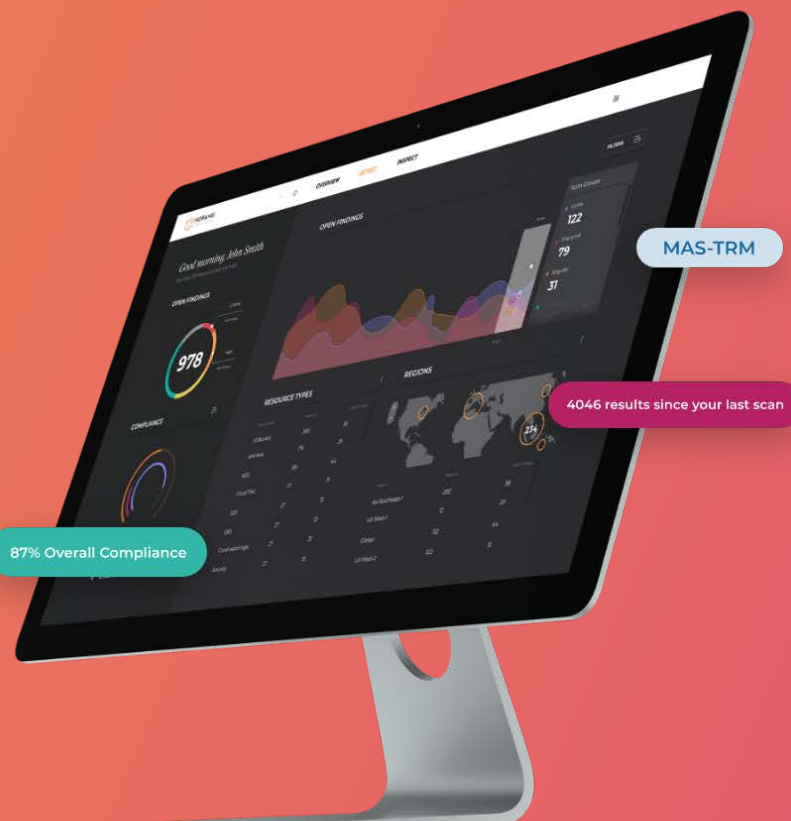




Horangi Warden: Continuous Cloud Security and Compliance

Identify, prioritize, and fix security threats with Horangi Warden.

Listed in Gartner 2020 Market Guide for Compliance Automation Tools in DevOps



Who is Warden for?



Security Teams



Compliance Teams



DevSecOps Teams



The Warden Advantage



Security

Continuous security monitoring identifies and protects you from top security risks.



Compliance

Ensure compliance of your cloud infrastructure with automated mapping of your cloud environment.



Easy to Use

Connect your cloud account and get visibility of your security posture in minutes.



With the sheer number of developer cloud accounts that we have, it is very challenging to keep track of how each is being configured. Implementing Warden to do the tedious work of monitoring was a no brainer for us. The amount of time I've saved and potential security incidents averted is enough reason to continue with this amazing software.

ALAN SCHMOLL, FOUNDER & CEO, ZAVE





Security

Warden continuously monitors your cloud environments for security vulnerabilities. Warden provides visibility of cloud posture across the major AWS and GCP resources including IAM, Amazon S3, ElasticSearch, ELBv2, CloudFront, Cloud Storage, Compute Engine, and Firewall Rules so you can prevent misconfiguring storage buckets, access controls, and more.

Compliance

Warden scans your cloud environment against the most recognized compliance and industry standards, including PCI DSS, NIST, and AWS Well-Architected Framework, helping organizations automate compliance and saving time.

Regional compliance standards such as MAS (Singapore) and BNM-RMIT (Malaysia) are also supported by Warden.

Easy to Use

Complete your setup on Warden in minutes and see your security posture by cloud resource, rule, or compliance standard. The change log in the Warden dashboard saves you time every day by alerting you to new issues that require your attention. Manage your security alerts and risk levels intuitively — Warden is integrated with task managers including GitHub, GitLab, and Jira.

