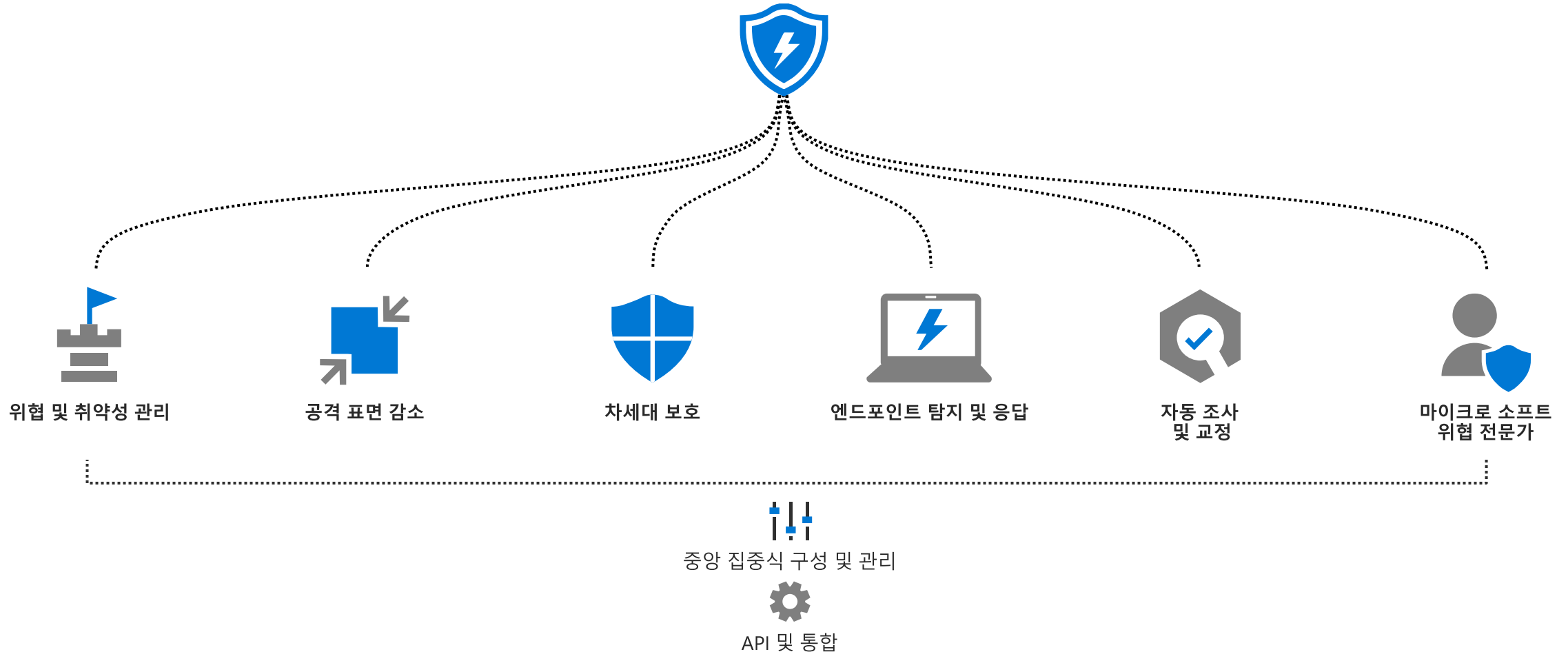


# Microsoft 365 Defender for Endpoint onboarding Introduce



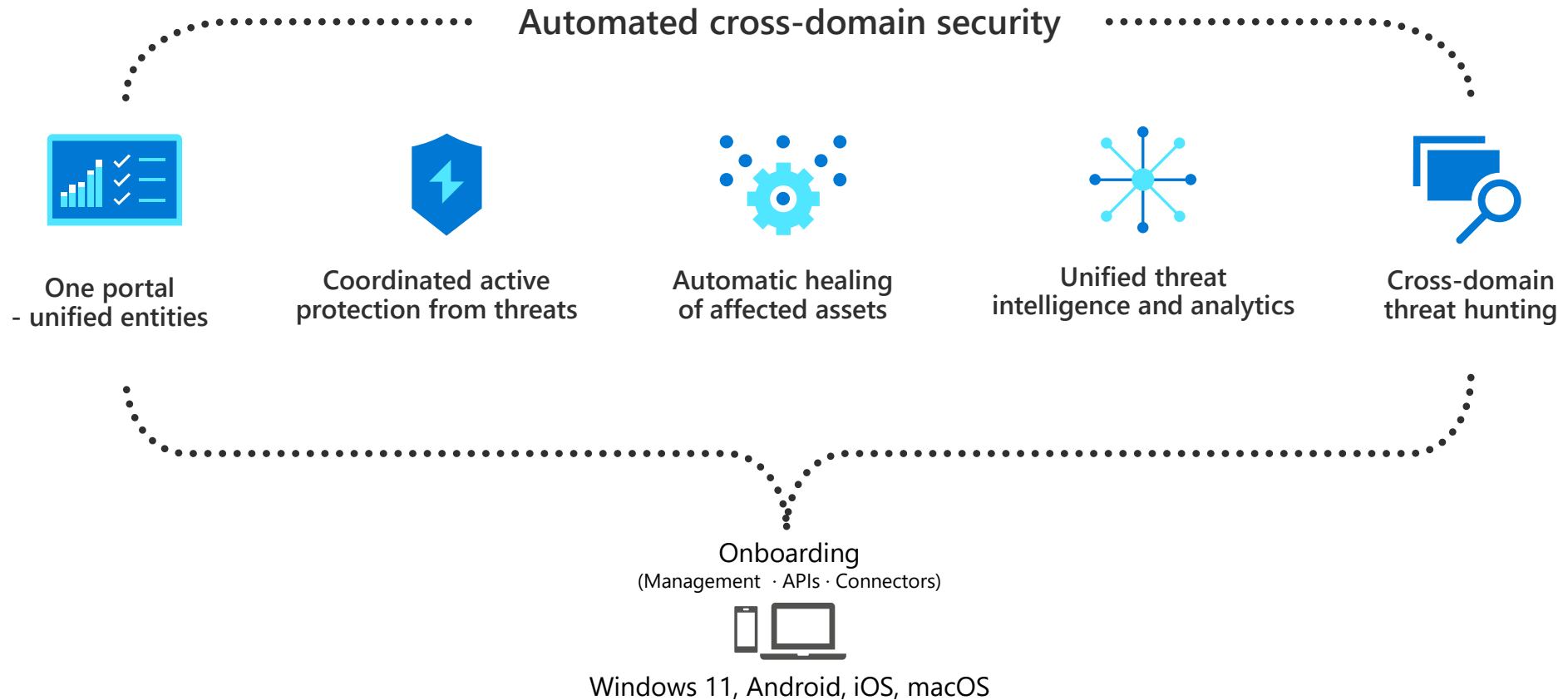
# Microsoft 365 Defender for Endpoint

Microsoft 365 Defender는 예방적 보호, 위반 후 검색, 자동화된 조사 및 대응을 위한 통합 엔드포인트 플랫폼입니다.



