
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC215

Automate data discovery with Amazon Macie

Himanshu Verma (he/him)
Principal Worldwide Security Specialist
AWS

Anuj Gupta (he/him)
Principal Solutions Architect
AWS

Carlos Carlos (he/him)
Director, Data Security
Oportun

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What we will cover

- Data protection drivers
- Amazon Macie benefits and features
- NEW! Macie automated sensitive data discovery demo
- Real-world application of Macie at Oportun
  - Business drivers
  - Design considerations
  - Solution, business outcomes, and what's next
- Key takeaways and Q&A

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Problem statements and use cases



Assessing your data privacy and security



Maintaining regulatory compliance



Identifying sensitive data during migrations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Amazon Macie?

DISCOVER AND PROTECT YOUR SENSITIVE DATA AT SCALE



- Amazon Macie is a data security service that discovers sensitive data using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks
- Customers use Amazon Macie to manage the data security posture of their Amazon S3 environment

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How Amazon Macie works



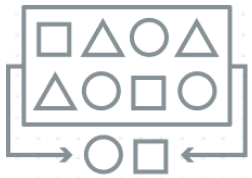
Amazon Macie

Enable Macie with one selection in the AWS Management Console or a single API call



Continually evaluate Amazon S3 storage

Automatically generate S3 bucket inventory and provide insights on bucket-level security and access controls



Automated sensitive data discovery

Automatically build an interactive data map of your sensitive data in S3



Full discovery scans

Run targeted, sensitive data discovery jobs based on results from the interactive data map



Take action

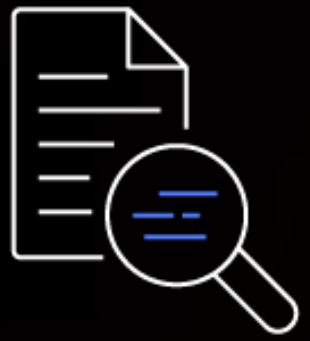
Generate findings and send to Amazon EventBridge and AWS Security Hub for automated remediation and workflow integration

aws

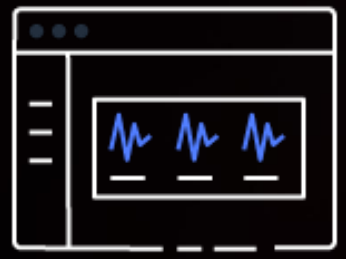
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Macie: Benefits

DISCOVER AND PROTECT YOUR SENSITIVE DATA AT SCALE



Automate sensitive data discovery at scale



Gain cost-efficient visibility into sensitive data



Assess your S3 bucket inventory for security and access controls



Reduce triage time with actionable reporting of sensitive data

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New feature:
Automated sensitive data discovery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Macie introduces automated sensitive data discovery



Macie **automatically** samples and analyzes objects in your S3 buckets, inspecting them for sensitive data (such as PII) and builds an **interactive data map**



