Cyber Security Conference 2021

SAMSUNG SDS

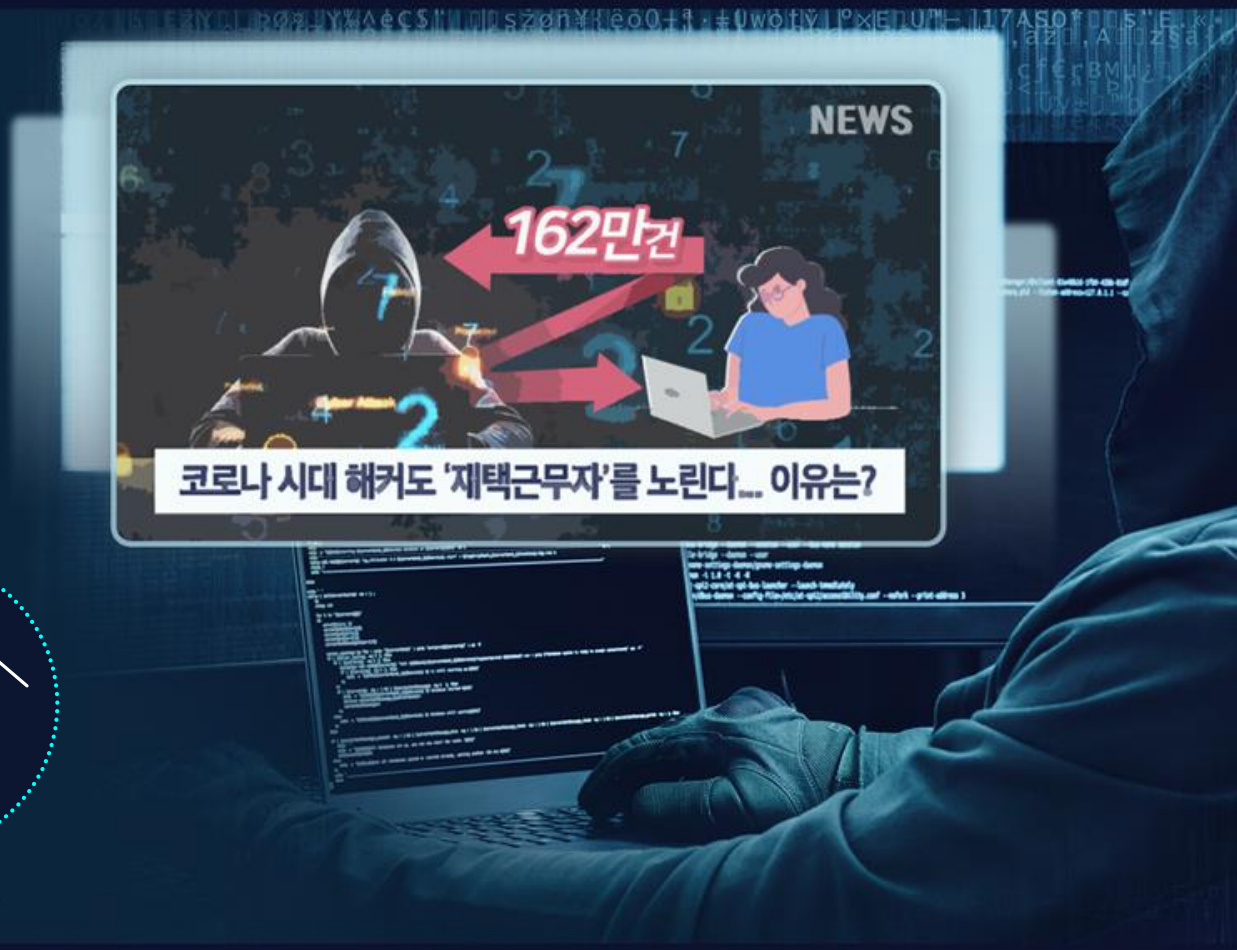
원격 근무 환경에서의

계정 보안 강화

한현희 프로 삼성SDS 보안솔루션팀

재택 환경준비의 어려움

“
코로나 시대
해커도 ‘재택근무자’를 노린다.
이유는?
”



*참고 : MBC 뉴스데스크 2021.01.03 https://imnews.imbc.com/replay/2021/nwdesk/article/6046997_34936.html

재택근무 정보보호 6대 실천수칙

재택근무, 보안관리자는 다 열외일수밖에 없었던 사유

사용자 실천 수칙

1. 개인PC 최신 보안 업데이트
2. 백신 프로그램 업데이트 및 검사
3. 공유기 보안설정/ 사설 WIFI 및 공용PC자제
4. 회사메일 권장, 개인메일 사용 주의
5. 불필요 웹사이트 이용 자제
6. 파일 다운로드 주의

보안관리자 실천 수칙

1. **원격근무시스템 사용 권장**
2. **일정 시간 부재 시 네트워크 차단**
3. **원격 접속 모니터링 강화**
4. **재택근무자의 사용자 계정 및 접근권한 관리**
5. 재택근무 보안지침 마련 및 보안인식 제고
6. 개인정보, 기업정보 등 데이터 보안

재택근무 정보보호 6대 실천수칙 (보안관리자)

특히, 구체적으로 어떤 부분이 어려운가?

고려사항

① 원격근무시스템 사용 권장
- 사내 보안정책에 따른 VPN 사용 권장
- 사내망 접속PC 보안환경 최신화/수시점검

② 일정 시간 부재 시 네트워크 차단
- 재택근무자가 사내 네트워크 접속 후 10~30분간 부재 시 네트워크 접속 차단 설정

③ 원격 접속 모니터링 강화
- 재택근무자의 사내 NW접속현황관리
- 우회 접속 집중 모니터링 실시

④ 재택근무자의 사용자 계정 및 접근권한 관리
- 재택근무자의 비밀번호 설정강화, 접근권한 최소화
- 원격근무시스템 접근 시 OTP등 2차 인증수단 적용

