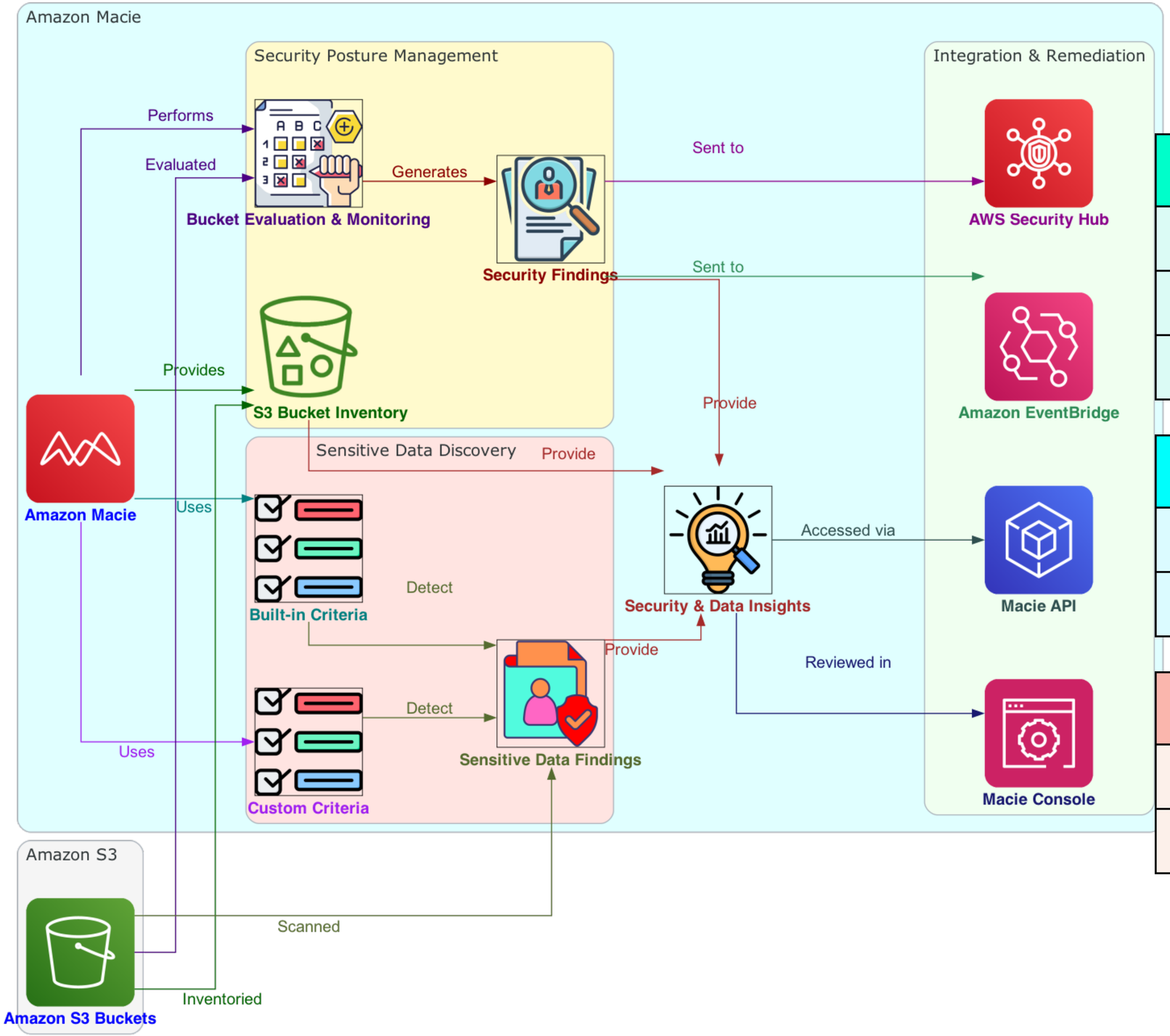
Amazon Macie

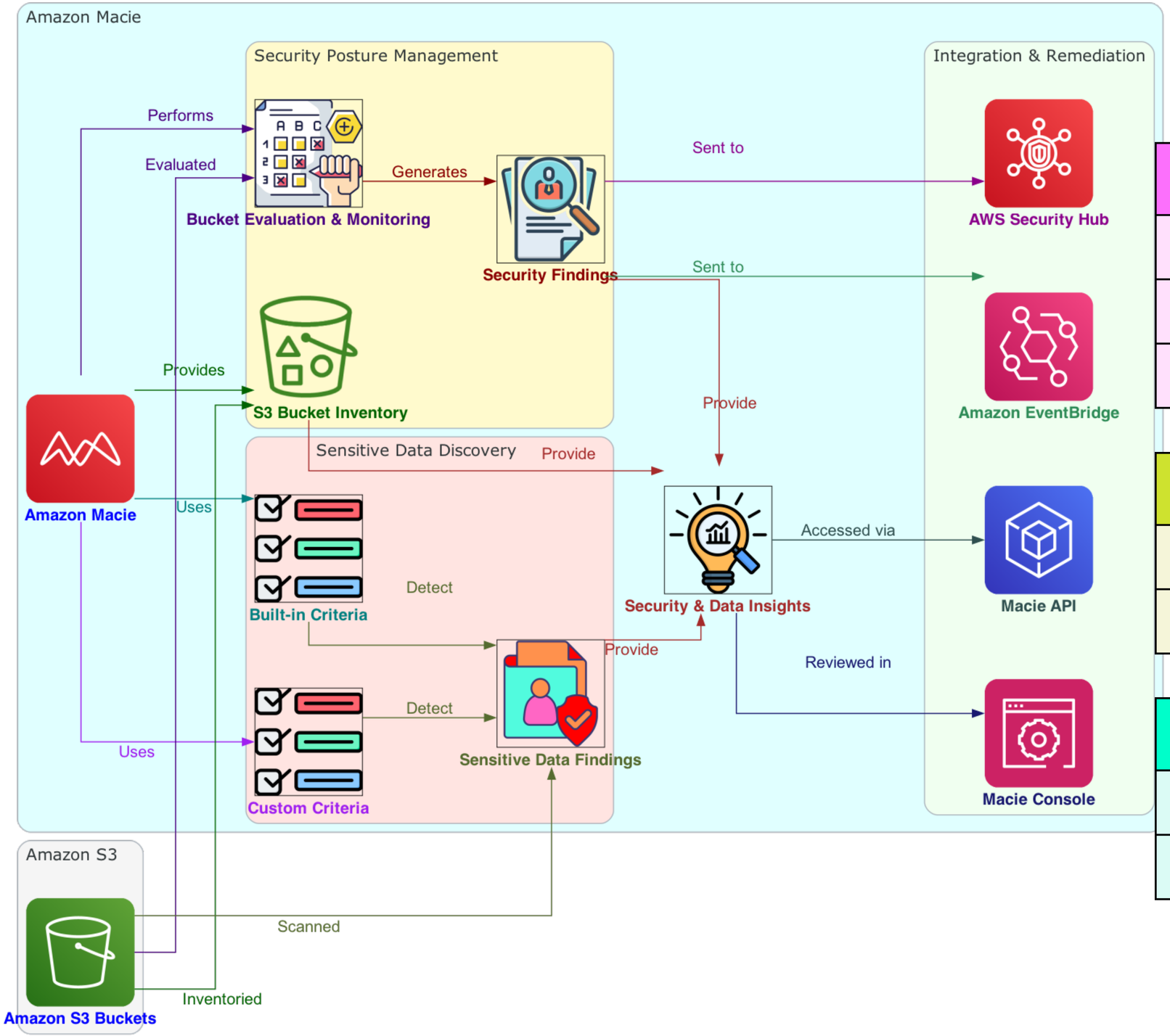
Table of Contents

Amazon Macie



1. 🔍 Discovers sensitive data
   - 🤖 Uses machine learning
   - 🔍 Employs pattern matching
   - 🗃️ Identifies data in Amazon S3
2. 🔒 Provides visibility into data security risks
   - 🔍 Offers overview of potential risks
   - 💡 Enables informed decisions
3. 🤖 Enables automated protection against risks
