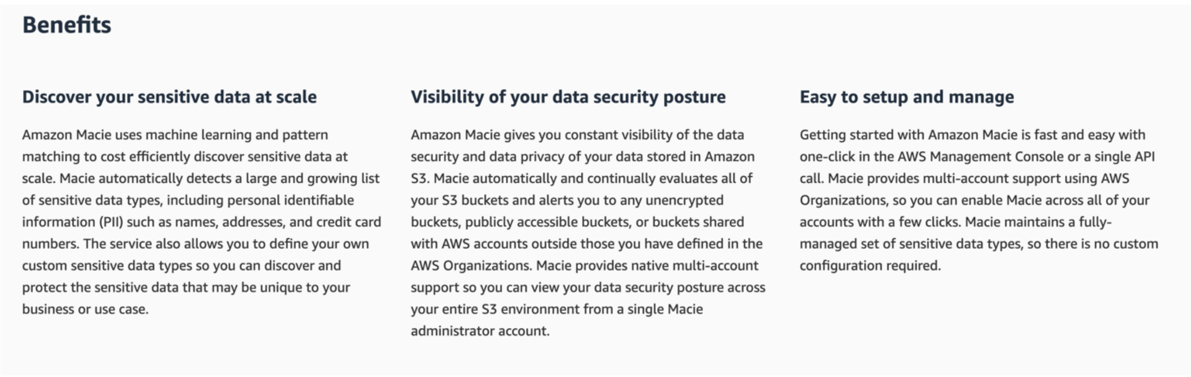
AWS - Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

- As organizations manage growing volumes of data, identifying and protecting their sensitive data at scale can become increasingly complex, expensive, and time-consuming.
- Amazon Macie automates the discovery of sensitive data at scale and lowers the cost of protecting your data.
- Macie automatically provides an inventory of Amazon S3 buckets including
  - a list of unencrypted buckets,
  - publicly accessible buckets, and
  - buckets shared with AWS accounts outside those you have defined in AWS Organizations.
- Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).
- Macie's alerts, or findings, can be searched and filtered in the AWS Management Console and sent to Amazon CloudWatch Events for easy integration with existing workflow or event management systems, or to be used in combination with AWS services, such as AWS Step Functions to take automated remediation actions.
- This can help you meet regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Privacy Regulation (GDPR).
- You can get started with Amazon Macie with a few clicks in the AWS Management Console.



Benefits

Discover your sensitive data at scale

Amazon Macie uses machine learning and pattern matching to cost efficiently discover sensitive data at scale. Macie automatically detects a large and growing list of sensitive data types, including personal identifiable information (PII) such as names, addresses, and credit card numbers. The service also allows you to define your own custom sensitive data types so you can discover and protect the sensitive data that may be unique to your business or use case.

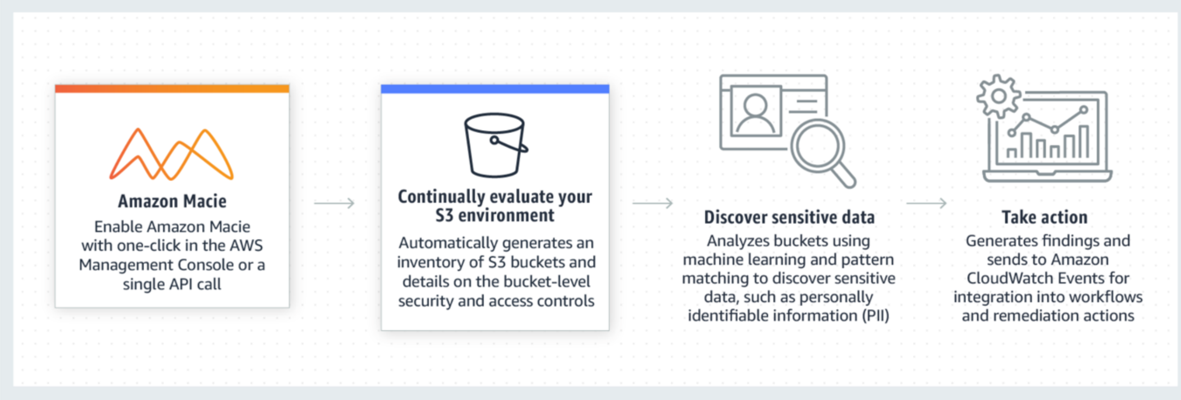
Visibility of your data security posture

