

# Azure DDOS Protection

**DDoS çok meşhur bir terim diyebiliriz. Peki Nedir bu DDoS ?**

Kötü niyetli kişilerin bir web sitesindeki düzenli ve sağlıklı hizmet veren trafiği kesmek için web sitesine çok sayıda istek göndererek gereksiz trafik yükü gibi saldırularla sisteminizin erişilebilirliğine zarar verecek saldırı türüdür.

Azure Cloud ortamınızda ağınıza ait Layer 3 ve Layer 4 Katmanlarının korunması için “ **Azure Protection Standart** ” hizmetini kullanarak Distributed Denial of Service ( DDoS ) saldırılarından ortamımızı nasıl koruruz bu makalede onu ele alacağım.

**Hadi Başlayalım :**

**Azure Cloud ortamında 2 tür DDoS Protection türü mevcuttur :**

- DDoS protection Basic
- DDoS protection Standard

**Azure DDoS Protection ,** Tüm Azure hizmetlerinde hali hazırda yerleşik olarak bulunan plan türüdür. Tamamen ücretsizdir.

**Azure DDoS Standard ,** Uygulamanıza , Web sitesinize yönelik saldırılar oluyorsa bu katman tam size göre ... Aylık 3000\$ gibi rakam ödenmekteidir.

Şimdi uygulama gerçekleştireceğiz fakat lütfen kurulumla alakalı işlemleri gerçekleştirdiğinizde ortamda uzun süre bu servisi tutmamanızı öneririm 😊

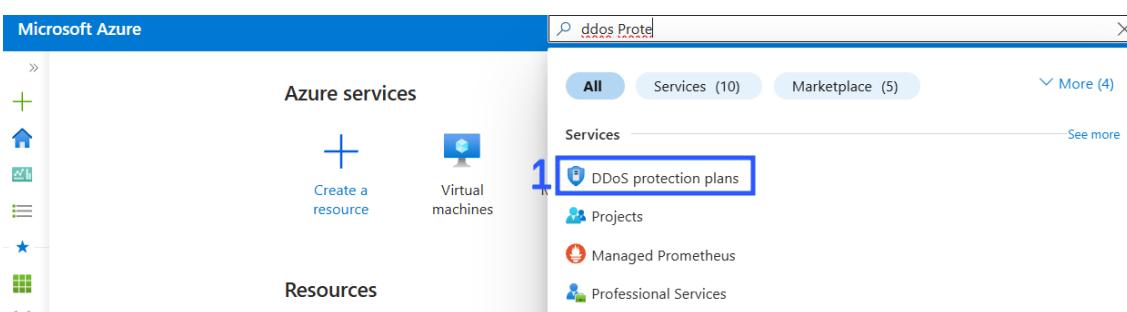
Kısa sürede deneyimleyerek uzun süre tutmadan ortamınızdan kaldırmanız önerilmektedir.

Evet yapacaklarını özetliyorum şimdi

İlk olarak Portal'a giriş yapıyorum. Ardından Portal'dan arama bölümünden « Azure DDOS Protection Plan » servisini buluyoruz ve Protection Plan dağıtıyoruz. Test işlemi için bir Adet Virtual Network kaynağı dağıtmamanız yeterlidir. Ardından korunacak kaynakları ekliyoruz ve sonrasında zaman kaybetmeden kaynakları ve planı sileceğiz.

O halde hadi işlemlere başlayalım 😊 Leetttssss Goooo

İlk öncelik olarak “ **DDOS Protection Plans** ” servisine giriş yapıyoruz



“ DDos Protection Plans ” oluşturmak için “ Create ” seçeneğini seçeriz.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar has 'Microsoft Azure' and a search bar. Below it, the left sidebar shows a tree view of resources. The main content area is titled 'DDoS protection plans' and shows a message 'Showing 0 to 0 of 0 records.' There are filter options for 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. At the top right, there are buttons for 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A large blue button labeled 'Create' is highlighted with a red box.