우려사항

VPN = 전통적인 악성코드 감염/전파경로

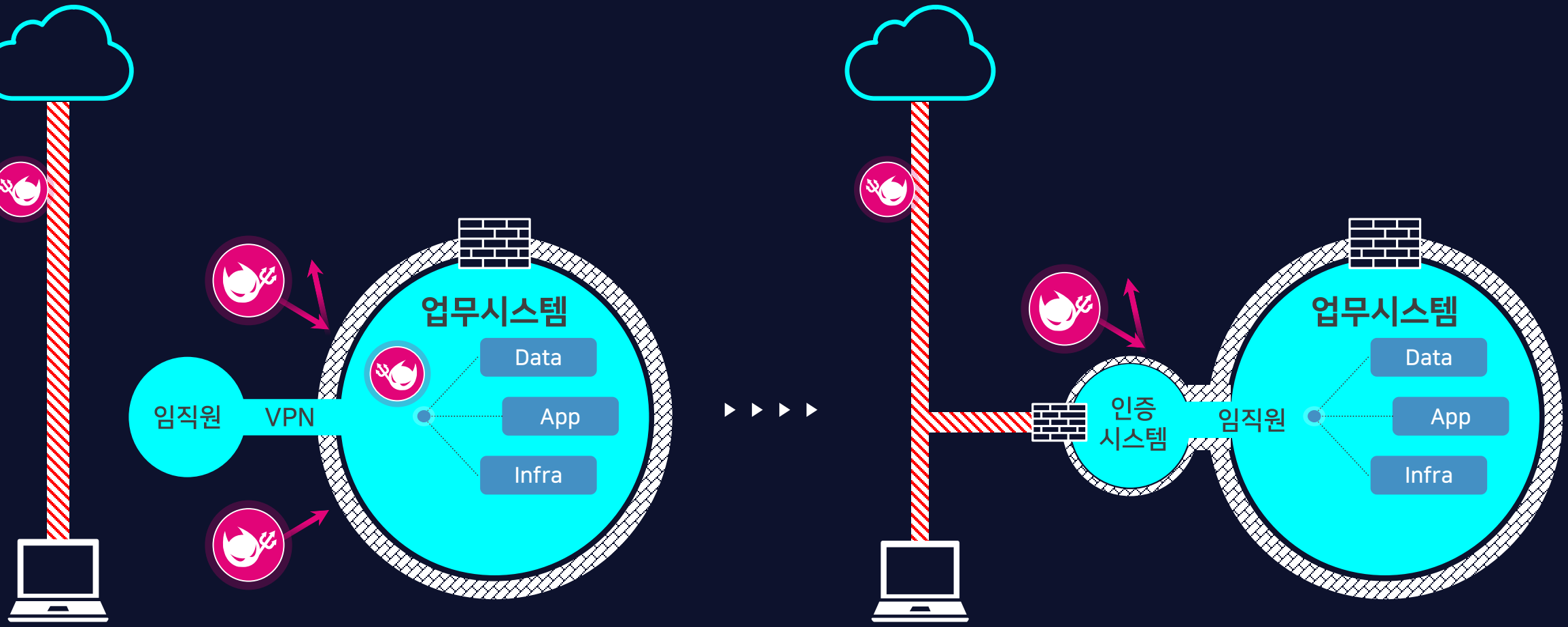
차단 = 장애, VOC

외부 클라우드 업무시스템 접속현황 관리/모니터링?

피싱사이트의 등장으로 계정 유출사고 빈번

① 안전한 원격근무시스템 구현

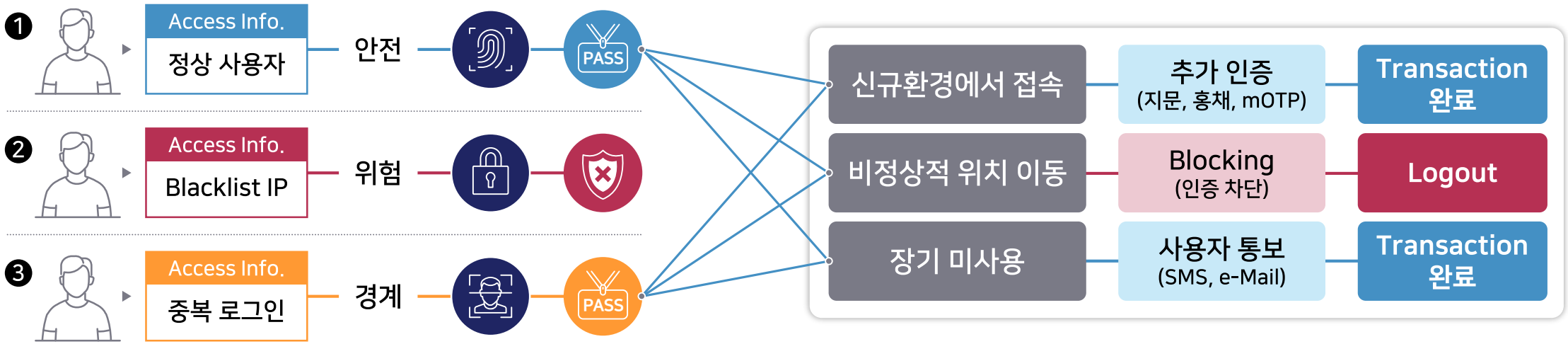
VPN 사용PC를 경유하여 업무시스템이 악성코드에 점유되지 않도록, 인증시스템에서 완충지대 역할수행 필요

