Use Case '누구에게 필요한가?

VMware Workspace ONE

이대근 차장
VMware EUC 팀

24th. Sep. 2020

Use Cases 누구에게 필요한가?

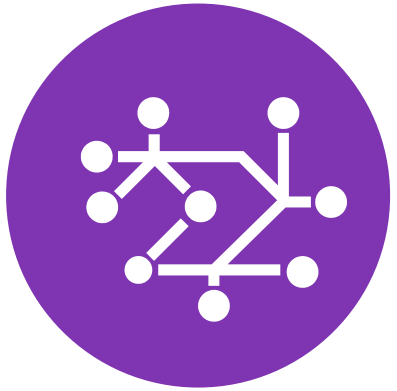
Workspace ONE 업무 방법 5가지

Per App VPN
가상 사설망

VDI
데스크톱
가상화

현대적인
관리방법
(모든 디바이스
통합 관리)

VMware
생산성 보안앱

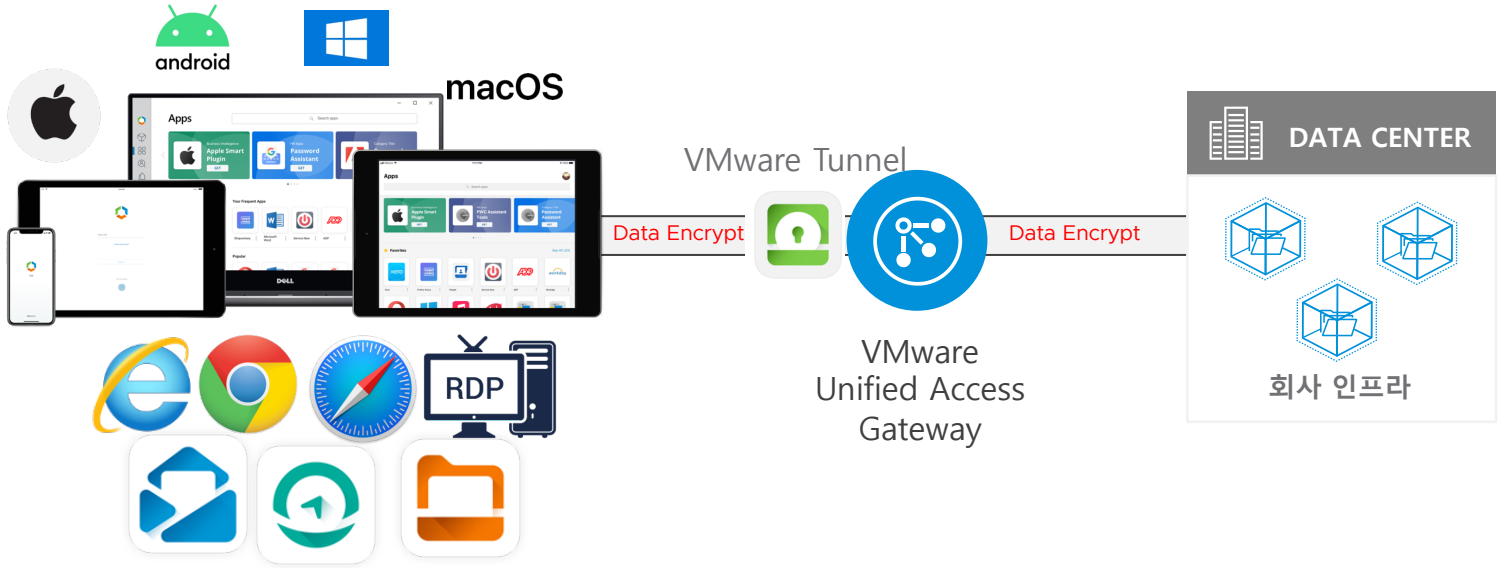


제로트러스트
관리방법

Per App VPN 가상 사설망

VMware Per App VPN(Tunnel)

