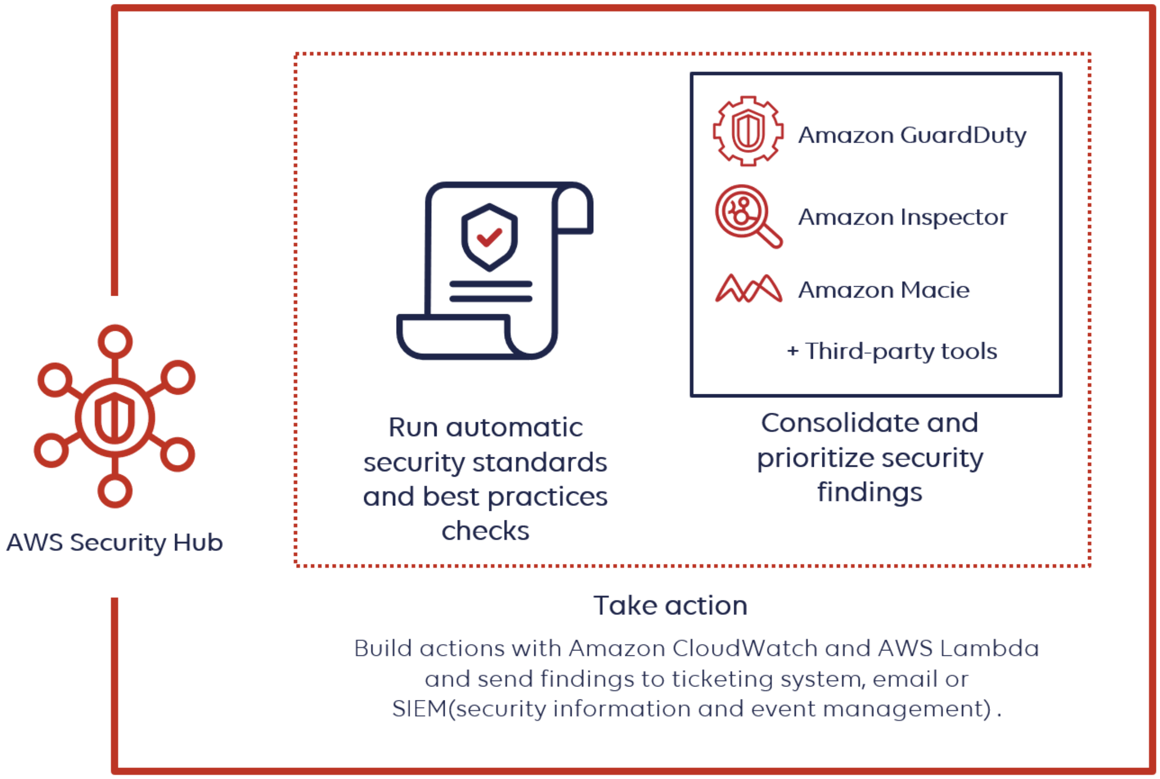
AWS Security Hub

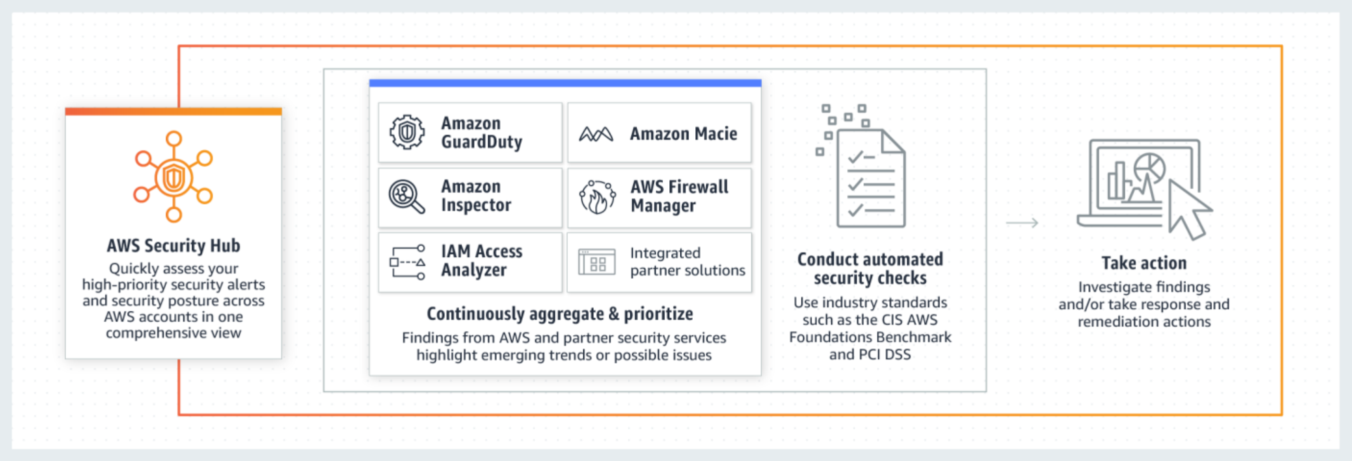
AWS Security Hub helps you compare your environment to industry standards and best practices for security by giving you a thorough overview of your AWS security state.

