Microsoft Security

제로 트러스트 보안

생산성을 유지하고
안전한 데이터 보호 방법

: 하이브리드 업무 환경을 위한 마이크로소프트의 엔드 투 엔드 보안과 제로 트러스트 전략으로 조직을 보호하기

홍세진 매니저

한국마이크로소프트 보안사업부

2023년 4월 19일

보안이 그 어느 때보다 중요해졌습니다.

원격 및 하이브리드 작업이 **300% 증가**했습니다.[1]

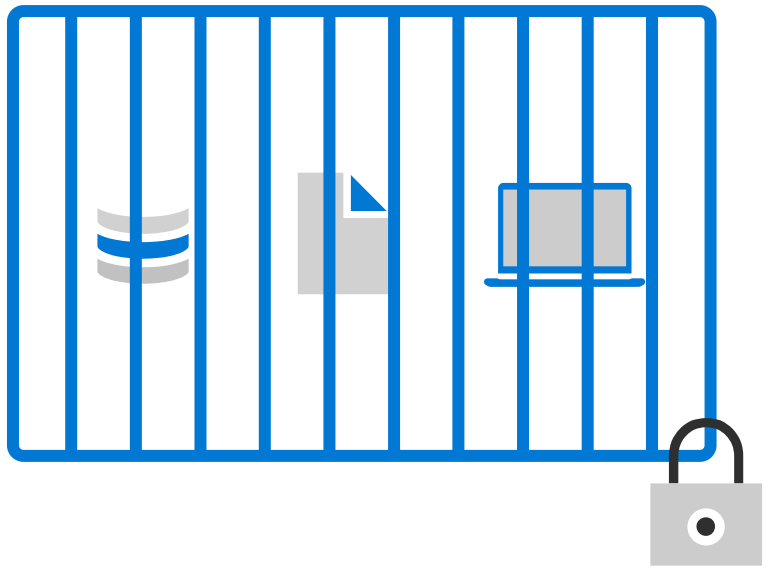
사이버 공격은 **점점 더 정교**해지고 있습니다.

피싱은 **데이터 유출**의 거의 **70%를 차지**합니다.[2]

1. Predictions 2021: Remote Work, Automation, And HR Tech Will Flourish, Forrester
2. Microsoft Digital Defense Report, October 2021.

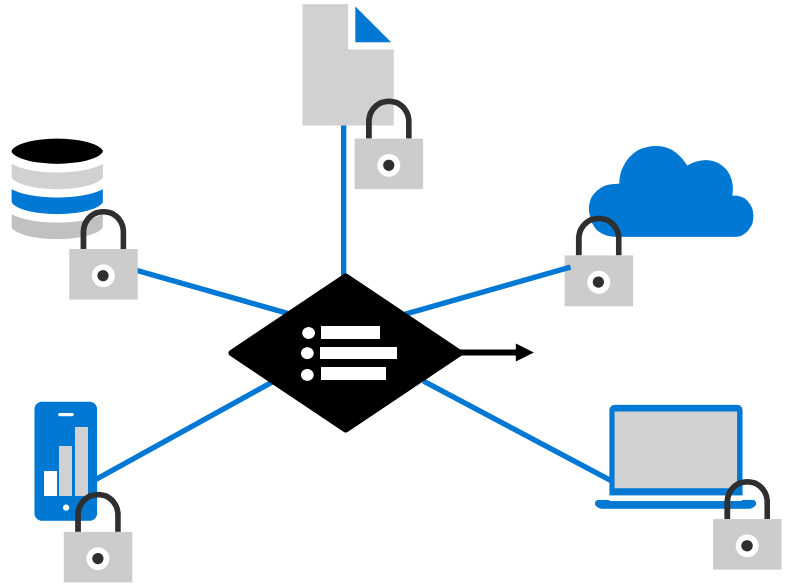
보안 패러다임의 변화

보안을 단순화하고 더 효과적으로 만들어야 한다.



Classic Approach

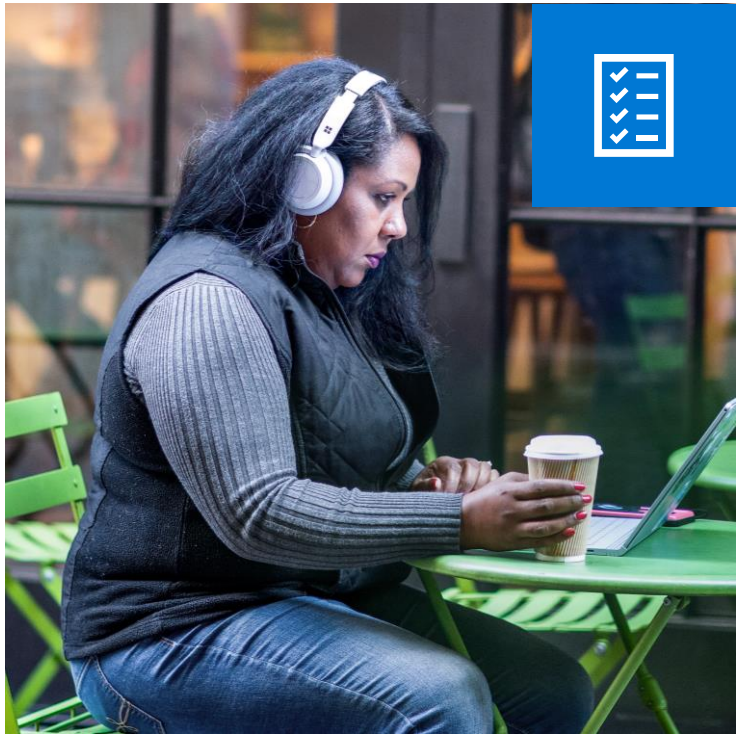
Restrict everything to a ‘secure’ network



