



# RedSeal Stratus

Achieve Continuous Compliance in  
Your Multi-Cloud Environment

## Why use RedSeal Stratus to maintain compliance in your multi-cloud environment?

- Simplifies and ensures continuous 24/7 compliance
- Minimizes non-compliance, audit failures, and potential regulatory oversight
- Enables customized compliance policies appropriate for your organization
- Quickly establishes a baseline for critical violations unique to your organization
- Provides extensive reporting on compliance status

## Eliminate Compliance Alert Fatigue with RedSeal Stratus

- Meet external and internal compliance mandates within budget and on-time
- Proactively run compliance checks
- View drill down details on violations and checks
- Follow remediation guidance through simple steps

RedSeal Stratus 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 Stratus reduces risk by mitigating exposure to threats, vulnerabilities and ransomware and continuously protecting the resources in your 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 to ensure compliance.

RedSeal Stratus 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 Stratus then assesses the risk of cloud resources by automatically calculating if cloud resources have exposure to the internet. The solution provides a detailed drill down on 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.

## RedSeal Stratus fortifies your multi-cloud environment with:

- Always-on compliance assessment and monitoring
- Comprehensive inventory discovery and mapping
- Visualization of connectivity between AWS and Azure clouds
- Drill down capabilities with remediation guidance

“Continuously monitoring my cloud environment for CIS benchmark violations helps me to stay on top of the failed checks so that immediate action can be taken.”

— RedSeal Stratus Customer

## Optimize Your Cloud Compliance

As organizations adopt more public cloud services and technologies, the ability to track their existing resources while maintaining compliance becomes increasingly difficult. This becomes more and more challenging in multi-cloud, global environments, introducing the risk of unknown and unsecured assets leading to compliance violations and audit failures. The result of these violations could be detrimental to an organization’s reputation, lead to increased regulatory oversight, and invoke potentially costly fines.

## Constant, Consistent Compliance Assessment

### Ensure your cloud environment is up-to-date and secure

RedSeal Stratus complements the security tools offered by Cloud Service Providers (CSPs) by providing more details of deployed resources across multiple clouds in one consistent view. RedSeal Stratus utilizes the knowledge base of multiple international industry standards and best practices as a foundation for its always-on compliance monitoring. For example, a key compliance assessment provided is for CIS Controls. By understanding all access paths across your clouds, RedSeal Stratus delivers a strong foundation for a CIS Top 20-based security strategy. Security teams can be confident that, as their organization’s clouds evolve and grow, so does their protection provided by RedSeal.

## Pinpoint Remediation Steps

### Quickly identify and resolve compliance violations across your enterprise

RedSeal Stratus enables security teams to create high-fidelity remediation strategies upon finding compliance violations of exposure and misconfiguration.

By analyzing the data of the security checkpoints and their associated policies (i.e., filters, controls), RedSeal Stratus 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.

---

### ABOUT REDSEAL ([redseal.net](https://redseal.net))

RedSeal — through its cloud security solution and professional services — helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal’s award-winning cloud security solution can bring all network environments— public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises — into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability’s associated risk. The company is based in San Jose, California.

