Lead the future
전자신문

10 YEARS ANNIVERSARY

CIO Summit 2019

Digital 2019, 연결하고 해석하고 지능화하라!

2019. 2. 21(목)

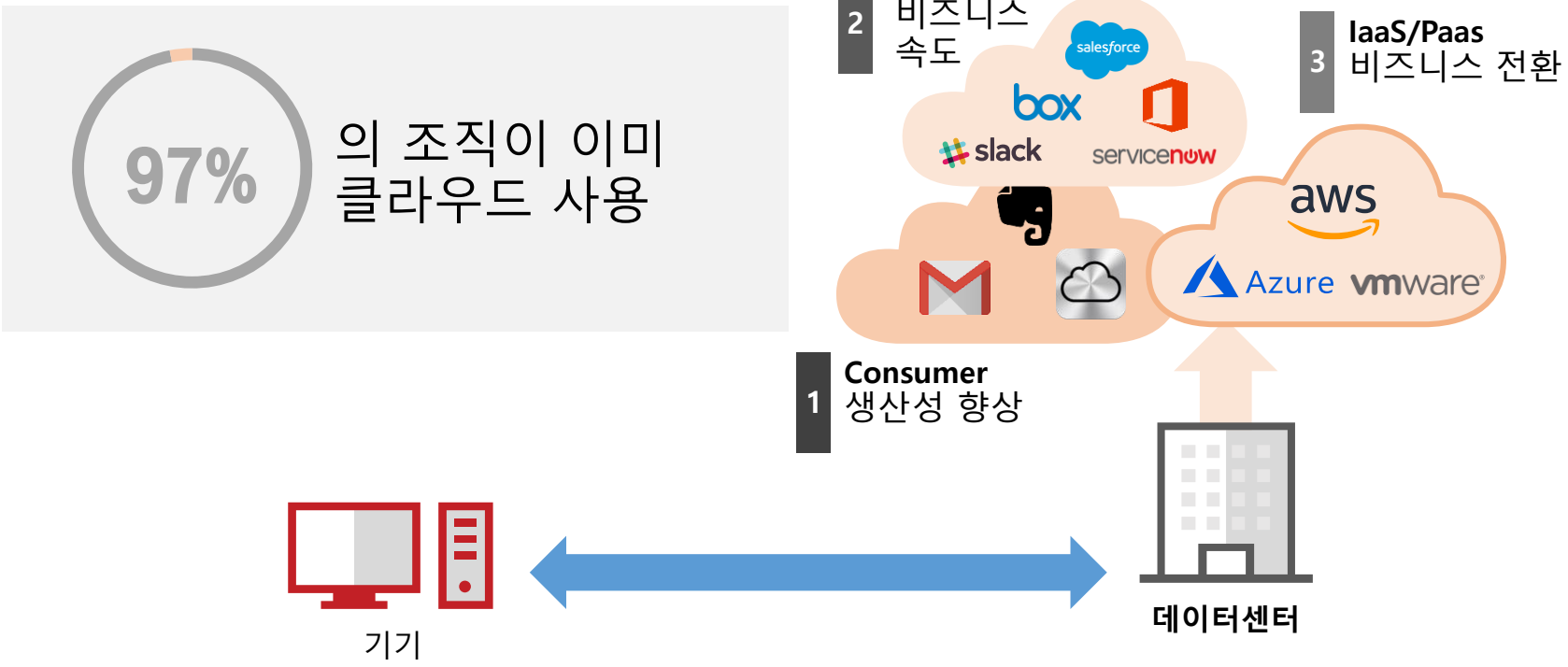
인터컨티넨탈 서울 코엑스 하모니볼룸(B1)

CIO Summit 2019

클라우드 데이터 보안을 위한 CASB 활용법

김영기 팀장
맥아피 코리아

Cloud 환경으로의 변화

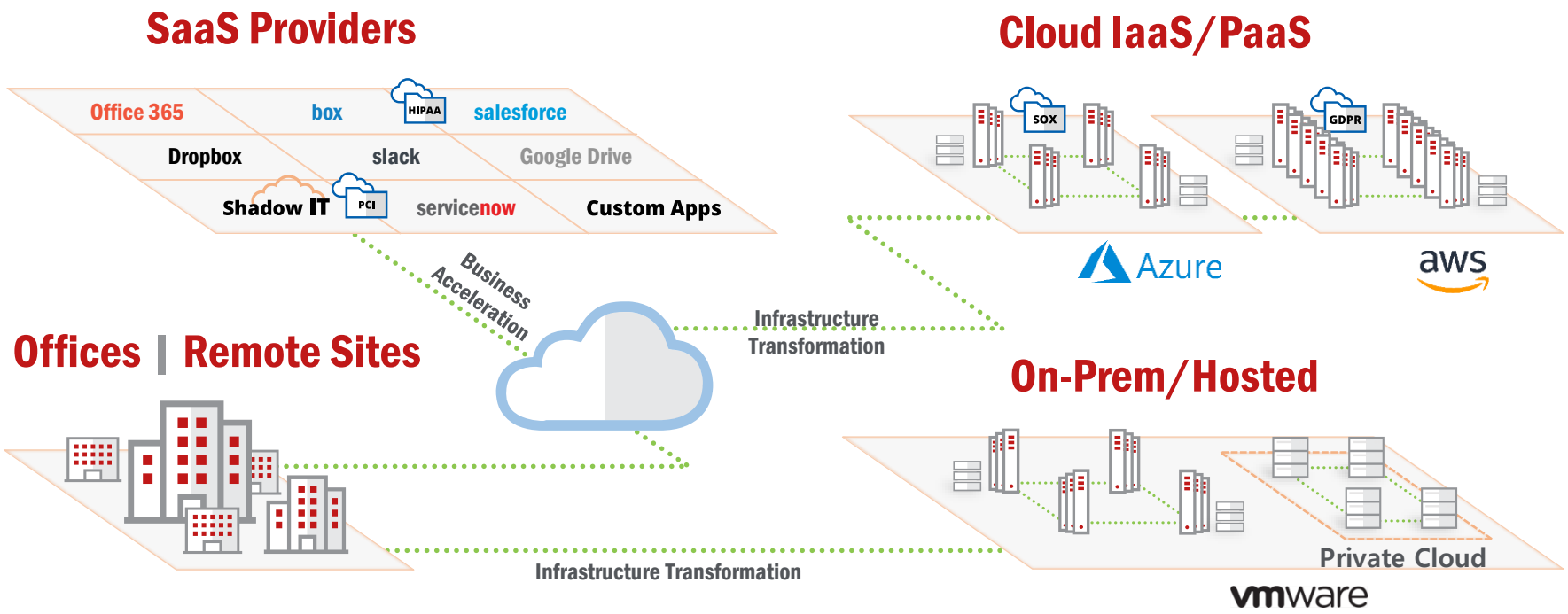


이미 Cloud로의 전환은 거부할 수 없는 변화이며,

이젠 Cloud를 얼마나 잘 활용하느냐를 고민할 때..

오늘날 엔터프라이즈 환경 변화

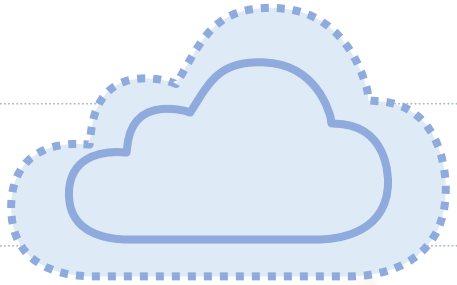
CIO Summit 2019



다양한 환경이 혼합된 하이브리드 환경으로 운영

What Does This Mean for Security?

