**Amazon Security Services**

**Contents**

Services Protected by [Amazon Security Services 2](#_Toc115190395)

[Amazon Inspector 2](#_Toc115190396)

[How Inspector Protects EC2 ? 3](#_Toc115190398)

[How Inspector Protects ECR ? 4](#_Toc115190399)

[Common Vulnerabilities found by Inspector 4](#_Toc115190398)

[Amazon GuardDuty 4](#_Toc115190402)

[EC2 Protection 5](#_Toc115190398)

[S3 bucket Protection 5](#_Toc115190398)

[Kubernetics Protection 5](#_Toc115190398)

[Common Malwares found by GuardDuty 6](#_Toc115190398)

**Amazon Security Services**

AWS provides **services that help you protect your data, accounts, and workloads from unauthorized access**. AWS data protection services provide encryption and key management and threat detection that continuously monitors and protects your accounts and workloads.

**Services Protected by Amazon Inspector**

The services protected by Amazon Inspector are Elastic Compute Cloud (EC2) Instances of AWS and Amazon Elastic Container Registry (ECR).

**How Inspector Protects EC2?**

Amazon Inspector is a service that automates security assessments and network accessibility testing for[**AWS EC2**](https://intellipaat.com/blog/what-is-amazon-ec2-in-aws/) instances. It aids in the detection of vulnerabilities in your EC2 instances and apps. Furthermore, it enables you to make security testing a more frequent event as part of the development and IT operations.

Amazon Inspector displays a clear list of security and compliance issues that have been prioritized by severity level. Furthermore, these discoveries may be analysed directly or as part of full evaluation records accessible through the API or the AWS Inspector UI. AWS Inspector security evaluations assist you in detecting unauthorized network access to EC2 instances as well as vulnerabilities on those EC2 instances.

It operates by first defining a target set of resources using tags, then configuring an assessment template that defines what we’re looking for (common vulnerabilities and exploits (CVEs), PCI requirements, and so on) and running an assessment against our target resources, examining the research results and reducing the issues discovered.

Amazon Inspector conducts an automated examination and delivers results reports with recommendations for environmental protection. To utilize this service, you must establish an AWS collection containing all the resources required for the application to progress and be tested.

It is then followed by the addition and execution of [**cloud security**](https://intellipaat.com/blog/what-is-cloud-security/) practices. You may also specify the length of the exam, which can range from 15 minutes to 12 hours or last for one day.

On the EC2 computers that host the application, an Inspector Agent observes the network, file system, and process activities. After gathering all of the necessary information, it is compared to the built-in security rules to discover security or compliance concerns.

**How Inspector Protects ECR?**

Amazon Inspector scans container images stored in Amazon ECR for software vulnerabilities to generate **Package Vulnerability** findings. For more information, see [Finding types in Amazon Inspector](https://docs.aws.amazon.com/inspector/latest/user/findings-types.html).

When you enable Amazon Inspector scans for Amazon ECR, you set Amazon Inspector as your preferred scanning service for your private registry. This replaces the default [**Basic scanning**](https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html), which is provided as a free service by Amazon ECR, with **Enhanced scanning**, which is provided and billed through Amazon Inspector.

The enhanced scanning provided by Amazon Inspector gives you the benefit of vulnerability scanning for both operating system and programming language packages at the registry level. You can review findings discovered using enhanced scanning at the image level, at each layer of the image, and on the Amazon ECR console. Additionally, you can review and work with these findings in other services not available for basic scanning findings, including AWS Security Hub and Amazon EventBridge.

Enhanced scanning gives you a choice between continuous scanning or on-push scanning at the repository level. Continuous scanning includes on-push scans and automated rescans. On-push scanning scans only when you push an image. For both options you can refine the scanning scope through inclusion filters.

Automated rescans are triggered for container images based on whether you use the continuous or on-push option in your **Enhanced scanning** settings. Whenever Amazon Inspector adds a new Common Vulnerabilities and Exposures (CVE) item to its database, eligible container images in Amazon ECR repositories configured with continuous scanning are scanned in response.

**List of common Vulnerabilities found by Inspector**

### Basic Search of CVE List

Searching the [CVE List](https://cve.mitre.org/cve/) provides you with an individual [CVE Record](https://cve.mitre.org/about/faqs.html#what_is_cve_record) and/or a list of all CVE Records.

#### Search by CVE ID

If you know the CVE ID number for a problem (for example, CVE-2009-0021), search by the number to find its description.

#### Search by keyword

Use a keyword to search the CVE List to find the official CVE Record for a known vulnerability.

#### Use specific keywords

You must use very specific keywords, such as an application name, when searching the CVE List.

