SAMSUNG SDS

REAL 2019

REALIZE YOUR VISION
THROUGH DIGITAL TRANSFORMATION

2019 . 5 . 8 . WED . The Shilla Seoul

Identity 중심의 Zero Trust 보안

김상진 팀장

기업 보안의 현재

$114B

2018년도 보안지출

여전히

66%

기업에 보안사고 발생

보안사고 발생 기업에 평균 5회 이상 보안사고 재발

*Source : Gartner, 2018

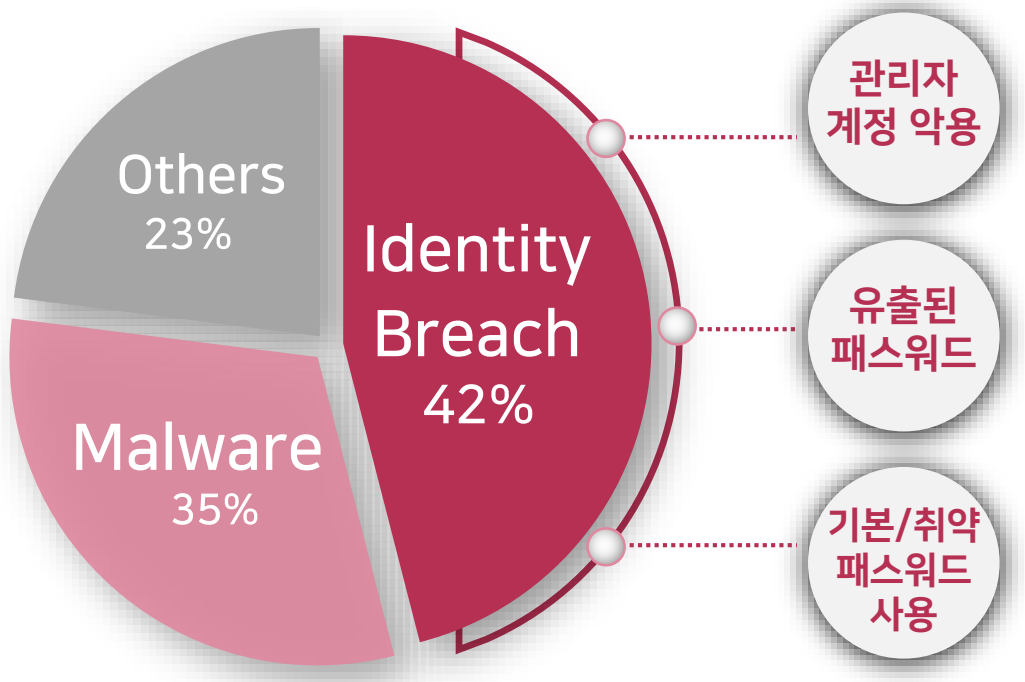
보안사고의 주된 위협 요인 – Identity Breach

설문조사

☑ 조사대상 : 800명 C-Level 임원

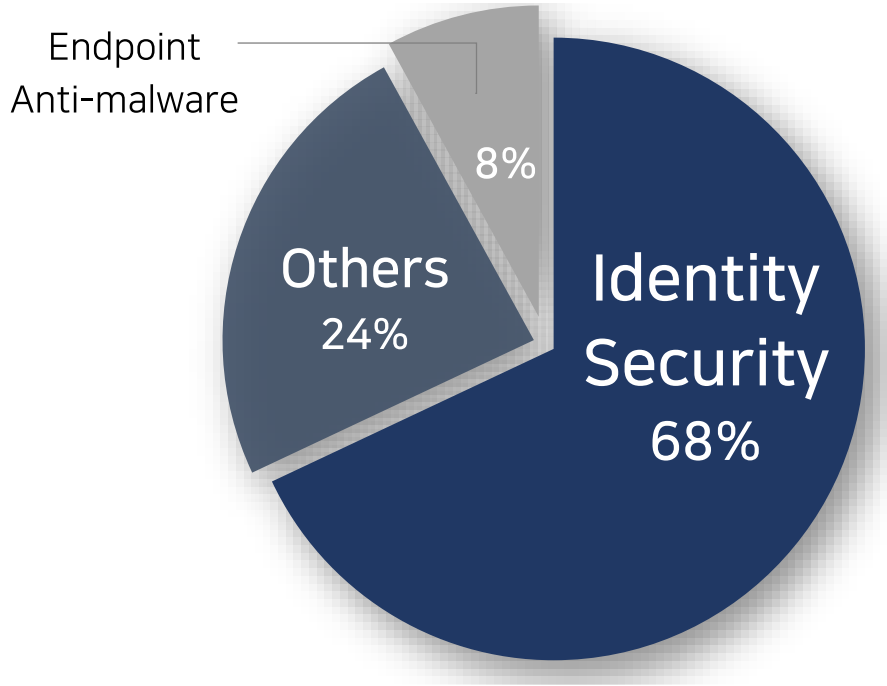
기업에서의 가장 큰 보안 위협

☑ 응답자 : 기술 임원(CISO, CIO, CTO)



