CloudHealth by vmware

SOLUTION BRIEF

CloudHealth Security Policies for Amazon Web Services

The Challenge

Cloud security starts with users. Without proper access controls and identity management, users can intentionally or unintentionally create security flaws with catastrophic outcomes.

According to Gartner, "through 2022, at least 95% of cloud security failures will be the customer's fault."[1] Therefore, organizations must understand their role in the shared responsibility model and take a proactive approach to cloud sercurity. As organizations continue to move production assets to the public cloud, it becomes critical to implement and closely monitor controls.

How CloudHealth Can Help

The CloudHealth platform helps you validate that you've properly and securely configured your Amazon Web Services (AWS) accounts, services, and resources. With configurable policies covering identity and access management, logging and monitoring, network security, and audit trails, CloudHealth identifies violations and makes recommendations for how you can improve your security posture.

The platform provides two default security policies, one based on The Center for Internet Security (CIS) AWS Foundations Benchmark and the other based on AWS Security Best Practices. You also have the option to create your own framework using a variety of individual policies.

"The CIS checks are fantastic, because that allows me to see the exact level of control I have over my system, and understand whether we're in compliance, all in one place." says Brent Strong, Manager of Cloud Engineering & Operations at Change Healthcare.

> ***"With CloudHealth, our Next Generation Managed Services (NGMS) team gets a holistic viewpoint across all our accounts to ensure compliance."***
>
> ***PAUL DUNLOP***
> Principal Cloud Architect, API Talent

[1] Gartner, Clouds Are Secure: Are You Using Them Securely?, Jay Heiser, 31 January 2018

How CloudHealth Security Policies for AWS Work

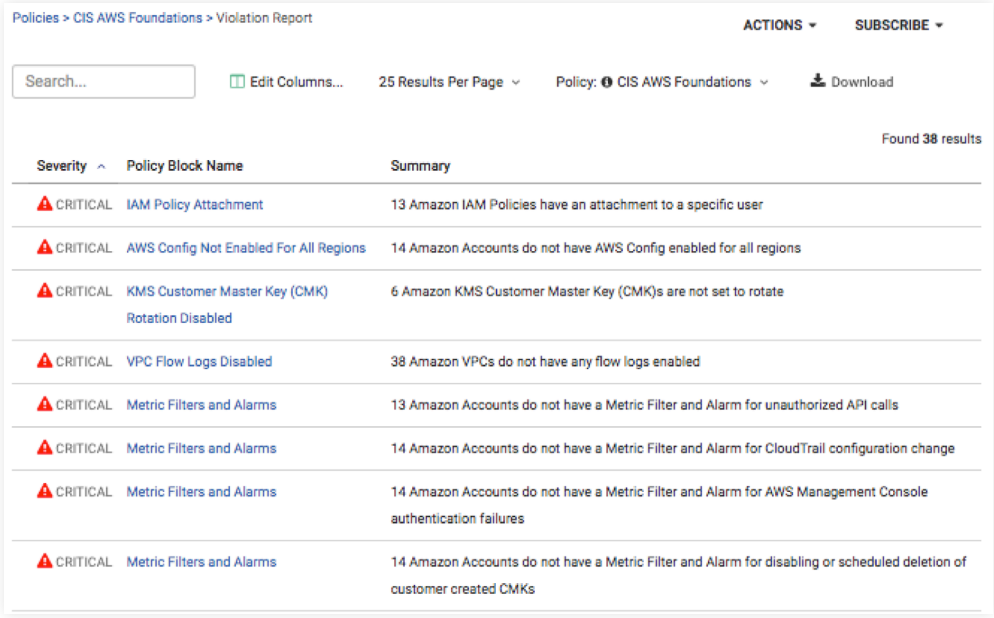
CloudHealth offers a dynamic policy engine, enabling you to drive optimization in an automated fashion. With CloudHealth Security Policies for AWS, you can:

- Receive automatic alerts that can be ranked and customized by severity (e.g. critical, high, medium).
- View all violations in a single report, which includes the full list of affected resources and recommended actions to remediate any issues.
- Configure security best practice policies across organizations, deliver violation reports via email, and exclude resources from future checks.

Futher enhance your security posture

With VMware Secure State you can leverage machine learning algorithms to detect critical misconfigurations, violation chains across objects, and anomalies that elevate the risk of a security breach.

Email vss@cloudhealthtech.com to schedule a demo.



Want to Learn More?

Visit us online **here** or email **info@cloudhealthtech.com** to learn how we can help you proactively monitor your AWS environment for security vulnerabilities.