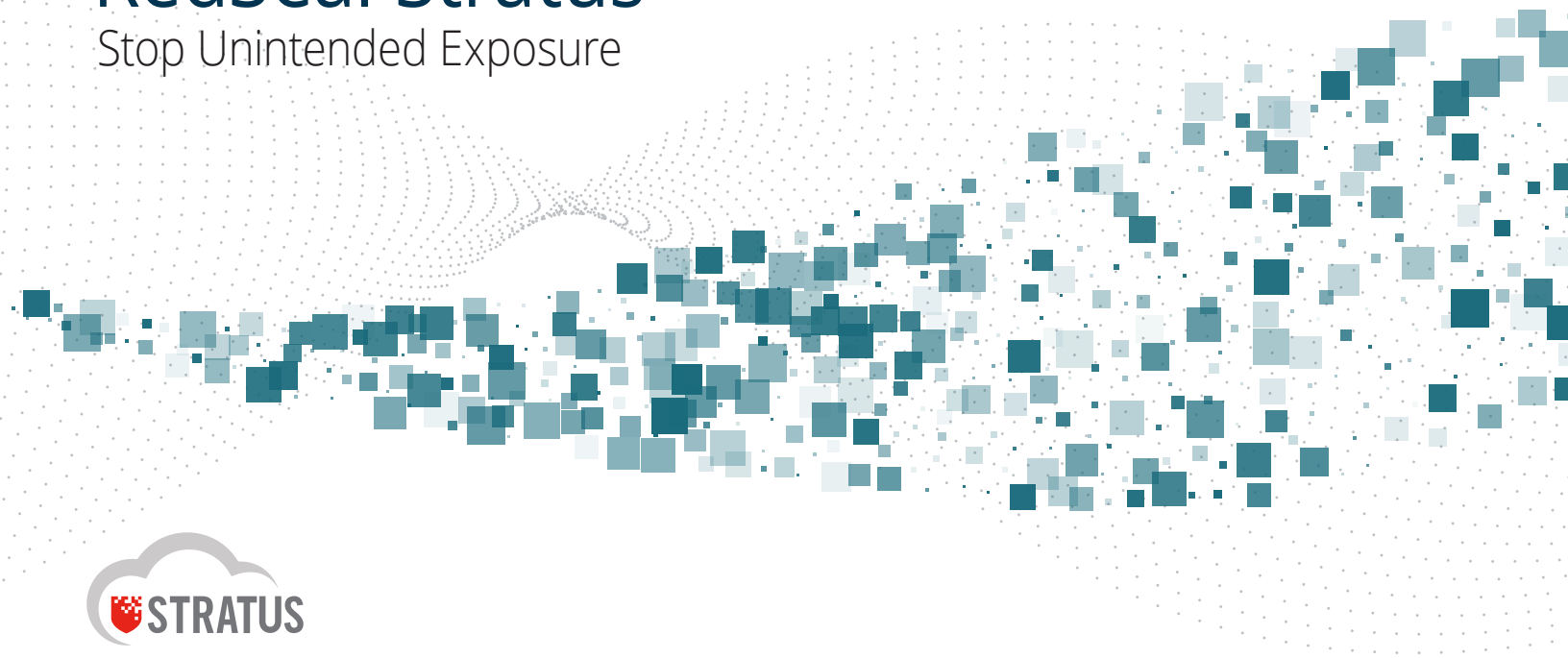
SOLUTION BRIEF | OVERVIEW

RedSeal Stratus

Stop Unintended Exposure



STRATUS

The Complexity of Cloud Computing Increases Security Risks

According to Gartner, through 2030, at least 99% of cloud security failures will be the customer's fault.

Cloud security is complex and distributed. In organizations with on-premise environments, the controls sit with the network security team who are responsible for the firewalls. In the cloud, security controls sit with multiple DevOps teams, Kubernetes policies, third parties and inside AWS and Azure natively. Cloud security controls may not be implemented by security teams but by numerous application developers. The impact is an exponential growth in misconfigurations that are leaving resources unintentionally exposed to the internet.

