Service Name

AWS Shield

Service Overview

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. It provides two tiers: Shield Standard (free) and Shield Advanced (paid subscription). Shield Standard automatically protects against common network and transport layer (Layer 3/4) DDoS attacks for services like CloudFront, Route 53, and Elastic Load Balancing. Shield Advanced offers enhanced protection with application layer (Layer 7) DDoS mitigation, 24/7 access to the AWS DDoS Response Team, advanced event visibility, proactive engagement, and cost protection against DDoS-induced usage spikes.

Key Use Cases

- Web application protection: Protecting internet-facing web applications from DDoS attacks that could cause downtime or service degradation
- E-commerce and critical business applications: Ensuring high availability for revenue-generating applications that require guaranteed uptime during attack scenarios
- Gaming and media streaming: Protecting applications with unpredictable traffic patterns from volumetric attacks and ensuring consistent user experience
- API and microservices protection: Safeguarding API gateways and distributed architectures from application layer request floods and sophisticated attacks

Features

- **Shield Standard**: Free automatic protection against common Layer 3/4 DDoS attacks with static threshold detection and inline mitigation
- **Shield Advanced**: Enhanced DDoS protection with application layer mitigation, health-based detection, and tailored traffic pattern analysis
- **AWS WAF Integration**: Automatic application layer DDoS mitigation using AWS WAF rules and rate-based controls included at no additional cost
- **Shield Response Team (SRT)**: 24/7 access to AWS DDoS experts for attack response, custom mitigation creation, and proactive engagement during incidents
- **DDoS Cost Protection**: Service credits to cover scaling charges resulting from DDoS attacks against protected resources
- **Advanced Event Visibility**: Real-time metrics, detailed attack reports, and CloudWatch integration for comprehensive DDoS event monitoring
- **Protection Groups**: Logical groupings of protected resources for enhanced detection, mitigation, and centralized management

- **Network Security Director**: Preview capability providing network topology visibility, security configuration analysis, and remediation recommendations

Value Proposition

AWS Shield provides comprehensive DDoS protection with the advantage of being deeply integrated into AWS infrastructure and services. Shield Standard is automatically included at no cost, providing immediate protection without configuration:

- Shield Advanced offers unique value through its AWS DDoS Response Team access, cost protection guarantees, and integration with AWS WAF at no additional charge for standard capabilities
- The service leverages AWS's massive global infrastructure scale for mitigation capacity and provides proactive engagement during attacks
- Unlike third-party solutions, Shield offers seamless integration with other AWS services, centralized management through AWS Firewall Manager, and the ability to protect both AWS-hosted and external resources through CloudFront and Route 53

Service Integration

AWS Shield integrates tightly with multiple core AWS services for comprehensive protection. Amazon CloudFront distributions and Amazon Route 53 hosted zones receive enhanced protection automatically:

- AWS WAF integration provides application layer mitigation included with Shield Advanced subscriptions
- Elastic Load Balancing (Application, Network, and Classic Load Balancers) can be protected when associated with Elastic IP addresses
- Amazon EC2 instances are protected through Elastic IP association
- AWS Global Accelerator standard accelerators receive automatic protection
- AWS Firewall Manager enables centralized Shield Advanced policy management across accounts
- CloudWatch provides metrics and monitoring for protected resources
- AWS Organizations supports consolidated billing for Shield Advanced across multiple accounts

Onboarding and Offboarding

Getting started with AWS Shield requires different approaches for each tier. Shield Standard is automatically enabled for all AWS customers at no cost and requires no configuration:

- For Shield Advanced, customers must subscribe through the AWS console or API, requiring a one-year commitment with $3,000 monthly fee plus usage charges

- The setup process involves subscribing to Shield Advanced, adding resource protections, configuring health-based detection with Route 53 health checks, setting up CloudWatch alarms and notifications, and optionally configuring AWS Shield Response Team support with emergency contacts
- Shield Advanced can be deployed using Infrastructure as Code tools including AWS CloudFormation and Terraform for automated configuration

Getting Started Guide: https://docs.aws.amazon.com/waf/latest/developerguide/getting-started-ddos.html

Data Removal

AWS Shield offboarding varies by tier. Shield Standard cannot be disabled as it's automatically included with AWS services. For Shield Advanced, customers can cancel subscriptions through the AWS console, but the one-year commitment must be fulfilled. During offboarding, all Shield Advanced protections are removed, custom mitigations are deleted, and SRT access is terminated. No customer data is stored by Shield itself, as it only analyzes traffic patterns in real-time. Historical attack and event data in CloudWatch follows standard CloudWatch retention policies and can be deleted according to customer preferences.

