Microsoft 365

엔드포인트 용 Microsoft Defender

Firstname Lastname
Job title

현행 라이선스 : Microsoft 365 E5 Security*

M365 E5 Security

Microsoft Defender for Office 365 Plan 2	강력한 제로 데이 보호 기능을 제공하여 알려지지 않은 멀웨어 및 바이러스로부터 조직을 보호하고 유해한 링크로부터 실시간으로 조직을 보호하는 기능을 포함한 클라우드 기반 전자 메일 필터링 서비스입니다. Plan1 외에도 Plan 2는 자동화된 조사 및 대응, 위협 추적기 및 공격 시뮬레이터를 제공합니다.
Microsoft Defender for Cloud Apps	멀티모드 CASB(Cloud Access Security Broker)입니다. 풍부한 가시성, 데이터 이동 제어 및 정교한 분석 기능을 제공하여 클라우드 서비스 전반에서 사이버 위협을 식별하고 방지합니다.
Azure Active Directory Plan 2	직원들이 로그인하고 리소스에 액세스할 수 있도록 지원하는 마이크로소프트의 클라우드 기반 ID 및 액세스 관리 서비스. P2는 Free 및 P1 기능 외에도 앱과 중요한 회사 데이터에 대한 위험 기반 조건부 액세스를 제공하는 Identity Protection과 관리자와 관리자의 리소스 액세스를 검색, 제한 및 모니터링하고 필요할 때 적시에 액세스할 수 있도록 지원하는 Priviled Identity Management를 제공합니다.
Microsoft Defender for Identity	사내 Active Directory 신호를 활용하여 조직에 대한 지능적 위협, 손상된 신원 및 악의적인 내부자 조치를 식별, 탐지 및 조사하는 클라우드 기반 보안 솔루션입니다.
Microsoft Defender for Endpoint Plan 2	예방적 보호, 위반 후 탐지, 자동화된 조사 및 대응을 위한 통합 엔드포인트 보안 플랫폼입니다. 이 제품은 위협 및 취약성 관리, 외과적으로 공격 표면을 줄이기 위한 도구, 위협 및 멀웨어 차단을 위한 차세대 보호, 지능적 공격을 탐지하기 위한 엔드포인트 탐지 및 대응, 위협에 대한 자동화된 조사 및 교정, 위협 관리 추적 서비스를 제공합니다.
Safe Documents**	Microsoft Defender for Endpoint를 사용하여 보호 보기 또는 Application Guard에서 열린 문서 및 파일을 검색하여 사용자가 열기 전에 Office 문서(Excel, PowerPoint, Word etc.)를 "알려진 위험 및 위협 프로필"에 대해 자동으로 검사합니다.
Application Guard for Office 365*	신뢰할 수 없는 문서를 격리하여 악의적이고 잠재적으로 유해한 위협으로부터 사용자를 보호합니다. 위험을 무릅쓰고 사용자가 악의적인 문서를 발견하면 해당 문서는 안전하게 격리됩니다.

* 브랜드 변경에 대한 자세한 내용은 참고 사항을 참조하십시오.
** Microsoft 365 E5 또는 Microsoft 365 E5 보안을 통해서만 제공가격 – ERP/사용자별/월별

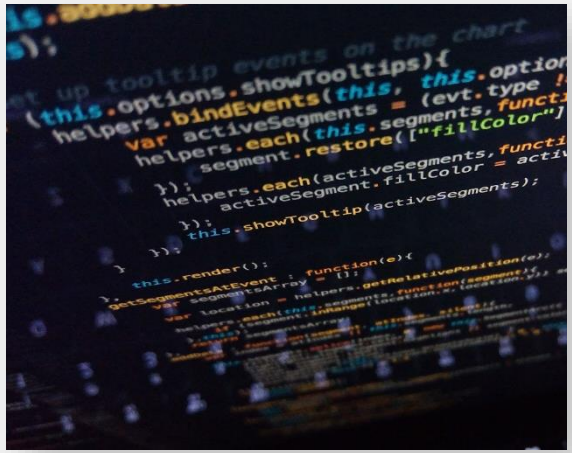
보호	Microsoft Defender in Active Mode	Microsoft Defender in Passive Mode	EDR in Block Mode
Real time protection	Yes	No	No
Cloud delivered protection	Yes	No	No
Attack Surface Reduction	Yes	No	No
File scanning and detection information	Yes	Yes	Yes
Threat remediation	Yes	When Microsoft Defender Antivirus is in passive mode, threat remediation features are active only during scheduled or on-demand scans.	Yes
Security intelligence updates	Yes	Yes	Yes

Defender AV가 active 일 때 지원되는 기능

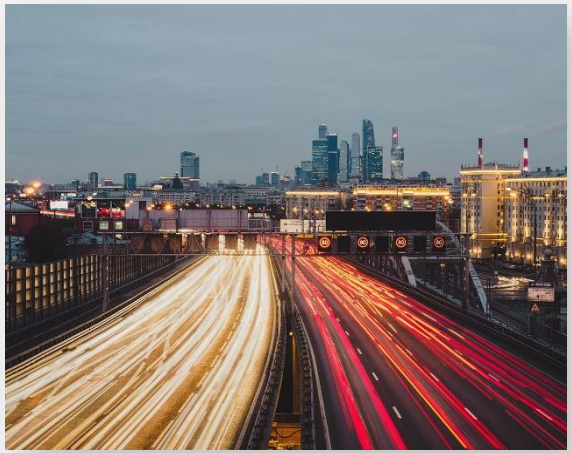
- Antivirus 시그널 공유
- 디바이스에 대한 Threat analytics 및 점수
- 성능
- 차단된 멀웨어에 대한 상세 내역
- 네트워크 보호
- 파일 차단
- 공격 표면 감소
- 감사(audit) 이벤트
- OneDrive를 통한 파일 복구
- 기술 지원

변화의 시대

이제는 모두가 기술 사업에 속함



기존 보안 도구는 속도를 맞추지 못함

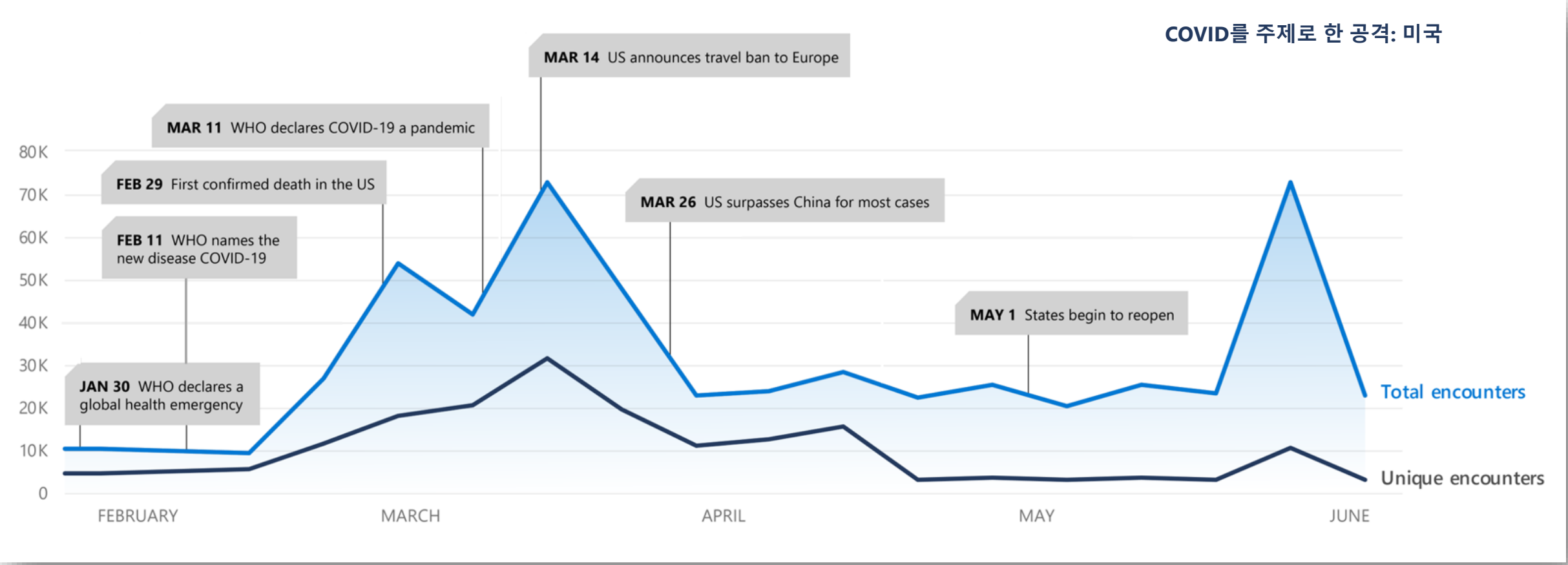


보안 전문가만으로는 그 공백을 메울 수 없음

규제 요구사항 및 비용이 증가함

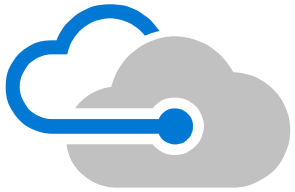
오늘날의 위협: 범죄 집단이 기회를 쫓아 움직임

뉴스 헤드라인과 일치하는 멀웨어 발생



Source: Microsoft Digital Defense Report 2020

우리가 다른 이유



에이전트 없는 클라우드 기반

추가적인 배포 또는 인프라가 없음. 지연 또는 업데이트 호환성 문제가 없으며 항상 최신 상태.

비교할 수 없는 가시성

기기, ID 및 정보 전반에 걸친 위협 및 공유 신호에 대한 업계 최고의 통찰력을 기반으로 구축.

자동화된 보안

몇 분 만에 경고에서 문제 해결로, 규모에 맞게 보안 수준을 한 차원 높이십시오.

엔드포인트 보안 분야의 업계 리더

Gartner는 2019년 **Endpoint Protection Platforms Magic Quadrant**에서 **Microsoft**를 리더로 선정.

Forrester는 2020년 **Enterprise Detection and Response Wave**에서 **Microsoft**를 리더로 선정.

MITREATT&CK 평가에서 **Microsoft Threat Protection**이 **실제 탐지에 있어 선도**.

악성코드 방지 기능은 독립적인 테스트에서 **지속적으로 높은 점수를 획득**.

Microsoft Defender ATP는 2020년 엔드포인트 보안 리뷰에서 **SC Media**의 **완벽한 별 5개 등급 평가**를 받음.

Microsoft는 RSAC 2020에서 **Cyber Defense Magazine**으로 **6 개의 보안 상을 수상**:

- ✔ 애플리케이션 격리 – Next Gen
- ✔ 엔드포인트 보안 – Editor's Choice
- ✔ 위협 및 취약성 관리 – Most Innovative
- ✔ 악성코드 탐지 – Best Product
- ✔ 관리되는 탐지 및 대응 – Market Leader
- ✔ 엔터프라이즈 위협 보호 – Hot Company

플랫폼 전반에서 엔드포인트 보안성 기능 제공

Windows macOS

Endpoints and servers

iOS

Mobile device OS

Windows 365
Azure Virtual Desktop

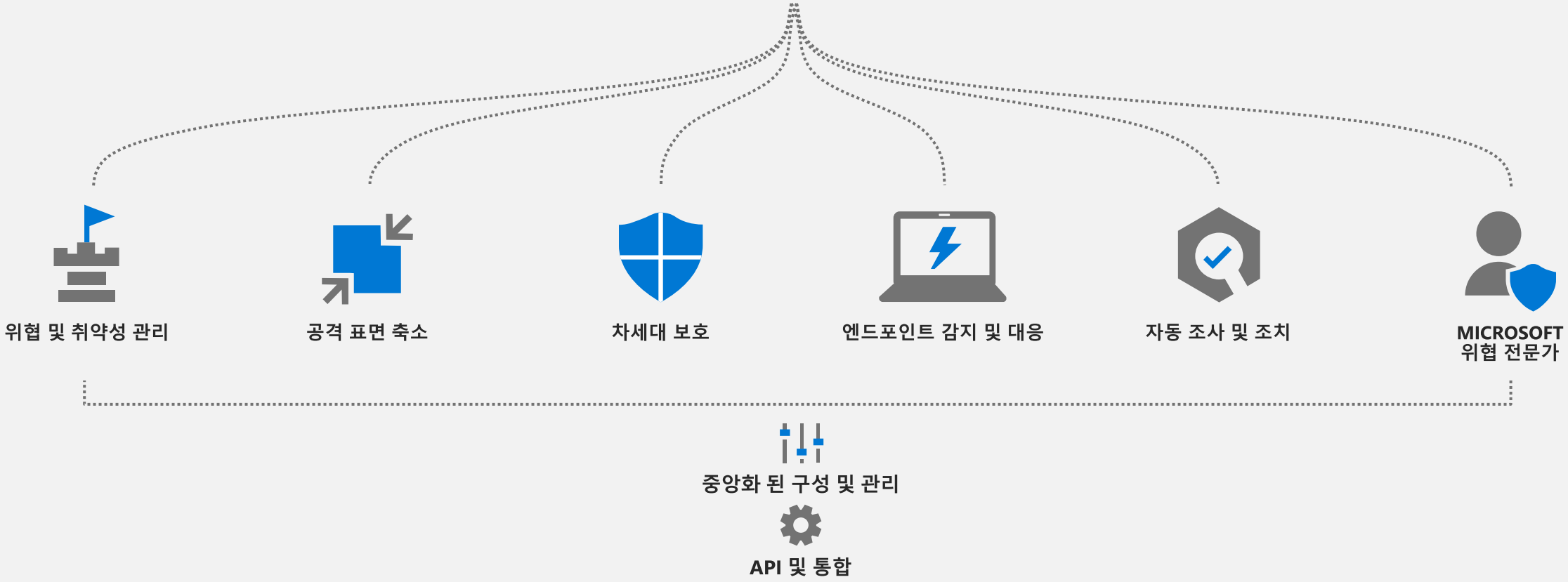
Virtual desktops

Cisco
Juniper Networks
HP Enterprise
Palo Alto Networks

Network devices

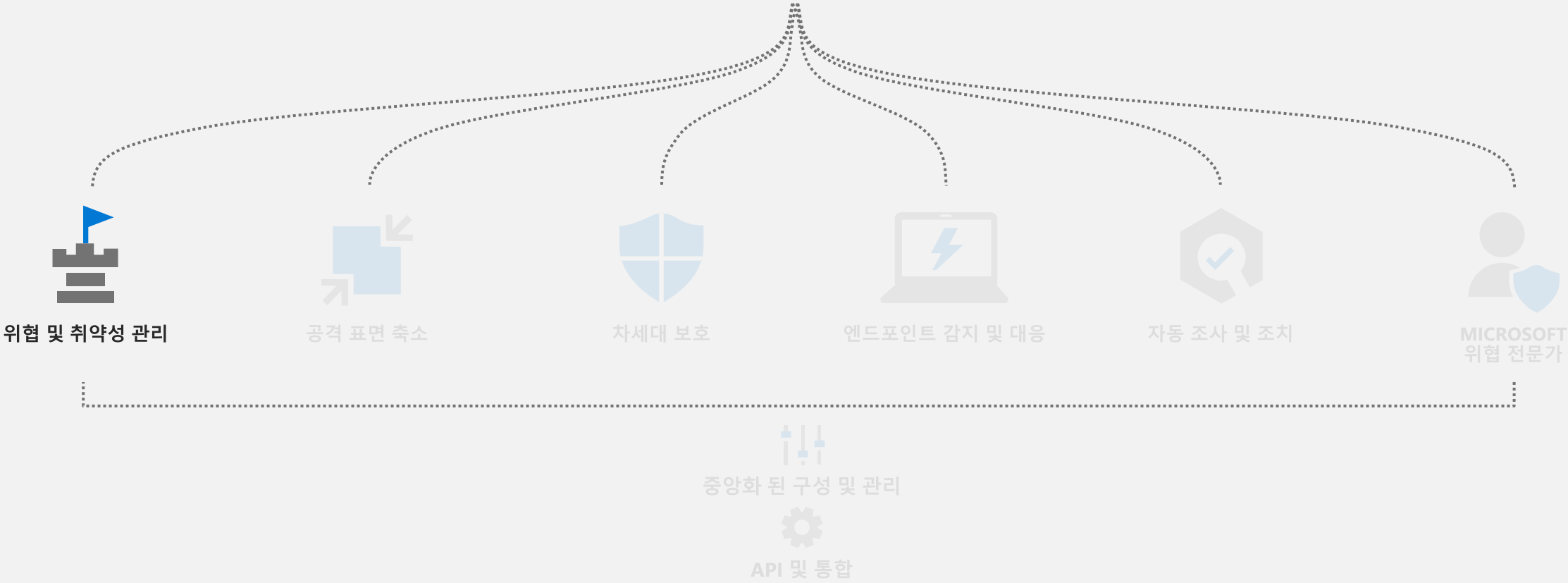
엔드포인트 용
Microsoft Defender

클라우드 기반의 내장된.



엔드포인트 용
Microsoft Defender

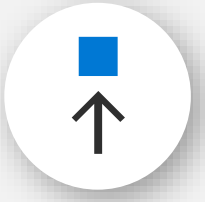
클라우드 기반의 내장된.



고객의 주요 당면 과제

발견

- 주기적인 스캐닝
- 사각지대
- 런타임 정보 없음
- “정적인 스냅샷”



우선 순위 지정

- 심각도 기준
- 누락된 조직 컨텍스트
- 위협 보기가 없음
- 대규모 위협 보고서

보상

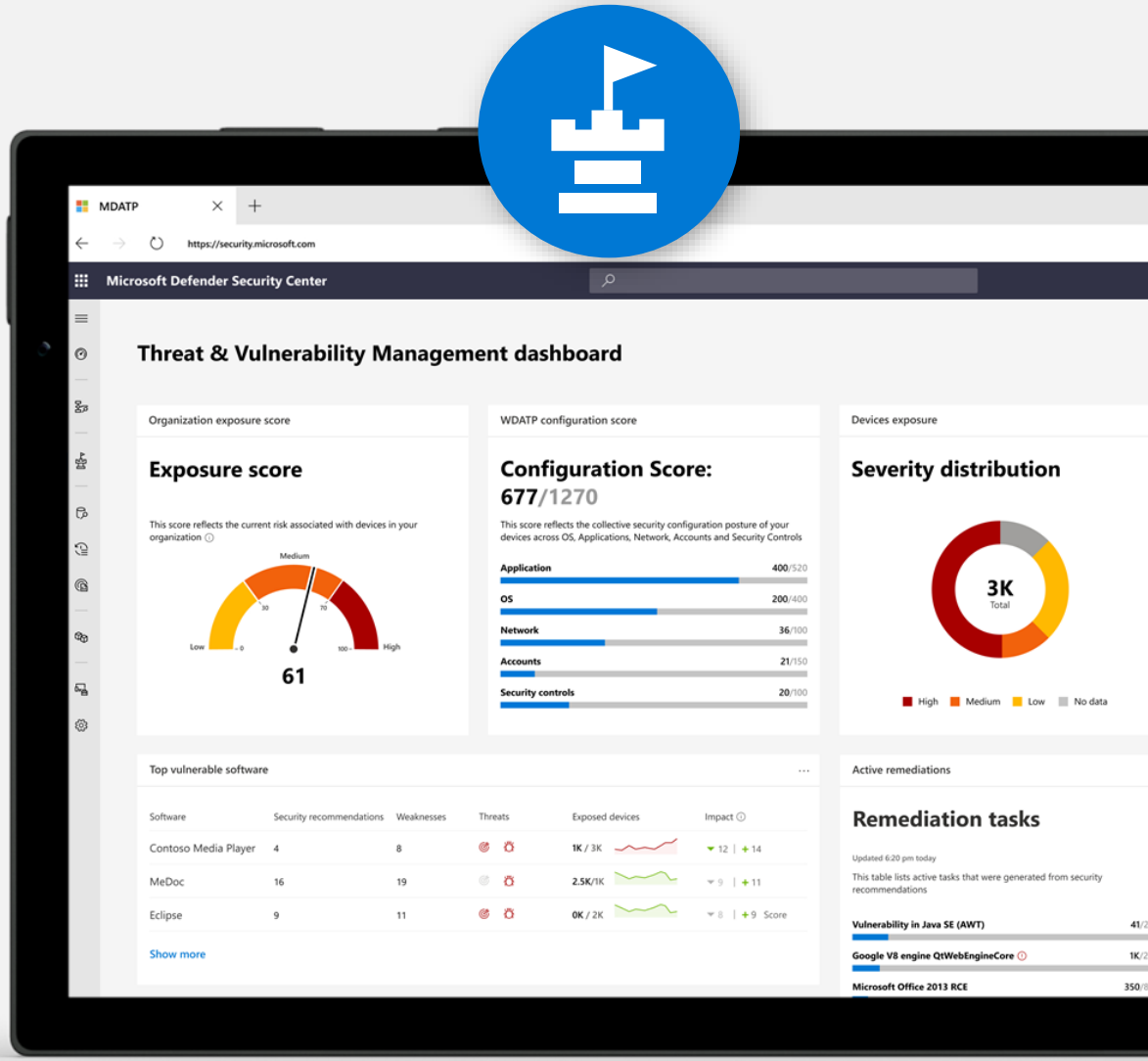
- 패치 대기중
- IT/보안 브리지 없음
- 수동적인 프로세스
- 검증 없음

높은 유지 관리 비용에도 불구하고 조직은 여전히 매우 취약

위협 및 취약성 관리

취약성 관리 프로그램을 성숙시키기 위한 위험 기반 접근 방식

1. 지속적인 실시간 검색
2. 상황을 인식한 우선 순위 지정
3. 내장된 엔드 투 엔드 조치 프로세스



1

지속적인 발견

전체 스택에 대한 광범위한 취약성 평가

악용하기 가장 쉬움

애플리케이션 확장 취약성

애플리케이션 내의 구성 요소와 관련된 애플리케이션에 특화된 취약성.
예: Grammarly Chrome Extension (CVE-2018-6654)

애플리케이션 런타임 라이브러리 취약성

응용 프로그램에 의해 로드되는 런타임 라이브러리에 존재(종속성).
예: Electron JS 프레임워크 취약성 (CVE-2018-1000136)

애플리케이션 취약성 (1st 및 3rd party)

평상시 발견되고 악용.
예: 7-zip 코드 실행(CVE-2018-10115)

OS 커널 취약성

OS 악용 완화 제어로 인해 최근 몇 년 동안 점점 더 많은 인기를 얻고 있음.
예: Win32 권한 상승(CVE-2018-8233)

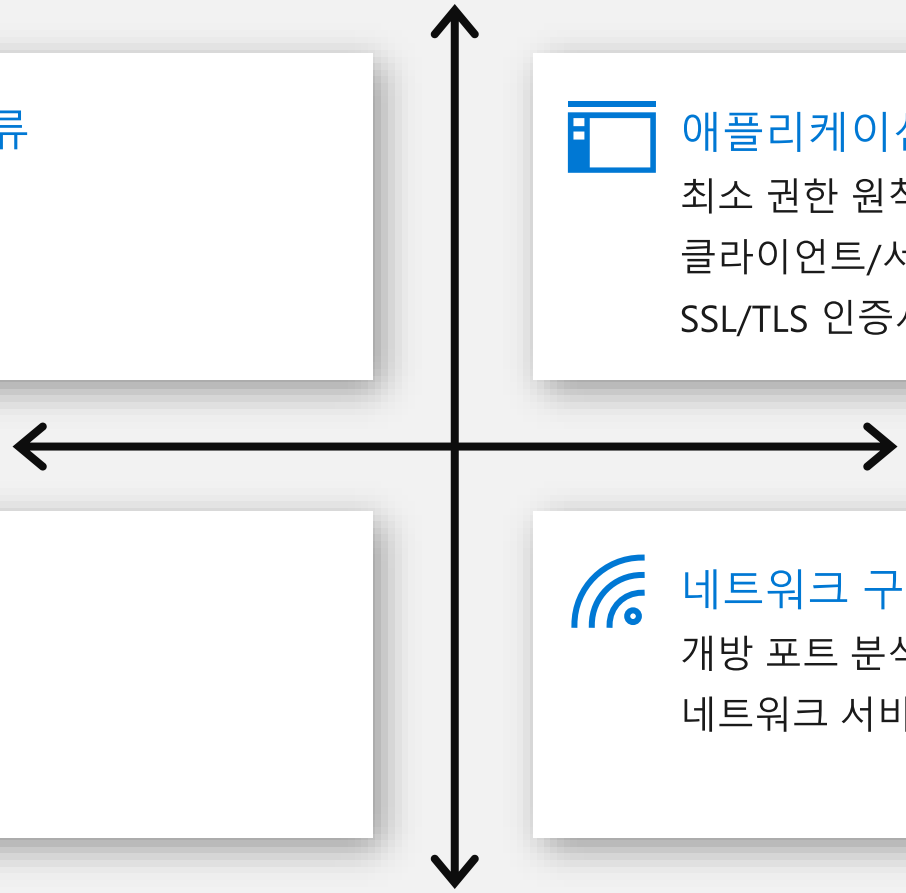
하드웨어 취약성 (펌웨어)

매우 활용하기 어렵지만 시스템의 루트 신뢰에 영향을 미칠 수 있음.
예: Spectre/Meltdown 취약성 (CVE-2017-5715)

발견하기 가장 어려움

1

지속적인 발견
광범위한 보안 구성 평가



운영 체제 구성 오류
파일 공유 분석
Security Stack 구성
OS 기준

애플리케이션 구성 오류
최소 권한 원칙
클라이언트/서버/웹 애플리케이션 분석
SSL/TLS 인증서 평가

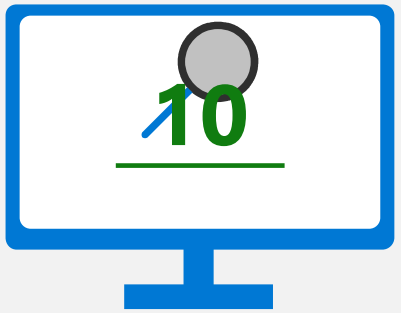
계정 구성 오류
암호 정책
권한 분석

네트워크 구성 오류
개방 포트 분석
네트워크 서비스 분석

2

위협 및 비즈니스 우선 순위 (“TLV”)

고객이 적시에 올바른 일에 집중할 수 있도록 지원



T

위협 환경

취약점 특성 (CVSS 점수, 취약한 날)
악용 특성 (공공의 착취 & 어려움, 번들)
EDR 보안 경고 (활성 경고, 위반 기록)
위협 분석 (라이브 캠페인, 위협 행위자)

L

위반 가능성

현재 보안 태세
인터넷 연결
조직 내 악용 시도

V

비즈니스 가치

HVA 분석 (WIP, HVU, 중요한 과정)
런타임 & 의존성 분석

3

자동 보상

IT 관리자와 보안 관리자 간의 연결

IT 팀과 보안 팀 간의 판도를 바꾸는 연결

Intune/SCCM을 통한 원 클릭 수정 요청

런타임 분석을 통한 자동화된 작업 모니터링

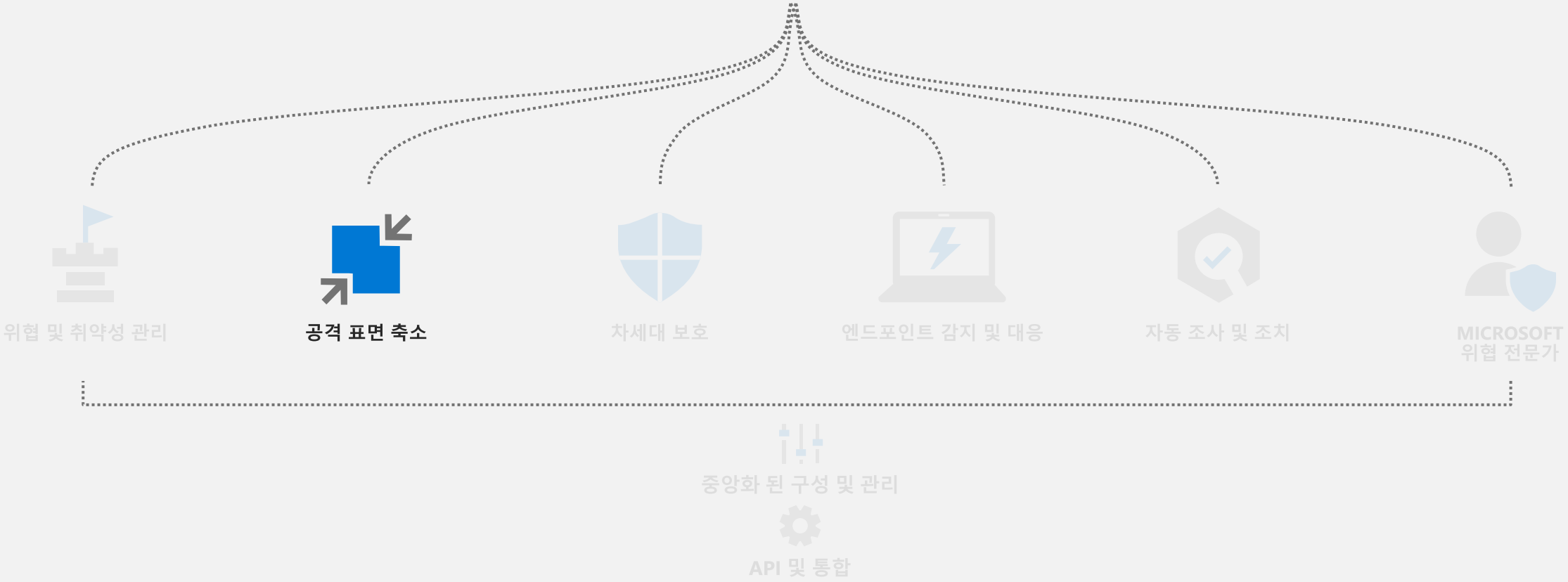
평균 완화 시간 KPI 추적

위험 완화/수락을 위한 풍부한 예외 경험

티켓 관리 통합 (Intune, Planner, Service Now, JIRA)

엔드포인트 용
Microsoft Defender

클라우드 기반의 내장된.



