Service Name

Amazon GuardDuty

Service Overview

Amazon GuardDuty is an intelligent threat detection service that continuously monitors AWS accounts, workloads, and data for malicious activity and unauthorized behavior. It uses artificial intelligence (AI), machine learning (ML), anomaly detection, and integrated threat intelligence to identify known attack patterns and potential security issues across multiple AWS data sources including CloudTrail logs, VPC Flow Logs, DNS query logs, Amazon S3 data events, Amazon Aurora login events, AWS Backup data, and runtime activity for Amazon EKS, Amazon EC2, Amazon ECS, and serverless container workloads. GuardDuty provides fully managed, scalable threat detection with one-step deployment requiring no additional software or infrastructure to deploy and manage.

Key Use Cases

- Account-level threat detection: Detecting unauthorized access, credential compromise, and anomalous API activities across AWS accounts
- Container and Kubernetes security: Monitoring Amazon EKS clusters for container-based exploits and unauthorized access through audit logs and runtime monitoring
- Data protection and compliance: Monitoring S3 buckets for data exfiltration attempts, unauthorized policy changes, and malware in stored objects
- Database security monitoring: Analyzing Amazon Aurora and RDS login activity for potential access threats and unauthorized database activities
- Multi-stage attack detection: Using Extended Threat Detection to correlate events across multiple data sources and identify sophisticated attack sequences
- Malware detection: Scanning EC2 instances, EBS volumes, S3 objects, and AWS Backup data for malware and malicious files

Features

- **Foundational Threat Detection**: Continuously monitors CloudTrail management events, VPC Flow Logs, and DNS query logs using machine learning and threat intelligence
- **S3 Protection**: Monitors S3 buckets for potential security risks including data exfiltration attempts and unauthorized policy changes
- **EKS Protection**: Analyzes Kubernetes audit logs from Amazon EKS clusters to detect container-based exploits and unauthorized activities
- **Runtime Monitoring**: Provides deeper visibility into threats by analyzing operating system-level events on EC2 instances, EKS clusters, and container workloads

- **Malware Protection**: Scans EBS volumes, EC2 instances, S3 objects, and AWS Backup data for malware without requiring agents
- **RDS Protection**: Analyzes login activity for Amazon Aurora and RDS databases to detect potential access threats
- **Lambda Protection**: Monitors Lambda function network activity through VPC Flow Logs to detect threats in serverless environments
- **Extended Threat Detection**: Uses AI/ML to correlate security signals across data sources and identify multi-stage attack sequences with Critical severity findings

Value Proposition

GuardDuty provides comprehensive, intelligent threat detection with no upfront infrastructure investment or ongoing maintenance requirements. It offers immediate deployment across AWS environments with machine learning-powered detection optimized specifically for cloud threats:

- The service provides cost-effective pay-as-you-go pricing with a 30-day free trial, automatic scaling without performance impact, and seamless integration with other AWS security services
- GuardDuty's Extended Threat Detection capabilities use advanced AI/ML to identify sophisticated multi-stage attacks that traditional security tools might miss, while its protection plans offer specialized monitoring for containers, databases, serverless functions, and data storage with industry-leading threat intelligence from AWS and third-party sources

Service Integration

GuardDuty integrates natively with core AWS services for comprehensive security coverage. It automatically analyzes data from AWS CloudTrail, Amazon VPC Flow Logs, Route 53 DNS logs, Amazon S3, Amazon EKS, Amazon Aurora, Amazon RDS, AWS Lambda, and AWS Backup:

- For response and automation, GuardDuty integrates with Amazon EventBridge for real-time event processing, Amazon SNS for notifications, AWS Lambda for automated remediation, and Amazon CloudWatch for monitoring and alerting
- It works seamlessly with AWS Security Hub for centralized security posture management, Amazon Detective for investigation workflows, AWS Organizations for multi-account management, and AWS IAM for access control
- GuardDuty findings can be exported to Amazon S3 for long-term storage and analysis beyond the 90-day retention period