CIO Summit 2019



새로운 취약점 발생

가시성 부족

이전 시스템과 새로운 시스템의
동시 관리 비용 증가

이전 보안 접근 방식의 낮은 효과

보안과 업무 부서 간의 불일치

클라우드 가시성과 데이터 보안 필요성

CIO Summit 2019

Cloud 사업 확산의 저해 요인 1위 " 보안 "

안전한 Cloud 보안 체계가 성공적인 Cloud 전환의 핵심포인트

주요 Cloud 보안 체계 구축 방안

안전이 보장된 Cloud 인프라 제공	Cloud 환경에 맞는 외부 침입 방지 체계 마련	Cloud 서비스의 데이터 보안 및 가시성 확보
AWS, MS 애저 등 Cloud 자체 인프라의 보안 인증 추진 및 보안 방안 마련	가상 IPS, Cloud WAF, Cloud 서버 보안 등 Cloud 환경에 적합한 솔루션 서비스 구축	**새로운 보안체계 필요**

보안 책임, 공유 책임

CIO Summit 2019

- 클라우드 채택을 보장하기 위해 고객사의 책임을 이해하는 것이 매우 중요.

Shared Security Responsibility Model

Private/ On-Premise	IaaS	PaaS	SaaS	Protection
Users	Users	Users	Users	IAM
Data (McAfee, Skyhigh)	Data (Skyhigh)	Data (Skyhigh)	Data (Skyhigh)	CASB, DLP, Encryption
Applications (McAfee)	Applications (McAfee)	Applications (McAfee)	Applications	Endpoint, IPS
Operating System (McAfee)	Operating System (McAfee)	Operating System	Operating System	
Network (McAfee)	Network (McAfee)	Network	Network	IPS
Hypervisor/ Virtualization (McAfee)	Hypervisor/ Virtualization	Hypervisor/ Virtualization	Hypervisor/ Virtualization	
Infrastructure (McAfee)	Infrastructure	Infrastructure	Infrastructure	
Physical (McAfee)	Physical	Physical	Physical	Guards

□ 고객 책임 ■ 클라우드 공급자 책임

2018 McAfee Cloud 위협 보고서 요약

CIO Summit 2019

- 클라우드에 있는 모든 파일의 21%는 민감한 데이터를 포함하고 있으며, 지난 2년간 17% 증가.
- 클라우드에서 중요 데이터를 공유하는 파일의 양이 53% 증가.
- 공개 접속 링크와 민감한 데이터를 공유하는 것이 지난 2년간 23% 증가.

- IaaS/PaaS 사용의 94%가 AWS 사용, IaaS/PaaS를 사용하는 조직의 78%가 AWS와 Azure를 모두 사용.

- 엔터프라이즈 조직은 평균 14개의 잘못 구성된 IaaS/PaaS 인스턴스를 실행.
  매월 평균 2,269건의 잘못된 구성 문제가 발생.
- AWS S3 버킷의 5.5%가 World 읽기 권한을 가지고 있어 대중에게 공개.

- 평균 조직은 매달 32억 건 이상의 이벤트를 클라우드에서 생성, 3,217건은 이례적이고 31.3건은 실제 위협.
- 클라우드 내 위협 이벤트(예: 손상된 계정, 권한 있는 사용자 또는 내부자 위협)가 27.7% 증가

- 전체 조직의 80%가 적어도 한 달에 한 번은 손상된 고객 위협을 경험.
- 전체 조직의 92%가 다크 웹에서 판매하기 위해 클라우드 자격 증명을 도용.
- 오피스 365의 위협은 지난 2년간 63% 증가.

- 평균적인 조직은 1,935개의 고유한 클라우드 서비스를 사용하며, 이는 작년보다 15% 증가. 대부분의 단체들은 약 100개 미만을 사용한다고 생각.

새로운 Cloud 보안 솔루션의 필요

CIO Summit 2019

Cloud 내에 있는 중요 데이터 파일 양 증가

대다수가 멀티 클라우드 사용

잘못된 구성 문제로 인한 이슈 지속

Cloud 이벤트 증가와 위협 분석 필요 증가

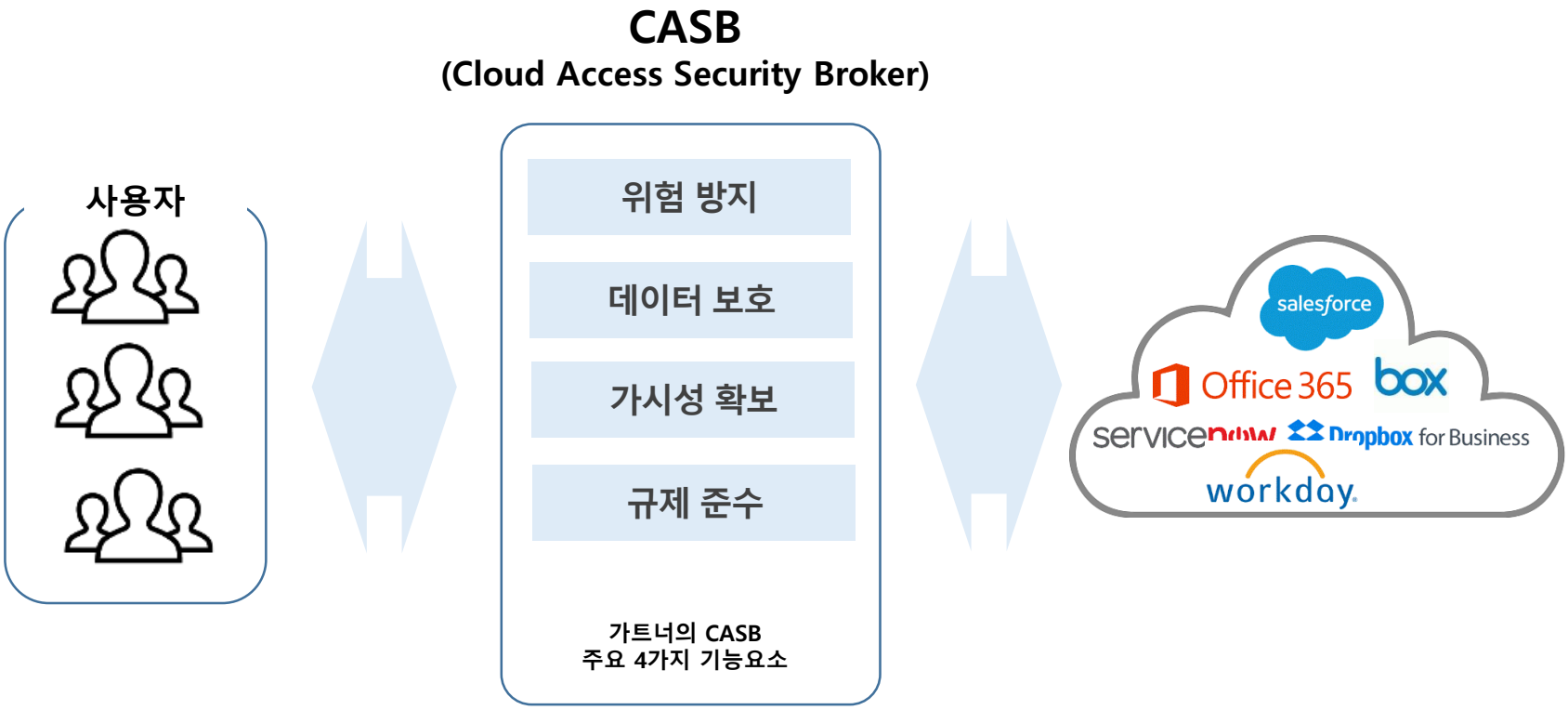
계정 탈취 및 도용 위험 증가

Shadow IT에 대한 인식 부족

중요데이터에 대한 **DLP 기능을 제공**하면서, 잘못된 구성에 대한 **모니터링**을 하고, 방대한 Cloud **이벤트를 분석하여 위협을 감지**하고 **계정 탈취를 분석 탐지**하면서 **멀티클라우드에 적용**이 되는 솔루션. **ShadowIT까지 탐지**해야 함

CASB 개념

CASB란 Cloud서비스에 대한 데이터유출방지, ShadowIT에 대한 가시성 확보 및 규제 준수를 멀티클라우드 환경에서도 지원할 수 있도록 Cloud에 종속적으로 설치 운영되는 것이 아닌 Broker 형태로 지원하는 보안 체계.
CASB는 그 자체가 가지고 있는 보안 기능 뿐 아니라 다양한 보안 제품과 연동하는 Security Broker 역할 수행.