Plan oluşturma adımda ortamınızda bir resource group mevcut ise onu seçerek devam edebilirsiniz. Mevcut değilse dilediğiniz bölgede “ **Create New** ” seçeneğini seçerek Yeni Resource Group dağıtabilirsiniz.

Ardından Planınıza vereceğiniz DDOS Protection Plan Name ( Proje , Uygulama , Yada ortam ismi olabilir ) belirleyerek kutucuğu doldururuz.

Planınızın oluşturulacağı bölgeyi seçiyoruz.

4.Bölgede bulunan “ **You can create a single DDoS protection plan and apply it to resources in all of your subscriptions** ” uyarısı ; tek bir DDOS Protection Planın oluşturulacağını ve bunu tüm aboneliklerimizde kaynaklara uygulayabileceğimizin bilgisini vermektedir.

Ardından “ **Next : Tags** ” seçeneğini seçerek devam ederiz. ( **Yada Tag’leme** yanı etiketleme işlemi gerçekleştirilmeyecekseniz kısayoldan “ **Review + create** ” seçeneğini seçerek ilerleyebilirsiniz )

The screenshot shows the 'Create a DDoS protection plan' wizard. Step 1: Project details. It shows a subscription dropdown set to 'Microsoft Azure Sponsorluk' (1). Below it, a resource group dropdown is set to 'Prod' (2). Under 'Instance details', the name is 'Prod-DDOS-Protect' (2) and the region is 'East US' (3). A note at the bottom states: 'You can create a single DDoS protection plan and apply it to resources in all of your subscriptions.' (4). At the bottom, there are 'Review + create' and 'Next : Tags' buttons, with 'Next : Tags' highlighted with a red box (5).

Herhangi bir etiketleme işlemi gerçekleştirmeyeceğim “ **Review + create** ” seçeneğini seçerek ilerliyoruz.

Microsoft Azure  Search resources, services, and docs (G+/)

Home > DDoS protection plans >

## Create a DDoS protection plan ...

Basics Tags Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags ↗](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	
<input type="text"/>	:	<input type="text"/>

[Review + create](#) [< Previous](#) [Next : Review + create >](#) Download a template for automation



Ardından “Validation passed” uyarısı aldık ve artık kaynağımızı gönül rahatlığıyla dağıtabiliriz. “Create” seçeneğini seçerek kaynak dağıtım işlemini başlatırız.

The screenshot shows the Microsoft Azure portal interface for creating a DDoS protection plan. The top navigation bar includes 'Microsoft Azure' and a search bar. The left sidebar has a tree view with icons for Home, DDoS protection plans, and other services like Storage, Functions, and Logic Apps. The main content area is titled 'Create a DDoS protection plan'. A green banner at the top says 'Validation passed' with a checkmark icon. Step 1 is highlighted in blue. Below it, there are tabs for 'Basics', 'Tags', and 'Review + create', with 'Review + create' being underlined. The 'Basics' section shows the following configuration:

Subscription	Microsoft Azure Sponsorluk
Resource group	Prod
Name	Prod-DDOS-Protect
Region	East US

The 'Tags' section shows 'None'. The 'Terms' section contains a note about accepting charges and a link to 'Read more about DDoS protection plan pricing'. At the bottom, there is a large blue 'Create' button labeled '2', and navigation buttons for '< Previous' and 'Next >'. A link to 'Download a template for automation' is also present.

Deployment işlemi başladı.

... Submitting deployment... >

Submitting the deployment template for resource group 'Prod'.

Deployment işlemi tamamlandı.

The screenshot shows the Microsoft Azure Deployment Overview page. The main message is "Your deployment is complete". Key details include:

- Deployment name: Microsoft.DdosProtectionPlan-20240923002848
- Subscription: Microsoft Azure Sponsorluk
- Resource group: Prod
- Start time: 9/23/2024, 12:38:51 AM
- Correlation ID: 9a6d1649-7988-414c-a577-13f71af6e3a

Below this, there are sections for "Deployment details" and "Next steps". A prominent blue button at the bottom says "Go to resource".

Azure DDOS Protection Plan oluşturma işlemleri tamamlandı.

