Microsoft

Microsoft 365 Virtual Training Day: Windows 및 Surface 디바이스 관리

Microsoft

디바이스 등록

모듈 의제

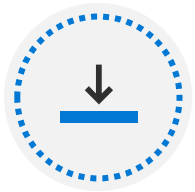
디바이스 인증 관리

Microsoft Endpoint Configuration Manager를 사용하는 디바이스 등록

Microsoft Intune를 사용하는 디바이스 등록

레슨 1: 디바이스 인증 관리

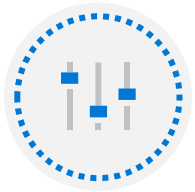
레슨 소개



Azure AD 조인

Azure AD 조인의 전제 조건, 제한 사항 및 이점

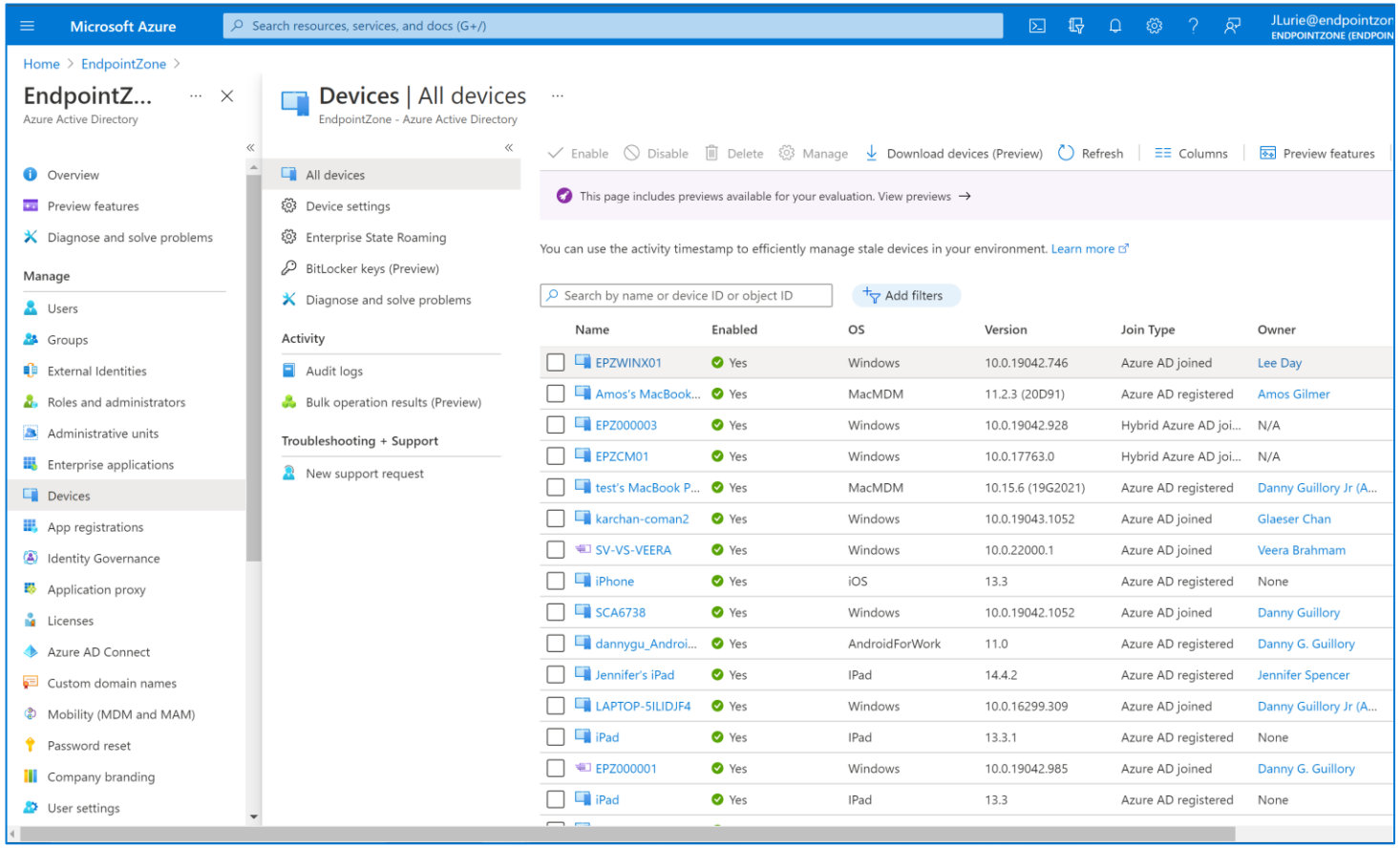
Azure AD에 디바이스 조인



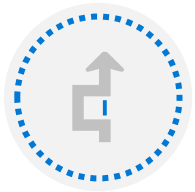
Azure AD에 조인된 디바이스 관리

Azure AD 조인 개요

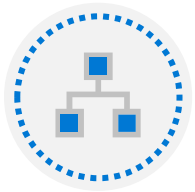
- Windows 10 에서 Azure AD에 조인 가능
- 일반적인 시나리오 :
  - 애플리케이션 및 리소스가 클라우드에 대부분 있음
  - 별도의 임시 계정
  - 사용자가 자신의 디바이스를 기업 환경에 조인할 수 있도록 허용
- 초기 설정 중 또는 그 이후에 디바이스에 조인
- 하이브리드 Azure AD 조인은 Azure AD를 통해 온-프레미스 도메인 조인 디바이스를 자동으로 등록



Azure AD 조인의 전제 조건, 차이점 및 이점



다중 테넌트는 AD DS로 구현하기가 매우 어렵습니다.



Azure AD는 핵심 인프라의 일부가 아닙니다.

Azure AD에는 AD DS와 다른 관리 기능이 있습니다.

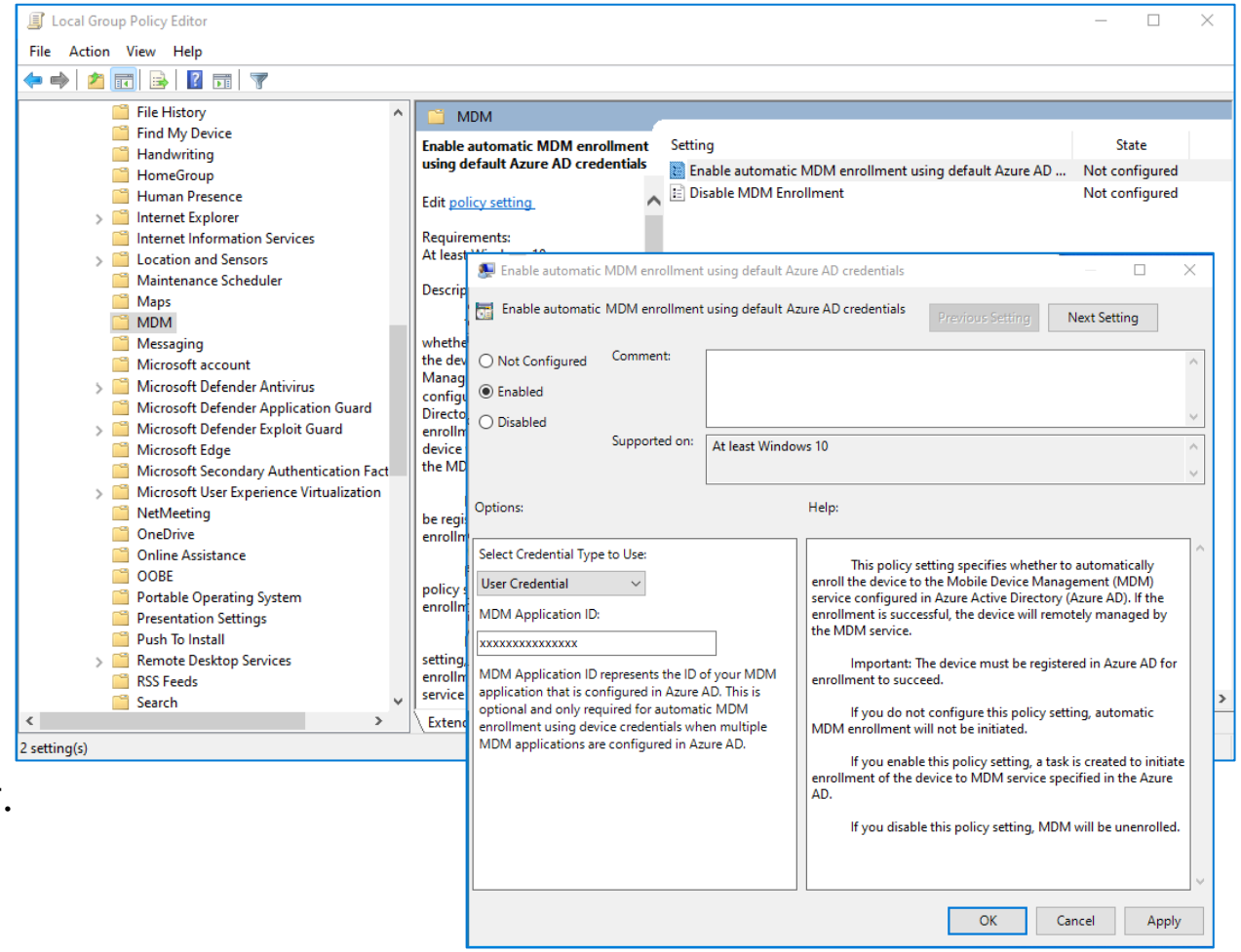
Azure AD는 다중 테넌트로 설계되었습니다.

Azure AD에 디바이스 조인

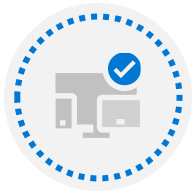
디바이스를 Azure AD에 조인하는 것은 간단한 절차입니다.

Windows 10 설치 중에 Azure AD에 조인하거나 설정 창, 스크립트 또는 여러 관리 도구를 사용하여 나중에 언제든지 조인할 수 있습니다.

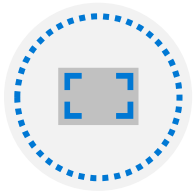
디바이스를 Azure AD에 조인하려면 Azure AD 개인 인증 정보가 필요합니다.



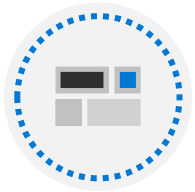
Azure AD에 조인된 디바이스 관리



그룹 정책은 온-프레미스 AD DS에 조인하는 디바이스를 관리합니다.



Azure AD에 조인하는 디바이스에 대해 그룹 정책을 항상 사용할 수 있거나 지원되는 것은 아닙니다.



Azure AD는 Intune과 같은 모바일 디바이스 관리(MDM) 서비스와의 통합을 지원합니다.

Intune과 Azure AD 간의 통합이 환경 설정되면 Azure AD에 조인하는 디바이스가 Intune에 자동으로 등록됩니다(추가 라이선스가 필요할 수 있음).

데모: Windows 10 디바이스 자동 등록

레슨 2: Microsoft Endpoint Configuration Manager를 사용하는 디바이스 등록

레슨 소개

Microsoft Endpoint Manager 소개

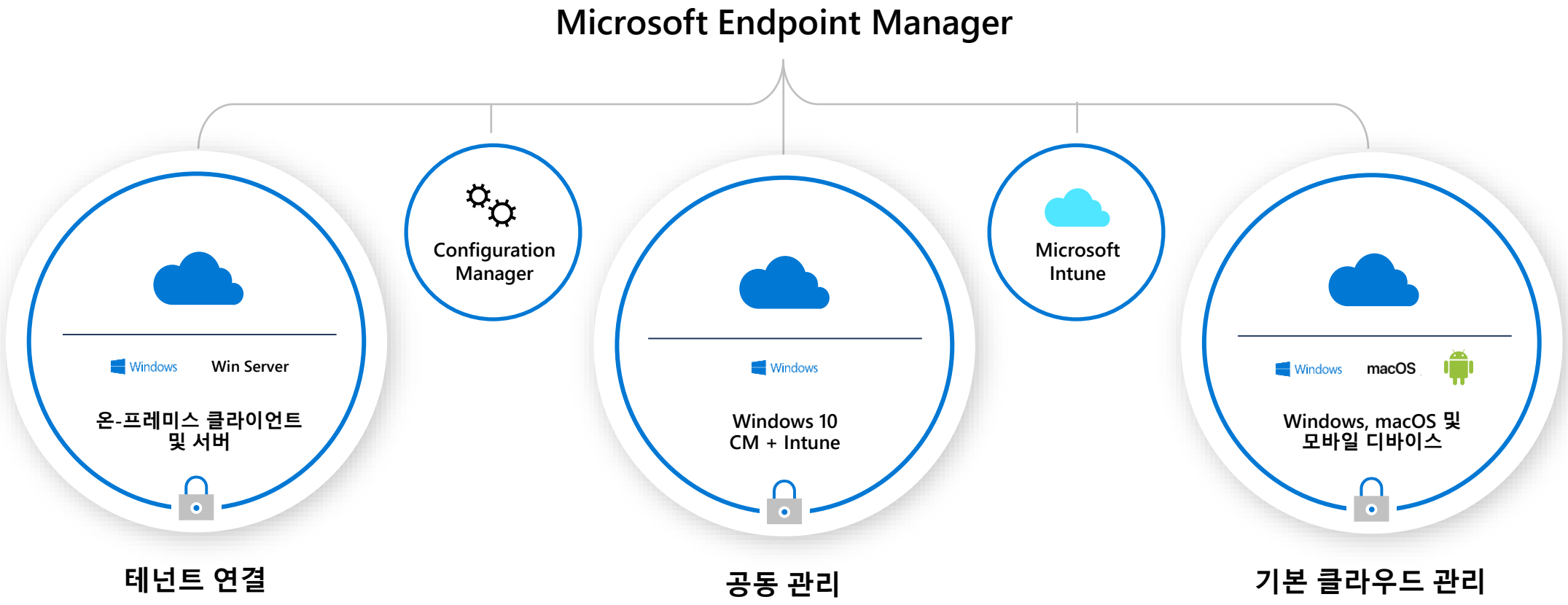
Microsoft Endpoint Configuration Manager 클라이언트 배포

Microsoft Endpoint Configuration Manager 클라이언트 모니터링

Microsoft Endpoint Configuration Manager 클라이언트 관리

Microsoft Endpoint Manager

원하는 속도로 클라우드에서 온-프레미스 엔드포인트 관리



Configuration Manager 클라이언트를 배포하는 이유

IT 관리자를 위한 이점

디바이스에 있는 소프트웨어 추적

하드웨어와 관련된 인벤토리 정보에 액세스

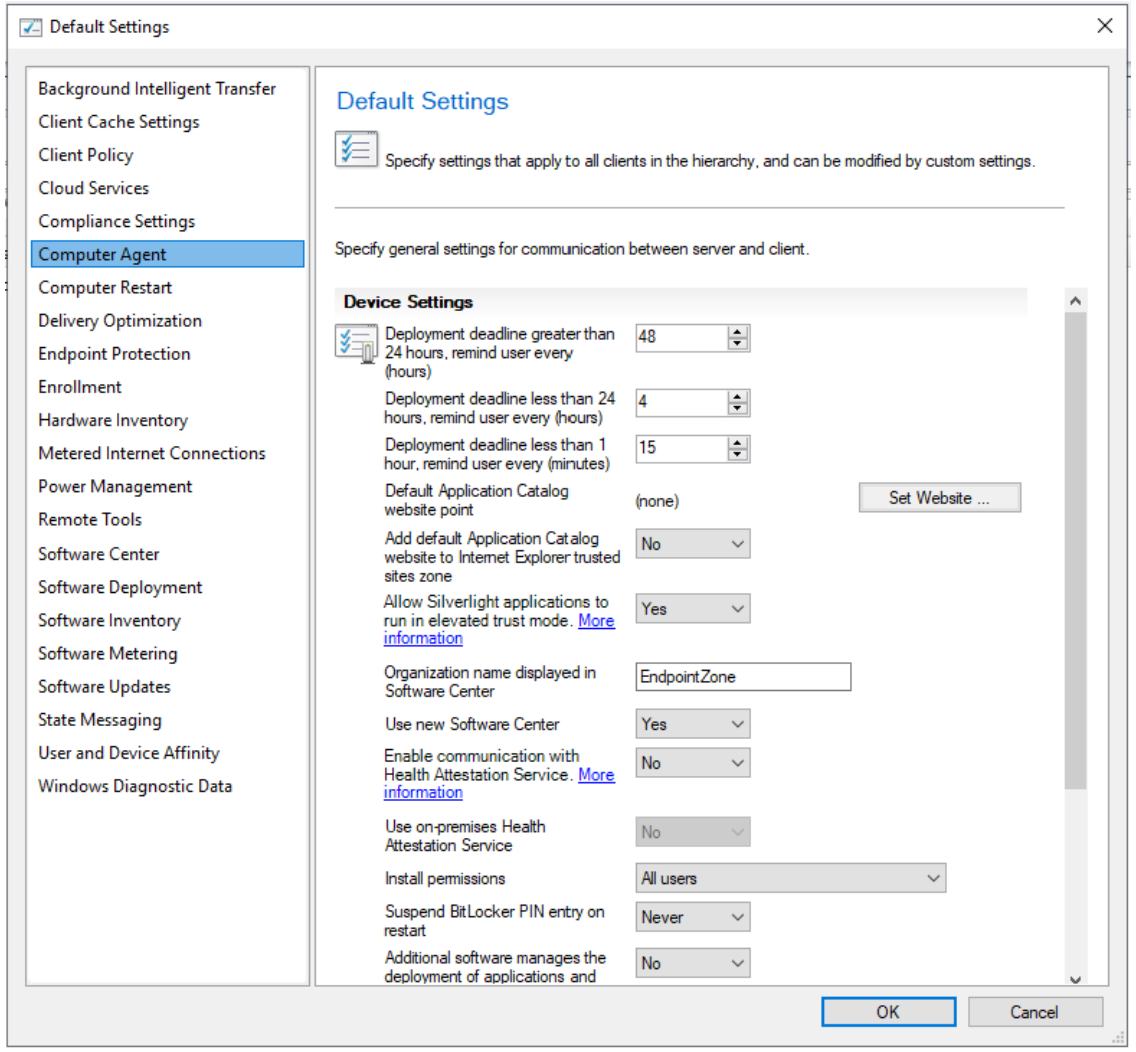
품질 및 기능 업데이트를 통해 디바이스 업데이트

OS 및 LoB 애플리케이션 관리 및 배포

최종 사용자를 위한 이점

사용자가 설치할 소프트웨어를 선택할 수 있는 기능이 다양한 소프트웨어 셀프 서비스 카탈로그 검색

중단을 최소화하도록 근무 시간 환경 설정



클라이언트 배포 옵션

클라이언트 푸시

Configuration Manager 콘솔에서 직접 Configuration Manager 클라이언트 배포

디바이스 검색(Active Directory LDAP 통합)

파일을 원본 컴퓨터에 복사하고 자동으로 설치 시작

초기 복사 프로세스로 인해 네트워크 트래픽이 증가할 수 있음

수동 배포

Configuration Manager 클라이언트 설치 원본 파일 및 설치 매개 변수가 포함된 스크립트 파일 배포

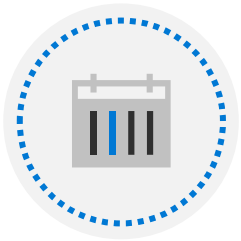
ccmsetup.exe 파일 또는 클라이언트 파일의 일부인 MSI에서 실행

제공 메커니즘으로 시간이 많이 걸릴 수 있음

OS 배포

작업 순서를 사용하여 Windows 10을 설치하고 설정할 때 Configuration Manager 클라이언트를 Windows 설정으로 슬립스트리밍하여 필요한 설치 매개 변수 제공

디바이스를 처음 빌드하거나 다시 빌드할 때 설치해야 함



Microsoft Intune

Intune은 Configuration Manager 클라이언트 설치를 추진하고 클라우드 관리 게이트웨이에 디바이스를 등록함

설치 후 Intune 또는 Configuration Manager에서 각 워크로드 관리

Microsoft Endpoint Configuration Manager 클라이언트 모니터링

클라이언트 온라인 상태. 온라인(할당된 관리 지점에 연결됨) 또는 오프라인

클라이언트 활동 활성(지난 7일 동안 Configuration Manager와 통신함) 또는 비활성

기본 사용자 60일 동안 가장 자주 로그인하는 것으로 계산된 이 디바이스의 기본 사용자

운영 체제 빌드 원격 관리에 연결하거나 이를 수행할 필요 없이 디바이스의 OS 버전을 참조합니다.

클라이언트 검사 Configuration Manager 클라이언트가 디바이스에서 실행하는 주기적인 평가의 상태입니다. 이 평가에서는 디바이스를 검사하고 발견된 몇 가지 문제를 해결할 수 있습니다.

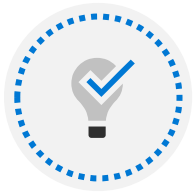
Microsoft Endpoint Configuration Manager로 관리

Configuration Manager 클라이언트가 설치되는 경우	• 사이트에 디바이스 할당 • 쿼리 기반 컬렉션에 디바이스 추가 • 인벤토리에 대한 디바이스 검색 및 인벤토리 데이터 업로드 • 규정 준수 검사, 필수 소프트웨어 푸시 등
컬렉션	• 공통성이 있는 디바이스 또는 사용자 표시 • 배포를 대상으로 지정 또는 보고서 실행과 같은 작업 수행
기타 관리 옵션	• 리소스 탐색기 시작 • 정책 검색 시작 • 컬렉션에 추가 • 클라이언트 설정 RSOP

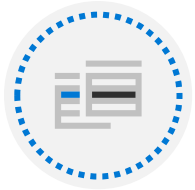
데모: Configuration Manager를 사용하여 Windows 10 디바이스 등록(선택 사항)

