REDSEAL

REDSEAL AND AMAZON WEB SERVICES

Level-Up AWS Cloud Security in Hybrid Environments

Modern security incidents span network fabrics

Amazon Web Services (AWS) is the world's most broadly adopted cloud, helping organizations lower costs, be more agile, and innovate faster. AWS makes it easy to spin up IT resources whenever you need them, however and wherever you want to run them. But all that flexibility can result in overwhelming complexity, especially for teams trying to secure growing, hybrid networks that span physical data centers, myriad devices, and multiple cloud environments.

Modern security incidents rarely have a single, simple root cause but often result from chains of mistakes made both in the cloud and on premises. Analyzing those chains to find the defensive gaps is impossibly hard for humans alone, but it can be simple with the right software. In a complex hybrid network, only automation can sniff out every forgotten loophole or overlooked pathway putting your AWS assets at risk.

Reduce cloud risk with RedSeal

RedSeal models your entire hybrid environment and delivers a visual map showing every asset that is connected, which assets are exposed to risk, and, most importantly, which technical controls need to change to block any unauthorized access or unexpected threats. RedSeal can pinpoint specific rules for AWS assets that are weak and show you the precise chain of mistakes made across load balancers, gateways, firewalls, security groups, service chains, and more.

aws

RedSeal benefits

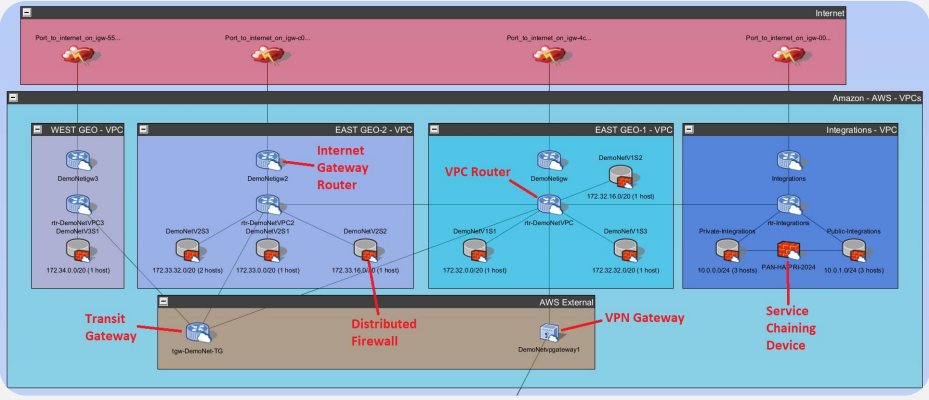
- Ensure continuous compliance with internal policies, external regulations, and best practices for secure cloud configuration, segmentation, and access
- Fortify security within and between public cloud, private cloud, and on-premises environments
- Discover networked cloud assets previously unknown or unaccounted for
- Get a single, comprehensive model to view and query your entire hybrid network at once

Enrich cloud security decision making with network exposure management

The RedSeal network exposure management platform helps you assess the security controls within and between your cloud-based and physical assets. You will need a license and plugin to bring AWS into your network model, but it's as easy as entering your AWS account number(s) and clicking a button. RedSeal pulls in all Virtual Private Clouds (VPCs), even ones you didn't know were created. Then, it analyzes all rules, configurations, segmentation, threats, and access—both east-west and north-south traffic—to deliver a prioritized list of issues and the details you need to remediate them efficiently.

With the RedSeal + AWS integration you can:

- See all VPCs in an AWS account
- View all security groups within a VPC
- View all AWS instances (hosts) associated with a particular security group
- See specific firewall rules that apply to an AWS instance (host)
- Query AWS subnets and view micro-segmentation
- View service chaining
- View connectivity among AWS, other clouds, and on-premises environments
- Validate compliance with cloud configuration, segmentation, and access rules



AWS Topology Map in RedSeal

Ensure continuous compliance in the AWS Cloud

In hybrid environments, cloud security depends on the security of the entire network. With RedSeal, your on-premises and cloud environments come under a unified security architecture that is continuously being modeled, analyzed, and checked for compliance with internal policies, external regulations, and best practices. RedSeal helps you understand access to (and from) AWS in hop-by-hop detail, assesses your segmentation and configurations against policies, and alerts you when violations or vulnerabilities are discovered. The integration of RedSeal with AWS enables you to correct or validate all aspects of your AWS deployment for unprecedented levels of security and compliance.

Contact RedSeal for more information or request a demo today.