성공적인 재택(원격) 근무 지원을 위한 보안

온라인으로 함께 하는
제6회 IBM Security Summit

한국IBM
박형근 실장

84%

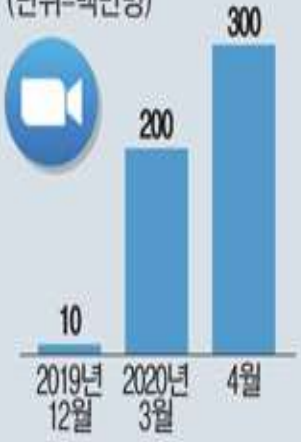
2020년 2월 초부터

원격 업무 툴 사용 급증

코로나 사태 이후에도 재택근무와 원격 근무 유지

줌 전 세계 일일 사용자 수

(단위=백만명)



*자료= 줌·외신 종합

원격근무 체제 지속하는 IT 업체들

트위터	희망자는 퇴직 때까지 자유롭게 재택근무 허용
구글	이동제한 해제 후에도 재택근무 및 온라인 행사 추진
페이스북	재택근무 기간을 올해 말까지 연장
카카오	주 1회 사무실 출근 · 주 4회 원격근무 체제 연장
SK텔레콤	직원 거주지 10~20분 위치에 거점 오피스 구축

출처: 매일경제

원격 근무

조사 대상 조직의 85%가 재택 근무 프로그램 통해 생산성 향상 보고

International Workplace Group

500명 직원 대상으로 한 스탠포드 대학 연구에서 직원 이탈 50% 감소

개인 기기 사용으로 직원 하루 58분 절약 및 생산성 34% 향상!

Frost & Sullivan

BYOD 허용 회사는 매년 직원당 평균 약 40만원 절약

Cisco

재택 근무 사용자 간 디지털 신뢰 구축

집에서 일하는 사용자는 모든 장치에서 작업

UEM(Unified Endpoint Management)은 사용할 장치 정의

아이덴터티 및 접근 관리(IAM)는 사용자 접근 확인

특권 접근 관리(PAM)로 내부자 위협 방지

능동 위험 기반 모니터링

보다 스마트한 보안을 제공하는

디지털 트러스트

올바른 조건에서

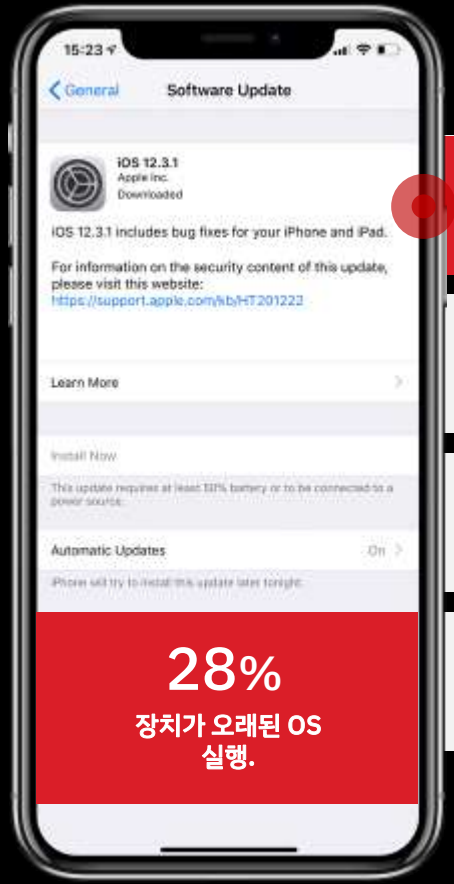
올바른 사용자가

올바른 데이터에

올바른 접근을

할 수 있도록 합니다.

원격 작업으로 인한 다양한 위험 수준



디바이스 위험

28%

장치가 오래된 OS 실행.

Forbes

Billionaires Innovation Leadership Money Consumer Industry Lifestyle BrandVoice

20,114 views | Jul 30, 2019, 03:11am

iPhone iMessage Security Vulnerability Lets Attackers Read Your Files From Anywhere

Davey Winder Senior Contributor

Cybersecurity

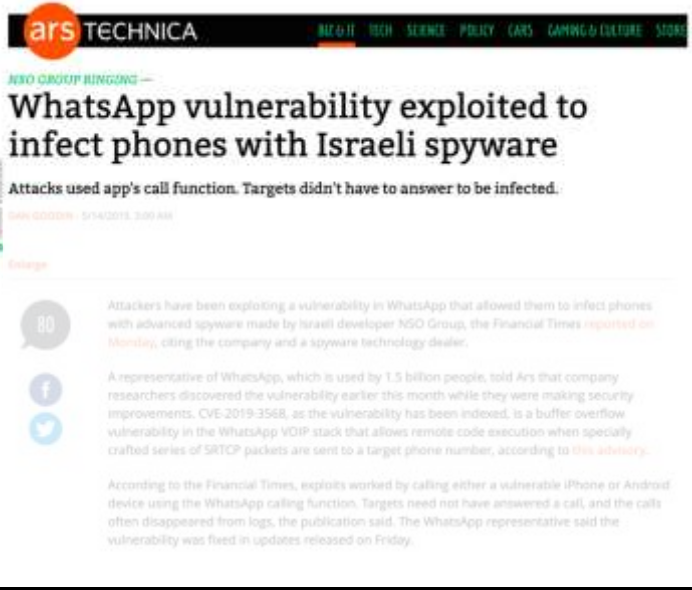
I report and analyse breaking cybersecurity and privacy stories

원격 작업으로 인한 다양한 위험 수준

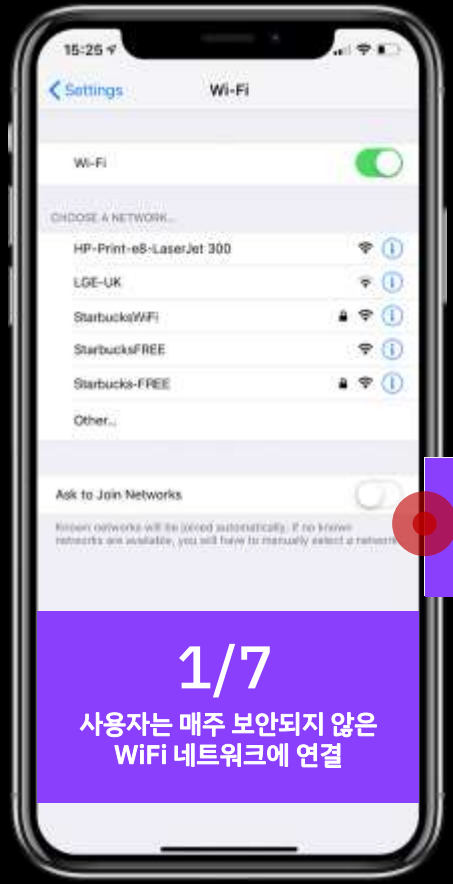
앱 위험

WhatsApp Pegasus

보안 결함으로 인해 해커는 사용자에게 전화를 걸어 감시 스파이웨어를 트리거할 수 있었습니다. iOS와 Android 모두에 영향을 미쳤습니다.