Backup/Restore and Disaster Recovery

AWS Shield does not provide backup and disaster recovery capabilities as it is a real-time DDoS protection service. Shield operates at the network perimeter and does not store or backup customer data. The service itself is designed for high availability across AWS's global infrastructure with automatic failover capabilities. For disaster recovery planning, customers should implement Shield protections in multiple regions and combine with other AWS services like AWS Backup for data protection and AWS Elastic Disaster Recovery for application recovery scenarios.

Backup Capabilities

AWS Shield does not have backup capabilities and does not integrate with AWS Backup. Shield is a real-time traffic analysis and mitigation service that does not store customer data requiring backup:

- The service configuration and protection settings are maintained in AWS's control plane but individual attack data is transient
- Customers should rely on other AWS services for backup needs while using Shield purely for DDoS protection of their applications and infrastructure

Disaster Recovery

AWS Shield does not directly support disaster recovery scenarios and does not integrate with AWS Elastic Disaster Recovery. However, Shield provides crucial availability

protection during disasters by maintaining DDoS mitigation capabilities across AWS regions:

- In disaster recovery architectures, Shield protections should be configured for both primary and secondary regions
- Shield's high availability design ensures continued DDoS protection even during regional failures, supporting overall disaster recovery objectives by maintaining application availability during recovery operations

Recovery Objectives

AWS Shield helps customers meet aggressive RTO objectives by providing immediate, automatic DDoS mitigation without manual intervention. Shield Standard offers real-time protection with no recovery delay. Shield Advanced provides faster detection and mitigation through health-based detection and proactive SRT engagement. The service maintains continuous protection availability across AWS's global infrastructure, supporting near-zero RTO for DDoS-related incidents. For RPO objectives, Shield's real-time nature means no data loss during DDoS attacks, though customers must implement separate backup strategies for comprehensive data protection.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/general/latest/gr/shield.html

FAQ: https://aws.amazon.com/shield/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/waf/latest/developerguide/shield-chapter.html

User Guide: https://docs.aws.amazon.com/waf/latest/developerguide/getting-started-ddos.html

API Reference: https://docs.aws.amazon.com/waf/latest/DDOSAPIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/shield/pricing/

Cost Optimization

AWS Shield offers several unique cost optimization features. Shield Standard is completely free for all AWS customers with no usage charges:

- Shield Advanced includes DDoS cost protection through service credits that cover usage spikes caused by DDoS attacks, preventing unexpected bills
- The subscription covers standard AWS WAF capabilities for protected resources, eliminating separate WAF charges
- Consolidated billing allows one Shield Advanced subscription to cover all accounts in an AWS Organizations family
- For multiple organizations, customers can request fee waivers to pay one subscription across all organizations
- The service's automatic mitigation reduces the need for expensive manual intervention and additional capacity provisioning during attacks

Savings Considerations

Main cost savings with AWS Shield come from avoided downtime and the DDoS cost protection feature. Shield Standard eliminates the need for third-party DDoS protection services for basic protection:

- Shield Advanced prevents revenue loss from DDoS-induced outages while providing cost protection against scaling charges during attacks
- The included AWS WAF capabilities reduce separate security tool costs
- Automated mitigation reduces operational overhead and the need for dedicated security personnel during incidents
- The service's integration with AWS infrastructure eliminates data transfer costs between separate security appliances
- For high-value applications, the cost of Shield Advanced is typically offset by preventing a single successful DDoS attack that could cause significant business impact and recovery costs