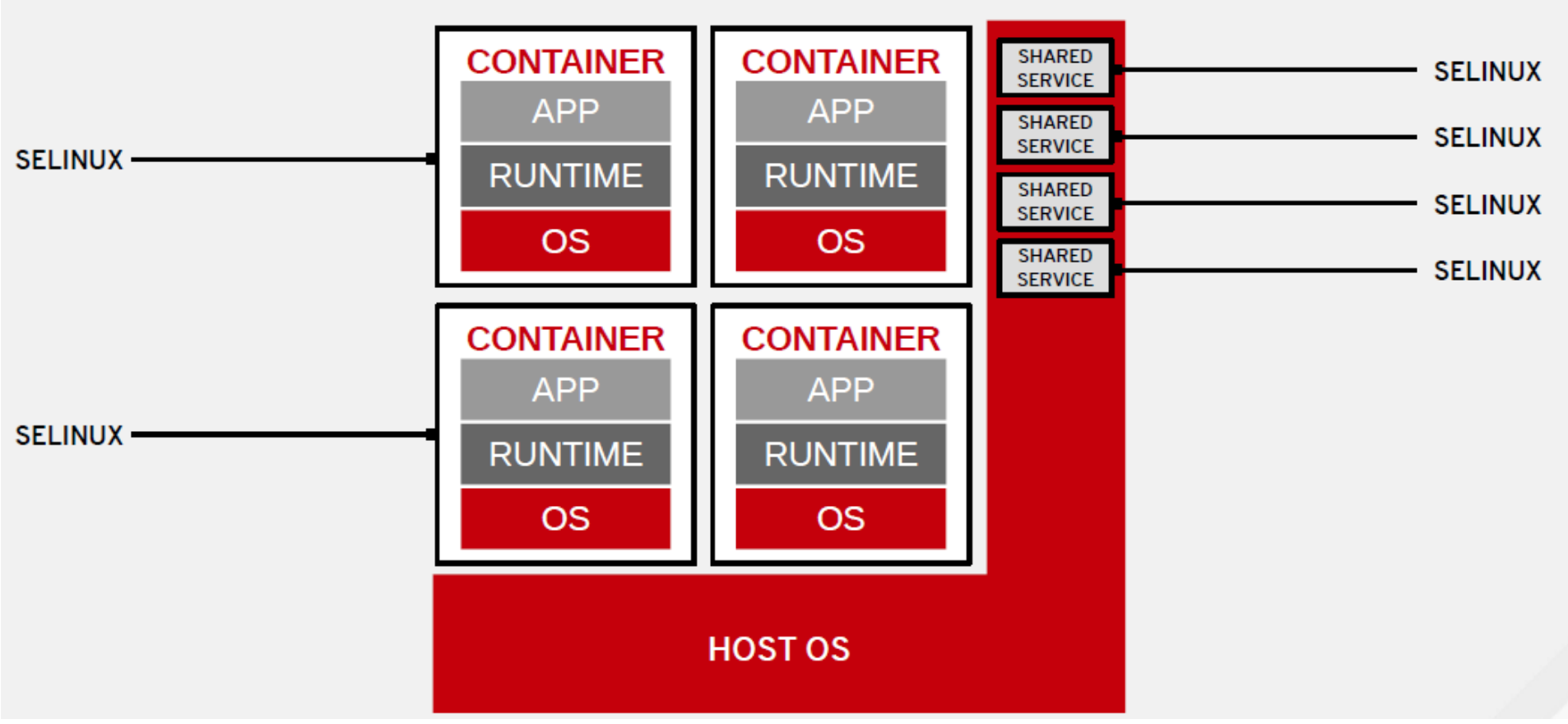
하이퍼바이저 보안

- VM 및 가상화 라이브러리들에 대한 접근 제어 정책
- Svirt를 이용한 VM 격리



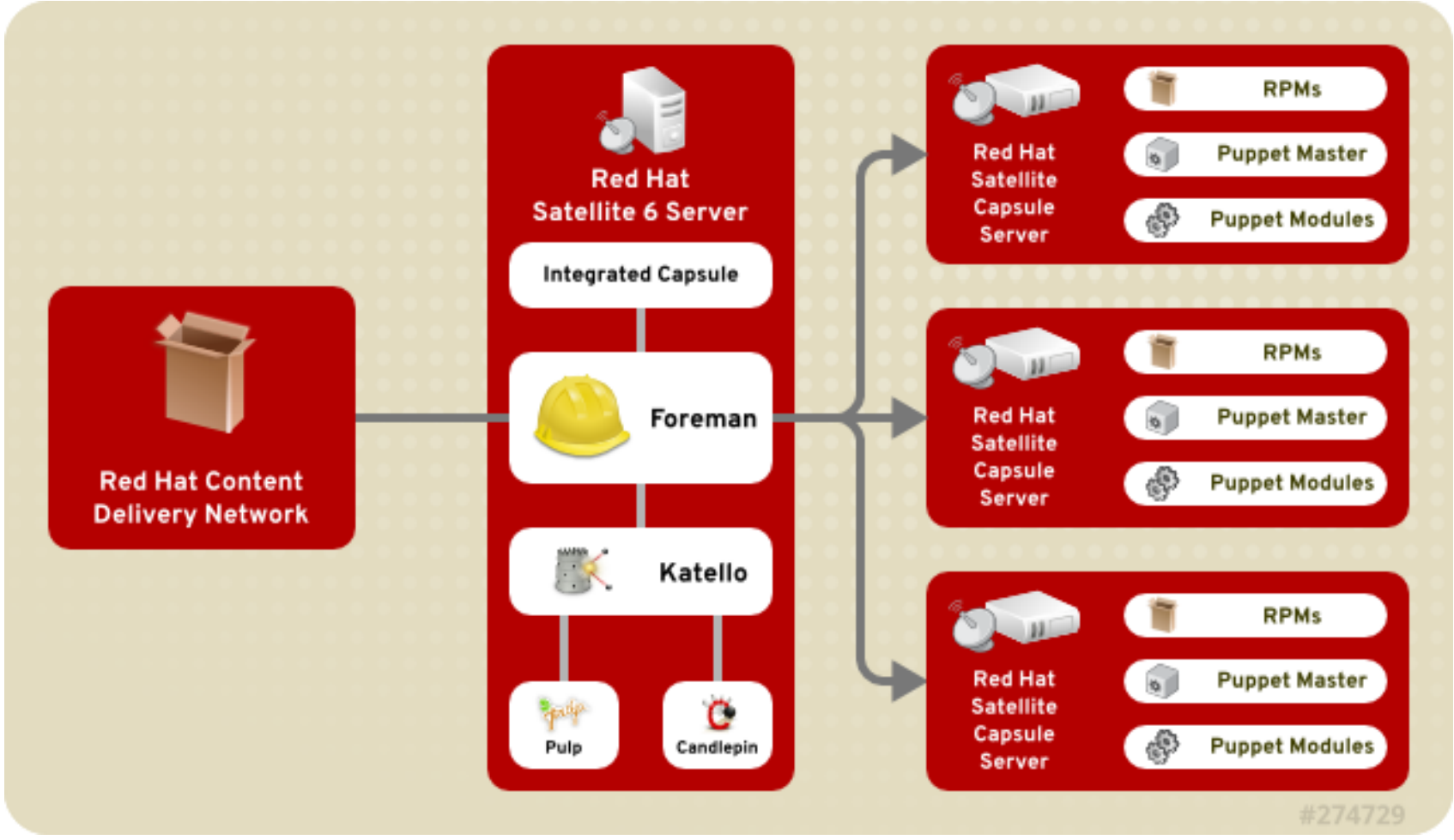
컨테이너 보안

- SELinux를 이용한 격리 정책
- Container별 / 공유서비스별 격리