레슨 3: Microsoft Intune를 사용하는 디바이스 등록

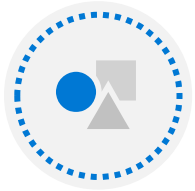
레슨 소개



MDM 서비스 활성화 및 배포

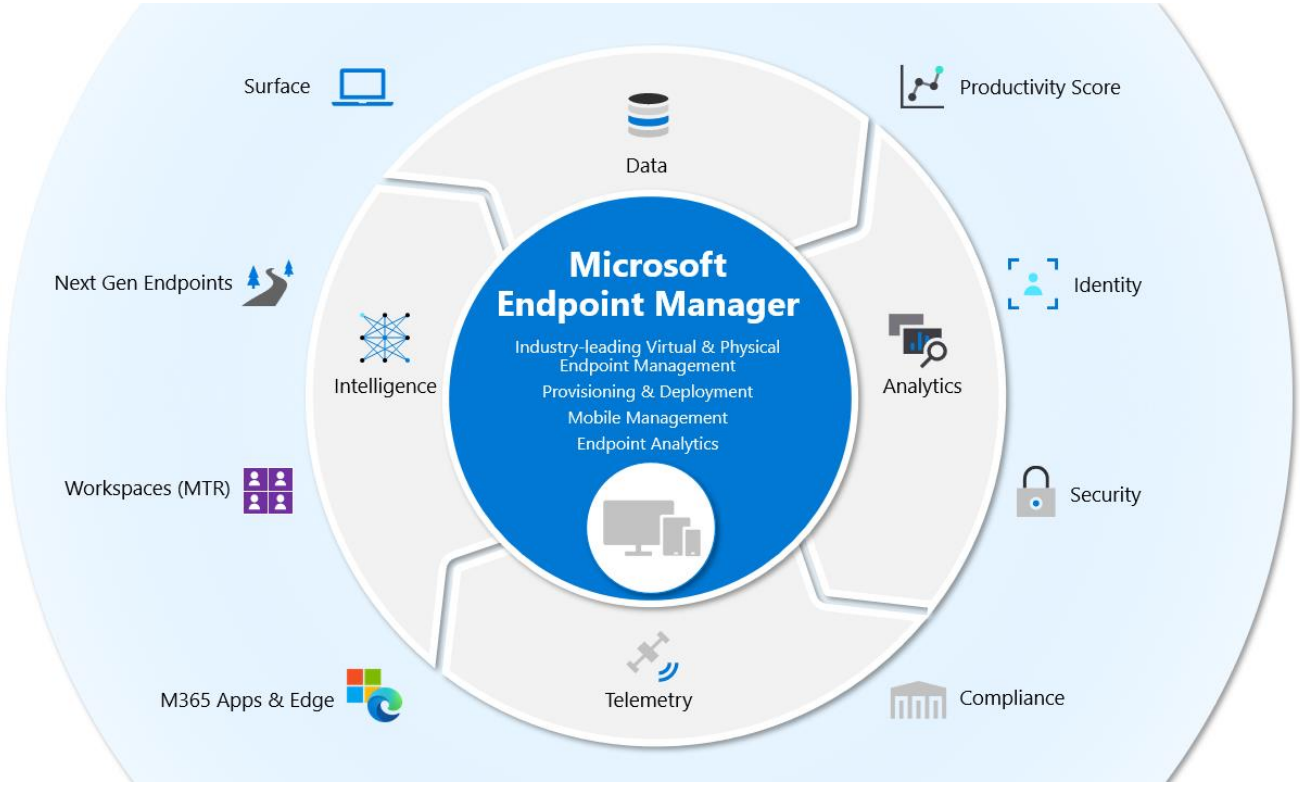


기업 등록 정책 관리



Intune에 Windows 등록

Microsoft Intune을 통한 디바이스 관리



- 디바이스 등록/등록 해제
- 원격 작업
- 애플리케이션 관리
- 인벤토리 및 분석
- 디바이스 보안 및 관리

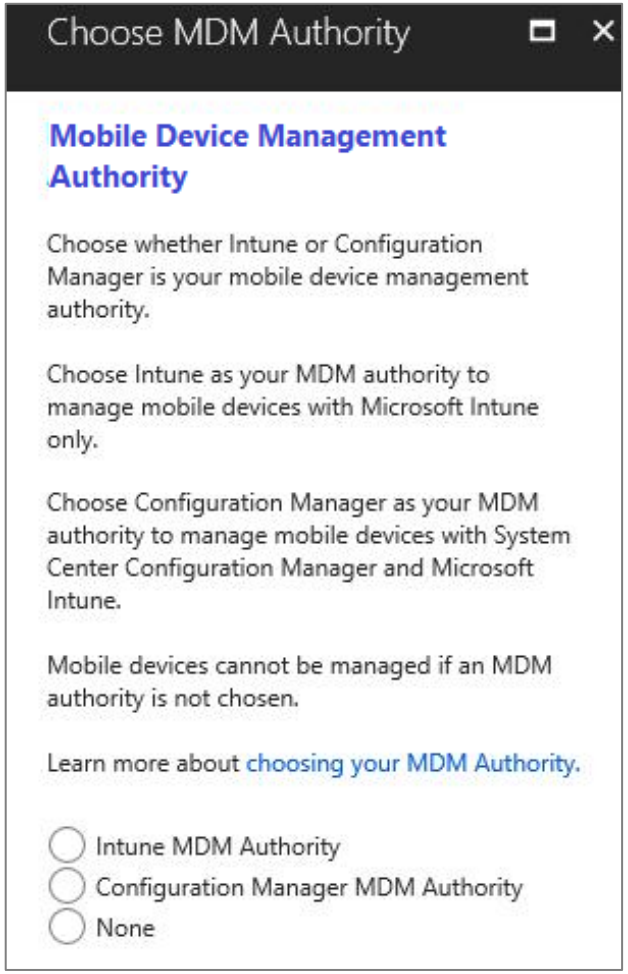
모바일, 데스크톱 및 IoT 전반에 걸친 일관된 MDM 기능 집합

모바일 디바이스 관리 활성화

MDM 기관으로 Intune 사용

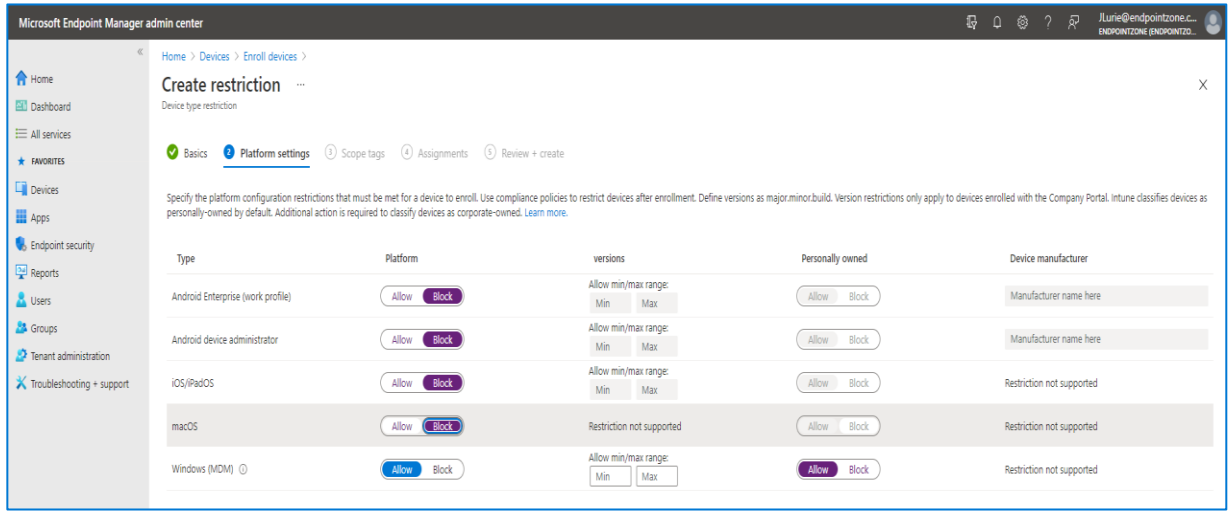
Apple MDM 푸시 인증서 받기

Apple의 디바이스 등록 프로그램을 사용하려는 경우 Apple Business 가입



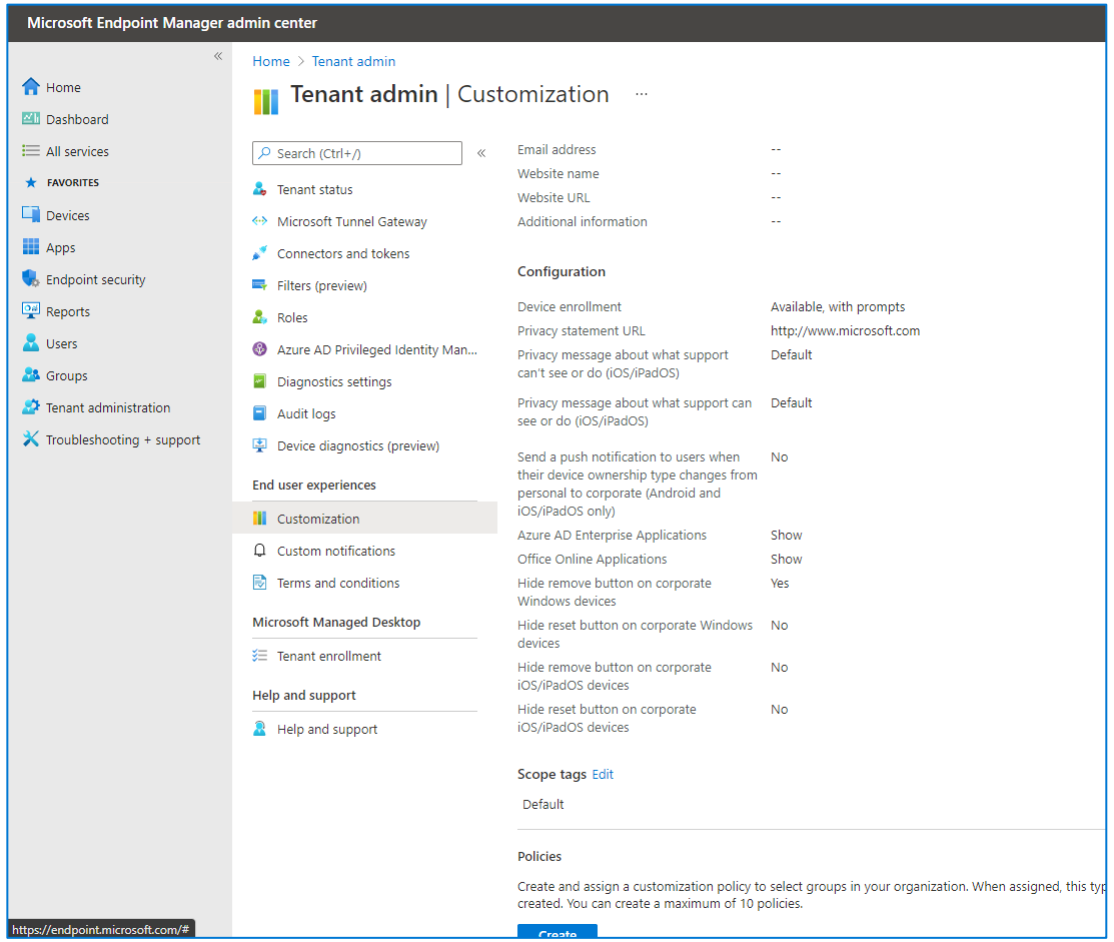
디바이스 등록 시 고려 사항

- 등록 방법 결정
  - 그룹 정책
  - Azure AD 조인
  - 수동(설정, 프로비저닝 패키지, 회사 포털 앱)
- 허용되는 디바이스 및 제한 사항 확인
- 등록이 선택 사항인지 또는 필수인지 확인



기업 등록 정책 관리

- 초기 Azure AD 도메인은 다음 모델을 따름
  - your-domain.onmicrosoft.com
- 사용자 지정 도메인 이름 중 하나 이상(예: Contoso.com) 추가(권장)
- Microsoft 365 관리 포털에 사용자 지정 도메인 이름 추가
- 자동 MDM 등록(권장) 또는 구성
- Azure AD Premium에 대한 라이선스가 없을 때 등록 및 디바이스 등록을 간소화하기 위해 CNAME 레코드 만들기



Intune에 Windows 디바이스 등록

Windows 10 디바이스를 Microsoft Intune에 등록하는 여러 가지 방법

- 회사 또는 학교 계정 추가
- 최신 앱 로그인(사용자 기반)
- MDM에만 등록(사용자 기반)
- Azure AD 조인(첫 실행 환경(OOBE))
- Azure AD 조인(Autopilot – 사용자 기반 배포 모드)
- MDM에만 등록(디바이스 등록 관리자)
- Azure AD 디바이스 등록 + 자동 등록 그룹 정책 개체
- 관리자 공동 관리 환경 설정
- Azure AD 조인(프로비저닝 패키지를 사용하는 대량 등록)

데모: Intune에 디바이스 등록

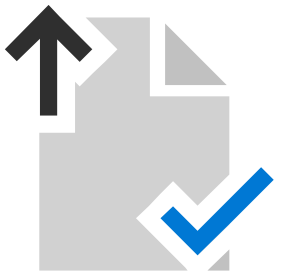
리소스

보안, 규정 준수 및 ID 블로그
Azure Active Directory 설명서
Microsoft Endpoint Manager IT 관련 커뮤니티 가입
Microsoft Endpoint Manager 블로그
Microsoft Endpoint Manager 설명서
Microsoft Intune 설명서
Configuration Manager 블로그
Microsoft Endpoint Configuration Manager 설명서
Microsoft Endpoint Manager 학습 경로
Configuration Manager 학습 경로

Microsoft

애플리케이션 관리

레슨 1:
애플리케이션 배포 및 업데이트



레슨 소개

Intune에 애플리케이션 추가

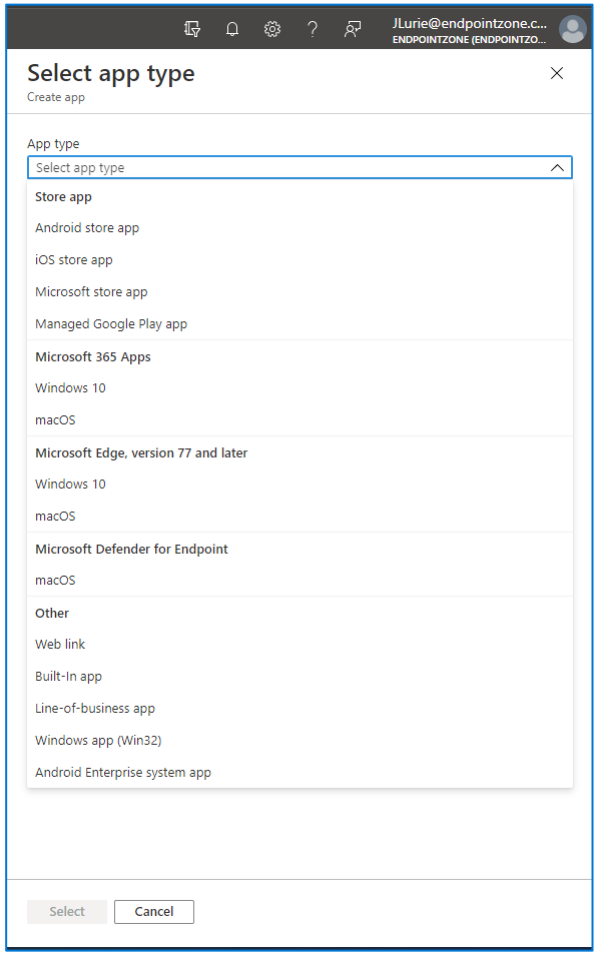
Configuration Manager를 사용하여 애플리케이션 배포

Intune에 앱 추가

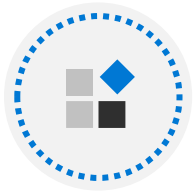
앱을 배포하거나 관리하기 전에 Intune에 앱을 추가해야 합니다.

지원되는 앱:

- 다양한 스토어(Apple 및 Google)의 애플리케이션
- Windows 스토어 또는 앱 카탈로그의 Windows 10용 앱
- Microsoft 365 앱
- 웹 링크
- 내장 앱(예: OneDrive 및 Edge)
- LOB 앱
- Win32 앱



Intune을 사용한 Win32 앱 관리



디바이스는 Azure AD에 조인되어 있어야 함

앱당 최대 크기 8GB

32/64비트 지원됨

Win32 콘텐츠 준비 도구는 .intunewin 파일을 만드는 데 사용됨

Intune에 앱 추가

- 앱 정보 및 요구 사항
- 명령 설치/제거
- 기존 환경 설정 및 앱에 대한 규칙
- 앱 반환 코드

데모: Intune으로 Windows 애플리케이션 배포

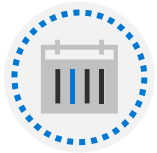
Configuration Manager를 사용하여 애플리케이션 배포

애플리케이션 모델의 요소

배포 유형

요구 사항

글로벌 조건



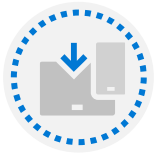
시뮬레이션된 배포

배포 애플리케이션

목적

수정

검색 방법



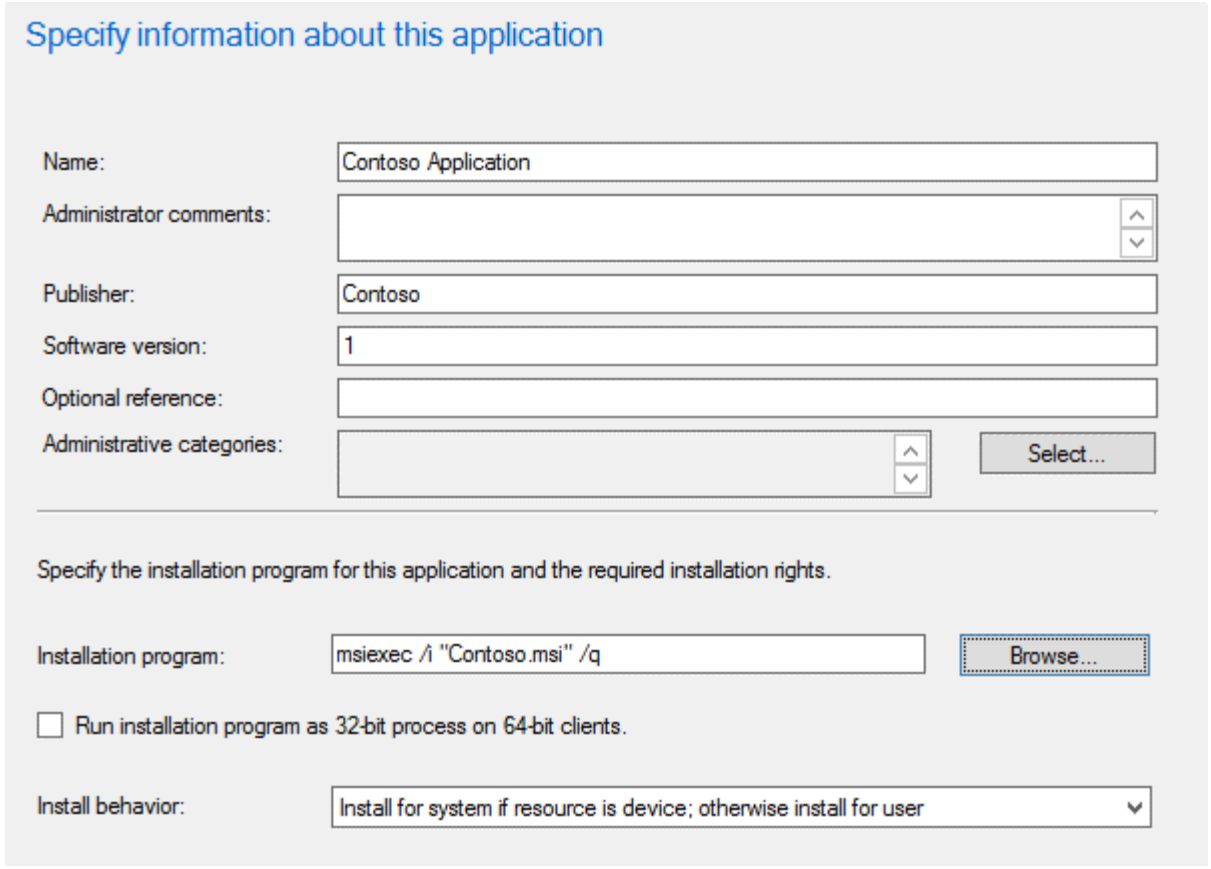
종속성

대체
애플리케이션 그룹

Configuration Manager에서 애플리케이션 만들기

애플리케이션을 만드는 방법은 다음과 같습니다.

1. Configuration Manager 콘솔에서 **소프트웨어 라이브러리** > **애플리케이션 관리** > **애플리케이션**을 선택합니다. **사용자 및 그룹**을 선택한 다음 **모든 사용자**를 선택합니다.
2. **홈** 탭의 **만들기** 그룹에서 **애플리케이션 만들기**를 선택합니다.
3. **애플리케이션 마법사 만들기**의 **일반** 페이지에서 **설치 파일에서 이 애플리케이션에 대한 정보 자동 검색**을 선택합니다.
    1. **유형**: **Windows Installer(*.msi 파일)**를 선택합니다.
    2. **위치**: 설치 파일 Contoso.msi의 위치를 입력합니다(또는 찾아보기를 선택하여 위치 선택).
4. **일반 정보** 페이지에서 애플리케이션에 대한 추가 정보를 제공할 수 있습니다.
5. **설치 프로그램** 필드에서 PC에 애플리케이션을 설치하는 데 사용할 전체 명령줄을 지정합니다.
6. **다음**을 선택합니다. **요약** 페이지에서 애플리케이션 설정을 확인한 다음 마법사를 완료합니다.



애플리케이션 배포를 위한 Endpoint Manager 솔루션 선택

애플리케이션 유형	Configuration Manager	Microsoft Intune
.MSI	예	예*
.IntuneWin	아니요	예
Office C2R	예	예
APPX/MSIX	예	예
스토어 앱	예	예
엔터프라이즈용 M365 앱	아니요	예
Appv	예	아니요

데모: Configuration Manager를 사용하여 Windows 10 앱 배포(선택 사항)

리소스

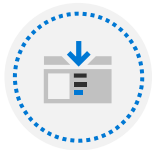
Microsoft Intune 설명서

Microsoft

Microsoft Endpoint Manager를 사용하는 배포(전반부)

모듈 의제

배포 준비 상태 평가



온-프레미스 배포 도구 및 전략

Autopilot을 사용하여 새 디바이스 배포

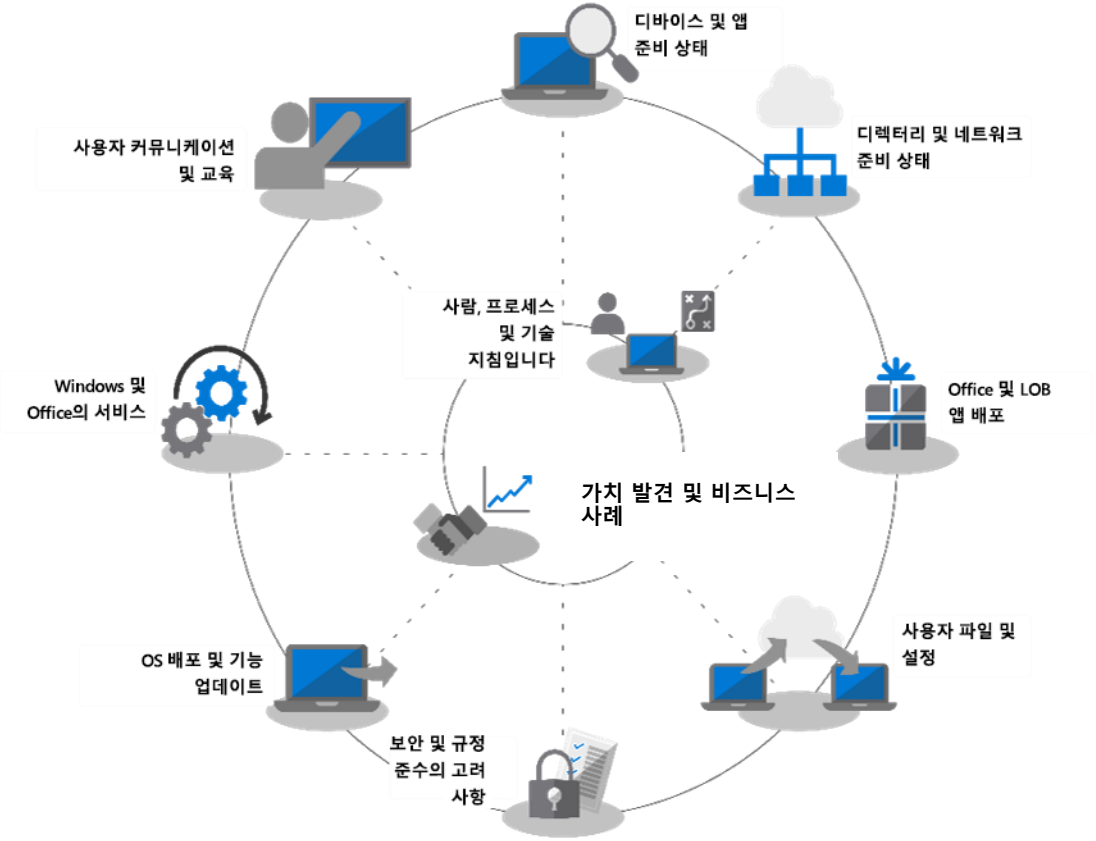
레슨 1: 배포 준비 상태 평가

레슨 소개

효과적인 엔터프라이즈급 데스크톱 배포에 대한 지침

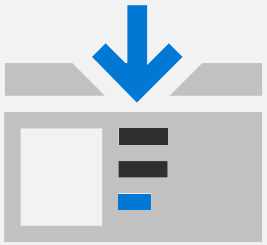
배포 지침

- 인벤토리를 검토하고 인프라 맵 설정
- 사용 중지할 디바이스 확인
- 복잡성 높은 애플리케이션 설치 지원 전략
- 가상화 기회 파악
- 데이터 마이그레이션 프로세스 수립
- 해당되는 경우 디바이스에서 데이터를 백업하는 방법 설정
- 전체 프로세스를 설명하는 배포 계획 수립
- 교육 및 배포 후 계획 수립



데모: Windows 및 Office 배포 랩 키트 검토(aka.ms/DeploymentLabKit)

레슨 2: 온-프레미스 배포 도구 및 전략



레슨 소개

기존 배포

Configuration Manager를 사용하여 Windows 10 배포

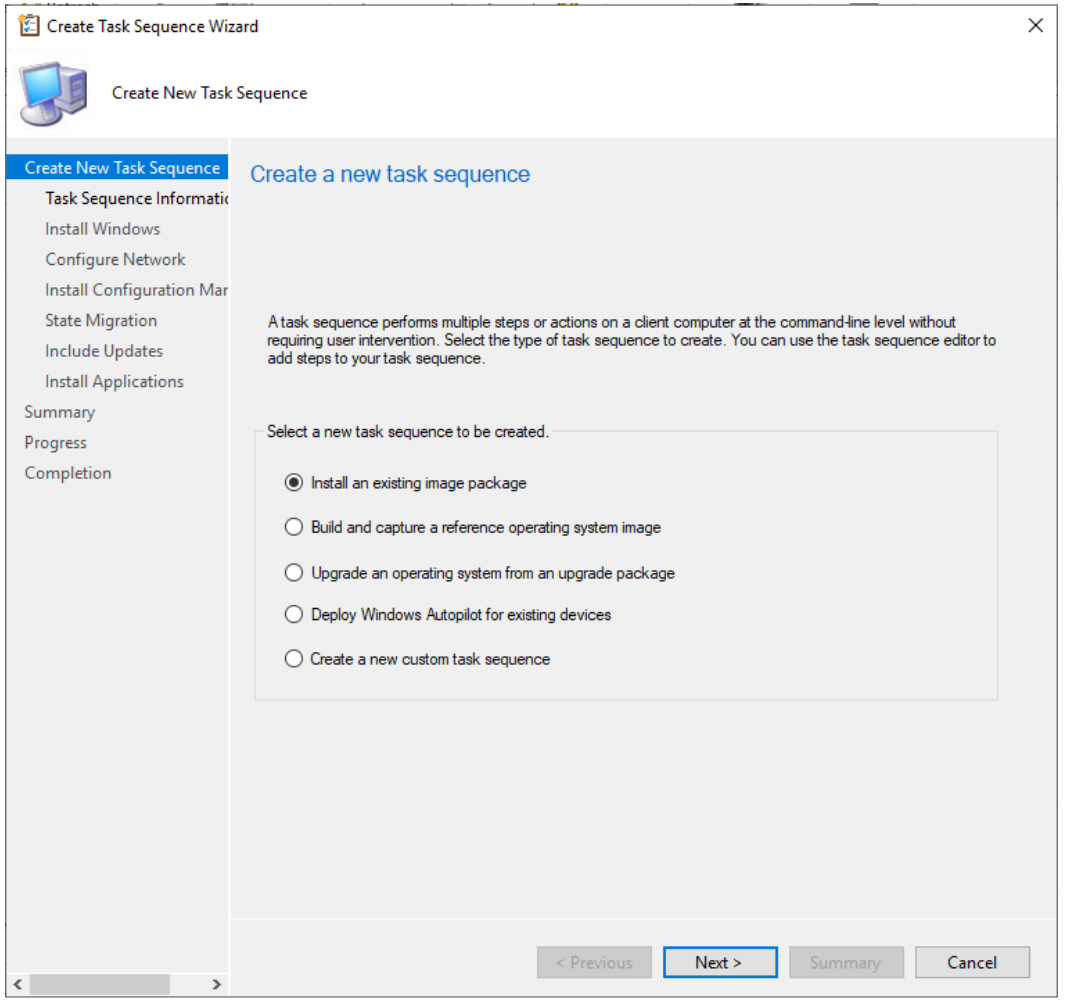
현재 위치 업그레이드 계획

기존 배포

기본 이미지	사용자 맞춤형 이미지
• 이미지를 만들 필요가 없음	• 이미지를 만들고 유지 관리해야 함
• 애플리케이션 및 설정은 별도로 적용해야 함	• 애플리케이션 및 설정은 사용자 맞춤형 이미지에 포함할 수 있음
• 아키텍처(x86/x64)당 이미지 한 개를 조직에 사용할 수 있음	• 조직 내 각 그룹의 환경 설정 및 애플리케이션 요구 사항(때로는 하드웨어)은 일반적으로 여러 이미지를 만들고 유지 관리하는 작업을 필요로 할 수 있음
• 애플리케이션 업데이트 시 이미지를 다시 빌드할 필요가 없음	• 애플리케이션 업데이트로 인해 이미지가 부실해져 이미지를 자주 업데이트하거나 다시 만들어야 함
• 환경 설정을 적용해야 하고 OS 이미지가 배포되면 애플리케이션을 설치해야 하므로 일반적으로 전체 배포 시간이 느려짐	• 이미지에 환경 설정 및 애플리케이션이 포함되어 있어 일반적으로 전체 배포 시간이 빨라짐
• 일부 애플리케이션은 설치를 자동화하기 어려울 수 있음	• 애플리케이션이 참조 컴퓨터에 설치되어 있는 경우, 일반적으로 이미지에 포함할 때 배포하기가 더 쉬움