   - 🛡️ Automates data protection
   - 🔒 Ensures proactive security approach

Amazon Macie



4. 📊 Offers inventory of S3 buckets

🔍 Evaluates security posture

🔒 Monitors security and access control

💪 Helps maintain strong security posture

5. 🚨 Generates findings for potential issues

🔍 Detects publicly accessible buckets

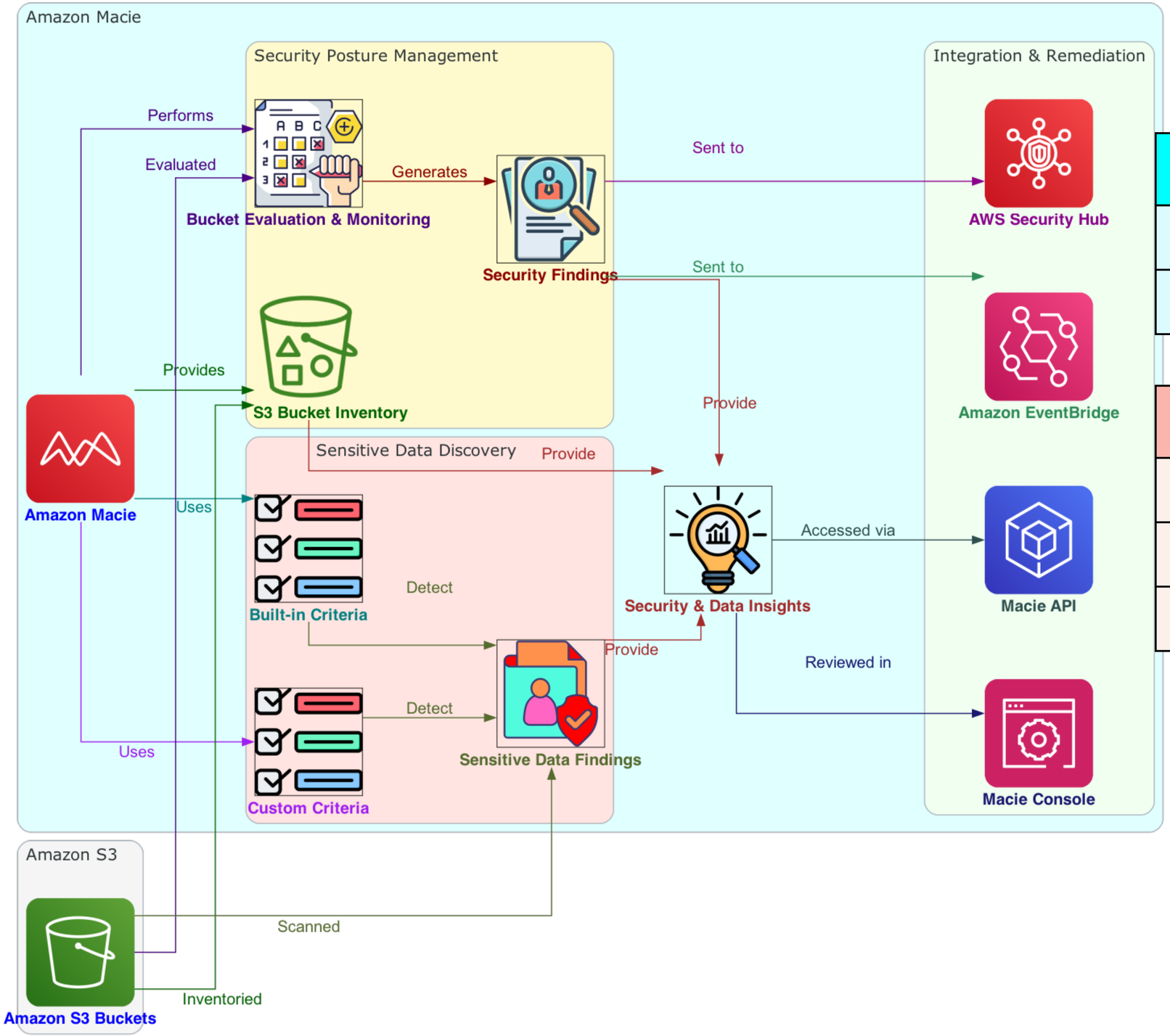
🔒 Keeps you informed about data security

