Symantec | aws

CIS Benchmarks™

Amazon Web Services (AWS) Cloud Security
A Configuration Checklist

From the experts at Symantec + Amazon Web Services

Many organizations believe that the security responsibility of their workloads lies entirely with the cloud service provider, when in reality it is a shared responsibility between the customer and provider. According to Gartner, "Through 2022, at least 95 percent of cloud security failures will be the customer's fault."*

The non-profit organization CIS (Center for Internet Security, Inc.) recently worked with security experts like Symantec and others around the globe to publish the CIS Amazon Web Services Foundations Benchmark that has become the industry benchmark for securing AWS public cloud environments. CIS Hardened Images™ are Amazon Machine Images of today's most popular operating systems – pre-configured to meet the globally-accepted cybersecurity best practice guidelines of the CIS Benchmarks™ – to help you start secure and stay secure while working in the cloud. For more information, please visit www.cisecurity.org/cis-benchmarks/

Symantec's new Cloud Workload Assurance solution enables customers to score the security posture of their AWS instances to ensure compliance against these benchmarks. In addition, based on our work with organizations worldwide, Symantec and Amazon Web Services have highlighted what we believe are the Top 10 most important and easiest steps for customers to take when moving their infrastructure to AWS. Use this hands-on, actionable checklist to ensure your cloud environments are secure and configured correctly – and avoid becoming part of the 95 percent.

* *Gartner, "Clouds Are Secure: Are You Using Them Securely?," Jay Heiser, January 31, 2018. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

Identity and Access Management

- ☐ Avoid the use of the "root" account
- ☐ Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
- ☐ Implement strong IAM password policies across accounts

Logging

- ☐ Ensure that CloudTrail is enabled all regions
- ☐ Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible

Monitoring

- ☐ Ensure a log metric filter and alarm exist for usage of the "root" account
- ☐ Ensure a log metric filter and alarm exist for IAM policy changes

Networking

- ☐ Ensure no security groups allow ingress from 0.0.0.0/0 to port 22
- ☐ Ensure the default security group of every VPC restricts all traffic
- ☐ Ensure routing tables for VPC peering are "least access"