McAfee CASB - Skyhigh

McAfee MVISION Cloud

McAfee Skyhigh Security Cloud

Skyhigh leads the CASB market

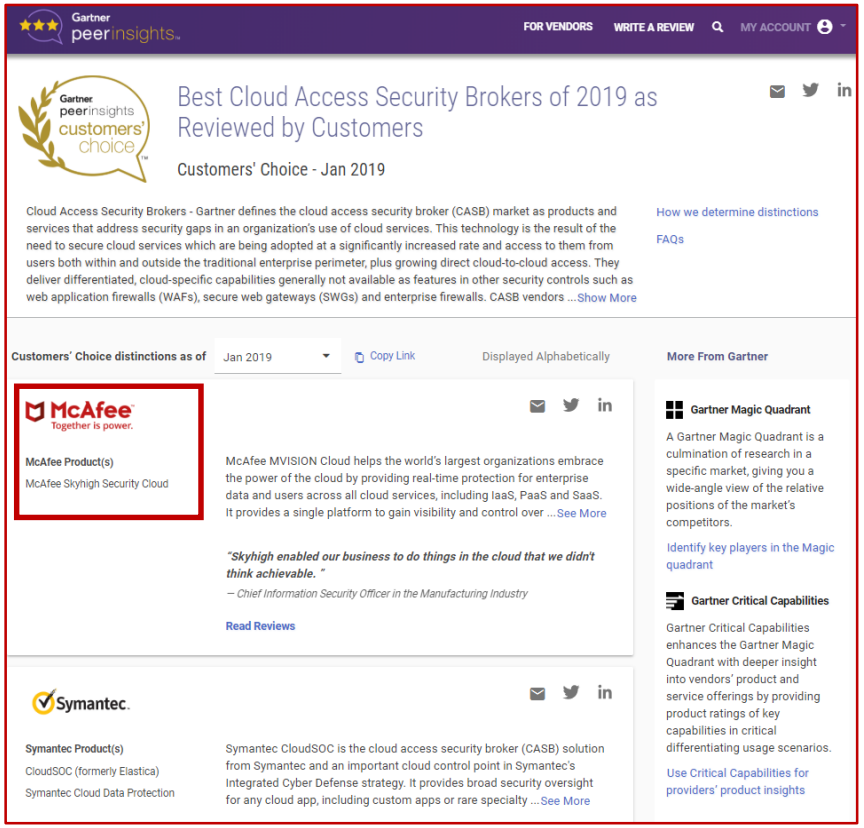
CIO Summit 2019

가트너 평가기관의 평가

Figure 1. Magic Quadrant for Cloud Access Security Brokers

Source: Gartner (October 2018)