고객의 주요 당면 과제

제로 데이

지속적으로 산업을
괴롭히는 제로 데이

네트워크 경계

경계가 침식되고 있으며,
강화하려면 고유한
솔루션이 필요

크로스 플랫폼

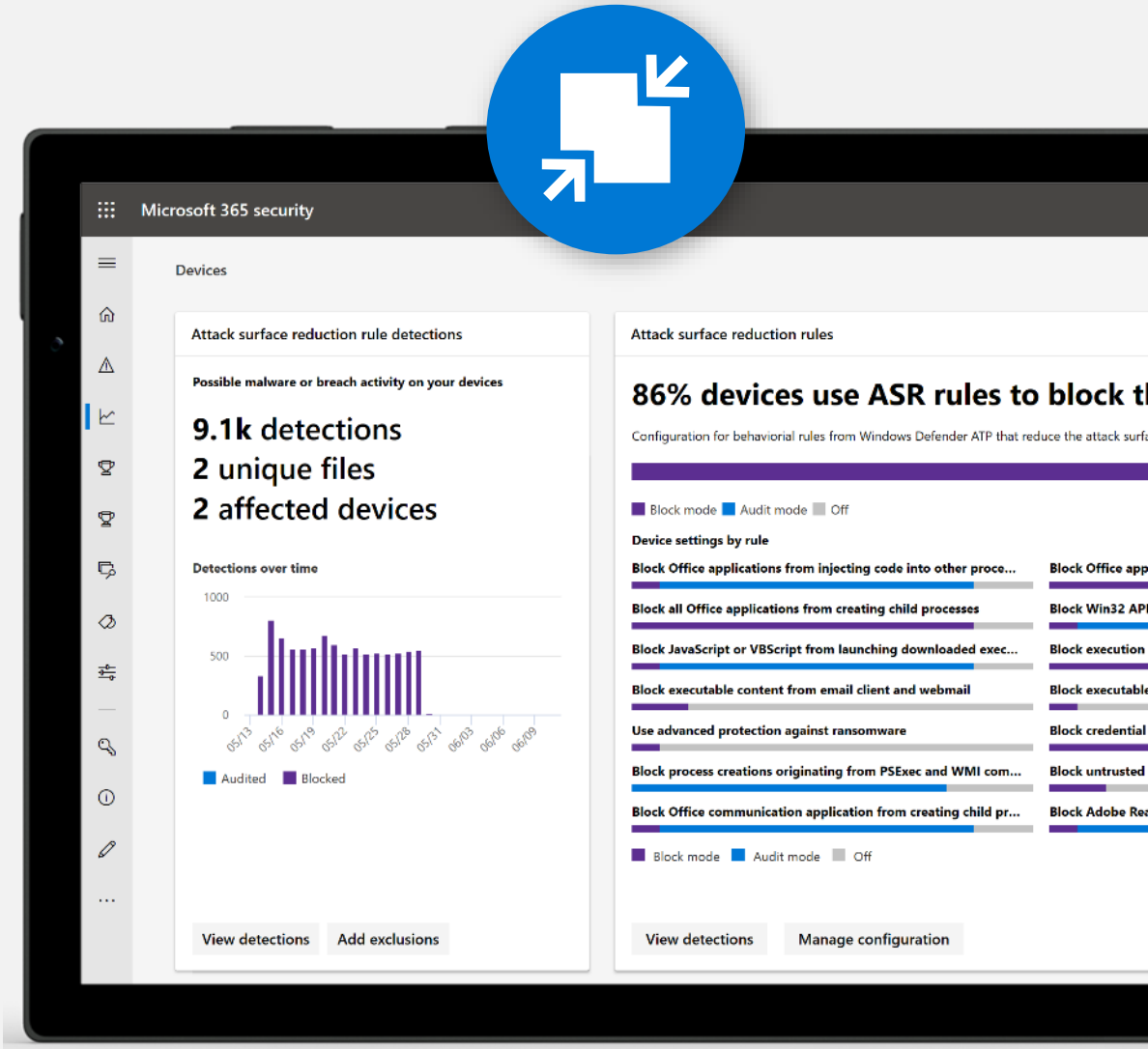
이기종 환경으로 인한
어려움

조직은 보안 상태를 사전 예방적으로 조정하는 데 어려움을 겪고 있습니다.

Attack Surface Reduction

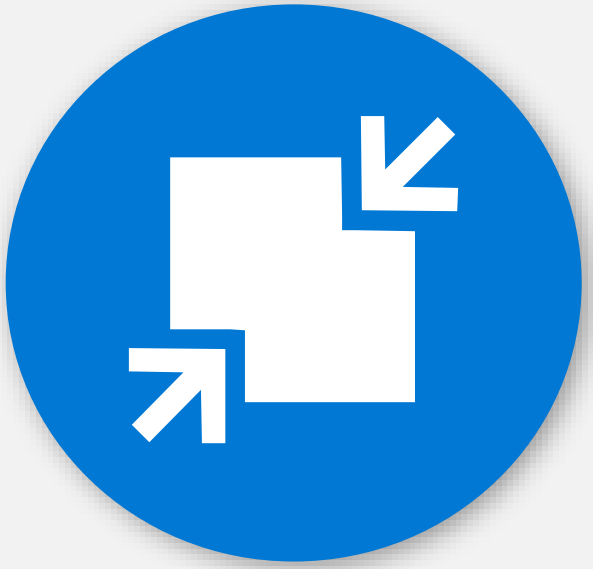
공격 표면적을 축소해 위험 제거

- 운영 중단 없이 시스템 강화
- 조직에 맞는 사용자 지정
- 영향을 시각화하고 간단히 활성화



Attack Surface Reduction

공격 및 악용 방지



HW 기반 격리

애플리케이션 제어

악용 방지

네트워크 보호

제어된 폴더 액세스

장치 제어

웹 보호

랜섬웨어 보호

신뢰할 수 없는 사이트에 대한 액세스 격리

신뢰할 수 없는 Office 파일에 대한 액세스 격리

호스트 침입 방지

악용 완화

파일에 대한 랜섬웨어 보호

평판이 낮은 대상으로의 트래픽 차단

레거시 애플리케이션 보호

신뢰할 수 있는 응용 프로그램만 실행하도록 허용

Attack Surface Reduction (ASR) 규칙

공격 표면을 최소화

클라우드 인텔리전스를 기반으로 하는 서명 없는 제어 엔트리 벡터. 예를 들어 Office 매크로의 동작과 유사한 Attack surface reduction (ASR) 제어.

생산성 앱 규칙

- Office 앱에서 실행 가능한 콘텐츠를 생성하지 못하도록 차단
- Office 앱에서 하위 프로세스 생성하지 못하도록 차단
- Office 앱이 다른 프로세스에 코드를 주입하지 못하도록 차단
- Office 매크로에서 Win32 API 호출 차단
- Adobe Reader가 하위 프로세스 생성하지 못하도록 차단

이메일 규칙

- 이메일 클라이언트 및 웹 메일에서 실행 가능한 콘텐츠 차단
- Office 커뮤니케이션 애플리케이션만 하위 프로세스 생성하지 못하도록 차단

스크립트 규칙

- 혼란스럽게 구성된 JS/VBS/PS/macro 코드 차단
- JS/VBS가 다운로드된 실행 파일 콘텐츠를 시작하지 못하도록 차단

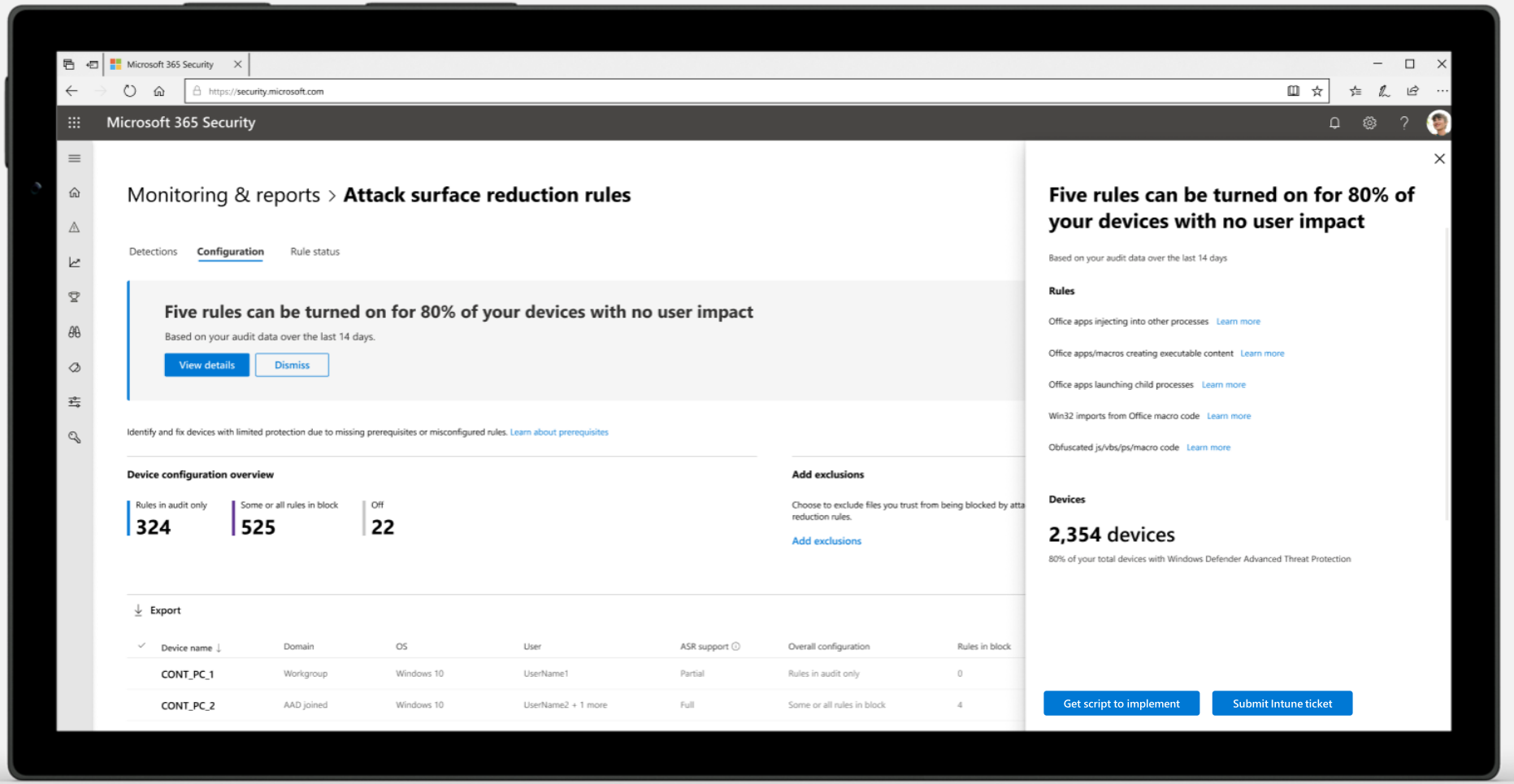
다양한 단계를 갖는 위협

- 실행 파일이 보급률 (1000 대의 컴퓨터), 사용 기간 (24 시간) 또는 신뢰할 수 있는 목록 기준을 충족하지 않는 경우 실행 파일 실행 차단
- USB에서 실행되는 신뢰할 수 없거나 서명되지 않은 프로세스 차단
- 랜섬웨어에 대한 고급 보호 기능 사용

래터럴 무브먼트 (횡적 이동 공격) 및 자격 증명 도용

- PSExec 및 WMI 명령에서 발생하는 프로세스 생성 차단
- Windows 로컬 보안 기관 하위 시스템(lss.exe)의 자격 증명 도용 차단
- WMI 이벤트 구독을 통한 지속성 차단

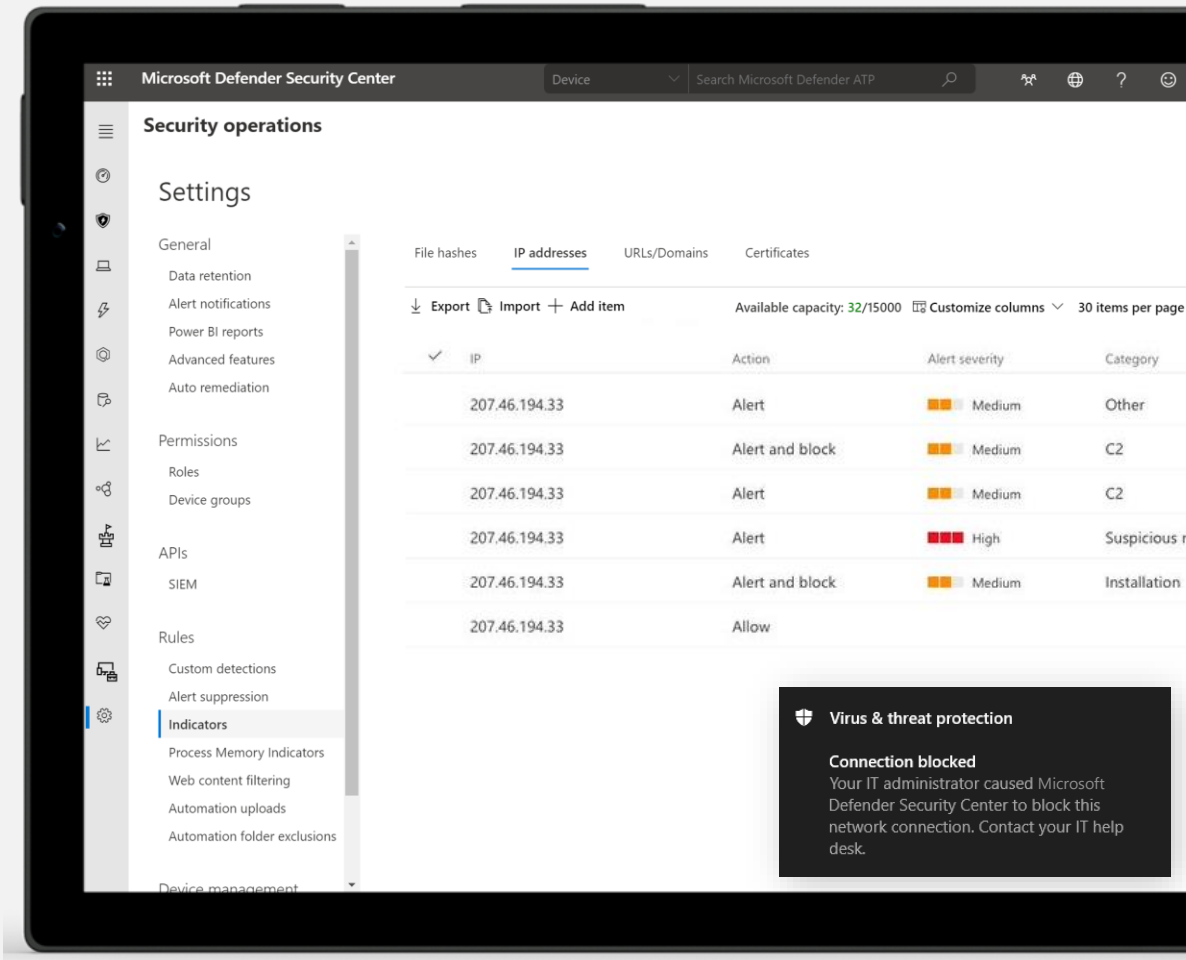
사용하기 쉬운 버튼: 차단 켜기



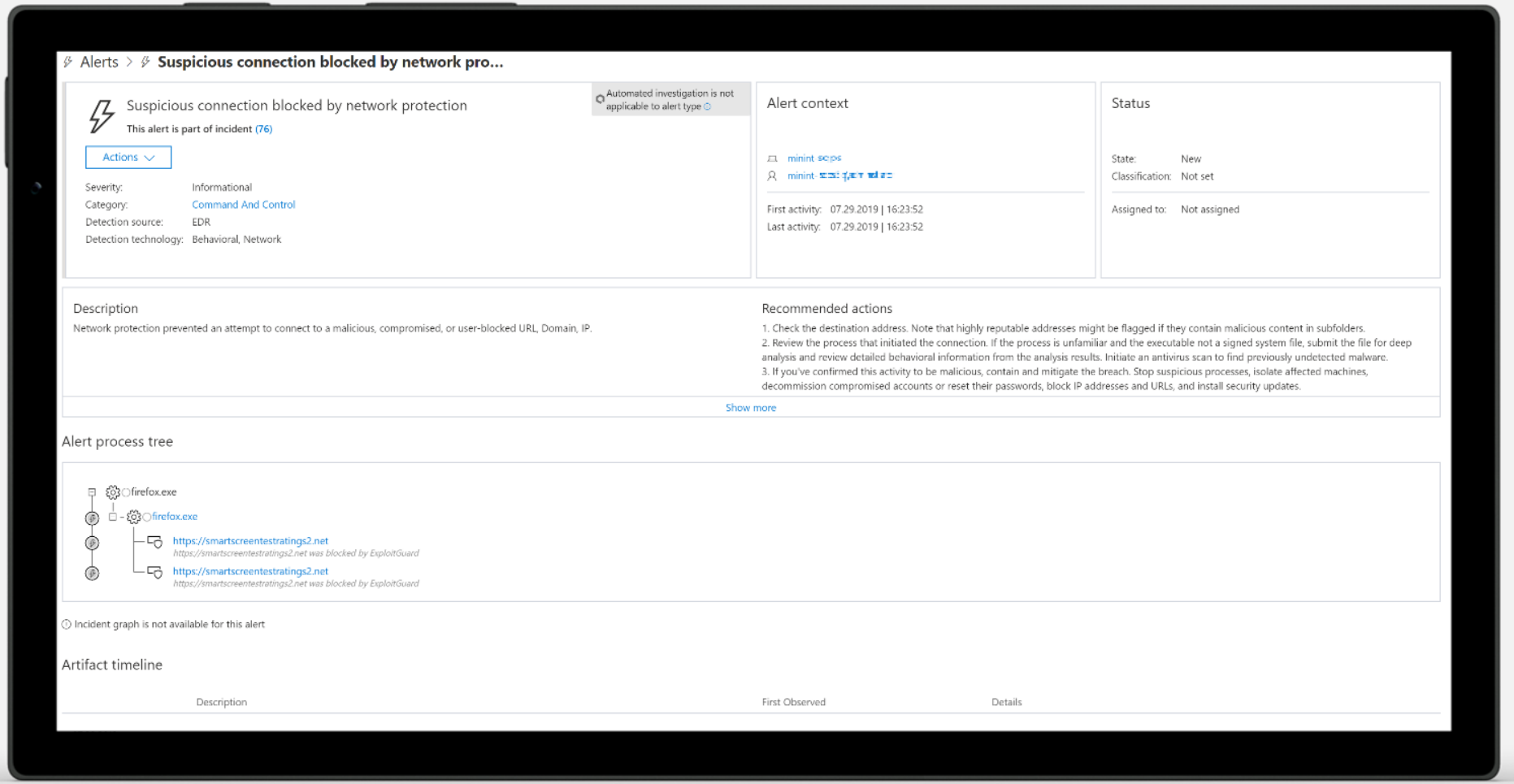
네트워크 보호

허용, 감사 및 차단

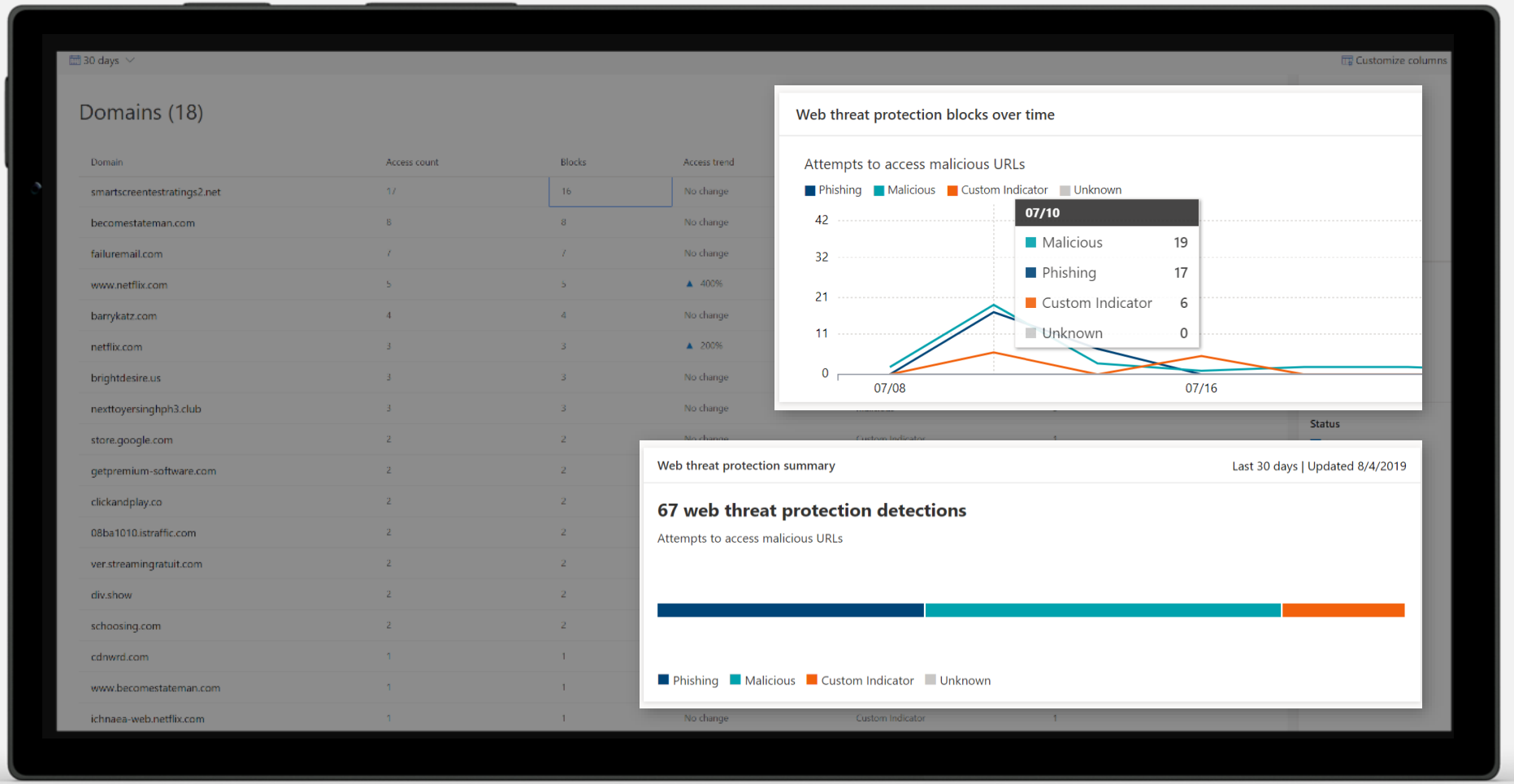
- 경계 없는 네트워크 보호("SmartScreen in the box")는 **Microsoft Edge뿐만 아니라 장치의 모든 앱을 사용하여** 사용자가 악의적이거나 의심스러운 네트워크 대상에 액세스하는 것을 방지합니다.
- 고객은 신뢰할 수 있는 고급 평판 데이터베이스 외에도 자체 TI를 추가 할 수 있습니다.