6. 📝 Automates discovery and reporting of sensitive data

🔍 Discovers sensitive data in S3

📊 Provides understanding of data landscape

Amazon Macie



7. 📈 Provides statistics and insights

🔍 Offers insights into S3 data security posture

🗺️ Helps identify sensitive data location

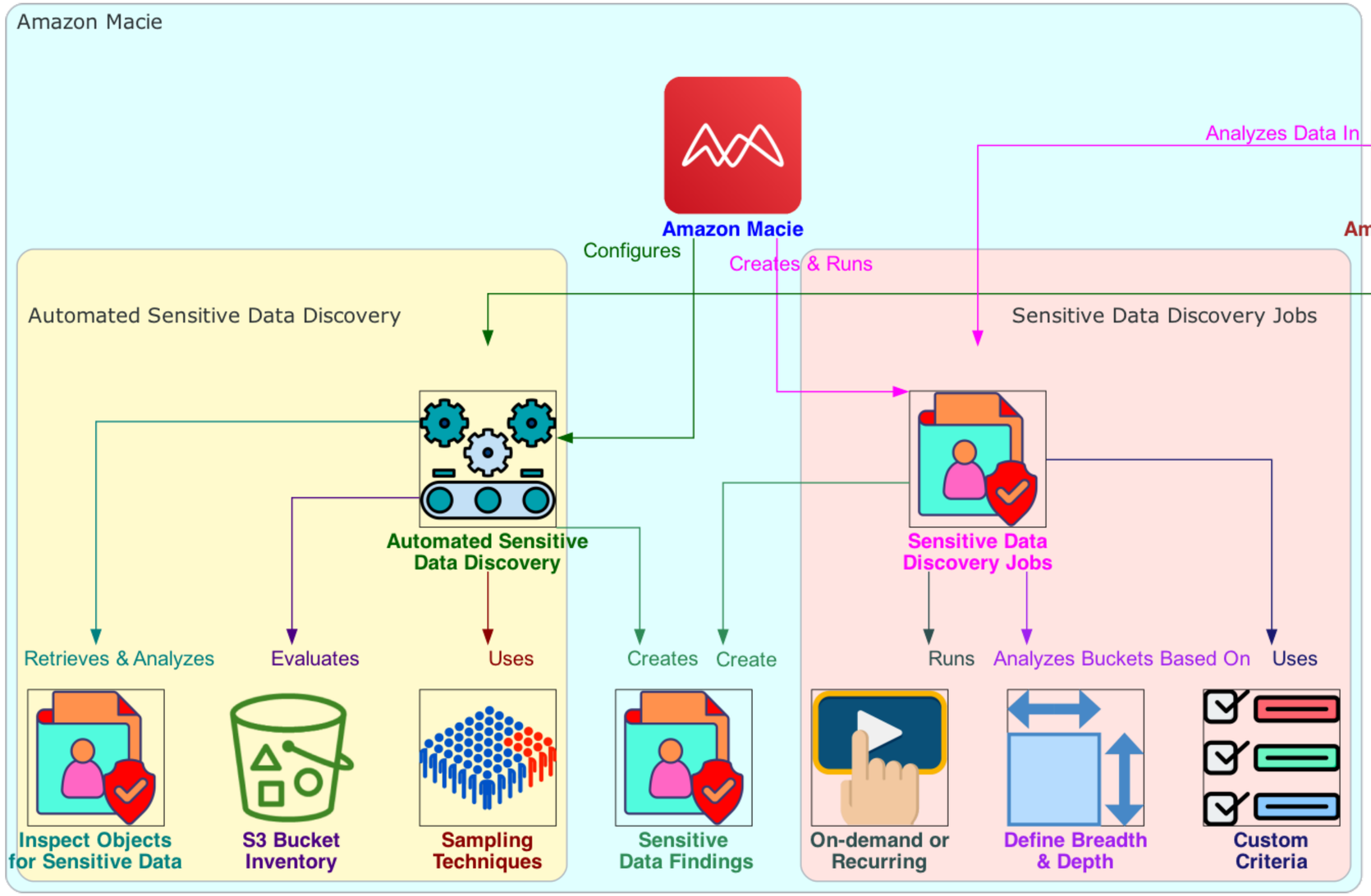
8. 🌉 Integrates with other services

🔗 Works with Amazon EventBridge

🔒 Connects to AWS Security Hub

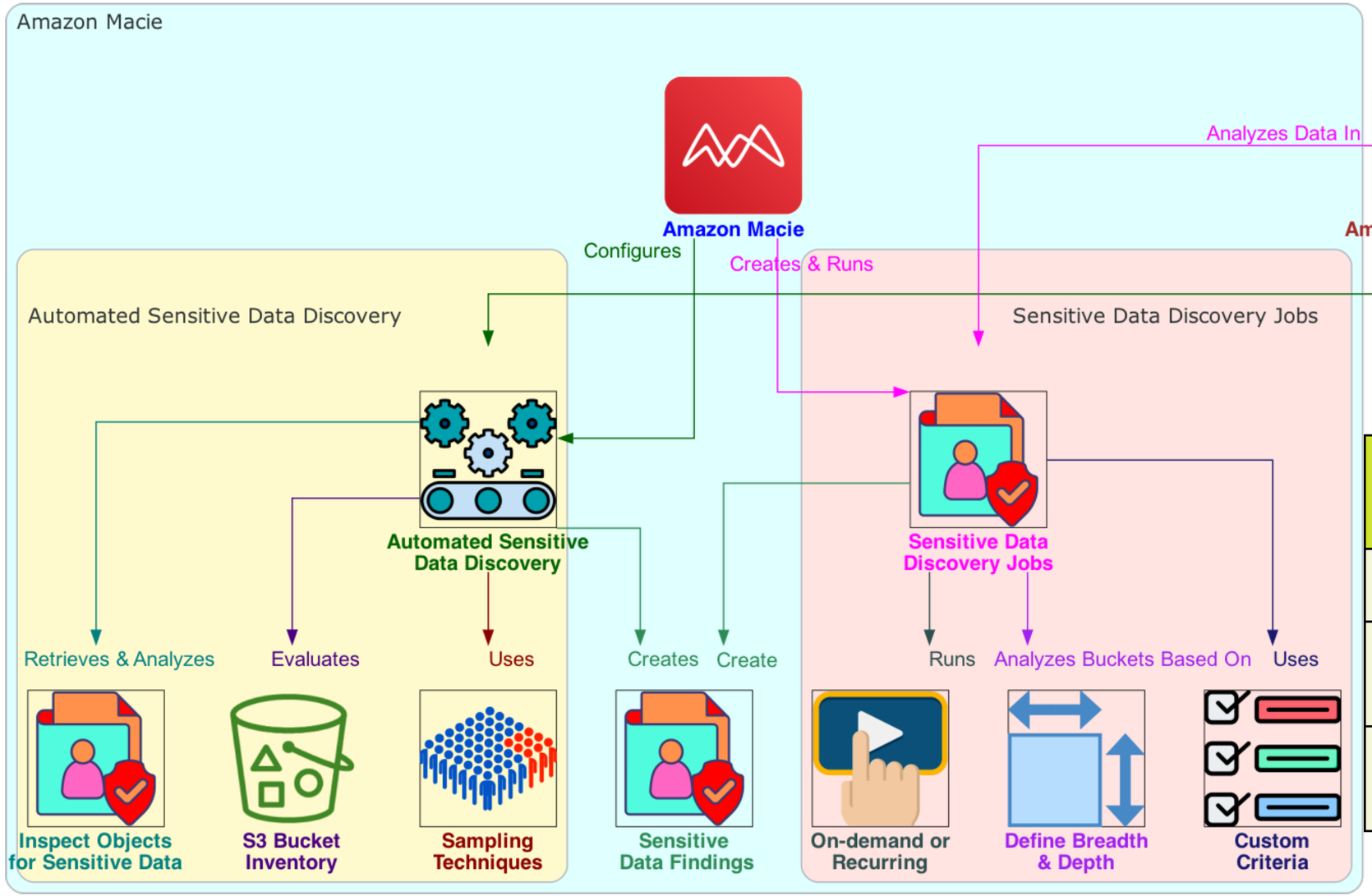
🧩 Enables comprehensive security approach

Automate the discovery of sensitive data



1. 🤖 Two methods
   - 🔄 Automated discovery
   - 🔎 Discovery jobs
2. 🚨 Sensitive data findings
   - 📝 Detailed reports
3. 🌍 Broad visibility with automated discovery
   - 🔍 Sensitive data in S3
   - 🔄 Continual evaluation of S3 inventory
   - 🔍 Sampling techniques
   - 🔎 Inspection for sensitive data