Onboarding and Offboarding

Getting started with GuardDuty requires only a few clicks in the AWS Management Console with no additional software or infrastructure deployment. Customers can enable

GuardDuty in standalone account environments by opening the GuardDuty console, selecting 'Amazon GuardDuty - All features', and clicking 'Get started' followed by 'Enable GuardDuty':

- For multi-account environments, customers can designate a GuardDuty administrator account and add member accounts through AWS Organizations or invitation-based management
- GuardDuty immediately begins monitoring foundational data sources upon activation, with Extended Threat Detection enabled by default
- Customers can generate sample findings to familiarize themselves with the interface and configure automated responses through EventBridge integration with SNS topics or Lambda functions for immediate operational readiness

Getting Started Guide:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_settingup.html

Data Removal

Customers can suspend GuardDuty to stop monitoring and finding generation while retaining existing findings, or completely disable GuardDuty to permanently delete all findings and configurations. Before offboarding, all member accounts must be disassociated or deleted. Suspending preserves data for potential re-enablement, while disabling permanently removes all GuardDuty data and cannot be recovered. Malware Protection for S3 operates independently and requires separate management during offboarding.

Backup/Restore and Disaster Recovery

GuardDuty itself does not provide backup and disaster recovery capabilities as it is a monitoring and threat detection service. However, it enhances backup security through Malware Protection for AWS Backup, which scans backup data for malware threats. GuardDuty findings can be exported to Amazon S3 for indefinite retention beyond the default 90-day period, providing long-term security event archival.

Backup Capabilities

GuardDuty does not have traditional backup capabilities as it is a security monitoring service. However, it integrates with AWS Backup through Malware Protection for AWS Backup to scan backup data for threats. Customers can export GuardDuty findings to S3 for long-term storage and configure EventBridge integration for automated processing and retention of security events.

Disaster Recovery

GuardDuty does not support disaster recovery scenarios directly as it is a threat detection service. It operates regionally and customers must enable it in each desired region.

GuardDuty enhances overall disaster recovery security posture by monitoring backup data through AWS Backup integration and providing threat detection during recovery operations.

Recovery Objectives

GuardDuty supports recovery objectives indirectly by providing continuous security monitoring during disaster recovery operations and scanning backup data for malware threats. It helps maintain security posture during recovery processes by detecting threats in real-time, ensuring that restored systems and data are not compromised, though it does not directly contribute to RPO/RTO metrics.

Service Constraints

Service Quotas:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_limits.html

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

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/guardduty/latest/ug/

User Guide: https://docs.aws.amazon.com/guardduty/latest/ug/

API Reference: https://docs.aws.amazon.com/guardduty/latest/APIReference/

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/guardduty/pricing/

Cost Optimization

GuardDuty offers several cost optimization features including a 30-day free trial for most protection plans, pay-as-you-go pricing based on data volume analyzed, and volume-based discounts for VPC Flow Logs and DNS query log analysis. Customers can optimize costs by selectively enabling protection plans based on their workload requirements, using trusted IP lists to reduce false positives, and leveraging the usage monitoring dashboard to track spending by data source:

- Malware Protection for S3 includes a 12-month free tier, and incremental scanning reduces costs by only scanning changed data
- The service provides granular cost visibility through the GuardDuty console usage page, allowing customers to monitor estimated monthly spend broken down by individual data sources and protection plans

Savings Considerations

Primary cost savings come from the fully managed service model eliminating infrastructure and operational overhead compared to self-managed threat detection solutions. The pay-as-you-go model means customers only pay for actual data analyzed rather than fixed capacity, with significant volume discounts available:

- The 30-day free trial allows cost evaluation before commitment, and selective protection plan enablement lets customers optimize for their specific security requirements
- GuardDuty's automation capabilities reduce manual security operations costs, while its integration with other AWS services eliminates the need for separate security tools and reduces overall security stack complexity and associated licensing costs