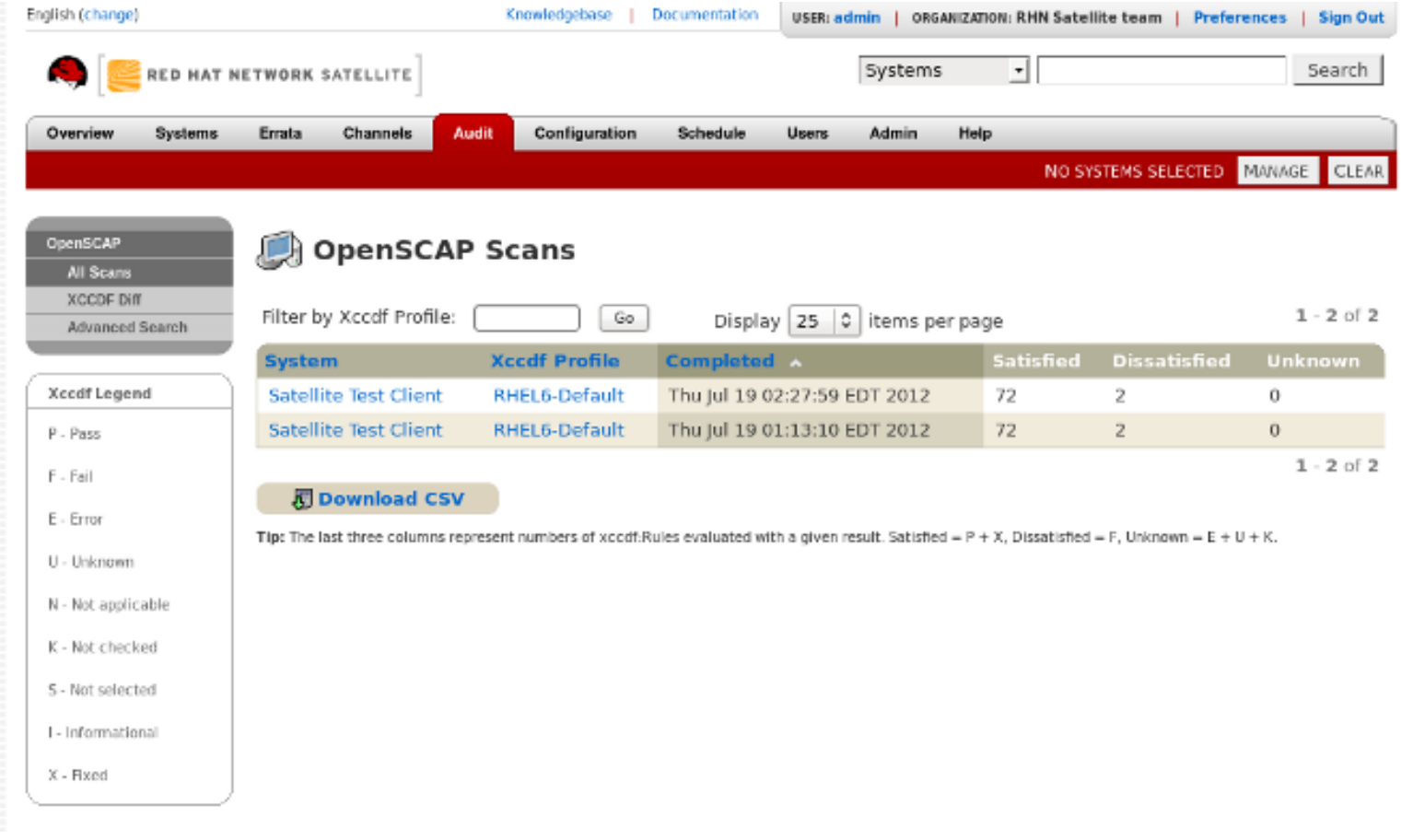
패치 관리

- RH Satellite를 이용한 패치 관리



OpenSCAP

- 리눅스 인프라의 표준 컴플라이언스 감사 솔루션
- NIST에 의해 관리되며, XCCDF 를 사용




redhat.
IT트렌드
클라우드 컴퓨팅
클라우드 컴퓨팅의 보안
레드햇 보안 정책
공개SW포털
OPEN SOURCE SOFTWARE

레드햇 보안 정책

