AWS Security Hub Pricing

Prioritizes your critical security issues and helps you respond at scale

Plans and Features Free Trial Benefits Pricing Details Pricing Examples FAQs

Pricing Overview

AWS Security Hub prioritizes your critical security issues and unifies your security operations to help you respond at scale. It detects critical issues by correlating and enriching signals across multiple AWS security services, for example, from Amazon GuardDuty for threat detection and Amazon Inspector for vulnerability management. This enables you to surface and prioritize risks in your cloud environment. Security Hub transforms signals into actionable insights that reduce security risks, improve your team's productivity, and protect your cloud environment.

Pricing Model

Security Hub uses a streamlined pricing model with consolidated per-resource charges. When you enable Security Hub, you receive the default level of coverage through the essentials plan and benefit from consolidated pricing across multiple services including Amazon Inspector, Amazon GuardDuty, AWS Security Hub CSPM, and other integrated security services. Existing billing for these security services seamlessly transitions to Security Hub streamlined pricing with no action required. Individual services remain available with standard pricing when Security Hub is not enabled. Security Hub provides the essentials plan as the default level of coverage with add-on capabilities available to extend your security coverage. Note that essentials plan charges are based on all monitored resources, regardless of which capabilities you use.

Essentials plan: Provides risk analytics, vulnerability management, security posture management, and security response management. Default coverage included with Security Hub.

Add-on capabilities to enhance your essentials plan:

- **Threat analytics plan powered by Amazon GuardDuty:** Detects potential security threats and unauthorized activities across your AWS environment.
- **Lambda code scanning powered by Amazon Inspector:** Identifies security vulnerabilities in Lambda function code.

Plans and features

Security Hub essentials plan

Capability	Powered by	Standard pricing	Security Hub essentials plan
EC2 vulnerability scanning	Amazon Inspector	Per instance	Included
EC2 CIS Benchmark assessment	Amazon Inspector	Per assessment per instance	Included
ECR vulnerability scanning	Amazon Inspector	Per image (on-push); Per rescan (retained images)	Included
Lambda vulnerability scanning	Amazon Inspector	Per Lambda function	Included
EC2/EBS malware protection	Amazon GuardDuty	Per GB	Included

Security Hub threat analytics plan

Capability	Powered by	Standard pricing	Security Hub threat analytics plan (requires Security Hub essentials)
CloudTrail threat analytics	Amazon GuardDuty	Per one million events	Per one million events
VPC & DNS logs threat analytics	Amazon GuardDuty	Per GB	Per GB
S3 threat analytics	Amazon GuardDuty	Per one million events	Per GB
EKS threat analytics	Amazon GuardDuty	Per one million events	Per GB
Lambda threat analytics	Amazon GuardDuty	Per GB	Per GB

AWS Lambda code scanning

Capability	Powered by	Standard pricing	Lambda code scanning (requires Security Hub essentials plan)
Lambda code scanning	Amazon Inspector	Per Lambda function	Per Lambda function

Estimate your costs before you start

Before enabling Security Hub, use the Security Hub Cost Estimator to understand your total estimated spend across your entire organization. This tool analyzes your actual AWS resources and current security service usage to provide accurate cost projections across all your accounts and regions. See how Security Hub streamlined pricing compares to your current individual service costs, identify potential savings, and plan your security budget with confidence—all before starting your free trial.

AWS Security Hub Free Trial Summary

Try AWS Security Hub at no cost with a 30-day free trial that includes essentials plan capabilities. Every AWS account in each Region enabled with Security Hub receives a free trial, even if you previously used AWS Security Hub CSPM or Amazon Inspector free trials. Add-on capabilities (threat analytics plan powered by Amazon GuardDuty and AWS Lambda code scanning powered by Amazon Inspector) are not included in the Security Hub free trial, though individual service free trials still apply if you have not used them previously. To help you plan ahead, use the Security Hub Cost Estimator to calculate your expected costs before enabling the service. During the free trial, you can monitor your usage through your AWS billing console to estimate your ongoing costs based on actual usage during the free trial.

Benefits

Why customers choose Security Hub plans

Start with everything you need

The Security Hub essentials plan is the default level of coverage you receive when you enable Security Hub and is required for all Security Hub functionality. It provides security capabilities including risk and exposure analytics, vulnerability management, security posture management, and security response management.