Cloud security challenges have become so prevalent that Gartner has defined Cloud Security Posture Management (CSPM) as a new category of security products designed to identify misconfiguration issues and risks in the cloud. CSPM solutions are typically used by security organizations that want the equivalent visibility and security that they've had with on-premise environments.

Furthermore, today's cloud-native applications are built on services that are based on containers orchestrated with Kubernetes. For example, Amazon's managed service for running Kubernetes is Elastic Kubernetes Service (EKS), but users can create security controls to protect their EKS clusters.

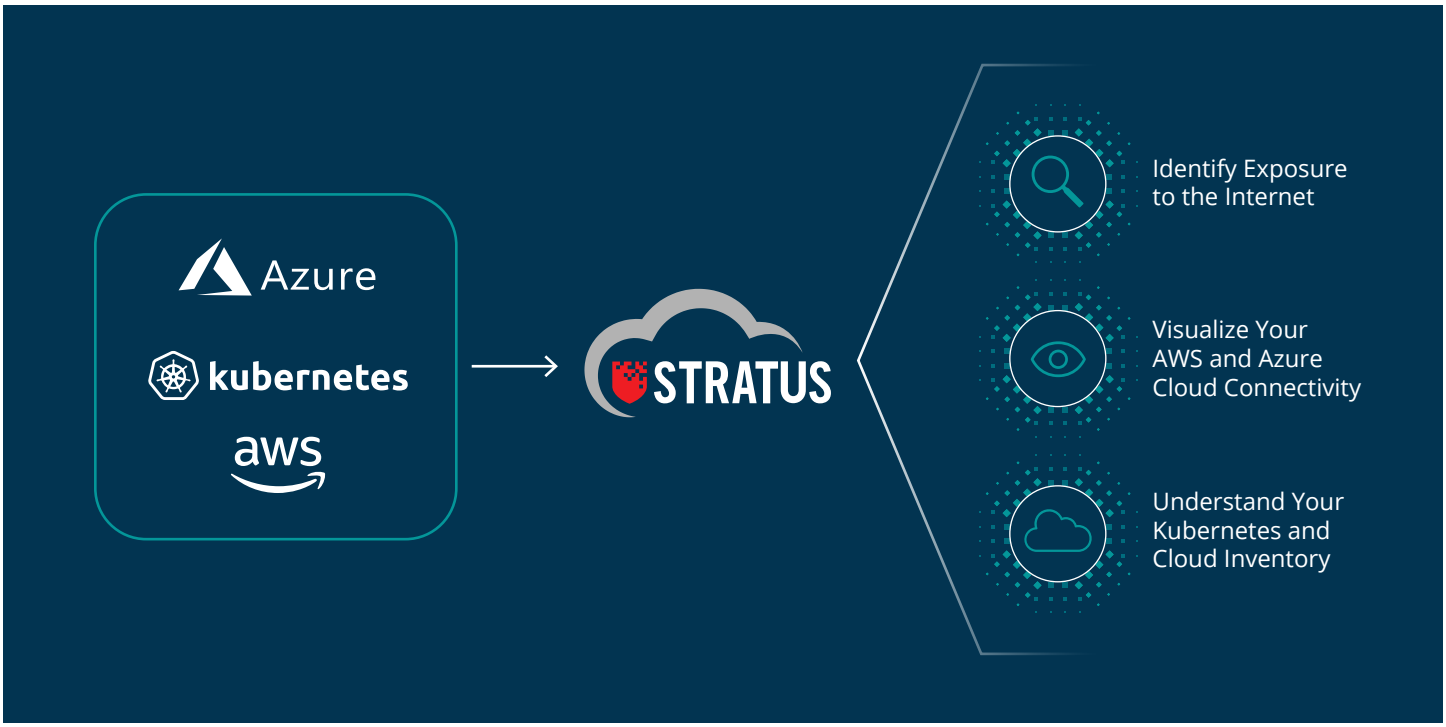
RedSeal's New SaaS-based CSPM Solution

RedSeal Stratus tells you what resources you have in your cloud and if they are exposed to the Internet, and accurately brings all your AWS and Azure network infrastructure into a single comprehensive visualization.

