글로벌 클라우드 금융서비스와 정보보호 전략

아마존 웹서비스
신 용 녀 이사

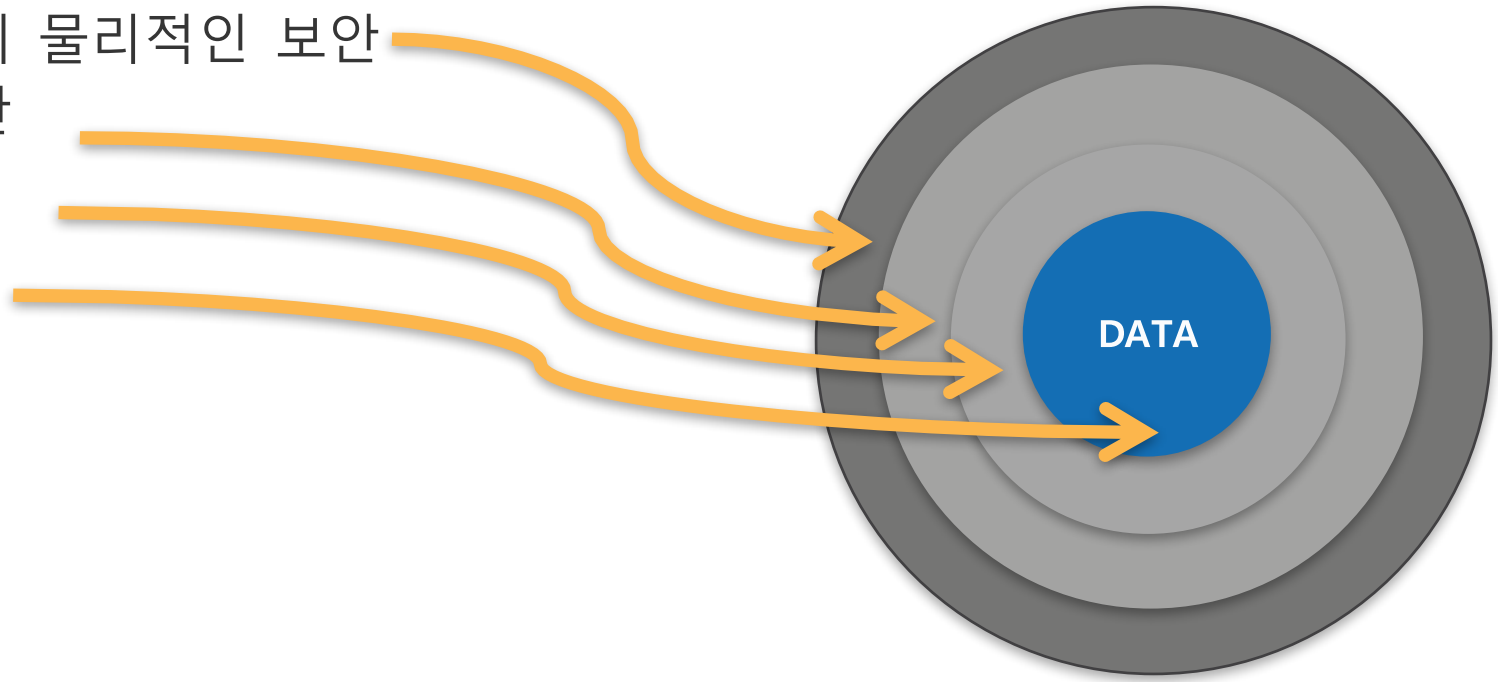
목 차

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

전통적인 방식 – 정적이고 고정적인 시스템

다 계층 보안

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

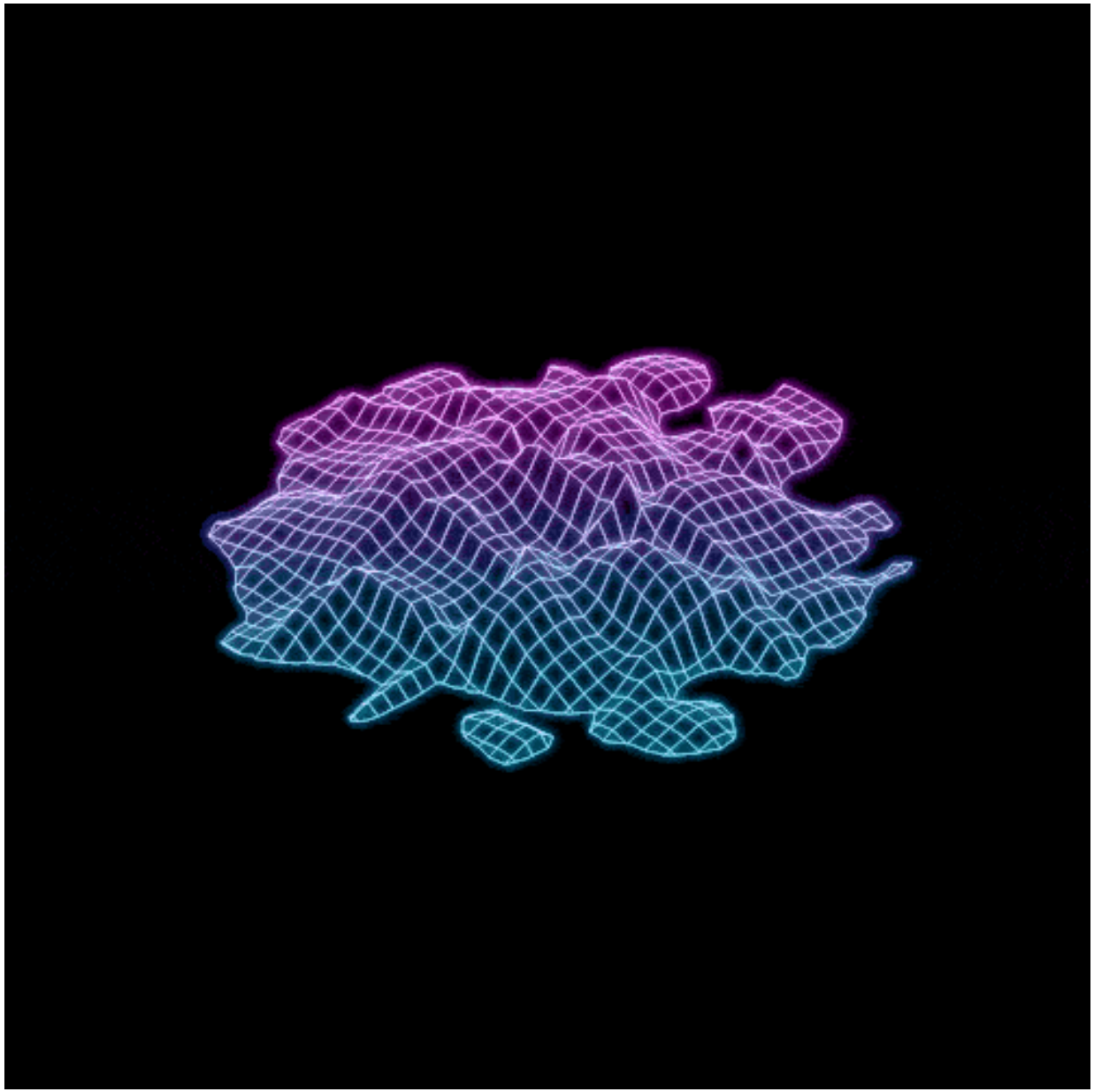


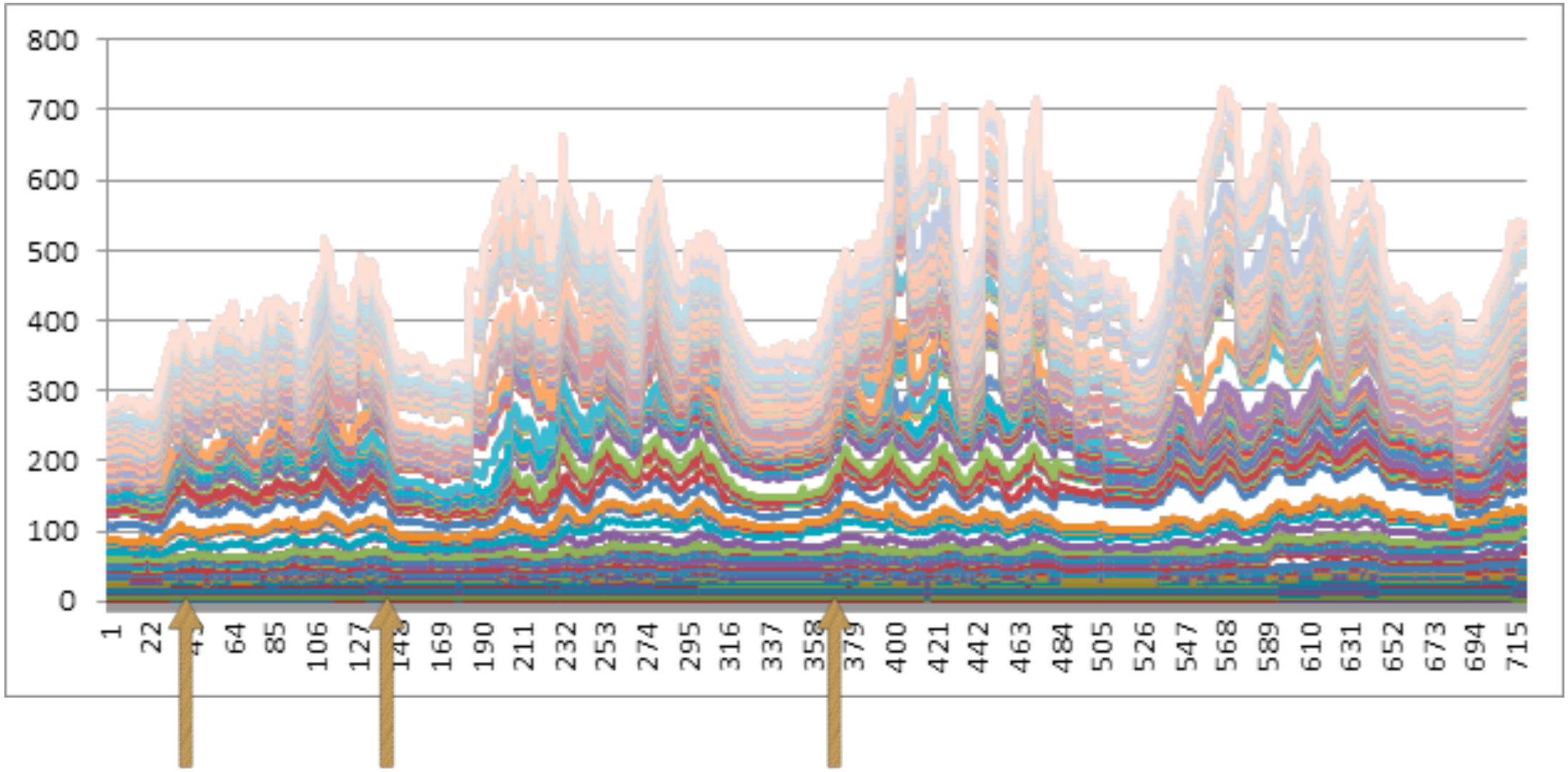
“Cloud applications have amorphous, polymorphic attack surfaces.”

