
AWS 101



아마존 웹서비스(AWS)와 함께하는 클라우드 컴퓨팅

윤석찬

AWS코리아, 테크에반젤리스트

AWS와 함께 하는 4주 클라우드 보안 강의

- 5월 2일 클라우드 컴퓨팅 및 AWS 소개
- 5월 9일 AWS 주요 서비스 사용 실습 (S3 및 CloudFront)
- 5월 23일 AWS 보안 관리 서비스 소개
- 5월 30일 AWS 보안 관리 서비스 실습 (WAF, IAM)

목 차

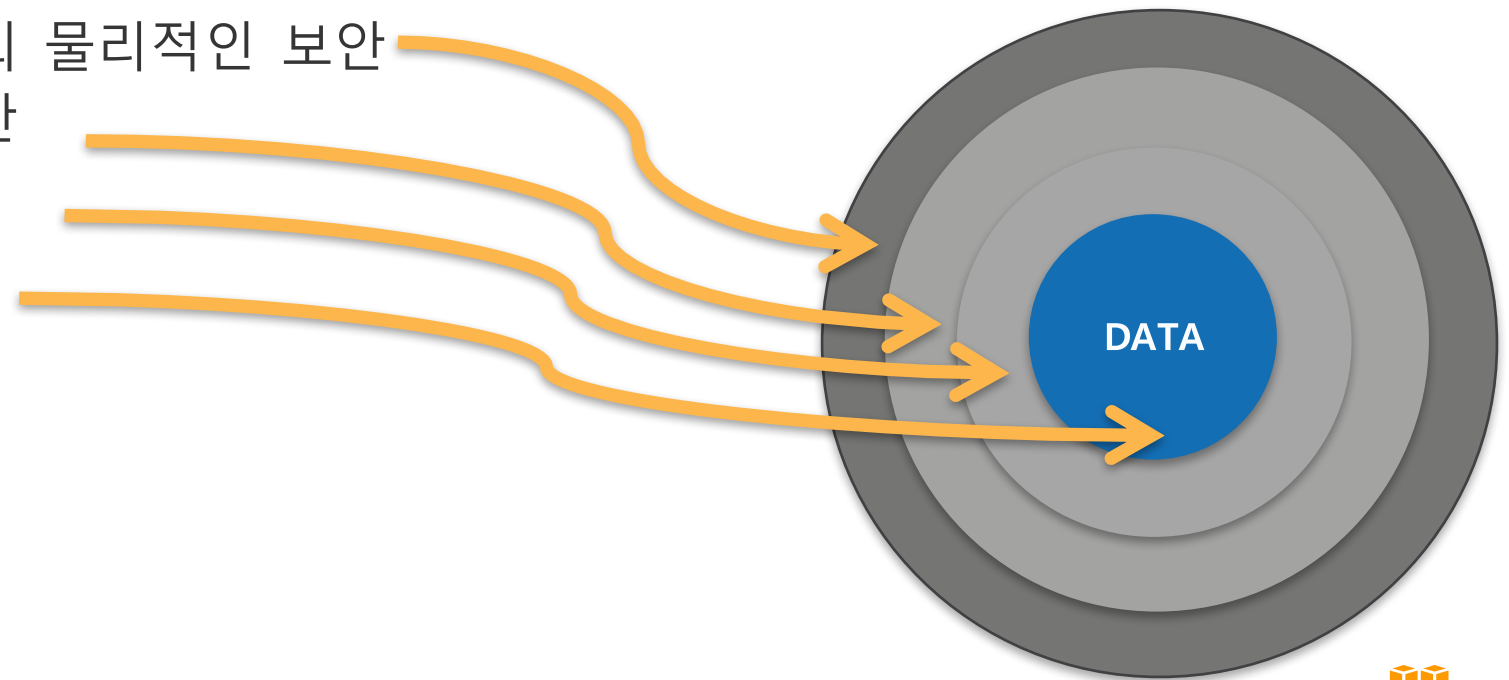
- 클라우드 보안
- AWS 책임 공유 모델
- 더 나은 가시성
- 더 나은 제어
- 더 나은 감사기능