제한된 Device와 App에서만 회사 DATA 접속하는 기능



Security

- ✓ 어플리케이션 중심 VPN으로 보안 관리가 가능
- ✓ 디바이스 상태에 따라 접속 제한

IT

- ✓ 조건별, 선택적으로 허용 가능
- ✓ 복잡한 조건도 관리가 편리함

Device, App, URL 기반으로 Per App vpn 가능

빠른 정책 및 설정으로 적용 가능
접속 요청과 동시에 연결

전송되는 Data 암호화

디바이스의 보안 정책 준수여부에 따라 접속 제한 가능

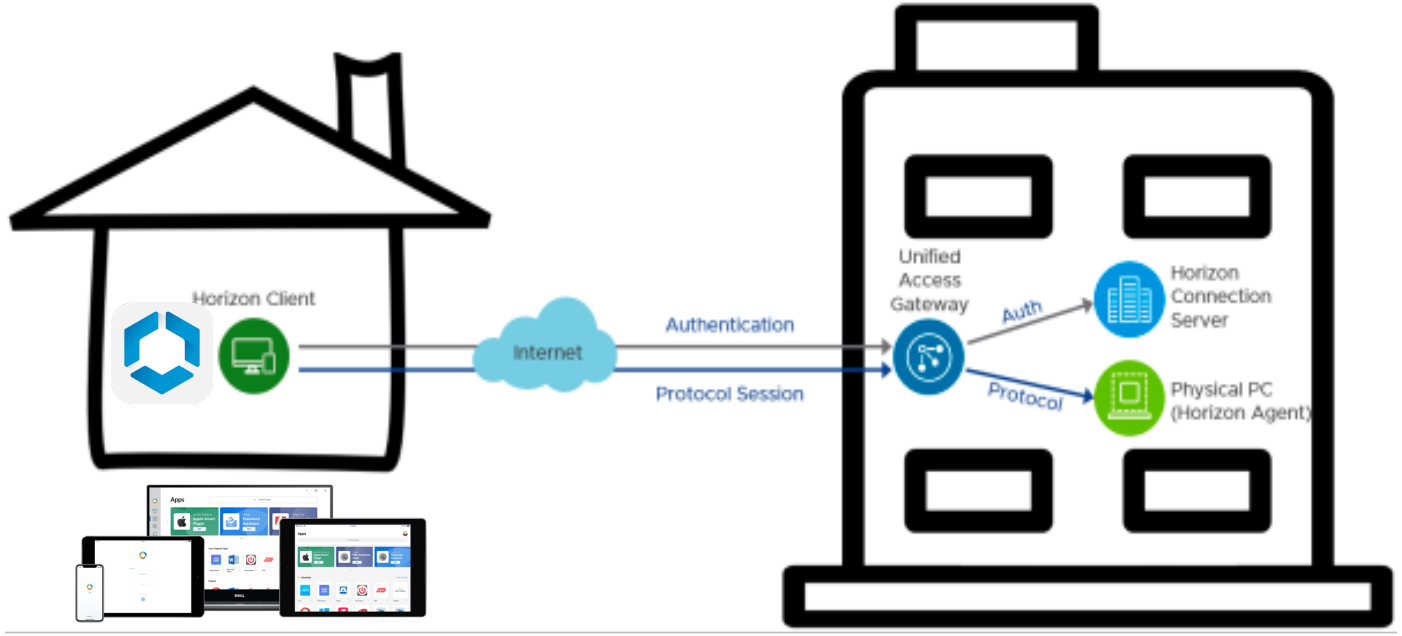
관리되는 디바이스에서만 가능함

VDI 데스크톱 가상화

VMware Horizon

VDI 데스크톱 가상화 (Physical VDI)

사무실 내에 물리PC의 VM화 (Physical VDI)



Security

- ✓ SSL VPN, 2차 인증을 통한 외부 접속 보안. Horizon Agent를 통한 단말 관리 및 통제.

IT

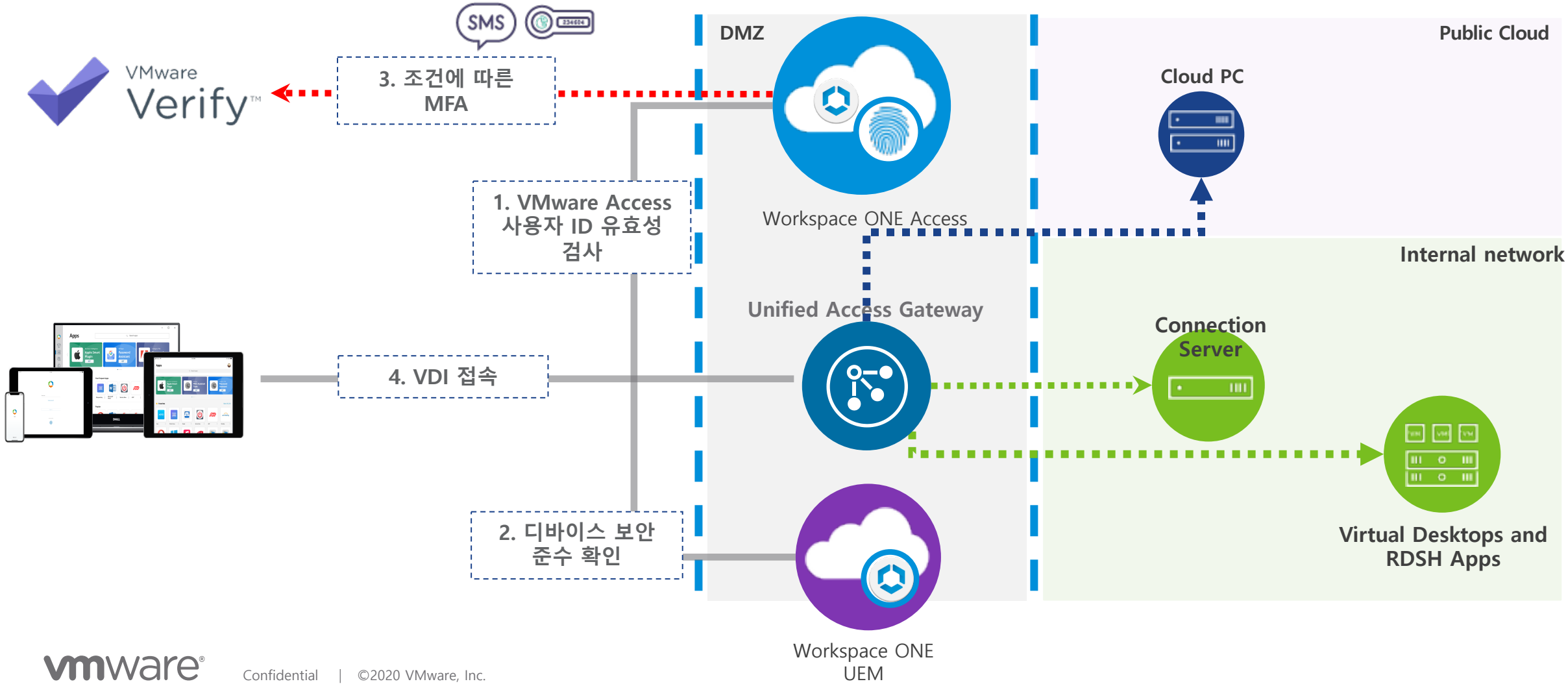
- ✓ 사무실 내에 위치한 물리 PC를 마치 VDI 와 같이 사용 가능.

VDI 데스크톱 가상화

- 업무의 연속성 유지
- 신속한 직원 환경 제공
- 엔드포인트 디바이스 분실 시 회사 데이터 손실 없음
- 취약성에 대한 중앙 집중식 패치
- **Endpoint Device 관리 부재** 업무 행위에 비해 많은 컴퓨트 자원이 필요