# Microsoft 365 Defender for Endpoint architecture

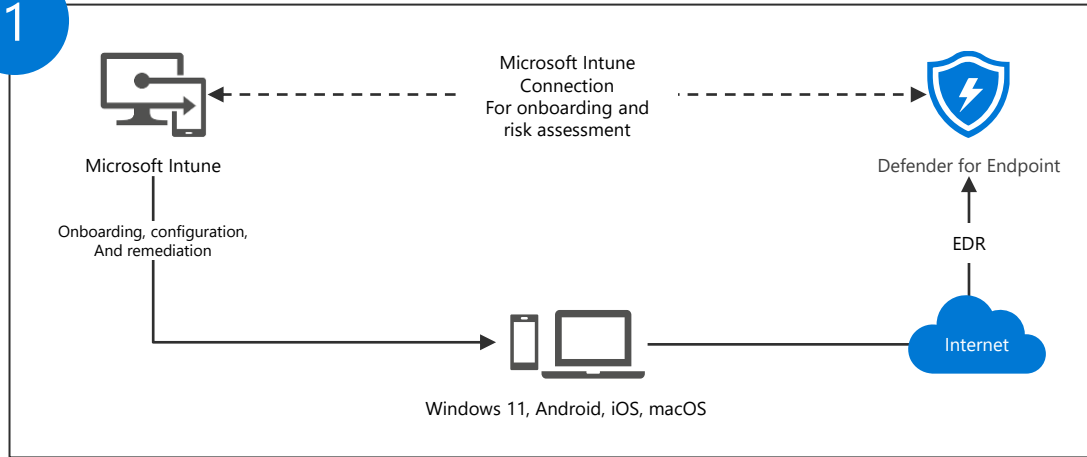
Microsoft 365 Defender는 예방적 보호, 위반 후 검색, 자동화된 조사 및 대응을 위한 통합 엔드포인트 플랫폼입니다.



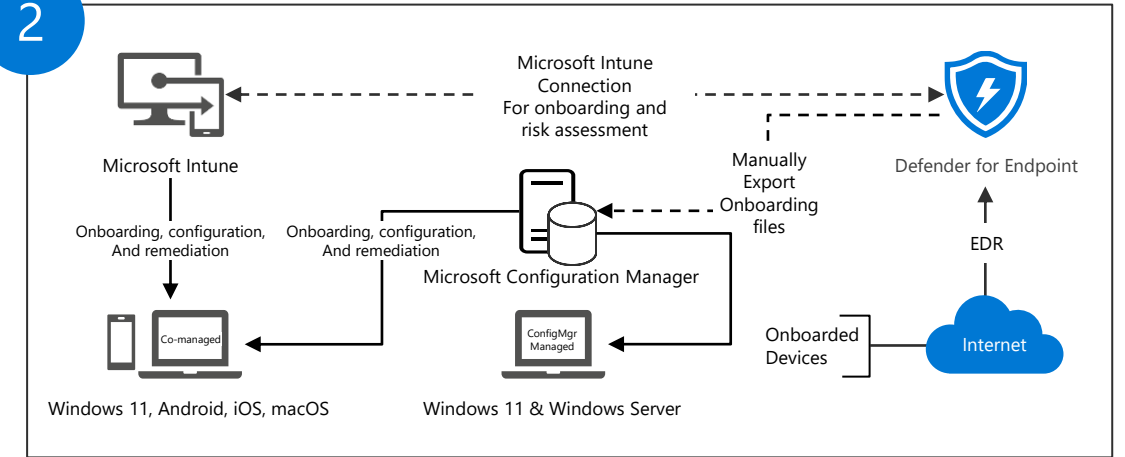
# Microsoft 365 Defender for Endpoint Onboarding

회사의 운영 인프라 환경에 맞춰 Defender for Endpoint에 관리 기기를 연결할 수 있습니다.