보안사고를 막을 수 있었던 방지책

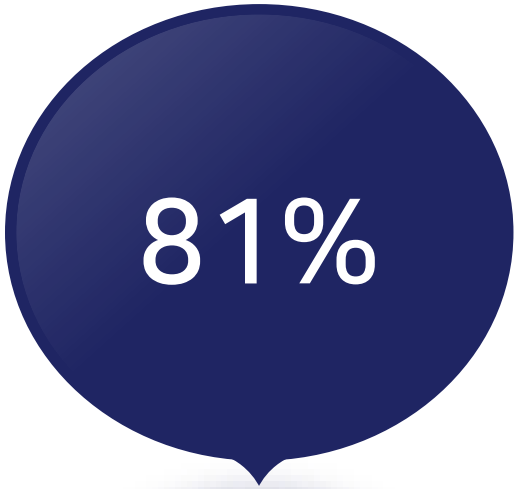
☑ 응답자 : 1회 이상 중대 보안사고를 경험한 기업 임원



*Source : Wall Street Journal, 2018

보안사고의 주된 위협 요인 – Identity Breach

분석결과



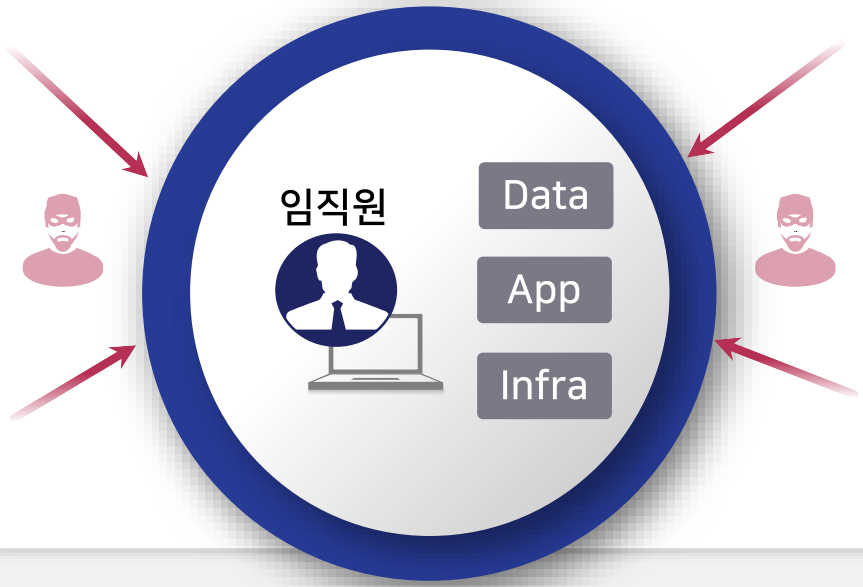
보안사고는 기본/취약 패스워드 사용,
유출된 패스워드와 연관 (Verision, 2017)

보안사고는 관리자 계정
악용과 연관 (Forrester , 2016)