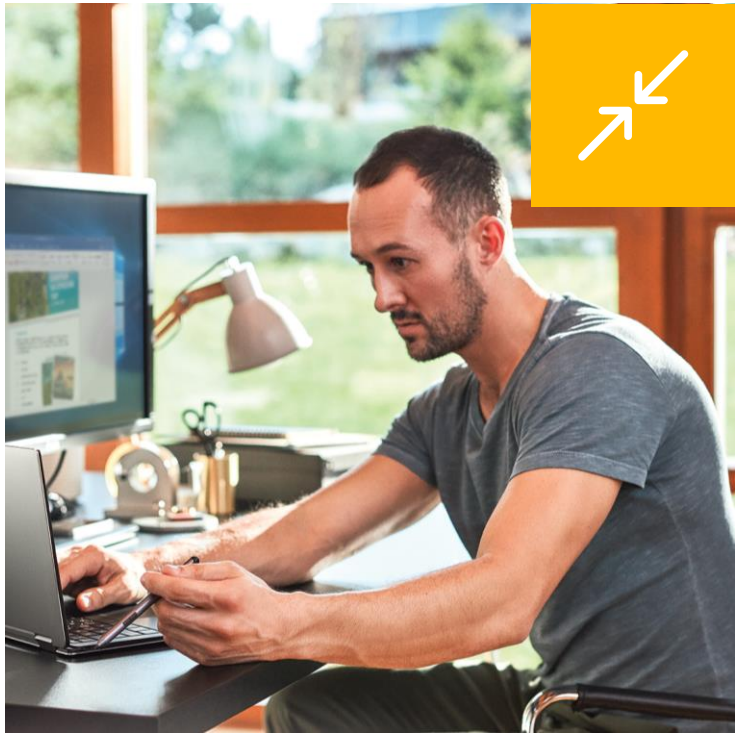
Zero Trust

Protect assets anywhere with central policy

새로운 현실에는 새로운 원칙이 필요



- 명확하게 검증
  Verify explicitly



- 최소 권한 액세스 사용
  Use least privilege access

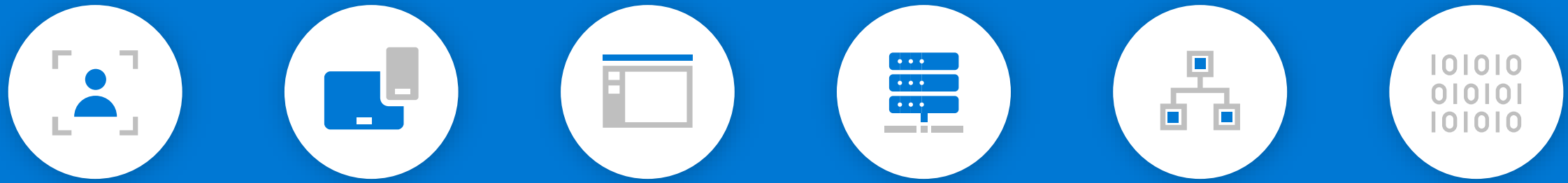
- 침해를 가정
  Assume breach

마이크로소프트 제로 트러스트

전체 디지털 자산에 대한 **적응형 제어** 및 **지속적인 검증**을 통해 액세스 보안에 대한 **통합적 접근**

디지털 자산 전반에 걸친 제로 트러스트

Governance

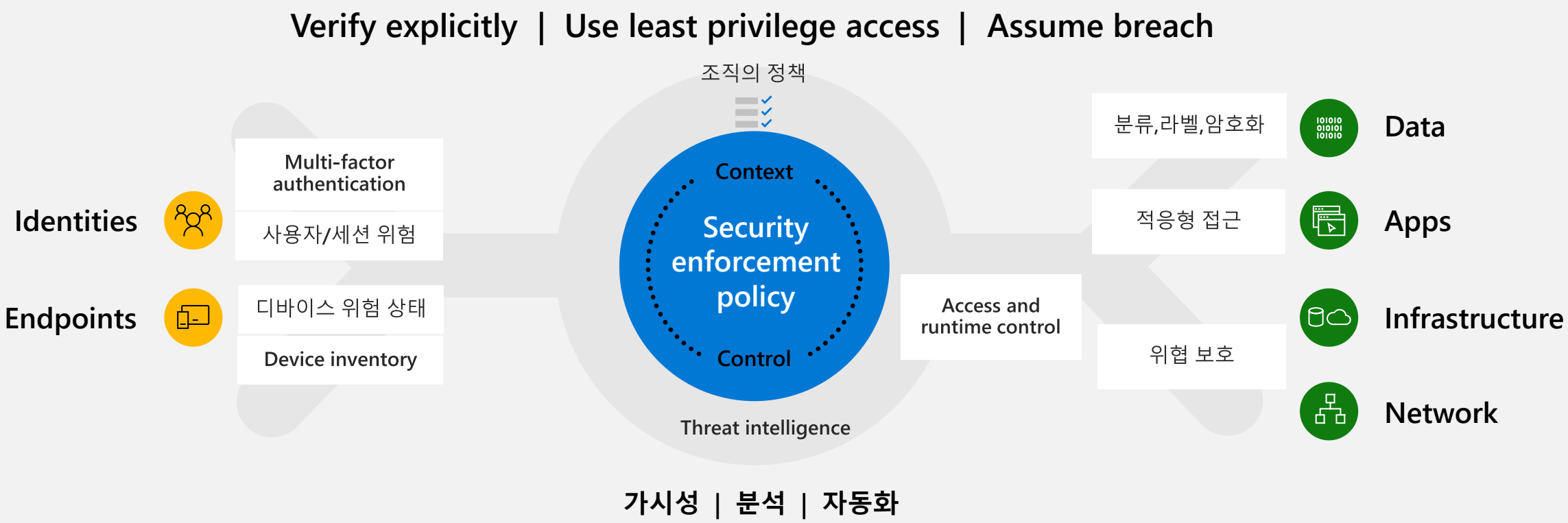


Identities | Endpoints | Apps | Infrastructure | Network | Data

Threat Protection

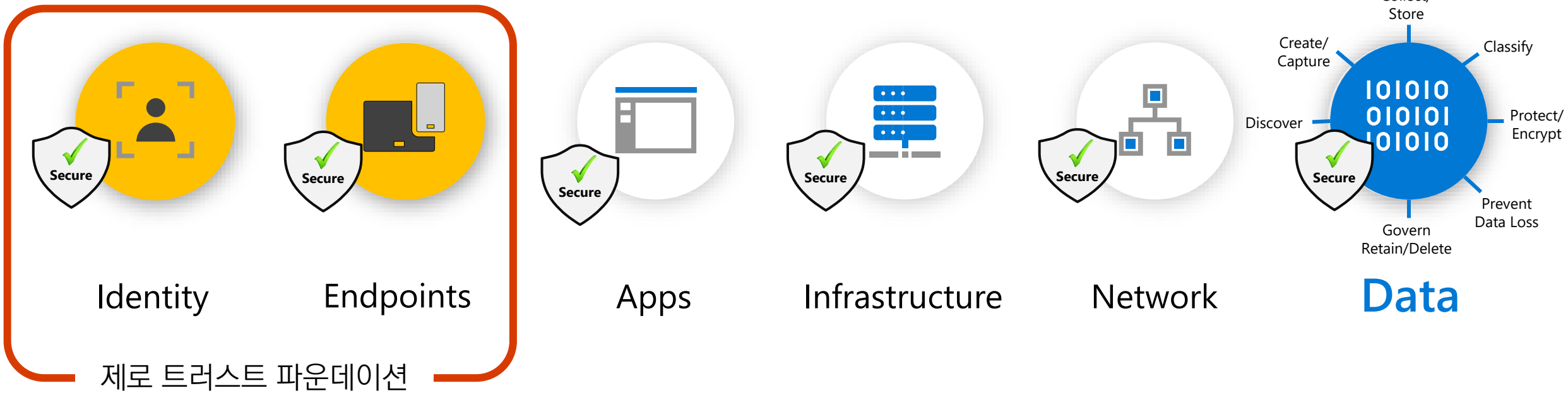
마이크로소프트 제로 트러스트 아키텍처

중요한 비즈니스 자산에 대한 보안 보장 강화



제로 트러스트 보안

오늘날 조직은 현대 환경의 복잡성에 효과적으로 대응하고, 모바일 인력을 수용하고, 사람, 장치, 애플리케이션 및 데이터를 어디에 있든 보호하는 새로운 보안 접근 방식이 필요합니다.



"침해사고를 당했다고 가정이 필요"

아이덴티티와 엔드포인트 보호

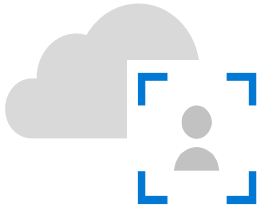
하이브리드 업무 환경 보호

데이터 보호

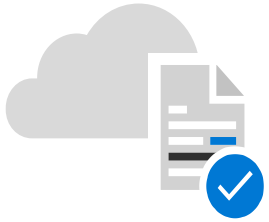
통합 보안 운영 및 자동화

강력한 인증 통해 모든 ID를 확인하고 보호해야 합니다.

SSO를 통해 모든 사용자 및 어플리케이션 연결



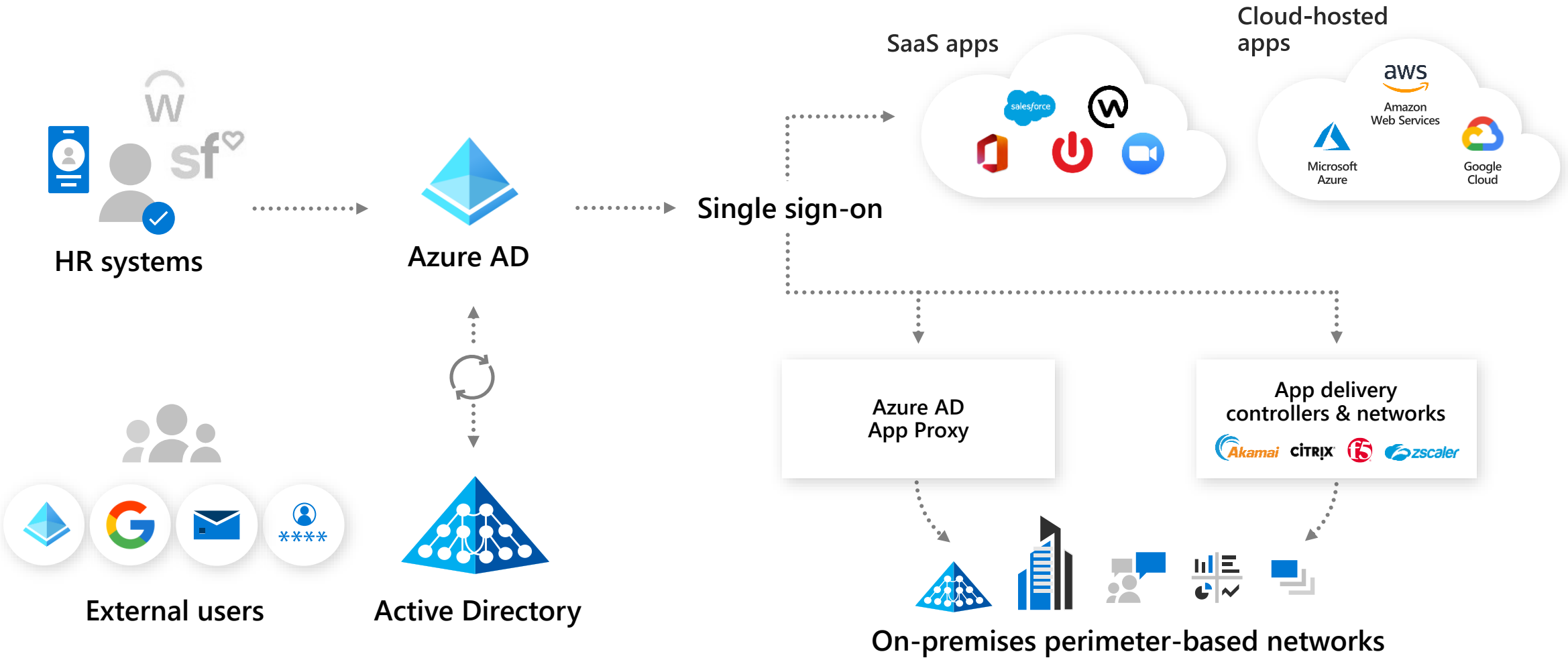
다단계 인증(MFA)으로 ID 보호



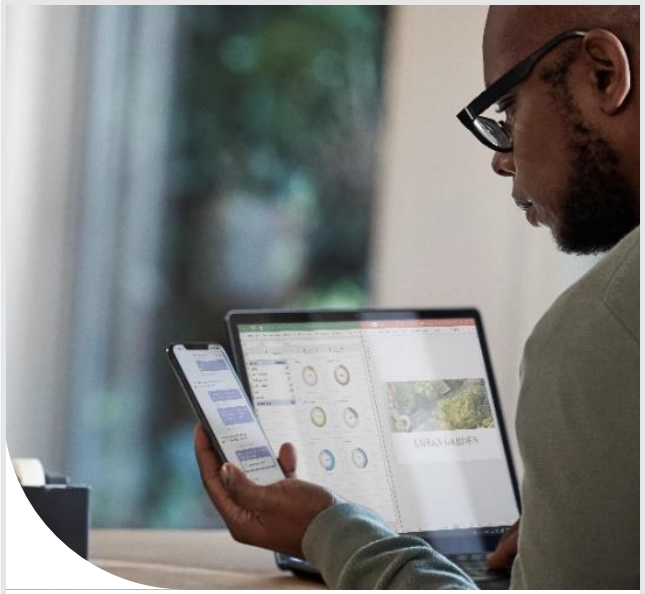
스마트한 정책으로 액세스를 제어하고 위험을 평가

강력한 거버넌스를 통해 최소 권한 액세스 적용

SSO를 통해 모든 애플리케이션에 대한 보안 액세스



다단계 인증(MFA)으로 ID 확인



광범위한
다단계 인증 옵션을
지원합니다.

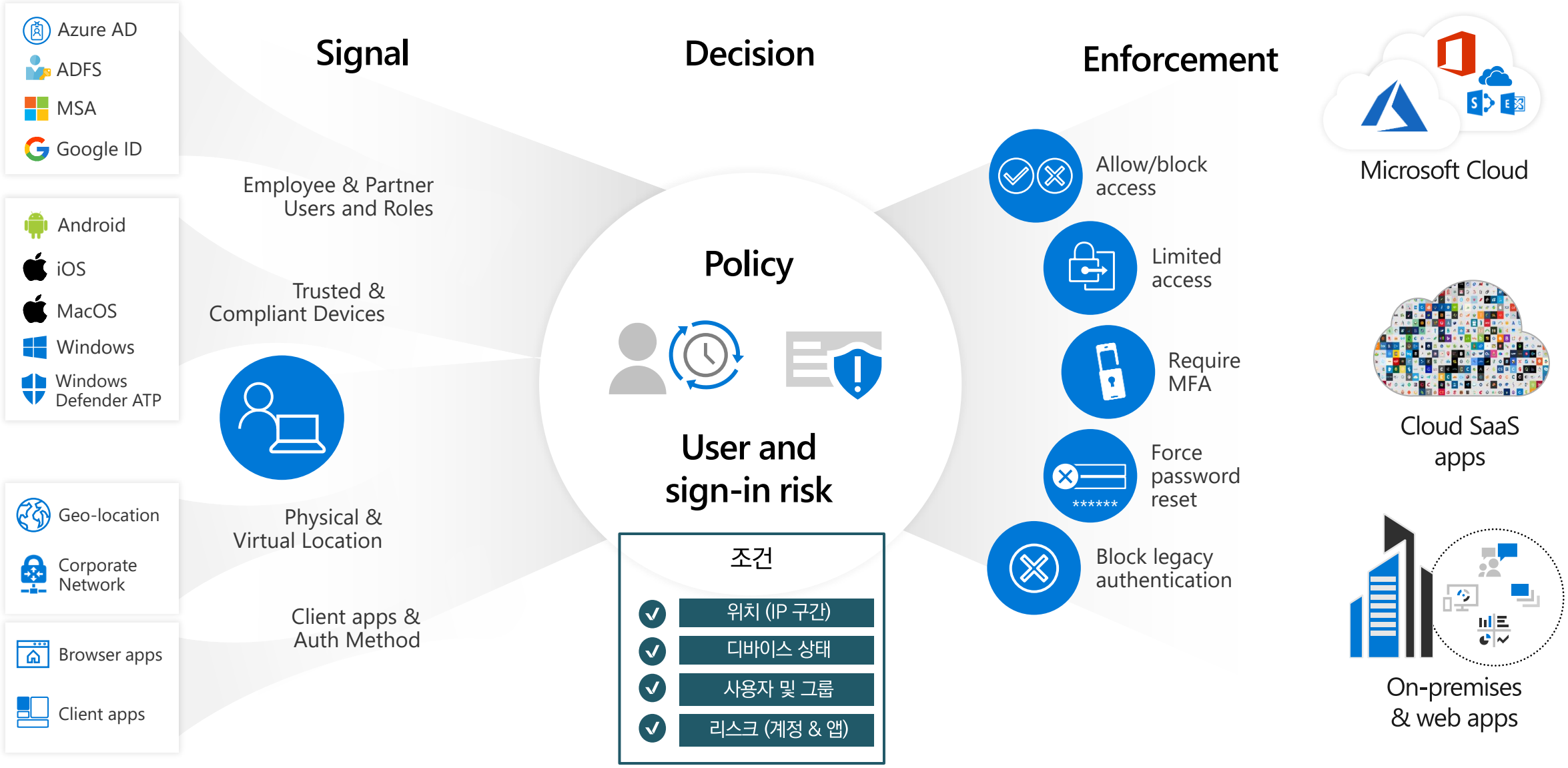
패스워드리스 기술 포함

- Microsoft Authenticator
- Windows Hello
- FIDO2 보안 키
- 생체 인식

- 푸시 알림
- 소프트 토큰 OTP
- 하드 토큰 OTP
- SMS, 음성

다단계
인증이
ID 공격의
99.9%를 차단합니다.