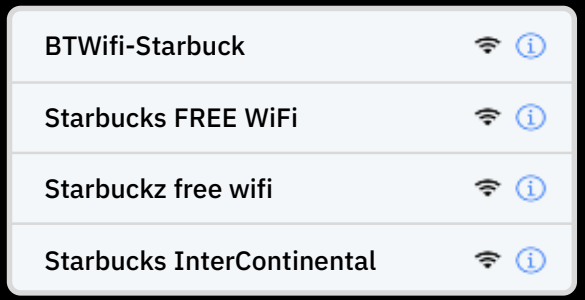
원격 작업으로 인한 다양한 위험 수준

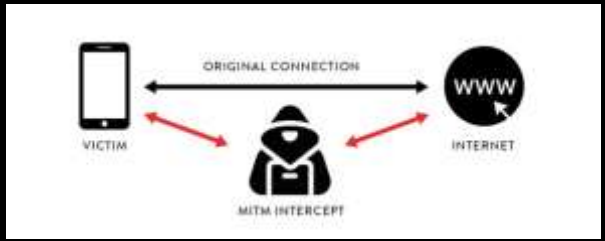


네트워크 위험

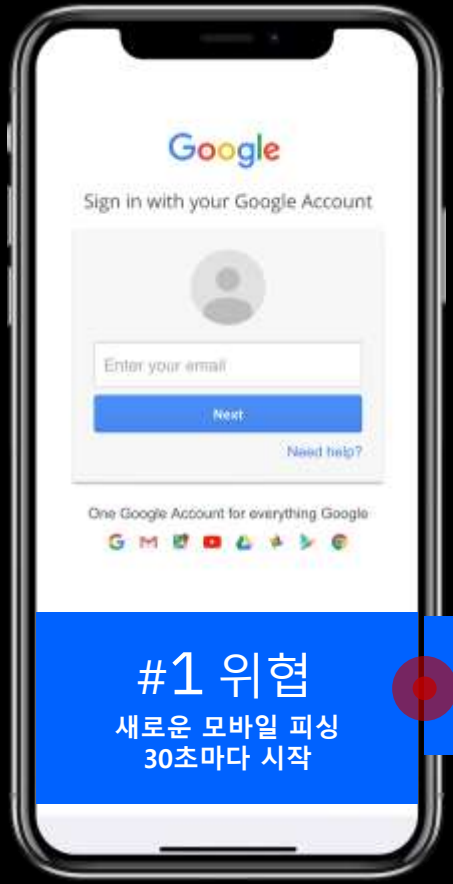
1/7

사용자는 매주 보안되지 않은
WiFi 네트워크에 연결





원격 작업으로 인한 다양한 위험 수준



#1 위협

새로운 모바일 피싱
30초마다 시작

콘텐츠 위험

UEM이란 무엇인가?

UEM은 모바일 장치 관리(MDM) 및 엔터프라이즈 이동성 관리(EMM)의 발전에 있어 다음 단계입니다.

스마트폰, 태블릿, 랩톱 및 IoT를 구성하고 관리하는 **단일 콘솔**

애플리케이션 통합
- 데이터 보호
- 디바이스 구성
- 사용 정책

최종 사용자 지원 및 수집 업무 분석을 향상시키기 위한 **단일 사용자 보기**

관련 기술(SIEM, IAM, CMT)의 활동을 조율하기 위한 **조정 지점**

즉시 사용 가능한 사용자 환경을 위한 UEM

최소한의 관리 혹은 관리가 필요 없는 PC와 맥 배포

- 대량 등록/ 무선(OTA) 프로비저닝
- 최종 사용자 셀프 서비스
- 엔터프라이즈 자원에 즉시 접근
- 통합 앱 카탈로그에 대한 SSO
- 커스텀 이미지를 만들 필요 없음
- 수동 구성 또는 업데이트 불필요

Apple 디바이스 등록 프로그램 (DEP)

Android Enterprise

삼성 Knox 모바일 등록(KME)

Windows Out-of-the-Box Experience

UEM와 함께 재택 근무 정책 준수 보장

자동 설정

- 이메일, 앱 및 정책의 기본 구성
- VPN 배포 및 구성

향상된 정책

- 세분화된 정책 구성
- 모범 사례와 연계된 AI 정책 권장 사항

원격 조치

- 원격 잠금
- 실시간 위치
- 공장 초기화
- 선택적 지움
- 사용자 셀프서비스 포탈

데이터 관리

- 한계 또는 속도 제한된 데이터 사용
- WiFi 전용 앱 강제화

IBM Security MaaS360

내재된 보안
- 기본 컨테이너화 및 데이터 손실 방지(DLP)

주문형 애플리케이션
- 기업 애플리케이션 및 컨테이너만 관리

경험의 통일
- 모든 장치에서 통합된 최종 사용자 경험 위해 MaaS360 PIM, Browser & Content Suite 배포

노트북 및 데스크탑 지원.
- 기본 패치 및 업데이트 관리, 레거시 앱 및 파일 배포

기업 데이터 컨테이너

거의 10년의 장치 관리 및 컨테이너가 여전히 강력해지고 있습니다.

원격 근무 시나리오에서 컨테이너는 중요한 데이터에 대한 접근 권한을 부여하고 DLP 통제를 제공하는 가장 빠르고 안전한 방법 중 하나입니다.

그렇게 동작하는 이유는

- 개인용 디바이스 상에서 데이터의 분리
- 안전하게 암호화된 샌드박스
- 유연성

최종 사용자의 간단한 지원 문제 처리

셀프 서비스 포털 최종 사용자는 자신의 컨텐츠, 앱 및 장치를 관리합니다.