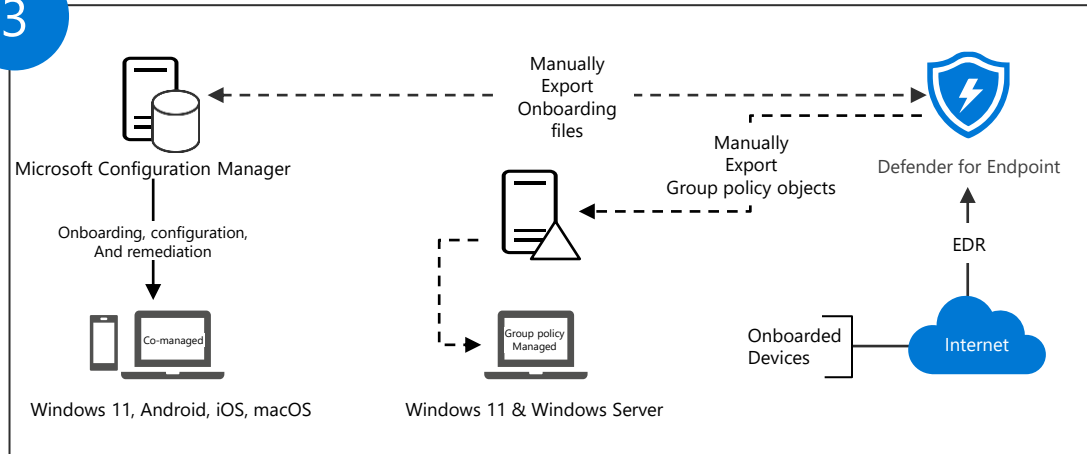
1



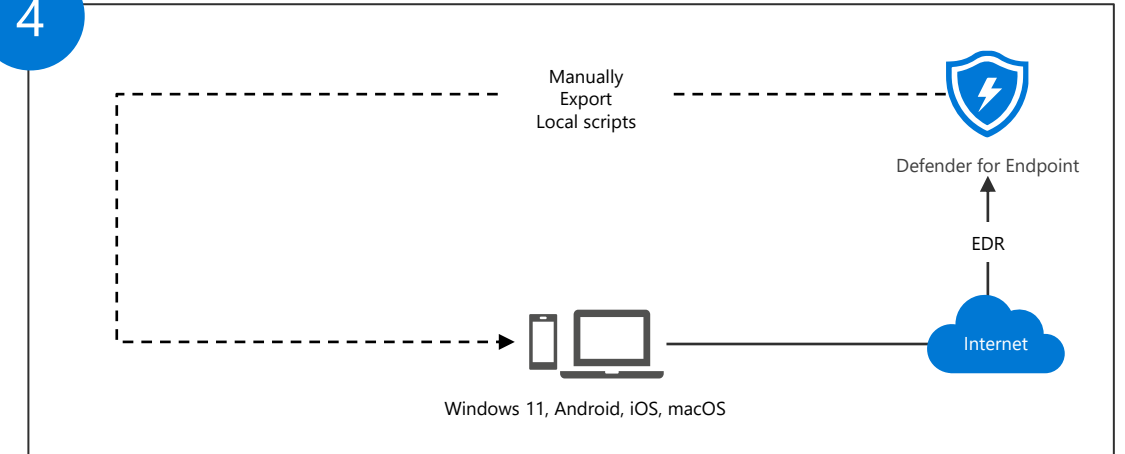
2



3



4



# Microsoft 365 Defender for Endpoint Onboarding 권한 [\(Link\)](#)

**장치 관리를 사용하도록 설정하려면** 사용하는 계정이 다음 역할 중 하나의 구성원이어야 합니다.

- 전역 관리자
- 보안 관리자
- 준수 관리자

**사용자 지정 계정을 사용하여 장치 관리 설정을 보려면** 계정이 다음 역할 중 하나여야 합니다.

- 전역 관리자
- 준수 관리자
- 준수 데이터 관리자
- 전역 읽기 권한자

**사용자 지정 계정을 사용하여 온보딩/오프보딩 페이지에 액세스하려면** 계정이 다음 역할 중 하나여야 합니다.

- 전역 관리자
- 준수 관리자

**사용자 지정 계정을 사용하여 장치 모니터링을 설정/해제하려면** 계정이 다음 역할 중 하나여야 합니다.

- 전역 관리자
- 준수 관리자

# Requirements

서비스에 디바이스를 온보딩하기 위한 몇 가지 최소 요구 사항이 있습니다.([Link](#))

## 라이선스 요구 사항

엔드 포인트용 Defender 플랜 1 및 플랜 2

서버용 엔드포인트용 Microsoft Defender 서버용 Defender 플랜 1 또는 클라우드용 Defender 제품의 일부로 계획 2

## 브라우저 요구 사항

Microsoft Edge / Google Chrome

## 바이러스 백신 구성 요구 사항

Microsoft Defender

## Microsoft Defender 바이러스 백신 조기 실행

맬웨어 방지(ELAM) 드라이버가 사용하도록 설정됨

## 하드웨어 및 소프트웨어 요구 사항

- Windows 10 Education
- Windows 10 Pro
- Windows 10 Pro Education
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 7 SP1 Enterprise([지원을 위해 ESU가 필요합니다.](#))
- Windows 7 SP1 Pro([지원을 위해 ESU 필요](#))
- Windows Server
  - Windows Server 2008 R2 SP1([지원을 위해 ESU 필요](#))
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 버전 1803 이상
  - Windows Server 2019 이상
  - Windows Server 2019 Core Edition
  - Windows Server 2022
- Windows Virtual Desktop
- Windows 365

# 플랫폼별 지원되는 기능

운영 체제	Windows 10 &11	Windows Server 2012 R2,2016,2019,2022,1803+	macOS	Linux
<a href="#">공격 표면 감소 규칙</a>	✓	✓	✗	✗
<a href="#">제어된 폴더 액세스</a>	✓	✓	✗	✗
장치 제어	✓	✗	✓	✗
<a href="#">방화벽</a>	✓	✓	✗	✗
<a href="#">Exploit Protection</a>	✓	✓	✗	✗
<a href="#">네트워크 보호</a>	✓	✓	✓ link	✓ link
<a href="#">차세대 보호</a>	✓	✓	✓	✓
<a href="#">변조 방지</a>	✓	✓	✓	✗
<a href="#">웹 보호</a>	✓	✓	✓ link	✓ link

# 플랫폼별 지원되는 기능

운영 체제	Windows 10 &11	Windows Server 2012 R2,2016,2019,2022,1803+	macOS	Linux
<a href="#">지능형 헌팅</a>	✓	✓	✓	✓
<a href="#">사용자 지정 파일 표시기</a>	✓	✓	✓	✓
<a href="#">사용자 지정 네트워크 표시기</a>	✓	✓	✓ link	✓ link
<a href="#">EDR 블록</a>	✓	✓	✗	✗
<a href="#">수동 모드</a>	✓	✓	✓	✓
감지 센서	✓	✓	✓	✓
엔드포인트 & 네트워크 디바이스 검색	✓	✗	✗	✗
<a href="#">취약성 관리</a>	✓	✓	✓	✓



