Public Cloud
구성오류로 발생하는 보안문제,
해법은?

노영길 매니저
Cloud Service MSS팀

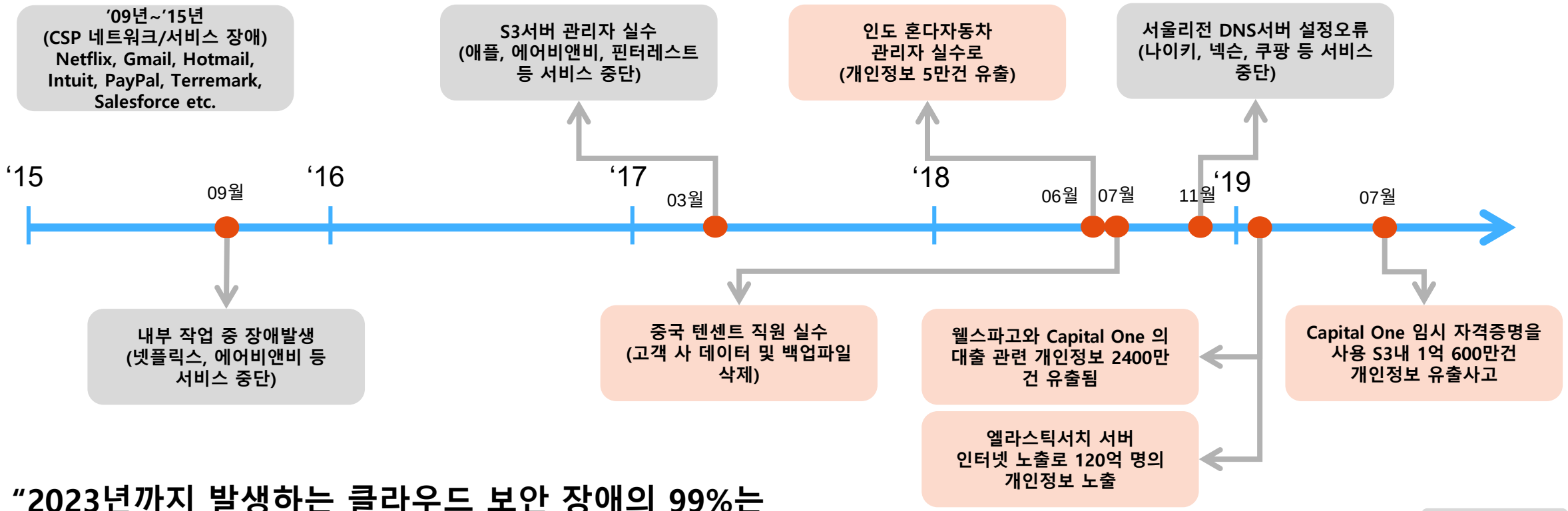
BESPIN GLOBAL

OpsNow
AUTOMATE
YOUR CLOUD OPERATION

퍼블릭 클라우드
구성 오류로 발생하는 보안문제와 해법

- 자주 실수하는 퍼블릭 클라우드 구성 오류
- 클라우드 구성오류&실수 완벽한 해결방법

클라우드 보안사고 사례



"2023년까지 발생하는 클라우드 보안 장애의 99%는 고객의 실수로 인해 발생할 것이라 전망"
(Gartner, 2019)

OpsNow AUTOMATE YOUR CLOUD OPERATION

어떻게 대비할 것인가? 가용성&보안사고 관점

하이브리드 클라우드	멀티 리전 사용	멀티 클라우드
최근 IDC에서도 큰 장애가 발생한 것을 보면 역시 근본적인 해결책은 아니다. 그리고, Trend를 버리고 안주할 수만 없는 게 현실!!	여러 리전에서 동시에 장애가 발생 할 수 있기 때문에 근본적인 해결책은 아니다. 사용자/ 관리자의 장애 포인트는 여전하죠!!	여러 클라우드에서 동시에 장애가 발생 할 수 있기 때문에 근본적인 해결책은 아니다. 제 각기 조금씩 다른 구성환경으로 인한 장애 포인트는 더 증가하기도 합니다.

멀티 클라우드로의 전환!! 보안 Risk는?

