Service Name

AWS Security Hub

Service Overview

AWS Security Hub is a unified cloud security solution that prioritizes critical security issues and helps organizations respond to threats at scale. Security Hub automatically correlates and enriches security signals from multiple sources including posture management, vulnerability management (Amazon Inspector), sensitive data discovery (Amazon Macie), and threat detection (Amazon GuardDuty). Through intuitive visualizations and near real-time risk analytics, it transforms complex security signals into actionable insights that enable informed security decisions. Security Hub includes automated response workflows, integrated ticketing systems, and exposure findings to help remediate risks, improve team productivity, and minimize operational disruptions across cloud environments.

Key Use Cases

- Centralized security operations: Unify security management across multiple AWS accounts and services with consolidated visibility and standardized finding formats
- Security posture management: Continuously monitor cloud configurations against security best practices and regulatory compliance frameworks like CIS, PCI DSS, and NIST
- Threat detection and response: Correlate security findings from multiple services to identify exposures, potential attack paths, and automate incident response workflows

Features

- **Exposure Findings**: Correlates findings from Security Hub CSPM, Amazon Inspector, and other AWS services to detect exploitable vulnerabilities and misconfigurations
- **Attack Path Visualization**: Interactive visualization showing how potential attackers can access and control resources associated with exposure findings
- **Automated Correlation**: Automatically correlates and enriches security signals across multiple AWS services to identify related findings
- **Multi-Account Support**: Centralized management across AWS Organizations with cross-Region aggregation of findings
- **Security Standards Compliance**: Automated security checks against industry frameworks including AWS Foundational Security Best Practices, CIS, PCI DSS, and NIST
- **Automation Rules**: Automated response workflows and integration with ticketing systems like Jira Cloud and ServiceNow ITSM

- **OCSF Integration**: Generates and receives findings in Open Cybersecurity Schema Framework for standardized data exchange
- **Historical Trends**: Up to 1 year of historical data with customizable widgets for exposures, threats, resources, and security coverage

Value Proposition

AWS Security Hub provides unmatched value through its unified approach to cloud security operations, eliminating the need to manage multiple disparate security tools and consoles. Unlike standalone security solutions, Security Hub automatically correlates findings across Amazon GuardDuty, Amazon Inspector, Amazon Macie, and AWS Config to provide contextualized risk prioritization and exposure analysis:

- Its streamlined pricing model consolidates charges across integrated security services, reducing complexity and cost
- The service offers near real-time risk analytics with automated correlation capabilities that transform overwhelming security alerts into prioritized, actionable insights
- Security Hub's deep AWS integration enables automated remediation workflows and seamless multi-account management through AWS Organizations, providing comprehensive security visibility without additional operational overhead

Service Integration

AWS Security Hub deeply integrates with core AWS security services to provide comprehensive coverage. Primary integrations include Amazon GuardDuty for threat detection, Amazon Inspector for vulnerability management, Amazon Macie for sensitive data discovery, and AWS Security Hub CSPM for cloud security posture management:

- Security Hub also integrates with AWS Config for configuration monitoring, AWS Identity and Access Management (IAM) for access control, AWS CloudTrail for API logging, and AWS Lambda for automated response functions
- Additional integrations include Amazon EventBridge for event routing, Amazon CloudWatch for monitoring and metrics, AWS Systems Manager for automated remediation, and AWS Organizations for multi-account management
- Third-party integrations are supported through standardized APIs, enabling connections with SIEM tools, ticketing systems like Jira and ServiceNow, and other security solutions

Onboarding and Offboarding

Customers can get started with AWS Security Hub through a straightforward onboarding process that begins with enabling Security Hub in the AWS Console. For individual accounts, users simply enable Security Hub and choose to enable all capabilities or customize them according to their needs:

- For AWS Organizations, the management account designates a delegated administrator who enables Security Hub and configures member accounts
- Prerequisites include enabling AWS Config and ensuring proper IAM permissions
- The service automatically creates necessary service-linked roles and recorders upon enablement
- Security Hub offers a 30-day free trial period, and customers can enable security standards like AWS Foundational Security Best Practices, CIS benchmarks, or PCI DSS based on their compliance requirements
- Integration with other AWS security services like GuardDuty, Inspector, and Macie can be configured simultaneously for comprehensive coverage

Getting Started Guide:
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-v2-enable.html

Data Removal

Security Hub offboarding involves disabling the service through the AWS Console or API, which removes access to the Security Hub dashboard and stops new finding ingestion. Existing findings are retained according to the service's 90-day retention policy, after which they are automatically deleted. Customers can manually archive findings before offboarding if needed. The service-linked roles and associated resources are cleaned up when Security Hub is disabled. For Organizations, the delegated administrator can disable Security Hub across all member accounts. Customers should ensure any automated workflows or integrations dependent on Security Hub are updated before offboarding to prevent service disruptions.