For existing Amazon Inspector customers

Gain streamlined vulnerability management with unified resource pricing for EC2 instance scans (both agent based and agentless), unlimited CIS Benchmark assessments, predictable ECR container image monitoring costs, and flat monthly Lambda function monitoring rates. This consolidation eliminates the complexity of managing multiple pricing models while providing comprehensive vulnerability coverage.

For existing Security Hub CSPM customers

Benefit from transitioning from usage-based to resource-based pricing while gaining more comprehensive vulnerability correlation capabilities, unlimited security checks and finding ingestions, and enhanced compliance monitoring against industry standards with automatic correlation to Amazon Inspector vulnerability data. This shift provides cost predictability while expanding security capabilities.

For existing Amazon GuardDuty customers —

The threat analytics plan powered by Amazon GuardDuty is available as an add-on that enhances your essentials plan by identifying active threats. When you enable the threat analytics plan, you benefit from the Security Hub consolidated pricing model while gaining enhanced risk context through automatic correlation of threat detection findings with vulnerability and compliance data from the essentials plan.

For all customers —

Beyond cost consolidation, the Security Hub essentials plan transforms security operations through automatic correlation of vulnerability findings with compliance checks, reducing alert noise through exposure prioritization. Security teams can focus on contextualized risks that combine threats and vulnerability severity with network exposure and misconfiguration gaps, all while benefiting from centralized operations, automated remediation workflows, and the flexibility to expand into more comprehensive coverage as security needs evolve.

Pricing Details

Security Hub essentials plan | Add-on capabilities

Security Hub essentials plan:

Security Hub essentials plancharges based on the average number of AWS resources monitored per month, with pricing anchored on Amazon EC2 instances

Region:

Europe (London) ▼

Measurement	Price per month
Average number of resource units per month	$4.10 per resource unit per month

Pricing is pro-rated based on the time resources are monitored per month. For detailed information on how pricing is calculated, see our FAQ.

Even though all supported resources are monitored for security risk, per-resource pricing only applies to four primary resource types: EC2 instances, ECR container images, Lambda functions, and IAM users and roles. All other monitored resources are included.

Pricing is anchored on Amazon EC2 instances as 1 resource unit, with AWS Lambda functions at 1/12 of a resource unit (12 functions = 1 resource unit), Amazon ECR container images at 1/18 of a resource (18 images = 1 resource unit), and AWS IAM users and roles at 1/125 of a resource (125 IAM resources = 1 resource unit).

Pricing Examples

Example 1: Small to medium organization

You have one AWS Region, US East (N. Virginia), and one account in your AWS deployment. In one month, your Security Hub environment analyzes 2 million CloudTrail management events, 800 GB of data events, network activity, and other logs, and monitors 500 EC2 instances for security risks.

Monthly cost calculation:

Security Hub essentials plan

EC2 instances: 500 × 1 unit = 500 units

Security Hub essentials plan total: 500 resource units × $3.75 per resource = $1,875.00

Threat analytics plan

CloudTrail management events: 2 million events at $4.00 per million events = $8.00

Data events, network activity, and other logs: 800 GB at $0.55 per GB (first 1,000 GB tier) = $440.00

Threat analytics total: $8+$400 = $448.00

Total monthly cost = $2,323.00

Example 2: Large organization

You have a large enterprise AWS deployment with a mix of different resource types. In one month, your Security Hub environment processes 100 million CloudTrail management events, 500 TB of security data from logs and events, and monitors a diverse set of AWS resources: 1,000 EC2 instances, 1,800 container images, 1,200 Lambda functions, and 120 IAM users.

Monthly cost calculation:

Security Hub essentials plan

EC2 instances: 1,000 × 1 unit = 1,000 units

ECR container images: 1,800 × 1/18 unit = 100 units

Lambda functions: 1,200 × 1/12 unit = 100 units

IAM users and roles: 1,250 × 1/125 unit = 10 units

Total resource units: 1,000 + 100 + 100 + 10 = 1,210 units

Security Hub essentials plan total: = 1,210 resource units × $3.75 per resource = $4,537.50

Threat analytics plan

CloudTrail management events: 100 million events at $4.00 per million events = $400.00 Data events, network activity, and other logs:

For 500 TB (512,000 GB total), the calculation is:

first 1,000 GB at $0.55 per GB = $550.00

next 9,000 GB at $0.25 per GB = $2,250.00

and remaining 502,000 GB at $0.10 per GB = $50,200.00

Total= $53,000.00

Threat analytics total: $400 + $53,000= $53,400.00

Total monthly cost = $57,937.50

Pricing Resources

- Cost Estimator Calculator
- Cloud Economics Resource Center

Page topics

FAQs 12

FAQs

Close all

What does Security Hub cost, and is there a free trial?