VDI 데스크톱 가상화 – 계속

집에서 업무 VDI 접속과 접근 제어, 디바이스 관리

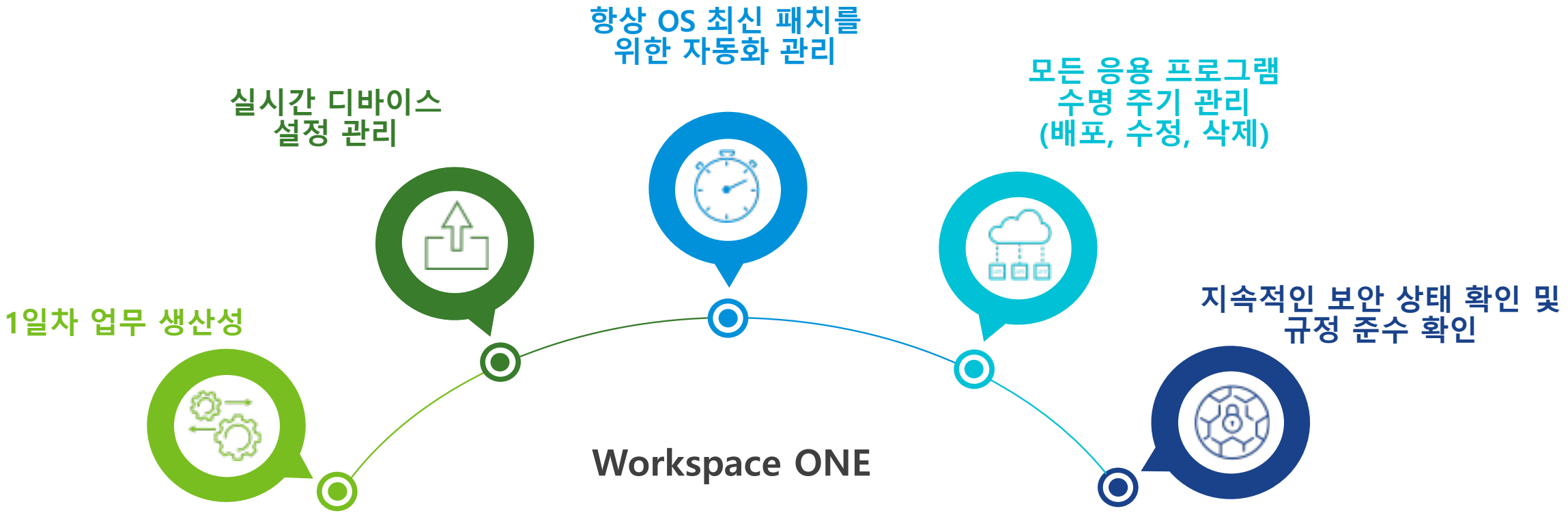


현대적인 관리방법

Windows10, macOS, Android, iOS

현대적인 관리방법이란?

클라우드 환경, 모바일에서 Win10, macOS, VDI까지



Windows 10 현대적인관리

온보딩부터 보안까지 한 번에 관리 가능

현대적인 관리방법

온보딩	설정	OS 업데이트	소프트웨어	보안
출근과 동시에 업무시작	MDM 구성	항상 최신 OS 업데이트	회사 앱 스토어 및 SSO	디바이스 상태 증명
OOBE 배포 방식	표준 Baselines & GPO 정책	세분화된 컨트롤	Win32 앱 관리	Data 보호
팩토리 프로비저닝	BIOS / 펌웨어 관리	배포 최적화 기능	P2P 배포 기능	센서 및 보안 준수
PCLM과 함께 관리 가능	자산 추적 기능	패치 분석 및 자동화	앱 인벤토리	BitLocker 관리 기능

Intelligence | **Automation**

macOS 현대적인관리

현대적인 관리방법

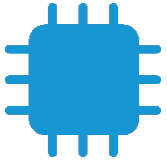
디바이스 / OS 관리

배포

- 장치 등록 프로그램
- Bootstrap Packages
- 이미지 없이 프로비저닝

설정

- APNs & AWCM
- 보안 정책 및 설정 즉시 배포
- 자산 추적 및 인벤토리



패치

- OS 업데이트 push (배포)
- 회사 SUS 구성

APP 관리

배포

- 어플리케이션 라이프 사이클 메니지먼트
- Native, Web, Virtual Apps
- 셀프 서비스 포탈과 SSO

디바이스 보안

보안

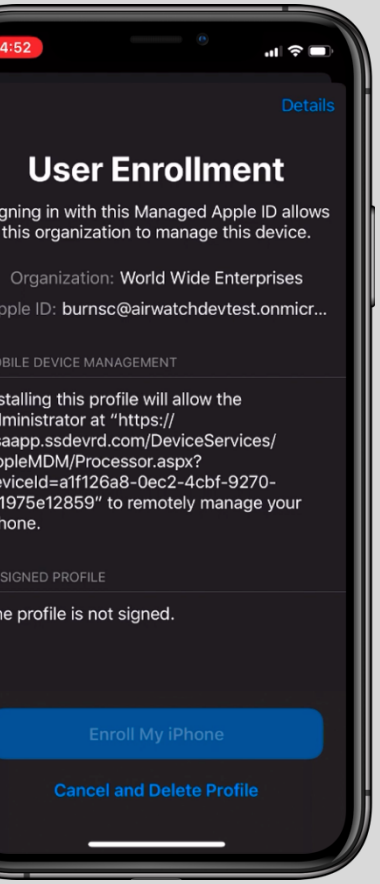
- Device 상태확인 & 보안 준수
- 패스워드, 인증서 주기 관리
- FileVault Encryption

macOS

새로운 모바일 디바이스 관리 방법

iOS User Enrollment/ Google Android Enterprise

현대적인 관리방법

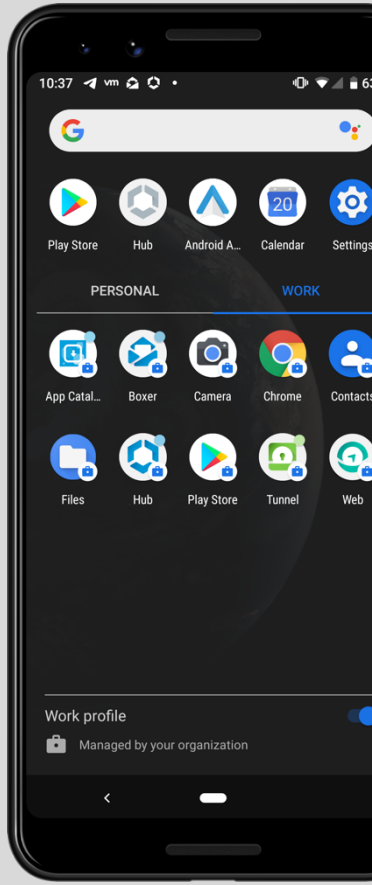


iOS User Enrollment

- iOS 13/iPadOS13 새로운 디바이스 등록 방법을 제공
- 개인 Apple ID가 아닌 기업에서 발급한 Apple ID를 통해 관리
- 메일, 연락처, 캘린더, 파일 및 키 체인에 대한 데이터를 분리.
- 모든 작업 데이터를 초기화하는 엔터프라이즈 기능 제공
- 관리자는 MDM 등록에 비해 디바이스 제어가 제한됨 (프라이버시 침해 방지를 위해)

