Continuity Software

# Coral™ – Achieve Best-of-Breed Infrastructure

## Plus Continuous Assurance for the AWS Well-Architected Framework

## Challenges to Reliability in your AWS environment

In dynamic cloud environments, new services and features are introduced all the time. Velocity of changes to services and apps that are not completely validated before each production update lead to misconfigurations and inject risks into production environments. Multiple DevOps and development groups maintaining the environment are not aligned with up-to-date best practices. All these can lead to outages, costly performance disruptions and data-loss incidents.

Achieving reliability in your AWS environment under such conditions is a real and known challenge, and one that needs to be addressed by a solution that continuously identifies misconfigurations that can lead to downtime and data-loss and automatically assures adherence to AWS Well-Architected.

## Coral™ for AWS
## Achieve reliability in your AWS environment

Coral™ is a SaaS solution that automatically and proactively detects misconfigurations and risks across all layers of your AWS environment including virtual machines, containers, networks, load balancers, databases, cloud storage, DNS, and more.

A built-in risk detection engine that utilizes machine learning algorithms and is based on a proprietary knowledgebase containing hundreds of best practice rules identifies misconfigurations and risks. The knowledgebase includes AWS best practices for adherence to the Well-Architected Framework. When a risk is detected, a detailed description and the recommended path for resolution are presented to the appropriate team for immediate remediation, before business is impacted.

## Benefits

60% of the top US banks use our knowledge-driven IT configuration analysis to prevent outages and data-loss.

**Assure 24x7x365 Reliability**

Automated and proactive misconfiguration detection prevents outages and protects data before it is lost, damaged, stolen, or unrecoverable

**Continuous Assurance for the AWS Well-Architected Framework**

Automate adherence to all five pillars of the AWS Well-Architected Framework: Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization

**Shift Left on your AWS Reliability**

Eliminate misconfigurations and risks as part of your CI/CD pipeline before they impact business; reduce time and cost of repairing post-production flaws

**Facilitate Automatic Healing**

Achieve faster response time and decrease operational costs with automated self-healing

# Coral™ and AWS – Better Together

Companies whose cloud environments reside on AWS have an advantage. AWS contributes to assuring reliability by maintaining infrastructure and services and providing the Well-Architected Framework guidelines and tool. The customer is responsible for architecting, assembling, configuring and operating their environment properly to assure reliability.

But, reliability is dependent upon following guidelines and best practices. Without an automated solution, it's impossible to comply with all the evolving best practices, especially in a dynamic cloud environment. Violations of best practices can lead to a significant impact on business.

With Coral™, misconfigurations and risks to reliability, due to non-compliance with vendor and industry best-practices or with AWS Well-Architected, are automatically and proactively detected across all components of your AWS environment. This leads to an 80% reduction in unplanned infrastructure outages.

## Features

### Deep Knowledge

The solution's powerful risk detection engine runs configuration analyses against an unequalled knowledge base of 300+ (and growing) rules of best practices from vendors, industry and power-users. Machine learning algorithms and crowd knowledge enable visibility into the AWS environment and configurations. Problem areas are pinpointed, allowing their repair before they erupt into costly disruptions to business.

### Visibility and Control

IT executives look for ways to continuously improve the reliability of their AWS environment. Hence, they need visibility and control to boost operational excellence and improve KPIs. Coral's intuitive dashboard with its compliance view provides the in-depth information needed so that managers can keep their finger on the pulse of multiple and geographically dispersed AWS environments. They can immediately see risks to availability and data throughout the enterprise's entire AWS environment, pinpoint areas of non-compliance with AWS Well-Architected, and the potential impact each risk may have on critical business services. Guidelines for proactive repair of risks are simple and easily executed.

## Case Study: Certsys adopts Coral™ to assure adherence to the AWS Well-Architected Framework

### Challenges

Certsys needed to be sure their environment was consistently in good standing with respect to the AWS Well-Architected Framework, the standard for reliability the company set for itself. They knew this was key to meeting their goals for disruption-free 24x7x365 availability and security.

### Solution

Initial scans of Certsys's AWS environment revealed 77 risks of non-compliance with AWS Well-Architected Framework standards alone. Most prominent were risks to security, reliability and operational excellence, pertaining to domains, such as virtual machines, databases, networking, and others. The solution provided clear explanations and instructions for repair.

### Results

Certsys uses Coral™ to ensure they continuously meet AWS Well-Architected Framework standards as well as vendor, community and industry best practices. Detected risks are reported as incidents on the ITSM tools they already use. Certsys has seen significant improvement in reliability and is confident in their ability to protect data.

## Get started with Coral™ for AWS

Visit Coral™ on AWS Marketplace to subscribe or get started with a Free Trial today.