



Microsoft Defender ATP ile Uçtan Uca Güvenlik

Microsoft Defender ATP ile Uçtan Uca Güvenlik

İçindekiler

Yazar Hakkında	3
Giriş	4
Threat & Vulnerability Management.....	6
Security Recommendations	8
Software Inventory	9
Weaknesses	10
Attack Surface Reduction	11
Next Generation Protection	15
Behavior-base, heuristic and real-time antivirus protection	15
Cloud-delivered protection.....	16
Dedicated protection and product updates	17
Endpoint Dedection & Response.....	18
Auto Investigation & Remediation	24
Advanced Hunting	26
Reports	30
Partners & API	31
MDATP Bitdefender GravityZone Entegrasyonu.....	31
MDATP Azure Sentinel Entegrasyonu	35
Settings.....	37
Windows Server 2008 R2 SP1, 2012 R2, 2016 Onboarding	37
Windows 10 Onboarding	41
System Center Configuration Manager SCEP Yapılandırması	46
AntiMalware Policy.....	49
Windows Defender Exploit Guard	66
Windows Defender ATP Policies.....	77
Windows Server 2016 Defender ATP Kurulumu.....	77
Group Policy ile Windows Defender Exploit Guard Yapılandırma	79
Attack Surface Reduction	79
Controlled Folder Access	81
Network Protection	84
Youtube Videoları.....	84
Faydalanan Kaynaklar	85
SON SÖZ	86

Yazar Hakkında



Profesyonel iş hayatımı 2008 yılında başladım. 12 Yıllık dönemde teknikerlikten başlayarak bir çok farklı pozisyonda çalıştım. Dünyanın en büyük sigorta şirketleri arasında yer alan Allianz Türkiye' de Kıdemli Sistem Uzmanı olarak çalışmaktan sonra beni heyecanlandıran bir teklif üzerine Dubai' ye taşındım ve iş hayatımı Emirates NBD bankasında Kıdemli Sistem Mühendisi olarak devam etmekteyim. Profesyonel iş yaşamım dışında yönetim kadrosunda yer aldığım www.mshowto.org sitesinde gönüllü yazarlık yapmaktadır. 20+ konferansta konuşmacı olarak yer aldım. 150+ makale ve bu yazı serisi ile birlikte yedinci E-Kitabımı yazmanın mutluluğunu yaşamaktayım.

- ✓ CEH | Certified Ethical Hacker
- ✓ MCT | Microsoft Certified Trainer
- ✓ MVP | Cloud and Datacenter 2019-200
- ✓ MVP | Enterprise Mobility 2016-2017,2018-2019
- ✓ MCSE | Server Infrastructure
- ✓ MCSA | Server 2012
- ✓ MCPS | Microsoft Certified Professional
- ✓ Microsoft Specialist: Server Virtualization with Windows Server Hyper-V and System Center Specialist
- ✓ Tenable Certificate of Proficiency
- ✓ ICSI | CNSS Certified Network Security Specialist

Giriş

Merhabalar,

Yazım içerisinde Microsoft Defender ATP' yi MDATP olarak kısaltarak kullanacağım. Gartner raporuna baktığımız zaman MDATP' nin 2019 yılı endpoint protection sıralamasında lider olduğunu göreceksiniz. Merak edenler aşağıdaki linkten detaylıca inceleyebilirler.

<https://www.microsoft.com/security/blog/2019/08/23/gartner-names-microsoft-a-leader-in-2019-endpoint-protection-platforms-magic-quadrant/>

Kişisel olarak neden MDATP' yi kullanırmı sorusunu kendime soracak olursam cevabım Microsoft kendi kernelini diğer 3rd parti vendor lardan daha iyi tanıyor diyerek cevaplayabilirim.

Bu yazı serisinde de MDATP' yi bilgim doğrultusunda derinlemesine incelemeye çalışacağım. Bildiğiniz üzere Defender Windows Server 2016 ve Windows 10 işletim sisteminde varsayılan olarak bulunmaktadır. Yazı içerisinde bu bölüm daha yüzeysel işlenecektir. Yazı serimizin asıl amacı varsayılan olarak ATP ajanının gelmediği yapıları nasıl koruyabileceğimize değinmektir. Elbette <https://securitycenter.windows.com> paneli içerisindeki önemli noktalara yazım içerisinde yer vereceğim.

Endpoint Protection ürünlerini her zaman yüklerin efendisindeki bu savaş sahnesine benzetirim. Artık düşman son kalemezi gelmiştir ve burayı da geçmesi gerekmektedir. Bu sebenteş dolayı son kalemizi en iyi şekilde korumamız gerekmektedir. Umuyorum bu döküman biraz da olsa buna katkı sağlayacaktır.



Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Antivirus (MDAV) (AV, EPP)

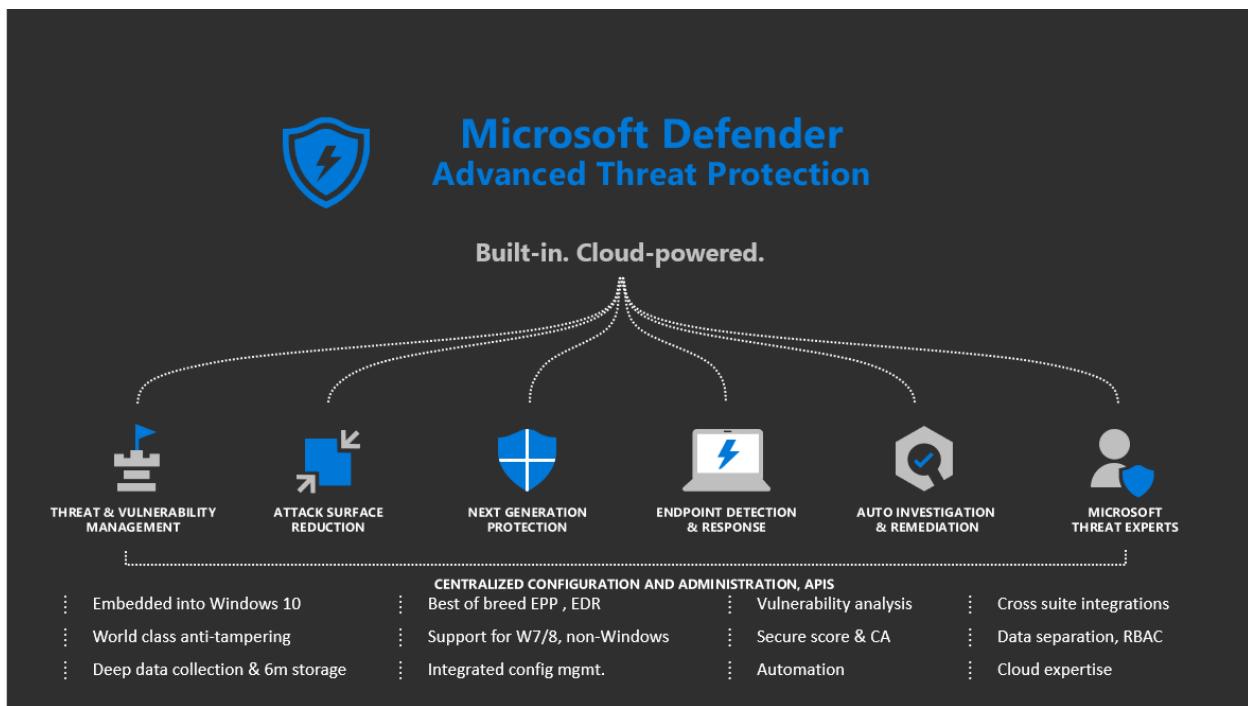
- Windows Server 2019
- Windows Server 2016
- Windows 10

System Center Endpoint Protection (SCEP) (AV, EPP)

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2

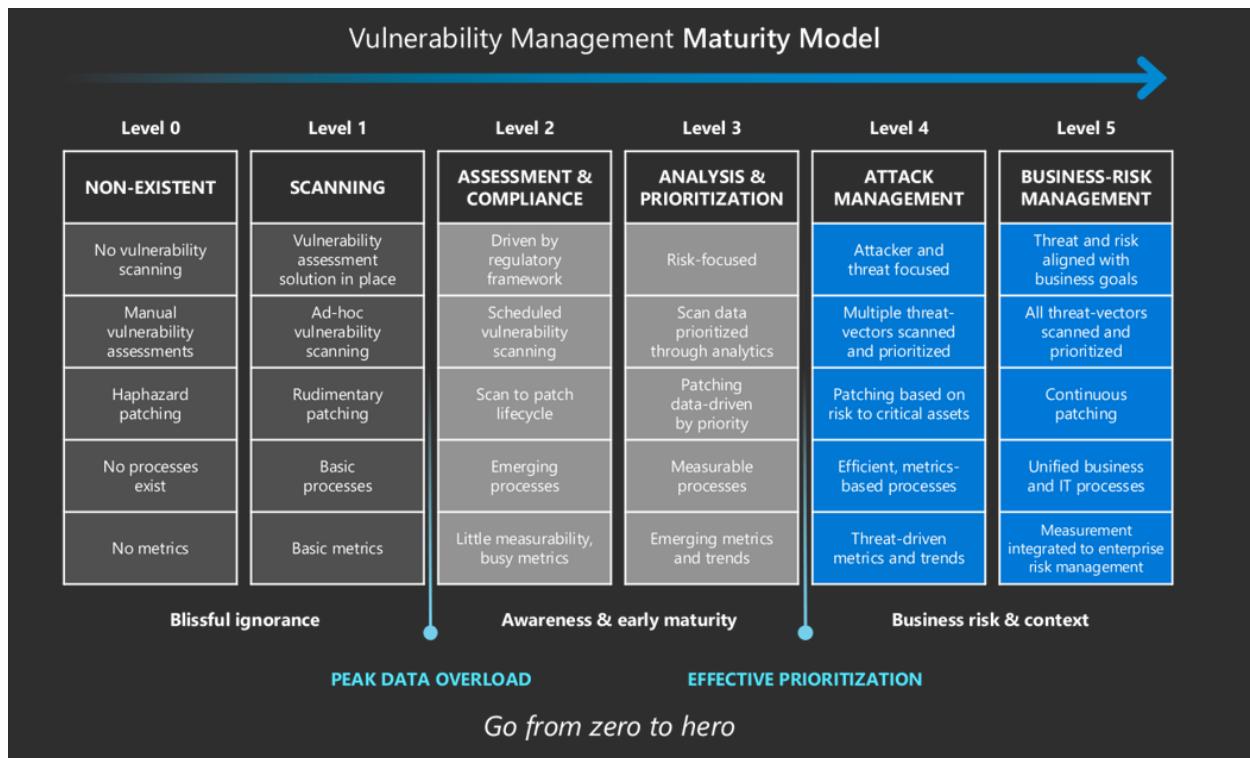
<https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/supported-configurations>

Genel hatları ile ürün altı alt başlıklardan oluşmaktadır ve yazım içerisinde herbirine ayrı başlıklar altında yer vereceğim.

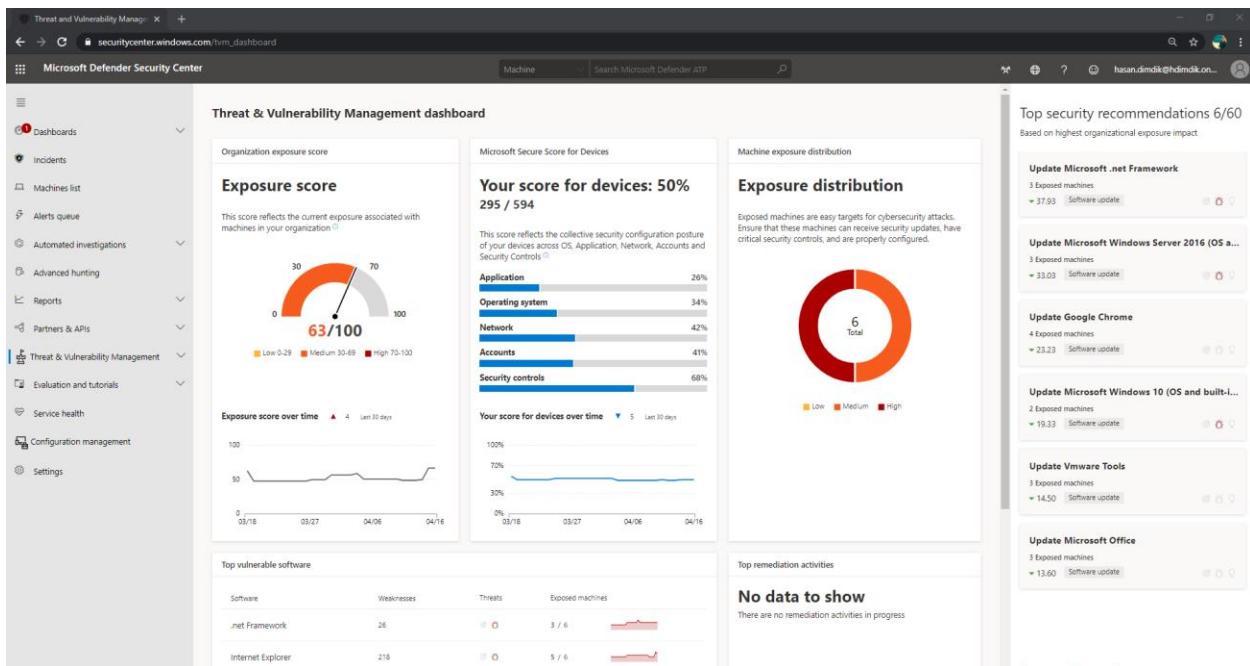


Threat & Vulnerability Management

Şirketler yapılarını her zaman daha iyileştirmeye çalışmaktadır. Endpoint Protection sadece yapımı koruyan araçlardan bir tanesi. İlk olarak olgunluk seviyemizi belirlememiz ve şirket yapısına göre denge gözeterek iyileştirmelerimizi yapmamız gerekmektedir. Aşağıda örnek tabloda olgunluk seviyesi modelini görebilirsiniz.



Threat & Vulnerability Management içerisinde yapımızdaki zaafiyetleri tek bir panel içerisinde görebiliyoruz. Bu bize iyileştirmeye nereden başlamamız gerekiğine dair bilgi de vermektedir. Diğer bir ifadeyle zayıf halkanın neresi olduğunu hızlıca belirleyebiliyoruz.



Security Recommendations

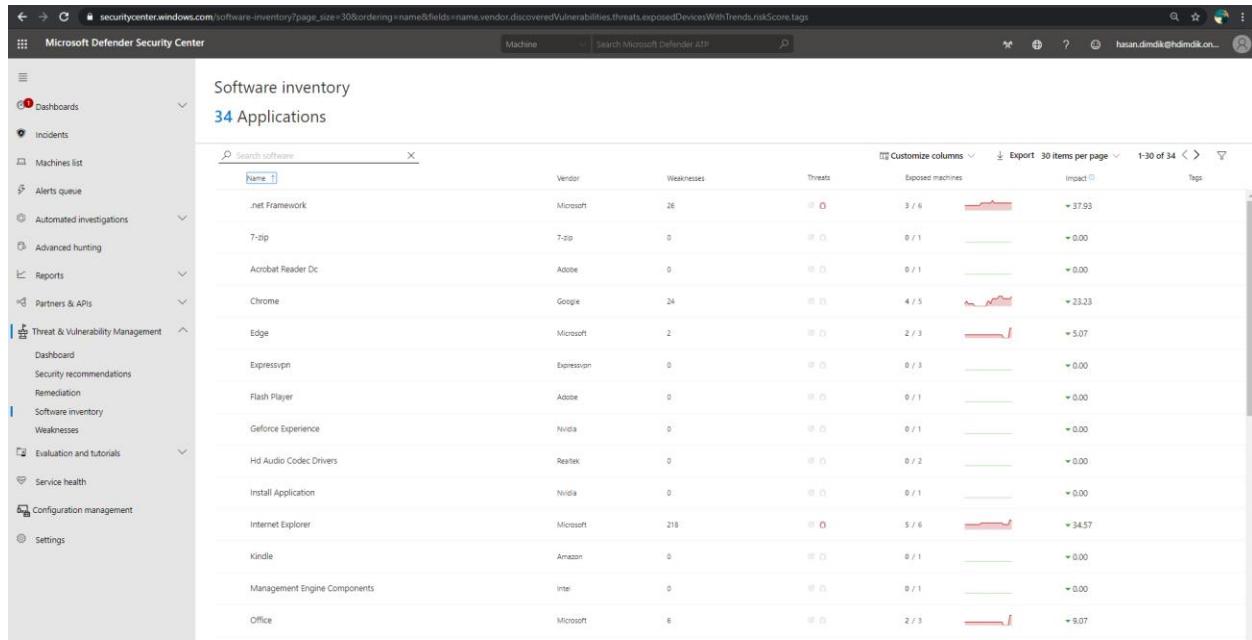
Güvenlik tavsiyeleri içerisinde EDR teknolojisi ile taranıp bulunan zaafiyetleri tek çatı altında görüyoruz. Buradaki açıklıkları incelediğimizde sadece endpoint e yönelik zaafiyetler değil GPO ile yapabileceğimiz sıkıştırmalar veya üçüncü parti yazılımlara ait tavsiyeleri de görüyoruz. Örneğin aşağıdaki ekran görüntüsünde Vmware tool ve Google Chrome' un güncellenmesi gerekiğine dair tavsiyelerde yer almaktadır.

Güvenlik tavsiyelerini endpoint özelinde de raporlayabiliyoruz.

Software Inventory

Şirketlerdeki en büyük sorunlardan bir tanesi kurum içerisinde yüklü olan uygulamaların bilinmiyor olması, diğer bir deyişle uygulama envanterine hakim olunamaması. Software inventory adından da anlaşıldığı gibi bu sorunumuzu çözmektedir. Elbette burdaki öncelikli amaç hangi uygulama

ne kadar yapımızda açılığa sebep oluyor bulmaktadır.(Expose cümlesini türkçeye çevirdiğimizde açığa çıkarmak, maruz bırakmak veya teşhir etmek anımlarına gelmektedir.)



The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a navigation sidebar with various options like Dashboards, Incidents, Machines list, Alerts queue, Automated investigations, Advanced hunting, Reports, Partners & APIs, Threat & Vulnerability Management (which is currently selected), Configuration management, and Settings. The main area is titled "Software inventory" and shows "34 Applications". A search bar at the top of this section has "Name: 1" typed into it. Below the search bar is a table with columns: Name, Vendor, Weaknesses, Threats, Exposed machines, Impact, and Tags. The table lists 14 different software items, each with its vendor, number of weaknesses, threats, exposed machines count, impact score, and a small chart icon. The impact scores range from 0.00 to 37.93.

Name	Vendor	Weaknesses	Threats	Exposed machines	Impact	Tags
.net Framework	Microsoft	26	0	3 / 6	37.93	
7-zip	7-zip	0	0	0 / 1	0.00	
Acrobat Reader Dc	Adobe	0	0	0 / 1	0.00	
Chrome	Google	24	0	4 / 5	23.23	
Edge	Microsoft	2	0	2 / 3	5.07	
Expressvpn	Expressvpn	0	0	0 / 3	0.00	
Flash Player	Adobe	0	0	0 / 1	0.00	
Geforce Experience	Nvidia	0	0	0 / 1	0.00	
Hd Audio Codec Drivers	Realtek	0	0	0 / 2	0.00	
Install Application	Nvidia	0	0	0 / 1	0.00	
Internet Explorer	Microsoft	218	0	5 / 6	34.57	
Kindle	Amazon	0	0	0 / 1	0.00	
Management Engine Components	Intel	0	0	0 / 1	0.00	
Office	Microsoft	6	0	2 / 3	9.07	

Weaknesses

Bildiğiniz üzere bir açılık CVE olarak değerlendirildiğinde alenen artık zaafiyetin ne olduğu herkes tarafından bilinmeli demektir. Bu durumda bırakın Black hat Hacker'ları Script Kiddie lerin bile hedefi olabileceğiniz anlamına gelmektedir. Bu bölümde detaylıca ilgili zaafiyetleri raporlayıp iyileştirmelere başlayabilirsiniz.

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a navigation sidebar with various sections like Dashboards, Incidents, Machines list, Alerts queue, Automated investigations, Advanced hunting, Reports, Partners & APIs, Threat & Vulnerability Management (which is expanded), Configuration management, and Settings. The main area is titled "Weaknesses" and shows "129k Vulnerabilities". A search bar at the top says "Search vulnerabilities". Below it is a table with columns: Name, Severity, CVSS, Related Software, Age, and Published on. The first row in the table is highlighted with a blue background and shows "CVE-2020-1014" with "High" severity and "7.8" CVSS. The right side of the screen displays detailed information for this specific vulnerability, including its ID (CVE-2020-1014), a "Report inaccuracy" button, a "Legal Notice" link, a "Vulnerability description" section (which includes a long technical paragraph about privilege elevation), "Vulnerability details" (listing CVE-ID, CVSS, and other metadata), "Threat Insights" (listing Public, Verified status, and Exploit kits), and a "Related Software" section.

Attack Surface Reduction

Atak yüzeyi kelimesini irdelediğimiz zaman saldırganın yapımı içerisinde sızabileceğimiz noktalar olarak değerlendirebiliriz. Savunan taraf olarak bizim görevimiz bu noktaları belirlemek ve daraltmaktır. Günümüzde artık bilgisayar kullanım alanları tamamen değişti. Bundan beş yıl öncesine baktığımızda her şey güvenlik duvarı arkasında korunmaktadır. Şimdi ise bu tarz bir kısıtlama bulunmamaktadır. Bring your own device kavramı ile sınırlar kalkmaya başladı, bir sonraki aşamada ise artık heryerden çalışabilir hale geldik. Bu sebepten klasik koruma önlemleri artık yetersizdir. Oyuna artık web tehditleri, yemleme saldırıcıları, akıllı cihazlar, ransomware, apt saldırıcıları, nesnelerin interneti gibi n tane kavram dahil oldu, yine bahsettiğim gibi şirket sınırları değişti ve cihazlar heryerden bağlanabilir hale geldi. Attack Surface Reduction ise tam bu noktadaki sıkıntımızı gidermek için tasarlanmıştır. Microsoft hali hazırda tüm tehditleri aktif olarak tarayıp kendi veri tabanını güncellemektedir, elbette davranışsal analizde bir oranda tehditleri engellemektedir. Eğer şirket yapısına özel block rule yazmak isterseniz security center a bağlandıktan sonra **Indicators** sekmesi içerisinde tanımlayabilirsiniz.

URL/Domain	Action	Alert severity	Scope	Expires on (UTC)	Title	Created by
http://www.hasandimdik.com/	Alert and block	Medium	All machines	HD Block	hasan.dimdik@hdimdik	
https://www.mshowto.org/	Alert only	High	All machines	May 3, 2020	Biggest Community	hasan.dimdik@hdimdik

Beş farklı metodla Attack Surface Reduction'ı yapılandırabiliriz. İlerleyen bölümlerde System Center Configuration Manager ve GPO ile nasıl atak yüzeyini daraltabiliriz degeneceğiz.

- Microsoft Intune
- Mobile Device Management (MDM)
- Microsoft Endpoint Configuration Manager
- Group Policy
- PowerShell

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-attack-surface-reduction>

Attack Surface Reduction

Resist attacks and exploitations



HW BASED ISOLATION

APPLICATION CONTROL

EXPLOIT PROTECTION

NETWORK PROTECTION

CONTROLLED FOLDER ACCESS

DEVICE CONTROL

WEB PROTECTION

RANSOMWARE PROTECTION

Isolate access to untrusted sites

Isolate access to untrusted Office files

Host intrusion prevention

Exploit mitigation

Ransomware protection for your files

Block traffic to low reputation destinations

Protect your legacy applications

Only allow trusted applications to run

Yunan mitolojisinde bildiğiniz üzere Aşil çok özel bir yere sahiptir ve nerdeyse ölümsüzdür, fakat küçük bir zaafiyeti içermektedir ki bu zaafiyet onun için ölümcüldür. Elbette aşil tendonundan bahsediyorum. Eğer saldırgan bu zafiyeti bilinçli veya şans eseri bulacak olursa etkisi yıkıcı olacaktır. Bu sebepten dolayı yapının sürekli taranıp zaafiyetlerin belirlenmesi güvenlik için önem arz etmektedir. Teknik detaylara ilerleyen bölümlerde değineceğiz.



Bu bölümle ilgili son düşünmek istediğim nokta ise bulutun gücü ile birlikte MDATP bizi aşağıdaki atak türlerinden korumaktadır.

Attack Surface Reduction (ASR) Rules



Minimize the attack surface

Signature-less, control entry vectors, based on cloud intelligence. Attack surface reduction (ASR) controls, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats

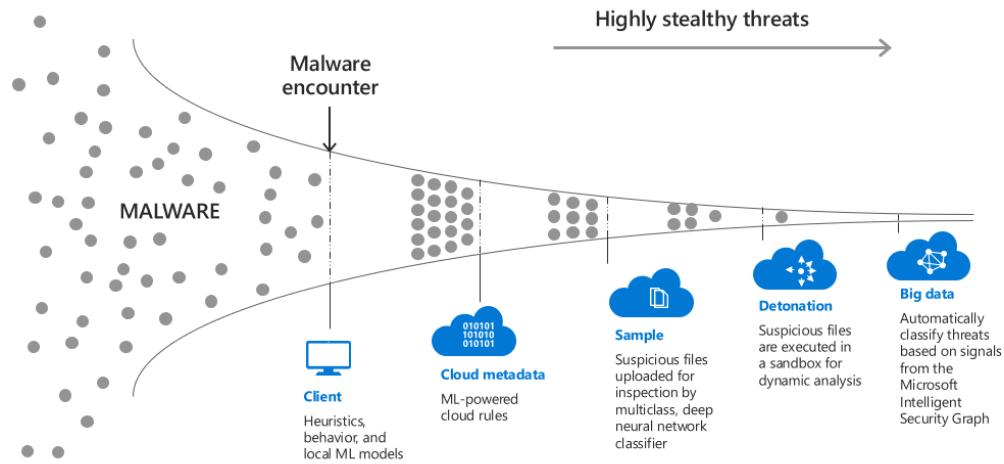
- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

Lateral movement & credential theft

- Block process creations originating from PSEExec and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

Next Generation Protection

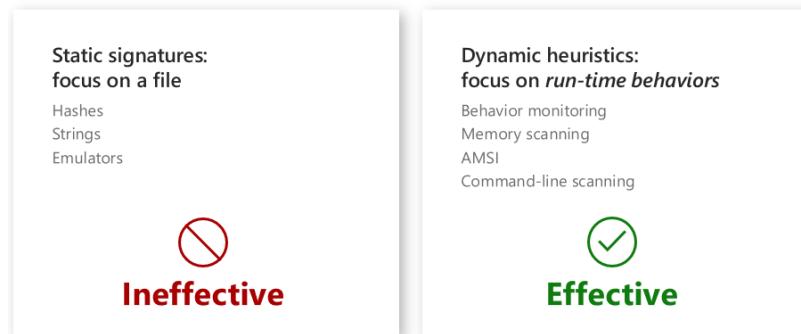
Bildiğiniz üzere imza tabanlı anti virüsler artık bizleri koruyamamaktadır. Kısımında olsa koruyabilmektedir diyebilirim ! (Yorumu size bırakıyorum 😊) Günümüz atakları ise artık daha sofistike , imza tabansız,fileless ve/veya Hardware lerin açıklarından faydalalararak gerçekleştirilen ataklar olarak karşımıza çıkmaktadır. Diğer bir sorun da saldırganların Endpoint Protectionları kolay bir şekilde devre dışı bırakmasıdır. Bu noktada ilgili ürünün bizi kernel seviyesine kadar koruması büyük önem arz etmektedir.



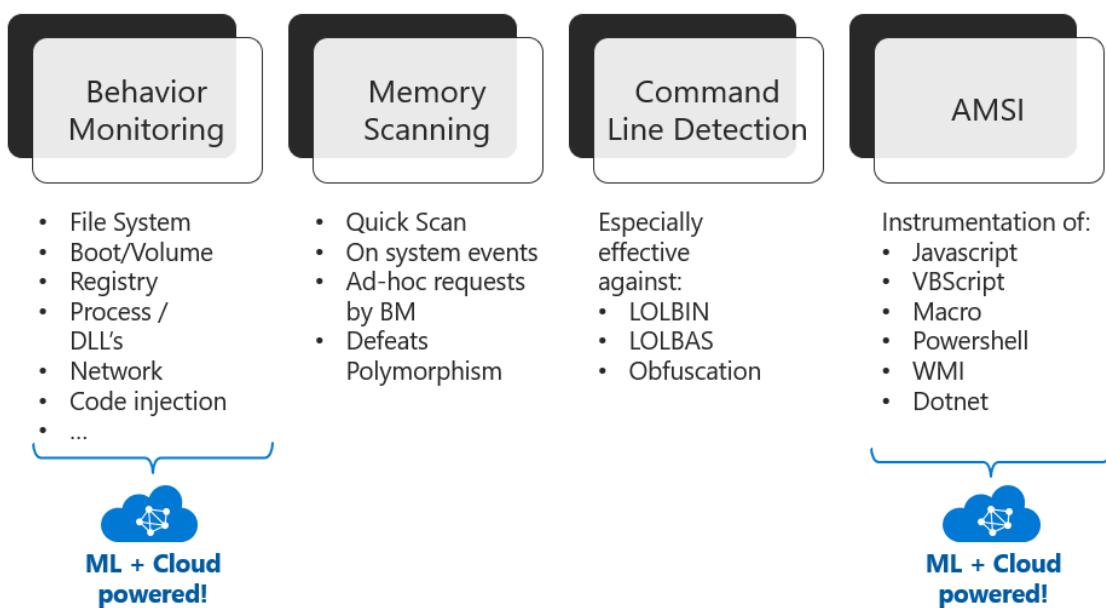
Teknik olarak Next Generation Protection nedir dersek bunu üç başlık altında toplayabiliriz.