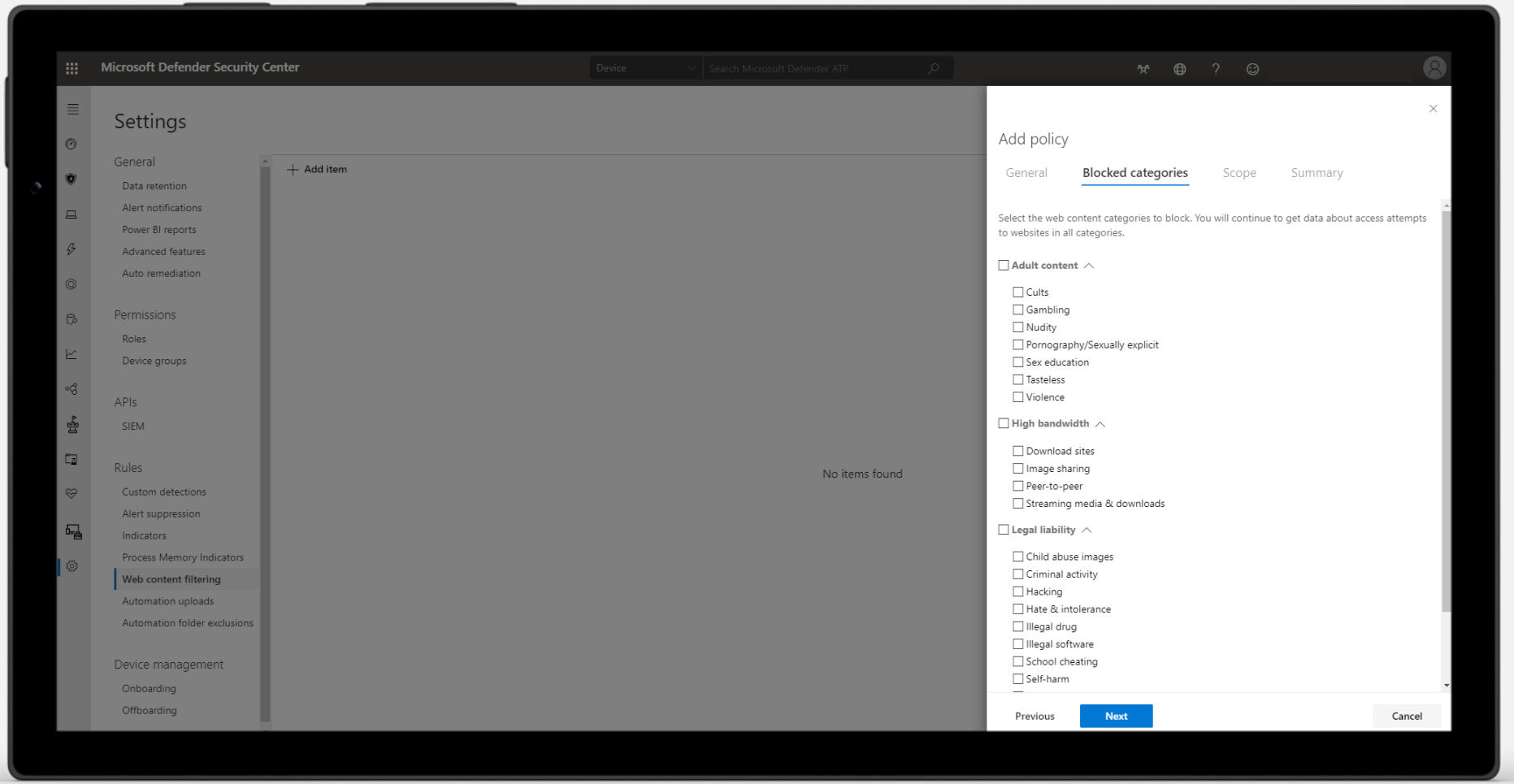
웹 위협 경고


Alerts > Suspicious connection blocked by network pro...
Suspicious connection blocked by network protection
This alert is part of incident (76)
Automated investigation is not applicable to alert type
Actions
Severity: Informational
Category: Command And Control
Detection source: EDR
Detection technology: Behavioral, Network
Alert context
First activity: 07.29.2019 | 16:23:52
Last activity: 07.29.2019 | 16:23:52
Status
State: New
Classification: Not set
Assigned to: Not assigned
Description
Network protection prevented an attempt to connect to a malicious, compromised, or user-blocked URL, Domain, IP.
Recommended actions
1. Check the destination address. Note that highly reputable addresses might be flagged if they contain malicious content in subfolders.
2. Review the process that initiated the connection. If the process is unfamiliar and the executable not a signed system file, submit the file for deep analysis and review detailed behavioral information from the analysis results. Initiate an antivirus scan to find previously undetected malware.
3. If you've confirmed this activity to be malicious, contain and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset their passwords, block IP addresses and URLs, and install security updates.
Show more
Alert process tree
firefox.exe
firefox.exe
https://smartscreentestratings2.net
https://smartscreentestratings2.net was blocked by ExploitGuard
https://smartscreentestratings2.net
https://smartscreentestratings2.net was blocked by ExploitGuard
Incident graph is not available for this alert
Artifact timeline
Description
First Observed
Details

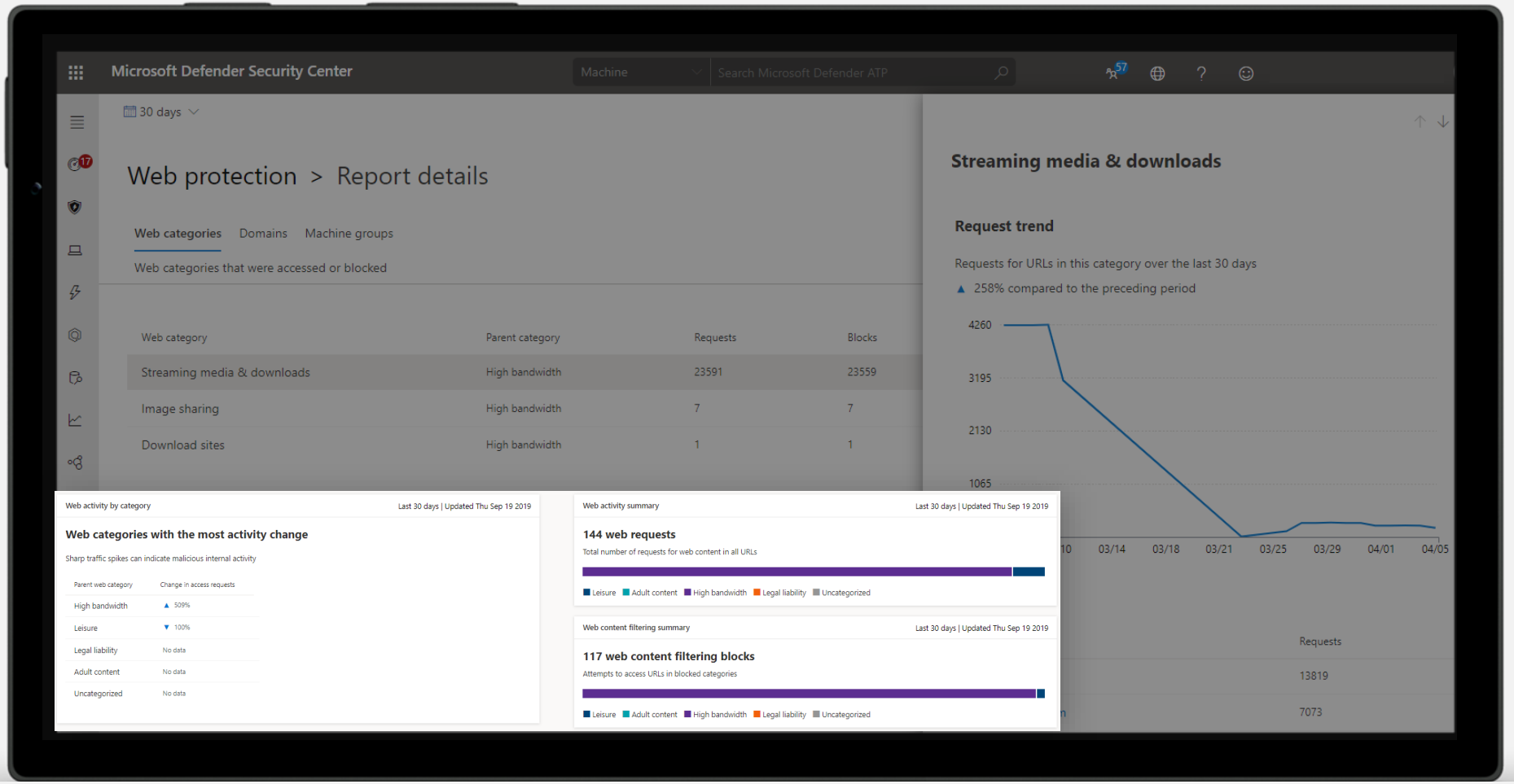
웹 위협 리포트


30 days
Customize columns
Domains (18)
Domain
Access count
Blocks
Access trend
smartscreentestratings2.net
becomestateman.com
failuremail.com
www.netflix.com
barrykatz.com
netflix.com
brightdesire.us
nexttoyersinghph3.club
store.google.com
getpremium-software.com
clickandplay.co
08ba1010.istraffic.com
ver.streamingratuit.com
div.show
schoosing.com
cdnwrd.com
www.becomestateman.com
ichnaea-web.netflix.com
Web threat protection blocks over time
Attempts to access malicious URLs
Phishing
Malicious
Custom Indicator
Unknown
42
32
21
11
0
07/10
Malicious 19
Phishing 17
Custom Indicator 6
Unknown 0
07/08
07/16
Status
Web threat protection summary
Last 30 days | Updated 8/4/2019
67 web threat protection detections
Attempts to access malicious URLs
Phishing
Malicious
Custom Indicator
Unknown

웹 콘텐츠 필터링 구성

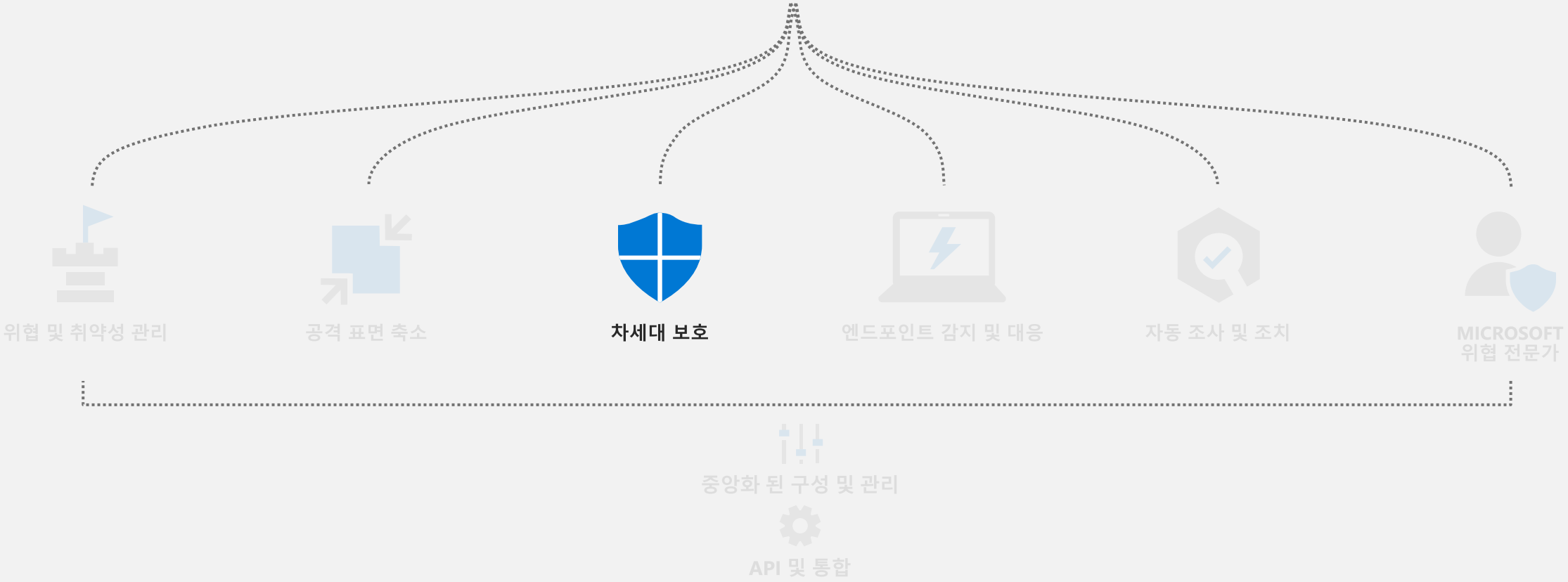

Microsoft Defender Security Center
Device
Search Microsoft Defender ATP
Settings
General
Data retention
Alert notifications
Power BI reports
Advanced features
Auto remediation
Permissions
Roles
Device groups
APIs
SIEM
Rules
Custom detections
Alert suppression
Indicators
Process Memory Indicators
Web content filtering
Automation uploads
Automation folder exclusions
Device management
Onboarding
Offboarding
Add item
No items found
Add policy
General
Blocked categories
Scope
Summary
Select the web content categories to block. You will continue to get data about access attempts to websites in all categories.
Adult content
Cults
Gambling
Nudity
Pornography/Sexually explicit
Sex education
Tasteless
Violence
High bandwidth
Download sites
Image sharing
Peer-to-peer
Streaming media & downloads
Legal liability
Child abuse images
Criminal activity
Hacking
Hate & intolerance
Illegal drug
Illegal software
School cheating
Self-harm
Previous
Next
Cancel

웹 콘텐츠 필터링 보고


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
30 days
Web protection > Report details
Web categories
Domains
Machine groups
Web categories that were accessed or blocked
Web category
Parent category
Requests
Blocks
Streaming media & downloads
High bandwidth
23591
23559
Image sharing
High bandwidth
7
7
Download sites
High bandwidth
1
1
Streaming media & downloads
Request trend
Requests for URLs in this category over the last 30 days
▲ 258% compared to the preceding period
4260
3195
2130
1065
03/14
03/18
03/21
03/25
03/29
04/01
04/05
Requests
13819
7073
Web activity by category
Last 30 days | Updated Thu Sep 19 2019
Web categories with the most activity change
Sharp traffic spikes can indicate malicious internal activity
Parent web category
Change in access requests
High bandwidth
▲ 509%
Leisure
▼ 100%
Legal liability
No data
Adult content
No data
Uncategorized
No data
Web activity summary
Last 30 days | Updated Thu Sep 19 2019
144 web requests
Total number of requests for web content in all URLs
Leisure
Adult content
High bandwidth
Legal liability
Uncategorized
Web content filtering summary
Last 30 days | Updated Thu Sep 19 2019
117 web content filtering blocks
Attempts to access URLs in blocked categories
Leisure
Adult content
High bandwidth
Legal liability
Uncategorized

엔드포인트 용
Microsoft Defender

클라우드 기반의 내장된.



고객의 주요 당면 과제

정기적인 업데이트에 의존하는 솔루션은 시간당 **7**백만 건의 고유한 위협으로부터 보호할 수 없습니다.

인식 가능한 실행 파일 차단에서 정교한 공격 기술을 사용하는 멀웨어로 전환되었습니다. (예: 파일 없는)

Attack Surface Reduction은 보안 상태를 크게 향상시킬 수 있지만 여전히 남아있는 표면에 대한 탐지가 필요합니다.

우리는 매달 **50**억 개의 고유한 인스턴스의 하이퍼 다형성 위협이 있는 세계에 살고 있습니다.

정적 vs 동적

정적 서명:
파일에 집중

해시
문자열
에뮬레이터

비효과적

동적 휴리스틱 접근:
런타임 동작에 집중

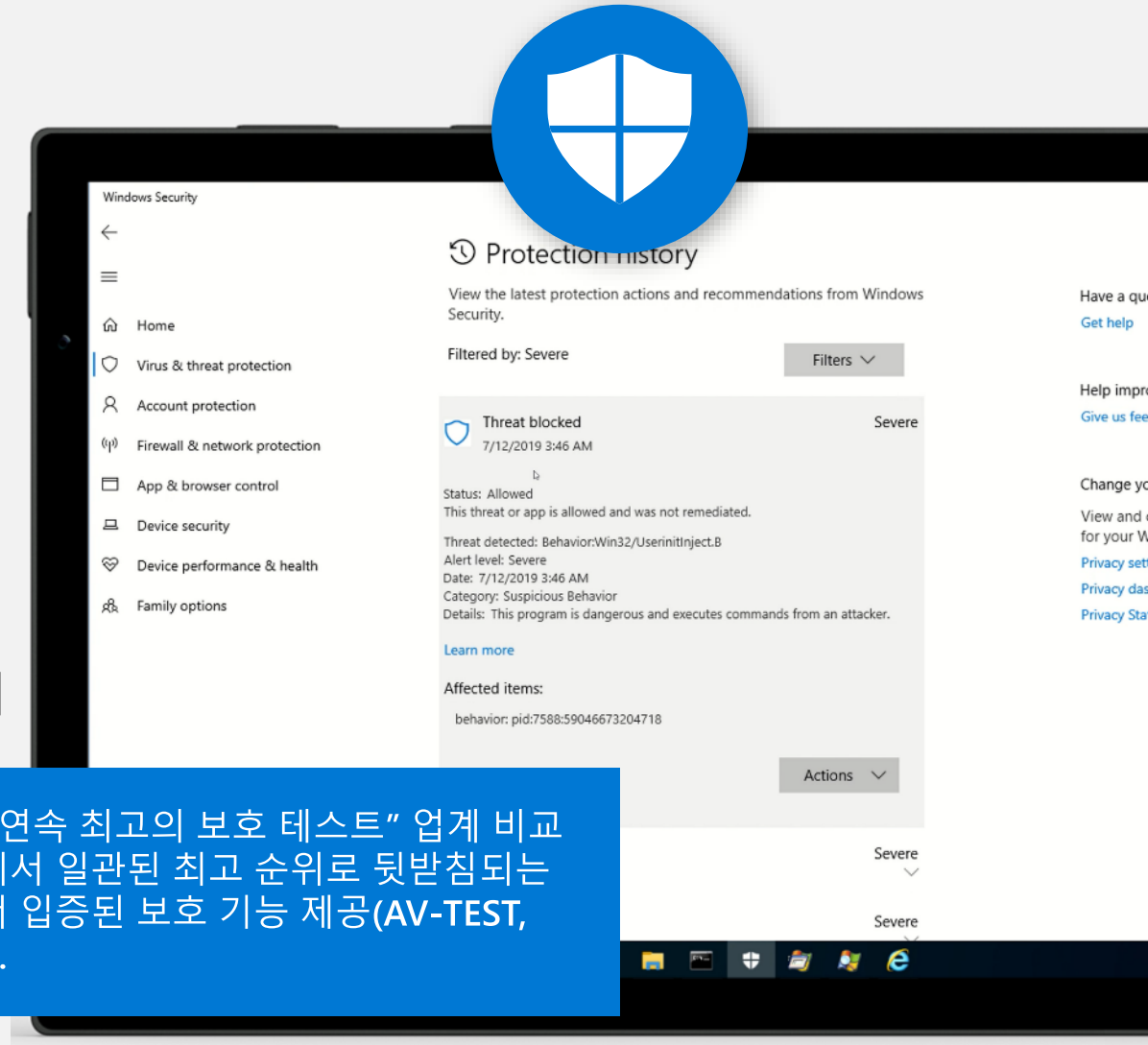
동작 모니터링
메모리 스캐닝
AMSI
명령줄 스캐닝

효과적

차세대 보호 기능

정교한 위협과 멀웨어 차단 및 해결

- 행동 기반 실시간 보호
- 파일 기반 및 파일 없는 멀웨어 차단
- 신뢰할 수 있거나 신뢰할 수 없는 응용프로그램에서 악의적인 활동 차단



"12개월 연속 최고의 보호 테스트" 업계 비교 테스트에서 일관된 최고 순위로 뒷받침되는 현장에서 입증된 보호 기능 제공(AV-TEST, SE Labs).

엔드포인트 용 Microsoft Defender 차세대 보호 엔진

메타데이터 기반의 ML
메타데이터를 분석하여 새로운 위협을 신속하게 차단

행동 기반 ML
프로세스 트리 및 의심스러운 동작 시퀀스를 사용하여 새로운 위협 식별

AMSI와 쌍으로 구성된 ML
쌍으로 구성된 클라이언트 및 클라우드 ML 모델을 사용하여 파일 없는 공격 및 인메모리 공격 탐지

파일 분류 ML
다중 클래스의 심층 신경 네트워크 분류기를 실행하여 새로운 멀웨어 탐지

폭발 기반 ML
알 수 없는 파일을 폭발시켜 새로운 악성 코드 탐지

평판 ML
직접적이든 연관성이든 나쁜 평판을 가진 위협 포착

스마트 규칙
전문가가 작성한 규칙을 사용하여 위협 차단

Cloud

Client

ML
클라이언트 기반 ML 모델을 사용하여 새로운 위협 및 알려지지 않은 위협 발견

동작 모니터링
의심스러운 런타임 시퀀스를 포함한 악의적인 동작 식별

메모리 스캐닝
메모리에서 실행 중인 악성 코드 탐지

AMSI 통합
파일 없는 공격 및 메모리 내 공격 탐지

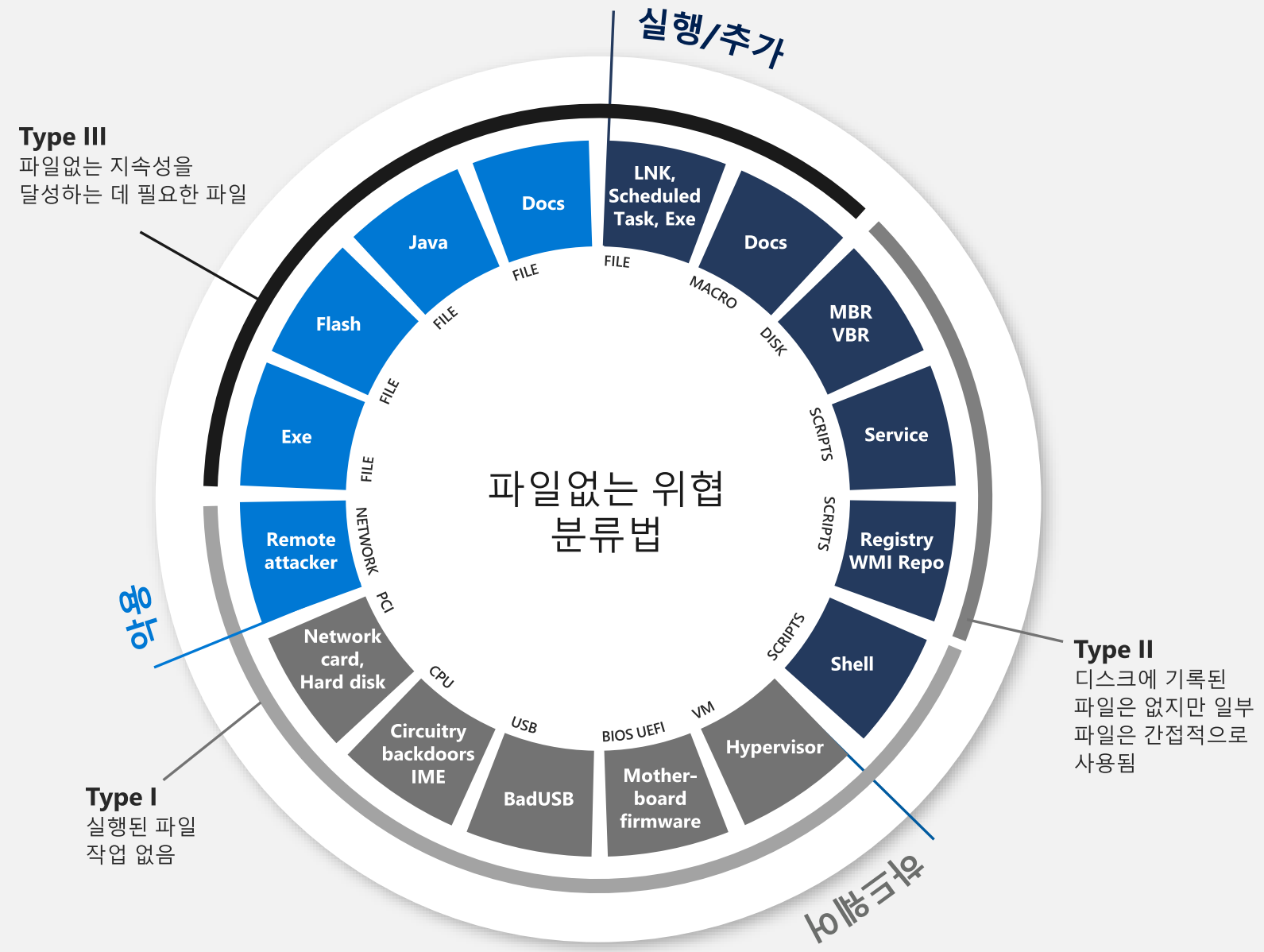
휴리스틱
유사한 특성을 가진 악성 코드 변종 또는 새로운 변종을 포착

에뮬레이션
실행 시 작동 방식에 따라 파일 평가

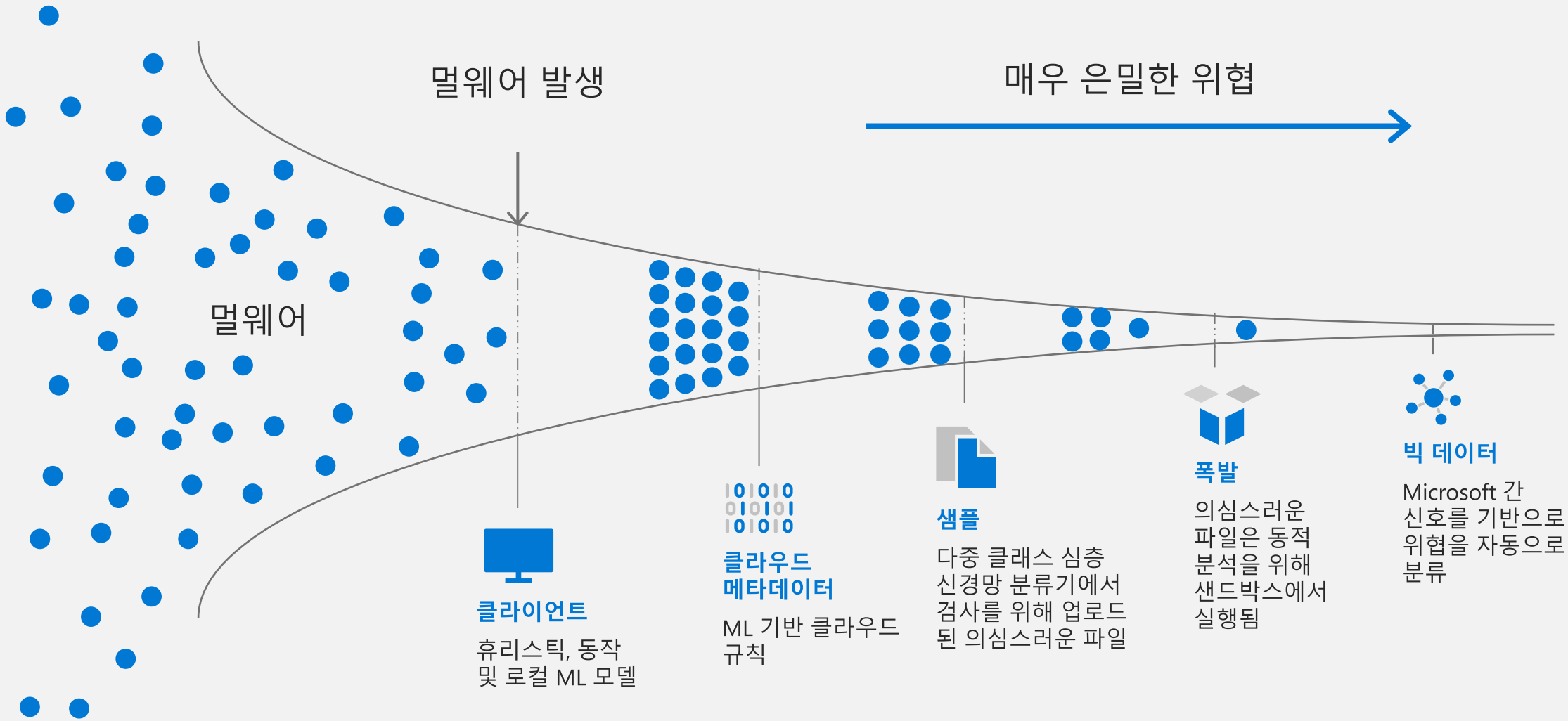
네트워크 모니터링
악성 네트워크 활동 포착

파일없는 보호의 혁신

- 악성 **URL**에 대한 호출을 차단하기 위한 동적 및 컨텍스트 **URL** 분석
- **AMSI**와 쌍으로 구성된 기계 학습에서는 스크립팅 동작의 고급 분석을 수행하기위해 **Antimalware Scan Interface(AMSI)**와 통합된 한 쌍의 클라이언트 측 및 클라우드 측 모델을 사용
- **DNS** 유출 분석
- 심층 메모리 분석