Security Hub **collects security data from AWS accounts**, services, and supported third-party partner products and assists you in analyzing security trends and identifying the most critical security issues.
It uses the Security Hub API to connect to Security Hub programmatically, which enables you to send the service direct ***HTTPS requests***.


Amazon GuardDuty
Amazon Inspector
Amazon Macie
+ Third-party tools
AWS Security Hub
Run automatic security standards and best practices checks
Consolidate and prioritize security findings
Take action
Build actions with Amazon CloudWatch and AWS Lambda and send findings to ticketing system, email or SIEM(security information and event management) .

How does Security Hub work?

When you enable Security Hub, ***it starts consuming, compiling, organizing, and prioritizing information from your enabled AWS services,*** including Amazon GuardDuty, Amazon Inspector, and Amazon Macie. Integrations with security products from AWS partners are another option. These partner solutions can then send Security Hub findings as well.
Additionally, ***Security Hub produces its own results*** by doing ongoing, automated security checks based on recommended AWS practices and accepted industry standards.
In Security Hub, insights can also be created. When you use the Number by the filter, a group of findings is combined together to form an insight. You can find common security problems that might need to be fixed with the aid of insights. You can generate your own unique insights or choose from the managed insights that Security Hub already offers.

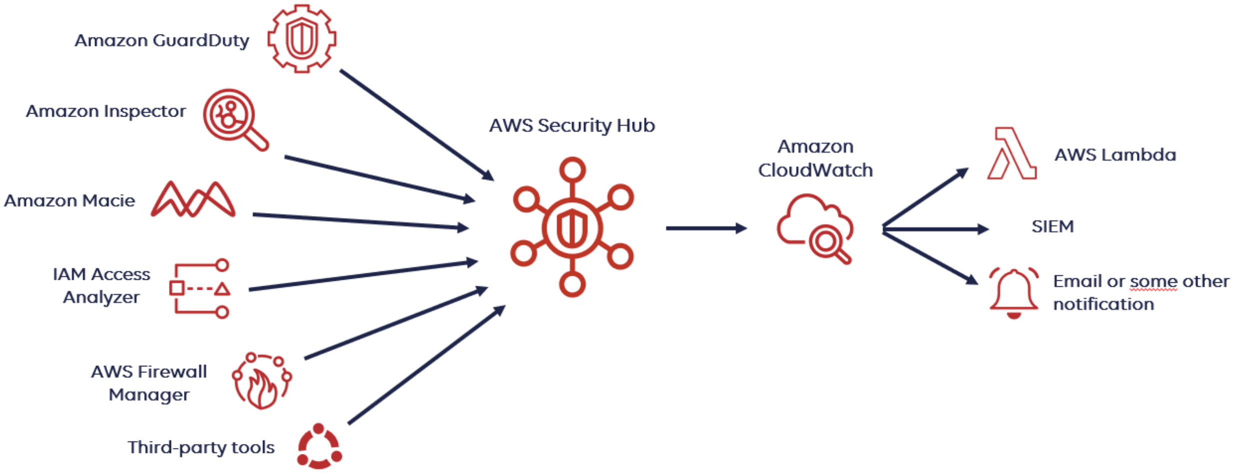

AWS Security Hub
Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view
Amazon GuardDuty
Amazon Macie
Amazon Inspector
AWS Firewall Manager
IAM Access Analyzer
Integrated partner solutions
Continuously aggregate & prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues
Conduct automated security checks
Use industry standards such as the CIS AWS Foundations Benchmark and PCI DSS
Take action
Investigate findings and/or take response and remediation actions

Important: Only results created after you enable Security Hub are detected and consolidated by Security Hub. Security discoveries that were created before you enabled Security Hub are not retrospectively detected and consolidated.

You must enable Security Hub in all AWS Regions to fully comply with CIS AWS Foundations Benchmark security assessments.