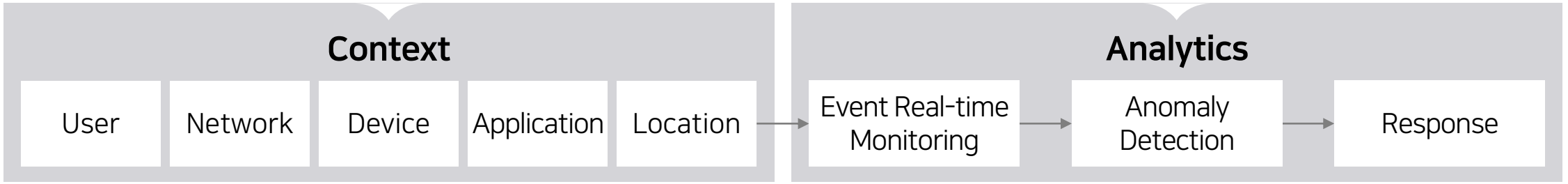


① 안전한 원격근무시스템 구현 – 접근통제 및 검사/로깅

Context 기반의 엄격한 접근통제

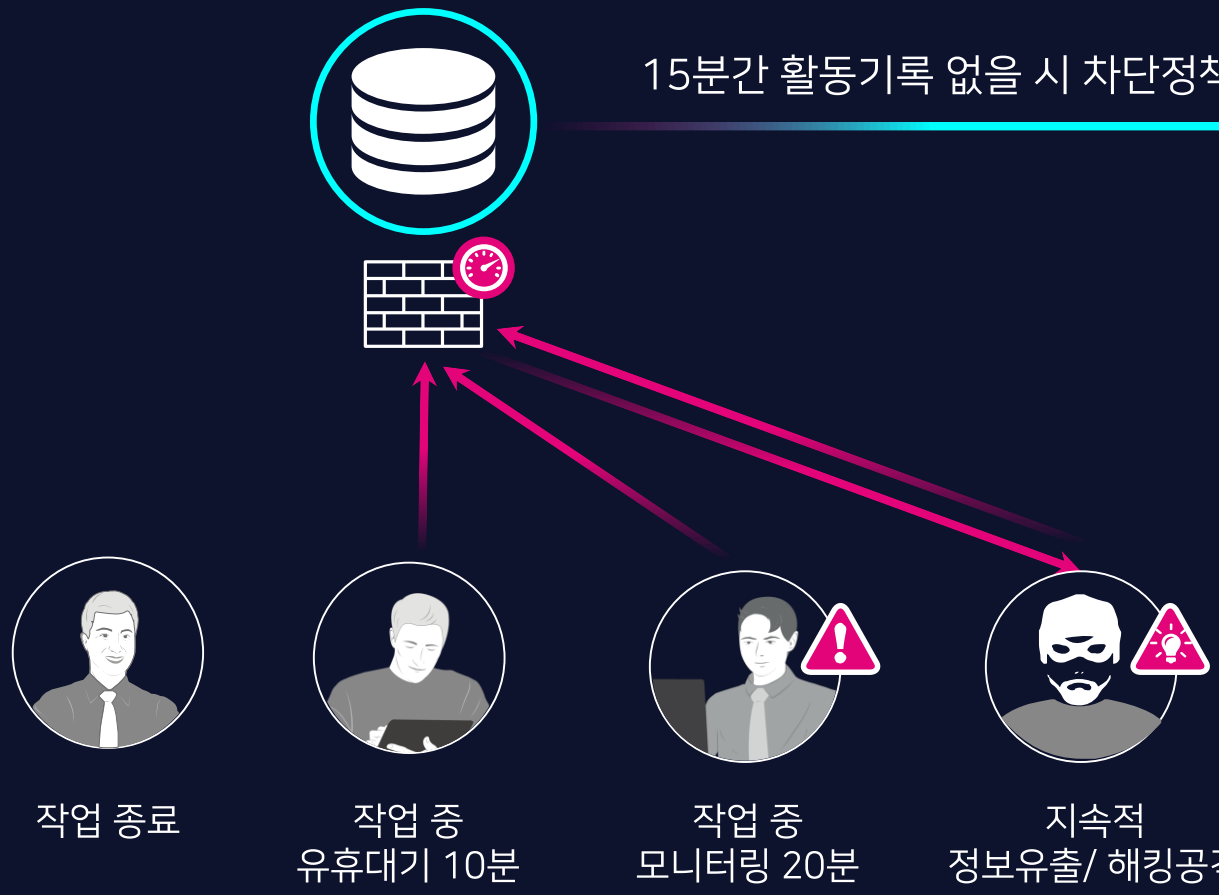
Analytics 기반의 이상행위 검사·로깅





② 업무시스템 접속 관리/차단

단순 시나리오에 따른 무조건적인 차단은 VOC발생으로 이어질 수 있으며 효과도 낮아, 유기적인 대응체계 구현 필요



유기적 대응체계

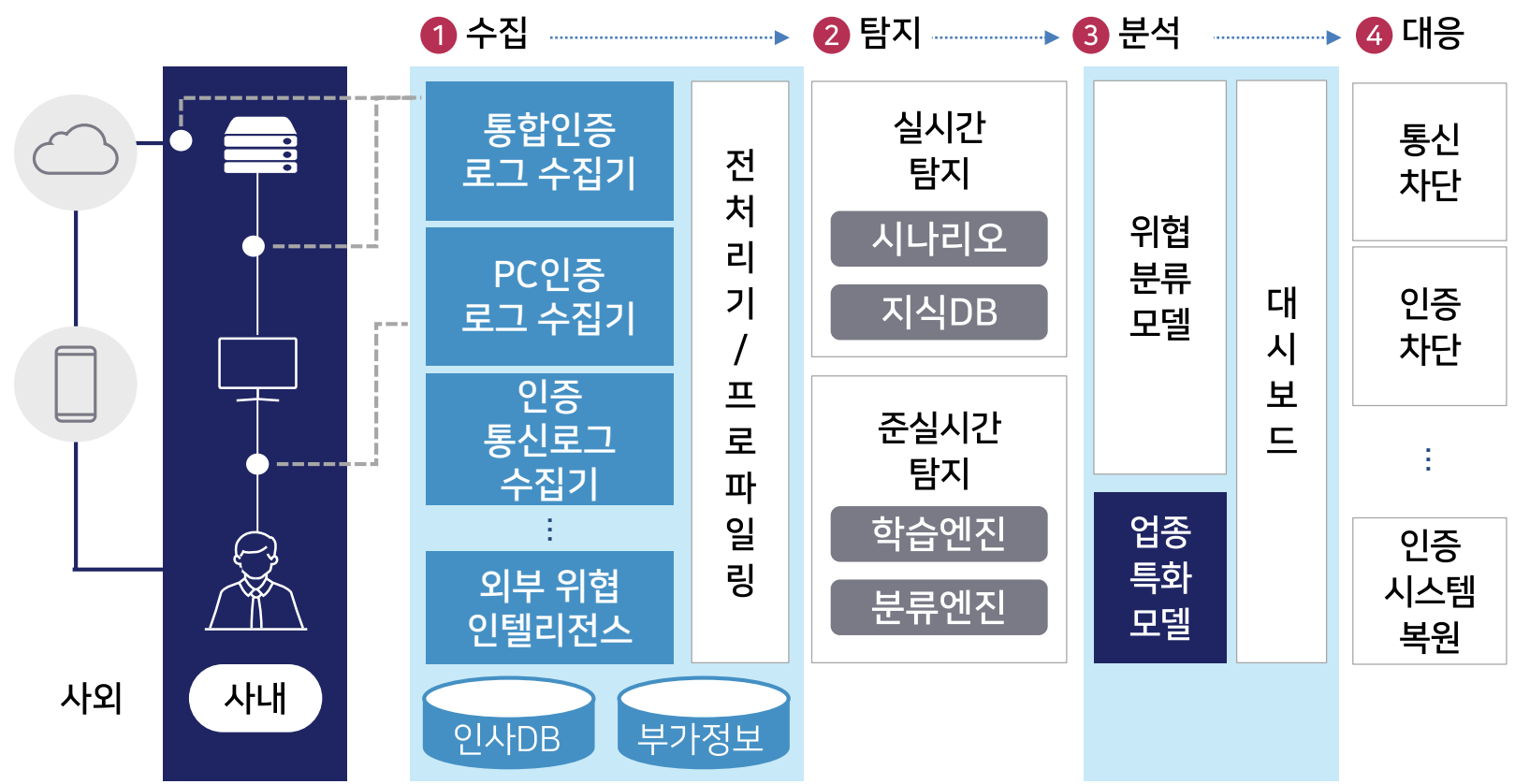
평균대기 10분
차단수행 15분

평균대기 20분
차단경고 25분
차단수행 30분

② 업무시스템 접속 관리/차단 – Analytics 플랫폼(1/4)

유기적인 접근통제 & 대응을 위한 Analytics Platform

구성



① 인증로그 수집 및 고속가공
- 통합인증 솔루션(SingleID) 제공로그
- PC인증 솔루션(AD) 제공로그
- 그 외 통신로그 및 외부인텔리전스 等

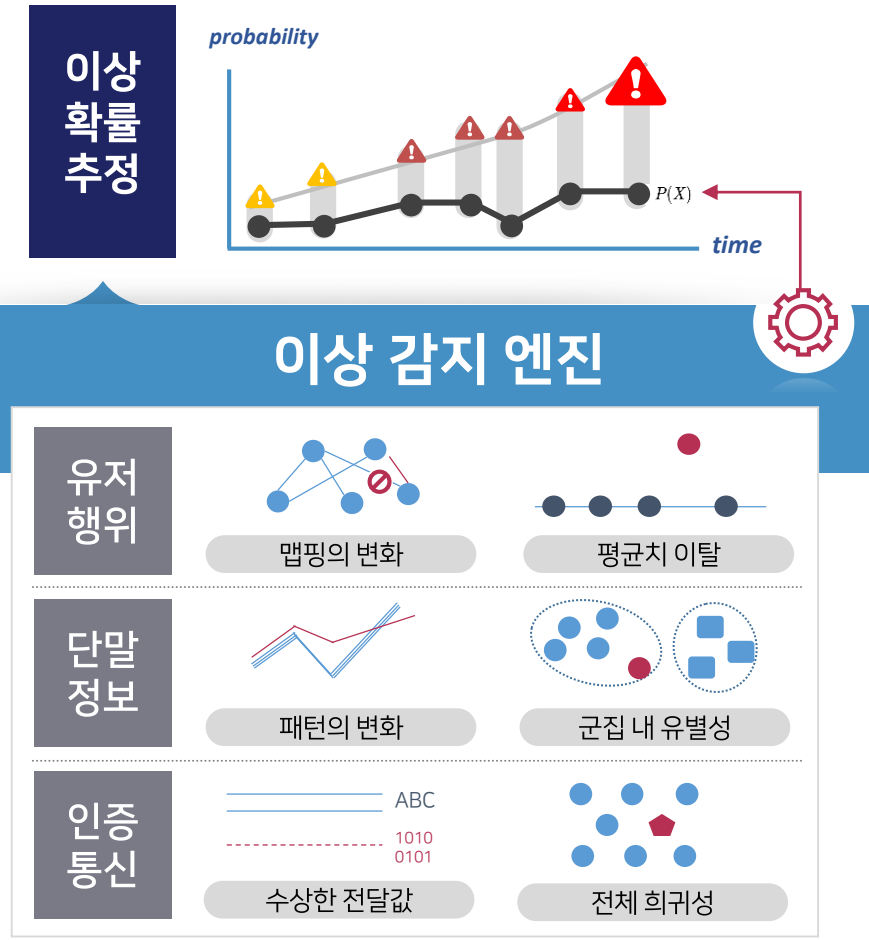
② 복합 이상행위 탐지
- 알려진 이상행위 실시간 탐지
- 알려지지 않은 이상행위 준실시간 탐지

③ 보안위협 및 업종특화 행위분석모델
- 이상행위에 대해 보안위협 분류
- 사용자 정의한 업종특화 특이점 분류

④ 차단/복구 및 타시스템 연계
- MFA 연계, 계정 차단, 설정복구 등 수행
- 비즈니스 로직과 연계

② 업무시스템 접속 관리/차단 – Analytics 플랫폼(2/4)

AI와의 접목으로 유기적이고 효과적인 보안위협 탐지/분석 수행

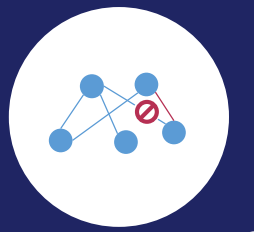


② 업무시스템 접속 관리/차단 – Analytics 플랫폼(3/4)