- 모든 디바이스에 걸쳐 컨텐츠 동기화
- 콘텐츠, 파일과 폴더의 추가와 공유
- 디바이스 상의 원격 조치
  - 위치, 잠금, 초기화, 패스코드 재설정
- 디바이스 정보 보기
  - 조치 히스토리, 하드웨어/네트워크 정보, 보안/컴플라이언스 상태

엔드포인트 관리 MaaS360 with Watson

단말 보안 위협 환경

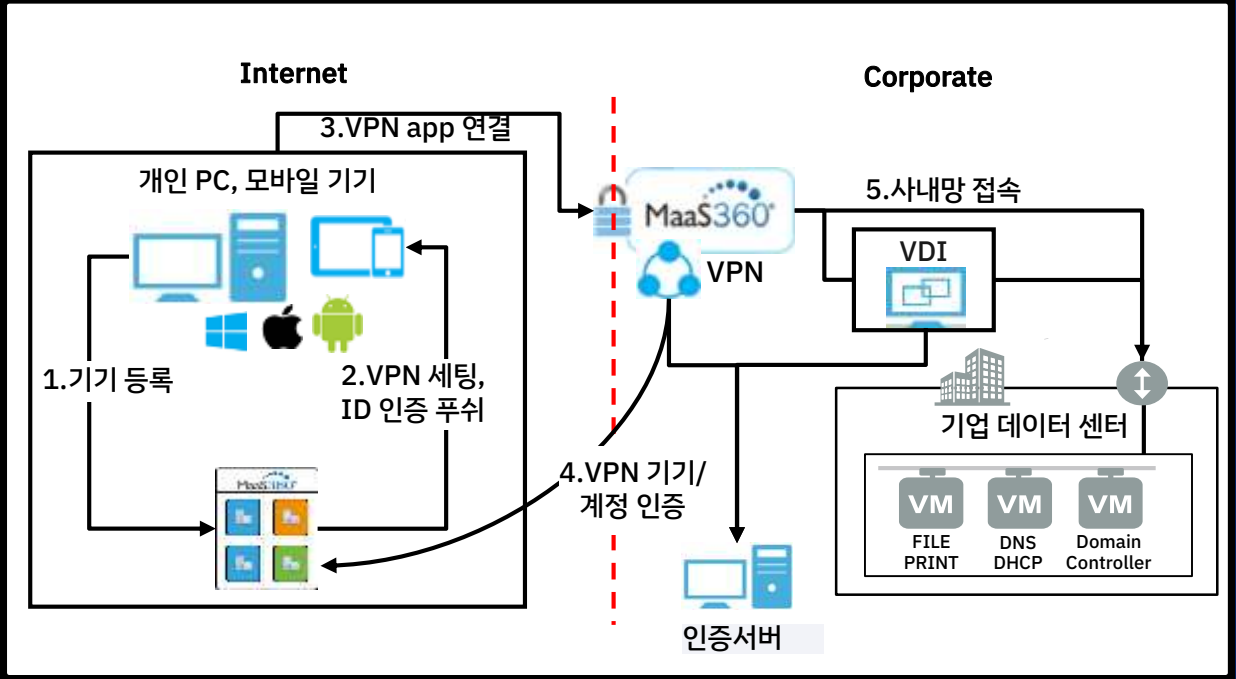
- 오래된 OS 버전 및 미패치 상태
- 다수 프리웨어/쉐어웨어 프로그램

악성 사용자 침투

- 키로깅/화면캡쳐
- 원격제어 환경 구성

외부 제어 기반 위협

- 대외비 정보 유출
- 내부망 침투 경로 활용



주요 기능

다양한 환경 지원 및 확장

- Windows/ MAC OS 환경 지원
- 사용자 대량 등록/ 무선 환경 프로비저닝 가능
- 사용자 셀프서비스

허용된 단말 및 애플리케이션 사용

- SSO 통합 애플리케이션 카탈로그
- 미인증 단말 접속 차단
- 애플리케이션 설치 제어
- 카메라 및 음성 녹음 사용 제어
- 위치 기반 제어
- USB 및 SD카드 사용 차단

설치 및 운영의 편리성

- 수동 설정 및 업데이트 불필요
- 사용자 셀프 서비스 기반

디바이스가 보호되었습니다.

이제 사용자 접근은 어떻습니까?

보다 생산적인 원격 근무 가능

- 공통 협업 및 생산성 도구에 대한 강력한 의존성: Slack, Zoom, Office 365, Box 등
- 별도의 사용자 이름과 비밀번호를 요구하지 않고 이러한 앱에 접근하려면 일관된 접근 방식 필요
- 최종 사용자는 업무 수행, 접근 요청 및 궁극적으로 로그인에 필요한 앱을 쉽게 찾을 수 있는 방법 필요
- 누가 어떤 앱에 어떤 조건에 접근할 수 있는지에 대한 정책 설정 및 시행

공통 ID 계층이 없으면 앱마다 다른 보안 제어 및 일관되지 않은 사용자 경험

1st Factor: Username1 / Password1
2nd Factor: SMS or Email OTP

1st Factor: Username2 / Password2
2nd Factor: None

1st Factor: Username3 / Password3
2nd Factor: Google Authenticator

IDaaS

SaaS(Software-as-a-Service)를 통해
구독 기반으로 제공되는 ID 및 접근 관리

싱글사인온(SSO)

멀티 요소 인증

사용자 라이프사이클 관리

권한 확인

감사, 보고 및 분석

IBM Cloud Identity

디바이스로부터 싱글사인온(SSO)
- 모든 장치에서 모든 애플리케이션으로 통합 애플리케이션 런치 패드 및 SSO 제공

어떤 대상 시스템으로 이중 요소 인증
- 유연한 MFA로 웹, 클라우드, 모바일, VPN 및 운영 체제 보호

사용자 권한 통제와 관리
- 애플리케이션에 대한 사용자 접근 요청, 승인, 프로비저닝 및 재인증

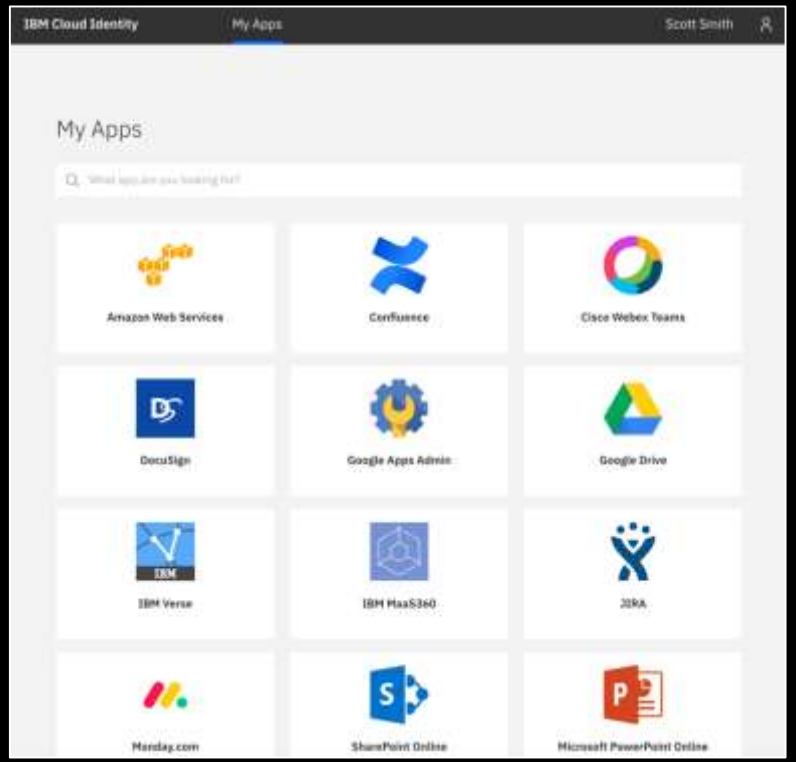
위험 기반 접근
- 위험이 높은 경우 사용자 속성의 전체 컨텍스트를 평가하고 MFA 시행.

