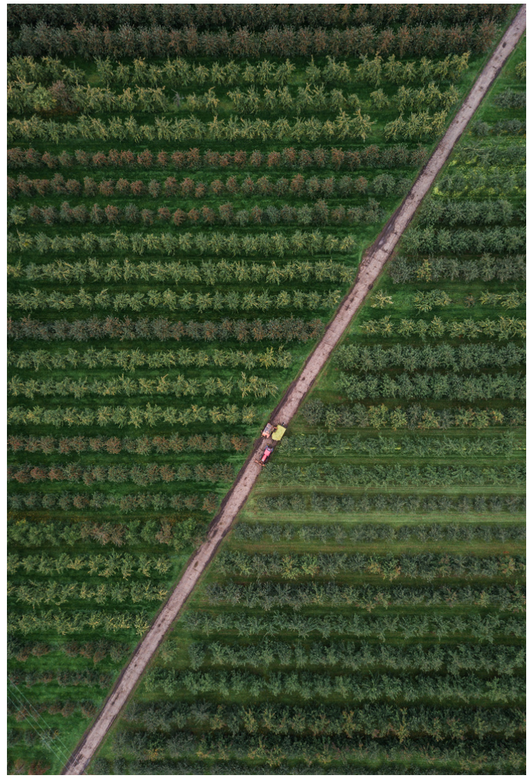
Cloud Infrastructure Vulnerability Assessment & Remediation

Our Customer, a US-based AgriTech Giant, was dealing with noncompliance and vulnerabilities within its large AWS infrastructure spread across 32 VPCs within four US Regions resulting in significant business risks.



A tool-based and automated remediation solution was needed to handle the volume of fixes to the environments.

Challenges

- Changes to be carried out in production environments without causing disruption to their business
- Every change to be planned and managed with the stakeholder
- Every change needs to be automated and tested with backout planning

Solution

Stanra assessed the infrastructure using tools and best practice frameworks.

Assess as per Well-Architected Framework for Security, Reliability, Performance Efficiency and Operational Excellence pillars.

A total of 90+ vulnerabilities were identified, like Unsafe Security groups, Unencrypted EBS volumes, RDS and AMIs, Unattached EBS volumes, Publicly accessible resources, MFA, password policies, group policies, Enabling of VPC flow logs, cloud trails, S3 versioning, multi-region availability.

Three-pronged plan: 1. Remediation 2. Implement best practices 3. Migration

- Developed scripts using Python and Terraform for automated modifications across the set-up
- Test the scripts in a development environment
- Workshop with customers and execution in Production.

Innovation

- Automated intervention, no manual activity
- Full backout planning.

Benefits

- Removable of system vulnerabilities and reduce business risk
- Moving to Well Architected Framework and implement best practices
- Automation

Result Highlights

90+ Vulnerabilities Removed

Full Backout Planning

Fully-Automated Interventions