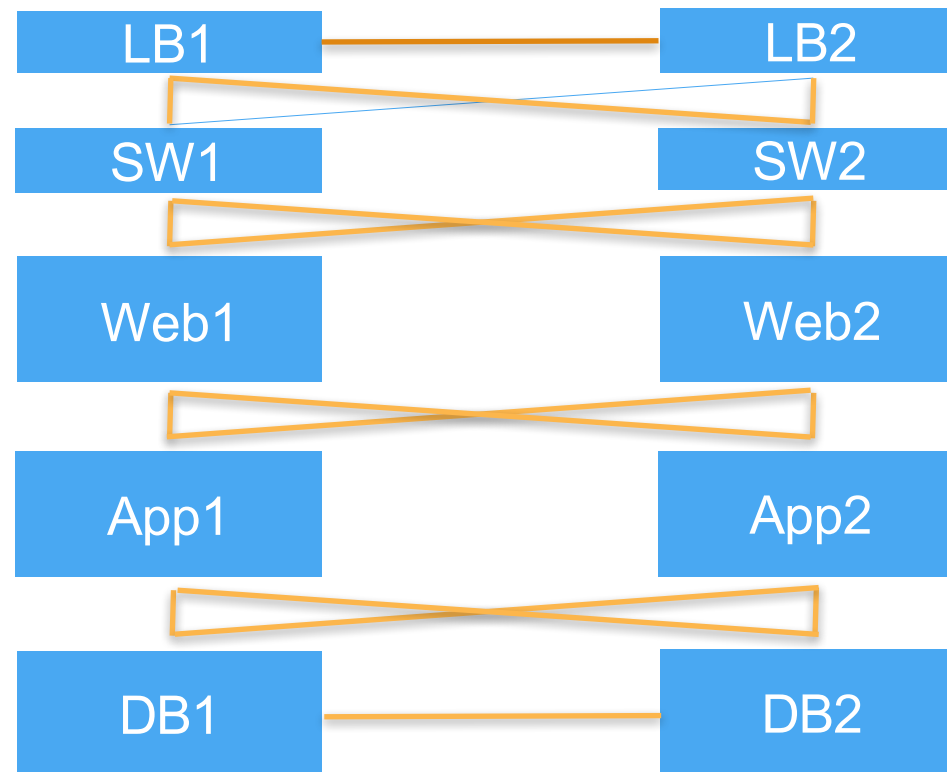
심층 방어

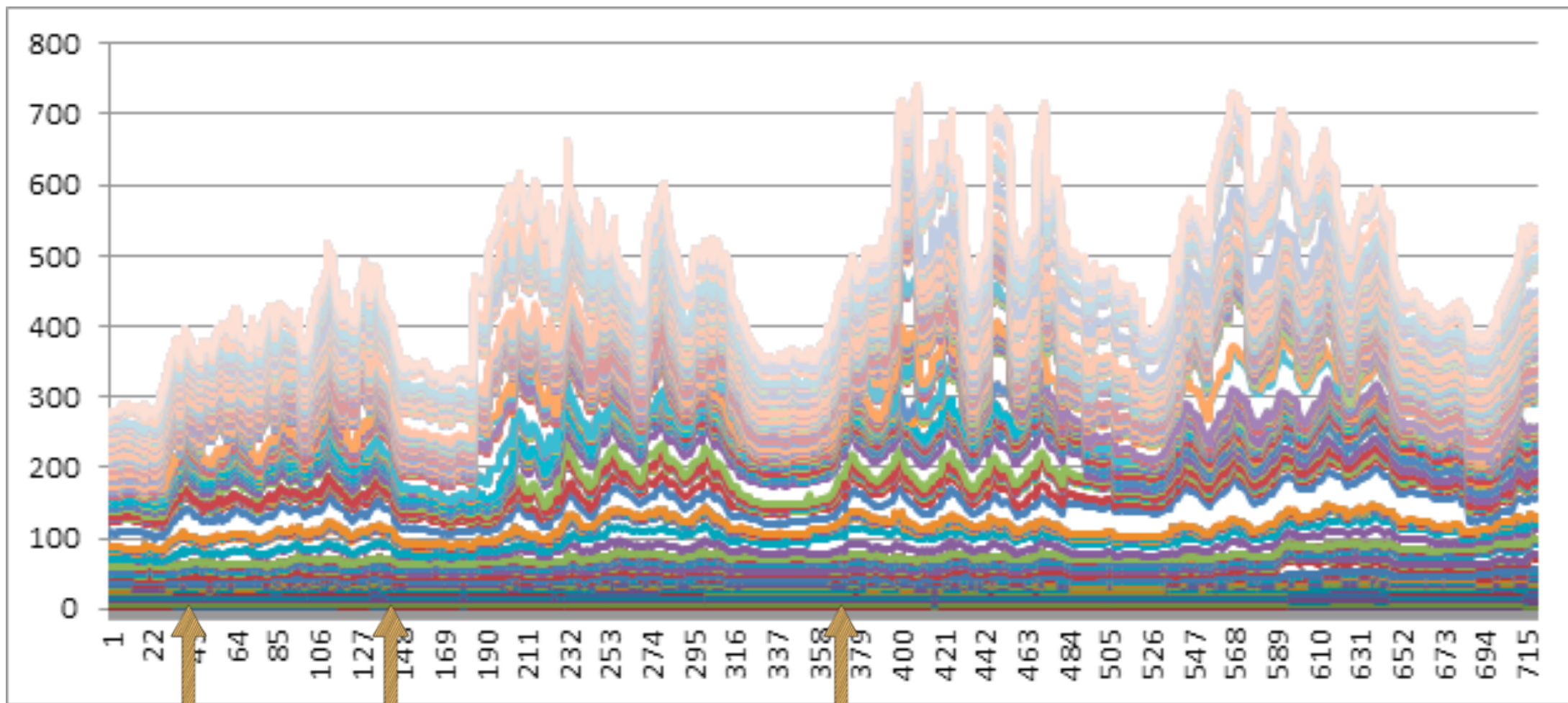
다 계층 보안

- 데이터 센터의 물리적인 보안
- 네트워크 보안
- 시스템 보안
- 데이터 보안



전통적인 방식 – 정적이고 고정적인 시스템





평균
HO
평균

평균
HO
평균

후가 시점의 평균

클라우드의 다이나믹한 환경을 전통적인 보안 접근방식으로 잘 방어할 수 있을까요?

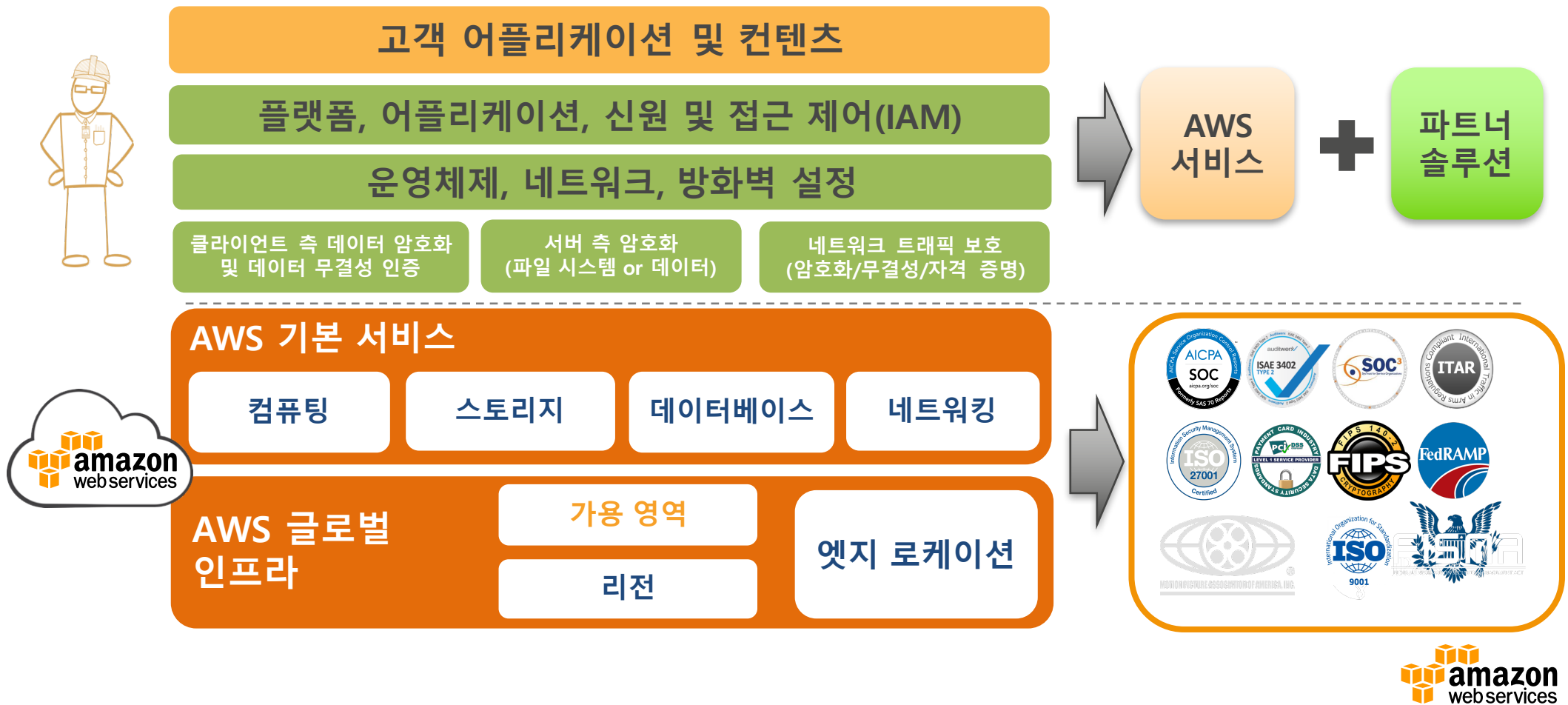


AWS는 클라우드에 최적화된 보안을 제공합니다.

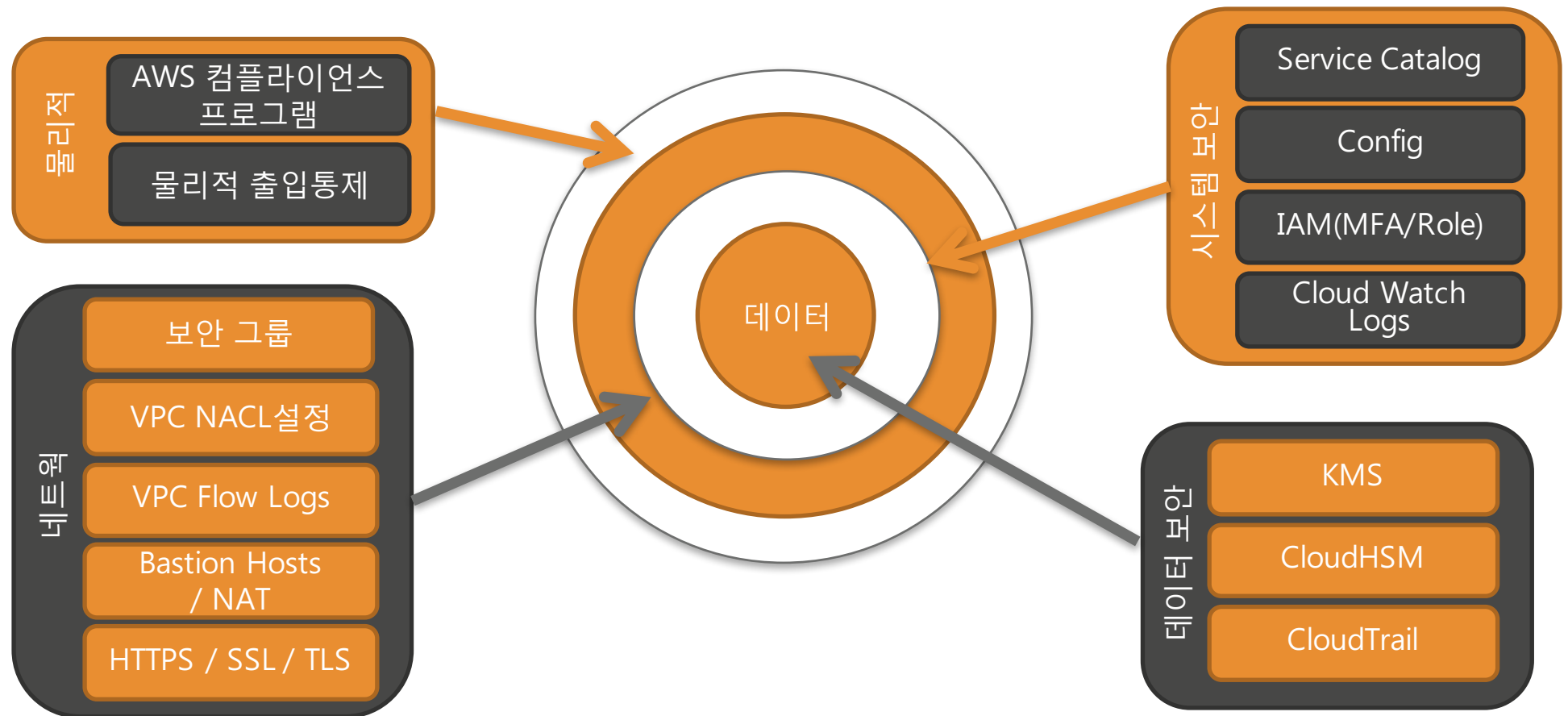


AWS와 고객이 보안을 함께 완성할 책임이 있습니다.