Behavior-base, heuristic and real-time antivirus protection

İmza tabanlı anti virüs programı kullanıyorsanız artık çok da fazla günümüz tehditlerini koruyamamaktadır(Umuyorum gerçekten yapınız bu şekilde korunmuyordur).Bu noktada oyuna **Behavior-base, heuristic and real-time antivirus protection** girmektedir. Bu özellik sayesinde artık sadece imza tabanı incelenmemektedir aynı zamanda davranış da işin içine girmektedir.



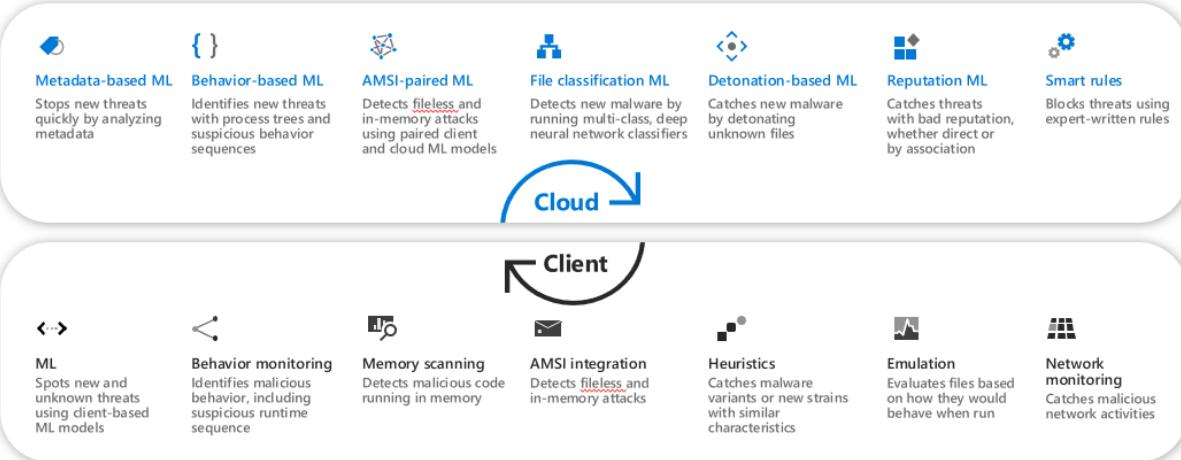
Davranışsal analiz elbette arka planda makina öğrenmesini kullanmaktadır ve aşağıdaki dört başlık altında etkin koruma sağlamaktadır.



Cloud-delivered protection

Bir önceki bölümde kısaca davranışsal analizin artık oyuna girdiğini belirtmiştık. Davranışsal analiz yeni bir tehditi ne kadar hızlı bir şekilde yakalayabilemektedir? Örneğin sıfırıncı gün atağından bahsedecek olursak klasik yöntemlerle bunu koruyamayacağımıza hemfikiriz. ATP ise aşağıda yer alan koruma motorları sayesinde etkin koruma sağlamaktadır.

Microsoft Defender ATP next generation protection engines



Aşağıdaki linkte nasıl koruduğunu anlatan videoyu izleyebilirsiniz.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/utilize-microsoft-cloud-protection-windows-defender-antivirus>

Dedicated protection and product updates

Tam bir koruma sağlamak istiyorsanız elbette sıkı şekilde gerekli update'leri yapıyor olmamız gerekmektedir. Bu noktada iki farklı update den söz ediyoruz. İlki **Protection updates**. MAPS periyodik olarak güvenlik update'lerini kontrol edip yeni gelen update varsa indirilmektedir. Aynı zamanda **Product Update** ile endpoint ajanlarının güncellenmesi sağlanmaktadır.

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/manage-updates-baselines-windows-defender-antivirus>

Endpoint Dedection & Response



- CORRELATED POST-BREACH DETECTION
- INVESTIGATION EXPERIENCE
- INCIDENT
- ADVANCED HUNTING
- RESPONSE ACTIONS (+EDR BLOCKS)
- DEEP FILE ANALYSIS
- LIVE RESPONSE
- THREAT ANALYTICS

MDATP nerdeyse gerçek zamanlı olarak tehditleri yakalar ve ilgili zararlıyı etkisiz hale getiririr. Elbette burada diğer önemli nokta ise ilgili atağın detaylarını görebilmektir. Bu analiz bize ilgili atağın/zararının genel bir saldırı/zararlı olduğu veya şirkete özel sofistike bir atak olup olmadığını belirlememizde faydalı olacaktır. Bu bölümün örnekle açıklamam daha faydalı olacaktır. Portalıma erişip **Alert Queue** geldiğimde yapım içerisinde oluşan tüm alarmları görebiliyorum. Bu aslında Detect kısmına karşılık gelmektedir.

Title	Severity	Incident	Status	Category	Machine	User	Classification	Investigation state	Last activity	Assigned to
Automated investigation started manually	Informational	17	New	Suspicious activity	h071		Not set	Unsupported OS	4/17/20, 11:39 AM	Unassigned
2 alerts: Mimikatz high-severity malware was detected	High	2 incidents	New	Grouped by: Threat family	h071		Multiple	N/A	4/17/20, 11:39 AM	Unassigned
'Mimikatz' high-severity malware was detected	High	18	New	Malware	h071		Not set	Unsupported OS	4/17/20, 11:39 AM	Unassigned
'Mimikatz' high-severity malware was detected	High	19	New	Malware	h071		True alert	Unsupported OS	4/17/20, 11:09 AM	Unassigned
Automated investigation started manually	Informational	16	New	Suspicious activity	win7client		Not set	Unsupported OS	4/17/20, 11:39 AM	Unassigned
Automated investigation started manually	Informational	15	New	Suspicious activity	ghost-surface		Not set	No threats found	4/17/20, 3:12 PM	Unassigned
Automated investigation started manually	Informational	13	New	Suspicious activity	h071		Not set	Unsupported OS	4/17/20, 11:24 AM	Unassigned
Automated investigation started manually	Informational	19	New	Suspicious activity	h071		Not set	Unsupported OS	4/17/20, 11:09 AM	Unassigned
'Minikatz' backdoor was detected	Low	12	New	Malware	h071		Not set	Unsupported OS	4/17/20, 11:05 AM	Unassigned
'Pyramex' malware was detected	Informational	12	New	Malware	h071		Not set	Unsupported OS	4/17/20, 11:06 AM	Unassigned
Automated investigation started manually	Informational	11	New	Suspicious activity	desktop-uluudu		Not set	No threats found	4/17/20, 10:39 AM	Unassigned
Automated investigation started manually	Informational	10	New	Suspicious activity	desktop-0vifou		Not set	No threats found	4/17/20, 8:53 AM	Unassigned
Automated investigation started manually	Informational	9	New	Suspicious activity	ghost-surface		Not set	No threats found	4/17/20, 8:23 PM	Unassigned
Suspicious behavior by a svchost.exe was observed	Medium	14	New	Execution	h071	A. Infected	Not set	Unsupported OS	4/17/20, 8:02 AM	Unassigned
Suspicious behavior by a svchost.exe was observed	Medium	14	New	Execution	h071	A. Infected	Not set	Unsupported OS	4/17/20, 8:02 AM	Unassigned

Örneğin ilgili sunucumda mimikatz çalıştırılmak istenmiş ve MDATP tarafından yakalanıp malware olarak kategorilendirilmiş. Detaylı olarak da process ağacını görebiliyoruz.

Microsoft Defender Security Center

Incidents > 12 > 'Mikatz' high-severity malware was detected

Incident details:

- Title:** 'Mikatz' high-severity malware was detected
- Severity:** High
- Category:** Malware
- Detection source:** Antivirus
- Detection technology:** Client
- Detection status:** Prevented
- Alert context:** h01
- Status:** New, True alert
- Assigned to:** Not assigned

Description: High-severity malware refers tools used by advanced Threat Activity Groups to target victims. Such Activity Groups may target individuals or institutions. They typically engage in industrial, military, diplomatic, and political espionage rather than more mundane activities such as identity theft or denial of service attacks. Some groups engage in acts of deliberate sabotage and destruction in order to cause real-world effects, such as disruptions to the victim's operations.

Recommended actions:

1. Isolate the alert.
2. Check for other suspicious activities in the machine timeline.
3. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.
4. Submit relevant files for deep analysis and review file behaviors.
5. Identify unusual system activity with system owners.
6. Scope the incident. Find related machines, network addresses, and files in the incident graph.
7. Contact and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset passwords, block IP addresses and URLs, and install security updates.
8. Contact your incident response team, or contact Microsoft support for investigation and remediation services.

Disclaimer: These guidelines are for reference only. They do not guarantee successful threat removal.

Show less

Alert process tree:

```

graph TD
    h01 --> mimiload.dll[mimiload.dll]
    h01 --> mimidrv.sys[mimidrv.sys]
    h01 --> mimilib.dll[milib.dll]
    h01 --> mimilb.dll[milmib.dll]
    h01 --> mimiv.sys[mimiv.sys]
    h01 --> mimikatz_trunk.zip[mimikatz_trunk.zip]
  
```

Incidents > 12 > 'Mikatz' high-severity malware was detected

Incident graph:

Artifact timeline:

Description	First Observed	Details
04.04.2020		
11:09:21 mimikatz_trunk.zip	04.04.2020 11:08:39	0576ea5b1ecbf487933b92340e83dc85f13eb1c
11:06:47 mimidrv.sys	04.04.2020 11:06:39	505146e82aa50888a9233004549afade54ed6
11:06:47 mimilib.dll	04.04.2020 11:06:39	da315ad2b7458212a97e58d0cc485d8450a599
11:06:47 mimilb.dll	04.04.2020 11:06:39	8791c1c80808d8288496a99baaddcd698fb4e7f
11:06:47 mimiv.sys	04.04.2020 11:06:39	a5f1b56915bdcaab032196134a3671233f0001c

Actions'ı tıkladıktan sonra Open Incident Page kısımına geliyorum ve üç farklı alarm aldığımı görüyorum.

Incidents > 12

Alerts (3) Machines (1) Investigations (0) Evidence (0) Graph

Incident list:

First activity	Title	Severity	Status	Linked by	Category	Machine	User	Classification	Last activity	Assigned to
4/4/20, 11:06 AM	'Mikatz' high-severity malware was detected	High	New	Same machine	Malware	h01		True alert	4/4/20, 11:09 AM	Unsigned
4/4/20, 11:06 AM	'Mimikatz' hash tool was detected	Low	New	Same machine	Malware	h01		Non set	4/4/20, 11:09 AM	Unsigned
4/4/20, 11:06 AM	Pymame malware was detected	Informational	New	Same machine	Malware	h01		Not set	4/4/20, 11:09 AM	hasan.dimik...

Evidence kısmında ise kanıt olarak nelerin şüpheli olarak algılandığını belirtmektedir.

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a navigation sidebar with various sections like Dashboards, Incidents, Machines list, Alerts queue, Automated investigations, Reports, Partners & APIs, Threat & Vulnerability Management, Evaluation and tutorials, Service health, Configuration management, and Settings. The main area is titled 'Incidents > 12' and has tabs for 'Alerts (3)', 'Machines (1)', 'Investigations (0)', 'Evidence (8)', and 'Graph (8)'. The 'Evidence (8)' tab is selected. Below it, there's a 'Files (8)' section with a table showing file details. The table includes columns for 'File Path', 'File Name', and 'Endpoint'. All files listed are 'Suspicious' and have paths starting with 'C:\Windows\Temp\mimikatz_trunk\'. The right side of the screen shows a 'Customize columns' dropdown and a '30 items per page' option.

Graph ise, zararlı nereye bulaştı, bulaştığı yerden başka yere geçti mi ? gibi verileri görsel olarak görmemize imkan sağlamaktadır veya diğer bir ifadeyle zararının davranış analizini görmemize imkan sağlamaktadır. Mimikatz_trunk.zip i tıkladığında iki farklı servis tarafından zararlı olarak algılandığını görüyoruz. Son olarak indicator seçeneği ile block kuralı oluşturabiliriz.

This screenshot shows a detailed view of the 'mimikatz_trunk.zip' file within the Microsoft Defender Security Center. The left sidebar is identical to the previous screenshot. The main area now focuses on the 'Graph' tab, which displays a network diagram. Nodes represent different endpoints or services, and edges represent connections between them. One node is highlighted with a red circle, indicating its importance. To the right of the graph, there's a large panel for the 'mimikatz_trunk.zip' file. It includes sections for 'File details', 'File Detections', 'Malware detected', and 'Observed worldwide' and 'Observed in organization (last 30 days)'. The 'File details' section shows SHA1, SHA256, MD5, Size (931.12 KB), and Signer (Unsigned file). The 'File Detections' section shows alert counts: High (2), Medium (0), Low (0), and Informational (0). The 'Malware detected' section lists 'HackTool/Win64/MikatzTrn' with sources 'Windows Defender AV' and 'Cloud service'. The 'Observed worldwide' section shows a count of 1.8k, first seen 5 months ago, and last seen 21 minutes ago. The 'Observed in organization (last 30 days)' section shows a count of 1, first seen 13 days ago, and last seen 21 minutes ago.

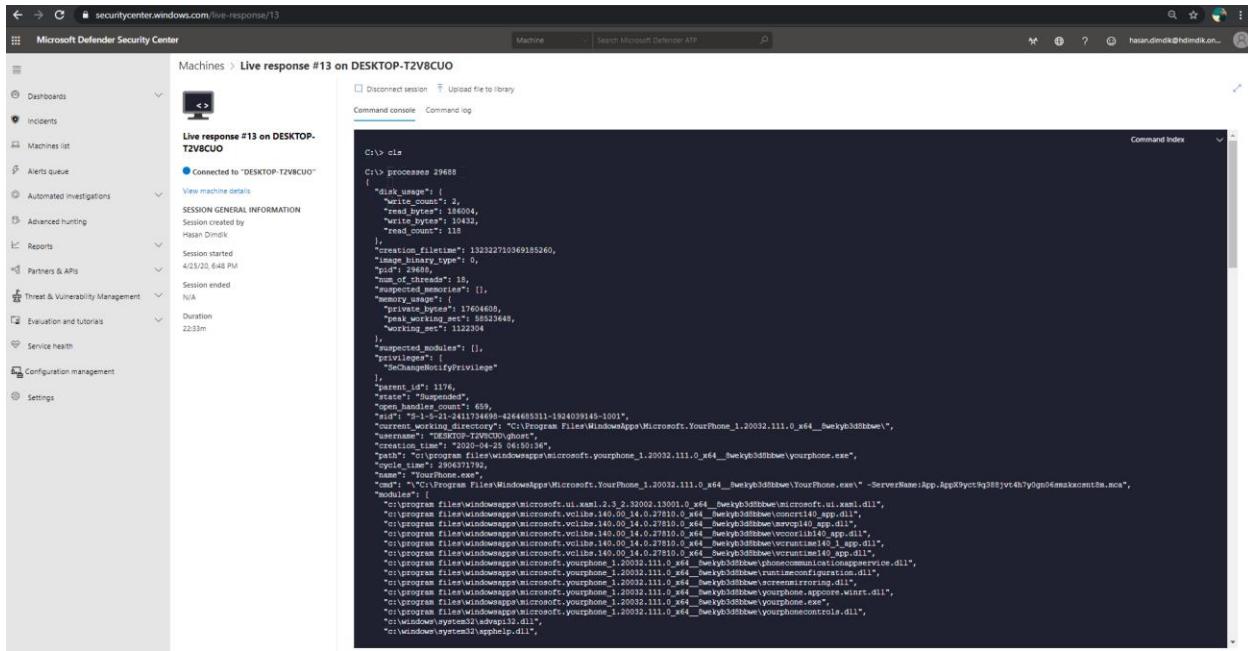
Endpointlerimiz üzerinde Live Session başlatabiliyoruz. Bu sayede canlı olarak şüphe oluşturan bir durum var ise incelenebilmektedir.

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a navigation sidebar with various sections like Dashboards, Incidents, and Machines list. The main area displays a 'Machines list' table with columns for Machine name, Domain, Risk level, Exposure level, OS platform, and Windows 10 version. A specific machine, 'desktop-t2v8cuo', is selected and shown in a detailed view on the right. This view includes device details such as Domain (Workgroup), OS (Windows 10 v64), Asset group (Windows10), Health state (Active), and Data sensitivity (None). It also shows Active alerts and 6 active alerts in 6 incidents. A prominent red box highlights the 'Initiate Live Response Session' button under the 'Device details' section.

Örnek olması açısından canlı oturum başlatıyorum. **Process** komutu ile istemci makinamda çalışan süreçleri görüyorum.

This screenshot shows a 'Live response #13 on DESKTOP-T2V8CUO' session. The left sidebar shows the machine is connected to 'DESKTOP-T2V8CUO'. The main area has a 'Command console' tab open, showing a list of running processes. The table includes columns for Name, PID, Parent Id, Status, User Name, Cpu Cycles (K), and Memory (K). The command prompt at the top shows 'C:\> cls'. The table lists thousands of processes, with many entries for 'svchost.exe' and other system services. A red box highlights the 'Command Index' link at the top right of the table.

Örneğin Yourphone isimli bir işlem gördüm ve bunun normal olmadığını varsayıyorum. **Processes 29688** komutu ile işleme ait detay bilgiye ulaşabiliyoruz.



Fileinfo komutu ile dosyamız hakkındaki bilgilere ulaşabiliyoruz ve daha fazlasını komut satırı ile yapabiliyoruz tabiki bunların en önemlisi analiz yapabiliyor olmamızdır. Bunun yanında kendi yazdığınız Powershell scriptleri çalıştırıp iyileştirmelerimizi yapabiliyoruz. Bu özellik özellikle SOC ekipleri için faydalı olacaktır.

Machines > Live response #13 on DESKTOP-T2V8CUO

```

Live response #13 on DESKTOP-T2V8CUO

Connected to "DESKTOP-T2V8CUO"

View machine details
SESSION GENERAL INFORMATION
Session created by
Hasan Dimlik
Session started
4/25/20, 6:48 PM
Session ended
N/A
Duration
28:34m

C:\> cls
C:\> fileinfo "c:\program files\windowsapps\microsoft.yourphone_1.20032.111.0_x64_8wekyb3d8bbwe\yourphone.exe"
{
    "c:\program files\windowsapps\microsoft.yourphone_1.20032.111.0_x64_8wekyb3d8bbwe\yourphone.exe": {
        "last_raw_access_error": 0,
        "packed": null,
        "size": 19049472,
        "read_only": false,
        "marked_as_trusted": 34404,
        "ms_verified": false,
        "hidden": false,
        "sha256": "1b0238c12f2d0185b7be49ddc61caa509cfds5c8a22618ff12327ecae38aad590",
        "type": "application/x-msdownload",
        "vendor": null,
        "digital_signature": null,
        "last_access_error": 0,
        "directory_type": [
            "Applications"
        ],
        "downloaded": false,
        "compressed": false,
        "path": "c:\program files\windowsapps\microsoft.yourphone_1.20032.111.0_x64_8wekyb3d8bbwe\yourphone.exe",
        "hash": "e0e57141f04e1c16aa3fb0172bb01a0f5e1b988",
        "created": "2020-04-17 7:20:11",
        "file_state_display": [
            "Default"
        ],
        "modified": "2020-04-17 17:20:38",
        "file_state": 0,
        "error": 0
    }
}
C:\>

```

Elbette üzerinde çalıştığımız, son kullanıcı bilgisayarı olduğu için herşeyin loglanması verilerin manupule edilebilmesinin de önüne geçmektedir.

Machines > Live response #13 on DESKTOP-T2V8CUO

CMd start time	# Command	Parameters	Entities	Duration	Status
4/25/20, 6:48 PM	3 - connect		0	2s	✓ Completed
4/25/20, 6:49 PM	4 - processes		260	10s	✓ Completed
4/25/20, 7:00 PM	5 - processes		254	10s	✓ Completed
4/25/20, 7:04 PM	6 - analyse	process 17192	0	0	✗ Failed
4/25/20, 7:04 PM	7 - processes		257	10s	✓ Completed
4/25/20, 7:06 PM	8 - analyse	process 29688	0	0	✗ Failed
4/25/20, 7:06 PM	9 - analyse	processes 29688	0	0	✗ Failed
4/25/20, 7:06 PM	10 - run	processes 29688	0	0	✗ Failed
4/25/20, 7:07 PM	11 - analyse	process 29688	0	0	✗ Failed
4/25/20, 7:07 PM	12 - processes	29688	1	6s	✓ Completed
4/25/20, 7:08 PM	13 - processes	29688	1	12s	✓ Completed
4/25/20, 7:11 PM	14 - analyse	process 29688	0	0	✗ Failed
4/25/20, 7:15 PM	15 - fileinfo	"c:\program files\windowsapps\microsoft.yourphone_1.20032.111.0_x64_8wekyb3d8bbwe\yourphone.exe"	1	10s	✓ Completed
4/25/20, 7:17 PM	16 - analyse	process 29688	0	0	✗ Failed

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/live-response-command-examples>

Auto Investigation & Remediation

Bu bölümde teorik anlatmak yerine akılda kalması açısından örnekle anlatmak daha mantıklı olacaktır. Özellikle daha sofistik , karmaşık , akıllı tasarlanmış zararlıları/saldırıları analiz etmek için kullanılmaktadır. Bu özelliğin kullanımı ile ilgili OS seviyesinde kısıt mevcut. Desteklenen işletim sistemi aşağıdadır.

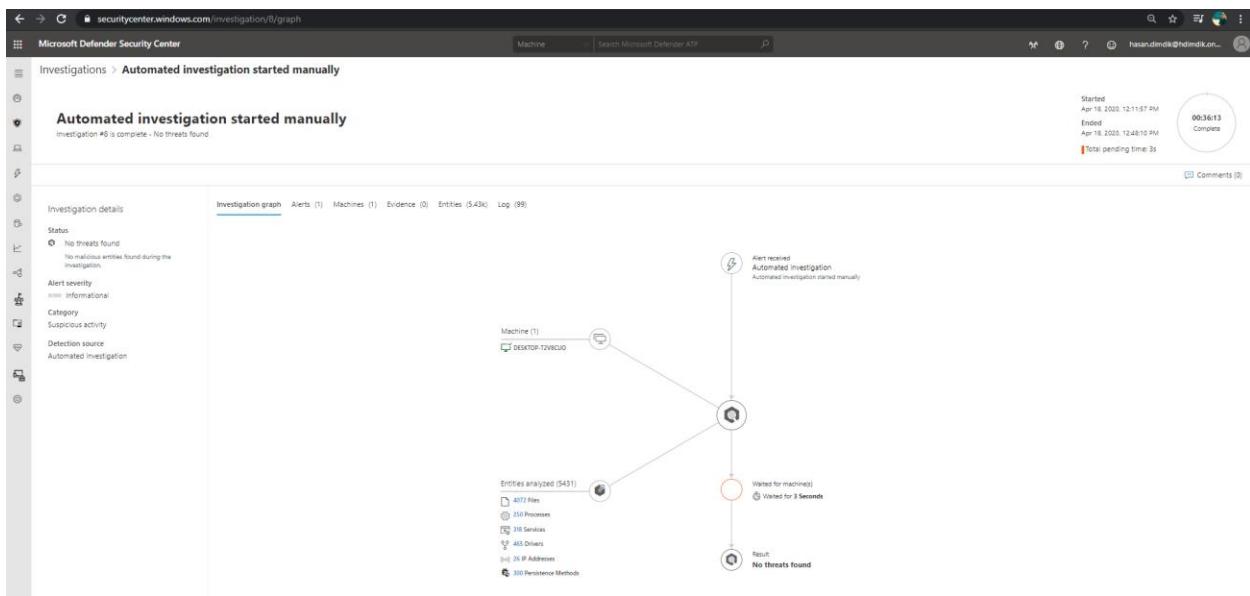
- Windows Server 2019
- Windows 10, version 1709 (OS Build 16299.1085 with [KB4493441](#)) or later
- Windows 10, version 1803 (OS Build 17134.704 with [KB4493464](#)) or later
- Later versions of Windows 10

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/automated-investigations>

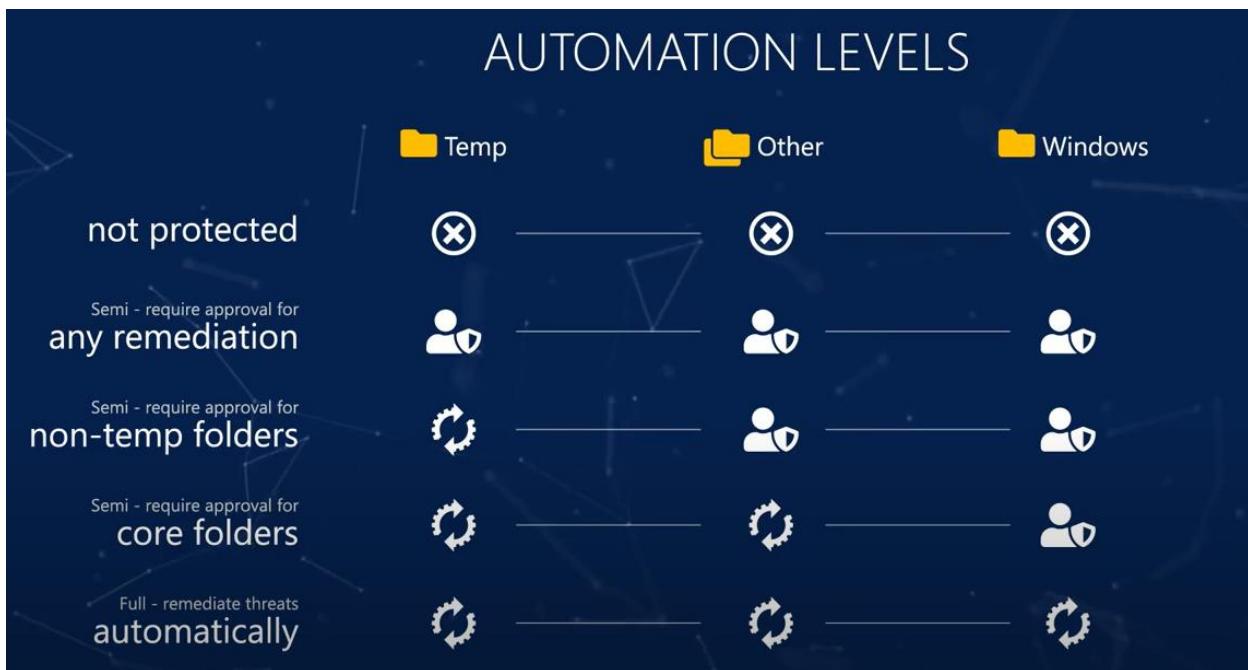
Örneğin aşağıdaki son kullanıcı bilgisayarında **Automated Investigation** başlattım.

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a sidebar with various navigation options like Dashboards, Threat analytics, Incidents, and Automated investigations. The main area is titled 'Machines list' and shows a table of machines with columns for Machine name, Domain, Risk level, Exposure level, and OS platform. One machine, 'desktop-t2v8cuo', is selected and highlighted with a red arrow. A context menu is open for this machine, with a red arrow pointing to the 'Initiate Automated Investigation' option under 'Active alerts'. The right side of the screen shows detailed information for the selected machine, including its device details, active alerts (with a count of 3), and a log of recent activities.

Bu bölümde kullanılmasının en temel sebeplerinden bir tanesi elbette hali hazırda bir zararlı yakalanmıştır veya alarm oluşmuştur ve araştırma başlatılabilir. Örneğimde zararlı olmadığı için daha sade sonuç getirdi. Bu noktadan sonra artık hangi processler başlamış, hangi registry değeri değiştirilmiş veya zararlı nereleme bulaşmış ve başka bir ortama bulaşmış mı gibi durumları görebiliyoruz.