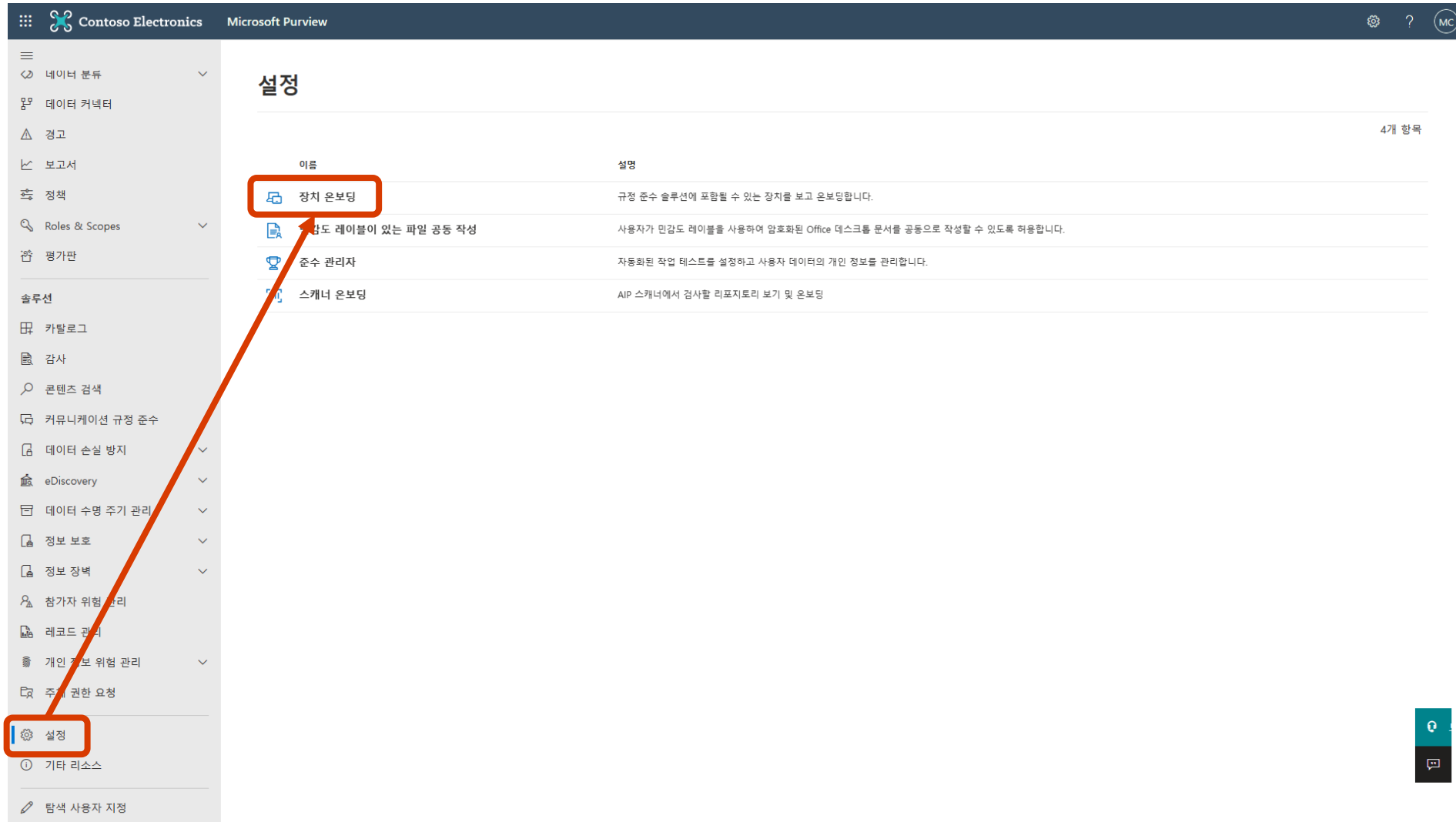
# 플랫폼별 지원되는 기능

운영 체제	Windows 10 &11	Windows Server 2012 R2,2016,2019,2022,1803+	macOS	Linux
<a href="#">AIR(자동 조사 &amp; 대응)</a>	✓	✓	✗	✗
<a href="#">디바이스 응답 기능: 조사 패키지 수집, AV 검사 실행</a>	✓	✓	✓ 1)	✓ 1)
<a href="#">디바이스 격리</a>	✓	✓	✓ 1)	✓
파일 응답 기능: 파일 수집, 심층 분석, 파일 차단, 중지 및 격리 프로세스	✓	✓	✗ 2)	✗ 2)
<a href="#">라이브 응답</a>	✓	✓	✓	✓

- 1) 라이브 응답을 사용하는 응답 기능  
 2) 라이브 응답을 사용하여 파일만 수집

# 온보딩 서비스 오픈 [\(link\)](#)

장치에서 중요한 항목을 모니터링하고 보호하려면 장치 모니터링을 사용하도록 설정하고 엔드포인트를 온보딩해야 합니다. 이러한 작업은 모두 Microsoft Purview 규정 준수 포털에서 수행됩니다.