책임 공유 모델

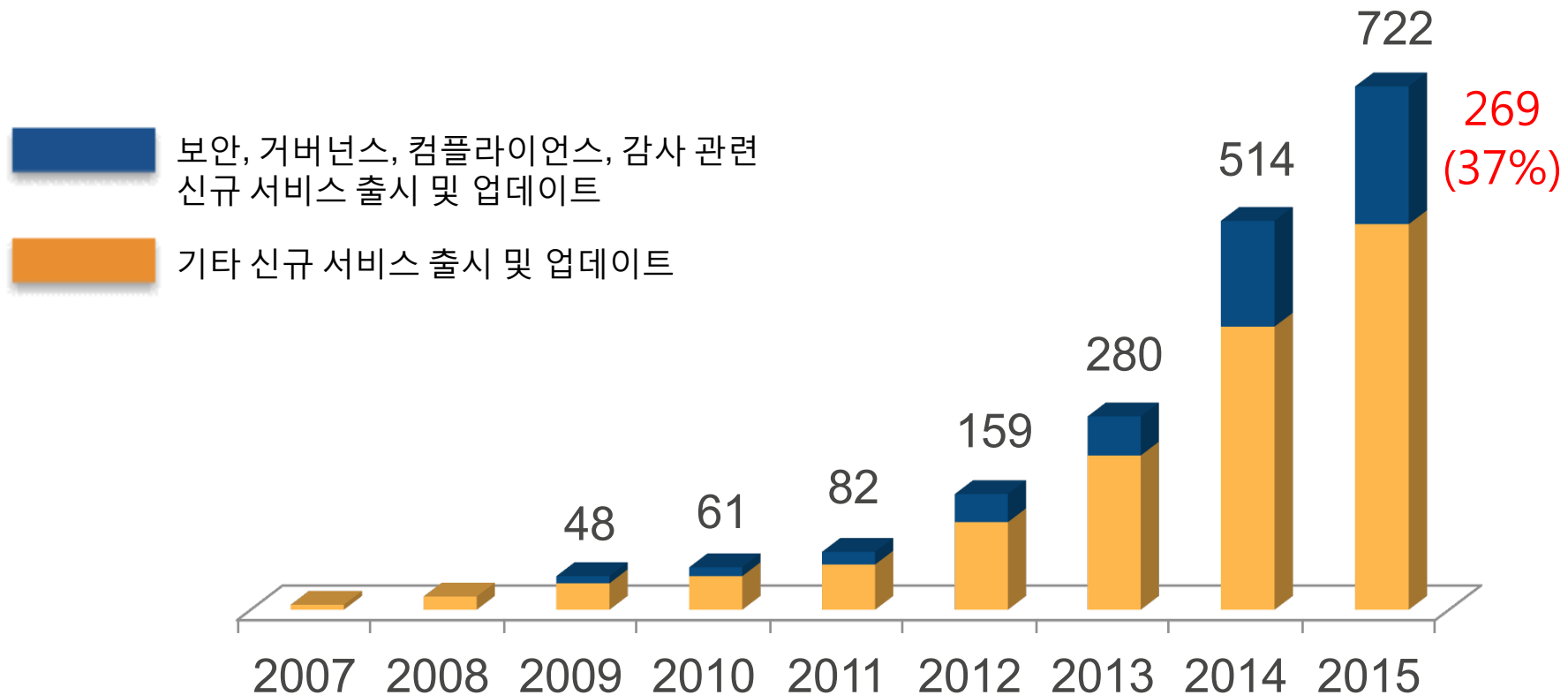


AWS 보안 기능들



보안은 AWS의 최우선 순위 과제입니다!

고객층의 증가와 더불어 더 나은 서비스 제공을 위해 **보안, 규제/감사, 거버넌스** 관련 다양한 업데이트를 빠르게 진행



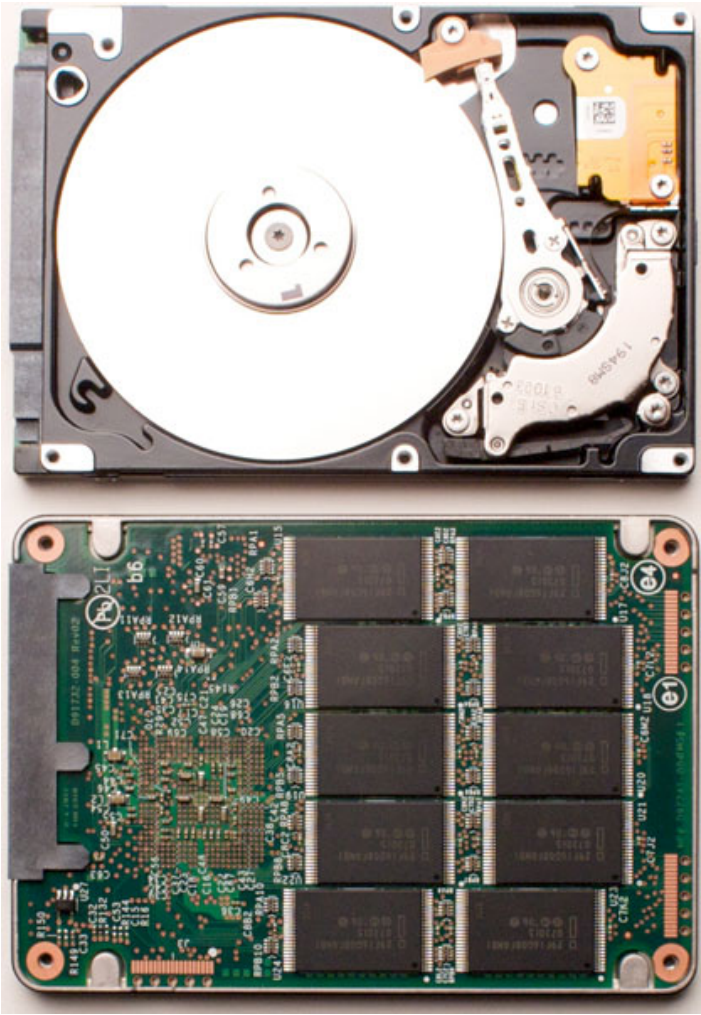
2015년에는 전년대비 40% 증가한, 722건의 새로운 서비스 및 기능을 출시

AWS는 주요 규제/표준/모범사례를 준수합니다.



규제/표준 준수 - 스토리지 보안

- 독자적인 스토리지 관리 기능으로 타인의 데이터 접근 완벽히 통제
- 사용전 디스크 청소(Disk Wiping)
- 데이터 저장 시 고객이 직접 암호화 적용 가능
- 산업표준에 따른 디스크 폐기 처리



이것이

이렇게



“우리의 경험을 바탕으로 보면,
AWS 클라우드가
우리의 데이터센터보다
더 안전할 수 있다고 생각합니다”

– Tom Soderstrom, CTO, NASA JPL

“AWS 의 보안은
여러분이 지금 수행하고 있는 것과
같은 **익숙함**을 제공하기 위해서
지속적으로 노력하고 있습니다.”

- **가시성**(Visibility)
- **제어**(Controllability)
- **감사 기능**(Auditability)

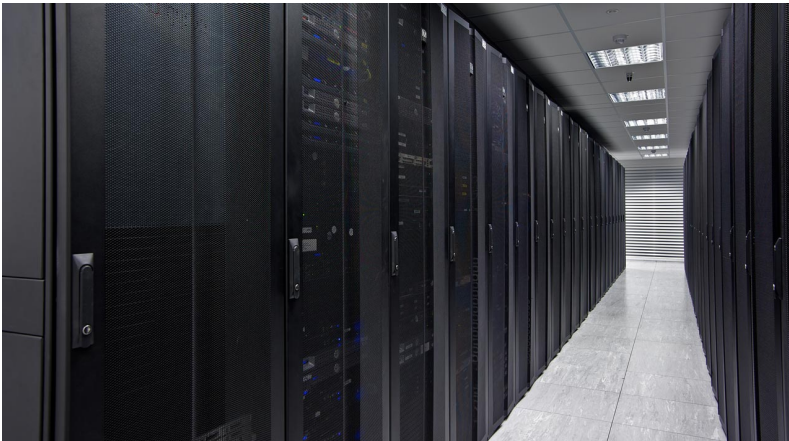
더 나은 **가시성**

(네트워크, 시스템, 감사)

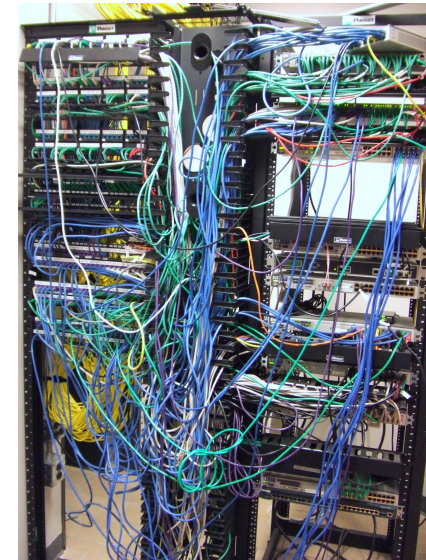
가시성: 보안의 기본 속성

여러분의 데이터 센터를 보면...

