Table of Contents

AWS DATA LOSS PREVENTION GUIDE

INTRODUCTION

Data loss is one of the key major issues every organization faces which includes their enterprise data i.e. sensitive data. Major issues like stolen data, evolving compliance requirements, data exfiltration, and insider threats have driven the importance of the adoption of data loss prevention tools and technologies.AWS Data loss prevention guide adjoin will help us in protecting business information, as data loss can affect the prominence of the company, its credibility, financial losses and also can have pernicious results on the growth of the organization.

Many organizations that have invested in data loss prevention tools might not be capable enough to address the challenges in AWS environments to protect data from theft or loss and comply with data privacy laws. It becomes increasingly challenging and important for any organization to evaluate the right set of security tools that meets their security requirements.

AWS ecosystem offers a rich set of tools and technologies to shield sensitive data and achieve continuous security monitoring which is compliant with leading data privacy regulation and laws. The other benefit it renders is AWS native tools are integrated with all AWS services and hence can be easily configured.

This article is intended for all security professionals looking to secure AWS workloads implementing strong data loss prevention controls that meet business and compliance requirements. It also covers important factors to be considered when selecting AWS native services and 3rd party tools with their capabilities to help take the decision.

DECISION DRIVERS FOR SELECTING THE RIGHT SECURITY TOOLS

Below factors can guide us on selecting the right security toolset.

DATA SECURITY COMPLIANCE

Data security compliance is one of the biggest concerns for enterprises who are transitioning to the cloud. However, it becomes evident for customers to clearly understand how compliance can be achieved in the cloud and capitalize on it.

- Security Policies should be applied to the sensitive data which is stored on AWS Virtual Machines, any AWS data services or applications that stores for processing data.
- Monitoring should be enabled on AWS virtual machines by using AWS native monitoring tools or any Host-based DLP agents which has some pre-existing policies.
- Alert or Notification must be enabled and should be integrated with any incident response program which can be AWS managed service or any 3rd party incident management solution which can be integrated effectively with AWS which could pose a challenge.

INTEGRATION AND DEPLOYMENT

Organizations that have already invested a huge amount of money for their on-premise security tools, think of utilizing the existing infrastructure when they plan to move to the cloud. This will come with integration challenges when external cloud vendors API's don't support them but AWS API's are easily accessible and are supported by many players in the arena. They should also look at architecture possibilities when they use 3rd party tools or integrate their existing setup in terms of integration and deployment. AWS offers a marketplace where we can find a lot of partner solutions or similarly call as 3rd party tools on-premise which are available as the SaaS model specifically designed for AWS to make integration and deployment easy for customers.

COST AND LICENSING MODEL

Cost plays an important role when selecting the right security toolset and its capabilities to ensure data is protected and compliance with data regulation and privacy laws.

Customers should think of below aspects when taking cost into consideration:

- Many customers prefer to use their existing on-premise security tools and extend this to AWS for data loss prevention which turns out a very feasible option but comes with integration challenges and its capabilities.
- Choosing the right kind of IT expense model - CapEx or OpEx which determines your business spends on the cloud understanding the trade-offs. Long term forecasts and

changes in technology should be always kept in mind when spending money to get better benefits for your business operations.

- AWS marketplace provides a lot of 3rd party tools as a SaaS model where they are billed on the usage or flat fee structure. Most of these solutions are compatible with elastic workloads in AWS and will give organizations the option to choose a mix of licensing models that makes the right fit for them.

DATA LOSS PREVENTION CAPABILITIES/CONTROLS

NETWORK (DATA IN MOTION)

- This technology should analyze network traffic (HTTP, FTP, Email, and HTTPS) to detect and report sensitive data in motion
- Prevent users from accessing unauthorized sites
- Ensure data exchange with third parties by means of using a secure channel
- Ensure that the remote access to the company network through a secured connection
- Log and monitor network traffic to identify sensitive data transfers

ENDPOINT DLP (DATA IN USE)

- This technology tracks and controls information flow between users and groups.
- Monitor and control access to physical devices.
- Application controls to block when confidential information is accessed.
- Control user capabilities on endpoint systems.
- Prevent copying of data to unapproved devices.

DATA DISCOVERY

- Capability to scan on-premises and cloud storage for the discovery of sensitive data.
- Discover data in unstructured or semi-structured content types.
- Capability to scan sensitive data stored at SharePoint, Exchange

DETECTION AND PROTECTION

- Supports powerful deduction techniques such as machine learning, structured data fingerprinting, document matching and watermarking.
- Advanced integration with file encryption and decryption capabilities.
- Data recognition against encryption algorithm, digital rights and how data is compressed.
- Supports regulatory compliance and intellectual property protection requirements

SOLUTION

AMAZON MACIE

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 coming later this year.