- Jason Chan

Director of Engineering, Cloud Security

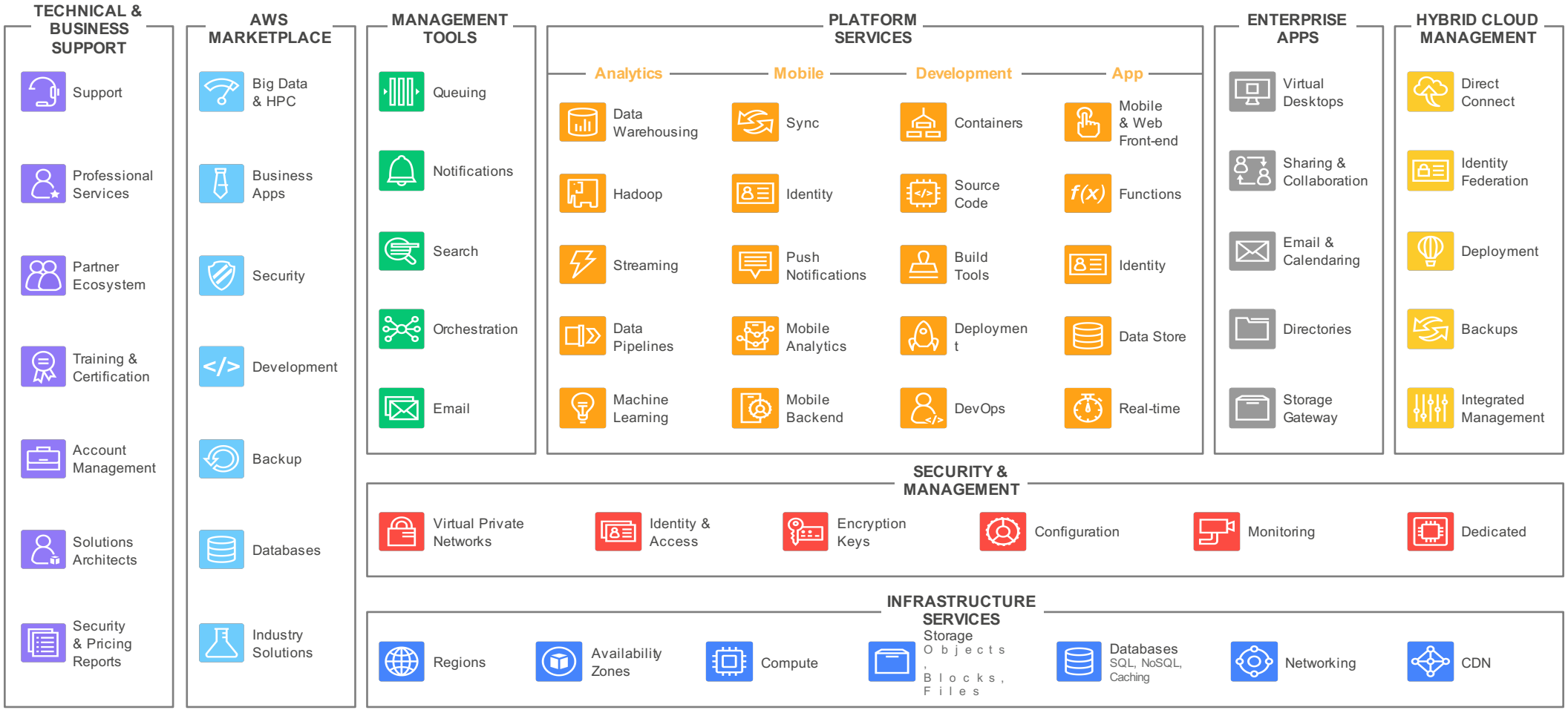
Netflix



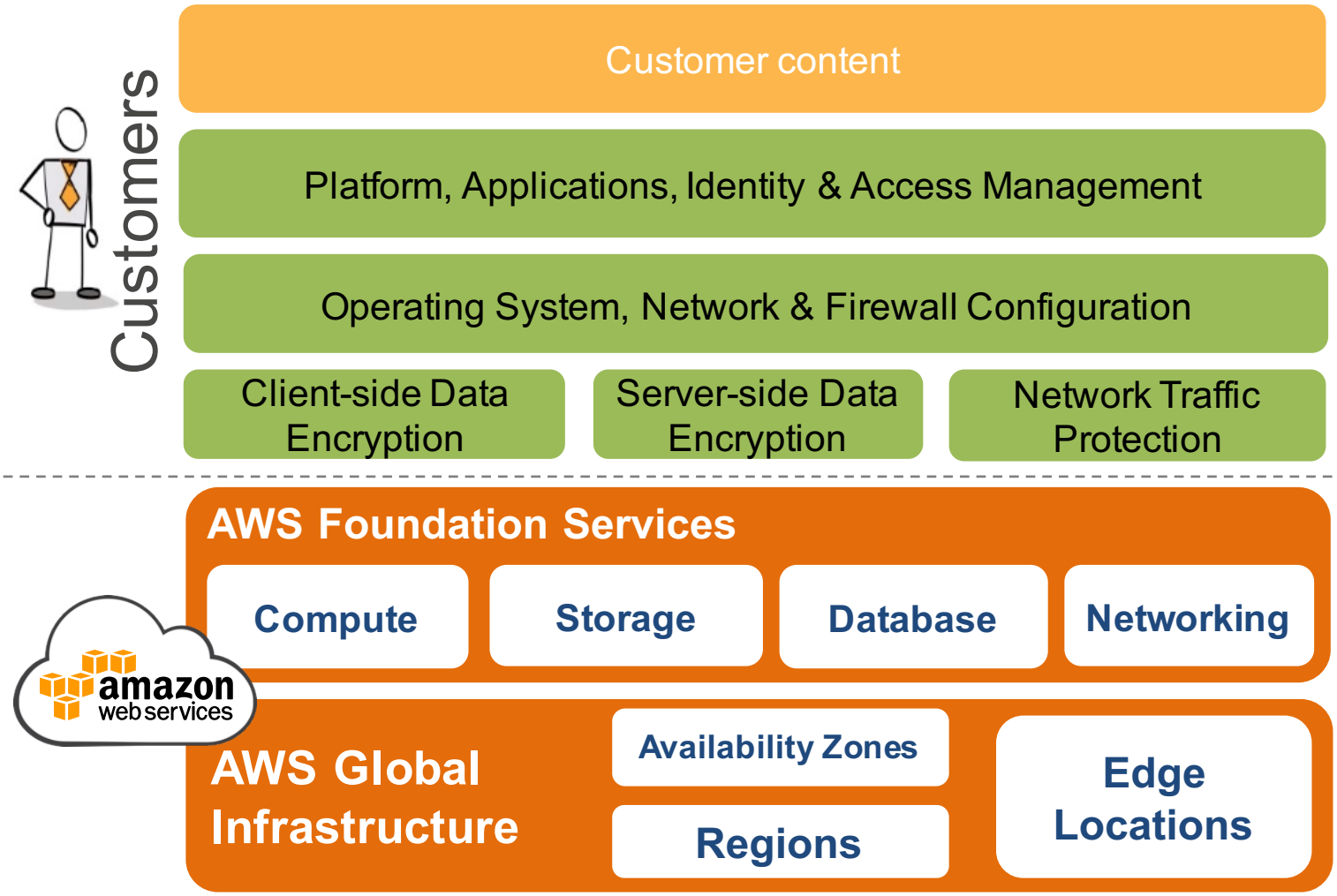

800
700
600
500
400
300
200
100
0
1
22
64
85
106
127
169
190
211
232
253
274
295
316
337
400
421
442
463
484
505
526
547
568
589
610
631
652
673
694
715
월요일
금요일
휴가 시즌의 끝

클라우드의 다이나믹한 환경을 전통적인 보안 접근방식으로 잘 방어할 수 있을까요?

폭 넓은 AWS 클라우드 서비스



AWS와 고객이 보안에 대한 책임 분담



Customers are responsible for their security **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

모든 고객은 동일한 AWS 보안 기초위에...

Customers

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption | Server-side Data Encryption | Network Traffic Protection

Customers are responsible for their security **IN** the Cloud