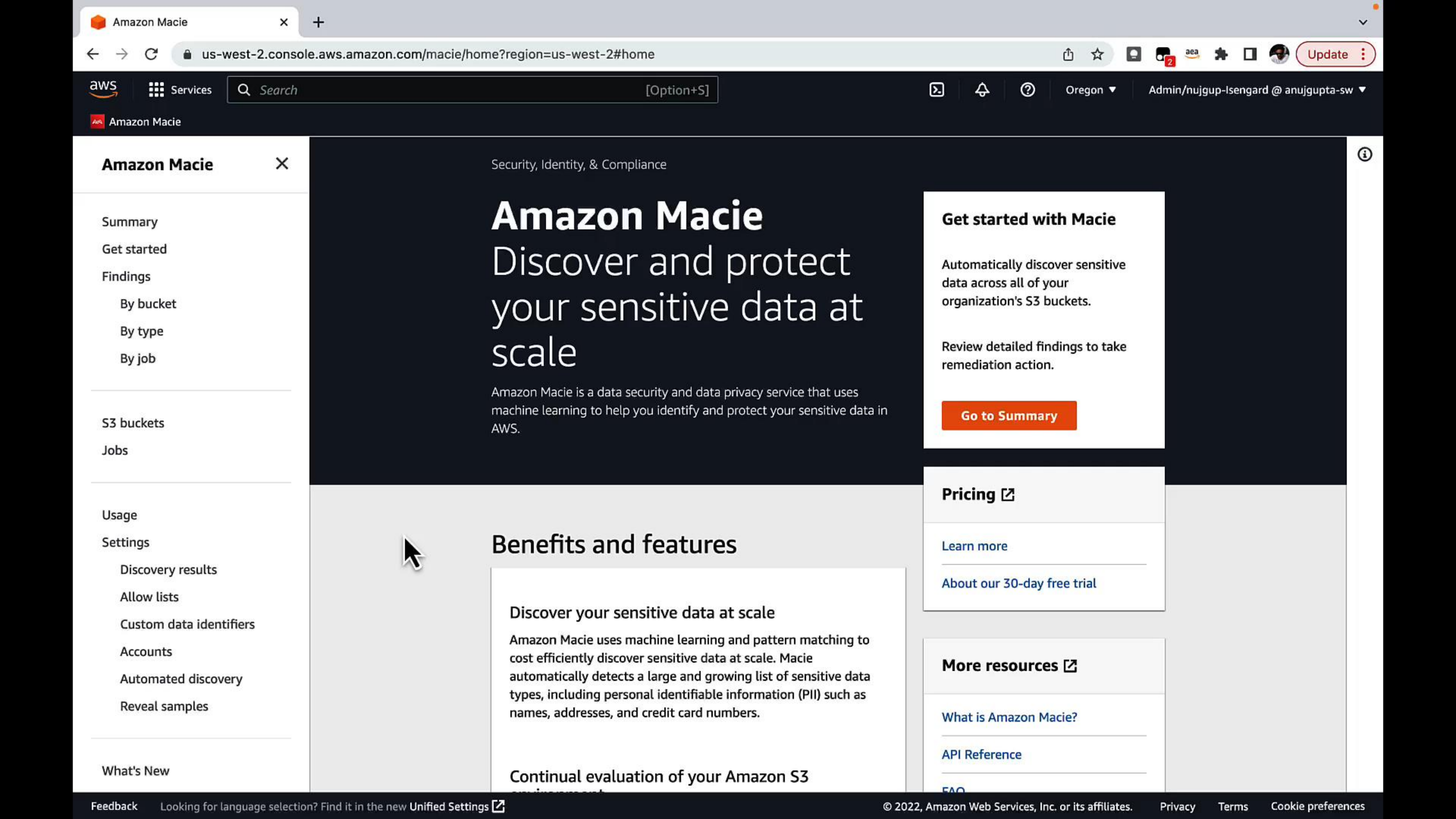
Enables **cost-efficient** and **broad visibility** into sensitive data stored in Amazon S3 across each AWS Account



Helps guide decisions to perform **targeted investigations** of specific S3 buckets

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Amazon Macie
us-west-2.console.aws.amazon.com/macie/home?region=us-west-2#home
Update
aws
Services
Search
[Option+S]
Oregon
Admin/nujgup-Isengard @ anujgupta-sw
Amazon Macie
Amazon Macie
Summary
Get started
Findings
By bucket
By type
By job
S3 buckets
Jobs
Usage
Settings
Discovery results
Allow lists
Custom data identifiers
Accounts
Automated discovery
Reveal samples
What's New
Security, Identity, & Compliance
Amazon Macie
Discover and protect your sensitive data at scale
Amazon Macie is a data security and data privacy service that uses machine learning to help you identify and protect your sensitive data in AWS.
Get started with Macie
Automatically discover sensitive data across all of your organization's S3 buckets.
Review detailed findings to take remediation action.
Go to Summary
Pricing
Learn more
About our 30-day free trial
More resources
What is Amazon Macie?
API Reference
FAQ
Benefits and features
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.
Continual evaluation of your Amazon S3
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Real-world application of Amazon Macie at Oportun

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OPORTUN + digit

Oportun is driven by a mission to provide inclusive, affordable financial services that empower our customers to build a better future



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Oportun's data security team

DATA SECURITY

OPORTUN | digit



Oswaldo Cruz
Sr. Data Security Engineer



Carlos Carlos
Director, Data Security

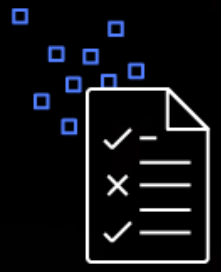


Armando Cardenas
Staff Security Engineer

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Business drivers



Security and compliance

- Data privacy and compliance requirements – for example, FTC Safeguards
- Remediation for improving data security posture and reduce risk



Operational excellence

- Overhead of maintaining custom patterns to match sensitive data
- Discover sensitive data at scale in a cost-effective manner



Metrics

- Time to discover data
- Create an inventory of sensitive data across all Amazon S3 data assets