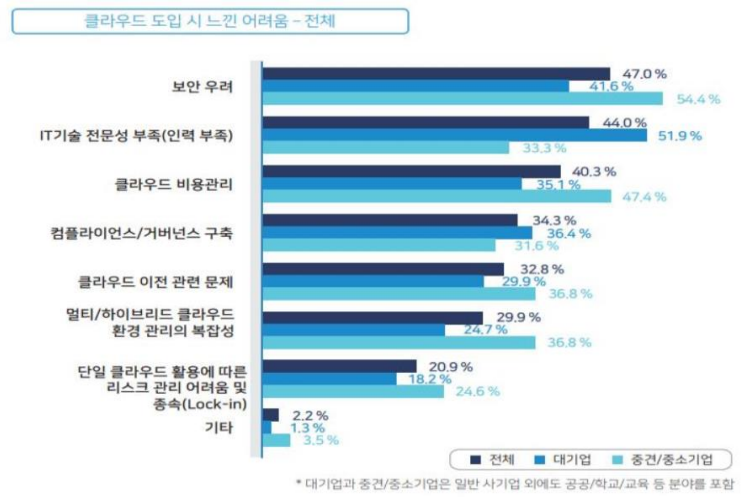
OpsNow AUTOMATE YOUR CLOUD OPERATION

***How a Hybrid Multicloud Strategy Can Overcome the Cloud Paradox, IBM, 2019.11.5**

- 85% 응답자가 멀티 클라우드를 운영 중
- 3년 후 98%가 멀티 클라우드로 전환할 예정
- 하이브리드 클라우드 환경에서 멀티 클라우드를 도입하겠다는 응답은 현재 77%에서 98%로 응답

기업 IT 의사결정자 10명 중 절반 이상이 3년 후 대부분 기업이 멀티클라우드 환경을 사용할 전망이라고 예측

***2019 국내 클라우드 도입의 현주소, 베스핀글로벌, 2019.5.29**



클라우드 도입 시 겪는 가장 큰 어려움으로 **보안(47%)응답**

멀티 클라우드 운용하는 거 보통 일이 아니죠!

멀티 클라우드 보안!!

