**AWS Macie**

General

Q: What is Amazon Macie?

Amazon Macie is an AI-powered security service that helps you prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in AWS. Amazon Macie uses machine learning to recognize sensitive data such as personally identifiable information (PII) or intellectual property, assigns a business value, and provides visibility into where this data is stored and how it is being used in your organization. Amazon Macie continuously monitors data access activity for anomalies, and delivers alerts when it detects risk of unauthorized access or inadvertent data leaks.

Q: What can I do with Amazon Macie?

You can use Amazon Macie to protect against security threats by continuously monitoring your data and account credentials. Amazon Macie gives you an automated and low touch way to discover and classify your business data. It provides controls via templated Lambda functions to revoke access or trigger password reset policies upon the discovery of suspicious behavior or unauthorized data access to entities or third-party applications. When alerts are generated, you can use Amazon Macie for incident response, using Amazon CloudWatch Events to swiftly take action to protect your data.

Data Analysis

Q: What data sources does Amazon Macie support?

The Amazon Macie service supports Amazon S3 and AWS CloudTrail. We plan to add support for user and content protection in customers Amazon EC2 environments (Windows, Linux, EBS), Amazon DynamoDB, Amazon RDS, Amazon EFS, and AWS Glue in 2018.

Q: How does Amazon Macie work?

Amazon Macie is a security service that provides customers both visibility and security for the content that they store in Amazon S3. Amazon Macie helps customers understand their data by automatically and continuously discovering, classifying, and intelligently and accurately assigning a business value to customer’s data. Through understanding the asset value of content and how it is being accessed, Amazon Macie is able to create contextual and narrative security alerts on challenges that our customers face, only alerting when high value content is being accessed in a way that creates risk for their business. Examples include Amazon Macie’s ability to detect global access permissions inadvertently being set on sensitive data, detect uploading of API keys inside source code, and verify sensitive customer data is being stored and accessed in a manner that meets their compliance standards.

Customers can enable Amazon Macie quickly and easily without the need to manually define and periodically update complicated data classifications and inflexible user roles. Amazon Macie combines machine learning with user behavior analytics to detect activity that signals potential risk to business-critical data or assets. For example, Amazon Macie can alert on the download of large quantities of source code by a user account that typically does not access that data, or sudden changes in permissions of Amazon S3 buckets that house data. Once enabled, customers can start receiving security and compliance alerts immediately and create automated policies to protect your data when suspicious activity is detected. Using natural language processing (NLP) methods to automate the classification of data and historical data access patterns to train its neural network, Amazon Macie continuously monitors your environment with no manual re-training required. Amazon Macie’s rich user interface provides accurate alerts with detailed evidence and actionable recommendations that allow you to spend time responding to the most relevant risks. Amazon Macie features a rich user interface that allows for security and compliance use cases; offering a set of APIs that will allow partners and customers to incorporate Amazon Macie's data classification and security anomaly detection capabilities directly into their own applications.

Security and Access

Q: What are some examples of suspicious activity that Amazon Macie can detect?

Amazon Macie analyzes activity of user, application, and service accounts associated with sensitive data that suggests risk to the business, such as inadvertent exposure of data, insider threats, or targeted attacks. Amazon Macie can alert on suspicious activity such as compromised user accounts enumerating and downloading large amounts of sensitive content from unusual IP addresses, or the download of large quantities of source code by a user account that typically does not access this type of sensitive content. A compliance-focused example of Amazon Macie includes detection of large quantities of high-risk documents shared publically or to the entire company, such as files containing personally identifiable information (PII), protected health information (PHI), intellectual properties (IP), legal or financial data. Additionally, customers also have the ability to use Amazon Macie’s dashboard to define their own alerts and policy definitions based on their security needs.

Q: How does Amazon Macie secure your data?

As part of the data classification process, Amazon Macie identifies customers’ objects in their S3 buckets, and streams the object contents into memory for analysis. When deeper analysis is required for complex file formats, Amazon Macie will download a full copy of the object, only keeping it for the short time it takes to fully analyze the object. Immediately after Amazon Macie has analyzed the file content for data classification, it deletes the stored content and only retains the metadata required for future analysis. At any time, customers can revoke Amazon Macie access to data in the Amazon S3 bucket.

Q: How does Amazon Macie automate security policies to protect data and enforce compliance workloads?

The first step towards building compliance policies including Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), or General Data Protection Regulation (GDPR) is around identifying where sensitive data exists across an organization. Amazon Macie automates this discovery phase, with highly accurate, machine learning based detection of over 70 data types related to Personally Identifiable Information (PII), Personal Health Information (PHI), regulatory documents, API keys and secret key material. Customers can get started quickly by enabling Amazon Macie’s compliance policies to alert on the existence of credential information embedded within source code and backups, or to automate policies about how PII and PHI can be safely stored and accessed. In addition to supporting data compliance use cases, Amazon Macie leverages a neural network-based artificial intelligence to identify changes to policies and access control lists that could indicate inadvertent overexposure of information, or suspicious access to content that could indicate a potential data breach. Amazon Macie allows customers to automate response and remediation through Amazon CloudWatch Events and a suite of templated AWS Lambda functions that can be customized to meet the specific needs of your organization.

Integration

Q: Can partner and third-party solutions integrate with Amazon Macie?

Yes, Amazon Macie will support API endpoints through the AWS SDK, allowing for integration by partners and third party solutions. Additionally, Amazon Macie will send all findings to CloudWatch Events, allowing for follow on integration by partners and third party solutions through any available triggers. This includes external case management and ticketing systems such as Atlassian JIRA, Splunk, HP ArcSight, and IBM Resilient Systems.

Languages

Q: Does Amazon Macie support multiple languages?

Natural Language Processing is a key feature of Amazon Macie, which needs to process and understand content to provide its full value. Amazon Macie’s NLP supports discovery and classification of content in multiple languages, but support to automatically translate and correlate content across languages is a roadmap item. Although some features of Amazon Macie will work on non-English content, such as user behavior analytics, Amazon Macie is optimized for English only at this time.

Getting Started

Q: How do I get started with Amazon Macie?

To get started with Amazon Macie, simply log in to the Amazon Macie console, run the provided CloudFormation templates to configure the necessary IAM roles and policies in your account, and select which S3 buckets to protect. Learn more about Amazon Macie and supported use cases by reading our [Blog](https://aws.amazon.com/blogs/security/) and [Documentation](http://docs.aws.amazon.com/macie/latest/userguide).