- Red Hat Enterprise Linux는 상용 유닉스와 동일한 EAL4+ 등급 취득
- 모든 보안 이슈는 발견된지 **3일 이내에 security fix 제공**
  - 보안 전담팀 운영 - security@redhat.com
  - 90%의 보안이슈가 zero day에 해결

- SELinux(Secure Enhanced Linux)& sVirt(Secure Enhanced Vitualization)
  - NSA에서 개발주도 / 커널에 포함된 강력한 보안기능

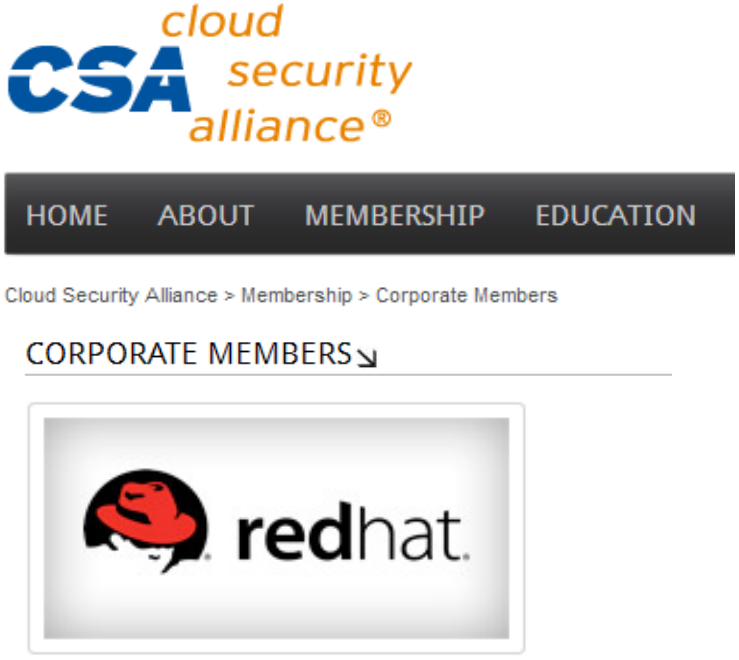
- Common Criteria certification
  - 20개이상의 정부기관에서 인정하는 신뢰성 있는 보안 인증
  - LSPP/RBACPP and CAPP at EAL 4+ w/ Red Hat Enterprise Linux 5, 6 & 7