한눈에 전체의상황이 다 들어오는
것을 원하시겠지만,



보통 이런 그림을 보시게 됩니다.



가시

하지

-
-
-
-
-

Firefox

EC2 Management Console

https://console.aws.amazon.com/ec2/v2/home?region=eu-west-1#Instances:

Services Edit admin @ 670934762290 Ireland Help

EC2 Dashboard
Events
Tags

INSTANCES

- Instances
- Spot Requests
- Reserved Instances

IMAGES

- AMIs
- Bundle Tasks

ELASTIC BLOCK STORE

- Volumes
- Snapshots

NETWORK & SECURITY

- Security Groups
- Elastic IPs
- Placement Groups

Launch Instance Connect Actions

Filter: All instances All instance types Search Instances 1 to 4 of 4 Instances

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
git	i-157c445d	m1.small	eu-west-1b	running	2/2 check...	None
adrien	i-38ea8477	m1.medium	eu-west-1b	running	2/2 check...	None
mail	i-4e507502	t1.micro	eu-west-1a	running	2/2 check...	None
minecraft	i-bee14ef3	m1.large	eu-west-1c	running	2/2 check...	None

Instance: i-157c445d Public DNS: ec2-46-137-170-115.eu-west-1.compute.amazonaws.com

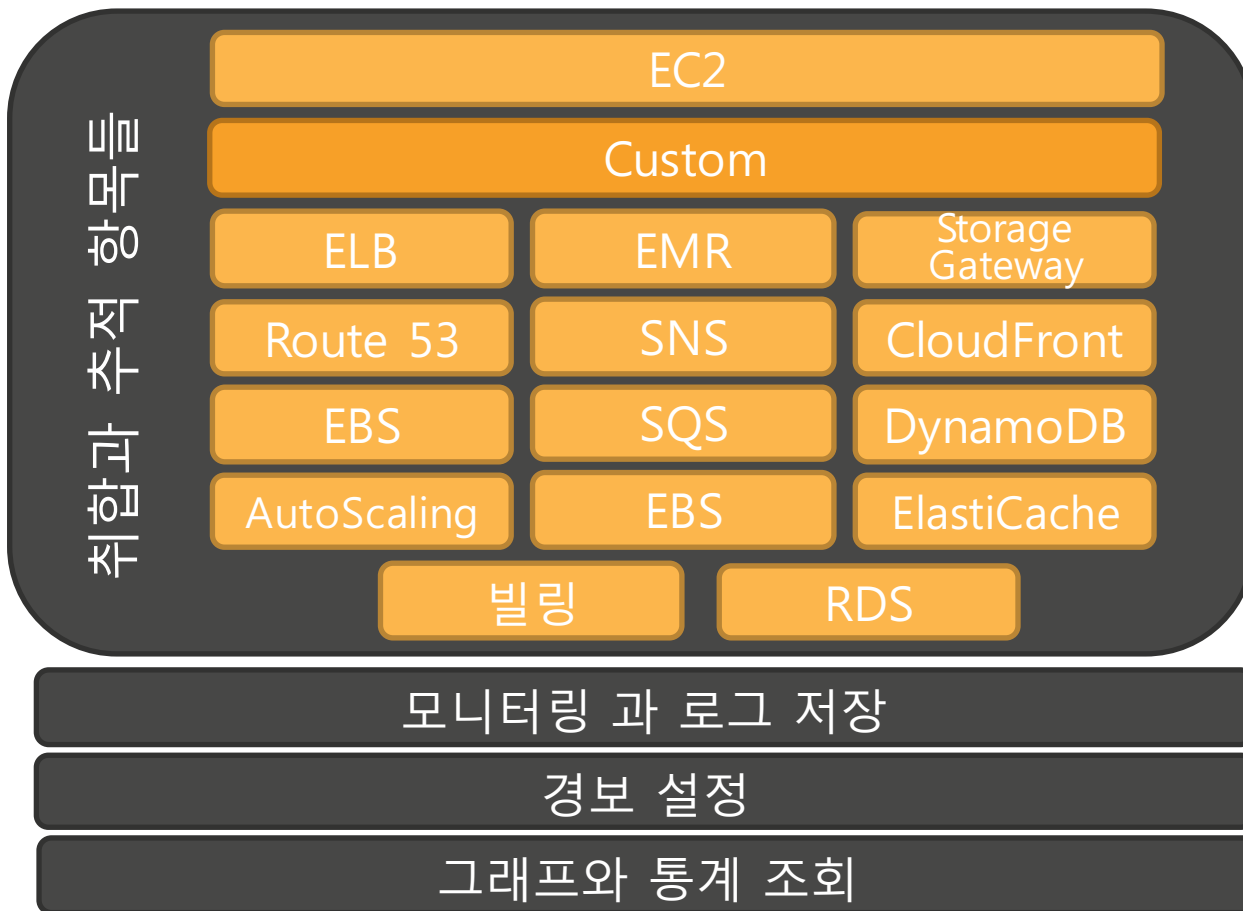
Description Status Checks Monitoring Tags

Instance ID	i-157c445d	Public DNS	ec2-46-137-170-115.eu-west-1.compute.amazonaws.com
Instance state	running	Elastic IP	46.137.170.115
Instance type	m1.small	Private DNS	ip-10-55-77-33.eu-west-1.compute.internal
Availability zone	eu-west-1b	Private IPs	10.55.77.33
Security groups	Git_Repository. view rules	Secondary private IPs	-
Scheduled events	No scheduled events	VPC ID	-