Buraya kadar yaptığımız adımları manuel olarak başlattık fakat adına da anlaşıldığı üzere otomatik araştırmanın amacı insan faktörünü ortadan kaldırarak aksiyon alırmaktır. Aşağıdaki tabloda otomasyon seviyesini belirleyebiliyoruz. Burdaki ayrimı elbette yapımızdaki istemci veya sunucu kategorileri, kullanım amacına göre ayırip gruplandırmak olası bir sorunun da önüne geçmesi açısından önem arz etmektedir.



Settings > Machines Groups sekmesinde **Add machine Group** diyerek gruplarını belirliyoruz ve **Automation Level** kısmında otomasyon seviyesini belirleyerek süreçlerin hangi oranda otomatize edileceğini de tanımlamış oluyoruz. Bu noktada yukarıdaki tablo referans olacaktır.

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a navigation sidebar with various sections like Dashboards, Incidents, Machines list, and Settings. Under Settings, the 'Machine groups' option is selected, highlighted by a red arrow. A large red arrow points from this selection to the 'Add machine group' button in the center of the page. The main area is titled 'Add machine group' and contains three tabs: General, User access, and Automation level. The General tab is active, showing fields for 'Machine group name' (Windows10) and 'Automation level' (Semi - require approval for all folders). The User access tab shows a single user entry: 'Windows 10 Test grubu'. The Automation level tab shows a preview of 10 machines. At the bottom, there are 'Next' and 'Cancel' buttons.

Advanced Hunting

Bu bölüm özellikle SOC ekiplerinin derinlemesine analiz için kullanacağı bir bölüm. Proaktif olarak yapıyı inceleme imkanı sunmaktadır. Şirketiniz için özel sorgular yazabilir veya hazır sorgular ile zararlı/tehdit analizini daha detaylı olarak yapabilirsiniz. Bir kaç örnekle Advanced Hunting özelliğini nasıl kullanabileceğimize bir bakalım.

Akillara elbette şu soru gelmektedir. Soru diline hakim değilim veya bilgi yok, bu durumda ilgili bölümü nasıl kullanacağım. Hemen cevaplayalım,

Microsoft yeterli sayıda hazır sorguları zaten panele eklemiş durumda.

Örneğin aşağıdaki sorgu bize işletim sistemi özelinde alınan alarmları listeyecektir.

DeviceAlertEvents

```
| join DeviceInfo on DeviceId
| summarize Count = count() by OSPlatform, Severity
```

OSPlatform	Severity	Count
Windows10	Informational	213
WindowsServer2016	Informational	5

İkinci örneğimiz bize bilgisayar bazında indirilen dosya isimlerini listeleyecektir.

```
// Lists all the files downloaded using popular browsers.
DeviceFileEvents
| where Timestamp > ago(7d)
| where FolderPath !has "$Recycle.Bin"
| where
    // Edge
    InitiatingProcessFolderPath endswith @"windows\system32\browser_broker.exe"
    // Internet Explorer x64
    or InitiatingProcessFolderPath endswith @"program files\internet
explorer\iexplore.exe"
    // Internet Explorer x32
    or InitiatingProcessFolderPath endswith @"program files (x86)\internet
explorer\iexplore.exe"
    // Chrome
    or (InitiatingProcessFileName =~ "chrome.exe" and FileName endswith
"crdownload")
    // Firefox
    or (InitiatingProcessFileName =~ "firefox.exe" and (FileName !endswith ".js"
or FolderPath !has "profile"))
| project Timestamp, DeviceName, InitiatingProcessFileName, FileName, FolderPath
| top 100 by Timestamp
```

```

Run query
1 // Lists all the files downloaded using popular browsers.
2 | where TimeStamp > ago(7d)
3 | where FolderPath has "Recycle.Bin"
4 | where
5 |   $browser = {
6     |     if($ProcessName -eq "iexplorer.exe")
7       |       "IE"
8     |     else if($ProcessName -eq "firefox.exe")
9       |       "Firefox"
10    |     else if($ProcessName -eq "chrome.exe")
11      |       "Chrome"
12    |     else if($ProcessName -eq "edge.exe")
13      |       "Edge"
14    |     else if($ProcessName -eq "opera.exe")
15      |       "Opera"
16    |     else if($ProcessName -eq "ieexplorer.exe")
17      |       "IE"
18    |     else
19      |       "Unknown"
20   }
21 | where InitiatingProcessName -eq $browser
22 | where InitiatingFolderPath -eq $browser
23 | project TimeStamp, DeviceName, InitiatingProcessName, FileName, FolderPath
24 | sort -Time

```

Timestamp	DeviceName	InitiatingProcessName	FileName	FolderPath
4/30/2021 21:38:48	desktop-02f0ce	chrome.exe	Unconfirmed 9216501.undownloaded	C:\User\high\Downloads\Unconfirmed\9216501.undownloaded
4/29/2020 9:43:57	desktop-02f0ce	iexplorer.exe	monitor[1].gif	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:58	desktop-02f0ce	iexplorer.exe	monitor[1].gif	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:58	desktop-02f0ce	iexplorer.exe	onekey[1].css	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:53	desktop-02f0ce	iexplorer.exe	MPF_SocialFacebook.png[1].png	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:53	desktop-02f0ce	iexplorer.exe	MPF_SocialTwitterpng[1].png	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:53	desktop-02f0ce	iexplorer.exe	oai[1].css	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:53	desktop-02f0ce	iexplorer.exe	20-042102[1].css	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:53	desktop-02f0ce	iexplorer.exe	mafri-min-m[1].css	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:53	desktop-02f0ce	iexplorer.exe	avant[1].css	C:\User\Man\AppData\Local\Microsoft\
4/29/2020 9:43:49	desktop-02f0ce	iexplorer.exe	wire-player[1].css	C:\User\Man\AppData\Local\Microsoft\
4/24/2020 4:59:01	desktop-02f0ce	chrome.exe	Unconfirmed 344821.undownloaded	C:\User\high\Downloads\Unconfirmed\344821.undownloaded
4/24/2020 4:59:02	desktop-02f0ce	chrome.exe	Unconfirmed 344821.undownloaded	C:\User\high\Downloads\Unconfirmed\344821.undownloaded

Sorgulara baktığımız zaman nerdeyse güncel olan tehditlerin sorguları hali hazırda geldiğini görüyoruz. Elbette sizlerde kendi sorgularınızı yapıp kullanabilirsiniz.

Daha detaylı bilgi için aşağıdaki linkler faydalı olacaktır.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-hunting-query-language>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-hunting-overview>

Reports

Adında anlaşılacağı gibi yapımızda aktivitelerin raporlandığı , algılanan tehditlerin hangi teknoloji(EDR,Antivirüs vb) tarafından yakalandığı, tehditin alarm seviyesi gibi High Level olayları görsel olarak görebileceğimiz basit anlaşılır arayüze sahip olan raporlama arayüzünün olduğu alan diyebiliriz.

Threat Protection Report (Top Screenshot):

- Alert trends:** Shows detection source of all alerts by creation date from Wed Apr 29 2020 - Thu Apr 30 2020. Legend includes: EDR, Antivirus, SmartScreen, 3rd party TI, Custom TI, Office ATP, Automated Investigation, Microsoft Threat Experts, Custom Detection, Azure ATP, Microsoft Cloud App Security, and 3rd Party Sensors.
- Alert status:** Shows detection source of currently unresolved alerts on Thu Apr 30 2020. Legend includes: EDR, Antivirus, SmartScreen, 3rd party TI, Custom TI, Office ATP, Automated Investigation, Microsoft Threat Experts, Custom Detection, Azure ATP, and Microsoft Cloud App Security.
- Filters:** Includes Detection Source (Any, EDR, Antivirus, SmartScreen, 3rd party TI, Custom TI, Office ATP, Automated Investigation, Microsoft Threat Experts, Custom Detection, Azure ATP, Microsoft Cloud App Security, 3rd Party Sensors), Category (Any, Backdoor, Collection, Command and control, Credential access, Credential钓鱼, Credential theft, Defense evasion, Denial of service, Discovery, Document exploit, Enterprise policy, Execution, Exfiltration, Exploit, General, In-kernel access, Installation, Lateral movement, Malware, Malware download, Network exfiltration, None, Not applicable, Persistence, Privilege escalation, Resource reuse, Reconnection, Remote access tool, Social engineering, Suspicious activity, Subprocess rehosts, Trojan, TrojanDownloader, Unquoted software, Virus, Watermark, File exploit, File fingerprinting).

Machine Health and Compliance Report (Bottom Screenshot):

- Machine trends:** Shows Health state from Wed Apr 29 2020 - Thu Apr 30 2020. Legend includes: Active (green), Impaired communications (orange), Inactive (red), and No sensor data (grey).
- Machine summary:** Shows Health state on Thu Apr 30 2020. Legend includes: Active, Impaired communications, and Inactive.
- Antivirus status for active Windows 10 machines:** Shows status from Wed Apr 29 2020 - Thu Apr 30 2020. Legend includes: Updated (green), Not updated (orange), Disabled (red), and Not reporting (grey).
- OS platform:** Shows OS platform from Wed Apr 29 2020 - Thu Apr 30 2020. Legend includes: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Linux, Mac OS, iOS, Android, and Other.
- Filters:** Includes Sensor health state (Any, Active, Impaired communications, Inactive, No sensor data), Antivirus status (Any, Updated, Not updated, Disabled, Not reporting), OS platform (Any, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Linux, Mac OS, iOS, Android, Other), Windows 10 version (Any, 1607, 1703, 1709, 1803, 1809, 1903, 1909, Future), and Machine group.

Partners & API

Bildiğiniz üzere Microsoft birden çok 3rd party vendor ile işbirliği yapıyor ve ilgili firmaların çözümleri ile Defender ATP' yi bağlayabiliyoruz.

The screenshot shows the Microsoft Defender Security Center interface. On the left, there's a navigation sidebar with sections like Dashboards, Threat protection, Reports, Threat & Vulnerability Management, and Evaluation and tutorials. Under 'Partners & APIs', the 'Partner applications' section is highlighted. It lists several partners with their logos and brief descriptions:

- Radar**: AttacIQ Platform integrates with MD-ATP to configure continuous attack safety on production assets. [Open partner page](#)
- ATTACK10**: AttacIQ Platform integrates with MD-ATP to configure continuous attack safety on production assets. [Open partner page](#)
- RSA NetWitness**: Share Microsoft Defender ATP Alerts to RSA NetWitness leveraging Microsoft Graph Security API. [Open partner page](#)
- DEMISTO**: Demisto integrates with Microsoft Defender ATP to enable security teams to orchestrate and automate endpoint security monitoring, enrichment and response. [Open partner page](#)
- SWIMLANE**: Swimlane incident response capabilities utilizing Swimlane and Microsoft Defender ATP together. [Open partner page](#)
- CyberResponse QYte**: QYte integrates with Microsoft Defender ATP to automate customers' high-speed incident response playbooks. [Open partner page](#)
- RAPID7**: Rapid7 InsightConnect integrates with Microsoft Defender ATP to accelerate, streamline, and integrate your time-intensive security processes. [Open partner page](#)
- Bitdefender GravityZone**: Bitdefender GravityZone is a layered next generation endpoint protection platform offering comprehensive protection against the full spectrum of sophisticated cyber threats. [Open partner page](#)
- SentinelOne**: Extend your Microsoft Defender ATP protection to macOS and Linux endpoints. Prevent, detect, respond, and hunt cyber-attacks across your organization. [Open partner page](#)
- Corrala**: Mobile solution - Protect your mobile devices with granular visibility and control from Corrala. [Open partner page](#)

MDATP Bitdefender GravityZone Entegrasyonu

Bu bölümde daha iyi anlamak adına Bitdefender GravityZone ile nasıl bağlayabileceğimize değineceğim. Open Partner page tıklıyorum ve beni partner web sitesine yönlendiriyor.

The screenshot shows the Bitdefender GravityZone website. At the top, there's a navigation bar with links for Home, Business, Partners, Company, and Labs. The main headline reads "Stop Advanced Threats, Stay Ahead of Attackers". Below it, a sub-headline says "Integrate GravityZone Cloud with Microsoft Windows Defender Advanced Threat Protection¹ to receive threat intelligence from Linux and Mac devices on the ATP Console." There are two main calls-to-action: "LOGIN" for existing customers and "FREE TRIAL" for new users. A small note at the bottom of the page states "For more information about Microsoft Windows Defender Advanced Threat Protection click here." On the right side, there's a sidebar with options for "FREE TRIALS", "INQUIRE", "CHAT", and "PHONE".

Login butonuna tıkladığımda API key girmem gerektiğini belirtiyor.

The integration of Bitdefender's GravityZone Enterprise Security for Endpoints with Microsoft's Windows Defender ATP now enables Microsoft customers to detect, view, investigate, and respond to advanced cyber-attacks and data breaches on MacOS and Linux-based endpoints within the Windows Defender ATP Console.

For help on completing the integration, check this KB article.

İlgili API Key' i almak için Bitdefender portalında yer alan **My Account** bölümüne geliyorum.

API keys kısmında Add butonuna tıklıyorum.

Two-factor authentication secures your GravityZone account with an extra layer of protection. With each GravityZone login, in addition to your password, you will also need a code generated by the Google Authenticator app on your mobile device.

Two-factor authentication is disabled

Enable

Control Center API

Access URL: <https://cloudgz.gravityzone.bitdefender.com/api>

Key	Created
https://cloudgz.gravityzone.bitdefender.com/api	

First Page | Page 0 of 0 | Last Page [20] | 0 items

What's New
For the full list of changes, check the [Release Notes](#).

MARCH 2020
Single Sign-On (SSO)
Added new single sign-on (SSO) authentication capability using the SAML 2.0 standard. The SSO options are available...
[show more](#)

Incidents
The GravityZone Elite Security bundle now includes the Incidents feature, where we provide the Root Cause Analysis of...
[show more](#)

EDR
You can now create custom tasks to scan your environment for known indicators of Compromise and generate detailed...
[show more](#)

Endpoint Risk Analytics
• You can now use the new scan & patch features to search and fix CVE of applications...
[show more](#)

Antimalware
You can now configure Security Servers'

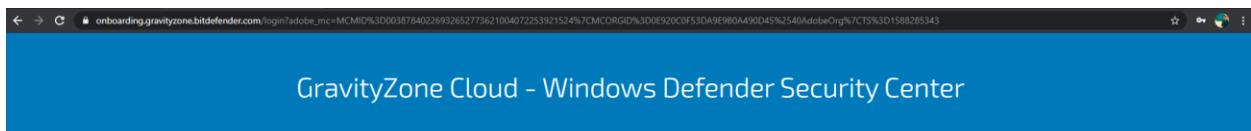
API key

Enabled APIs:

<input checked="" type="checkbox"/> Companies API	<input checked="" type="checkbox"/> Reports API
<input checked="" type="checkbox"/> Licensing API	<input checked="" type="checkbox"/> Accounts API
<input checked="" type="checkbox"/> Packages API	<input checked="" type="checkbox"/> Incidents API
<input checked="" type="checkbox"/> Network API	<input checked="" type="checkbox"/> Quarantine API
<input checked="" type="checkbox"/> Integrations API	<input checked="" type="checkbox"/> Event Push Service API
<input checked="" type="checkbox"/> Policies API	

Save **Cancel**

İlgili ayarları kaydettikten sonra API key ini portala kopyalayıp Submit butonuna tıkıyorum.



Bu adımla birlikte entegrasyonu tamamlamış oluyoruz. Peki bize nasıl bir faydası olacak? Özellikle Linux, android veya MacOs işletim sistemi kullanıyorsanız ilgili entegrasyonla birlikte bu işletim sistemleri üzerindeki zararlı faaliyetleri veya virüs bulunması durumunda Security Center içerisinde de görebilme kabiliyeti kazanıyoruz(Detect and Response)

Kaynak : <https://www.bitdefender.com/support/bitdefender-gravityzone-and-microsoft-windows-defender-atp-integration-1987.html>

MDATP Azure Sentinel Entegrasyonu

Azure Sentinel portalına eriştiğten sonra **Data Connectors** sekmesine geliyorum ve **open connector page** butonunu tıklıyorum.

The screenshot shows the Azure Sentinel Data connectors page. On the left, there's a sidebar with options like Overview, Logs, News & guides, Threat management (Incidents, Workbooks, Hunting, Notebooks), Configuration (Analytics, Playbooks, Community, Settings), and Data connectors (which is currently selected). The main area displays a list of connectors: Forcepoint DLP (Preview), Forcepoint NGFW (Preview), Fortinet, Microsoft Cloud App Security, Microsoft Defender Advanced Threat Protection (Preview), Microsoft web application firewall (WAF), Office 365, One Identity Safeguard, and Palo Alto Networks. Below this list, there's a summary: 39 Connectors, 7 Connected, and 1 Coming soon. To the right, a detailed view of the Microsoft Defender Advanced Threat Protection (Preview) connector is shown. It includes a status summary: Connected, Microsoft Provider, 6 days ago Last Log Received. A description explains that Microsoft Defender Advanced Threat Protection is a security platform designed to prevent, detect, investigate, and respond to advanced threats. It mentions that alerts are generated in Microsoft Defender ATP and sent to Azure Sentinel. A chart shows data received over time, with a peak of 6 on April 19 and another on April 26. At the bottom right, there's a blue button labeled "Open connector page".

Ön gereksinimleri sağladığımıza emin oluyoruz ve **Connect** butonuna basarak entegrasyonu tamamlıyoruz. (Ben daha önceden aktif ettiğim için Disconnect butonu gözükmektedir)

The screenshot shows the Microsoft Defender Advanced Threat Protection (Preview) configuration page. At the top, there are tabs for Instructions (selected) and Next steps. Below this, a section titled "Prerequisites" is outlined with a red border. It lists three requirements: Workspace (read and write permissions required), Tenant Permissions (required 'Global Administrator' or 'Security Administrator' on the workspace's tenant), and License (required Microsoft Defender Advanced Threat Protection). A red arrow points from the text "Connecting Microsoft Defender Advanced Threat Protection will cause your data that is collected by Microsoft Defender Advanced Threat Protection service to be stored and processed in the location that you have configured your Azure Sentinel workspace." to the "Disconnect" button. The "Configuration" section below contains a brief description and the "Disconnect" button. At the bottom left, there's a large number "14" and at the bottom right, a small "Page 35".

Workbooks lar bizim dashboard larımız, kontrol etmek için **Workbooks** sekmesine geliyorum.

The screenshot shows the Microsoft Azure Azure Sentinel Workbooks page. The left sidebar has a 'Workbooks' link under 'Threat management'. A red arrow points from this link to the 'Security Alerts' card in the main content area. The main content area displays three cards: 'One Identity' (ONE IDENTITY LLC&A), 'Palo Alto Network Threat' (PALO ALTO NETWORKS), and 'Security Alerts' (MICROSOFT). The 'Security Alerts' card includes a 'View template' and 'Save' button. The top right corner shows the user's name 'hasan.dimdik@hdimdik... HD'.

İlgili alarmların artık Azure Sentinelle geldiğini gözlemliyorum.

The screenshot shows the Microsoft Azure Azure Sentinel Security Alerts Dashboard. The left sidebar has a 'Security Alerts' link under 'Threat management'. A red arrow points from this link to the 'Security Alerts by Product' chart in the main content area. The chart shows 'All' alerts at 47, 'Microsoft Defender Adv...' at 47, and other products at 0. The top right corner shows the user's name 'hasan.dimdik@hdimdik... HD'.

The screenshot shows the Azure Sentinel Security Alerts workbook interface. At the top, there's a navigation bar with 'Home', 'Azure Sentinel workspaces', 'Azure Sentinel | Workbooks', and 'Security Alerts'. Below the navigation is a search bar and a user profile icon.

Top Entities in Security Alerts

Target	Entity_Type	count_↑↓
hd01	host	29
wac	account	10
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	file	10
e02115f9d93290cbfd5837677f5e1cd5fc515a532cf02c4...	filehash	10
5f710a36565d26b17ef57e87f3aeed1910513b8d9	filehash	10
349f666bd2fa869ed047707c5723b9f1	filehash	6
\avchost.exe	file	4
desktop-t2v8cuo	host	3
hd01	host	3
9a42fa1870472c38a56c0a70f62e57a3cdc0f5bc142f3a400...	filehash	2
da37dac5732bc5c7a62355b0c2414aa2a96c731cb7fb133...	filehash	2

Count of Entities in Security Alerts by Type

Type	Count
host	~60
file	~42
filehash	~35
other	~5
other	~2
other	~1

Settings

Windows Server 2008 R2 SP1, 2012 R2, 2016 Onboarding

Yazım içerisinde iki temel parçanın olduğuna değinmiştim. İlkı mma ajanları. Bu bize EDR özelliği kazandırıyor. İlk yapmamız gereken ilgili ajanları endpoint lerimize kurmak olacak. Büyük bir yapıda elbette tek tek kuramayacağımıza göre merkezi olarak dağıtmamız mantıklı olacaktır. Ben örneğimde SCCM kullanacağım. (Tüm adımları göstermeyeceğim) İlk olarak portala eriştiğten sonra **Settings** sekmesi içerisinde **Onboarding** sekmesini tıklıyorum. **Configuration connection** içerisindeki parametreleri bir yere kopyalıyorum.

Onboarding - Microsoft Defender

securitycenter.windows.com/preferences2/onboarding

Microsoft Defender Security Center

Settings

Select operating system to start onboarding process: Windows Server 2008 R2 SP1, 2012 R2 au...

1. Turn on server machine monitoring

2. Install Microsoft Monitoring Agent

3. Configure connection

4. Run a detection test

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $r = [System.Net.WebClient]::new(); $r.DownloadFile('http://127.0.0.1:443/test/mo!/test\m�ice.exe'); Start-Process -FilePath $r.downloadfile -WorkingDirectory C:\test\m�ice.exe
```

SCCM konsolunu açtıktan sonra applications sekmesine gelerek işlemlere başlıyoruz. **Deployment Types** olarak **Script** seçmiştim. **Programs** sekmesine geliyoruz **Installation progress** kısmına aşağıdaki komutu yapıştırıyoruz. Kırmızı alanları editlemeyi unutmayın. Demo ortamında internete proxy üzerinden çıktığım için komuta dahil ettim.