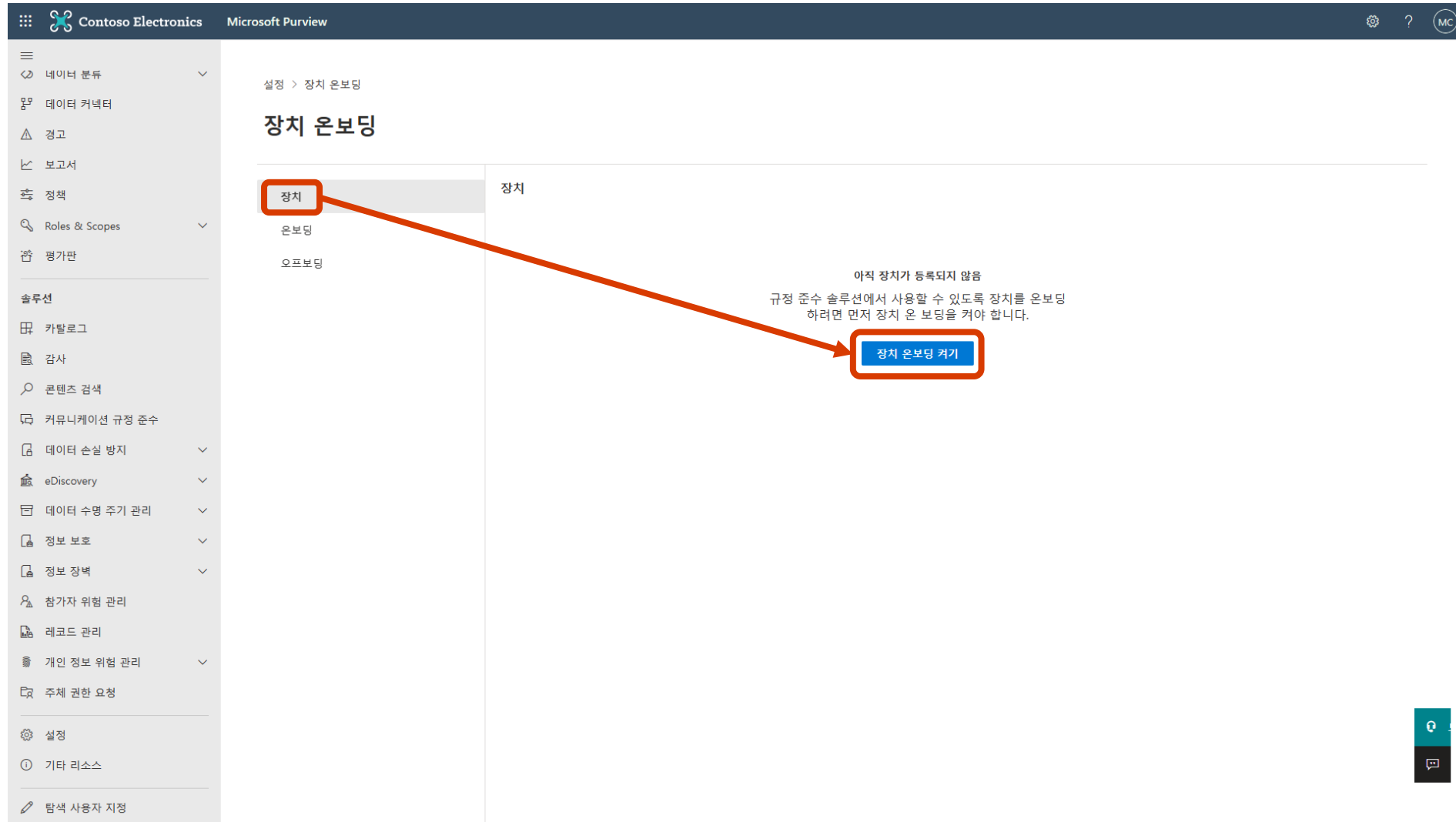


The screenshot displays the Microsoft Purview Compliance portal interface. The top navigation bar shows 'Contoso Electronics' and 'Microsoft Purview'. The left sidebar contains a list of navigation items, with '설정' (Settings) highlighted at the bottom. The main content area is titled '설정' (Settings) and displays a table of settings. The table has two columns: '이름' (Name) and '설명' (Description). The first row, '장치 온보딩' (Device Onboarding), is highlighted with a red box. An orange arrow points from the '장치 온보딩' icon in the left sidebar to the '장치 온보딩' row in the table.

이름	설명
장치 온보딩	규정 준수 솔루션에 포함될 수 있는 장치를 보고 온보딩합니다.
강도 레이블이 있는 파일 공동 작성	사용자가 민감도 레이블을 사용하여 암호화된 Office 데스크톱 문서를 공동으로 작성할 수 있도록 허용합니다.
준수 관리자	자동화된 작업 테스트를 설정하고 사용자 데이터의 개인 정보를 관리합니다.
스캐너 온보딩	AIP 스캐너에서 검사할 리포지토리 보기 및 온보딩

# 온보딩 서비스 오픈 [\(link\)](#)

장치에서 중요한 항목을 모니터링하고 보호하려면 장치 모니터링을 사용하도록 설정하고 엔드포인트를 온보딩해야 합니다. 이러한 작업은 모두 Microsoft Purview 규정 준수 포털에서 수행됩니다.