Automate the discovery of sensitive data



4. 🎯 Targeted analysis with discovery jobs

- 🔍 Deeper analysis
- 🎚️ Customizable breadth & depth
- 🗃️ Specific S3 buckets
- 🔍 Sampling depth
- ⚙️ Custom criteria based on S3 properties

5. 🔎 Customizable job parameters

- 🗃️ S3 buckets to analyze
- 🔍 Sampling depth for object selection
- ⚙️ Custom criteria from S3 properties

6. ⏰ Job scheduling

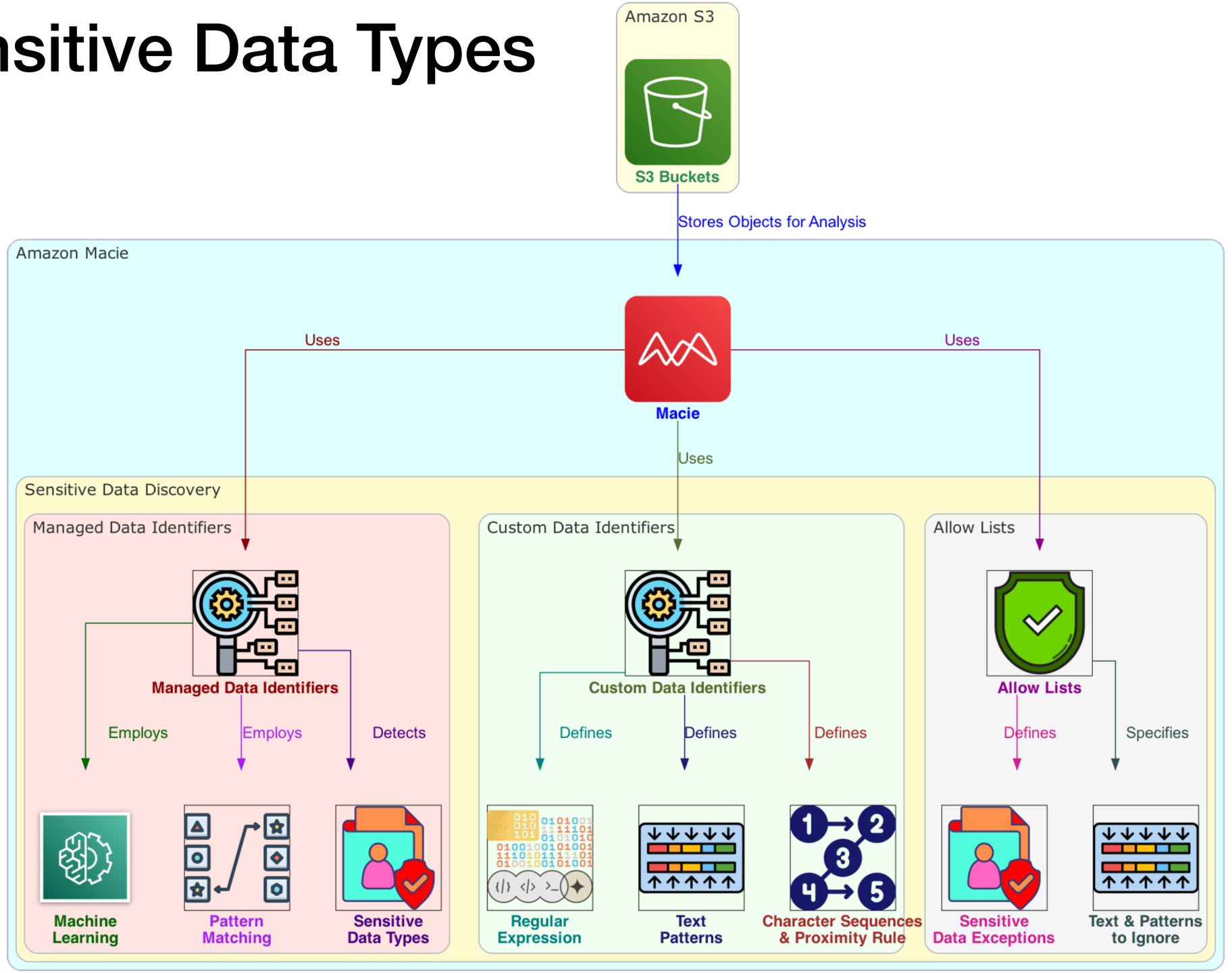
- 🔄 On-demand analysis & assessment
- 🔁 Recurring for periodic monitoring

7. 🔒 Comprehensive view of data & risks

- 📊 Data stored in S3
- 🔒 Associated security or compliance risks

Discovering Sensitive Data Types

1. 🤖 Managed data identifiers
   - 🧠 Machine learning
   - 🔍 Pattern matching
   - 🗃️ Analyzes S3 objects
2. 📊 Detects sensitive data
   - 🔒 PII
   - 💰 Financial information
   - 🔑 Credentials data
   - 🌍 Multiple countries and regions
3. 🔧 Custom data identifiers
   - 🔍 Regex for text patterns
   - 🔠 Optional character sequences
   - 📏 Proximity rules for refinement