엔드포인트 용 Microsoft Defender NGP 보호 파이프라인



동적: 행동 모니터링

다음의 활동에 대하여 모니터링:

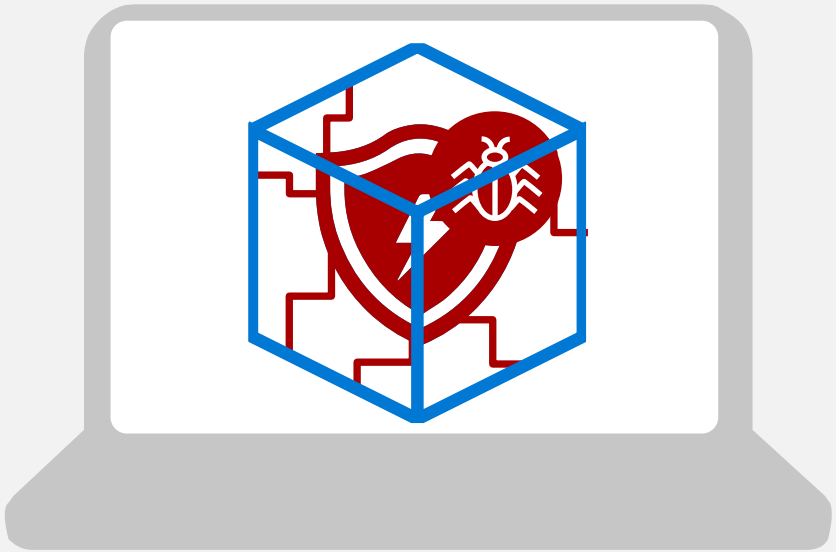
- 파일
- 레지스트리 키
- 프로세스
- 네트워크 (기본 **HTTP** 검사)
- ... 그리고 몇 가지 특정 활동

휴리스틱은:

- 일련의 이벤트 감지
  예: "malware.exe"라는 이름의 파일이 생성됨
- 이벤트 데이터 검사
  예: AutoRun 키가 생성되고 "malware.exe"가 포함됨
- 다른 정적 신호와의 상관 관계
  예: "malware.exe"에는 DotNet 실행 파일임을 나타내는 속성이 존재
- 몇 가지 기본 교정 수행
  예: BM 이벤트가 감염을 보고한 경우 "malware.exe" 삭제
- 실행중인 프로세스의 메모리 스캔 요청

바이러스 백신 엔진의 샌드박스 화

Then

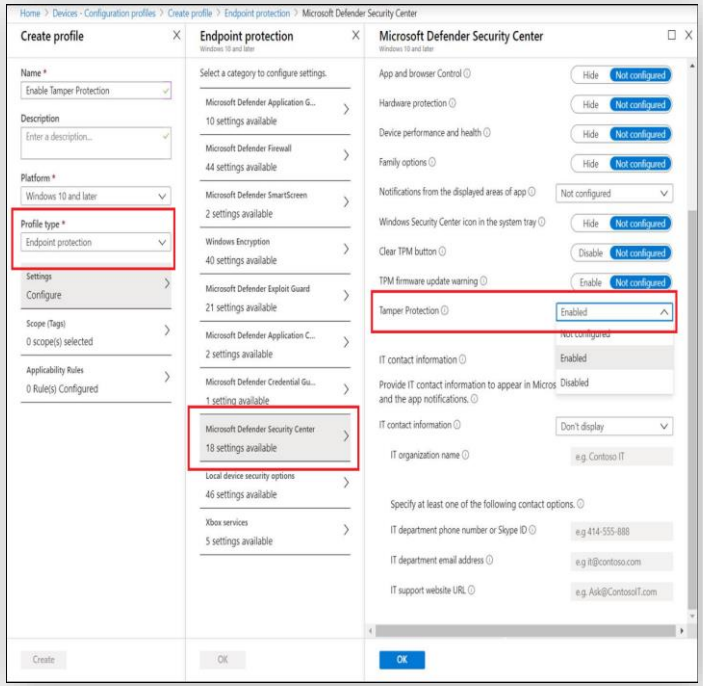


Now

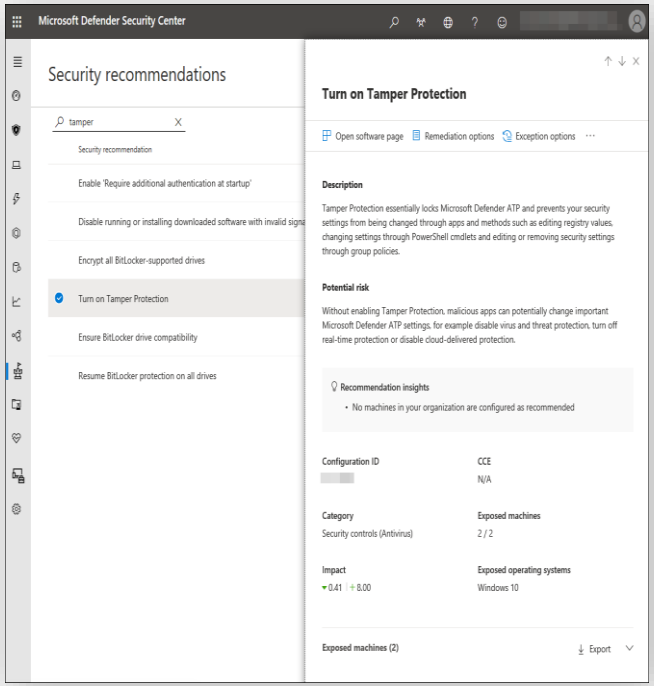
보다 자세한 내용은 블로그 참조

변조 방지 – 암호 없는, 안전한, e2e

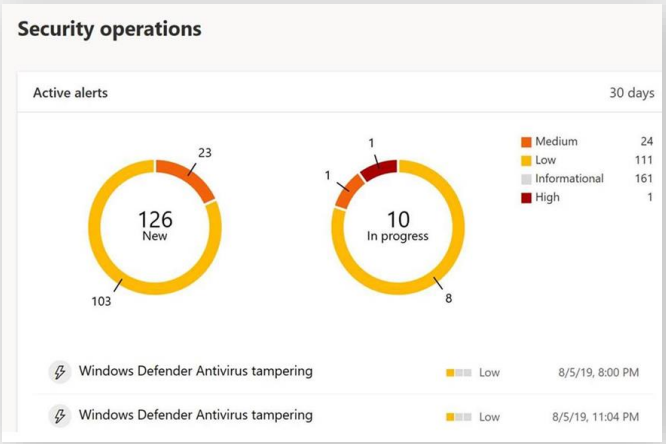
원활하고 안전하며 암호가 없는 구성



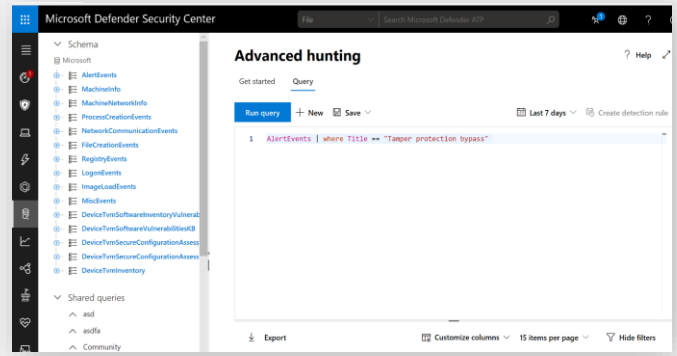
위협 및 취약성 관리 – 보안 권장 사항



System Guard 및 EDR 신호를 기반으로 한 변조 경고



고급 헌팅



보다 자세한 내용은 [블로그](#) 참조

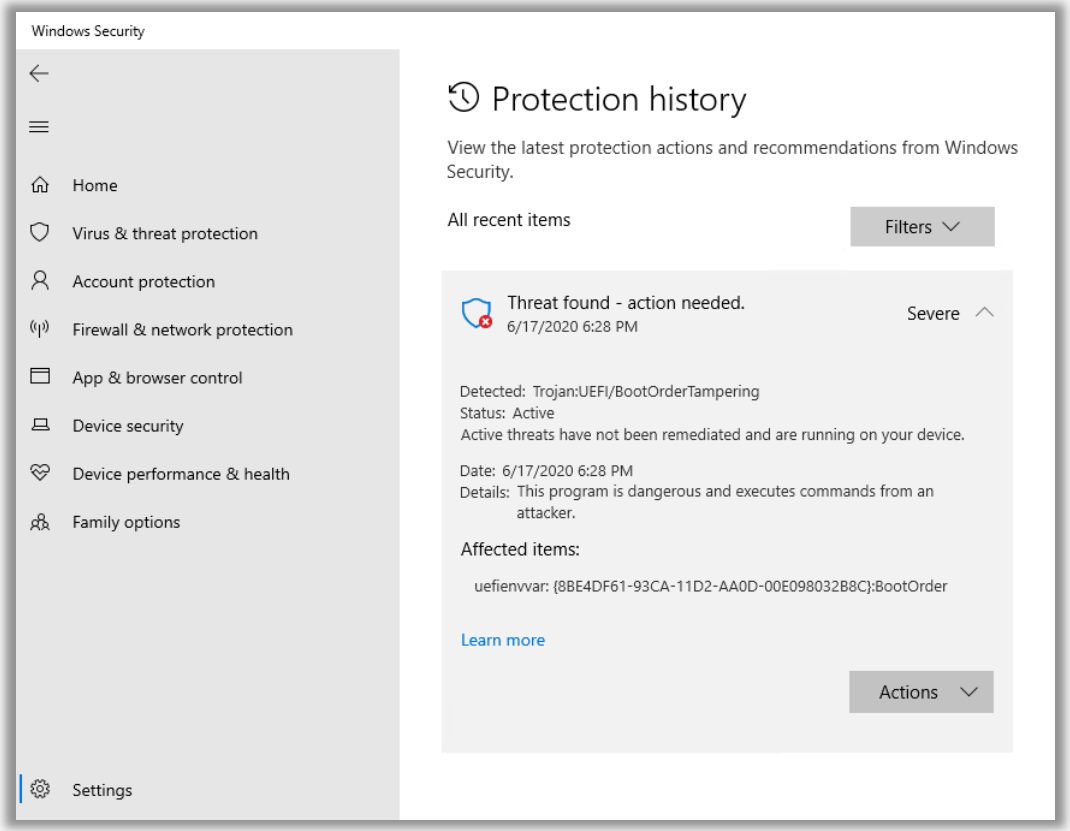
펌웨어 및 하드웨어 보호

UEFI 스캐너는 머더보드 칩셋과 상호 작용하여 런타임에 펌웨어 파일 시스템을 읽고 여러 솔루션 구성 요소를 사용하여 동적 분석을 수행:

- SPI(Serial Peripheral Interface)를 통해 펌웨어에 도달하는 UEFI anti-rootkit
- 펌웨어 내부의 컨텐츠를 분석하는 전체 파일 시스템 스캐너
- 공격 및 악의적인 동작을 식별하는 탐지 엔진

Microsoft Defender 보안 센터

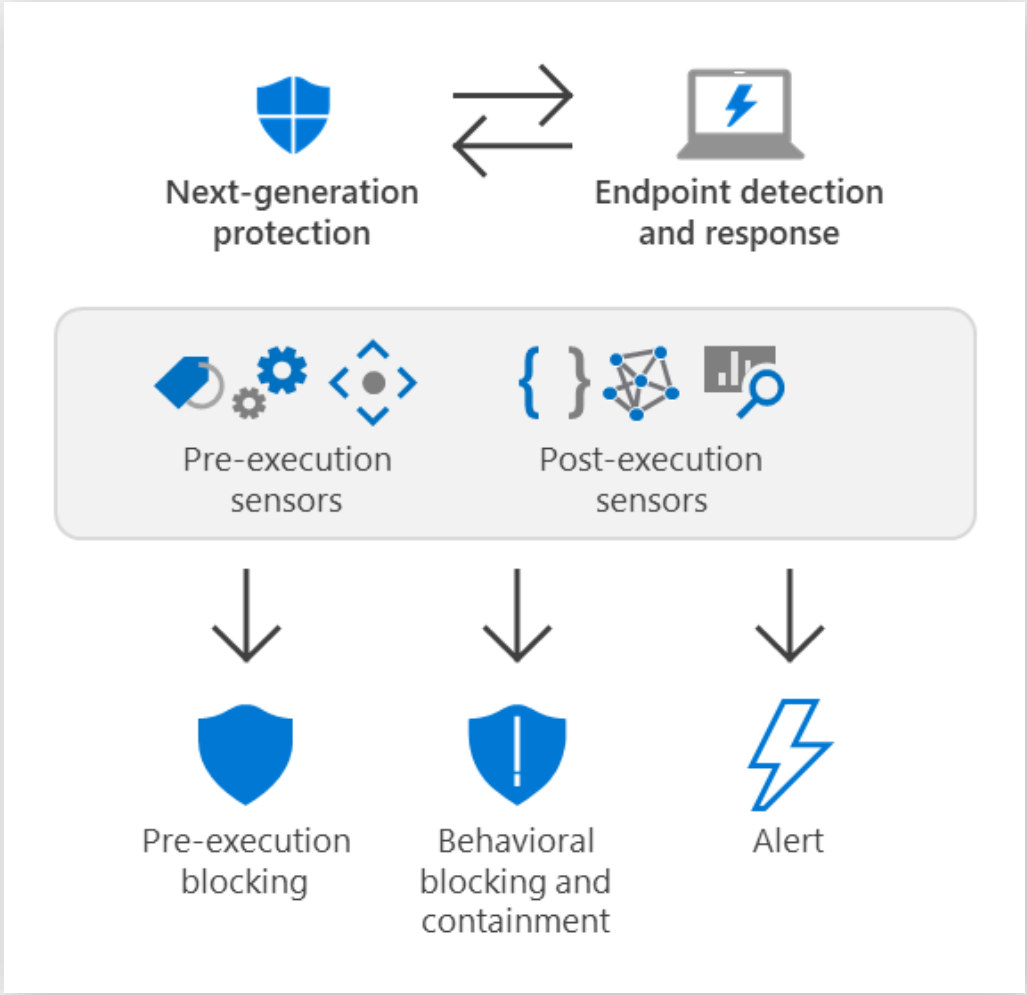
스캔 및 감지



보다 자세한 내용은 [블로그] 참조

동작 차단 및 격리

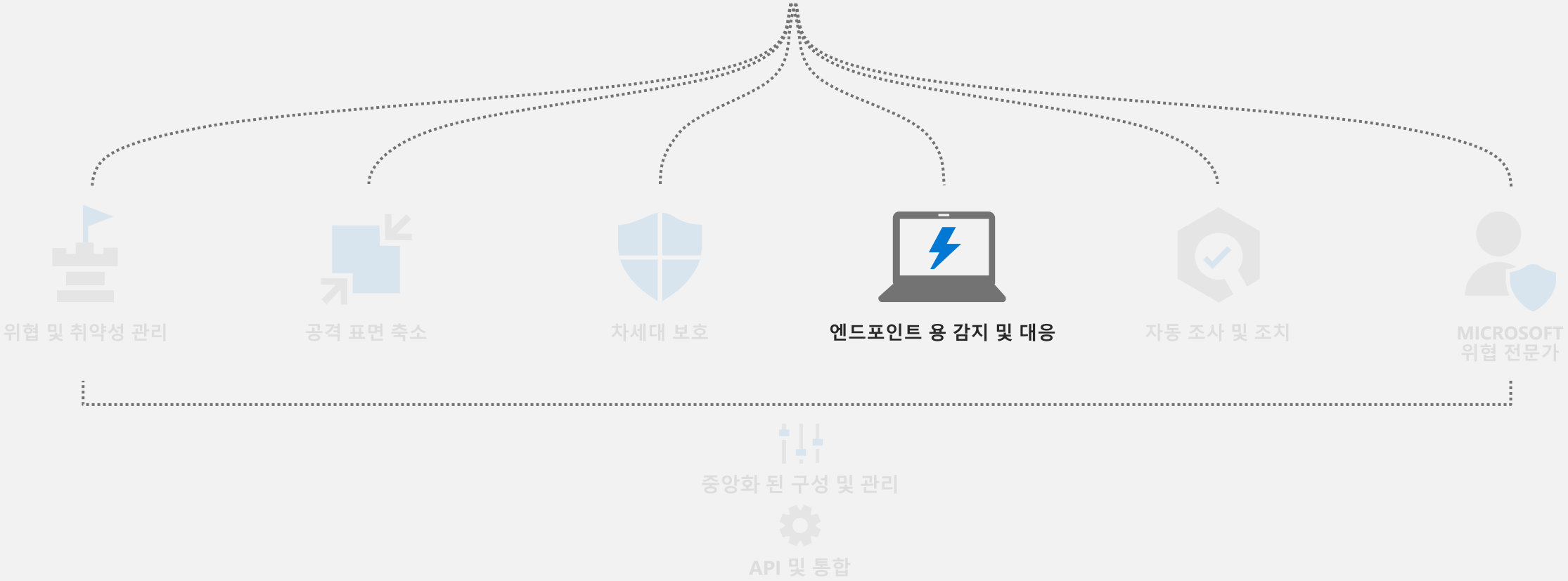
- 위협이 진행되기 전에 즉시 중지
- **Microsoft**는 **kill chain**및 **payload**(엔드포인트, **Office, ID** 등)를 통해 신호를 검색할 수 있는 고유한 기능을 갖춤
- 몇 가지 주요 사항 :
  - 사전/사후 침해 AI- 및 ML- 기반 동작 차단 및 격리
  - 첫 확인에 멀웨어를 탐지하여 몇 분 내에 다른 엔드포인트에서 차단 (1 – 5 minutes)
  - Microsoft Defender for Endpoint는 주요한 AV가 아닌 경우에도 악의적인 동작을 차단/방지하여 추가 보호 계층을 제공



Read the blog for more details

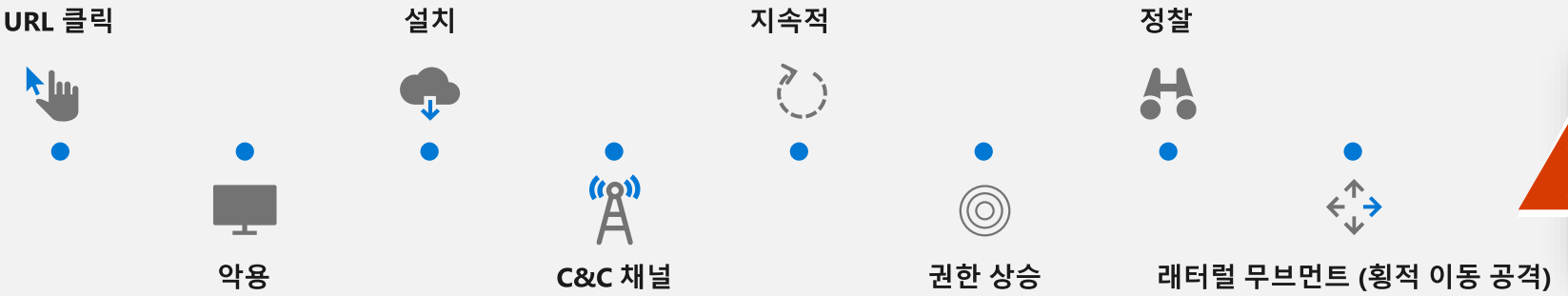
엔드포인트 용
Microsoft Defender

클라우드 기반의 내장된.



고객의 주요 당면 과제

공격이 점점 더 복잡해지고 여러 단계로 확장됨에 따라
탐지된 위협을 이해하기가 어렵습니다.



손상된 시스템의 46%가
멀웨어가 없었습니다.

네트워크 및 다양한 센서를 통한
지능형 공격을 추적하는 것은
어려운 과제입니다.

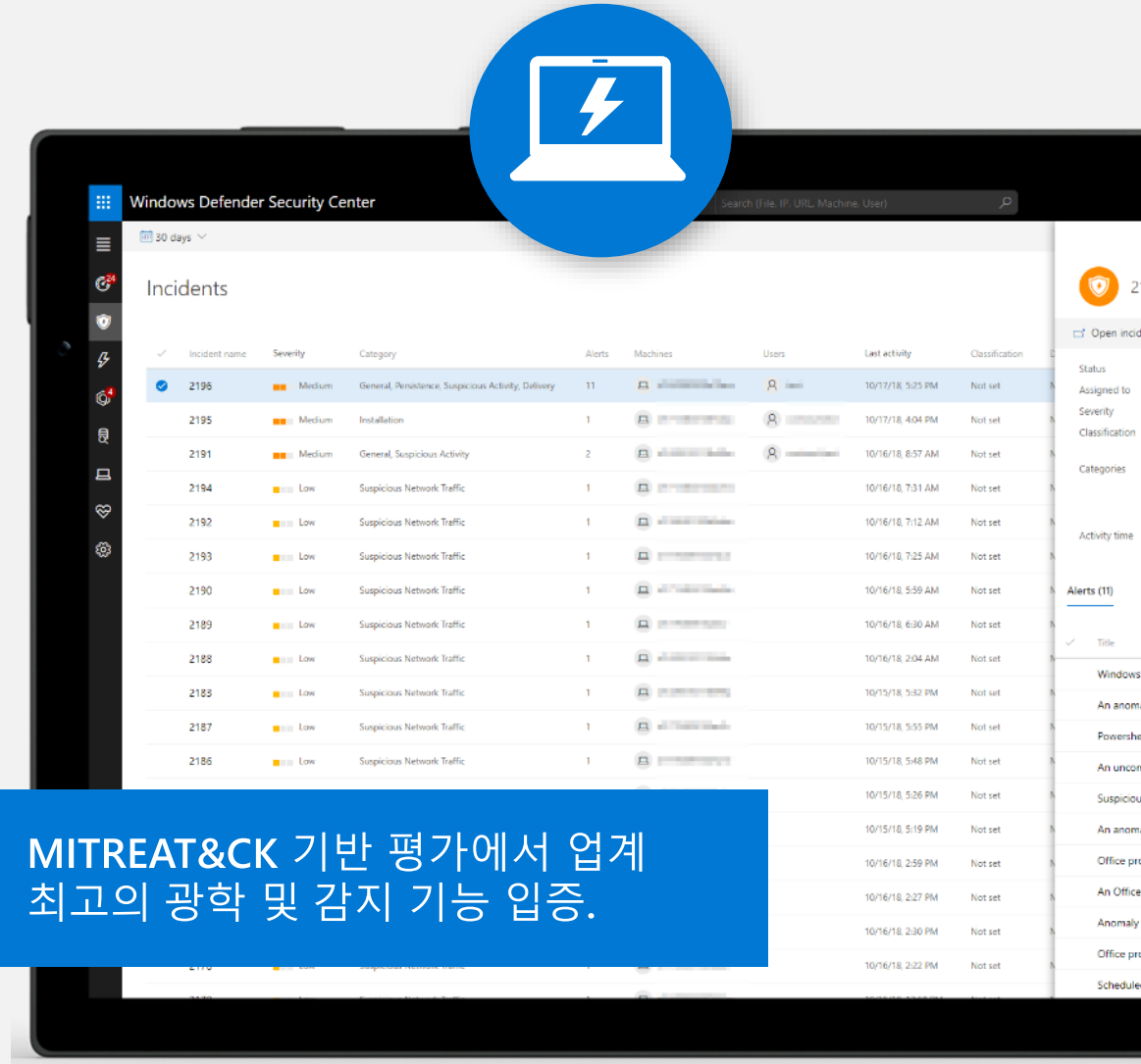
감염된 장치가 1개 일지라도 증거
및 경고를 수집하는데 시간이
오래 걸릴 수 있습니다.

공격자는 회피 기법을
사용합니다.

엔드 포인트 탐지 및 대응

지능형 지속적인 공격 탐지 및 조사

- 상관된 동작 경고
- 6개월 이상의 데이터 조사 및 탐색
- 다양한 대응 조치



엔드 포인트 탐지 및 대응

상관 관계 위반 후 감지

조사 경험

사건

고급 헌팅

대응 조치 **(+EDR blocks)**

심층 파일 분석

실시간 대응

위협 분석

분류 및 조사

경고 내용 이해

자세한 설명, 풍부한 컨텍스트, 전체 프로세스 실행 트리를 제공하는 경고 조사 환경.

