### **AWS Shield and AWS Shield Advanced**

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that helps safeguard applications running on AWS. AWS Shield comes in two tiers: **AWS Shield Standard** and **AWS Shield Advanced**. Shield Standard provides free DDoS protection for all AWS customers, while Shield Advanced offers enhanced protection with additional features and cost protection against large-scale attacks.

### **1. Overview of AWS Shield**

* **Service Purpose**: AWS Shield is designed to protect AWS infrastructure and applications from Distributed Denial of Service (DDoS) attacks.
* **Key Features**:
  + Continuous monitoring and automatic protection against DDoS attacks.
  + Integrated with AWS services (Amazon CloudFront, Elastic Load Balancing, AWS Global Accelerator, etc.).
  + Two protection tiers:
    - **AWS Shield Standard**: Provides free, baseline DDoS protection for all AWS customers.
    - **AWS Shield Advanced**: Offers enhanced protection, 24/7 DDoS response team (DRT) access, and cost protection.
* **Primary Focus Areas**:
  + Mitigating volumetric attacks.
  + Application layer (Layer 7) protection.
  + Cost protection for scaling resources during attacks.

### 

### 

### 

### 

### 

### 

### 

### **2. Key Differences: AWS Shield Standard vs. AWS Shield Advanced**

| **Feature** | **AWS Shield Standard** | **AWS Shield Advanced** |
| --- | --- | --- |
| **Protection Type** | Automatic DDoS protection | Enhanced DDoS protection with customization |
| **DDoS Attack Types Covered** | Network and transport layer | Network, transport, and application layers |
| **Cost** | Free | Paid (subscription) |
| **24/7 Support** | No | Yes, via the AWS DDoS Response Team (DRT) |
| **Global Threat Environment** | Basic protection, no visibility | Access to detailed attack diagnostics |
| **Attack Cost Protection** | No | Yes (cost recovery for scaling resources) |
| **Advanced Reporting** | No | Yes (real-time metrics, attack analysis) |
| **WAF Integration** | No | Yes (automated mitigation rules) |

### **3. AWS Shield Standard**

#### **a. Overview:**

* AWS Shield Standard is automatically available to all AWS customers at no extra cost.
* Provides protection against most common DDoS attacks, including network and transport layer attacks, such as SYN/ACK floods and UDP reflection attacks.
* Shield Standard leverages AWS's globally distributed infrastructure to absorb large-scale attacks and prevent them from affecting customer workloads.

#### **b. Protection Focus:**

* **Layer 3/4 Protection**: Network-level DDoS attacks, such as ICMP floods, UDP reflection, or TCP SYN/ACK floods.
* **Automatic Mitigation**: AWS Shield Standard continuously monitors network traffic and automatically protects applications without customer intervention.
* **Service Integration**: Works automatically with AWS services like Amazon CloudFront, Elastic Load Balancing (ELB), and AWS Global Accelerator.

#### 

#### **c. Use Cases:**

* Protecting web applications from basic DDoS attacks.
* Defending network-based services and endpoints.
* Preventing disruptions due to volumetric and state-exhaustion attacks.

#### **d. Limitations:**

* Limited to network and transport layer DDoS protection.
* No advanced diagnostics or visibility into attacks.
* No access to the AWS DDoS Response Team (DRT) for customized mitigation.

### **4. AWS Shield Advanced**

#### **a. Overview:**

* AWS Shield Advanced provides enhanced DDoS protection beyond what Shield Standard offers, including application layer (Layer 7) protection, access to 24/7 support from the AWS DDoS Response Team (DRT), and cost protection for scaling resources during an attack.
* Designed for businesses running mission-critical applications that need deeper insights and advanced mitigation techniques for large-scale DDoS attacks.
* Shield Advanced is a paid service that requires a subscription.

#### **b. Key Features of AWS Shield Advanced:**

##### **1. Layer 3/4 and Layer 7 DDoS Protection:**

* Protects against both network/transport layer attacks and application-layer (Layer 7) attacks, such as HTTP floods.
* **Layer 7 (Application Layer) Attacks**: Targets the application directly, such as sending large numbers of HTTP requests to overwhelm a web server.

##### **2. DDoS Response Team (DRT):**

* 24/7 access to the **AWS DDoS Response Team (DRT)**, a team of security experts that help mitigate large-scale or complex attacks.
* DRT assistance includes customizing and tuning AWS Web Application Firewall (WAF) rules to block attack traffic more effectively.

##### **3. Real-time Attack Metrics and Visibility:**

* Provides access to detailed metrics, dashboards, and reports via Amazon CloudWatch and the AWS Management Console.
* Offers real-time visibility into ongoing attacks, including attack vectors, traffic patterns, and attack duration.

##### **4. Cost Protection:**

* Shield Advanced provides **DDoS Cost Protection**, which helps recover scaling costs incurred due to legitimate traffic surges caused by an attack.
* AWS credits are provided for scaling infrastructure, such as Auto Scaling or CloudFront, to absorb excess traffic during a DDoS event.

##### **5. Advanced Threat Intelligence:**

* AWS Shield Advanced integrates with **AWS Threat Intelligence**, which provides insights into global DDoS attack trends and helps anticipate future threats.
* Offers **proactive security advice** based on AWS’s global view of DDoS attack patterns.

##### **6. Web Application Firewall (WAF) Integration:**

* Full integration with **AWS WAF**, allowing automated rule creation to mitigate application-layer (Layer 7) attacks.
* AWS WAF rules can automatically block malicious traffic, such as bad bots or HTTP floods, without affecting legitimate traffic.