재택근무를 악용하여 내부자료 유출가능성이 높은 상황에 대한 감지/분석 및 유기적 대응 시나리오

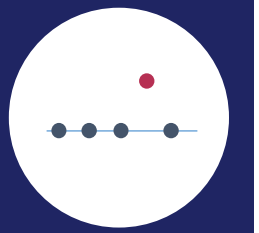
탐지 요약

맵핑의 변화



- 평소: 개발자포탈, 방화벽신청시스템, Github, JIRA
- 특이: 특허준비 자료실, 퇴직금 시스템

평균치 이탈



- 평소: 일 평균 문서조회 3건
- 특이: 분당 문서조회 10건 이상

패턴의 변화

- 평소: 주간 시간대에 사내에서 접속
- 특이: 야간에 사외에서 접속

분석 및 자동조치 내용

내부자 정보유출 의심

- 인사상 특이사항이 있는 임직원이, 평소와 다른 시간대에 민감자료가 있는 시스템에 사외에서 접속 및 대규모로 문서조회(경쟁우위 특허준비.docx 외) 수행

* 본 시나리오에 대해 사전 설정된 자동조치방안에 따라, 추가 문서조회 시 마다 복합인증을 받도록 조정 및, 타 민감자료 시스템 접근 시 관리자 승인을 받도록 권한조정 (1시간 전)

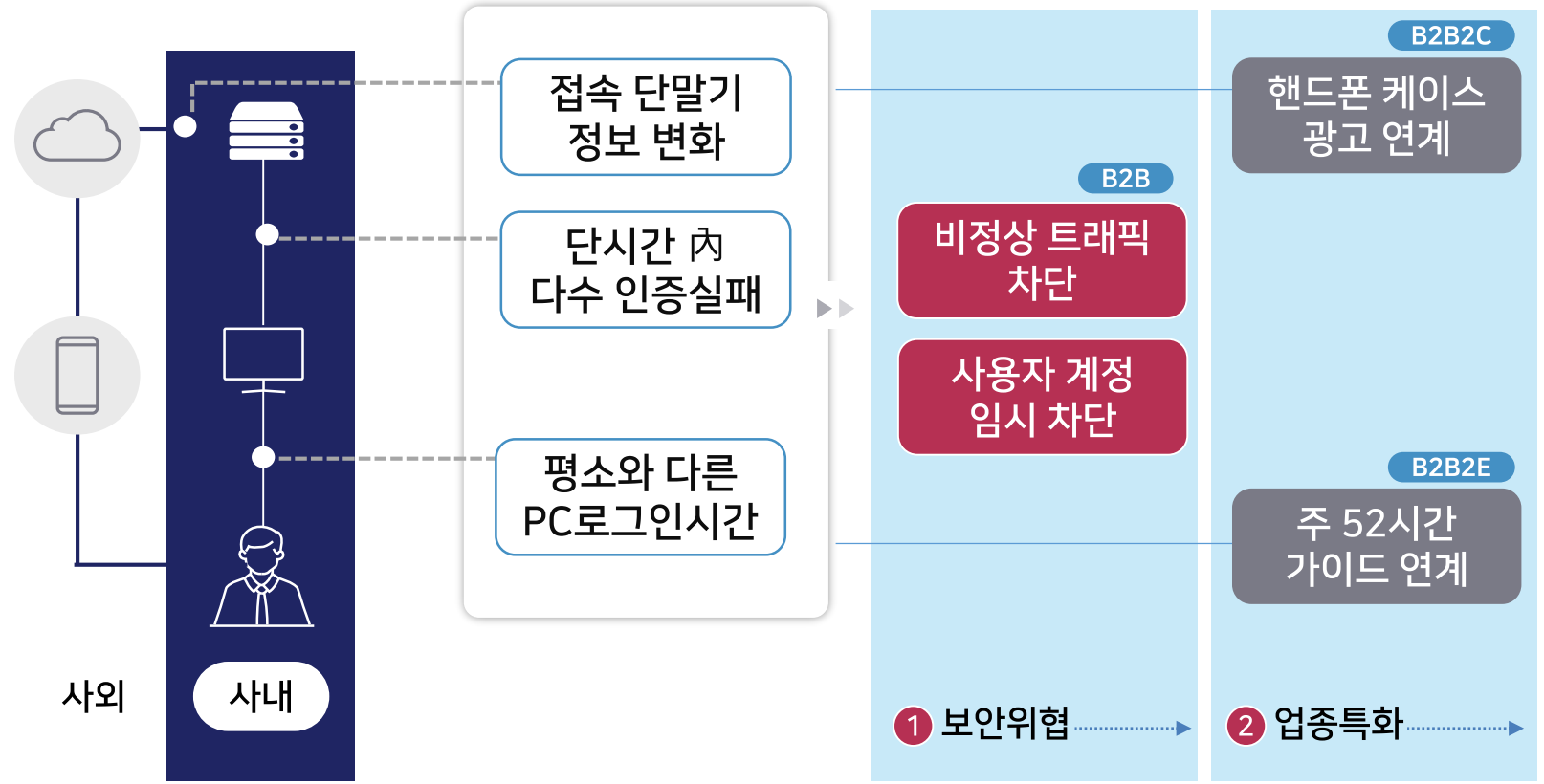
행위자 정보

- **직무** : 개발자
- **고과** : 최근 인사고과 하락 심함
- **이력** : 협력업체에게 ID/PW를 무단 대여하여 적발 (`19.2)

② 업무시스템 접속 관리/차단 – Analytics 플랫폼(4/4)

단순히 보안위협 분석/대응을 넘어서, 고객 비즈니스에 부가가치를 줄 수 있도록 발전 중

활용 범위



① 보안위협 탐지/대응

- 장시간 미사용 임직원의 접속 탐지
- 단시간 내 비정상적인 접속위치 변경
- 로그인 실패 반복
- Blacklist IP에서의 로그인

② 업종 특화모델 탐지/대응

- 사업화 연계 (광고 노출요소)
- 컴플라이언스 연계 (주52시간 등)

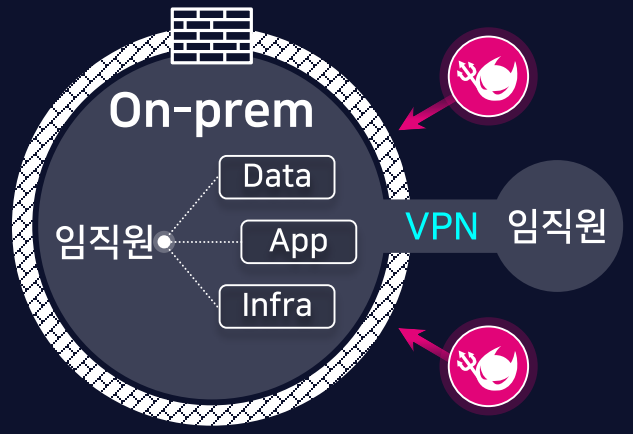
③ 효과적인 원격접속 모니터링 강화

On-Prem시스템 뿐만 아니라 외부 클라우드 업무시스템에 대한 통합 가시성 확보 필요

AS-WAS

On-prem내 자산 Access 관리

관문 네트워크 중심의 보안

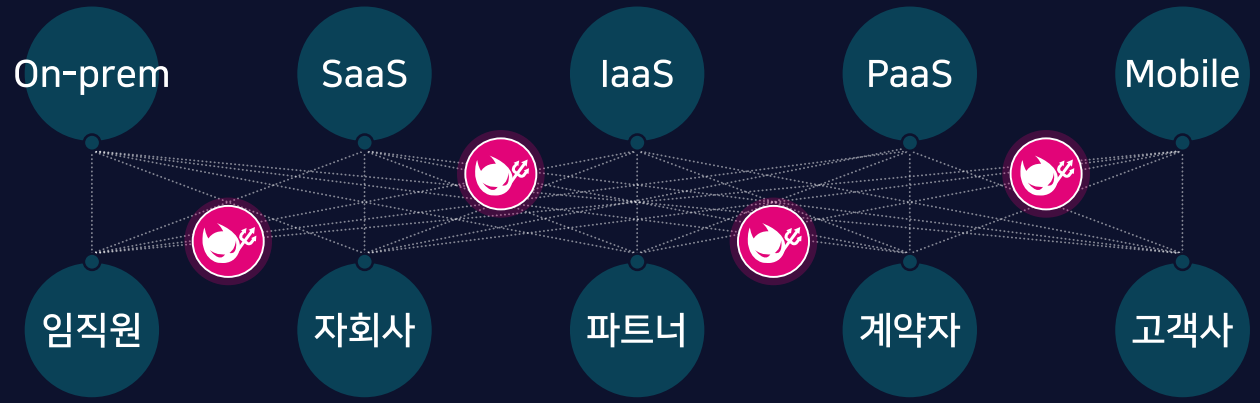


임직원 ID 관리

AS-IS

Resources

네트워크 경계 사라짐 (Cloud, Mobile, Remote Work)