장치 활동 조사

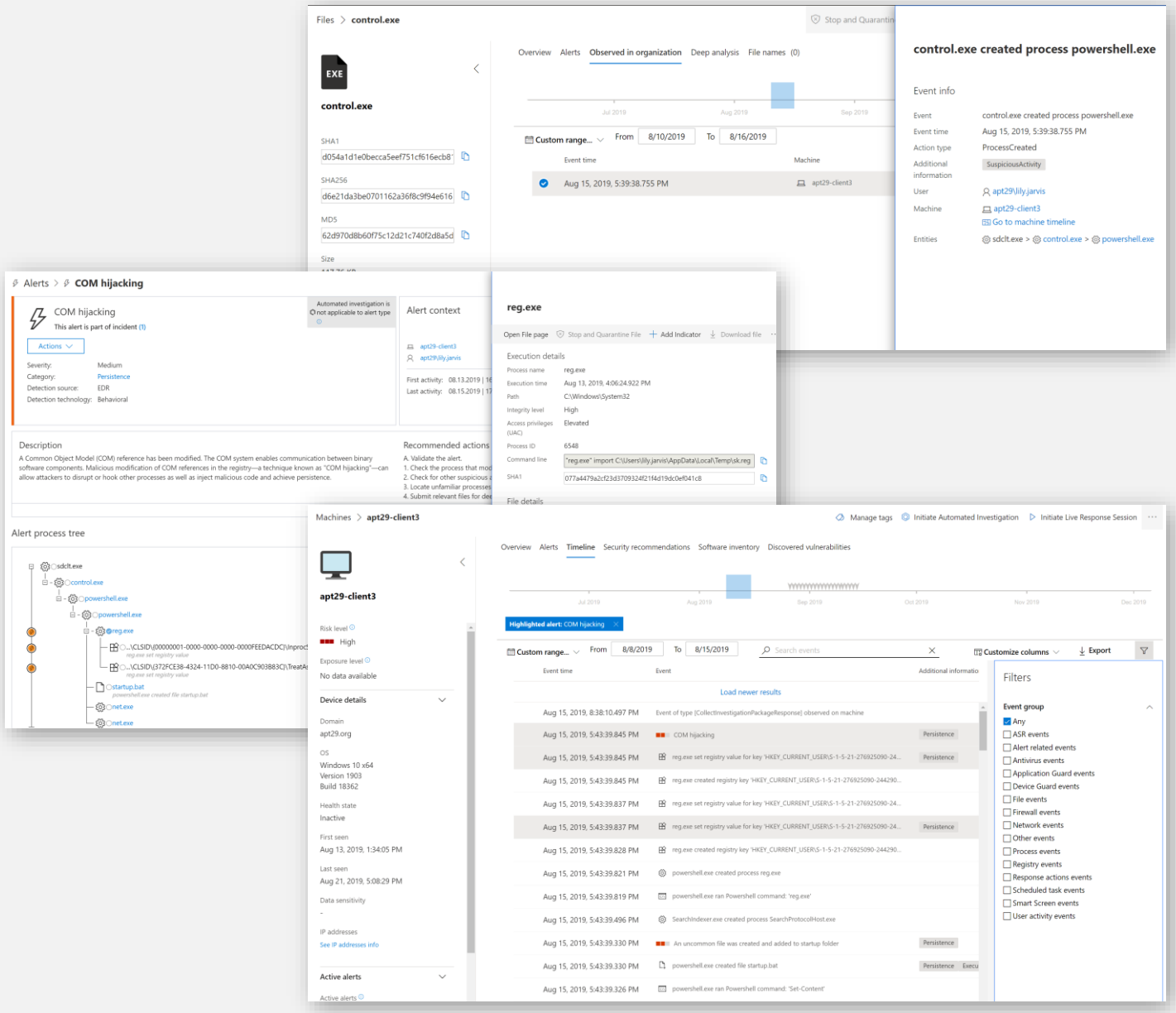
활동, 필터링 및 검색을 드릴다운 할 수 있는 전체 시스템 타임라인.

풍부한 지원 데이터 및 도구

조직 및 세계적 확산, 심층 분석 샌드박스를 포함한 파일, **IP, URL**에 대한 프로필 지원.

침해 범위 확대

상황에 따라 영향을 받는 다른 컴퓨터/사용자에게 피벗.



사건

엔드 투 엔드 공격 스토리 설명

스토리 재구성

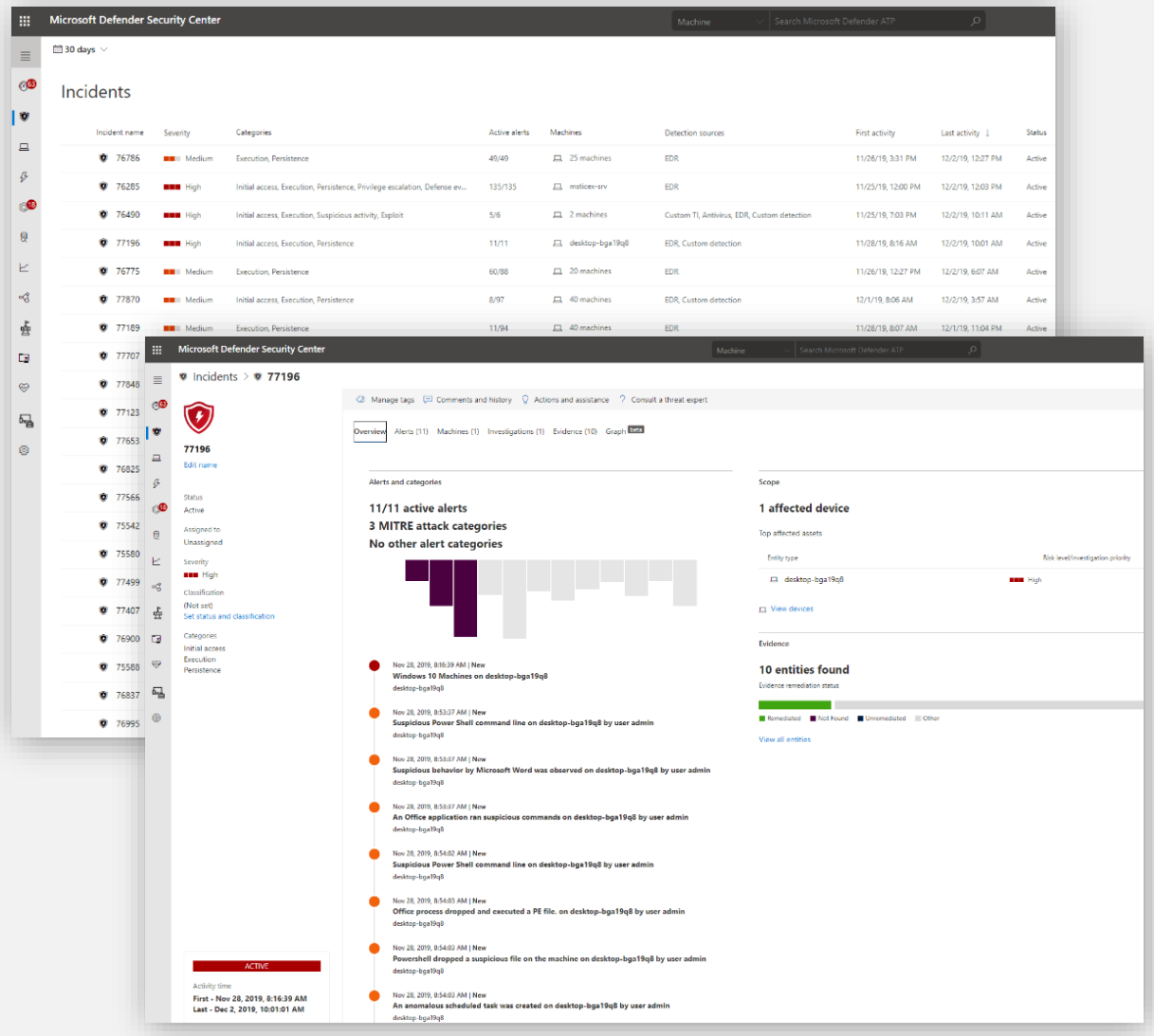
광범위한 공격 사례는 관련 경고 및 관련 엔티티를 통합할 때 더 잘 설명됩니다.

사건 범위

분석가는 여러 엔티티를 포함하는 복잡한 위협의 범위에 대해 더 나은 관점을 얻게 됩니다.

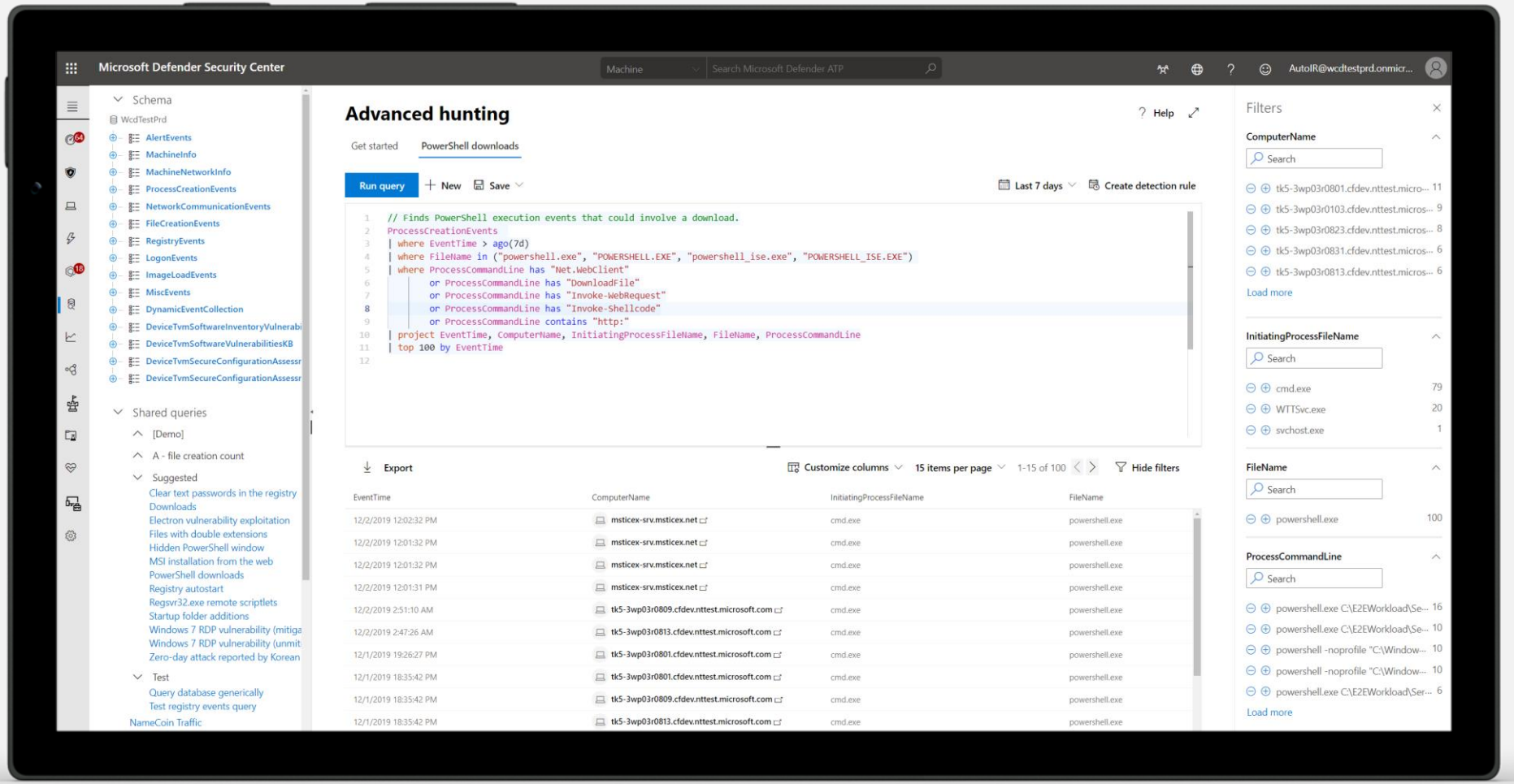
높은 정확도, 낮은 노이즈

공격을 조사하고 대응하는 데 필요한 부하와 노력을 효과적으로 줄입니다.



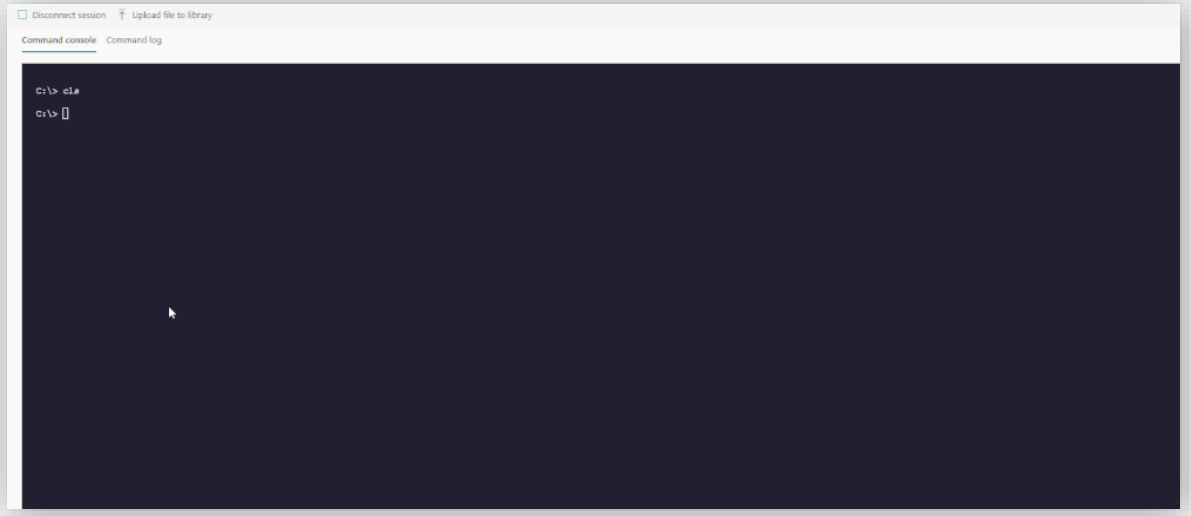
[Announcement blog]

사용자 지정 탐지 및 사용자 지정 응답을 통한 고급 헌팅



실시간 응답

- 원격 시스템에 대한 실시간 연결
- 엔트포인트 용 **Microsoft Defender Auto IR** 라이브러리 활용 (메모리 덤프, **MFT** 분석, 원시 파일 시스템 액세스 등)
  - 확장 된 수정 명령 + 간편한 실행 취소
- 전체 감사
- 확장 가능(자신의 명령 작성, 자신만의 도구 구축)
- **RBAC+** 권한
- **Git-Repo** (도구 공유)



위협 분석

주요 위협에 대처하는 방법 확인

위협에 대한 상태 보기

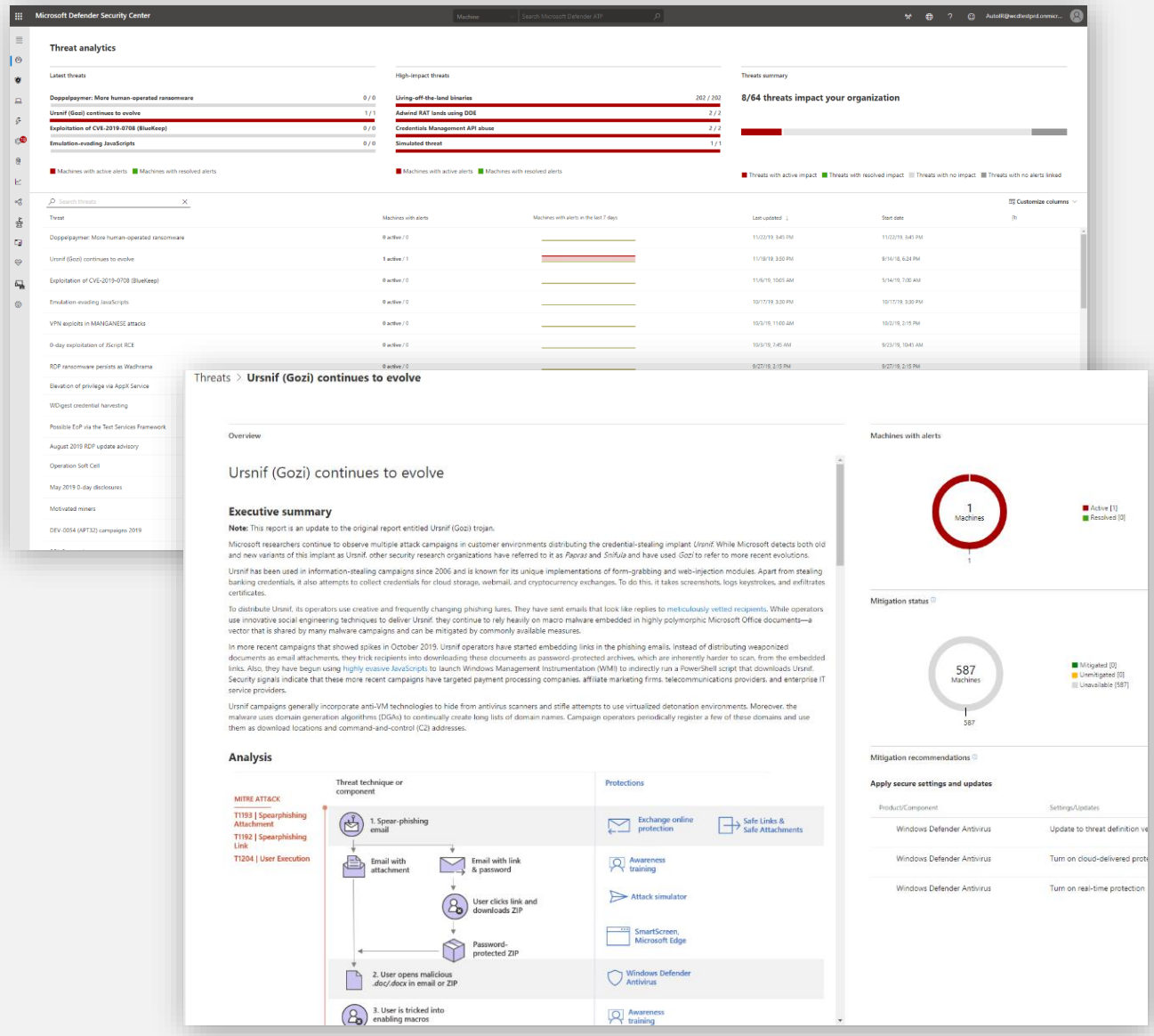
대화형 보고서를 통해 중요하고 새로운 캠페인에 대한 점수를 확인.

보호되지 않은 시스템 식별

실시간 통찰력을 통해 위협 요소가 환경에 미치는 영향 평가.

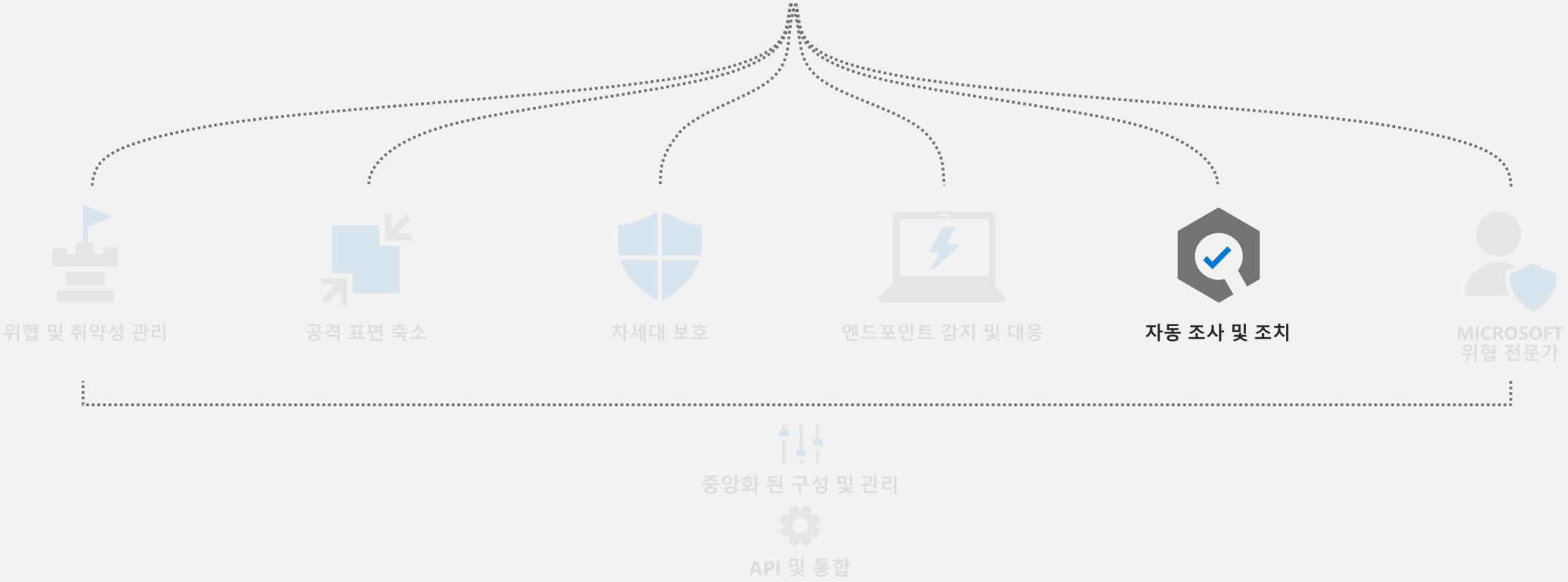
가이드

보안 복원력을 향상시키거나 위협을 방지하거나 억제하기 위한 권장 조치를 제공



엔드포인트 용
Microsoft Defender

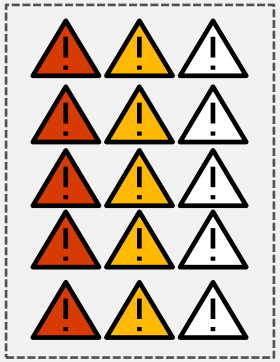
클라우드 기반의 내장된.



고객의 주요 당면 과제

- 더 많은 위협, 더 많은 경고는 분석가의 피로로 이어짐
- 경고 조사에는 시간이 많이 소요됨
- 전문성을 위해서는 높은 비용이 듦
- 수동으로 해결 작업 적용하는데 시간이 필요함
- 사이버 보안 인재 부족

수동 경고 조사 및 해결 작업에 압도된 분석가



분석가 1

분석가 2

엔드 포인트를 위한 Microsoft Defender Auto IR 란?

보안 자동화란...
사이버 위협을 조사하고 해결하기 위해 인간이 취해야 할 이상적인 단계를 모방

보안 자동화가 아닙니다...
시스템에 경보가 있는 경우 → 자동 분리

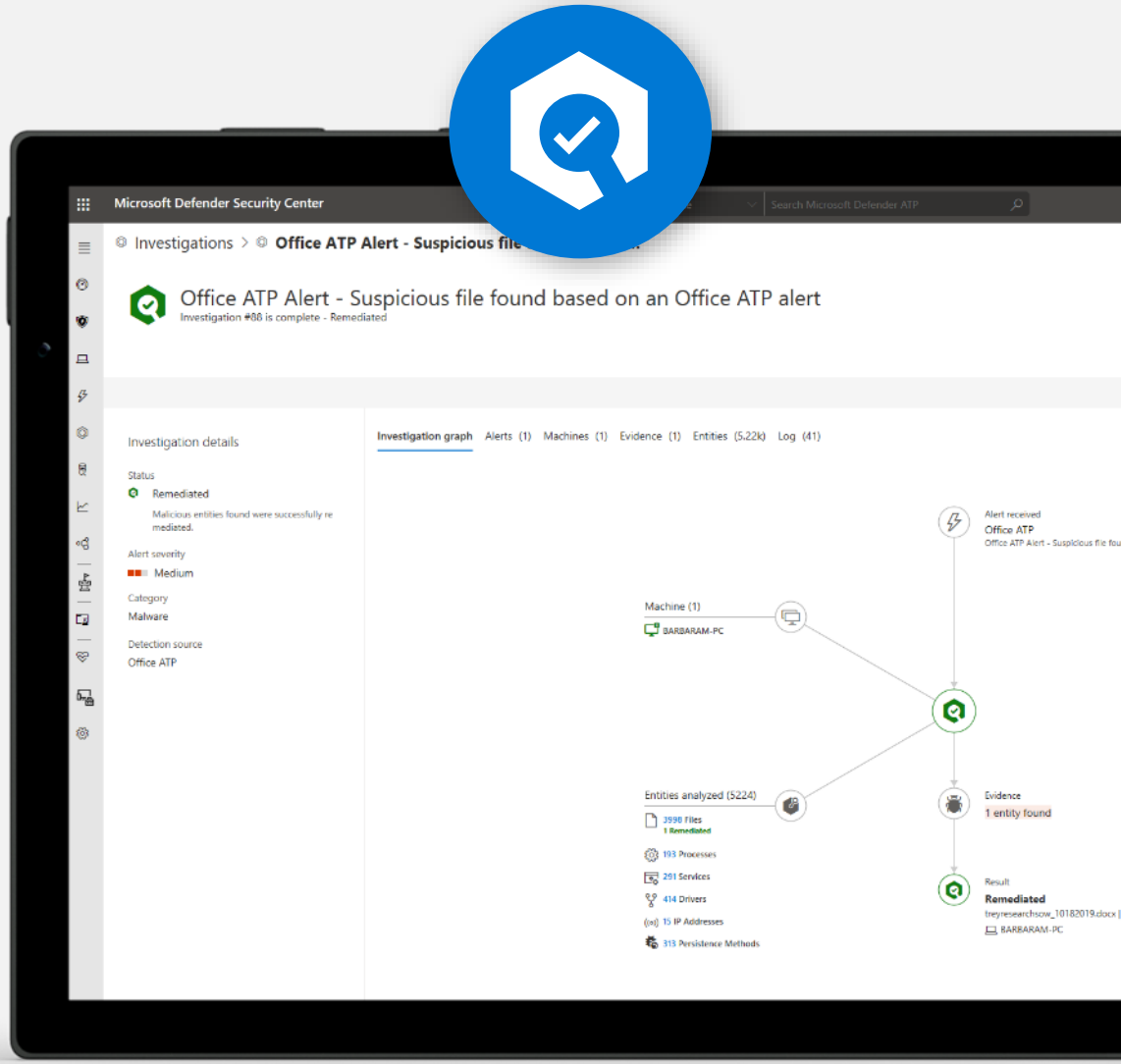
위협을 조사하고 해결할 때 분석가가 취하고 있는 단계를 살펴보면 다음과 같은 상위 단계를 식별할 수 있습니다. :

1. 위협이 작업을 필요로 하는지 여부 확인
2. 필요한 수정 조치 수행
3. 다음에 어떤 추가 조사가 필요한지 결정
4. 모든 경고에 대해 필요한 횟수만큼 반복 ☺