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Feedback

AWS CloudWatch

AWS 리소스와 AWS기반 어플리케이션에 대한 모니터링 서비스

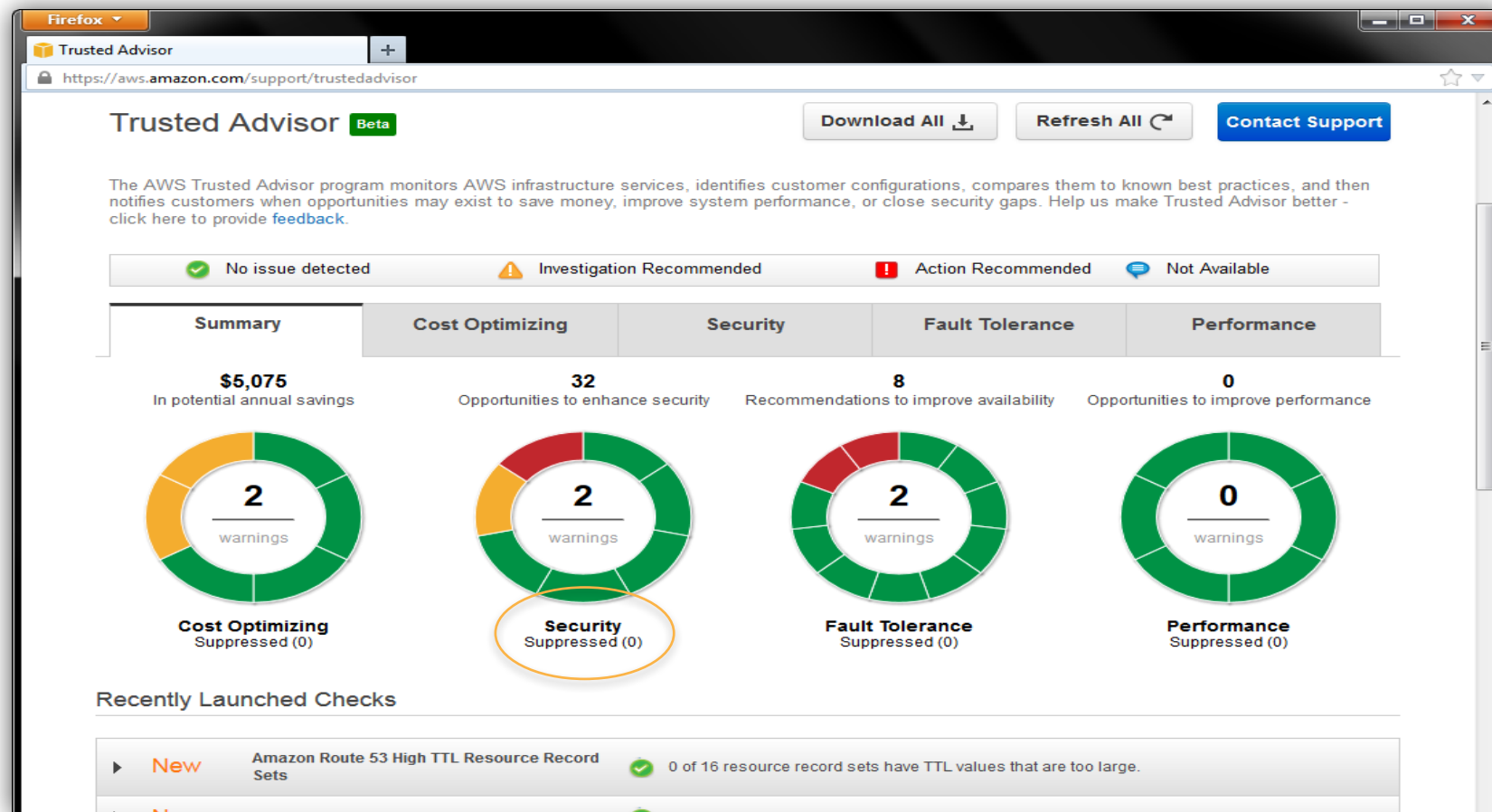


CloudWatch Logs로 모든 것을 모니터링

- **Amazon CloudWatch Logs**: EC2 인스턴스나 다른 자원에 대해서 시스템, 애플리케이션 및 커스텀 로그를 모니터링 할 수 있음. 예를들면;
- 웹 서버의 HTTP 로그 파일을 모니터링하고 에러(404 등)를 식별하기 위해 **CloudWatch Metrics**의 필터를 사용하여 지정된 기간 내에 발생 횟수를 카운트
- 404 에러의 횟수가 사전에 설정된 임계치에 도달하게 되면 **CloudWatch Alarms** 가 통지를 할 수 있음.
=> 문제의 원인을 파악하기 위해 자동으로 티켓을 생성하도록 사용 가능



AWS Trusted Advisor Security



The AWS Trusted Advisor program monitors AWS infrastructure services, identifies customer configurations, compares them to known best practices, and then notifies customers when opportunities may exist to save money, improve system performance, or close security gaps. Help us make Trusted Advisor better - [click here to provide feedback](#).



No issue detected



Investigation Recommended



Action Recommended



Not Available

Summary

Cost Optimizing

Security

Fault Tolerance

Performance

**Security Groups - Specific Ports Unrestricted**

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

[\(Show more\)](#)

▶ 12 of 71 security group rules allow unrestricted access to a specific port.

Updated: 2013-09-06 05:32 PDT

**Security Groups - Unrestricted Access**

Checks security groups for rules that allow unrestricted access to a resource.

[\(Show more\)](#)

▶ 20 of 71 security group rules have a source IP address with a /0 suffix.

Updated: 2013-09-06 06:06 PDT

**IAM Use**

Checks for your use of AWS Identity and Access Management (IAM).

[\(Show more\)](#)

At least one IAM user, group, or role has been created for this account.

Updated: 2013-09-06 05:57 PDT

**Amazon S3 Bucket Permissions**

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions.

[\(Show more\)](#)

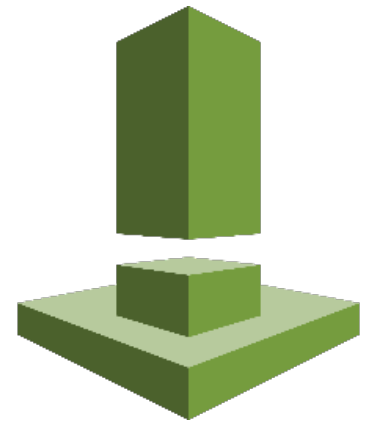
0 of 9 buckets have permission properties that grant global access.

Updated: 2013-09-06 05:32 PDT

**MFA on Root Account**

AWS Inspector

- Agent 기반 - 어플리케이션 보안 수준 진단
- 보안 진단 결과 – 가이드 제공
- API를 통한 자동화
- Rule Package
 - CVE (common vulnerabilities and exposures) – 수천개 항목
 - Network security best practices – 4개 항목
 - Authentication best practices – 9개 항목
 - Operating system security best practices – 4개 항목
 - Application security best practices – 2개 항목
 - PCI DSS 3.0 readiness – 25개 항목



더 나은 제어

(데이터, 사용자, 네트워크)

컴퓨팅과 스토리지의 위치를 고객이 직접 선택 가능



퍼스트 클래스 보안 및 규정준수는
암호화로 시작됩니다
(그리고 끝나지 않습니다!)

Encryption - 전송중 / 저장시 암호화



전송 중 암호화

HTTPS

SSH

SSL/TLS

VPN

Object

저장 시 암호화

Object

Database

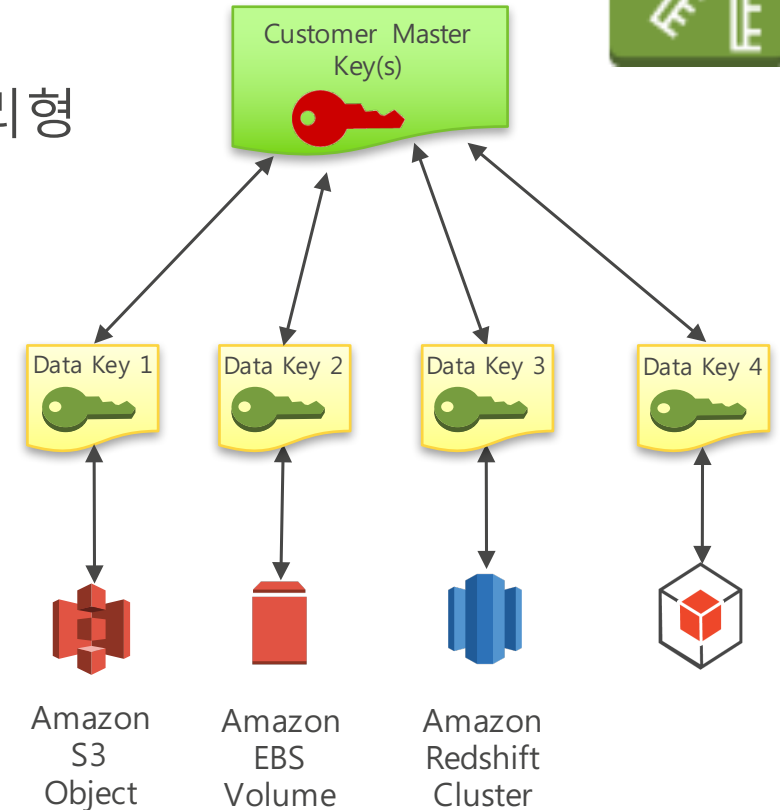
Filesystem

Disk

자세한 정보가 담긴 백서, ["Securing Data at Rest with Encryption"](#).

AWS KMS - 암호화키 생성/보관/관리

- 암호화키를 안전하게 생성/보관/관리 해주는 관리형 서비스
- 중앙 집중 암호화 키 관리:



자세한 내용을 담고 있는 백서: [KMS Cryptographic Details](#).

다양한 AWS 서비스들과 통합



CLUSTER DETAILS

NODE CONFIGURATION

ADDITIONAL CONFIGURATION

REVIEW

default.redshift-1.0 ▼

Parameter group to associate with this cluster.

☐ None ☒ KMS ☐ HSM

[Learn more about database encryption](#)

CriticalData ▼



Protects critical data in my applications

This account ()



AWS Key Management Service

Integrated with Amazon EBS

Create Volume ✕

Type ⓘ
Size (GiB) ⓘ
IOPS ⓘ

General Purpose (SSD) ▼
100 (Min: 1GiB, Max: 1024GiB)
300 / 3000 (3000 IOPS bursts and baseline of 3 IOPS per GB)

Availability Zone ⓘ
Snapshot ID ⓘ

us-east-1b ▼
Search (case-insensitive)

Encryption ⓘ
Master Key ⓘ

☒ Encrypt this volume
CriticalData ▼

Key Details

Description
Account
KMS Key ID

This key protects critical data in my account
This account (██████████)
██████████-a0ec-33d40cac295

Cancel Create

USER에 대한 더 나은 제어

AWS Identity and Access Management (IAM)

AWS서비스와 리소스에 대한 안전한 접근 통제.