Discovering Sensitive Data Types

4. 🔐 Identifies proprietary data

🧩 Particular scenarios

🧠 Intellectual property

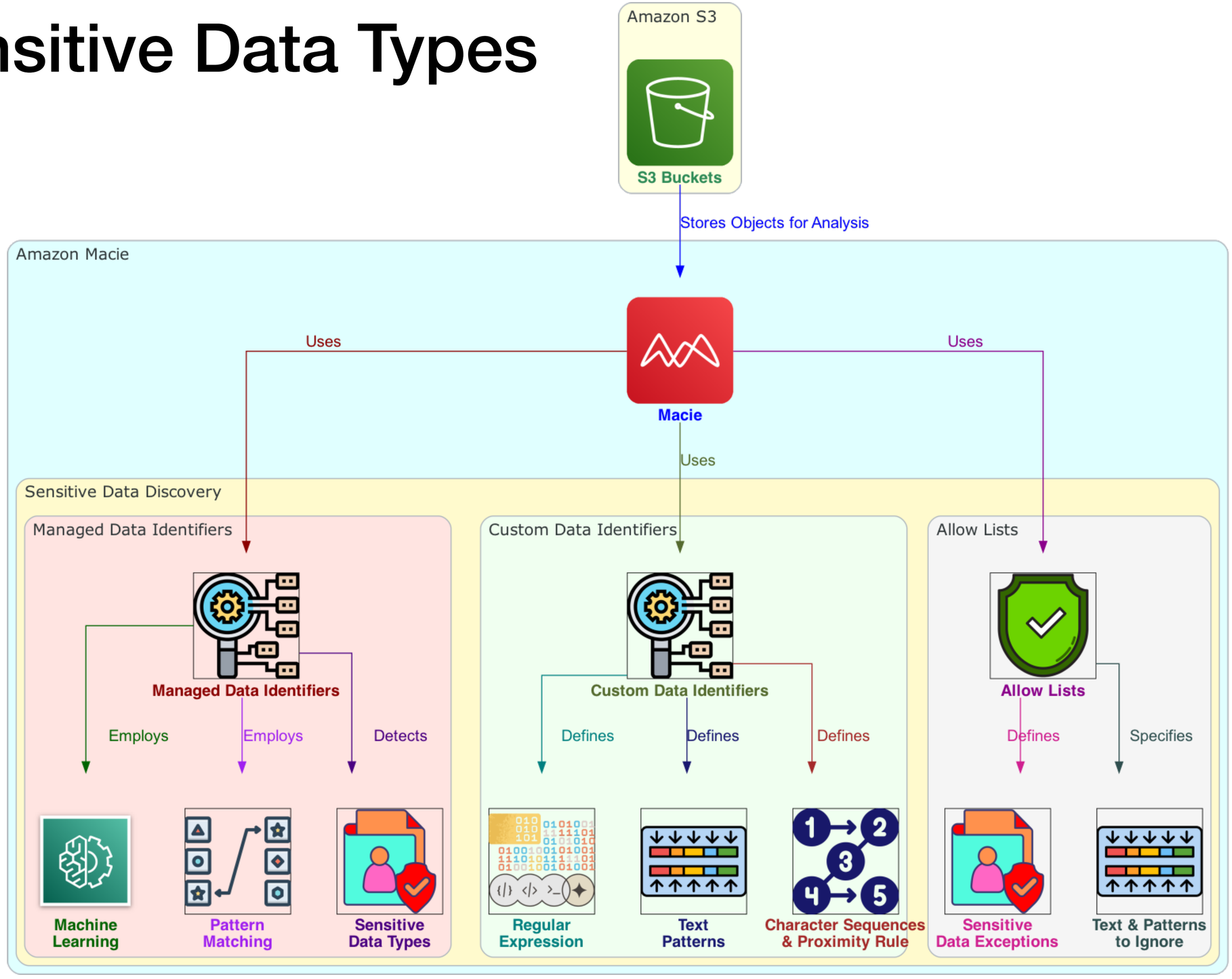
➕ Supplements managed identifiers

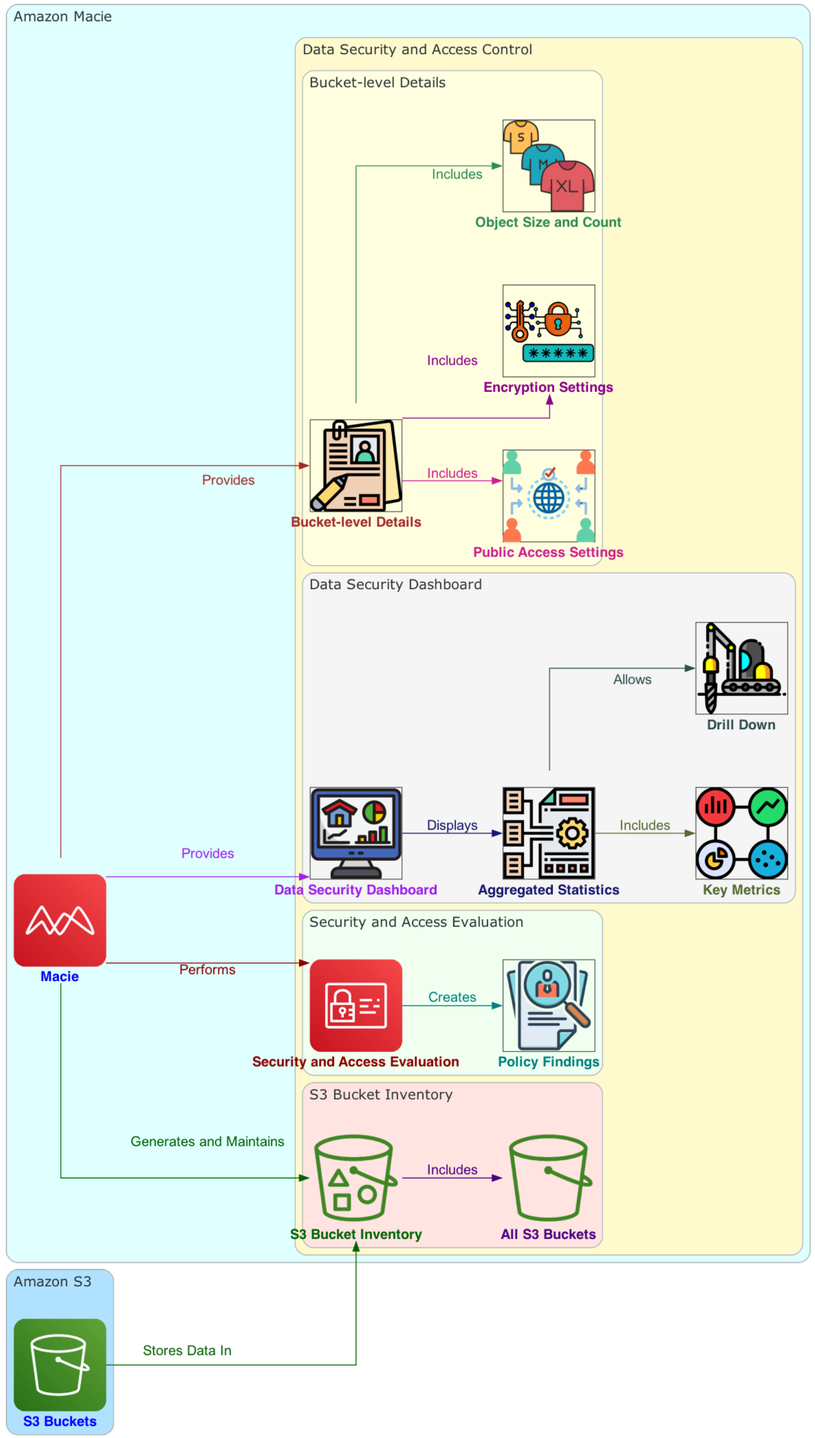
5. ⚖️ Allow lists

❌ Define exceptions

🔍 Specific text and patterns to ignore

🌐 Environment-specific exceptions





Evaluating and Monitoring Data Security with Amazon Macie

1. 📊 Automatic S3 bucket inventory

- 🆕 Generated when Macie enabled
- 🔄 Continuously maintained

2. 🔍 Continuous evaluation and monitoring

- 🔒 Security and access control
- 🟢 Starts when Macie enabled

3. 🚨 Policy findings

- 🔍 Potential security or privacy issues
- 🔎 Review and address

4. 📈 Dashboard

- 📊 Aggregated statistics for S3 data
- ➕ Complements specific findings

5. 🔑 Key metrics

- 🌐 Publicly accessible buckets
- 🤝 Shared with other AWS accounts
- 🔍 Drill down to review data