Security Hub offers a 30-day free trial that includes Security Hub essentials plan capabilities, which uses resource-based pricing. Every AWS account in each Region receives a free trial, and you remain eligible even if you previously used AWS Security Hub CSPM or Amazon Inspector free trials. Add-on capabilities including threat analytics plan by Amazon GuardDuty and AWS Lambda code scanning powered by Amazon Inspector are not included in the Security Hub free trial. After the free trial, costs are based on the AWS resources you monitor (EC2 instances, container images, Lambda functions, IAM users/roles) and threat analytics plan usage (CloudTrail events and log data volume).

What are the Security Hub pricing plans and what's included?

Security Hub offers the essentials plan as the default, with the ability to add threat analytics plan or Lambda code scanning capabilities as needed. The essentials plan includes risk analytics, vulnerability management, security posture management, and security response management. The threat analytics plan adds Amazon GuardDuty-powered monitoring of AWS account activity, VPC flow logs, DNS logs, and other security data. See the plan details section for complete feature descriptions.

What security value does the Security Hub essentials plan provide?

The Security Hub essentials plan delivers security protection across four key areas:

- **Risk and exposure analytics** - Automatically identifies and prioritizes your most critical security issues by correlating findings across your environment, helping you focus on what matters most and respond faster to threats.
- **Vulnerability management** - Continuously scans your EC2 instances, container images, and Lambda functions for software vulnerabilities and configuration weaknesses, enabling you to remediate security gaps before they can be exploited.
- **Security posture management** - Evaluates your AWS environment against industry security standards and best practices to identify misconfigurations, helping you maintain compliance and reduce your attack surface.
- **Security response management** - Provides a centralized view of your security findings with automated workflows, enabling your team to investigate and remediate issues more efficiently across your entire AWS environment.

Together, these capabilities help you reduce security risks, improve team productivity, and maintain a strong security posture across your cloud infrastructure.

Does Security Hub monitor all my AWS resources?

Yes, Security Hub monitors all relevant AWS resources in your environment to provide more comprehensive security coverage. Essentials plan pricing is based on four resource types: EC2 instances, ECR container images, Lambda functions, and IAM users and roles. This simplified pricing model makes it easier to estimate and manage your Security Hub costs.

Do I need both the Security Hub essentials plan and threat analytics plan?

No, you don't need both plans. The Security Hub essentials plan is the default level of coverage you receive when you enable Security Hub and is required for all Security Hub functionality. It provides security capabilities including risk and exposure analytics, vulnerability management, security posture management, and security response management. The threat analytics plan is an add-on that enhances your essential plan with threat monitoring capabilities powered by Amazon GuardDuty.

The threat analytics plan cannot be used alone - it requires the Security Hub essentials plan as its foundation. While most essentials plan features work independently, malware protection for Amazon EC2 is a special case: it's included in the essentials plan but only functions when you also have the threat analytics plan active, because it relies on GuardDuty threat detection to identify suspicious activity before scanning for malware.

You can start with just the essentials plan and add threat analytics capabilities later as your security monitoring needs evolve.

How can I estimate costs before enabling?

AWS provides a cost estimation tool to help you estimate Security Hub costs before enabling the service. See Security Hub Cost Estimator page for more details.

How can existing Amazon Inspector and AWS Security Hub CSPM customers benefit from the Security Hub essentials plan?

The Security Hub essentials plan combines Amazon Inspector and AWS Security Hub CSPM capabilities into a single, predictable resource-based pricing model that simplifies costs while enhancing security operations.

Existing Amazon Inspector customers gain streamlined vulnerability management with unified resource pricing for EC2 instance scans (both agent based and agentless), unlimited CIS Benchmark assessments, predictable ECR container image monitoring costs, and flat monthly Lambda function monitoring rates. This consolidation eliminates the complexity of managing multiple pricing models while providing comprehensive vulnerability coverage.

Security Hub CSPM customers benefit from transitioning from usage-based to resource-based pricing while gaining more comprehensive vulnerability correlation capabilities, unlimited security checks and finding ingestions, and enhanced compliance monitoring against industry standards with automatic correlation to Amazon Inspector vulnerability data. This shift provides cost predictability while expanding security capabilities.