Check Details MED OPEN

CloudWatch Log Metric Filter and Alarm for CloudTrail Configuration Changes Not Enabled

CloudWatch Alarm
Notes: Metric filter based on the pattern not found.
[Staging] Warden main AWS account
global

Description Compliance Recommendation History

It was discovered that one or more AWS accounts do not have a CloudWatch alarm for CloudTrail configuration changes.

AWS CloudTrail is a service that enables governance, compliance, and auditing of your AWS account. With CloudTrail, you can log, continue to audit, and investigate account activity related to actions across your AWS infrastructure, including console actions, API actions, and actions taken through the AWS SDKs, command line tools, and other AWS services. CloudTrail provides a history of your AWS account activity, including actions taken through the console, AWS SDKs, command line tools, and other AWS services. This history is used for security analysis, resource change tracking, and troubleshooting.

Amazon CloudWatch is a monitoring and observability service that provides actionable insights to monitor your applications, respond to system operational issues, optimize resource utilization, and get a unified view of operational monitoring and operational data in the form of logs, metrics, and events. CloudWatch provides a unified view of AWS resources, applications, and services that run on servers.

You can use CloudWatch to detect anomalous behavior in your environment. You can use CloudWatch to monitor logs and metrics side by side, take automated actions, troubleshoot issues, and optimize resource utilization. Real-time monitoring and alerting help you detect and respond to issues as they occur. You can direct CloudTrail Logs to CloudWatch Logs and establish correlations between CloudTrail events and CloudWatch alarms.

This rule checks for the following:

- Multi-region CloudTrail <trail> is active
- Multi-region CloudTrail <trail> captures all Management Events
- Active multi-region CloudTrail <trail> is piping all logs to a CloudWatch Log Group
- Metric filter associated with <metric> is created on the log group following filter pattern: "filterPatterns": [{"eventName": "CreateTrail", "eventName": "DeleteTrail", "eventName": "UpdateTrail"}]
- CloudWatch Alarm <alarm> is created on <metric>
- CloudWatch Alarm will send notifications to an SNS Topic <topic>
- SNS Topic <topic> has at least one SNS Subscription which will receive notifications

IMPLICATION
Monitoring changes to CloudTrail's configuration helps ensure that the configuration is correct and that the activities performed within the AWS account.

REFERENCES

- <https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/recv-log-files-from-multiple-regions.html>
- <https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html>
- <https://docs.aws.amazon.com/sns/latest/dg/SubscribeTopic.html>

YOUR SECURITY BRIEF
You have 964 open Findings matching these Filters.

Critical	High	Medium	Low	Informational
34	262	648	20	0

Rule Title	Scoring	FILTERS
CloudWatch Log Metric Filter and Alarm for CloudTrail Configuration Changes Not Enabled	0/1 Pass, 4 Fail	35
IAM Password Policy - Lowercase Characters Required Not Configured	0/1 Pass, 4 Fail	
CloudWatch Log Metric Filter and Alarm for Management Console Sign-in Without MFA Not Enabled	0/1 Pass, 4 Fail	
AWS GuardDuty Not Enabled	0/1 Pass, 65 Fail	
Hardware MFA Not Enabled for Root Account	0/1 Pass, 4 Fail	
IAM Password Policy - Numbers Required Not Configured	0/1 Pass, 4 Fail	
CloudWatch Log Metric Filter and Alarm for Network Gateway Changes Not Enabled	0/1 Pass, 4 Fail	
IAM Password Policy - Prevent Reuse of Last 24 Passwords Not Configured	0/1 Pass, 4 Fail	

CloudTrail S3 Bucket Not Secure 70 FINDINGS

CRIT

It was discovered that one or more CloudTrail S3 Buckets has Access Control List (ACL) permissions which makes it accessible to "Everyone" or "Any AWS Authenticated User". Using a loose set of permissions for S3 Buckets with CloudTrail logs allows unauthorized users access to sensitive CloudTrail logs of the AWS account.

VIEW SUMMARY VIEW ISSUE



Interested in improving your cloud security?

14-DAY FREE TRIAL

CONTACT US