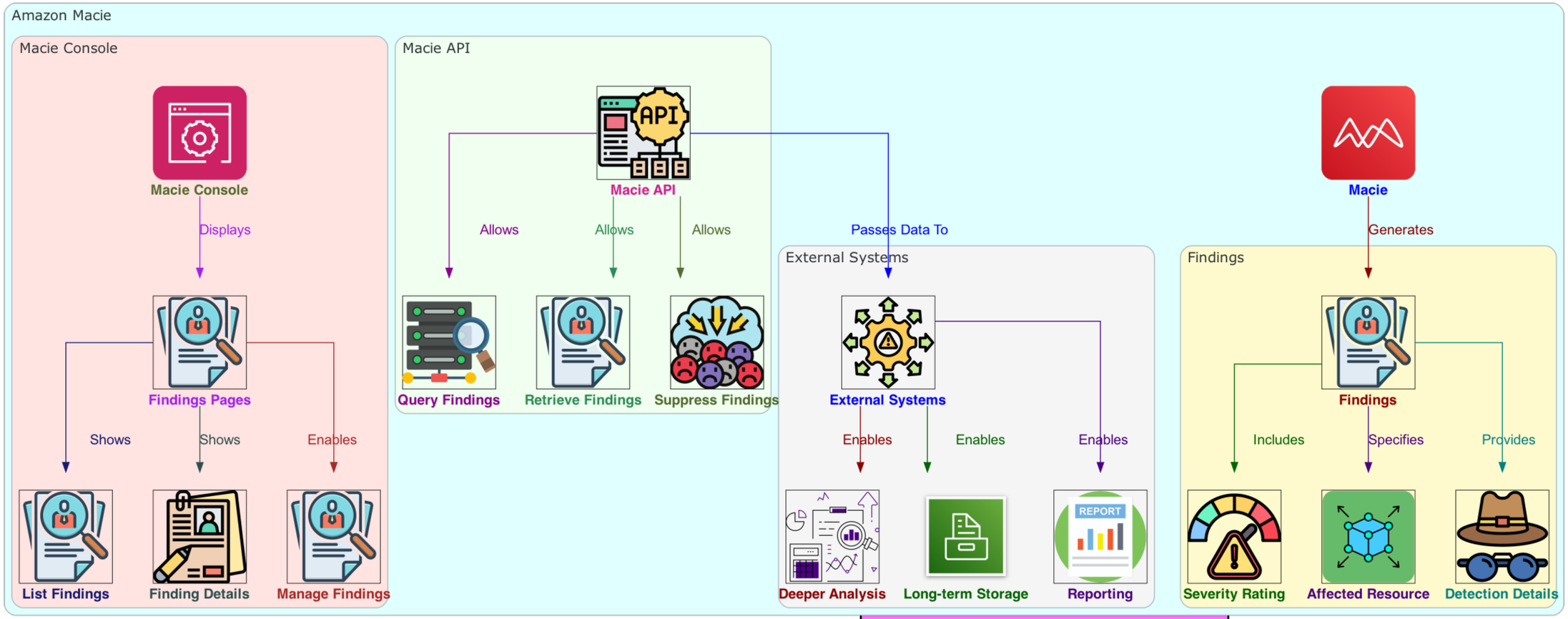
6. 🗃️ Detailed bucket information

- 📊 Statistics for individual buckets
- 🔒 Public access settings
- 🔐 Encryption settings
- 📏 Object size and count

7. 🔎 Browsing and filtering inventory

- 🗂️ Browse S3 bucket inventory
- 🔍 Sort and filter by fields
- 🎯 Locate specific buckets or data

🔍 Reviewing and Analyzing Findings in Amazon Macie



1. 📝 Findings
📊 Detailed reports
🔍 Sensitive data or security issues
🗃️ S3 objects or buckets

2. 🧯 Finding details
⚠️ Severity rating
🎯 Affected resource
🔍 Detection details

3. 🖥️ Macie console
📂 Findings pages
🗂️ List findings
🔍 Individual finding details

4. 🗂️ Findings management
🗂️ Grouping options
🔍 Filtering options
🔢 Sorting options
🚫 Suppressing options

5. 🌐 Macie API
🔍 Query findings
📩 Retrieve findings
🚫 Suppress findings

6. 🔄 Passing data to external systems
🧠 Deeper analysis
💾 Long-term storage
📊 Reporting purposes

Integrating Macie Findings with Other Services and Systems

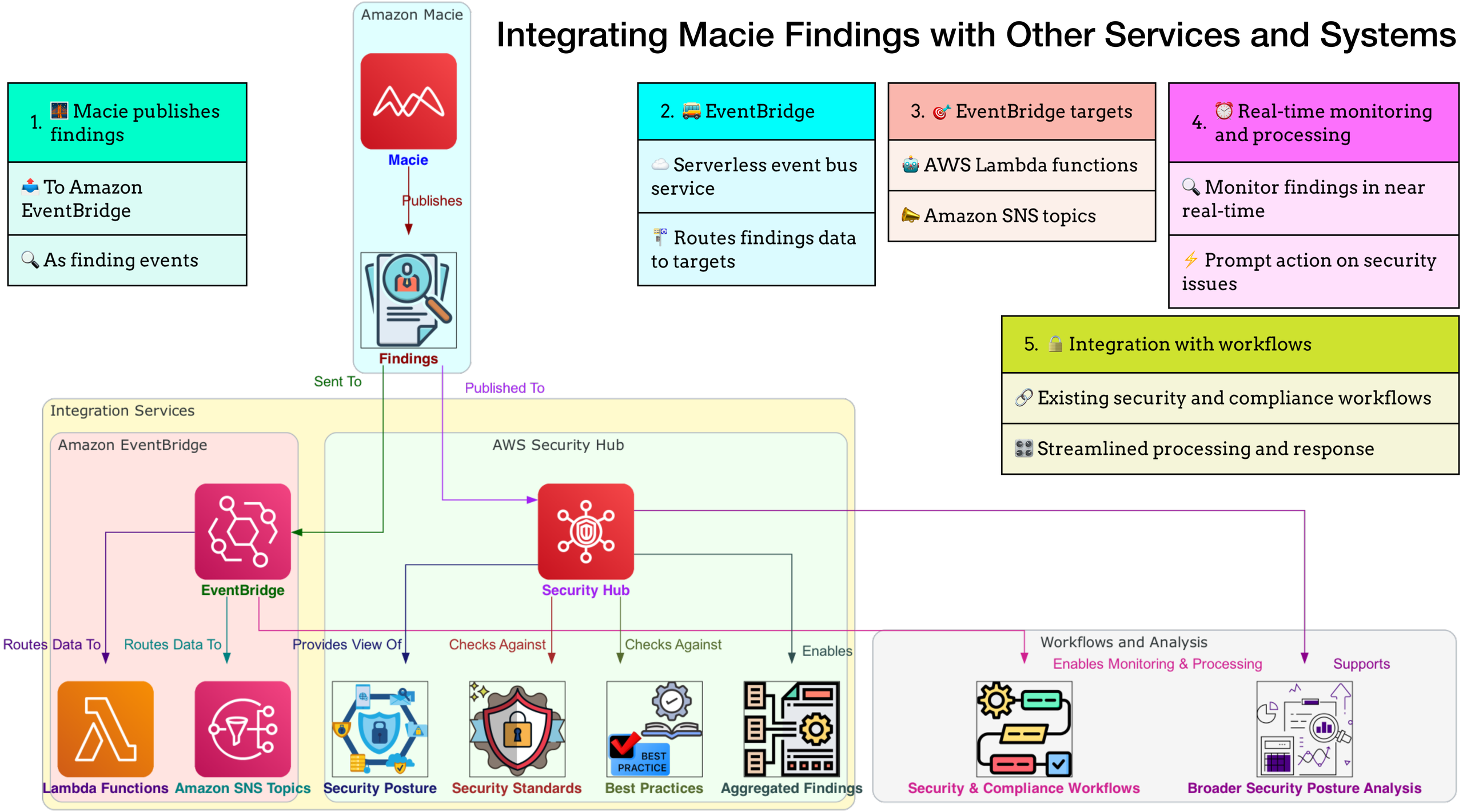
1. 🍎 Macie publishes findings
   - 📩 To Amazon EventBridge
   - 🔍 As finding events