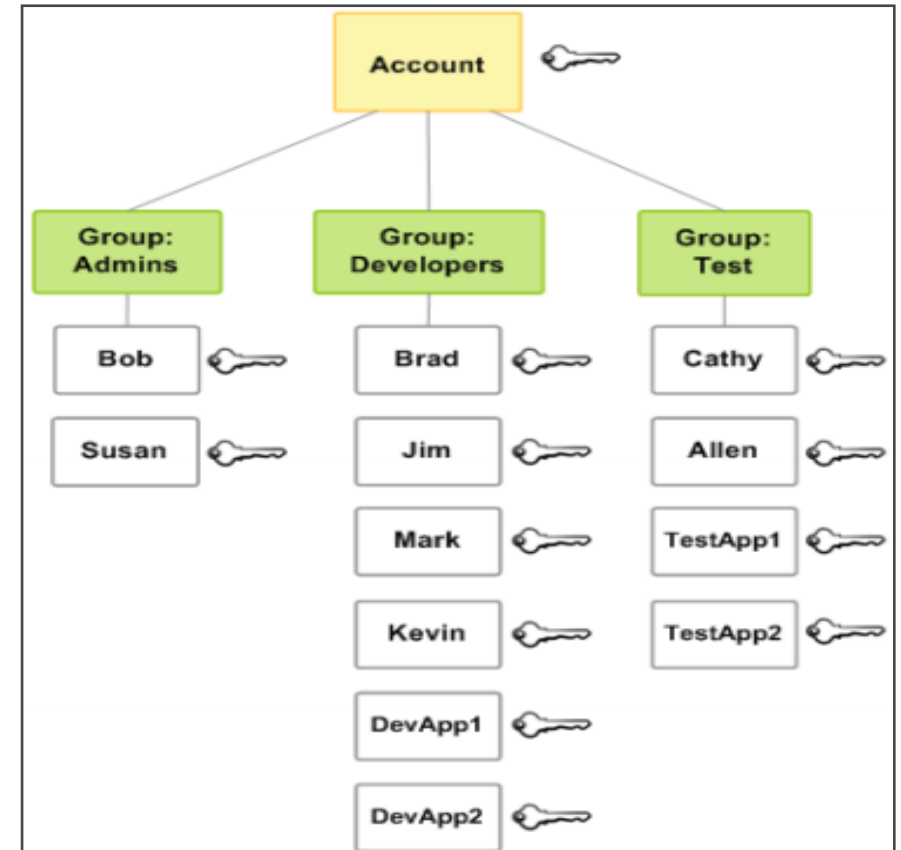
사용자 이름 /
사용자

사용자 그룹
관리

중앙화된 접근
제어 관리

계정에서 누가 무엇을 할 수 있는지 제어

- 사용자, 그룹, 롤(Role) 및 권한
- 제어
 - 중앙집중식
 - 잘 갖춰진 – APIs, 자원 및 AWS 관리 콘솔
- 보안
 - 기본적으로 안전함(거부 규칙)
 - 다중 사용자, 개별 보안 신원 및 권한



Firefox

IAM Management Console

https://console.aws.amazon.com/iam/home?region=eu-west-1#users

admin@670934762290 Global Help

Services Edit

Dashboard

Create New Users User Actions

Details

Groups

Users

Roles

Password Policy

Manage User Permissions

Cancel

Set Permissions

Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.

☒ **Select Policy Template**

and groups.

- Read Only Access**
Provides read-only access to AWS services and resources. **Select**
- AWS CloudFormation Read Only Access**
Provides access to AWS CloudFormation via the AWS Management Console. **Select**
- CloudFront Full Access**
Provides full access to the CloudFront console plus the ability to list Amazon S3 buckets via the AWS Management Console. **Select**

☐ **Policy Generator**

☐ **Custom Policy**

Group Policies

There are no group policies attached to this user.

Creation Time

2012-11-04 11:33 UTC+0200
2013-10-15 21:37 UTC+0300
2013-07-11 16:49 UTC+0300
2013-10-07 10:40 UTC+0300

User belongs to.

