"클라우드 보안의 시작 – 시스코 CloudLock"

클라우드 보안을 위한 CASB 솔루션

이성철이사
시스코 코리아

목차

1. 업무환경의 변화에 따른 고객 보안 요구 사항
2. CASB(Cloud Access Security Broker) 소개
3. 시스코 클라우드락(CloudLock)
4. 고객 사례 및 맺음말

업무환경의 변화에 따른 고객 보안 요구사항

By 2018, Gartner 예측 :

회사 데이타 트래픽의 25%는 기업의 perimeter security를 우회하여 이용될 것이다.

과거의 업무 환경

현재의 업무 환경

원격
사용자

랩탑 / 태블릿 사용자

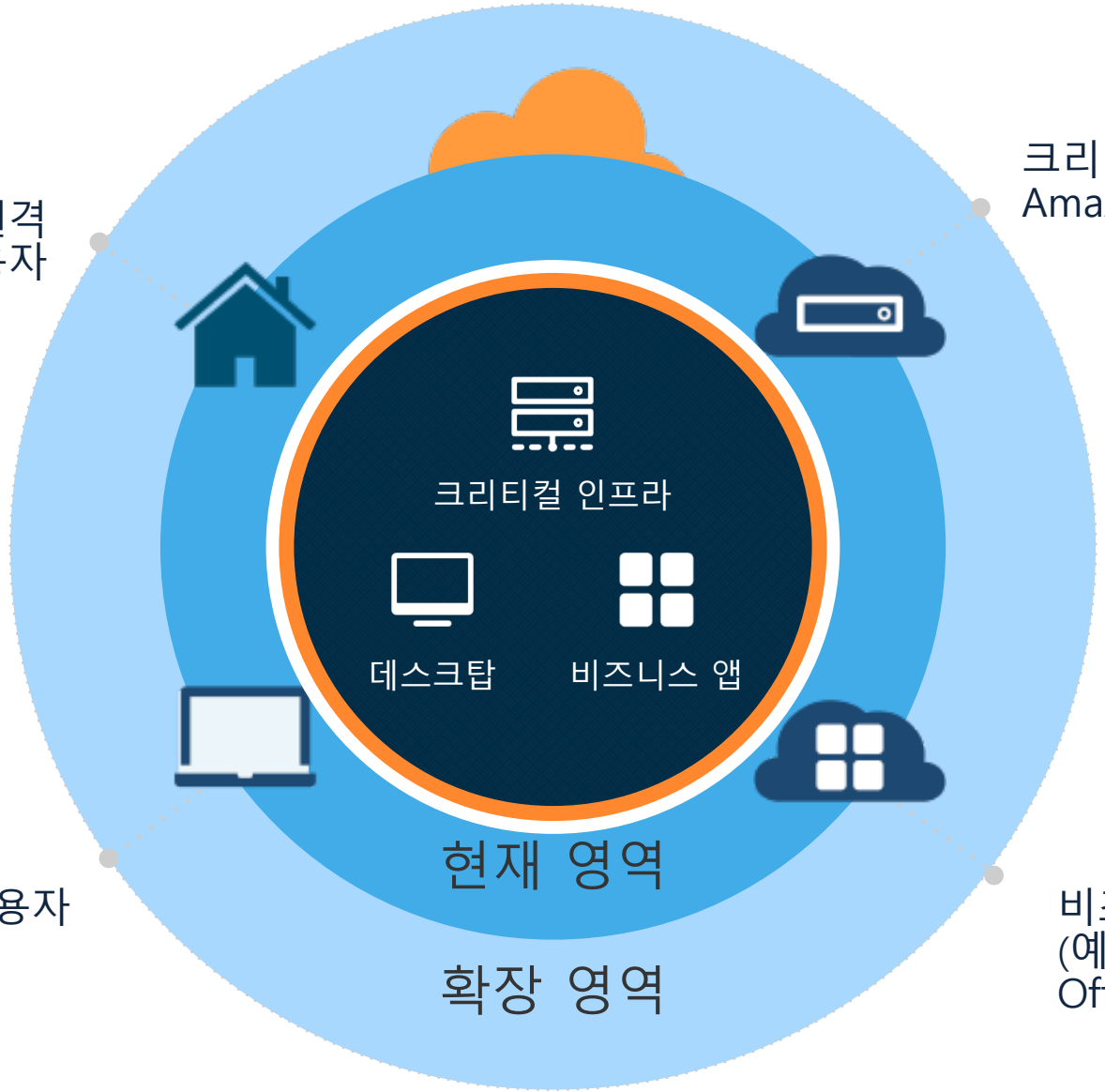
사용자

크리티컬 인프라 – ***IaaS & PaaS*** (예, Amazon, Azure, etc.)

데이터 & 앱

비즈니스 앱 - ***SaaS***
(예, Salesforce, Dropbox, Office365, Google)

현재의 업무 환경에서 확장된 사용 환경



원격
사용자

사용자

랩탑 / 태블릿 사용자

크리티컬 인프라 – ***IaaS & PaaS*** (예, Amazon, Azure, etc.)

데이터 & 앱

비즈니스 앱 - ***SaaS***
(예, Salesforce, Dropbox, Office365, Google)

클라우드로 모든 것이 구현된 세상

CLOUD

ON - PREMISE

CloudLock
CyberSecurity Fabric

비즈니스 앱 (Public SaaS)

salesforce
Office 365
Google Apps
Dropbox
servicenow
box
slack
workday
NETSUITE

People

iOS
OAUTH
IoT

커스텀 앱 (PaaS & IaaS)

amazon web services
force.com
Google Compute Engine
Microsoft Azure
ORACLE CLOUD SOLUTIONS
IBM SOFTLAYER