Configuration Manager를 사용하여 Windows 10 배포: 소개

- **최신 데스크톱 여정에서 Configuration Manager의 역할**
  - Intune 및 Autopilot과 같은 최신 관리 도구와 Configuration Manager의 혁신적인 변화를 통해 이제 과거의 작업 방식과 더욱 현대적인 애자일 방식의 작업 방법을 연결하는 중요한 역할을 할 수 있습니다.
- MDT 기반 구축
  - OS 배포 중에 활용할 광범위한 작업 순서 변수에 대한 액세스
  - MDT 규칙 엔진은 OS 배포를 지원하는 많은 내장 옵션을 제공
  - 코드에 대한 지식 없이 Windows 기능을 설치할 수 있는 기능
  - 템플릿 작업 순서 마법사를 통한 로그 파일 수집



데모: Configuration Manager 관리 콘솔 검토(선택 사항)

Configuration Manager를 사용하여 Windows 10 배포: 소개

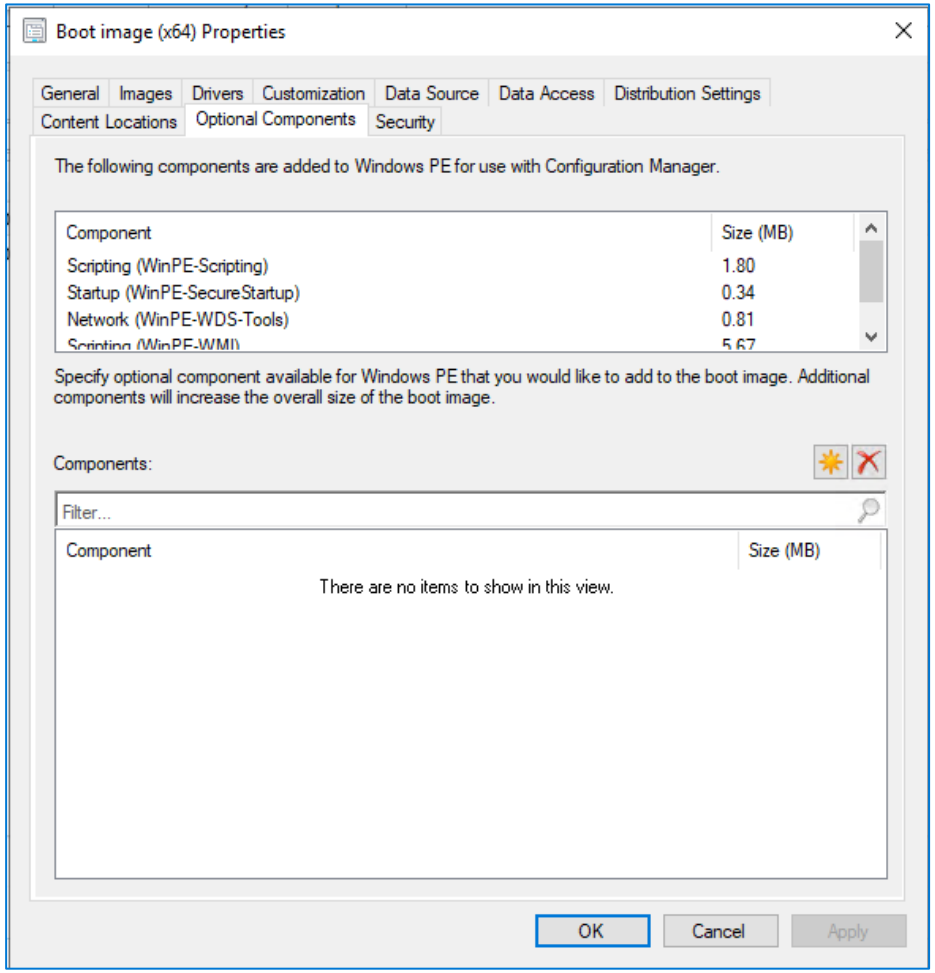
Configuration Manager 살펴보기

- OS 배포
- 애플리케이션 관리
- 업데이트 관리
- 서비스 관리
- 디바이스 인벤토리(CMDB)
- 기본 라이선스 추적
- 셀프 서비스 소프트웨어 카탈로그
- 클라우드 관리 기능
- 실시간 쿼리 및 보고
- 엔터프라이즈급 확장성
- Azure AD 통합
- Desktop Analytics을 통한 선제적 케이던스 채택
- 원격 제어
- 사용자 설정 캡처 및 복원

Configuration Manager를 사용하여 Windows 10 배포: 소개

배포 구성 요소 Configuration Manager 살펴보기

- **부팅 이미지**
  - Windows 10 배포를 시작하는 데 사용되는 Windows 사전 설치 환경(Windows PE) 이미지
  - PXE(사전 부팅 실행 환경) 서버를 사용하여 CD 또는 DVD, ISO 파일, USB 디바이스 또는 네트워크를 통해 부팅 이미지 시작
  - 두 개의 기본 부팅 이미지: 하나는 x86 플랫폼을 지원하고 다른 하나는 x64 플랫폼 지원
- **사용자 맞춤형 부팅 이미지 지정 시 고려 사항**



Configuration Manager를 사용하여 Windows 10 배포: 소개

배포 구성 요소 Configuration Manager 살펴보기

OS 이미지

Windows 이미징(WIM) 파일 형식에 저장됨

컴퓨터에 운영 체제를 성공적으로 설치하고 환경 설정하는 데 필요한 참조 파일 및 폴더의 압축 컬렉션

모든 운영 체제 배포 시나리오에 대한 운영 체제 이미지를 선택해야 함

운영 체제 업그레이드 패키지

운영 체제의 소스 설정 파일

이 패키지를 사용하여 디바이스에 바닐라 이미지를 전달할 수도 있음

DVD 또는 마운트된 ISO 파일에서 운영 체제 업그레이드 패키지를 Configuration Manager로 가져옴

디바이스 및 드라이버

배포 중인 운영 체제 이미지에 디바이스를 포함하지 않고 대상 컴퓨터에 디바이스 드라이버를 설치할 수 있음

Configuration Manager는 소프트웨어 라이브러리 워크스페이스에서 드라이버와 드라이버 패키지라는 두 노드로 환경 설정된 드라이버 카탈로그 제공

소프트웨어 업데이트

소프트웨어 업데이트를 추적하고 클라이언트 컴퓨터에 적용하는 작업을 관리할 수 있는 도구 및 리소스 집합 제공

Configuration Manager는 MDT의 기본 제품을 기반으로 하며 유형 또는 OS별로 업데이트를 분리하고 릴리스 관리를 위해 기존 프로세스로 작업할 수 있는 관리 평면 제공

작업 순서

Configuration Manager는 작업 순서를 사용하여 완전히 자동화할 수 있고 사용자 상호 작용(제로 터치 설치 또는 ZTI)이 필요하지 않은 일정에 따른 배포 제공

Configuration Manager(소프트웨어 업데이트 패키지, 애플리케이션 모델 및 클라우드 관리 게이트웨이)의 구성 요소 자동화

Configuration Manager를 사용하여 Windows 10 배포: 관리 및 모니터링

Configuration Manager를 사용하여 Windows 10 배포를 환경 설정하는 방법

작업 순서

MDT 작업 순서와 유사하지만 애플리케이션에서 만든 패키지 및 스크립트와 같은 다른 요소를 활용할 수 있음

Configuration Manager 작업 순서 엔진을 MDT 바이너리와 통합하여 유연성을 높일 수 있음

작업 순서를 사용하는 시나리오

배포 컬렉션

작업 순서를 만든 후 배포 컬렉션에서 이를 대상으로 지정하여 성공적인 제공 가능

의도하지 않은 OS 제공 방지

알 수 없는 컴퓨터를 대상으로 지정하여 생성된 작업 순서를 시작하는 기능으로 획득한 새 디바이스 표시

Configuration Manager를 사용하여 Windows 10 배포: 관리 및 모니터링

Configuration Manager를 사용하여 Windows 10 배포 문제 해결

보고

Configuration Manager에 환경 설정된 보고 서비스 지점을 사용하면 SQL Server Reporting Services(SSRS) 및 Power BI Report Server의 고급 보고 기능을 사용할 수 있는 도구 및 리소스 집합에 액세스할 수 있음

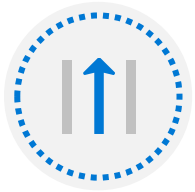
로그 파일

Configuration Manager는 문제 해결을 지원하기 위해 클라이언트와 서버 측 모두에 수많은 로그 파일 생성

예:

- Ccmsetup.log
- SMSTS.log
- AppEnforce.log
- Execmgr.log

현재 위치 업그레이드 계획

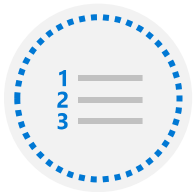


Windows 10에 대한 권장 경로

모든 데이터, 설정, 앱 및 드라이버 보존

언제든지 롤백할 수 있음

Windows 설정 활용

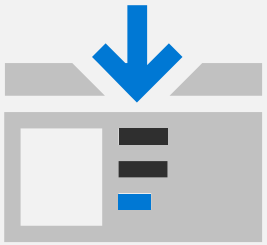


MDT 또는 Configuration Manager를 활용하는 작업 순서 사용

현재 위치 업그레이드에 대한 고려 사항

시나리오	현재 위치 업그레이드	새로 설치
32비트 운영 체제에서 64비트로 이동 (예: Windows 7 32비트에서 Windows 10 64비트로)	아니요	예
한 버전의 Windows에서 하위 대상 버전으로 이동 (예: Windows 10, 버전 21H1에서 버전 1909로)	아니요	예
기존 디바이스는 최소 하드웨어 사양 충족 (무료 디스크 공간 포함)	예	예
기존 앱은 대상 버전과 호환됨	예	예
기존 OS 언어는 대상 버전과 동일함	예	예
운영 체제를 멀티 부팅/이중 부팅하려는 경우	아니요	예
표준 install.wim을 사용하려는 경우	아니요	예
운영 체제 이미지를 만들고 유지 관리해야 하는 경우 (또는 앱, 드라이버 및 설정으로 업데이트해야 하는 새 ISO 파일)	아니요	예

레슨 3: Windows Autopilot을 사용하는 최신 배포



레슨 소개

Autopilot을 이용한 최신 배포

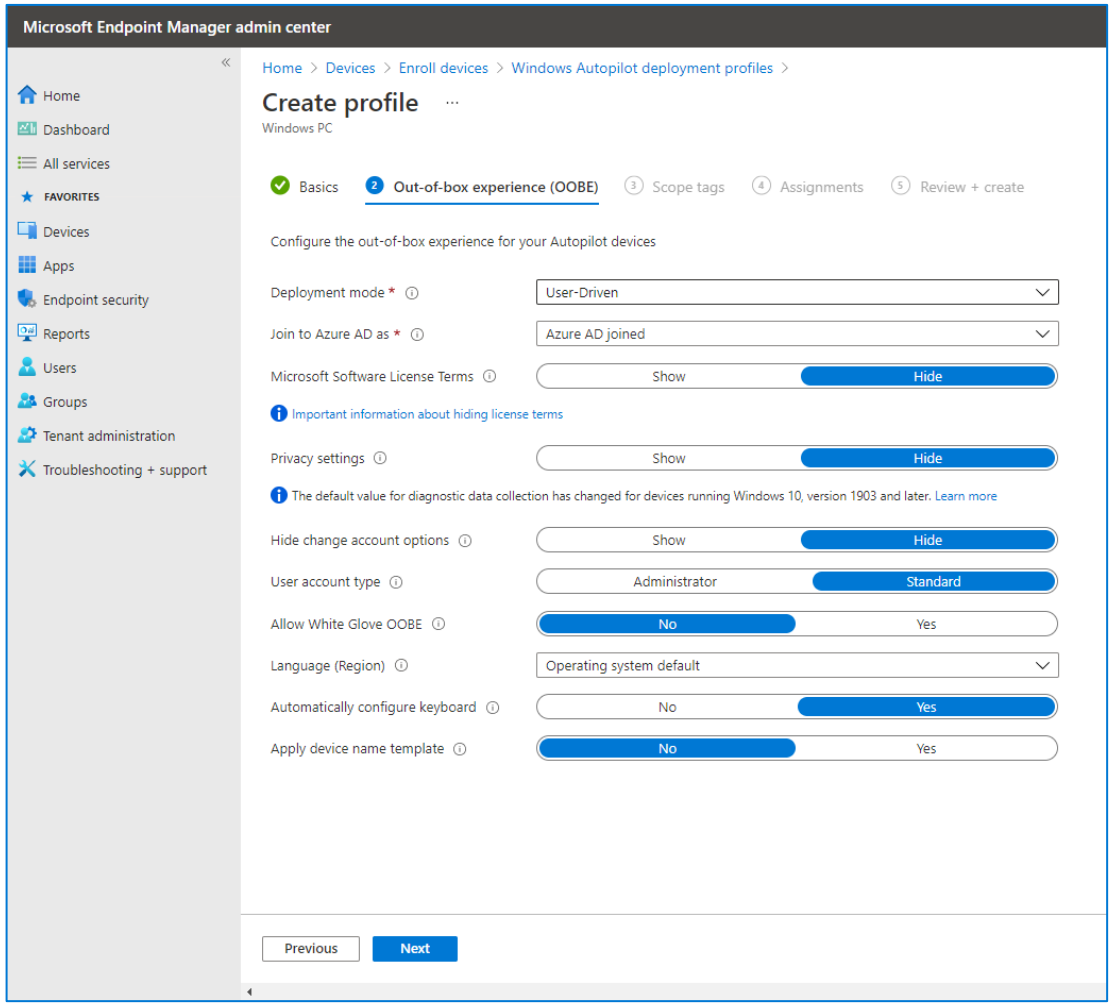
Windows Autopilot의 요구 사항

Autopilot용 디바이스 ID 준비

디바이스 등록 및 OOBE 사용자 지정

Windows Autopilot을 이용한 최신 배포

- 이미지, 드라이버 또는 인프라 없음
- 사용자 맞춤형으로 첫 실행 환경 지정
- 새 디바이스에는 일반적으로 Windows 10이 설치되어 있음
- 디바이스 새로 고침



Windows Autopilot을 이용한 최신 배포

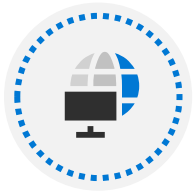
Autopilot과 기존 방법 비교

	기존 배포	최신 배포
Windows 10 이미지 배포	예	아니요
사전 설치된 운영 체제에서 사용할 수 있음	예	아니요
이전 Windows 10 설치 필요	아니요	예
온-프레미스 인프라 사용	예	아니요
배포 준비를 위한 도구	Windows ADK, Windows 배포 서비스, Microsoft Deployment Toolkit(MDT) 및 Configuration Manager	Windows Configuration Designer 및 Windows Autopilot

Windows Autopilot의 요구 사항

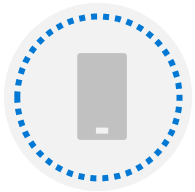
디바이스에는 Windows 10이 사전 설치되어 있어야 함

- Windows 10 Pro, Enterprise 또는 Education



디바이스에는 인터넷 연결이 있어야 함

- Windows Autopilot은 클라우드 서비스임

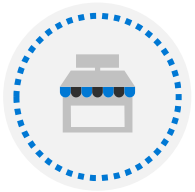


Intune 또는 기타 모바일 디바이스 관리 서비스(선택 사항)

- 배포된 Windows 10 디바이스 관리용

디바이스는 조직에 등록해야 함

- 클라우드에 업로드된 디바이스별 정보

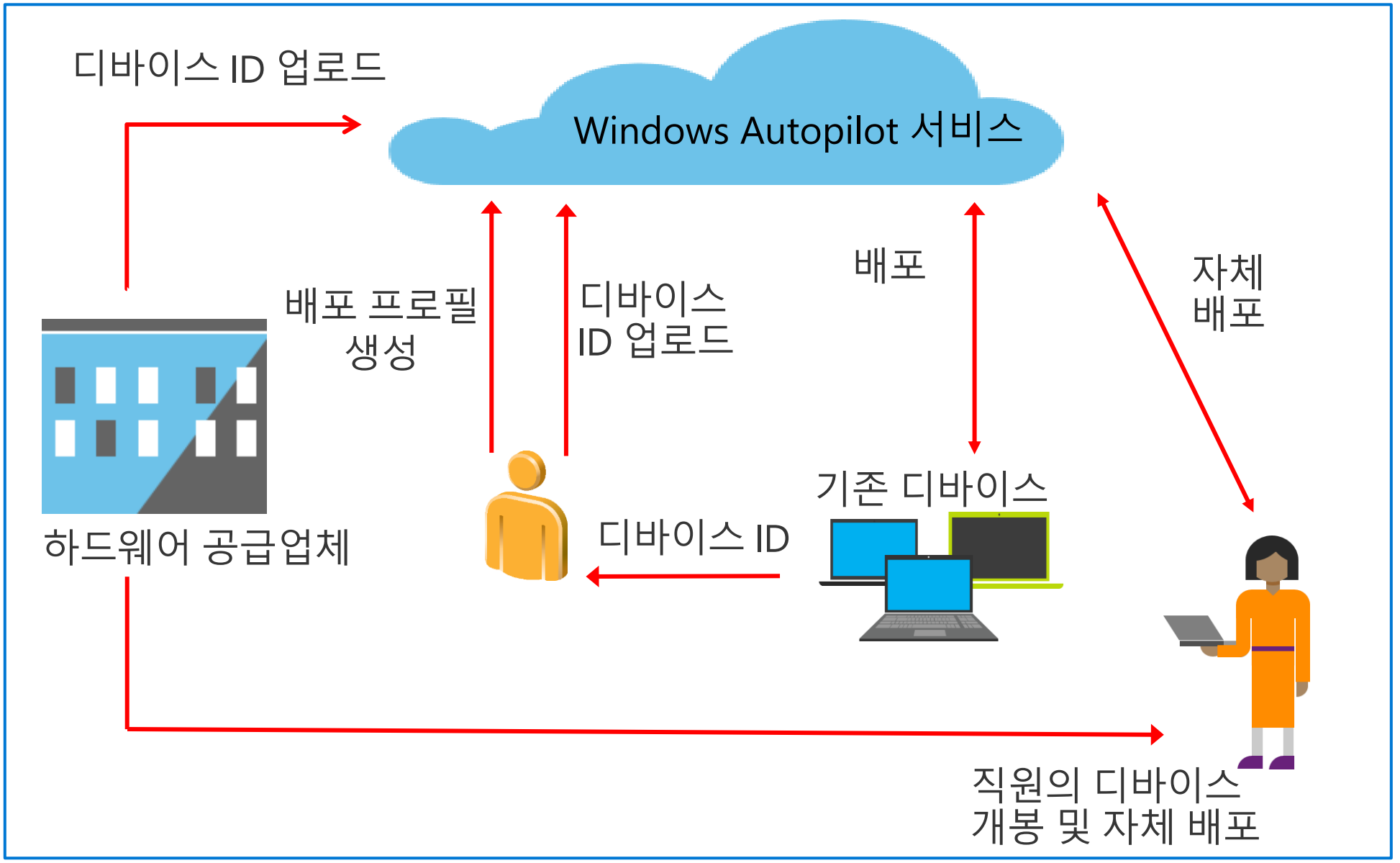


조직은 Azure AD를 사용해야 함

- 또한 비즈니스용 Microsoft Store 또는 Intune을 사용해야 함

필요한 URL에 대한 액세스

Autopilot용 디바이스 ID 준비



디바이스 등록 및 OOBE 사용자 지정

1단계
Windows Autopilot 배포 파일 만들기

디바이스에 적용할 설정을 지정하는 필수 프로필

Windows Autopilot을 사용하여 여러 배포 프로필을 만들고 사용할 수 있지만 단일 프로필만 사용하여 각 디바이스를 배포할 수 있습니다.

2단계
배포 프로필 적용

배포 프로필을 적용하기 전까지는 Windows Autopilot이 디바이스의 OOBE 설정 단계를 관리하지 않습니다.

Windows Autopilot은 프로필을 적용하는 디바이스의 OOBE 설정 단계를 제어합니다.

모듈 3 리소스

Windows Autopilot 설명서
Windows IT 관련 커뮤니티 가입
Windows IT Pro 블로그
Windows 기술 설명서
Windows 학습 과정

Microsoft

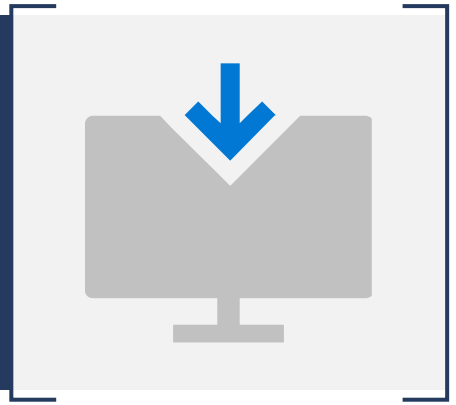
Microsoft Endpoint Manager를 사용하는 배포(후반부)