2. 🚌 EventBridge
   - ☁️ Serverless event bus service
   - 🚦 Routes findings data to targets

3. 🎯 EventBridge targets
   - 🤖 AWS Lambda functions
   - 📣 Amazon SNS topics

4. ⏰ Real-time monitoring and processing
   - 🔍 Monitor findings in near real-time
   - ⚡ Prompt action on security issues

5. 🔒 Integration with workflows
   - 🔗 Existing security and compliance workflows
   - 🎛️ Streamlined processing and response



Integrating Macie Findings with Other Services and Systems

6. 🔍 Publish findings to Security Hub

🏰 Centralized security management

7. 📈 Comprehensive security posture view

🌐 Across entire AWS environment

8. 🔪 Check against standards and best practices

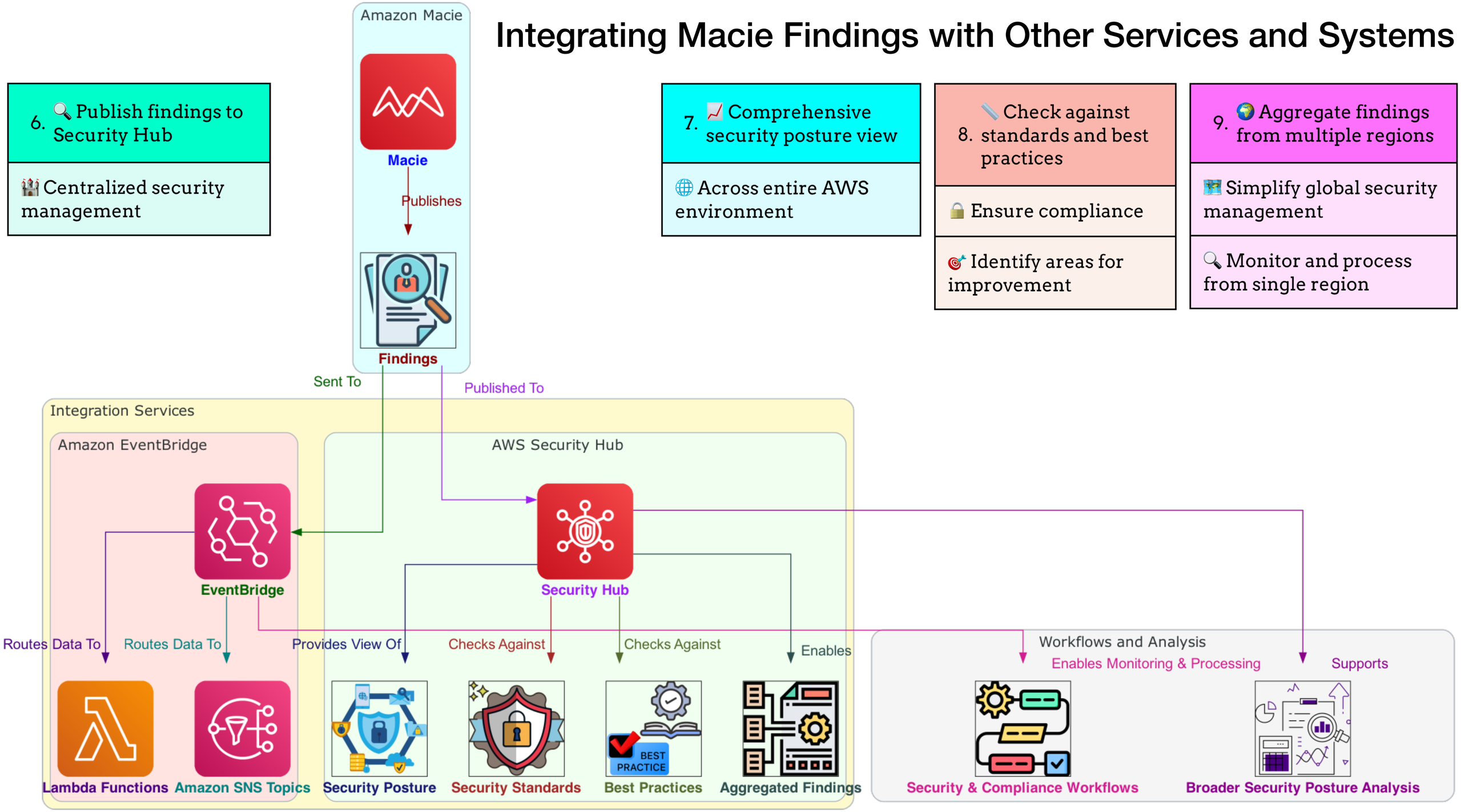
🔒 Ensure compliance

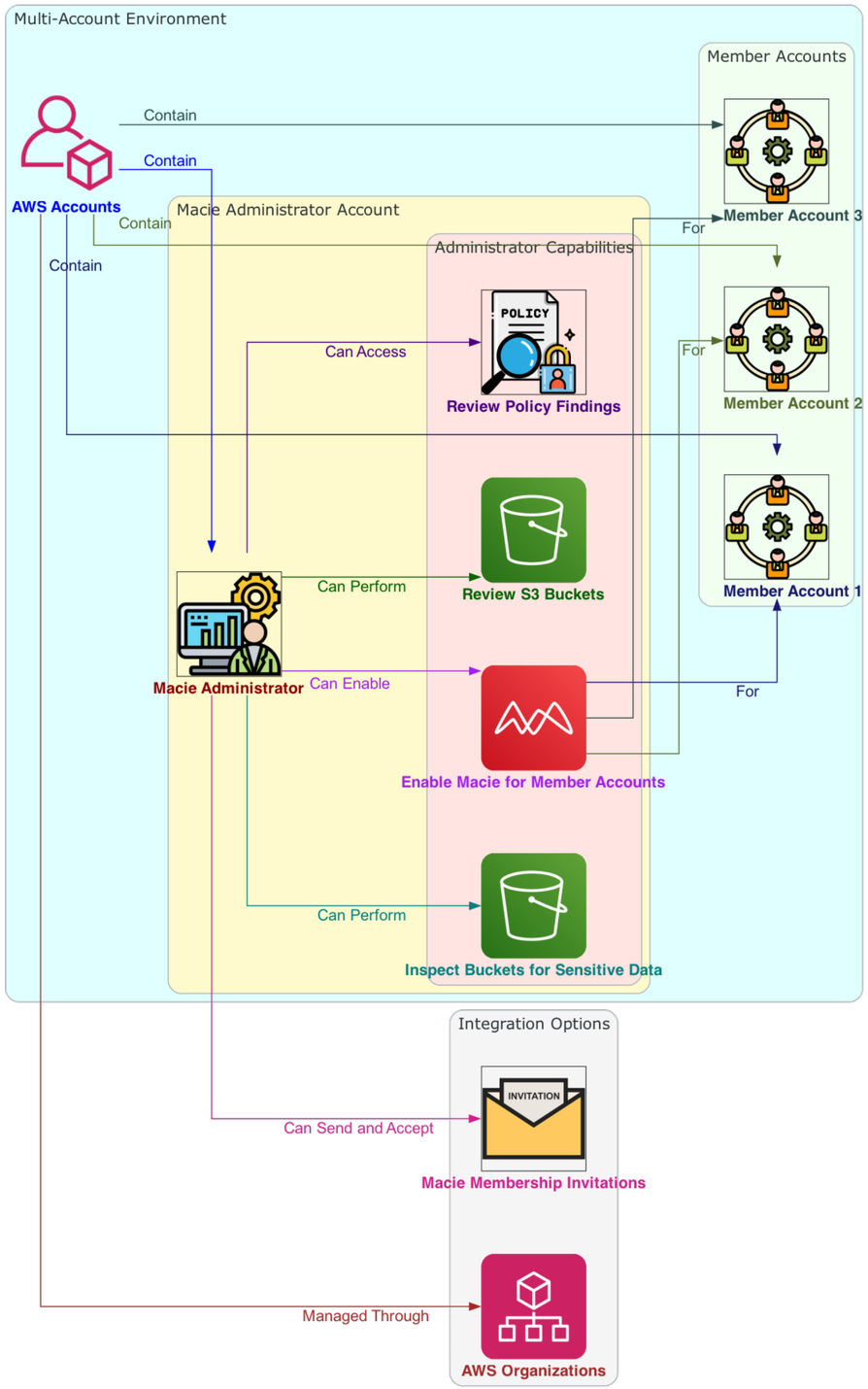
🎯 Identify areas for improvement

9. 🌍 Aggregate findings from multiple regions

🗺️ Simplify global security management

🔍 Monitor and process from single region





Centrally Managing Multiple Macie Accounts

1. 🌐 Manage Macie for multiple AWS accounts