AWS 245

Azure 145

GCP 115

… Ali Cloud

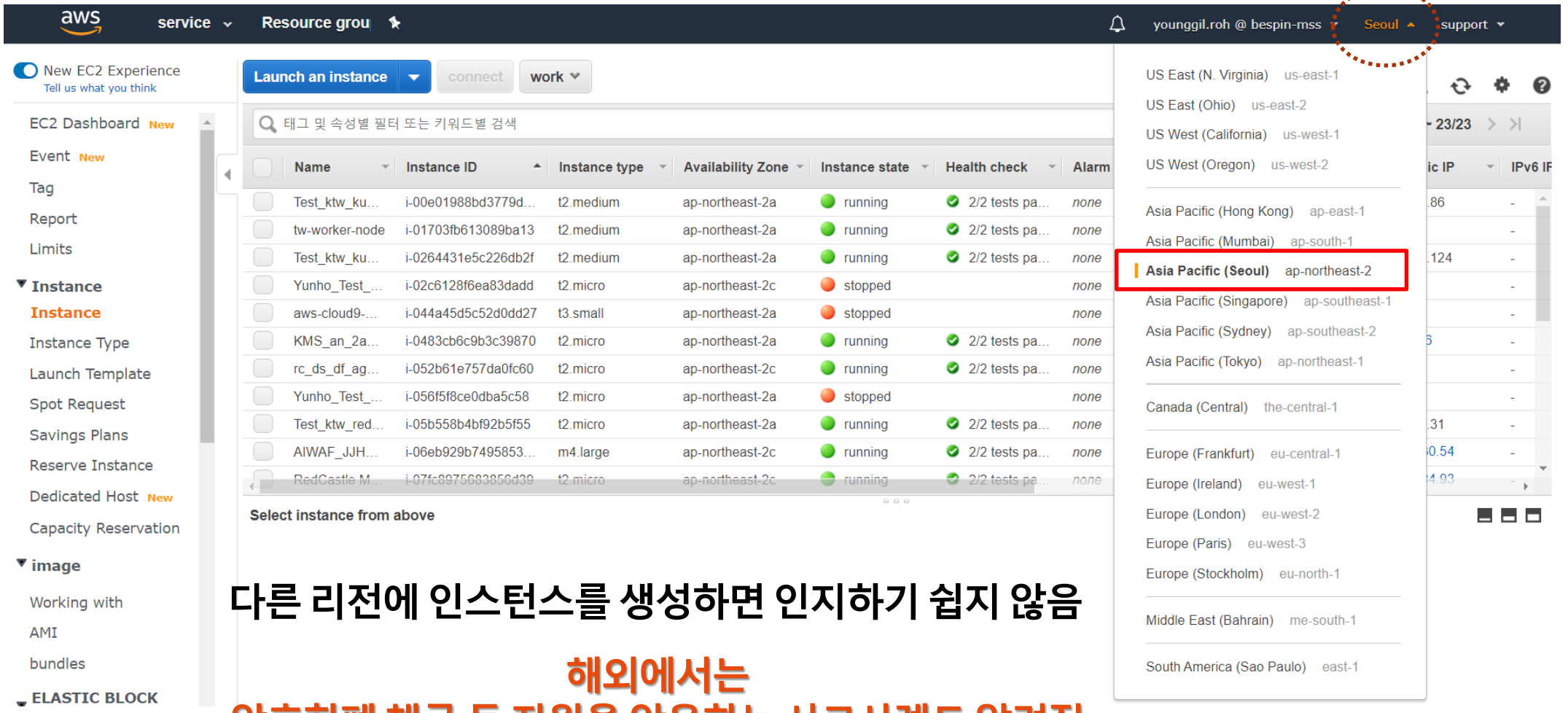
멀티 클라우드 용어비교

OpsNow
AUTOMATE
YOUR CLOUD OPERATION

서비스 설명	aws	Azure	Google Cloud Platform
가상 서버	EC2: Elastic Computer Cloud	Virtual Machine	GCE: Computer Engine
가상 디스크	EBS : Elastic Block Store	Disk Storage	Persistent Disk
객체 저장소	S3: Simple Storage Service	Blob Storage	Cloud Storage
파일 저장소	EFS: Elastic File System	File Storage	Cloud Filestore
플랫폼 서비스	EB: Elastic Beanstalk	App Service	GAE: App Engine
서버리스	Lambda	Functions	Cloud Function
컨테이너	Amazon ECS	Azure Kubernetes Service(AKS)	Kubernetes
DNS 서비스	Route 53	DNS	Cloud DNS
부하 분산	ELB: Elastic Load Balancer	Load Balancer	Cloud Load Blaccing

클라우드 Native 환경에는
이에 맞는 전문적 전략, 지식, 기술 노하우를 모두 검토해서 마이그레이션 /관리필요

AWS EC2 컴퓨팅 자산식별(예시)