Beyond cost consolidation, the Security Hub essentials plan transforms security operations for all customers through automatic correlation of vulnerability findings with compliance checks, reducing alert noise through exposure prioritization. Security teams can focus on contextualized risks that combine vulnerability severity with network exposure and compliance gaps, all while benefiting from centralized operations, automated remediation workflows, and the flexibility to expand into more comprehensive threat detection as security needs evolve.

What happens to my existing Amazon Inspector, GuardDuty, and Security Hub CSPM billing when I enable Security Hub?

Existing billing for security services seamlessly transitions to Security Hub streamlined pricing with no action required. You'll receive consolidated charges under Security Hub instead of separate service bills for the capabilities included in Security Hub plans.

How does pricing works across Organization accounts?

Security Hub provides account-level flexibility within AWS Organizations. When you enable Security Hub in an account, that account receives streamlined pricing across security services. When you don't enable Security Hub in an account, that account uses individual service pricing for each security service. This means within a single AWS Organization, you can have some accounts using Security Hub streamlined pricing model while other accounts continue with individual service pricing, determined at the account level based on whether Security Hub is enabled in that specific account.

How is the "average number" calculated for resources like EC2 instances, container images, Lambda functions, and IAM users/roles?

EC2 instances: Average number of EC2 instances = (total hours of active instances / number of hours in a month, i.e., 720 hours). For example, you have 3 instances that were active for different amounts of time during a month: The first for 360 hours, the second for 350 hours, and the third for 10 hours, adding up to a total of 720 hours of active instances. Therefore, 720 hours total of instances being scanned that month / 720 hours in the month = 1 average EC2 instance.

Container images: Number of container images scanned = Number of container images pushed to Amazon ECR each month plus number of container images that are in scope for re-scanning during the month, based on Amazon Inspector re-scan configuration. Amazon Inspector performs an initial scan of each container image pushed to Amazon ECR. Additionally, Amazon Inspector re-scans container images for new vulnerabilities based on the time frames you configure for image push date, image pull date, and image last in-use date. Example: You have 5,000 images in your Amazon ECR repository and push 500 additional images to Amazon ECR in a month. You have configured image monitoring for 14 days based on the last in-use date. During the month, 75 container images from the repository are deployed to Amazon ECS or Amazon EKS clusters. Amazon Inspector monitors and charges based on the actual duration each image is monitored within your configured window - this includes both the 75 active images while they remain in use and the 500 newly pushed images for their respective monitoring periods. Note that charges apply only for the time each image is actually monitored (up to 14 days by default), not necessarily for the entire month, and this monitoring period can be customized based on your needs.

Lambda functions: Eligible Lambda functions are based on functions marked $LATEST and were invoked or updated in the last 90 days. Average number of Lambda functions = (total hours of Security Hub coverage for a Lambda function)/ (number of hours in a month, i.e., 720 hours). Security Hub coverage hours represent the time from when the Lambda function is deployed to the time it is deleted.

Example: You have 3 deployed Lambda functions that were monitored by Security Hub for different amounts of time during a month: The first for 720 hours, the second for 350 hours, and the third for 10 hours, adding up to a total of 1,080 hours of deployed Lambda functions being scanned. Therefore, 1,080 hours total of Lambda functions being scanned that month / 720 hours in the month = 1.5 average Lambda functions.

IAM users and roles: Average number of IAM users and roles = Number of IAM users or roles that existed during the month, prorated daily.

What services or capabilities require separate pricing?

Capabilities not explicitly listed in the Security Hub plans continue to be billed through their original services. For example, you will only receive GuardDuty billing for any remaining GuardDuty capabilities that are not included in the threat analytics plan.

Can I use individual security services without Security Hub?

Yes, individual services like Amazon Inspector, GuardDuty, and Security Hub CSPM remain available with their standard pricing when Security Hub is not enabled.

Learn
What Is AWS?
What Is Cloud Computing?
What Is Agentic AI?
Cloud Computing Concepts Hub
AWS Cloud Security
What's New
Blogs
Press Releases

Resources
Getting Started
Training
AWS Trust Center
AWS Solutions Library
Architecture Center
Product and Technical FAQs
Analyst Reports
AWS Partners

Developers
Builder Center
SDKs & Tools
.NET on AWS
Python on AWS
Java on AWS
PHP on AWS
JavaScript on AWS

Help
Contact Us
File a Support Ticket
AWS re:Post
Knowledge Center
AWS Support Overview
Get Expert Help
AWS Accessibility
Legal

Back to top ↑

Amazon is an Equal Opportunity Employer: Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.

Privacy Site terms Cookie Preferences © 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.