조건부 액세스를 이용한 사용자 및 디바이스 액세스 보안 강화



지능형 위협으로 부터 안전하게 분산된 엔드포인트 보호

Microsoft Defender for Endpoint

자산 식별

자산 발견

위험 식별

위협 및
취약성 관리

예방

공격 표면 감소

차세대 백신
(NGAV)

P1

탐지 및 대응

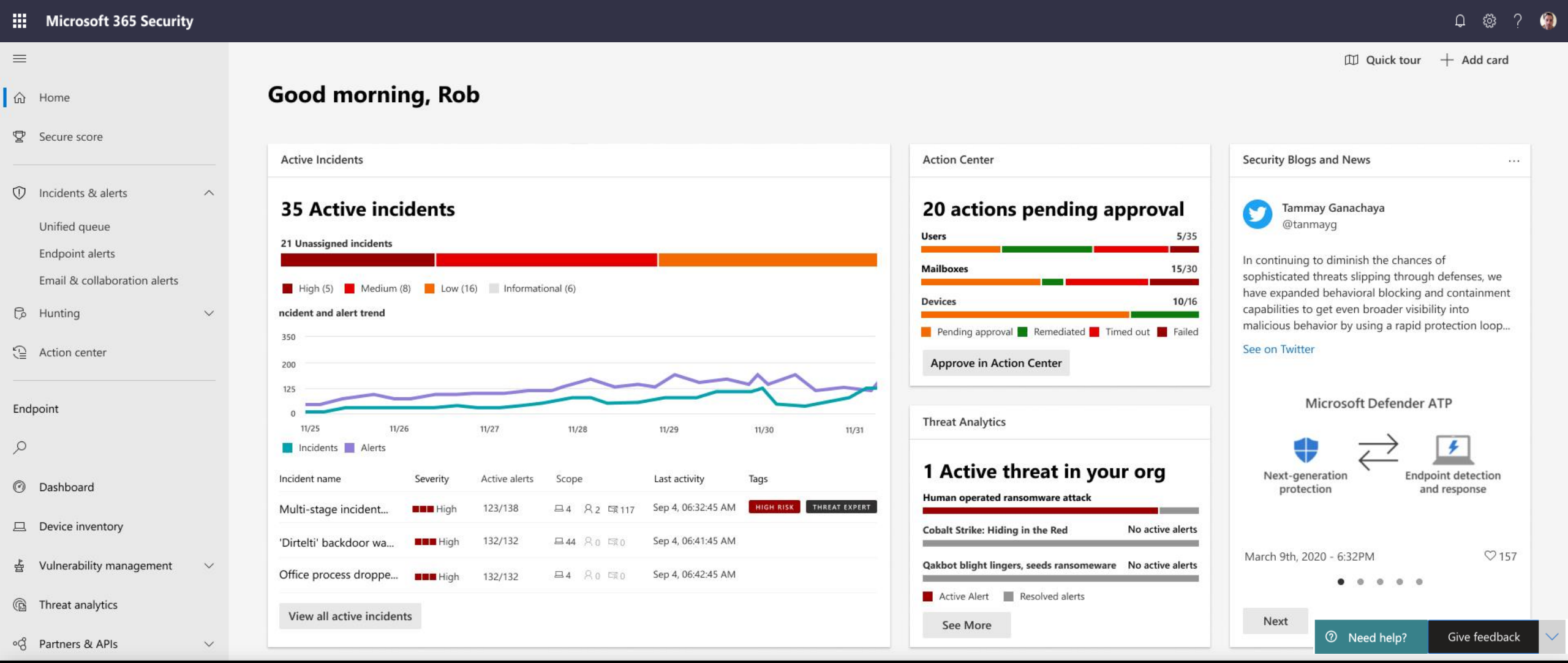
탐지 및 대응
(EDR)

자동화

자동 조사
및 조치

보안 전문가
서비스

보안 통합 관리 P1



Microsoft 365 Defender 통합 포털

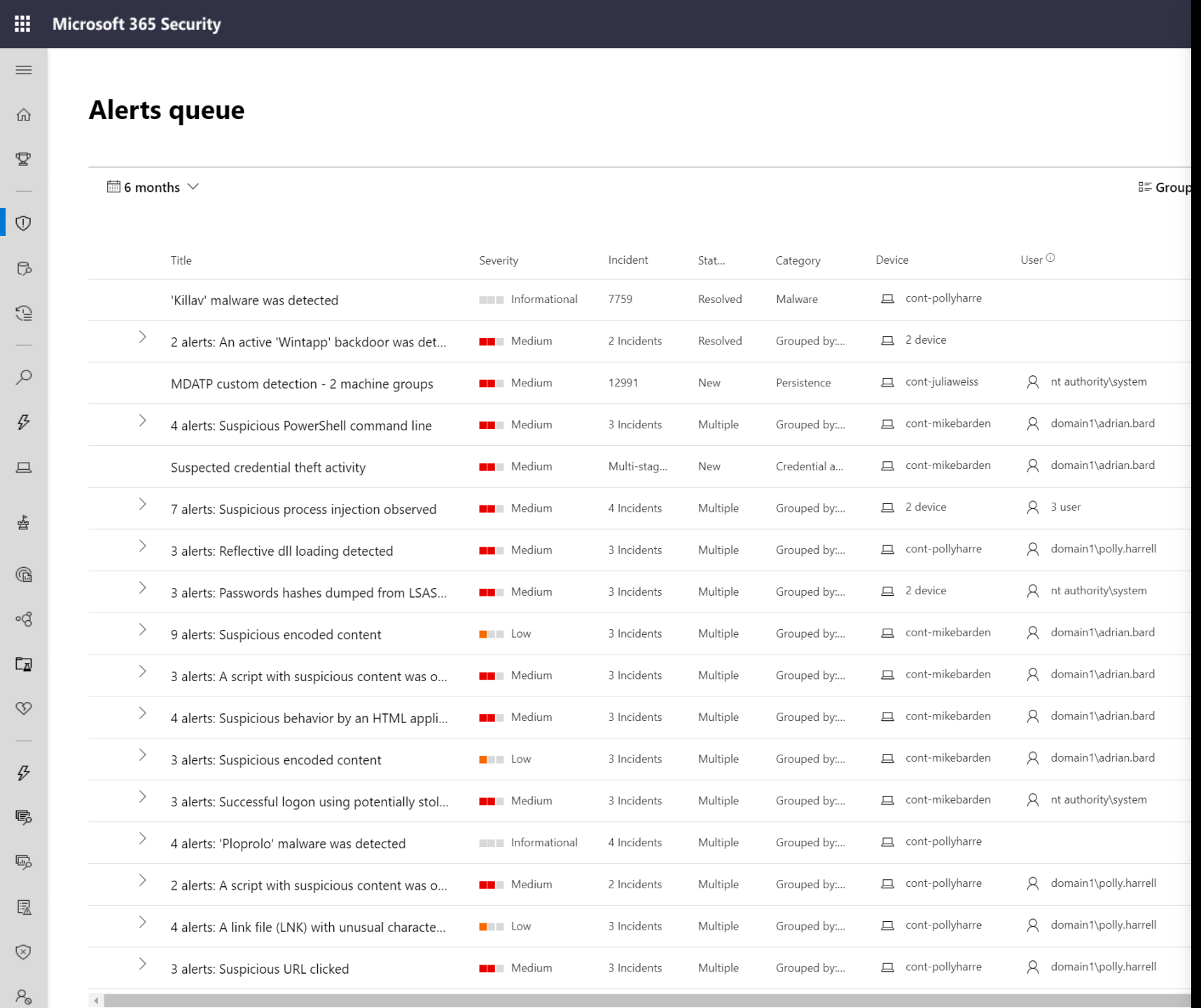
→ Microsoft 365 E5 라이선스 또는 개별 제품 E5 라이선스

→ 현재 사용 중인 E5 제품이 하나인 경우에도 Microsoft 365 Defender를 사용하고 지속적으로 확장하여 다양한 제품이 주는 가치를 활용하세요.

Microsoft 365 Defender 대시보드

→ 조직의 전반적인 보안 상태

→ 다음으로 우선순위가 높은 SOC 작업 항목은 무엇입니까?



하루 1,000건의 위협 시도

→ 평균적인 규모의 조직에서 하루에 Microsoft 365 Defender가 의심스럽거나 악의적인 시도를 마주하는 횟수

→ 매우 긴 알림 대기열...

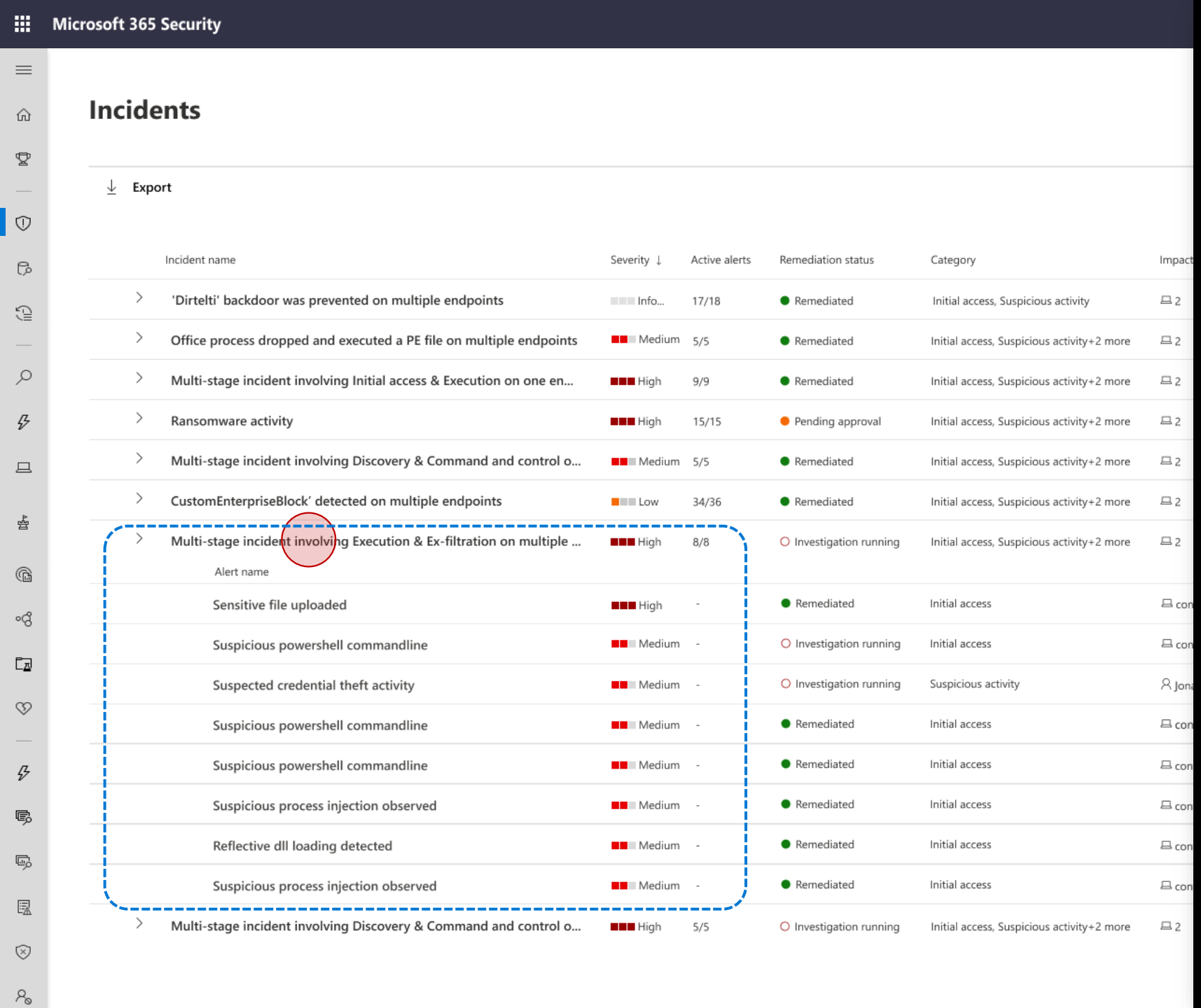
보호가 우선입니다.