```
msiexec /i MMASetup-AMD64.exe /qn NOAPM=1
ADD_OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE=0 OPINSIGHTS_WORKSPACE_ID=xxxxxxxxxx
OPINSIGHTS_WORKSPACE_KEY=xxxxxxxxxxxxx AcceptEndUserLicenseAgreement=1
OPINSIGHTS_PROXY_URL=192.168.1.222:3128
```

Home | Folder

Create | Saved Searches | Search | Manage Access Accounts | Create Prestaged Content File | Revision History | Update Statistics | Create Deployment Type Application | Convert to .MSIX | Export | Delete | Reinstate | Copy | Refresh | Simulate Deployment | Deploy | Create Phased Deployment | Distribute Content | Move | Classify | View Relationships | Proper

Software Library > Overview > Application Management > Applications

MMA Agent Properties

Deployment Types

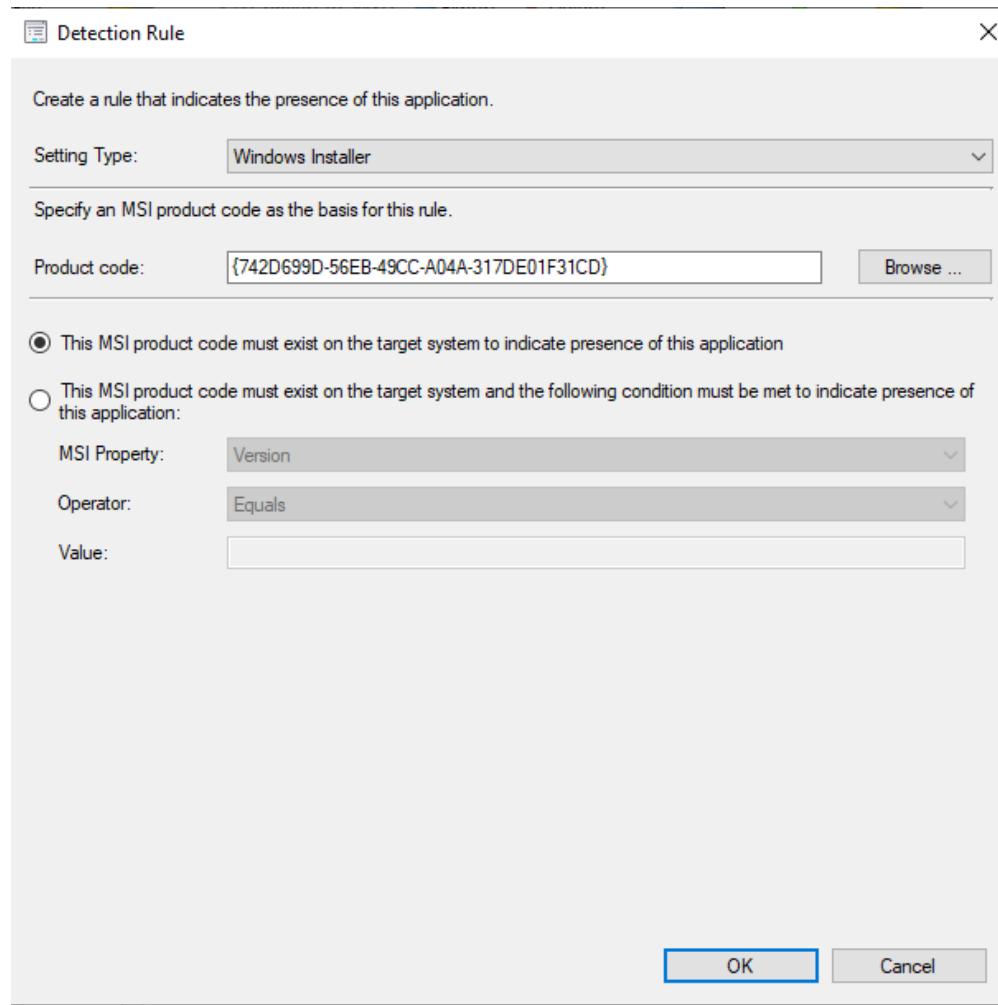
Install Behavior

Programs

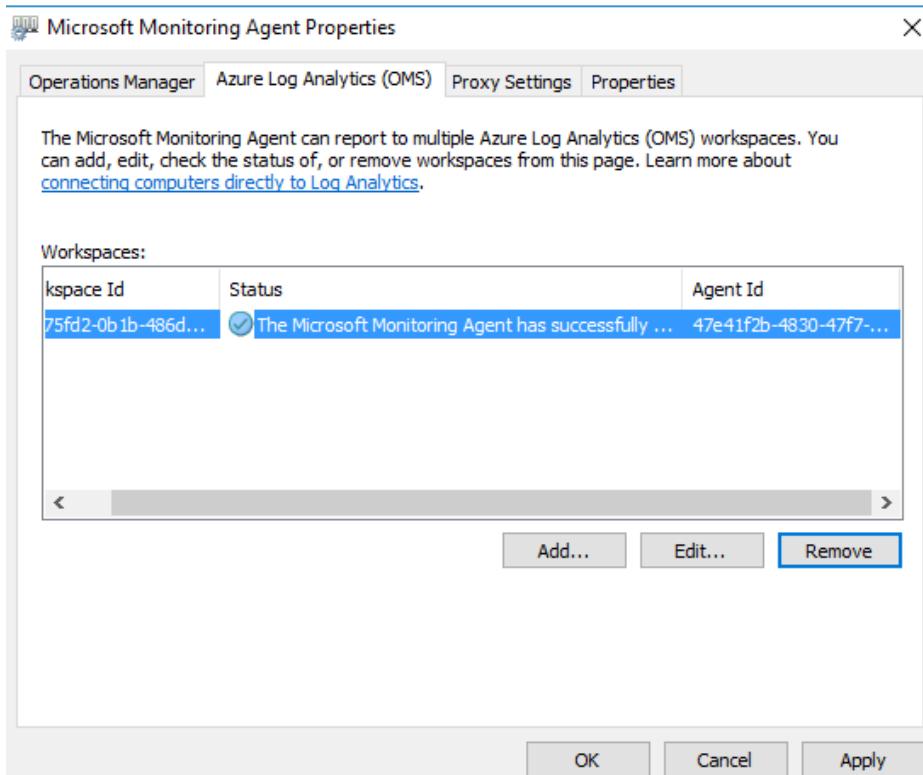
AcceptEndUserLicenseAgreement=1 OPINSIGHTS_PROXY_URL=192.168.1.222:3128

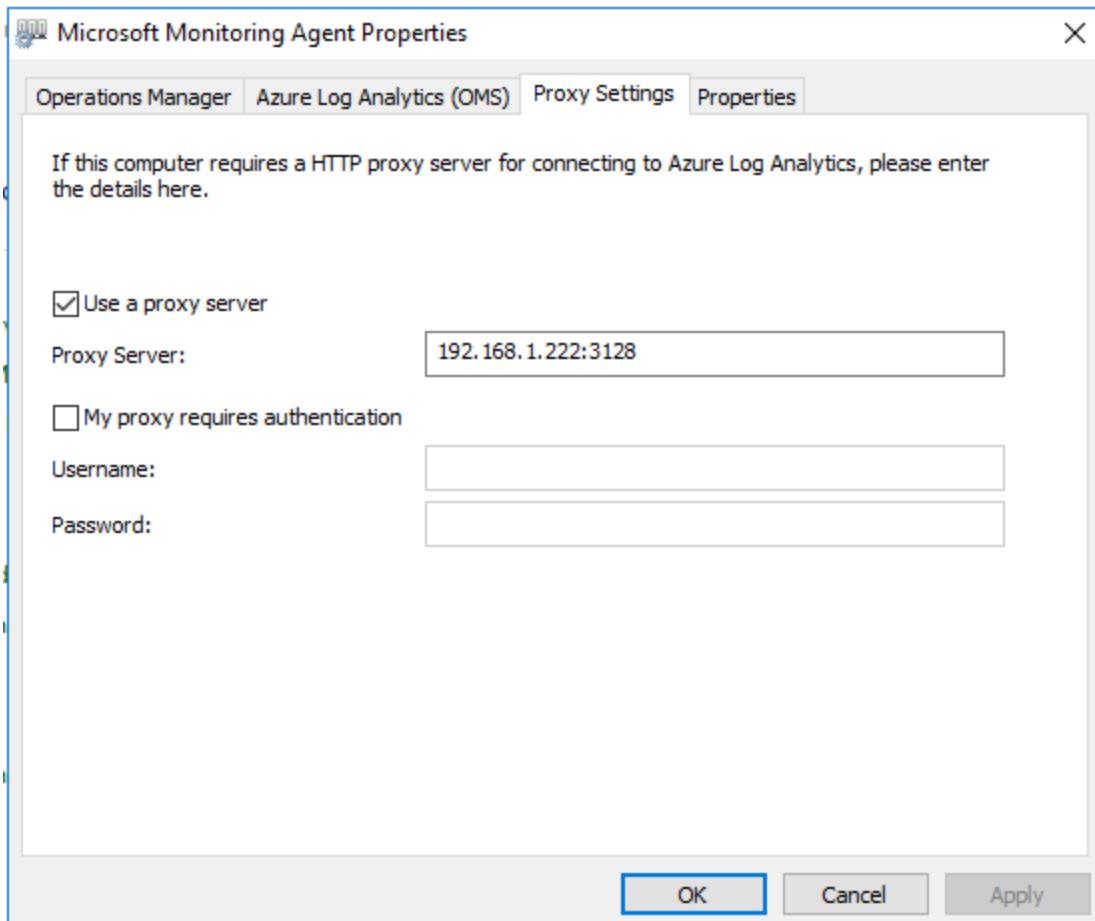
Detection Rule olarak **Windows Installer** seçip ilgili parametreyi ekliyorum ve geriye kalan işin makyaj kısımlarını tamamlıyoruz 😊

{742D699D-56EB-49CC-A04A-317DE01F31CD}



Son olarak ilgili collection lara mma agent imi dağıtıyorum.





Eğer yapınızda sunucularınız internete direk olarak çıkmıyorsa OMS Gateway yapılandırmamız gerekmektedir. Gerekli port ve URL ieri aşağıdaki dökümandan okuyabilirsiniz.

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

Aynı adımlar Windows 7 SP1 ve Windows 8.1 içinde geçerli. Yazının ilerleyen bölümlerinde Windows Server 2008 R2 SP1, 2012 R2 için SCEP yapılandırmasını göreceğiz. Simdilik burada bırakıyorum.

Windows 10 Onboarding

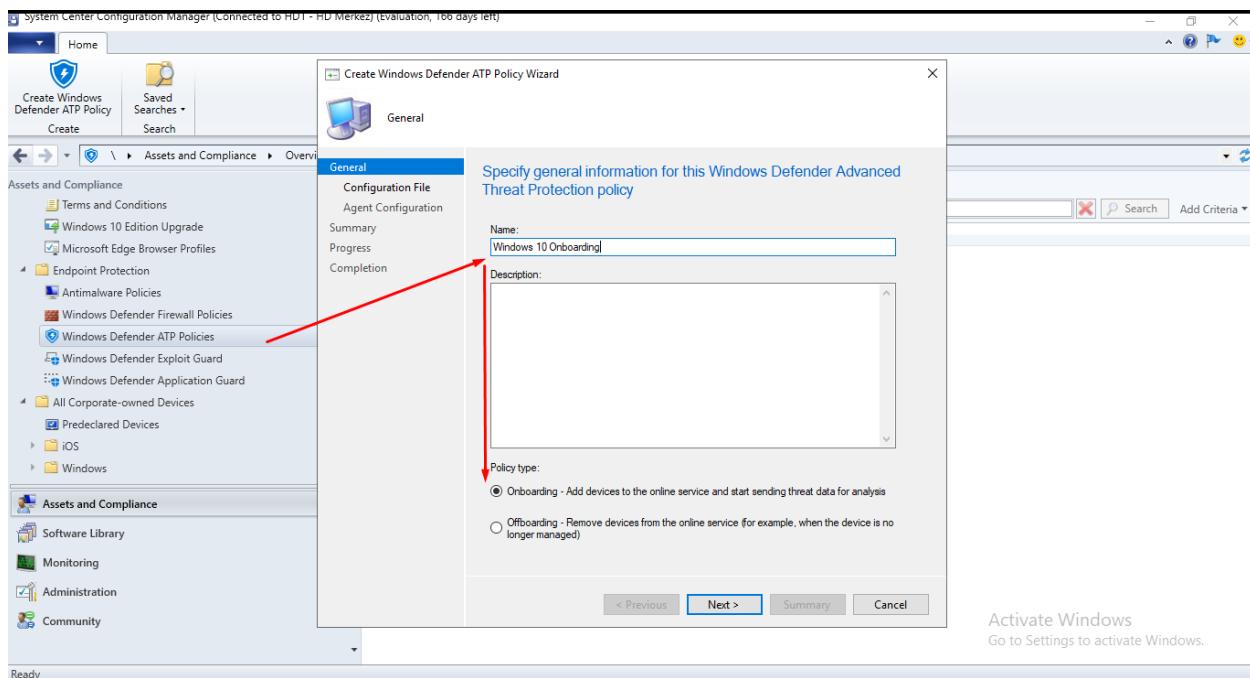
Bu adımda işlemler biraz daha basitleşiyor. İlgili ajanları group policy veya SCCM ile dağıtabiliyoruz. Örneğimde SCCM ile nasıl onboarding işlemini tamamlayabileceğimizi göstereceğim. Panelimde Onboarding sekmesini açıyorum ve işletim sistemi olarak **Windows 10** u seçip **Download package** ile gerekli onboarding yükleme dosyasını indiriyorum ve SCCM sunucuma kopyalıyorum.

The screenshot shows the Microsoft Defender Security Center interface. The left sidebar is collapsed. The main area is titled "Settings". Under "Machine management", the "Onboarding" tab is selected. A large central panel is titled "1. Onboard a machine". It says "First machine onboarded: Completed". Below this, it says "Onboard machines to Microsoft Defender ATP using the onboarding configuration package that matches your preferred deployment method. For other machine preparation instructions, read Onboard and set up." There is a link to "Microsoft Endpoint Configuration Manager". A "Download package" button is visible. Below this, another section titled "2. Run a detection test" is shown, stating "First machine detection test: Completed". It provides instructions to open a Command Prompt window and run a specific command. A copy button is available for the command text. At the bottom, there is a call-to-action button labeled "Explore simulations & tutorials".

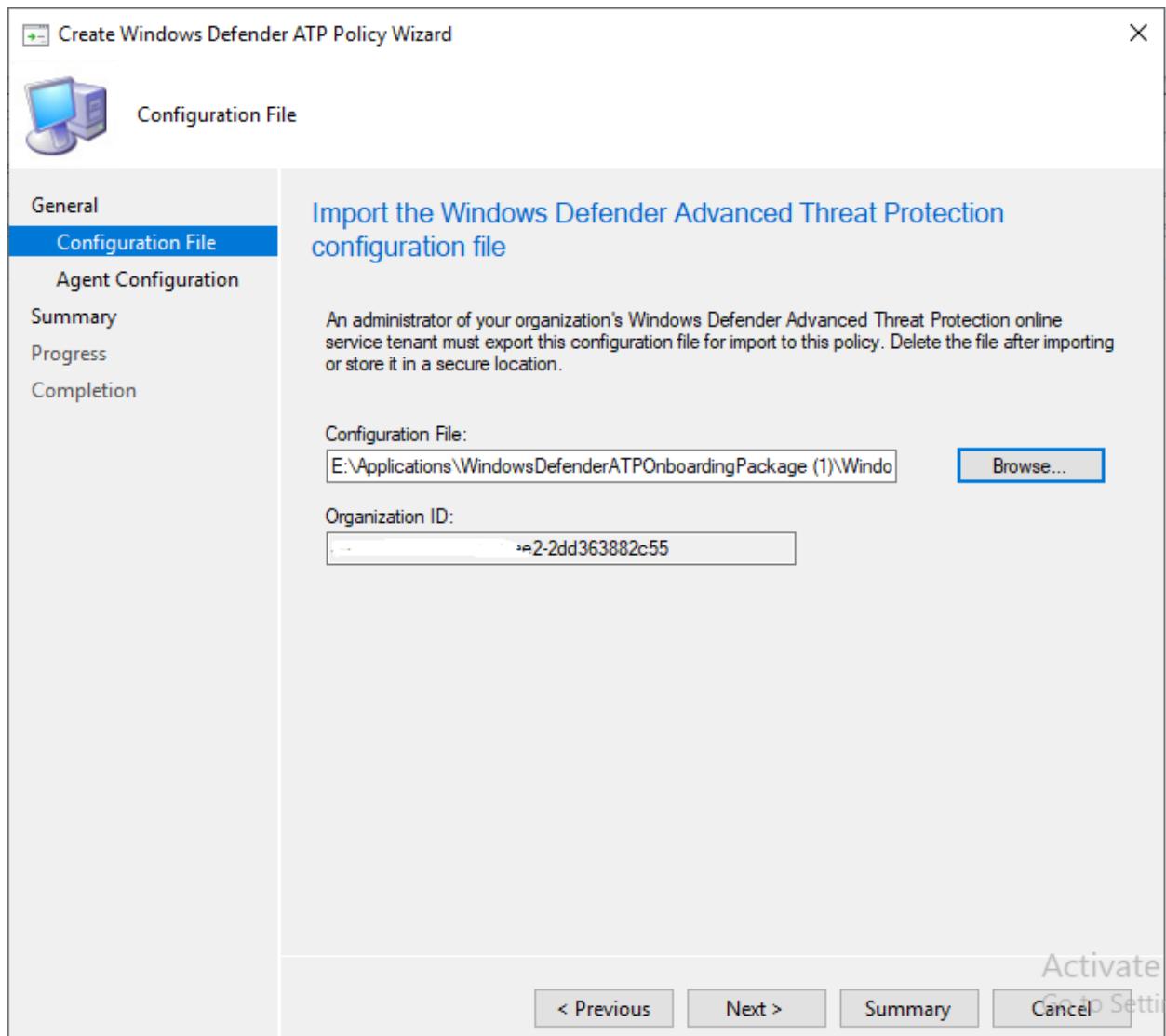
Dosyanın uzantısının .onboarding olduğunu kontrol ediniz.

The screenshot shows a Windows File Explorer window. The address bar indicates the path: "This PC > tools (E) > Applications > WindowsDefenderATPOnboardingPackage (1)". The main area shows a file named "WindowsDefenderATP.onboarding" with a size of 8 KB, modified on 4/6/2020 at 1:24 PM. The file type is listed as "ONBOARDING FILE". The left sidebar shows "Quick access", "Desktop", and "Downloads".

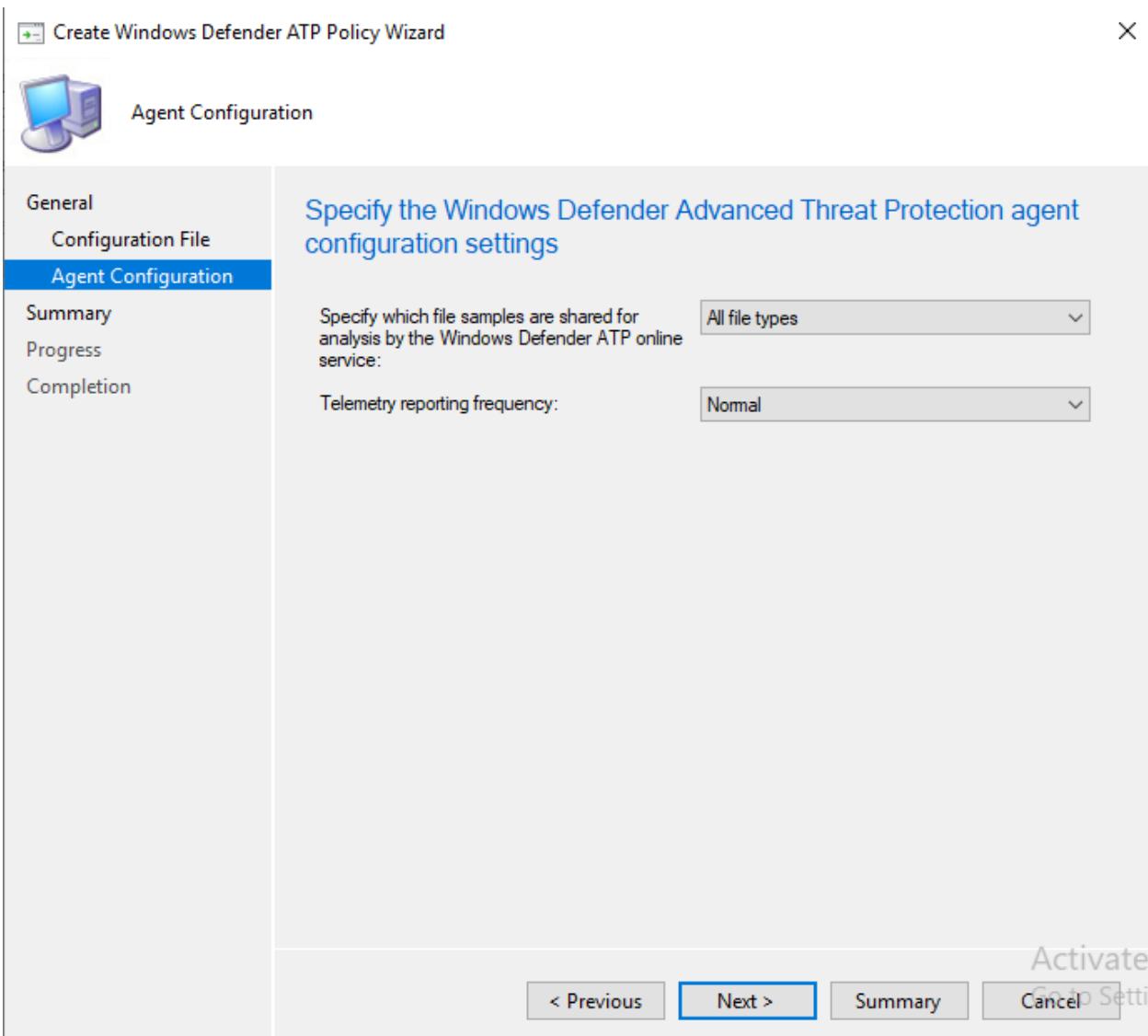
SCCM konsolunu açtıktan sonra asset and Compliance sekmesi içerisinde yer alan Windows Defender ATP Policies sekmesini sağ tıklayıp **Create Windows Defender ATP Policy** diyerek işlemimize başlıyoruz. Onboarding yapacağımız için onboarding seçeneğini seçip devam ediyorum.



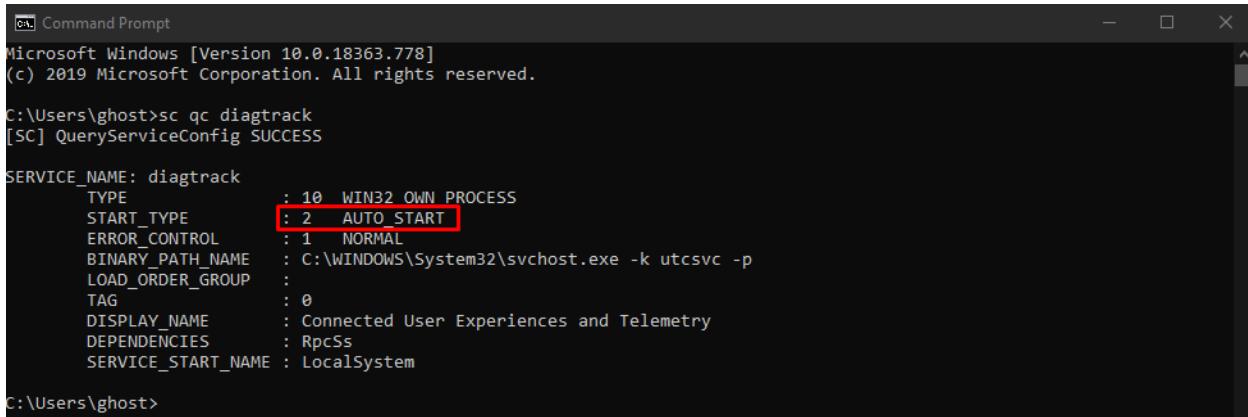
Portaldan indirmiş olduğum onboardıng dosyasını gösteriyorum ve devam ediyorum.



Bu bölüm tamamen yapınız ile alakalı. Analiz dosyalarının cloud a gönderilmesine izin verecek miyiz gibi ayarları yapıyoruz . İşlemi tamamladıktan sonra Windows 10 istemcilerimin olduğu collection a dağıtıyorum.



Onboarding işleminin başarılı olması için diagtrack servisinin AUTO_START olması gerekmektedir. Sorun yaşarsanız bu bilgi bir köşede dursun 😊



```
Windows PowerShell - Command Prompt
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ghost>sc qc diagtrack
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: diagtrack
    TYPE               : 10  WIN32 OWN PROCESS
    START_TYPE         : 2   AUTO_START
    ERROR_CONTROL     : 1   NORMAL
    BINARY_PATH_NAME  : C:\WINDOWS\System32\svchost.exe -k utcsvc -p
    LOAD_ORDER_GROUP  :
    TAG               : 0
    DISPLAY_NAME      : Connected User Experiences and Telemetry
    DEPENDENCIES      : RpcSs
    SERVICE_START_NAME: LocalSystem