Şimdi DDOS Protection plan üzerinde varolan kaynağı veya yeni kaynak nasıl ekleriz ? onu deneyimleyeceğiz

**Virtual Network dağıtıma için detaylı makaleme aşağıdaki linkten erişebilirsiniz.**

<https://www.cozumpark.com/azure-virtual-network-kavrami-ve-olusturma-islemleri/>

Şimdi Var olan « **Prod-VNET10** » adında bir virtual network'ü « Protected Resources » bölümüne ekleyeceğim.

“ **Virtual Networks** ” bölümüne girdiğimde “ **Prod-VNET10** ” kaynağının olduğunu görüyorum. Amacım bunu DDOS Protection servisine resource olarak eklemek olacaktır.

The screenshot shows the Microsoft Azure Virtual Networks page. The table displays one record:

Name	Resource group	Location	Subscription
Prod-VNET10	Prod	East US	Microsoft Azure Sponsorluk

Ayrıca “Virtual Network” dağıtım esnasında da “Azure DDoS Protection Plan” aktif hale getirebileceğinizi göz önünde bulundurmanızı öneririm.

## Create virtual network ...

Basics Security IP addresses Tags Review + create

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more.](#)

Enable Azure Bastion

### Azure Firewall

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. [Learn more.](#)

Enable Azure Firewall

### Azure DDoS Network Protection

Azure DDoS Network Protection is a paid service that offers enhanced DDoS mitigation capabilities via adaptive tuning, attack notification, and telemetry to protect against the impacts of a DDoS attack for all protected resources within this virtual network. [Learn more.](#)

Enable Azure DDoS Network Protection

“Prod-DDOS-Protect” Plan bölümüne girerek “Settings – Protected Resources” seçeneğini seçeriz.

The screenshot shows the Microsoft Azure portal interface for a DDoS protection plan named "Prod-DDOS-Protect". The left sidebar menu includes "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings" (which is expanded to show "Protected resources" with a red '1'), "Properties", "Locks", "Monitoring" (with "Alerts" and "Metrics" sub-options), "Automation" (with "CLI / PS", "Tasks (preview)", and "Export template" sub-options), and "Help". The main content area displays the "Protected resources" section with a sub-section titled "Manage protected resources". It contains the text: "Enable your DDoS protection plan on a virtual network to automatically mitigate DDoS attacks on your networks." Below this is a "Add protected resource" button. To the right, there are three cards: "Telemetry and reporting" (describing Azure Monitor for real-time DDoS mitigation metrics), "View metrics" (button), and "DDoS protection planning" (describing preparation and best practices). The top navigation bar shows the URL "Home > Microsoft.DdosProtectionPlan-20240923002848 | Overview" and various Azure service icons.

Yukarıdaki tarafta belirtilen bir çok servisin ve kaynağı ekleyerek arkalarındaki tüm kaynaklar için bu saldırıyı engelleme olanağınız super derecede var.

Gerçekten bu kadar kaynak çeşitliliği servisin kullanılabilirliği açısından şahane diyebilirim.

Prod-DDOS-Protect | Protected resources

VNET Firewall Application Gateway Bastion Host Load Balancer NIC Virtual Machine Scale Set

No results.

< Previous Page 1 of 1 Next >

“Add” seçeneğini seçeriz.

Prod-DDOS-Protect | Protected resources

VNET Firewall Application Gateway Bastion Host Load Balancer

No results.

< Previous Page 1 of 1 Next >

Subscription , Resource Group seçeneğini seçeriz. Ardından kaynaklarımın bulunduğu Prod-VNET10 kaynağımı seçerek “ Add ” seçeneğini seçerek kaynak ekleme işlemini gerçekleştiriyoruz.

### Add virtual network to DDoS plan

Prod-DDOS-Protect

Choose a virtual network you would like to add to your DDoS plan. [Learn more](#)

Subscription *	1 Microsoft Azure Sponsorluk
Resource group *	2 Prod
Virtual network *	3 Prod-VNET10

**Add** **Cancel**

Ekleme işlemi gerçekleştiriliyor.