→ Microsoft 365 Defender는 완벽한 보호 스택입니다!

→ Microsoft 365 도메인 전반에 걸친 협업을 통한 보호 강화

→ 70%의 시도를 완벽히 차단 - 즉각적인 SOC 조치 불필요

1,000건의 위협 시도
↓
300개의 알림



알림-인시던트

→ 동일한 공격과 관련된 알림을 단일 SOC 작업 항목으로 연결

→ 인시던트 제목이 내용 및 우선순위를 암시

→ 타사 도구 통합을 위한 인시던트 API

300개의 알림
↓
40건의 인시던트

자동 자체 복구

→ Microsoft 365 워크로드 전반에 걸친 손상된 자산의 자동 조사 및 시정

→ 75%의 인시던트를 자동 해결

40건의 인시던트
↓
10건의 인시던트

Microsoft 365 Security

Incidents > Multi-stage incident involving Initial access, Execution & Ex-filtration cross multiple assets

Summary | Alerts (25) | Devices (2) | Users (2) | Mailboxes (1) | Investigations (12) | Evidence (54)

Alerts and categories

25/25 active alerts
6 MITRE ATT&CK tactics
2 other alert categories

Jun 2, 2020, 3:57:59 PM | **New**
Suspicious URL clicked on cont-pollyharre

Jun 2, 2020, 3:58:22 PM | **New**
A link file (LNK) with unusual characteristics was opened on cont-pollyharre

Jun 2, 2020, 3:58:26 PM | **New**
Suspicious PowerShell command line on cont-pollyharre

Jun 2, 2020, 3:58:26 PM | **New**
Suspicious PowerShell command line on cont-pollyharre

Jun 2, 2020, 3:58:34 PM | **New**
A script with suspicious content was observed on cont-pollyharre

Scope

2 impacted devices
2 impacted users
1 impacted mailbox

Top impacted entities

Entity type	Risk level/investigation priority	Tags
cont-pollyharre	High	IT Team
cont-mikebarden	High	IT Team
mike.barden	No data available	Office 365 admini
adrian.bard	No data available	
polly.harrell@mtptestlab01.onmicr...	No data available	

View entities

Evidence

54 entities found

View all entities

인시던트 요약

→ 모든 공격 자료를 한 곳에 자동 수집
→ MITRE 매핑
→ 범위 & 영향 받은 엔터티
→ 관련 알림
→ 자동 복구 상태
→ 수집된 전체 증거

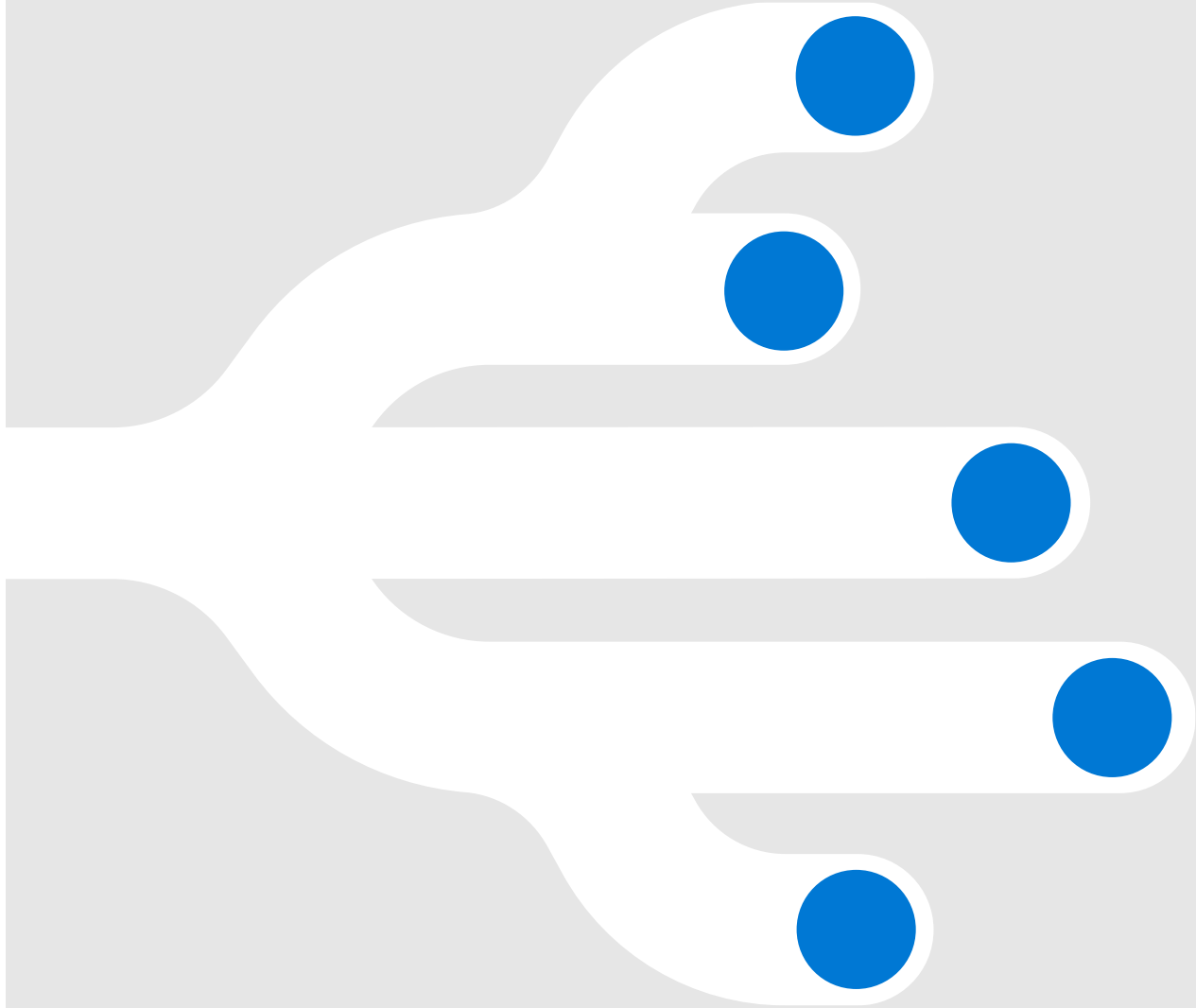
→ **보다 빠르고 효율적인 조사**

아이덴티티와 엔드포인트 보호

하이브리드 업무 환경 보호

데이터 보호

통합 보안 운영 및 자동화



디바이스 위험 기반 조건부 액세스에 대한 Intune 위협 보호

위협 방지 파트너는 다음을 감지합니다.

- 악성 앱
- 디바이스 조작
- 네트워크 익스플로잇
- 데이터 개인정보 보호 위반

EMS의 역할:
Intune이 규제 준수 평가
Azure AD가 조건부 액세스 시행

Intune Azure AD

허용
MFA 시행
디바이스 등록

Office 365
Microsoft Azure

액세스 차단
디바이스 초기화

Microsoft Defender ATP 통합

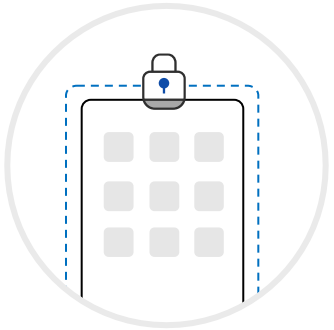
iOS 및 Android에서의 모바일 위협 방어(MTD) 파트너

Microsoft Lookout Symantec ZIMPERIUM
pradeo Google Play Protect Check Point

Intune은 대부분의 디바이스에서 데이터 보호 지원

모바일 **디바이스** 관리 (MDM)

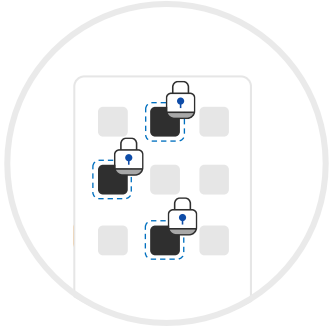
조건부 액세스:
관리형 및 규제 준수 디바이스에 대한 액세스 제한



- 관리용 디바이스 등록
- 설정, 인증서, 프로필 프로비저닝
- 디바이스 규제 준수 보고 및 측정
- 디바이스에서 기업 데이터 삭제

모바일 **애플리케이션** 관리(MAM)