C:\Users\ghost>
```

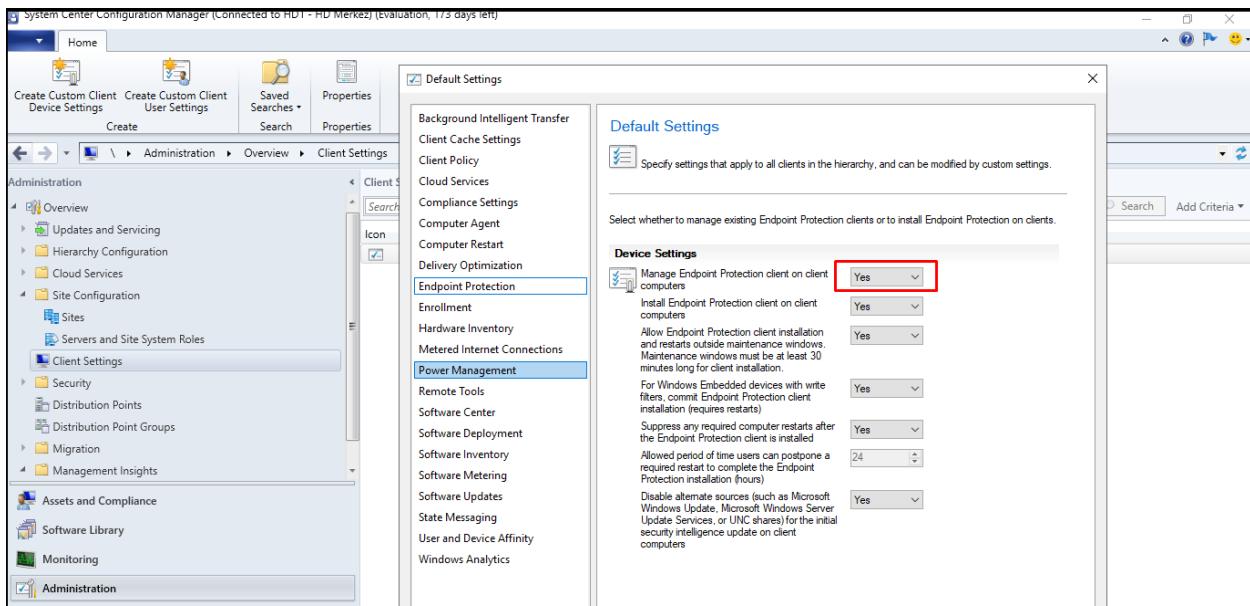
Buraya kadar olan kısımda Onboarding işlemlerini tamamladık. EDR çözümümüz artık çalışır durumda.

System Center Configuration Manager SCEP Yapılandırması

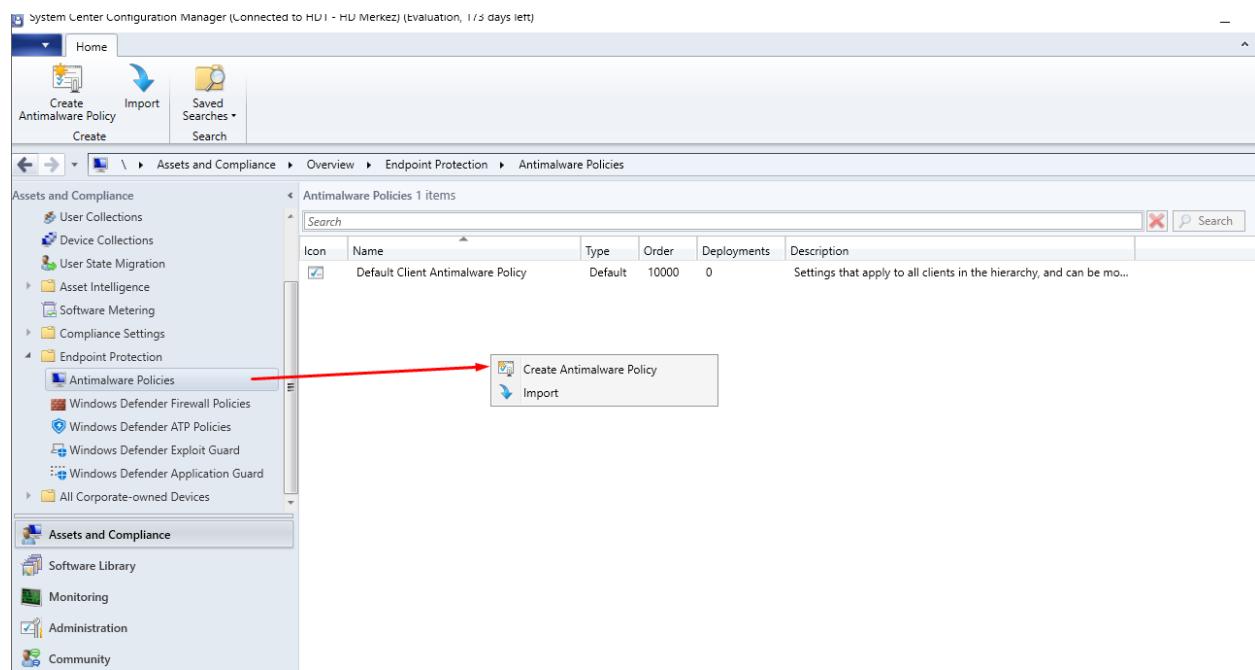
Giriş bölümünde **Attack Surface Reduction** kısmını SCCM ile yapılandıracığımızdan bahsetmiştık. MDATP ve SCEP konularına hakim değilseniz neden buna ihtiyaç var sorusu akıllara gelecektir. Hemen bu soruyu cevaplayalım. Yapıyı incelediğimiz zaman EDR teknolojisinden faydalananın MMA ajanlarını sunucularımıza yüklememiz gerekiyor, bu sayede MDATP portalında sunucularımıza görebiliyoruz ve yukarıda detaylıca bahsettiğimiz CVE açıklığı varmı sunucu envanteri gibi verileri artık raporlayabilir hale geliyoruz. Fakat bu bize koruma sağlamamaktadır. Bu noktada da yapıyı ikiye ayıriyoruz. Eğer sunucu tarafında Windows Server 2016 veya üstü, istemci tarafında ise Windows 10 OS leriniz mevcut ise varsayılan olarak Defender ATP gelmektedir ve Defender ATP ajanı aktif ise koruma sağlayabiliyoruz. Fakat bu versiyonlardan düşük işletim sistemi sürümlerine sahipseniz System Center Endpoint Manager' dan yararlanmamamız gerekiyor.

Not: Kafa karışıklığına sebep olmamak için her bir konu başlığında ilgili özelliğin desteklediği işletim sistemlerini paylaşacağım. Lütfen ilgili linkleri dikkatlice okuyunuz. (Özellikle Windows Defender Exploit Guard bölümündeki paylaştığım kaynakları dikkatlice okuyunuz)

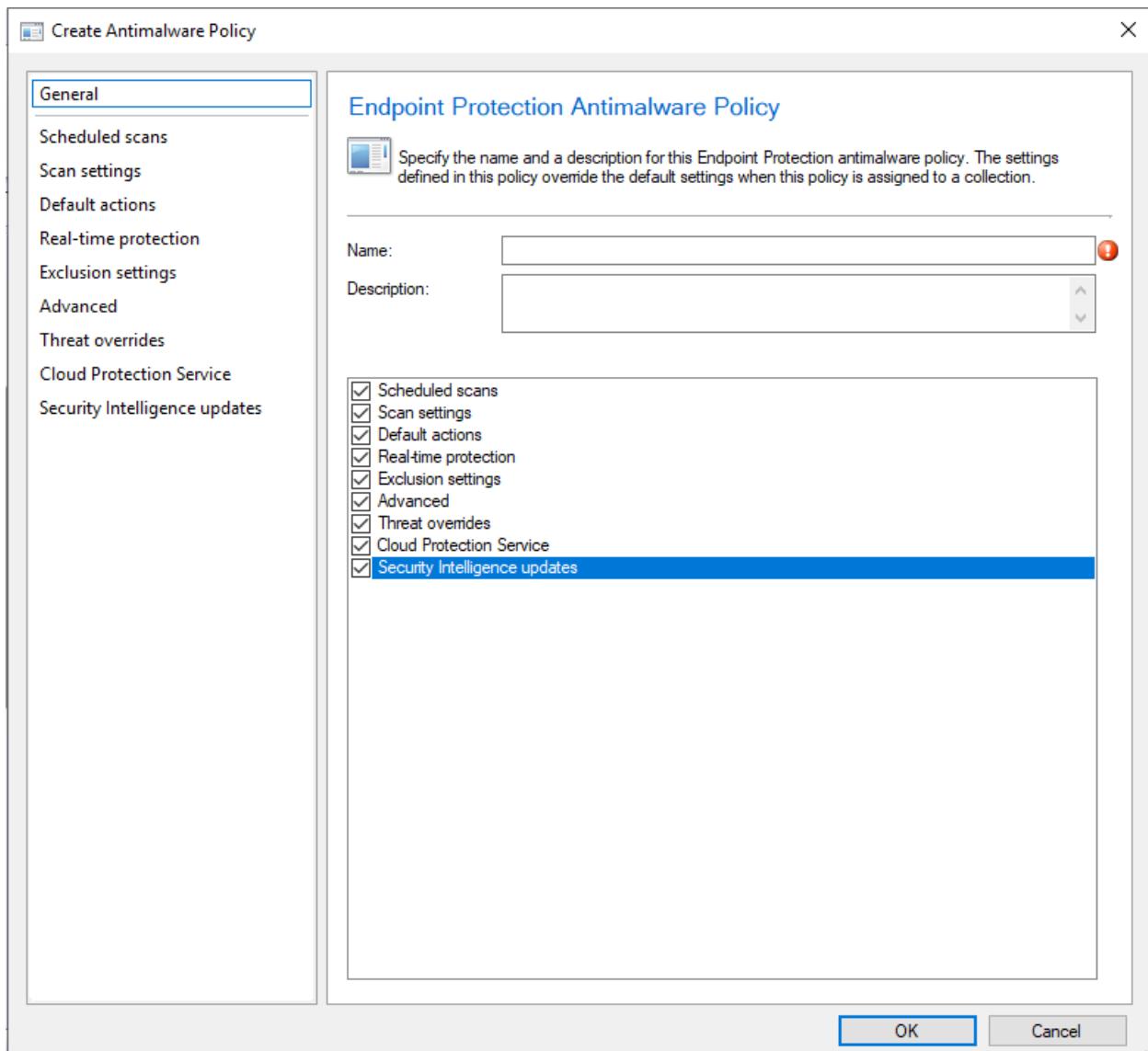
SCCM Portalımıza eriştiğten sonra yapılandırmamıza **Client Settings'** den başlıyoruz. **Endpoint Protection** sekmesine geliyoruz. **Manage Endpoint Protection client on client computers** ayarını **yes** olarak değiştiriyoruz.



İkinci adımda ise **Antimalware Policy** oluşturuyoruz.



Tam koruma sağlama açısından tüm seçenekleri seçiyorum.



AntiMalware Policy

Desteklenen sürümler (Server,Client)

System Center Configuration Manager (SCCM) Current Branch (CB)

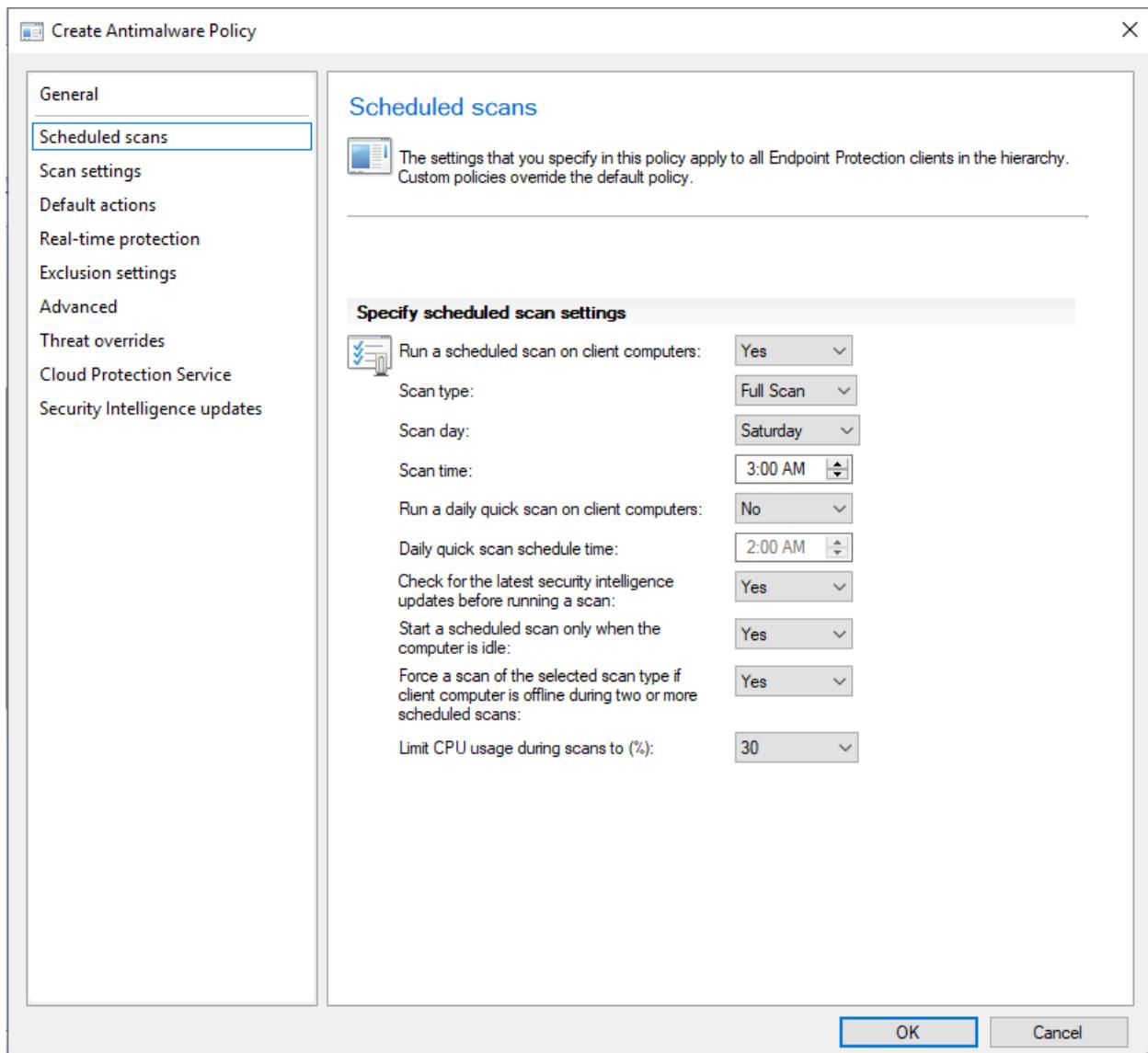
Microsoft Defender Antivirus

- Windows Server 2019
- Windows Server 2016
- Windows 10

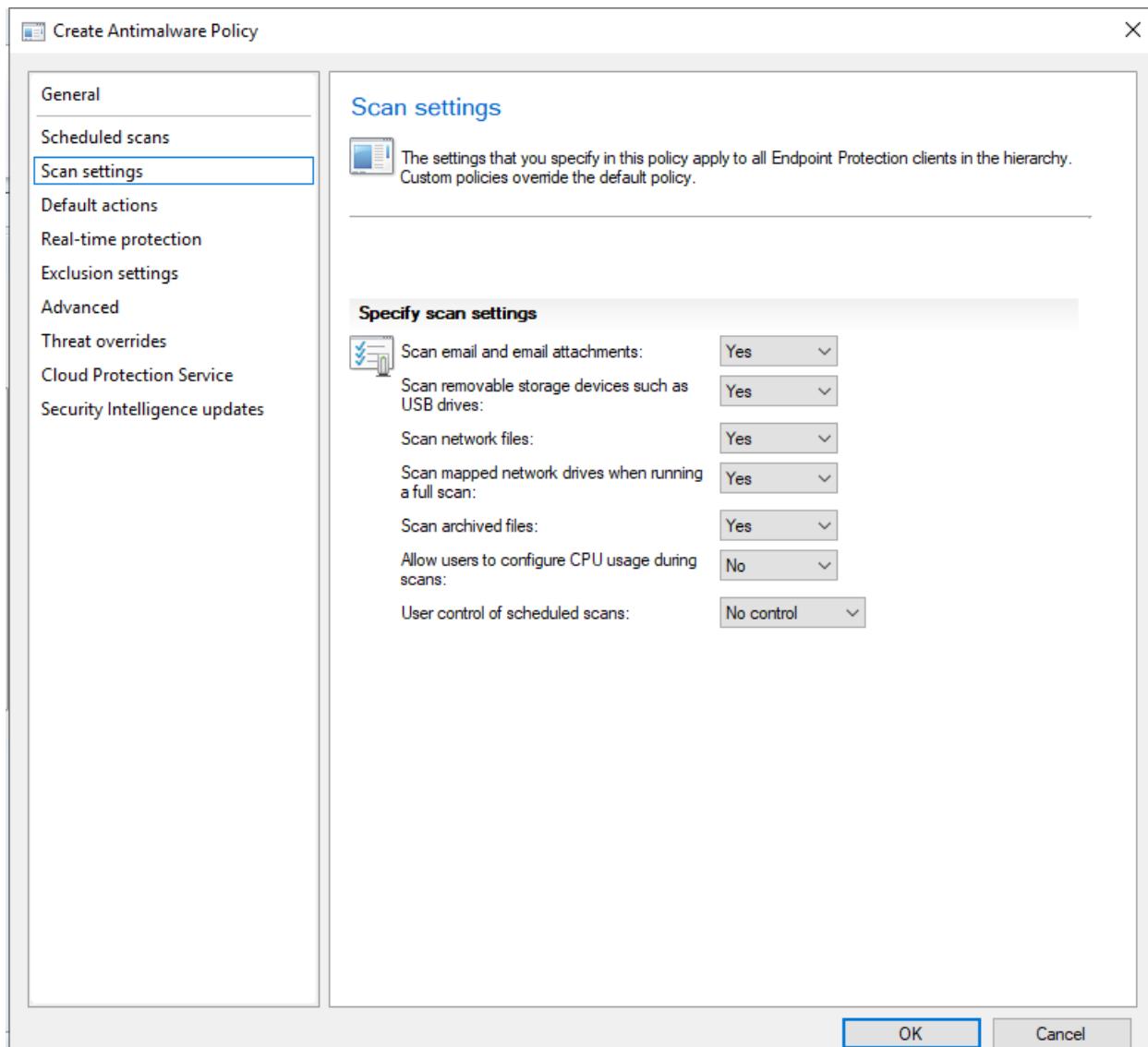
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2
- Windows 8.1
- Windows 8
- Windows 7 SP1
- Windows Vista

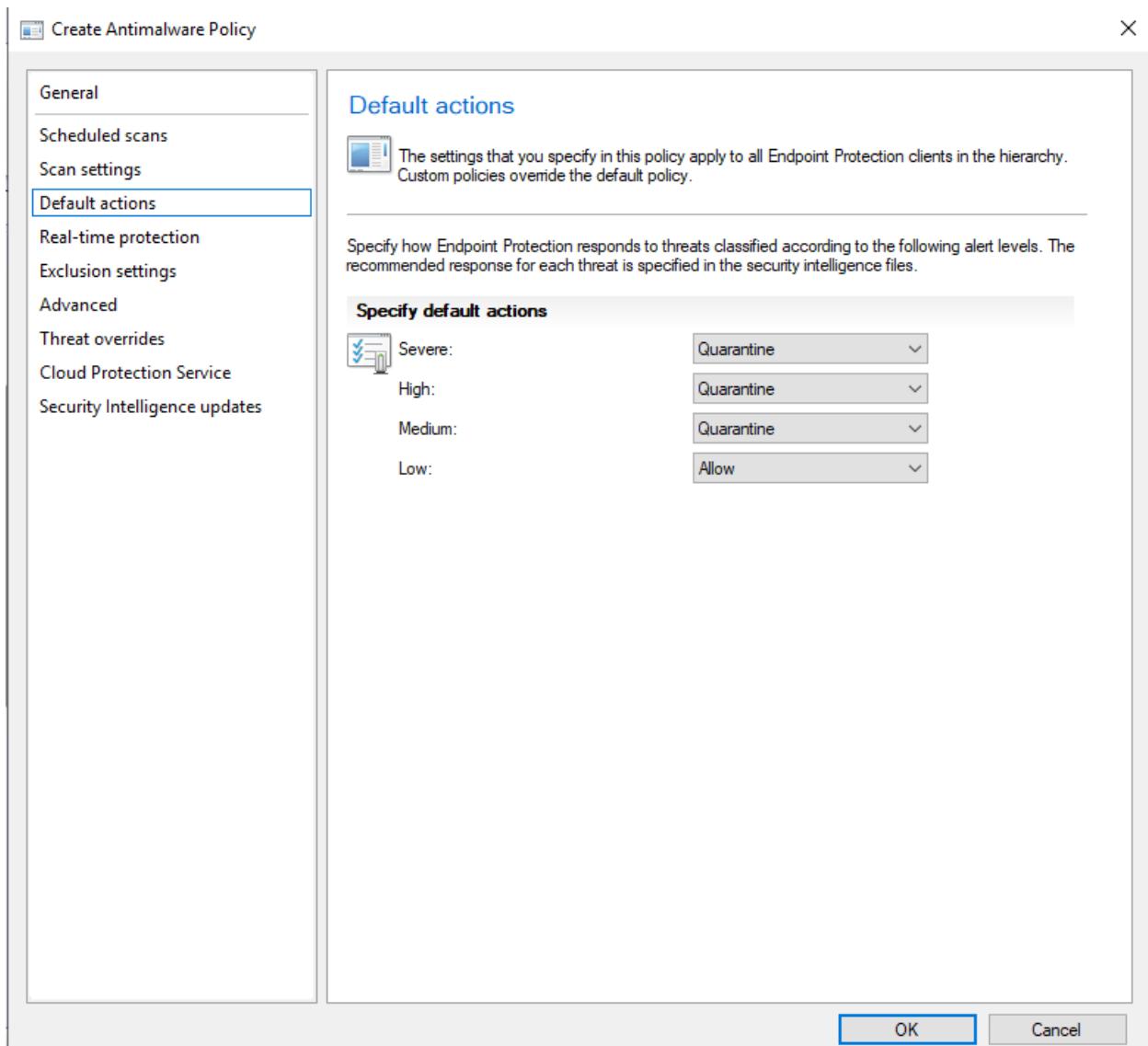
Scheduled Scan sekmesinde tarama tipini, gününü , saatini CPU kullanımını kısıtlama gibi ayarları yapabiliyoruz.



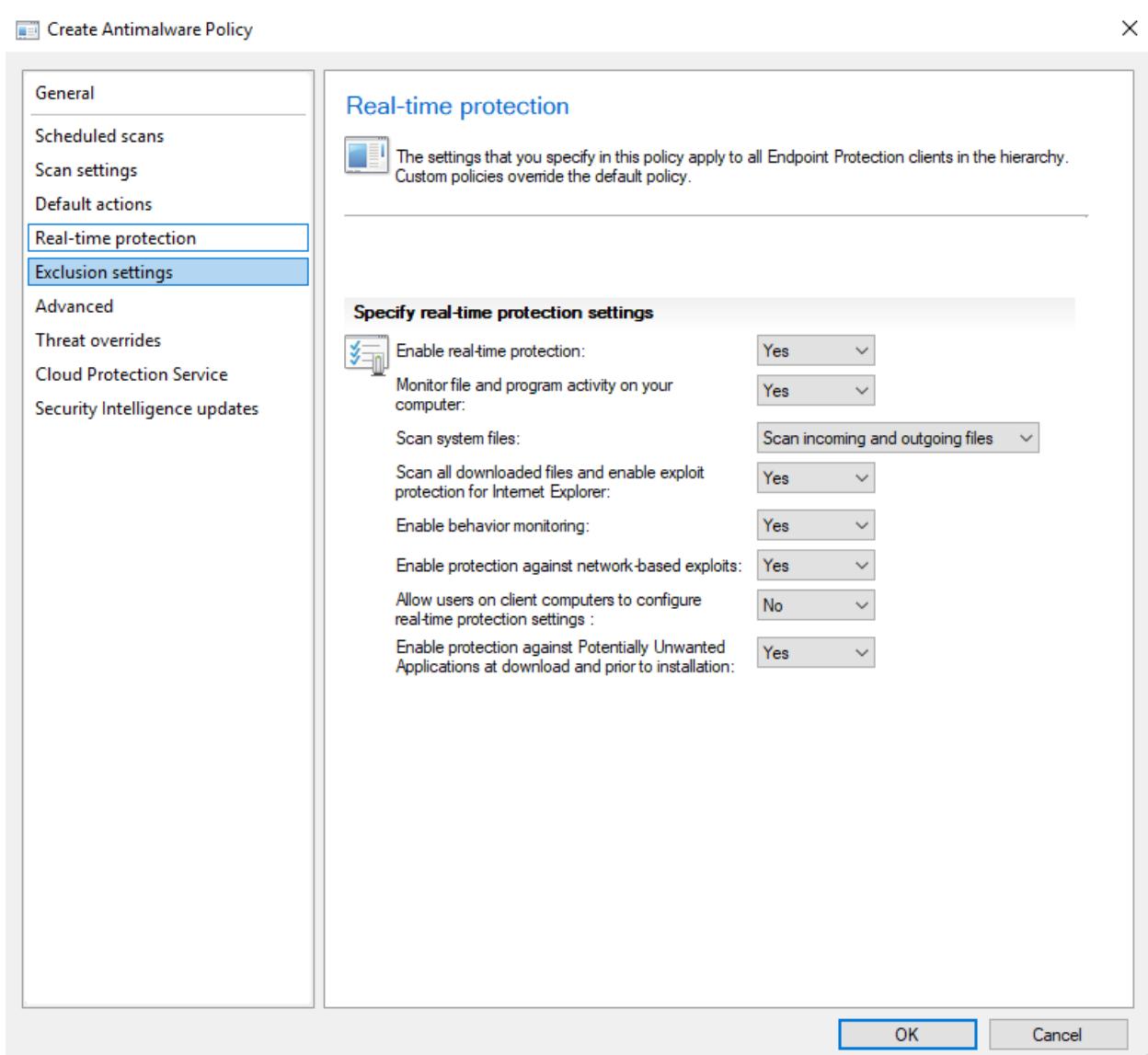
Scan Settings sekmesinde nelerin taranacağı(harici cihazlar, arşiv alanları, e mail içerisindeki ekler, network dosyaları vb..) kullanıcılara kontrol verip vermeyeceğimizi belirleyebiliyoruz.



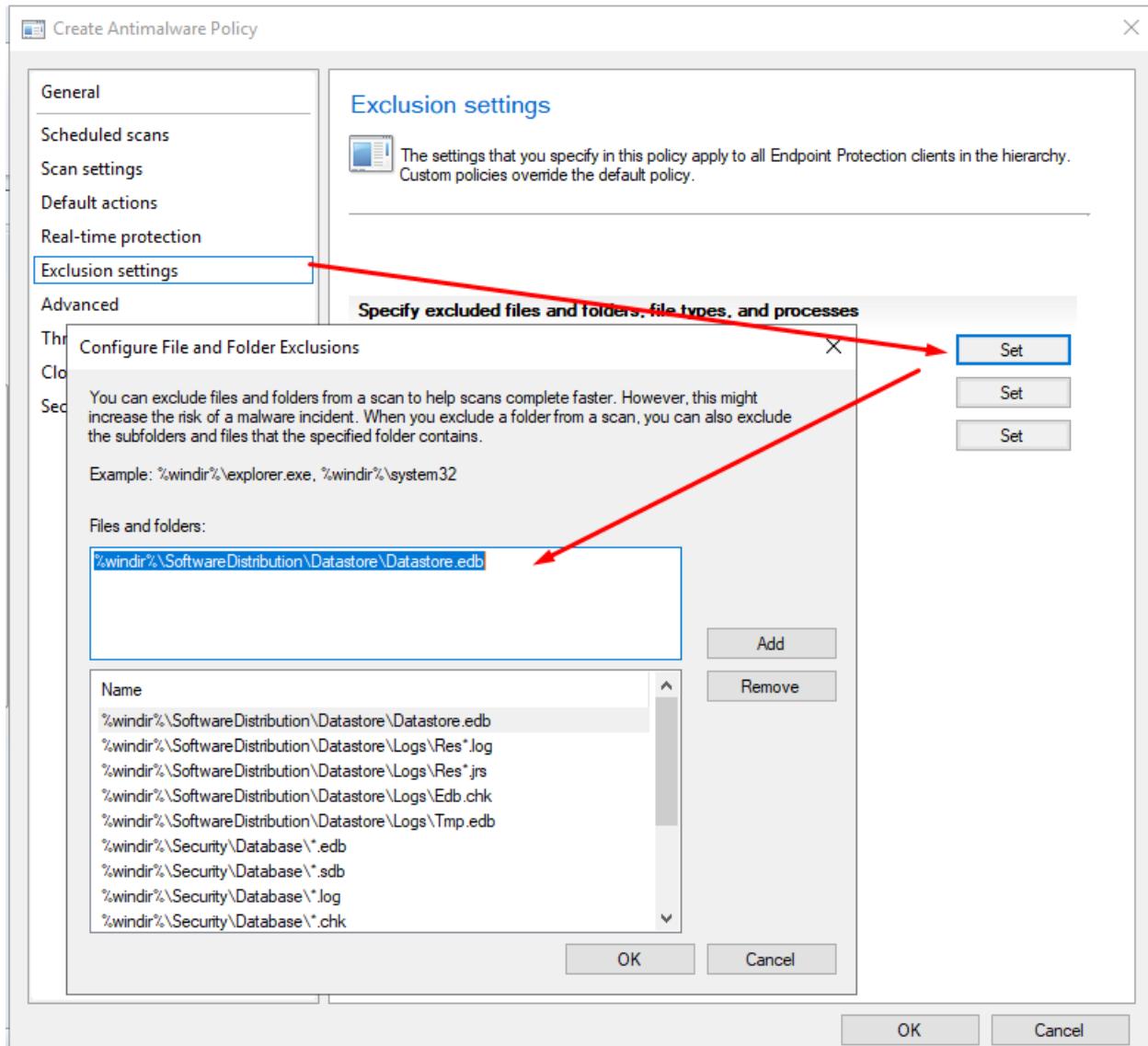
Default Action sekmesinde zararlı yakalandığı zaman nasıl aksiyon alınacağını belirliyoruz.



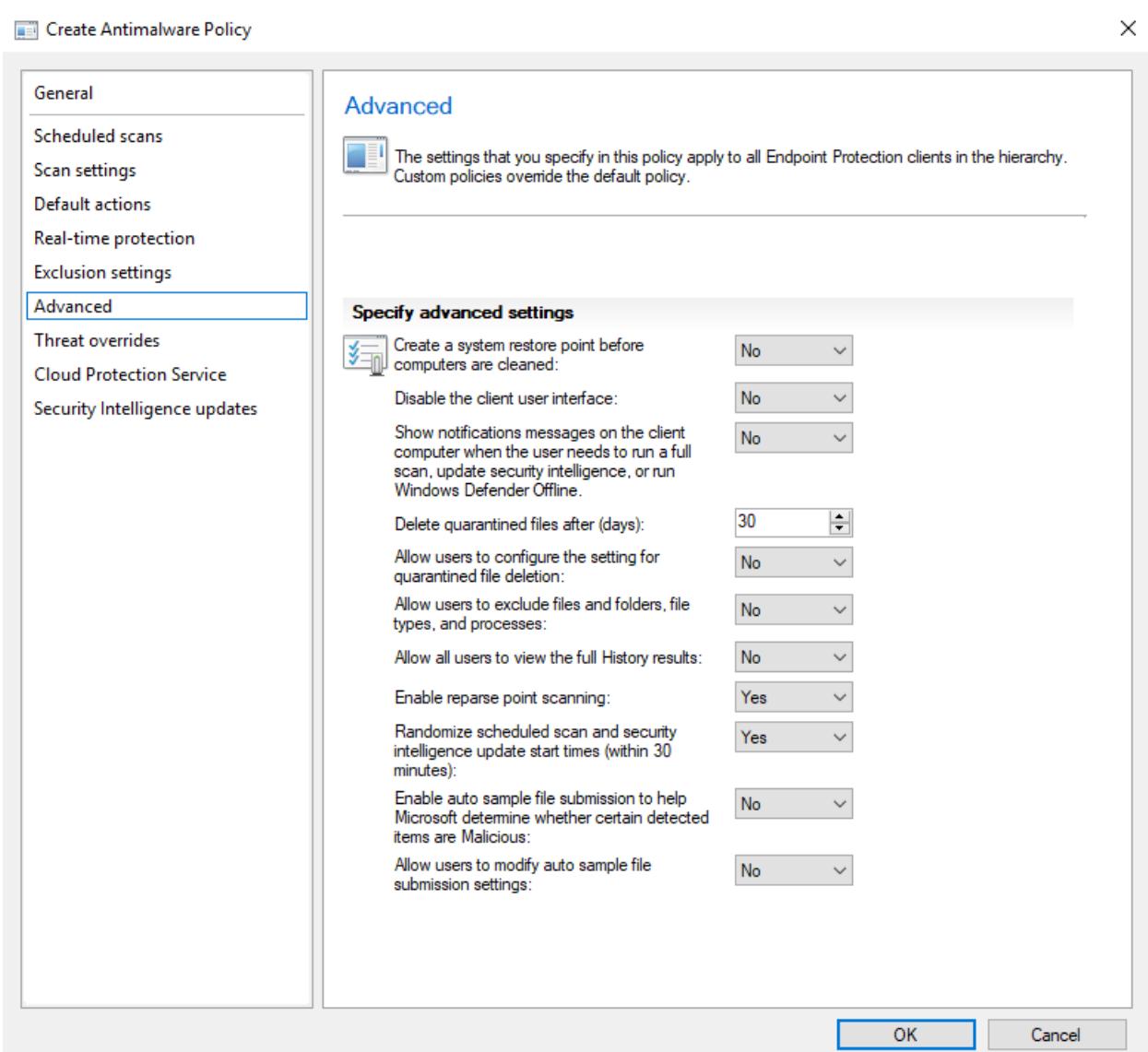
Real-time protection ayarlarımız içerisinde dikkatlice yapılandırmamız gereken sekmelerden en kritik olanı diyebilirim. Endpoint lerimizdeki dosya veya uygulamaların aktivitesini, davranışsal analizi aktif edebileceğimiz , Network tabanlı exploit lere karşı koruma sağladığımız ve gelen/ giden dosyaların taranıp taranmayacağı belirleyeceğimiz ayarların bulunduğu bölümdür.



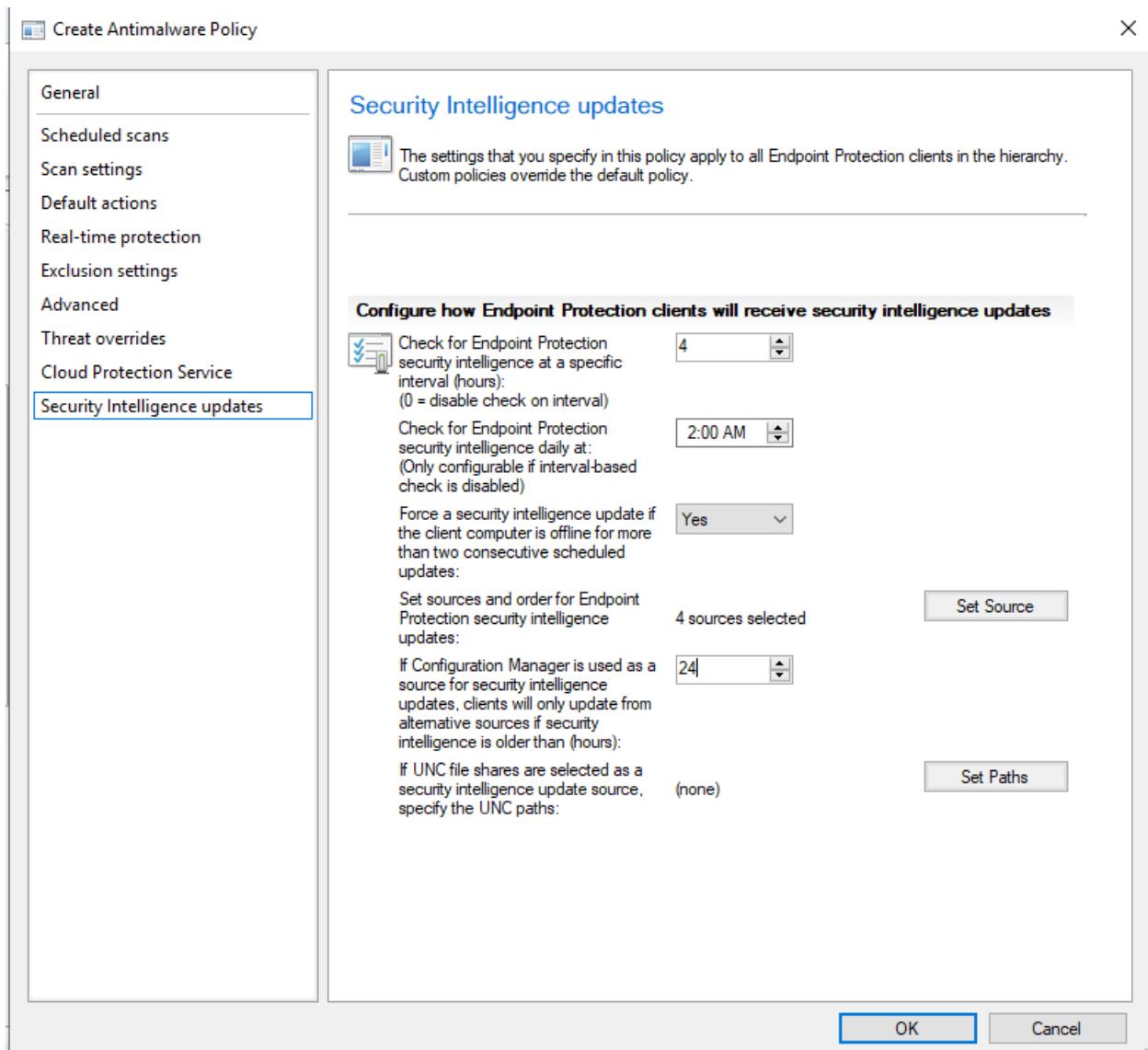
Exclusion Settings sekmesinde ise taranmasını istemediğimiz dosya, dizin vb. var ise tanımlayabiliyoruz.



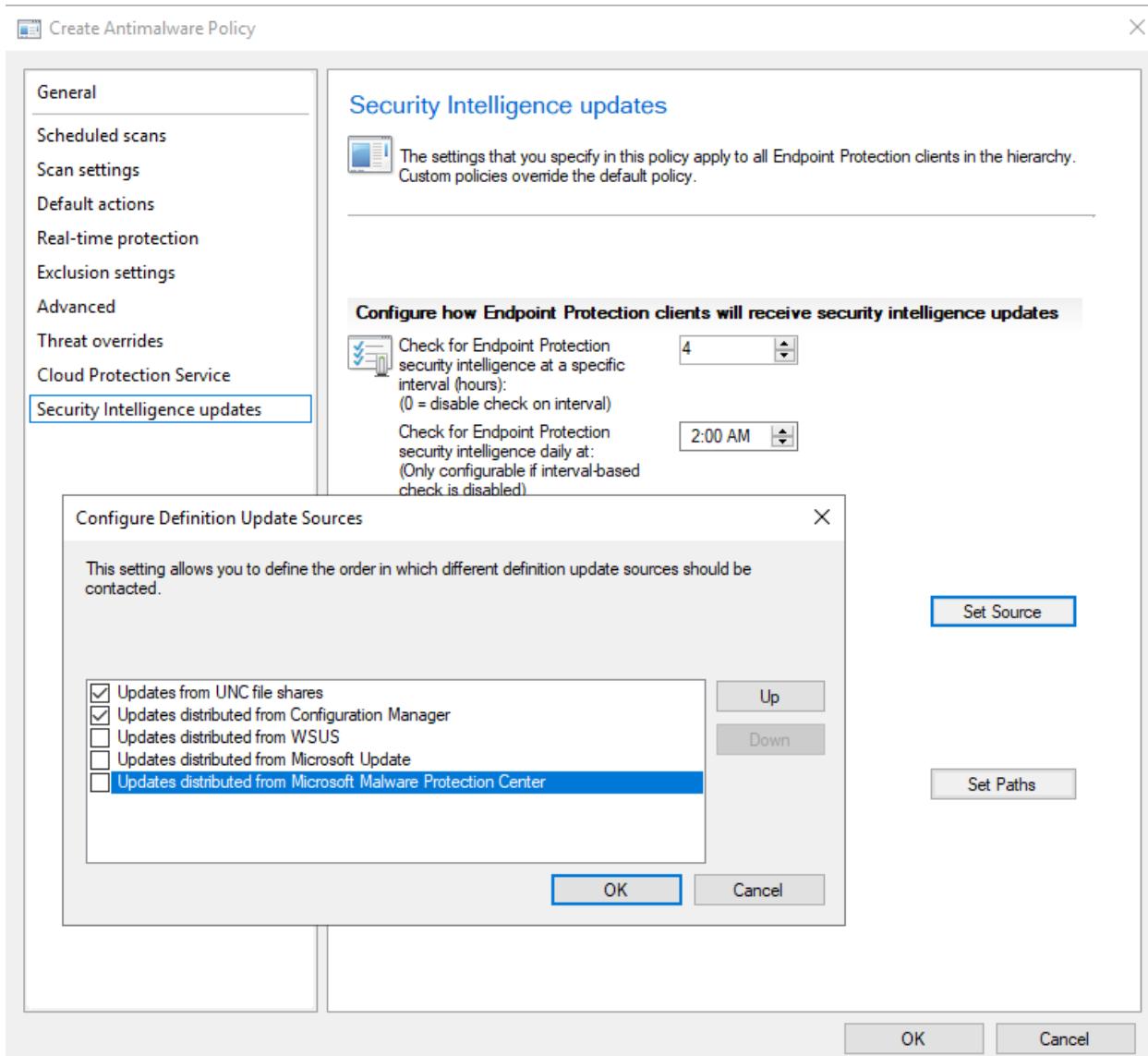
Advanced sekmesinde ise bir tarama başlatıldığında son kullanıcıya bunu pop-up çıkarıp gösterecek miyiz ? Yakalanan bir zararlı temizlenmeden önce restore point oluşturacak mıyız ? Kullanıcıya bu zararlıyı silme için yetki verecekmiyiz? Karantinaya alınan bir zararlıyı ne zaman sileceğiz ? gibi ayarları yapılandırabiliyoruz.



Security Intelligence Updates sekmesinde ise endpointlerin kaç saatte bir kontrol edileceği ayarını belirliyoruz. Bu bölümde yapılandırmamız gereken kritik bir ayar bulunmaktadır. **Set Source** butonunu tıklayarak hangi kaynaklardan bu update lerin alınacağını belirliyoruz.



Örneğimde ilk seçenek olarak UNC Path' den kontrol etmesini ve değişiklik var ise ilgili update leri almasını istiyorum. İkinci seçenek olarak SCCM' i seçiyorum.

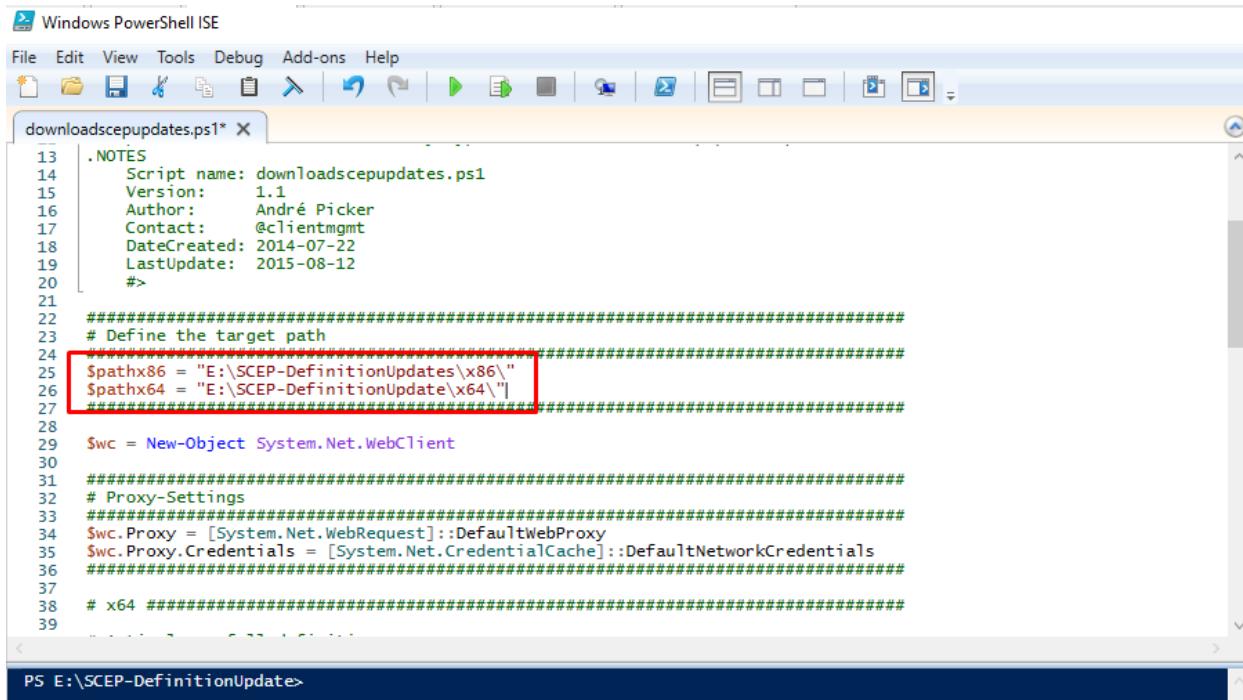


Bu noktada akillara şu soru gelmektedir. UNC Path belirttiğim gibi hoş ama nasıl otomatik olarak güncellemeleri indirip sunucu ve istemcilere göndereceğiz ?

İlk olarak aşağıdaki linkte yer alan Powershell Script' i indiriyoruz ve yazana teşekkür etmeyi unutuyoruz.

<https://gallery.technet.microsoft.com/scriptcenter/SCEP-Definition-Updates-to-fde57ebf>

Yapımıza göre ilgili paketlerin indirileceği bölümü değiştiriyoruz.



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
downloadsepupdates.ps1* X
13 .NOTES
14     Script name: downloadsepupdates.ps1
15     Version: 1.1
16     Author: André Picker
17     Contact: @clientmgmt
18     DateCreated: 2014-07-22
19     LastUpdate: 2015-08-12
20     #>
21
22 ######
23 # Define the target path
24 #####
25 $pathx86 = "E:\SCEP-DefinitionUpdates\x86\"  
$pathx64 = "E:\SCEP-DefinitionUpdate\x64\"|  
#####
26 # Proxy-Settings
27 #####
28 $wc = New-Object System.Net.WebClient
29
30 #####
31 # Proxy-Settings
32 #####
33 $wc.Proxy = [System.Net.WebRequest]::DefaultWebProxy
34 $wc.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials
35
36 #####
37 # x64 #####
38
39
```

