Monitor Sensitive Data Exposure in AWS S3 and Azure Storage with DLP

Contents

Introduction

This document describes how to monitor sensitive data exposure in AWS S3 and Azure Storage using Data Loss Prevention (DLP).

Overview

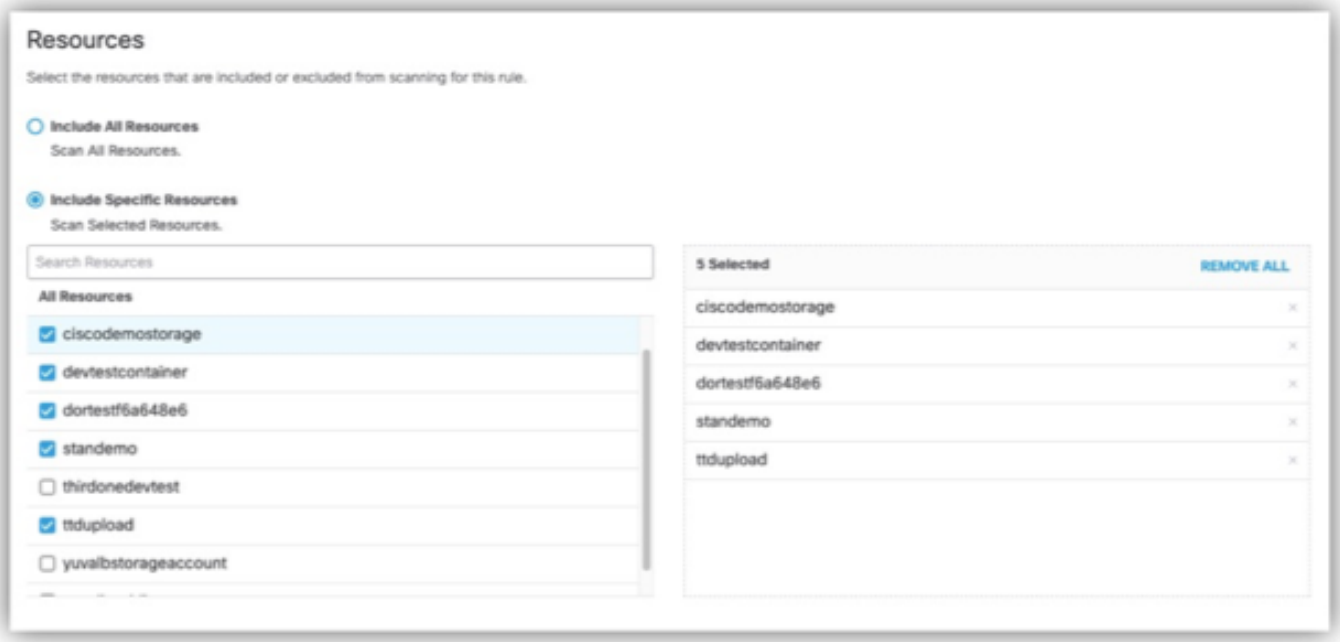
With new connectors for AWS S3 and Azure Storage, you can now scan for sensitive data exposure within your cloud environments. These capabilities help you discover and monitor exposed credentials—such as API keys, secrets, and tokens—as well as sensitive data, including personally identifiable information (PII), financial records, and healthcare information that may be exposed to the public web.

What Is Scanned in AWS S3 and Azure File Storage?

- **AWS S3:**
  DLP performs both an initial discovery scan for preexisting sensitive data and continuous monitoring for new or updated files. You can specify which S3 buckets to scan by selecting them in your DLP rule.

- **Azure File Storage:**
  DLP supports initial discovery and ongoing monitoring for new or updated files. You can choose the specific Azure containers to scan within your DLP rule.

You can tailor DLP scanning by selecting the exact AWS S3 buckets or Azure containers to match your needs and priorities.



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 approach avoids the risk of disrupting mission-critical IaaS environments while still enabling you to monitor sensitive data exposure effectively.

Locate AWS S3 Buckets and Azure Storage Blobs for Manual Remediation

To assist with manual remediation, the DLP report includes detailed information:

- The report displays the actual S3 bucket or blob name, making it easy to search in AWS or Azure consoles.
- Each DLP violation event provides the resource name, the destination URL, and, when available, the resource ID.
- Use this information to locate and address DLP violations efficiently within your AWS S3 buckets and Azure storage blobs.

Related Resources

Refer to Umbrella documentation for detailed guidance:

- Enable SaaS API Data Loss Protection for AWS Tenants
- Enable SaaS API Data Loss Protection for Azure Tenants
- Add a SaaS API Rule to the Data Loss Prevention Policy
- Data Loss Prevention Report