CloudHealth® TECHNOLOGIES

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 2020, 80 percent of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities." 1 As production assets move to public clouds, it becomes critical to closely monitor controls in place.

HOW CLOUDHEALTH CAN HELP

CloudHealth helps organizations validate that they have properly and securely configured access their AWS environment with security best practice rules and policies. With deep checks on identity and access management (IAM) configurations, security groups, and Virtual Private Cloud (VPC), CloudHealth discovers and delivers actionable insight on security risks. Customers now have the ability to stay ahead of cloud security threats.

ALERT LOGIC® & CloudHealth® TECHNOLOGIES

Delivering visibility to protect your cloud

To enhance customers' security posture, CloudHealth partners with Alert Logic, the leader in security and compliance solutions for the cloud, to integrate incident alerts into the CloudHealth platform. Together, Alert Logic and CloudHealth can protect your sensitive data by identifying suspicious activity, obtaining context around security incidents and vulnerabilities, and providing incident validation and remediation steps, so you can successfully address the challenges associated with the evolving threat landscape.

WHAT ARE CLOUDHEALTH SECURITY POLICIES FOR AWS?

The Cloud Health policy engine is a powerful utility that enables customers to define granular policies and automate them. Now, with Cloud Health Security Policies for AWS included in the policy engine, customers can:

- Implement configurable policy-driven security alerts based on deep security best practice rules that are ranked according to severity.
- Flag policies for inclusion in the Policy Violation Report, which goes beyond simple alerting to provide deeper insight into the state of the violation, including affected resources and policy rule documentation.
- Define best practices across organizations, manage policy violations, automatically alert on critical issues, deliver violation reports via email, and suppress exempted resources.
- Provision fine-grained visibility using Perspectives that apply to specific business entities for service-level management, meaning that health checks can be customized for a particular business group.

"The cloud helps us pick up speed and bring innovations to our customers faster. CloudHealth helps us effectively manage the cost associated with that speed."

- Greg Nicastro, EVP of Product Development and Saas Operations, Veracode

"The integration between CloudHealth and Alert Logic [enables] customers to be more immediately aware of exposures and respond to threats within their cloud environment."

-Misha Govshteyn, Co-Founder & Chief Strategy Officer, Alert Logic

ABOUT CLOUDHEALTH TECHNOLOGIES

CloudHealth is changing the way organizations manage cloud environments through a policy-driven approach and focus on cloud governance. The company's cloud services management platform consolidates, evaluates, analyzes, and optimizes data from disparate data sources. This results in an optimally performing cloud environment, enabling enterprises and service providers to align cloud operations with business objectives, while reducing costs and ensuring service levels are being met. The company is backed by Scale Venture Partners, .406 Ventures, and Sigma Prime Ventures, and is headquartered in Boston, MA.

For more information, ***VISIT WWW.CLOUDHEALTHTECH.COM***

1 Source: Gartner, Magic Quadrant for Public Cloud Storage, Worldwide, July 26, 2016