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

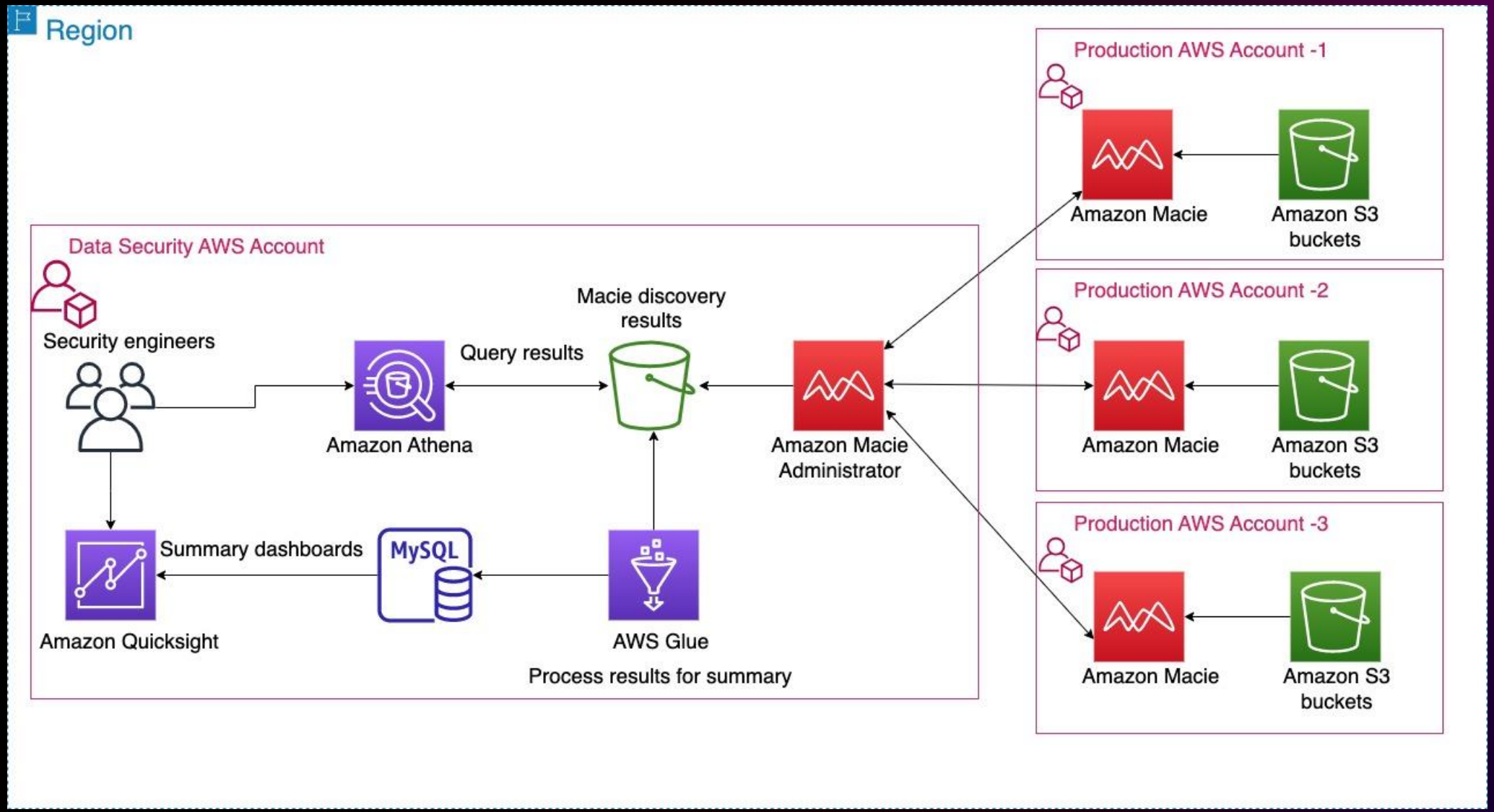
Design considerations

- Cost-effective
- Reduced operational overhead
- Automated sensitive data discovery for new data types
- Accuracy of sensitive data discovery to reduce false positive
- Easy integration with AWS services
- Ability to visualize results and build a workflow



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Solution design



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Business outcome



95% higher accuracy compared to alternatives



80% reduction in time to discover sensitive data



Improved data security posture management



Prioritize risk remediation

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What’s next

- Building automated remediation workflows
- Enhanced risk score profiles
- Increased scanning capabilities for other data asset types
- Executive summary dashboards

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways

- Identifying and protecting growing volumes of data can become increasingly complex and time-consuming
- Amazon Macie is a data security service to help you address these challenges
- Amazon Macie automates the discovery of sensitive data, provides visibility into data security risks, and enables automated protection against those risks
- Amazon Macie provides continuous visibility into your data security posture, which helps to reduces data security risks

Tip: Use a mix of different data types across multiple S3 buckets for proof of concept

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recommended sessions

- CMP306: Building apps to isolate & process sensitive data with AWS Nitro Enclaves
- STG315: Configuring Amazon S3 security settings and access controls
- CMP302: Confidential computing with AWS compute

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do I get started

TECHNICAL HOW-TO BLOG



Launch blog for automated sensitive data discovery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Himanshu Verma (he/him)

LinkedIn - himanshu-verma-wg

Anuj Gupta (he/him)

LinkedIn - anuj-gupta-24795310

Carlos Carlos (he/him)

LinkedIn - carloscarlos1



Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.