모듈 의제

Autopilot을 사용하여 새 디바이스 배포

동적 배포 방법

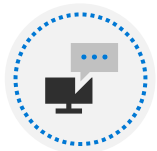
레슨 1:
Autopilot을 사용하여 새 디바이스 배포



레슨 소개

Windows Autopilot 데모

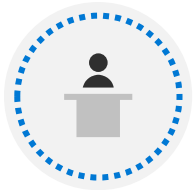
Autopilot 시나리오



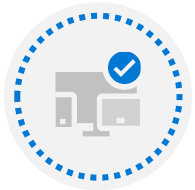
Windows 10 Autopilot 문제 해결

데모: 배포 프로필 생성 및 적용

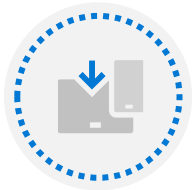
Autopilot 시나리오



Windows Autopilot 사용자 기반 모드



Windows Autopilot 자체 배포 모드

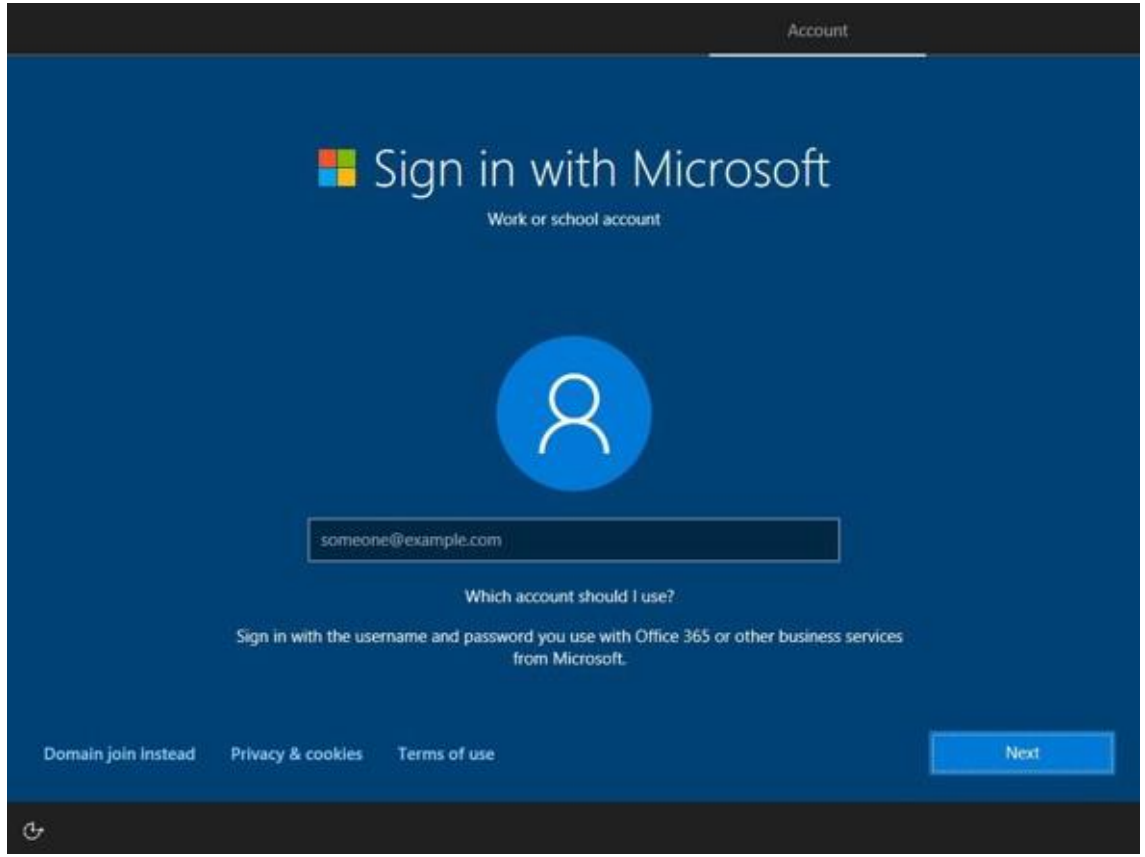


기존 디바이스를 위한 Autopilot

사전 프로비저닝된 배포를 위한 Windows Autopilot

Windows Autopilot 재설정

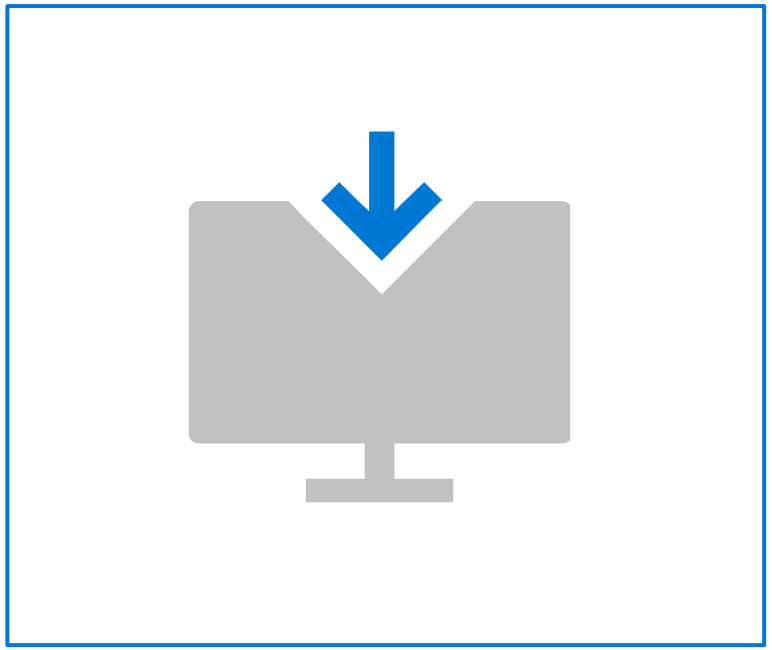
기본 OOBE 환경 및 Autopilot OOBE 환경 비교



기본 OOBE 설정 단계

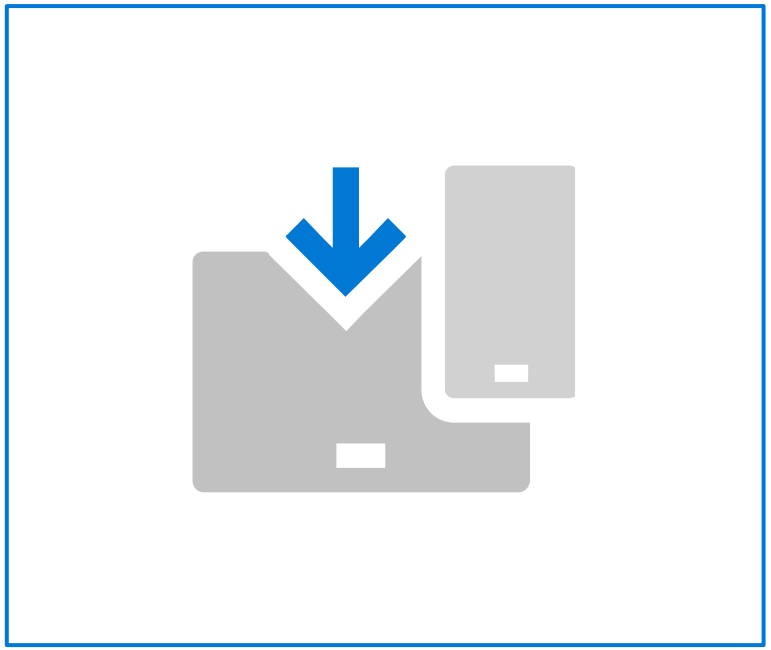
Windows Autopilot의 OOBE 설정 단계

동적 프로비저닝 방법



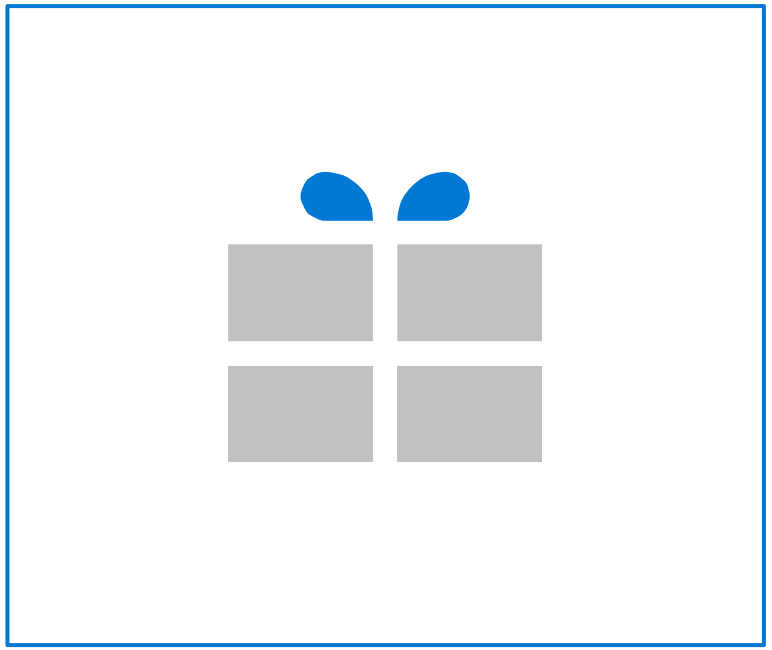
Subscription Activation

Windows 10의 버전 변경



모바일 디바이스 관리

기존 Windows 10 디바이스를 자동 등록하여
환경 설정 정책 및 설치된 애플리케이션 적용



프로비저닝 패키지

환경 설정의 설정을 이동식 미디어를
사용하거나 디바이스에 직접 다운로드하여
Windows 10에 적용

데모: Subscription Activation 및 프로비저닝 패키지 검토

Windows 10 Autopilot 문제 해결

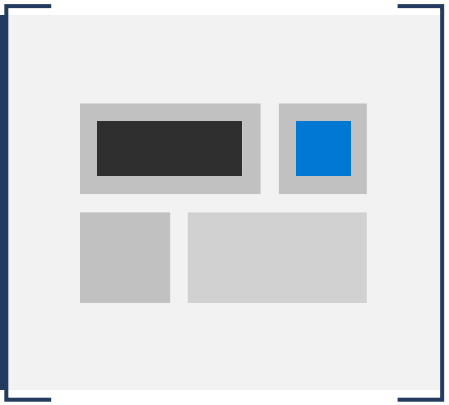
Windows Autopilot의 문제를 해결할 때 이해해야 할 주요 사항은 다음과 같습니다.

Autopilot 흐름	1. 네트워크 연결 설정 2. Autopilot 프로필 다운로드 3. 사용자가 인증됨(사용자 기반 배포 모드만) 4. Azure AD 조인 발생 5. 자동 MDM 등록 6. 설정 적용됨

프로필 다운로드	1. 인터넷에 연결된 사용자 연결 디바이스 확인
	2. 프로필이 존재하고 할당되었는지 확인
	  1. 빈 프로필이 다운로드된 경우 Microsoft Endpoint Manager 관리 센터를 확인하고 프로필 할당
	  2. 디바이스를 재부팅하여 새 프로필을 다운로드할 수 있음
	3. 디바이스에 하나의 프로필만 할당되었는지 확인

수행할 주요 작업	1. 라이선싱 및 프로필 및 사용자 할당이 적절한지에 대해 Azure AD 및 Microsoft Intune 검토 2. Azure AD 조인 문제 및 MDM 등록 문제 찾기 3. 문제 해결 로그 수집 mdmdiagnosticstool.exe –area Autopilot –cab <path>

레슨 2: 동적 배포 방법



레슨 소개

자동 MDM 등록을 통한 Azure AD 조인

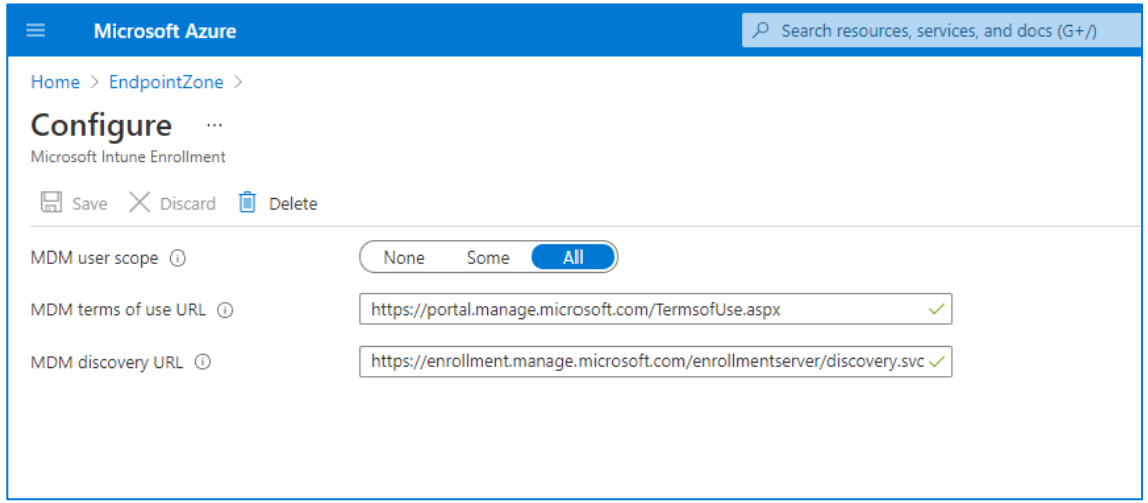
자동 MDM 등록을 통한 Azure AD 조인

설명

- Azure AD에 디바이스를 등록하고 Intune에 자동으로 등록
- 디바이스 프로비저닝 간소화
- BYOD(Bring Your Own Device : 개인용 디바이스를 업무용으로 사용)/CYOD 시나리오에 적용

Azure AD/MDM을 사용하면 다음을 수행할 수 있습니다.

- 디바이스를 Azure AD에 자동으로 조인
- 사용자의 디바이스를 MDM 서비스에 자동 등록
- MDM 정책을 사용하여 조인된 디바이스 환경 설정



데모: MDM 등록을 통한 자동 Azure AD 조인

Lesson 3: 최신 관리로의 마이그레이션 계획

레슨 소개

공동 관리 – 실질적인 최신 관리 방식

공동 관리를 위한 전제 조건

최신 관리 고려 사항

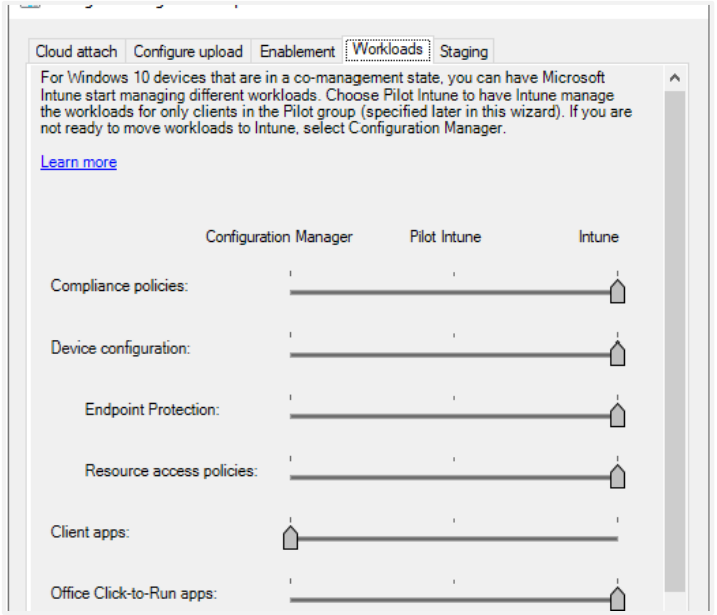
최신 관리 업그레이드 또는 마이그레이션

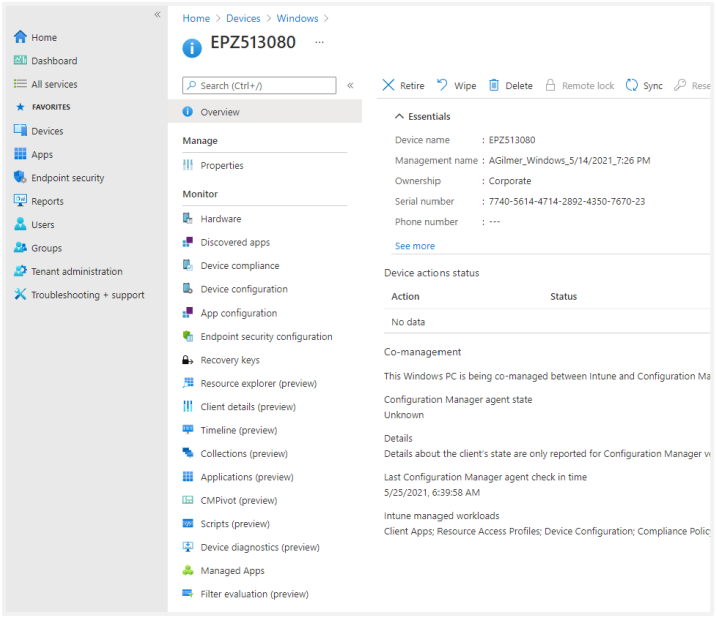
최신 마이그레이션: 데이터 마이그레이션

최신 마이그레이션: Intune을 사용하는 새로운 디바이스

공동 관리: 실질적인 최신 관리 방식

- 최신 관리로의 마이그레이션 간소화
- 첫날부터 누리는 최신 관리의 이점
- 온-프레미스 Configuration Manager 및 Intune을 사용하여 관리되는 디바이스
- 온-프레미스 환경에 연결되지 않더라도 Intune에서 디바이스를 관리할 수 있음





공동 관리를 위한 전제 조건

하이브리드 Azure AD 조인 디바이스만 가능

컴퓨터 계정을 Azure AD에 동기화하려면 최신 Azure AD 연결을 설치하고 환경 설정해야 함

Intune MDM을 설정하고 자동 등록을 환경 설정해야 함

모든 사용자에게 Enterprise Mobility + Security(EMS) 또는 Intune 라이선스가 할당되어야 함

Windows 10, 버전 1709 이상 사용해야 함

Azure AD 자동 등록이 활성화되어 있음

공동 관리 계획

워크로드를 Intune으로 마이그레이션

- **리소스 액세스 정책**
  - 이메일 프로필
  - Wi-Fi 프로필
  - VPN 프로필
- **인증서 프로필**
- **Windows 업데이트 정책**
- **디바이스 환경 설정**
- **Microsoft 365 선택-실행 앱**

- **Endpoint Protection**
  - Windows Defender Application Guard
  - Windows Defender Firewall
  - Windows Defender SmartScreen
  - Windows Encryption
  - Windows Defender Exploit Guard
  - Windows Defender Application Control
  - Windows Defender 보안 센터
  - Windows Defender Advanced Threat Protection
  - Windows Information Protection
  - BitLocker

데모: 공동 관리 환경 설정

최신 관리 고려 사항

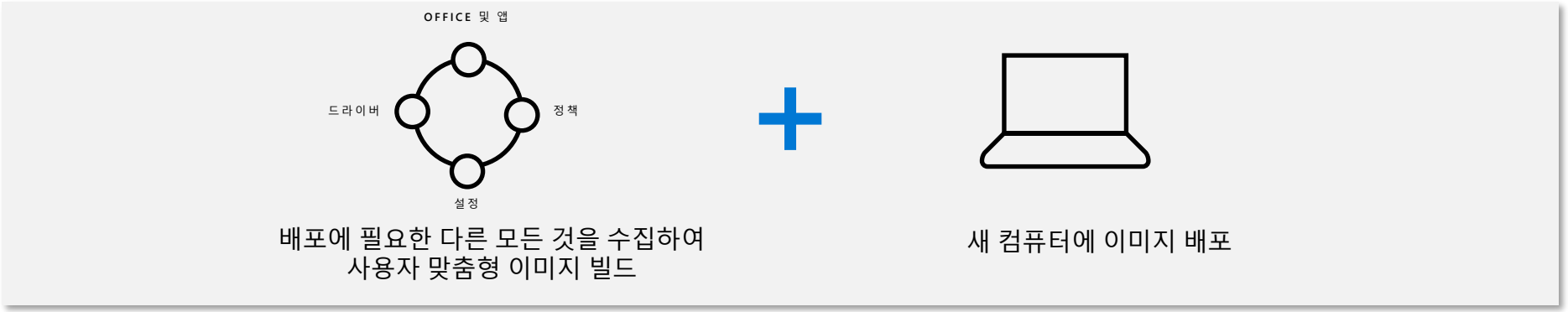
최신 마이그레이션 고려 사항

	MDT	Configuration Manager	Windows Autopilot
골든 이미지 생성 필요	예	예	아니요
디바이스를 다시 빌드하거나 재설정할 수 있음	예	예	예
운영 체제 미설치 빌드를 수행할 수 있음	예	예	아니요
사전 설치된 운영 체제에서 사용할 수 있음	예(사전 설치된 운영 체제가 초기화됨)	예(사전 설치된 운영 체제가 초기화됨)	예
디바이스가 빌드될 때 애플리케이션 설치	예	예	예
빌드 후 애플리케이션 배포	아니요	예	예
사용자 데이터 마이그레이션(USMT)	예	예	아니요(OneDrive 알려진 폴더 사용 권장)
현재 위치 업그레이드 수행	아니요	예	아니요(배포만 가능)

최신 방식으로 이미징 사용

최신 관리 방법을 이용한 이미징 사용이 필요할 수 있는 시나리오

- 디바이스가 Windows로 부팅할 수 없으므로 운영 체제 미설치 빌드 필요
- 운영 체제 미설치 배포
- 클라이언트 스토리지 드라이브 교체
- 디바이스가 회사에서 표준화되지 않고 최신 버전의 Windows 10으로 조달됨



최신 마이그레이션: 업그레이드 및 마이그레이션

사용자 상태 및 데이터 마이그레이션

사용자 데이터 마이그레이션	• 디바이스 교체 • 디바이스는 이전 OS에서 Windows 10으로 업그레이드되고 있으며 현재 위치 업그레이드 불가능(예: 32비트 Windows에서 64비트 Windows로) • 새로 설치 필요
마이그레이션 시나리오	• 단계별: 원본 컴퓨터와 대상 컴퓨터가 다름 • 초기화 및 로드(새로 고침 마이그레이션): 원본 컴퓨터와 대상 컴퓨터가 동일

사용자 데이터를 기존 방식으로 마이그레이션

Configuration Manager에서 USMT 사용

Configuration Manager에서 USMT 패키지 만들기

사용자 맞춤형 USMT 패키지를 만들거나 기본 패키지 사용

상태 마이그레이션 지점 설정(Configuration Manager 사이트 시스템 역할)

데이터를 저장하는 파일 공유 역할

다음과 같은 고유한 해시 저장

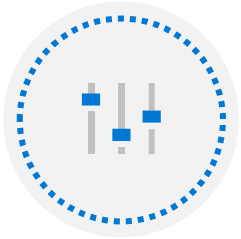
- 데이터를 캡처할 수 있는 디바이스
- 업그레이드된 디바이스
- 복원할 관련 데이터

작업 순서

USMT 포함 가능

다음과 같은 경우 작업 순서에서 발생

- 설정 캡처
- 선택한 옵션에 따라 사용자 설정 복구



마이그레이션을 위해 USMT 템플릿 사용

사용자 프로필에서 수집된 데이터를 제어하는 xml 템플릿:

- MigApp.xml
- MigDocs.xml
- MigUser.xml
- ConfigMgr.xml

사용자 데이터를 최신 방식으로 마이그레이션

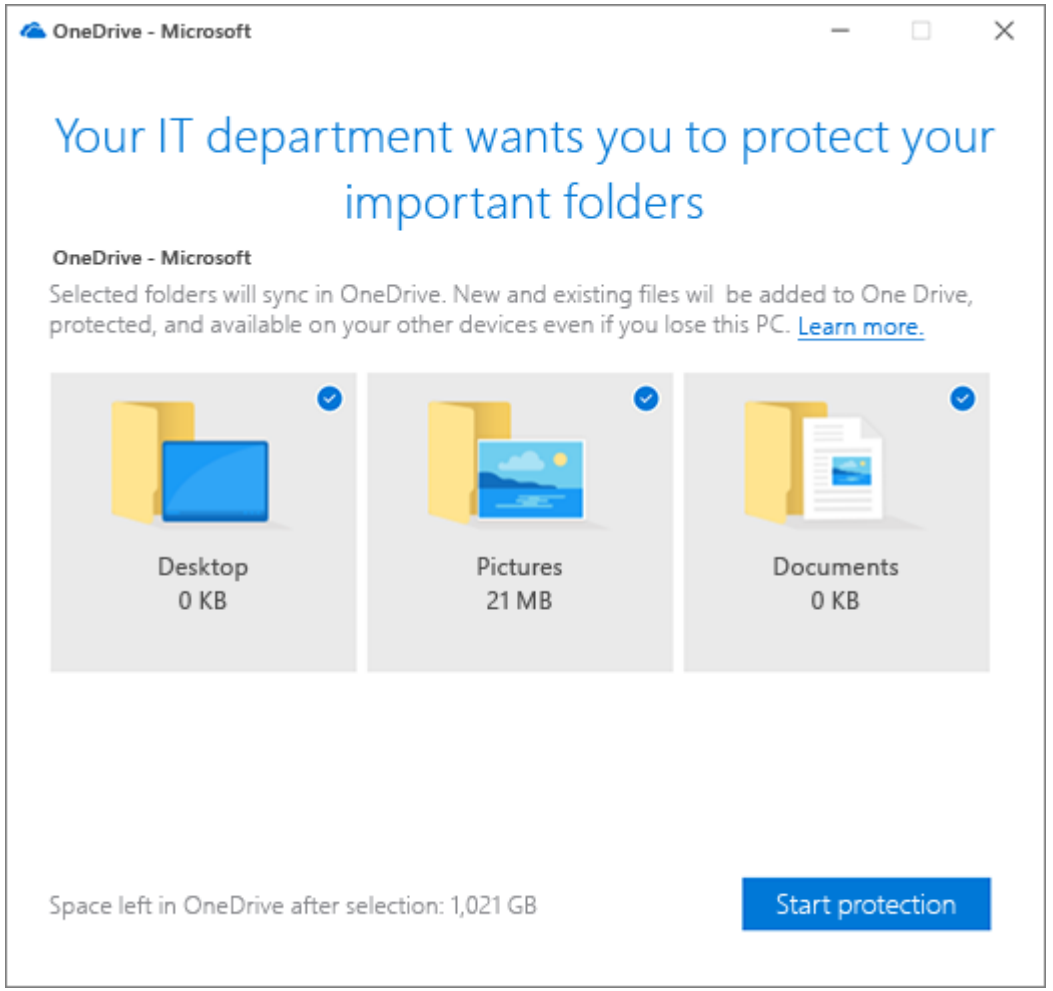
알려진 폴더 이동 - 사용자 설정 관리에 대한 최신 대안

사용자 파일을 OneDrive로 자동 마이그레이션

프롬프트 또는 자동 작업

구현할 때 대역폭을 염두에 두기

폴더 리디렉션 또는 지원되지 않는 파일 유형을 사용하는 경우 KFM을 사용할 수 없음



최신 마이그레이션: 업그레이드 및 마이그레이션

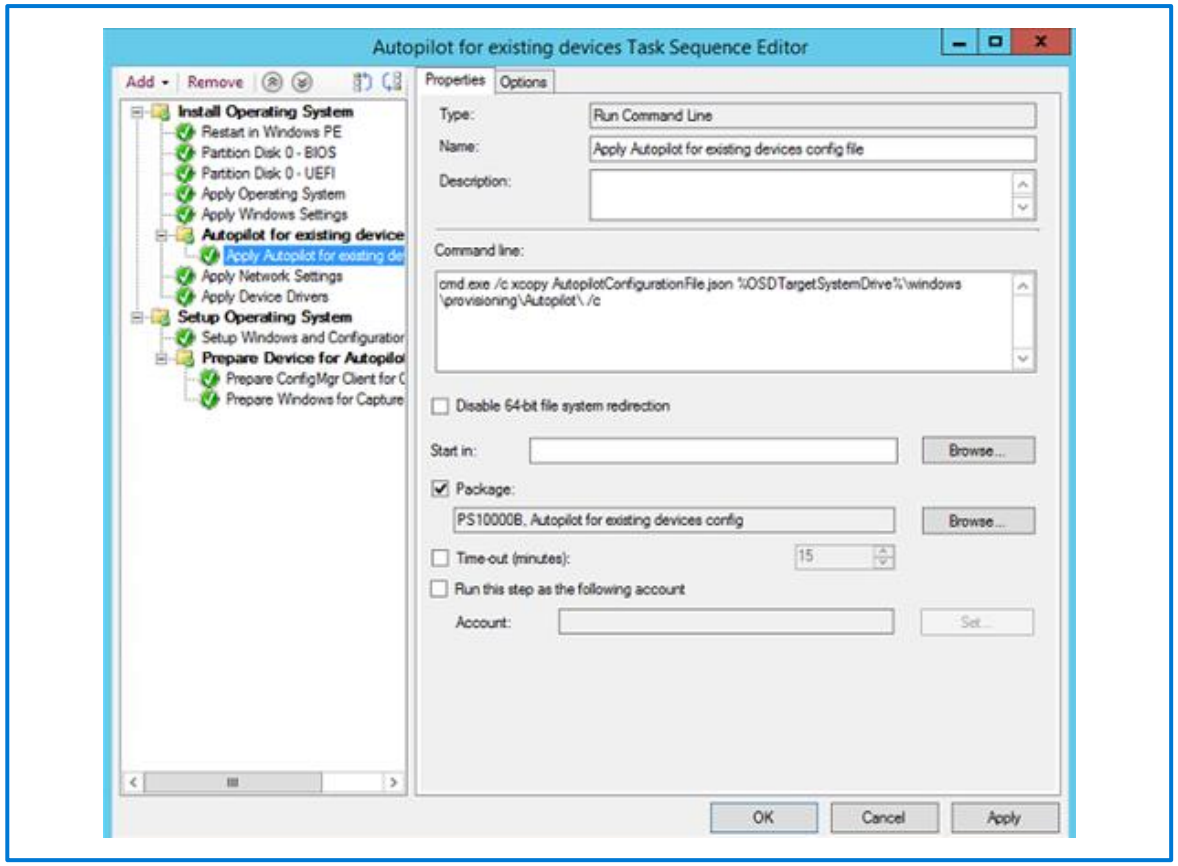
마이그레이션 고려 사항

현재 위치 업그레이드	마이그레이션
환경 유지	표준화된 환경 제공
앱을 다시 설치하거나 데이터를 전송할 필요 없음	마이그레이션 대상을 제어할 수 있음
필요한 경우 업그레이드를 롤백할 수 있음	환경 정리
특정 업그레이드 경로만 가능	앱을 다시 설치해야 함
현재 위치 Windows 10 이미지를 사용해야 함	사용자 맞춤형 Windows 10 이미지를 사용할 수 있음