What can help security teams better manage this increased risk?

- Complete and up-to-date visualization of their cloud infrastructure
- Detailed knowledge of Kubernetes resources and policies
- Identify which resources are exposed to the Internet–and how

REDSEAL

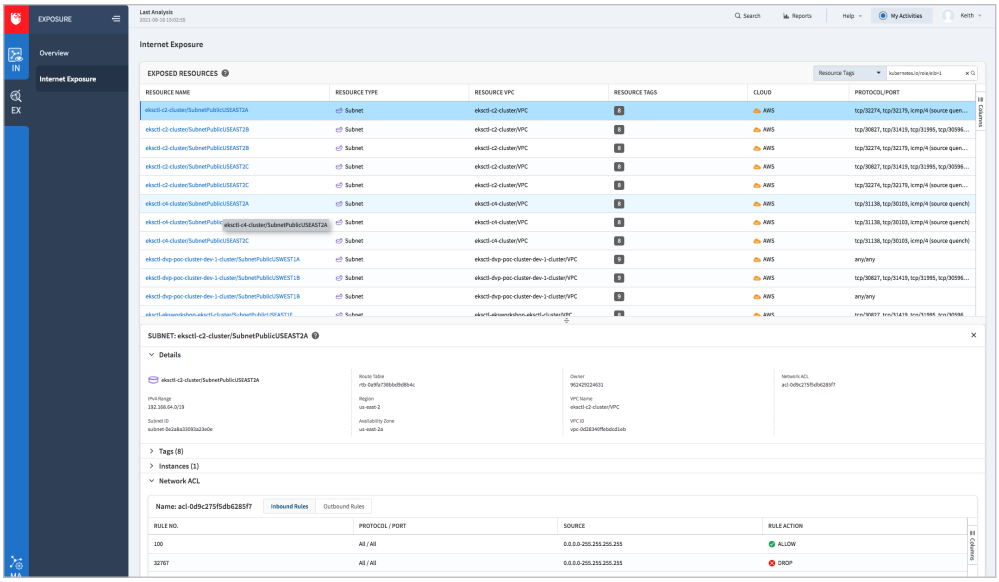


Immediately Identify Exposure to the Internet

Several of the largest data breaches occurred when cloud misconfigurations left critical resources exposed to untrusted networks. RedSeal Stratus provides much greater detail than tools provided by native CSPs, enabling security teams with a built-in report of all resources exposed to the Internet, pre-calculated and grouped by tags.

Tags are fundamental in cloud environments because they enable you to categorize your resources with different labels, such as purpose, owner, or environment. These are important when you have multiple resources of the same type—you can quickly identify specific resources based on the tags that you've assigned.

Stratus Real Exposure



RedSeal Stratus provides:

- Out-of-the-box overview of Internet exposed resources by tags
- Drill down capabilities to identify exact security controls in cloud accounts, VPCs, NACLs, and security groups
- Key information to inform your remediation options, from security groups to specific identification of ports/protocols controlling the access that may be allowing exposure

Visualize Your AWS and Azure Cloud Architecture with Maps and Inventory

After addressing unintended exposure, security teams also need to understand the connectivity between and within cloud resources. Native CSP tools provide basic capabilities to monitor and secure cloud environments, which may be sufficient for smaller, cloud-first companies. However, teams at larger enterprises are being asked to secure huge cloud environments and benefit from a visual, interactive model of their organization's cloud resources.

RedSeal Stratus enables security teams to:

- View a map of all AWS accounts, Azure subscriptions, VPCs, VNets, gateways, and subnets
- Visualize the connections between and within your AWS and Azure resources
- View your AWS and Azure inventory and drill down into details in milliseconds

Other security products may show you connectivity where there is traffic, using an agent-based approach, but only RedSeal Stratus can show you all connectivity possible including those without traffic–using an agentless approach.