**MICROSOFT AZURE**

... Updating the virtual network

Updating the virtual network 'Prod-VNET10'.

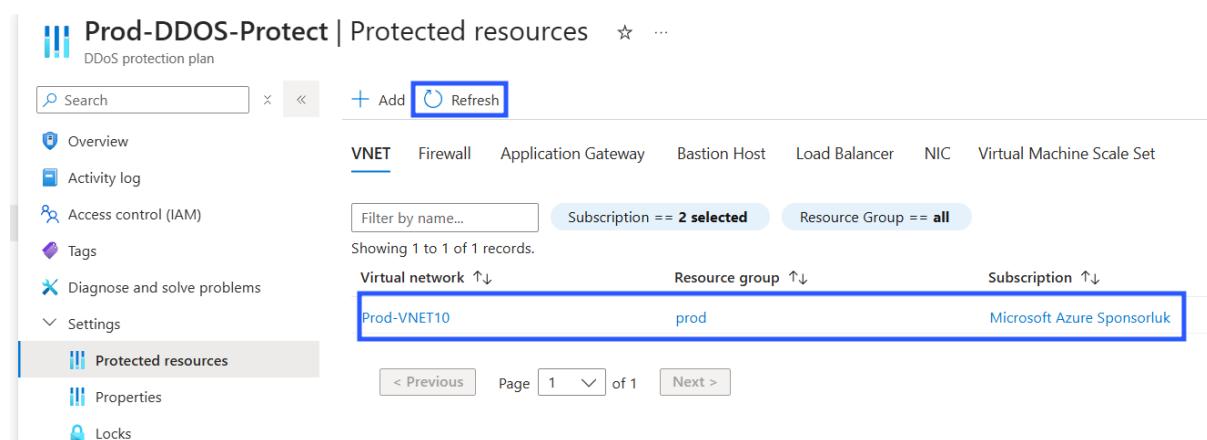
Ekleme işlemi gerçekleştirildi.



**✓ Updated the virtual network**

Successfully updated the virtual network 'Prod-VNET10'.

“ Refresh “ seçeneğini seçerek eklediğimiz kaynağımızı eklemiş oluruz.



The screenshot shows the Azure portal interface for managing a DDoS protection plan. The main title is "Prod-DDOS-Protect | Protected resources". On the left sidebar, under "Protected resources", there is one entry: "Prod-VNET10". The "Subscription" dropdown at the top indicates "2 selected" and "Microsoft Azure Sponsorluk". The "Refresh" button is highlighted with a blue border.

Tebrikler artık VNET'e bağlı tüm kaynaklarımız korunmaktadır. İşlem tamamlanmıştır.

**NOT :** Kaynak kaldırma işlemine dağıtıığınız gibi başlayabilirsiniz. İlk önce eklemiş olduğumuz VNET , Protected Resources bölümünden silmeniz gerekmektedir. Ardından Plan bölümünden “ Delete ” seçeneğini seçerek Plan kaldırma işlemini tamamlayarak kaynakları temizleyebilirsiniz.

DDoS Protection üzerinde tamamen koruma istiyorsanız ; Azure Entra ID Tenant’ınızı birden çok aboneliğinize bağlayabilirsiniz.

Ayrıca şunu da belirtmek te fayda var: Azure DDOS protection altyapı düzeyinde korumak sağlamaktadır.