Contoso Electronics Microsoft Purview

설정 > 장치 온보딩

## 장치 온보딩

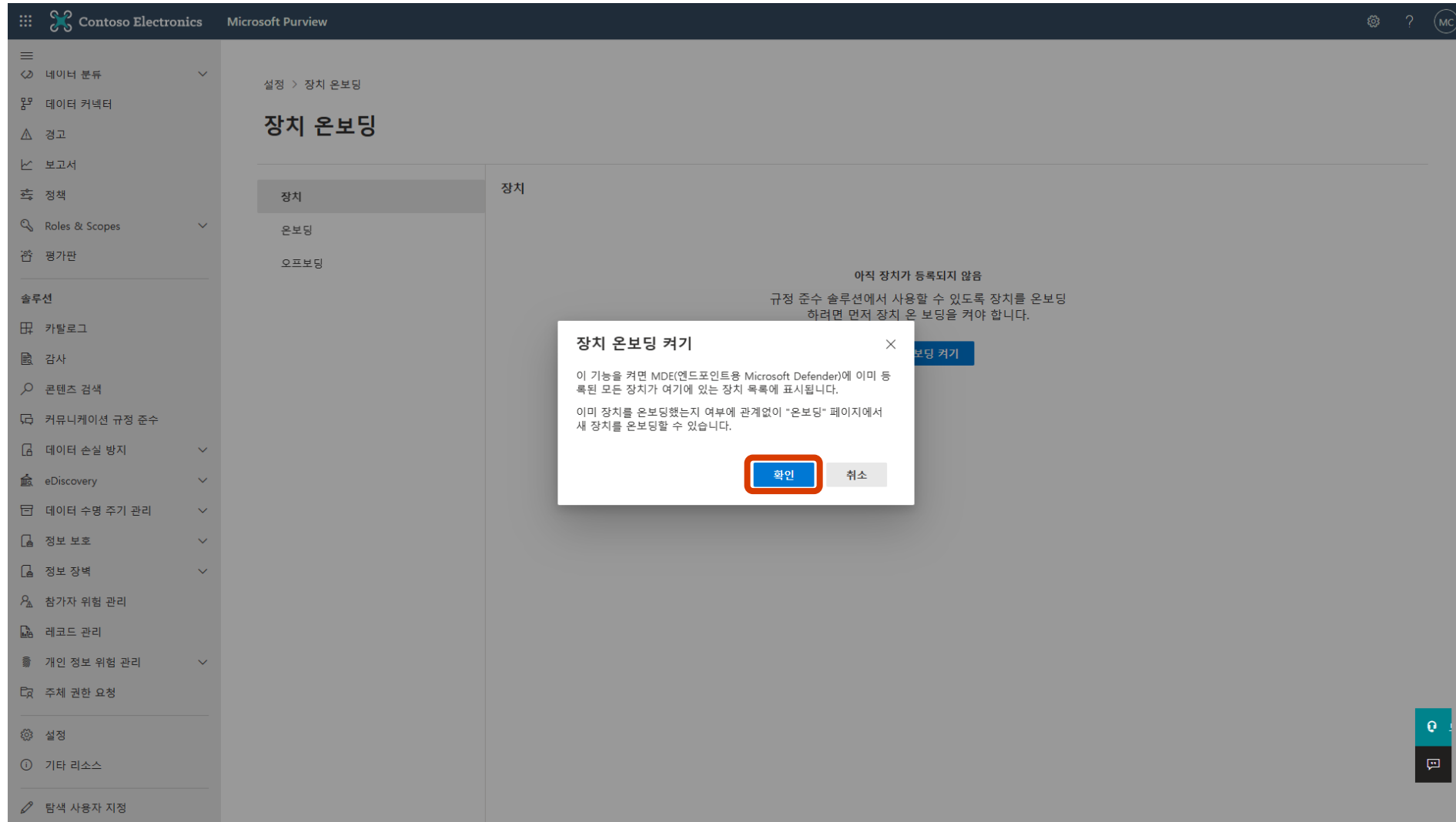
장치	장치
온보딩	
오프보딩	

아직 장치가 등록되지 않음  
규정 준수 솔루션에서 사용할 수 있도록 장치를 온보딩하려면 먼저 장치 온보딩을 켜야 합니다.

[장치 온보딩 켜기](#)

# 온보딩 서비스 오픈 [\(link\)](#)

장치에서 중요한 항목을 모니터링하고 보호하려면 장치 모니터링을 사용하도록 설정하고 엔드포인트를 온보딩해야 합니다. 이러한 작업은 모두 Microsoft Purview 규정 준수 포털에서 수행됩니다.



# 온보딩 서비스 오픈 [\(link\)](#)

장치에서 중요한 항목을 모니터링하고 보호하려면 장치 모니터링을 사용하도록 설정하고 엔드포인트를 온보딩해야 합니다. 이러한 작업은 모두 Microsoft Purview 규정 준수 포털에서 수행됩니다.

The screenshot shows the Microsoft Purview Compliance portal interface. The left sidebar contains navigation options such as '네이더 분류' (Nether Classification), '데이터 커넥터' (Data Connector), '경고' (Warning), '보고서' (Report), '정책' (Policy), 'Roles & Scopes', '평가판' (Evaluation), '솔루션' (Solution), '카탈로그' (Catalog), '감사' (Audit), '콘텐츠 검색' (Content Search), '커뮤니케이션 규정 준수' (Communication Compliance), '데이터 손실 방지' (Data Loss Prevention), 'eDiscovery', '데이터 수명 주기 관리' (Data Lifecycle Management), '정보 보호' (Information Protection), '정보 장벽' (Information Barrier), '참가자 위험 관리' (Participant Risk Management), '레코드 관리' (Record Management), '개인 정보 위험 관리' (Personal Information Risk Management), '주체 권한 요청' (Subject Access Request), '설정' (Settings), '기타 리소스' (Other Resources), and '탐색 사용자 지정' (Search Customization). The main content area is titled '장치 온보딩' (Device Onboarding) and shows a table with columns '장치' (Device) and '온보딩' (Onboarding). A modal dialog is open in the center, titled '장치 모니터링이 켜져 있습니다.' (Device monitoring is turned on). The dialog text states: '이 작업은 시간이 걸릴 수 있으므로 페이지를 새로 고쳐서 진행 상황을 자주 확인합니다.' (This task may take time, so refresh the page frequently to check progress). It also mentions: '이 기능을 켜면 MDE(엔드포인트용 Microsoft Defender)에 이미 등록된 모든 장치가 장치 목록에 표시됩니다.' (When you enable this feature, all devices already registered in MDE (Microsoft Defender for Endpoint) will be displayed in the device list). A '확인' (Confirm) button is highlighted with a red box.

# 온보딩 서비스 오픈 [\(link\)](#)

장치에서 중요한 항목을 모니터링하고 보호하려면 장치 모니터링을 사용하도록 설정하고 엔드포인트를 온보딩해야 합니다. 이러한 작업은 모두 Microsoft Purview 규정 준수 포털에서 수행됩니다.