Amazon Macie gives you constant visibility of the data security and data privacy of your data stored in Amazon S3. Macie automatically and continually evaluates all of your S3 buckets and alerts you to any unencrypted buckets, publicly accessible buckets, or buckets shared with AWS accounts outside those you have defined in the AWS Organizations. Macie provides native multi-account support so you can view your data security posture across your entire S3 environment from a single Macie administrator account.

Easy to setup and manage

Getting started with Amazon Macie is fast and easy with one-click in the AWS Management Console or a single API call. Macie provides multi-account support using AWS Organizations, so you can enable Macie across all of your accounts with a few clicks. Macie maintains a fully-managed set of sensitive data types, so there is no custom configuration required.

How it works



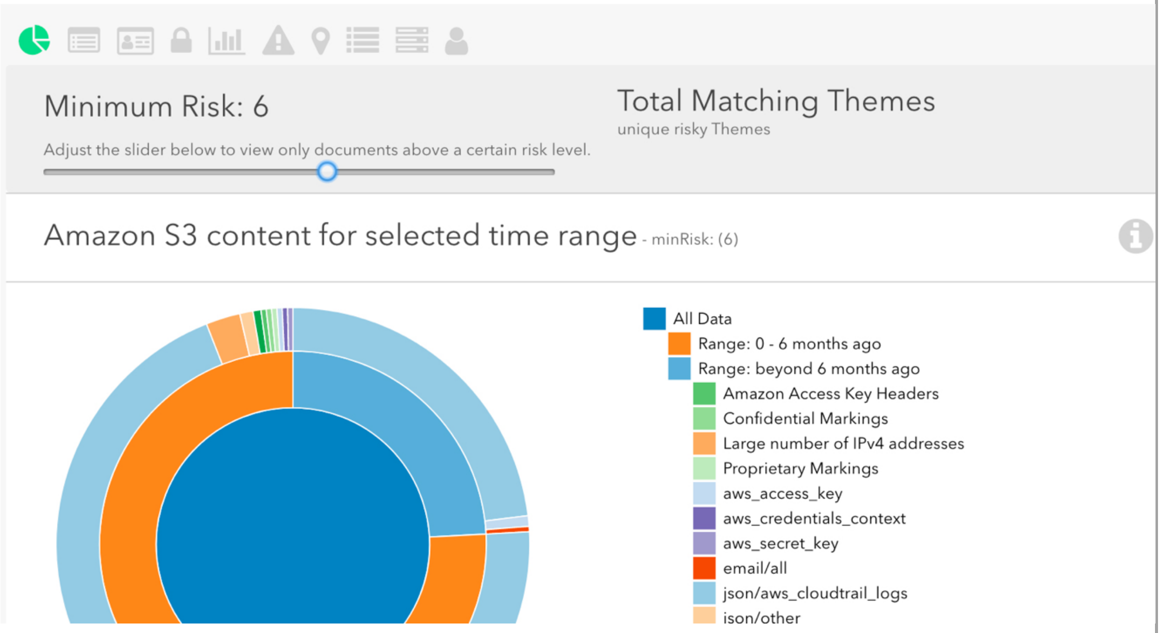
Amazon Macie
Enable Amazon Macie with one-click in the AWS Management Console or a single API call

Continually evaluate your S3 environment
Automatically generates an inventory of S3 buckets and details on the bucket-level security and access controls

Discover sensitive data
Analyzes buckets using machine learning and pattern matching to discover sensitive data, such as personally identifiable information (PII)

Take action
Generates findings and sends to Amazon CloudWatch Events for integration into workflows and remediation actions

- **Amazon Macie** is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.
- Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.
- The fully managed service continuously monitors data access activity for anomalies and generates detailed alerts when it detects the risk of unauthorized access or inadvertent data leaks.
- Today, Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS data stores soon.