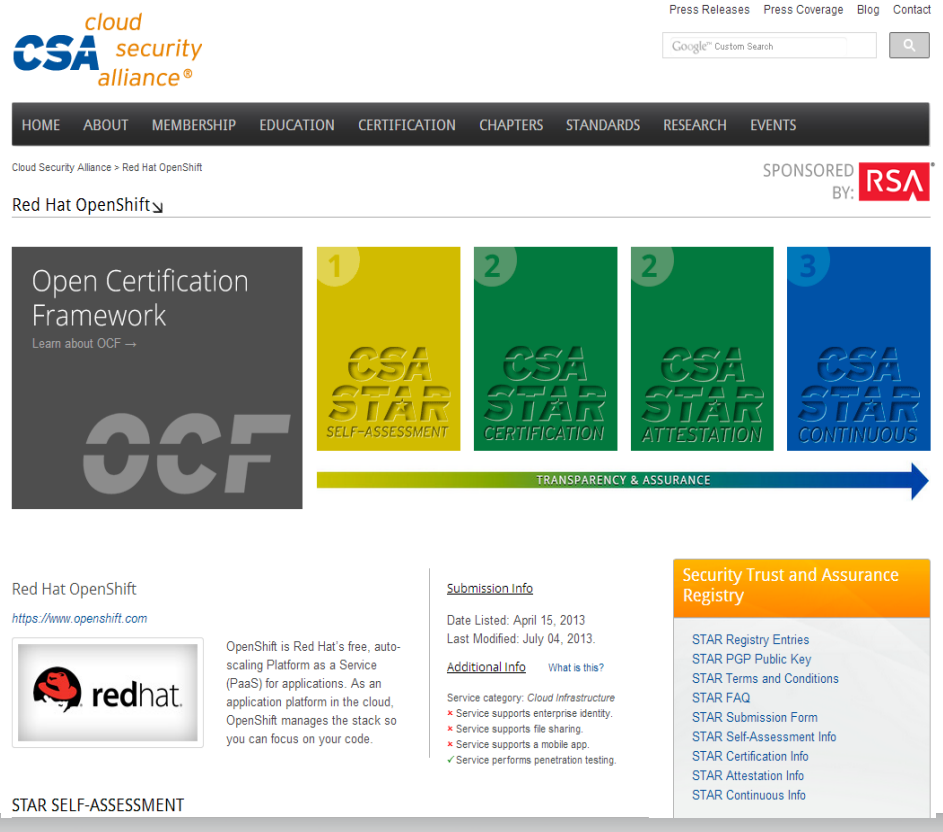
	RHEL5	RHEL6
Common Criteria EAL4+/CAPP/RBACPP/LSPP	Dell, HP, IBM, SGI	Dell, HP, IBM, SGI

Source URL : http://www.redhat.com/solutions/industry/government/certifications.html

클라우드 보안협회 멤버

- CSA(Cloud Security Alliance)
- 2010년부터 CSA 활동 시작, 2012년 기업 멤버로 CSA가입
- Red Hat focus on **Open standards and Security** in the Cloud