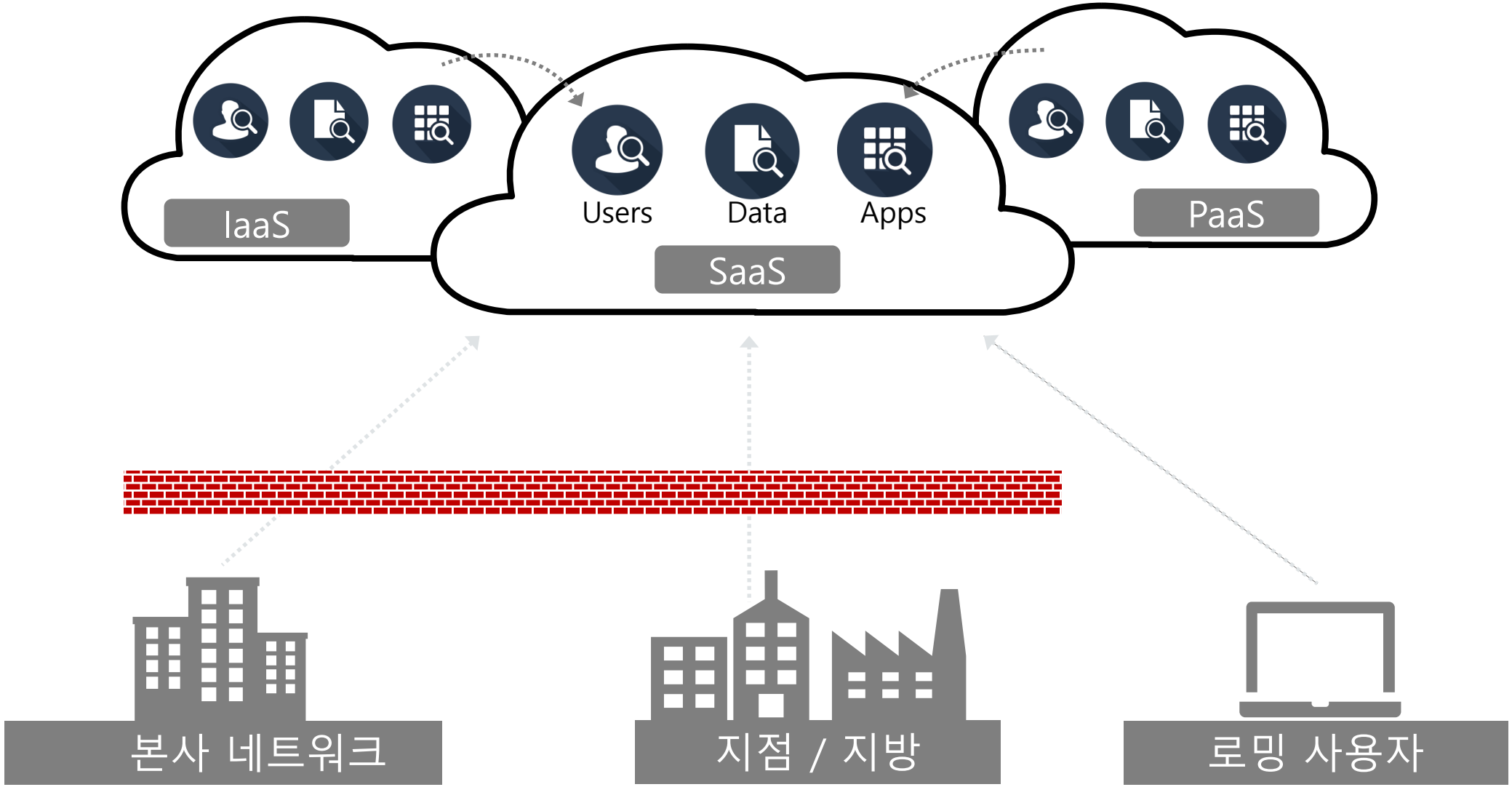
On-prem Security Solutions

Messaging & Collaboration
HR & Skills
Sales & marketing
Finance

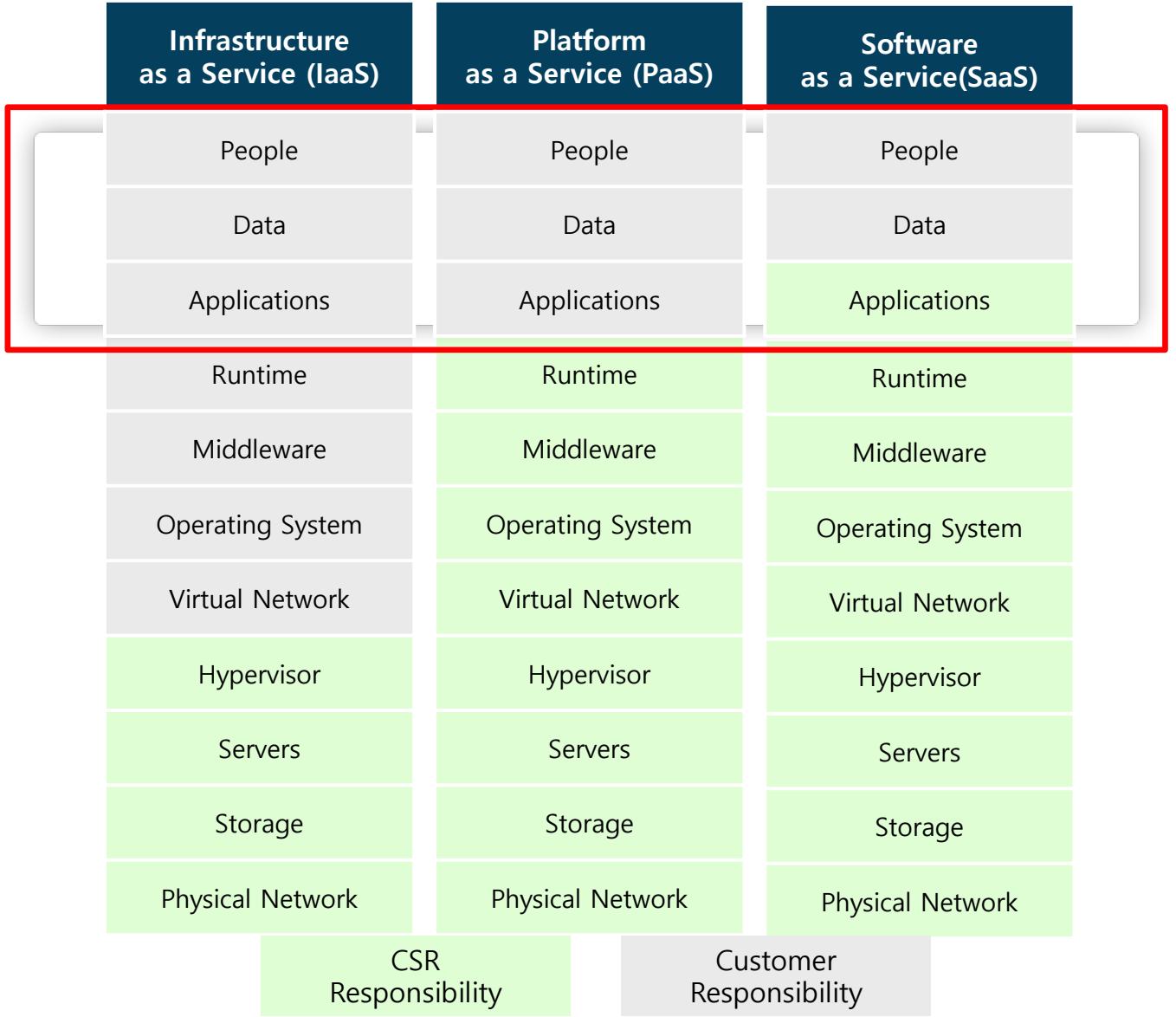
Sharepoint
Apps

App Server
Database

그렇다면 클라우드 보안은?



클라우드 영역별 책임 소재 – SaaS / PaaS / IaaS



*Gartner Research Paper: Mind the SaaS Security Gaps Published: 19 May 2016

클라우드 서비스 사업자의 보안

싱글 플랫폼만 지원

소수의 문제만 해결

보안 전문가나 보안관점으로 접근이 부족

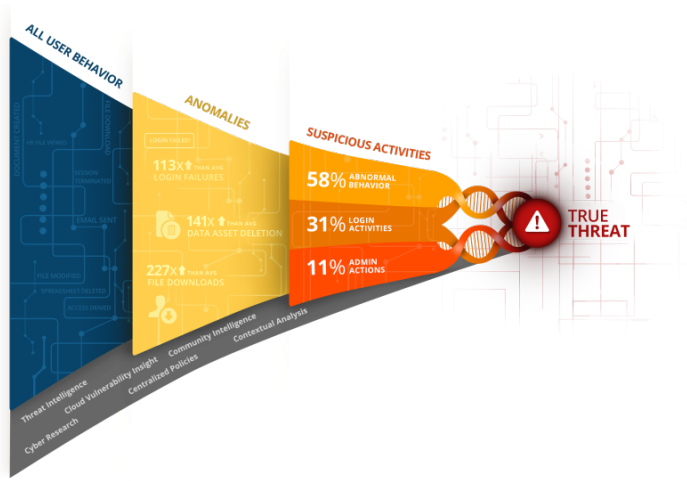
추가 과금

인시던트 관리 부재

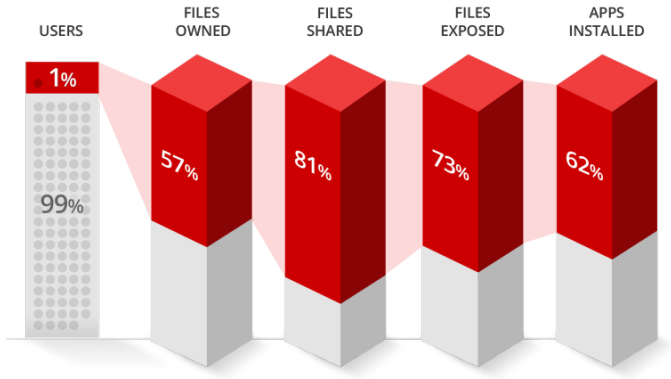
미약한 치료 방안

클라우드 사용 고객이 보호 받고 싶은 대상

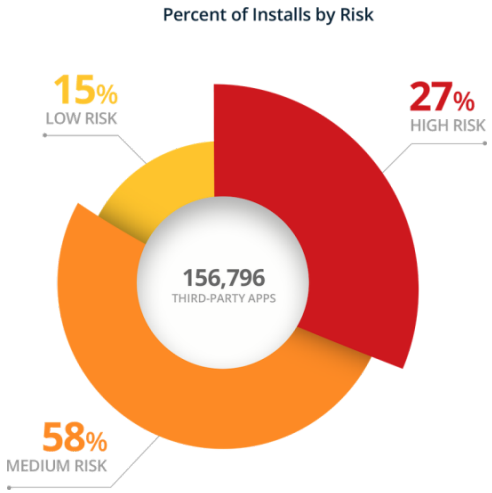
사용자 / 계정



데이타



어플리케이션



Source: CloudLock CyberLab

고객의 주요 고민들

사용자/계정

- 내 클라우드 앱에서 누가 무슨일을 하고 있는지?
- 위협적인 계정을 어떻게 감지할 것인지?
- 악의적인 내부자가 정보를 외부로 유출하고 있는지?

데이터

- 내 클라우드에서 기밀 유지 및 규제해야 할 데이터가 있는지?
- 정책 위반 발생시 어떻게 감지해야 할 것인지?
- 사건 처리를 어떻게 자동화 할 것인지?

애플리케이션

- 앱 사용과 리스크를 어떻게 모니터링 할 것인지?
- 3rd 파티와 연동된 앱이 있는지?
- 위협스러운 앱을 어떻게 찾아내고 관리할것인지?

CASB(Cloud Access Security Broker) 소개

2016년 IT 보안 기술중의 가장 중요한 분야

CASB

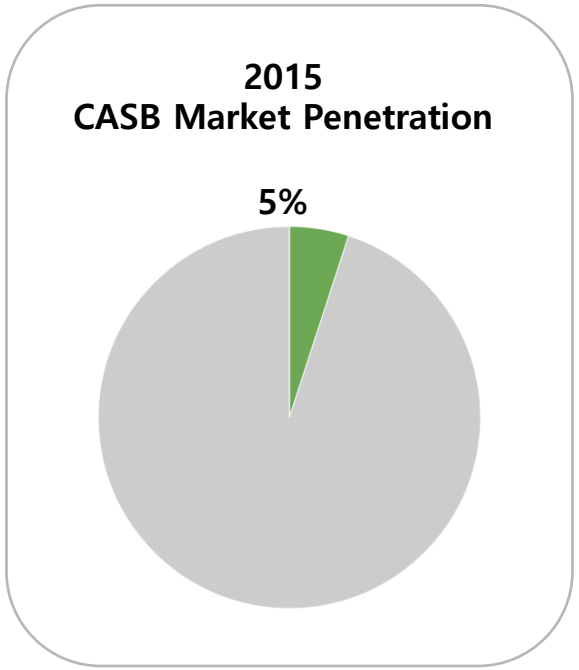
Cloud Access Security Broker

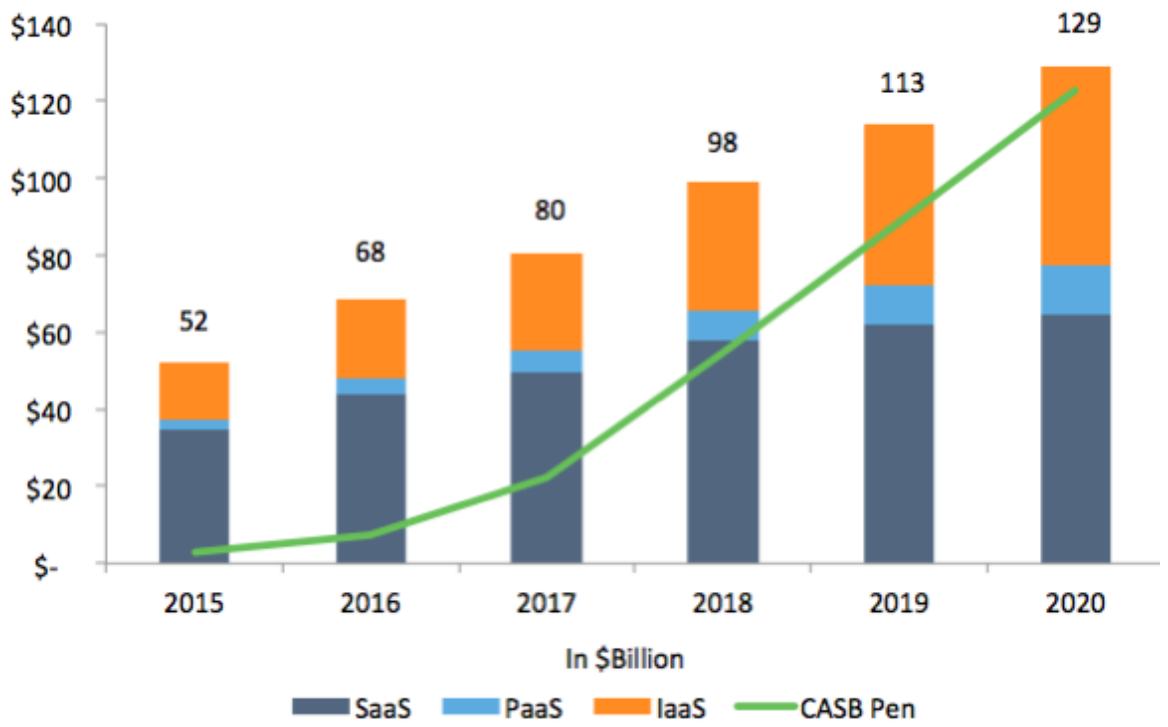
Source: Gartner, 2016

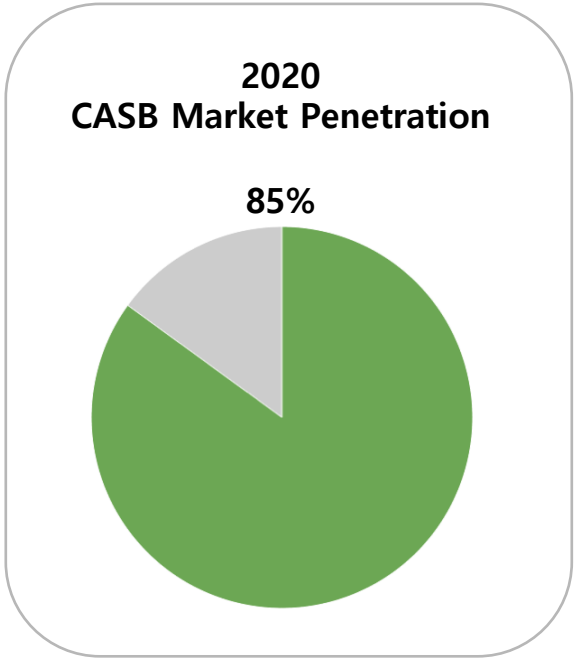
CASB(Cloud Access Security Broker) 시장

- 가트너에 의해서 2012년 정의된 개념
- Gartner 마켓 가이드: “Cloud Access Security Brokers (CASB) 는 클라우드 서비스와 모바일 사용이 심각하게 증가함에 따라 발생되는 보안의 갭을 해결하기 위한 방법이다. CASB는 오늘날의 웹방화벽(WAFs)과 시큐어 웹게이트웨이(SWGs)와 엔터프라이즈 방화벽에서 일반적으로 제공되지 못하는 차별화된 기능을 제공한다. CASB는 모든 사용자나 디바이스에 다양한 클라우드 서비스를 동시에 제어할수 있는 통합 컨트롤을 제공한다”. APIs & Proxies (forward and reverse) 방식으로 제공한다.