Minimum Risk: 6

Adjust the slider below to view only documents above a certain risk level.

Total Matching Themes

unique risky Themes

Amazon S3 content for selected time range - minRisk: (6)

🟦 All Data
🟧 Range: 0 - 6 months ago
🟦 Range: beyond 6 months ago
🟩 Amazon Access Key Headers
🟩 Confidential Markings
🟧 Large number of IPv4 addresses
🟩 Proprietary Markings
🟦 aws_access_key
🟪 aws_credentials_context
🟪 aws_secret_key
🟥 email/all
🟦 json/aws_cloudtrail_logs
🟧 json/other

Securing Data with Macie

- Protect many data types, API keys, and secrets
- Verify compliance with company's policies
- Identify changes in users and their changes in data access patterns over time

Amazon Macie Features

- Automated security classification of monitored data access patterns
- Monitor daily usage for anomalies over defined time
- Protect potential data loss through data visibility and analysi
- Custom reports and alert management when issues arise

Amazon Macie Use Cases

Sensitive Data Protection

Data Breaches

Data Leaks

Unauthorized Access

Amazon Macie Setup

- Log in to your AWS account as administrator
- Select AWS region to operate in
- Accept service – linked role for Macie
- Select S3 bucket to analyze data patterns

Classifying Data

General Data Protection Regulation (GDPR)

Personally Identifiable Information (PII)

Personal Health Information (PHI)

Payment Card Industry (PCI)

Data Classification Types

File Extension

- accdb
- .java
- .pdf

Theme

- Attorney Client Privileged
- Banking Keywords
- Confidential Markings
- Credit Card Keywords
- Social Security Keywords

Data Classification Types

Regex

- CVE
- Router Config
- DSA Private Key
- Encrypted RSA Private Key
- Swift Codes
- AWS_ SECRET_KEY

Personally Identifiable Information

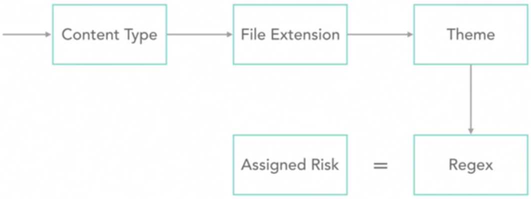
- Mailing Address
- Full Name
- Credit Card Numbers
- Drivers License IDs

Data Classification Types

Vector Machine-Based Classifiers

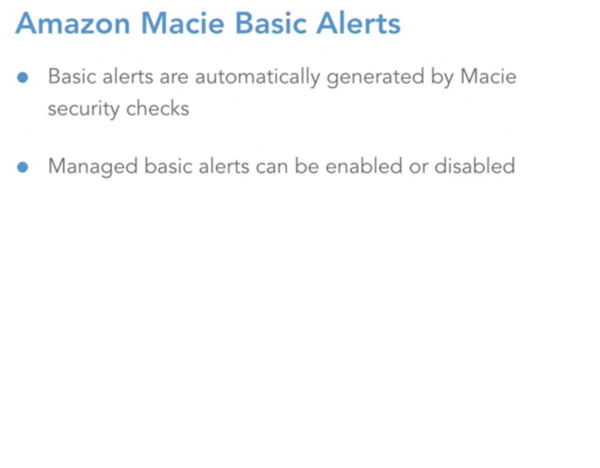
Financial	Application Logs	Encryption Keys
JSON	Email	Source Code

