MONITORING SECURITY IN THE AMAZON CLOUD

Introduction

Amazon Cloud security configurations are the necessary controls enabled for identifying security breaches and data thefts, and ensuring integrity and confidentiality in your environment. These configurations play a vital role for your applications deployed on the Cloud, as they provide the satisfaction that your environment is safe from both internal and external attacks.

By continuously monitoring and analyzing your AWS security you ensure that any theft or security breach event is immediately identified and mitigated, and also ensure that all actions are recorded and can be used for auditing purposes in the future. With the right correlation between events, they also allow you to foresee any possible security events that can be remediated - before they even occur.

AWS Shared Responsibility Model

As shown in the diagram below, the AWS Shared Responsibility Model is designed to determine which security controls are AWS's, and which ones are yours. With the Shared Responsibility model, securing hardware, software (to run the infrastructure), and the network is AWS's responsibility - while maintaining the security of operating systems and your applications and data are on your shoulders.

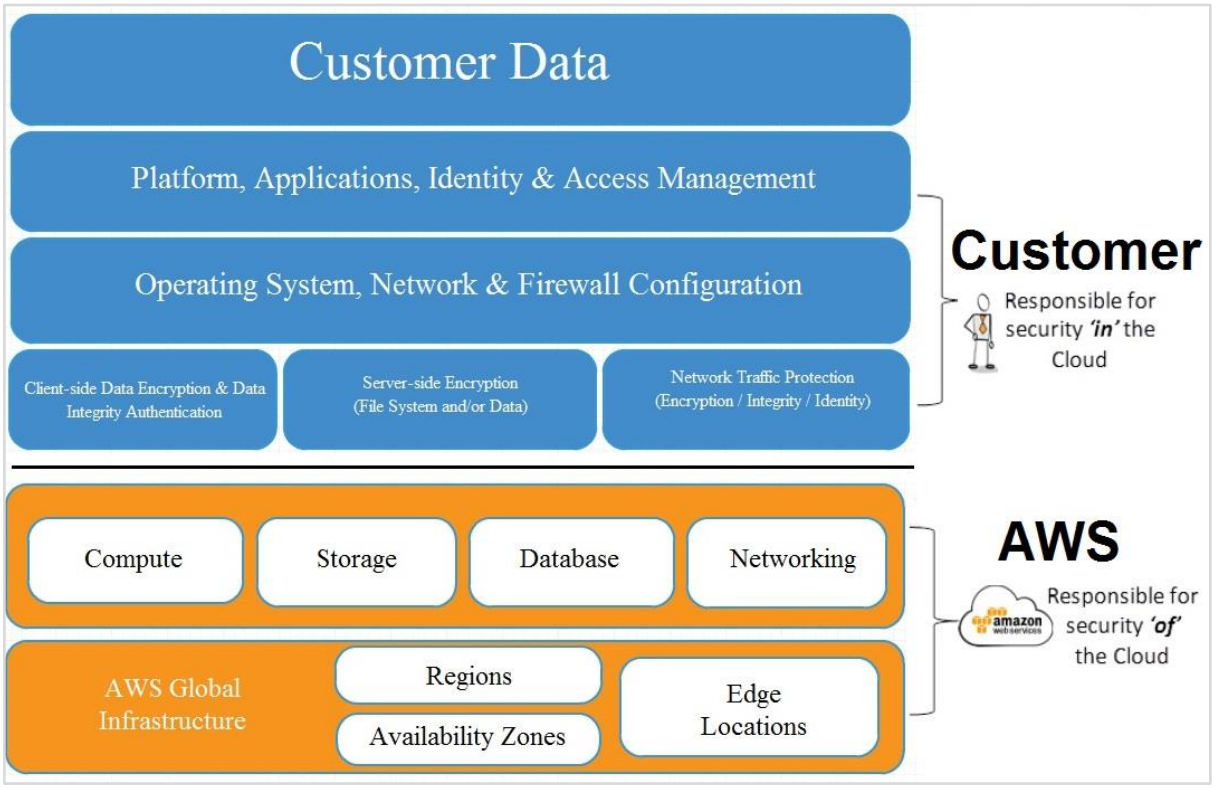

Image #1: AWS Shared Responsibility Model image source

AWS has already published various certifications on achieving global security standards - such as PCI-DSS, HIPAA, SOC, ISO 27001, FedRAMP, FISMA, etc. These are found on the AWS Compliance page, which provides complete transparency about security controls inside AWS's underlying infrastructure

and operations. AWS has also published a handy Compliance Enablers guide, which helps provide additional information for achieving necessary compliance levels.