The screenshot displays the Microsoft Purview Compliance portal interface. The top navigation bar includes the 'Contoso Electronics' logo and the 'Microsoft Purview' title. A left-hand sidebar contains a menu with various options: 홈, 준수 관리자, 데이터 분류, 데이터 커넥터, 경고, 보고서, 정책, Roles & Scopes, 평가판, 솔루션, 카탈로그, 감사, 콘텐츠 검색, 커뮤니케이션 규정 준수, 데이터 손실 방지, eDiscovery, 데이터 수명 주기 관리, 정보 보호, 정보 장벽, 참가자 위험 관리, 레코드 관리, 개인 정보 위험 관리, 주체 권한 요청, and 설정. The main content area is titled '장치 온보딩' (Device Onboarding) under the '설정' (Settings) section. It features a sub-menu with '장치' (Devices) and '온보딩' (Onboarding). The '장치' section includes a description of device monitoring, a '내보내기' (Export) button, and tabs for 'Windows 디바이스 모니터링 꺼짐' and 'macOS 디바이스 모니터링 꺼짐'. A table below shows columns for '장치 이름' (Device Name), '상태' (Status), '구성 상태' (Configuration Status), '마지막으로 본 것' (Last Seen), 'OS', and 'OS 버전' (OS Version). The table is currently empty, with a message '사용할 수 있는 데이터 없음' (No data available) at the bottom. A '더 많은 항목 로드' (Load more items) button is visible above the table.

# 로컬 스크립트를 사용하여 Windows 장치 온보딩 [\(link\)](#)

개별 디바이스를 Microsoft 365에 수동으로 온보딩 할 수 있습니다.

Contoso Electronics Microsoft Purview

설정 > 장치 온보딩

## 장치 온보딩

장치  
온보딩  
오프보딩

온보딩 프로세스를 시작할 운영 체제 선택:  
Windows 10

규정 준수 센터에 장치를 온보딩하려면 기본 설정된 배포 방법을 선택하고, 관련 구성 패키지를 다운로드하고, 각 방법에 대해 제공되는 문서의 지침을 따릅니다.

배포 방법  
로컬 스크립트(최대 컴퓨터 10대에 사용...)

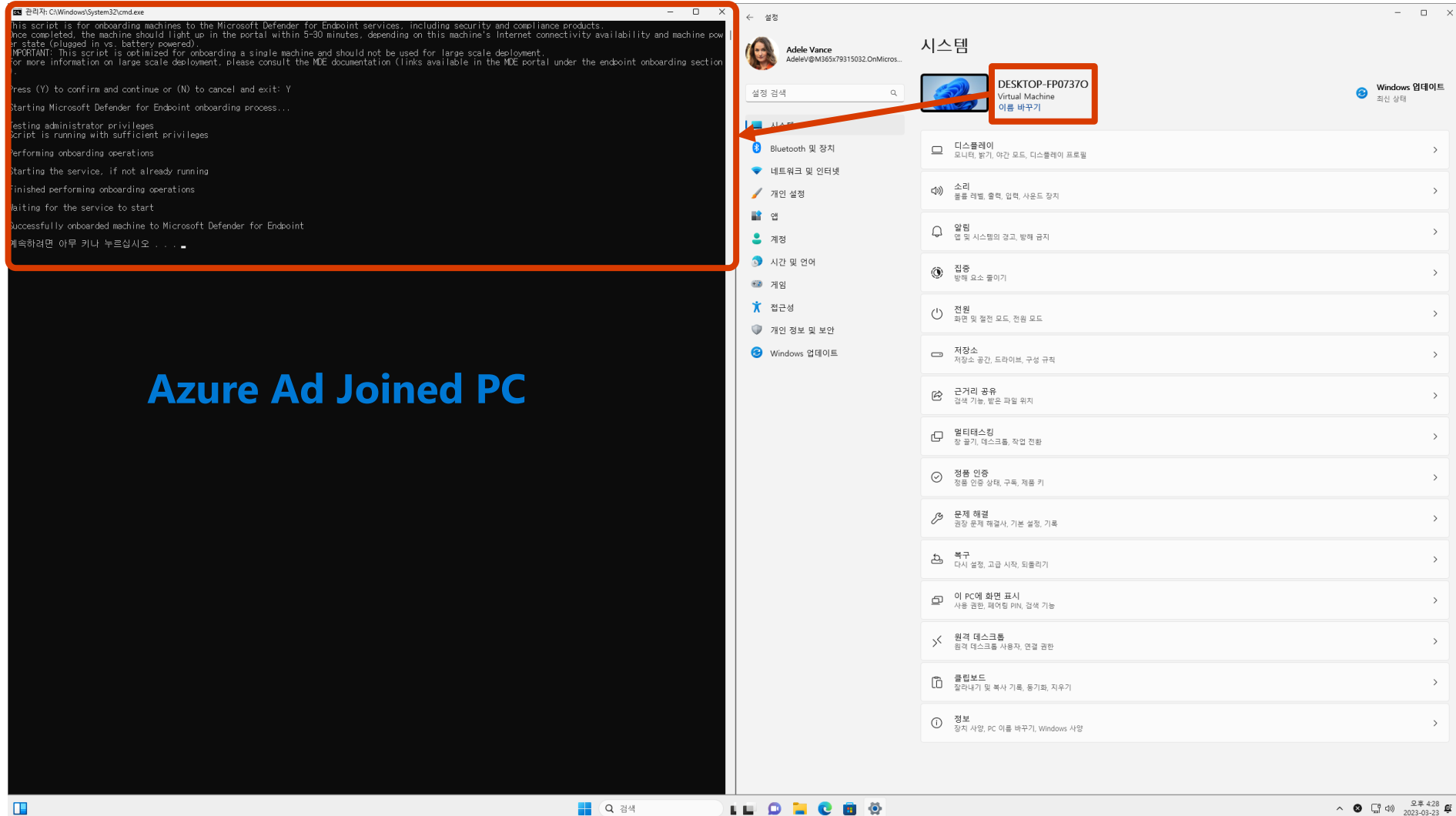
이 스크립트는 1-10개의 장치를 온보딩하는 데 적합되었습니다. 10개를 초과하여 온보딩하려면, 다른 배포 방법을 선택하십시오.  
[로컬 스크립트를 사용하여 장치를 온보딩하는 지침](#)  
이 문서에서는 엔드포인트용 Microsoft Defender로 장치 온보딩에 대해 설명하지만 그 지침은 규정 준수 센터로의 온보딩과 동일합니다..

