How to Detect Threats in Your AWS Environment with Amazon GuardDuty

Amazon GuardDuty provides a cost-effective and easy-to-deploy threat detection service that continuously monitors for unauthorized activity in the cloud — all with a single click of a button.

How do threats get in?

Common user mistakes that could result in security issues include:

Applications with unpatched vulnerabilities or insecure code

Misconfigured Identity and Access Management (IAM) permissions

Insecure Virtual Private Cloud (VPC) configurations

Misconfigured data storage buckets that are publicly accessible

The use of default passwords or insecurely stored passwords and keys

Why are some threats difficult for users to detect?

IT security professionals have a unique set of challenges, such as:

Outside parties that adapt their Tactics, Techniques, and Procedures (TTPs)

Shortage of the right security skills, making it harder to quickly detect and respond to threats

Dynamic nature of projects creates avenues for misconfiguration

Alert overload and fatigue distract from critical alerts that need attention

So, what steps can you take to help protect your cloud environment?

Strategy: Automate with managed threat detection

To improve your overall security posture, you need a managed threat detection service that:

Continuously monitors for unauthorized activities using analytic techniques that include machine learning

Provides high time to value (i.e., gets up and running fast with low false positives)

Integrates with other security tools to enable an ecosystem of layered threat detection

Leverages key AWS data sources and can incorporate custom threat lists and trusted IP lists

Enables automation for response actions to unauthorized activity

Stronger, smarter, and more automated security reduces distractions and enables you to focus your expertise where it really matters.

Amazon GuardDuty can help

Amazon GuardDuty is a managed threat detection service that continuously monitors for unauthorized behavior to help protect Amazon Web Services accounts and workloads.

GuardDuty has impressive features that hit all the high points:

Managed threat detection

Easy one-click activation

No architectural or performance impact

Continuous monitoring for indicators of compromise

Discovery of threats associated with users, accounts, and workloads

Findings provided in minutes and prioritized by potential threat

No agents, sensors, or network appliances necessary

Built-in anomaly detection with machine learning

Get Started with Amazon GuardDuty

Try Amazon GuardDuty for 30 days at no cost. You will receive full access to GuardDuty features and its detection findings during the free trial.

aws