Android Enterprise Work Profile

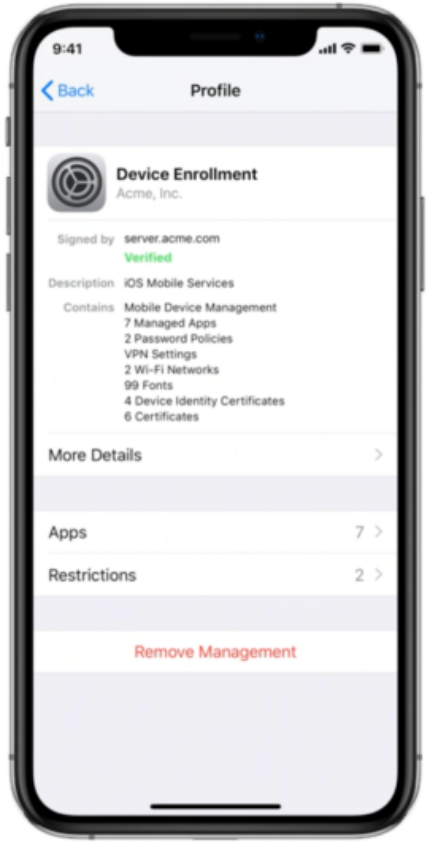
- 장치에서 회사 및 개인 데이터를 분리
- 모든 작업 데이터를 초기화하는 엔터프라이즈 기능
- 관리자는 MDM 등록에 비해 컨트롤이 제한되어 있습니다.



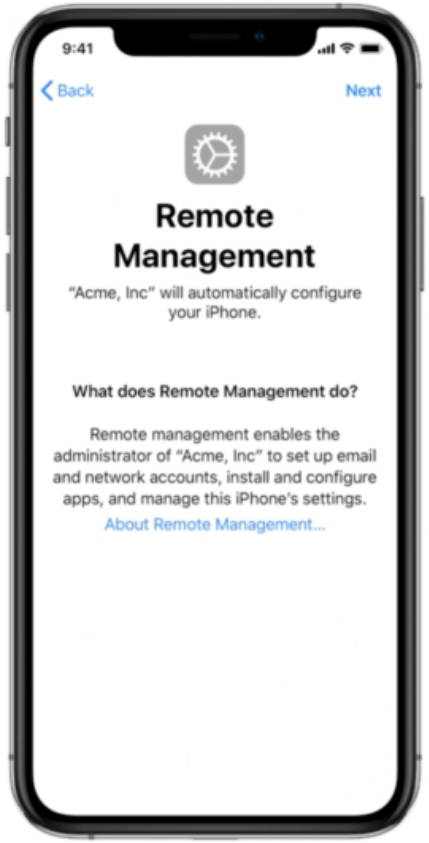
새로운 모바일 디바이스 관리 방법

iOS User Enrollment

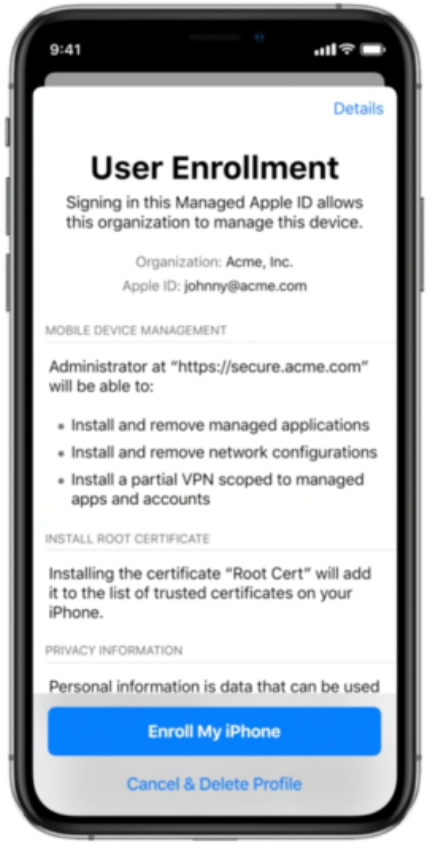
현대적인 관리방법



기존 MDM 방식
(개인 소유 단말)



Supervised MODE
(회사 소유)



User Enrolment 방식
(개인 소유 단말)

개인 Apple ID가 아닌 기업에서 발급한 Apple ID를 통해 관리

메일, 연락처, 캘린더, 파일 및 키 체인에 대한 데이터를 분리.

모든 작업 데이터를 초기화하는 엔터프라이즈 기능 제공

관리자는 MDM 등록에 비해 디바이스 제어가 제한됨 (프라이버시 침해 방지를 위해)