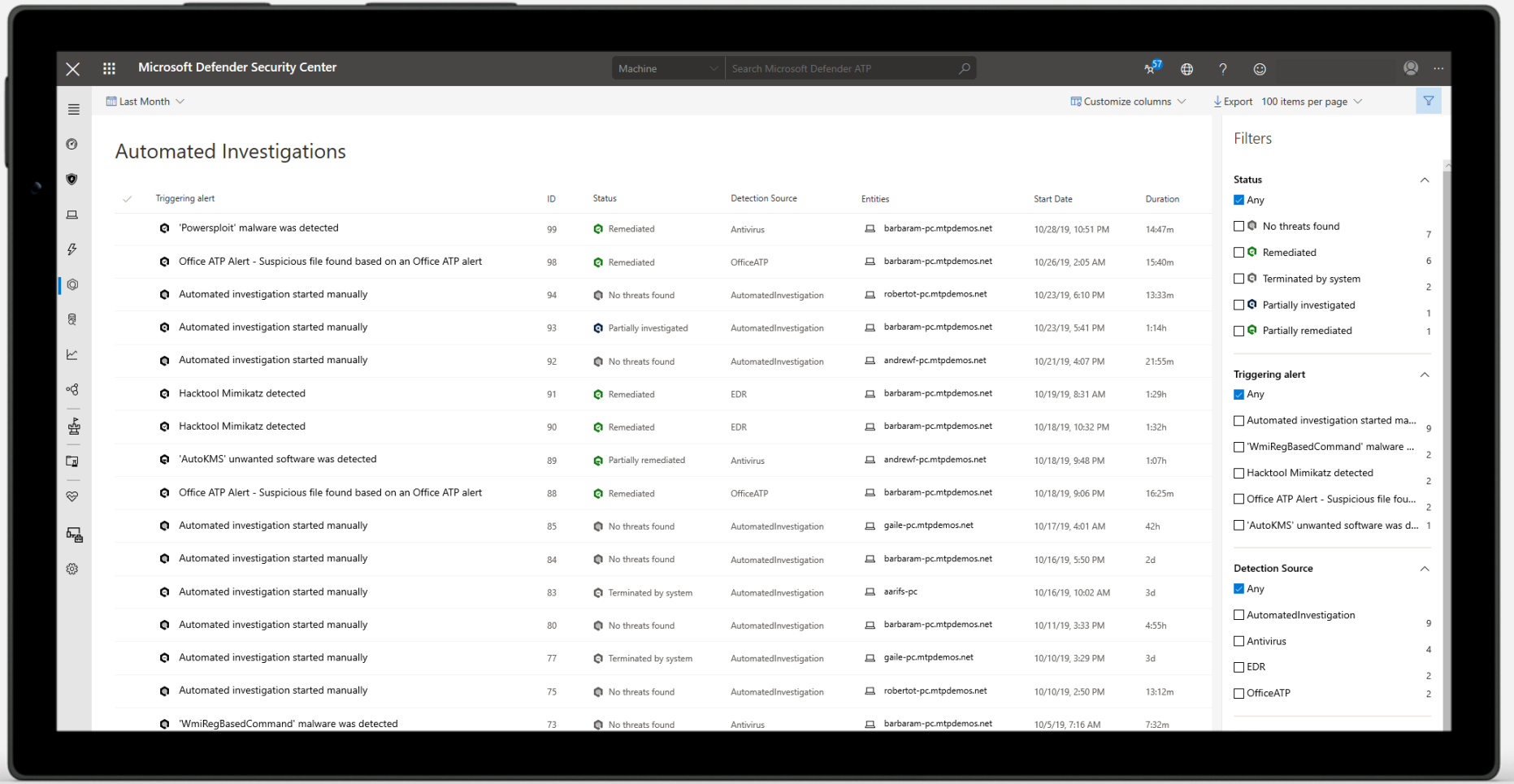
자동 조사 및 해결

경고를 자동으로 조사하고 몇 분 안에 복잡한 위협을 해결

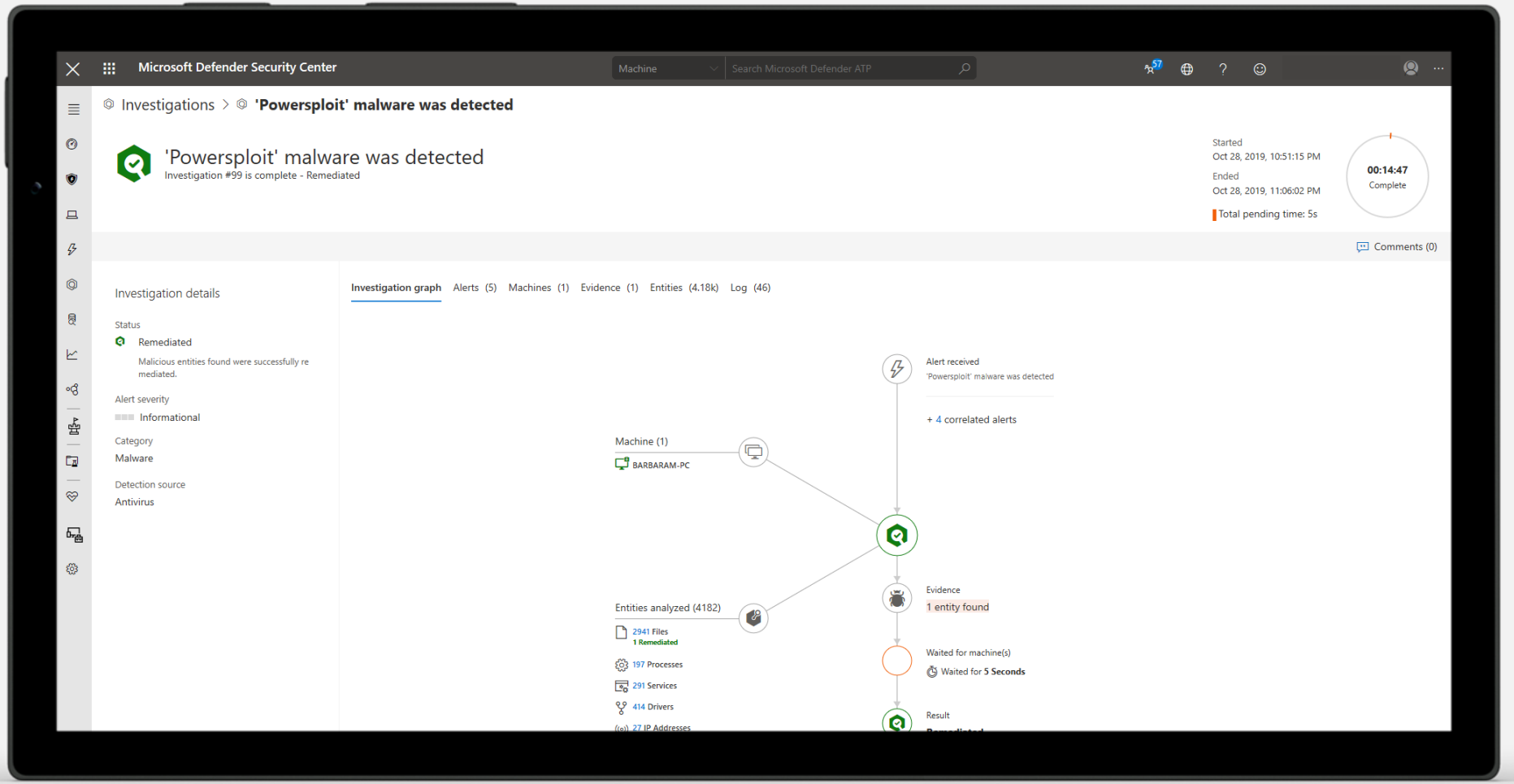
- 분석가가 취할 이상적인 조치들을 모방
- 파일 또는 메모리 기반 공격 대처
- 무제한 용량으로 **24x7** 작동



자동 조사 대기열

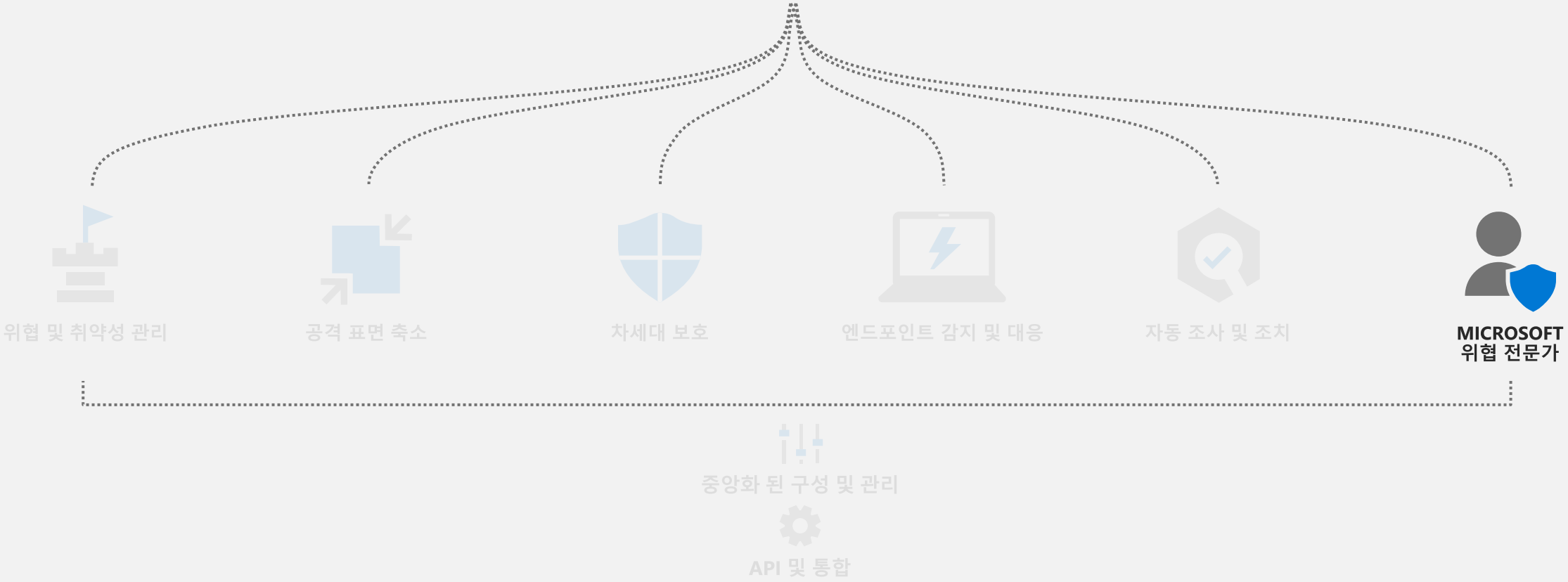

Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
Last Month
Customize columns
Export
100 items per page
Automated Investigations
Triggering alert
ID
Status
Detection Source
Entities
Start Date
Duration
'Powersploit' malware was detected 99 Remediated Antivirus barbaram-pc.mtpdemos.net 10/28/19, 10:51 PM 14:47m
Office ATP Alert - Suspicious file found based on an Office ATP alert 98 Remediated OfficeATP barbaram-pc.mtpdemos.net 10/26/19, 2:05 AM 15:40m
Automated investigation started manually 94 No threats found AutomatedInvestigation robertot-pc.mtpdemos.net 10/23/19, 6:10 PM 13:33m
Automated investigation started manually 93 Partially investigated AutomatedInvestigation barbaram-pc.mtpdemos.net 10/23/19, 5:41 PM 1:14h
Automated investigation started manually 92 No threats found AutomatedInvestigation andrewf-pc.mtpdemos.net 10/21/19, 4:07 PM 21:55m
Hacktool Mimikatz detected 91 Remediated EDR barbaram-pc.mtpdemos.net 10/19/19, 8:31 AM 1:29h
Hacktool Mimikatz detected 90 Remediated EDR barbaram-pc.mtpdemos.net 10/18/19, 10:32 PM 1:32h
'AutoKMS' unwanted software was detected 89 Partially remediated Antivirus andrewf-pc.mtpdemos.net 10/18/19, 9:48 PM 1:07h
Office ATP Alert - Suspicious file found based on an Office ATP alert 88 Remediated OfficeATP barbaram-pc.mtpdemos.net 10/18/19, 9:06 PM 16:25m
Automated investigation started manually 85 No threats found AutomatedInvestigation gaile-pc.mtpdemos.net 10/17/19, 4:01 AM 42h
Automated investigation started manually 84 No threats found AutomatedInvestigation barbaram-pc.mtpdemos.net 10/16/19, 5:50 PM 2d
Automated investigation started manually 83 Terminated by system AutomatedInvestigation aarifs-pc 10/16/19, 10:02 AM 3d
Automated investigation started manually 80 No threats found AutomatedInvestigation barbaram-pc.mtpdemos.net 10/11/19, 3:33 PM 4:55h
Automated investigation started manually 77 Terminated by system AutomatedInvestigation gaile-pc.mtpdemos.net 10/10/19, 3:29 PM 3d
Automated investigation started manually 75 No threats found AutomatedInvestigation robertot-pc.mtpdemos.net 10/10/19, 2:50 PM 13:12m
'WmiRegBasedCommand' malware was detected 73 No threats found Antivirus barbaram-pc.mtpdemos.net 10/5/19, 7:16 AM 7:32m
Filters
Status
Any
No threats found 7
Remediated 6
Terminated by system 2
Partially investigated 1
Partially remediated 1
Triggering alert
Any
Automated investigation started ma... 9
'WmiRegBasedCommand' malware ... 2
Hacktool Mimikatz detected 2
Office ATP Alert - Suspicious file fou... 2
'AutoKMS' unwanted software was d... 1
Detection Source
Any
AutomatedInvestigation 9
Antivirus 4
EDR 2
OfficeATP 2

조사 그래프


Microsoft Defender Security Center
Machine
Search Microsoft Defender ATP
Investigations
'Powersploit' malware was detected
'Powersploit' malware was detected
Investigation #99 is complete - Remediated
Started
Oct 28, 2019, 10:51:15 PM
Ended
Oct 28, 2019, 11:06:02 PM
Total pending time: 5s
00:14:47
Complete
Comments (0)
Investigation details
Status
Remediated
Malicious entities found were successfully re mediated.
Alert severity
Informational
Category
Malware
Detection source
Antivirus
Investigation graph
Alerts (5)
Machines (1)
Evidence (1)
Entities (4.18k)
Log (46)
Alert received
'Powersploit' malware was detected
+ 4 correlated alerts
Machine (1)
BARBARAM-PC
Entities analyzed (4182)
2941 Files
1 Remediated
197 Processes
291 Services
414 Drivers
27 IP Addresses
Evidence
1 entity found
Waited for machine(s)
Waited for 5 Seconds
Result

엔드포인트 용
Microsoft Defender

클라우드 기반의 내장된.



고객의 주요 당면 과제

위협이 점점 더 복잡해짐에 따라 경고 처리에 대한 추가 컨텍스트 및 지침이 필요할 수 있습니다.

- 추가적인 위협 컨텍스트 필요
- 필요할 때 연락할 위협 전문가가 없음
- 경고 처리에 대한 지침 누락
- 중요 알림을 놓칠 수 있음
- 이 경고나 이벤트가 정말로 우리 조직에 중요한가요?

Managed Threat Hunting 서비스

추가적인 감시 및 분석 계층으로 위협 요소가 누락되지 않도록 지원

침해를 놓치지 마십시오

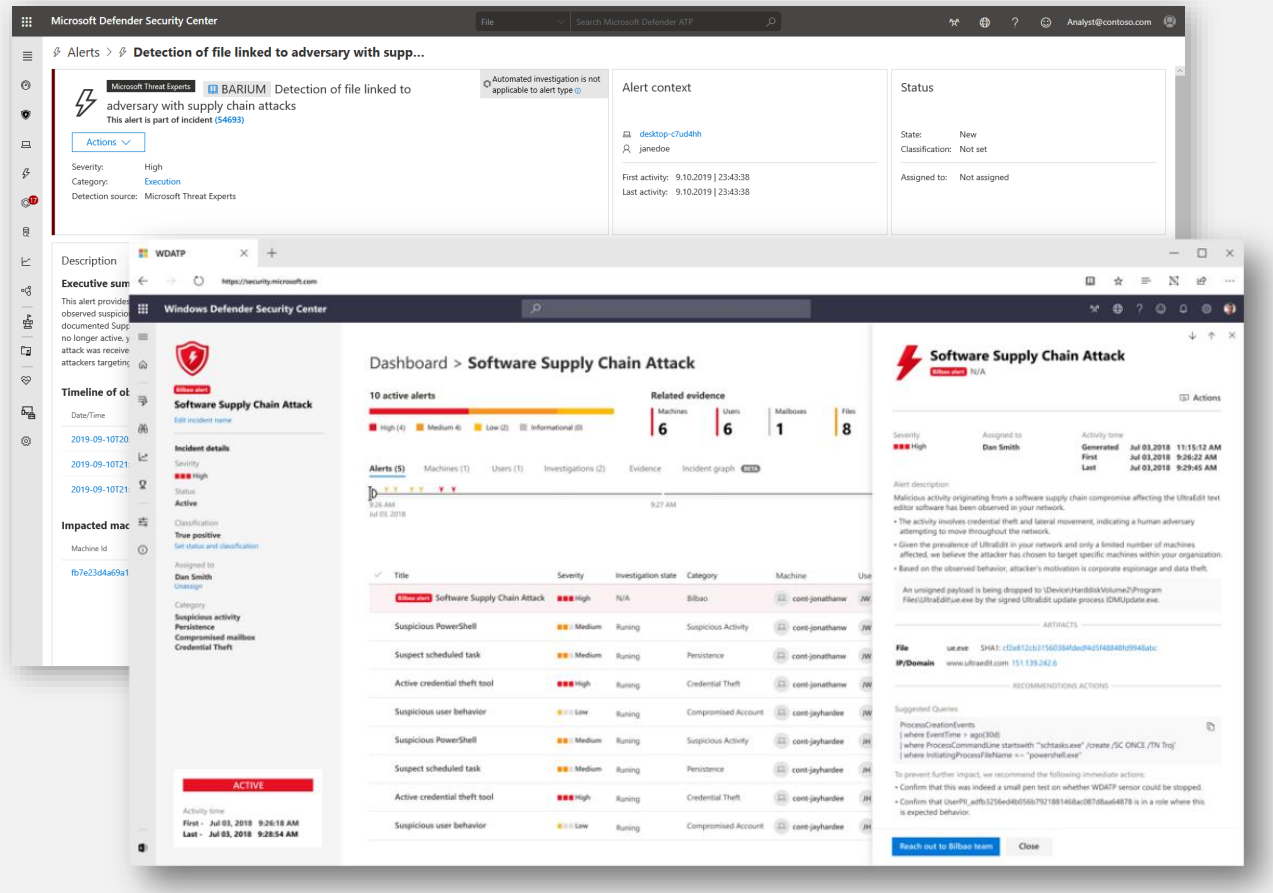
위협 전문가가 당신을 도와줍니다.

Microsoft 위협 전문가를 통해 고유한 환경에서 이상 징후 또는 알려진 악성 행위를 사전에 파악.

온디맨드 전문가

편하게 이용 가능한 세계적 수준의 전문가.

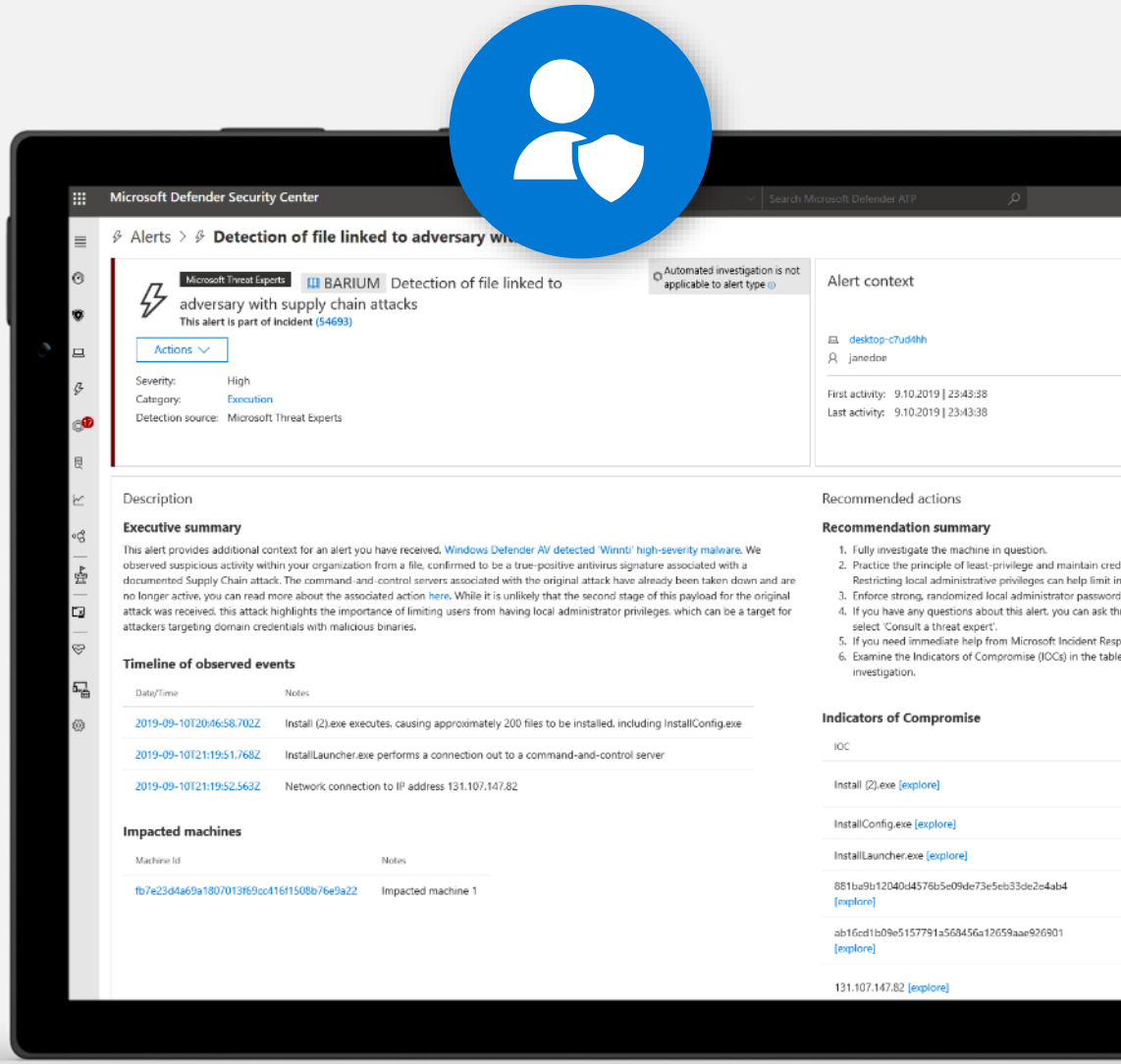
경고, 멀웨어 또는 위협 컨텍스트에 대한 질문이 있습니까? 숙련된 Microsoft 위협 전문가에게 문의하세요.



Microsoft 위협 전문가

SOC에 대한 심층적인 지식과 사전 예방적 위협 탐색 제공

- 전문가 수준의 위협 모니터링 및 분석
- 경고를 통한 환경에 특화된 컨텍스트
- 세계적 수준의 전문가에 직접 접근



Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Execution
Detection source: Microsoft Threat Experts

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 23:43:38

Status

State: New
Classification: Not set

Assigned to: Not assigned

Description

Executive summary

This alert provides additional context for an alert you have received, Windows Defender AV detected 'Winnti' high-severity malware. We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action here. While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

Timeline of observed events

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

Impacted machines

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f1508b76e9a22	Impacted machine 1

Recommended actions

Recommendation summary

1. Fully investigate the machine in question.
2. Practice the principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
3. Enforce strong, randomized local administrator passwords. Use tools like LAPS.
4. If you have any questions about this alert, you can ask through Experts-on-Demand! From this alert page click the Actions menu and select 'Consult a threat expert'.
5. If you need immediate help from Microsoft Incident Response consider opening a Premier support case.
6. Examine the Indicators of Compromise (IOCs) in the table below, and use the suggested Advanced Hunting queries to continue your investigation.

Indicators of Compromise

IOC	Type	Notes
Install (2).exe [explore]	filename	File used to install numerous files, including the true-positive InstallConfig.exe
InstallConfig.exe [explore]	filename	True-positive malicious file
InstallLauncher.exe [explore]	filename	File performing network connection to command-and-control
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 [explore]	hash	SHA1 for Backdoor:Win32/Winnti.X!dha, labelled as InstallConfig.exe
ab16cd1b09e5157791a568456a12659aae926901 [explore]	hash	SHA1 for file labelled as InstallLauncher.exe
131.107.147.82 [explore]	ip	Command-and-control server launched from InstallLauncher.exe

Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Execution
Detection source: Microsoft Threat Experts

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 23:43:38

Status

State: New
Classification: Not set

Assigned to: Not assigned

Description

Executive summary

This alert provides additional context for an alert you have received, Windows Defender AV detected 'Winnti' high-severity malware. We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action here. While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

Timeline of observed events

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

Impacted machines

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f1508b76e9a22	Impacted machine 1

Recommended actions

Recommendation summary

1. Fully investigate the machine in question.
2. Practice the principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
3. Enforce strong, randomized local administrator passwords. Use tools like LAPS.
4. If you have any questions about this alert, you can ask through Experts-on-Demand! From this alert page click the Actions menu and select 'Consult a threat expert'.
5. If you need immediate help from Microsoft Incident Response consider opening a Premier support case.
6. Examine the Indicators of Compromise (IOCs) in the table below, and use the suggested Advanced Hunting queries to continue your investigation.

Indicators of Compromise

IOC	Type	Notes
Install (2).exe [explore]	filename	File used to install numerous files, including the true-positive InstallConfig.exe
InstallConfig.exe [explore]	filename	True-positive malicious file
InstallLauncher.exe [explore]	filename	File performing network connection to command-and-control
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 [explore]	hash	SHA1 for Backdoor:Win32/Winnti.X!dha, labelled as InstallConfig.exe
ab16cd1b09e5157791a568456a12659aae926901 [explore]	hash	SHA1 for file labelled as InstallLauncher.exe
131.107.147.82 [explore]	ip	Command-and-control server launched from InstallLauncher.exe

Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

- Manage alert
- View machine timeline
- Open incident page
- Print alert
- Consult a threat expert

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 23:43:38

Status

State: New
Classification: Not set

Assigned to: Not assigned

Executive summary

This alert provides additional context for an alert you have received, Windows Defender AV detected 'Winnti' high-severity malware. We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action here. While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

Timeline of observed events

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

Impacted machines

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f1508b76e9a22	Impacted machine 1

Recommended actions

Recommendation summary

1. Fully investigate the machine in question.
2. Practice the principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
3. Enforce strong, randomized local administrator passwords. Use tools like LAPS.
4. If you have any questions about this alert, you can ask through Experts-on-Demand! From this alert page click the Actions menu and select 'Consult a threat expert'.
5. If you need immediate help from Microsoft Incident Response consider opening a Premier support case.
6. Examine the Indicators of Compromise (IOCs) in the table below, and use the suggested Advanced Hunting queries to continue your investigation.

