Service Name

AWS Security Hub CSPM

Service Overview

AWS Security Hub Cloud Security Posture Management (CSPM) is a comprehensive cloud security service that helps organizations manage and assess their security state in AWS by collecting security data, analyzing trends, and identifying priority security issues. The service performs automated security best practice checks against AWS resources to identify misconfigurations and evaluate security posture, with alignment to industry and regulatory frameworks including AWS Foundational Security Best Practices, CIS, PCI DSS, and NIST. Security Hub CSPM provides centralized visibility across multiple AWS accounts and regions, consolidates findings from various AWS security services and third-party products, and offers automation features for triaging and remediation through integration with Amazon EventBridge.

Key Use Cases

- Continuous Security Posture Assessment: Automatically evaluate AWS resources against security best practices and compliance frameworks with real-time monitoring and scoring
- Multi-Account Security Management: Centrally manage security across AWS Organizations with delegated administration and cross-region aggregation of findings
- Compliance Monitoring and Reporting: Track compliance status against industry standards like CIS, PCI DSS, and NIST with detailed control findings and security scores

Features

- **Automated Security Checks**: Performs continuous security best practice checks against AWS resources using prepackaged security standards and custom controls
- **Cross-Region Aggregation**: Consolidates findings and provides unified view across multiple AWS regions from a single aggregation region
- **Security Score Calculation**: Evaluates security posture with automated scoring based on control status across all enabled standards
- **Central Configuration**: Enables delegated administrators to configure Security Hub CSPM settings across multiple accounts and organizational units
- **Automation Rules**: Automatically updates findings, triggers responses, and integrates with ticketing, SOAR, and SIEM tools
- **Finding Consolidation**: Aggregates findings from AWS services and partner integrations in standardized AWS Security Finding Format (ASFF)

Value Proposition

Security Hub CSPM provides unmatched value through its comprehensive approach to cloud security posture management with automated, continuous security checks across multiple compliance frameworks simultaneously. Unlike standalone security tools, it offers centralized multi-account management through AWS Organizations integration, reducing operational overhead while improving security coverage:

- The service eliminates the complexity of managing disparate security tools by consolidating findings from multiple AWS services and third-party products into a single standardized format
- Key differentiators include real-time security scoring, cross-region aggregation capabilities, and deep integration with the AWS ecosystem for automated remediation workflows

Service Integration

Security Hub CSPM integrates deeply with core AWS services to provide comprehensive security coverage. Primary integrations include AWS Config for resource configuration monitoring and security checks, Amazon GuardDuty for threat detection findings, Amazon Inspector for vulnerability assessments, and Amazon Macie for sensitive data discovery:

- The service also integrates with AWS Organizations for multi-account management, Amazon EventBridge for automation workflows, AWS CloudTrail for audit logging, and IAM Access Analyzer for access management insights
- Additional integrations include AWS Systems Manager for patch management findings, AWS Firewall Manager for security policy compliance, and Amazon Detective for security investigation capabilities

Onboarding and Offboarding

Getting started with Security Hub CSPM involves enabling the service through the AWS Console, API, or CLI, with two primary setup methods available. Organizations can integrate with AWS Organizations by designating a delegated administrator account and enabling central configuration for multi-account management, or manually enable the service and invite member accounts individually:

- Essential prerequisites include enabling AWS Config with appropriate resource recording in each region where Security Hub CSPM will be used
- Initial setup automatically enables default security standards (AWS Foundational Security Best Practices and CIS AWS Foundations Benchmark) unless configured otherwise
- The service offers a 30-day free trial period to evaluate capabilities before charges begin

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

Data Removal

Offboarding from Security Hub CSPM involves disabling the service through the console or API, which deactivates all standards and controls, stops finding generation and ingestion. Active findings are permanently deleted after 90 days and archived findings after 30 days. To retain findings during offboarding, customers can export them to S3 using custom actions with EventBridge rules before disabling the service. Multi-account environments require disassociating member accounts before the administrator account can be disabled.

Backup/Restore and Disaster Recovery

Security Hub CSPM does not provide traditional backup and restore capabilities as it is a security posture management service that generates findings based on current resource configurations. The service maintains finding history and audit trails, but does not store customer data that requires backup. Findings and configuration data are managed by AWS and replicated across availability zones within each region for high availability.

Backup Capabilities

Security Hub CSPM does not have built-in backup capabilities and does not integrate with AWS Backup service. The service focuses on security posture assessment rather than data backup. Finding data and configurations are managed internally by AWS with built-in redundancy and high availability, but customers cannot perform traditional backup operations on this service data.

Disaster Recovery

Security Hub CSPM does not directly support disaster recovery scenarios and does not integrate with AWS Elastic Disaster Recovery. The service is designed for security monitoring and assessment rather than business continuity. AWS manages the service infrastructure with built-in resilience, but customers should focus on disaster recovery for the underlying AWS resources being monitored by Security Hub CSPM.

Recovery Objectives

Security Hub CSPM does not directly contribute to RPO and RTO objectives as it is not a backup or disaster recovery service. However, it supports business continuity by continuously monitoring security posture and identifying vulnerabilities that could impact recovery processes. The service helps maintain security during disaster recovery scenarios by ensuring recovered resources meet security best practices and compliance requirements.

Service Constraints

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

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

Technical Requirements

Service Documentation:
https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

User Guide: https://docs.aws.amazon.com/securityhub/latest/userguide/

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/cspm/pricing/

Cost Optimization

Security Hub CSMP offers several unique cost optimization opportunities including selective control disabling to reduce security check volumes and associated charges. Organizations can disable controls for global resources in non-primary regions to avoid duplicate charges while maintaining comprehensive coverage:

- The service provides a cost estimator tool for predicting monthly expenses across integrated security services
- Volume pricing tiers reduce per-check costs as usage scales
- Strategic use of central configuration eliminates redundant administrative overhead across multiple accounts
- Customers can optimize AWS Config recording settings specifically for Security Hub CSPM to reduce associated Config charges while maintaining security coverage

Savings Considerations

Primary cost savings stem from consolidating multiple security tools into a single platform, reducing licensing and operational costs. The 30-day free trial allows thorough evaluation before commitment, and volume pricing provides economies of scale for large deployments:

- Integration with existing AWS services eliminates need for third-party security tools and associated data transfer costs

- Automated finding correlation reduces manual security analysis time and associated labor costs
- Central configuration across AWS Organizations significantly reduces administrative overhead compared to managing security tools across individual accounts
- Organizations can strategically disable unnecessary controls and optimize AWS Config resource recording to minimize ancillary service charges while maintaining comprehensive security coverage