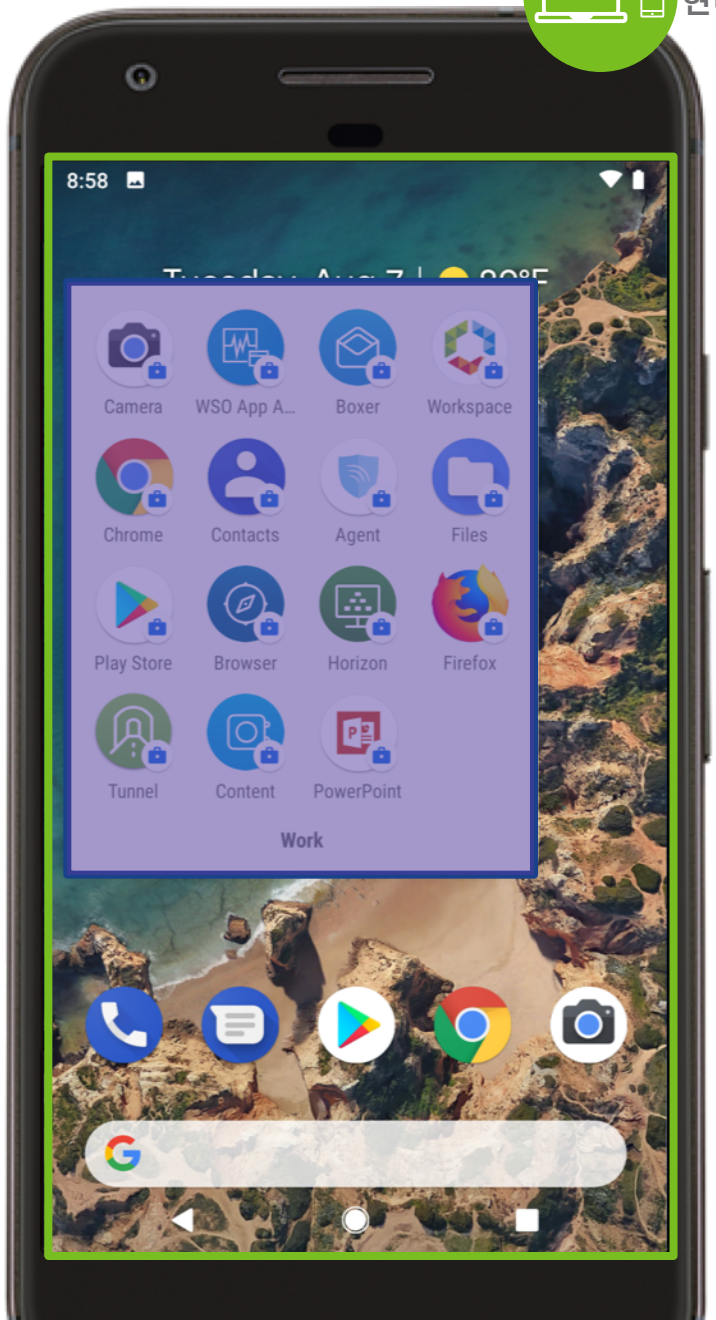
새로운 모바일 디바이스 관리 방법

Android Enterprise, 영역별 분리 관리 기능

현대적인 관리방법

Work관리 장치
(Work managed)
Google Play – 개인용
단말 정책 - 개인용

업무 프로필
(Work profile)
Google Play - 회사 업무용 app
보안 정책 - 회사 업무 프로파일



- **Android의 새로운 UI로 사용자 환경 개선**
  - 개인/ 업무로 나누어져 있으며 시각적으로 분리되어 있음
- **공유 방지**
  - 업무 앱 및 개인 앱과 데이터 간 공유 차단
- **사용자는 다음에 대한 별도의 구성 가능:**
  - 자격증명, 계정, 앱, 보안
  - MDM 정책도 분리되어 배포 적용

VMware 생산성 보안앱

직원의 생산성을 향상 시킬 수 있는 VMware 보안앱

VMware 생산성 보안앱

Workspace ONE - VMware보안 생산성 Apps

Hub

- 통합 온보딩
- SSO가 있는 앱 카탈로그
- 알림 및 작업
- 사람 검색

Boxer

- 메일, 캘린더 및 주소록
- 모바일 플로우
- 통합 파일 액세스
- Exchange, Lotus 및 GSuite

Web

- 원활한 인트라넷 액세스
- 통합 인증
- 보안 네트워크 터널
- 특수 키오스크 모드

Content

- 회사 리포지토리 접속
- 관리되는 콘텐츠 게시
- PDF 파일에 주석 달기
- Office 파일 편집

Smartfolio

- 관리되는 콘텐츠 게시
- 빠른 액세스 UI
- 비즈니스 라인 워크 플로우

Notebook

- Outlook Notes
- Outlook 작업
- 신고 된 이메일
- 통합 워크 플로

Send

- M365 앱에서 파일 편집 허용
- Intune SDK 활성화
- VMware Boxer를 통해 파일 전송 기능
- 강력한 Intune DLP 적용

