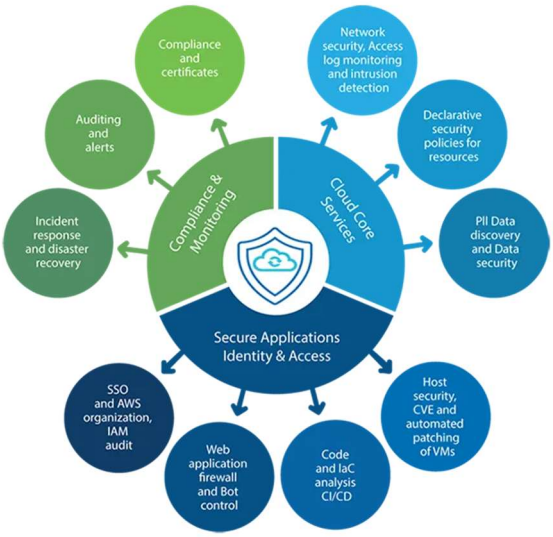
AWS Security Review Service

Public cloud environments provide much-needed technology innovations to businesses that face the challenges of not being able to innovate at a pace. However, adopting cloud technologies present businesses with a more significant challenge of securing their cloud infrastructure because the security in the cloud is a shared responsibility. Dozens of companies have reported hacks into their infrastructure, loss of user/company data, millions in revenue loss, and not to mention damage to their reputation.



Rocky Road Solutions (RRS) provides a superior cloud security review service to safeguard an organization's cloud infrastructure. The deliverable of this service is a detailed report listing all areas of possible vulnerabilities, weaknesses, and misconfigurations in your cloud environment. Along with this report, we will provide immediate fixes for critical security issues in the production environment while ensuring business continuity.

Service Highlights

Below is a summary of activities completed by our cloud security experts to prepare the cloud security review report for your cloud infrastructure:

AWS WAF: We review and set up application static and dynamic security using AWS WAF.

Security of identity and access management (IAM): IAM security is reviewed in the light of industry best practices for accounts, organizations, users, management of credentials and secrets, and policy enforcement. This review ensures that no employee, application service role, or process can compromise the security of AWS accounts.

Security of the network: All network assets, including VPCs, gateways, and routing configurations, are reviewed to ensure isolation, protection, and intrusion detection controls are in place. Public ingress/egress endpoints are evaluated for security, compliance, and regional/global availability.

Data and Communication Security: Review all cloud storage technologies, including EBS/EFS volumes, object storage, and storage gateways for required encryption, versioning, and backup. Review data security in transit to ensure appropriate TLS protocols are being used. Review of security controls set up to ensure only correctly assigned owners have access to storage.

Security of Compute resources: We will review EC2/ECS/EKS and serverless/fargate compute resources and ensure all AWS CIS best practices are followed regarding patching and CVE advisories. We will check existing periodic, and on-demand vulnerability scanning controls

and IAM/Kubernetes service accounts so only authorized users and applications can provision or use compute resources.

Continuous Security Setup

RRS engineers will set up continuous capture and logging of all traffic flows in and out of VPC and storage of AWS API audit trials so intrusion detection and unauthorized access /usage of services can immediately be prevented. We will set up Configuration monitoring controls based on customer security requirements, including:

- Operational-Best-Practices-for-AWS well-architected framework
- CIS Benchmark for CIS AWS Foundations Benchmark, v1.2.0, Level 1, 2
- Operational-Best-Practices-for-CIS-Critical-Security-Controls
- Any additional security control, including PCI_DSS, NIST, SOC, HIPAA, and GDPR

We will also set up AWS security hub reporting for all controls so a 360-degree view of security is available all the time and can be set up.

- AWS GuardDuty for advanced intrusion detection
- AWS Macie for PII data security
- Web application firewalls for public endpoint security

RRS Advantage

Our commitment to our clients is that we will do everything possible to ensure your AWS accounts are secure. If your monthly cloud billing is less than $25,000, then we will secure all AWS accounts within four weeks at a fixed price of $25,000*.

For Additional Information

For any additional inquiries please send email at contact@rockyroadsolutions.com and out team will contact you within 1 to 2 business days.