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Feedback

amazon web services

NETWORK에 대한 더 나은 제어

AWS Cloud 내에 격리된 사설 네트워크를 생성

AWS

VPC

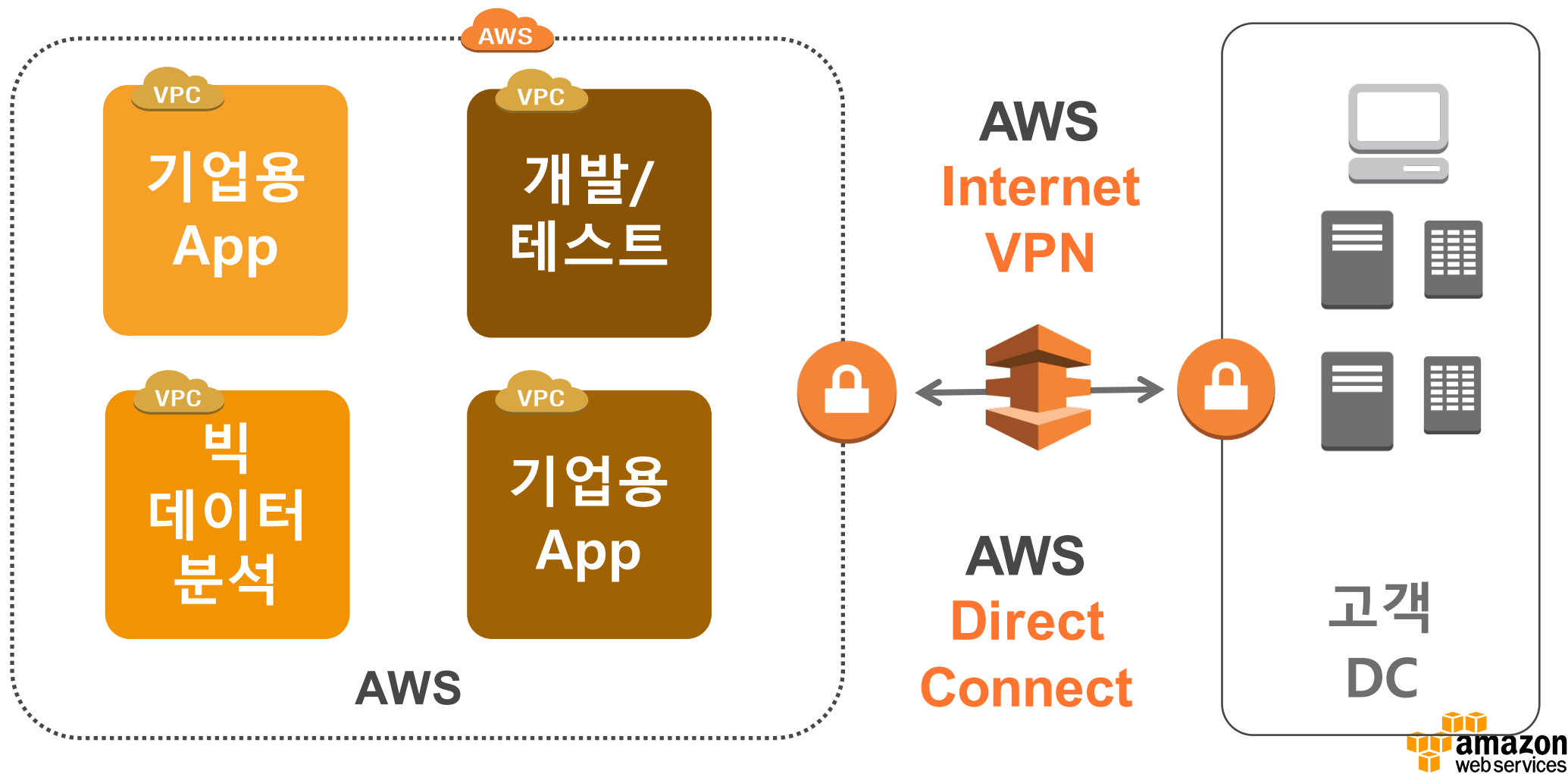
AWS Virtual Private Cloud

- 논리적으로 분리된 일종의 가상 사설망을 제공
- VPC상에서 사설 IP대역을 선택
- 적절하게 서브네팅하고 EC2 인스턴스를 배치

AWS network security

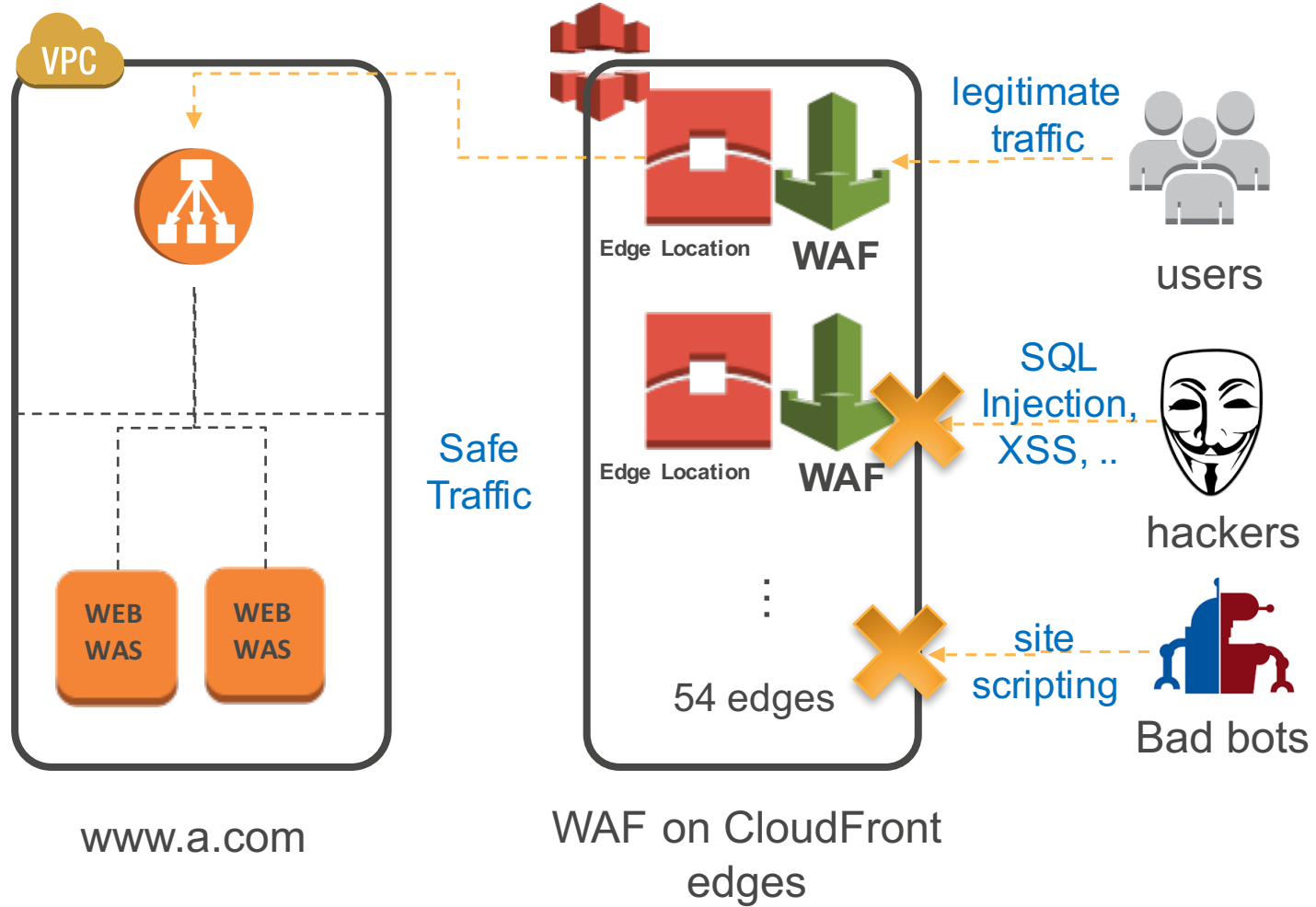
- AWS 는 IP Spoofing과 같은 레이어 2 공격 차단
- 소유하지 않은 EC2인스턴스에 대한 스니핑 불가
- 외부와의 모든 라우팅과 연결을 통제

기존 데이터 센터에 안전하게 연결



AWS WAF

웹방화벽



더 나은 감사기능

(컴플라이언스, 히스토리, 로그)

감사 증적

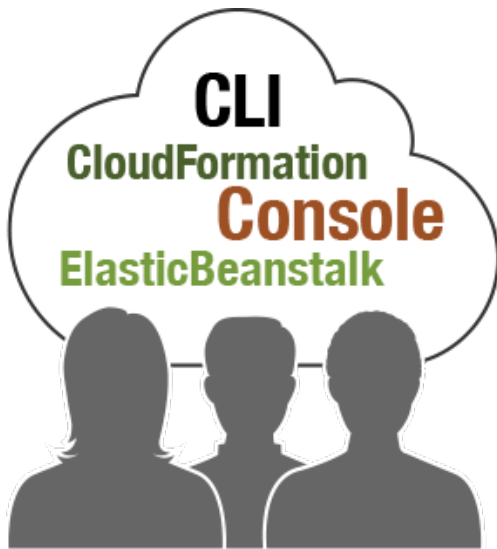
- 많은 수의 컴플라이언스 감사작업에서 **임의 시간**에 시스템상태에 대한 접근을 필요 (i.e., PCI, HIPAA)
- 모든 리소스와 그것들의 구성정보에 대한 **완벽한** 인벤토리는 어떤 순간에도 활용 가능해야 한다.



But what does a jellyfish have to do with compliance?

AWS CloudTrail

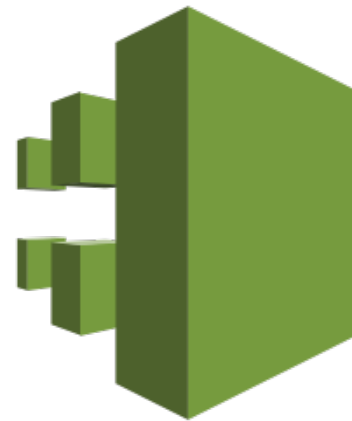
AWS상의 모든 관리작업에 대한 로깅



모든 작업은 API
콜로 처리됨...



사용하는 서비스와
인스턴스들이 늘어
남에 따라 ...

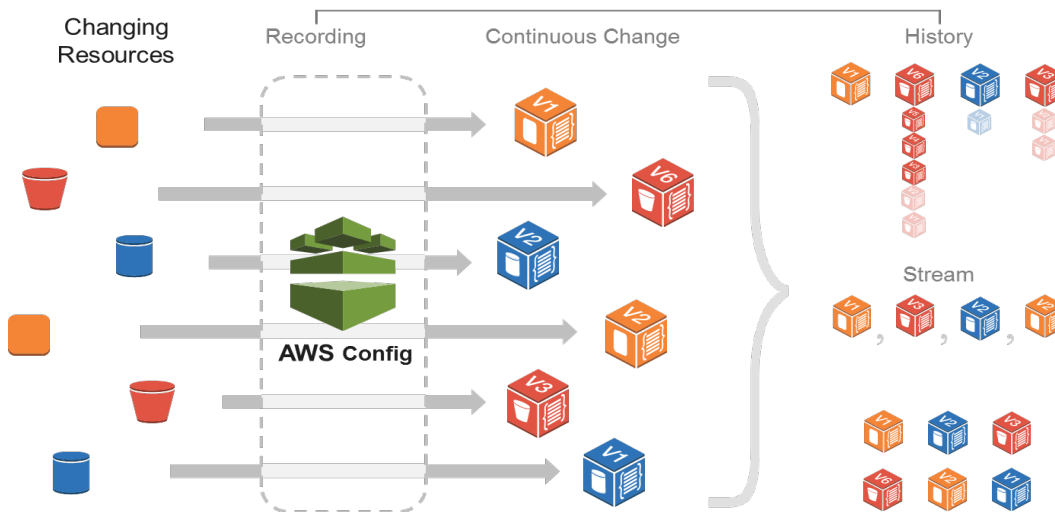


CloudTrail은
계속해서 모든
API 요청들에
대해 신뢰성 있는
기록을 수행...

User	Action	Time
Tim	Created	1:30pm
Sue	Deleted	2:40pm
Kat	Created	3:30pm

AWS Config

AWS리소스에 대한 **인벤토리** 관리와 **구성정보** 변경관리 및 통보(AWS SNS)



보안 분석: 나는 안전한가요?

규정 감사: 어디에 증거가 있나요?

변경 관리: 이 변경에 대한 영향은?

문제 해결: 무엇이 변경되었나요?

보안 분석

감사
컴플라이언스

변경 관리

Troubleshooting

Discovery

필요에 따라 네트워크/보안 관련 다양한 솔루션들을 선택하실 수 있습니다.