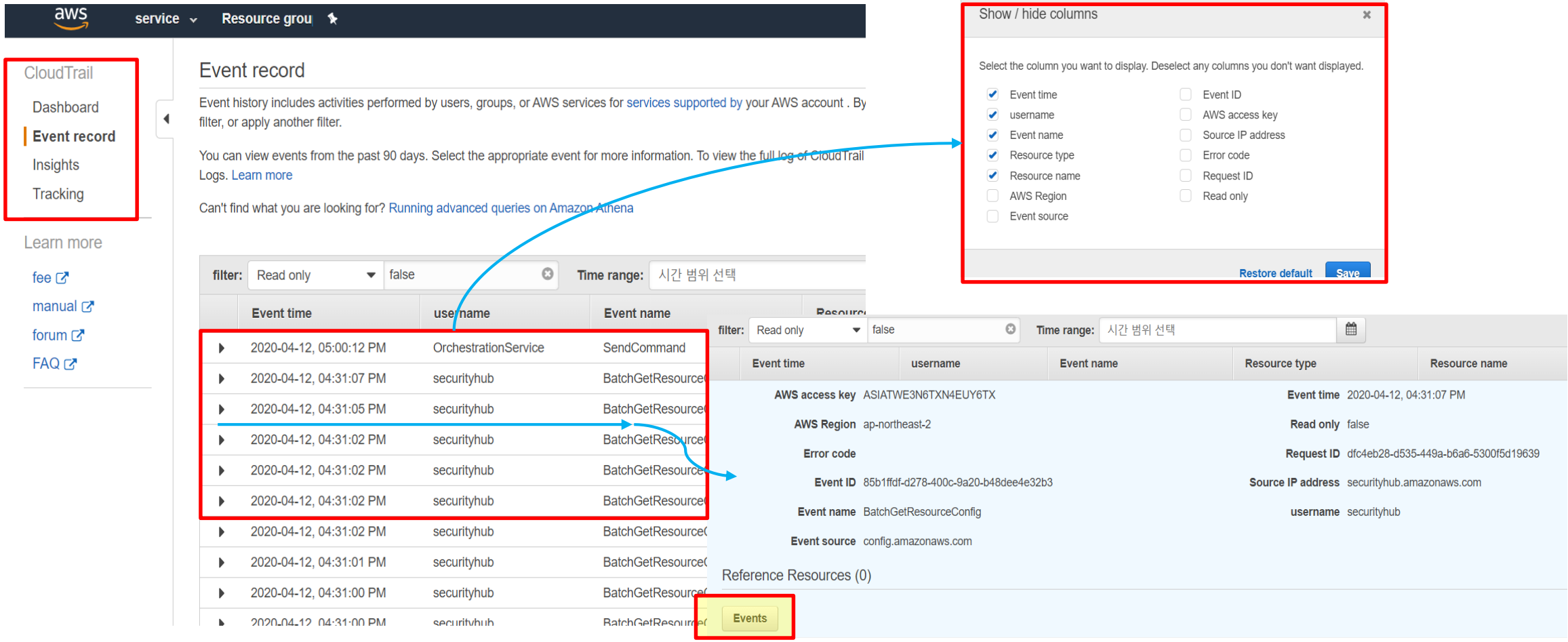
다른 리전에 인스턴스를 생성하면 인지하기 쉽지 않음

해외에서는
암호화폐 채굴 등 자원을 악용하는 사고사례도 알려짐

AWS 감사 모니터링(예시)

OpsNow AUTOMATE YOUR CLOUD OPERATION

CroudTrail을 로그설정을 통한 이벤트 모니터링 만으로 보안관리 쉽지 않음



AWS 감사 모니터링(예시)- 계속

OpsNow AUTOMATE YOUR CLOUD OPERATION

이벤트 로그에 대한 모니터링 정책을 수립하고 자동화 하지 않는다면 유연한 클라우드 관리 어려움

[지원 서비스 예시]

이벤트명	설명
ConsoleLogin	AWS 콘솔 로그인
CreateUser	IAM 계정 생성
DeleteUser	IAM 계정 삭제
RunInstances	VM 인스턴스 생성
StartInstances	VM 인스턴스 시작
RebootInstances	VM 인스턴스 재시작
StopInstances	VM 인스턴스 중지
TerminateInstance	VM 인스턴스 삭제
CreateBucket	S3 버킷 생성
CreateAccessKey	액세스 키 생성
UpdateAccessKey	액세스 키 활성화/비활성화
DeleteAccessKey	액세스 키 삭제
PutBucketAcl	S3 버킷 접근제어 설정
PutBucketPolicy	S3 버킷 정책 설정
AuthorizeSecurityGroupIngress	인바운드 트래픽 허용
AuthorizeSecurityGroupEgress	아웃바운드 트래픽 허용
StopLogging	CloudTrail 로깅 비활성화

지원 서비스 범위 159EA

퍼블릭 클라우드 구성오류 대응은?

OpsNow AUTOMATE YOUR CLOUD OPERATION

클라우드는 상시 감사체계가 필요합니다.

잘못된 구성 → 부적절한 변경 관리 → 데이터 유출

사용자 과실과 관련된 'ID ▪ 자격증명 ▪ 키 관리'

높은 권한을 가진 계정을 탈취하는 '계정 도용'

내부자 및 협력업체 직원이 악의적으로 접근하는 '내부자 위협'

승인되지 않은 애플리케이션(섀도우 IT영역)

'클라우드 서비스 '남용과 악의적 사용'

취약한 기능을 해킹해 파고드는 '보안에 취약한 인터페이스와 API 사용'

승인된 애플리케이션을 사용함에 따라 발생하는 보안 문제

사용자 식별, 리소스 보호, 이상행위분석 등 보안위협 시나리오!!

- 클라우드관리계정에 2Factor 인증이활성화되어있는가?
- S3 등객체스토리지가외부에노출된상태는아닌가?
- S3 등객체스토리지에대한접근로그가활성화되어있는가?
- 클라우드감사로그를 비활성화하려고시도하는가?
- SSH나RDP등인터넷구간에서가상머신에접근차단하고있는가?
- VM에대해포트스캐닝이나SSH 브루트포스등공격이발생하는가?
- 다른리전에서고비용의VM (GPU 장착등)을생성하여사용하는가?