조건부 액세스:
이메일 또는 파일 액세스에 사용 가능한 앱 제한



- 사용자에게 모바일 앱 게시
- 앱 구성 및 업데이트
- 앱 인벤토리 & 사용 보고
- 모바일 앱 내 기업 데이터 보호 및 제거

애플리케이션을 사용하고, 가시성을 확보하고, 안전하게 구성

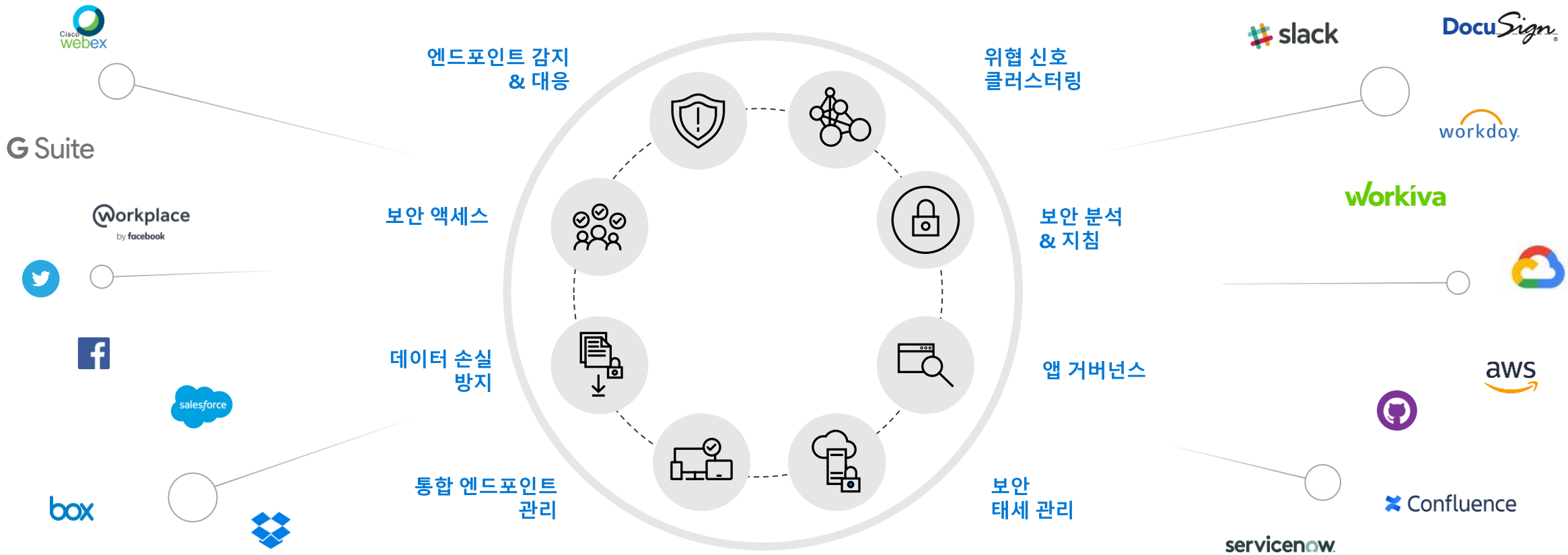
Microsoft Defender for Cloud Apps

클라우드 구현, 모니터링 및 거버넌스를 위한 필수 CASB

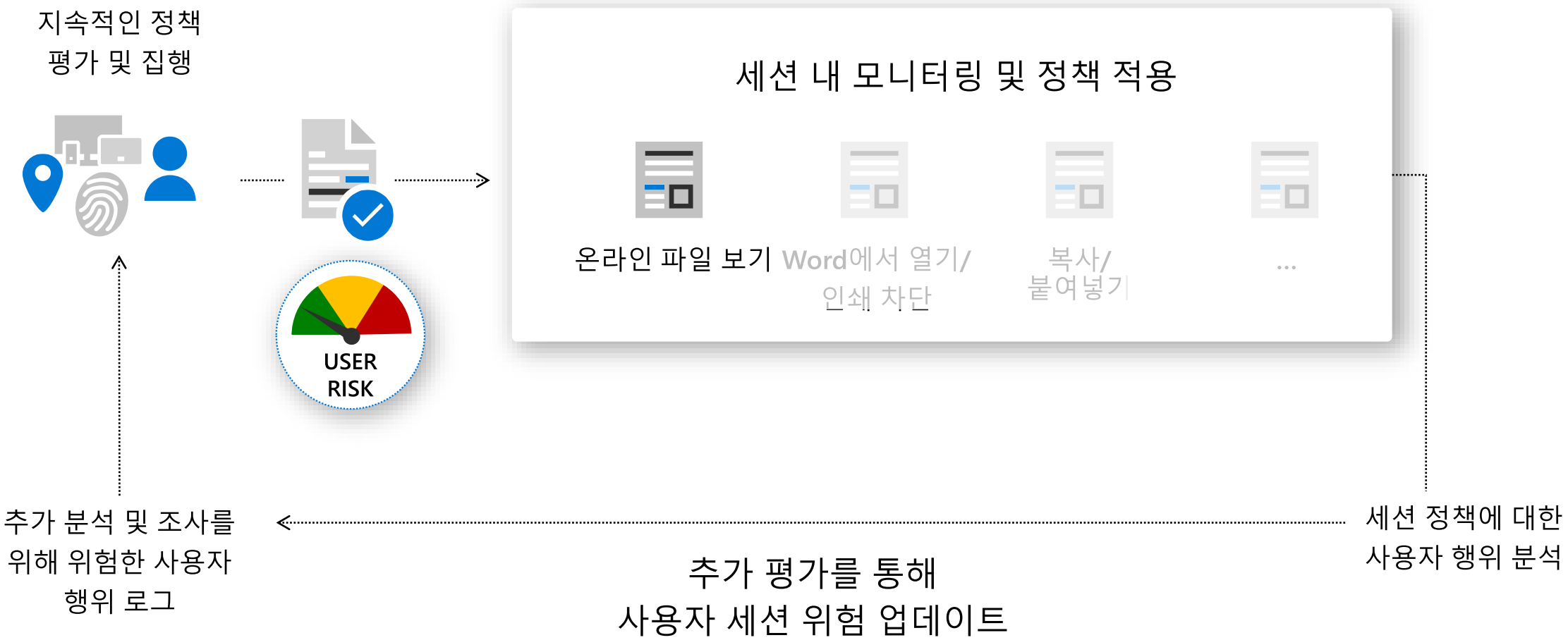
간단한 배포

광범위한 Microsoft 제품 스택과의 기본 통합을 바탕으로 한 고유한 기능

모든 앱을 지원



사용자 환경 앱 탐색 및 제어, 정책 적용을 세션으로 확장

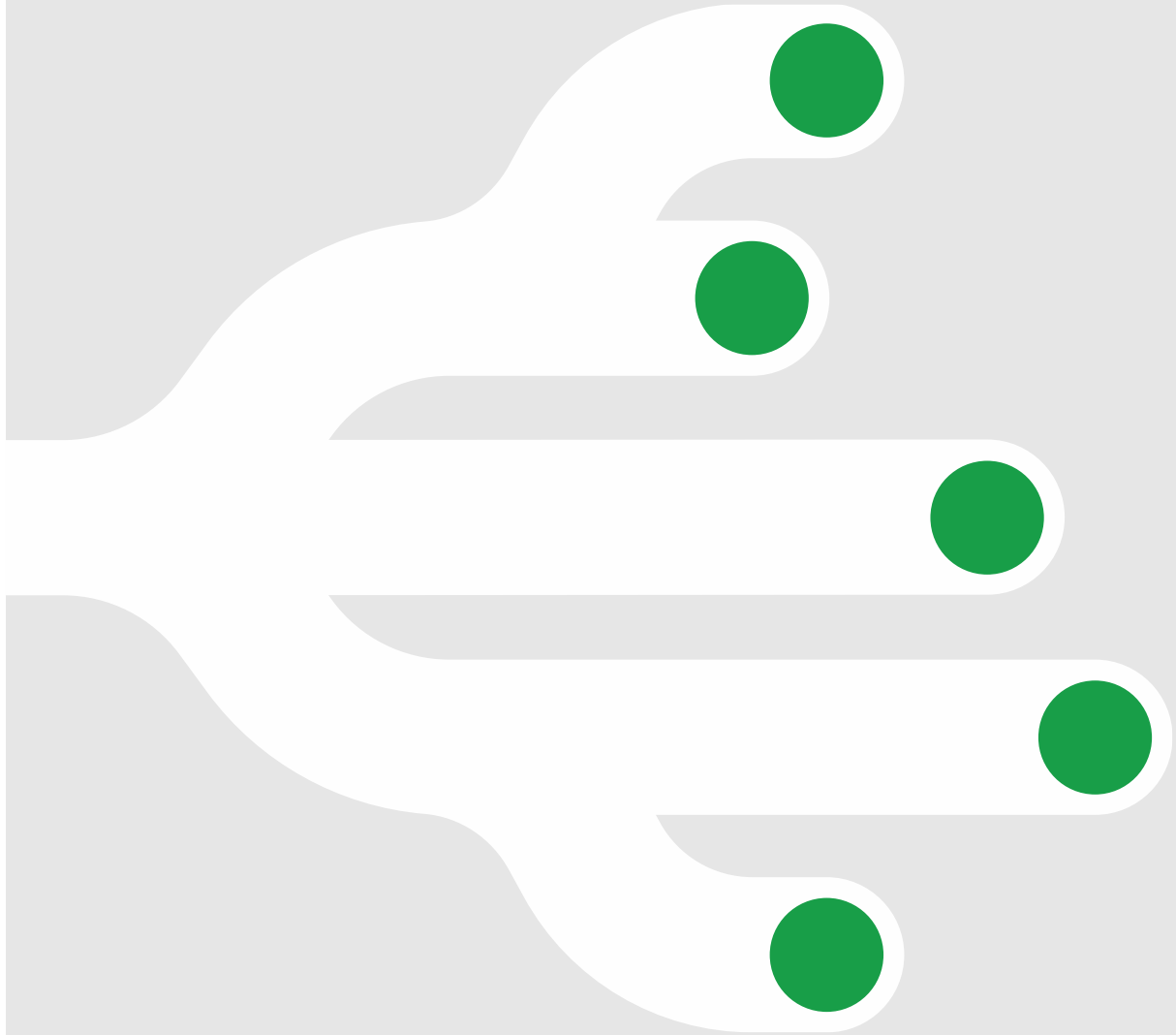


아이덴티티와 엔드포인트 보호

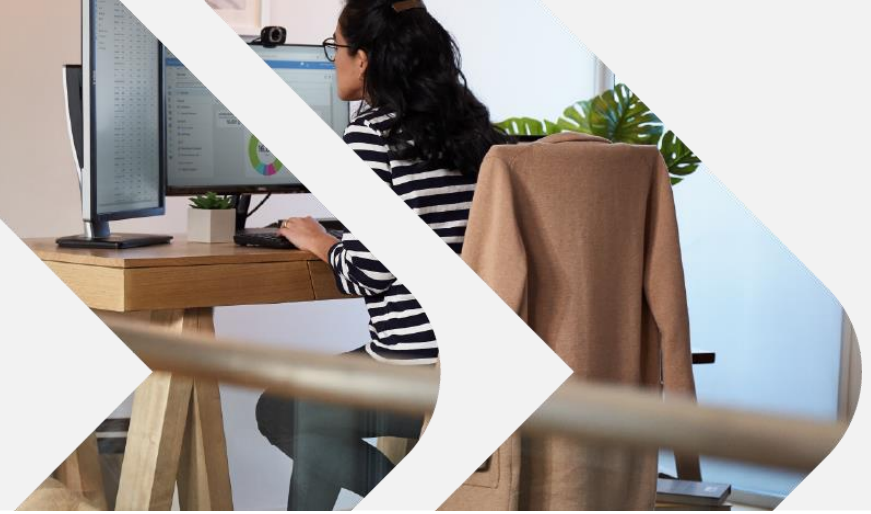
하이브리드 업무 환경 보호

데이터 보호

통합 보안 운영 및 자동화



데이터 액세스는 전통적인 비즈니스 경계를 벗어나 진화하고 있습니다.