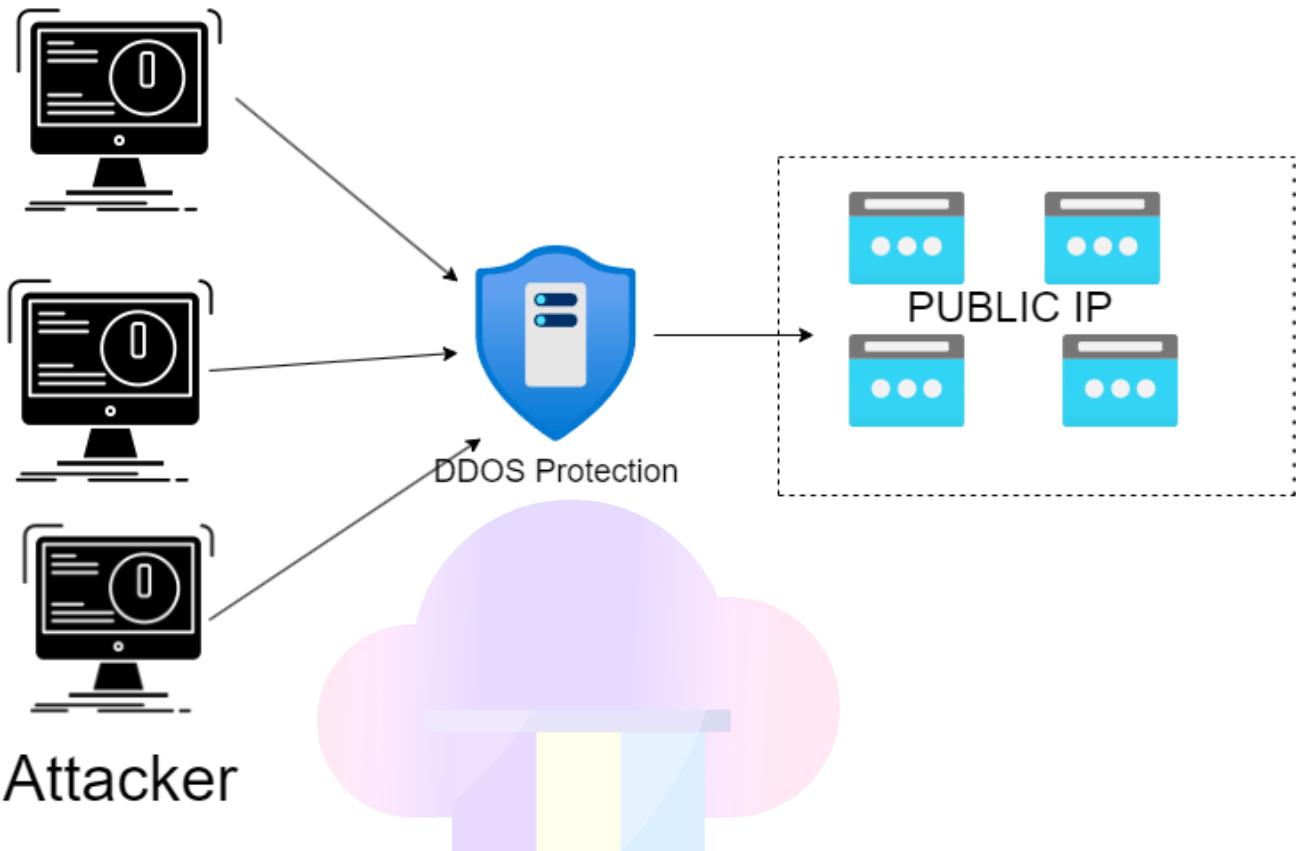
**İlgimi çeken planlara ait karşılaştırmalar hakkında bilgi vermek istedim :**

Özellik	DDOS Infrastructure Protection	DDoS protection Standard Plan
Metrik ve Uyarı İzleme	Yok	Var
Saldırıyı minimize etme	Var	Var
Aktif izleme ve algılama	Var	var
Maliyet Optimizasyonu	Yok	Var
Hızlı müdahale	Yok	Var

**DDOS Protection'a Public IP'leri ilişkilendirdiğinizde korunacak kaynaklar aşağıdaki gibidir :**

Kaynak	Korunma Metodu
Virtual Machines	Public IP
Network Virtual Appliances ( NVA )	Public IP
Load Balancers	Public IP
Application Gateway	Public IP
Azure Firewall	Public IP
Azure Bastion	Public IP
VPN Gateway	Public IP

Azure DDOS Protection Plan sizleri Layer 3 ve Layer 4 , Layer 7 Katmanındaki saldırılarından koruyabilmektedir. Ayrıca Volumetric yani hacimsel saldırılarından da korumuş olur.