Cards

- 명함 스케너
- 명함을 연락처로 변환
- Exchange서버와 동기화
- VMware Boxer 또는 native 메일 등에 구성 가능

Verify

- 멀티 팩터 인증 클라이언트
- 푸시 승인
- 시간 기반 OTP
- SMS 기반 인증

PIV-D

- Derived 자격증명
- 모든 주요 CA를 지원
- SMIME: 암호화/Signing
- Authentication Certificates

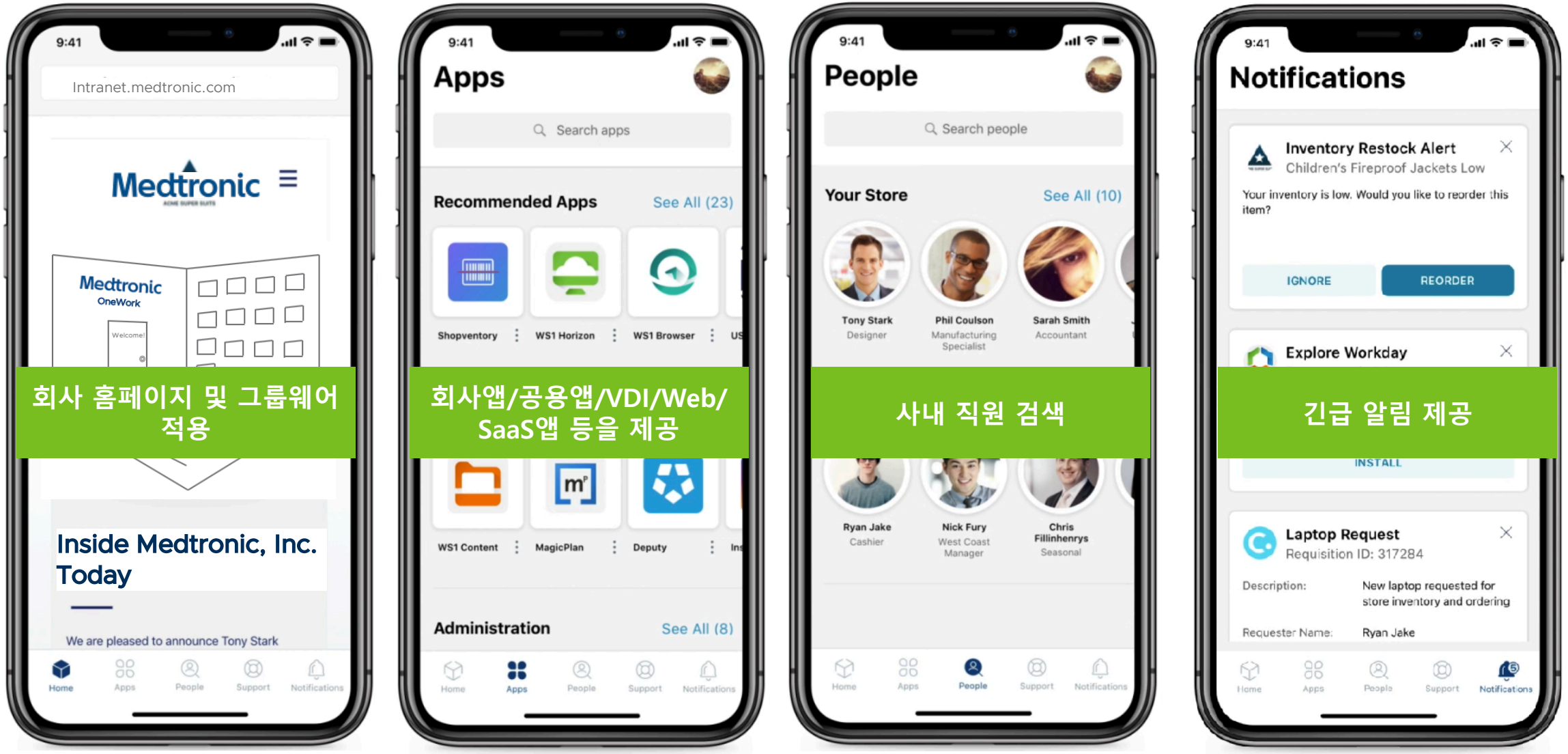
Tunnel

- 보안 네트워크 터널
- 앱당 VPN(MDM)
- 네이티브 앱 및 브라우저
- 원활한 사용자 경험 제공

Workspace ONE Intelligent Hub (Hub Service)

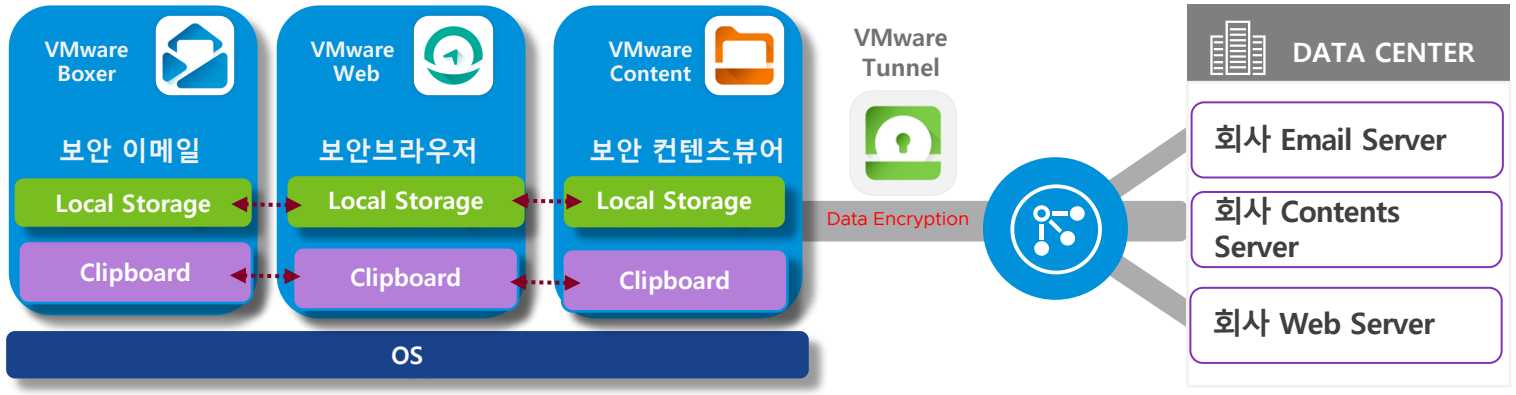
Hub를 통해 직원의 사용성을 높여 업무의 효율성을 증대

VMware 생산성 보안앱



VMware 보안 Apps을 통한 안전한 접근

회사 DATA를 보호하며, 사용자에게는 편리하게 제공



IT 정책에 따른 데이터 보호/관리

- 어플리케이션에서 만들어지는 데이터는 안전하게 저장되며, 앱 간 상호작용을 막아 데이터 유출 차단

Security

- ✓ UAG를 통해서 구간 암호화 및 traffic에 관리가 가능
- ✓ 회사 데이터에 대한 관리를 통해 보안을 높일 수 있음

IT

- ✓ IT관리자는 앱에 대한 추가 개발없이 서비스 제공 가능

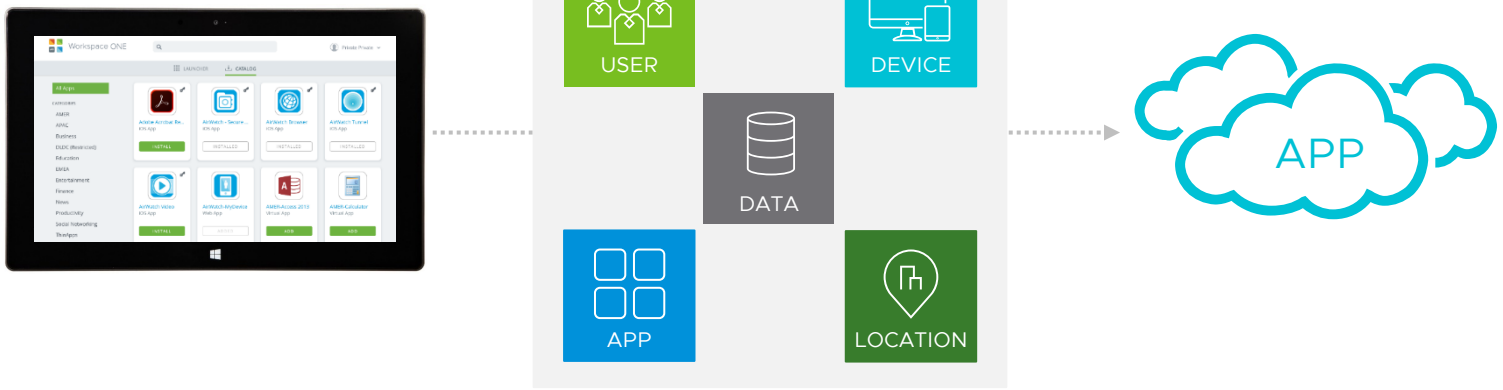
VMware 생산성 보안앱

- 익숙한 사용자 경험 제공
- 업무에 활용에 편리하여 생산성 증가
- 저장되는 Data, 전송되는 Data 암호화
- 디바이스의 보안 정책 준수여부에 따라 접속 제한 가능
- 관리되는 디바이스에서만 가능함