기업 환경의 변화 – Borderless

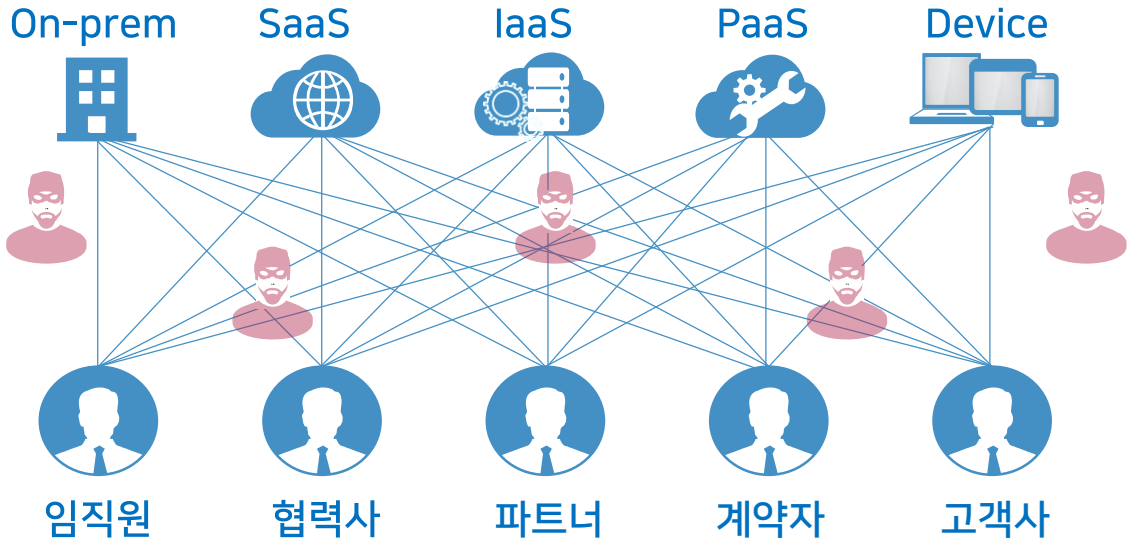
안/밖 경계 구분

사용자 · 기업자산은
네트워크 경계 안에 존재



경계가 없어짐

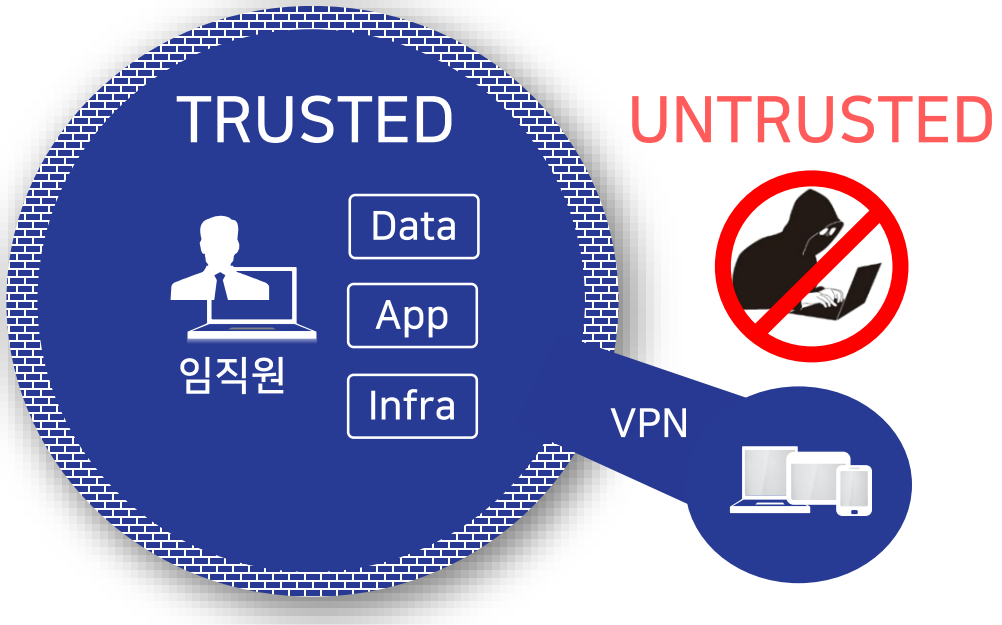
사용자 · 기업자산 · 위협은 어디나 존재



90%	15만개	8B	5B
클라우드 사용 기업	기업용 클라우드 앱	모바일 디바이스	IoT 디바이스

기업 환경의 변화 – Zero Trust 보안 필요

네트워크 경계 보안



Perimeter-centric Security

- Inside = Trusted & Trust, but verify
- Full network access

Zero Trust 보안

Identity-centric Security

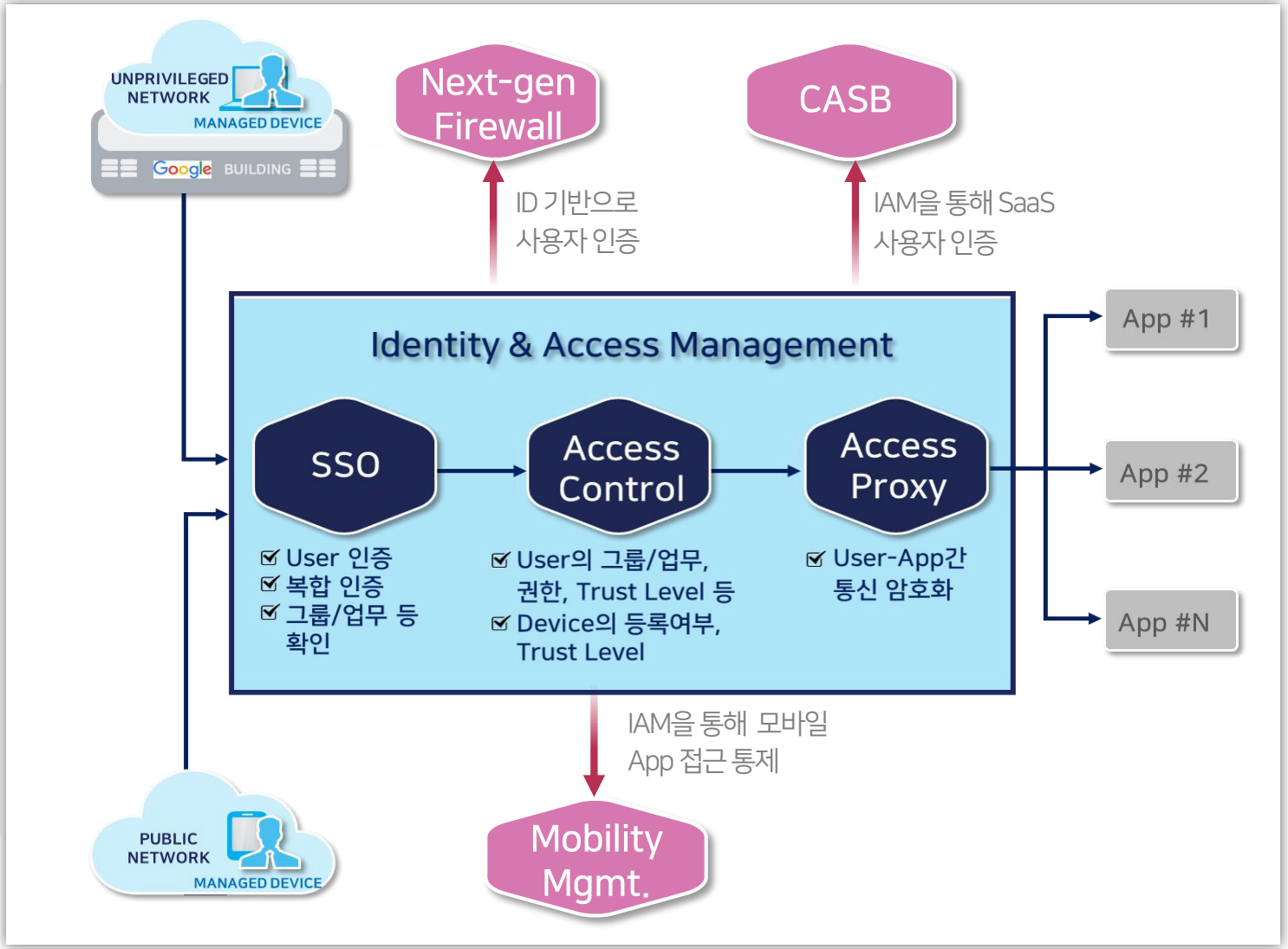
- Never trust, always verify
- Access only to authorized services