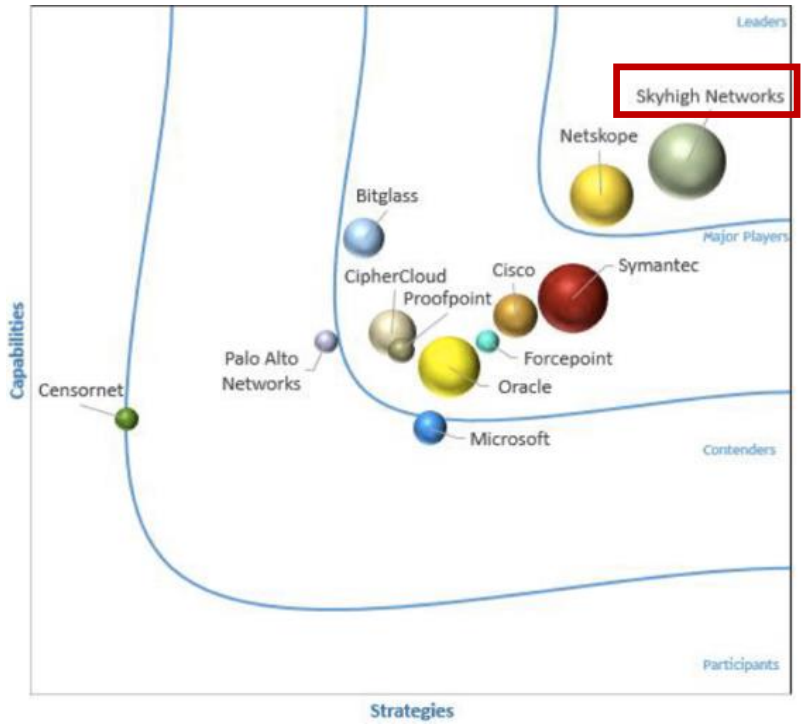
가트너 고객들의 평가



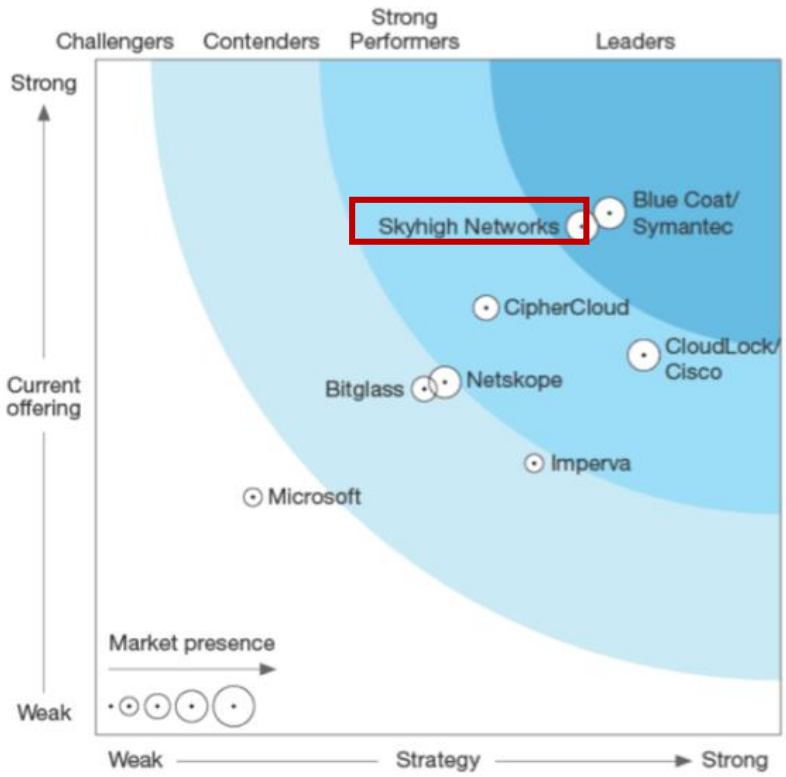
CASB 인증 및 평가에서 유일한 3관왕

CIO Summit 2019

IDC



FORRESTER®



가장 많은 CASB 고객 확보

CIO Summit 2019

네트워크 보안의 데이터 보호 한계

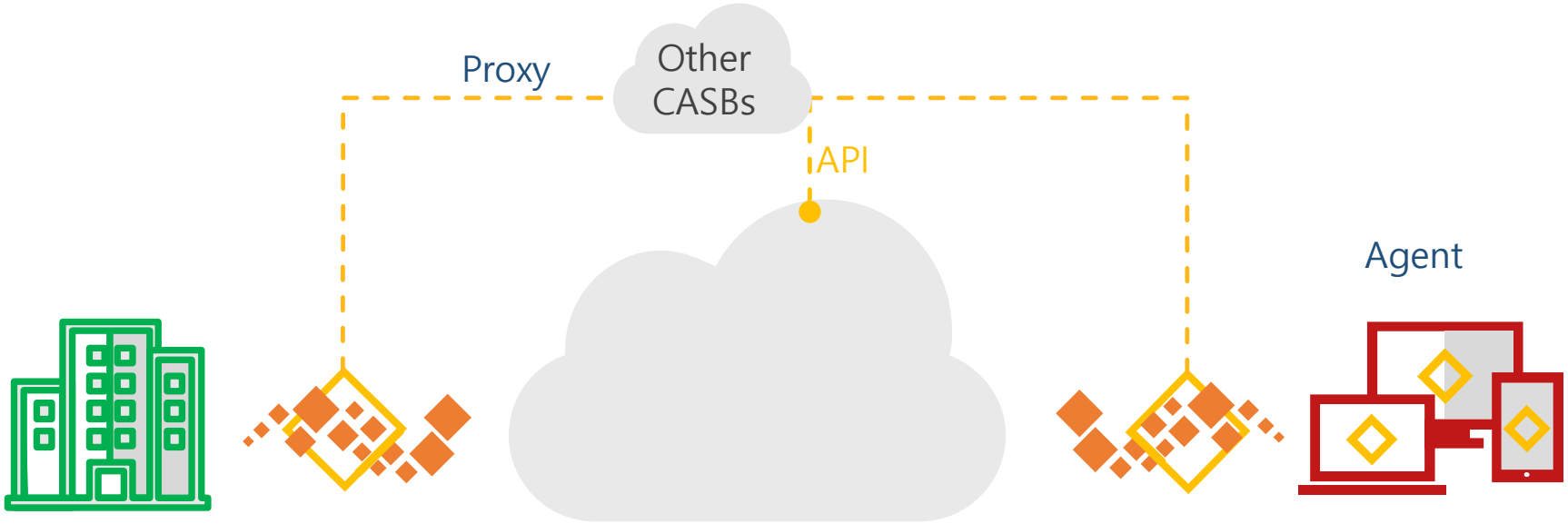
Cloud native 트래픽의 경우 기업 network 에서 감지 불가능

Cloud 트래픽의 50%는 cloud to cloud 트래픽으로 감지 불가능

외부에서 upload 하는 트래픽 감지 불가능

기존의 CASB의 데이터 보호 한계

CIO Summit 2019

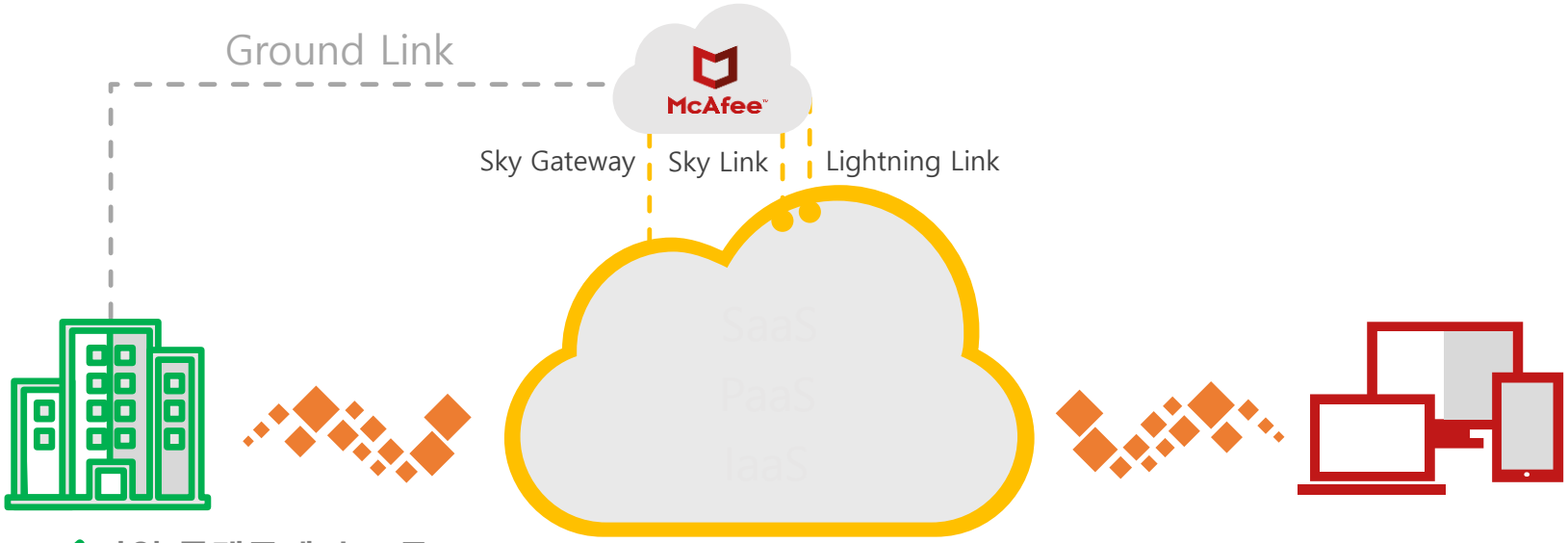


- ✓ 실시간
- ✗ 완벽한 보호
  - ✗ 기존의 저장된 데이터
  - ✓ 데이터 업로드
  - ✗ Cloud 내 생성된 데이터
  - ✓ 표준 apps
  - ✗ 인증서 고정 apps

- ✗ 실시간
- ✓ 완벽한 보호
  - ✓ 기존의 저장된 데이터
  - ✓ 데이터 업로드
  - ✓ Cloud 내 생성된 데이터
  - ✓ 표준 apps
  - ✓ 인증서 고정 apps