---

amazon web services

AICPA SOC

ISAE 3402 TYPE 2

PCI DSS LEVEL 1 SERVICE PROVIDER

FIPS 140-2 CRYPTOGRAPHY

HIPAA

ISO

ITAR

FedRAMP

MOTION PICTURE ASSOCIATION OF AMERICA

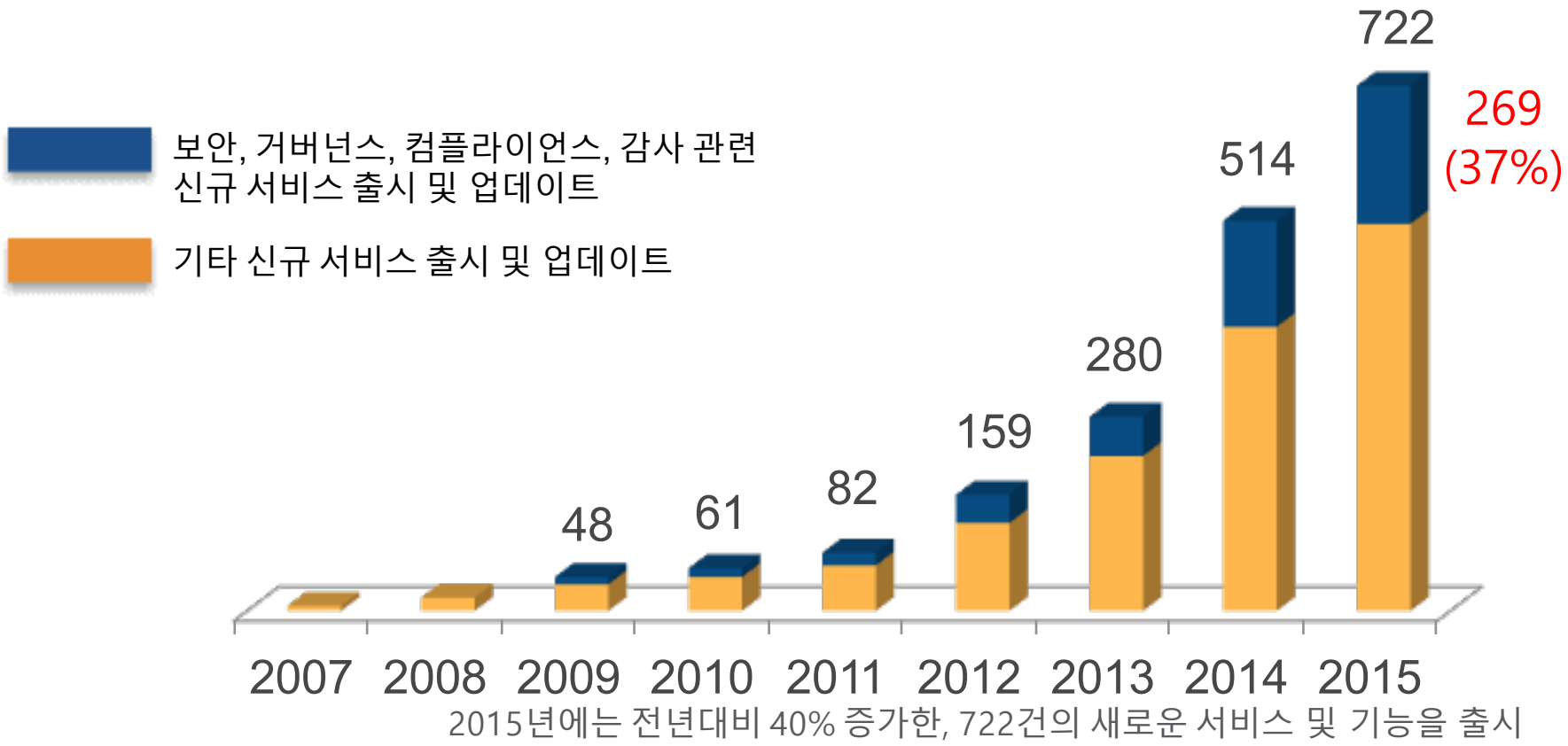
FISMA

Independent validation by experts

- Every AWS Region is in scope
- SOC 1 (SSAE 16 & ISAE 3402) Type II
- SOC 2 Type II and public SOC 3 report
- ISO 27001 Certification
- Certified PCI DSS Level 1 Service Provider
- FedRAMP Certification, HIPAA capable

보안은 AWS의 최우선 순위 과제입니다!

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



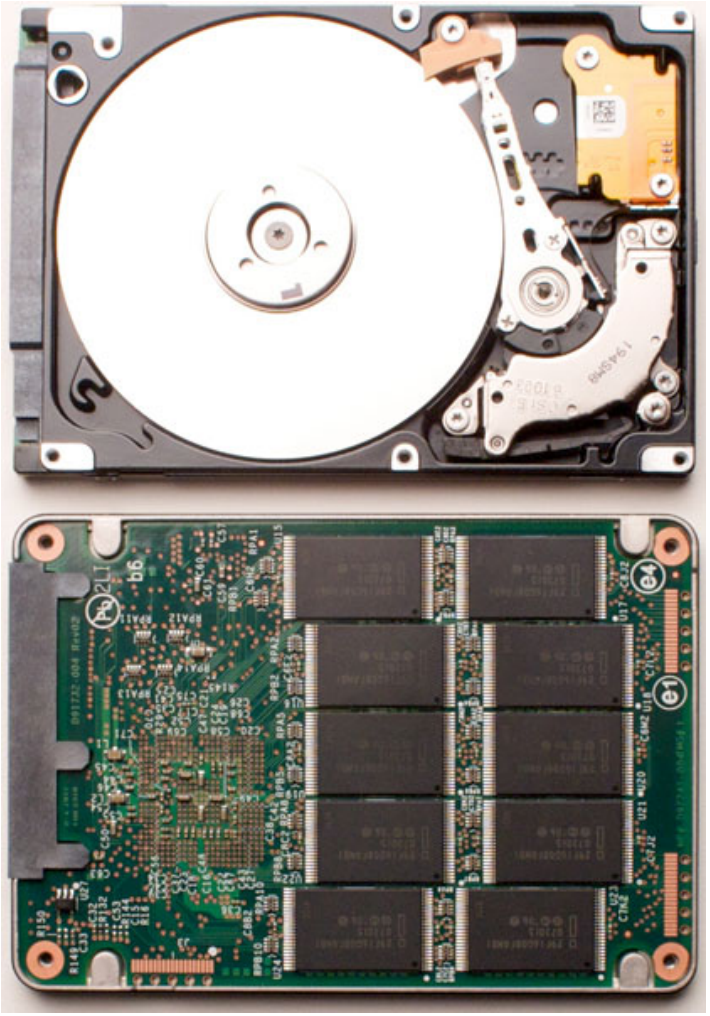
2015년에는 전년대비 40% 증가한, 722건의 새로운 서비스 및 기능을 출시

AWS는 주요 규제/표준/모범사례를 준수합니다.