Zero Trust 보안 모델 – Identity-centric Security

Google Beyond Corp

BeyondCorp is a security model that builds upon seven years of building zero trust networks at Google, ….

By shifting access controls from the network perimeter to individual devices and users, BeyondCorp allows employees to work more securely from virtually any location without the need for a traditional VPN.



Zero Trust 보안 모델 – 구현원칙

원칙 1

아이덴티티 검증

정보자산 접근시, 경계 구분 없이
허가된 사용자·디바이스 여부를 확인

원칙 2

엄격한 접근통제

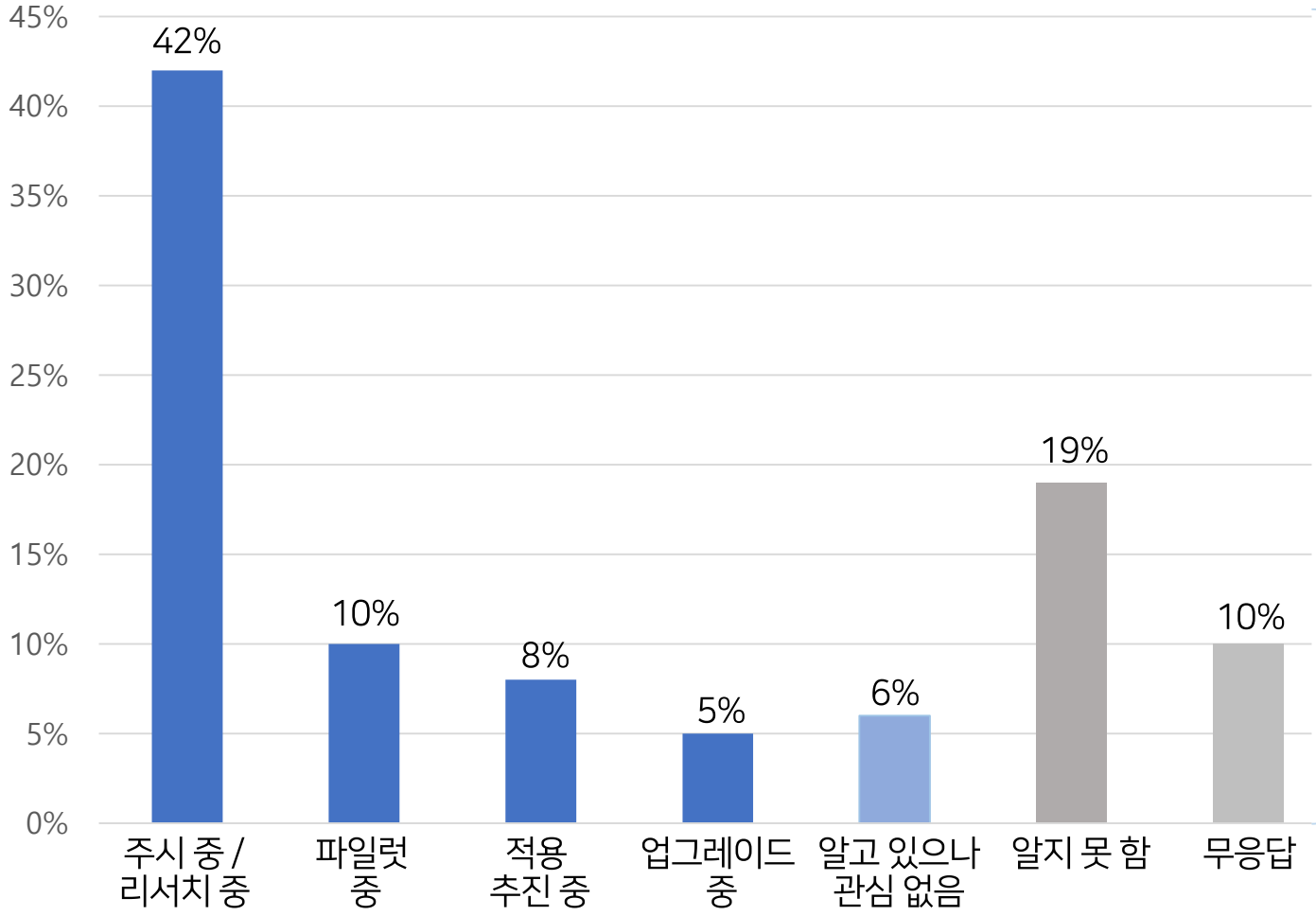
면밀한 접근통제를 통해 꼭 필요한
정보자산까지만 접근허용

원칙 3

검사 · 로깅

모든 트래픽 검사·로깅을 통해
사용자 활동에 보안에 위배가
없는지 확인

Zero Trust 보안 모델 – 도입 추세



IT보안 의사결정자

71% 가

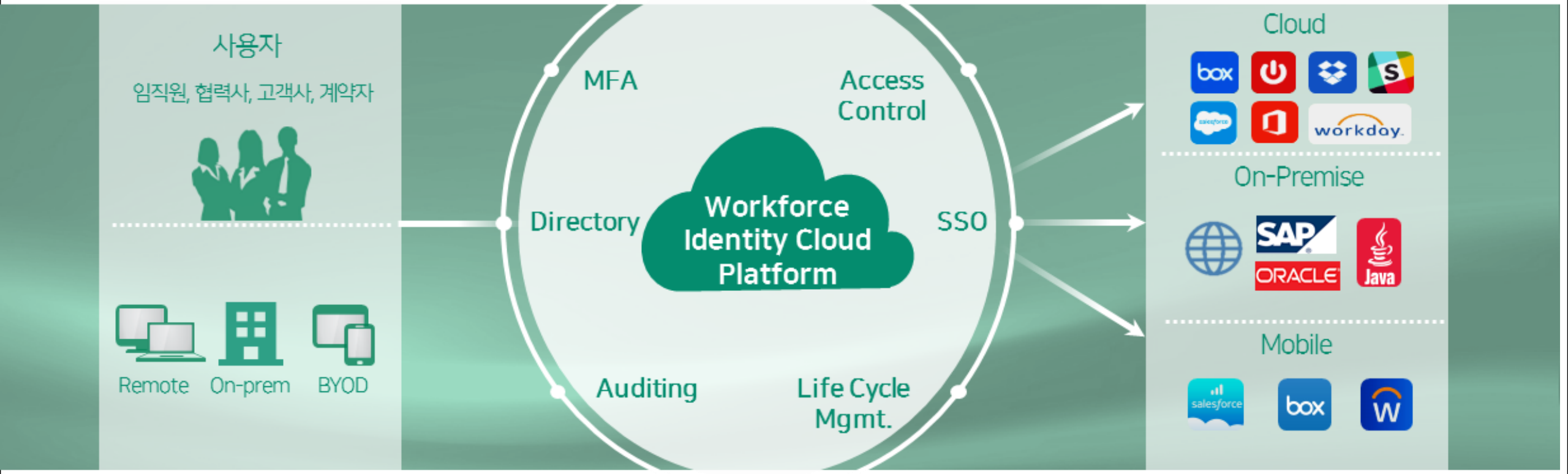
Zero Trust 모델에 대해

알고 있으며, 65%가 관심

*Source : IDG, 2018 (Global 2000 기업 대상 설문조사)

삼성SDS가 준비하는 Identity 중심의 Zero Trust 보안

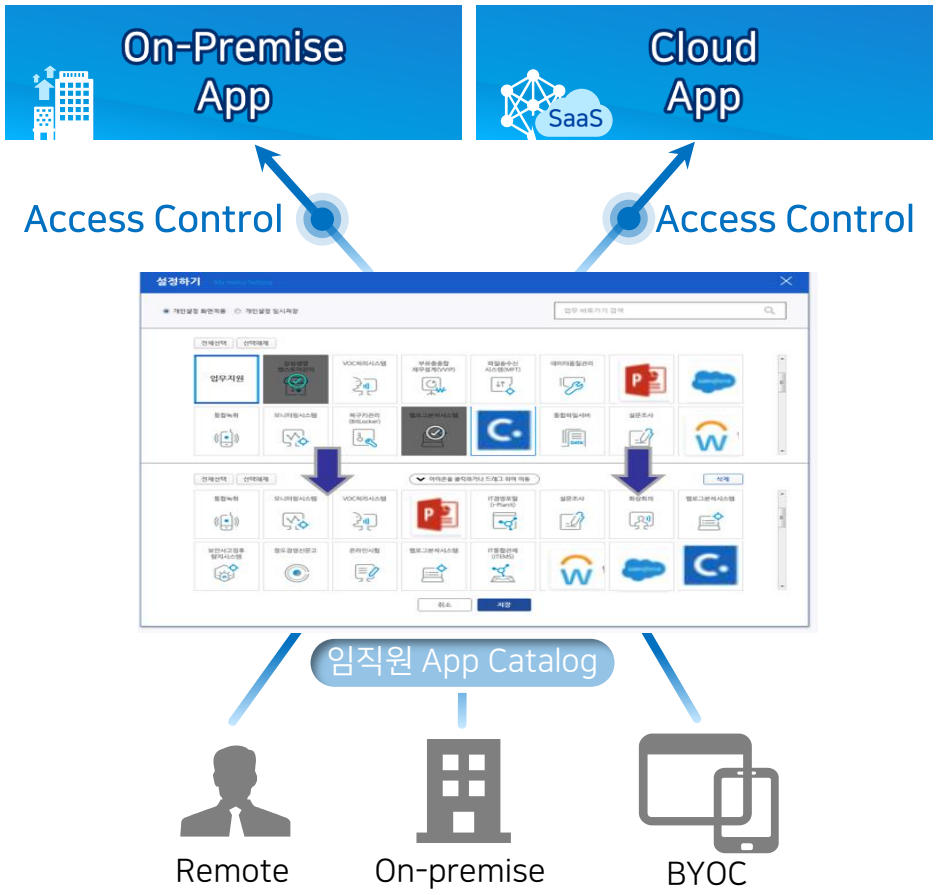
☑ Zero Trust의 3가지 구현원칙을 바탕으로 한 클라우드 기반 IAM 서비스를 '19.3Q 런칭 예정



