REDSEAL

RedSeal Cloud

Identify critical resources inadvertently exposed to the internet

Continuous assessment and mitigation of exposure to the internet

RedSeal Cloud is a trusted and proven Cloud-Native Application Protection Platform (CNAPP) offering both security posture assessment and workload protection management capabilities for public cloud environments. RedSeal Cloud reduces risk by mitigating exposure to threats, vulnerabilities and ransomware and continuously protecting the resources in your Amazon AWS and Microsoft Azure clouds. It consistently identifies misconfigurations across these cloud environments based on cloud security best practice benchmarks, common frameworks and industry standards.

RedSeal Cloud proactively discovers your cloud resources, automatically builds the relationship between the resources, and then provides an in-depth visualization of the topology and hierarchy of your cloud infrastructure, including connectivity between all resources and the internet. Uniquely, this proactive assessment of potentially exposed resources does not require active traffic flow—providing an additional layer of upfront protection.

RedSeal Cloud then assesses the risk of cloud resources by automatically calculating if cloud resources have exposure to the internet. The solution allows a detailed drill down for exposed resources to identify the impacted resources, attack path analysis, and precisely how the exposure has occurred and provides remediation guidance for the ticket system.

Fast and accurate multi-cloud exposure detection

As organizations adopt more public cloud services and technologies, the ability to keep up with the latest security practices becomes increasingly complex. Misconfigurations are the norm—leading to inadvertent exposure of proprietary data and assets to unauthorized individuals. RedSeal Cloud analyzes cloud resources and connectivity from an end-to-end perspective and quickly identifies what resources are exposed to the internet, resulting in a significantly lower risk posture.

Why use RedSeal Cloud to stop unintended exposure?

- Accurately visualize your entire infrastructure
- Confidently identify exposed critical resources and data
- Easily remediate incidents via seamless ticketing integration
- Quickly gain root cause analysis with full attack path analysis
- Easily display cloud security posture over time
- Understand where you are most exposed by account, tag, and security group-based identification and prioritization

RedSeal Cloud mitigates exposure with:

- Out-of-the-box (OOTB) reporting
- Continuous risk assessment
- Drill down capabilities with remediation guidance and insights
- Simple, agentless deployment
- Seamless integration with ticketing/remediation systems like Jira

RedSeal Cloud provides:

- A list of resources (subnets/ instances) deemed critical grouped by AWS accounts, Azure subscriptions, AWS VPCs, Azure VNETs, tags and subnets
- Specific ports, protocols, and services that are open and exposed (e.g., HTTPS (443), SSH/TCP (22), SMTP/TCP (25), RDP) with exposure details
- Full attack path analysis to critical resources – highlighting all possible paths and policy details associated with each path
- Information about what traffic that can enter/exit a hop on an attack path and what controls are enabling entry/exit

Reveal all unintended exposure in a single view

Discover and mitigate unintended access to critical and vulnerable cloud resources
RedSeal complements AWS and Microsoft Azure's security tools by providing details of affected resources in one intuitive and consistent view across these multiple cloud environments. Utilizing an agentless, API-based approach, it readily discovers all resources deployed in your environment and presents them to you in a 'single pane of glass.' An agentless implementation significantly decreases operations time and expense while simplifying the infrastructure.

RedSeal Cloud checks for common, unintentional exposures – such as public access to cloud workloads and misconfigured web services and provides details highlighting each exposure and its level of severity. Providing short- and long-term monitoring and analysis, RedSeal Cloud offers SecOps teams fast and effective continuous risk assessment across their clouds, protecting critical resources.

Pinpoint remediation steps

Understand how to quickly identify and mitigate risk with high-fidelity insights
RedSeal Cloud enables security teams to create high-fidelity remediation strategies. By analyzing the data of the security checkpoints and their associated policies (i.e., filters, controls), Cloud proactively identifies and calculates all possible paths, ports and protocols used from the internet to critical resources (not just paths with active traffic) to best pinpoint which exposure to address first. Using intelligent vulnerability calculations, security teams can perform root cause analysis and raise a remediation ticket for the group of resources that could be impacted by one or more security policies.

The ticket will cover the impacted resources, verification, remediation steps and risk, if they are not fixed. Via a combination of extensive reporting capabilities and integration with out-of-the–box ticketing systems like Jira, security teams can expedite their incident response programs. This integrated reporting capability in Cloud also allows SecOps and DevOps teams to better collaborate and resolve exposure and vulnerabilities in critical resources.

> "Through 2025, at least 99% of cloud security failures will be the customer's fault."
>
> — Gartner, Innovation Insight for Cloud Security Posture Management, January 2019, by analyst Neil MacDonald