보안 기준을 **지속적으로 개선하기** 위해서 모든 것을 구축합니다

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
같은익숙함을 제공하기 위해서
지속적으로 노력하고 있습니다."

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

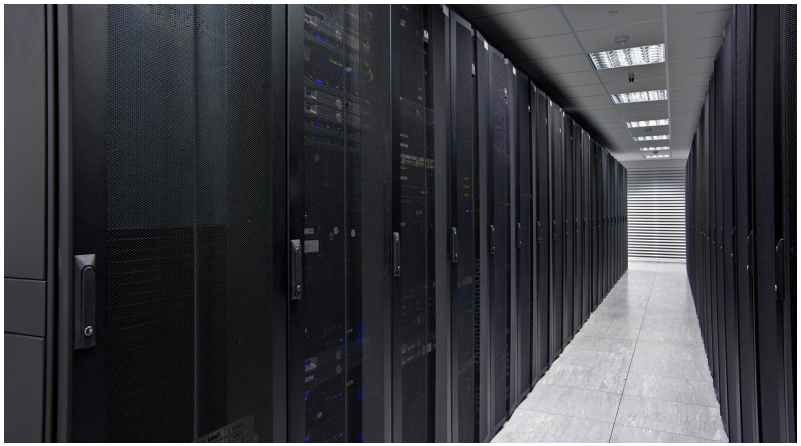
더 나은 가시성
(네트워크, 시스템, 감사)

amazon web services

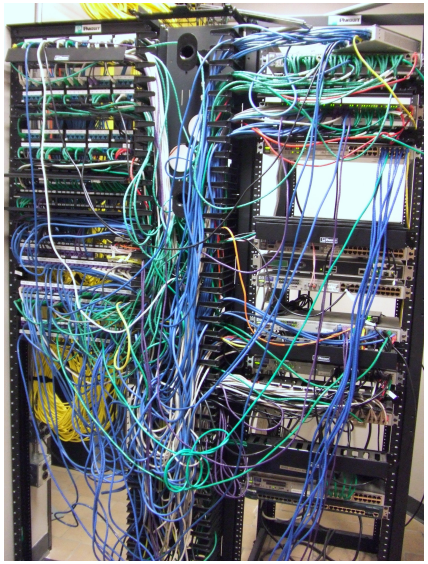
가시성: 보안의 기본 속성

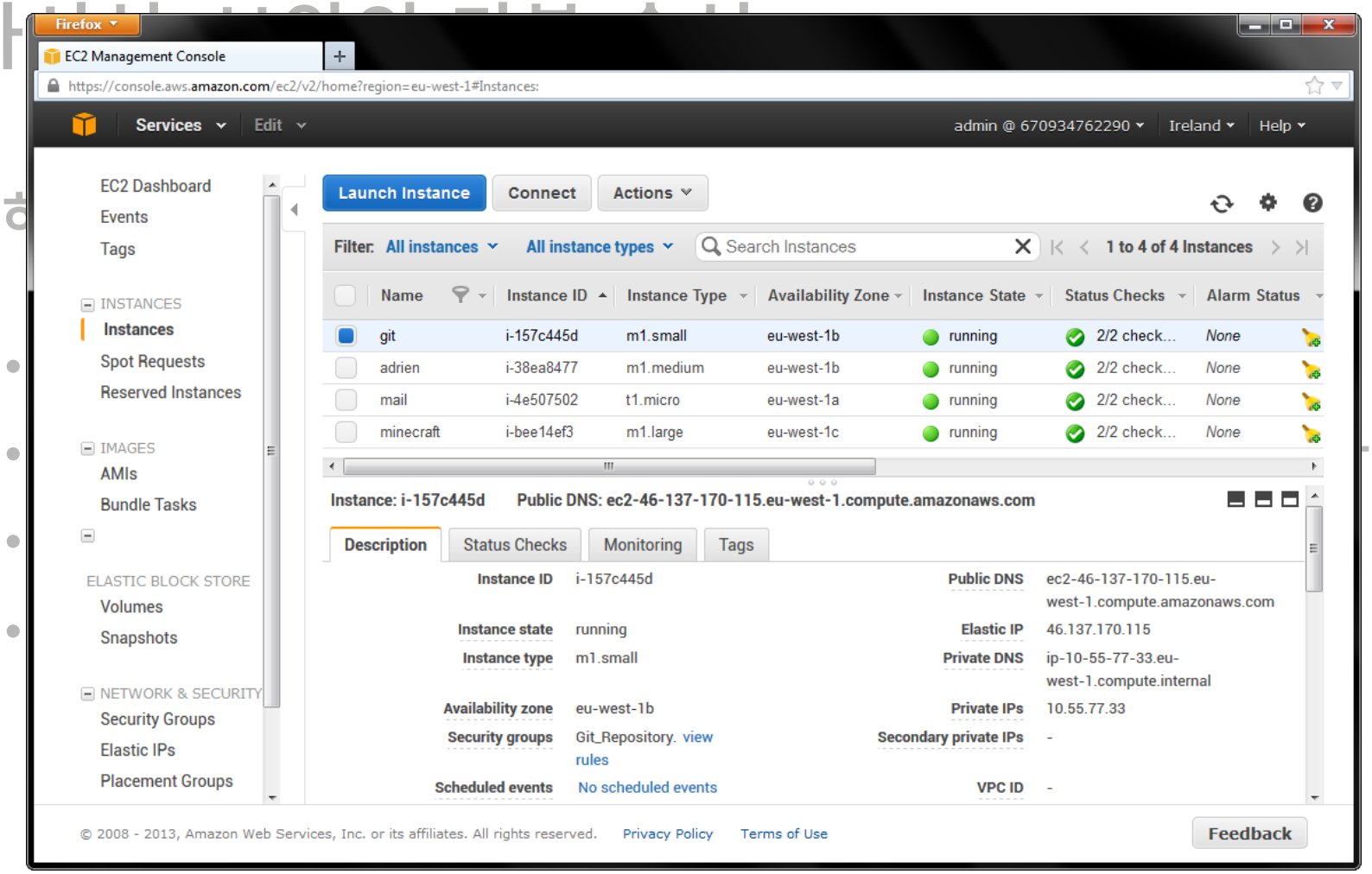
여러분의 데이터 센터를 보면...

한눈에 전체의상황이 다 들어오는 것을 원하시겠지만,



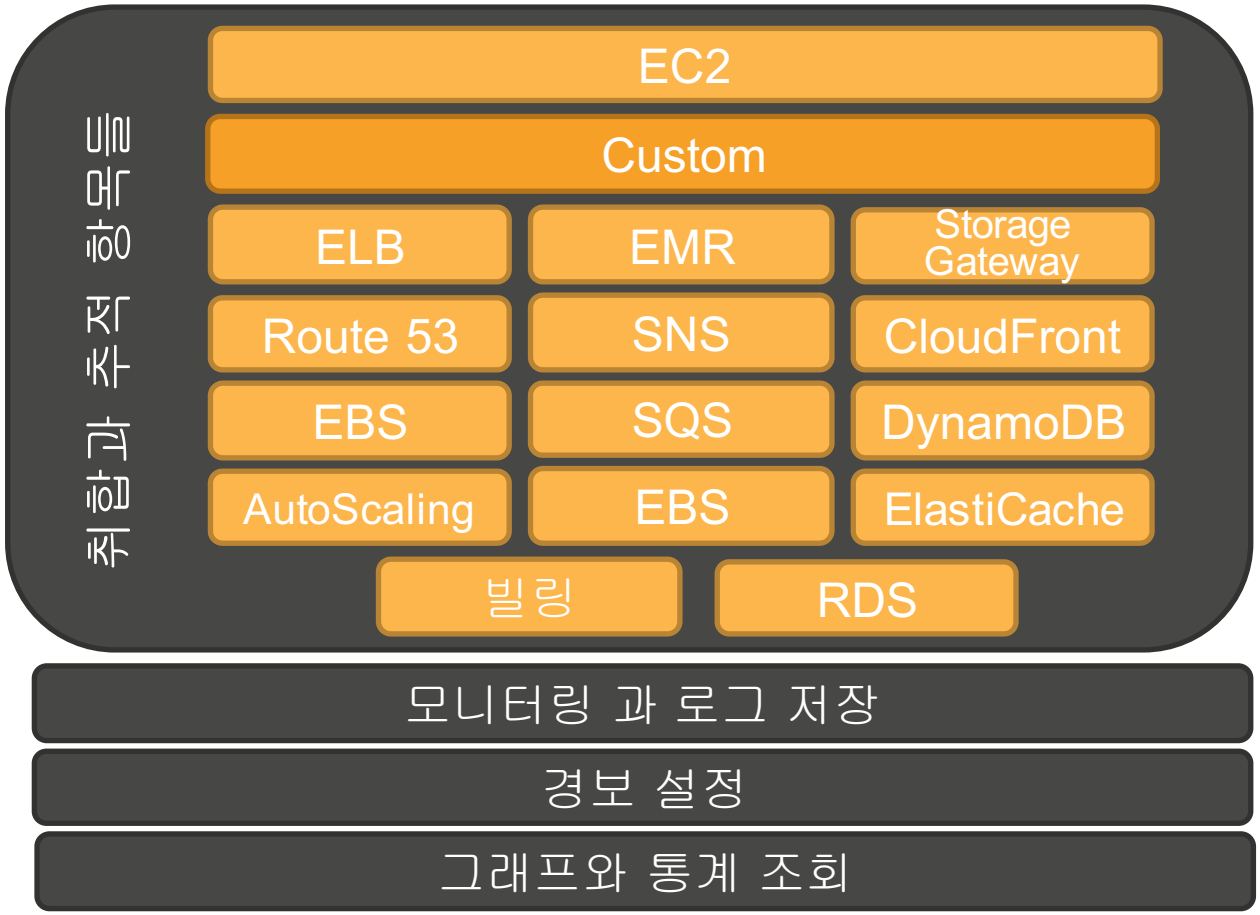
보통 이런 그림을 보시게 됩니다.

