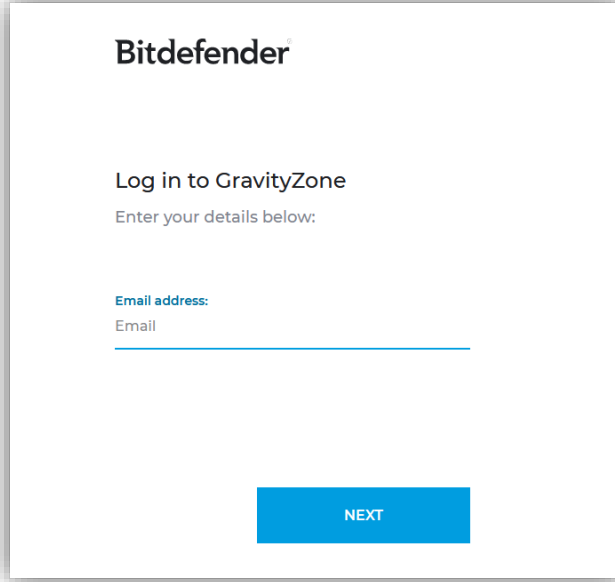


Bitdefender Gravityzone Yönetim Panelinde Dosya Taramadışı Bırakma İşlemi

Bitdefender ürünlerini bilgisayarlara kurduğunuz zaman birtakım engellemeler yapacaktır, bu zararlı dosyalar dışında zararsız dosyaları da içerebilir. Dolayısı ile bir programın zararsız olduğundan emin olduğumuz zaman bu programı veya dosyayı tarama dışı bırakmamız mümkün.

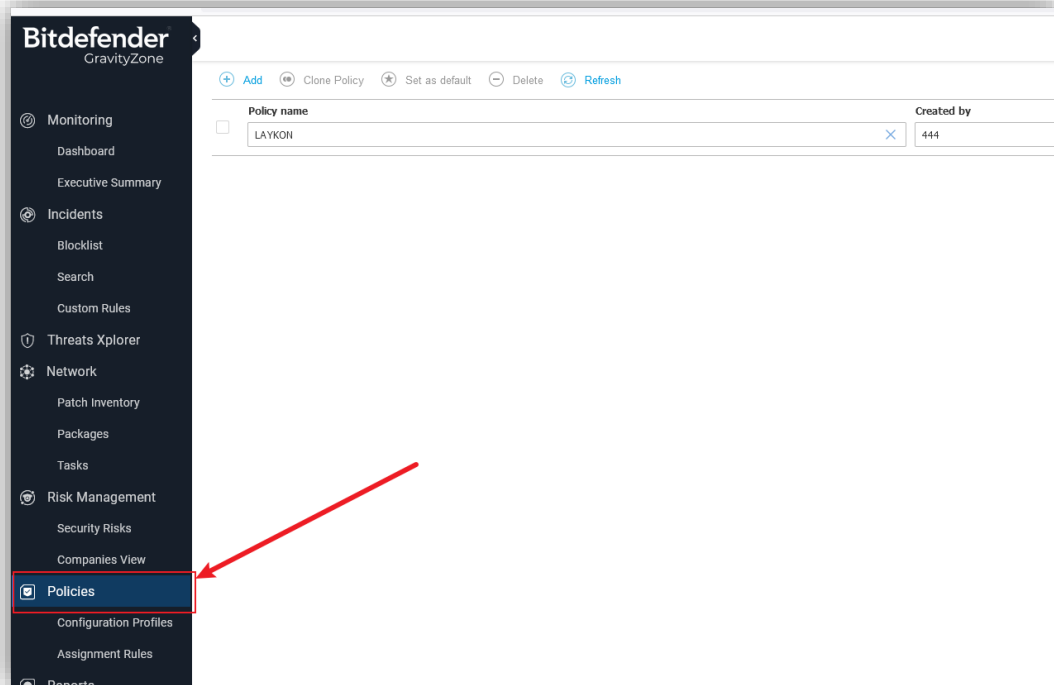
BİR DOSYA VEYA PROGRAMI TARAMA DIŞI BIRAKMAK:

- 1- Bitdefender Gravityzone yönetim paneline giriş yapın:

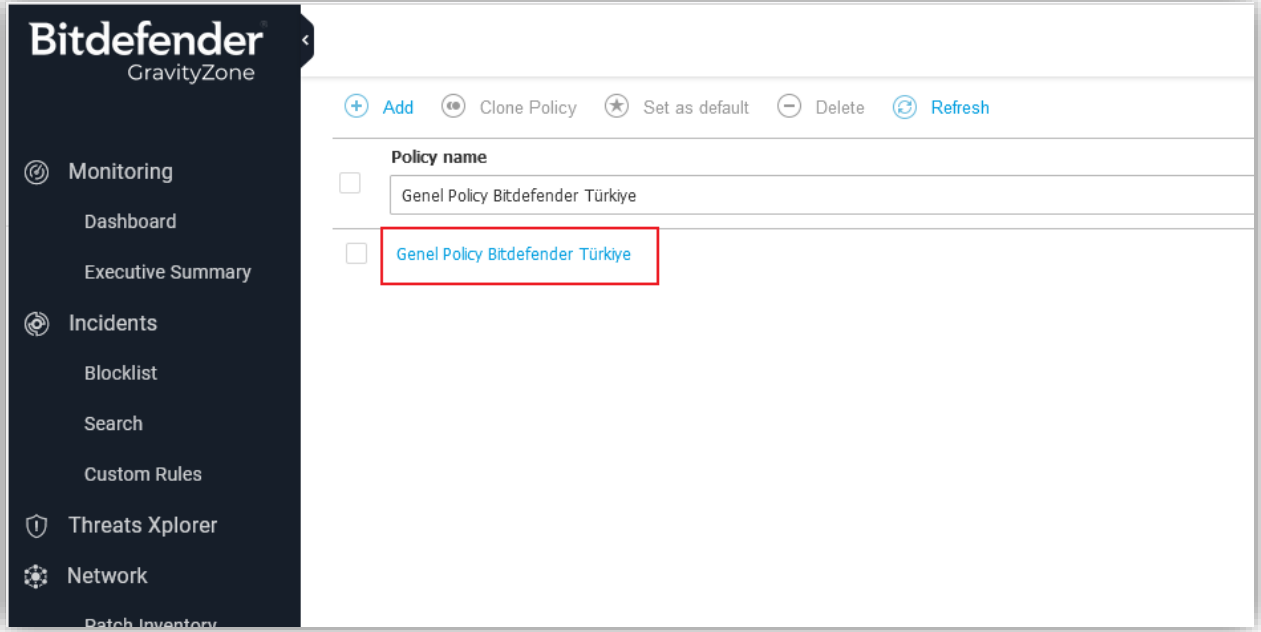


The image shows the Bitdefender GravityZone login interface. At the top, the Bitdefender logo is displayed. Below it, the text 'Log in to GravityZone' is centered, followed by the instruction 'Enter your details below:'. There is a label 'Email address:' in blue, and a text input field with the placeholder 'Email'. At the bottom, there is a blue button labeled 'NEXT'.