Examples: **Sendmail, wu-ftp, ToolTalk, ps**, etc.

**Services Protected by GuardDuty**

GuardDuty is an intelligent threat detection service that continuously monitors your AWS accounts, Amazon Elastic Compute Cloud (EC2) instances, Amazon Elastic Kubernetes Service (EKS) clusters, and data stored in Amazon Simple Storage Service (S3) for malicious activity without the use of security software or agents.

**EC2 Protection**

Once the feature is enabled, GuardDuty **Malware Protection** will initiate a malware scan in response to relevant EC2 findings. You don't have to deploy any agents, there are no log sources to enable, and there are no other configuration changes to make.

**S3 Bucket Protection**

S3 protection enables Amazon GuardDuty to monitor object-level API operations to identify potential security risks for data within your S3 buckets.

GuardDuty monitors threats against your Amazon S3 resources by analyzing AWS CloudTrail management events and CloudTrail S3 data events. These data sources monitor different kinds of activity, for example, CloudTrail management events for S3 include operations that list or configure S3 buckets.

GuardDuty monitoring of CloudTrail management events is on by default for all accounts that have enabled GuardDuty and is not configurable. CloudTrail S3 data event logs are a configurable data source in GuardDuty. By default, S3 protection is enabled for new detectors, for accounts created before the addition of S3 protection this data source must be enabled manually. The processes for enabling or disabling S3 data event monitoring is covered in this topic.

It is strongly recommended that you enable S3 protection in GuardDuty. If the feature is disabled, GuardDuty is unable to fully monitor or generate findings for suspicious access to data stored in your S3 buckets.

**Kubernetes Protection**

GuardDuty Kubernetes Protection enables Amazon GuardDuty to detect suspicious activities and potential compromises of your Kubernetes clusters within Amazon Elastic Kubernetes Service (Amazon EKS).

Kubernetes Protection is an optional enhancement that enables GuardDuty to consume Kubernetes data sources.

It is recommended that you do not disable Kubernetes Protection in GuardDuty. If the feature is not enabled, the ability of GuardDuty to monitor or generate findings for suspicious activity within your Amazon EKS environment is limited.

**List of malwares detected by GuardDuty**

Malware Protection scans for threats such as **trojans, worms, crypto miners, rootkits, and bots**, that might be used to compromise workloads, repurpose resources for malicious use, and gain unauthorized access to data.

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\_finding-types-ec2.html

**Examples**

## **Trojan:EC2/DNSDataExfiltration**

### An EC2 instance is exfiltrating data through DNS queries.

**Default severity: High**

* **Data source:** DNS logs

This finding informs you that the listed EC2 instance in your AWS environment is running malware that uses DNS queries for outbound data transfers. This type of data transfer is indicative of a compromised instance and could result in the exfiltration of data. DNS traffic is not typically blocked by firewalls. For example, malware in a compromised EC2 instance can encode data, (such as your credit card number), into a DNS query and send it to a remote DNS server that is controlled by an attacker.

Remediation recommendations:

If this activity is unexpected, your instance may be compromised.

## **2. CryptoCurrency:EC2/BitcoinTool.B!DNS**

### An EC2 instance is querying a domain name that is associated with cryptocurrency-related activity.

**Default severity: High**

* **Data source:** DNS logs

This finding informs you that the listed EC2 instance in your AWS environment is querying a domain name that is associated with Bitcoin or other cryptocurrency-related activity. Bitcoin is a worldwide cryptocurrency and digital payment system that can be exchanged for other currencies, products, and services. Bitcoin is a reward for bitcoin-mining and is highly sought after by threat actors.

**Remediation recommendations:**

If you use this EC2 instance to mine or manage cryptocurrency, or this instance is otherwise involved in blockchain activity, this finding could be expected activity for your environment. If this is the case in your AWS environment, we recommend that you set up a suppression rule for this finding. The suppression rule should consist of two filter criteria. The first criteria should use the **Finding type** attribute with a value of CryptoCurrency:EC2/BitcoinTool.B!DNS. The second filter criteria should be the **Instance ID** of the instance involved in blockchain activity. To learn more about creating suppression rules see [Suppression rules](https://docs.aws.amazon.com/guardduty/latest/ug/findings_suppression-rule.html).

If this activity is unexpected, your instance is likely compromised.

## **3. Impact:EC2/PortSweep**

### An EC2 instance is probing a port on a large number of IP addresses.

**Default severity: High**

* **Data source:** VPC Flow Logs

This finding informs you the listed EC2 instance in your AWS environment is probing a port on a large number of publicly routable IP addresses. This type of activity is typically used to find vulnerable hosts to exploit.

**Remediation recommendations:**

If this activity is unexpected, your instance may be compromised.