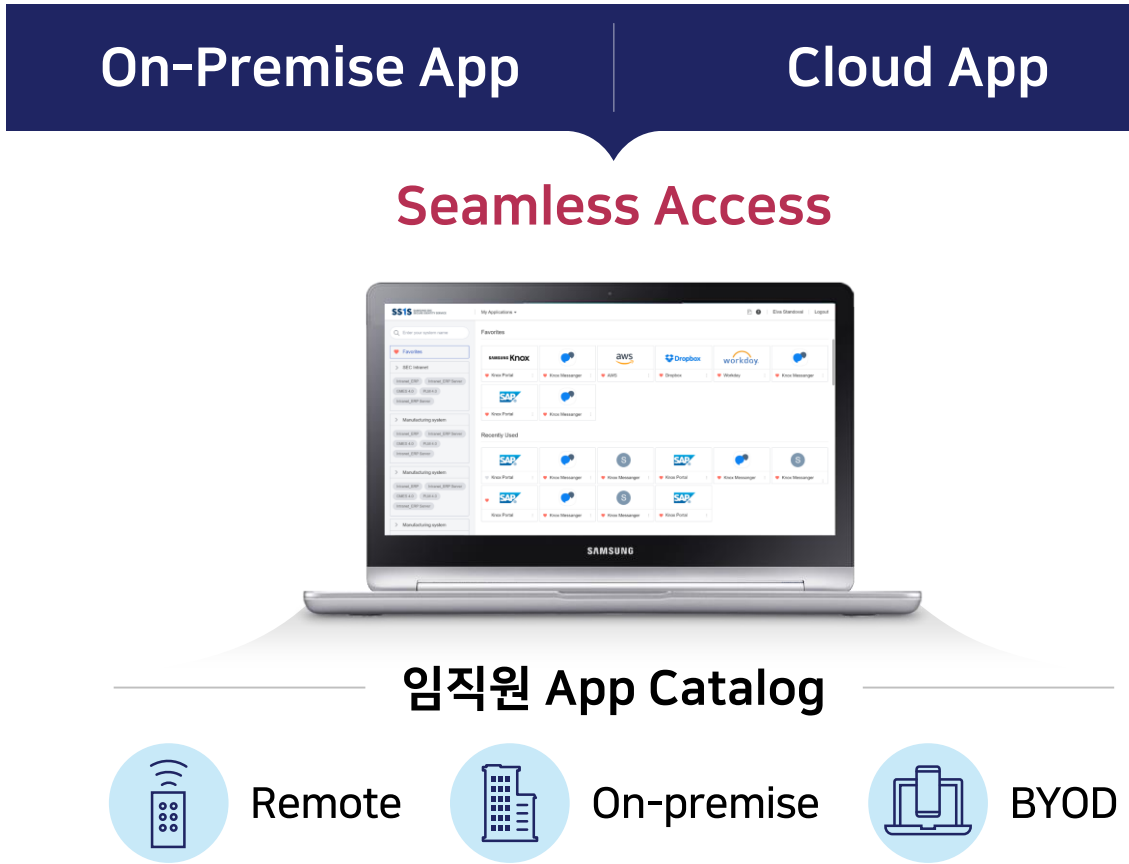
Identities

Identity Breach **위험성** ↑

ID·Access 관리 **복잡성** ↑

③ 효과적인 원격접속 모니터링 강화 – Cloud Workspace

흩어진 SaaS App.들을 찾아 다니며 로그인 하지 않고, CASB서비스와 결합된 Cloud Workspace 한 곳에서
단일ID로 로그인 하여 협업할 수 있는 서비스 공간 제공



✔ 사용 편의 향상

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

✔ 적용 편의성 향상

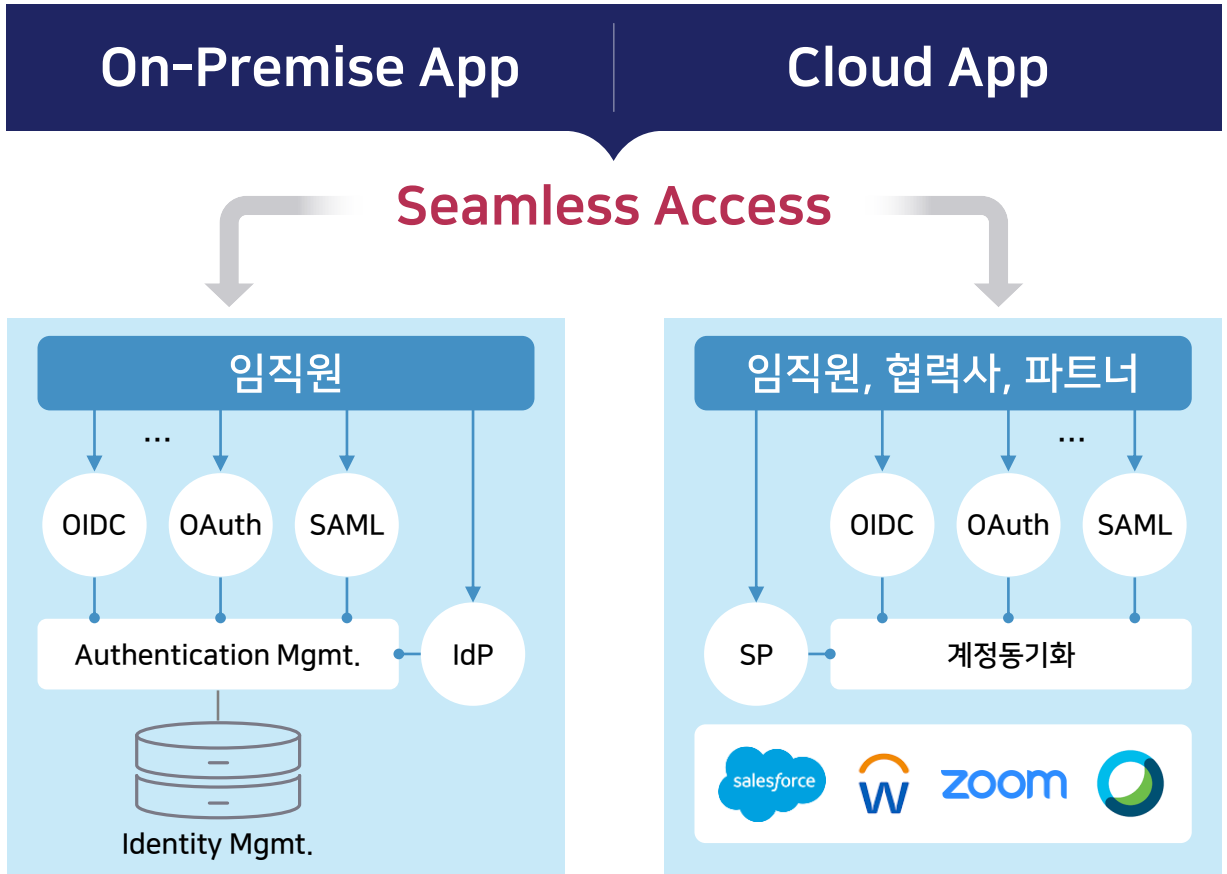
- On-prem, Cloud App의 개별 계정·접근통제 관리 복잡성 해소
- 흩어져 있는 SaaS App.과의 사전 연계로 접근통제 정책의 손쉽고 신속한 적용