Şimdi geldik kritik soruya ben bu servisi nasıl test edebilirim 😊 Dayanıklılığını yada gerçekten koruma gerçekleştiriyor mu ? Gerçekleştir miyor mu bununla alakalı simülasyon gerçekleştirebiliyor muyuz ? diye soranlar olabilir.

Microsoft'un izin vermiş olduğu partnerlerden saldırı sumülasyonlarını yapmanız önerilmektedir.  
Bunlardan biri " Red Button "

<https://www.red-button.net/ddostesting/>

The screenshot shows the Red Button website's DDoS testing interface. The main heading is "The Most Realistic DDoS Simulation Testing". Below it is a sub-headline: "Harden your DDoS defenses against the tactics and strategies of top hackers.". At the bottom, it says "Authorized DDoS Test Partner" and lists "Azure" and "AWS" as partners. The right side of the page is heavily obscured by a large amount of illegible, dark-colored simulated DDoS attack code.

İkincisi " Mazebolt "

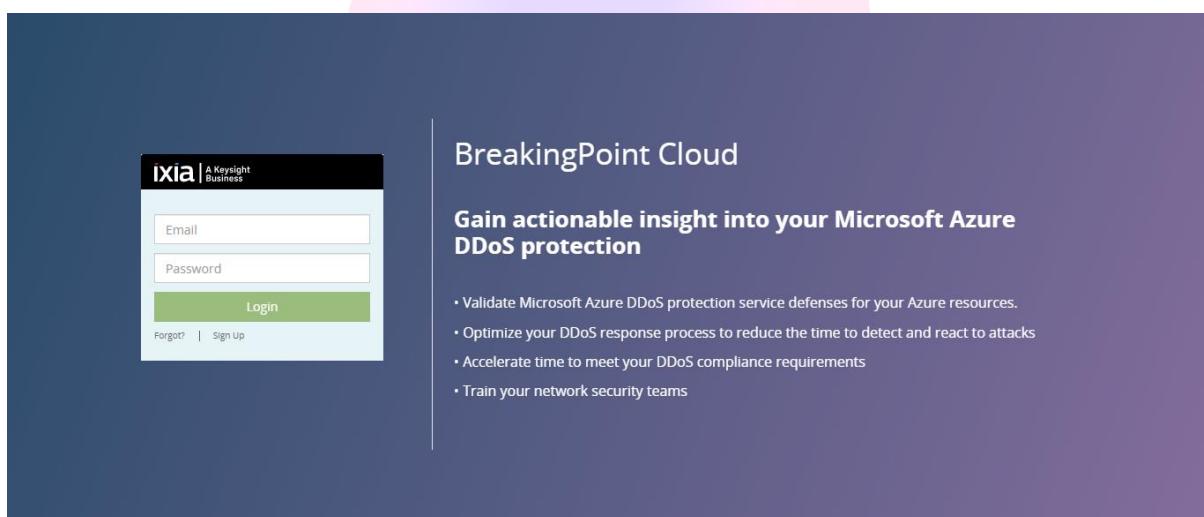
<https://mazebolt.com/microsoft-partner/>



The landing page features the Microsoft Azure logo and the MazeBolt logo side-by-side. The main title is "Enhance Microsoft Azure DDoS Protection with MazeBolt RADAR™". Below the title, a subtitle states: "MazeBolt RADAR™ provides continuous vulnerability testing of the entire DDoS attack surface for Azure Cloud assets." A green button labeled "EXPLORE RADAR™ TESTING →" is visible.

Üçüncüsü " BreakingPoing Cloud "

<https://www.breakingpoint.cloud/login>



The page shows a screenshot of the BreakingPoint Cloud login interface, which includes fields for Email and Password, and a green "Login" button. To the right, the service is described as "BreakingPoint Cloud" and "Gain actionable insight into your Microsoft Azure DDoS protection". A bulleted list details the benefits:

- Validate Microsoft Azure DDoS protection service defenses for your Azure resources.
- Optimize your DDoS response process to reduce the time to detect and react to attacks
- Accelerate time to meet your DDoS compliance requirements
- Train your network security teams