Examine Your Kubernetes (EKS, AKS, and GKE) Inventory

According to AWS, a majority of organizations have experienced container security incidents. Securing EKS clusters starts with understanding your inventory, if you have over permissive accounts, and identifying if you have services unintentionally residing outside of your defined clusters.

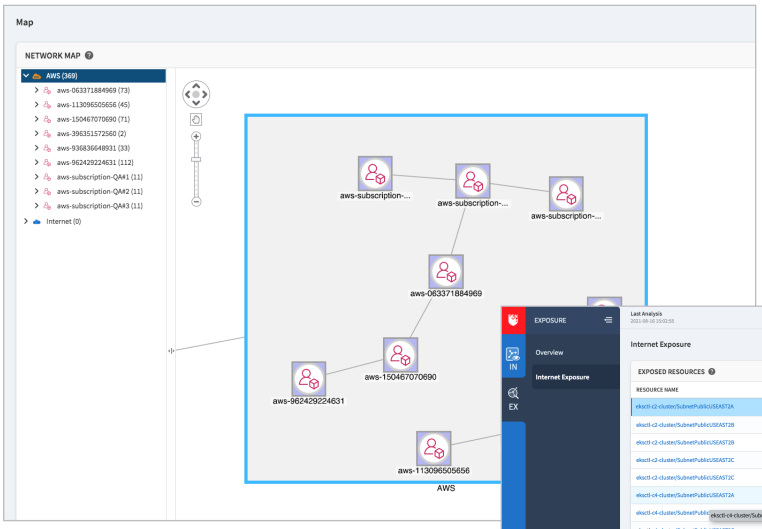
With RedSeal Stratus, you can go beyond the native tools available in your CSP too:

- View and search EKS inventory, and drill down into each resource, including namespace, pods, services, and clusters
- Identify overly permissive user and service accounts
- Quickly identify how services can access a cluster

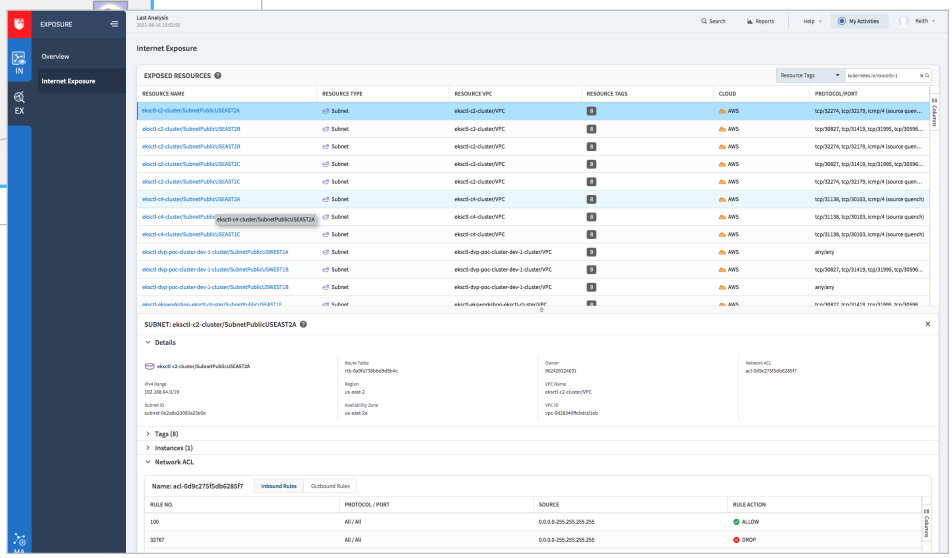
See Through the Cloud Complexity

RedSeal Stratus is a cloud security solution for the modern day that provides security teams with a unified, interactive view of their AWS and Azure environments, EKS, AKS, and GKE inventory, and exposed resources that can lead to costly data breaches.

Maps and Inventory



Kubernetes Inventory



ABOUT REDSEAL (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.

REDSEAL

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net

© 2022 RedSeal. All rights reserved.