제로 트러스트 관리 방법

제로트러스트 보안 모델

강력한 사용자 상태 기반 정책 관리



Security

- ✓ 정책에 어긋나는 상태 변화 시 바로 어플리케이션 및 데이터 접근 차단
  > 사외 접속 시 특정 앱 차단
- ✓ 규정 위반 사고 식별 및 인지 시간 25% 단축

IT

- ✓ 기존 인증 관리 연계
- ✓ 수동 규정 준수 관리 불필요

Integrates identity and device compliance
계정과 단말의 상태를 조합하여 다양한 정책 생성 가능

Mobile application management for ANY app
기존 앱 수정/변경 없이 모든 모바일 어플리케이션 관리 가능

Access controls and DLP for comprehensive security
네트워크, 기기, 클라우드상의 앱 및 데이타 보호를 위한 접근 제어 및 DLP 정책 적용 가능

Automated remediation
리포트 제공뿐만 아니라 규정 위반 발생 시 알람 및 자동 조치

Built-in micro segmentation policies
VMware NSX와 연계하여 네트워크 보호 및 리소스 격리 가능

*Based on internal VMware deployment

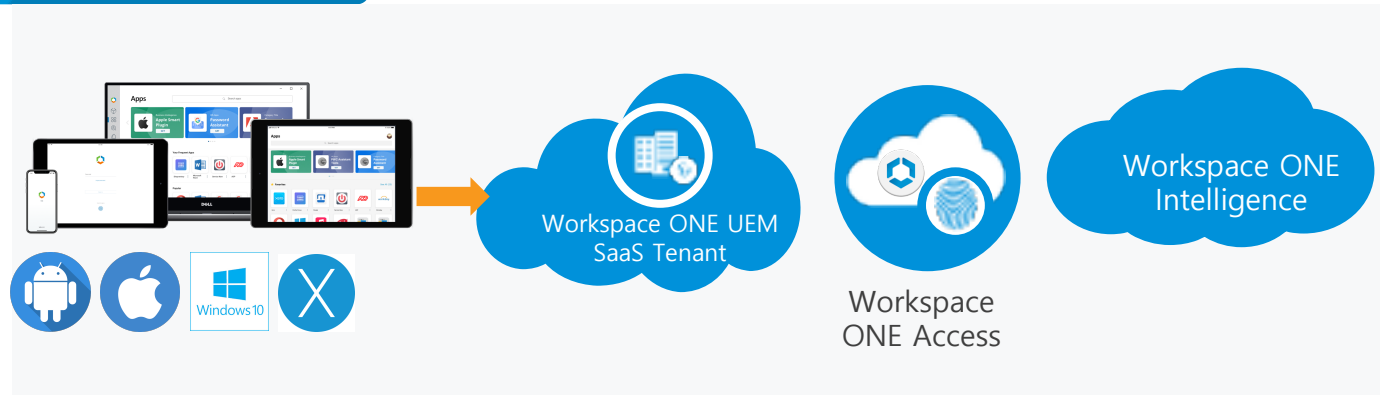
제로트러스트 SaaS서비스 접속 예시

SAAS 서비스/회사 서비스 접속 Control

Public Saas Service (Cloud)

- 조건 별 Access Control
- 사용자, 디바이스, 접근 네트워크 기반으로 접속 허용
- 허용된 사용자/디바이스가 아닐 경우 Saas서비스 접속 차단

Workspace ONE (Cloud)



Benefits

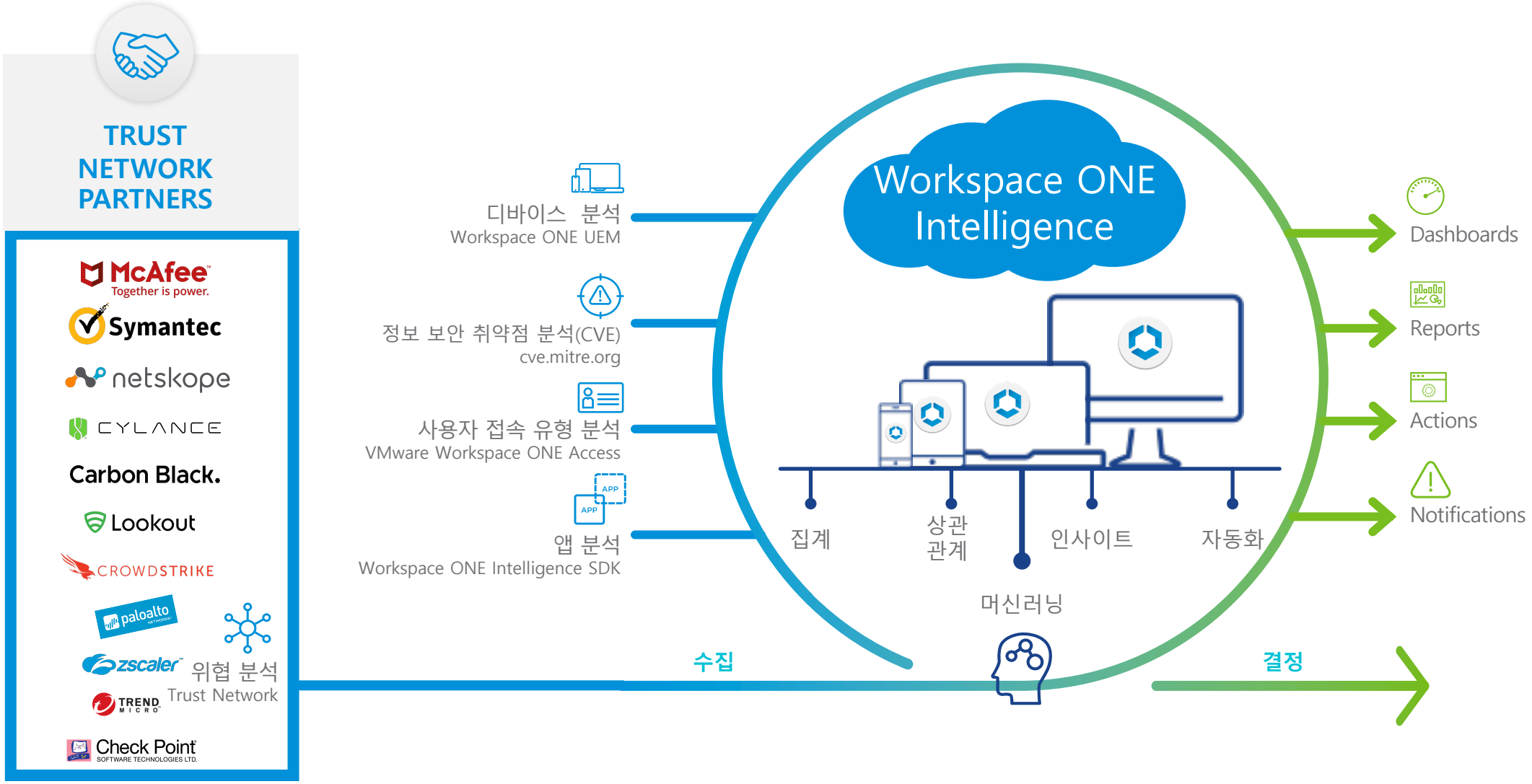
- 완벽한 스마트워크 구현 가능
- 회사 Device를 100%관리 가능 (Windows10, macOS 관리, 어플리케이션 관리 등)
- SaaS 서비스 접속 이력 관리 가능
- 개인 Device 사용 시 디바이스 등록 후 사용 가능(등록되지 않은 Device는 접속이 불가)