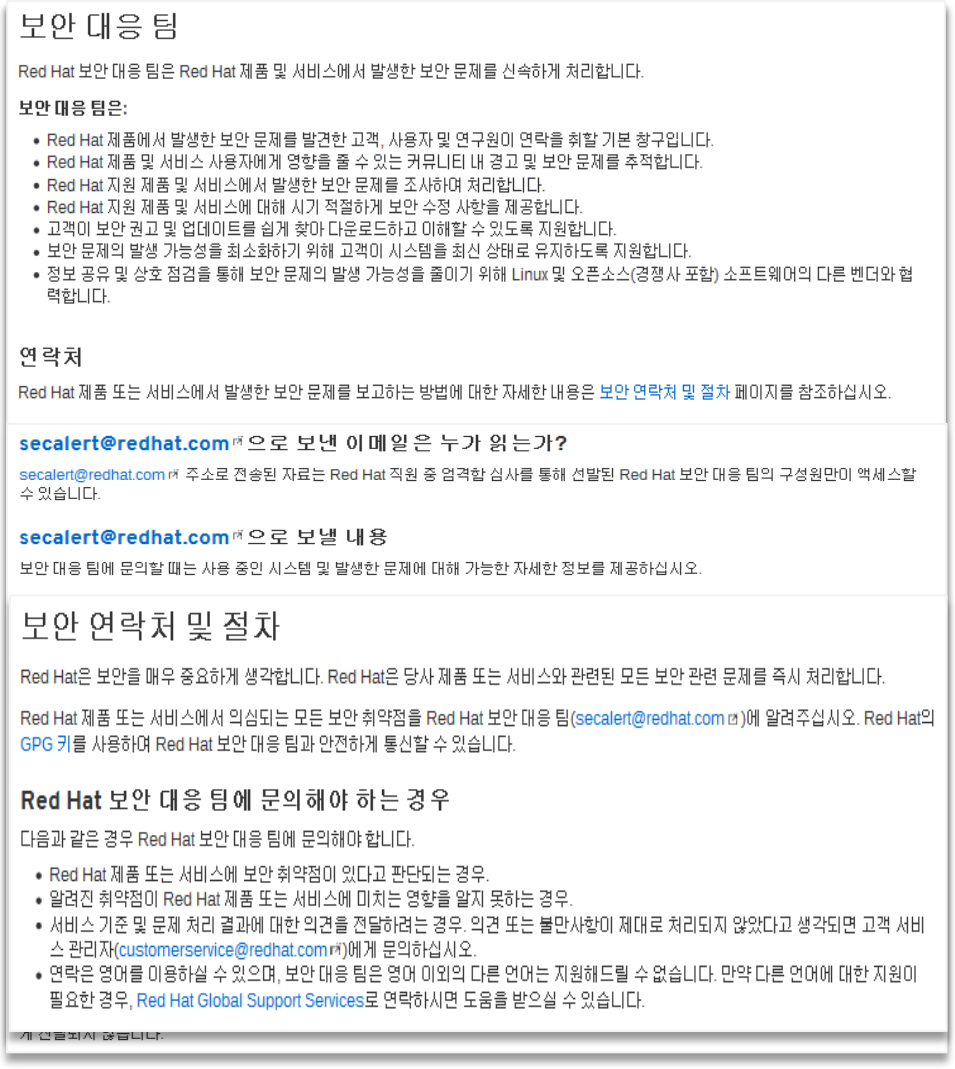


RHEL 보안 인증 현황

구분	RHEL4	RHEL5	RHEL6
Common Criteria EAL3+/CAPP	HP, SGI, Unisys		
Common Criteria EAL4+/CAPP	IBM		
Common Criteria EAL4+/CAPP/RBACPP /LSPP		Dell, HP, IBM, SGI	
In evaluation for Common Criteria		BSI-DSZ-CC-0724, includes virtualization	BSI-DSZ-CC-0754, includes virtualization
Directorate of Central Intelligence Directive (DCID) 6/3	PL3+. See your Red Hat account manager for more details and sign up for the gov-sec mailing list.		
DISA Security Technical Implementation Guides (STIG)	There are many options for meeting the STIG requirements. See your Red Hat account manager for more details and sign up for the gov-sec mailing list.		
FIPS 140-2	NSS (Cert. #814, #815, #1293, #1280)	• Kernel Crypto API (Cert. #1387) • libgcrypt (Cert. #1305) • NSS(Cert.#814,#815,#1293,#1280) • OpenSSH Client (Cert. #1385) • OpenSSH Server (Cert. #1384) • OpenSSL (Cert. #1320) • openswan (Cert. #1386)	evalution: • kernel crypto API • libgcrypt • openswan • OpenSSH Client • OpenSSH Server • OpenSSL
OVAL	See the Red Hat Security OVAL Webpage(https://access.redhat.com/site/articles/221883)		
NISPOM Chapter 8	See NISPOM Chapter 8 Knowledge Base Article		
Section 508 Accessibility	VPAT for RHEL	VPAT for RHEL5	VPAT for RHEL6

보안 대응팀

- **Red Hat** 보안 대응팀
- https://access.redhat.com/site/ko/security/team
- 커뮤니티 내 경고 및 보안 문제 추적
- 보안 문제 조사 및 처리, 수정사항 제공
- Linux 및 오픈소스 소프트웨어 타 벤더와 협력
- **Secalert@redhat.com**
- Red Hat 제품 또는 서비스 보안 취약점 판단시 문의
- 알려진 취약점에 대한 사항들 문의



보안 대응 팀

Red Hat 보안 대응 팀은 Red Hat 제품 및 서비스에서 발생한 보안 문제를 신속하게 처리합니다.