Indicators of Compromise

IOC	Type	Notes
Install (2).exe [explore]	filename	File used to install numerous files, including the true-positive InstallConfig.exe
InstallConfig.exe [explore]	filename	True-positive malicious file
InstallLauncher.exe [explore]	filename	File performing network connection to command-and-control
881ba9b12040d4576b5e09de73e5eb33de2e4ab4 [explore]	hash	SHA1 for Backdoor:Win32/Winnti.X!dha, labelled as InstallConfig.exe
ab16cd1b09e5157791a568456a12659aae926901 [explore]	hash	SHA1 for file labelled as InstallLauncher.exe
131.107.147.82 [explore]	ip	Command-and-control server launched from InstallLauncher.exe

Alerts > **Detection of file linked to adversary with supp...**

Microsoft Threat Experts | BARIUM | Detection of file linked to adversary with supply chain attacks

This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Execution
Detection source: Microsoft Threat Experts

Alert context

desktop-c7ud4hh
janedoe

First activity: 9.10.2019 | 23:43:38
Last activity: 9.10.2019 | 23:43:38

Description

Executive summary

This alert provides additional context for an alert you have received, Windows Defender AV detected 'Winnti' high-severity malware. We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action here. While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

Timeline of observed events

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

Impacted machines

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f1508b76e9a22	Impacted machine 1

Recommended actions

Recommendation summary

1. Fully investigate the machine in questio
2. Practice the principle of least-privilege a
   Restricting local administrative privileges
3. Enforce strong, randomized local admini
4. If you have any questions about this aler
   select 'Consult a threat expert'.
5. If you need immediate help from Micros
6. Examine the Indicators of Compromise (
   investigation.

Indicators of Compromise

IOC
Install (2).exe [explore]
InstallConfig.exe [explore]
InstallLauncher.exe [explore]
881ba9b12040d4576b5e09de73e5eb33de2e [explore]
ab16cd1b09e5157791a568456a12659aae92 [explore]
131.107.147.82 [explore]

Microsoft Threat Experts - Trial

Your Experts on Demand trial version expires in 41 days from your Microsoft Threat Experts enrolment. Contact your Microsoft representative to get a full subscription.

Learn more about Microsoft Threat Experts – Experts on Demand

Consult a threat expert

Get Microsoft Threat Experts advice and insights about suspicious activities in your organization.

Ensure that the portal page for the alert or machine in question is in view while providing information for this inquiry.

Note: This and other relevant information will be shared with Microsoft Threat Experts to enable the best response to your inquiry.

Inquiry topic *

https://securitycenter.windows.com/alert/da637073841040265613_-882982118

Thank you for sending this Threat Expert alert. Can you help us investigate this threat further including whether you think we were targeted, and whether this and other machines in our company were compromised?

Email *

Enter the email address you'd like Microsoft Threat Experts to send their reply

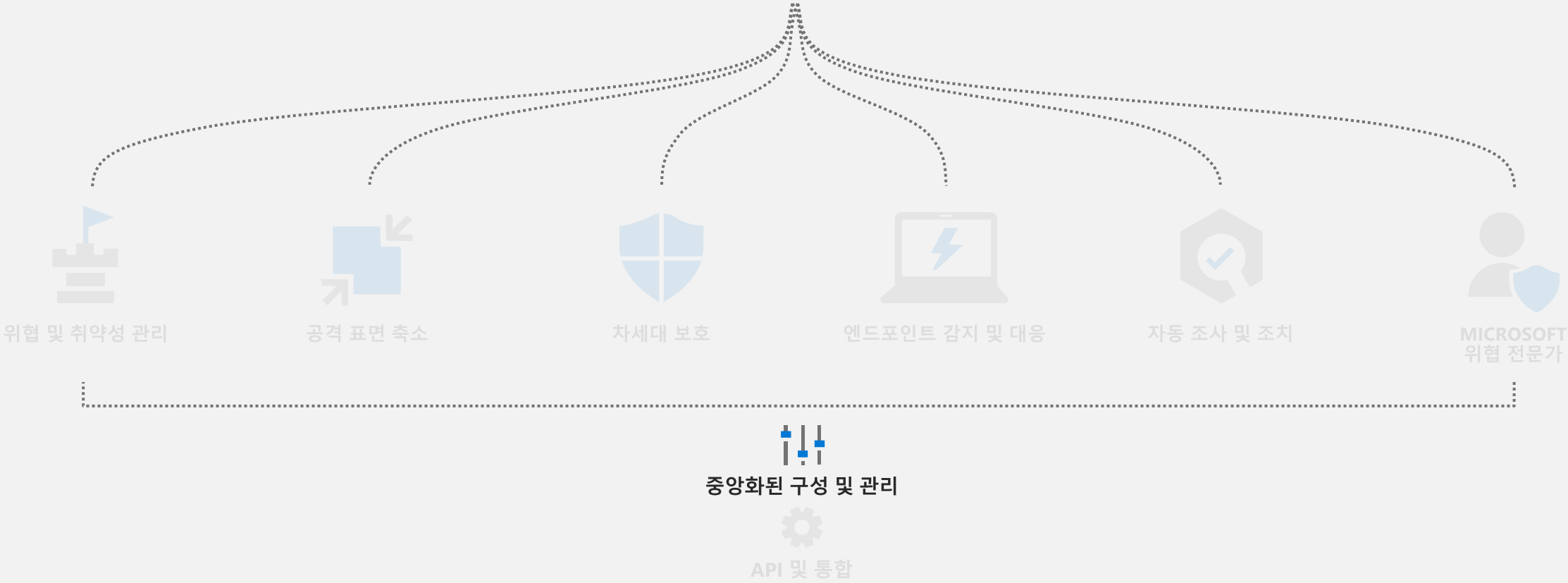
Analyst@contoso.com

Submit

Privacy statement.

엔드포인트 용
Microsoft Defender

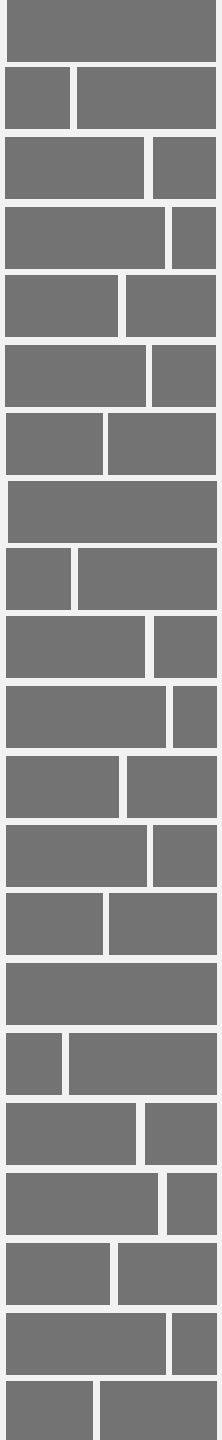
클라우드 기반의 내장된.



역사적 역할 및 마찰

보안 팀

- 보안 모니터링 및 위험 감소를 담당
- 위협, 보안 사고, 노출 및 완화 파악
- 보안 정책 정의
- 영향을 받은 장치/사용자에 대한 신속한 문제 해결이 우선 순위

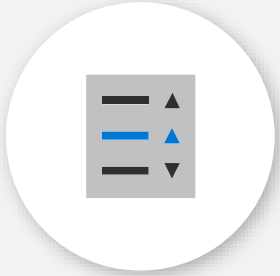


IT 팀

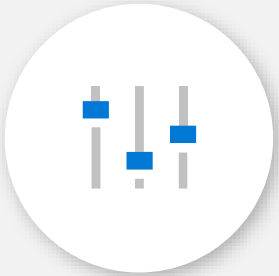
- 보안 정책을 포함한 정책 구성 담당
- 변경에 대한 영향 및 글로벌 정책 롤아웃 단계를 분석
- 안정적인 IT 환경과 낮은 비용이 우선 순위