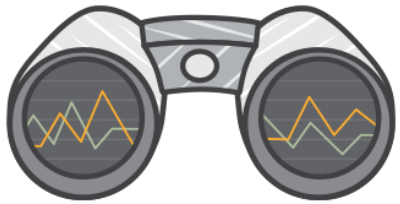



Firefox
EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=eu-west-1#Instances:
Services
Edit
admin @ 670934762290
Ireland
Help
EC2 Dashboard
Events
Tags
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & 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
Instance state running
Instance type m1.small
Availability zone eu-west-1b
Security groups Git_Repository. view rules
Scheduled events No scheduled events
Public DNS ec2-46-137-170-115.eu-west-1.compute.amazonaws.com
Elastic IP 46.137.170.115
Private DNS ip-10-55-77-33.eu-west-1.compute.internal
Private IPs 10.55.77.33
Secondary private IPs -
VPC ID -
© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Feedback

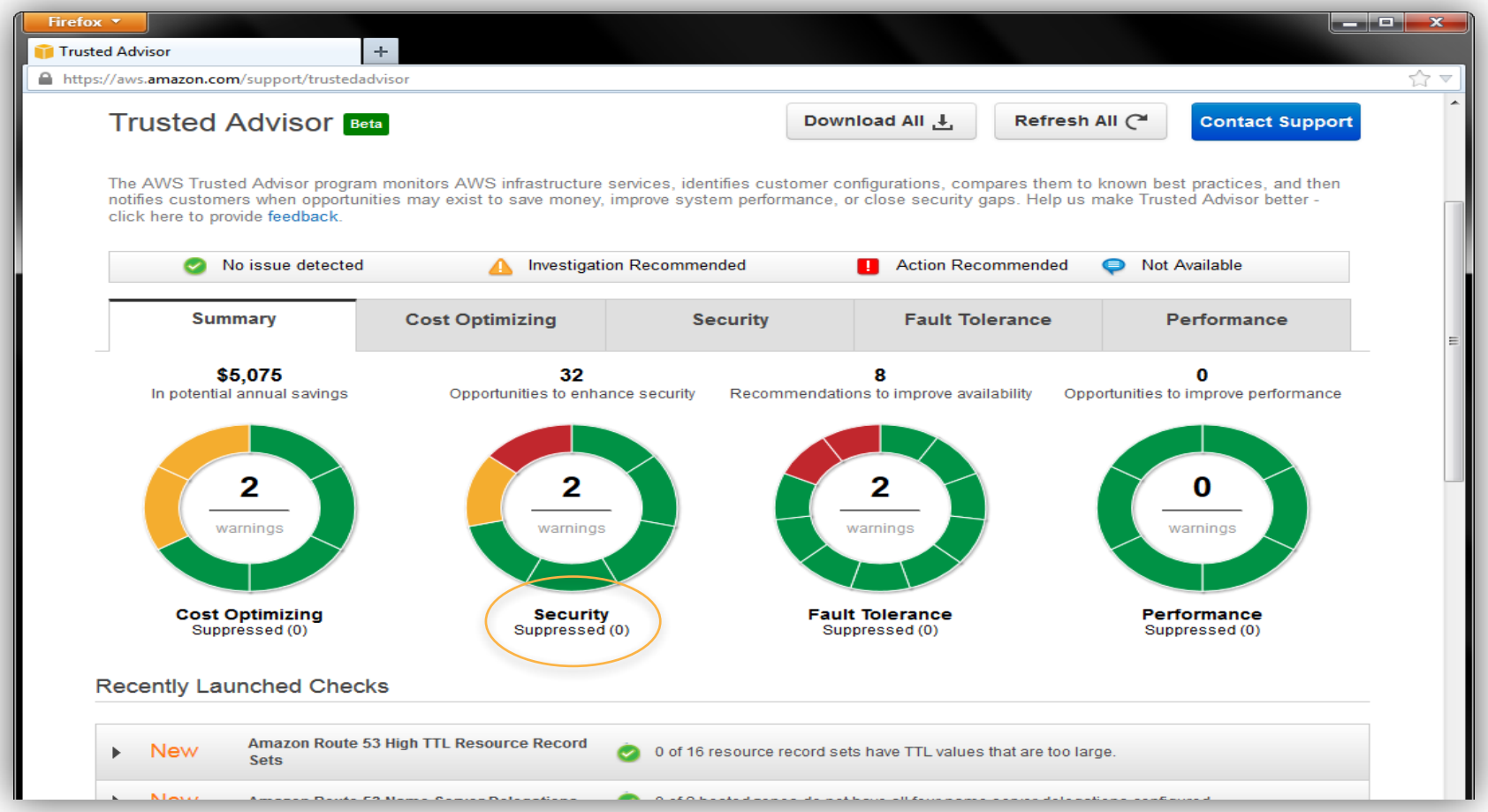
AWS CloudWatch

AWS 리소스와 AWS기반 어플리케이션에 대한 모니터링 서비스



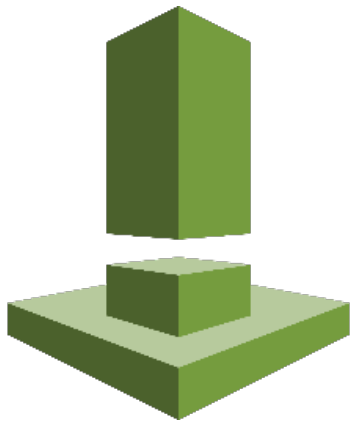


AWS Trusted Advisor Security



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)