아이덴터티 분석
- 접근 위험을 보고 해당 위험 정보를 바탕으로 조치

필요한 모든 앱을 쉽게 검색 및 접근

직원이 클라우드에서 또는 데이터 센터에서 실행 중인 근무 환경 애플리케이션을 쉽게 검색 및 사용 가능

- 애플리케이션에 대한 검색과 모든 접근
- 접근 요청
- 설정과 프로파일 관리
- 이중 요소 인증 디바이스 등록
- 사용자 이름과 패스워드 변경



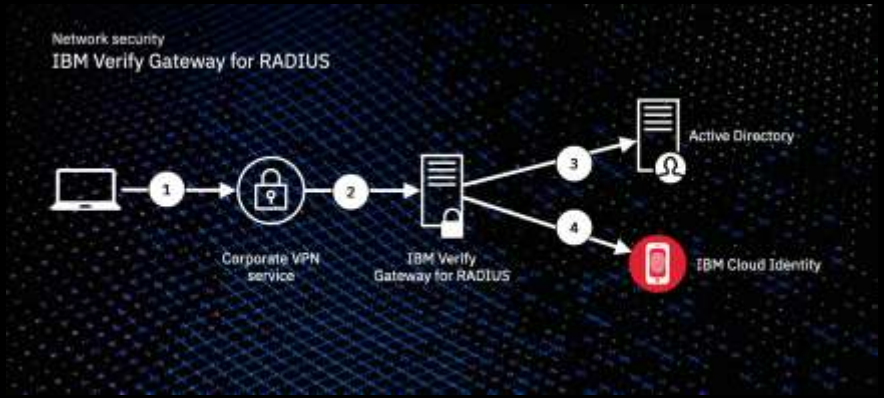
다중 인증으로 보안 강화

- 애플리케이션, VPN, Linux, Windows 및 메인 프레임에 대한 다중 인증
- FIDO U2F / FIDO 2 지원
- Passwordless 인증: QR 코드, 모바일 푸시, 혹은 디바이스 상의 생체 인증
- 쉽고 즉시 적용할 수 있는 정책:
  - 모든 세션
  - 모든 데스크톱 접근에 대해
  - 새로운 디바이스에 대해
- 위험 기반 조건부 접근을 위해 트리거 되는 항목
  - IP 주소
  - 지역적 위치
  - 사용자 / 그룹 속성
  - 위험 기반 분석
  - UEM 등록과 준수

원격 근무 보호

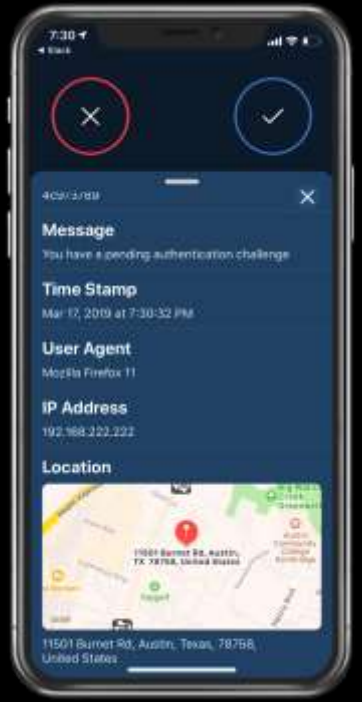
IBM Verify로 VPN을 통해 연결하는 사용자를 위해 MFA를 쉽게 시행하십시오.

RADIUS 용 IBM Verify Gateway와 상호 작용하면 사용자 인증 중에 단일 단계가 추가됩니다.



검증의 단순함을 추가하십시오.

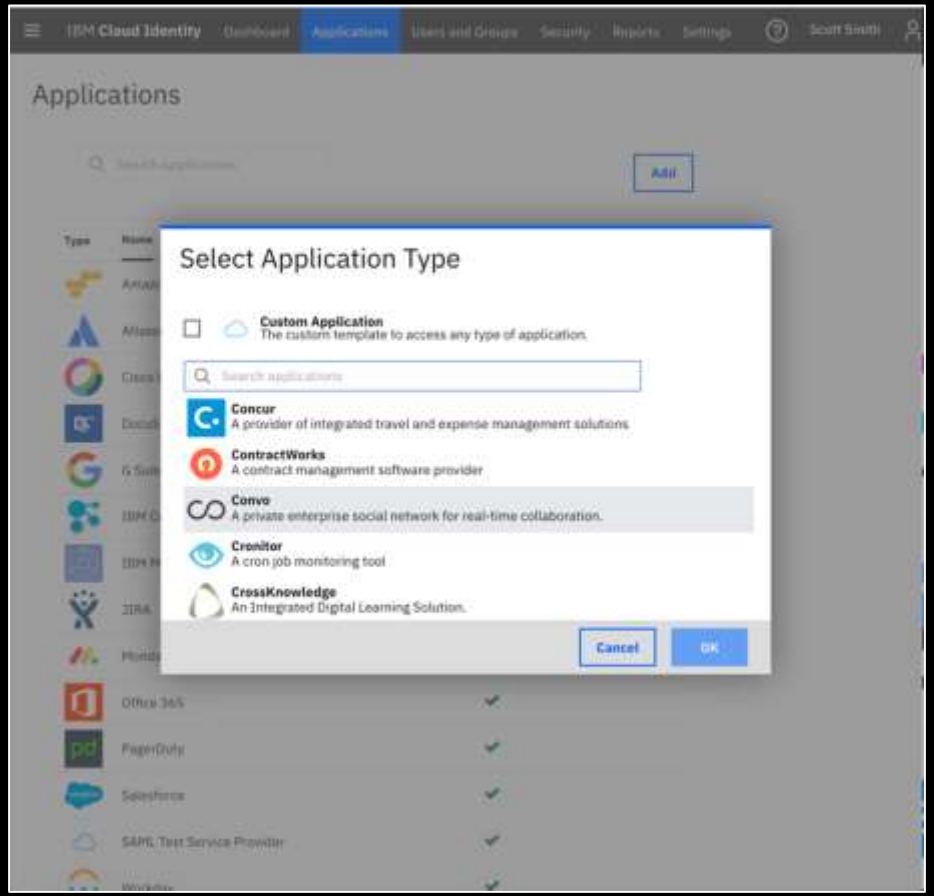
1. 사용자는 모바일 장치 또는 랩톱을 사용하여 VPN에 연결
2. VPN이 RADIUS 게이트웨이에 연결
3. 사용자는 비밀번호로 인증
4. 쉬운 두 번째 단계로 IBM Verify로 MFA 수행



