**What is AWS Shield?**

AWS Shield is a managed AWS Cloud service for **DDoS (Distributed Denial of Service (DDoS))** protection against all known infrastructure (layer 3 and 4) attacks.

AWS Shield is available at **two different tiers, AWS Shield Standard and AWS Shield Advanced**, and AWS Shield Advanced has a lot more power and protection on offer than the Standard version.

### AWS Shield Standard

AWS Shield Standard is free, and it offers DDoS protection against some of the more common layer 3, the network layer, and layer 4, the transport layer, DDoS attacks. This protection is **applied automatically** and transparently to your **Elastic Load Balancers, Amazon CloudFront distributions, and Amazon Route 53.**

**AWS Shield Standard is also available in the StormIT** [**CDN security**](https://www.stormit.cloud/cdn-security/) **solution.**

### AWS Shield Advanced

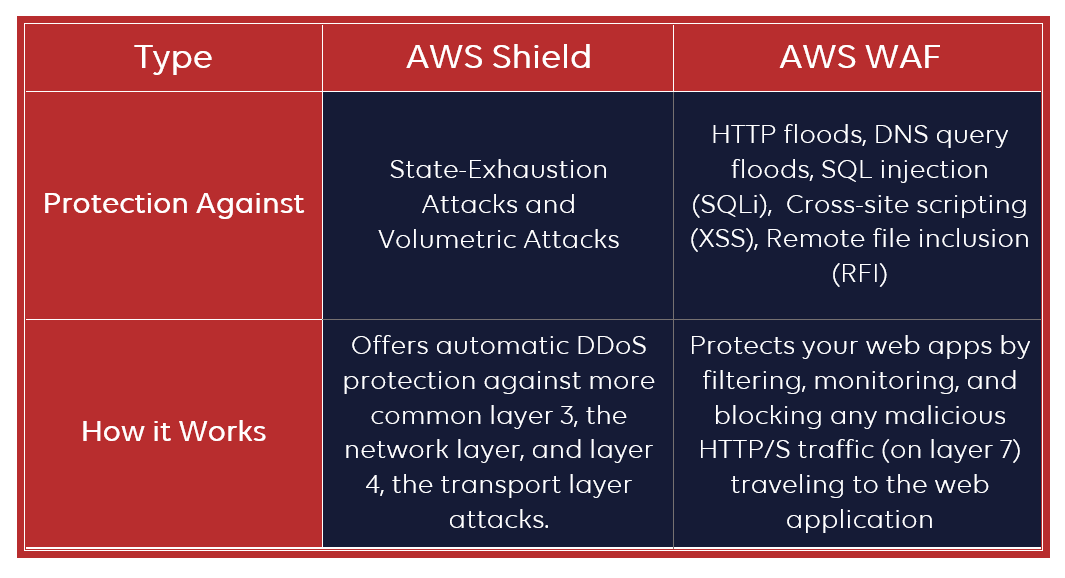
This paid service provides additional DDoS mitigation capability, intelligent attack detection, and mitigation against attacks at the application (AWS WAF included) and network layers.

Shield Advanced also provides additional detection and mitigation against large and sophisticated DDoS attacks and near real-time visibility into attacks.

## What is the difference between AWS WAF and AWS Shield?

These two services are included in the AWS Edge Services ecosystem and provide DDoS protection. The difference between them is that **AWS WAF**[(Web Application Firewall)](https://www.stormit.cloud/blog/what-is-a-web-application-firewall/" \t "_blank) **provides protection on the application layer** and **AWS Shield protects the infrastructure layers** of the OSI model.

You will find more information about AWS Shield vs AWS WAF in the table below.



**AWS WAF is included in AWS Shield Advanced subscription**, so basically, AWS Shield is not a WAF(web application firewall), but if you use the Advanced subscription, you will get a WAF for free.