##### **7. Global Threat Environment Dashboard:**

* Provides customers with a **Global Threat Environment Dashboard** that offers insights into the threat landscape, including the largest DDoS attacks observed globally.
* Customers can compare their own attack metrics with global attack trends.

#### **c. Service Integration:**

* **Amazon CloudFront**: Shield Advanced integrates seamlessly with CloudFront, providing advanced DDoS protection for globally distributed content.
* **Elastic Load Balancing (ELB)**: Protects load-balanced applications across multiple AWS Availability Zones.
* **AWS Global Accelerator**: Shields global applications and speeds up the recovery of DDoS attacks by rerouting traffic across healthy endpoints.

### 

### 

### 

### **5. Use Cases for AWS Shield and Shield Advanced**

#### **a. Web Application Protection:**

* For mission-critical websites and services that require high availability during DDoS attacks.
* Shield Advanced integrates with AWS WAF to protect against web-based Layer 7 attacks.

#### **b. Media and Content Delivery:**

* For services distributing large amounts of content globally (e.g., media streaming or live events), Shield protects content distribution networks (CDNs) like CloudFront from being overwhelmed by attacks.

#### **c. Gaming Services:**

* Online gaming platforms, which are often targeted by DDoS attacks, can use Shield Advanced for both volumetric and application-level protection to ensure minimal disruption.

#### **d. Financial Services:**

* High-value financial services that process transactions and sensitive data use Shield Advanced for continuous monitoring and real-time attack mitigation to ensure business continuity.

#### **e. Government and Public Sector:**

* Organizations that cannot afford downtime, such as government websites or emergency response systems, benefit from Shield Advanced’s comprehensive protection and cost guarantees.

### **6. Pricing for AWS Shield Advanced**

* **Subscription Fee**: Shield Advanced has a flat monthly fee, which is region-specific. For example, the fee is around **$3,000 per month per organization** (price may vary by region).
* **Data Transfer Charges**: Customers are charged based on the volume of data transfer that Shield Advanced protects during an attack, but they benefit from **DDoS cost protection** credits for unexpected scaling costs.
* **Cost Protection for Scaling Resources**: Shield Advanced provides credits for scaling resources like Auto Scaling and ELB to handle increased traffic caused by a DDoS attack.

### **7. Best Practices for Using AWS Shield and Shield Advanced**

#### **a. Architect for Resilience:**

* Use **Amazon CloudFront** and **Elastic Load Balancing** with Shield Advanced to distribute traffic and reduce the attack surface.
* Implement **Auto Scaling** to automatically adjust resource capacity and absorb legitimate traffic spikes during DDoS attacks.

#### **b. Leverage AWS WAF:**

* Deploy **AWS WAF** in conjunction with Shield Advanced to mitigate application-layer (Layer 7) attacks.
* Regularly update WAF rules to block known attack patterns and IP addresses.

#### **c. Monitor Threat Activity:**

* Use the **Global Threat Environment Dashboard** in Shield Advanced to stay informed of emerging threats and adjust your security posture accordingly.
* Regularly review **CloudWatch** metrics for anomalies or suspicious traffic patterns.

#### **d. Prepare an Incident Response Plan:**

* Develop a comprehensive incident response plan that includes engaging the **AWS DDoS Response Team (DRT)** during high-severity DDoS attacks.
* Test your response plan periodically to ensure smooth execution during a real attack.

#### **e. Review Shield Advanced Reports:**

* Continuously review Shield Advanced’s attack diagnostics and reports to identify potential weaknesses and optimize your DDoS protection strategies.

#### **f. Use Route 53 for DNS Protection:**

* AWS Route 53 provides additional DDoS protection for DNS-based attacks when used in combination with Shield Advanced. Route 53’s globally distributed infrastructure can absorb large-scale DNS queries, preventing DNS-related outages.

### 

### 

### **8. AWS Shield Advanced vs. Third-Party DDoS Solutions**

#### **a. AWS Shield Advanced vs. Cloudflare:**

* **AWS Shield Advanced**: Provides deep integration with AWS services and offers cost protection during DDoS attacks, which is particularly useful for AWS-native applications.
* **Cloudflare**: Known for its DDoS protection as a CDN provider, Cloudflare offers protection for websites and services hosted across multiple clouds or on-premises environments.
* **Difference**: Shield Advanced is optimal for AWS workloads, whereas Cloudflare is a better option for multi-cloud or hybrid architectures.

#### **b. AWS Shield Advanced vs. Akamai Prolexic:**

* **Akamai Prolexic**: A specialized DDoS protection service that provides global mitigation capacity with scrubbing centers for large-scale attacks.
* **AWS Shield Advanced**: Offers AWS-native integrations and 24/7 access to the DRT. Shield Advanced includes cost protection and seamless integration with services like AWS WAF.
* **Difference**: Shield Advanced is more tightly integrated with AWS services, whereas Prolexic is platform-agnostic and offers scrubbing-based mitigation.

### **9. Limitations of AWS Shield and Shield Advanced**

* **AWS-Only Focus**: Shield and Shield Advanced are designed for AWS workloads, meaning they don't protect services hosted outside of AWS.
* **Subscription Cost**: Shield Advanced may be costly for smaller businesses, particularly the fixed monthly fee.
* **No Automatic Mitigation for Application Attacks in Shield Standard**: While Shield Standard covers basic DDoS attacks, application-layer protections (Layer 7) require Shield Advanced.
* **DDoS Protection Only**: Shield focuses solely on DDoS attacks. Customers may need additional security solutions like AWS WAF and GuardDuty to address other types of security threats.