Assigning Risk



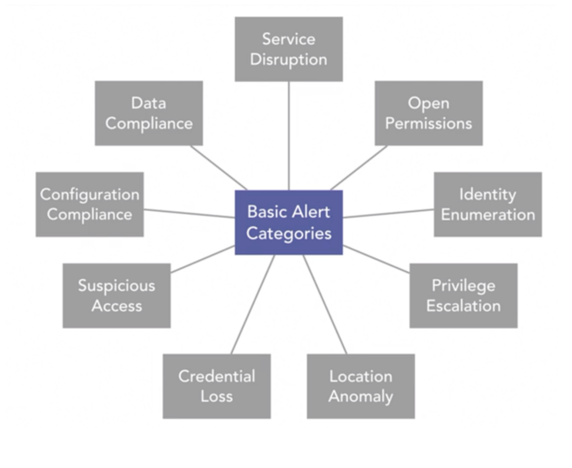
Amazon Macie Predictive Alerts

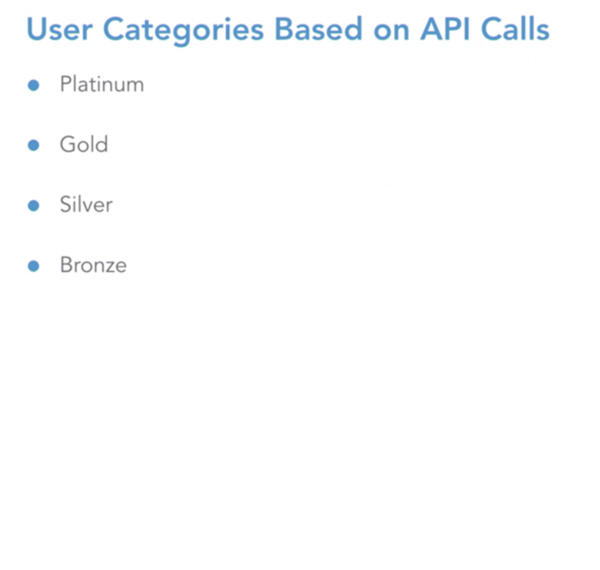
- Continual monitoring by Macie creates “normal baseline’
- Macie then monitors abnormalities from established baseline activity
- Any abnormal activity in AWS account generates alerts



Amazon Macie Basic Alerts

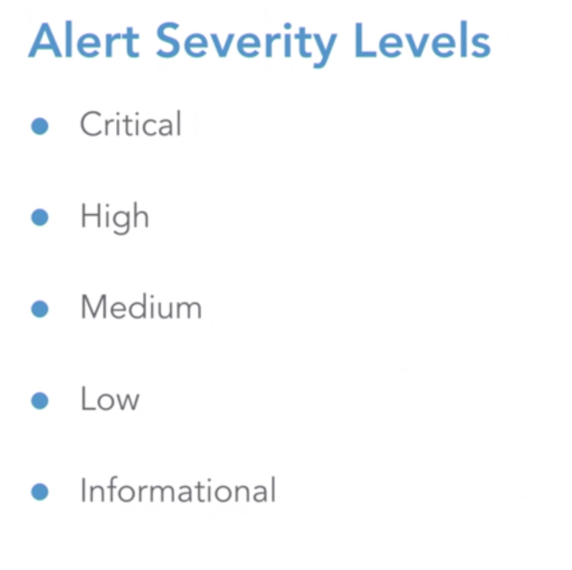
- Basic alerts are automatically generated by Macie security checks
- Managed basic alerts can be enabled or disabled