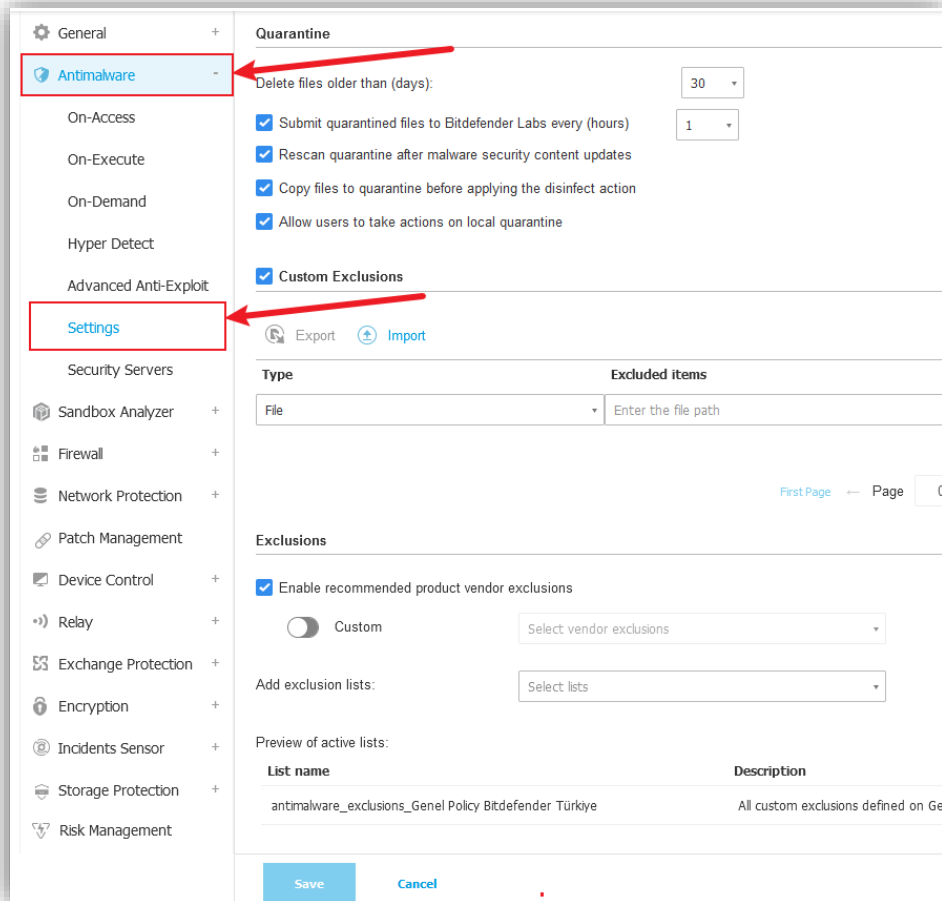
- 2- Sol menüden **policies** kısmına gidin:



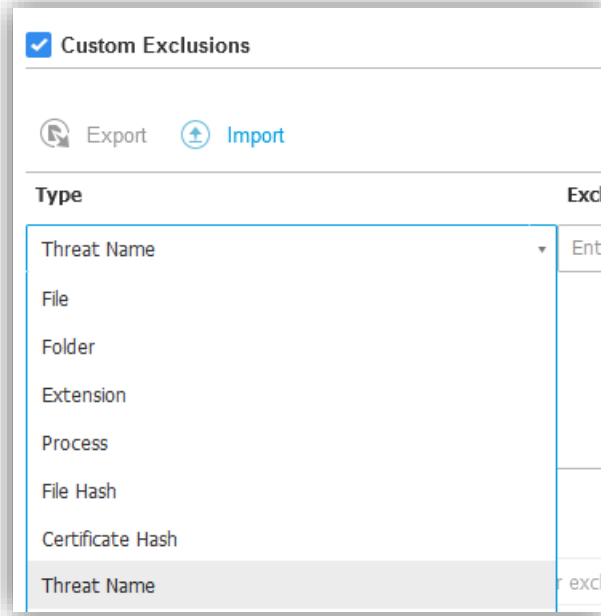
3- Programı eklemek istediğiniz kuralı bulup üzerinde tıklayın:



4- Karşınıza çıkan policy yapılandırma ekranında **Antimalware** kısmında **Settings** bölümü üzerinde tıklayın



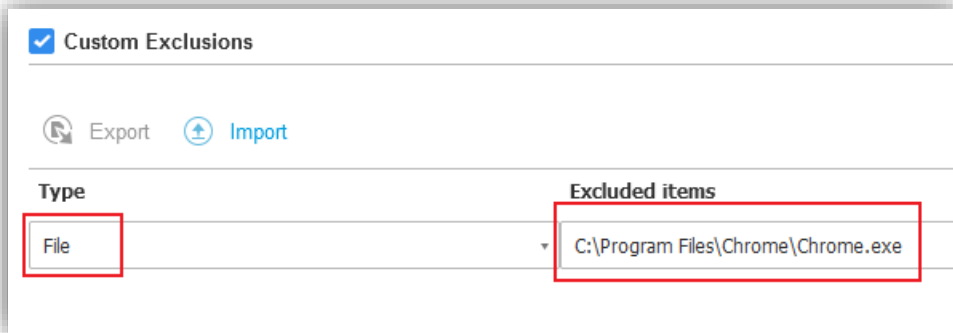
- 5- Bu kısımda **Custom Exclusions** seçeneğinin aktif olmasından emin olun ve aşağıda **Type** bölümü üzerinde tıklayın