허가된 사용자·디바이스가 접근정책 준수 시에 한번의 인증으로 권한 내의 다양한 업무 App에 액세스를 허용

삼성SDS 클라우드 Identity 주요 서비스 1. SSO

☑ On-prem, Cloud, Mobile을 아우르는 단일 Identity & Access 체계로 보안 및 관리 · 사용 편의성 향상



☑ 적용 편의성 향상

- On-prem, Cloud App의 개별 계정·접근통제 관리 복잡성 해소
- SaaS와의 사전 연계로 접근통제 정책의 손쉽고 신속한 적용

※ 기존 On-prem IAM과 SaaS 연계에 하루 이상 소요 (79%)

- 하루~이하 : 19%, 일주~이하 : 44%, 한달~이하 : 26%, 3개월 이상 : 9%

☑ 보안 향상

- On-prem/Cloud/Mobile App에 예외 없는 접근통제 적용
- SAML 등 표준 인증으로 패스워드 유출 위험 ↓
- 로그·정책·모니터링 단일화로 가시성 ↑, 잠재적 위험 제거

☑ 사용 편의 향상

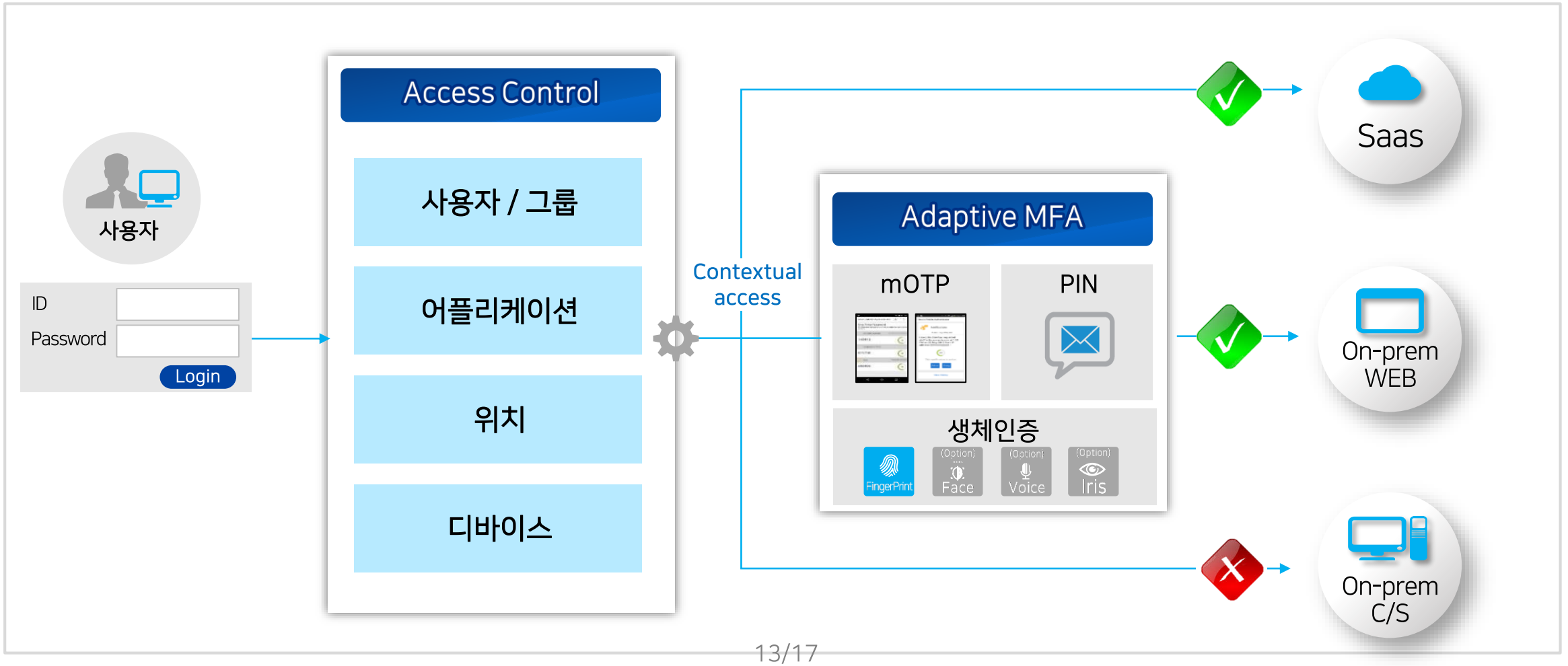
- 사용 디바이스, App 유형에 구애 없이 1회 인증
- 임직원 App Catalog 서비스를 통한 빠른 찾기·접속