FEATURES OF AMAZON MACIE

DATA DISCOVERY AND CLASSIFICATION

Amazon Macie enables you to identify business-critical data and analyze access patterns and user behavior as follows:

- Continuously monitor new data in your AWS environment
- Use artificial intelligence to understand access patterns of historical data
- Automatically access user activity, applications, and service accounts
- Use natural language processing (NLP) methods to understand data
- Intelligently and accurately assign business value to data and prioritize business-critical data based on your unique organization
- Create your own security alerts and custom policy definitions

DATA SECURITY

Amazon Macie enables you to be proactive with security compliance and achieve preventive security as follows:

- Identify and protect various data types, including PII, PHI, regulatory documents, API keys, and secret keys
- Verify compliance with automated logs that allow for instant auditing
- Identify changes to policies and access control lists
- Observe changes in user behavior and receive actionable alerts

- Receive notifications when data and account credentials leave protected zones
- Detect when large quantities of business-critical documents are shared internally and externally

AWS MARKETPLACE

As of now, AWS does not offer a complete DLP solution. The following list is not meant to be comprehensive but will highlight notable 3rd party capabilities from recognized vendors with data loss prevention offerings for AWS. The AWS Marketplace provides a wide range of data loss prevention solutions that can complement AWS native services and can help organizations implement a strong data loss prevention system.

- When choosing a 3rd party solution, whether to replace or complement AWS native functionalities, customers should look for a tool that is easy to configure and supports their operational integration requirements. Data generated from AWS must be ingested, parsed and visualized in a central dashboard with AWS specific charts. Methods for creating alarms and alerts, or for searching and correlating events should be a required functionality.
- AWS Marketplace could be a solution for customers with advanced data loss prevention requirements and do not have an existing investment such as organizations that work with PII or PHI data.
- The AWS Marketplace offers AWS specific solutions for data loss prevention in a Software as a Service delivery model or CASB with or without a preconfigured Amazon Machine Image and the billing is simplified by being added to AWS existing bills.
- If the organization has a multi-cloud strategy, the solution should have support across other cloud service providers.
- For a highly elastic cloud workload, the licensing model per instance might not be appropriate.
- Some of the DLP solutions support Amazon Bring Your Own License (BYOL).

SYMANTEC ENDPOINT PROTECTION

Symantec Endpoint Protection delivers faster, more advanced protection against today's sophisticated attacks. This multi-layered, industry-leading solution features a single powerful agent designed to protect your AWS machines from known and unknown threats without compromising performance.

- Unrivaled Security - Stops mutating malware, targeted attacks and advanced threats with intelligent security and layered protection - Provides Network Threat Protection, unique Insight reputation analysis and SONAR behavioral monitoring
- Blazing Performance - Performance so fast your users won't even know it's there- Virtual optimization layers that protect your high-density virtual environment
- Smarter Management - Singular management console across physical and virtual platforms with granular policy control

MCAFEE CLOUD WORKLOAD SECURITY – PAYG

McAfee Cloud Workload Security delivers comprehensive security for Amazon EC2. Cloud Workload Security discovers EC2 across all VPCs and deploys protection designed for an elastic cloud environment. Workloads can now be protected from advanced malware, remote exploits, and data theft.

- Discovers workloads across cloud environments, assesses and deploys protection designed for an elastic cloud environment. It offers 1. Visualization of your cloud workloads 2. Security posture assessment 3. Security group management 4. Firewall audit and hardening 5. IP traffic visibility and threat insights for instances 6. Remediation of your cloud workloads 7. Network traffic visibility
- Protection for Windows and Linux instances using Endpoint Security, Firewall, Intrusion Prevention, Application Control, File Integrity Monitoring and Encryption Management of EBS volumes
- Manage security policies with powerful reporting and alerting using McAfee ePolicy Orchestrator (ePO).

WATCHTOWER AI: DATA CLASSIFICATION, PROTECTION & LOSS PREVENTION (DLP)

Watchtower uses machine learning to identify business-critical data, like customer PII, across your SaaS, APIs, and data infrastructure. Supports data security & compliance initiatives with respect to GDPR, HIPAA, PCI DSS, and other compliance regimes.

- Continuously monitor sensitive data that is flowing into and out of all the services you use.
- Machine learning classifies your sensitive data & PII automatically, so nothing gets missed.
- Setup automated workflows for quarantines, deletions, alerts, and more - saving you time and keeping your business safe.
- Integrate with products including AWS services like Redshift, Aurora, RDS, S3, Dynamo, CloudTrail, etc.

- Leverage pre-tuned, standard detectors of PII out of the box, e.g. credit card numbers, emails, phone numbers, social security numbers, API keys, etc. or easily setup Custom Detectors.
- Rich analytics to examine all your PII risk, both in real-time and historically.
- Workflow builder to setup runtime policies with respect to sensitive data.
- Other integrations include-SaaS/Cloud Apps like Slack, Dropbox, Box, G Suite, Zendesk, Salesforce & Service Cloud, GitHub and Logging & Databases like Mongo, Splunk, Logentries, Elastic