사례

- K사 (2020)
  - Saas 서비스 접속 관리 (Zero-Trust)
- N사 (2019)
  - 회사 Email 보안 접속 관리
- S사 (2018)
  - Windows10 현대적인 관리 방법 관리
- S사 (2016)
  - Android 디바이스 중앙 관리 통제

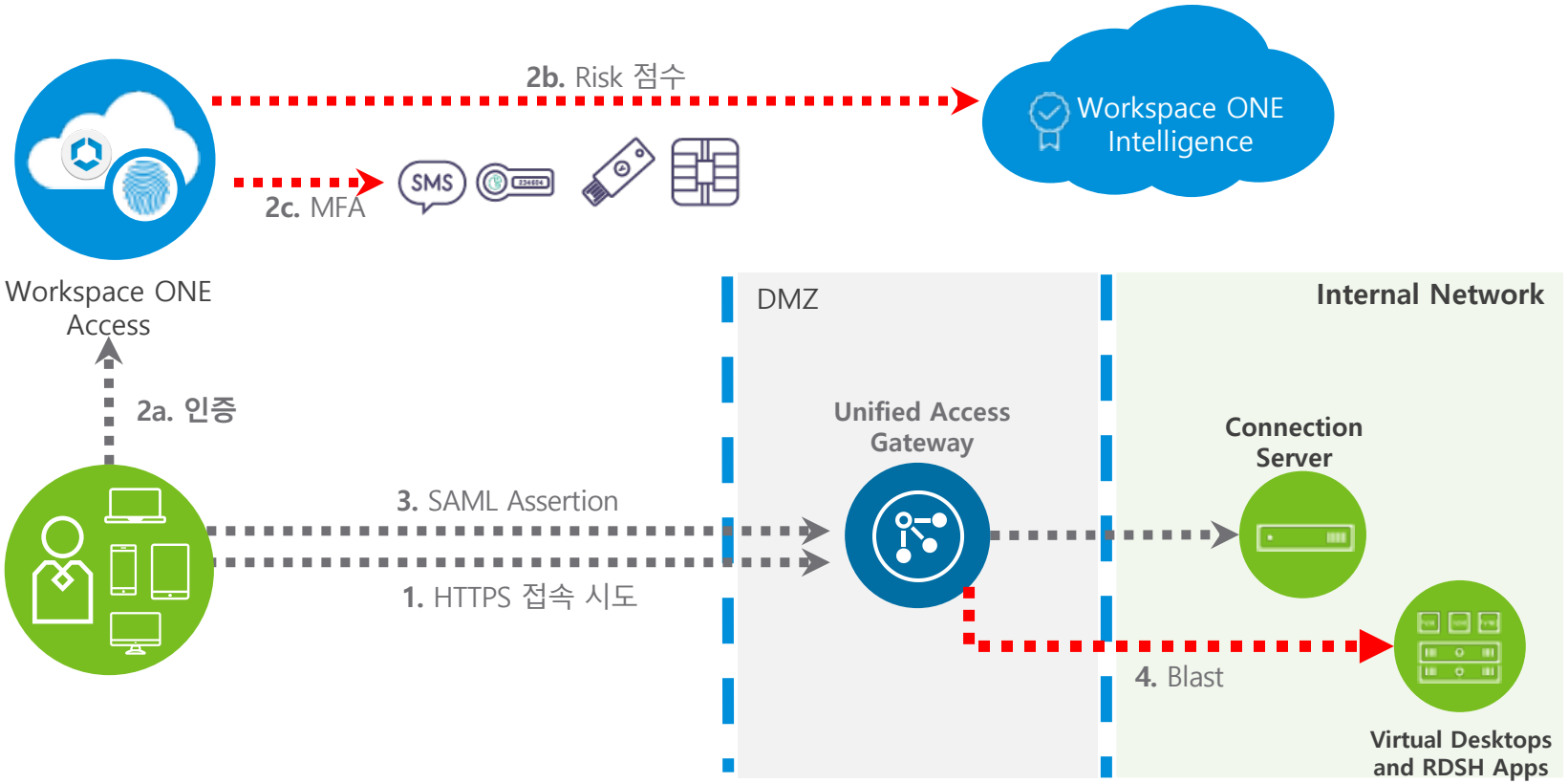
Workspace ONE Intelligence + Trust Network Partner

현대 디지털 작업 공간을 위한 통찰력과 자동화



Workspace ONE Intelligence 사용 사례

Workspace ONE Intelligence에서 위험 점수가 정규화



제로 트러스트 관리 방법

1. 사용자 VM 접속 시도

2a. Workspace One Access에서 사용자 인증

2b. Workspace ONE Intelligence에서 Risk 점수 확인 후 응답

2c. Risk 점수에 따른 MFA

3. 인증 후 접속 SAML 토큰으로 Access

원격근무! Workspace ONE으로 시작하십시오!

완벽한 디지털 워크스페이스 플랫폼

VMware

- VMC
- VCF
- NSX
- Velocloud
- Avi

Ecosystem

- Dell
- Identity (Okta)
- Workday
- Trust Network
- ...

CIO	CISO	LOB/HR	Employees
Visibility & Manageability	Security & Compliance	Engagement & Retention	Experience & Privacy

Thank You