Build in the cloud with confidence

While AWS provides secure cloud infrastructure, through the Shared Responsibility Model, you are responsible for securing the workloads, applications, and data that you run on AWS—that’s where Trend Micro can help.

Our services help you map to the AWS Well-Architected Framework so you can build stable cloud architectures and meet ongoing compliance requirements, keeping your environment secure and scalable.

Establish a strong cloud foundation with the AWS Well-Architected Framework

The AWS Well-Architected Framework provides a consistent approach to building cloud architectures that can scale over time. By adopting your approach to the Shared Responsibility Model with the six pillars of the AWS Well-Architected Framework, it takes any guesswork out of the process. Leverage consistent best practices and guidance for your architecture so you can focus on building great solutions in the cloud, fast.

Continuously safeguard your AWS investments with Trend Micro Cloud One™ – Conformity

Securing what you build in the cloud is not a one-and-done scenario. It’s an ongoing process that should adapt over time. Conformity provides automated checks and clear remediation steps based on the AWS Well-Architected Framework—keeping you on top of the latest from AWS and best practices.

Steer clear of security risks with just-in-time alerts

A data breach can happen in an instant. Conformity can deliver the latest information and tools to help you secure what you have in the cloud.

Without Conformity:

• PII data breach due to misconfiguration
  - Your company has to report to its shareholders about this massive data breach and do major damage control.
  - When your PII is made public, you don’t receive a notification. Six months later, all your data has been hacked and shared.
  - You’ve activated an Amazon S3 bucket to store personally identifiable information (PII) about your customers.

With Conformity:

• Keeping hackers out of your Amazon S3 bucket
  - This time you’re the same engineer, but you have Conformity.
  - Conformity identifies the risk in real time and notifies you that your Amazon S3 bucket is publicly readable and not encrypted.
  - Conformity sends you a message with instructions from Knowledge Base on how to configure your Amazon S3 bucket so it’s no longer public.
  - You put yourself in the line of protecting customer PII and upholding your shared responsibility efficiently.

Copyright © 2022 Trend Micro Incorporated. All rights reserved. [INF03_Conformity_AWS_Infographic_220527US.ai]