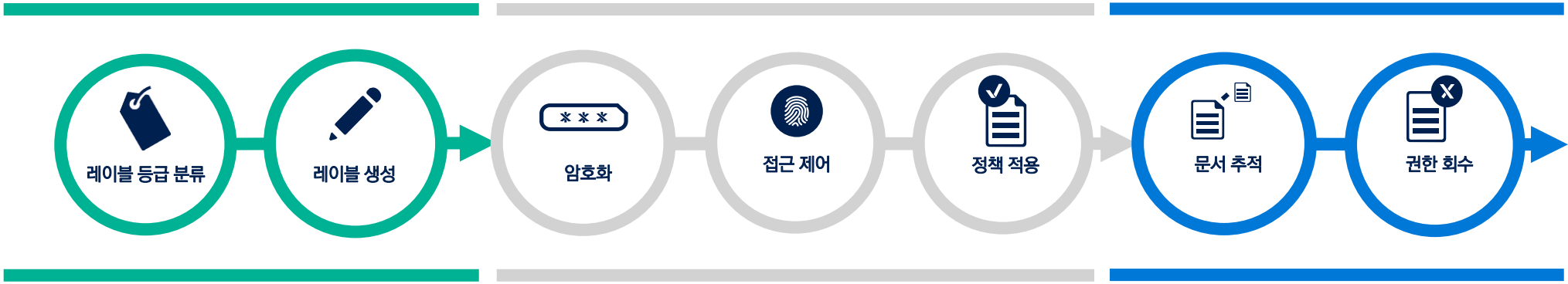


다양한 클라우드

다양한 앱

다양한 플랫폼

중요 정보유형을 분류 및 레이블을 정의한 후, 정보유출에 대한 관리



주요기능

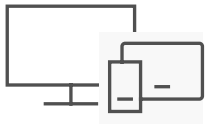
- 보안 등급에 따른 레이블 체계 분류
- 등급별 레이블 생성 (예, 일반, 대외비 등)

주요기능

- 레이블 별 정책 설정
  - 암호화 여부
  - 접근 가능한 사용자 지정
    (내부인/외부인, 특정 사용자/그룹/도메인)
  - 사용자별 권한 지정
    (읽기, 편집, 저장, 인쇄, 복사 및 붙여넣기 등)

주요기능

- 누가 문서에 접근했는지 추적
- 필요에 따라 접근 권한 회수
  (기능 지원하는 파일 포맷 제한)



디바이스

애플리케이션

클라우드

온프레미스

Purview Information Protection 기반 정보 유출 탐지 및 예방

Windows
MacOS
iOS
Android

Office 365

Endpoint DLP

클라우드 업로드
앱 제어
USB 드라이브
네트워크
인쇄
클립보드
블루투스
RDP

데이터 분류 서비스

민감 정보 유형

기본 제공
CCN/SSN/라이선스
이중 키 암호화
명명 엔터티
템플릿 10종(금융, IP, 법률, 헬스케어...)

맞춤형
RegEx
사전
지문
EDM

학습 가능한 분류자
샘플 콘텐츠
테스트
검증
게시

민감도 레이블

공개
일반
기밀
...

SDK를 통해 타사 도구로 확장 가능

Defender for Cloud Apps

온프레미스

Microsoft Purview 데이터 거버넌스 서비스

ADLS
SQL DB
Azure Files
Blob
Cosmos DB
S3

고급 규제 준수 솔루션

eDiscovery(프리미엄)
Insider Risk Management
Communication Compliance
Microsoft Priva

데이터 보안 사고는 언제 어디서나 발생 가능

데이터가 생성되고 데이터가 이동할 때 위협 요소를 검증합니다.

Email

이메일을 통해 기밀 파일을 받음

Messages

Teams를 통해 몇몇 동료와 파일 사본 공유

Cloud apps

외부 공급업체와 공유하기 위해 개인 Dropbox 계정에 사본을 업로드했습니다.

Devices

오프라인으로 작업하기 위해 파일 사본을 장치에 다운로드했습니다.

부주의

Data expose → Data leak → Data hoarding

Shared storage

SharePoint에서 비정상적인 양의 기밀 파일 다운로드 및 삭제

Email

이메일을 통해 외부 수신자에게 한 파일의 사본을 보냈습니다.

Cloud apps

두 개의 기밀 파일을 개인 Dropbox 계정에 업로드했습니다.

Devices

기밀 파일 1개 인쇄기밀 파일 3개를 USB에 저장

Malicious

Data sabotage → Data theft → Data theft → Data theft

Insider Risk Management 개요

가장 중요한 위험을 지능적으로 탐지하고 완화

프라이버시 보호

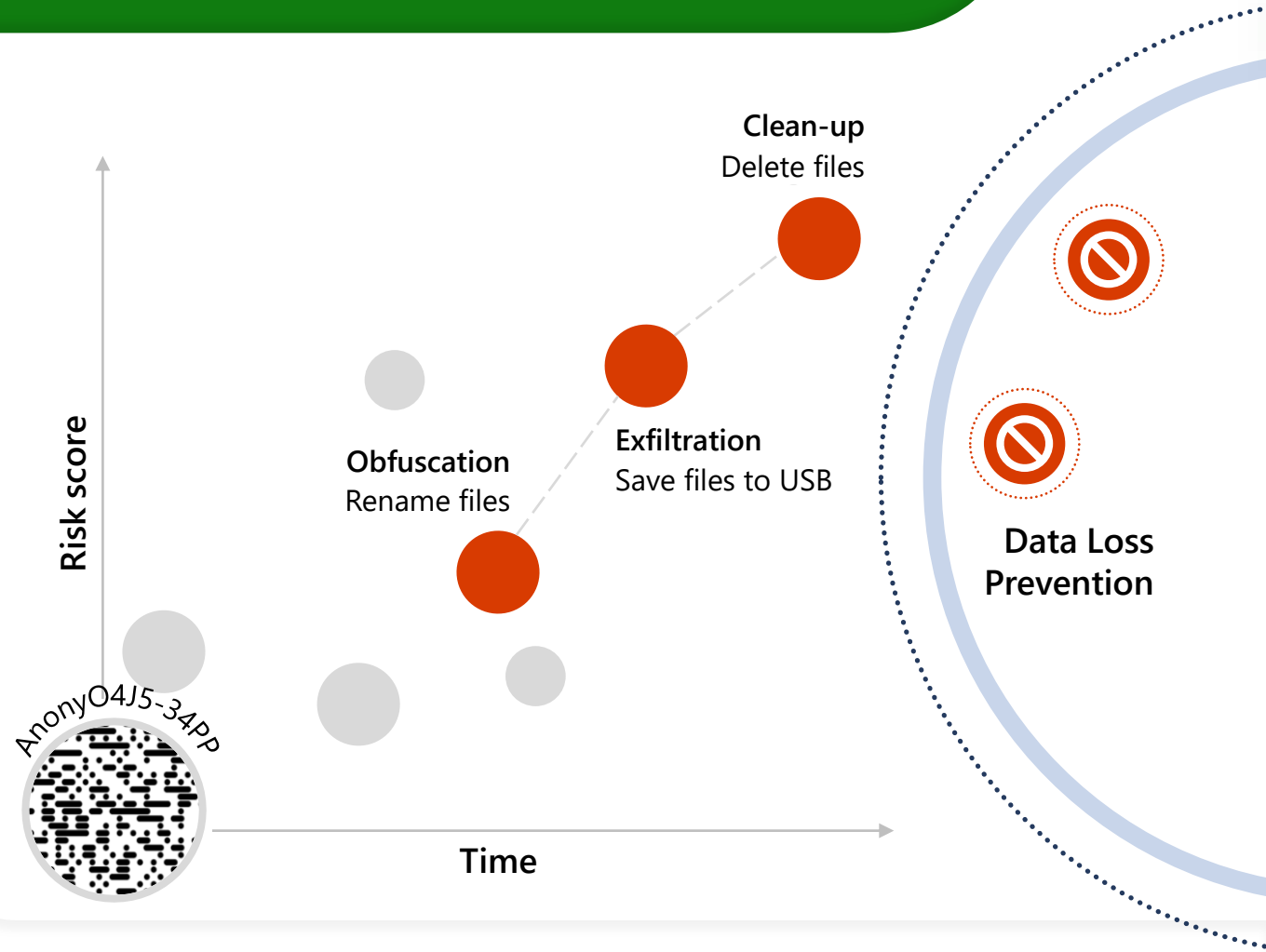
사용자 신뢰를 보호하고 가명화 및 강력한 개인 정보 보호 제어를 통해 전체적인 내부자 위험 프로그램을 구축합니다.

쉬운 배포 및 운영

엔드포인트 에이전트가 필요하지 않은 100개 이상의 빌트인된 기계 학습 모델 및 지표로 숨겨진 위험을 식별합니다.

자동화된 적응형 조치

DLP 제어를 동적으로 적용하는 강화된 조사 및 Adaptive Protection(적응형 보호)으로 완화를 촉진합니다.