PS E:\SCEP-DefinitionUpdate>

İlgili Powershell Script' i sürekli manuel çalıştırılamayacağıma göre Task Schedular ile bu bölümü otomatize ediyoruz.

Create Task

X

General Triggers Actions Conditions Settings

Name: SCEP Definition Updates

Location: \

Author: HD\sccmadm

Description:

Security options

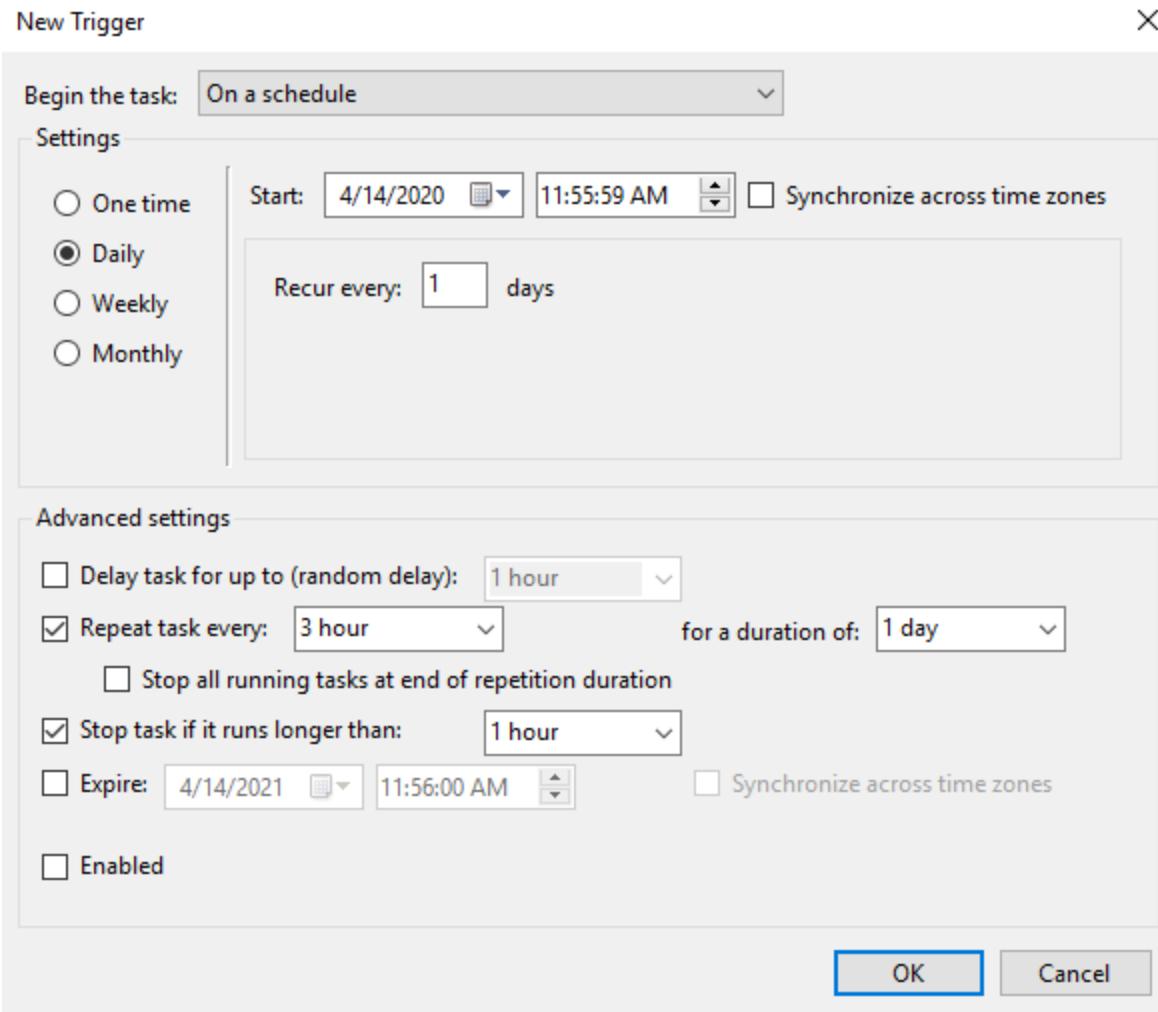
When running the task, use the following user account:
HD\sccmadm [Change User or Group...](#)

Run only when user is logged on
 Run whether user is logged on or not

Do not store password. The task will only have access to local computer resources.
 Run with highest privileges

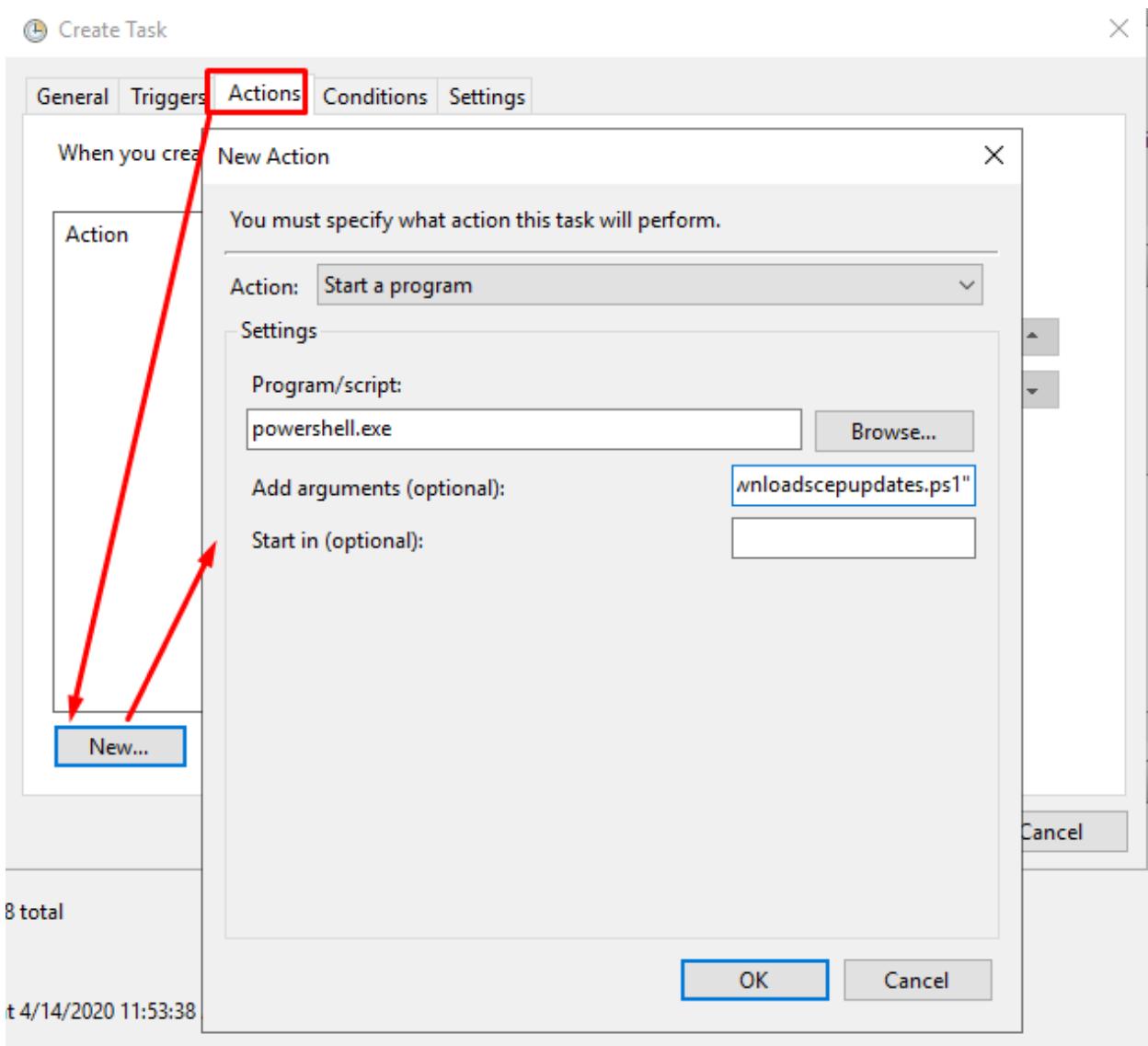
Hidden Configure for: Windows Vista™, Windows Server™ 2008

[OK](#) [Cancel](#)

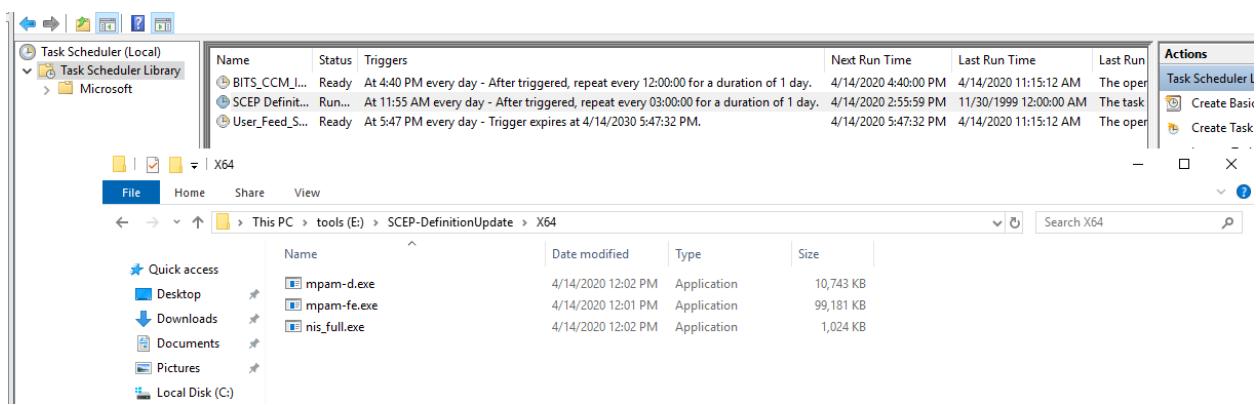


Action kısmında scriptimizi tanımlıyoruz.(Yapınza göre editlemeyi unutmayın)

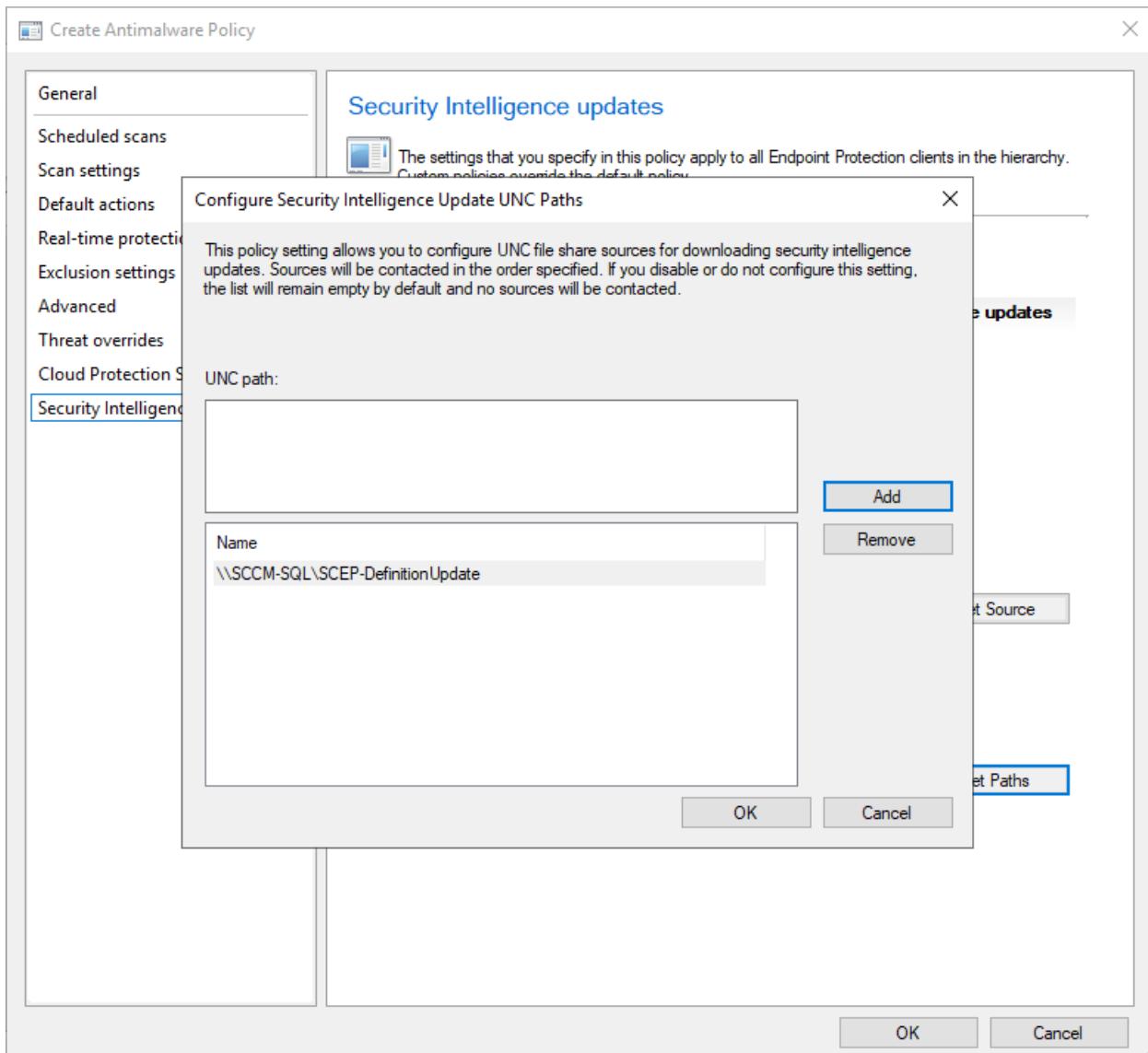
-file "E:\SCEP-DefinitionUpdate\downloadscepupdates.ps1"



Test için manuel olarak çalıştırıyorum ve başarılı şekilde ilgili dosyalarımın indirildiğini görüyorum.



Daha sonra ilgili Path i aşağıdaki UNC Path bölümünde tanımlıyorum.



Yapilandırmamızı tamamladıktan sonra Antimalware Policy ayarını ilgili Collection' lara dağıtmayı unutmayın.

The screenshot shows the SCCM interface with the following details:

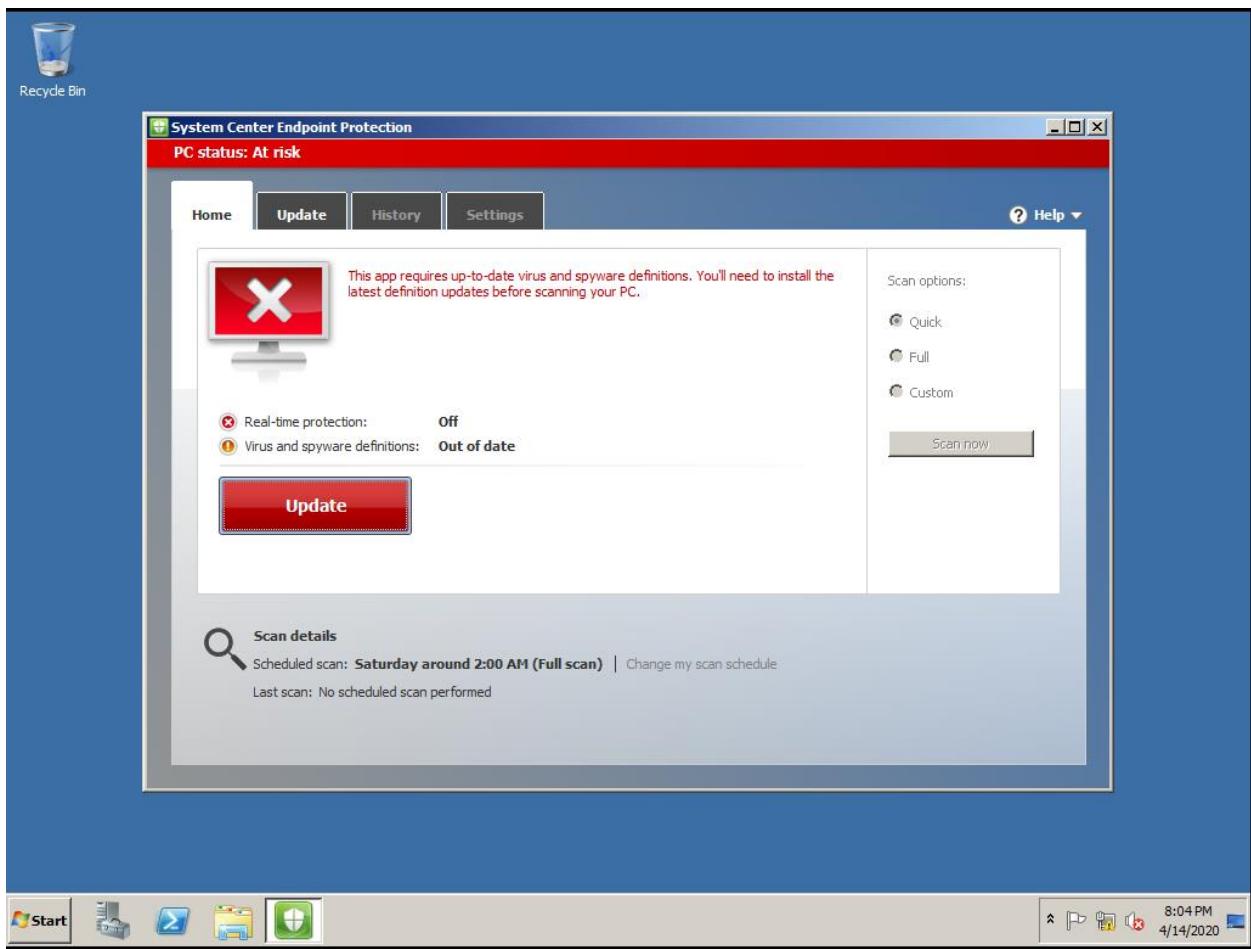
- Top Bar:** System Center Configuration Manager (Connected to HDI - HD Merkez) (Evaluation, 1/3 days left)
- Toolbar:** Home, Create, Import, Saved Searches, Increase Priority, Decrease Priority, Export, Copy, Refresh, Merge, Delete, Deploy, Set Security Scopes, Properties.
- Breadcrumb:** Assets and Compliance > Overview > Endpoint Protection > Antimalware Policies
- Left Navigation:** Assets and Compliance (User Collections, Device Collections, Asset Intelligence, Software Metering, Compliance Settings, Endpoint Protection (Antimalware Policies, Windows Defender Firewall Policies, Windows Defender ATP Policies, Windows Defender Exploit Guard, Windows Defender Application Guard)), Assets and Compliance (Software Library, Monitoring, Administration, Community).
- Table:** Antimalware Policies 2 items

Icon	Name	Type	Order	Deployments	Description
<input checked="" type="checkbox"/>	Default Client Antimalware Policy	Default	10000	0	Settings that apply to all clients in the hierarchy, and can be modified.
<input checked="" type="checkbox"/>	Windows_Defender_Policy	Custom	1	0	

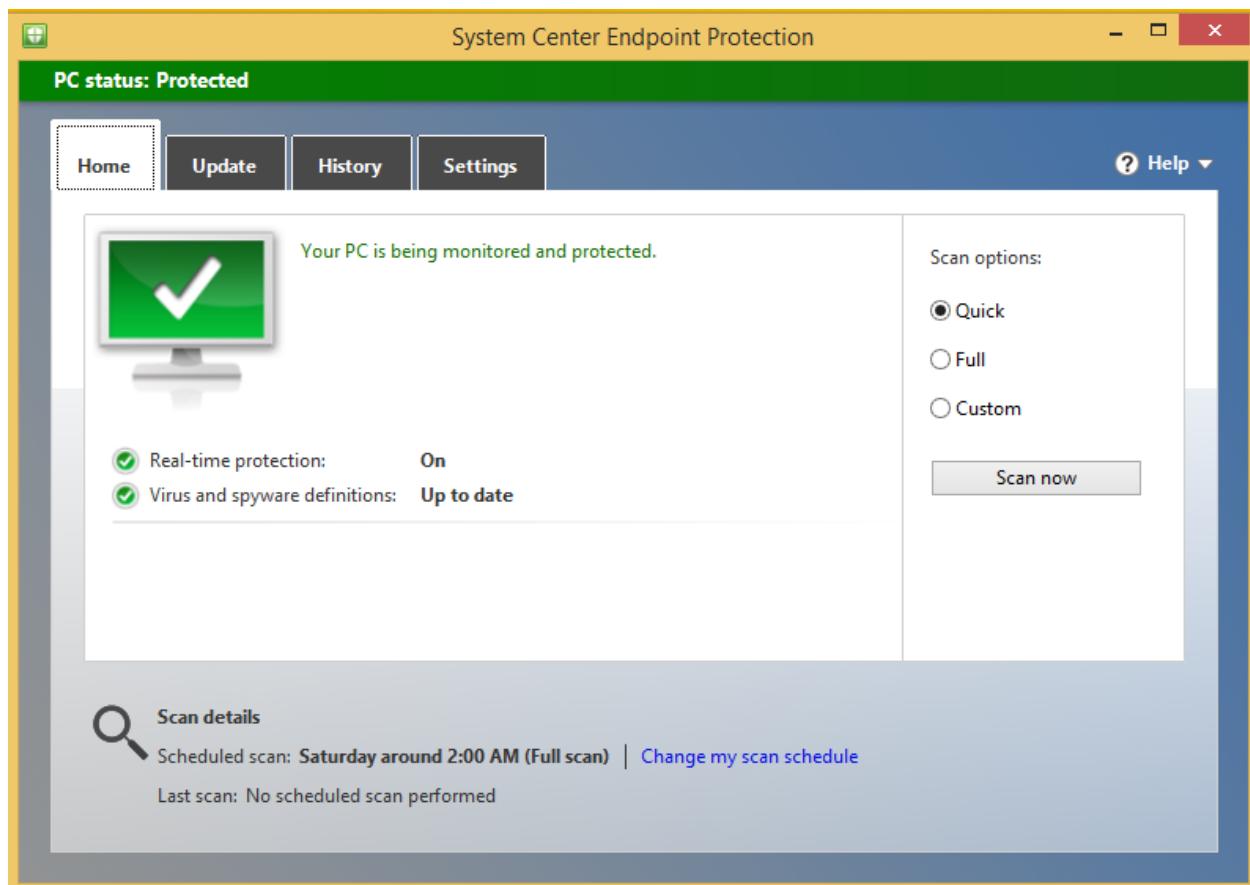
- Context Menu (for Windows_Defender_Policy):**
 - Increase Priority
 - Decrease Priority
 - Export
 - Copy
 - Merge
 - Refresh F5
 - Delete Delete
 - Deploy
 - Set Security Scopes
 - Properties
- File Properties:**

Date Created:	4/14/2020 12:13 PM
Created By:	HD\sccmadm
Date Modified:	4/14/2020 12:13 PM
Modified By:	HD\sccmadm
- Bottom:** Ready, Summary, Deployments.