CASB 마켓 점유율은 2020년까지 85%까지 **확대**

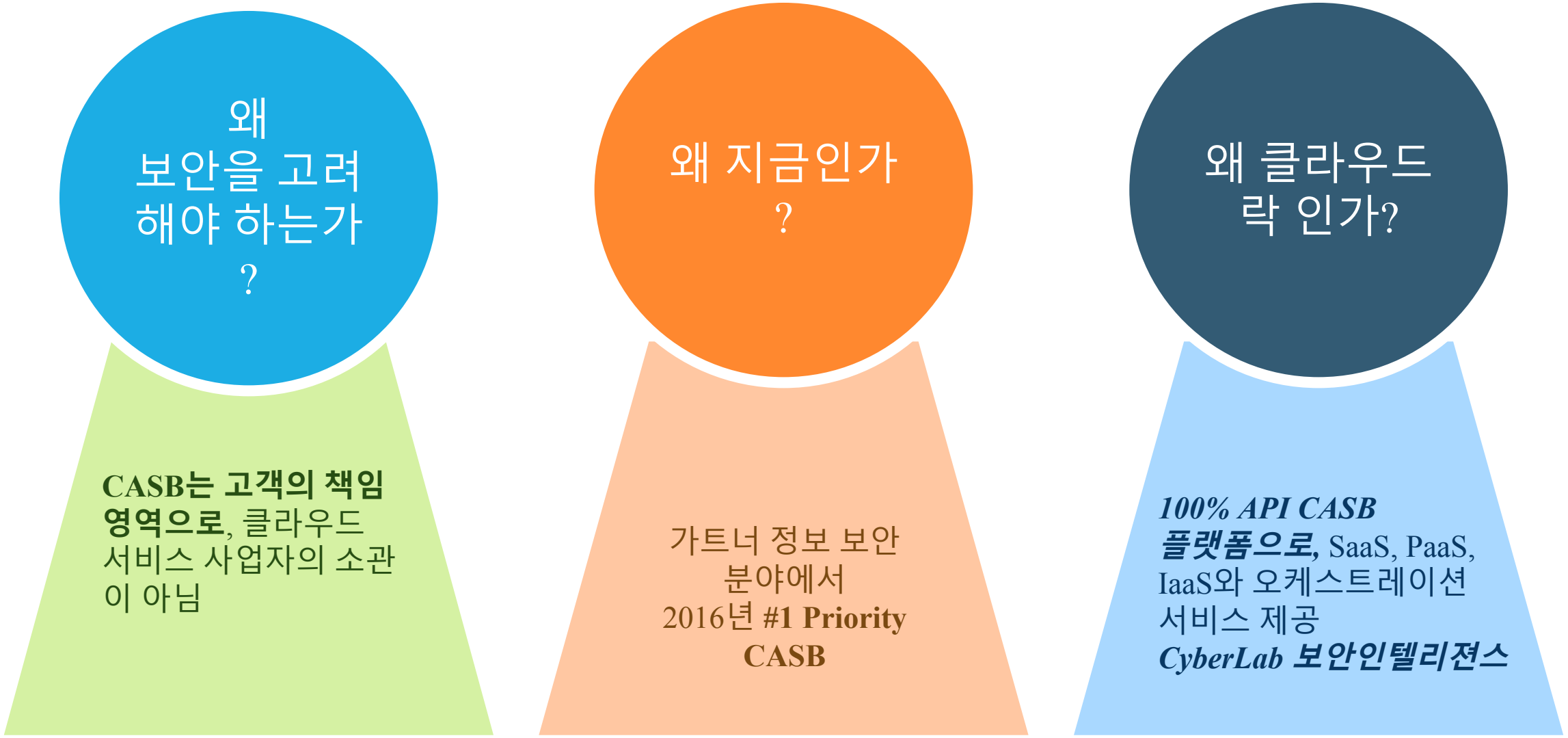






1. 2017년말 CASB $500M Market
2. 2016년말 한국 클라우드 시장규모는 $750M 예측

클라우드 보안을 지금 고려해야 하는 이유?



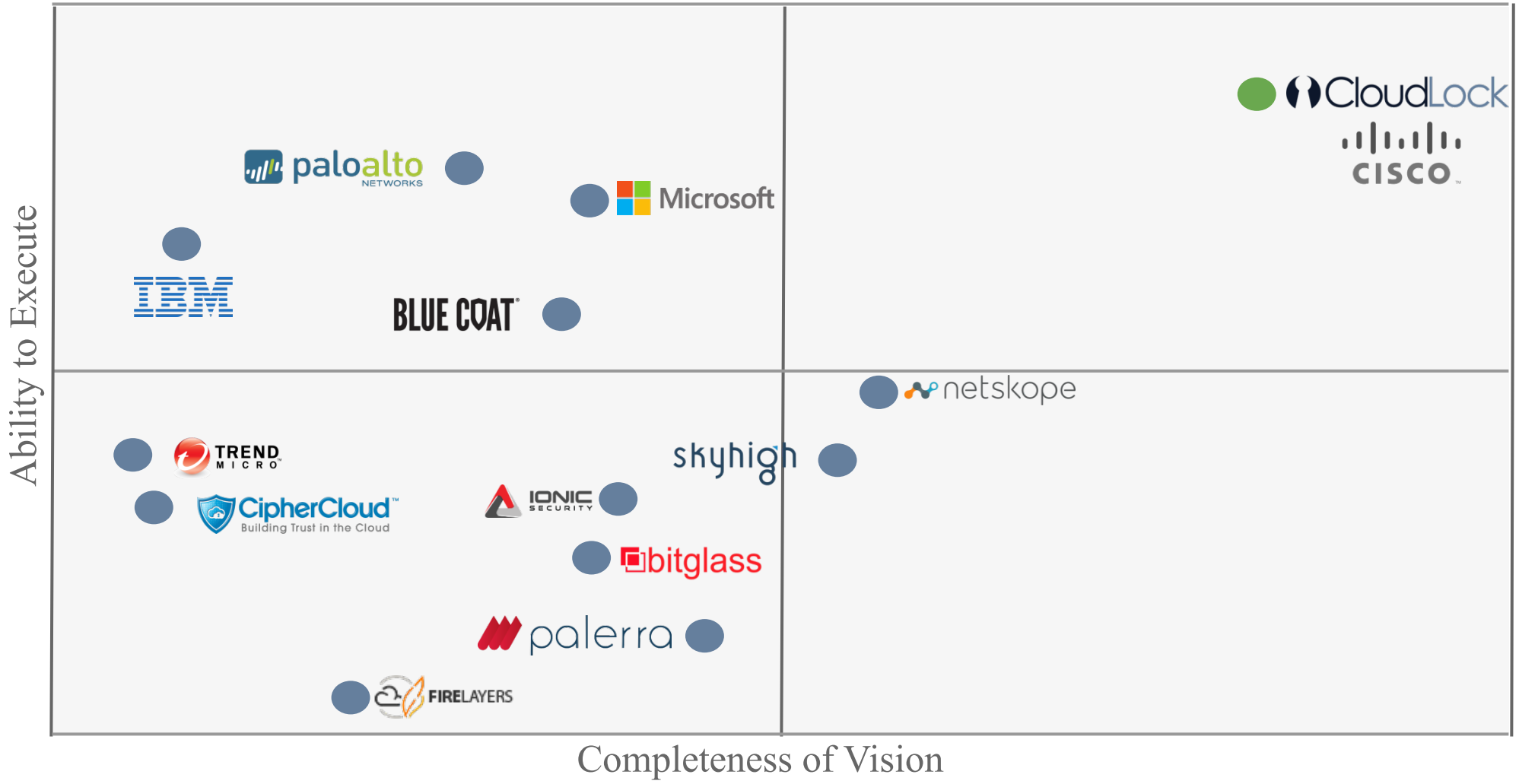
시스코 클라우드락(CloudLock)

시스코 클라우드락(CloudLock)

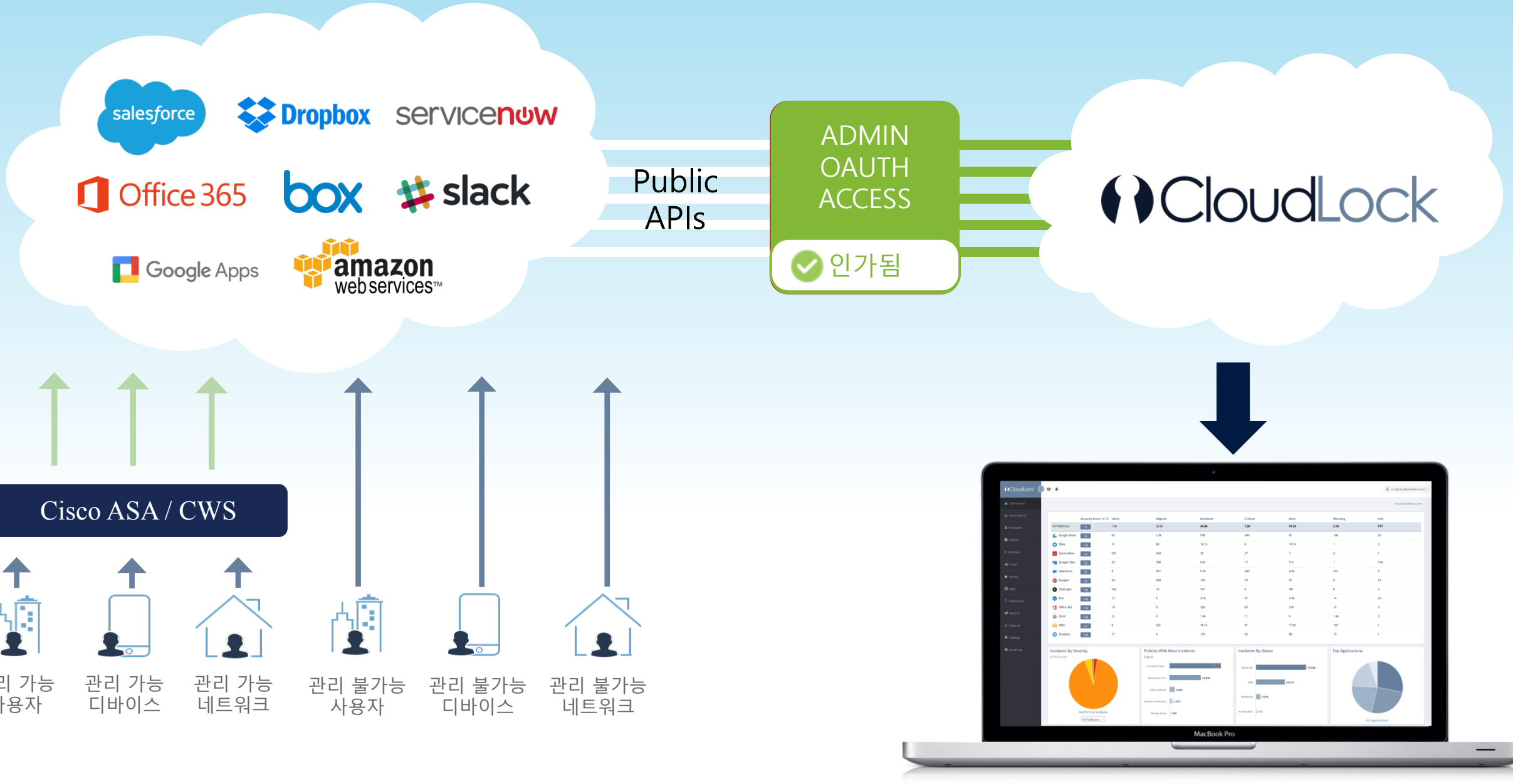
클라우드락은 CASB을 리딩하는 벤더로서, SaaS, PaaS
및 IaaS를 보호하기 위해서 100% 클라우드-전용 API 방식의
사이버 시큐리티 플랫폼을 제공, 전 세계 700여 고객들이 사용