머신러닝을 활용하여 행위 이벤트 중에서 가장 중요한 내부자 위험 식별

컨텍스트 파악
이벤트 상관 분석

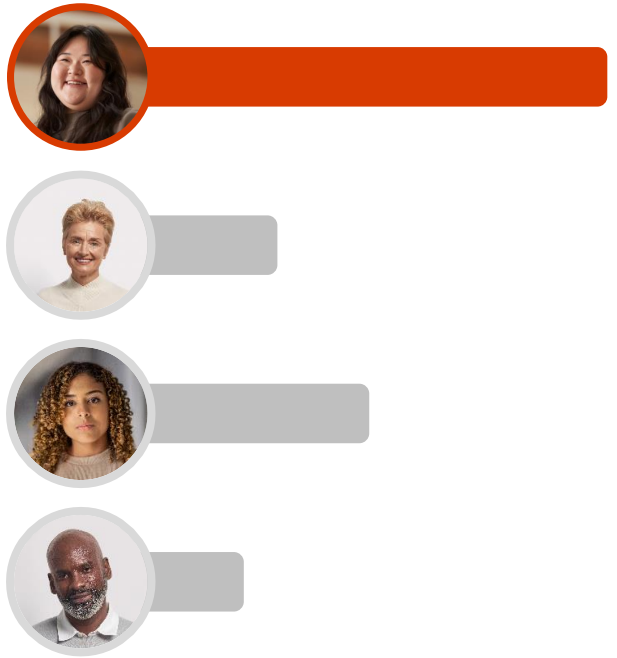
행위 의도 이해
전체 시퀀스 탐지

Obfuscation
Downgrade labels

Clean-up
Delete files

Exfiltration
Save files to a USB

벤치마킹
이상 징후 탐지

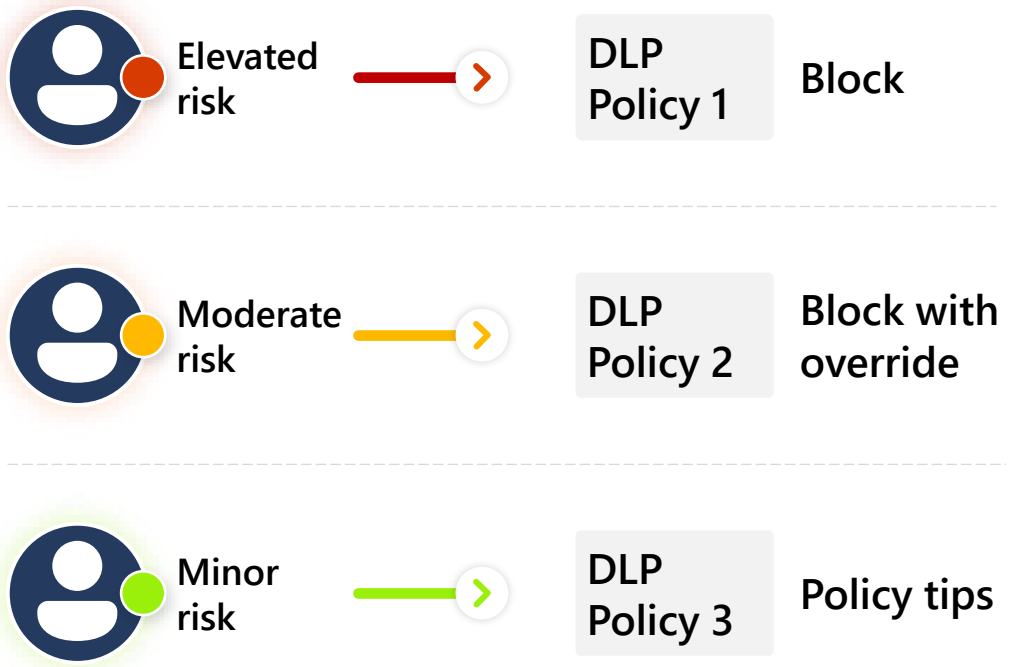


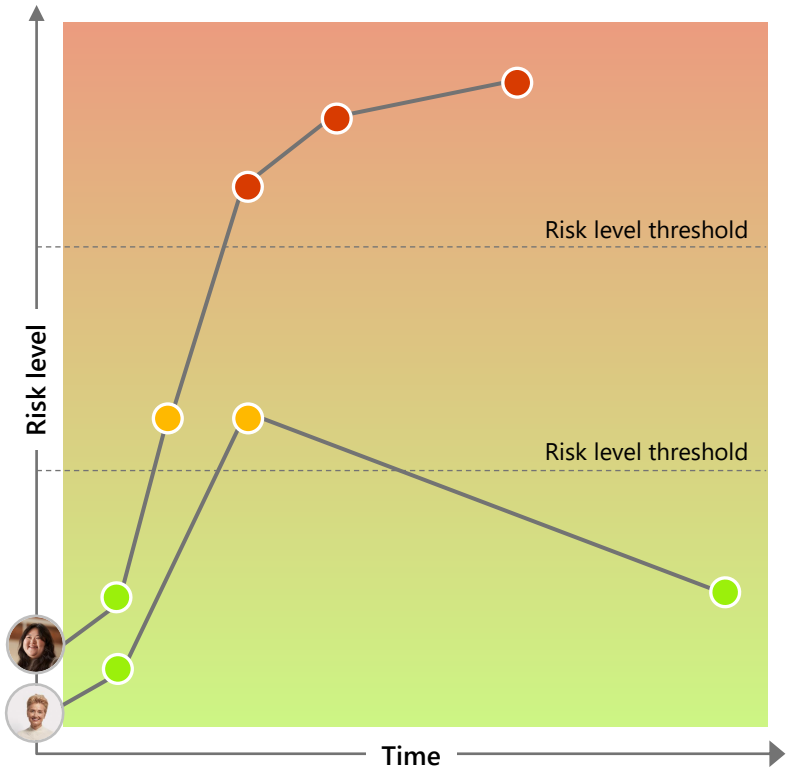
Adaptive Protection으로 탐지 및 조치 시간 개선

감지된 위험 수준에 따라 적절한 DLP 정책을 동적으로 할당

높아진 내부자 위험을 자동으로 완화합니다.

다른 사람들은 생산성을 유지하고 적절한 데이터 처리 모범 사례에 대해 교육합니다.