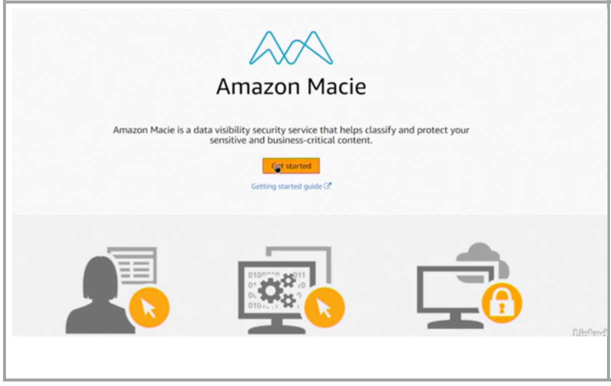
User Categories Based on API Calls

- Platinum
- Gold
- Silver
- Bronze



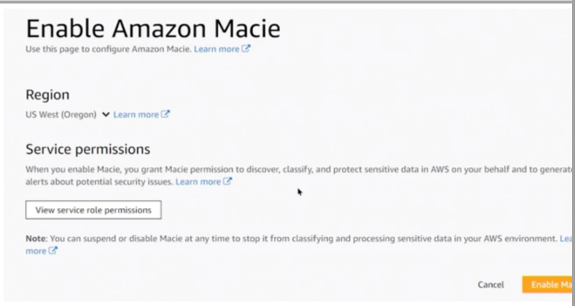
Alert Severity Levels

- Critical
- High
- Medium
- Low
- Informational



Amazon Macie

Amazon Macie is a data visibility security service that helps classify and protect your sensitive and business-critical content.



Enable Amazon Macie

Use this page to configure Amazon Macie. Learn more

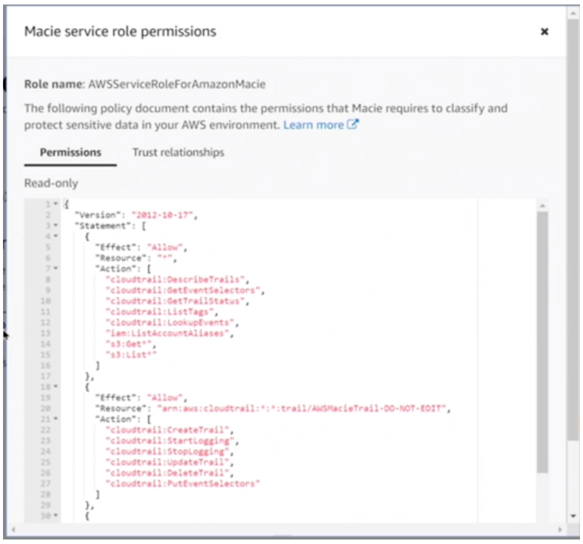
Region

US West (Oregon) Learn more

Service permissions

When you enable Macie, you grant Macie permission to discover, classify, and protect sensitive data in AWS on your behalf and to generat alerts about potential security issues. Learn more

Note: You can suspend or disable Macie at any time to stop it from classifying and processing sensitive data in your AWS environment. Lea more



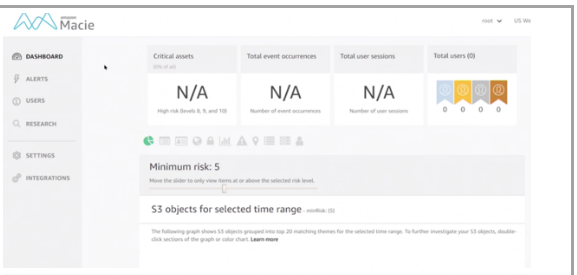
Macie service role permissions

Role name: AWSServiceRoleForAmazonMacie

The following policy document contains the permissions that Macie requires to classify and protect sensitive data in your AWS environment. Learn more