Windows Server 2008 R2 sunucumda Endpoint Protection ajanının yüklediğini görüyorum fakat güncel değil.



Update butonunu tıklıyorum ve başarılı şekilde ilgili UNC Path' den güncellemerin çekildigini gözlemliyorum.



Windows Defender Exploit Guard

Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

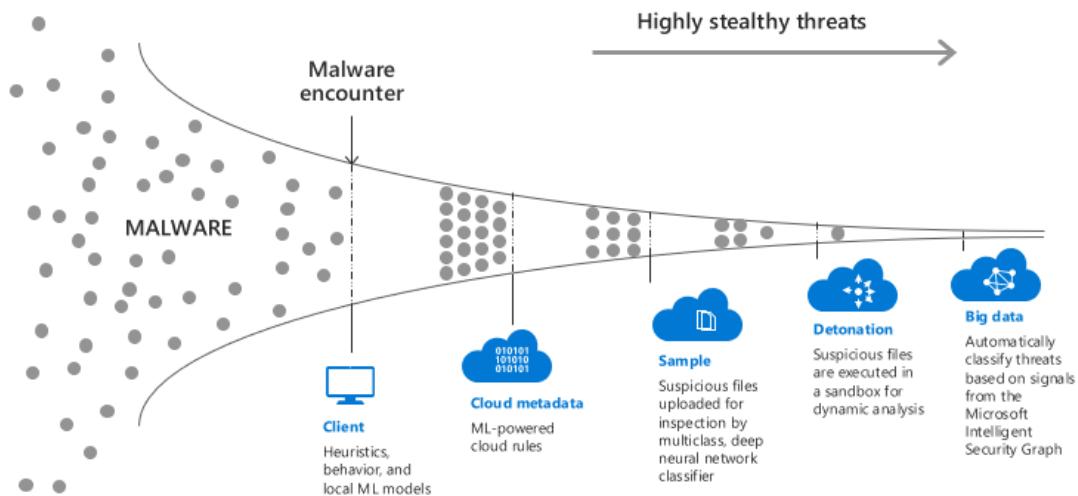
Microsoft Defender Antivirus

- Windows Server 2016
- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

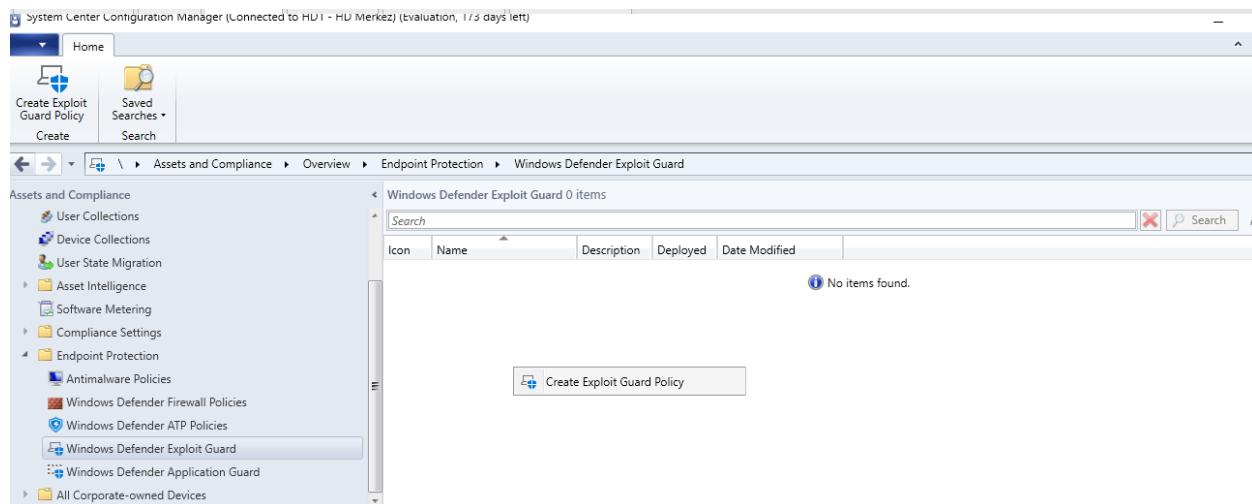
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

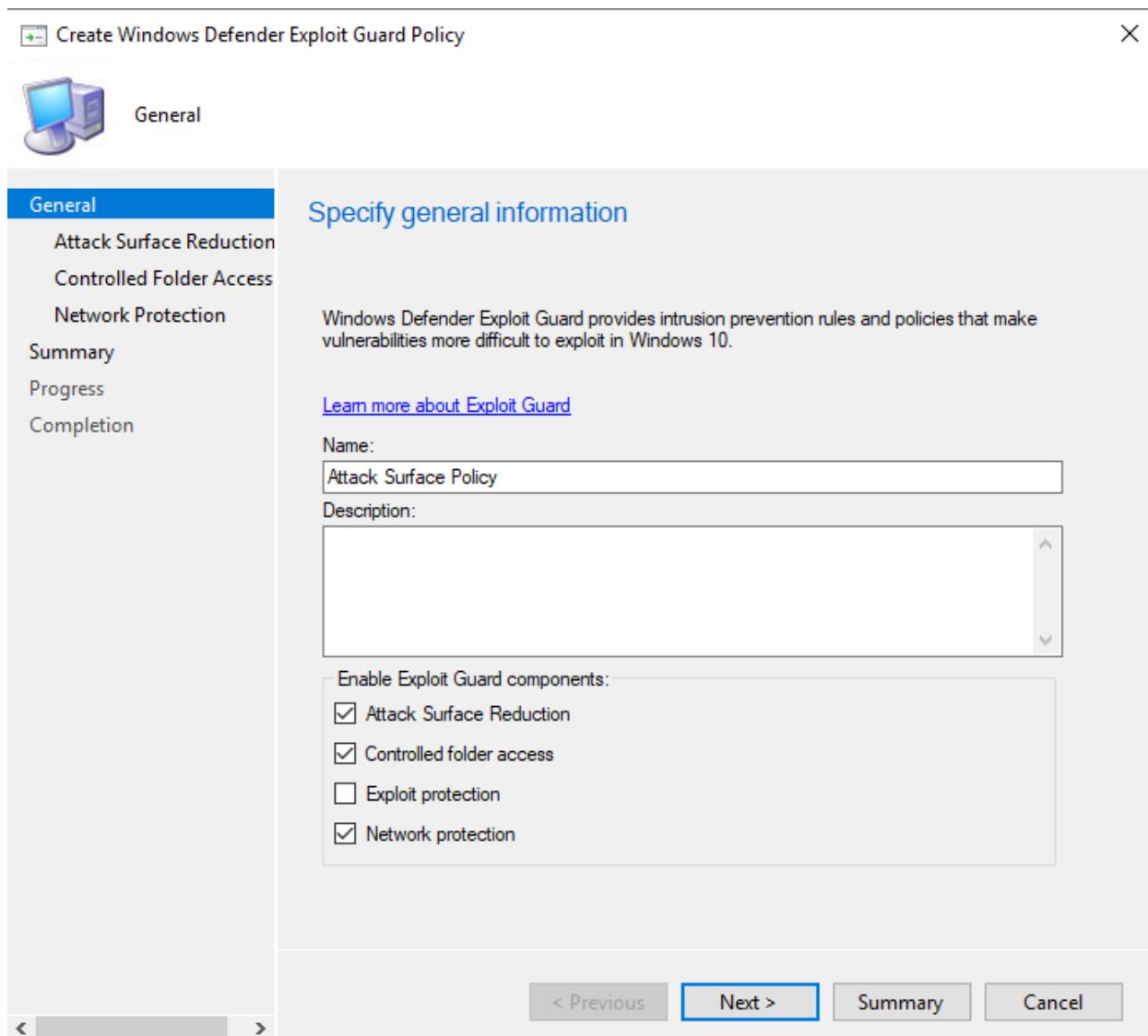
Exploit Guard özelliği sayesinde özellikle sıfırıncı gün saldırıları, kötü amaçlı yazılımlar, sofistike saldırılar, imza tabansız zararlılar, Fileless tehditler, Ransomware atakları, Hardware lere karşı yapılan saldırılar ve daha fazlasına karşı koruma sağlamaktadır.



Kısa açıklamadan sonra yapılandırmamız gereklidir. SCCM konsolunuza açıyoruz ve Endpoint Protection sekmesi içerisinde yer alan Windows Defender Exploit Guard sekmesine geliyoruz ve **Create Exploit Guard Policy** ile işlemimize başlıyoruz.



Kuralımıza isim veriyoruz ve Exploit Guard içerisinde neleri aktif etmek istiyorsak ilgili seçenekleri seçiyoruz.



Dikkatli Okuyunuz ! Batman olmaya çalışmayız, projedeki bir hata sizi Joker yapabilir 😊

- Yapılandırmaya kesinlikle **Audit Mode** olarak başlayınız.
- İlgili ayarları tüm yapıya dağıtmadan testlerinizi var ise test ortamında yapınız.
- Eğer bu proje bir ürünü diğer ürünlle değiştirme(Replacement) ise exclusionları çok dikkatli şekilde eski ortamdan yeni ortama taşıyınız.
- Hypervisor katmanında bir koruma sağlıyorsanız ve bunu MDATP + Scep ile yeniliyorsanız Performans testlerini yapmanızı tavsiye ederim. İlgili testte başlamadan önce özellikle Storage üzerindeki I/O değerlerini not alınız ve Full Scan vb testleri başlatıp tekrar değerleri kontrol ediniz.

Not: Tüm ayarların açıklamasına tek tek girmeyeceğim. Lütfen detay bilgi için erişimi çok zor olan Bing' den yararlanınız.

Attack Surface Reduction

System Center Configuration Manager (SCCM) Current Branch (CB)

Desteklenen İşletim Sistemleri

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

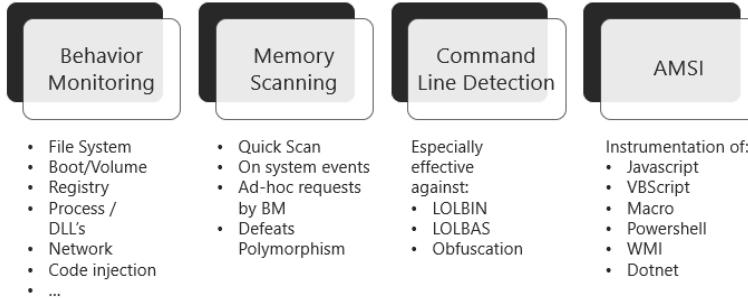
Microsoft Defender Antivirus

- Windows Server 2016
- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

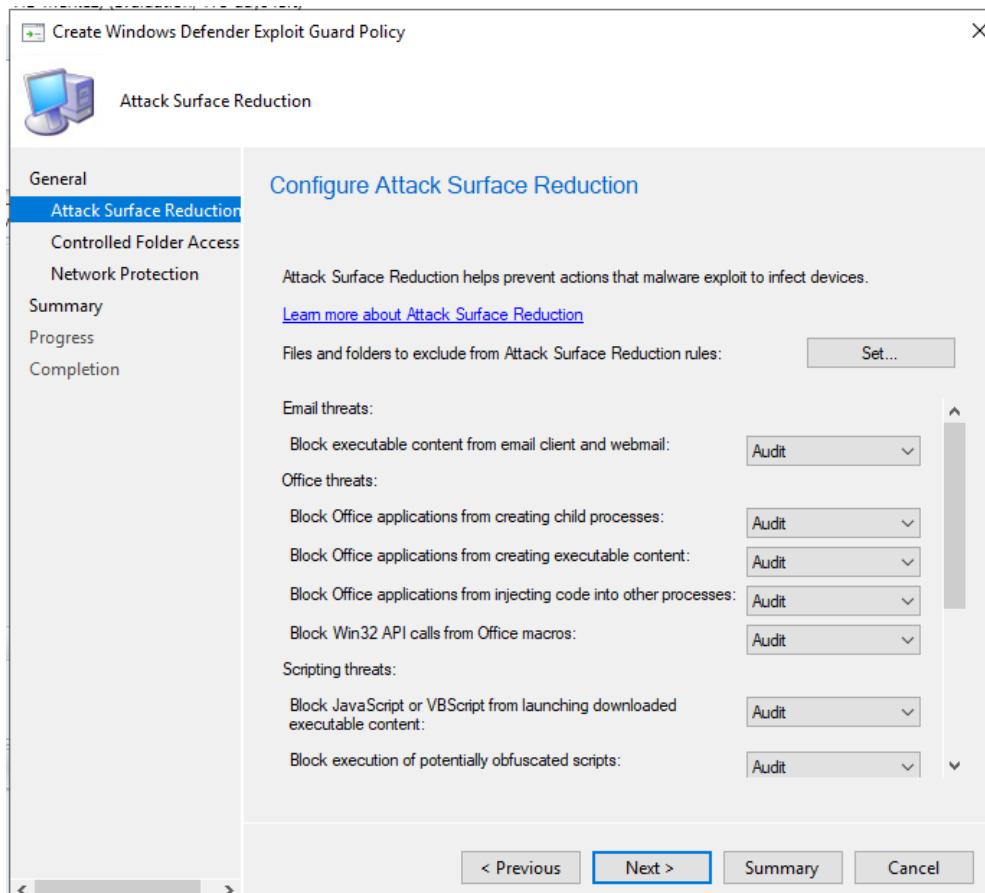
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

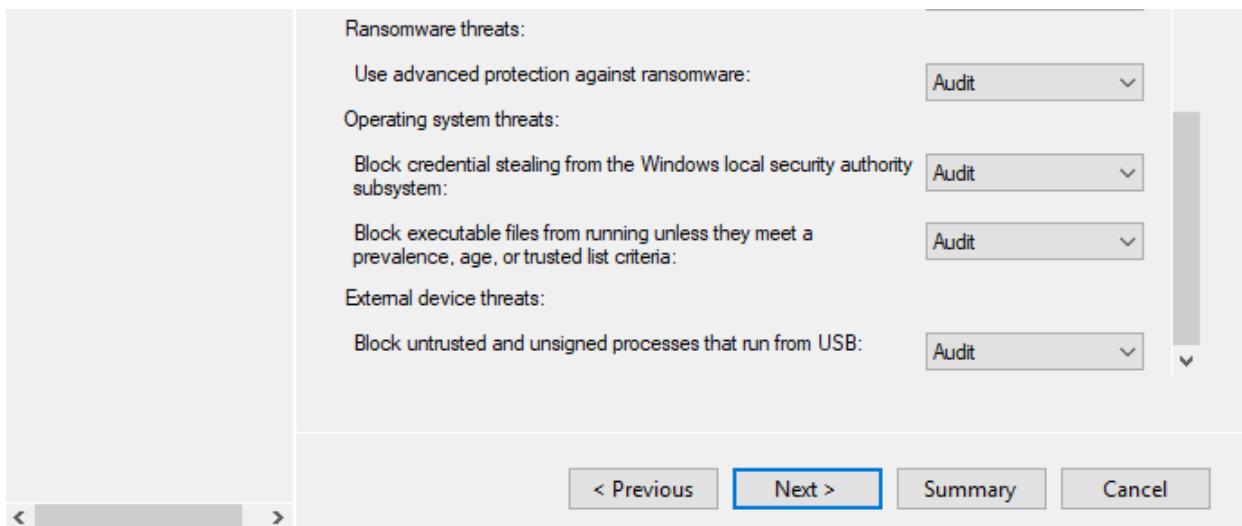
ASR ile birlikte aşağıdaki atak vektörlerine karşı koruma sağladığımızı belirtmişik.



Zararlılar en fazla ofis dökümanları, phishing saldıruları, Javascript, Vbscript ler üzerinden bulaşmaktadır. Attack surface reduction özelliği ile birlikte malware lere karşı etkin koruma sağlayabiliyoruz.



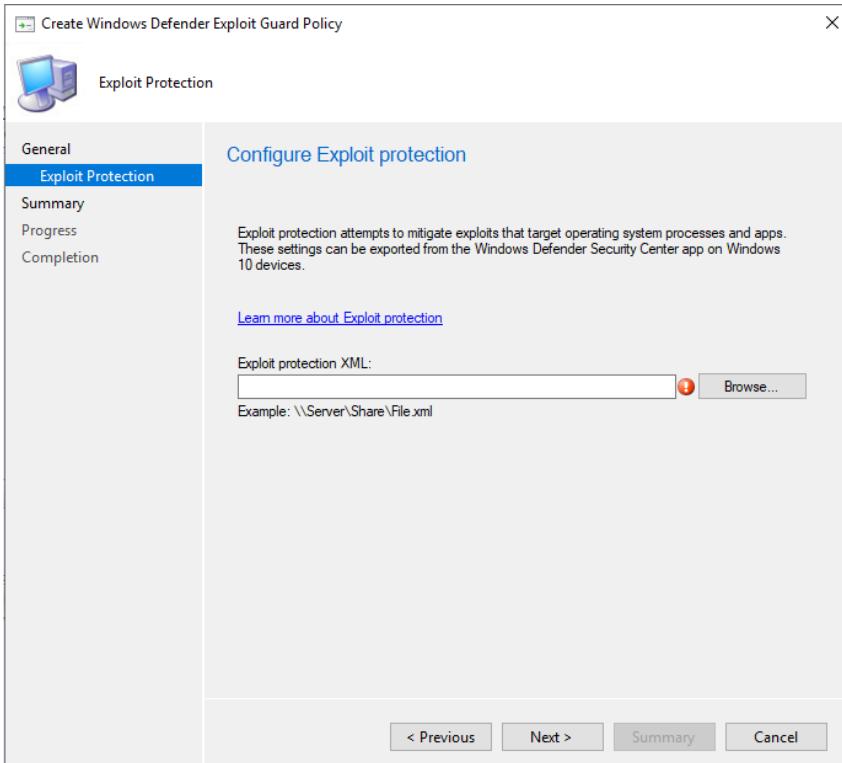
Eğer yapınız içerisinde harici cihazları(USB, External HDD vb) bloklamak istiyorsanız ayarımızı burada yapıyoruz.



<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

Exploit Protection

Bildiğiniz üzere exploit protection Enhanced Mitigation Experience Toolkit(EMET) in yerine geldi diyebiliriz. Bildiğiniz üzere EMET 31 Temmuz 2018' de expire oldu. Hali hazırda EMET kullanıyorsanız ilgili kuralı **ConvertTo-ProcessMitigatinPolicy -EMETFile.xml -outfilepath file.xml** şeklinde export edip Exploit protection içerisinde tanımlayabilirsiniz.



<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/exploit-protection>

Control Folder Access

Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

Microsoft Defender Antivirus

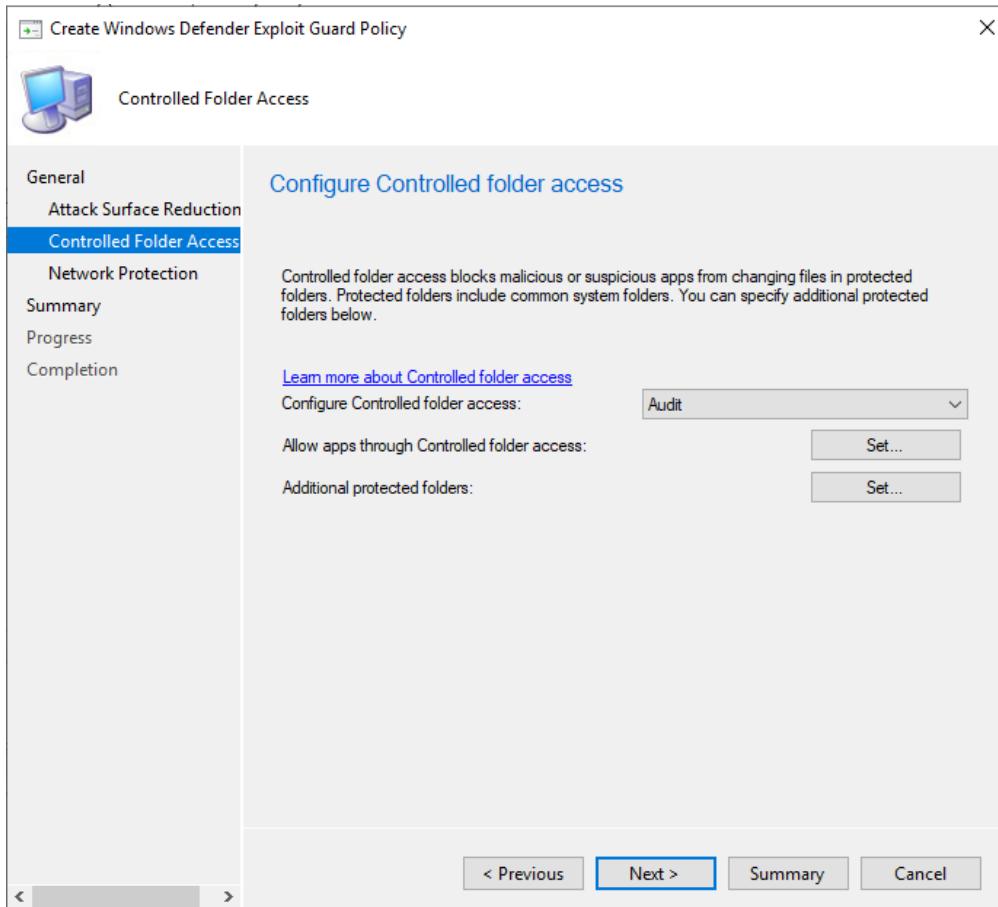
- Windows Server 2016

- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

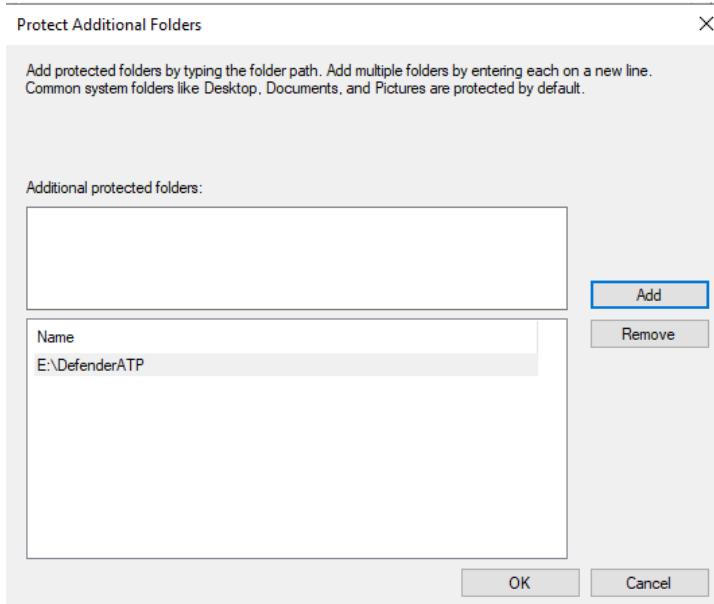
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

Son senelerde bildiğiniz üzere Ransomware atakları ciddi artış gösterdi ve firmalar çok ciddi veri ve para kaybettiler. İlgili ayar ile bu atağın önüne geçebiliyoruz. Bu bölümde Audit Disk Sector Only seçeneğini de seçebilirsiniz ve bir sonraki aşamada Block rule olarak Block Disk Sector şeklinde yapılandırabilirsiniz. Bu tamamen neyi ne kadar korumak istediğiniz ve yapınız ile alakalı.



Örneğin **Additional protected folders** seçeneği ile korumak istediğiniz dosyaların dizinlerini burada tanımlayabilirsiniz. Aynı kısıtlamayı uygulamalar içinde yapabiliyoruz.



<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders>

Network Protection

Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB) running:

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

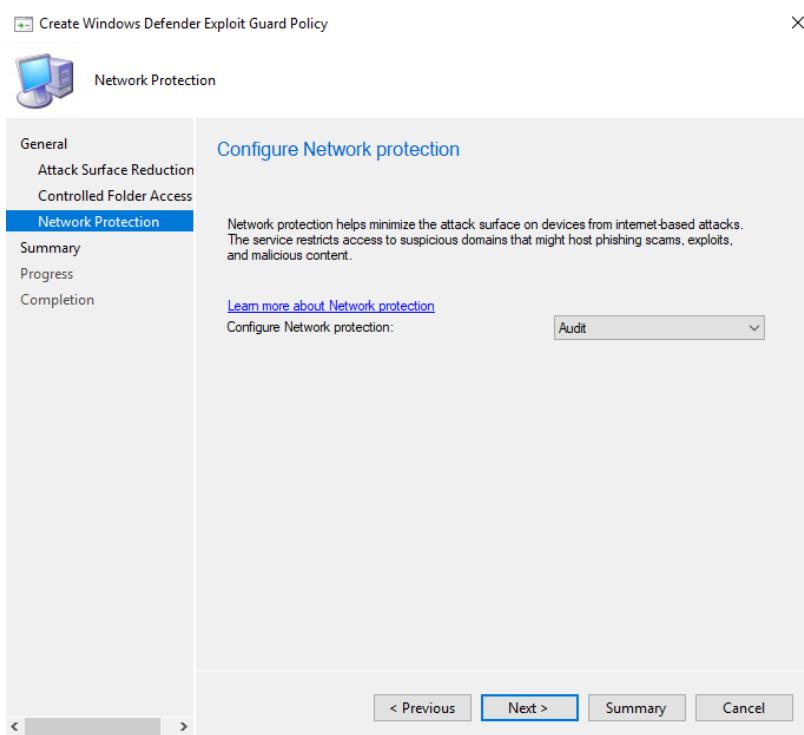
Microsoft Defender Antivirus

- Windows Server 2016
- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

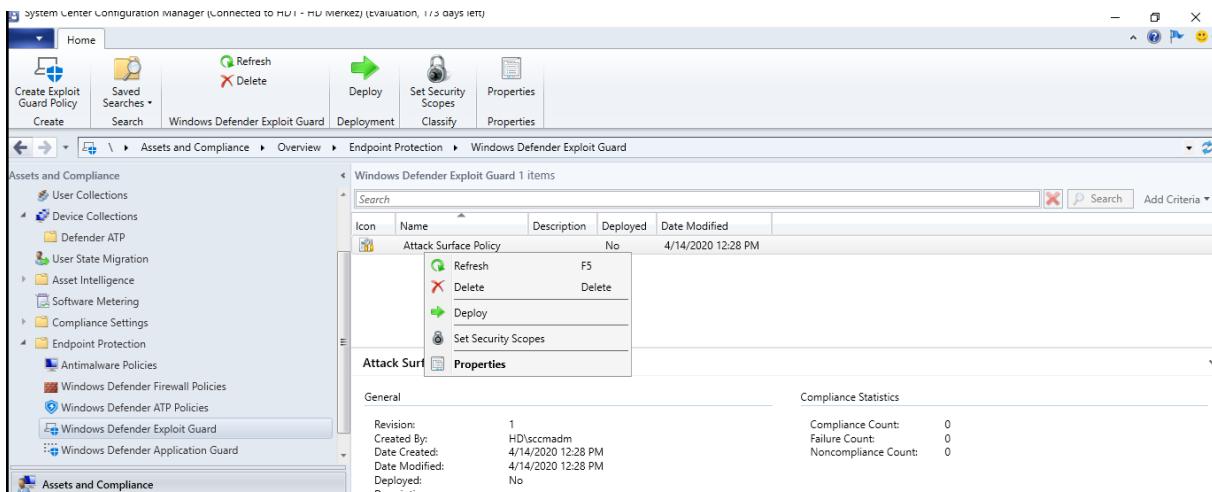
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

İlgili seçenekin yapılandırılması halinde reputasyonu düşük olan Domain lerle olan bağlantı engellenecektir. Bu ayarı aslında Microsoft Defender Smartscreen' in devamı gibi düşününebilirsiniz. Microsoft Defender Smartscreen bizi yemleme saldırısı, zararlı içeren web siteleri, uygulamalar, indirilen ve potansiyel tehdit oluşturan tehditlere karşı korumaktadır.