- **IDF Israeli Defense** 인텔리전스에서 설립
- **API 접근법** 클라우드 앱 모니터링의 선구자

CASB 주요 벤더사


paloalto NETWORKS
Microsoft
IBM
BLUE COAT
CloudLock
CISCO
netskope
skyhigh
TREND MICRO
CipherCloud
Building Trust in the Cloud
IONIC SECURITY
bitglass
palerra
FIRELAYERS
Ability to Execute
Completeness of Vision

클라우드락 CASB - API 액세스 (Cloud to Cloud)



클라우드락 플랫폼

CASB for SaaS

클라우드 비즈니스 앱 사용 보호

CASB for IaaS/PaaS

클라우드에서 중요한 인프라스트럭쳐 사용 보호

Cloud Security Orchestration

클라우드 시큐리티 워크플로우

CloudLock Cloud Security Fabric™

클라우드락 플랫폼

클라우드 비즈니스 앱 사용을 보호

클라우드에서 중요한 인프라스트럭쳐의 사용을 보호

클라우드 시큐리티 워크플로우

CloudLock Cloud Security Fabric™

- User Behavior Analytics
- Apps Firewall
- DLP
- Encryption Management
- Configuration Security
- Central Auditing

클라우드락 시큐리티 페브릭™

Office 365
salesforce
box
Google Apps
Dropbox
slack
servicenow

SaaS

클라우드상에서의 비즈니스앱 사용을 보호

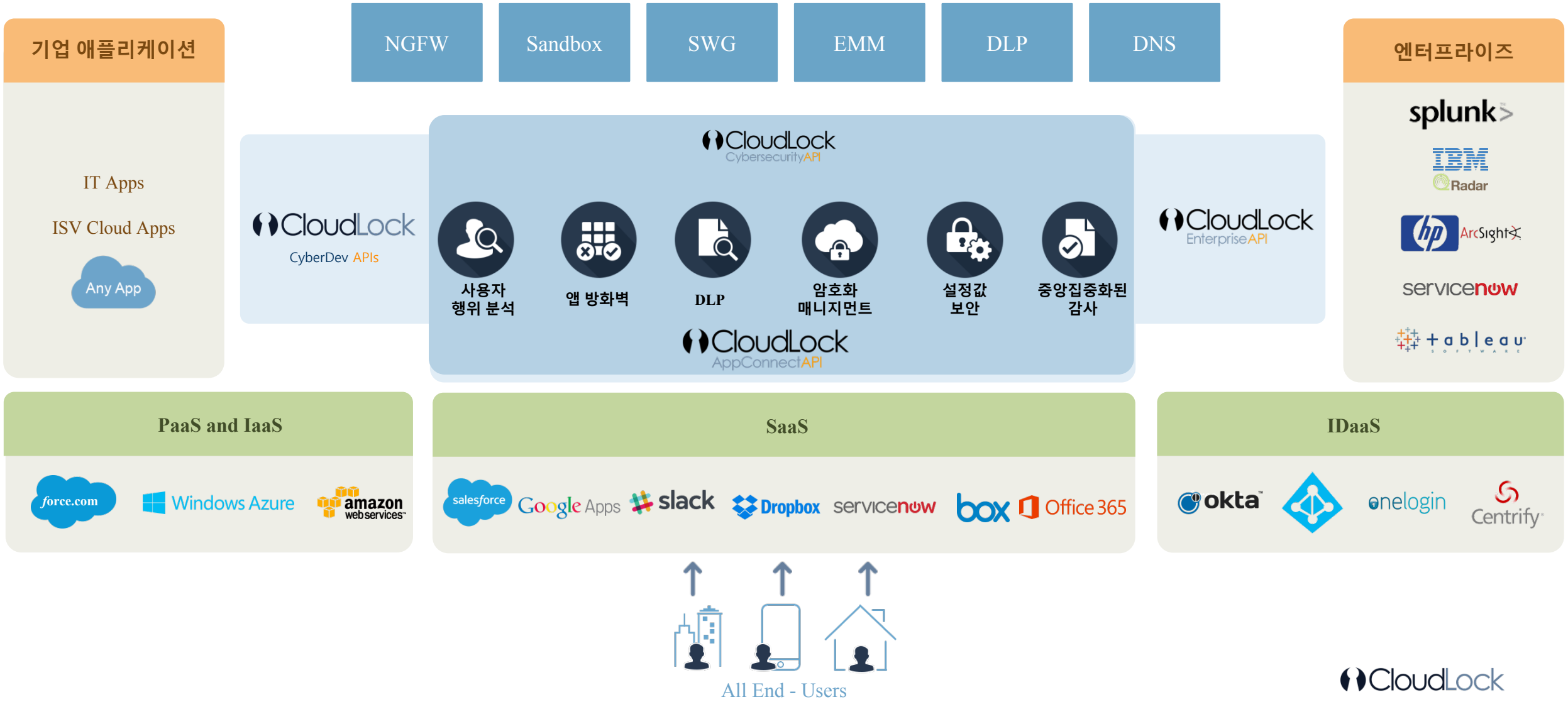
IaaS / PaaS

클라우드상에의 주요한 인프라스트럭쳐의 사용을 보호

amazon web services
force.com

CloudLock

클라우드락 사이버 시큐리티 패브릭 – 동작 원리



클라우드락 사이버랩 & 거대한 클라우드 사용 데이터셋

CloudLock CyberLab

이스라엘 국방 사이버 인텔리젼스와 결합하여 제공
전 세계에서 가장 큰 CASB & 클라우드 시큐리티 플랫폼

클라우드 사이버
시큐리티 / 연구 조사

1B+
1일 처리량

규정 위반 조사

10M+
1일 사용자수

사이버 시큐리티 평가

160K
애플케이션 수

클라우드 2016 최우선 위협에 대한 대응

2016 Top Threats	CloudLock
데이타 탈취	✓
취약한 계정 정보과 접속 제어	✓
보안에 취약한 인터페이스와 API	✓
계정 탈취	✓
감염된 내부자들	✓

Source: Cloud Security Alliance (CSA), 2016

cloud CSA security alliance℠

클라우드락의 기업 클라우드 보호 방법

데이터 유출은 클라우드 기반 DLP로 방어
- 민감한 데이터를 보호하기 위해 SaaS/PaaS 환경을 끊임없이 모니터링
- 퍼블릭 클라우드 앱을 정보유출 방지 솔루션으로 보호함
- 라이프 사이클의 모든 활동을 관리하고 응답을 자동화함

규정 준수(컴플라이언스)는 리포팅 및 정책
- PII, PCI, PHI, 그리고 IP 데이터를 발견하고 제어
- PCI DSS, HIPAA, SOX, CIPA, FISMA와 FERPA와 같은 규정을 준수
- 자동화된 정책 리스크를 컨트롤 함

CloudLock
차별화 기능

클라우드 멀웨어는 앱 방화벽으로 방어
- 쉐도우 앱이 기업 환경에 끼칠수 있는 위험을 탐지
- 앱에 대한 인사이트 확보 가능
- 앱 작동 여부를 제어

해킹당한 어카운트는 UEBA로 제어
- 유저 활동을 모니터링하여 이상을 감지함
- 권한이 있는 유저들의 액세스 변화를 트래킹 함
- 해킹 발생 시 실시간으로 보안팀에 경보

* UEBA : User and Entity Behavior Analytics

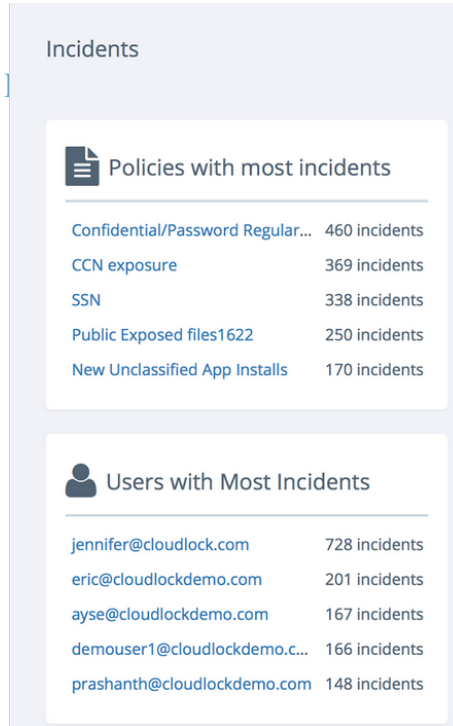
보안 관리자를 통한 보안 운영과 포렌식
- 이상 행동을 조사함
- 중요 행동의 감사 추적을 문서화 함
- 컴플라이언스로 포렌식을 위한 증거를 유지

CASB 핵심 영역 - 4가지 주요 요소

1 가시성	• Shadow IT와 허용된 어플리케이션 컨트롤 파악 • 통합된 클라우드 서비스 사용량과 유저가 데이터에 접근한 디바이스와 장소 정보 제공
2 규정 준수	• 데이터 레지던스와 법규 및 표준에 대한 컴플라이언스 준수 • 클라우드 사용 용도를 확인할 수 있고 특정 클라우드 서비스의 리스크를 확인
3 위협 방어	• 원하지 않는 디바이스와 사용자 그리고 클라우드 서비스에 접근하려는 애플리케이션들로부터 보호 • 위협 인텔리전스와 멀웨어 인식에 따른 사용자와 개체의 행위 분석(UEBA)
4 데이터 보안	• 원하지 않는 데이터 분류(카테고리 저장) 및 조회를 방지하는 데이터 중심 보안 정책을 실행하는 기능 제공 • 민감한 데이타에 접근하는 사용자 행위를 모니터링하거나 권한 상승을 모니터링 • 감사, 경고, 차단, 격리, 삭제, 암호화/토큰화하는 수준의 정책들이 적용

* Shadow IT : 조직에서 미처 등록하거나 관리하지 못하는 애플리케이션, 모바일, 기기 등

1 가시성(Cloud Native API-Based 사이버시큐리티플랫폼)



우리회사 클라우드 App에서 사용자들이 무슨일들을 하고 있나?

사용자 계정에 문제가 생긴것을 어떻게 알수 있지?

우리회사 클라우드에는 민감정보 / 위험한 정보 / 규제해야 되는 정보들이 있나?

우리회사 클라우드에서 민감한 정보를 어떻게 암호화 / 격리 시킬수 있나?

회사 직원들이 어떤 Shadow Apps 을 쓰고 있지?

Shadow Apps 이 제재를 받는 사이트와 연결이 되어 있는 거는 아닌가?