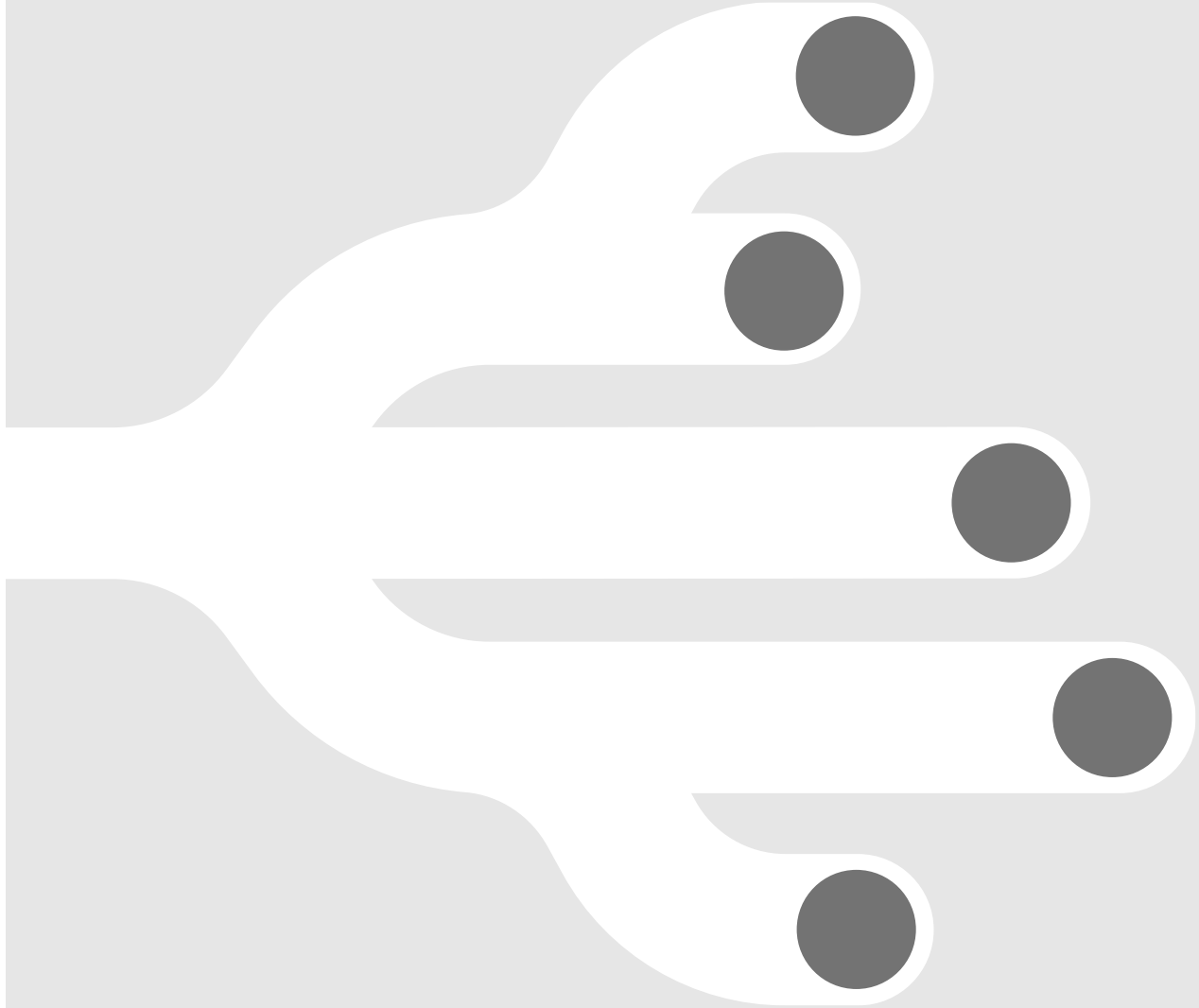


아이덴티티와 엔드포인트 보호

하이브리드 업무 환경 보호

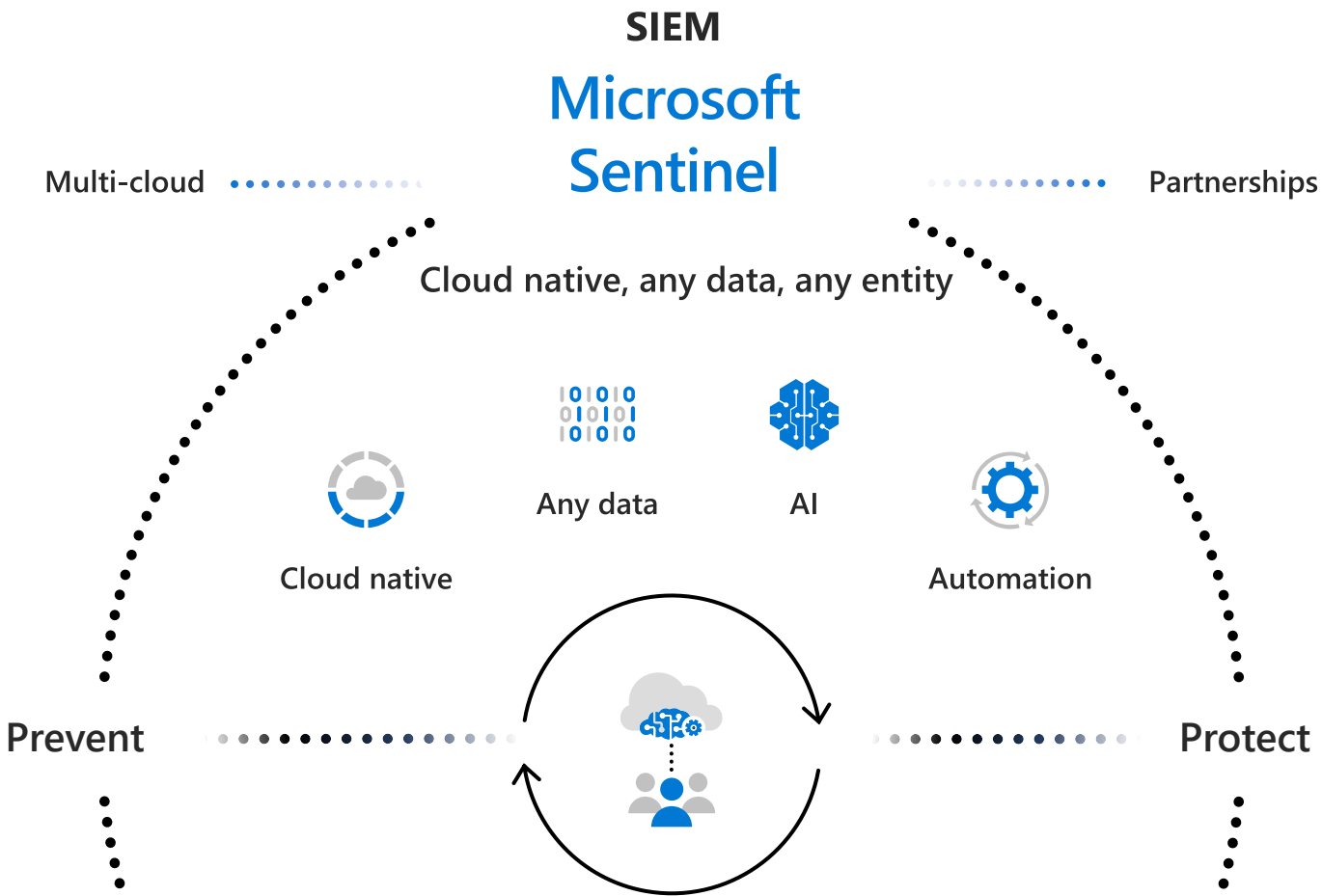
데이터 보호

통합 보안 운영 및 자동화



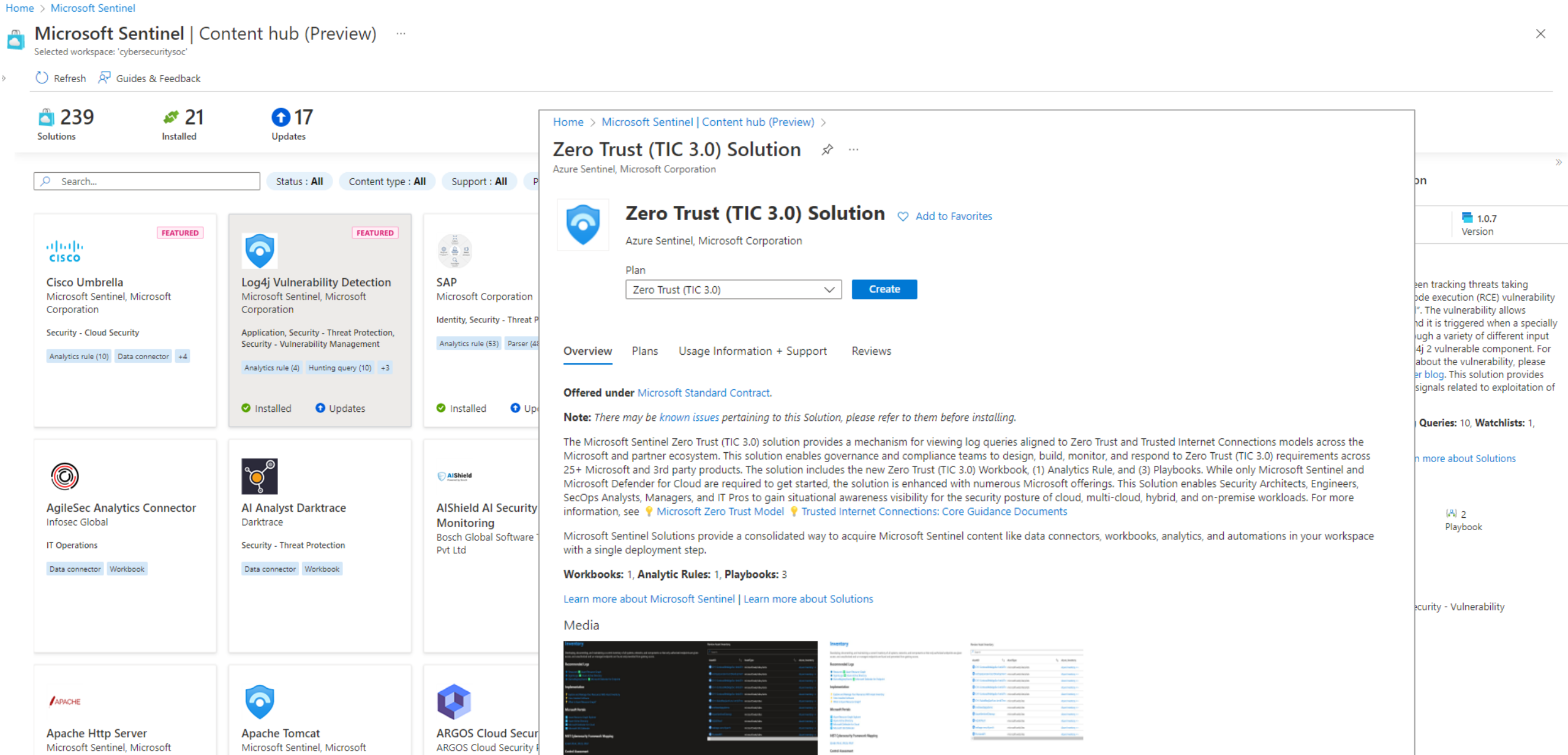
Microsoft Sentinel 기업 전반에 걸쳐 인사이트 확보

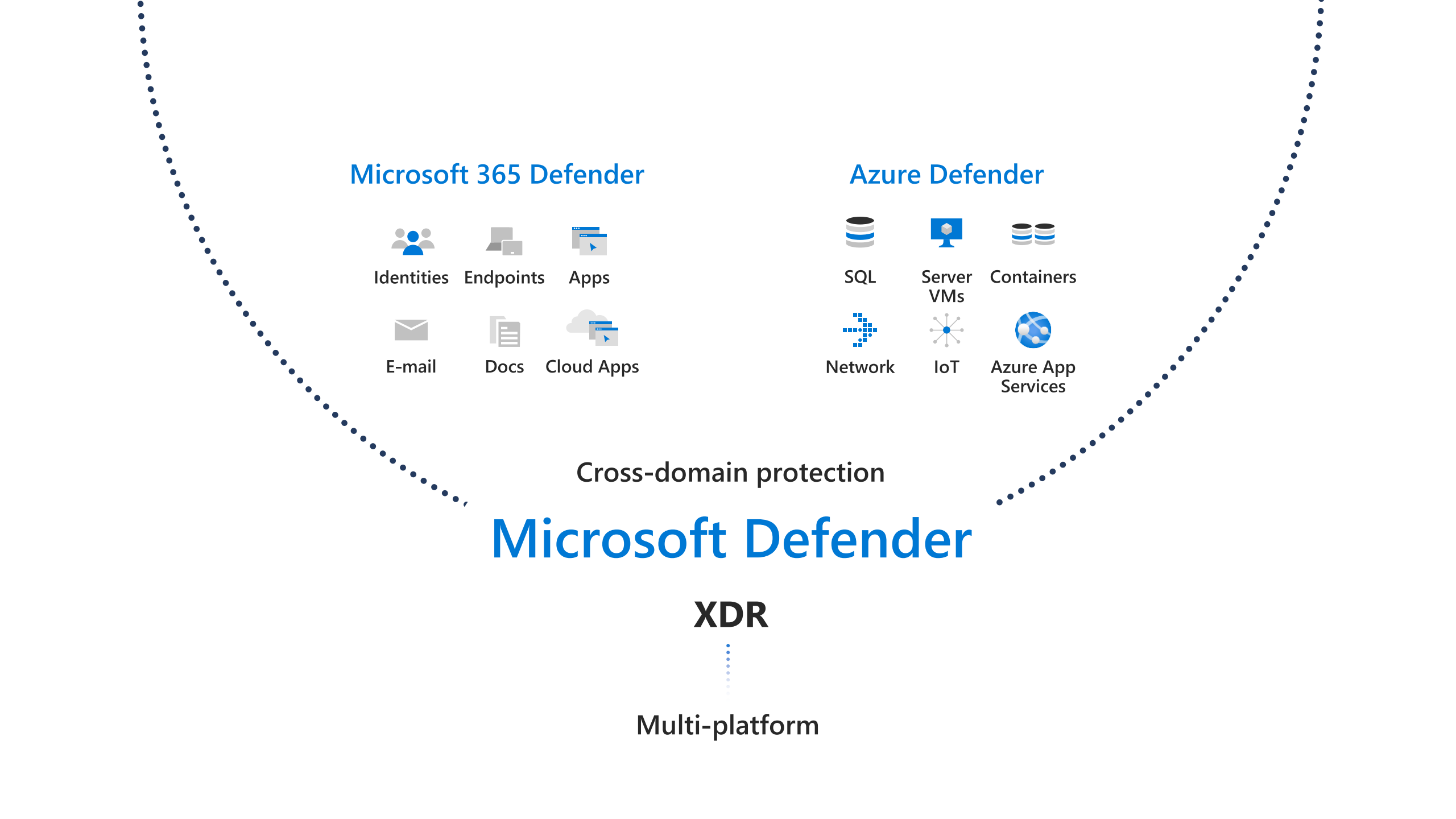
클라우드 네이티브 SIEM으로 공격 체인 시각화 및 조사

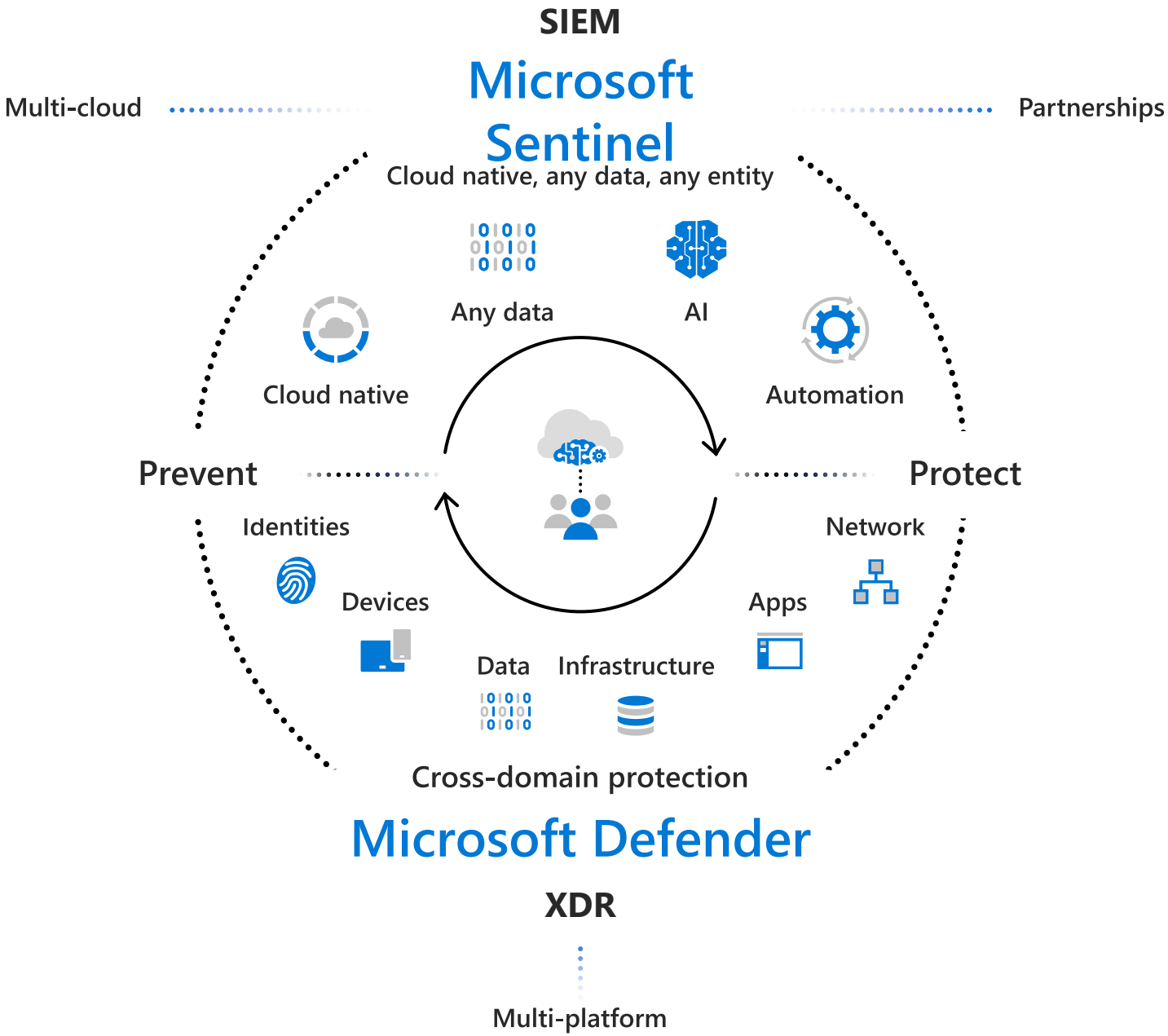


- 클라우드 규모에서 보안 데이터를 수집하고 기존 도구와 통합
- AI를 활용하여 긴급 위협을 탐지하고 경고 피로도를 90%까지 줄입니다.
- 빌트인된 오케스트레이션 및 자동화로 신속하게 대응

Microsoft Sentinel TIC 3.0 제로 트러스트 프레임워크




Microsoft 365 Defender
Identities
Endpoints
Apps
E-mail
Docs
Cloud Apps
Azure Defender
SQL
Server VMs
Containers
Network
IoT
Azure App Services
Cross-domain protection
Microsoft Defender
XDR
Multi-platform


SIEM
Microsoft Sentinel
Multi-cloud
Partnerships
Cloud native, any data, any entity
Any data
AI
Cloud native
Automation
Prevent
Protect
Identities
Network
Devices
Apps
Data
Infrastructure
Cross-domain protection
Microsoft Defender
XDR
Multi-platform

Thank you

Microsoft Korea - STU Security

OFFICE 02-531-8185
FAX 02-531-4600
E-mail krstusec@microsoft.com