현재 위치 업그레이드

기존 레거시 디바이스에 대해 Windows Autopilot으로 모던 데스크톱 배포 채택

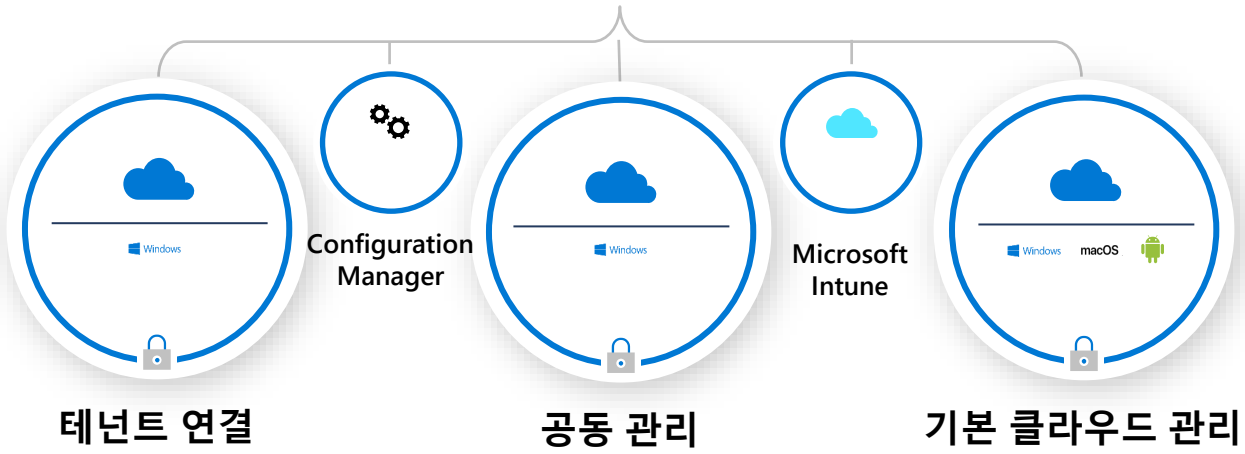
기존 도메인 조인 엔드포인트를 Azure AD 관리 디바이스로 변환하고 동일한 자동화 내에서 모두 다시 빌드



최신 마이그레이션: 워크로드 마이그레이션

클라이언트 관리를 Intune으로 마이그레이션

클라우드 관리로 마이그레이션 시작	• 최신 관리로의 마이그레이션 간소화 • 첫날부터 누리는 최신 관리의 이점 • Configuration Manager 및 Intune을 사용하여 관리되는 디바이스 • 온-프레미스 환경에 연결되지 않더라도 Intune에서 디바이스를 관리할 수 있음
소규모 또는 새 조직은 클라우드에서 시작해야 함	• Intune에서 제공하는 OS 환경 설정 기능으로 요구 사항 충족 • 애플리케이션이 최신 상태이며 상대적으로 단순한 설치 • 기존 레거시 애플리케이션이 과도하게 많지 않음 • 기존 환경 설정 관리 배포는 비교적 단순함

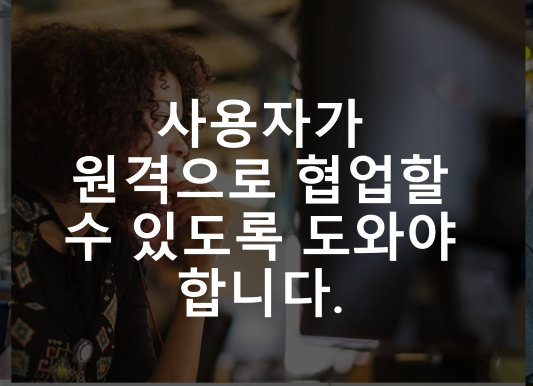


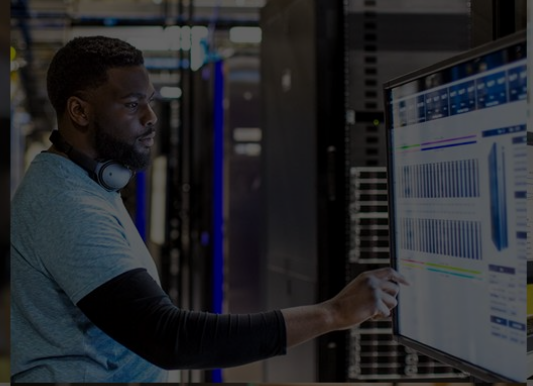
리소스

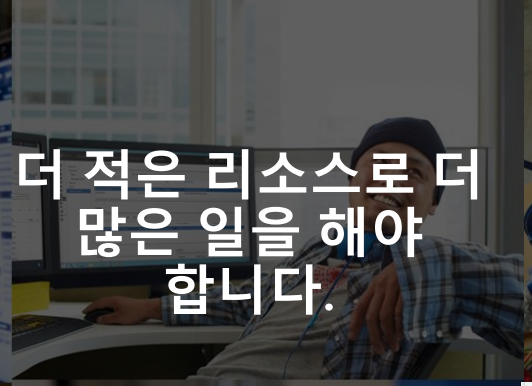
Windows Autopilot 설명서
Windows IT 관련 커뮤니티 가입
Windows IT Pro 블로그
Windows 기술 설명서
Windows 학습 과정

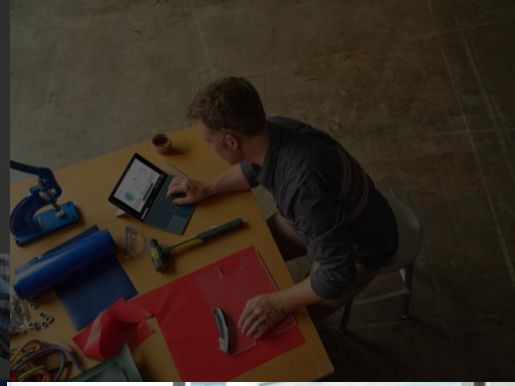
Microsoft

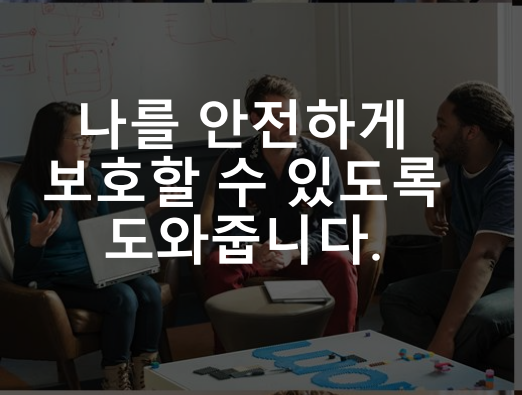
Autopilot을 통해 Surface 배포

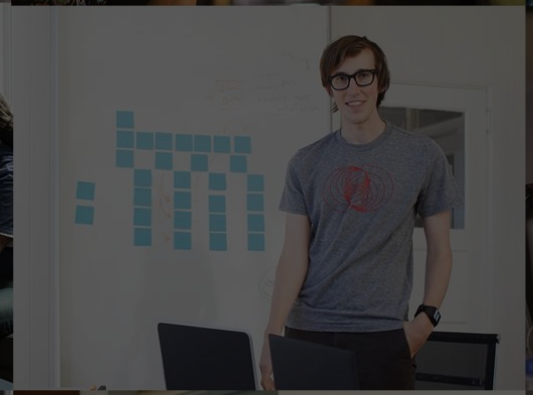

사용자가
원격으로 협업할
수 있도록 도와야
합니다.

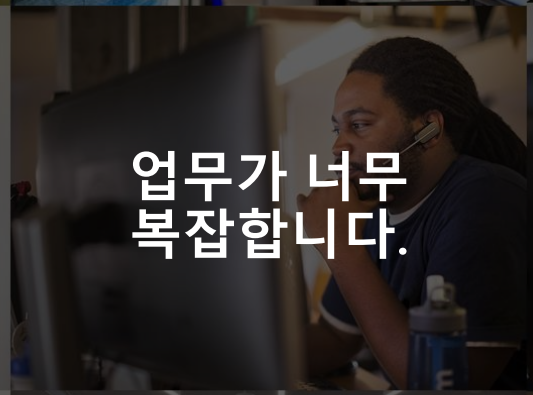


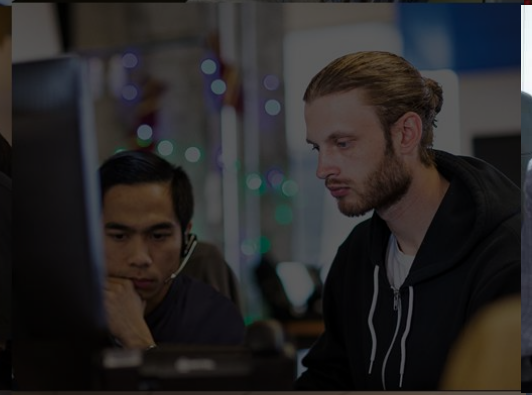

더 적은 리소스로 더
많은 일을 해야
합니다.



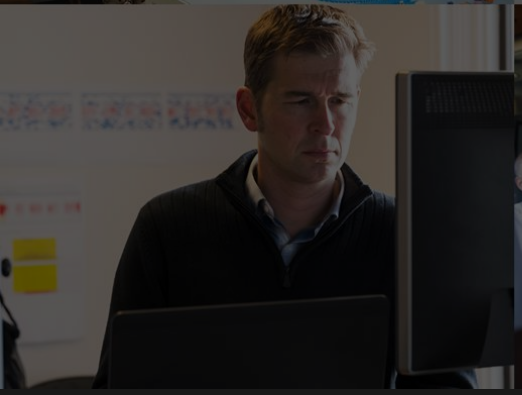

나를 안전하게
보호할 수 있도록
도와줍니다.

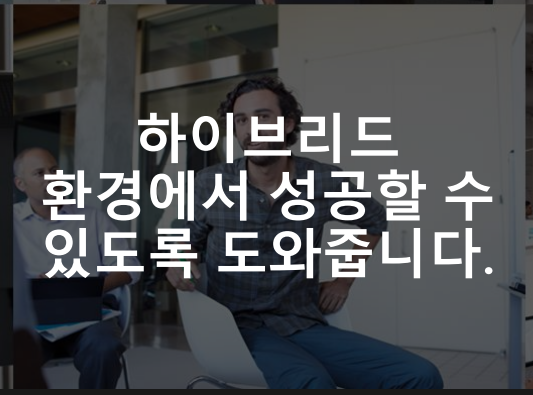


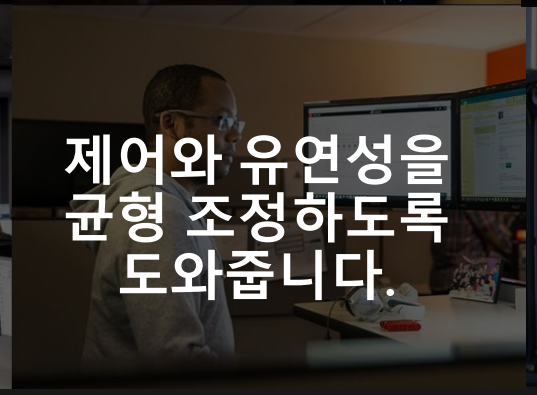

업무가 너무
복잡합니다.



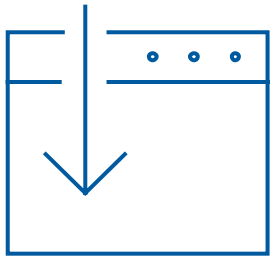

사용자에게 만족을
드리고 싶습니다.




하이브리드
환경에서 성공할 수
있도록 도와줍니다.


제어와 유연성을
균형 조정하도록
도와줍니다.

Microsoft Surface와 M365를 함께 사용하면 비용이 절감되고 복잡성이 감소되므로 IT 전문가들이 좋아합니다.

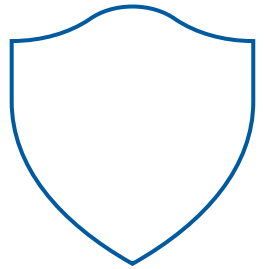


간소화

배포

완벽한 디바이스

관리

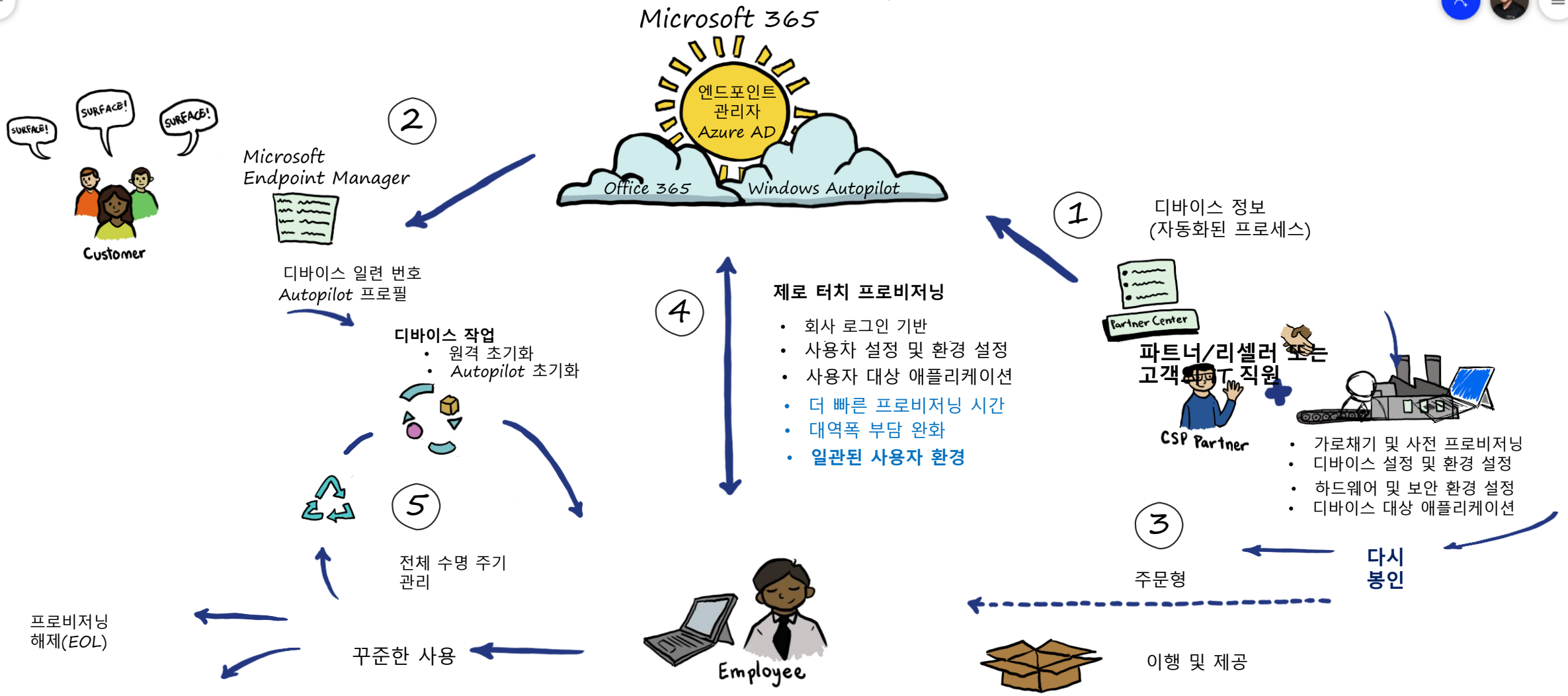


인텔리전트

보안

+보안 하드웨어

수명 주기 전반의 Surface 디바이스: Windows Autopilot 및 White Glove



Surface의 Windows Autopilot

최종 사용자는 Surface를 사용하여 즉시 생산 활동에 참여할 수 있습니다.

- OEM만 반환된 디바이스를 자동으로 등록 취소/재등록
- 파트너 채널 사용 및 준비
- 조작 가능하고 완성도가 높은 무료 영업 및 지원
- 상업용 SKU는 Office Pro Plus 및 정리된 이미지를 통해 가장 빠른 Autopilot 환경을 구축하도록 조정됩니다.
- 최신 세대 제품의 모든 상업용 SKU에 대한 PKID 및 OS 버전 번호

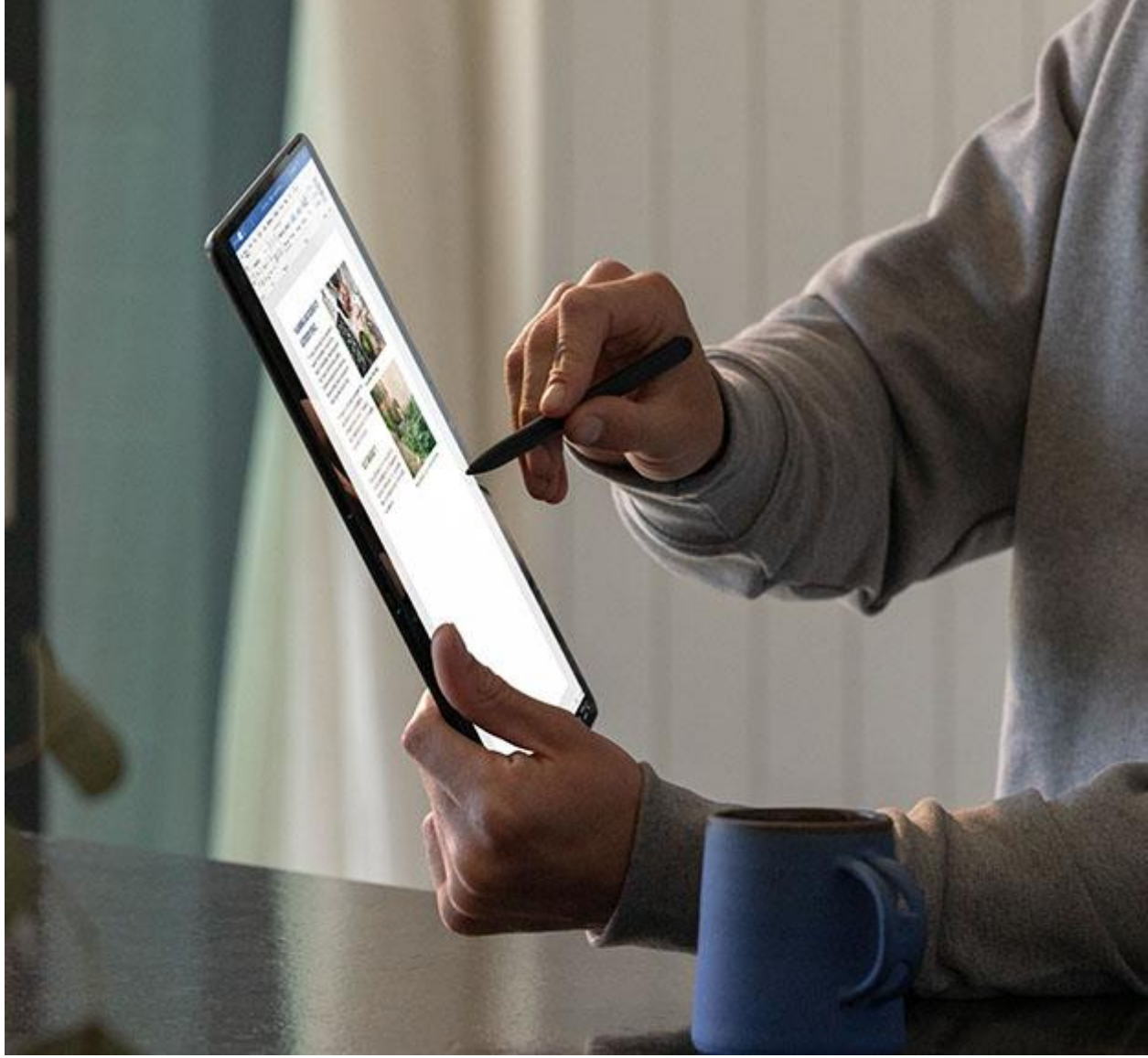
간소화된 배포

- Autopilot을 통한 제로 터치 배포
- IT 복잡성을 줄여주는 파트너 전문 지식
- 원격으로 교체하고 다시 사용하기 위한 수명 주기 전략

IT 부서에 따르면 배포된 디바이스당 **25분이** 절약된다고 합니다.[1]

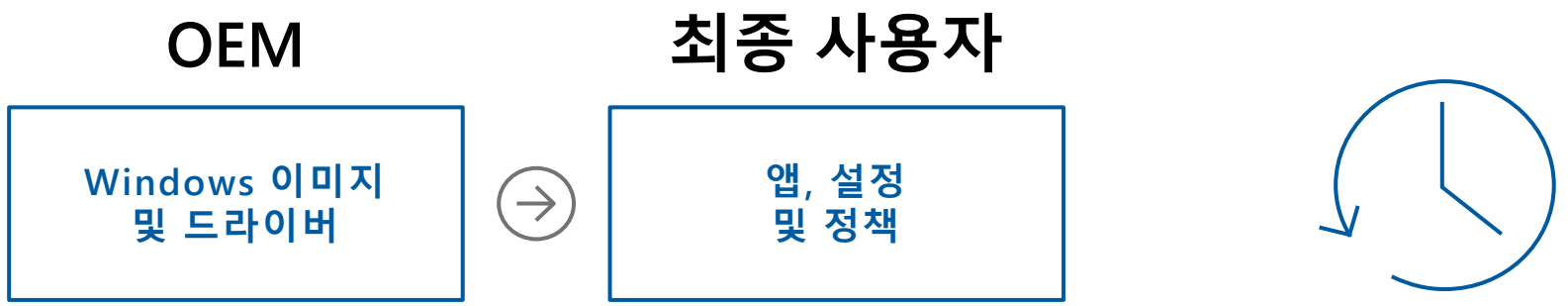
78%는 Surface 디바이스를 배포할 경우 타사 디바이스를 배포할 때에 비해 IT 시간과 비용이 절감되었다는 것에 동의합니다.[1]

[1]Forrester Total Economic Impact™ 연구:
Maximizing your ROI from Microsoft 365 Enterprise with Microsoft Surface(Microsoft Surface로 Microsoft 365 Enterprise ROI 극대화)

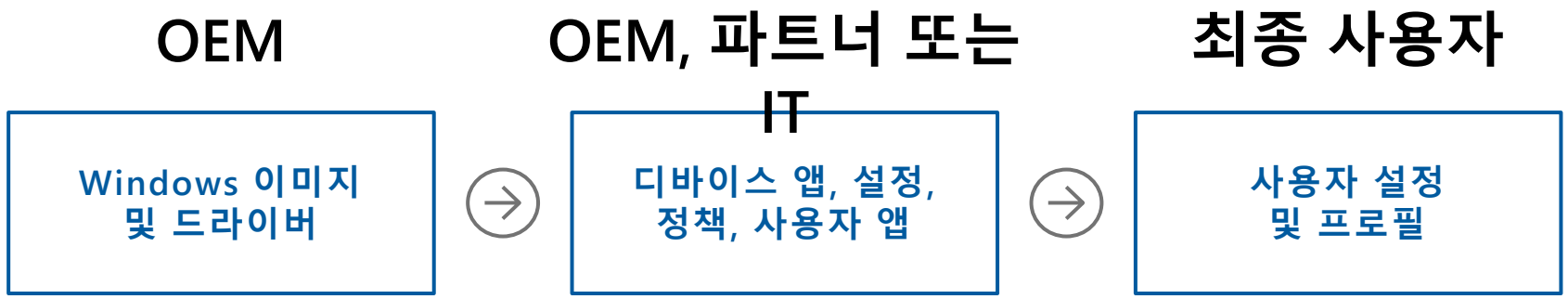


Windows Autopilot
White Glove

Autopilot:

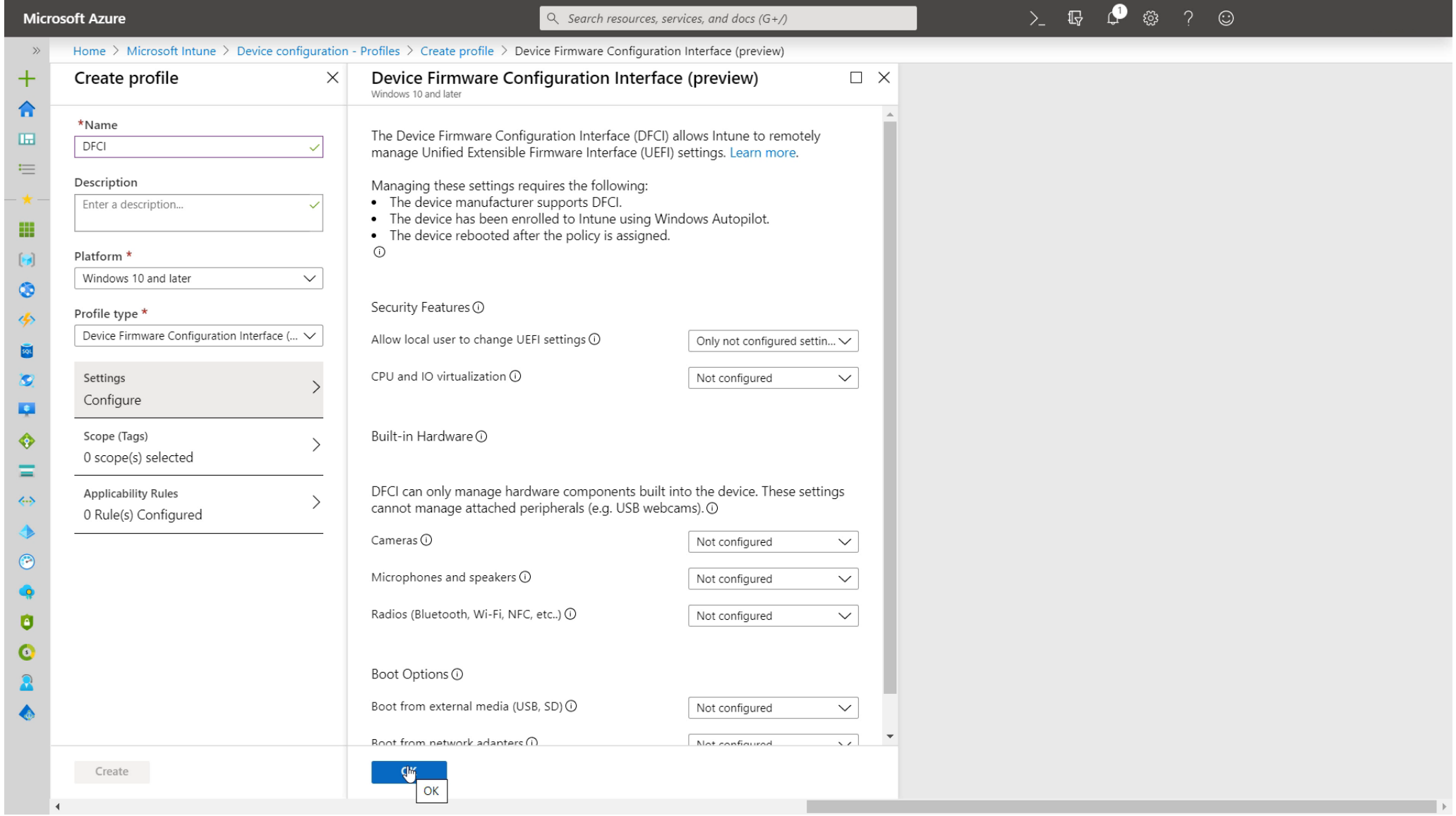


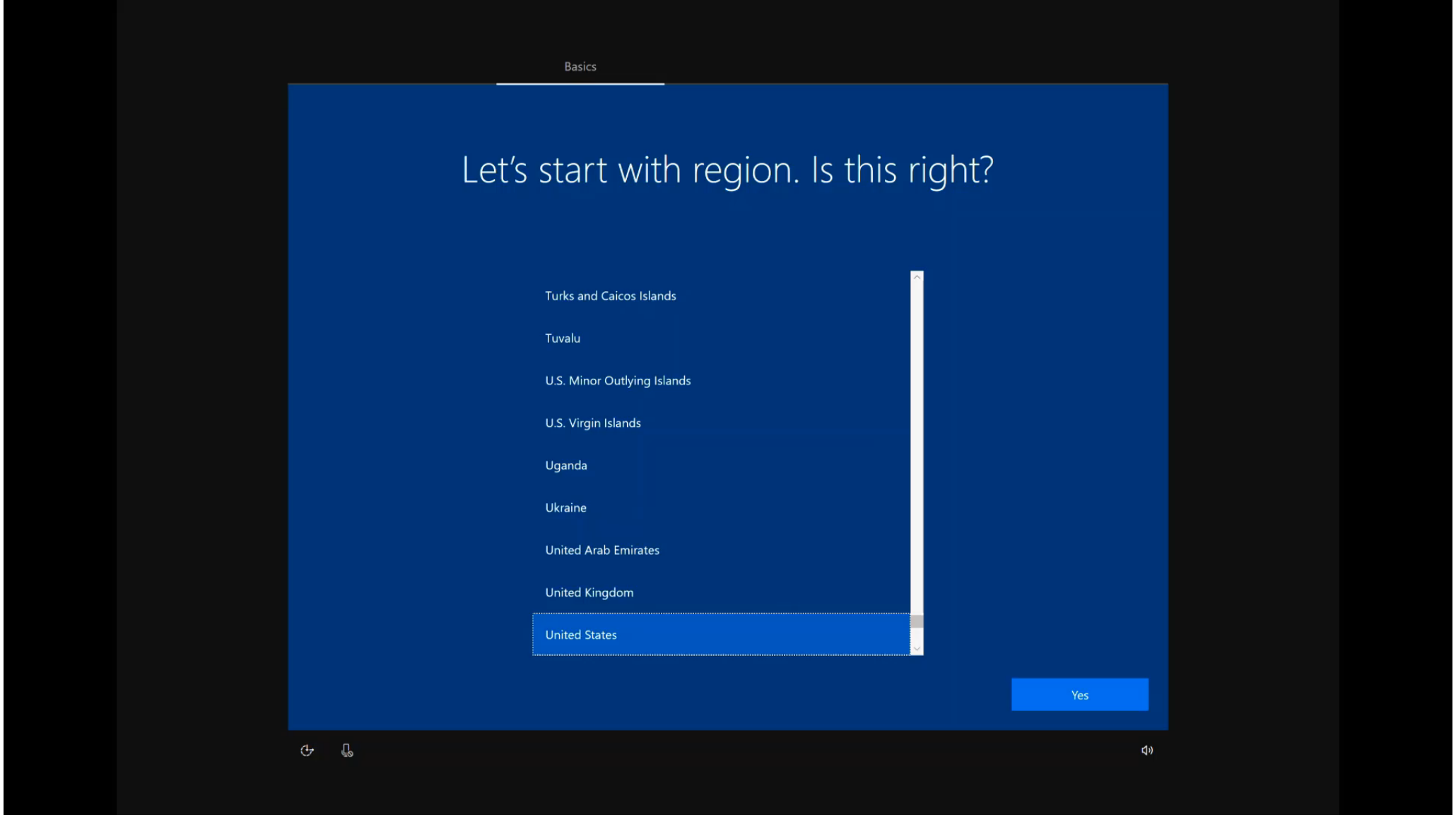
Autopilot White Glove:

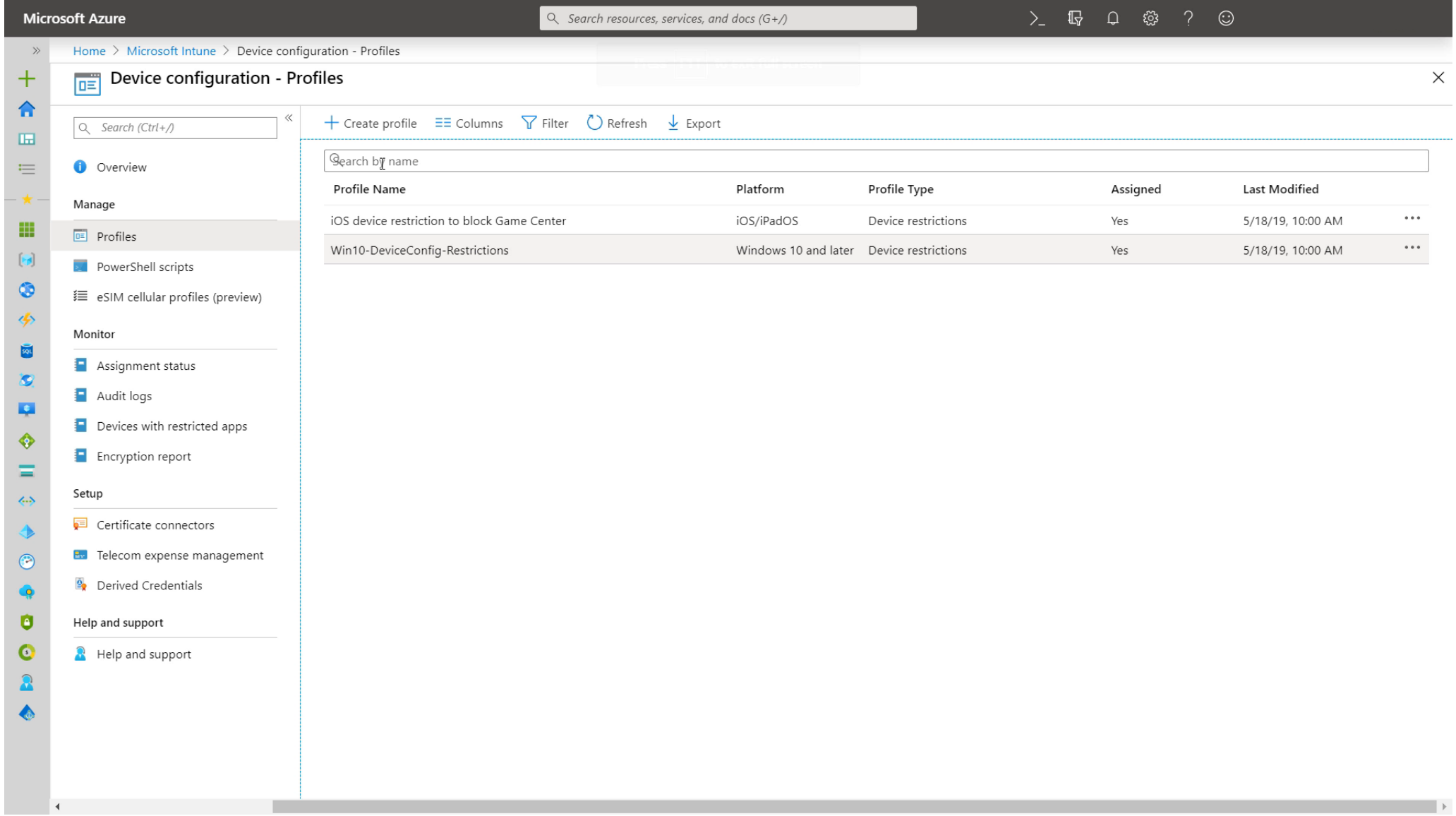


데모

DFCI, Autopilot(White Glove) -> 전체 생산성


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Intune > Device configuration - Profiles > Create profile > Device Firmware Configuration Interface (preview)
Create profile
*Name
DFCI
Description
Enter a description...
Platform *
Windows 10 and later
Profile type *
Device Firmware Configuration Interface (...
Settings
Configure
Scope (Tags)
0 scope(s) selected
Applicability Rules
0 Rule(s) Configured
Create
Device Firmware Configuration Interface (preview)
Windows 10 and later
The Device Firmware Configuration Interface (DFCI) allows Intune to remotely manage Unified Extensible Firmware Interface (UEFI) settings. Learn more.
Managing these settings requires the following:
The device manufacturer supports DFCI.
The device has been enrolled to Intune using Windows Autopilot.
The device rebooted after the policy is assigned.
Security Features
Allow local user to change UEFI settings
Only not configured settin...
CPU and IO virtualization
Not configured
Built-in Hardware
DFCI can only manage hardware components built into the device. These settings cannot manage attached peripherals (e.g. USB webcams).
Cameras
Not configured
Microphones and speakers
Not configured
Radios (Bluetooth, Wi-Fi, NFC, etc..)
Not configured
Boot Options
Boot from external media (USB, SD)
Not configured
OK


Basics
Let's start with region. Is this right?
Turks and Caicos Islands
Tuvalu
U.S. Minor Outlying Islands
U.S. Virgin Islands
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States
Yes


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Intune > Device configuration - Profiles
Device configuration - Profiles
Search (Ctrl+/)
Overview
Manage
Profiles
PowerShell scripts
eSIM cellular profiles (preview)
Monitor
Assignment status
Audit logs
Devices with restricted apps
Encryption report
Setup
Certificate connectors
Telecom expense management
Derived Credentials
Help and support
Help and support
Create profile
Columns
Filter
Refresh
Export
Search by name
Profile Name
Platform
Profile Type
Assigned
Last Modified
iOS device restriction to block Game Center
iOS/iPadOS
Device restrictions
Yes
5/18/19, 10:00 AM
Win10-DeviceConfig-Restrictions
Windows 10 and later
Device restrictions
Yes
5/18/19, 10:00 AM

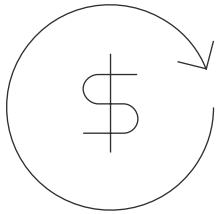
Microsoft

Surface-Chip 클라우드 보안

오늘날의 작업 공간에는 통합 보안 솔루션이 필요합니다.

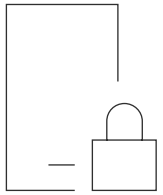
- ✓ 조직이 원격 근무를 중심으로 운영되고 있습니다.
- ✓ 현재 네트워크 인프라는 오늘날의 보안을 고려해서 구축되지 않았습니다.
- ✓ 특히 펌웨어 수준에서 대상 지정된 공격이 점점 더 정교해지고 있습니다.
- ✓ 고객은 원격 근무에 적응하면서 포괄적인 보호를 보장하기 위해 보안 계층을 추가해야 합니다.

데이터 위반 비용 증가



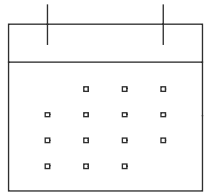
386만 달러
(USD)

전 세계 기업의 총 평균 데이터 위반 비용, 2017년 대비 6.4% 증가[1]



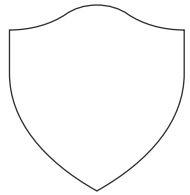
> 1,240억 달러
(USD)

2019년 전 세계적으로 정보 보안을 위한 예상 지출 비용[2]



190
일

데이터 위반을 식별하는 데 걸리는 평균 시간 [1]



100억 달러
(USD)

2027년 전 세계적으로 직원 대상 보안 인식 교육을 위한 예상 지출 비용[3]

[1]NASCIO, Ponemon Institute의 2018 데이터 위반 비용 연구, 2018년 9월. [2]Gartner, 2019년에 전 세계 정보 보안 지출이 1240억 달러(USD)를 초과할 것으로 예상, 2018년 8월. [3]https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019, 2019년 6월.

알고 계셨습니까? IT 그 이상의 보안 효과

경영진 및 재무

40%

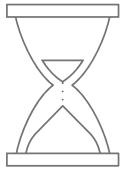
공격 후 3년이 경과한 시점에도, 침해 당한 기업의 지수는 40% 이상 낮게 나타납니다. [4]

제품 개발

96%

사이버 범죄자의 96%가 독점 IP와 같은 정보를 수집하기 위해 공격합니다. [4]

HR 및 운영



24x

평균 가동 중지 비용이 평균 랜섬웨어 금액보다 24배 높습니다. [4]

법률

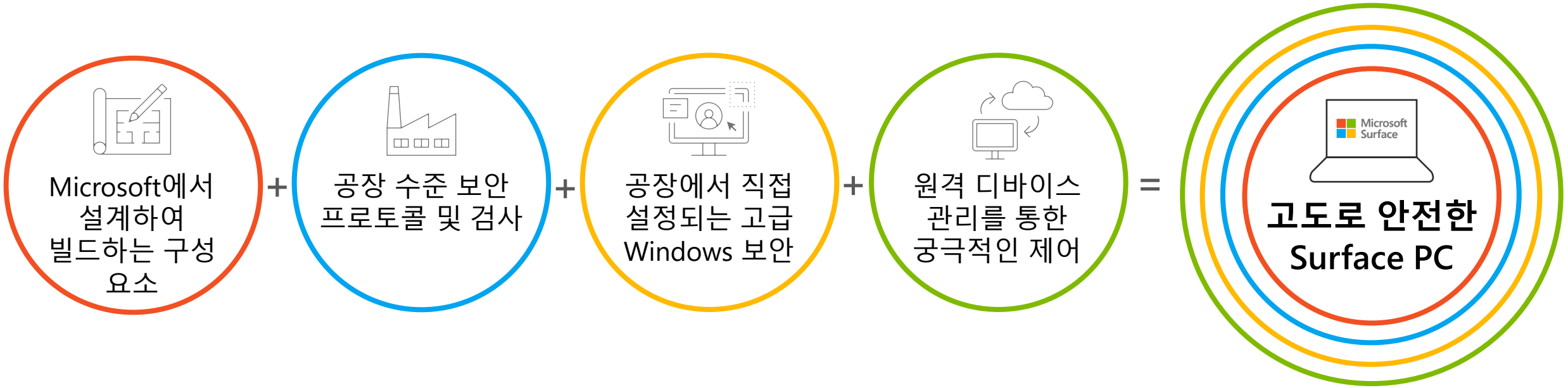
소송 및 벌금

PII를 도난당한 고객이 회사를 상대로 소송을 제기하고 규제 당국에 의해 벌금이 부과될 수 있습니다. [11]

[1] 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2020] EDITION] – Comparitech, 2020년 7월, https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[2] https://www.blackstratus.com/risk-liability-assessment/

디바이스 보호가 절실히 필요합니다.

해결책은 무엇일까요? 계층화된 보안을 채택한 Microsoft Surface를 선택하십시오.



칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안

칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안

Microsoft에서 설계하여 빌드하는 구성 요소

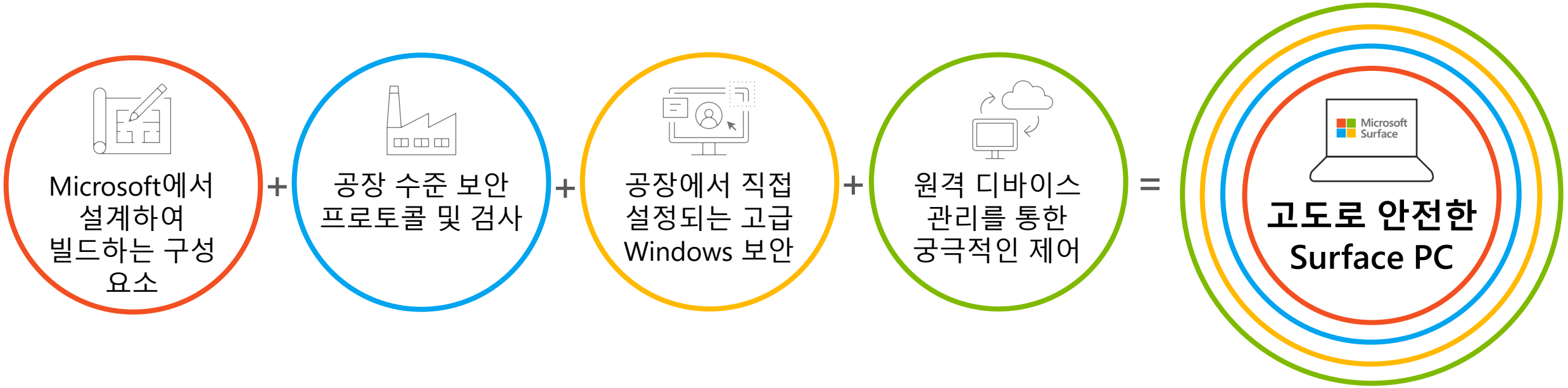
Microsoft, 부팅 보안 및 펌웨어 관리용 UEFI 빌드

데이터 보호를 보장하는 TPM 2.0 보안 프로세서

Windows 10 및 Microsoft 365 Defender 엔터프라이즈 방어 제품군, 개별 결합형보다 내장형이 우수

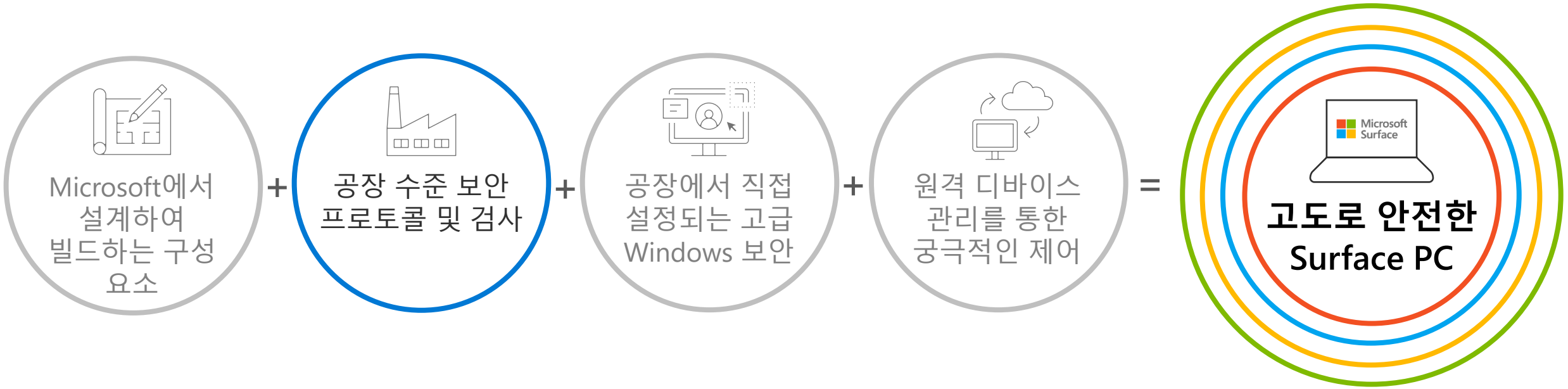
칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안



칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안



칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안

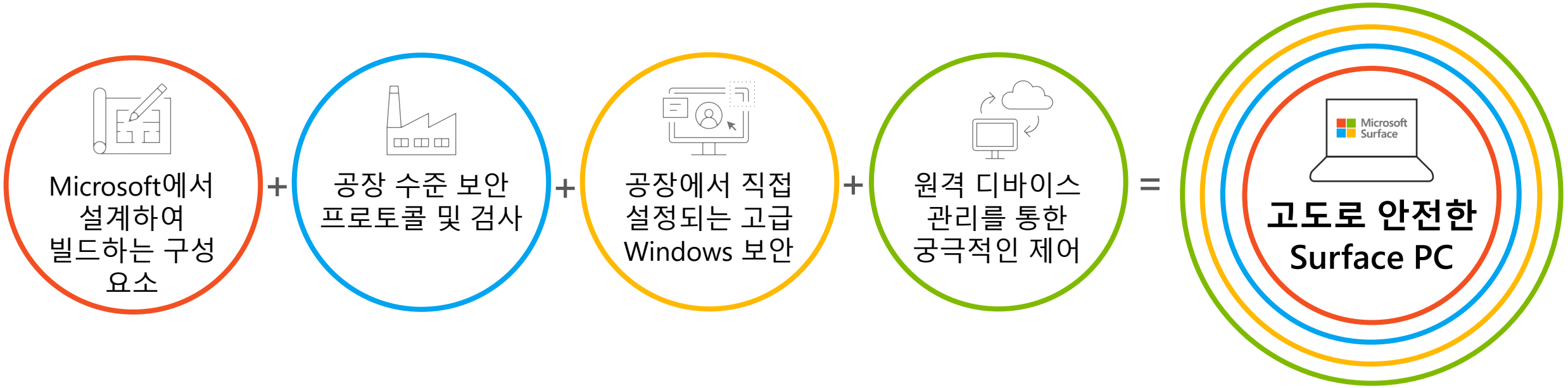
최종 조립 위치에서 구성품 검사 및 테스트

Microsoft에서 개발하고 유지 관리하는 펌웨어, 드라이버 및 OS 사용

Microsoft 리셀러까지 안전한 물류

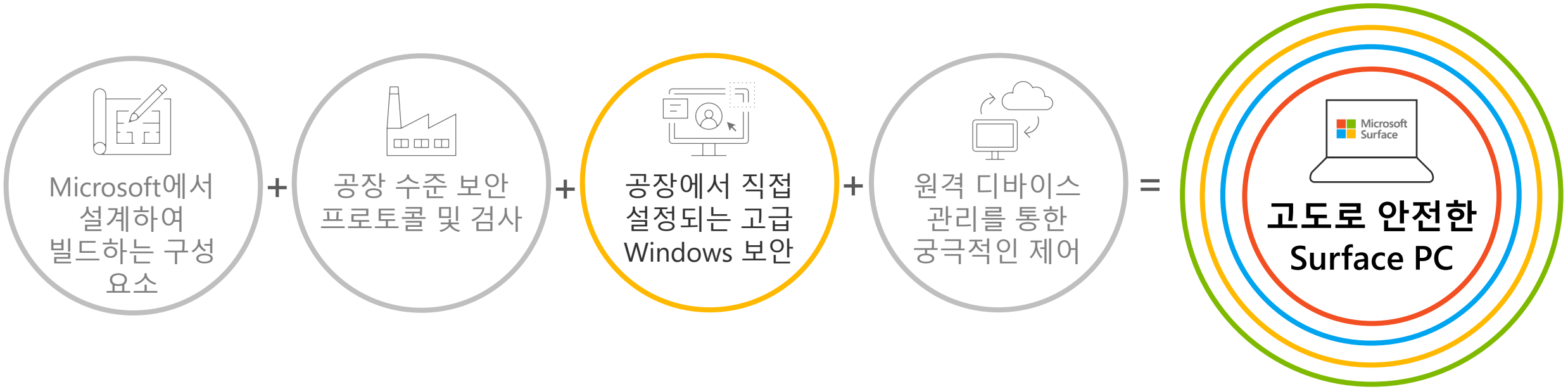
칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안



칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안



칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안

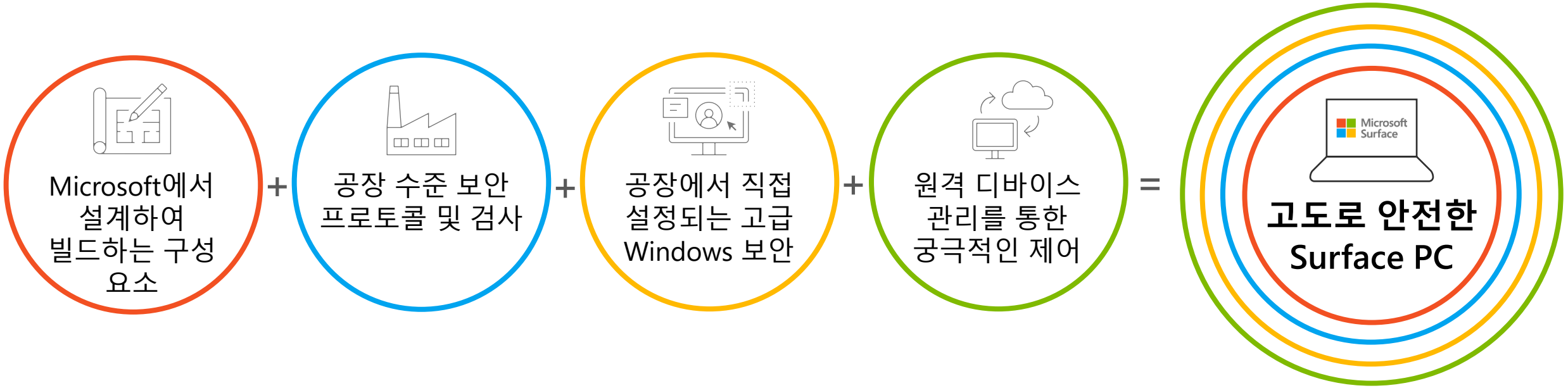
Windows 10의 코어에서
애플리케이션과 데이터를 분리하는
VBS(가상화 기반 보안)