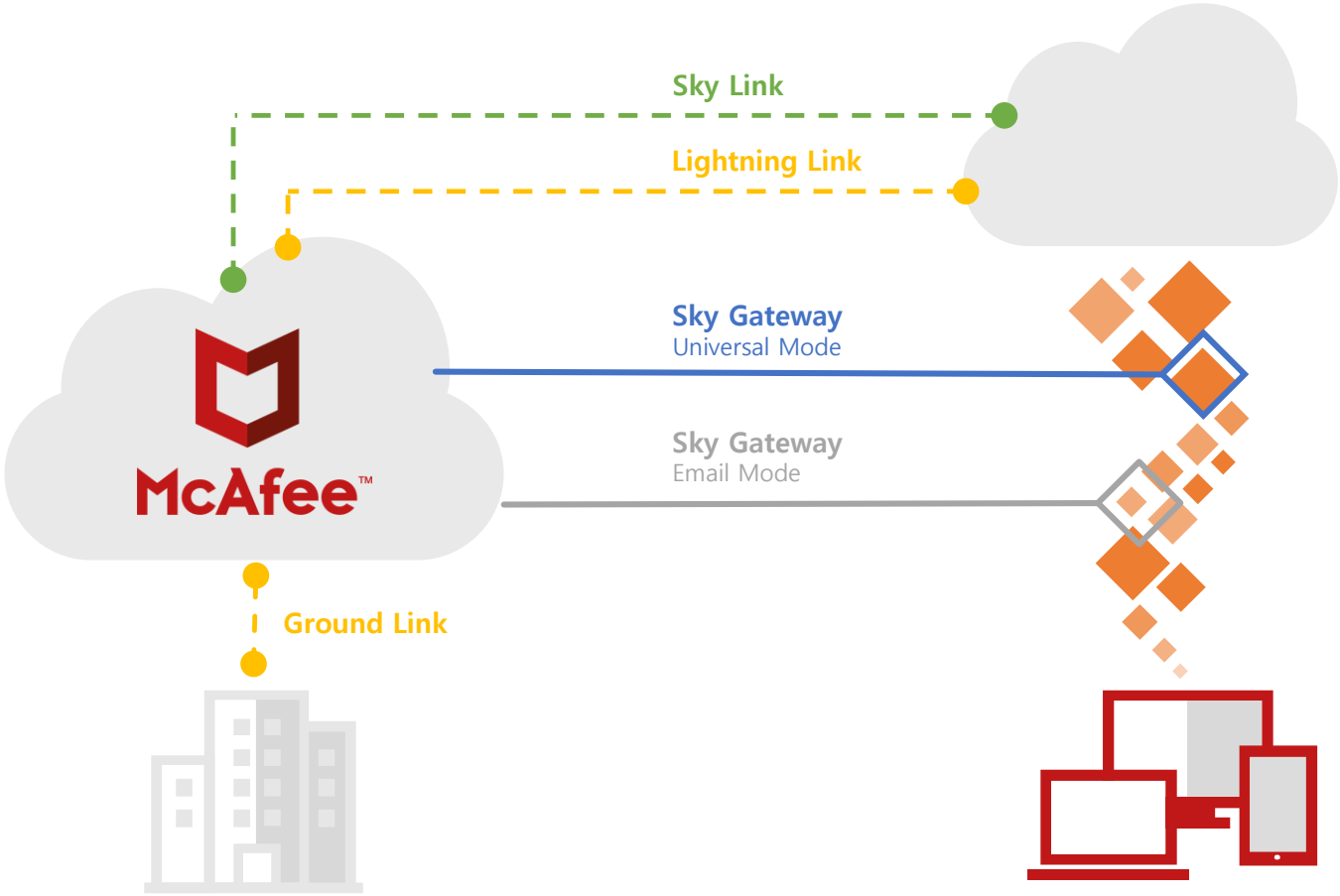
- ✓ 설치 어려움
- ✓ 에이전트 충돌

Skyhigh만의 독특한 접근 방식



- ✔ 단일 플랫폼에서 모든 Cloud 서비스에 대해 일관된 정책
- ✔ 실시간
- ✔ 완벽한 보호
  - ✔ 기존의 저장된 데이터
  - ✔ 데이터 업로드
  - ✔ Cloud 내 생성된 데이터
  - ✔ 표준 apps
  - ✔ 인증서 고정 apps
- ✔ Agent 불필요
- ✔ 충돌 X

McAfee Skyhigh 보안 클라우드 아키텍처



기존 On-premise 제품 기능과 비교

CIO Summit 2019

Usecase	On-Premise DLP / Webgateway	McAfee Skyhigh (CASB)
클라우드에 있는 데이터 내 개인정보 검출	X	On-demand Scan 또는 파일 접근 시 검사
클라우드에 있는 개인정보 파일 격리/삭제	X	클라우드DLP 기능으로 격리/삭제 제공
내외부에서 클라우드에 민감정보파일 업로드 시 차단	내부만 가능	내외부 모두 가능
SaaS 전용 앱을 통해 데이터 업로드 시 차단	X	네이티브 앱을 통한 데이터 업로드도 처리
모바일 접근 차단	X	별도 에이전트 없이 제공
비인가 기기 접근 차단	X	인증서연동으로 제공
민감 데이터 외부 공유 시 차단	X	클라우드 DLP 로 제공
클라우드 사용자 행위 모니터링	API로 로그 다운로드 후 별도 분석 필요	자체 기능 제공
클라우드 사용자 이상행위 분석	SIEM 연동 필요	자체 기능 제공
클라우드 관리 설정 변경 모니터링	X	모니터링 기능 제공
클라우드 사용 로그 보관(6개월 이상)	로그 다운로드 후 별도 보관	클라우드 상에 1년까지 보관