*Source : IBM, 2017 ; 500명 대상 설문조사

삼성SDS 클라우드 Identity 주요 서비스

2. Access Control & MFA

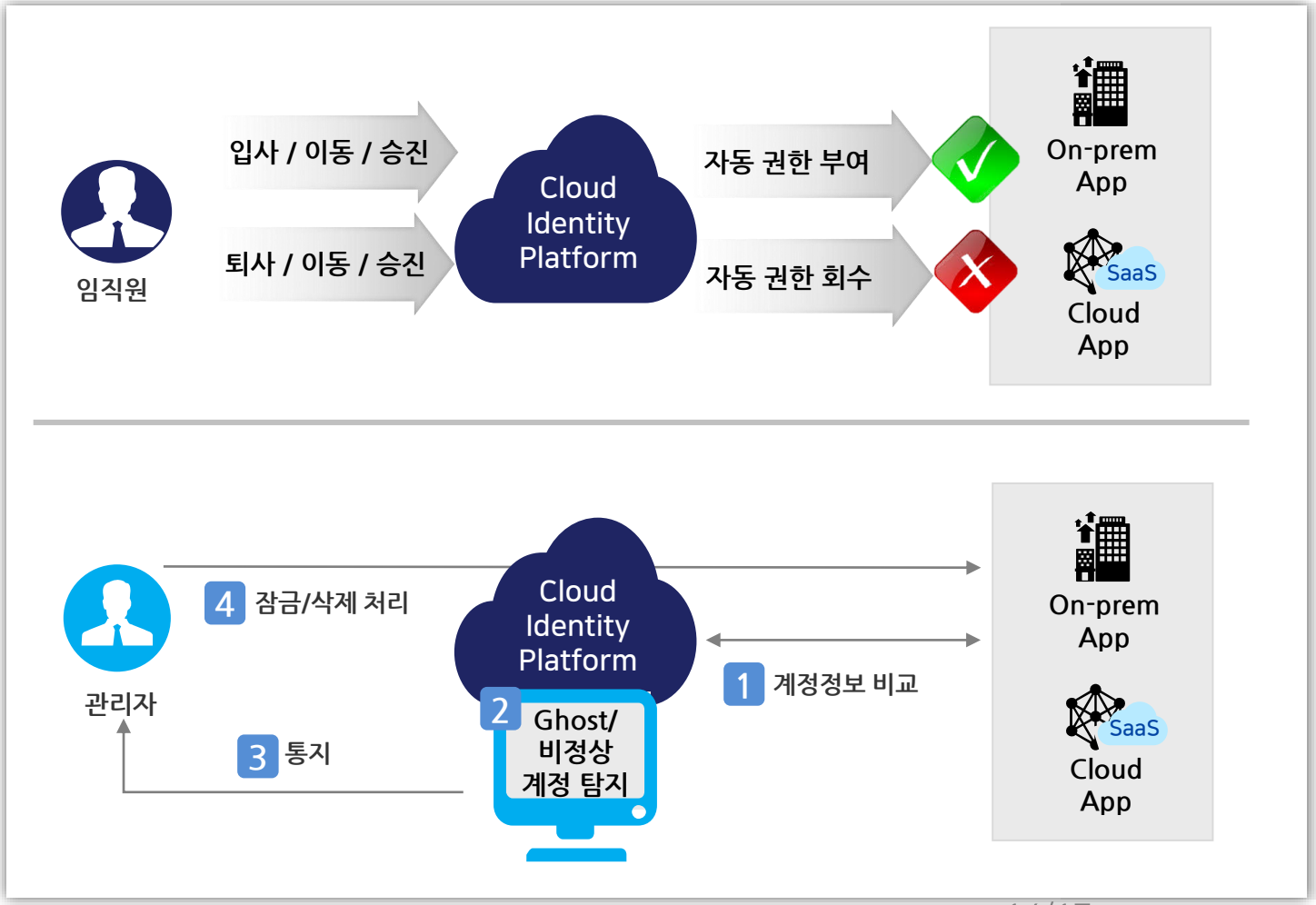
- ☑ 면밀한 접근통제로 비인가 접근 통제 강화
- ☑ 다양한 방식의 복합인증 지원으로 사용자 편의 만족



삼성SDS 클라우드 Identity 주요 서비스

3. Life Cycle Mgmt.

☑ On-prem과 Cloud App의 계정·권한 Life-Cycle 관리 자동화를 통해 보안위험 제거, 업무 지연방지 및 관리 효율성 증대



☑ 인사정보와 동기화된 자동 권한 부여/회수

- 적시에 필요한 권한 부여로 업무 지연 방지
- 적시에 불필요한 권한 회수로 비인가 접근 방지

☑ Ghost 및 비정상 계정탐지

- 개별 App에 임의로 생성된 계정(Ghost) 탐지를 통한 잠재적 보안 위험 제거
- 사용자 계정 발급 및 변경 이력 감사·계정접속 이력 추적을 통한 비정상 계정탐지