Windows 10이 정품인지 확인하는
보안부팅 및 Boot Guard

데이터를 보호 및 암호화하는
Bitlocker, 암호 없는 로그인을
지원하는 Windows Hello

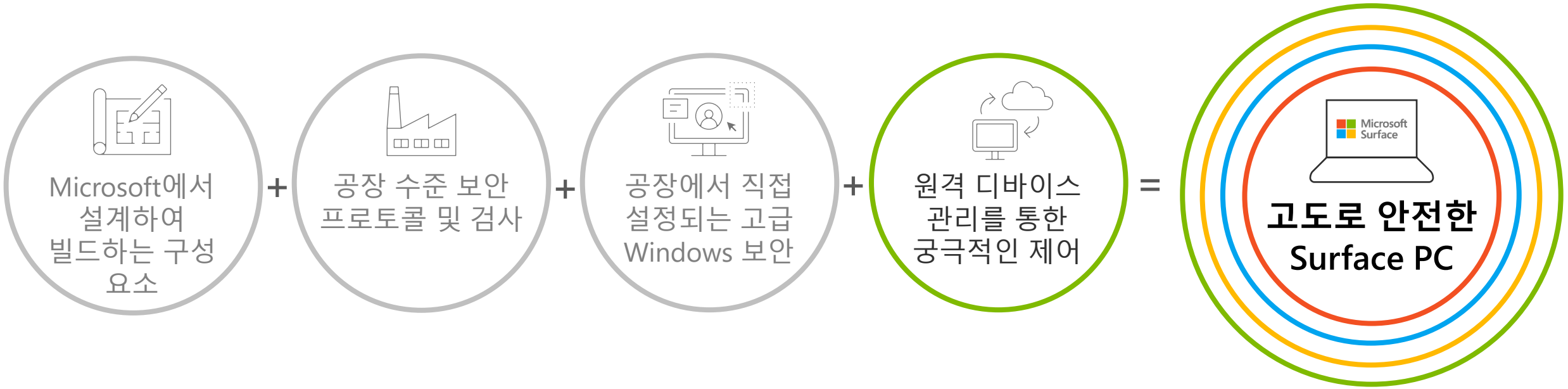
칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안



칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안



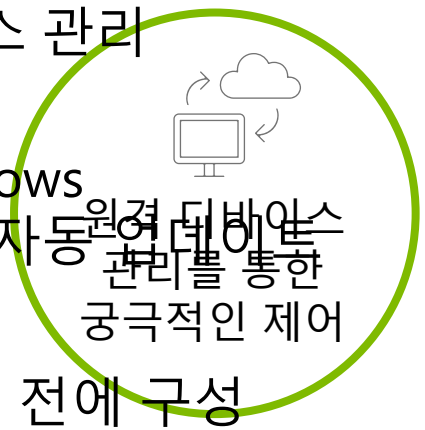
칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안

MEM(Microsoft Endpoint Manager)을 통해 클라우드에서 완벽하게 디바이스 관리

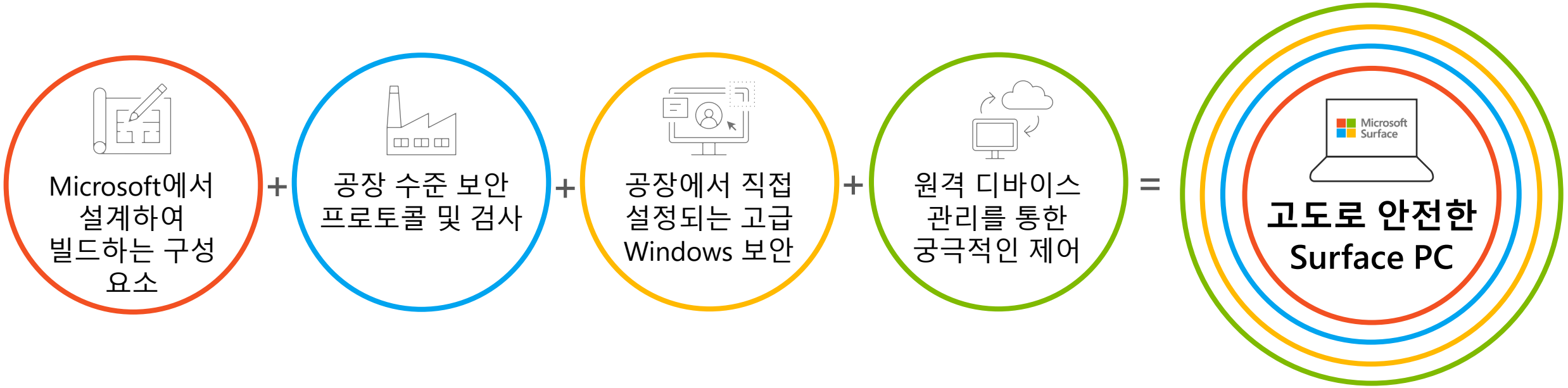
비즈니스용 Windows 업데이트를 통해 자동 업데이트

MEM을 통해 부팅 전에 구성 요소를 비활성화하는 세분화된 펌웨어 관리



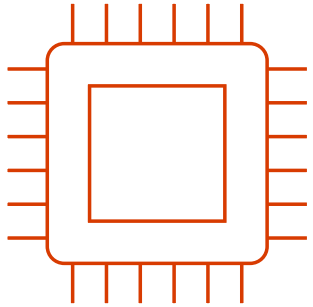
칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

심층 방어: Surface를 통해 계층화된 보안



칩부터 클라우드까지 Surface의 모든 계층은 Microsoft에 의해 개발되고 유지 관리되므로 궁극적인 제어와 사전 예방적 보호가 가능하고 어디서나 어떤 방식으로든 안심하고 작업할 수 있습니다.

펌웨어 방어가 중요한 이유



"2022년까지 펌웨어 업그레이드 계획이 없는 조직의 70%가 펌웨어 취약성으로 인해 공격을 당할 것입니다."

- Gartner

2018년 1월
모든 x86, PowerPC 및 엄선된 ARM 디바이스의 프로세서 수준에 존재하는 스펙터 및 멜트다운 취약성

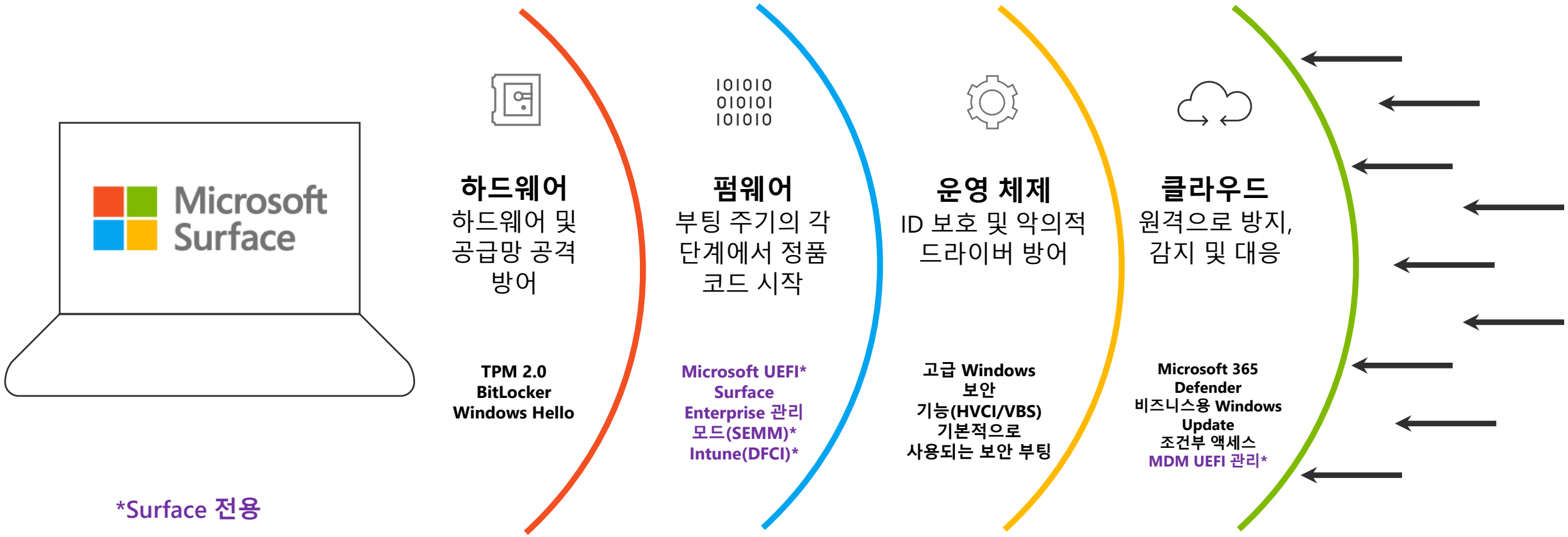
2019년 1월
ASUS 펌웨어에 대한 ShadowHammer 공급망 공격에 100만 개 미만의 디바이스 감염

2020년 9월
MosaicRegressor가 UEFI를 겹쳐 쓰고 스파이 행위 및 데이터 유출에 사용되는 부트킷으로 확인되었습니다.

2020년 9월
미국 국가안보국(NSA)에서 UEFI/펌웨어에 대한 보안 부팅과 보호를 권장하는 기술 보고서를 발행했습니다.

2020년 12월
Trickbot 맬웨어가 UEFI 취약성을 대상으로 지정하여 펌웨어를 덮어쓰고 OS를 부트킷으로 도용하기 시작했습니다.

칩-클라우드 보안이 Surface DNA에 내장되어 있습니다.



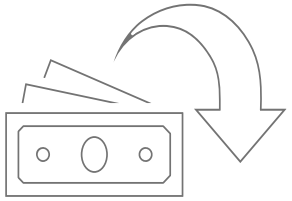
*Surface 전용

Microsoft 365 기반 Surface 디바이스로 위험을 줄이고 비용 절감

20%↓

Surface 사용자의

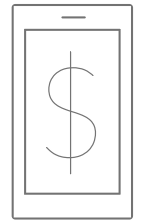
보안 위반 감소



17%↓

엔드포인트 보안

지출 감소



14%↓

모바일 디바이스

관리 비용 감소

***출처**: Microsoft를 대신하여 Forrester Consulting에서 실시한 위탁 Total Economic Impact™ 연구, 2020년 7월. "Maximizing Your ROI from Microsoft 365 Enterprise With Microsoft Surface(Microsoft Surface를 통해 Microsoft 365 Enterprise ROI 극대화)"*

Surface 보안: 엔드포인트 보안의 최적 기준

- ✓ Windows에 내장된 강화 하드웨어 보안 기능을 사용하여 악성 코드로부터 보호할 수 있습니다.
- ✓ 완벽한 클라우드 기반 디바이스 관리와 OS에서 펌웨어로의 업데이트를 통해 IT 복잡성 감소
- ✓ 보안 프로세서 보호: BitLocker(데이터 보호 및 암호화), Windows Hello(암호 없는 로그인)
- ✓ Microsoft, 펌웨어 및 Windows 10의 신뢰성 확인을 위한 오픈 소스 UEFI(BIOS) 작성

Microsoft Surface 및 보안 코어 PC

접근 방식은 다르지만 동일한 결과: Microsoft의 동급 최강 엔드포인트 보안

	Surface 디바이스	보안 코어 PC
하드웨어 신뢰 루트로 보호	✓	✓
펌웨어 수준 공격 방어	✓	✓
확인되지 않은 코드에 대한 액세스 방지	✓	✓
외부 위협으로부터 ID 보호	✓	✓

Microsoft Surface 및 보안 코어 PC

접근 방식은 다르지만 동일한 결과: Microsoft의 동급 최강 엔드포인트 보안

	하드웨어 신뢰 루트로 보호	펌웨어 수준 공격 방어	확인되지 않은 코드에 대한 액세스 방지	외부 위협으로부터 ID 보호
Surface 디바이스	☑ Surface의 신뢰 루트는 각 단계에서 서명과 측정을 검사하여 다음 부팅 단계로 진행하기 전에 각 단계가 안전하고 신뢰할 수 있는지 엄격하게 확인합니다.	☑ Microsoft는 서드파티 소스 코드에 의존하지 않고 펌웨어를 처음부터 끝까지 직접 빌드합니다. 따라서 Microsoft는 지속적인 업데이트를 제공하여 펌웨어 수준까지 최신 위협으로부터 보호할 수 있습니다.	☑ HVCI(하이퍼바이저 코드 무결성)를 사용하여 Windows 10 디바이스를 확인되지 않은 코드로부터 보호합니다. 신뢰할 수 있는 컴퓨팅 베이스 내에서 실행되는 코드는 무결점으로 운영되며 익스플로잇 또는 공격의 대상이 되지 않습니다.	☑ Windows Hello[2]를 통해 외부 위협으로부터 ID를 보호합니다. Credential Guard는 보안 환경에서 ID 및 도메인 개인 인증 정보를 격리하고 보호합니다.
보안 코어 PC	☑ 선도적 PC 제조업체 및 실리콘 공급업체와 협력하여 보안 코어 PC에서는 업계 표준 하드웨어 신뢰 루트를 최신 CPU에 내장된 보안 기능과 함께 사용합니다.	☑ 보안 코어 PC에서는 최신 CPU의 하드웨어 기반 보안을 사용하여 시스템을 신뢰할 수 있는 상태로 실행함으로써 지능형 맬웨어가 시스템을 변조하고 펌웨어 수준에서 공격하는 것을 방지합니다.		

Surface 보안 사양

보안 기능	W10 O/S 기능	Surface + OEM	Surface 전용	이는 무엇을 의미합니까?
사용자 지정 빌드된 UEFI			예 [1]	표준 기본 입/출력 시스템(BIOS)을 더 빠른 시동과 향상된 보안을 포함한 새로운 기능으로 대체합니다. 서드파티의 개입 없이 Microsoft에서 구축한 UEFI(통합형 확장 펌웨어 인터페이스)를 사용하면 디바이스의 하드웨어 제어 성능이 크게 향상되고 반응 시간이 단축됩니다. [1]
DCFI(디바이스 펌웨어 환경 설정 인터페이스)			예 [2]	제로 터치 디바이스 프로비저닝을 통해 클라우드 스케일 원격 펌웨어 관리를 제공합니다. Microsoft의 자체 UEFI를 사용하면 더 강력한 DCFI를 구현하여 조직에서 하드웨어 요소를 비활성화하고 Intune을 통해 UEFI를 원격으로 잠글 수 있습니다. [1]
보호된 DMA 액세스			예	이동식 SSD 또는 외부 스토리지 디바이스 사용과 관련된 잠재적 보안 취약성을 완화합니다. 최신 Surface 디바이스는 기본적으로 DMA 보호 기능이 설정된 상태로 제공됩니다.
Surface 데이터 지우개			예	Surface 디바이스에서 데이터를 안전하게 지우기 위해 부팅 가능한 USB 도구를 제공합니다.
SEMM(Surface Enterprise 관리 모드)			예	온-프레미스, 하이브리드 및 클라우드 환경에서 UEFI 펌웨어 설정의 중앙 집중식 엔터프라이즈 참여를 지원합니다.[1]
이동식 SSD		예	예 [3]	조직에서 데이터를 보호하고 데이터 보존 정책을 준수하도록 도와줍니다.
물리적 TPM 2.0		예		물리적 개별 TPM 2.0 칩을 사용하여 암호, PIN 번호 및 인증서를 저장하기 위한 안전한 샌드박스 환경을 구현합니다.
BitLocker	예	예	예	물리적 TPM 및 UEFI와 결합하여 크게 개선되고 통합된 암호화 솔루션을 제공합니다.

[1] Surface Go 및 Surface Go 2는 서드파티 UEFI를 사용하며 DFCI를 지원하지 않습니다. DFCI는 현재 Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7 및 Surface Pro X에서 사용할 수 있습니다. Surface UEFI 설정 관리에 대해 자세히 알아보십시오.
[2] DFCI는 현재 Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7 및 Surface Pro X에서 사용할 수 있습니다. Surface UEFI 설정 관리에 대해 자세히 알아보십시오.
[3] Surface Laptop 3, Surface Laptop Go 및 Surface Pro X에서 사용 가능한 이동식 SSD 3, 하드 드라이브는 반드시 숙련된 기술자가 Microsoft 지침에 따라 탈착해야 합니다. 하드 드라이브를 교체하면 손상 또는 안전 위험이 발생할 수 있으므로 권장되지 않습니다.

Surface 보안 사양*(계속)*

보안 기능	W10 O/S 기능	Surface + OEM	Surface 전용	이는 무엇을 의미합니까?
비즈니스용 Windows Hello	예	예	예	PC 및 모바일 디바이스에서 암호를 강력한 2단계 인증으로 바꾸십시오. 이 인증은 디바이스에 연결되고 생체 인식 또는 PIN을 사용하는 새로운 유형의 사용자 개인 인증 정보로 환경 설정됩니다.
보안 부팅	예	예	예	UEFI 및 TPM 2.0에서 사용하도록 설정하면 서명되고 측정되고 올바르게 구현된 코드만 Surface 디바이스에서 실행될 수 있습니다.
Microsoft Defender with Endpoint	예	예	배송 사용	엔터프라이즈 네트워크가 지능형 위협을 예방, 감지, 조사 및 대응할 수 있도록 설계된 엔터프라이즈 엔드포인트 보안 플랫폼을 제공합니다.
Windows Defender Credential Guard	예	예	배송 사용	주요 시스템과 사용자 기밀을 격리하고 강화하여 사용자 개인 인증 정보에 대한 공격을 수행하기가 훨씬 어려워집니다.
Windows Defender Application Control	예	예	배송 사용	컴퓨터를 맬웨어로부터 강화하여 악성 코드를 방지합니다. 이전에 안전한 것으로 확인되지 않은 코드는 실행할 수 없습니다.

[1] Surface Go 및 Surface Go 2는 서드파티 UEFI를 사용하며 DFCI를 지원하지 않습니다. DFCI는 현재 Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7 및 Surface Pro X에서 사용할 수 있습니다. Surface UEFI 설정 관리에 대해 자세히 알아보십시오.
[2] DFCI는 현재 Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7 및 Surface Pro X에서 사용할 수 있습니다. Surface UEFI 설정 관리에 대해 자세히 알아보십시오.
[3] Surface Laptop 3, Surface Laptop Go 및 Surface Pro X에서 사용 가능한 이동식 SSD 3, 하드 드라이브는 반드시 숙련된 기술자가 Microsoft 지침에 따라 탈착해야 합니다. 하드 드라이브를 교체하면 손상 또는 안전 위험이 발생할 수 있으므로 권장되지 않습니다.

Surface는 칩부터 클라우드까지 보호됩니다.

- **칩 수준부터 클라우드까지 안전하게 관리**
  - 각각 다른 역할을 하는 실리콘, 펌웨어, OS 및 클라우드 서비스
- **심층 방어**
- **독립적 방어 하위 구성 요소 계층화**

칩부터

- UEFI(TPM 2.0 포함)
- SEMM
- 보안 부팅
- BitLocker
- MDM UEFI 관리
- Windows Hello

클라우드까지

- 고급 Windows 보안 기능
- 조건부 액세스
- 비즈니스용 Windows Update
- Microsoft Defender ATP
- Intune 초기화 및 사용 중지

보안 부팅

신뢰할 수 있는 OS만 부팅하는 보안 표준

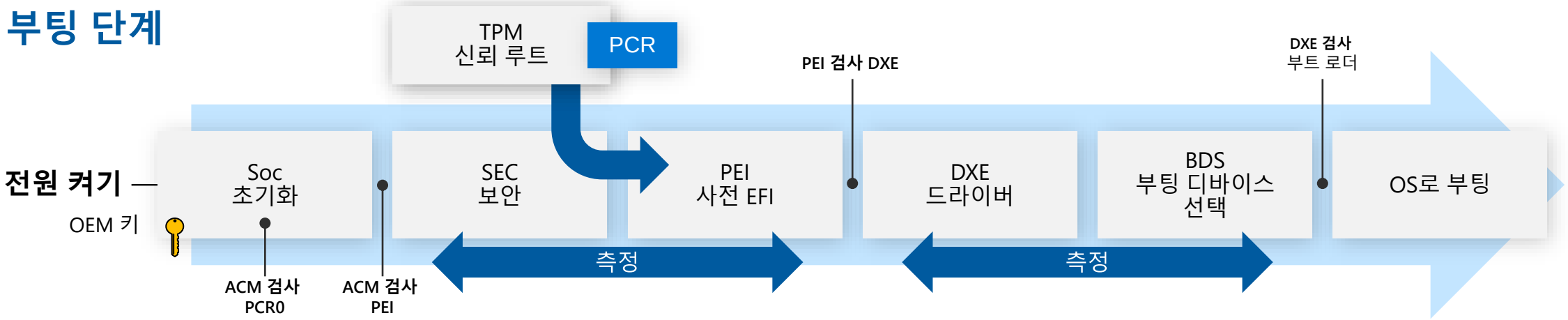
신뢰 체인

- HW에 고정된 신뢰 루트
- 각 단계에서 다음을 확인합니다.
- Boot Guard, 보안 부팅

보안 구성 요소

- SoC 보안 프로세서 - 공급업체 및 OEM 키
- TPM 2.0 - 보안 프로세서
  - 암호화 엔진
  - 키
  - 측정
  - VMK(BitLocker)

부팅 단계



Surface 펌웨어

Surface에서 펌웨어 빌드

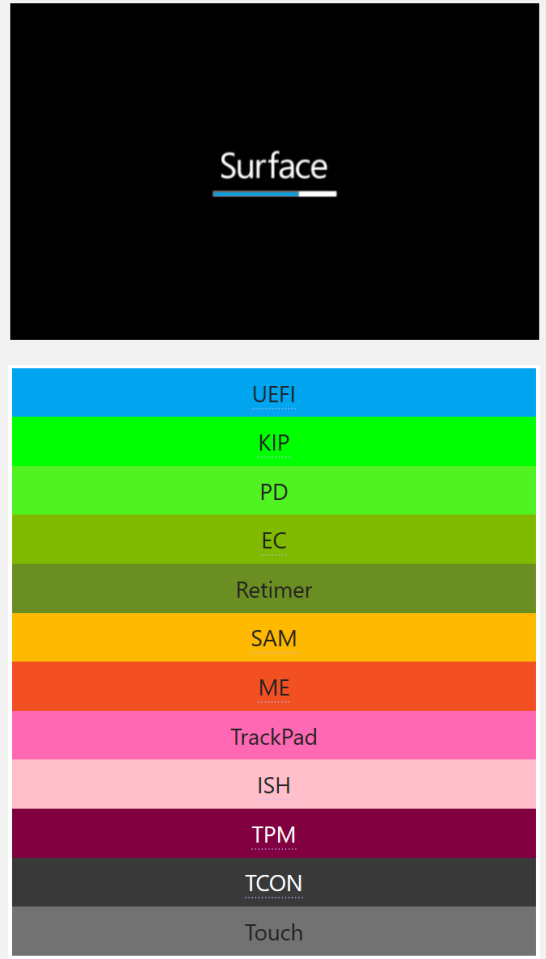
- Surface에서 UEFI/컨트롤러/센서/SoC 펌웨어 빌드
- Windows의 UEFI 프로젝트 Mu
  오픈 소스 기반 Surface UEFI
- 공급망 공격 완화

A-B 업데이트 메커니즘

- 손상된 업데이트로부터 보호

Windows 업데이트를 통해 FW를 최신 상태로 유지

- Windows 서명 드라이버를 통해 캡슐 업데이트 래핑
- Surface 서명 캡슐 업데이트
- UEFI를 통해 FW 업데이트 페이로드 적용
- 컬러 진행률 표시줄은 업데이트 중인 FW를 나타냅니다.