On your end, monitoring your AWS security configurations is crucial and can help you achieve transparency that supports your responsibility for taking the correct mitigation actions.

AWS Security Key Services

Security and compliance controls in your environment are applicable at various levels - including internal organizational procedures, the AWS architecture level, and the application level. AWS security configurations possess many challenges, and proper control needs to be in place to mitigate those challenges.

The challenges can be related to a security mindset in an organization's workforce; a separation of duties between multiple parties; visibility in change management; separation between various environments (production, testing, development); maintaining multiple AWS accounts; or abstraction between multiple departments in an organization.

To ensure that all necessary security controls are in place, there are some key AWS services that need be effectively configured and monitored.

Those AWS services include:

- **Identity and Access Management (IAM) –** IAM security controls require ensuring no one logs in with a root account, MFA (Multi Factor Authentication) is enabled, and a strong IAM password policy is in place, limiting access to IAM users and using IAM roles instead of API keys.
- **Security Groups and Network Access Control Lists (NACLs) –** The right combination of security groups and NACLs act as an important firewall for your environment. This ensures that your resources such as EC2 and RDS instances are accessible from only the necessary IPs, and backend tiers (e.g., the database) are only accessible from the application layer.
- **Data Encryption -** AWS helps you achieve data encryption both in transit and at rest. For data in transit, AWS enables SSL termination at Elastic Load Balancer, and re-encrypts your traffic using backend authentication. For data at rest, AWS offers various solutions like Key Management Service (KMS), CloudHSM, Server Side Encryption, etc. If you want to use any third party solutions, you can certainly leverage security products from AWS partners, which are specifically designed for AWS encryption-related use cases.

Third Party Security Tools

In addition to the security controls offered by AWS, third party tools, such as CloudCheckr, are needed to help close the gaps, especially when it comes to large enterprise footprints. These tools might offer far more granular visualizations or allow you to continuously audit your application and OS security controls.