amazon web services

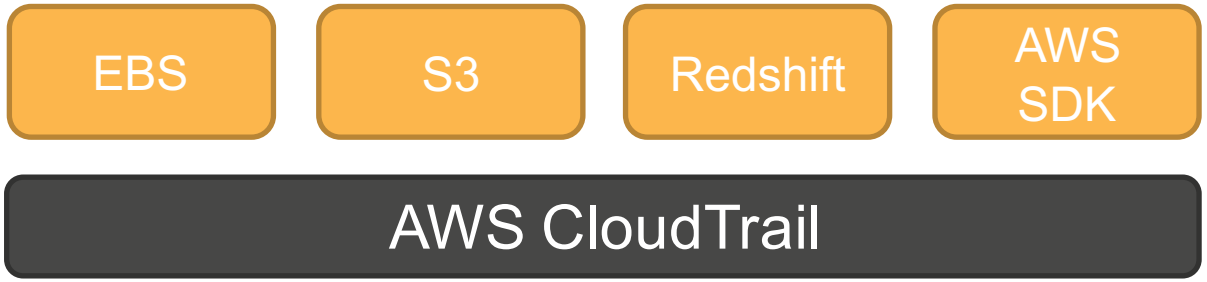
컴퓨팅과 스토리지의 위치를 고객이 직접 선택 가능

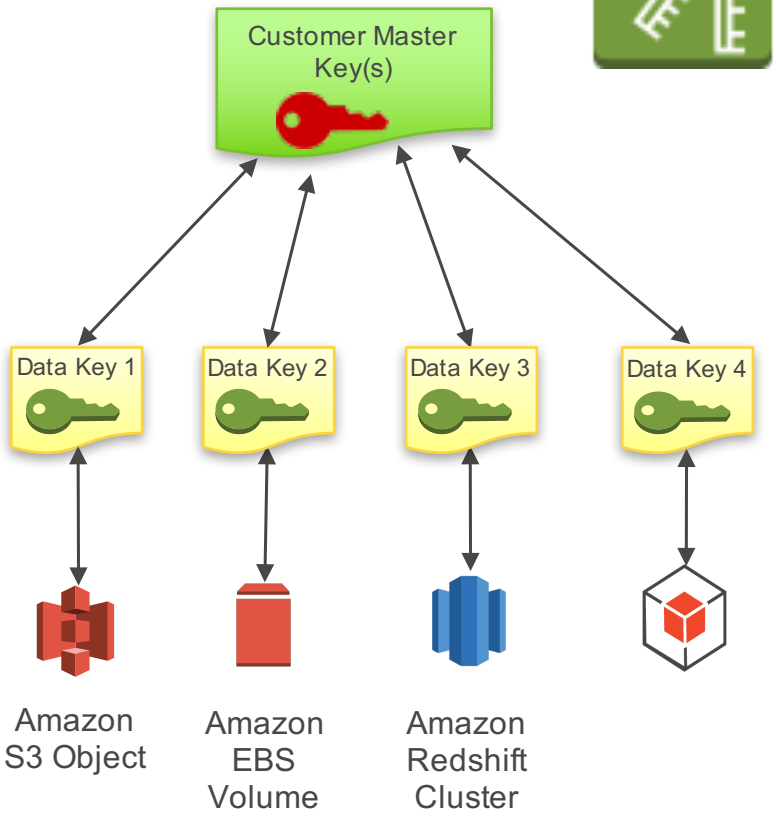
퍼스트 클래스 보안 및 규정준수는
암호화로 시작됩니다
(그리고 끝나지 않습니다!)

AWS KMS - 암호화키 생성/보관/관리

암호화키를 안전하게 생성/보관/관리 해주는 관리형 서비스(전송 중/저장 시 암호화)

중앙 집중 암호화 키 관리:

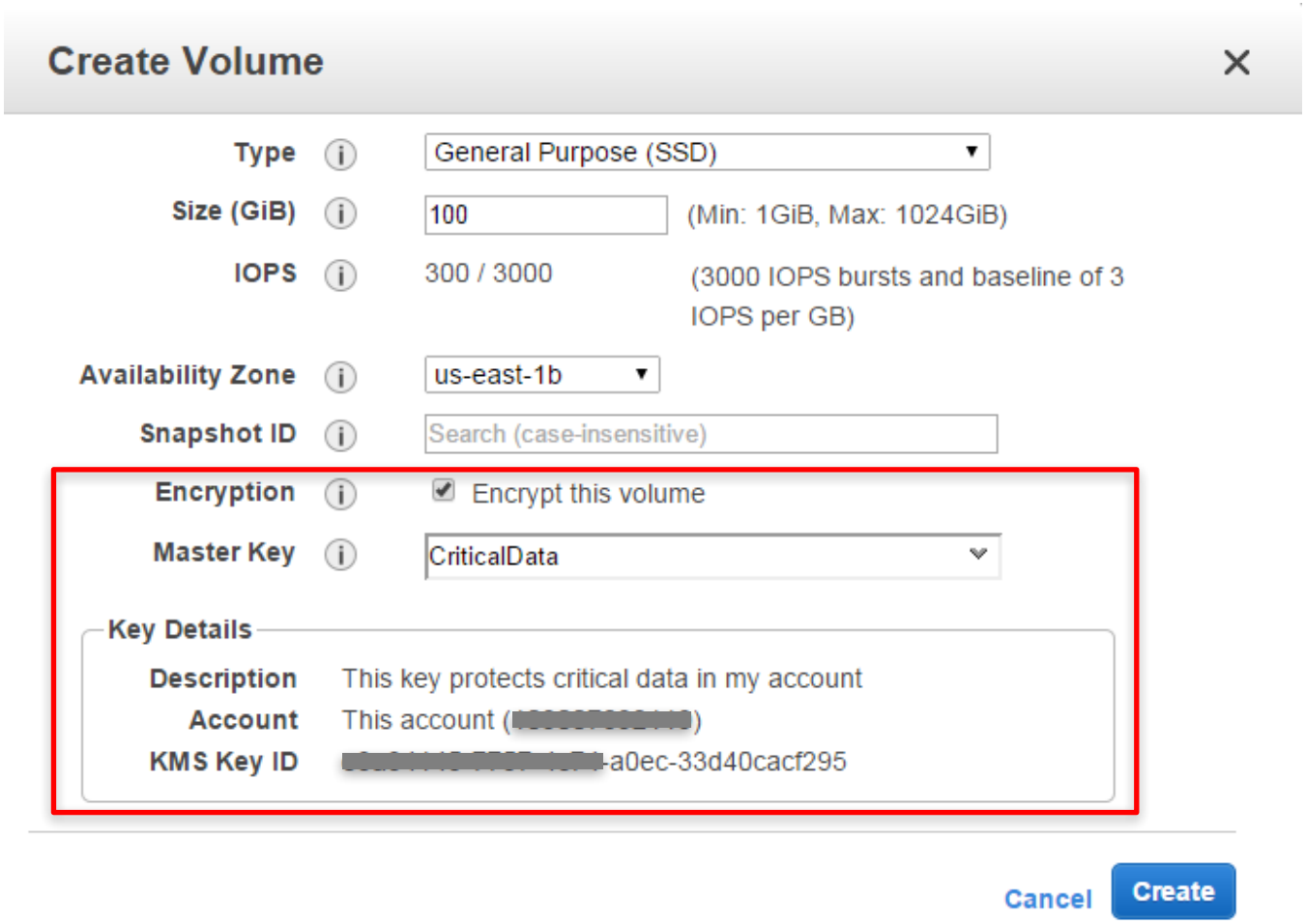




자세한 내용을 담고 있는 백서: KMS Cryptographic Details.

AWS Key Management Service

Integrated with Amazon EBS



AWS Identity and Access Management (IAM)

AWS서비스와 리소스에 대한 안전한 접근 통제.