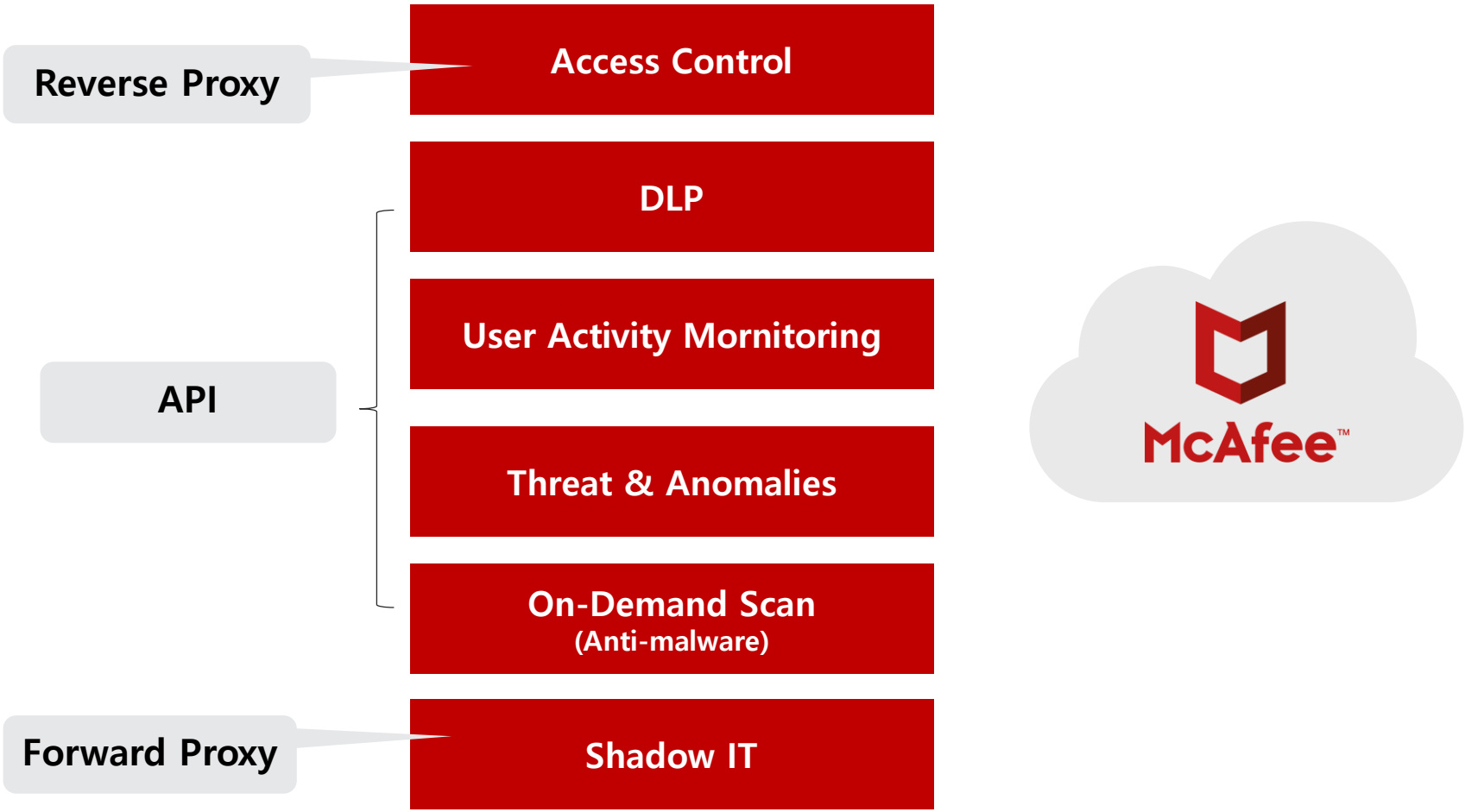
클라우드 보안에 대한 새로운 시각

CIO Summit 2019

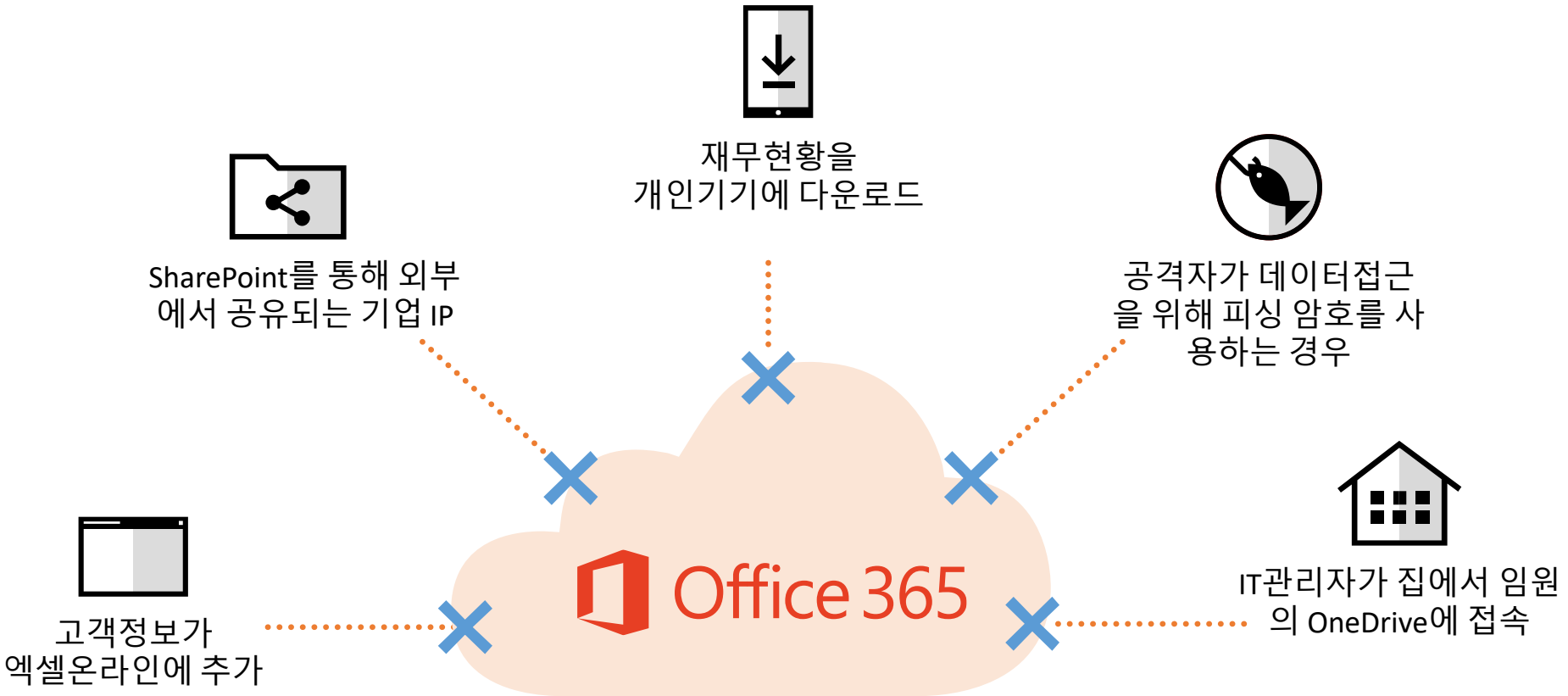
클라우드 보안은 더 이상 기존 방식이 아닌

클라우드 관점으로 접근해야 합니다.