Bu adımla birlikte artık yapılandırmamızı tamamlıyoruz. Son olarak da ilgili ayarı ilgili Collection' a uyguluyoruz.



<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/network-protection>

Windows Defender ATP Policies

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Advanced Threat

Desteklenen İşletim Sistemleri

- Windows 10, version 1909, 1809 , 1803, 1709
- Windows Server 2019

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201909>

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201903>

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201809>

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201803>

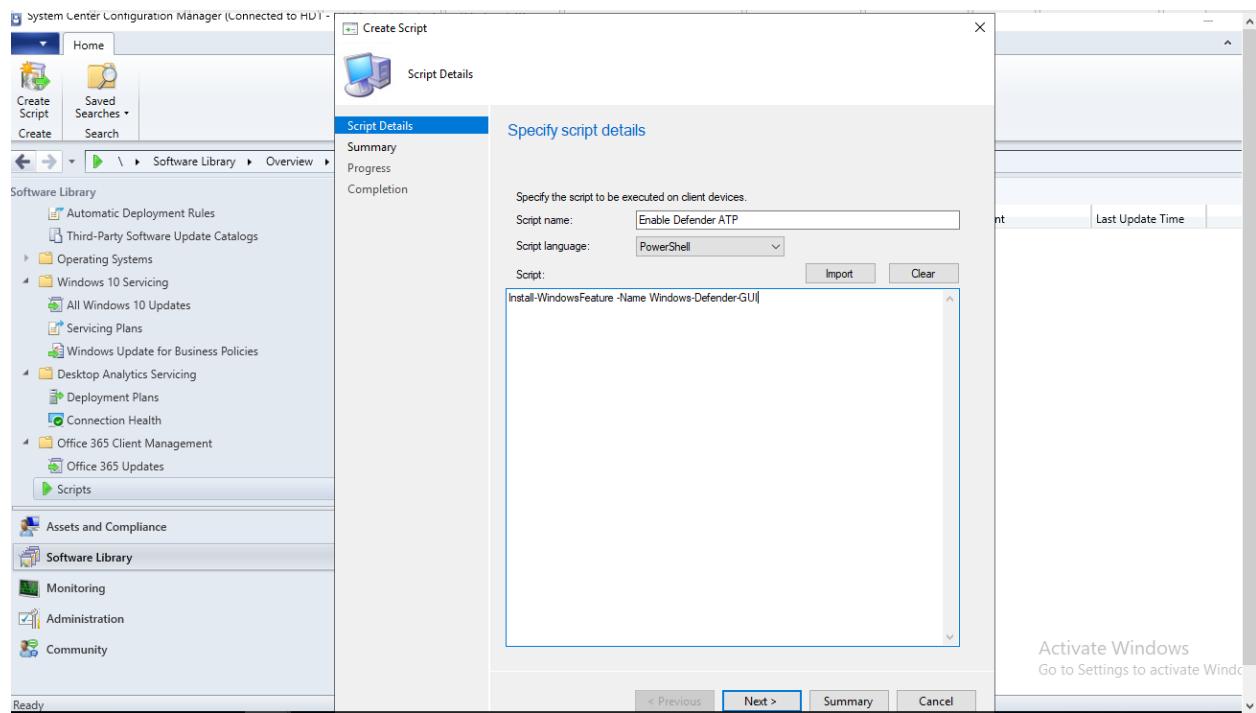
<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201709>

İlgili bölüm Windows 10 Onboarding başlığı altında anlatılmıştır.

Windows Server 2016 Defender ATP Kurulumu

Bir önceki bölümümüzde Windows Server 2008 R2 SP1, 2012 R2 , Windows 7/8.1 işletim sistemlerine SCEP ajanı kurulumunu anlatmıştım. Windows Server 2016 işletim sisteminde hali hazırda bu özellik

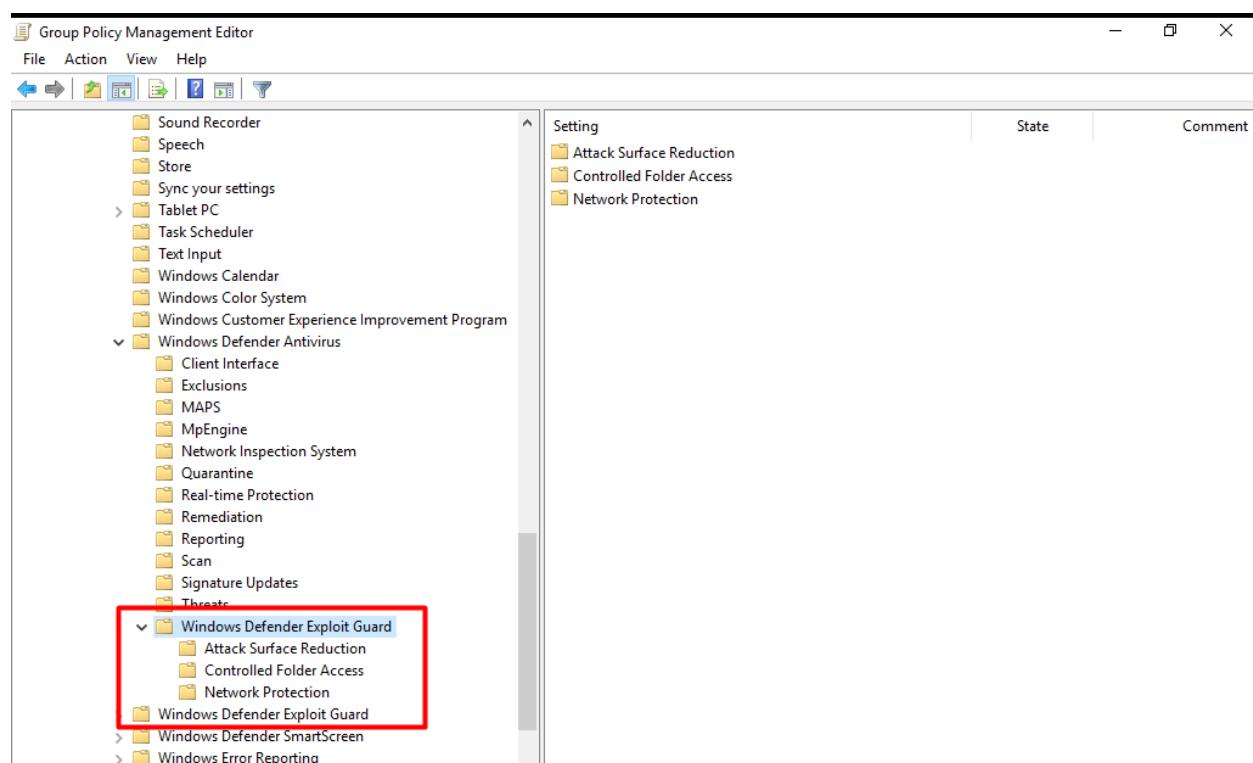
mevcut fakat aktif olmadığını varsayılmı. Yine imdadımıza SCCM yetişiyor bu sefer Powershell' den küçük bir yardım alağacağız. Bildığınız üzere SCCM içerisinde script özelliği mevcut ve Powershell' i destekliyor. Bende bunu kullanarak Defender ATP' yi aktif hale getireceğim. **Install-WindowsFeature - Name Windows-Defender-GUI** komutunu script içine kopyalıyorum, elbette script dili powershell olmalı. Daha sonra next next diyerek işlemimi tamamlıyorum ve ilgil script i Windows Server 2016 Collection larına dağıtıyorum. Bu işlemden sonra sunucuların restart edilmesi gerekmektedir !!!



Group Policy ile Windows Defender Exploit Guard Yapılandırma

Attack Surface Reduction

Configure Attack Surface Reduction Rules



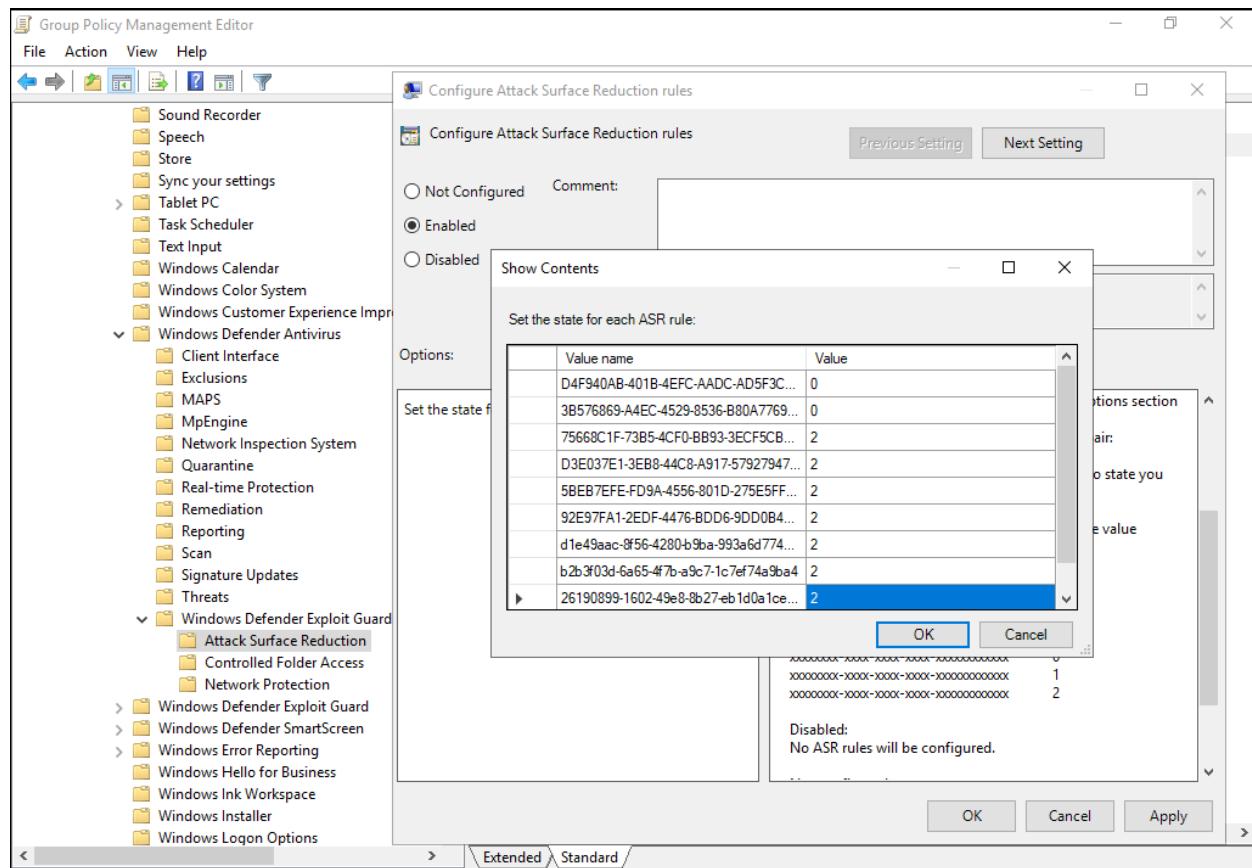
Group Policy ile yapılandırma kısmı malesef biraz daha meşakatlı diyebilirim. Bu bölümde de değere 2 vererek başlangıç için Audit olarak yapılandırıyorum.

Rule Description	Rule GUID
Block all Office applications from creating child processes	D4F940AB-401B-4EFC-AADC-AD5F3C50688A
Block Office applications from creating executable content	3B576869-A4EC-4529-8536-B80A7769E899
Block Office applications from injecting code into other processes	75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
Block JavaScript or VBScript from launching downloaded executable content	D3E037E1-3EB8-44C8-A917-57927947596D
Block execution of potentially obfuscated scripts	5BEB7EFE-FD9A-4556-801D-275E5FFC04CC
Block Win32 API calls from Office macro	92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B

Block process creations originating from PSEXEC and WMI commands	d1e49aac-8f56-4280-b9ba-993a6d77406c
Block untrusted and unsigned processes that run from USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
Block only Office communication applications from creating child processes	26190899-1602-49e8-8b27-eb1d0a1ce869

Daha fazlasına aşağıdaki linkten erişebilirsiniz.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

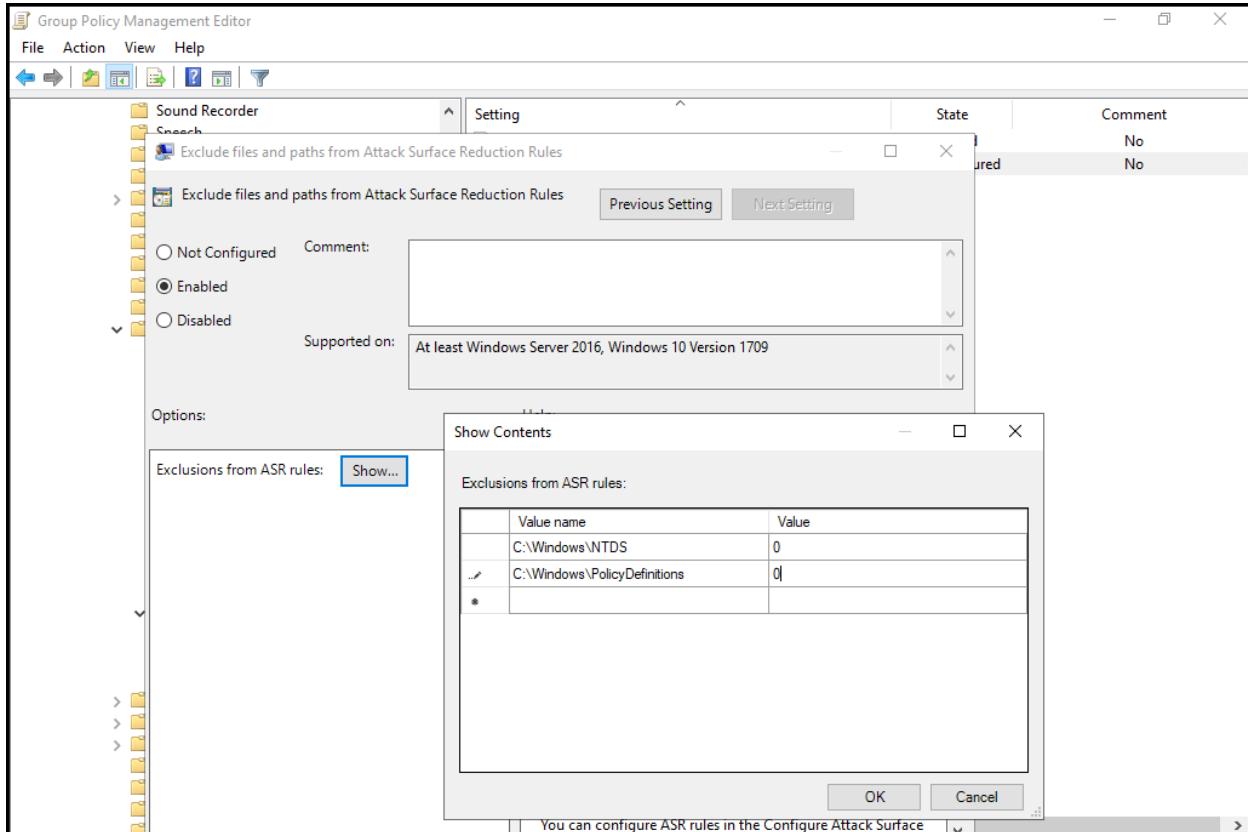


Peki yapılandırmamızı Audit olarak yapılandırdık. Takibini nasıl yapacağız ?

- Event ID 1121 -- blocking mode events
- Event ID 1122 -- audit mode events
- Event ID 5007 -- changing settings events

Exclude files and paths from Attack Surface Reduction (ASR) rules

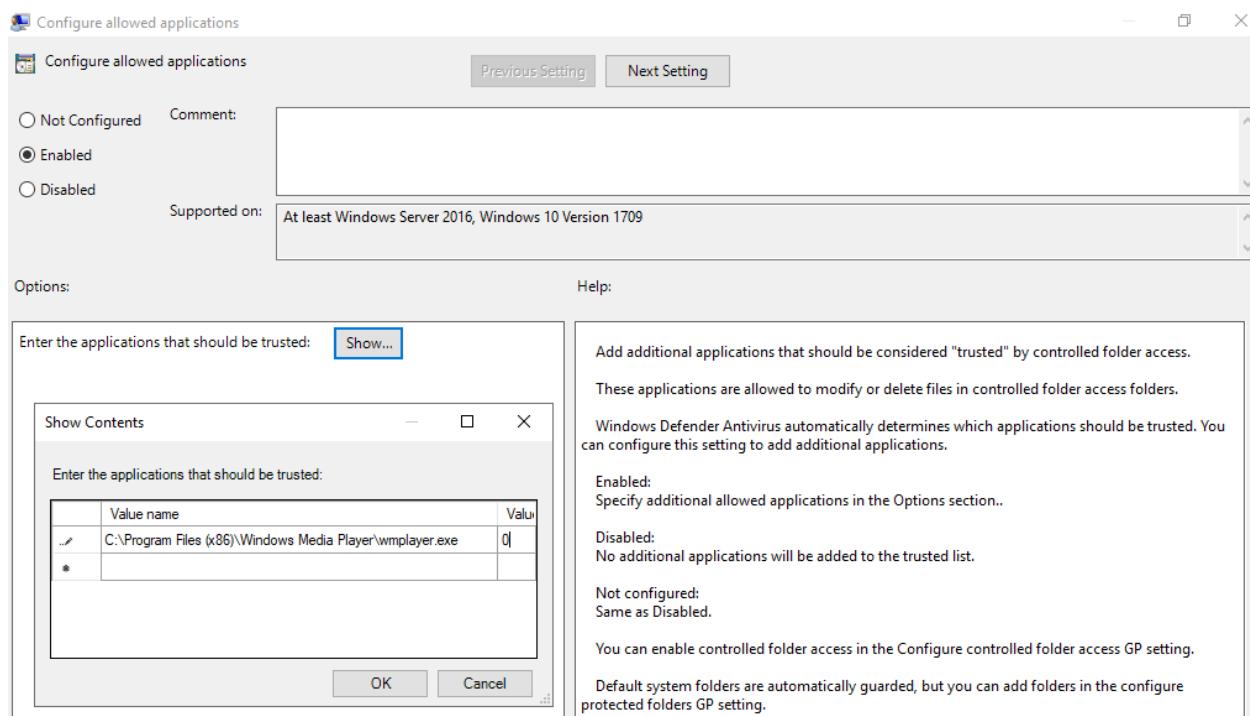
Yapınıza göre ve uygulama sunucularınızın çeşidine göre ASR kuralı için exclusion yazmanız gerekirse aşağıdaki örnekte olduğu gibi yapılandırabilirsiniz.



Controlled Folder Access

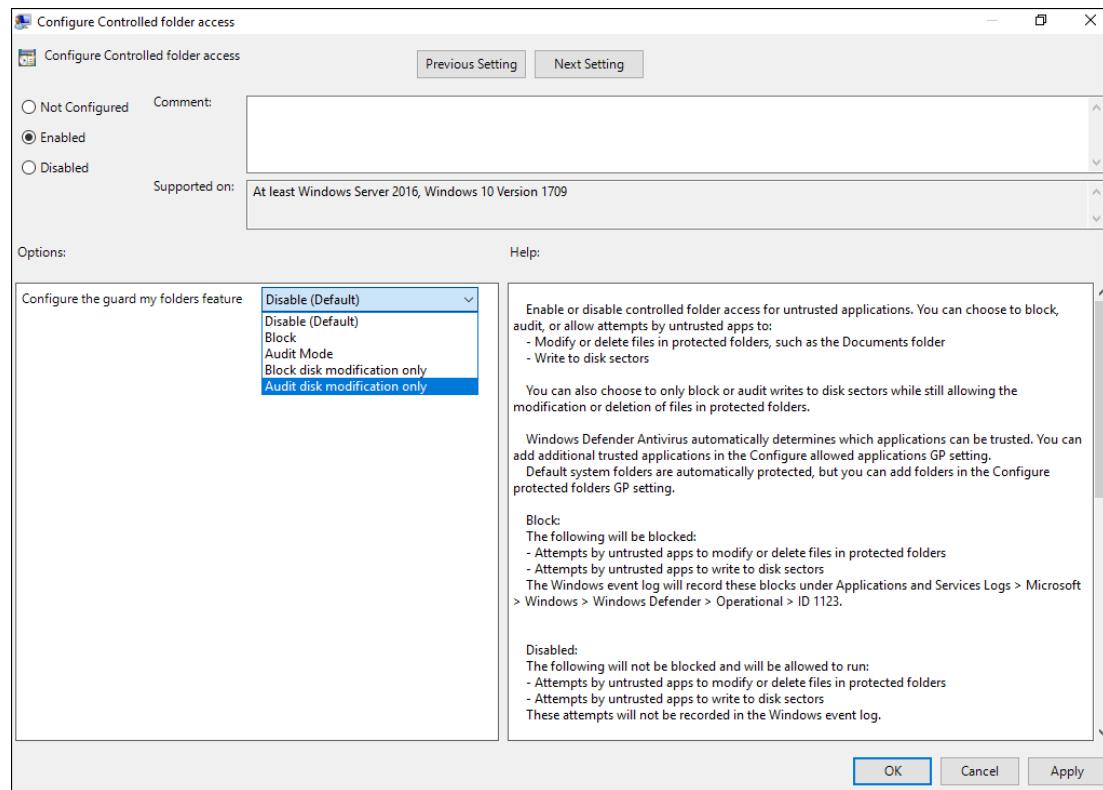
Configure Allowed Applications

Aşağıdaki örnekte olduğu gibi kurumunuza ait kullanılmasına izin vereceğiniz uygulamaları aşağıdaki şekilde belirleyebiliyoruz.



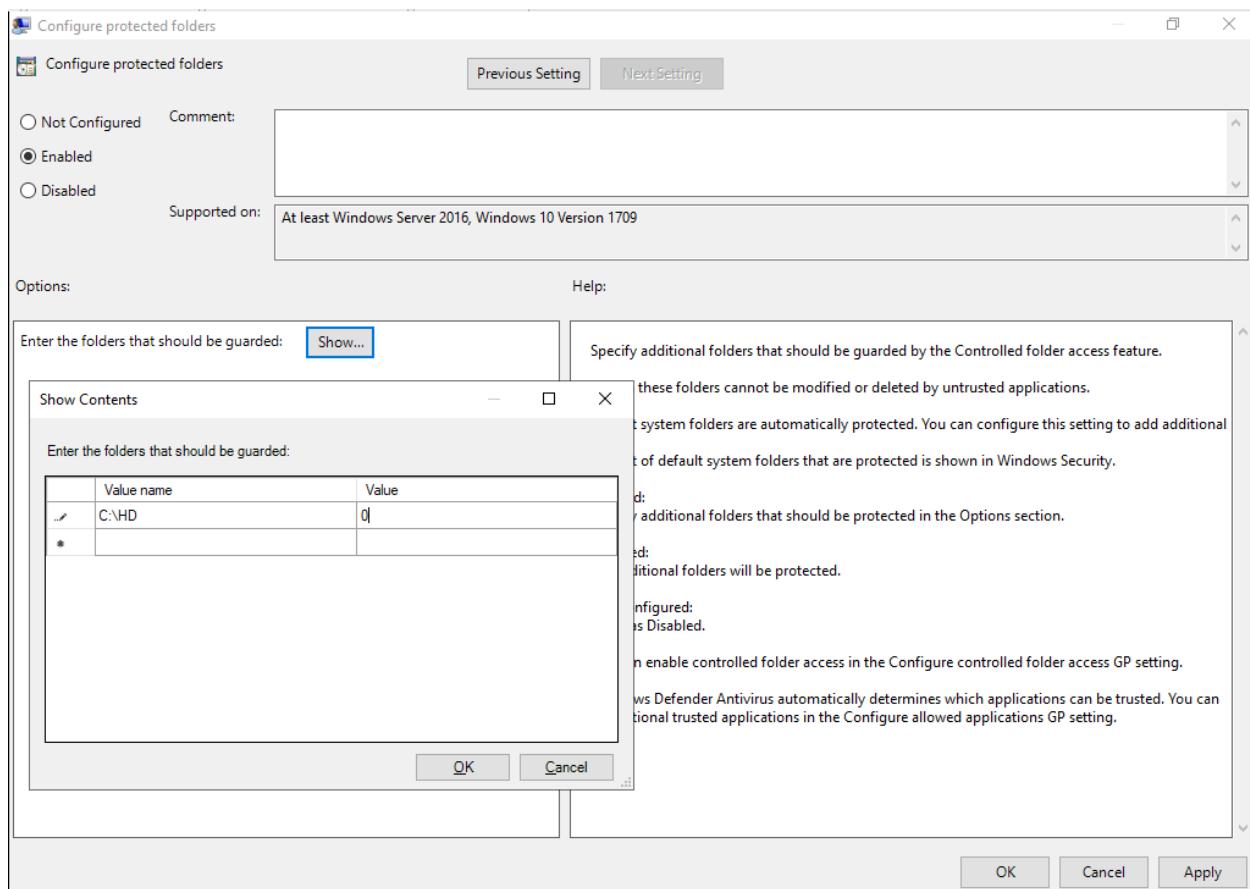
Configure Controlled Folder Access

Bu bölüme Exploit Guard bölümünde debynmiştim. Aynı ayarları Gpo ile de yapılandırabiliyoruz.



Configure Protected Folders

Yapınız içerisinde sizin önemli olan bir klasörün olduğunu varsayıyalım ve bu klasör üzerinde kesinlikle değişiklik yapılmasını istemiyorsanız bu kuralı aktif edebilirsiniz.



Network Protection

Prevent users and apps from accessing dangerous websites

İlgili kuralın aktif edilmesi durumunda reputasyonu düşük, tehlikeli kategoride yer alan domain lerden uygulama indirilmesi engellenmektedir. Audit mode ile başlanmasını tavsiye ederim.

Youtube Videoları

- <https://www.youtube.com/watch?v=6TiHx6Pbqns&t=2s>
- <https://www.youtube.com/watch?v=C5TNKypFNaQ&t=555s>

Faydalanan Kaynaklar

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction-faq>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/next-gen-threat-and-vuln-mgt>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/>
- <https://techcommunity.microsoft.com/t5/microsoft-defender-atp/introducing-a-risk-based-approach-to-threat-and-vulnerability/ba-p/377845>
- <https://techcommunity.microsoft.com/t5/microsoft-defender-atp/bg-p/MicrosoftDefenderATPBlog>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/onboarding#endpoint-detection-and-response>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-attack-surface-reduction#group-policy>
- <https://yongrhee.wordpress.com/>

SON SÖZ

Güvenlik kavramını ele alırken öenmle dikkat etmemiz gereken bir nokta var hiç bir aman %100 güvende olmayacağız. Saldırı ve savunma bir satranç oyunudur. Bunu lütfen aklınızdan hiç bir zaman çıkarmayınız.



Yazmış olduğum bu E-Kitabı genç yaşta Mide Kanserine yenik düşen meslektaşım,dostum ve ustadıma adıyorum. En son konuştuğumuzda Hasanım yeni E-Kitabın ne zaman bitiyor, yayına da artık okuyayı demiştin. Okumanı çok isterdim, yorumlarını duymak güzel olurdu ama olmadığından olmadı güzel kardeşim 😞 Mekanın cennet olsun dostum.....



Bu E-Kitap çok değerli meslektaşım **Uğur DEMİR** anısına ithafen yazılmıştır.

Saygılarımla

Hasan DİMDİK | CEH | MVP | MCT