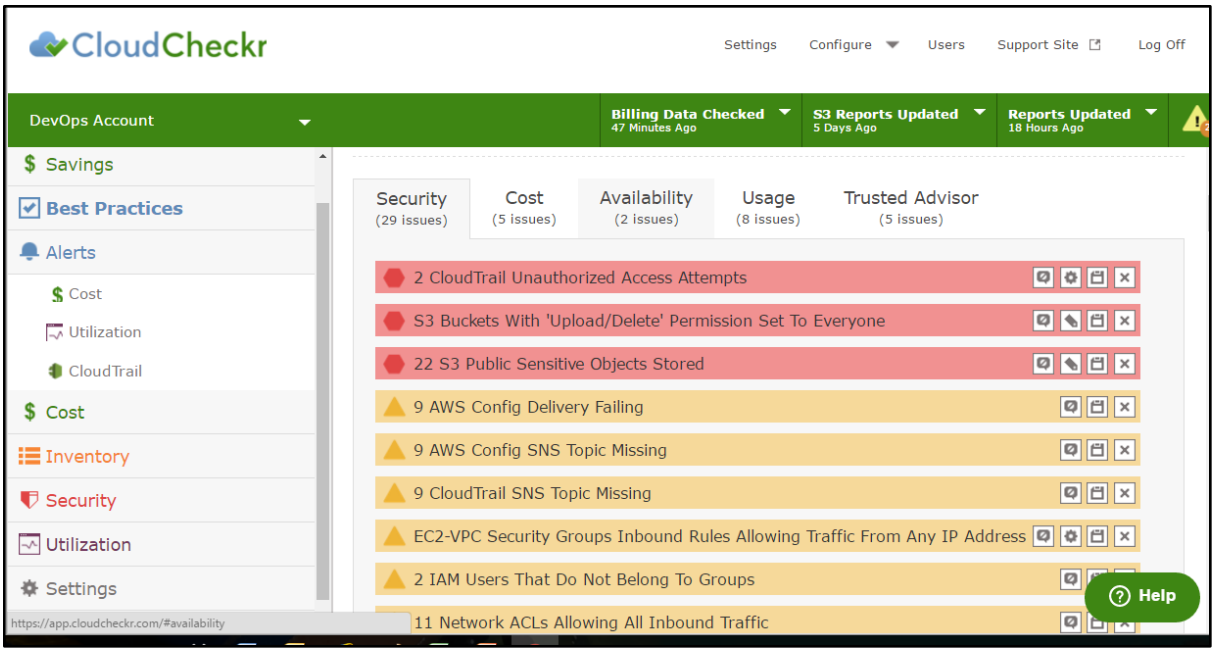

Image #2: CloudCheckr AWS Security Insights

However, it is important to note that the same tools used at a data center may or may not be applicable for architectures on the Cloud. For example, monitoring tools like Nagios provide performance metrics, but lack major features like integration with CloudWatch, various application-specific plugins, CloudTrail integrations, etc.

The same holds true for firewall devices or firewall rules management using 'iptables', where visibility and auditing is a problem as compared to managing them using Security Groups and NACLs. On the operating system and application level, security controls offered by AWS may not fulfill organization security and compliance controls. For example, AWS does not offer any host or network-based intrusion prevention systems or integrity monitoring controls. This leads to the requirement of third party tools to be configured at the host or network level. On the whole, users are best served looking for cloud-native solutions, and avoiding 'cloud-washed' data center tools.

Implementing Proper Visibility

Ensuring that all necessary security controls are in place is just the beginning, as maintaining and continuously auditing takes the game to the next level. After applying all security controls, however, various threats will inevitably pop up - including modifications in security configurations such as disabling log delivery or modification to log files; new users breaching security and operation controls; new services/features/controls introduced by AWS that should be thoroughly tested and integrated; or hitting service limits that might lead to a failure of resource creation. There is also a need to place only necessary alerts and dashboards, as too many alerts and visualizations may lead to missing out on critical security events.

To achieve necessary compliance and security controls in your dynamic cloud environment, you should continually implement proper monitoring and logging to enhance your environment's transparency. This is another area where a third party tool such as CloudCheckr becomes invaluable.

Access Control

Access control configurations define the communication between resources; for example, when a developer cannot access production instances or a web layer cannot directly talk to a database layer. As mentioned, these controls can be achieved by enforcing the right IAM policies, IAM roles to resources, tightly configured and monitored security groups, and NACLs.

Access control configuration change events can be monitored and trigger alerts by pushing relevant IAM logs to CloudWatch or Elasticsearch (as described below), or by leveraging any third party SIEM tools. These monitoring metrics can provide valuable visualizations and patterns about user access behavior. Setting necessary real time alerts is critical in order to be notified on any policy change that can lead to a breach.

Audit and Change Logs

We recommended enabling AWS CloudTrail, which keeps a complete audit trail of your AWS account activities. The CloudTrail logs can be shipped to an S3 storage bucket, which must be isolated with restricted access.

Each log delivery should trigger a notification so that any misconfiguration in AWS CloudTrail can be immediately detected. These audit logs can be fed either to a centralized logging system or AWS CloudWatch, and necessary alerts can be set where any misconfiguration or security breach activity notification can be triggered. For that matter, you should leverage third party solutions, such as CloudCheckr, that can help you overcome the complexities involved in analyzing the CloudTrail rough logs data, and provide actionable insights. Using these tools you will be able to search, analyze, and alert on any security configuration change. Without third party tools, users risk missing critical issues as they manually parse through millions of JSON logs.