🏢 Multiple accounts in AWS environment

🔧 Central management of Macie

2. 🤝 Two integration options

🔗 AWS Organizations

📩 Macie invitations

3. 👥 Designated Macie administrator

👑 Performs tasks, accesses settings

🔐 For member accounts in organization

4. 🔍 Review S3 bucket information and policy findings

🪣 For member account buckets

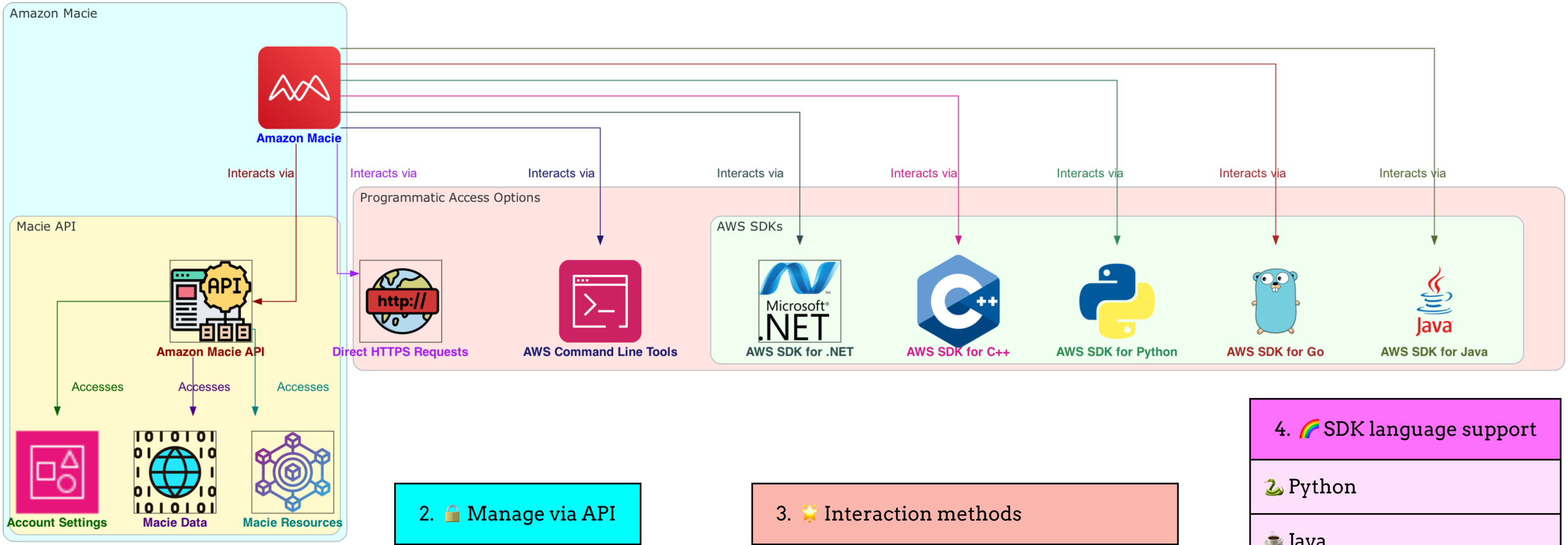
5. 🔎 Inspect member account buckets

🔍 For sensitive data

6. 🔑 Enable Macie for member accounts

🔗 If associated through AWS Organizations

🔧 Programmatic Interaction with Amazon Macie 🚀



1. 🌐 Amazon Macie API
🗝️ Comprehensive access
🖥️ Alternative to Macie console

2. 🔒 Manage via API
⚙️ Account settings
📊 Access data
🗃️ Control resources
🤖 Programmatic flexibility, automation

3. 💥 Interaction methods	
📩 Direct HTTPS requests	
💻 AWS command line tools	
📚 AWS SDKs	🧩 Libraries, sample code
	🔌 Simplify Macie integration

4. 🌈 SDK language support
🐍 Python
☕ Java
🐹 Go
🪟 PowerShell
🔢 C++
🌐 .NET

Thanks for Watching