Backup/Restore and Disaster Recovery

AWS Security Hub operates as a managed service where AWS handles infrastructure resilience and data durability. Security Hub findings and configurations are automatically replicated across multiple Availability Zones within a region for high availability. The service provides cross-Region aggregation capabilities allowing findings to be viewed from a central aggregation region for disaster recovery scenarios. However, Security Hub itself is not a backup service and does not provide backup capabilities for customer data. Organizations must implement separate backup strategies for their underlying AWS resources that Security Hub monitors and configure cross-Region aggregation to maintain security visibility during regional outages.

Backup Capabilities

Security Hub does not provide backup capabilities and is not integrated with AWS Backup. As a security management service, Security Hub focuses on aggregating and analyzing security findings rather than backing up data:

- The service maintains findings for 90 days with automatic retention management

- Organizations requiring backup of security configurations or findings data should implement custom solutions using APIs to export findings data or leverage third-party integrations for long-term storage and analysis of security data

Disaster Recovery

Security Hub supports disaster recovery through its cross-Region aggregation feature, which allows findings from multiple linked regions to be aggregated in a central region. This capability ensures security visibility is maintained even if individual regions experience outages:

- However, Security Hub does not integrate with AWS Elastic Disaster Recovery as it is not a workload that requires disaster recovery orchestration
- The service's multi-AZ architecture and AWS-managed infrastructure provide inherent resilience, and cross-Region aggregation serves as the primary disaster recovery mechanism for maintaining security operations continuity

Recovery Objectives

Security Hub helps customers meet RPO and RTO objectives through its cross-Region aggregation capabilities and near real-time finding correlation. The service provides continuous monitoring with minimal data loss potential (low RPO) through automated finding ingestion from integrated security services. For RTO, Security Hub's cross-Region aggregation ensures security visibility can be quickly restored from alternative regions during outages. The service's automated correlation and exposure findings help prioritize critical security issues, enabling faster incident response times. However, specific RPO/RTO values depend on the underlying AWS services and customer's cross-Region configuration strategy.

Service Constraints

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

FAQ: https://aws.amazon.com/security-hub/features/

Technical Requirements

Service Documentation:
https://docs.aws.amazon.com/securityhub/latest/userguide/index.html

User Guide: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub-v2.html

API Reference:
https://docs.aws.amazon.com/securityhub/1.0/APIReference/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/security-hub/pricing/

Cost Optimization

AWS Security Hub offers unique cost optimization through its streamlined pricing model that consolidates charges across integrated AWS security services. The service uses resource-based pricing anchored on Amazon EC2 instances, eliminating complex per-finding charges:

- Security Hub includes a 30-day free trial and free tiers for finding ingestion events (10,000 per month) and automation rule evaluations (1 million per month)
- The Cost Estimator feature helps organizations compare costs with and without Security Hub, estimate costs before enabling capabilities, and export estimates for budgeting
- Volume pricing reduces per-resource costs for larger deployments
- By centralizing security operations, Security Hub reduces operational overhead and eliminates the need for multiple specialized security tools, providing cost efficiency through unified management and reduced complexity

Savings Considerations

Security Hub delivers significant cost savings by consolidating multiple security tools into a unified solution, reducing licensing costs for disparate security products. The service eliminates operational overhead associated with managing multiple security consoles and tools, reducing staffing costs for security operations teams:

- Automated correlation and prioritization reduce time spent on manual security analysis and false positive investigation
- Cross-Region aggregation minimizes the need for regional security teams and infrastructure
- The streamlined pricing model with volume discounts provides predictable costs compared to pay-per-finding alternatives
- Integration with AWS native services reduces data transfer costs and eliminates the need for third-party security data aggregation solutions
- Organizations can achieve 30-70% cost reduction in security operations through automated workflows and reduced manual intervention requirements