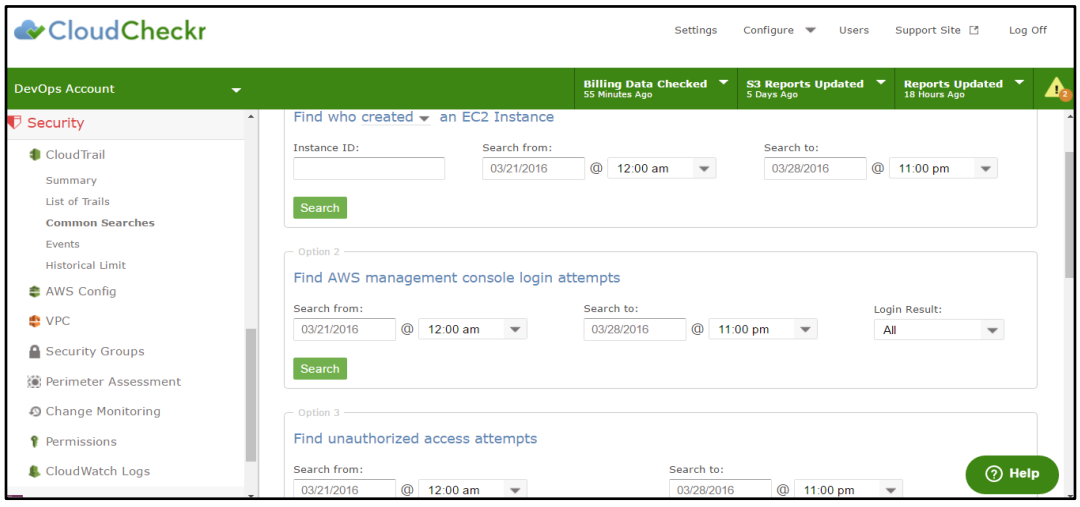

Image #3: CloudCheckr's CloudTrail Analysis

AWS additionally provides VPC logs, which allow you to capture network traffic flowing between network interfaces in a VPC. These logs can be shipped to Amazon CloudWatch logs. This becomes a great security feature, where all network traffic details are captured and retained for further network auditing and packet analysis purposes.

Monitoring with CloudWatch

AWS CloudWatch comes with a rich set of features that not only monitor the performance of your infrastructure, but intake logs from various AWS services like AWS CloudTrail and VPC logs, etc. The AWS CloudWatch logs agent also allows you to send instance and application logs directly to it. After log delivery to CloudWatch, various alerts can be configured based on regular expressions, and any security control breach activity can be identified and notified. For example, if anyone logs into AWS Management Console using a root account, an alert can immediately be triggered based on the event captured in CloudTrail, and then fed to CloudWatch.

Leveraging AWS Elasticsearch

The AWS Elasticsearch service allows you to process incoming logs from various AWS services, instances, and applications; trigger alerts based on events; and leverage on dashboards for visualizations; while AWS Config Rules allows you to continuously monitor compliance by defining guidelines for provisioning and configuring AWS resources in your environment. These guidelines are based on a set of predefined best practices or custom written rules. Any deviations from these guidelines can alert security administrators and automatically take actions defined as part of the rules - including terminating or deleting resources.

Continuous Security Assessments

Amazon Trusted Advisor acts as a boon for security administrators. Trusted Advisor continuously monitors your environment and publishes details about basic performance, security, or budget breaches in your environment. At the same time, it should be noted that there are limited metrics published by Trusted Advisor that are only available with the AWS premium support package. During the recent AWS re:Invent 2015 show, AWS also introduced the Amazon Inspector service, which performs an automated security assessment of your applications deployed on AWS. It comes with predefined policies, and your application is tested against those policies.

For enterprises and larger and more complex environments, there are third party tools that provide the greater depth and flexibility required by these users. For example, CloudCheckr automatically scans and reports on over 350 issues as compared to the 45 reported on within Trusted Advisor. CloudCheckr also allows users to create aggregated security views and alerts across hundreds of accounts - as opposed to having to manually administer and check each account individually.