• • •

퍼블릭 클라우드 보안 컴플라이언스 필요성

OpsNow AUTOMATE YOUR CLOUD OPERATION

클라우드 서비스 확대에 따른 신속한 보안 대응 및 컴플라이언스 대응은 이렇게...

고객의 어려움	해결 방안
클라우드 시스템 설정 오류 및 실수에 의한 보안 사고 증가	자동화된 설정 오류 체크 통해 보안 사고 방지 필요
클라우드 워크로드 변경 시 컴플라이언스 적용 어려움	자원 변화에 대한 지속적인 컴플라이언스 감사(Audit) 필요
멀티 클라우드 사용 확대에 따른 일관된 보안관리 어려움	모든 클라우드 자원에 대한 가시성 확보 필요
급변하는 클라우드 기술에 대한 보안 적용 어려움	보안 전문 업체의 업계 베스트 프랙티스와 지원 필요
컨테이너,서버리스 서비스의 보안 적용 어려움	컨테이너/서버리스 특화된 보안기능과 가시성 확보 필요

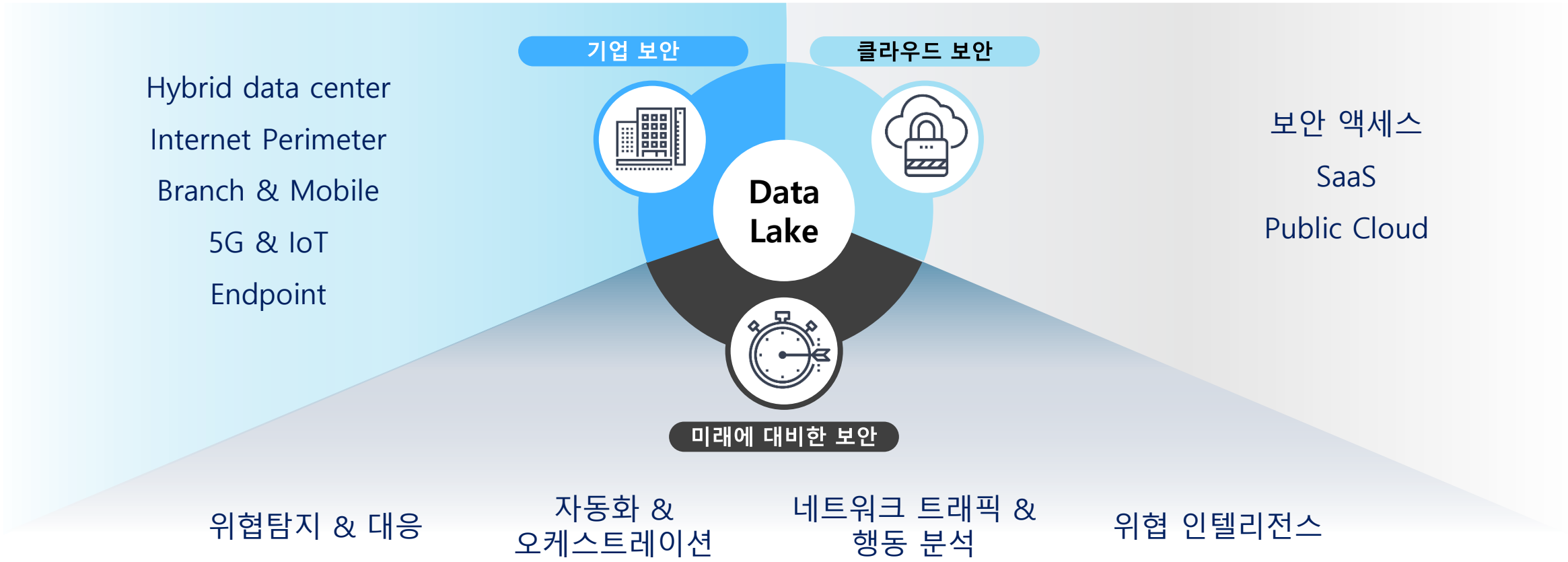
OpsNow
AUTOMATE
YOUR CLOUD OPERATION

2. 프리즈마 클라우드 소개

클라우드 보안 요구사항의 증가