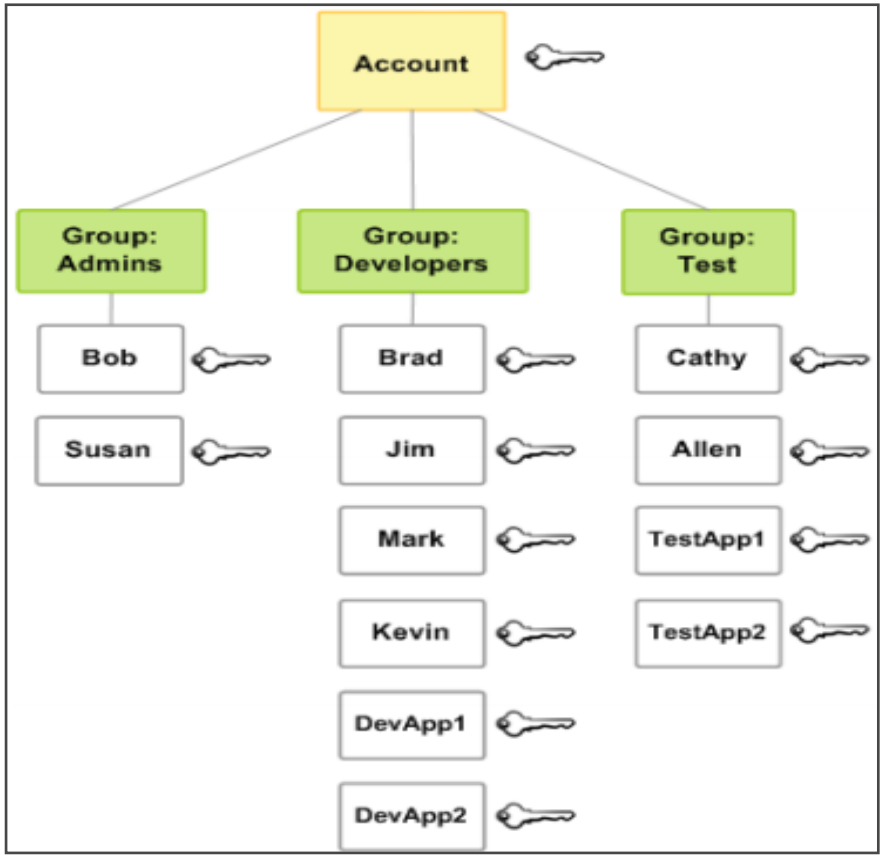
사용자 이름 / 사용자

사용자 그룹 관리

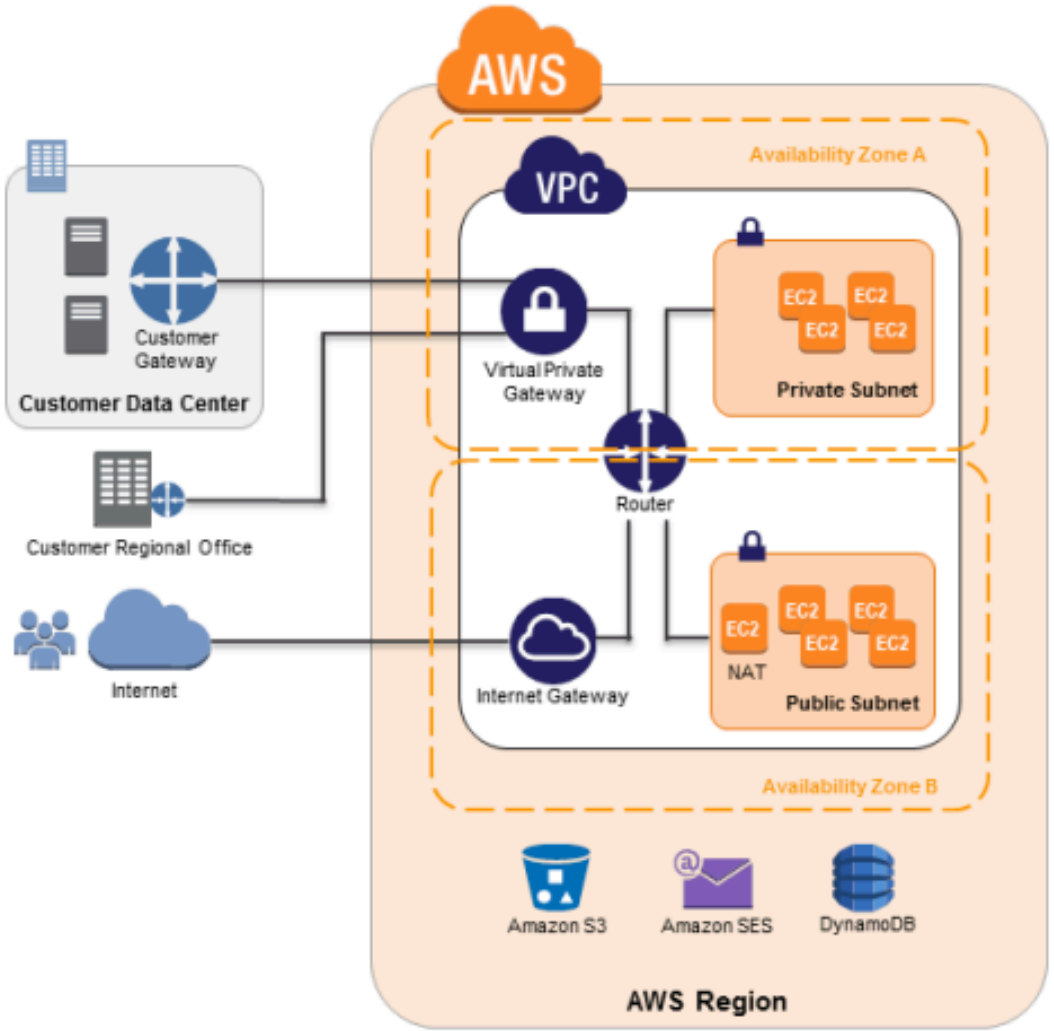
중앙화된 접근 제어 관리

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



네트워크 서비스 : VPC(Virtual Private Cloud)

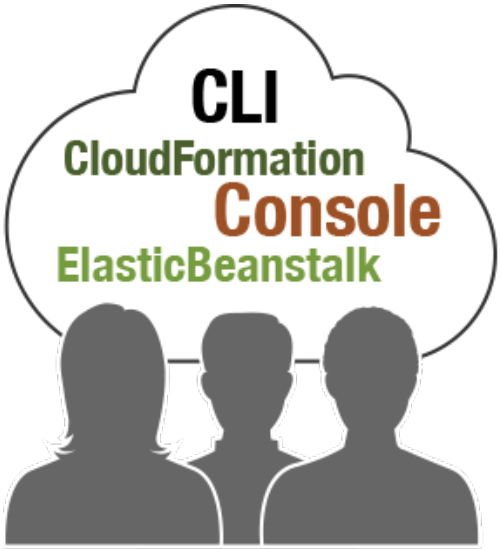


더 나은 감사기능
(컴플라이언스, 히스토리, 로그)

amazon web services

AWS CloudTrail

AWS상의 모든 관리작업에 대한 로깅



모든 작업은 API 콜로 처리됨...

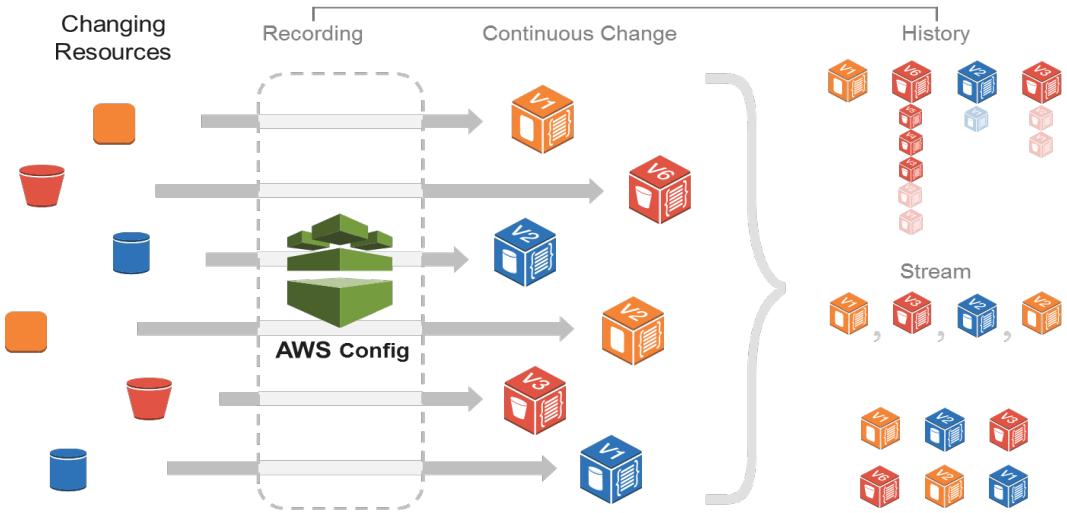
사용하는 서비스와 인스턴스들이 늘어남에 따라 ...

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

AWS 리소스에 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

AWS Config Rules

- 변경된 내역에 대해 검증하는 규칙 설정
- AWS가 제공하는 내장된 규칙 사용
- AWS Lambda를 활용한 커스텀 규칙 지원
- 지속적인 진단수행을 자동화
- 컴플라이언스 시각과나 위험한 변경을 식별하기 위해 대쉬보드 제공

AWS Config Rules

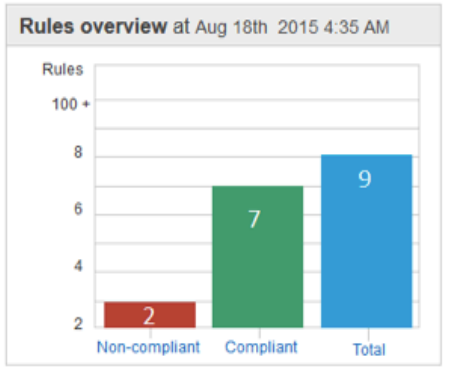
Rules

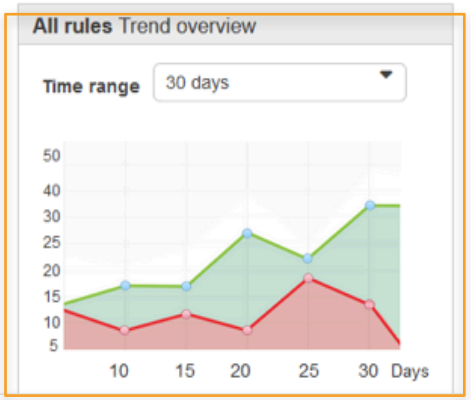
Status

This view determines if any rule that applies to the resource is currently non-compliant. You can view compliance by rule, which tells you if any resource within scope of the rule is currently non-compliant.