✔ 사용자 Self-Service 제공

- 개인정보 조회 및 수정
- 시스템 사용 권한 신청
- 비밀번호 변경, FAQ

③ 효과적인 원격접속 모니터링 강화 – Single Sign On

On-Premise, Cloud를 아우르는 단일 ID기반의 통합 관리 체계로 사용 편의성·적시성 향상



✔ 사용 편의 향상

- 단일 ID로 사내/사외 시스템 간 SSO로 통합 접속
- 계정동기화로 편리한 사용자 관리

✔ 적용 편의성 향상

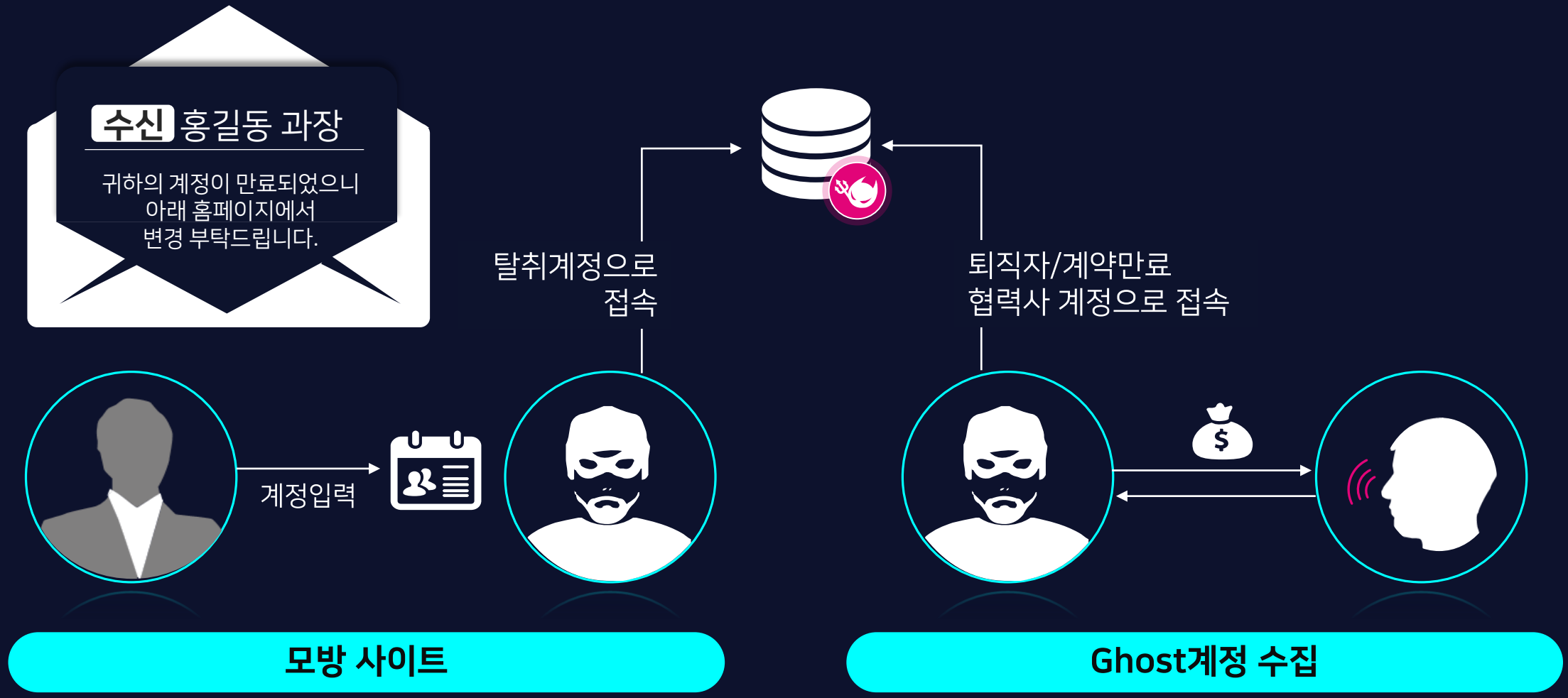
- SAML 2.0, OpenID, OAuth 2.0 등 표준인증 기술 적용
- 개발자 포털을 통해 사전 검증 및 Test 수행 지원