OpsNow AUTOMATE YOUR CLOUD OPERATION

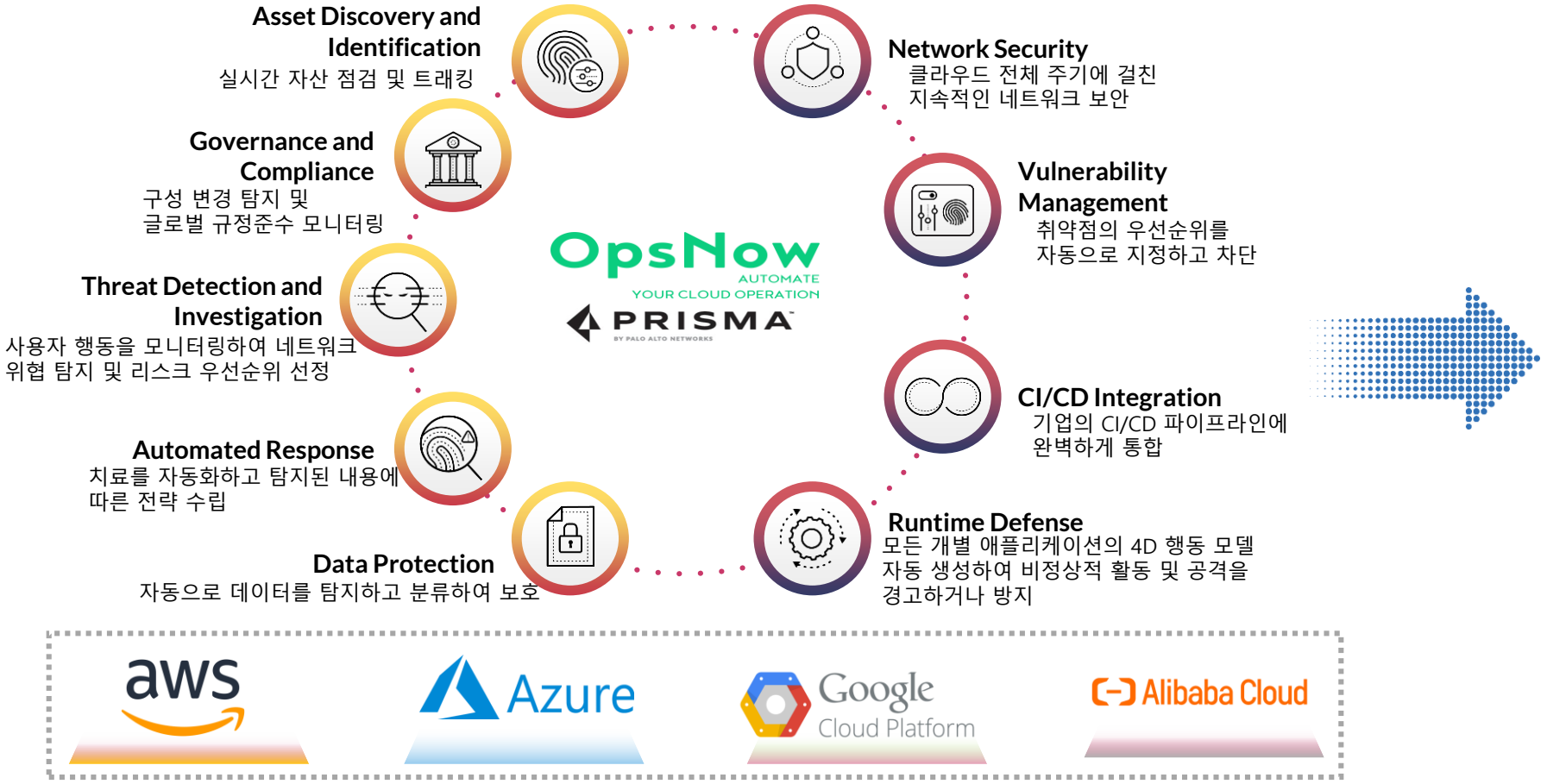
Digital Transformation과 더불어 다각화된 클라우드 보안에 대한 필요성 대두



프리즈마(Prisma) 클라우드 통합 제품 개요

OpsNow AUTOMATE YOUR CLOUD OPERATION

클라우드 전체 라이프사이클에 걸쳐 클라우드 보안에 대한 기업의 우려를 해소



Cost Saving

보안 기능의 통합 제공으로
운영 비용 및 복잡성 감소

Compliance

지속적인 보안 및 거버넌스 규정 준수

Agility

속도와 민첩성

보안 컴플라이언스 주요 기능

OpsNow AUTOMATE YOUR CLOUD OPERATION

지속적인 보안 모니터링 및 컴플라이언스 체크

Prisma Cloud

API

제공 영역

스토리지 | 계정 | 인스턴스 | 서버리스/ 컨테이너

Check List

- MFA를 활성화할 수 있습니까?
- 민감한 데이터가 노출됩니까?
- 어떤 서비스가 구동되고 있습니까?
- 누가 이 리소스에 접근합니까?

