Service Name

Amazon Inspector

Service Overview

Amazon Inspector is an automated vulnerability management service that continuously scans AWS workloads for software vulnerabilities and unintended network exposure. It automatically discovers and assesses Amazon EC2 instances, container images in Amazon ECR, AWS Lambda functions, and code repositories for known vulnerabilities and security issues. The service provides risk-based prioritization with Inspector risk scores, integrates seamlessly with AWS Security Hub and Amazon EventBridge for centralized security management, and supports both agent-based and agentless scanning methods to maximize coverage across diverse infrastructure configurations.

Key Use Cases

- Continuous vulnerability scanning: Automatically assess EC2 instances, Lambda functions, and container images for software vulnerabilities without manual intervention
- DevSecOps integration: Integrate vulnerability scanning into CI/CD pipelines to identify security issues before production deployment
- Multi-account security management: Centrally manage vulnerability assessments across multiple AWS accounts using AWS Organizations with delegated administrator capabilities
- Compliance and governance: Meet security compliance requirements by continuously monitoring workloads for vulnerabilities and generating comprehensive security reports
- Container security: Scan container images in Amazon ECR repositories for operating system packages and programming language vulnerabilities throughout the development lifecycle

Features

- **Automated Discovery and Scanning**: Continuously discovers and scans EC2 instances, Lambda functions, ECR container images, and code repositories without requiring manual configuration
- **Inspector Risk Score**: Provides contextualized risk scoring based on CVE information, network accessibility, and environment-specific factors to prioritize remediation efforts
- **Multi-Scan Methods**: Supports both agent-based scanning using SSM Agent and agentless scanning using EBS snapshots for maximum coverage flexibility

- **AWS Organizations Integration**: Enables centralized management across multiple accounts with delegated administrator capabilities and organization-wide policy enforcement
- **Security Hub Integration**: Automatically publishes findings to AWS Security Hub and Amazon EventBridge for centralized security monitoring and automated response workflows
- **Code Security Scanning**: Scans application source code, dependencies, and Infrastructure as Code for vulnerabilities using SAST, SCA, and IaC analysis
- **CIS Benchmark Assessments**: Performs Center for Internet Security benchmark assessments for operating system security configuration compliance

Value Proposition

Amazon Inspector eliminates the operational overhead of deploying and maintaining traditional vulnerability management solutions by providing fully managed, automated scanning across all AWS workloads. Unlike third-party solutions, Inspector offers native AWS integration with Security Hub, EventBridge, and Organizations, enabling seamless automation and centralized management:

- The service provides highly contextualized risk scoring that considers network accessibility and environment-specific factors, delivering more accurate prioritization than standalone CVE scanners
- With support for both agent-based and agentless scanning, Inspector maximizes coverage while minimizing infrastructure requirements
- The service scales automatically with your AWS environment and includes a 15-day free trial with pay-per-scan pricing that eliminates upfront investments

Service Integration

Amazon Inspector integrates deeply with core AWS security and management services to provide comprehensive vulnerability management. It publishes findings directly to AWS Security Hub for centralized security monitoring and to Amazon EventBridge for automated workflow triggers and notifications:

- The service leverages AWS Systems Manager Agent for agent-based scanning and uses Amazon EBS snapshots for agentless assessments
- Inspector integrates with AWS Organizations for multi-account management and policy enforcement, enabling delegated administrator capabilities
- It works seamlessly with Amazon ECR for container image scanning and AWS Lambda for serverless function assessments
- The service also integrates with developer tools for CI/CD pipeline scanning and exports Software Bill of Materials (SBOM) data for compliance reporting

Onboarding and Offboarding

Getting started with Amazon Inspector requires minimal configuration through the AWS Management Console or APIs. Users can activate Inspector with a single click, which automatically enables all scan types (EC2, ECR, Lambda, and Code Security) by default:

- The service creates necessary service-linked roles automatically and begins discovering eligible resources immediately
- For multi-account environments, organizations can designate a delegated administrator and use AWS Organizations policies for automated deployment across accounts and OUs
- Inspector starts scanning within minutes of activation and provides immediate visibility through the dashboard
- The service includes hybrid scanning by default, combining agent-based and agentless methods for maximum coverage without requiring pre-configuration of scanning infrastructure

Getting Started Guide:
https://docs.aws.amazon.com/inspector/latest/user/getting_started_tutorial.html

Data Removal

Deactivating Amazon Inspector removes all scan settings, suppression rules, and findings data from your account. Users should export findings to Amazon S3 before deactivation to retain vulnerability reports. The deactivation process can be performed through the console or API, and results in immediate cessation of scanning and billing. For organization-managed deployments, deactivation must be done through AWS Organizations policies. Inspector automatically closes and deletes findings after 3 days when resources are terminated or become ineligible for scanning.

Backup/Restore and Disaster Recovery

Amazon Inspector does not provide traditional backup and disaster recovery capabilities as it is a scanning service that generates findings rather than storing critical business data. The service operates regionally and findings are stored within the activated region. Users can export findings and SBOM data to Amazon S3 for external backup purposes. Inspector automatically recreates findings upon resource rescans, making data restoration unnecessary. The service relies on AWS infrastructure resilience and does not require separate disaster recovery planning.

Backup Capabilities

Amazon Inspector does not have built-in backup capabilities and does not integrate with AWS Backup since it is a vulnerability assessment service that generates transient findings data. Users can export findings as reports to Amazon S3 for retention purposes:

- The service automatically manages finding lifecycle, closing findings when vulnerabilities are remediated and recreating them during rescans
- Inspector stores findings regionally and does not require traditional backup mechanisms

Disaster Recovery

Amazon Inspector does not support traditional disaster recovery mechanisms and does not integrate with AWS Elastic Disaster Recovery. The service is regionally deployed and findings are specific to the region where resources are scanned:

- In case of regional failure, Inspector would need to be reactivated in alternate regions where workloads are deployed
- The scanning functionality would resume automatically once resources are available in the recovery region without requiring data restoration

Recovery Objectives

Amazon Inspector does not directly contribute to RPO and RTO objectives as it is a vulnerability assessment service rather than a business continuity solution. However, Inspector supports security resilience by continuously identifying vulnerabilities that could impact system availability. The service enables rapid security assessment of disaster recovery environments by automatically scanning recovered resources. Inspector's continuous scanning ensures that security posture is maintained during recovery scenarios, supporting overall business continuity objectives through proactive vulnerability management.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/inspector/latest/user/quotas.html

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

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/inspector/latest/user/index.html

User Guide: https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html

API Reference: https://docs.aws.amazon.com/inspector/v2/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/inspector/pricing/

Cost Optimization

Amazon Inspector offers several cost optimization strategies including resource exclusion through tagging to prevent scanning of non-critical instances, which eliminates unnecessary charges. The service provides a 15-day free trial for each scan type, allowing customers to evaluate usage before incurring costs:

- Organizations can optimize costs by using hybrid scanning mode that automatically selects the most cost-effective scanning method (agent-based vs
- agentless) based on instance characteristics
- Customers can also leverage suppression rules to filter out acceptable findings, reducing noise and focusing scanning resources on critical vulnerabilities
- The service supports selective activation of scan types, enabling customers to enable only required scanning capabilities rather than all features

Savings Considerations

The primary cost savings with Amazon Inspector come from eliminating the need for traditional vulnerability scanning infrastructure and associated operational overhead. Customers save on licensing costs for third-party vulnerability scanners, dedicated scanning servers, and specialized security staff for tool management:

- The pay-per-scan pricing model eliminates upfront capital investments and scales costs directly with usage
- Inspector's automated discovery and continuous scanning reduce the need for manual security assessments and penetration testing
- Integration with existing AWS services like Security Hub and EventBridge eliminates costs for additional integration tools
- The service's ability to automatically close remediated findings reduces ongoing storage and management costs compared to solutions that accumulate stale vulnerability data