PaaS and IaaS

force.com

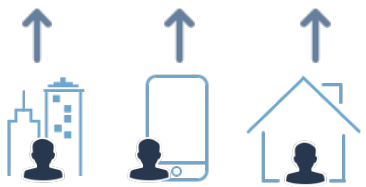
amazon web services

SaaS

salesforce Google Apps slack Dropbox servicenow box Office 365

IDaaS

okta onelogin Centrify



최종 사용자

2 컴플라이언스 (70여개 이상의 미리 정의 된 정책을 제공)

PII

- SSN / ID numbers
- 운전면허증 번호
- 패스포트 정보

PHI

- HIPAA
- Health Identification numbers (global)
- 처방 정보

Education

- 부적절한 컨텐츠
- 학생 대출 신청 정보
- FERPA(Family Educational Rights and Privacy Act) compliance

PCI

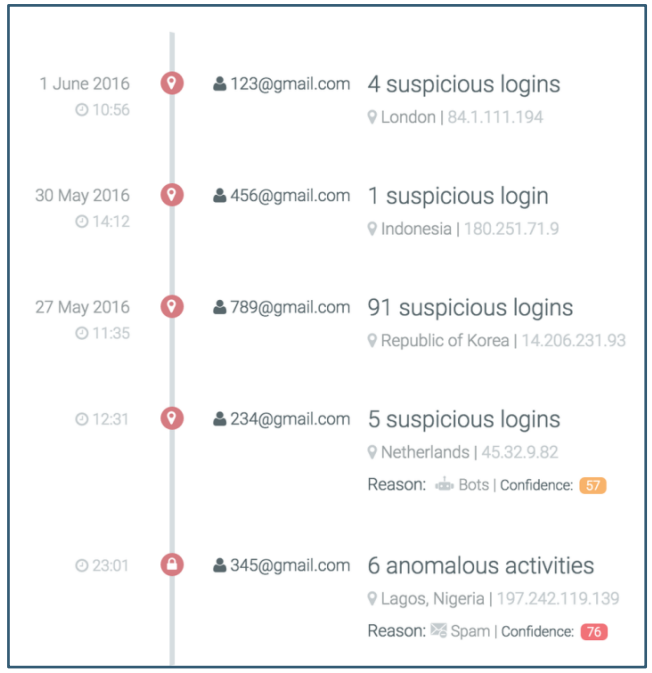
- 신용카드 번호
- 은행 계좌 번호
- SWIFT codes

General

- 이메일주소
- IP 주소
- 패스워드 / 로그인 정보

3 위협 보호

1. 리스크 벤치마크



2. 위협 경고 제공

2. Unusual behavior for user **TzQzwWgKJJUj5l5I2vC9fpkEKekHt8Hu4vsOc=**

Activity breakdown for this user:

Timestamp	Country	City	Activity	IP Address	IP Risk
May 11th 2016, 23:20:16.000	United States	New York	user login	162.243.XX.XX	71 (Bots)
May 11th 2016, 23:15:21.000	United States	New York	user logout	162.243.XX.XX	71 (Bots)
May 11th 2016, 22:36:12.000	Chile	Santiago	user login	191.101.XX.XX	
May 11th 2016, 22:34:21.000	United States	Raleigh	user logout	107.13.48.36	
May 11th 2016, 22:27:02.000	United States	Raleigh	user login	107.13.48.36	

3. 침해 사고 타임라인 제공

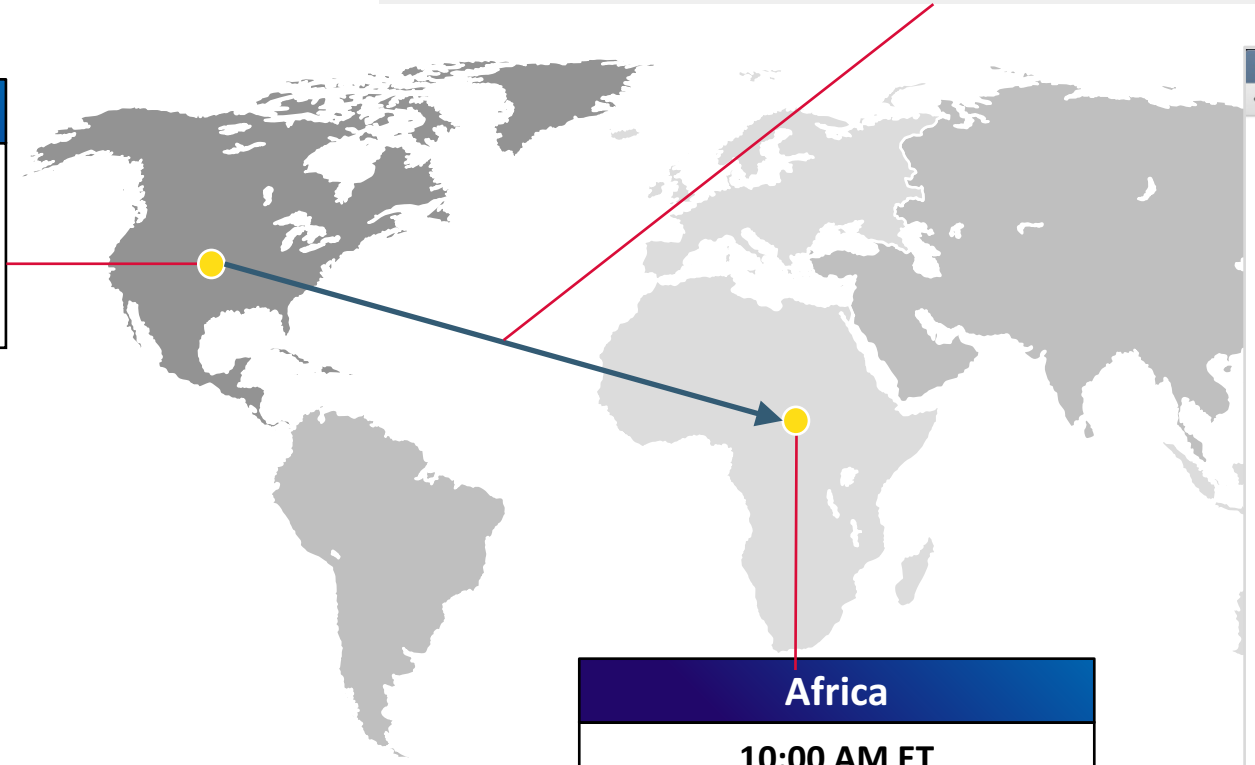
4 사용자와 개체의 행위 분석(UEBA)

- 미국에서 중앙아프리카까지의 거리: 7,362 miles
- 시속 800 마일로 9.2시간의 비행시간이 소요됨

North America

9:00 AM ET

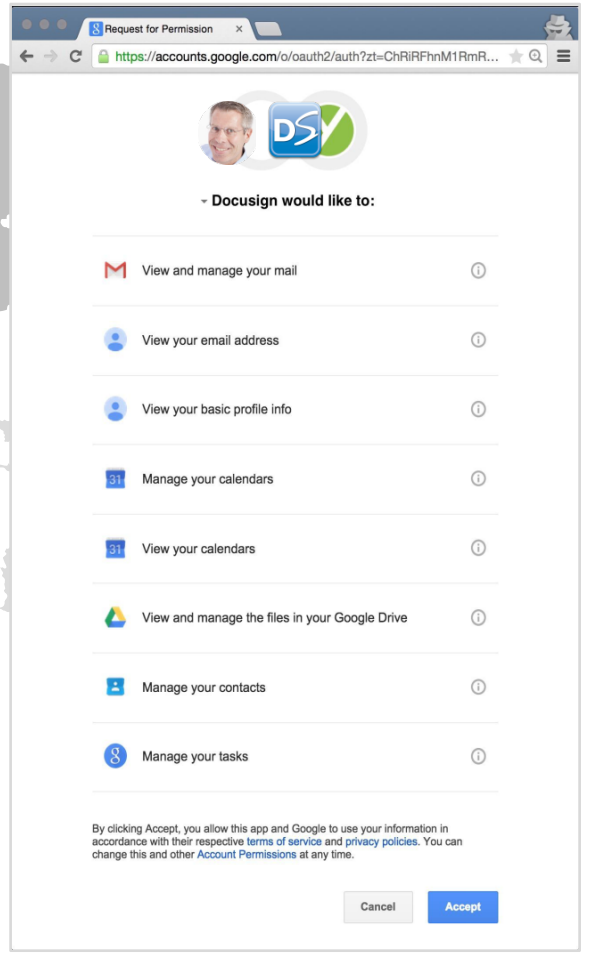
- Login to: Google Apps



Africa

10:00 AM ET

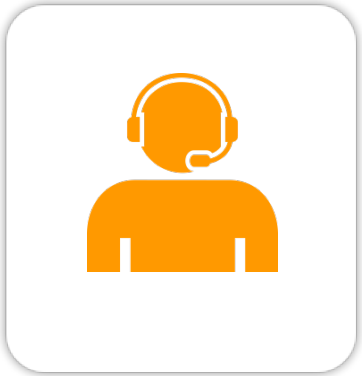
- Data export from: salesforce



의심스러운 로그인과 행위들은 데이터 탈취나 시스템 감염행위를 목적으로 계정 탈취를 했다고 경고창을 띄웠다.