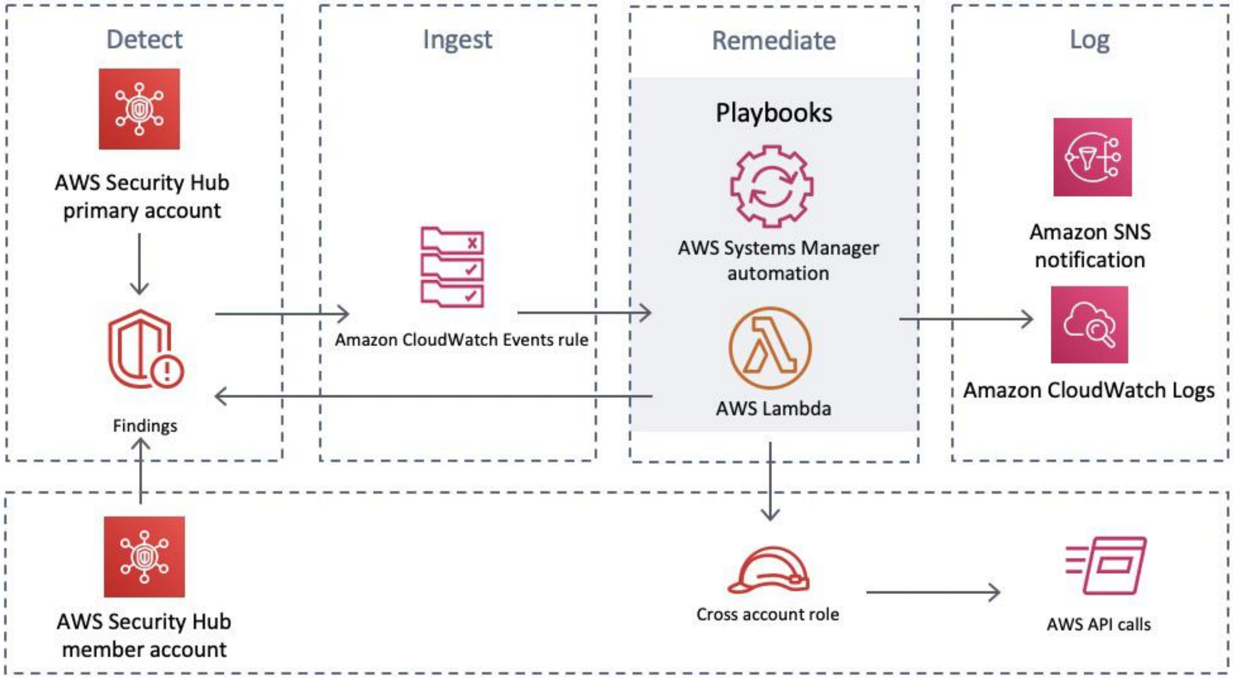
Benefits of AWS Security Hub

- **Reduced effort to collect and prioritize findings:** The work required to gather and prioritize security discoveries across accounts from integrated AWS services and AWS partner products is reduced by Security Hub. It is unnecessary to manage findings data from various forms since Security Hub analyses finding data in accordance with a common finding format.
- **Automatic security checks against best practices and standards:** Based on AWS best practices and industry standards, Security Hub automatically performs continual account-level configuration and security checks.
- **Consolidated view of findings across accounts and providers:** Your security discoveries from different accounts and supplier products are combined by Security Hub, and the results are shown on the Security Hub portal.
- **Ability to automate remediation of findings:** The Amazon EventBridge integration is supported by the Security Hub. You can specify unique actions to be taken when a finding is received in order to automate the remediation of certain findings.



AWS Security Hub features

An automatic, continuous security best practice check is carried out on your AWS resources by the AWS Security Hub, a cloud security posture monitoring service. To make it easier for you to respond to security alerts (i.e. findings) from multiple AWS services and partner products, Security Hub collects them in a common format.