- 6- Bu ekranda karşınıza çıkan birtakım seçenekler var bu seçeneklerin açıklaması aşağıdaki gibidir:

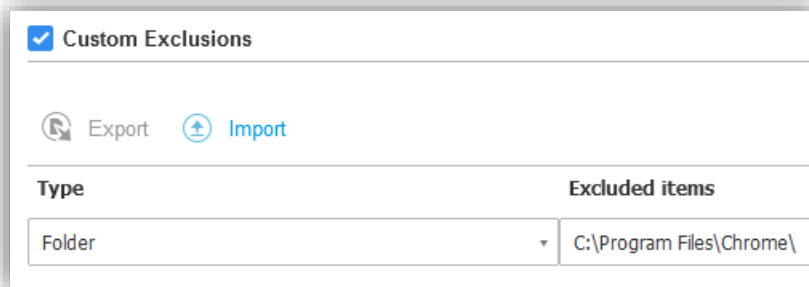
- **File:**

- Tarama dışı bırakmak istediğimiz dosya adresini yazmamız gerekiyor, ilgili makinede dosya konumuna göre girilir



- **Folder:**

- Tarama dışı bırakmak istediğimiz klasör adresini yazmamız gerekiyor



- **Extention:**

- Tarama dışı bırakmak istediğimiz dosya uzantısı yazmamız gerekiyor

☒ Custom Exclusions

 Export

 Import

Export exclusions (available only for saved policies)

Type	Excluded items
Extension	jpg;txt;avi

- **Process:**

- Tarama dışı bırakmak istediğimiz Process adresini yazmamız gerekiyor

☒ Custom Exclusions

 Export

 Import

Type	Excluded items
Process	C:\Program Files\Chrome\Chrome.exe

- **File Hash:**

- Tarama dışı bırakmak istediğimiz dosyanın SHA256 HASH kodunu girmemiz lazım.

☒ Custom Exclusions

 Export

 Import

Export exclusions (available only for saved policies)

Type	Excluded items
File Hash	• 3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

- **Certificate Hash:**

- Tarama dışı bırakmak istediğimiz sertifika HASH kodunu yazıyoruz.

☒ Custom Exclusions

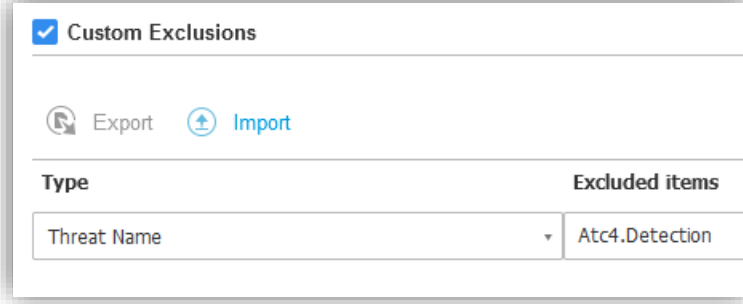
 Export

 Import

Type	Excluded items
Certificate Hash	a909502dd82ae41433e6f83886b00d4277a32a7b

- **Threat Name:**

- Tarama dışı bırakmak istediğimiz tehdit ismini giriyoruz
Bu isim Bitdefender tarafından belirleniyor ve tehditlerinin ismini karantina bölümünde bulmanız mümkün