✔ 사용자 Self-Service 제공

- 다양한 SaaS App. 사전연계로 계정등록 즉시 사용
- SaaS向 서비스로 즉시 확장 가능

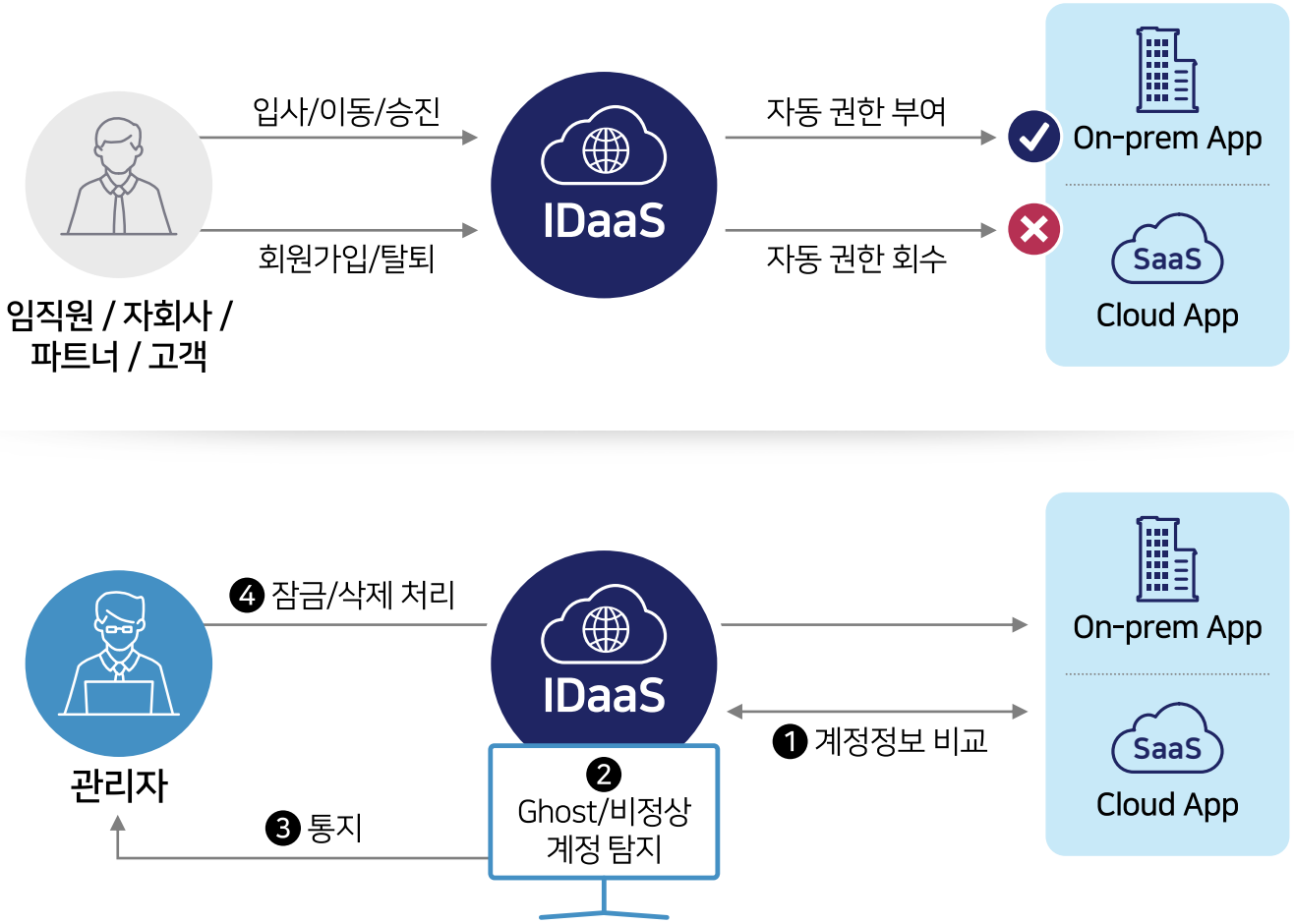
④ 재택근무자의 사용자계정 및 권한관리

Ghost계정에 대한 관리 및, 본인인증에 대한 강화로 탈취계정에 대한 대응 필요



④ 재택근무자의 사용자계정 및 권한관리 - 계정관리

허가된 사용자 ID 생성부터 폐기까지 Life cycle 관리 및 비정상 계정(Ghost) 검증으로 보안성 강화



✔ 허가된 사용자 ID Life cycle 관리

- 허가된 사용자에 대한 적시 권한 부여
- 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

④ 재택근무자의 사용자계정 및 권한관리 – 인증수단 강화

사용자 편의성 증대를 위해 모바일 BYOD와 App.을 활용하여 PIN번호 및 OTP 입력없이 간편터치 방식의 인증지원으로 One Touch 인증 서비스 제공

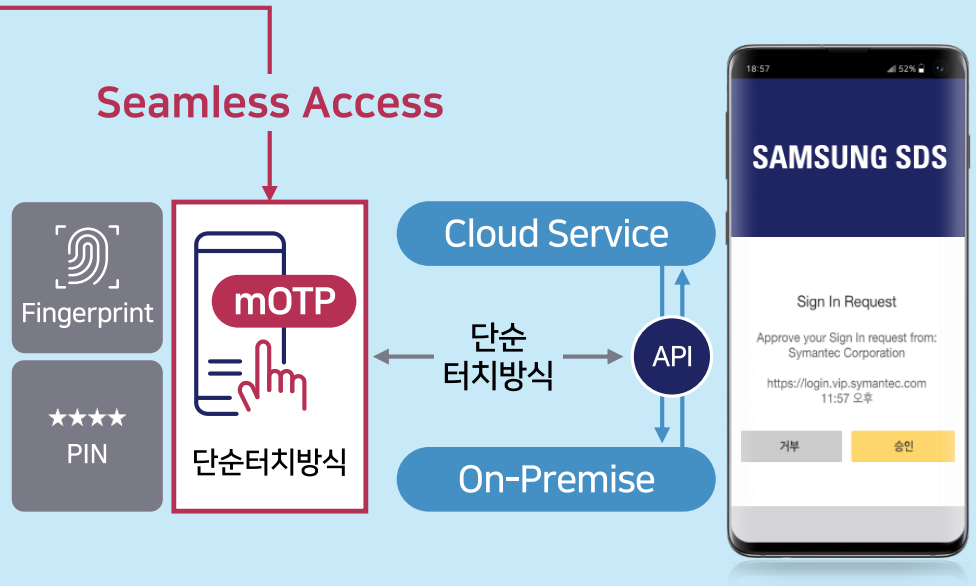
AS-IS ▸▸ To-Be

간편인증 서비스

편의성 향상	본인 확인	복합인증	생체 인증	중요 시스템 관리	모바일 보안강화

간편터치방식 mOTP 인터페이스

PIN번호 및 OTP 입력없이 간편터치방식의 인증지원으로 편리하게, 쉽게, 안전한 인증 서비스 제공



재택근무에 대한 효과적 준비를 위한 요구사항들

허가된 **사용자**만

허가된 **접근권한** 내에서

허가된 **정보자산**에 한해서

정상적인 Context일 때만

I. Secure Access

Access 필요한 **모든 사용자**가

한 번의 인증으로

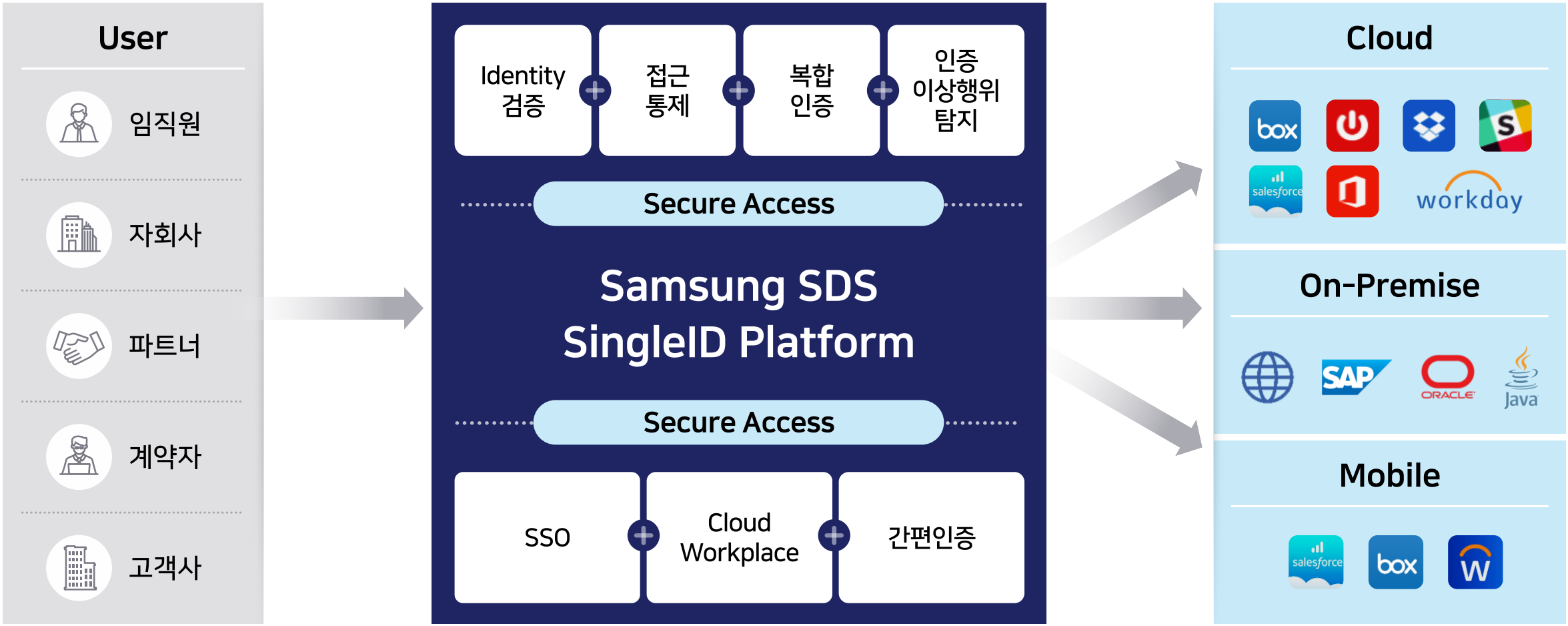
Anywhere, Any Device / Browser로

On-prem 부터 **Cloud App** 까지

II. Seamless Access

Secure & Seamless Access – SingleID Platform

허가된 사용자·디바이스가 접근정책 준수 시에 **한번의 인증으로** 권한 내의 **다양한 업무 App**에 액세스 제공



사례) SmartID 체계 개요

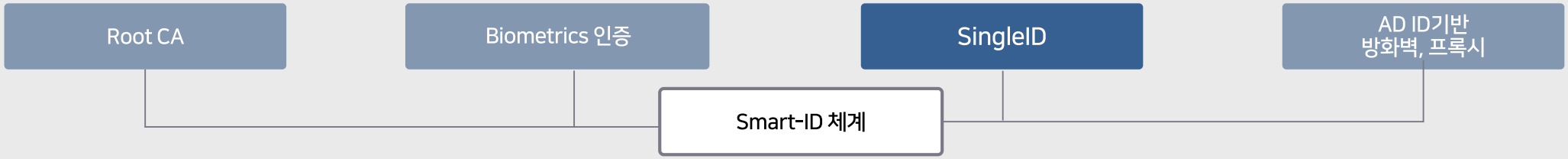
SmartID(단일ID, 안면인식)로 모든 임직원이 모든 업무 환경 사용이 가능한 Secure & Seamless Access 체계