보안 대응 팀은:

- Red Hat 제품에서 발생한 보안 문제를 발견한 고객, 사용자 및 연구원이 연락을 취할 기본 창구입니다.
- Red Hat 제품 및 서비스 사용자에게 영향을 줄 수 있는 커뮤니티 내 경고 및 보안 문제를 추적합니다.
- Red Hat 지원 제품 및 서비스에서 발생한 보안 문제를 조사하여 처리합니다.
- Red Hat 지원 제품 및 서비스에 대해 시기 적절하게 보안 수정 사항을 제공합니다.
- 고객이 보안 권고 및 업데이트를 쉽게 찾아 다운로드하고 이해할 수 있도록 지원합니다.
- 보안 문제의 발생 가능성을 최소화하기 위해 고객이 시스템을 최신 상태로 유지하도록 지원합니다.
- 정보 공유 및 상호 점검을 통해 보안 문제의 발생 가능성을 줄이기 위해 Linux 및 오픈소스(경쟁사 포함) 소프트웨어의 다른 벤더와 협력합니다.

연락처

Red Hat 제품 또는 서비스에서 발생한 보안 문제를 보고하는 방법에 대한 자세한 내용은 보안 연락처 및 절차 페이지를 참조하십시오.

secalert@redhat.com으로 보낸 이메일은 누가 읽는가?

secalert@redhat.com 주소로 전송된 자료는 Red Hat 직원 중 엄격한 심사를 통해 선발된 Red Hat 보안 대응 팀의 구성원만이 액세스할 수 있습니다.

secalert@redhat.com으로 보낼 내용

보안 대응 팀에 문의할 때는 사용 중인 시스템 및 발생한 문제에 대해 가능한 자세한 정보를 제공하십시오.

보안 연락처 및 절차

Red Hat은 보안을 매우 중요하게 생각합니다. Red Hat은 당사 제품 또는 서비스와 관련된 모든 보안 관련 문제를 즉시 처리합니다.

Red Hat 제품 또는 서비스에서 의심되는 모든 보안 취약점을 Red Hat 보안 대응 팀(secalert@redhat.com)에 알려주십시오. Red Hat의 GPG 키를 사용하여 Red Hat 보안 대응 팀과 안전하게 통신할 수 있습니다.

Red Hat 보안 대응 팀에 문의해야 하는 경우

다음과 같은 경우 Red Hat 보안 대응 팀에 문의해야 합니다.

- Red Hat 제품 또는 서비스에 보안 취약점이 있다고 판단되는 경우.
- 알려진 취약점이 Red Hat 제품 또는 서비스에 미치는 영향을 알지 못하는 경우.
- 서비스 기준 및 문제 처리 결과에 대한 의견을 전달하려는 경우. 의견 또는 불만사항이 제대로 처리되지 않았다고 생각되면 고객 서비스 관리자(customerservice@redhat.com)에게 문의하십시오.
- 연락은 영어를 이용하실 수 있으며, 보안 대응 팀은 영어 이외의 다른 언어는 지원해드릴 수 없습니다. 만약 다른 언어에 대한 지원이 필요한 경우, Red Hat Global Support Services로 연락하시면 도움을 받으실 수 있습니다.

취약성 평가 시스템

- 취약성 평가 시스템
- 레드햇 CVE
- https://access.redhat.com/security/cve/
- CVE Database내 레드햇의 취약점 및 보안 관련 사항 표준화 목록
- CVSS(공통 취약성 평가 시스템) : 심각도 평가 제공
- Red Hat의 CVSS v2 기반 평가 점수

CVSS(Common Vulnerability Scoring System; 공통취약성평가시스템)

CVSS(공통취약성평가시스템) 기반 점수는 취약성의 일정한 특성인 접근 벡터, 접근 복잡도, 인증, 기밀성, 무결성 및 가용성을 점수화함으로써 상세한 심각도 평가를 제공합니다.

2009년 이후의 취약성 전체 및 기존의 일부 취약성에 대해 CVSS 버전 2 기반의 평가 점수가 제공됩니다. 본 점수표는 CVE별 페이지(Red Hat 보안 공지의 참고 사항 섹션에 링크가 있음) 및 보안 평가 페이지에 나와 있습니다.