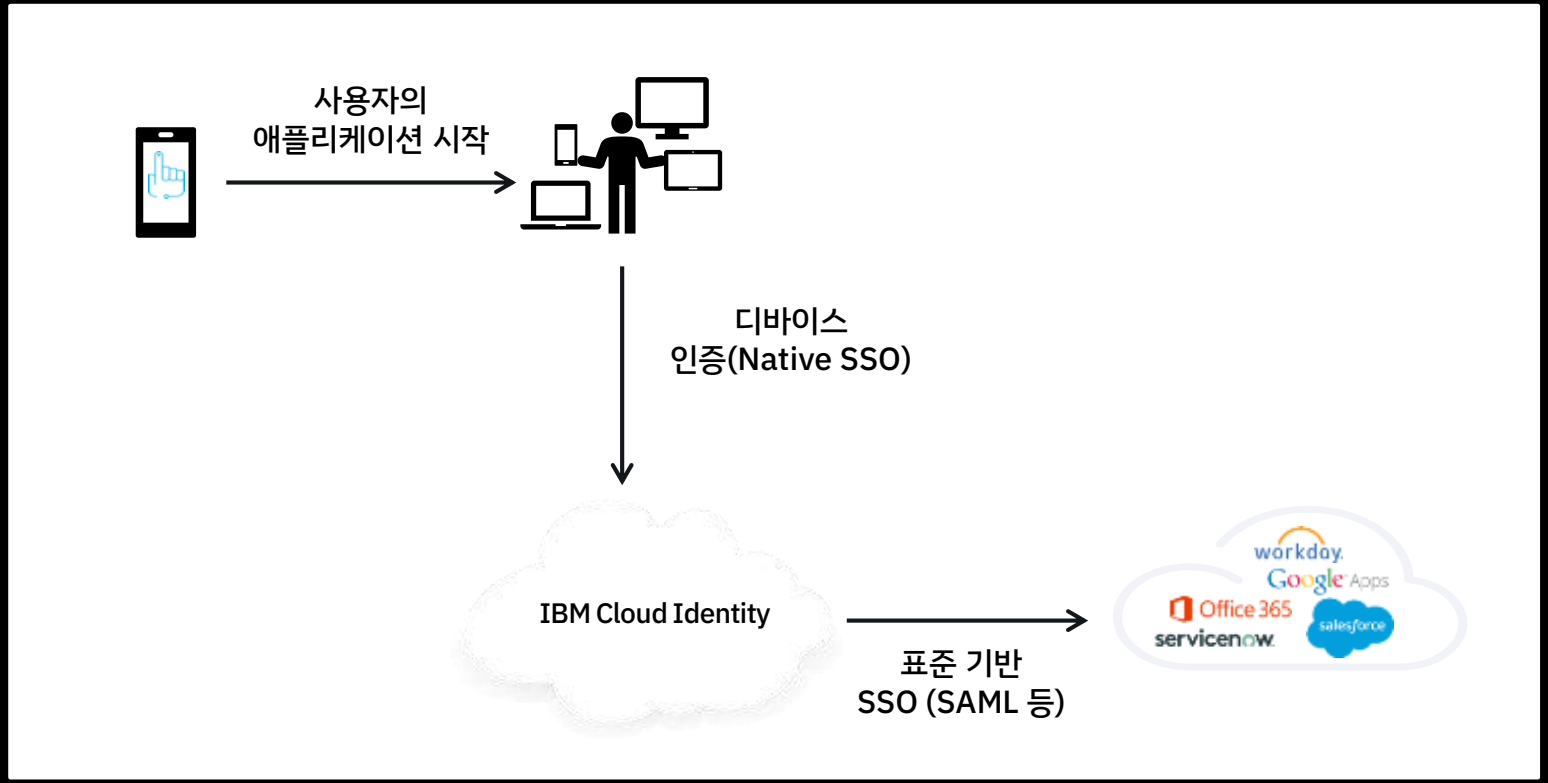
몇 주가 아닌 몇 분 만에 새로운 앱 탑재

- 몇 분 내에 SaaS 앱 설정
- 간편하고 빠른 커넥터
- 단계별 가이드
- 향상된 속성
- 산업 표준 기반 커스텀 애플리케이션 연계:

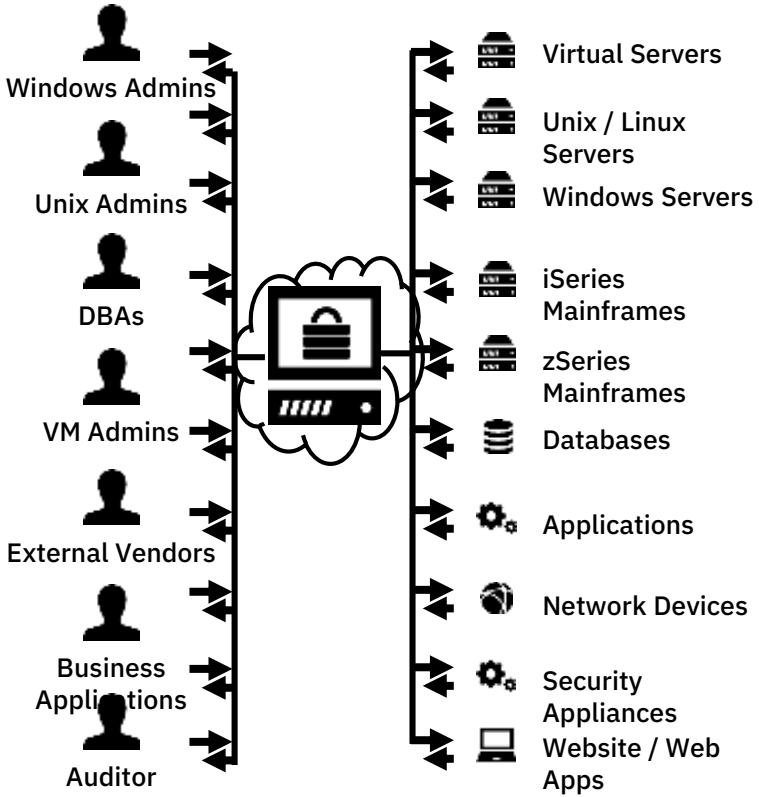
  OAuth2, OIDC과 SAML2.0
- 원클릭 활성화와 기존 IAM 인프라와 연동