클라우드락 고객의 혜택

10분 이내에
정책 적용 가능

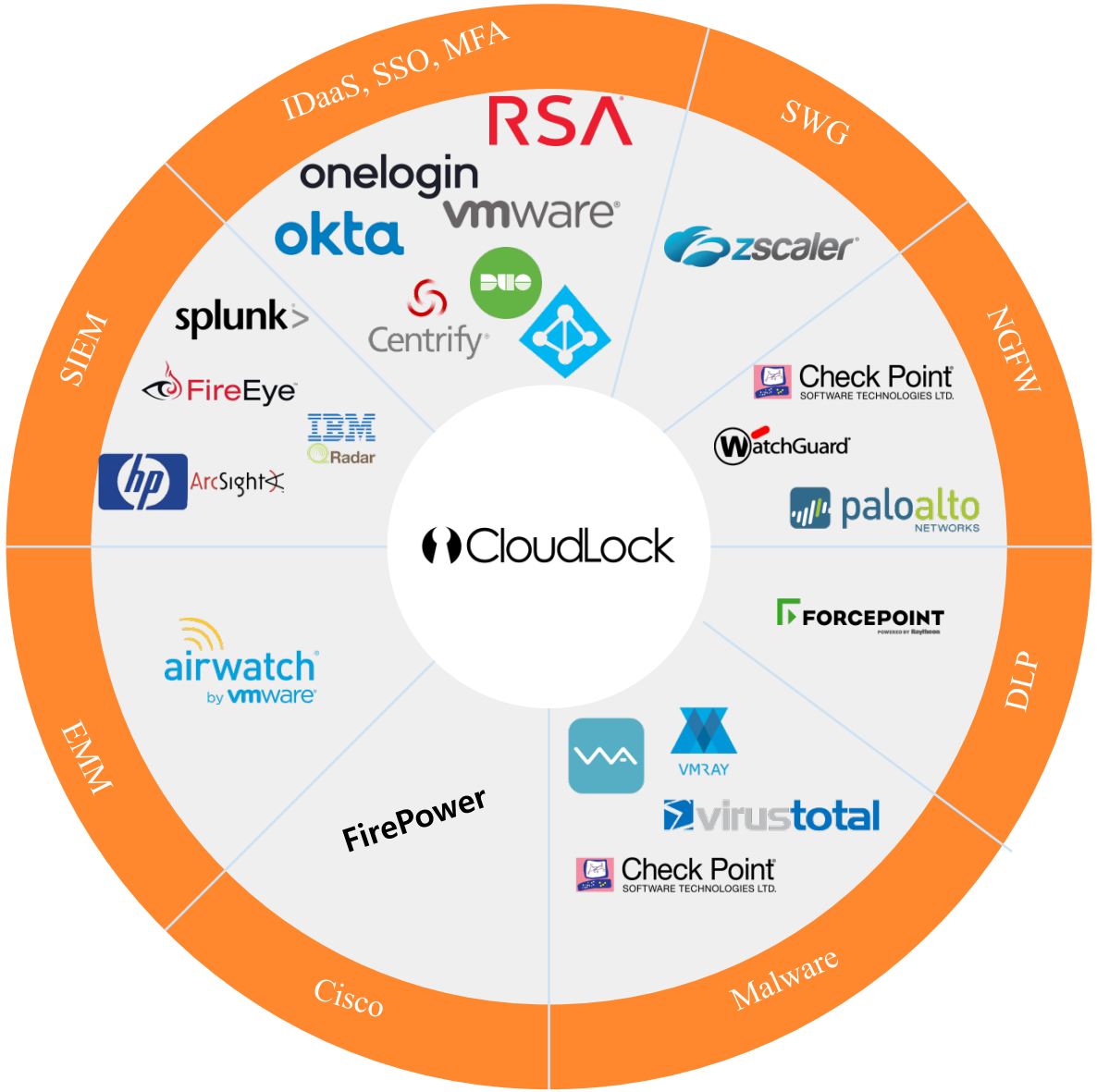


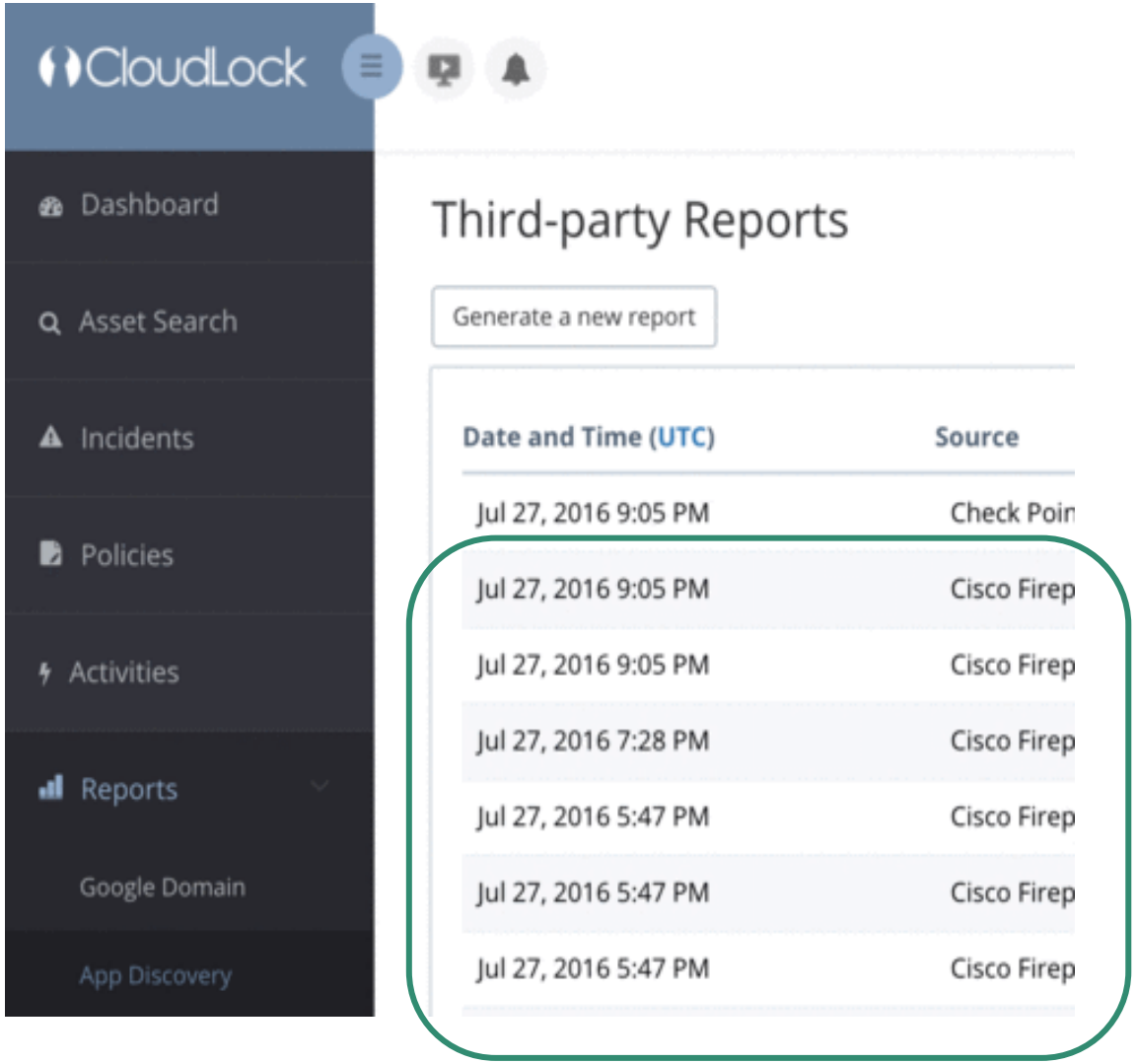
클라우드락 사이버랩을 통한
인텔리젼스 고객 지원 팀

클라우드락 커넥트
커뮤니티 인사이트 제
공

세계 최고의 시큐리티
전문가의 백업 제공

다양한 파트너 에코시스템 구축





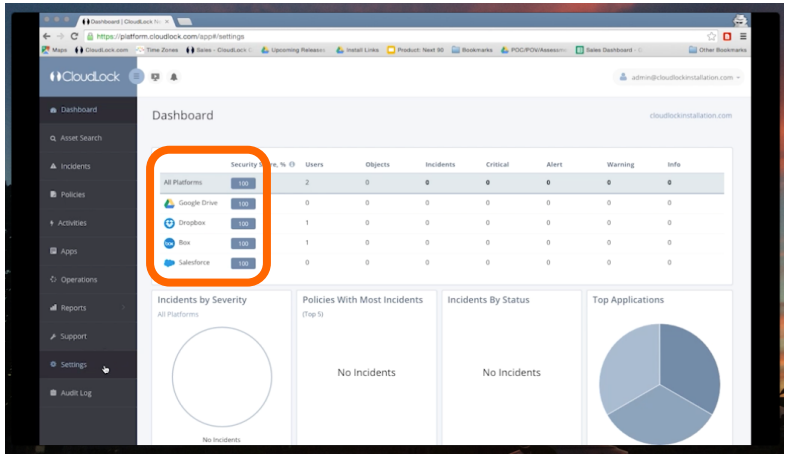
고객 FAQ

질문

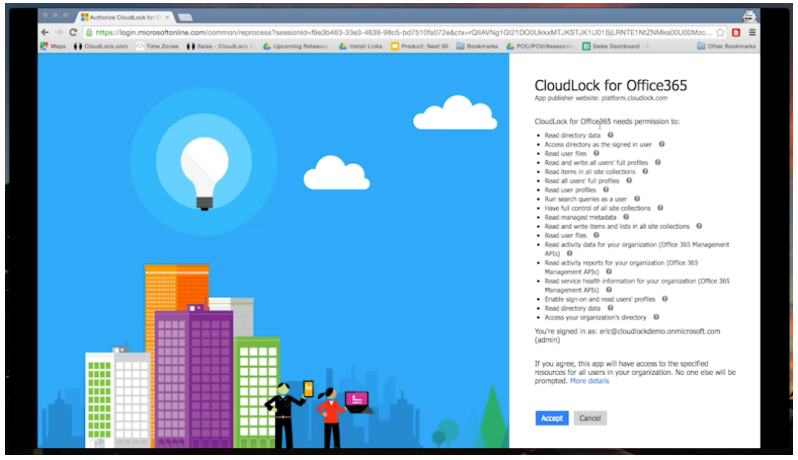
1.Office365에 적용 시 클라우드락과 연동방식에 대해 구체적으로 설명

클라우드락은 클라우드 시스템과 API연동방식으로 구현되어 있습니다. 클라우드락에서 Apps API를 통해서 Office365을 선택하고 어드민 계정으로 로그인하여 Office365에서 필수권한을 허용하면 설치가 완료되며, 기존 Office365사용중에도 가능합니다. 연동까지 시간은 약 10분 정도 소요됩니다.

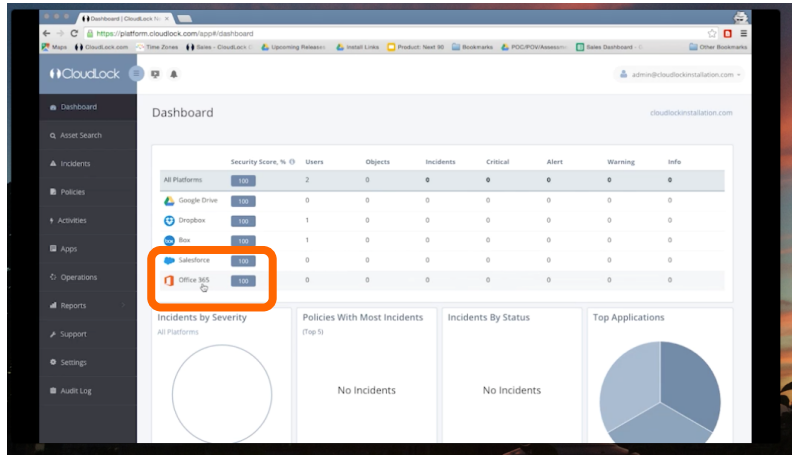
1. 클라우드락 대시보드에서 Office365을 설치하는 화면입니다.



2. Office365 관리자 계정이름과 해당 관리자가 가진 권한이 나타나면서 클라우드락 계정 담당자가 관리자 권한을 획득하는 것을 인증하는 순서입니다.



3. 대시보드에 Office365 앱 제어 화면이 생성되고 관리자 모드로 운영을 할 수 있게 됩니다.



질문

2. 연동 시 MS와 협의가 필요한지 여부 확인

사전협의가 필요하지 않습니다. 클라우드락은 오픈 API로 연동되기 때문에 1번 사항에서 설명 드린 대로 권한 인증만 필요합니다.

3. 연동 시 고객사에서 고려해야 할 사항 명시 (AD, SSO 오픈 등)

어드민 계정 정보만 클라우드 락에 연동해 주시면 됩니다. 1번 연동방식에서 설명드린 내용처럼 AD, SSO의 별도 조정은 필요하지 않습니다.

질문

4. Cloudlock 에서 제공하는 보안 기능(특히 office365 관련)에 대해 구체적으로 설명

① Office 365에 있는 중요 정보를 검색하고 외부 유출을 차단하고
② 보안 정책과 컴플라이언스에 위배되는 내용을 사전에 감지 차단하고 가이드에 기반하여 사용 권고

1 Office365사용자 그룹을 전체 또는 특정그룹으로 설정하여 모니터링

Monitoring Scope

The monitoring scope for a platform is the set of user accounts to be monitored by CloudLock policies. For Office 365, the monitoring scope is established by specifying groups established in your Office 365 platform. The monitoring scope defaults to monitoring your entire platform. To change this setting to monitor only specific groups, use the *Monitoring Scope* tool in the *Settings* panel:

2 Office365사용자가 6가지 유형(누가 정보에 접근할수 있는지, 특정그룹에서 특정사용자가 접근권한을 줄것인지, 외부 도메인(조직)의 인증받은 사람에게 허락할것인지 등)의 정보 접근 및 외부 공유 권한을 부여하고 예외조항으로 특정사람들에게는 컨텐트가 공유되어도 모니터링하지 않게 설정이 가능

Exposure in CloudLock for Office 365 Policies

Exposure refers to the kinds of users who can access information, ranging from specific internal individuals to internal groups, people external to a domain (and organization), and so on. CloudLock offers the following exposure categories for policies specific to Office 365:

- **Public with link** means a link to the content has been made public (this can result in content being even more widely exposed, as links themselves can be easily exchanged).
- **Shared with everyone** means the content is available and searchable by anyone.
- **Shared with everyone except external users** means the content is available to anyone inside your domain.
- **Shared exclusively with internal users** means the content is available to anyone outside your domain, but not to anyone inside the domain.
- **Shared with any external user** means at least one user ID outside your Office 365 domain has access to the content even though sharing may not be completely public.
- **Specific shares** can include both internal and external users, listed by ID and/or domain.
- **Exceptions** are specific user IDs that do not trigger incidents even when the content is shared with them. This list is also known as a *whitelist*.