CVSS v2 기반 평가 점수

CVSS v2 기반 평가 점수표는 취약성의 일정한 측면과 관계가 있습니다.

- 접근 벡터(AV: Access Vector): 취약성에 접근하는 방식. 예: 시스템에 대한 로컬 접근의 필요 여부 또는 네트워크 상에서 취약성이 원격으로 악용될 수 있는 가능성.
- 접근 복잡도(AC: Access Complexity): 취약성이 발현되는 데 필요한 추가 조건. 예를 들어 뜻밖의 구성이 필요할 수 있습니다.
- 인증(Au: Authentication): 공격자가 요구하는 인증.
- 기밀성(C: Confidentiality): 취약성이 악용될 경우 정보 유출의 위험.
- 무결성(I: Integrity): 취약성이 악용될 경우 공격자가 시스템 상의 데이터를 수정할 수 있는 위험.
- 가용성(A: Availability): 취약성이 악용될 경우 공격자가 서비스 거부를 초래할 수 있는 위험.

공식을 통해 이 측정 지표가 0.0(위험 없음)과 10.0(최고 위험) 사이의 범위에서 하나의 기준 점수로 변환됩니다. 기준 평가 점수에 대한 자세한 내용은 A Complete Guide to the Common Vulnerability Scoring System Version 2.0(공통취약성평가시스템 버전 2.0 상세 설명서)을 참조하십시오.

Red Hat의 CVSS v2 기반 평가 점수 활용

Red Hat은 기준 점수 할당 시 CVSS v2 표준에 부합하도록 노력합니다. 일부의 경우 특정 점수를 받은 이유가 명확하지 않을 수 있습니다. 일반적 유형의 취약성 예와 이에 대한 Red Hat의 해석 및 평가 전형이 아래에 나와 있습니다.

CVE 데이터베이스

CVE 이름에 따른 Red Hat 취약점

MITRE Corporation이 관리하고 있는 CVE (Common Vulnerabilities and Exposures) 프로젝트는 취약점 및 보안 관련 사항에 대한 용어를 표준화한 목록입니다.

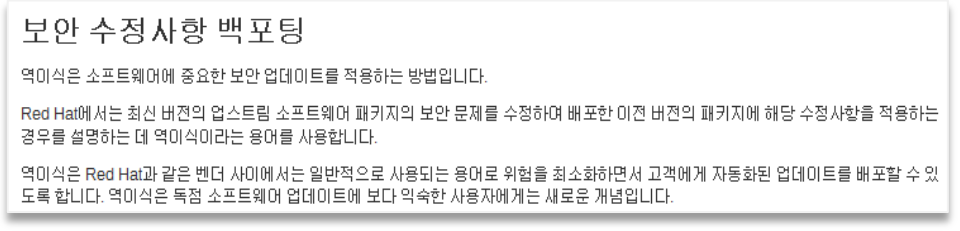
2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002 | 2001 | 2000 | 1999

Show 10 entries Filter:

CVE	개요	영향	공개 날짜
CVE-2014-0001	Buffer overflow in client/mysql.cc in Oracle MySQL and MariaDB before 5.5.35 allows remote database servers to cause a denial of service (crash) and possibly execute arbitrary code via a long server version string.	Moderate	2014-01-30

Red Hat 보안 대응체계 (계속)

- 보안 경고, 버그 수정 및 기능 개선
  - https://access.redhat.com/site/ko/security/updates/active
  - 레드햇 모든 제품에 대한 보안 업데이트 정보 제공
- 보안 수정 사항 백포팅
- **Life Cycle 및 Update 정책**
  - https://access.redhat.com/site/ko/security/team
  - 주요 릴리즈 라이프사이클 제공
  - 기본 10년 Production 지원, EUS 3년



We've been **OPEN** all along.

It's in our DNA.

It's not lip service. Or cloud washing.

Open is what we do. And how we do it.

With every step forward, Red Hat opens another layer of the technology stack.

Cloud is the next step—the next open innovation.


redhat
감사합니다