사용자 간 장치에서 애플리케이션에 이르기까지 통합 환경 제공



특권 시스템 보호



원격 직원 및 타사 공급 업체에서

- 전체 자격 증명 관리를 위한 **단일** 온 프레미스 구성 요소만 필요
- 권한있는 계정 위험 **자동 식별**
- 의심스러운 행동에 대한 **지속적인 모니터링** 및 권한 있는 계정의 안전한 저장
- 악의적인 권한 있는 계정 활동에 대한 **실시간 탐지**, 경고 및 대응
- 애플리케이션 제어를 통한 **최소 권한 강제화**

원격 근무 보호 및 활성화

- 모바일 장치 및 데이터 보호
- 사용자 및 장치 보호
- 보다 안전한 확장 환경
- 내부자 위협 방지
- 악의적인 결과를 방지하기 위한 접근 조정

MaaS360 with Watson

- AI를 사용하여 모바일 및 IoT 장치에서 보안을 단순화하고 관리하는 개방형 클라우드 기반 플랫폼

90일 무료 사용

- 정책 및 애플리케이션 개선을 식별하는 통찰력을 얻음. 새로운 취약점을 사전에 해결

Cloud Identity

- 웹, 모바일 및 클라우드 환경에서 사용자 접근 간소화
- AI 기반 적응형 접근을 사용하여 사용자 위험 수준을 지속적 평가

90일 무료 사용

- 다단계 위험 기반 인증 및 자격 증명 연동을 통한 클라우드 제공 싱글사인온
- 사전 구축 된 수천 개의 앱 커넥터 및 템플릿

Secret Server

- 비밀번호 보관, 감사 및 권한 있는 접근 제어를 통해 권한 있는 계정을 보호하여 공격 영역 최소화

30일 무료 사용

- 매우 빠른 설정 및 구성 경험.

Trusteer

- 발급 및 BYO 장치의 위험 탐지 및 사용자 행동 분석에 대한 규칙 및 AI 접근 방식

빠른 배치 옵션

- SMB를 위한 가격 -> Enterprise
- 최소 12 달
- SIEM으로 데이터 전송

사용자와 디바이스의 보안이
유지되면 다음은 무엇입니까?

원격 근무는 인프라 및 엔드 포인트 보안에 새로운 과제 제기

- 기존 원격 접근 역량 확장
- 원격 접근을 해결하기 위한 인프라 및 엔드포인트 솔루션
- 기본 협업 앱에서 중요한 비즈니스 앱에 이르기까지 조직 전체에 다양한 수준의 접근 요구 존재
- 데이터 손실 방지 프로그램이 마련되어 있는지 확인
- 중요한 비즈니스 애플리케이션을 지원하기 위해 제한된 현장 기술과 전문지식

빠르게 성장하는 원격 근무 보호

고려해야 할 여러 가지 요소

- 최종 사용자에게 적절한 도구, 프로세스 및 교육 제공
- 요구가 단기적이라 생각되더라도 장기 전략 수립
- 네트워크 서지와 같은 중단 계획
- 회사 보안 및 규정 준수 표준 준수
- 올바른 사람과 애플리케이션이 회사 네트워크 및 데이터에 접근하고 있는지 확인
- 위험을 이해하고 미리 완화