고객 요구사항

간단하고 크로스 플랫폼인 통합 엔드포인트 보안 관리 콘솔



직관적인 고급 정책 관리 기능



세밀하고 완전하게 제어하는 보안

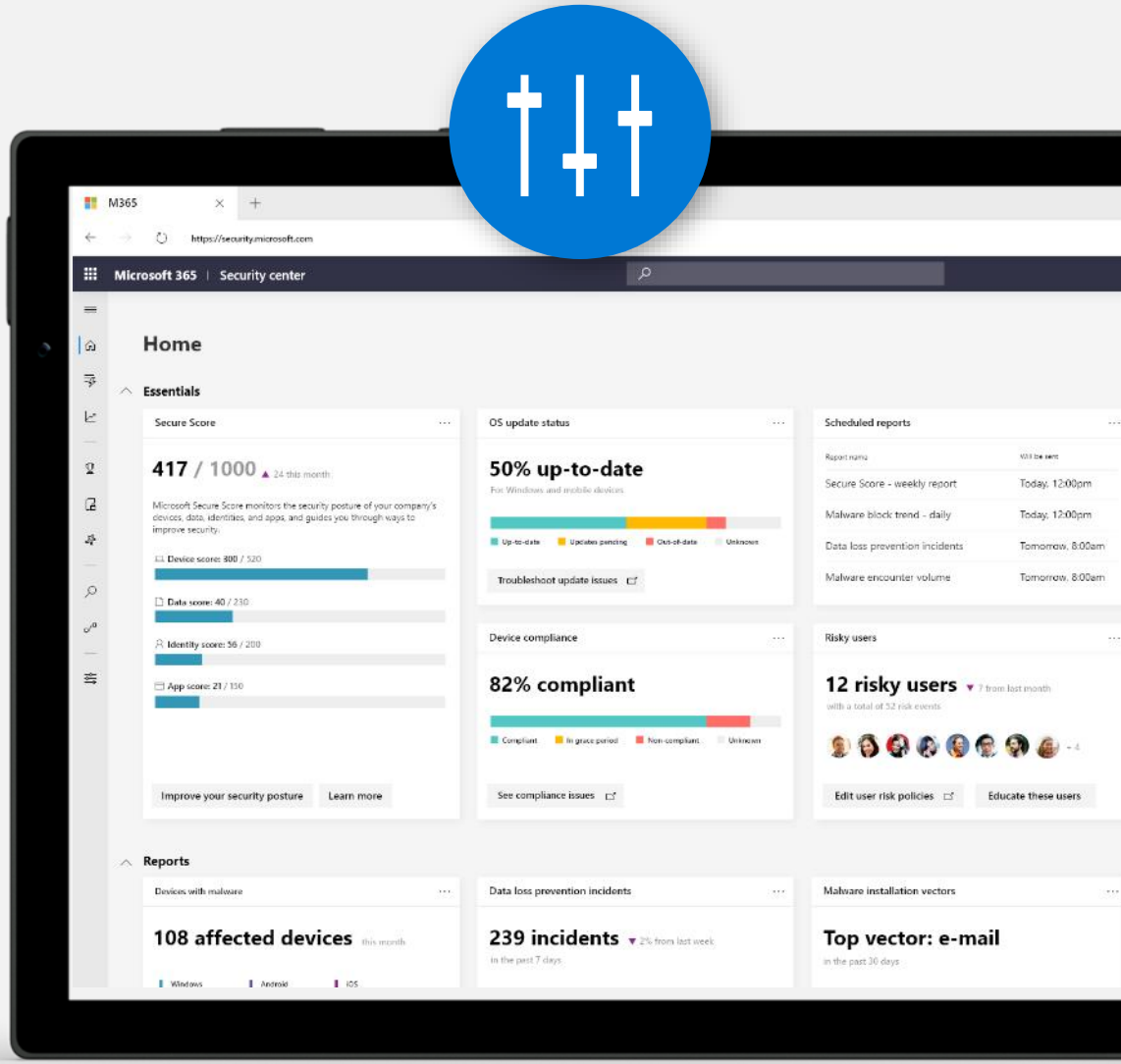
엔드포인트 상태에 대한 지속적인 평가 및 보고

원활하고 마찰이 없음

보안 관리

환경의 변화를 평가, 구성 및 대응

- 중앙에서 보안 평가 및 구성
- 상세한 모니터링 및 가시성을 위한 다양한 보고서 및 대시 보드
- 정책 평가와 정책 시행 간의 원활한 통합



엔드포인트 보안 관리

모든 장치

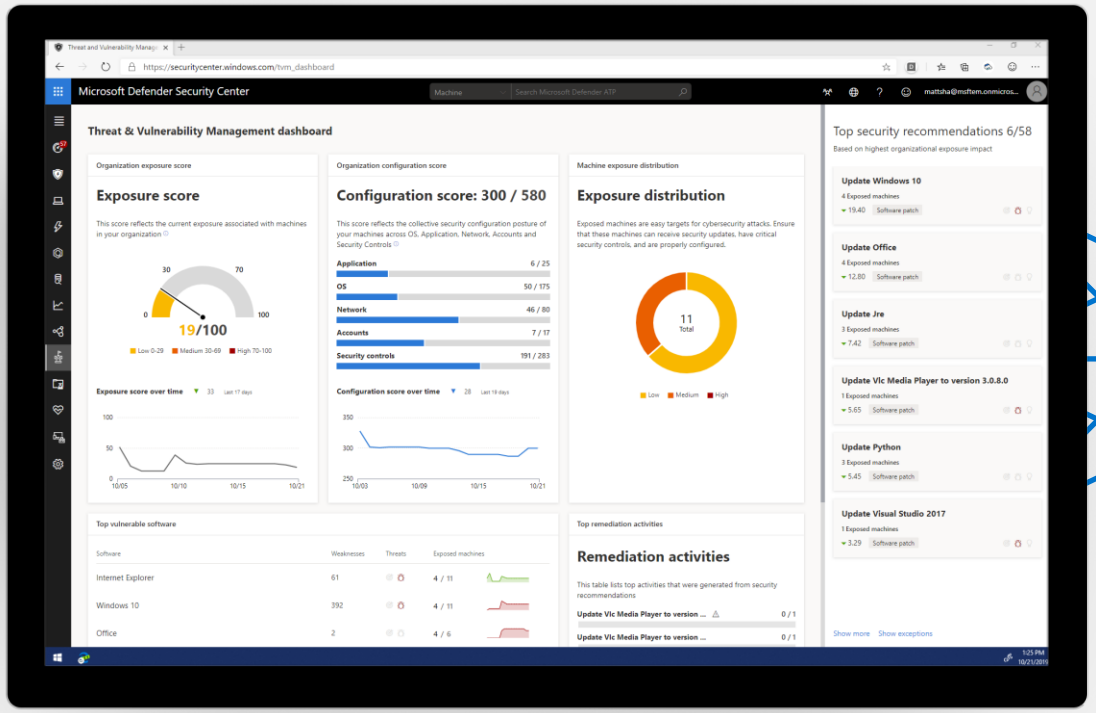
보안 관리자 경험

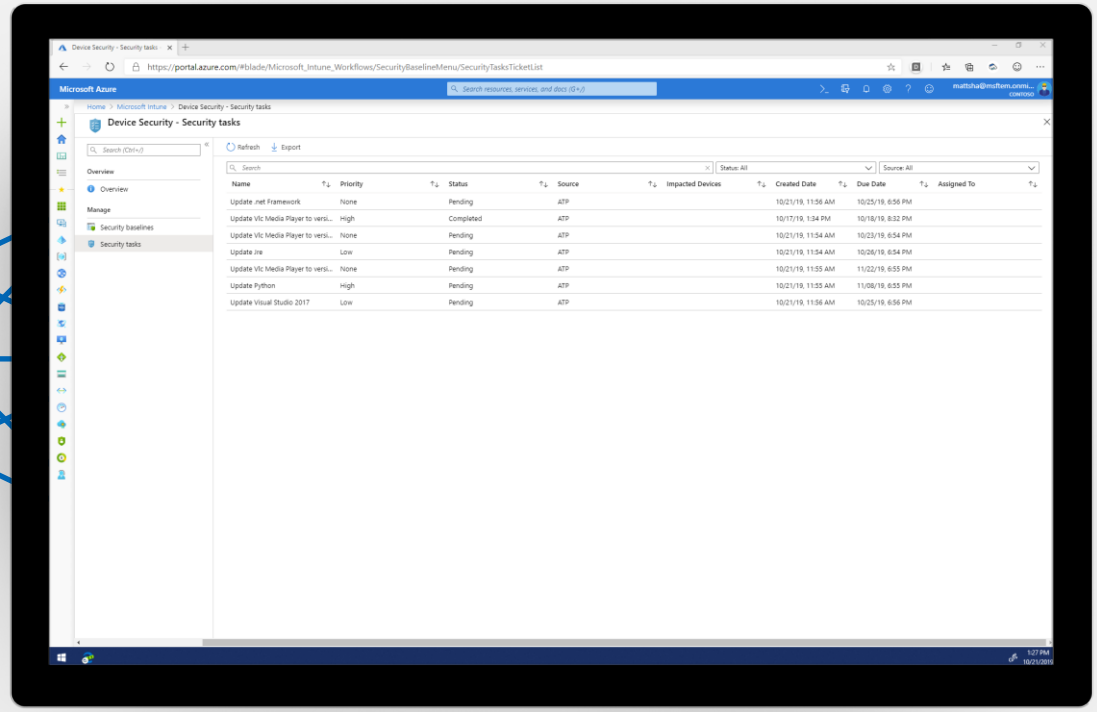
보안 기준

보안 작업

Windows, Mac, Linux, Android 또는 iOS의 모든 장치에 대한 보안 정책 대상 지정

원활한 통합





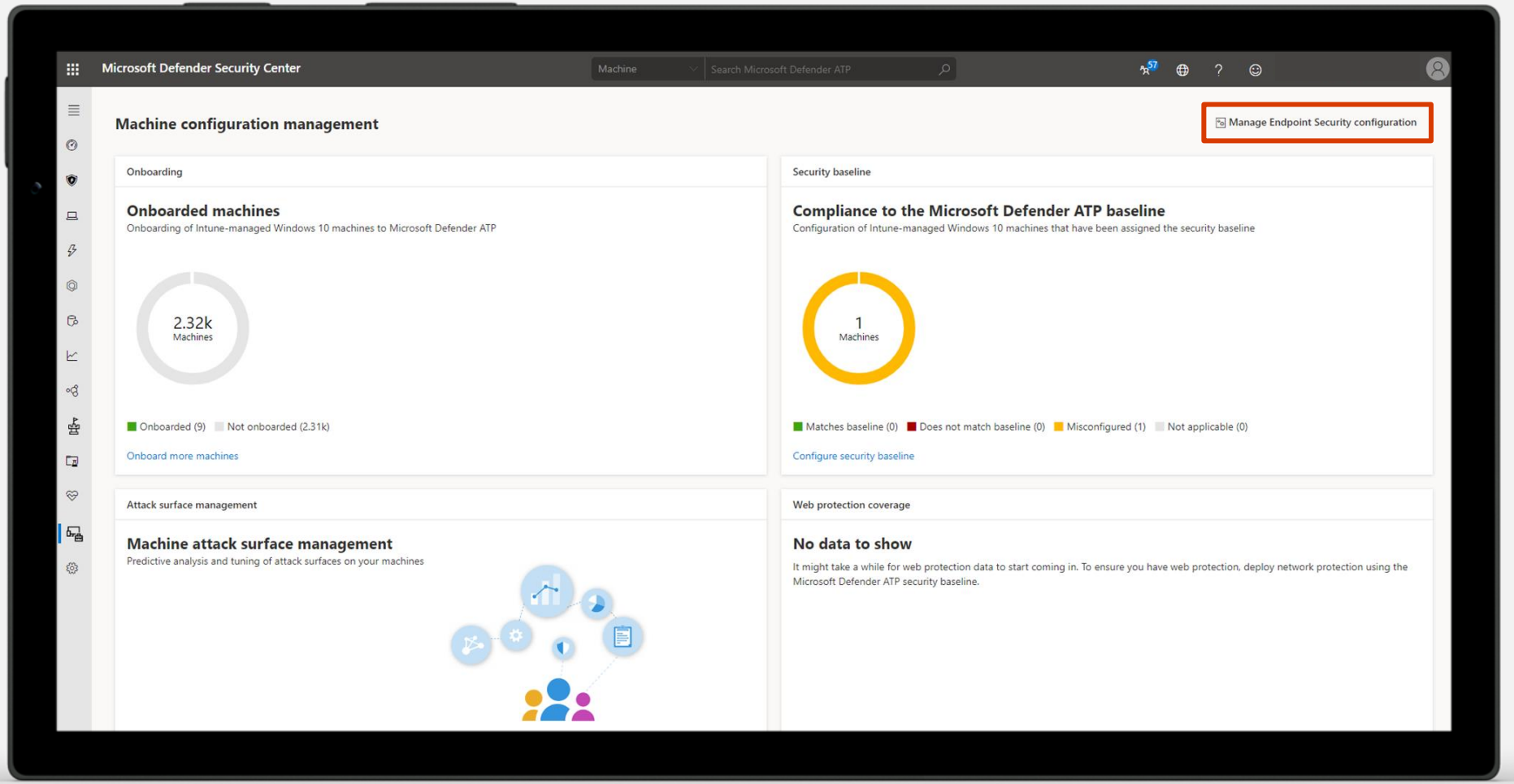
엔드포인트 용 Microsoft Defender

정책 평가

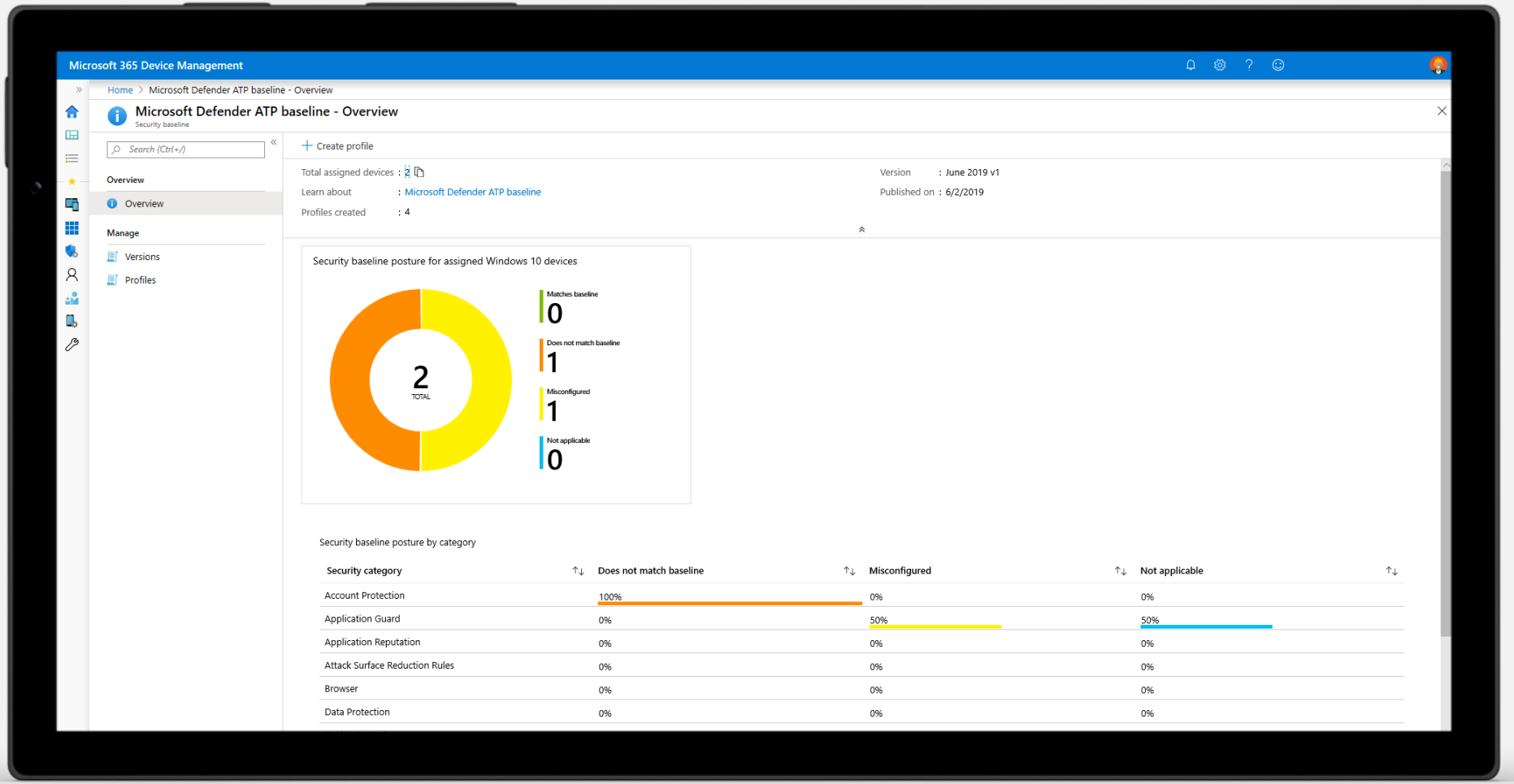
Microsoft Endpoint Manager

정책 시행

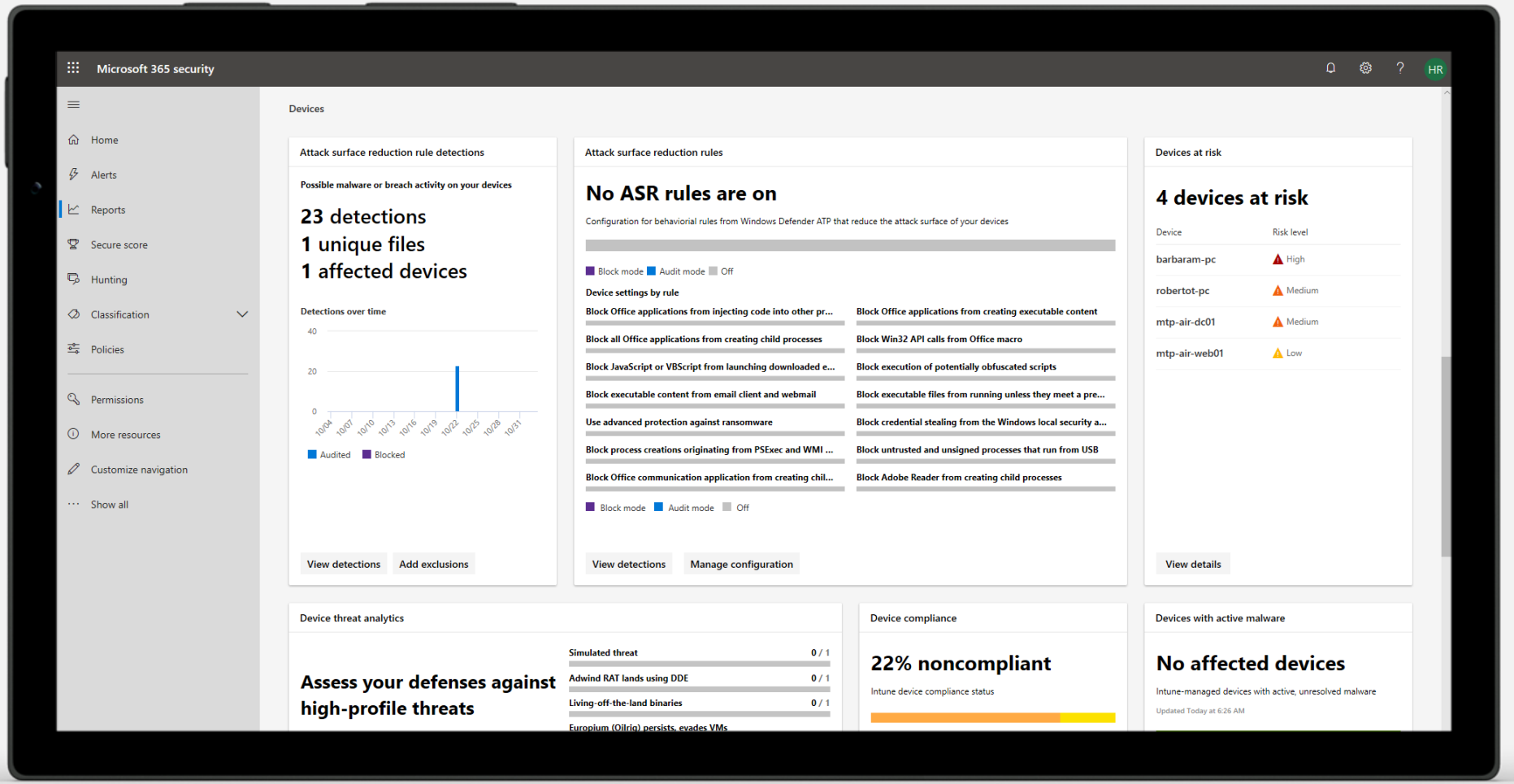
콘솔에서 관리 컨트롤에 쉽게 액세스



Microsoft Endpoint Manager에서 보안 제어 및 기준선 설정

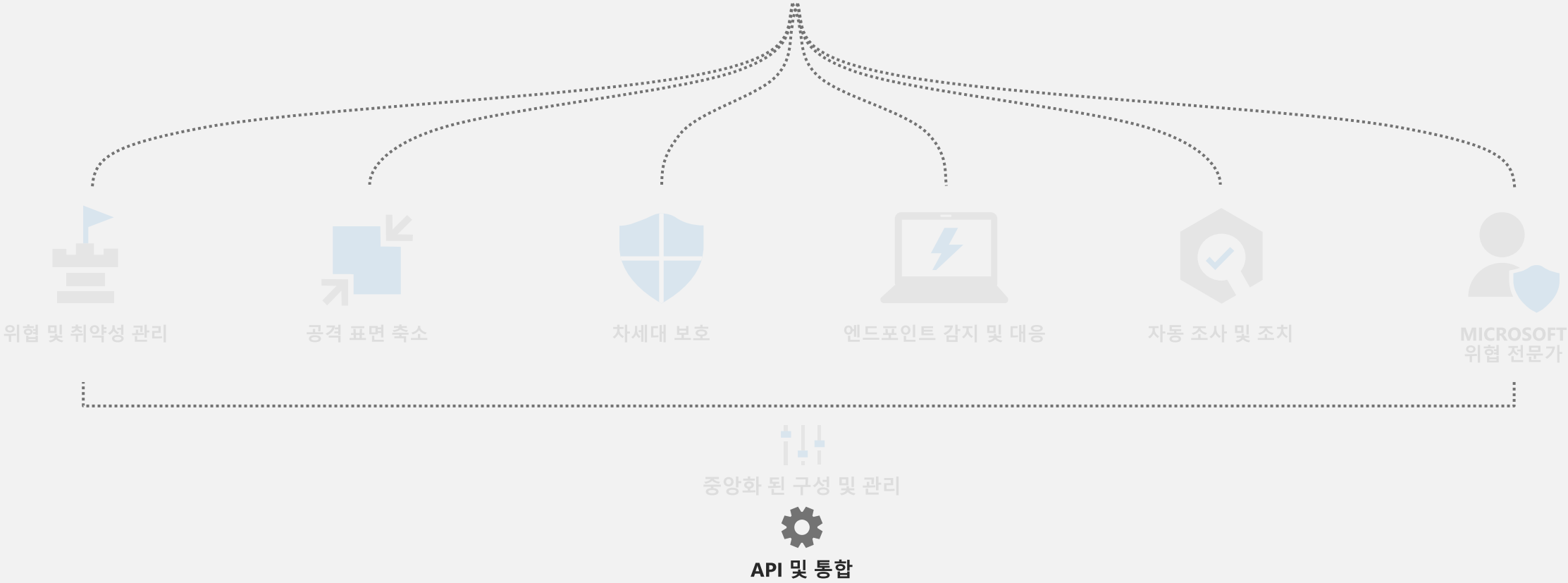


Endpoint용 Microsoft Defender에서 다양한 보고서 작성

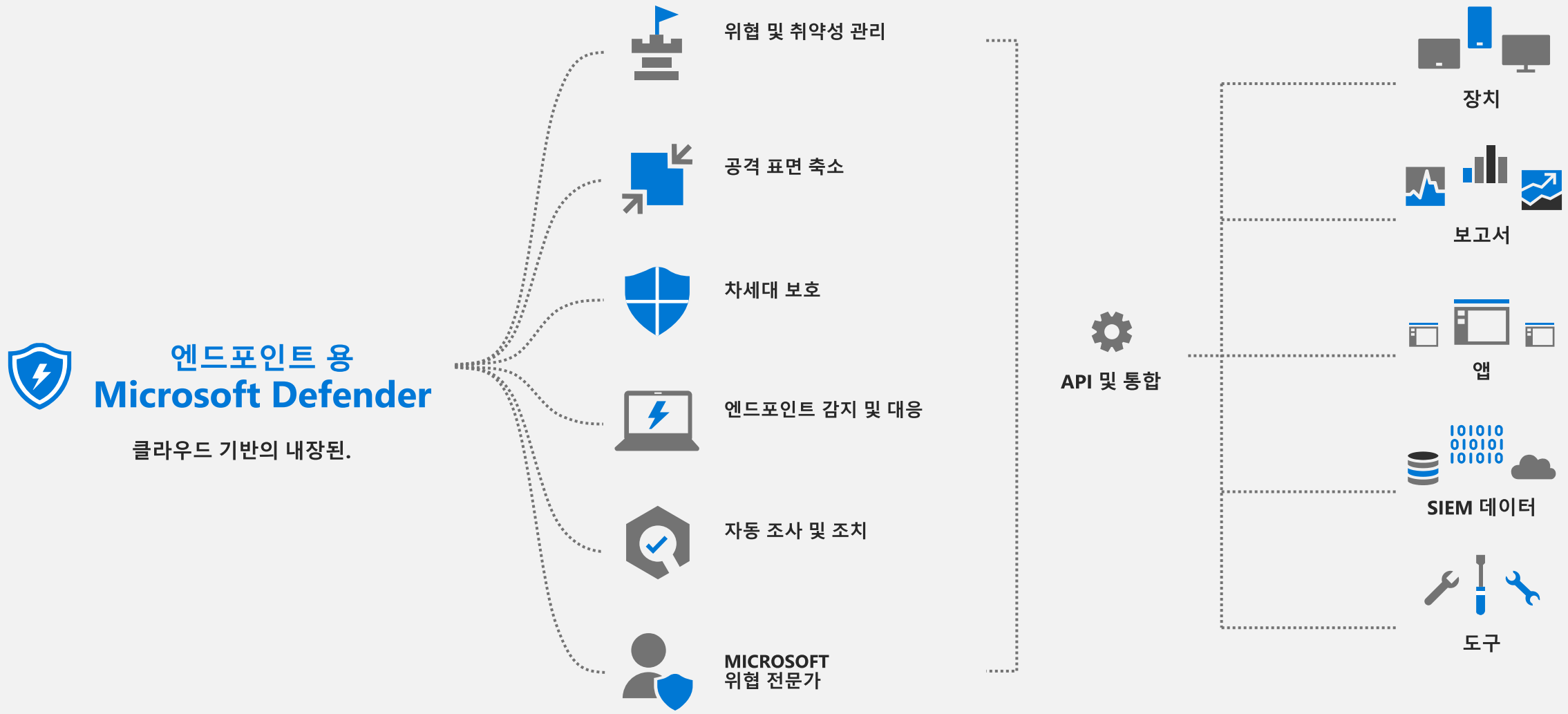


엔드포인트 용
Microsoft Defender

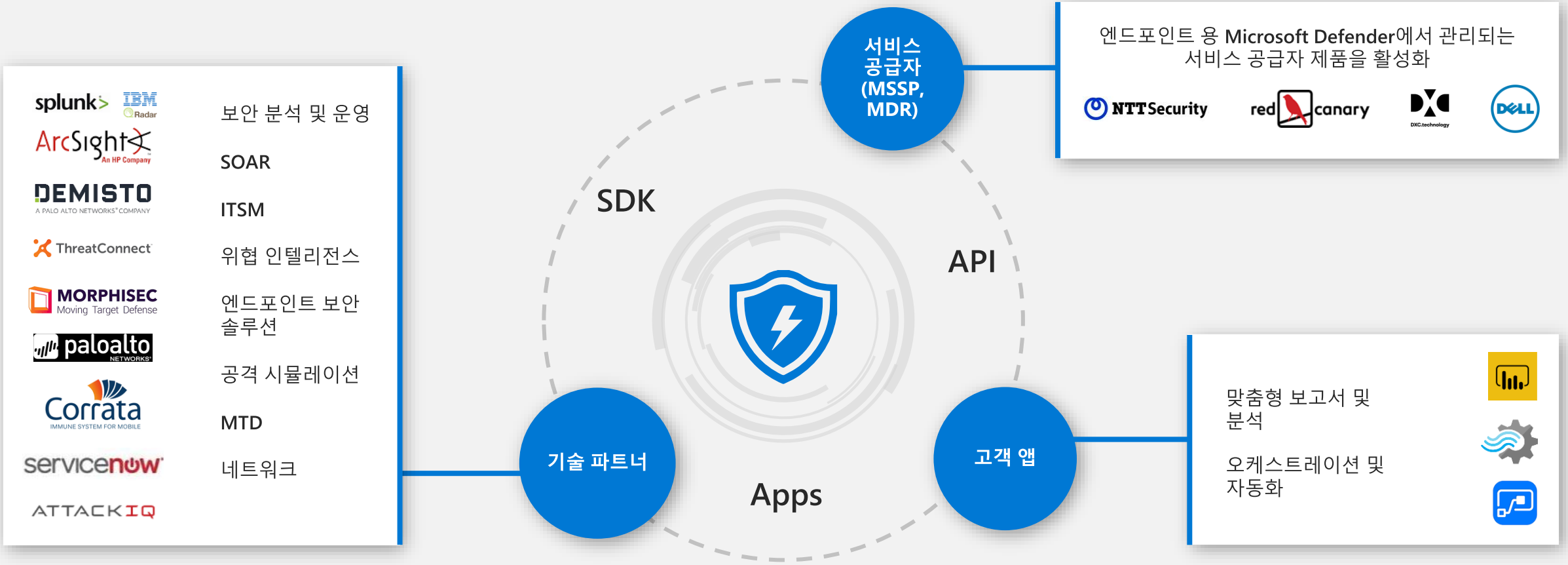
클라우드 기반의 내장된.



플랫폼과 연결


엔드포인트 용
Microsoft Defender
클라우드 기반의 내장된.
위협 및 취약성 관리
공격 표면 축소
차세대 보호
엔드포인트 감지 및 대응
자동 조사 및 조치
MICROSOFT
위협 전문가
API 및 통합
장치
보고서
앱
SIEM 데이터
도구

에코시스템 및 API를 통한 엔드포인트 용 Microsoft Defender



+ Query API
+ Streaming API
+ Actions API
+ Threat intel API, Vulnerability API
+ Application connectors (PBI, Flow, SNOW)
+ Microsoft Security Graph connector
+ AAD authentication & authorization
+ RBAC controls
+ Developer kit
+ Partner integration kit
+ Developer License

엔드포인트 용 Microsoft Defender API 및 파트너

연결된 솔루션의 손쉬운 개발 및 추적

API 탐색기

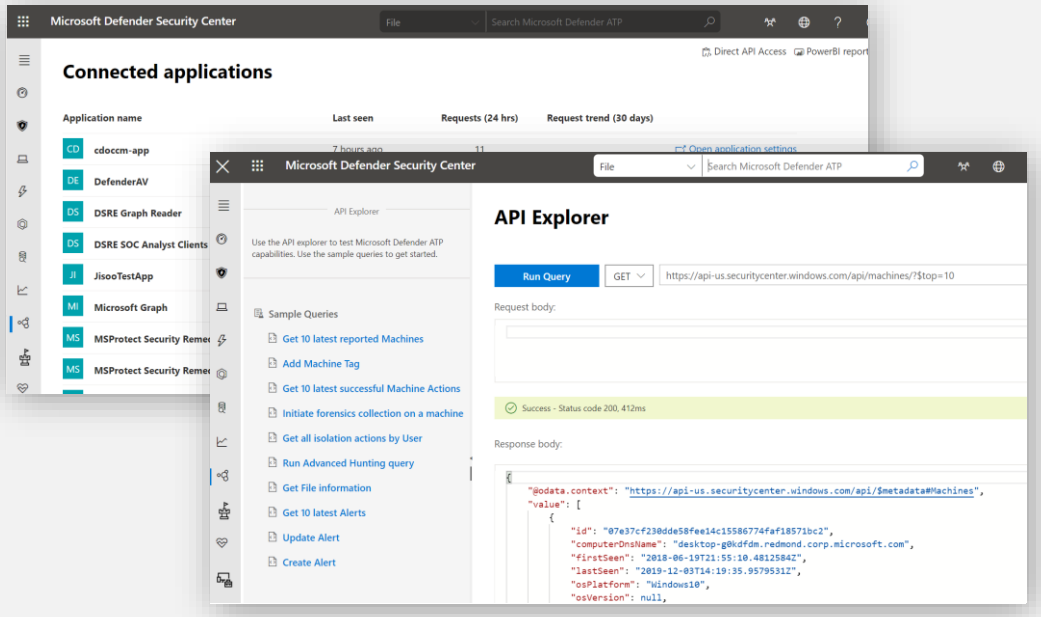
- 다양한 엔드포인트 용 **Microsoft Defender API**를 대화식으로 탐색

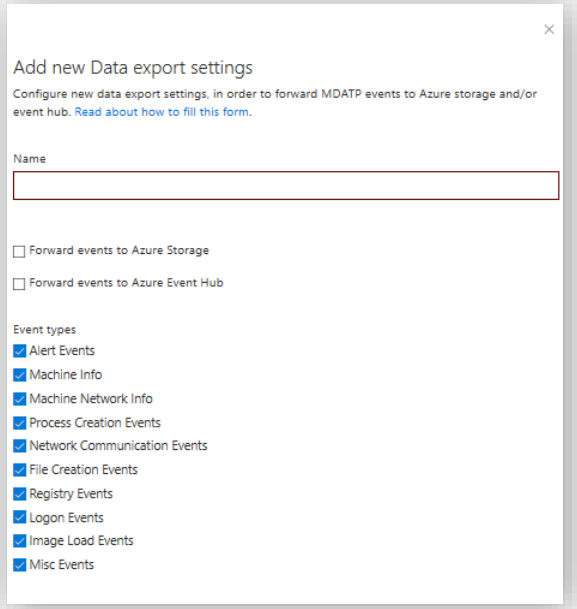
통합된 컴플라이언스 평가

- 조직에서 엔드포인트 용 **Microsoft Defender** 플랫폼과 통합되는 앱 추적.

데이터 내보내기 API

- 고급 헌팅 이벤트를 스토리지 계정으로 스트리밍하도록 엔드포인트 용 **Microsoft Defender** 구성





Cross-platform

엔드포인트 용 Microsoft Defender (Mac)

크로스 플랫폼 여정의 첫 번째 단계

위협 예방

- Mac OS를 위한 실시간 MW 보호
- 엔드포인트 용 Microsoft Defender 콘솔에 표시되는 멀웨어 탐지 경고

엔터프라이즈 급

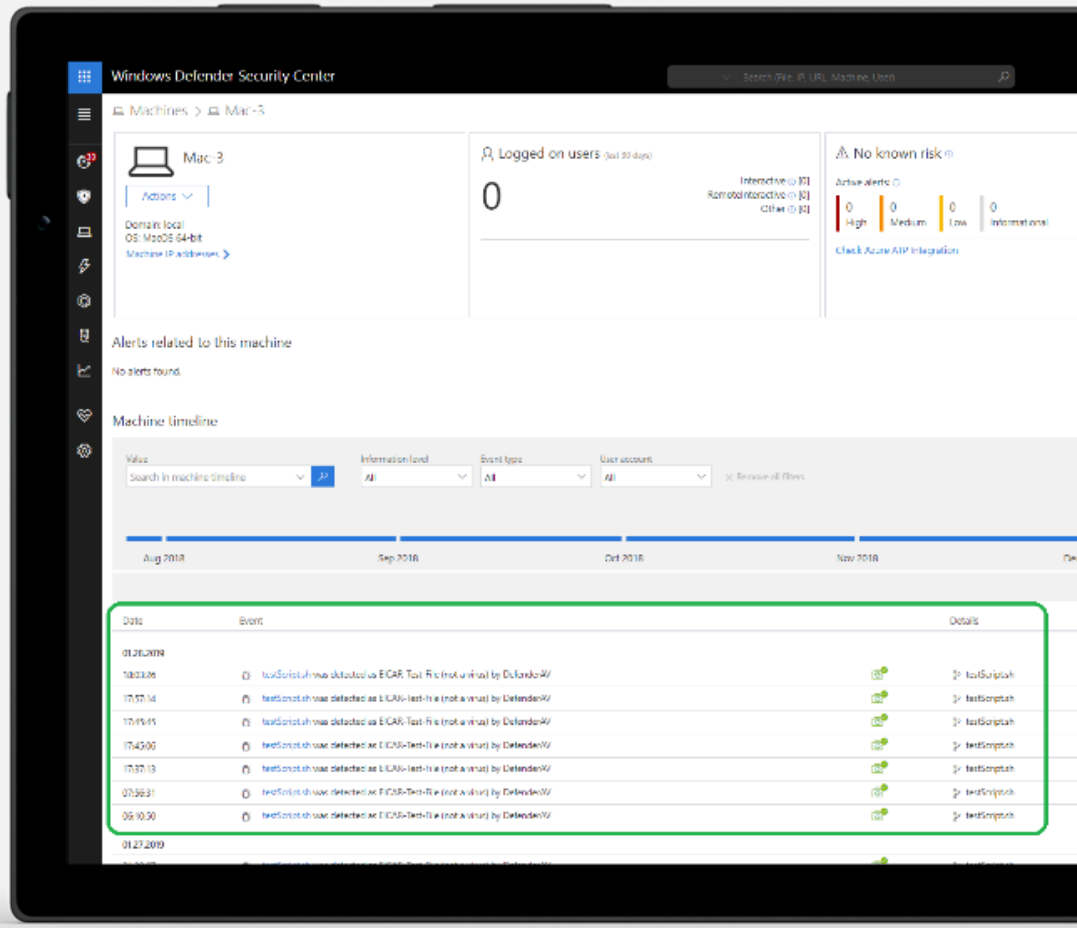
- 가벼운 배포 및 온보딩 프로세스
- 성능, 침입 없음
- 규정 준수, 개인 정보 보호 및 데이터 주권 요구 사항에 부합

공격 탐지 및 조사를 가능하게 하는 풍부한 사이버 데이터

- 파일, 프로세스, 네트워크 활동을 포함한 관련 활동 모니터링
- 엔티티 간의 모든 범위의 관계를 포함하는 상세 데이터 보고
- 장치에서 발생하는 모든 상황을 보여줌

엔드포인트 용 Microsoft Defender 기능과 원활하게 통합

- 킬 체인의 탐지 사전
- Mac OS를 포함한 모든 컴퓨터의 6 개월 원시 데이터
- 기록되는 모든 항목에 대한 평판 데이터
- 모든 엔드 포인트에 대한 단일 창 Mac OS
- Mac OS를 포함한 모든 원시 데이터에 대한 고급 헌팅
- 맞춤형 TI
- Mac OS를 포함한 전체 데이터 모델에 대한 API 액세스
- SIEM 통합
- 규정 준수 및 개인 정보 보호
- RBAC



엔드포인트 용 Microsoft Defender (Linux)

클라이언트:

- AV 예방
- 전체 명령줄 경험 (스캐닝, 구성, 에이전트 상태)

Microsoft Defender 보안 센터에 기본 경고 및 컴퓨터 정보 표시.

EDR 기능은 곧 점차적으로 밝아질 것입니다.

바이러스 백신 경고:

- ✓ 심각도
- ✓ 스캔 유형
- ✓ 장치 정보 (hostname, 기계 식별자, 테넌트 식별자, 앱 버전, 및 OS 유형)
- ✓ 파일 정보 (이름, 경로, 사이즈 및 해시)
- ✓ 위협 정보 (이름, 유형 및 상태)

장치 정보:

- ✓ 기계 식별자
- ✓ 테넌트 식별자
- ✓ 앱 버전
- ✓ Hostname
- ✓ OS 유형
- ✓ OS 버전
- ✓ 컴퓨터 모델
- ✓ 프로세서 아키텍처
- ✓ 장치의 가상머신 여부

현재 제공되는 엔드포인트 용 Microsoft Defender (Android)

웹 보호

- **Anti-phishing**
- 안전하지 않은 네트워크 연결 차단
- 사용자 지정 표시기: **URL** 허용/차단

멀웨어 스캔

- 멀웨어 경고, **PUA**
- 파일 스캔
- 스토리지 및 메모리 주변 장치 스캔

단일 창을 통한 보고서

- 피싱에 대한 경고
- 악성 앱에 대한 경고
- **Microsoft Defender** 보안 센터에서 보고서 자동 연결

조건부 액세스

- 위험한 장치 차단
- 준수하지 않은 장치 표시

지원되는 구성

- 장치 관리자
- **Android Enterprise** (작업 프로필)

Microsoft 라이선스

- 엔드포인트 용 **Microsoft Defender**를 제공하는 사용자 단위 라이센스에 포함
- 라이선스 사용자 당 **5**개의 적격 장치
- 여러분의 계정관리 팀 또는 **CSP**에 문의하세요

Microsoft Defender for Endpoint (iOS) current offering

웹 보호

- **Anti-phishing**
- 안전하지 않은 네트워크 연결 차단
- 사용자 지정 표시기: **URL** 허용/차단

단일 창을 통한 보고서

- 피싱에 대한 경고
- **Microsoft Defender** 보안 센터에서 보고서 자동 연결

지원되는 구성

- 감독
- 감독되지 않음

Microsoft 라이선스

- 엔드포인트 용 Microsoft Defender를 제공하는 사용자 단위 라이센스에 포함
- 라이선스 사용자 당 **5**개의 적격 장치
- 여러분의 계정관리 팀 또는 **CSP**에 문의하세요

시작하는 방법

Evaluation Lab & Tutorials

설정

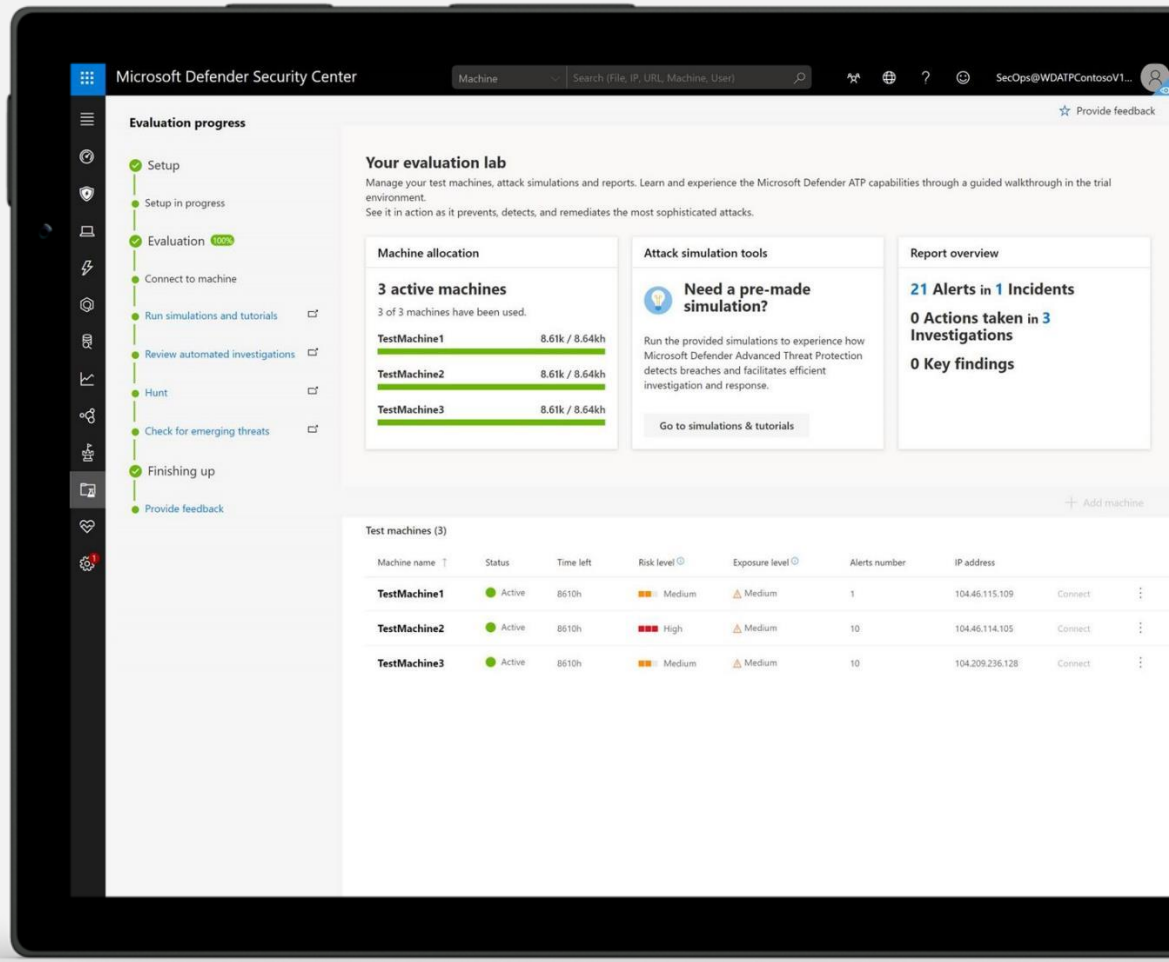
- 최신 OS 버전
- 사전 구성된 보안 기준
- 엔드포인트 용 Microsoft Defender에 온보딩
- 스택 전체에서 전체 감사 모드.
- 사전에 정의된 평가 도구
- 여러 개의 상호 연결된 장치(측면 이동)

시뮬레이션

- 엔드포인트 용 Microsoft Defender의 사전 제작된 시뮬레이션 "Do it yourself" 시나리오
- 마법사 기반 경험(고객에게 제품 기능 안내)
- 완전한 유연성 (실제 시스템 RDP 액세스 가능)
- 훈련과 교육은 성공적인 PoC에 있어 중요한 부분

보고서

- 둘러보기
- 실시간 생성되는 보고서
- 고객의 테넌트 데이터와는 별도로 결과를 자체 포함
- 요약 보고서
- 추가적인 엔드포인트 용 Microsoft Defender 관련 기능을 강조



엔드포인트 용 Microsoft Defender를 사용하려면? 퍼블릭 미리보기 기능 켜기

체험 신청하기: https://aka.ms/DefenderEndpoint
블로그 확인하기: https://aka.ms/MSDEBlog

Microsoft 365

감사합니다