Monitor Malware Risks in AWS S3 and Azure Storage with Cloud Malware

Contents

Introduction

This document describes how to monitor and address malware risks in AWS S3 and Azure Storage with Cloud Malware.

Overview

With this feature, you can now discover and monitor malware risks within your AWS S3 and Azure Storage environments. A key use case is identifying files infected with malware that can steal credentials or exploit vulnerabilities, increasing the risk of lateral movement within your environment or to other environments.

Supported Response Actions for AWS and Azure

Currently, only monitoring is supported as a response action for AWS S3 and Azure Storage. Automatic remediation actions, such as file deletion or quarantine, are not available. This limitation prevents accidental disruption of mission-critical services while still allowing you to monitor for sensitive data exposure and malware risks.

Related Resources

- Enable Cloud Malware Protection for AWS Tenants
- Enable Cloud Malware Protection for Azure Tenants