인증서 기반
네트워크 **자동연결**

Biometrics
PC 로그인

Biometrics로
업무시스템 통합 로그인

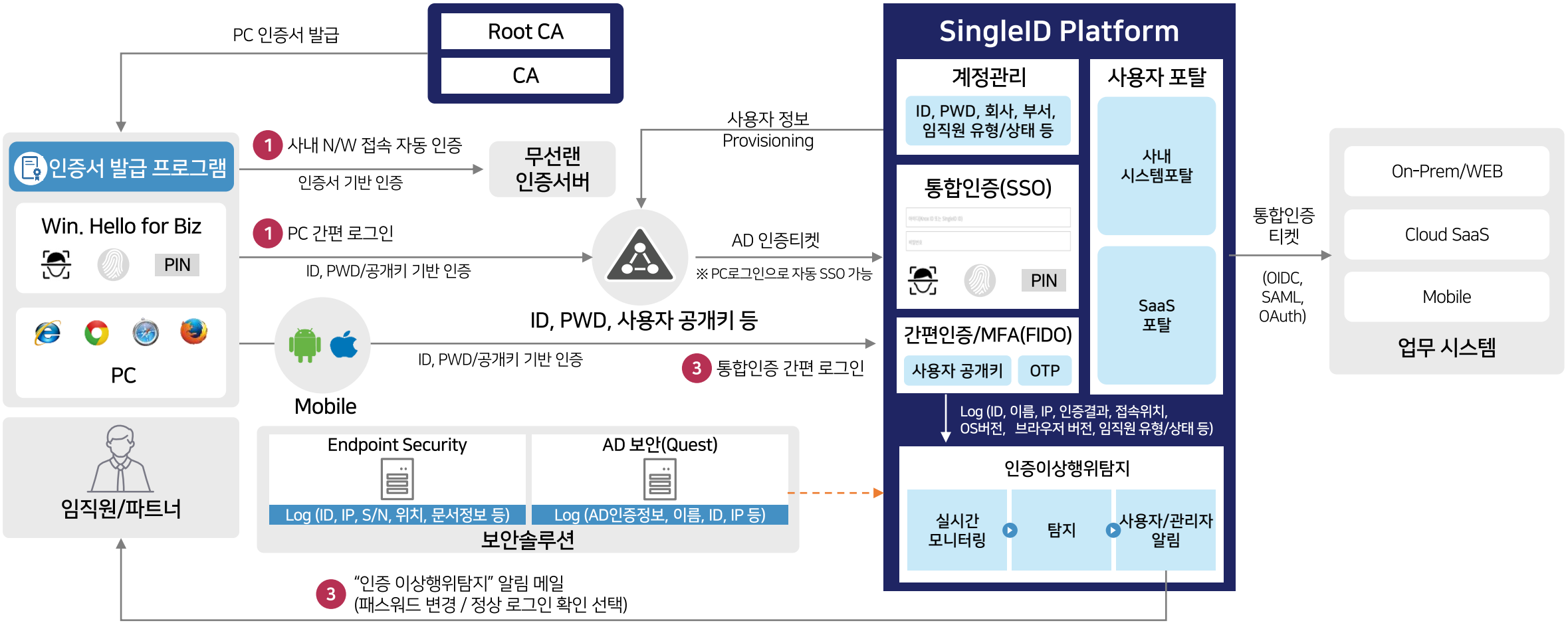
ID기반으로 네트워크
권한 부여



※ Smart ID란? One-ID, Biometrics, One-Pass On-Premise부터 Cloud까지 지원

사례) SmartID 체계 구성

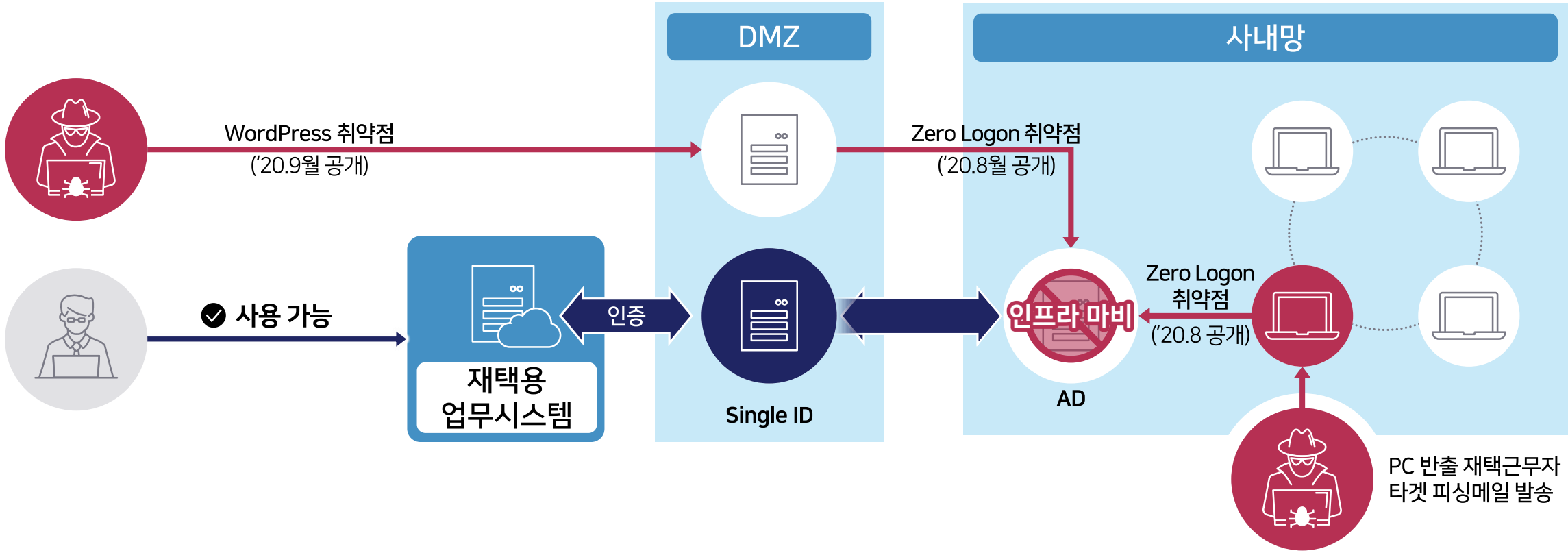
SmartID(단일ID, 안면인식)로 모든 임직원이 모든 업무 환경 사용이 가능한 Secure & Seamless Access 체계



사례) SmartID 체계 보안성

MS Active Directory를 타켓팅한 공격으로 사내 인프라 붕괴 시에도, 통합인증체계 정상운용 가능

ZeroLogon취약점(전체 패치는 '21년 상반기 발표) 기반 공격사례



기대효과

Zero Trust를 실현하는 첫 단계인 **SingleID Platform** 도입시의 효과

보안사고

유출/취약 패스워드 이용,
계정 악용에 따른 Identity Breach

기술 비용

기술 연계 비용,
기능/솔루션 중복 투자

사용자 생산성

단일 ID로 업무시스템에 1회 로그인,
필요 업무시스템 적시 사용

* Source : Forrester

코로나 이후의 세계

집안에 머무는 시간이 즐거우면 어떻게 될까? .. 결국 편안한 집에서 휴식을 즐기는 쪽으로..

Know ledge
(ID/PW)

Identity
(Face, Mobile)

Things
(IoT, Device)

Thank you

SAMSUNG SDS