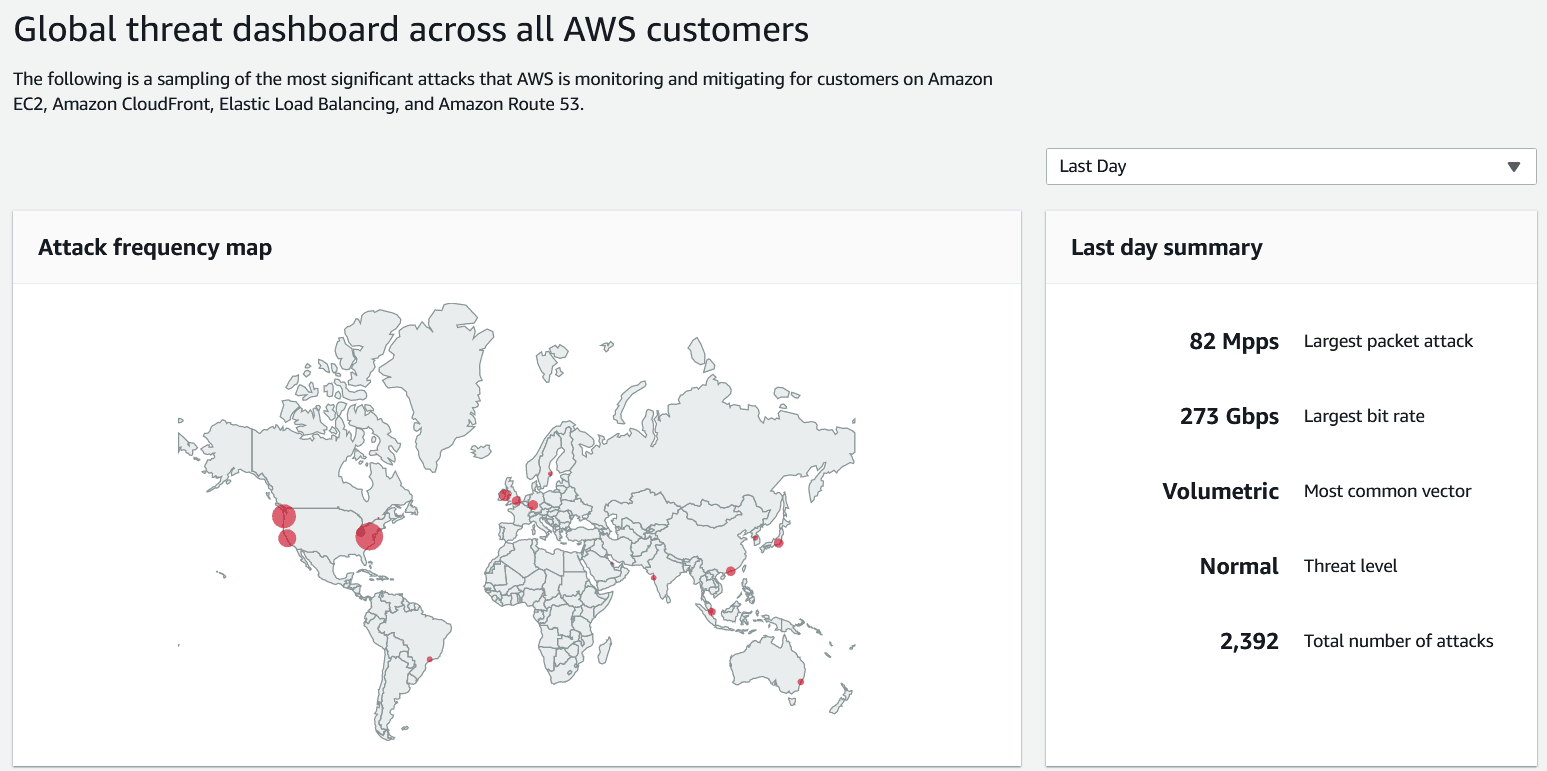
## Benefits of using AWS Shield DDoS protection

There are some general benefits of using AWS Shield for the protection of AWS Cloud resources, but also the protection of third-party solutions (on-premises or other cloud providers):

* **Easy to use:** Like most AWS services, AWS Shield is an easy-to-use service designed to allow you to protect your applications quickly and easily. AWS Shield can be used for existing applications or new applications using the AWS Management Console. **No routing changes are required for enabling these protections.**
* **Cost-efficient:** AWS Shield Standard is automatically enabled for all AWS customers at no additional cost. With AWS Shield Advanced, customers get AWS WAF and AWS Firewall Manager at no additional cost.