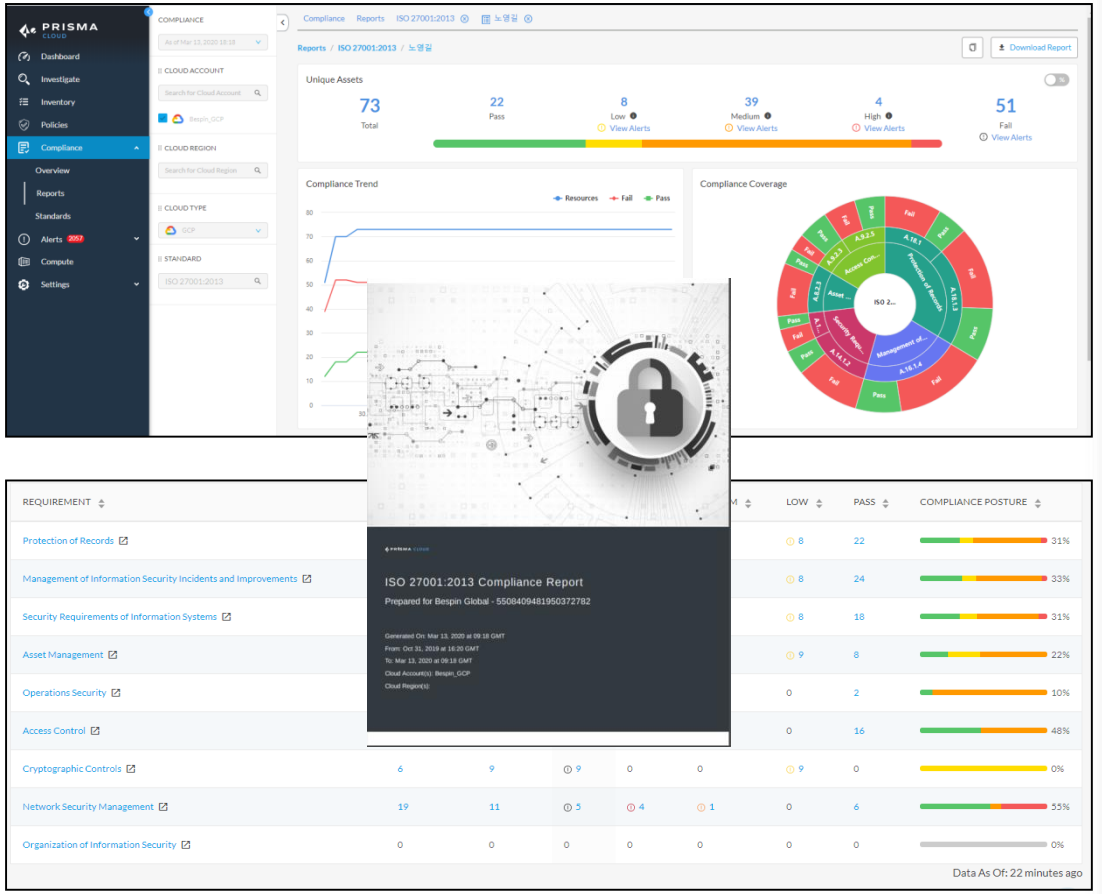
SOC 2 | HIPAA | NIST | ISO 27001 | GDPR | PCI DSS | aws | Azure | Google Cloud Platform