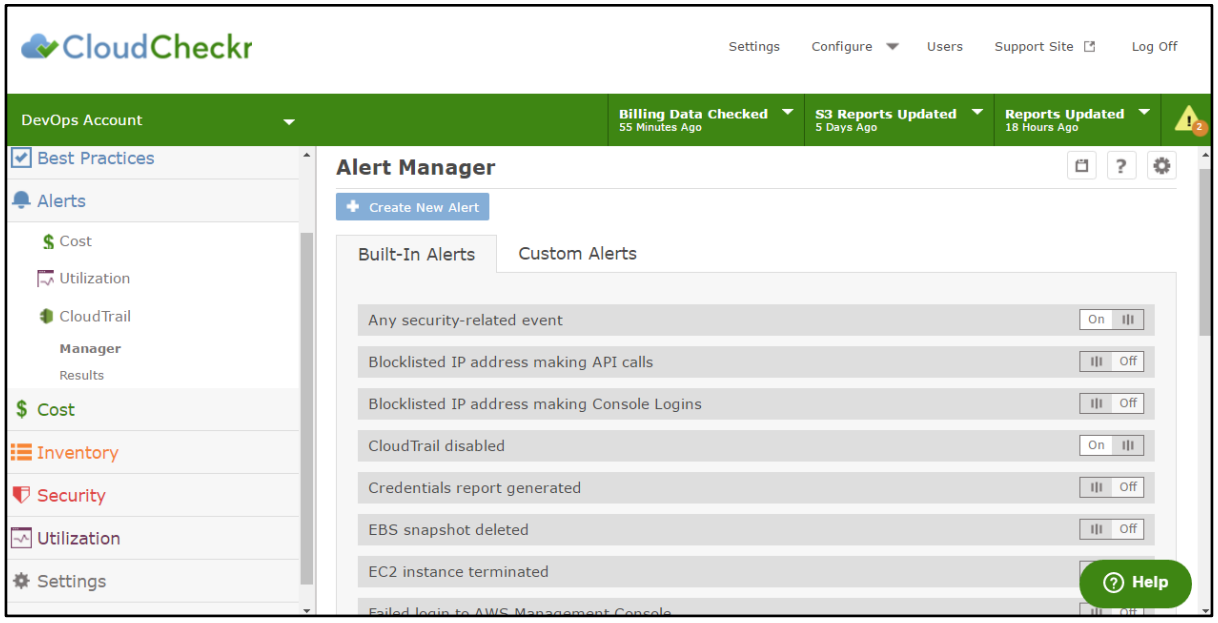

Image #4: CloudCheckr Alert Manager

Summary

Security Configuration monitoring in AWS is a critical component for managing your infrastructure and applications. Security Configuration helps you achieve data security, transparency about actions performed across your environment, and audit control and compliance for a complete and comprehensive audit trail on your entire AWS account.

Using the services and security controls described above, configuring them correctly, and controlling and monitoring them with comprehensive tools will lead to a secure and compliant environment for your enterprise, and ensure that your cloud-based assets are well-protected.

About CloudCheckr

CloudCheckr is a web-based software application that allows you to see and understand what is happening within your Amazon Web Services deployments.

Amazon provides the Amazon Management Console to configure and set up your AWS account. CloudCheckr takes it from there. It does not replace the functionality of the Amazon Management Console – in fact you don't ever make any updates to AWS through CloudCheckr. CloudCheckr is designed to report on and analyze what resources you are and are not using, where your spending is not optimized, what your account looked like historically, and what is changing in your account.

CloudCheckr uses the Amazon Web Services API to look at your AWS setup. CloudCheckr connects to your AWS account and grabs a "snapshot" of all of the settings and details on your account. This snapshot is then used to analyze your usage, costs, and provide best practice advice.

CloudCheckr capabilities include:

- Discovering and visualizing what's running in AWS
- Understanding costs in AWS
- Analyzing your usage in AWS
- Monitoring for changes in your AWS environment
- Hundreds of best practice checks covering security, availability, cost, and usage
- Maintaining a historical record of your cloud configuration

Contact Us

support@cloudcheckr.com
585-413-0869
www.cloudcheckr.com