### Benefits of AWS Shield Standard:

* **Traffic monitoring:** AWS Shield Standard inspects incoming traffic to your network and applies a combination of traffic signatures, anomaly algorithms, and other analysis techniques to detect malicious traffic. It sets some static thresholds for each of your resource types, but does not provide any custom protections.
* **DDoS mitigation:** Over 99% of infrastructure layer attacks detected by AWS Shield Standard are automatically mitigated in less than one second.
* **Global threat dashboard:** You are provided with general information about DDoS attacks on the AWS network. You can find this information in the AWS Management Console in the global threat dashboard.



### Benefits of AWS Shield Advanced

* **Advanced real-time metrics and reports:** You can always find information about the current status of your DDoS protection and you can also see the real-time report with AWS CloudWatch metrics and attack diagnostics.
* **Cost protection for scaling:** This helps you against bill spikes after a DDoS attack that can be created by scaling of your infrastructure in reaction to a DDoS attack.
* **AWS WAF included:** Mitigate complex application-layer attacks (layer 7) by setting up rules proactively in AWS WAF to automatically block bad traffic.
* **You get 24×7 access to our DDoS Response Team (DRT)** for help and custom mitigation techniques during attacks. To contact the DRT you will need the Enterprise or Business Support levels.

## How does AWS Shield work?

A DDoS attack is made in an attempt to make an online service such as a website or web service unavailable by overwhelming it with malicious traffic. This is where AWS Shield comes in.

**Amazon Route 53, Elastic Load Balancer and Amazon CloudFront** DDoS protection is automatically provided by AWS Shield Standard, at no additional charge.

To start using **AWS Shield Advanced** you will need to go through some basic steps. At the start, you will subscribe to AWS Shield Advanced and then choose which resources it will protect.

You can add **Advanced Shield** protection for any of the **following resource types:**

* [Amazon CloudFront](https://www.stormit.cloud/cdn-services/) distribution
* [Amazon Route 53](https://www.stormit.cloud/blog/amazon-route-53/) hosted zone
* AWS Global Accelerator
* Elastic Load Balancer(ELB)
* Amazon Elastic Compute Cloud (Amazon EC2) Elastic IP addresses

Shield Advanced protects only the resources that you specify. It’s best to read more about Shield Advanced in the [AWS tutorial](https://docs.aws.amazon.com/waf/latest/developerguide/getting-started-ddos.html) that describes how to get started with it.

As a general countermeasure against DDoS attacks, AWS's infrastructure is designed to be DDoS resilient and equipped with a DDoS mitigation system that can automatically detect and filter excess traffic 24/7.

## What does AWS Shield protect against?

**AWS Shield Standard protects** your applications and websites against these types of DDoS attacks:

* **State-Exhaustion Attacks (layer 4) - SYN Flood:** Consumes the TCP connection state tables present in many network infrastructure and security devices, as well as the application servers themselves. The attacker quickly initiates a connection to a server without finalizing the connection. These attacks can block access for legitimate users, sometimes even leaving defenses wide-open to data exfiltration.
* **Volumetric Attacks (layer 3):** Also referred to as network floods, and includes UDP floods (UDP reflection attacks) and ICMP floods. This type of attack occurs when a network is **overwhelmed by a large amount of malicious traffic**, causing your applications or services to become unavailable to users.