Skyhigh Key Feature

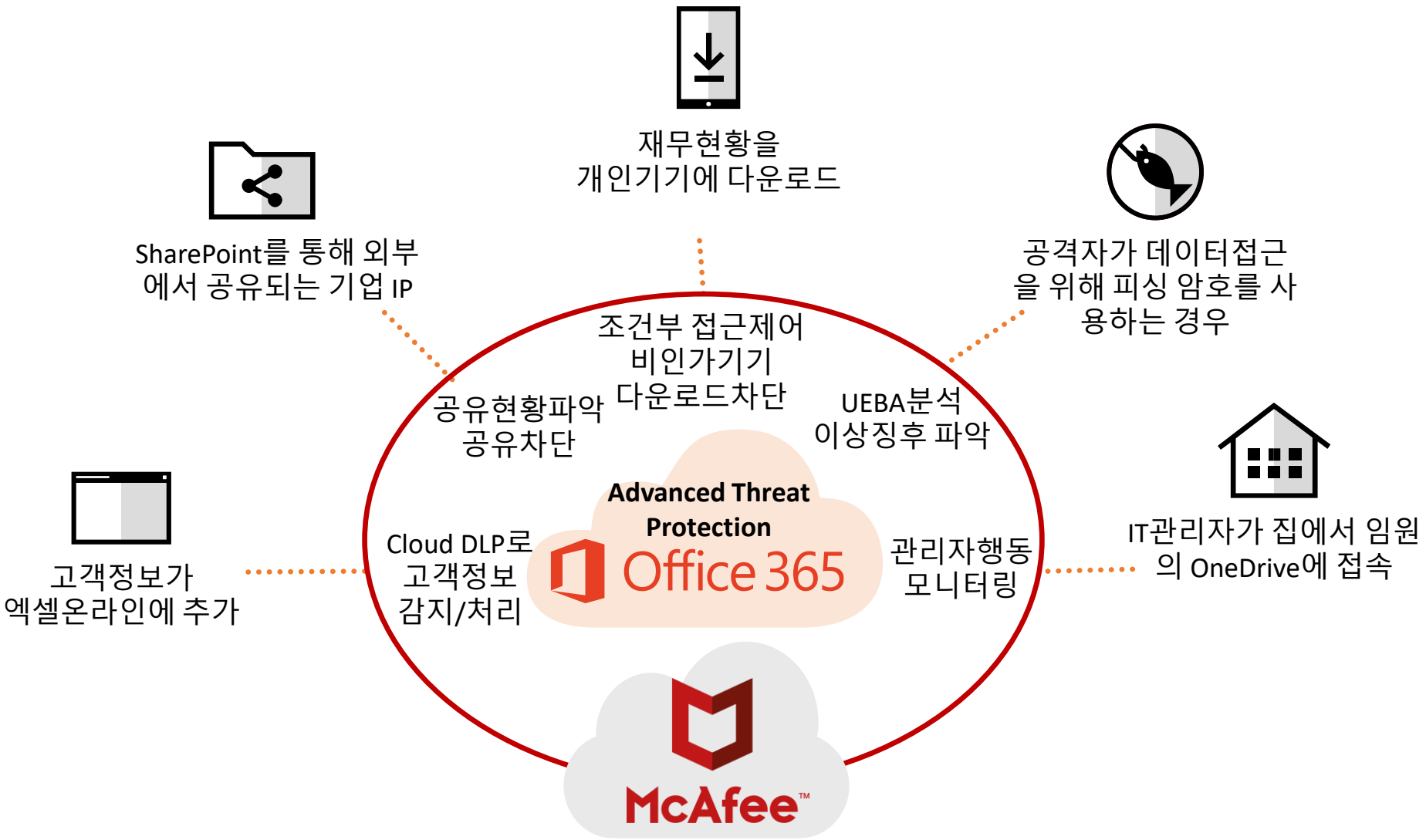


O365 데이터 유출 요인과 Skyhigh 대응기능



O365 위험 요인과 Skyhigh 대응기능

CIO Summit 2019

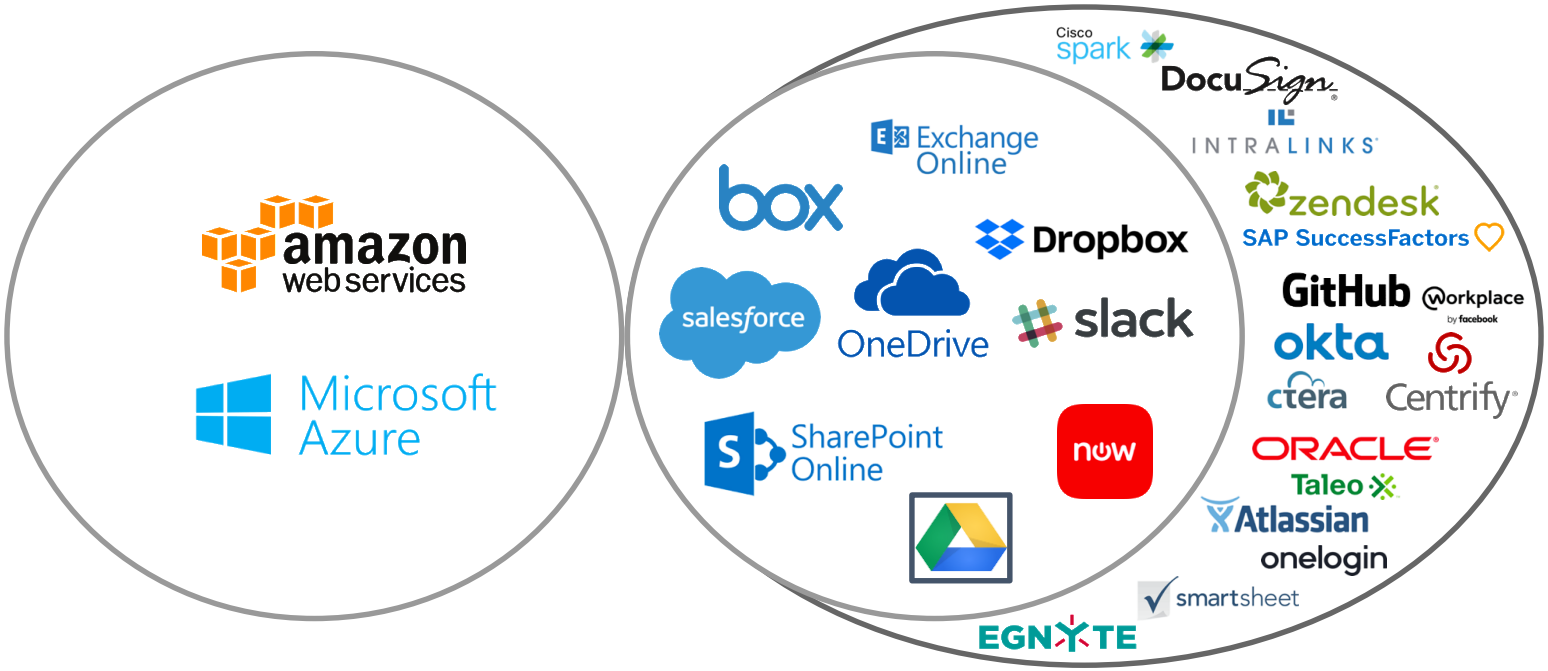


Skyhigh Connect Catalog

CIO Summit 2019

- 사전 통합된 응용 프로그램의 카탈로그. 지원되는 모든 허가된 서비스가 포함.
- **카탈로그는 현재 30개 이상의 SaaS서비스로 구성되어 있으며 이는 다른 CASB보다 3배 이상 많은 수치.**