Surface Enterprise Management Mode

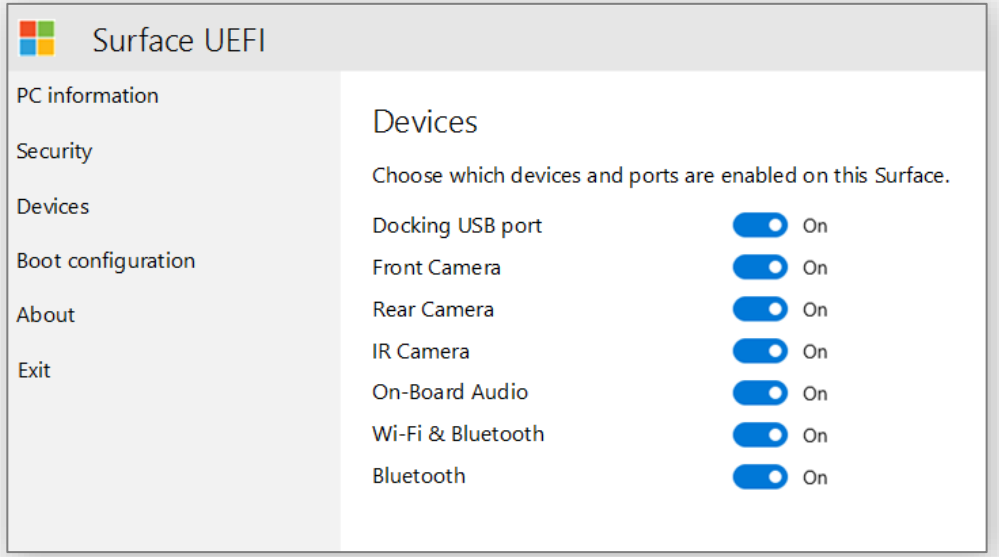
볼륨 배포를 위한 UEFI 소프트웨어 도구

UEFI 펌웨어 환경 설정 보호 및 관리

독립 실행형 도구 또는 SCCM과 통합

개별 구성 요소, 부팅 순서 및 고급 설정 관리

- 디바이스 비활성화 및 잠금(드릴링 없음!)
- UEFI 전면 페이지 잠금



Intune/MDM을 통한 SEMM
의 DFCI/Cloud UEFI 관리 기능

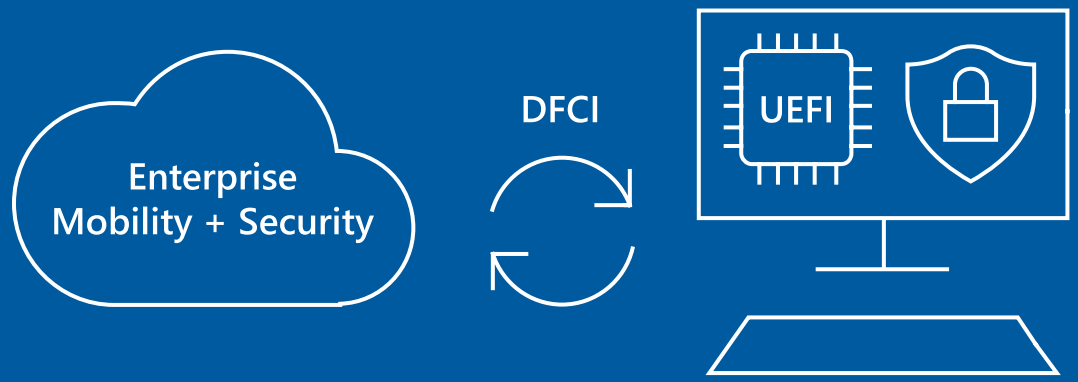
제로 터치 디바이스 프로비저닝을 통한 클라우드 스케일 원격 펌웨어 관리

BIOS 암호 제거, 보안 설정 제어(부팅 옵션 및 내장된 주변 장치 포함)

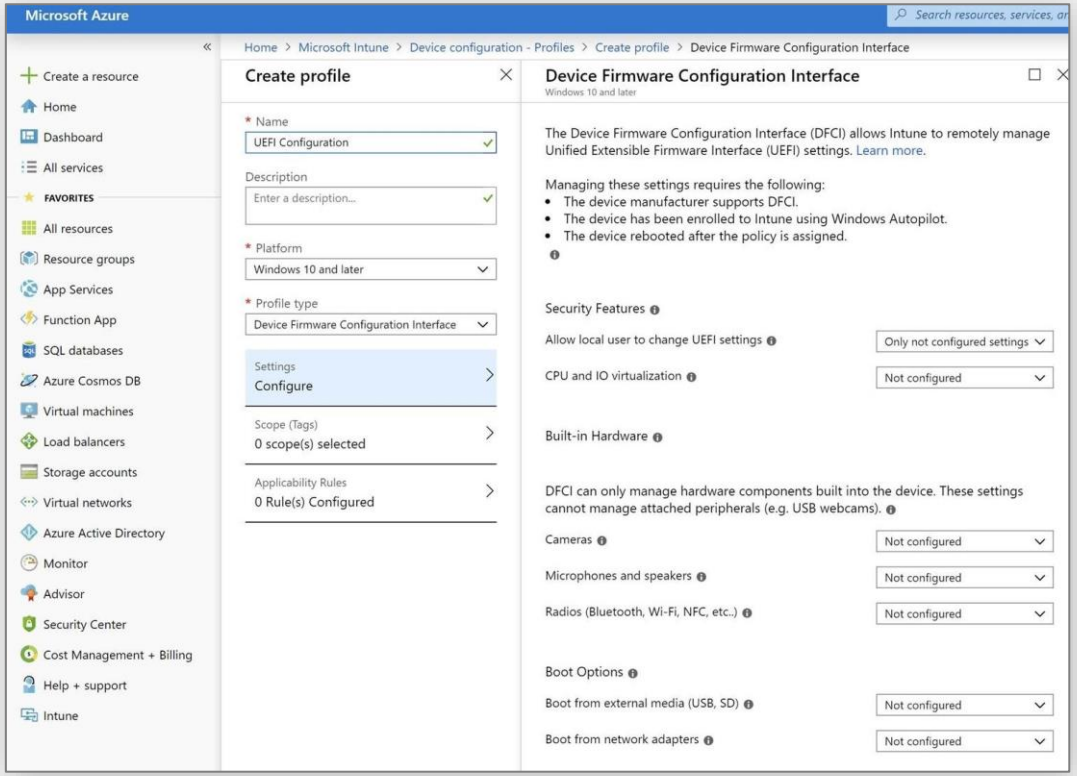
향후 고급 보안 시나리오의 토대 구축

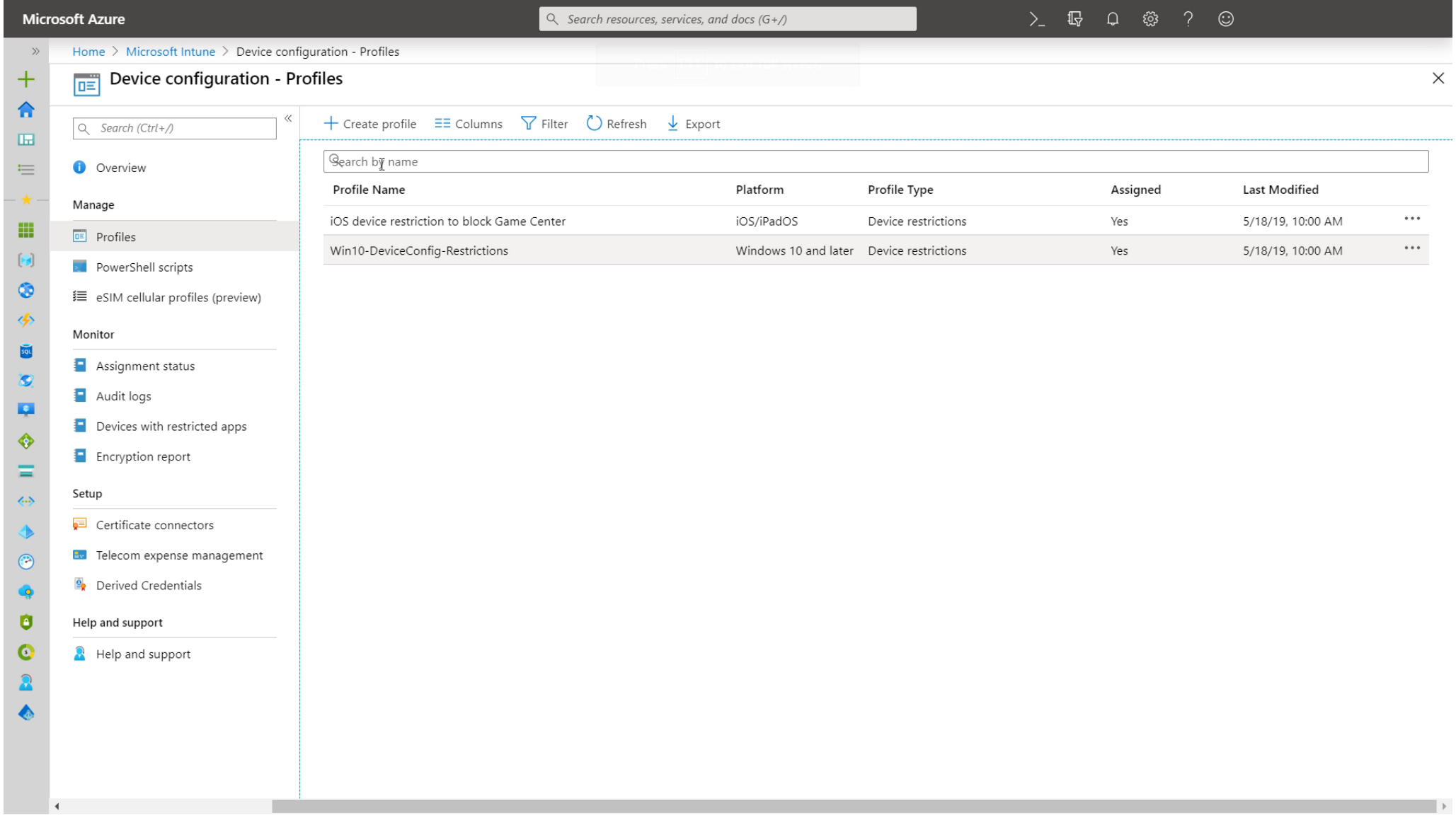
BRK2362 – Ignite Online
Microsoft Intune을 통해 Surface UEFI BIOS 설정 관리

Surface에서 먼저 구현됨



DFCI 라이브 데모


Microsoft Azure
Search resources, services, ar
Home > Microsoft Intune > Device configuration - Profiles > Create profile > Device Firmware Configuration Interface
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Intune
Create profile
* Name
UEFI Configuration
Description
Enter a description...
* Platform
Windows 10 and later
* Profile type
Device Firmware Configuration Interface
Settings
Configure
Scope (Tags)
0 scope(s) selected
Applicability Rules
0 Rule(s) Configured
Device Firmware Configuration Interface
Windows 10 and later
The Device Firmware Configuration Interface (DFCI) allows Intune to remotely manage Unified Extensible Firmware Interface (UEFI) settings. Learn more.
Managing these settings requires the following:
The device manufacturer supports DFCI.
The device has been enrolled to Intune using Windows Autopilot.
The device rebooted after the policy is assigned.
Security Features
Allow local user to change UEFI settings
Only not configured settings
CPU and IO virtualization
Not configured
Built-in Hardware
DFCI can only manage hardware components built into the device. These settings cannot manage attached peripherals (e.g. USB webcams).
Cameras
Not configured
Microphones and speakers
Not configured
Radios (Bluetooth, Wi-Fi, NFC, etc.)
Not configured
Boot Options
Boot from external media (USB, SD)
Not configured
Boot from network adapters
Not configured


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Intune > Device configuration - Profiles
Device configuration - Profiles
Search (Ctrl+/)
Overview
Manage
Profiles
PowerShell scripts
eSIM cellular profiles (preview)
Monitor
Assignment status
Audit logs
Devices with restricted apps
Encryption report
Setup
Certificate connectors
Telecom expense management
Derived Credentials
Help and support
Help and support
Create profile
Columns
Filter
Refresh
Export
Search by name
Profile Name
Platform
Profile Type
Assigned
Last Modified
iOS device restriction to block Game Center
iOS/iPadOS
Device restrictions
Yes
5/18/19, 10:00 AM
Win10-DeviceConfig-Restrictions
Windows 10 and later
Device restrictions
Yes
5/18/19, 10:00 AM

BitLocker

드라이브를 암호화하여 데이터 및 OS 보호

OOBE 중에 자동 디바이스 암호화가 사용하도록 설정되는 경우:

- TPM이 있는 경우
- 보안 부팅을 사용 가능으로 설정한 경우

Bitlocker 복구

- 보안 및/또는 부팅 변경이 이루어진 경우

이동식 SSD

- DMA 다시 매핑 보호

비즈니스용 Windows Hello

Surface에서는 암호를 강력한 2단계 인증으로 대체합니다.

신뢰할 수 있는 인증

- 얼굴 인식
- 지문 인식
- 강력한 디바이스 기반 PIN

OOBE 중에 저장된(암호화된) 암호 또는 PIN과 결합

생체 인식이 올바르면 TPM 키를 잠금 해제하여 PIN에 액세스하고 로그인 허용

고급 Windows 보안 기능

VSM(Virtual Secure Mode: 가상 보안 모드)

- VBS(가상화 기반 보안),
  하이퍼바이저에 대한 보안 구역

Microsoft Defender Application Control

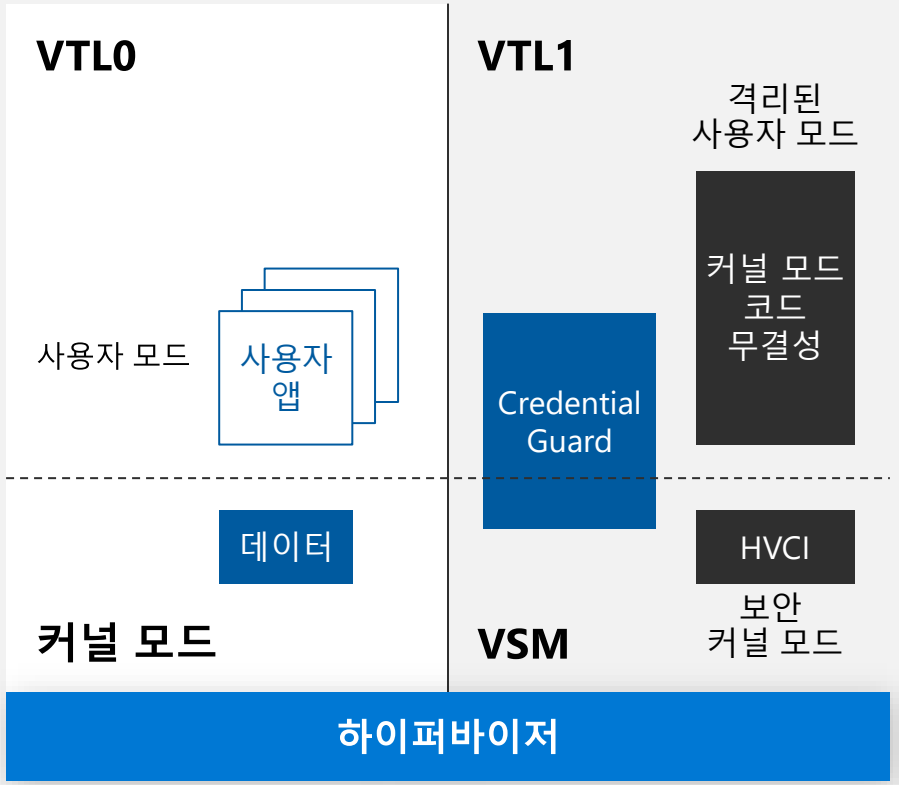
- 맬웨어에 대한 Surface 강화

Credential Guard

- 키 시스템 및 사용자 비밀 격리

HVCI(하이퍼바이저 코드 무결성)

- 코드 수정으로부터 드라이버/앱 보호
- Trustlets에 유효한 인증서가 있는지 확인



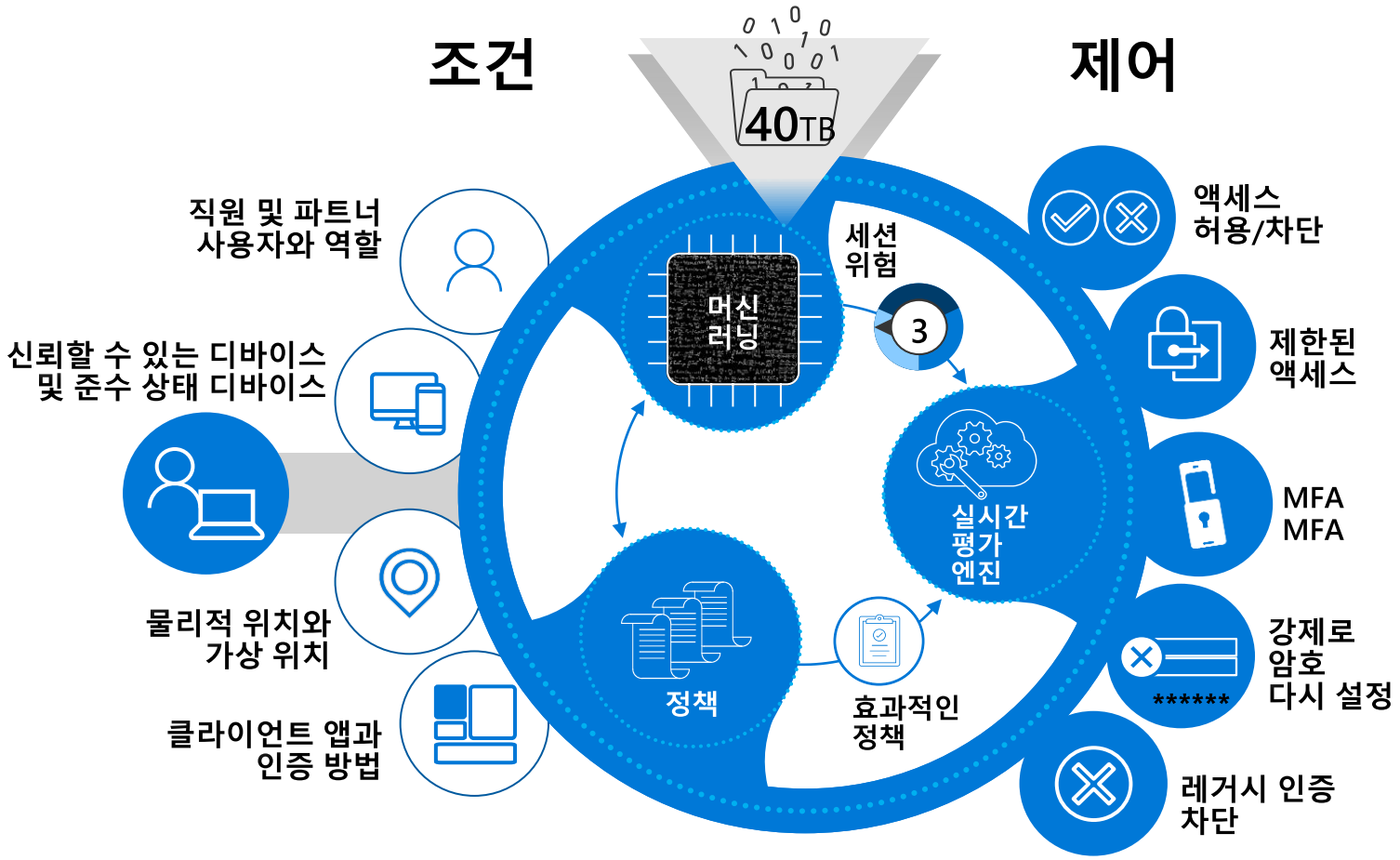
조건부 액세스

액세스 제어 및 Surface 보호

조건부 액세스

- Intune 관리형 정책
- 규정 준수에 따라 디바이스에 액세스 권한 부여
- 비준수 디바이스는 차단 또는 자동으로 수정

지오펜싱, 자동화 상태 변경 및 네트워크 기반 펌웨어 관리(확실하지 않음)



Microsoft Defender ATP

공격 감지, 조사, 대응

에이전트 없음, 클라우드 기반

- 항상 최신 상태 유지

탁월한 광학

- Windows 10에 내장되어 Microsoft Intelligent Security Graph와 데이터 교환

자동화 보안

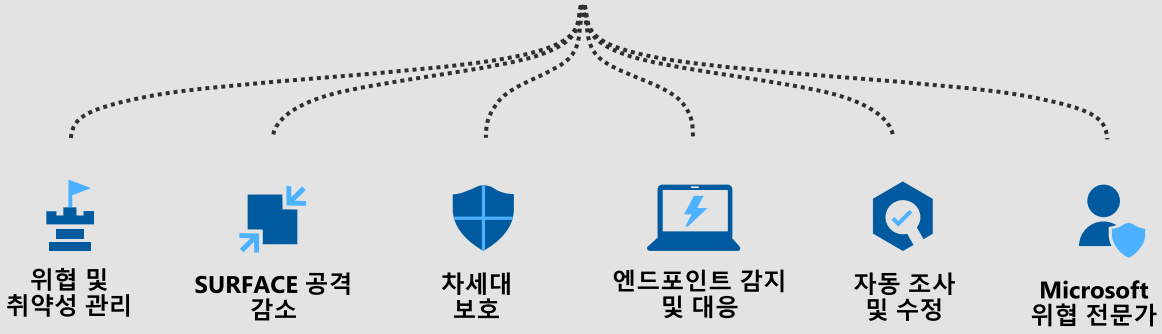
- 경고 후 몇 분 이내에 수정

동기화된 방어

- Microsoft365 전체 공유, 디바이스/ID/데이터

Microsoft Defender ATP

내장. 클라우드 기반



비즈니스용 Windows Update

최신 보안 방어를 통해 항상 최신 상태로 유지

Surface는 Windows와 긴밀하게 협력하여
Windows 업데이트를 통해 모든 업데이트 푸시

Configuration Manager, Intune
및 WSUS와 통합

테스트를 위해 배포 고리 활용

Windows Analytics를 통해 보고

Intune 초기화 및 사용 중지

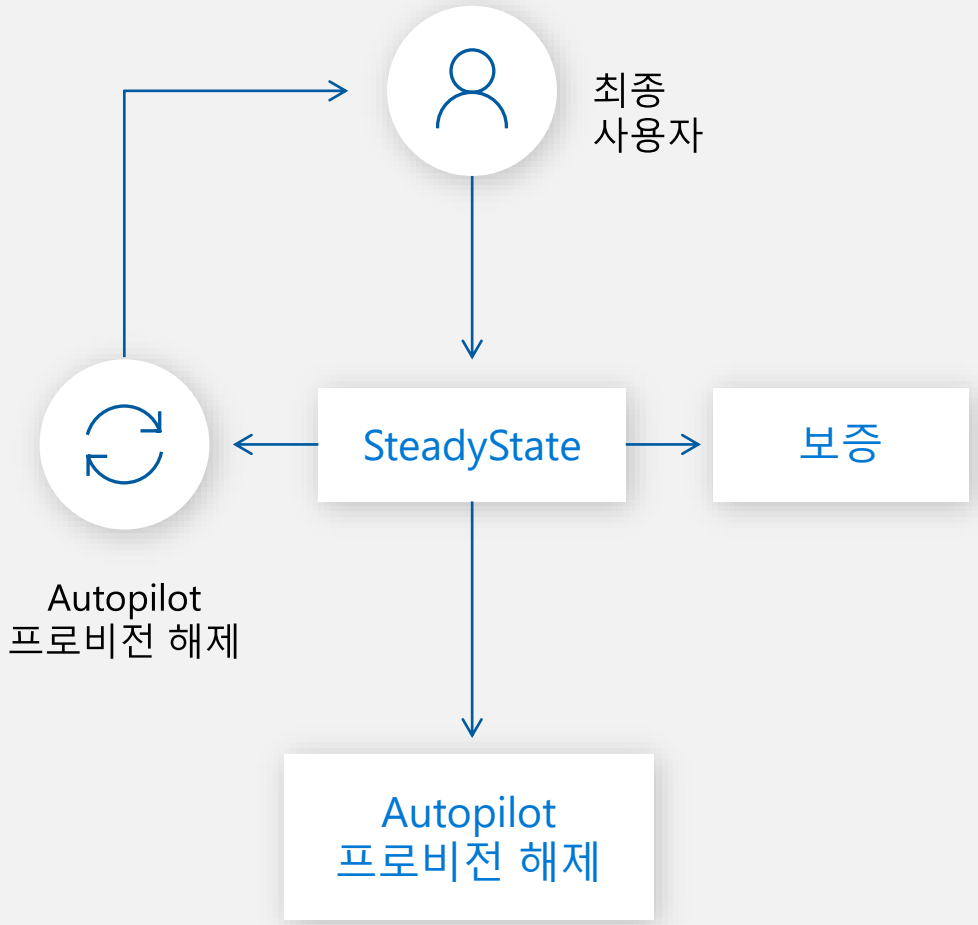
원격으로 Surface 용도 변경 또는 초기화

초기화 - OOBE로 복원

- 새 원격 사용자를 위한 디바이스 용도 변경
- 도난당한 디바이스 초기화

사용 중지 - Intune에서 디바이스 제거

- 사용자에게 BYOD(Bring Your Own Device : 개인용 디바이스를 업무용으로 사용) 디바이스 다시 제공
- 보증을 통해 디바이스 교체



Surface Tools for Business

Surface 보호 강화

배포

- Surface Enterprise 관리 모드
- Surface Deployment Accelerator(스크립트: 오픈 소스)

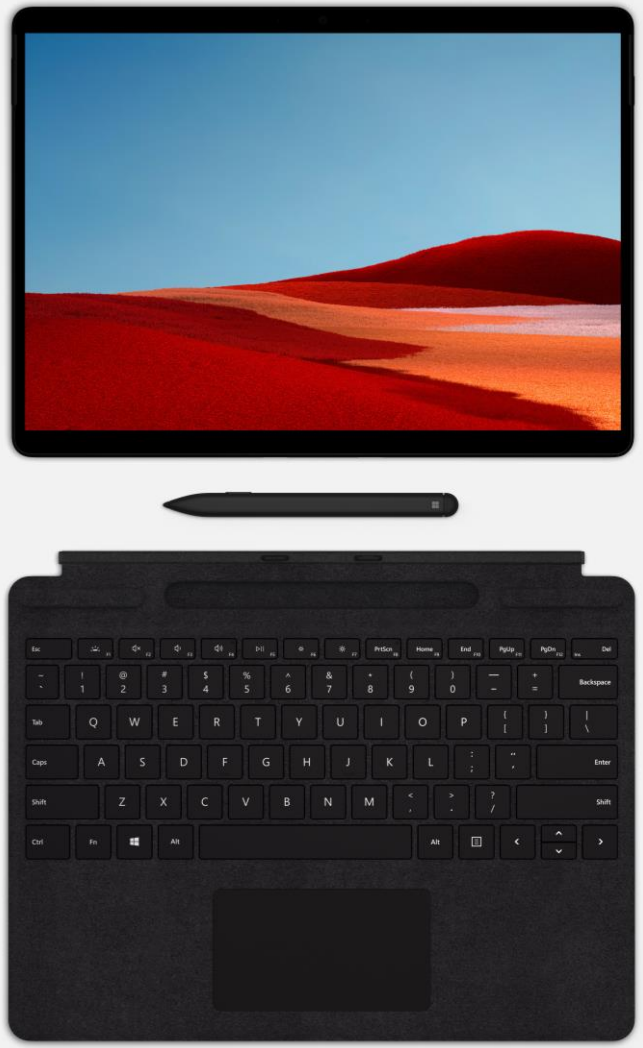
관리

- Surface Dock 펌웨어 업데이트 프로그램(자동)
- Surface 밝기 제어
- 비즈니스용 Surface 진단 툴킷

사용 중지

- Surface 데이터 지우개

다운로드: aka.ms/SurfaceTools
설명서: aka.ms/SuraceToolsDocs
동영상: aka.ms/SurfaceToolsVideo



요점

처음부터 동급 최강의 보안을 제공하도록 구축

Surface는 칩부터 클라우드까지 보호됩니다.

- Surface, Windows 및 EMS에서 최초이자 최고의 보안 혁신 제공
- Microsoft에 의해 엄격하게 제어되는 Surface 펌웨어
- 자동 업데이트를 통해 보안을 최신 상태로 유지
- 클라우드를 통해 엔터프라이즈 디바이스를 안전하게 관리

칩부터

- UEFI(TPM 2.0 포함)
- SEMM
- 보안 부팅
- BitLocker
- MDM UEFI 관리
- Windows Hello

클라우드까지

- 고급 Windows 보안 기능
- 조건부 액세스
- 비즈니스용 Windows Update
- Microsoft Defender ATP
- Intune 초기화 및 사용 중지

Microsoft

감사합니다.