Cloud Management Assessor

ENSURE THE SECURE CONFIGURATION OF YOUR CLOUD ASSETS

According to a recent analyst report, 53% of companies that use cloud storage services like Amazon S3 have failed to correctly configure a storage bucket, resulting in an unintended exposure of sensitive data. This is largely due to human error during the configuration process. Because companies are racing to move IT resources into the cloud, the number of inexperienced people setting up and managing cloud assets is high and will remain that way for years to come. Tripwire's Cloud Management Assessor (CMA) is designed to minimize these errors whether they occur in storage elements, cloud subscriptions or third party SaaS services.

Highlights

- Ensure the secure configuration of your AWS, Azure and GCP accounts to prevent incidents
- Verify AWS and Azure configurations against CIS Benchmarks to safeguard systems
- Monitor your cloud management accounts for changes that could result in breaches, non-compliance, downtime or surcharges
- Gain visibility across multiple AWS, Azure and GCP accounts
- Integration with AWS CloudTrails allows customers to scan only AWS buckets and objects that have changed

Cloud Management Assessor Benefits

Rapidly identify errors in the configuration of cloud subscriptions, storage accounts and third party SaaS services. This reduces the window during which sensitive assets may be exposed to attack.

Use a single tool to monitor configuration of Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) accounts. This minimizes operational challenges

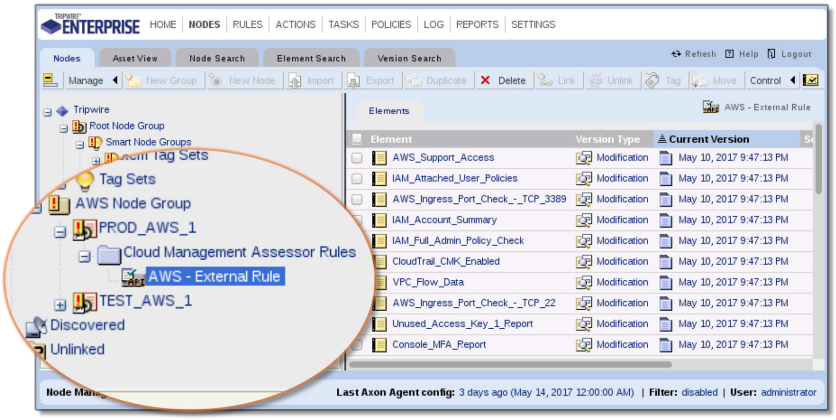

Fig 1. Seamlessly monitor your cloud management account configuration from within Tripwire Enterprise. AWS Nodes appear right along with the rest of your host, database and network devices.

associated with user education, tool integration and operator efficiency.

Monitors cloud storage objects for unauthorized content changes. Content such as web graphics are frequently the target of hacktivists that wish to disrupt operations and damage a company's reputation. Detecting unauthorized change is the first step to minimizing these events.

Permits Tripwire Enterprise users to leverage on-premise investments to monitor cloud assets. It is not necessary to invest in expensive new tools and operator training.

Cloud Management Assessor Features

Cloud Management Assessor enables Tripwire® Enterprise customers to harden cloud assets in four ways. Customers can monitor the configuration of cloud management features. These services can be performed for Amazon Web Services (AWS), Microsoft Azure and GCP accounts. Similarly, CMA monitors the configuration of third party SaaS offerings such as Salesforce.com. CMA is able to perform File Integrity Monitoring (FIM) on cloud storage elements such as AWS S3 and Azure Storage blobs. This will identify unauthorized change whether the change was caused by bad actors or by accident. And finally, CMA is able to verify configuration settings for compliance with the Center for Internet Security (CIS) standards/drafts.

Configuration Assessment

Cloud Management Assessor can automatically assess the configuration of your AWS S3 buckets and Azure Storage blobs to determine if they are exposed to anonymous Internet access, and report on objects that have become recently exposed.

Customers can monitor the configuration of cloud management features such as Identity and Access Management, Logging, Monitoring, Networking and more via the cloud management command line interface. As an example, an organization may have a policy limiting users to operations within a small number of regions that are regularly monitored. This is done so that that it is not possible to spin up instances in remote regions (a pattern associated with crypto-mining) that receive little attention. If a user's default region is changed to South America or China, CMA will issue a notification.

The proliferation of third party SaaS services introduces a new attack surface that can also be opened through misconfiguration. CMA is able to monitor the configuration of these new services and insure that they are not changed by accident or malice.

File Integrity Monitoring

Cloud Management Assessor can scan each of the buckets and objects you have stored in Amazon S3 and Azure Blob storage to make sure that those objects do not change without authorization. This capability can be useful in markets such as retail where product pricing and photographs may be placed in storage elements for use on an Internet accessible website. If these files change outside the normal change control process, CMA can alert the operator to a potential problem.

Ready for a Demo?

Let us take you through a demo of Tripwire Enterprise and answer any questions you have. Visit **tripwire.com/contact/request-demo/**

TECMA42a 1806