**AWS Shield Advanced** protects your apps against the same attacks as Standard version with some specific function, but because it also includes AWS WAF, it protects against:

* **Application-Layer Attacks (layer 7) - HTTP floods, DNS query floods**: Composed of requests (HTTP GETs and DNS queries are popular) that are designed to consume application resources. An example is an attacker who continuously uses a website functionality (submitting a contact form or any API requests) where he knows that it causes database and application processing.
* **Other Application-Layer Attacks:** [SQL injection](https://en.wikipedia.org/wiki/SQL_injection) (SQLi), [Cross-site scripting](https://en.wikipedia.org/wiki/Cross-site_scripting) (XSS), [Remote file inclusion](https://en.wikipedia.org/wiki/File_inclusion_vulnerability) (RFI) and more web application attacks and threats from the OWASP Top 10 publication.

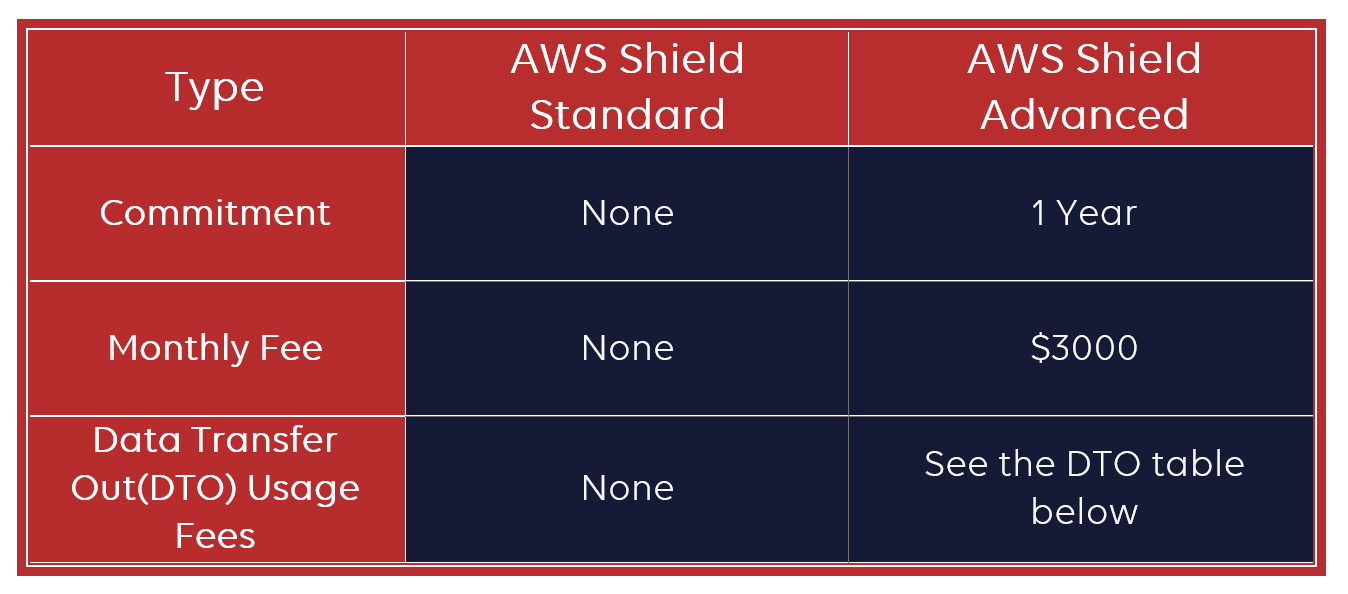
## Can you use AWS Shield to protect applications or websites not hosted in AWS?

Yes, it is possible to use AWS Shield and other AWS Edge services (Amazon Route 53, Amazon CloudFront, and AWS WAF) with custom origins because you can set any public domain or IP as the origin in the CloudFront distribution setup or in Route 53. Learn more about our CDN solution in the last section of this article.

## AWS Shield pricing

There is no charge for inbound data transfer on AWS and you do not pay for DDoS attack traffic that is mitigated by AWS Shield.

The table below describes the main difference between the pricing of Shield Standard and Shield Advanced.