인프라 보안

로그 모니터링

계정 및 접근제어

구성 및 취약점 제어

데이터 보호



SaaS



M-Pin SSO
Authentication
for Enterprises



SaaS



SaaS



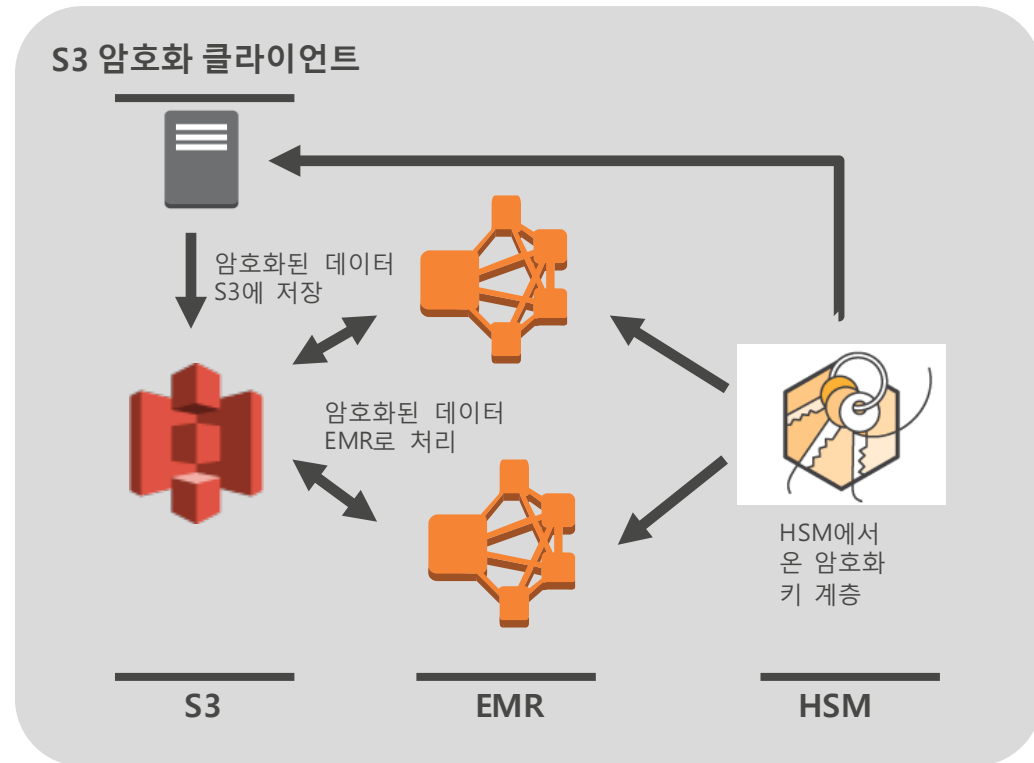
더 이상 보안은
클라우드 도입을 가로막는
걸림돌이 아닙니다!



사례 연구 : 암호화 기반의 빅 데이터 분석

"나스닥 그룹은 클라우드 도입 이후 아마존 Redshift를 사용하기 때문에 매우 만족하고 있다. 현재, 매일 우리가 아마존 Redshift에 55 억 행 데이터가 처리 되고 있습니다."

-- Nate Simmons,
Principal Architect



EMR 이용시에만 암호 해독

<http://aws.amazon.com/cn/solutions/case-studies/nasdaq-fincloud/>
<http://aws.amazon.com/solutions/case-studies/nasdaq-omx/>



AWS 보안 센터

다양한 보안 정보 및 문서를 제공하는 AWS 보안 포털: <http://aws.amazon.com/security>

보안 백서

- 보안 프로세스 소개
- AWS 리스크 및 컴플라이언
- AWS 보안 베스트 프랙티스

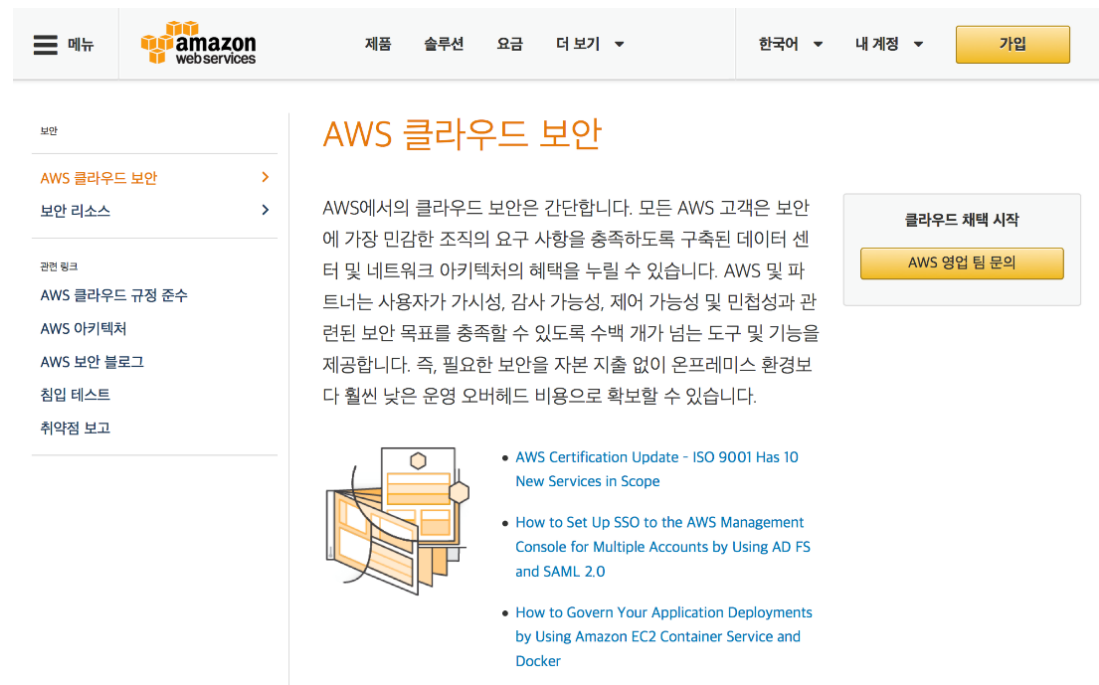
보안 리소스

취약점 리포팅

침해 테스트
신청 절차

수상한 이메일
신고

보안 게시판



The screenshot shows the AWS Security Center homepage. At the top is the AWS logo and navigation links for '제품' (Products), '솔루션' (Solutions), '요금' (Pricing), and '더 보기' (More). There are also links for '한국어' (Korean), '내 계정' (My Account), and a '가입' (Sign Up) button. The main content area is titled 'AWS 클라우드 보안' (AWS Cloud Security). It includes a paragraph explaining that AWS Cloud Security is simple and helps meet the requirements of the most sensitive organizations. Below this, there are two columns of links. The left column lists '보안' (Security), 'AWS 클라우드 보안' (AWS Cloud Security), '보안 리소스' (Security Resources), '관련 링크' (Related Links), 'AWS 클라우드 규정 준수' (AWS Cloud Compliance), 'AWS 아키텍처' (AWS Architecture), 'AWS 보안 블로그' (AWS Security Blog), '침입 테스트' (Penetration Testing), and '취약점 보고' (Vulnerability Reporting). The right column lists 'AWS Certification Update - ISO 9001 Has 10 New Services in Scope', 'How to Set Up SSO to the AWS Management Console for Multiple Accounts by Using AD FS and SAML 2.0', and 'How to Govern Your Application Deployments by Using Amazon EC2 Container Service and Docker'. There is also a '클라우드 채택 시작' (Get Started with Cloud) button and an 'AWS 영업 팀 문의' (Contact AWS Sales Team) button.

보안

AWS 클라우드 보안 >

보안 리소스 >

관련 링크

AWS 클라우드 규정 준수

AWS 아키텍처

AWS 보안 블로그

침입 테스트

취약점 보고

AWS 클라우드 보안

AWS에서의 클라우드 보안은 간단합니다. 모든 AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다. AWS 및 파트너는 사용자가 가시성, 감사 가능성, 제어 가능성 및 민첩성과 관련된 보안 목표를 충족할 수 있도록 수백 개가 넘는 도구 및 기능을 제공합니다. 즉, 필요한 보안을 자본 지출 없이 온프레미스 환경보다 훨씬 낮은 운영 오버헤드 비용으로 확보할 수 있습니다.

클라우드 채택 시작

AWS 영업 팀 문의

- [AWS Certification Update - ISO 9001 Has 10 New Services in Scope](#)
- [How to Set Up SSO to the AWS Management Console for Multiple Accounts by Using AD FS and SAML 2.0](#)
- [How to Govern Your Application Deployments by Using Amazon EC2 Container Service and Docker](#)

보안 리소스 및 블로그

AWS 보안 리소스

개발자
정보

기고문 +
튜토리얼

보안 제품

백서

보안 리소스, 교육, 도구들에 대한 광범위한 소개:

<http://aws.amazon.com/security/security-resources/>

AWS 보안 블로그

AWS보안 및 컴플라이언스와 관련된 최신 정보를 제공:

<http://blogs.aws.amazon.com/security/>

<https://aws-preview.aka.amazon.com/ko/blogs/korea/>

이제는 **보안**과 **규제준수**가
클라우드를 도입하는
중요한 이유가 되고 있습니다!

다음 시간에는...

- AWS IAM 및 AccessKey 제어 실습
- AWS CloudFront 실습
- AWS WAF 실습