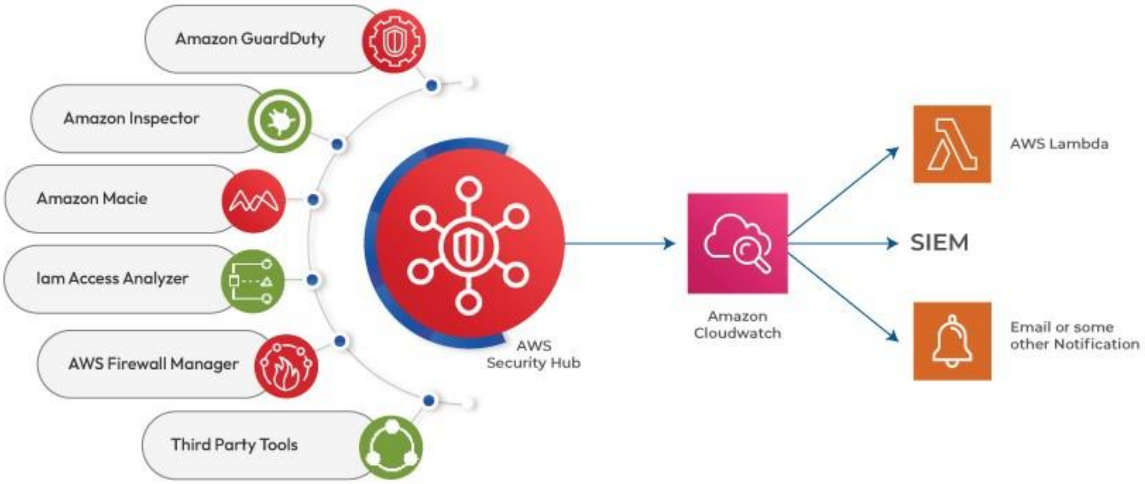


1. **Automated, continuous security best practice checks:** You can access the AWS Foundational Security Best Practices standard using Security Hub's automated security controls.
2. **Consolidated findings across AWS services and partner integrations:** When AWS security services are enabled in your environment, Security Hub automatically gathers and aggregates the results.
3. **A single, standardized data format for all of your findings:** Traditionally, parsing and normalizing each data source to convert it into a common format for search, analytics, response, and remedial actions was required when merging security alerts into a single system.
4. **Security standards aligned to regulatory and industry compliance frameworks:** The Center for Internet Security (CIS) AWS Foundations Benchmark and the Payment Card Industry Data Security Standard (PCI DSS) are two additional standards offered by Security Hub in addition to the AWS Foundational Security Best Practices standard.
5. **An automated response, remediation, and enrichment actions:** Using Security Hub's interaction with Amazon EventBridge, you can design unique automated response, remediation, and enrichment workflows.
6. **Multi-account and AWS Organizations support:** With a few clicks in the AWS Security Hub UI, you can link several AWS accounts and combine findings across those accounts.
7. **Cross-Region aggregation of findings:** To get a centralized view of all your discoveries across all your accounts and all your linked Regions, you can choose an aggregator Region and attach some or all Regions to that aggregator Region using AWS Security Hub.

8. **Integrations with ticketing, chat, incident management, investigation, GRC, SOAR, and SIEM tools:** Security Hub has integrations with numerous ticketing, chat, incident management, threat investigation, Governance Risk and Compliance (GRC), Security Orchestration Automation and Response (SOAR), and Security Information and Event Management (SIEM) tools that can automatically receive findings from Security Hub in addition to dozens of AWS security services and partner products that integrate with Security Hub.

9. **Security scores and summary dashboards:** For each standard, each account across all activated standards, and the entire set of accounts linked to your administrator account, Security Hub delivers a straightforward 0-100 security score.

10. **Filtering, grouping, and saving searches for your findings:** The AWS Security Finding Format's fields can be used to filter findings, and GroupBy statements can be used to group discoveries into buckets.



Security checks	Pricing
First 100,000 checks/account/region/month	$0.0010 per check
Next 400,000 checks/account/region/month	$0.0008 per check
Over 500,000 checks/account/region/month	$0.0005 per check

Ingested Findings	
Ingested findings associated with Security Hub’s security checks	free
First 10,000 events/account/region/month	free
Over 10,000 events/accounts/regions/month	$0.00003 per event

1. **Conduct Cloud Security Posture Management (CSPM):** With built-in mapping capabilities for popular frameworks like CIS, PCI DSS, and more, automated checks based on a collection of security policies selected by professionals can help you reduce your risk and streamline compliance management.
2. **Initiate Security Orchestration, Automation, and Response (SOAR) workflows:** With Security Hub’s interface with EventBridge, you can automatically enhance discoveries, correct them, or submit them to ticketing systems.
3. **Save time and money by simplifying integrations:** By combining the connectors between AWS services and your downstream tooling and by standardizing your findings, you may make data ingestion into your Security Information and Event Management (SIEM), ticketing, and other tools easier and more efficient.
4. **Correlate your security findings to discover new insights:** By searching, correlating, and aggregating various security discoveries by accounts and resources, you can better prioritize the reaction and repair efforts of your central security teams and DevSecOps teams.