CASB Connect Catalog



IaaS Security Layers

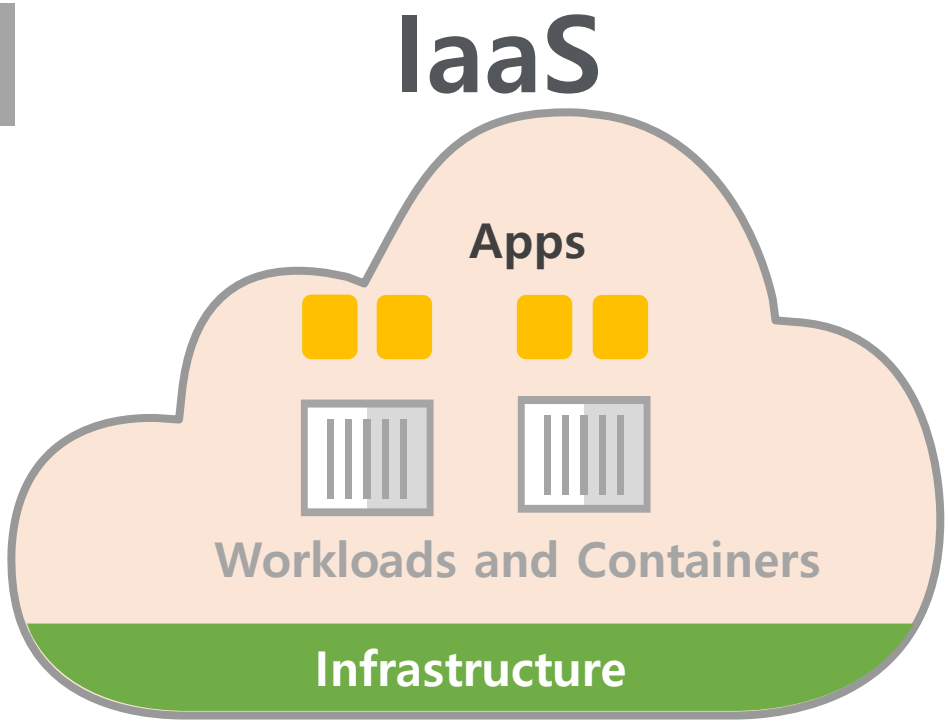
McAfee Skyhigh CASB 1 3

McAfee CWS 2

3 앱의 데이터 보호

2 워크로드 및 컨테이너 탐지 및 보안

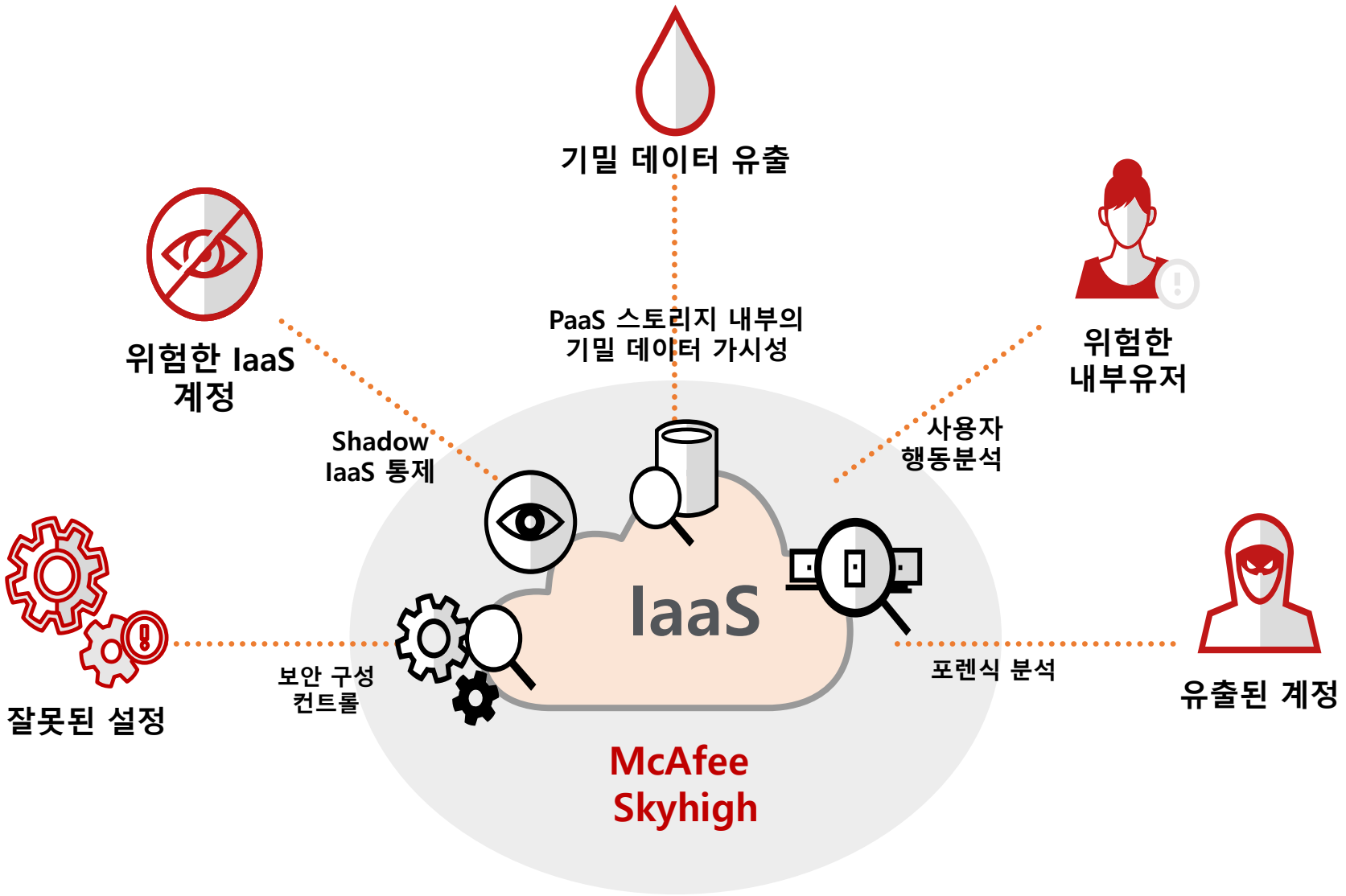
1 보안 오류 감지 및 수정



aws

Microsoft Azure

IaaS 데이터 유출 요인과 Skyhigh 대응기능



IaaS 주요 CASB 사용 사례

CIO Summit 2019

1. IaaS 리소스의 보안 구성 모니터링
CIS 수준 1, 2 정책을 준수하지 않는 보안 설정으로 IaaS 리소스 식별.

2. 위험한 IaaS 계정 관리
Shadow IT 사용량 확인 및 위험한 IaaS 사용량 제어 회수.

3. 기밀 데이터의 가시성
AWS S3 및 Azure 스토리지에 저장된 규제/고가치 데이터의 가시성 확보.

4. 고급 위협 보호
손상된 계정, 내부자/권한 사용자 위협, 멀웨어 탐지.

5. 활동 모니터링 및 포렌식
법의학 수사를 위한 감사 활동 추적 포착 및 분류

McAfee의 차별화 요소 Top 5

CIO Summit 2019

설치 테스트가 쉽다 – API 방식으로 쉽고 간편하게 설치/ 운영할 수 있다.

다양한 DLP 기능 – 관리자가 원하는 기능 조건을 대부분 지원한다.

가장 넓은 지원 범위 – Skyhigh가 지원하지 못하면 다른 CASB도 지원 못한다.

빠른 응답속도 – 빠른 처리성능을 바탕으로 실제적 보안효과를 제공한다.

국내 기술지원 – 90% 이상 국내에서 기술지원이 가능하여 대응이 빠르다.

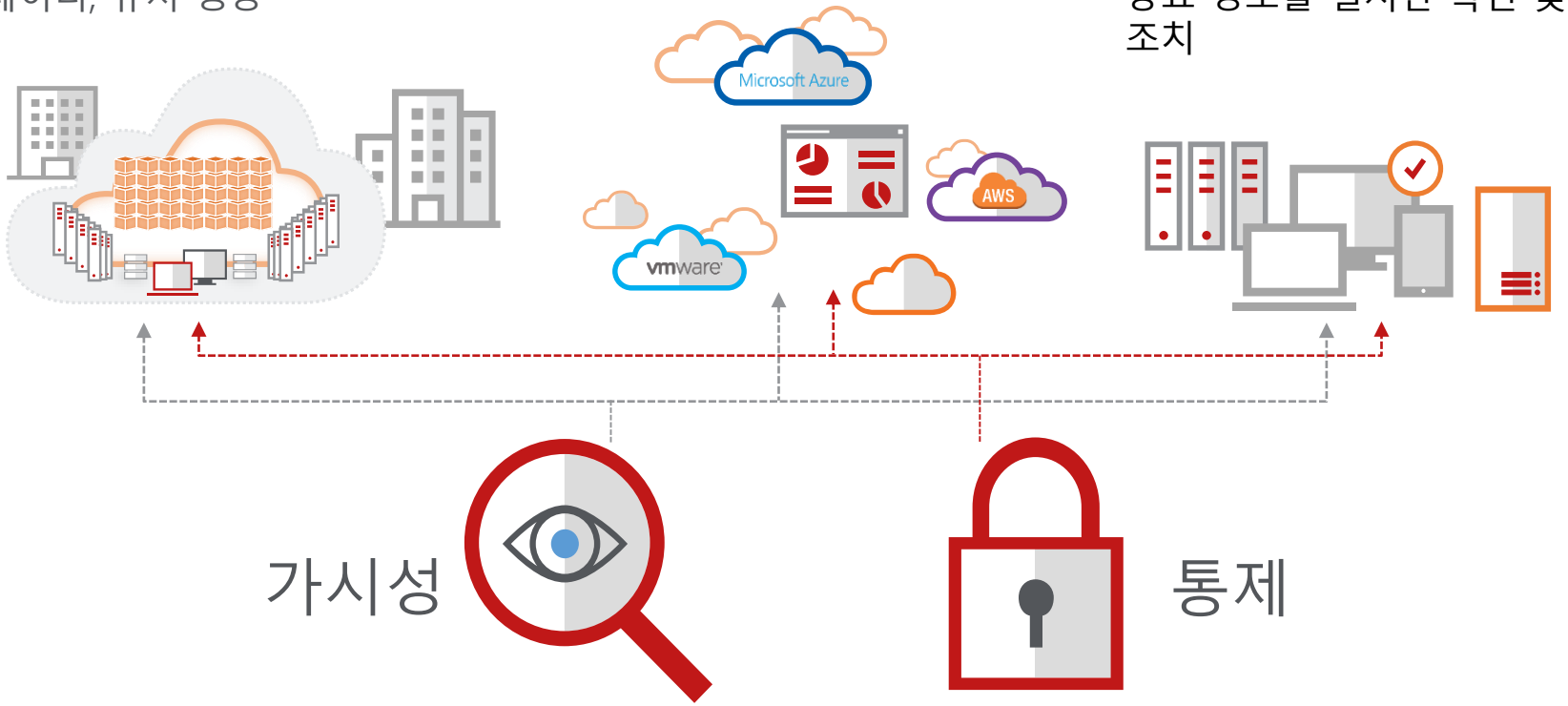
McAfee 클라우드 보안 프레임워크

CIO Summit 2019

완벽한 가시성 확보
클라우드 내의 데이터, 워크로드, 컨테이너, 유저 행동

보안 관리
멀티 클라우드 포괄

지속적 보호 적용
정책 위반 시정을 위한 중요 정보를 실시간 확인 및 조치



이제 클라우드 보안은
맥아피와 상의하세요