기업 IT 비즈니스 시스템 및 직원에 대한 원격 접근 보안을 위한 모범 사례

안전한 컴퓨터 / 안전한 디바이스

IT 보안 기반 홈

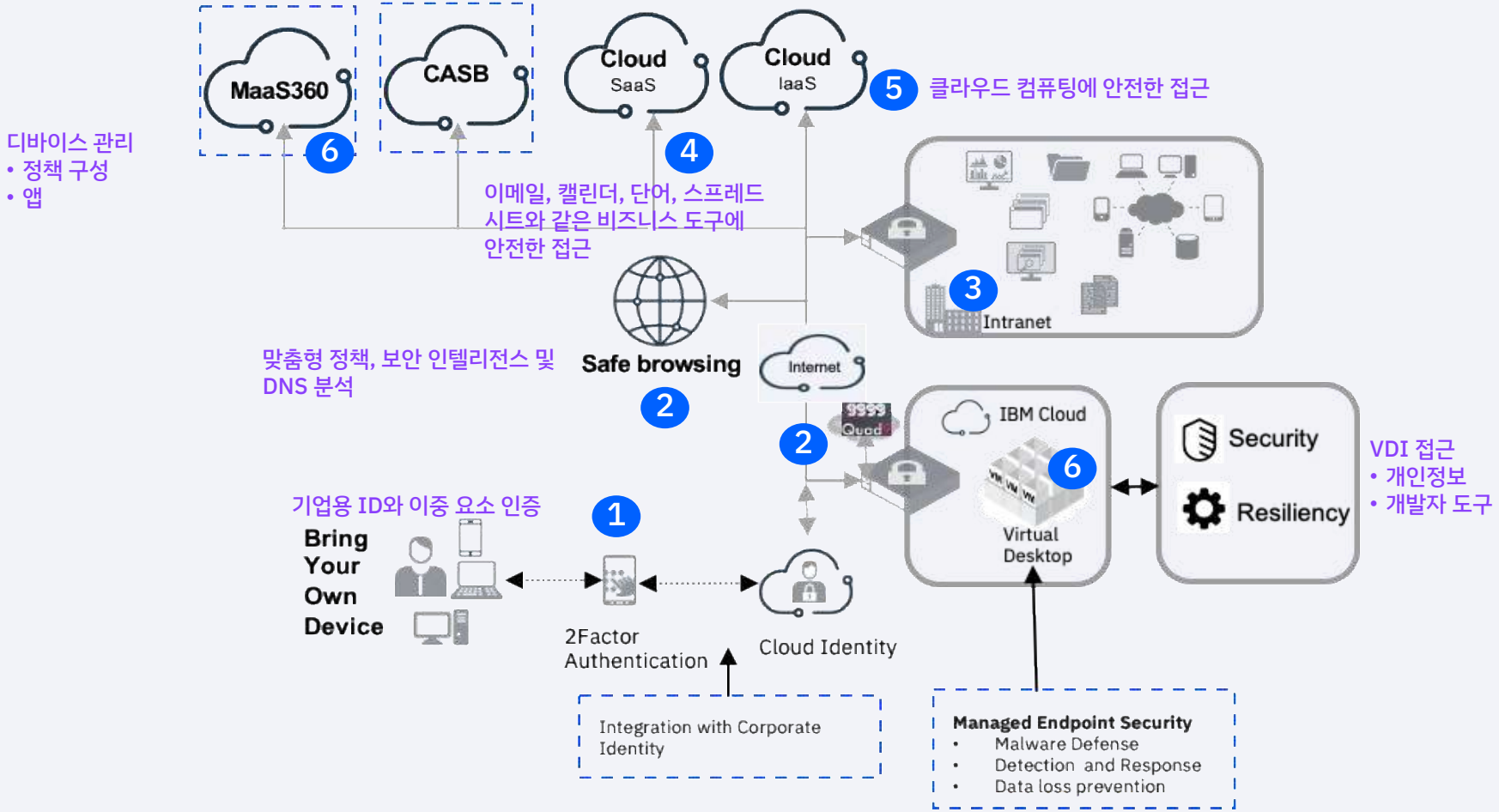
공공 인터넷 접근

공공 클라우드 환경 혹은 스토리지 디바이스의 사용

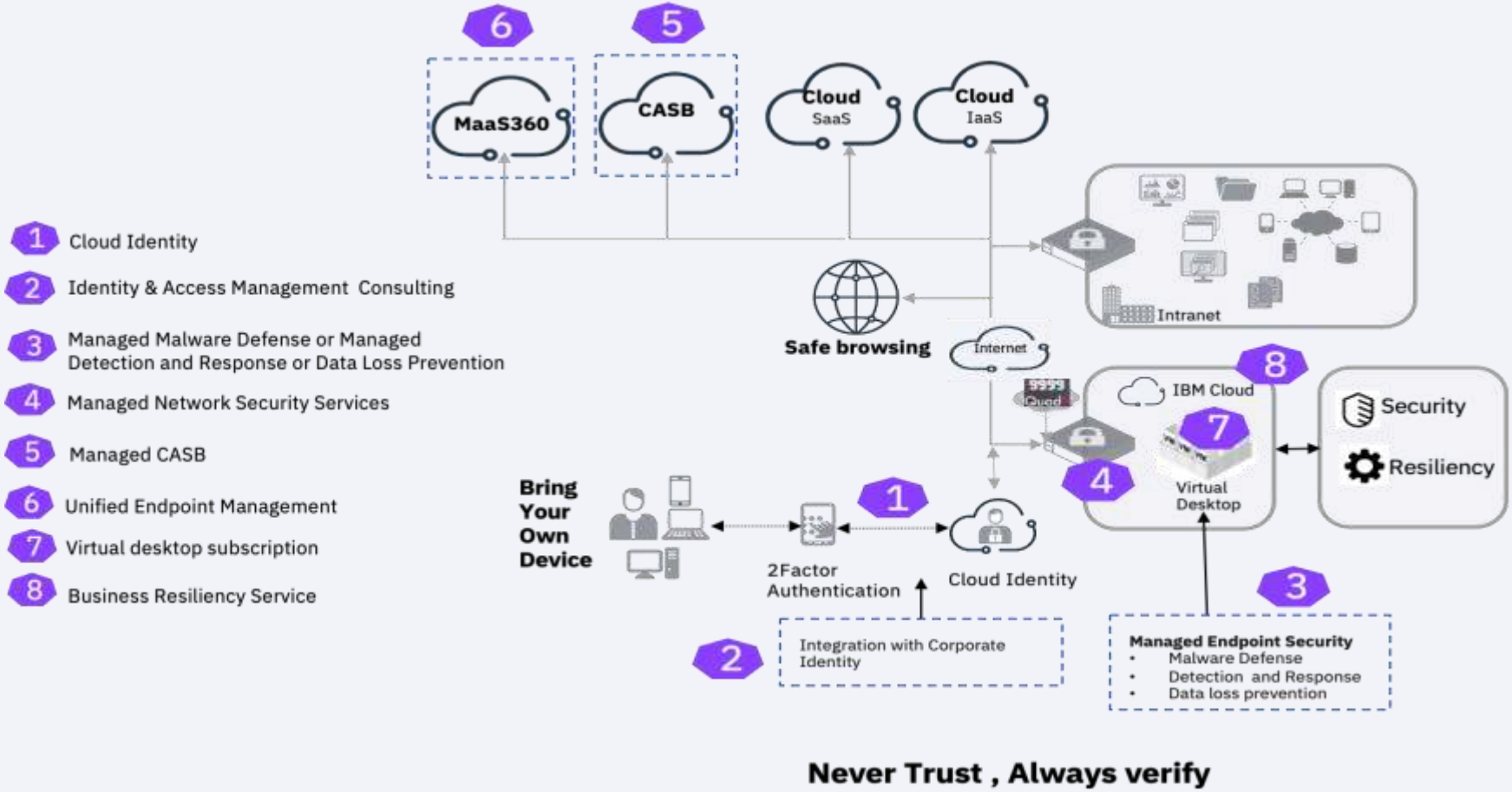
피싱 공격

안전하게 암호화된 통신

원격 근무는 대부분의 회사와 직원의 문화 변화

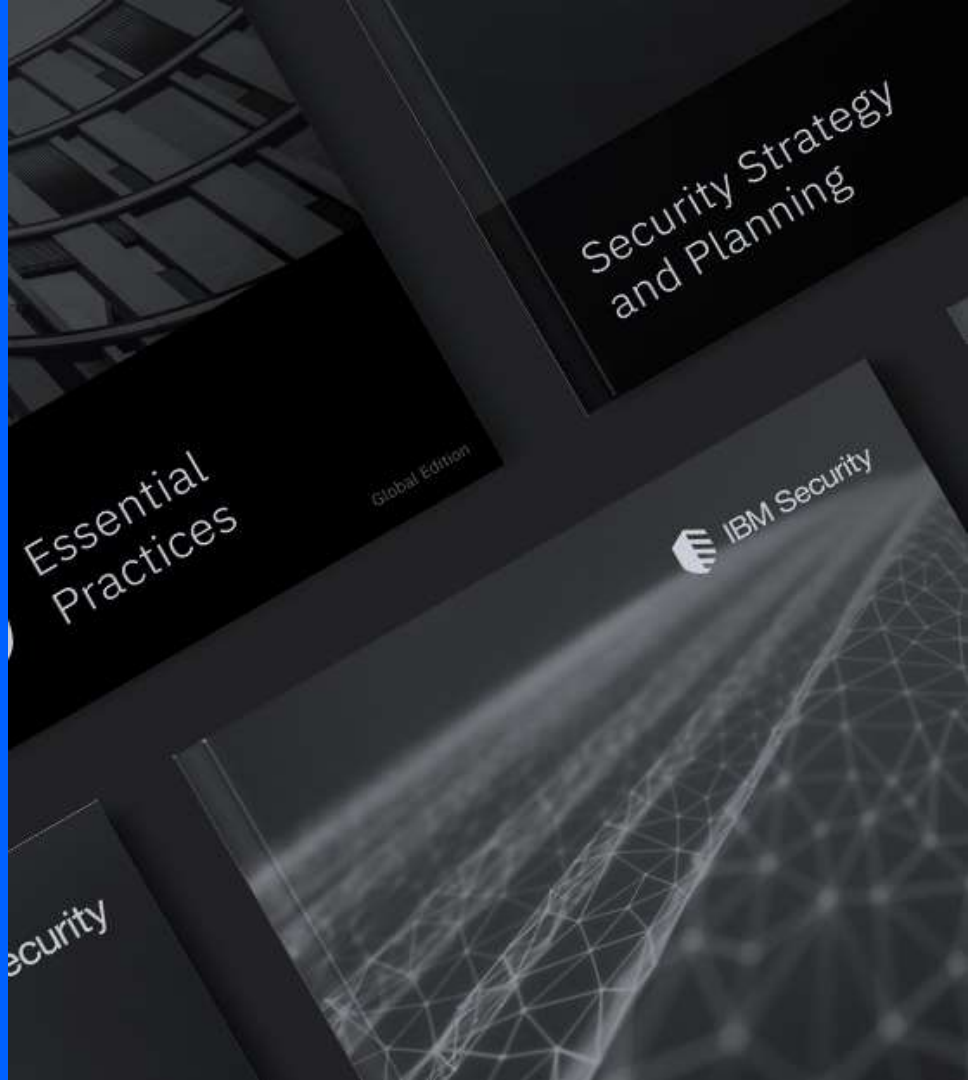


원격 근무는 대부분의 회사와 직원의 문화 변화



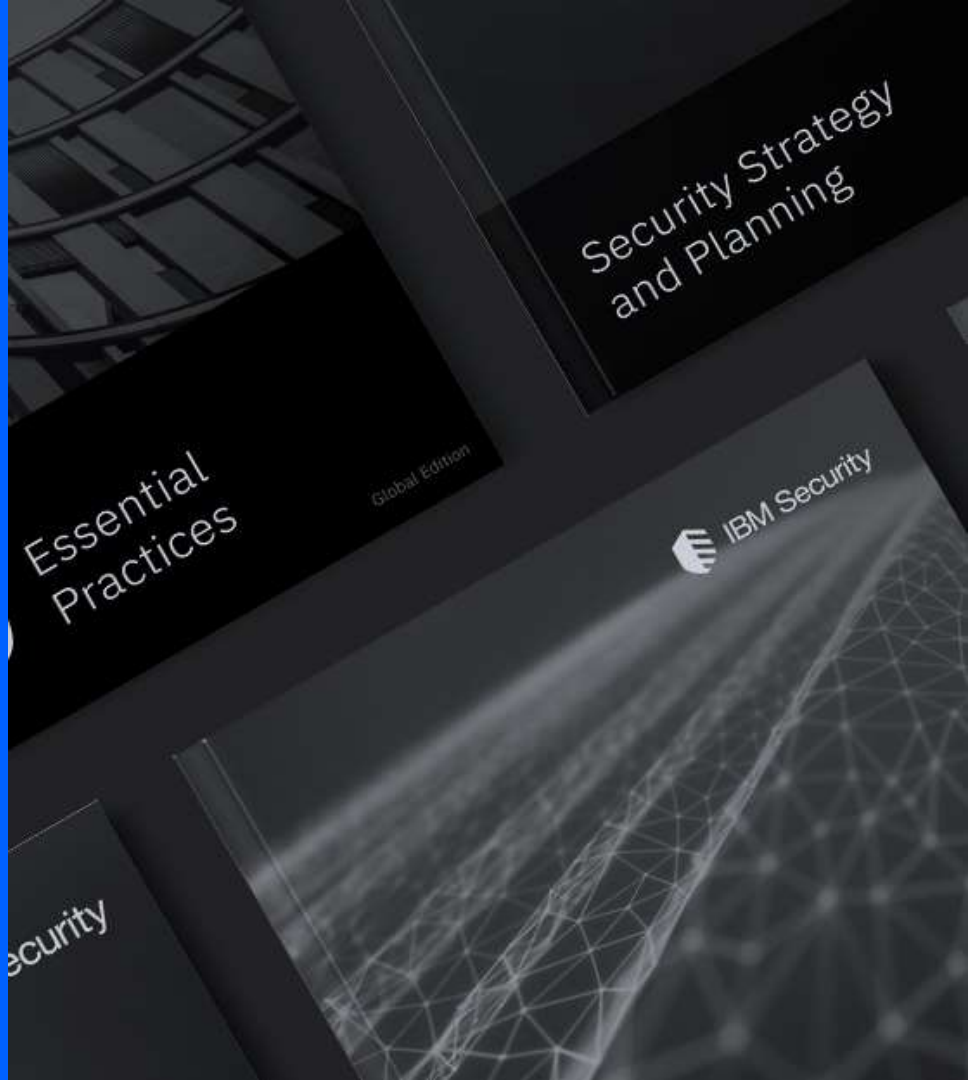
확장 환경을 보호하기 위해 인프라 및 엔드 포인트 전문지식 추가

- 선제적 및 상황 중심적 보호
- 멀티 벤더 지원
- 보안 수준에 대한 실시간 보기
- 보안 사고에 대한 해결
- 비즈니스 지속성을 보장하는 서비스 수준
- 포괄적인 감사 보고서



원격 근무를 위한 신뢰할 수 있는 파트너를 추가할 경우의 이점

- 24 시간 연중 무휴 탐지 및 지능형 위협 대응
- 기업과 함께 발전하는 확장 가능한 보안 전략
- 위협 인텔리전스, 사고 대응 및 위협 사냥
- 광범위한 업계 전문 지식 및 현지화 된 지원
- AI 기반 플랫폼 및 가상 SOC
- 하이브리드 멀티 클라우드에서 전문지식을 갖춘 클라우드에 대한 준비



감사합니다

Follow us on:

ibm.com/kr-ko/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

IBM Security

IBM