Read-only

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": "*",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "iam:ListAccountAliases",
        "s3:Get*",
        "s3:List*"
      ]
    },
    {
      "Effect": "Allow",
      "Resource": "arn:aws:cloudtrail:*:*:trail/AWSMacieTrail-DO-NOT-EDIT",
      "Action": [
        "cloudtrail:CreateTrail",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:PutEventSelectors"
      ]
    },
    {
```



Critical assets (0% of all): N/A — High risk (levels 8, 9, and 10)

Total event occurrences: N/A — Number of event occurrences

Total user sessions: N/A — Number of user sessions

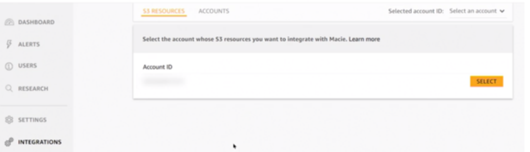
Total users (0): 0 0 0 0

Minimum risk: 5

Move the slider to only view items at or above the selected risk level.

S3 objects for selected time range - minRisk: (5)

The following graph shows S3 objects grouped into top 20 matching themes for the selected time range. To further investigate your S3 objects, double-click sections of the graph or color chart. Learn more

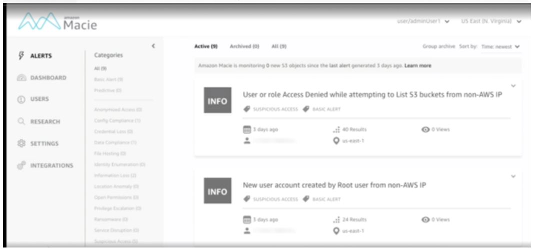


Selected account ID: Select an account

Select the account whose S3 resources you want to integrate with Macie. Learn more

Account ID

[redacted]



Amazon Macie is monitoring 0 new S3 objects since the last alert generated 3 days ago. Learn more

INFO — User or role Access Denied while attempting to List S3 buckets from non-AWS IP

SUSPICIOUS ACCESS · BASIC ALERT

3 days ago · 40 Results · 0 Views · [redacted] · us-east-1

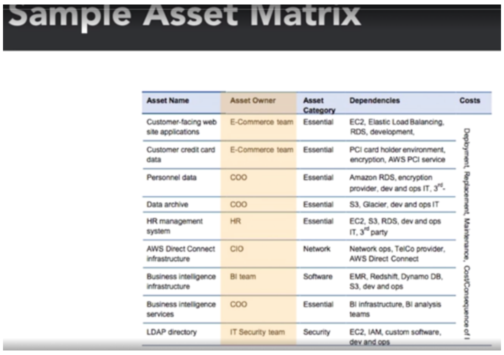
INFO — New user account created by Root user from non-AWS IP

SUSPICIOUS ACCESS · BASIC ALERT

3 days ago · 24 Results · 0 Views · [redacted] · us-east-1

Data Classification and Protection

1. Object tagging
2. Using services to classify data
3. Encryption
4. Backup and restore



Sample Asset Matrix

Asset Name	Asset Owner	Asset Category	Dependencies	Costs
Customer-facing web site applications	E-Commerce team	Essential	EC2, Elastic Load Balancing, RDS, development,	Deployment, Replacement, Maintenance, Cost/Consequence of l
Customer credit card data	E-Commerce team	Essential	PCI card holder environment, encryption, AWS PCI service	
Personnel data	COO	Essential	Amazon RDS, encryption provider, dev and ops IT, 3rd-	
Data archive	COO	Essential	S3, Glacier, dev and ops IT	
HR management system	HR	Essential	EC2, S3, RDS, dev and ops IT, 3rd party	
AWS Direct Connect infrastructure	CIO	Network	Network ops, TelCo provider, AWS Direct Connect	
Business intelligence infrastructure	BI team	Software	EMR, Redshift, Dynamo DB, S3, dev and ops	
Business intelligence services	COO	Essential	BI infrastructure, BI analysis teams	
LDAP directory	IT Security team	Security	EC2, IAM, custom software, dev and ops	

Notable Issues

- No single asset owner
- Business inefficiencies
- Multiple unsynchronized, unreplicated copies

Real-world Takeaways

- 9 unsynchronized copies
- Lacked data governance and security processes
- Severe risk for data protection