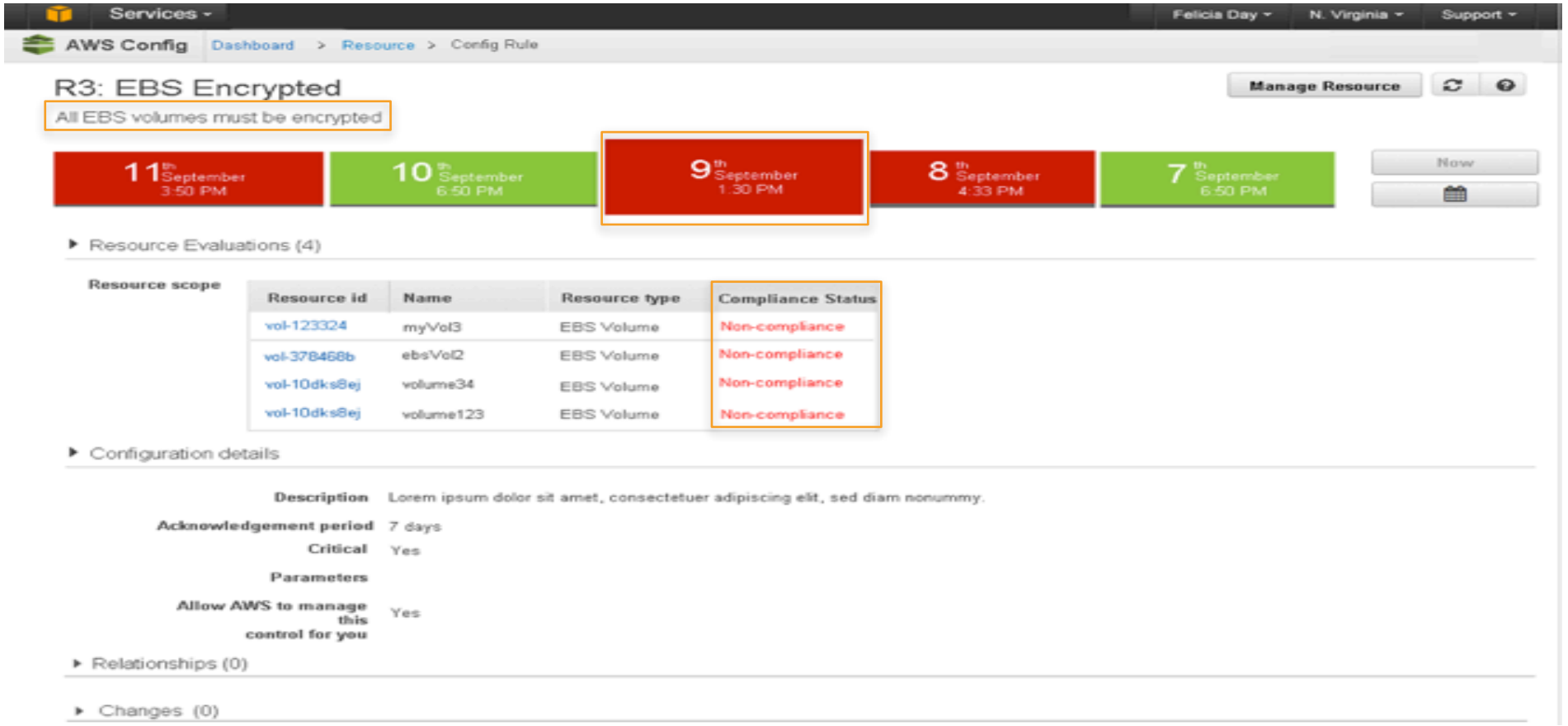
Add rule(s)

Rule name	Compliance status	Edit rule
CloudTrailEnabled	1 Non-compliant resource(s)	
VerifyVolumeEncrypted	1 Non-compliant resource(s)	
AttachedEIPs	Compliant	
EC2InstanceProfileRoleRestricted	Compliant	
InstancesInVPC	Compliant	
SecurityGroupPorts	Compliant	
SecurityGroupSSHPort	Compliant	
TagsOnResources	Compliant	
UpdatedUsersKeys	Compliant	





AWS Config Rules



AWS Marketplace:
네트워크/보안 파트너 생태계

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

Nasdaq

What Nasdaq 요구사항

- 기존 데이터웨어 하우스의 저렴하게 교체
- 비용은 줄이고, 데이터 용량 및 처리는 증대

왜 AWS (특히 아마존 Redshift)를 선택

- 보안 및 규정 준수 요구 사항을 충족
- 현재 전제된 기능을 희생하지 않고 비용을 개선

기대효과

- 아마존 Redshift에 하루 평균 데이터의 55 억행 처리 가능 (2014년 10월의 피크날, 데이터의 140 억행 처리)
- 회사 내 여러 부서에서 데이터를 접근 및 분석, 처리가 가능한 환경 구현

http://aws.amazon.com/cn/solutions/case-studies/nasdaq-finqloud/
http://aws.amazon.com/solutions/case-studies/nasdaq-omx/

사례 연구 : 규제 감시 및 리스크 사전 분석

"시장에서 AWS 모니터링 플랫폼을 사용하여 우리는 40 %의 비용 절감을 달성 할 것으로 예상하지만, 더 중요한 장점은 새로운 비즈니스를 얻는 것입니다 : 우리가 할 수 있는 일에 집중하고 새로운 혁신을 할 수 있는 것은 귀중한 혜택입니다.
-- Steve Randich, CIO

FINRA 요구사항
- 시장 감시 인프라를 구축하는 플랫폼
- 300 억건의 매일 발생하는 시장 이벤트의 저장 및 분석을위한 지원

AWS를 선택한 이유
- FINRA의 보안 및 요구 사항 만족
- 유연한 플랫폼 (하둡, 하이브 및 HBase를), 아마존 EMR, 아마존 S3 동적 클러스터 배포를 통한 구축

기대효과
- 유연성, 속도와 비용 절감을 증가
- AWS를 사용하는 비용은 $1에서 $1M 까지 탄력적으로 활용할 수 있었음

http://aws.amazon.com/cn/solutions/case-studies/finra/

사례 연구 : 고성능 컴퓨팅 (HPC)

"AWS를 사용하여, 최대 10일 이내 우리가 원하는 결과를 도출하고 최소 10분 이내 컴퓨팅을 활용하여 분석 및 시뮬레이션을 완료할 수 있었다. 빠르게 변화하고 있는 정보와 이벤트를 찾아내는 능력을 확대할 수 있었다."

-- Peter Phillips, Managing Director

AON BENFIELD

Aon 요구사항

- 고성능 컴퓨팅을 통한 고차원 산술 및 분석
- 적은 비용으로 단시간에 결과를 얻을 수 있는 컴퓨팅

AWS를 선택한 이유

- 저가의 그래픽 컴퓨팅 능력 그래픽 처리 장치 (또는 GPU에)의 빠른 확장
- 전반적 기술 컴퓨팅 환경과 기능을 제공하며, 빠른 전개

기대효과

- AWS 작업으로 불과 몇 분에 보험 정책을 검증하고 다시 계산이 가능.
- 프로그램의 위험을 빠르게 분석해서 고객에게 더 나은 상품을 제공하고 평가할 수 있음
- 비용 절감은 고객의 보험료를 줄이기 위해 사용

http://aws.amazon.com/cn/solutions/case-studies/aon/

사례 연구 : 클라우드 올인 은행

"데이터 센터와 백업 및 재해복구 센터에 대한 전면재조정함에 따라 8개의 센터에서 3개의 센터까지 조정을 완료하고 최종적으로는 2개의 센터만 유지하는것을 결정: 우리가 할 수 있는 일에 집중하고 새로운 혁신을 할 수 있는 것은 귀중한 혜택입니다.

CapitalOne 요구사항

- 최신 IT 기술 수용 및 환경 도입에 따른 클라우드 기반의 플랫폼 체계 수립

AWS를 선택한 이유

- 클라우드 기반의 IT 운영 및 관리 체계로 IT 서비스사/파트너 등 계층 없이 실시간 직접 확인 가능

기대효과

- 4개 사업부로 확대 적용(Retail Bank/Investing/Auto Finance/IT-InfoSec)
- 데이터센터 이관 완료로 인해 년간 1조 5천억 IT 운영 및 자산에 대한 관리 비용 절감(500개 App, 4000개 운영VM)

https://aws.amazon.com/ko/solutions/case-studies/capital-one/

더 이상 보안은
클라우드 도입을 가로막는
걸림돌이 아닙니다!

이제는 보안과 규제준수가
클라우드를 도입하는
중요한 이유가 되고 있습니다!

Thank You

SEOUL

amazon web services