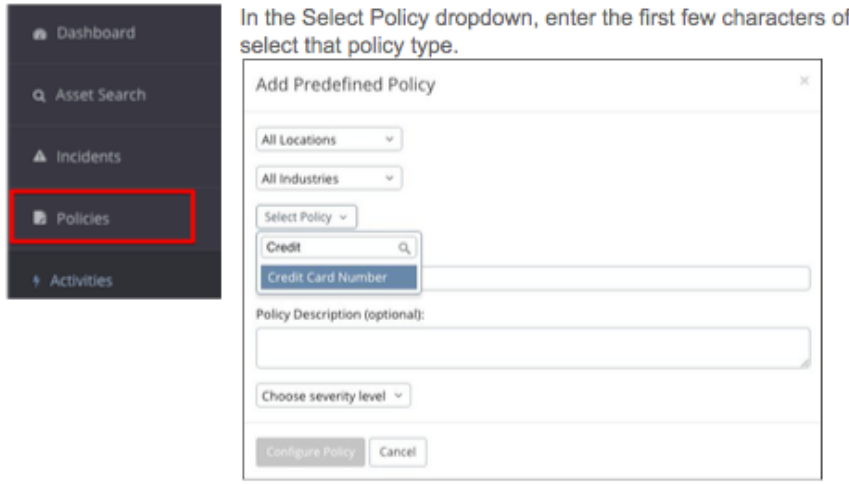
4. Cloudlock 에서 제공하는 보안 기능(특히 office365 관련)에 대해 구체적으로 설명

③ Office 365에 중요 정보를 확인하고 누가/어느 장소에서 접근을 하는지,어디서 생성했는지를 확인합니다.

④ 사용자에게 영향도 없이 Office 365 보안 정책을 적용하고

3 클라우드락에서 사용자가 특정장소에서 Office365에 접속하고(해당 국가가 허용국가) 사용자도 사전에 인증을 받은 사용자인지 확인

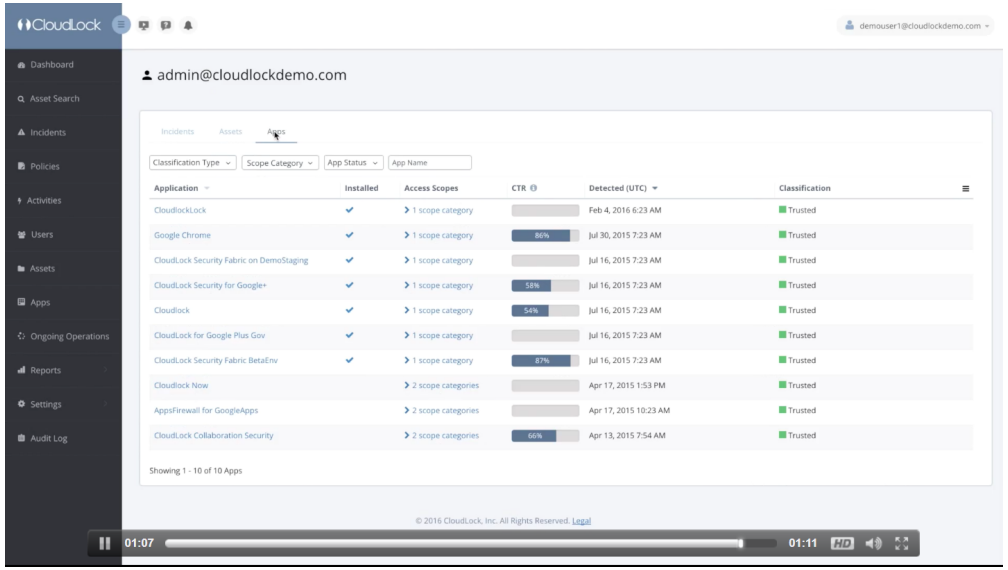
4 사용자가 Office365을 사용하는 중에도 중단없이 정책항목을 선택하여 적용하면 바로 운영에 반영



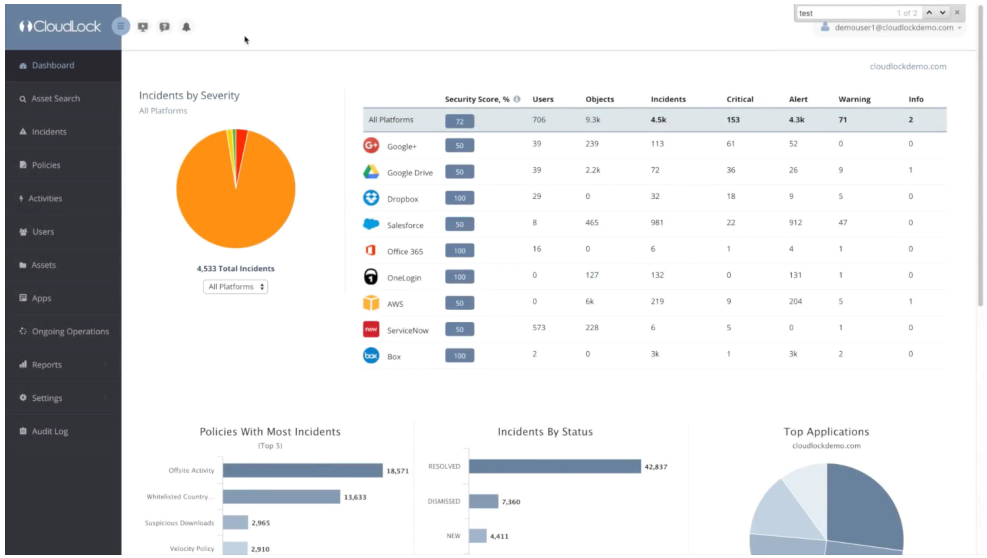
4. Cloudlock 에서 제공하는 보안 기능(특히 office365 관련)에 대해 구체적으로 설명

⑤ 보안 정책과 차단을 관리자를 통해서 운영 및 자동화하고
⑥ 보안 인시던트 정보를 대시보드로 보여주며, 고객사 사용중인 보안제품(SIEM, IPS)와 연동

5 관리자를 통해서 보안 정책 차단을 자동화

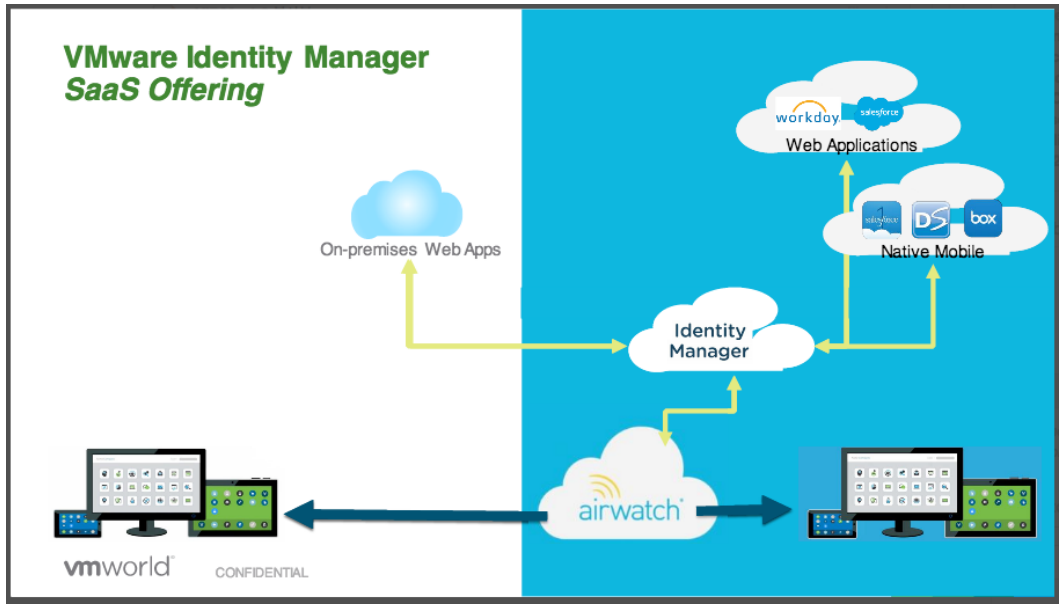


6 보안인시던트 정보를 대시보드로 보여주며, 고객사 사용중인 보안제품(SIEM, IPS)와 연동



5. 직원들이 개인적으로 사용하는 클라우드(dropbox 등)가 있다면, 이를 제어할 수 있는 방법이 있는지 확인(없다면, 개인용은 막고 기업용 box를 Cloudlock 과 연동하여 제공 방안)

클라우드락에 등록되어 있지 않은 클라우드를 제어하기 위해서는 회사 지급 단말(노트북,핸드폰, 스마트 패드)을 사용하는 유저는 노트북은 고객사에서 사용하시고 있는 DLP와 매체제어 그리고 인증 솔루션을 통해서 **접속이 허용된 사이트와 애플리케이션만 접속해서 사용하도록 설정이 되어 있고** 나머지 모바일 단말은 **MAM(Mobile Device Management) 솔루션을 사용**하여 인증단계부터 개인용으로 클라우드에 접속 하는 것을 차단할 수 있습니다.