삼성SDS 클라우드 Identity 서비스 특징

☑ Zero Trust 실현과 보안 Up, 업무 효율 Up, 관리 비용 Down을 지원하는 Identity & Access 관리 플랫폼

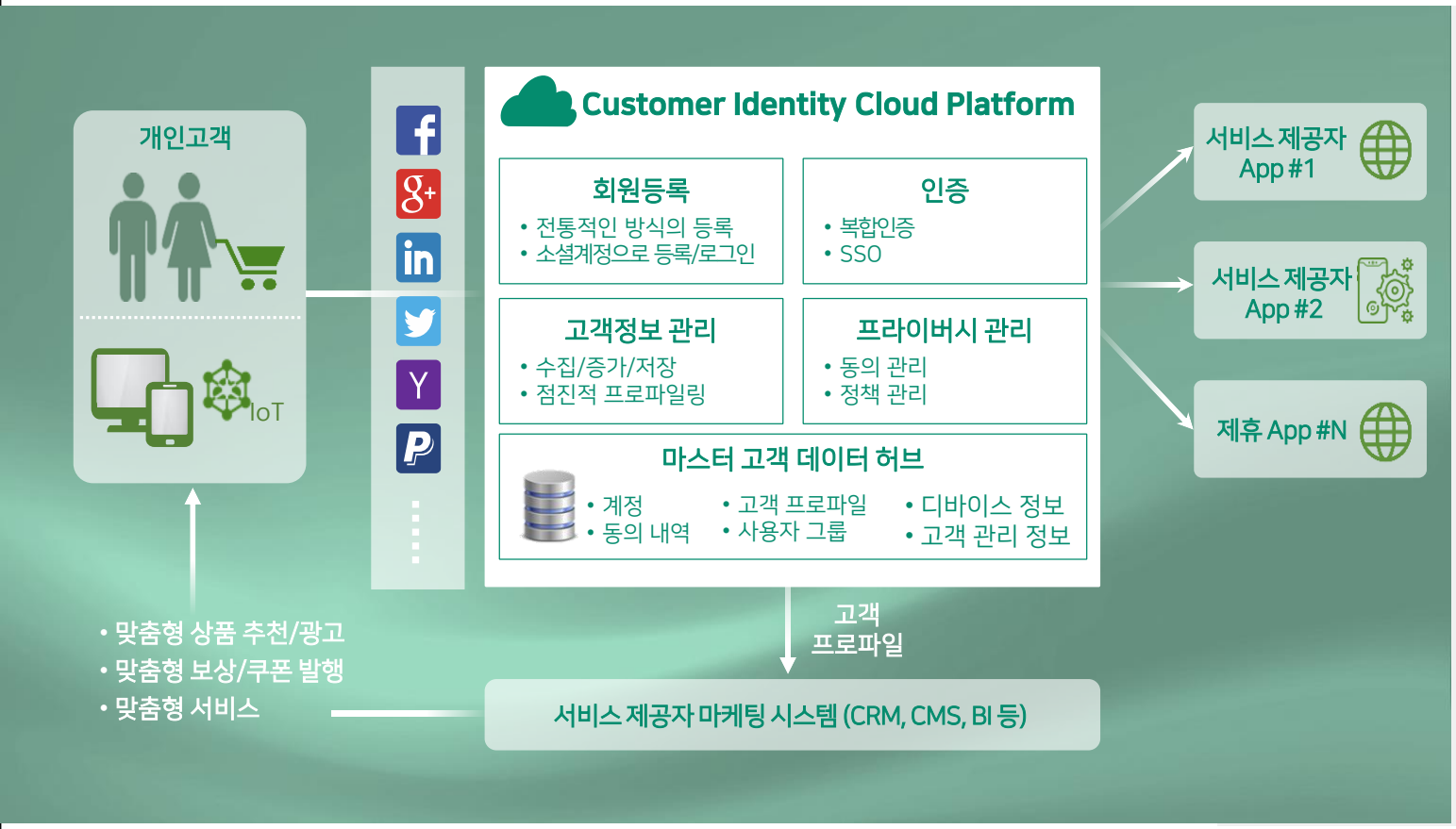
Zero Trust 3대 구현원칙

Hybrid 업무환경의 SSO

SaaS형 IAM 플랫폼

삼성SDS가 준비하는 또 하나의 클라우드 Identity 서비스

- ☑ 개인고객이 사업자 어플리케이션 접속에 필요한 회원가입, 로그인, 인증 관리와 개인 맞춤형 서비스/마케팅에 활용할 수 있는 고객 정보 수집 · 분석 · 관리 서비스를 제공
- ☑ '19年 하반기 서비스 런칭 (기술 파트너 : Akamai Technologies)



☑ 소셜계정으로 간편 회원가입/로그인

- 전세계적으로 많이 사용하는 소셜계정과 연동을 통한 회원 가입률, 방문율 향상

☑ 고객 맞춤형 서비스/마케팅/보상 지원

- 소셜계정에서 실시간· 지속적인 고객동의 프로파일 수집을 통한 풍부한 고객정보 확보
- 분산된/다양한 소스로부터 수집된 고객정보의 통합관리로 정확한 고객분석
- 활용동의 고객정보만 선별하여 고객사 마케팅시스템에 제공

☑ 고객 정보보호 관리 부담 해소

- 고객의 계정 및 개인정보를 각 국가의 개인정보보호 규제를 준수하여 활용·관리
- 다양한 복합인증 지원으로 비인가 접근 차단에 대한 고객 정보보호 의무 준수

Identity 중심의 Zero Trust 구현 효과

☑ Zero Trust를 실현하는 첫 단계인 Identity &Access Management Platform 도입시의 효과

보안사고 감소

비용 절감

기술 비용 절감

*Source : Forrester, 2017

Legacy, perimeter-centric models of information security are of no use in today's digital businesses, as they are no longer bounded by the four walls of their corporation.
Instead, CIOs must move toward a Zero Trust approach to security that is data- and identity-centric …

Thank you

Q&A

SAMSUNG SDS

Realize your vision