패키지 다운로드

다운로드  
DeviceComplianceOnboardingPackage.zip(으)...  
열기 다른 이름...  
자세히 보기

# 로컬 스크립트를 사용하여 Windows 장치 온보딩 [\(link\)](#)

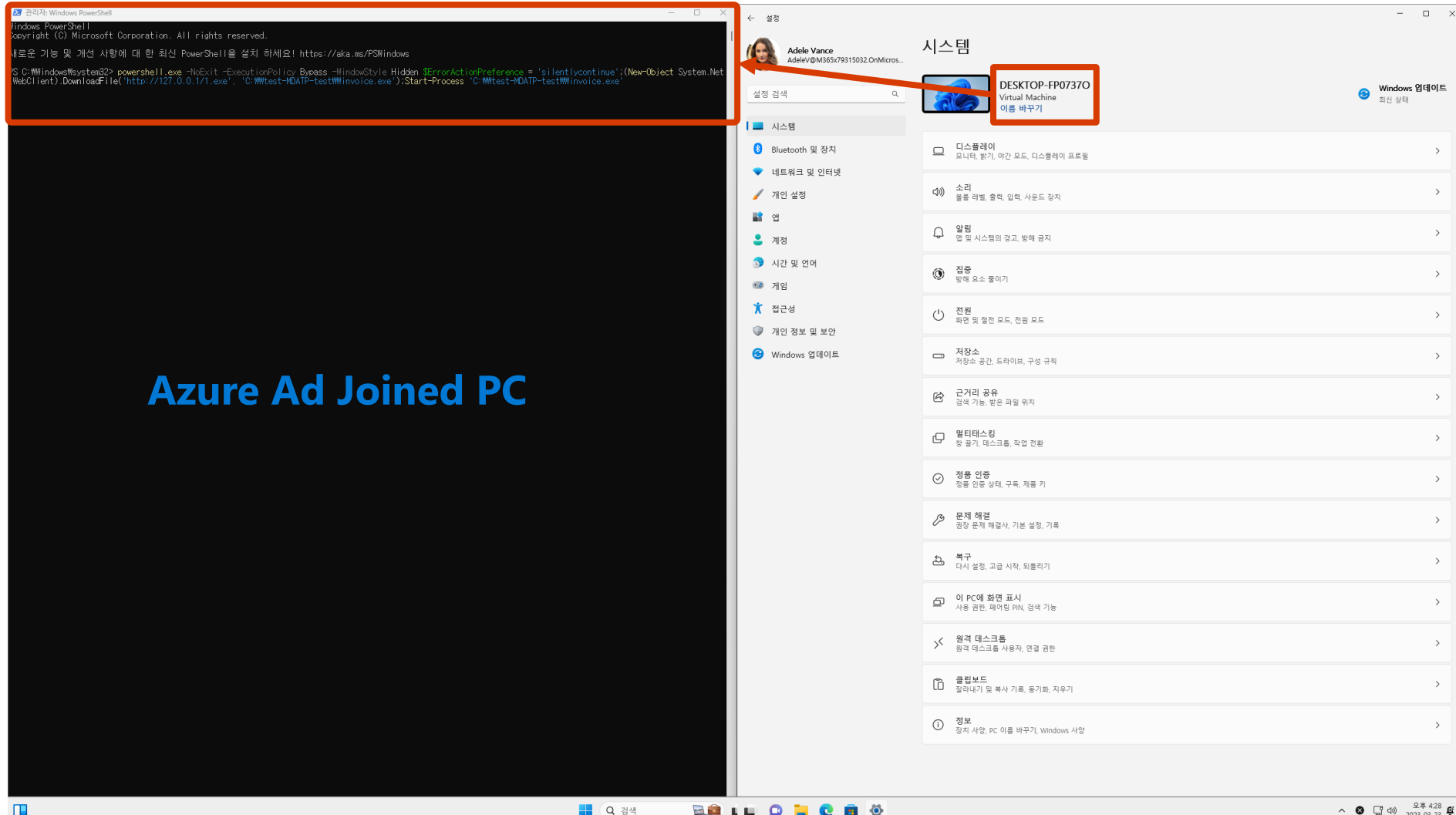
개별 디바이스를 Microsoft 365에 수동으로 온보딩 할 수 있습니다.





# Microsoft Defender 디바이스에서 검색 테스트 실행 [\(LINK\)](#)

장치가 서비스에 성공적으로 추가되었는지 확인하거나 확인하는 것은 전체 배포 프로세스에서 중요한 단계입니다. 예상되는 모든 장치가 관리되고 있는지 확인합니다.



# Microsoft Defender 디바이스에서 검색 테스트 실행 [\(LINK\)](#)

장치가 서비스에 성공적으로 추가되었는지 확인하거나 확인하는 것은 전체 배포 프로세스에서 중요한 단계입니다. 예상되는 모든 장치가 관리되고 있는지 확인합니다.

Contoso ElectronicsMicrosoft Purview

홈

준수 관리자

데이터 분류

데이터 커넥터

경고

보고서

정책

Roles & Scopes

평가판

솔루션

카탈로그

감사

콘텐츠 검색

커뮤니케이션 규정 준수

데이터 손실 방지

eDiscovery

데이터 수명 주기 관리

정보 보호

정보 장벽

참가자 위험 관리

레코드 관리

개인 정보 위험 관리

주체 권한 요청

설정

설정 > 장치 온보딩

장치 온보딩

장치

이러한 온보딩된 장치의 활동은 활동 탐색기와 같은 기능을 통해 검토하거나 참가자 위험 관리 및 DLP(데이터 손실 방지)와 같은 규정 준수 솔루션으로 모니터링할 수 있습니다. 자세히 알아보기

내보내기Windows 디바이스 모니터링 꺼짐macOS 디바이스 모니터링 꺼짐2개 항목검색

필터 다시 설정 필터

머칠 후 다시 보기: 30 상태: 모두 구성 상태: 모두 OS: 모두 OS 버전: 모두

장치 이름	상태	구성 상태	마지막으로 본 것	OS	OS 버전
desktop-fp0737o	Active	Valid	2023년 3월 23일 오후 3:50	Windows11	22H2
desktop-r905ptk	Active	Valid	2023년 3월 23일 오후 3:50	Windows11	22H2

더 많은 항목 로드



감사합니다.