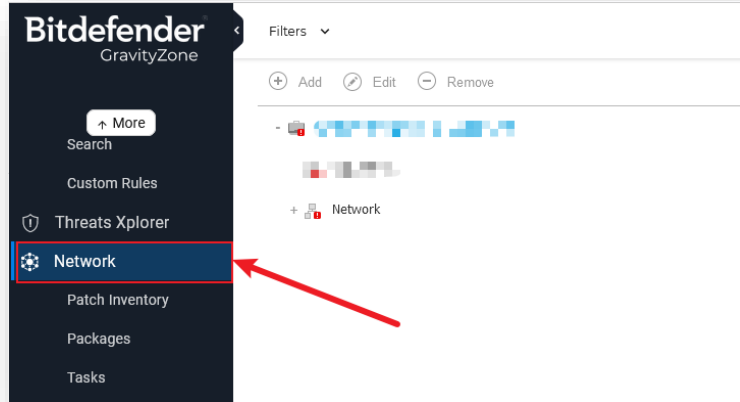


Bu adımlar bitince Policy kaydedin ve kısa bir süre sonra makinelerde engellenen programı tekrar çalıştırın.

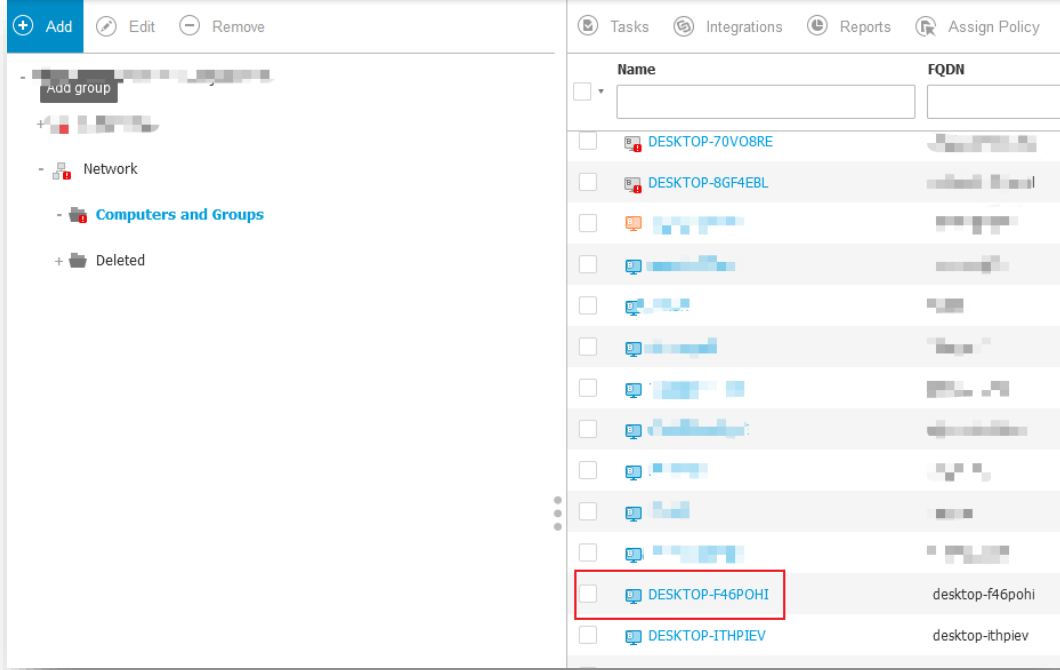
Önemli:

- Dikkat edilmesi gereken nokta düzenlenen ve izin verilen kuralı hangi makinelerin kullandığı, sizin düzenlediğiniz ve izinli program eklediğiniz kural sorun yaşanan makine tarafından kullanılmıyorsa makinedeki problem giderilmeyecektir.
- Makinelerin hangi kuralı aldığını, sorun yaşanan makine üzerinde hangi kuralın etkin olduğunu görmek için aşağıdaki adımları takip edin:

1- Gravityzone yönetim panelinde **Network** bölümüne gidin.



2- Bu kısımda **Computers and Groups** bölümüne giderek ilgili makineyi bulun ve üzerinde tıklayın.



3- Üzerinde tıkladığınız makine bilgileri kısmında **Policy** bölümüne gidin, bu kısımda ilgili makinenin hangi kuralı aldığını görebileceksiniz. İzinli web siteyi buradaki kuralda yapmanız gerekiyor. Bu ekrandan da kural üzerinde tıklayarak değişiklik yapmanız mümkün.