리소스를 찾아내고 모니터링

안전한 스토리지 서비스

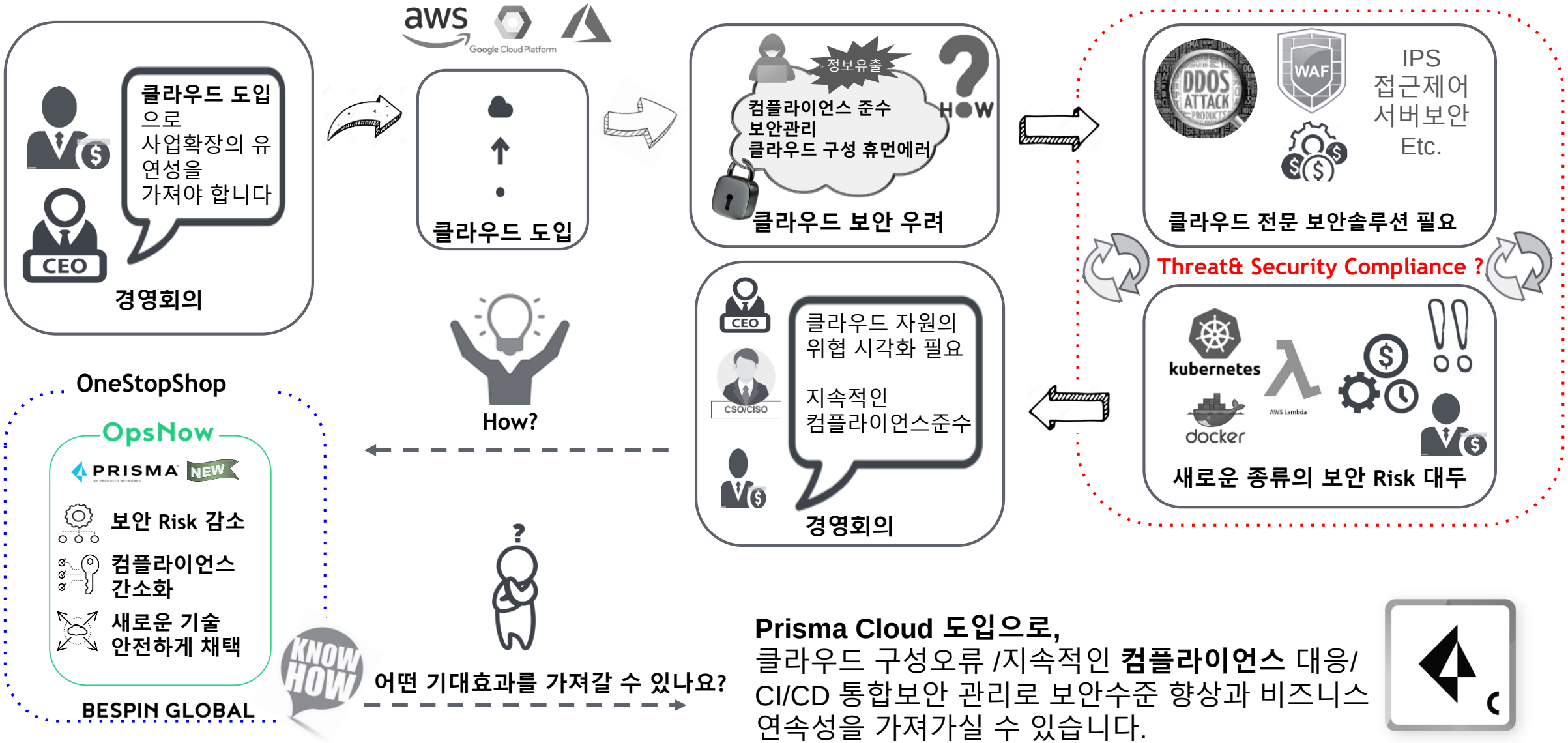
컴플라이언스 리포팅

컴플라이언스 대시보드



취약요소에 대한 지속적인 모니터링 베스핀글로벌과 함께!!

OpsNow AUTOMATE YOUR CLOUD OPERATION



Prisma Cloud 도입으로,
클라우드 구성오류 /지속적인 **컴플라이언스** 대응/
CI/CD 통합보안 관리로 보안수준 향상과 비즈니스 연속성을 가져가실 수 있습니다.

OpsNow
AUTOMATE
YOUR CLOUD OPERATION

Demo 시연

류기현 매니저
Cloud Service MSS팀

Demo 시나리오

OpsNow
AUTOMATE
YOUR CLOUD OPERATION

1. 클라우드 이벤트 탐지

2. 클라우드 구성오류 확인

3. 클라우드 컴플라이언스 대응