### AWS Shield Standard

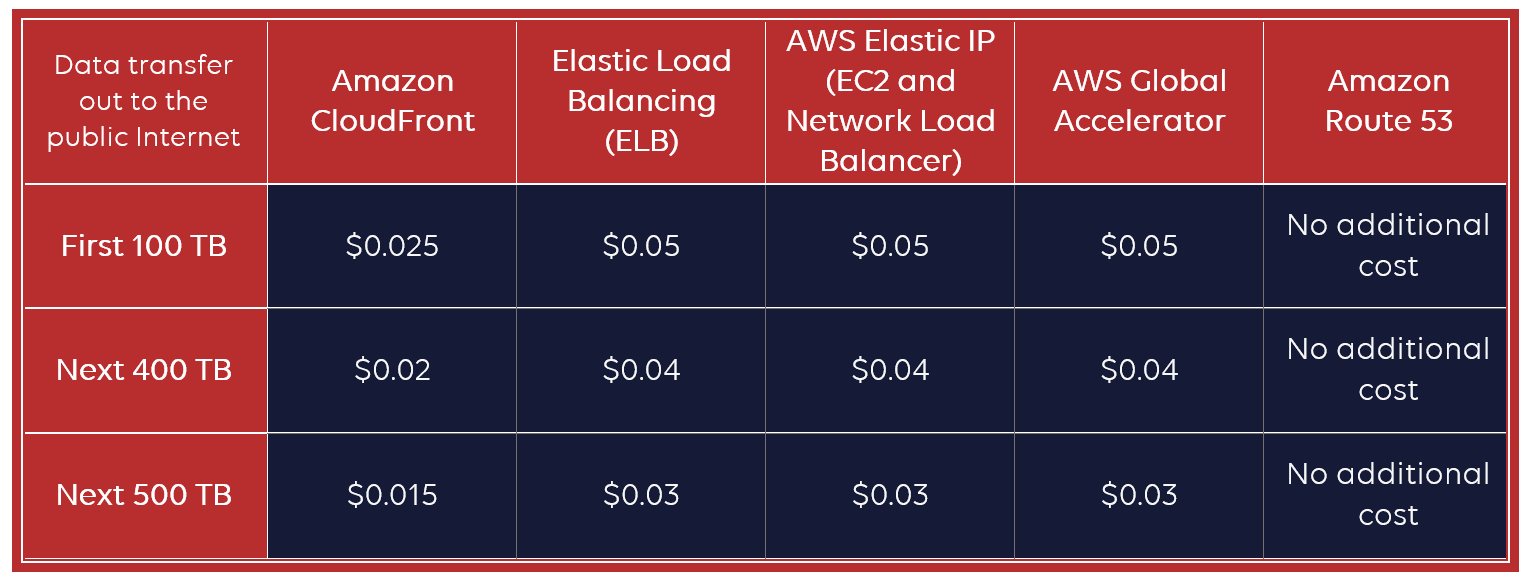
AWS Shield Standard is built into the AWS services that you can use for your web applications. There are **no additional costs for AWS Shield Standard**.

### AWS Shield Advanced

AWS Shield Advanced is a paid service that provides additional protections for internet-facing applications. You will pay $3000 per organization subscribed to AWS Shield Advanced with a subscription commitment of at least one year. If your organization has [multiple AWS accounts](https://www.stormit.cloud/blog/aws-organizations-how-to-manage-multiple-aws-accounts/), you will pay the monthly fee once.

#### Data Transfer Out Usage Fees (per GB) for AWS Shield Advanced

In addition to standard fees on Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53, AWS Global Accelerator, and Amazon Elastic Compute (EC2) you will have to pay **fees per GB of DTO from these services** when you choose to protect them with Shield Advanced.



#### Pricing example: AWS Shield Advanced protecting Amazon CloudFront distribution

If you enable Shield Advanced protection for your Amazon CloudFront distribution and you block any other possibility of connection to your resources such as EC2 or ELB behind it, you don’t need to protect any other services with Shield Advanced.

At the end of the month, you will pay the AWS Shield Advanced monthly fee of $3,000. In addition to the monthly fee, you will be charged the AWS Shield Advanced usage-based fee of Data Transfer out at $0.025 per GB