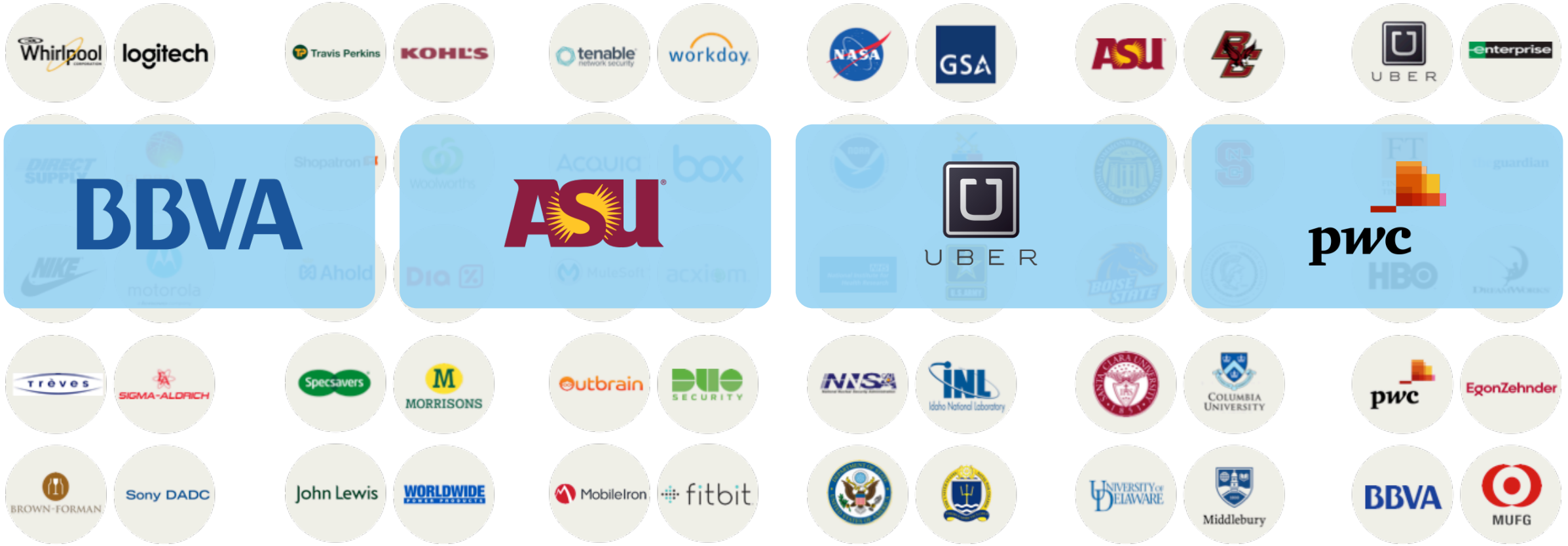


예) V사 MAM 솔루션의 적용

고객사례 및 맺음말

고객 레퍼런스 : 700개 이상의 각 산업별 선도고객

제조업 | 리테일 | 하이테크 | 퍼블릭 | 하이에듀케이션 | 기타

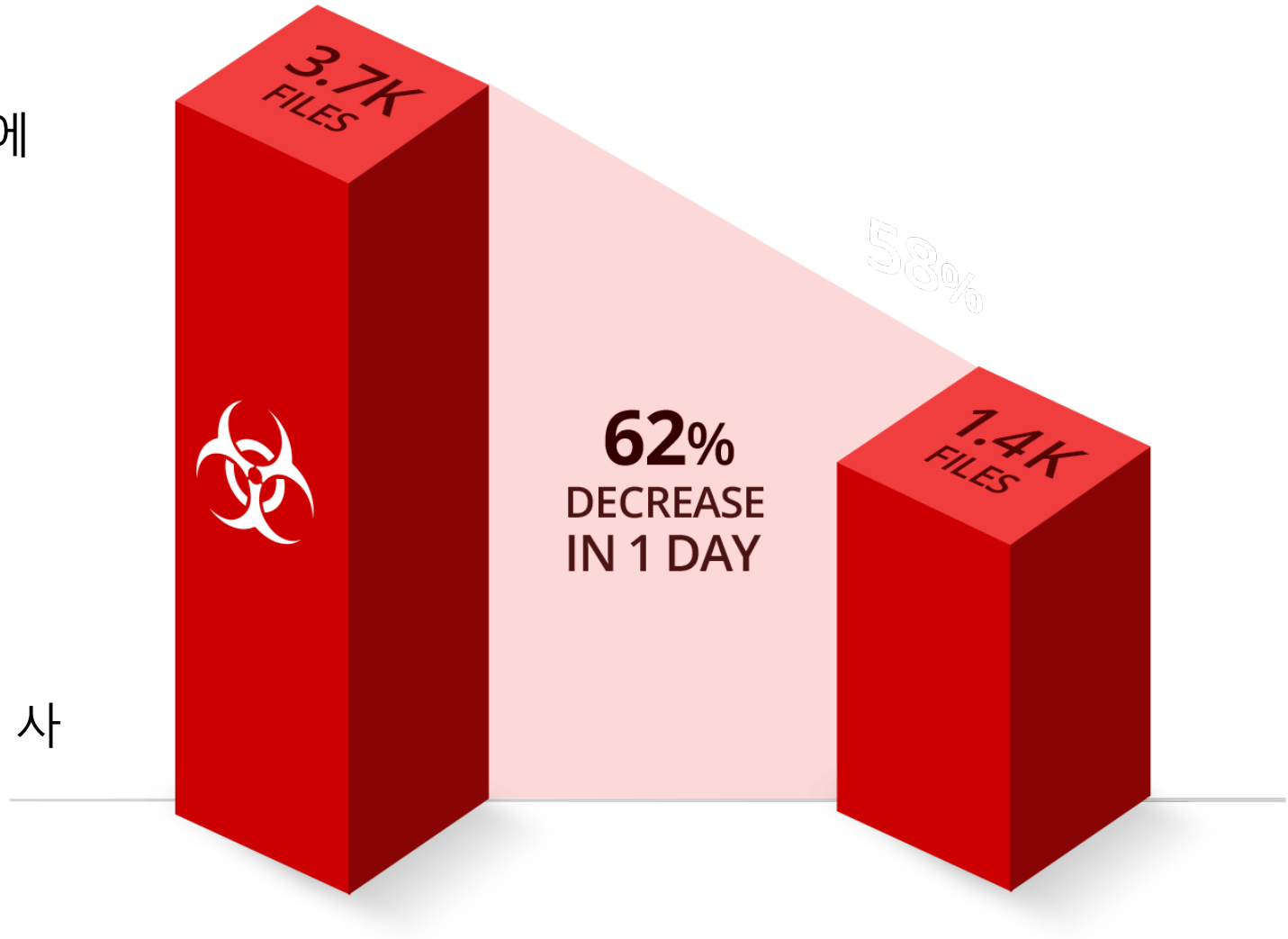


고객 성공 사례: 신속한 ROI 경험

- 미국 소재의 여행사
- 회사 내부 파일이 외부 사용자에 대량 노출
- 클라우드락을 통해 공공

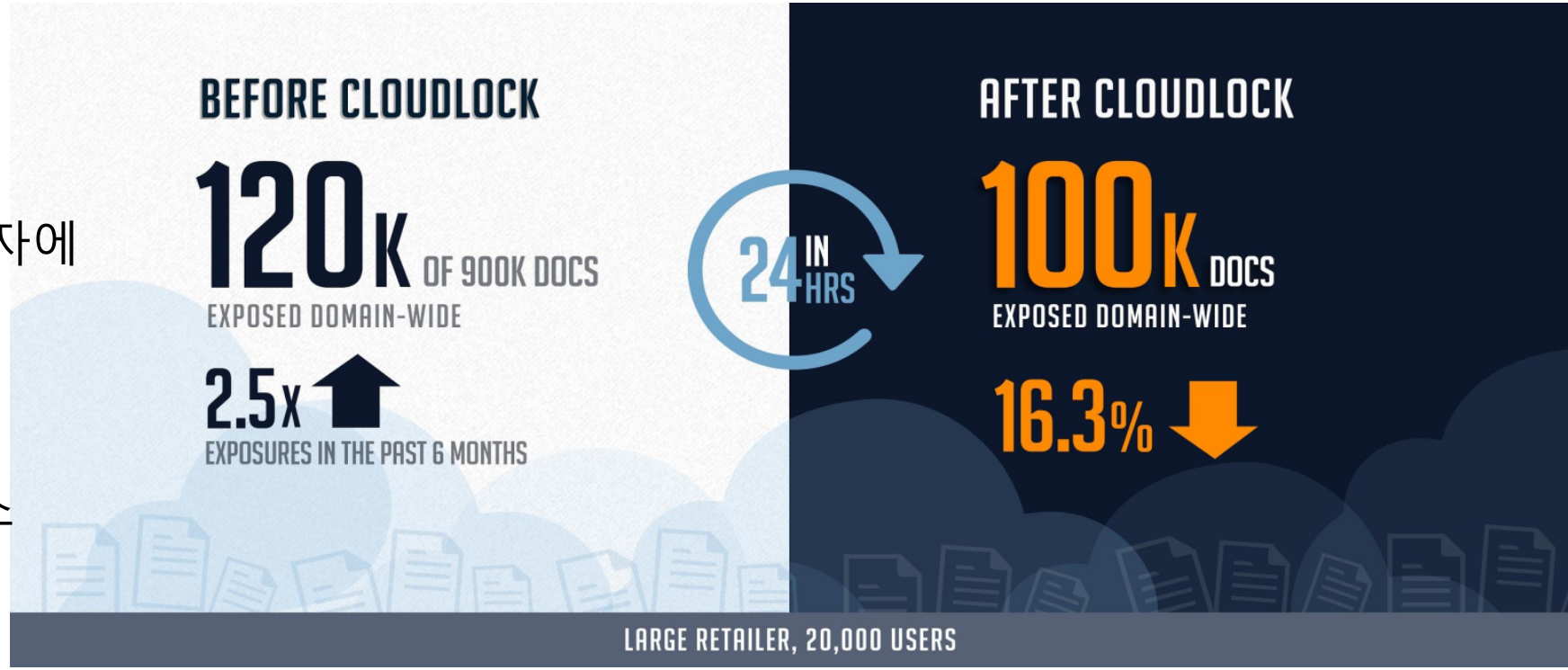
  노출도가 62% 감소함
- 핵심사용자에 대한 공공

  노출도 확인 및 관리
- 신속한 ROI 구현
- 임직원 보안교육으로 클라우드 사용에 대한 보완



고객 성공 사례: 신속한 교정

- 미국 소재의 유통회사
- 회사 내부 파일이 외부 사용자에 대량 노출
- 클라우드락을 통해 공공 노출도가 하루에 16.3% 감소



고객 성공 사례: 데이타 가시성

Ahold Delhaize

Stop&Shop · Hannaford · FOOD LION · Peapod

- 미국&유럽에서 375,000명의 임직원이 근무하는 6,500개 가맹점을 가진 푸드도매상
- 안전한 클라우드 사용및 글로벌 대량 데이터에 대한 안전한 클라우드사용
- 클라우드락 시큐리티 적용
- 글로벌 클라우드 사용에 대한 가시성제공
- 중요데이타에 대한 외부 노출 리스크제거
- 클라우드 플랫폼 사용자에 대한 제어

"클라우드락이 우리에게 제공해주는 가장 큰 장점은 사용자가 어떤 행동을 하고 있는지를 볼수 있다는 것이다. 어떤 데이타를 클라우드에 저장하고 현명하게 위협에 대처할수 있는 방법을 익힐수 있었다. 뉴스채널에 우리 회사가 나오는 것을 원치 않으며 클라우드락이 없이는 어떤 데이타가 외부로 흘러가고 있는지 그것을 어떻게 적절히 관리할수 있는지 알수 없었을 것이다"– David Duchan

Information Security Engineer

클라우드락의 강점

클라우드기반	바로 적용해서 기능 구현이 가능한 100% 클라우드API 기반의 사이버 시큐리티 플랫폼 - 설치 시간 10분, 설치후 바로 적용
관리 / 운영 용이	.클라우드 일어난 행위를 소급해서 확인할수 있는 보안 분석 .퍼블릭 클라우드 관리자가 네트워크, 프락시 또는 게이트웨이와 상관없이 공용 API를 통해서 유저에게 전혀 영향을 주지않고 관리
다양한 클라우드 환경수용	.SaaS, PaaS, IaaS, and IDaaS가 적용 대상 .다양한 보안 파트너 에코시스템을 통한 기존 운영환경과의 통합 적용
스마트 인텔리전스제공	.CyberLab(이스라엘과 미국 기반의 인텔리젼스 제공)과 대량 사용자 커뮤니티의 신뢰도 제공
다양한산업기반 고객보유	.각 산업별 다양한 고객을 보유(산업별/유저별 다양한 보안 대응 널리지) : 700개 이상 고객

THERE'S NEVER BEEN A

BETTER TIME

to make the impossible possible