REDSEAL

MODEL AND UNDERSTAND
YOUR HYBRID DATA CENTER

SOLUTION OVERVIEW

Microsoft Azure represents a new paradigm in datacenter design, replacing datacenter hardware with purely logical management tasks. Microsoft Azure allows you to provision a (logically isolated) Virtual Network (VNet). As you add more subnets to your VNet, it becomes harder to visualize your architecture and the access it provides. This large scale, multi-tenant resource sharing introduces a lot of entities with complex relationships. As a result, malicious attacks may exist between the platform and between the VNets. As your VNet grows and connects other VNets, virtual networks and legacy on-premise physical networks, it gets even more difficult to understand what is exposed to the internet, where attackers can go, and what access a given host has. A high concentration of resources leads to more security threats and potential for damage than in traditional environment.

UNIFY PHYSICAL, VIRTUAL, AND CLOUD SECURITY

With RedSeal, your physical, private cloud, and Azure VNet become a unified security architecture—capable of being modeled, tested and measured. RedSeal gives you the means to assess the security controls of your Azure VNet-based assets as well as your connected corporate data center. You will be able to analyze both east-west and north-south traffic as well as micro-segmentation.

RedSeal can also drill into the Azure VNet ruleset, providing you with the specific rules that apply to an individual host. You'll easily be able to ensure that only authorized access is allowed.

Microsoft Azure

BENEFITS

Unify security architecture across all your network environments

RedSeal models your Azure VNet along with your physical and private cloud assets. You'll have a single comprehensive model to view and query your entire hybrid data center.

Validate policy compliance instantly

RedSeal integrates with Azure VNet network security groups (NSGs) so you can define access policies and validate any Azure VNet changes against them to ensure secure access.

Verify compliance with industry configuration guidelines

Azure VNet config and RedSeal can determine if network devices comply with configuration guidelines like STIGs and RedSeal's checks against industry best practices.

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

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

REDSEAL AND MICROSOFT AZURE PUBLIC CLOUD

MODEL, TEST, AND MEASURE CLOUD AND HYBRID ARCHITECTURE

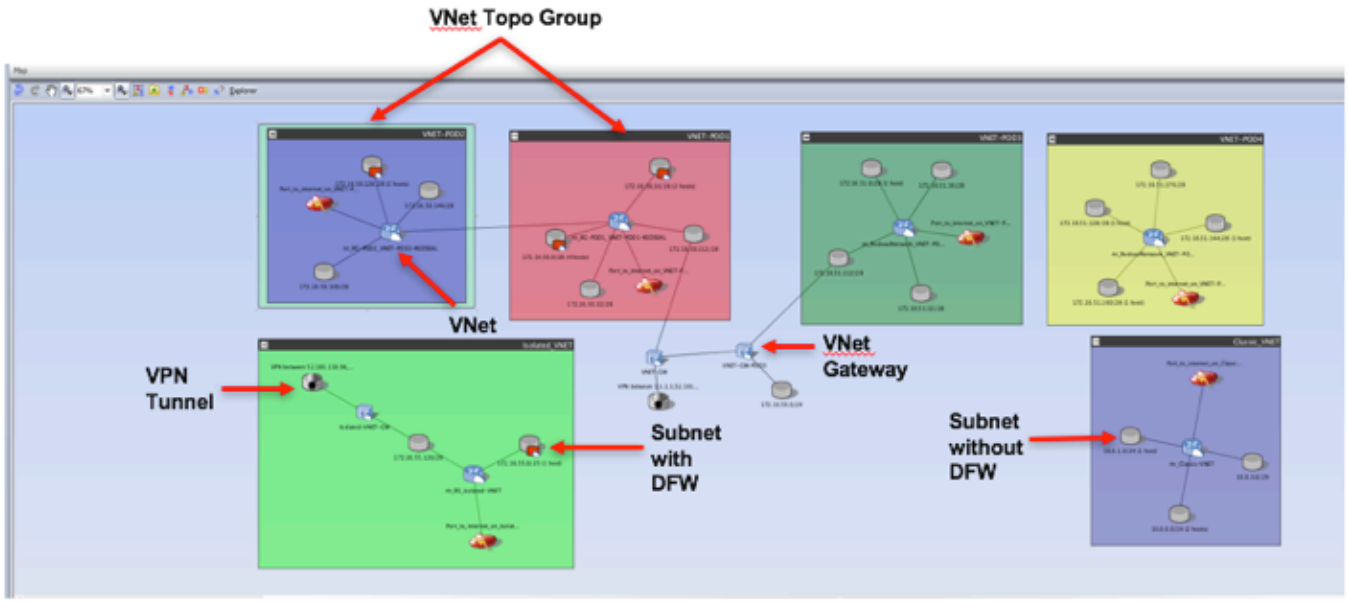
The integration of Microsoft Azure VNet with RedSeal's platform provides your team much needed visibility and context for prioritizing vulnerabilities, accelerating incident investigation, managing compliance, and improving the overall resilience of your infrastructure.

RedSeal models the following Microsoft Azure components to visualize and simplify manageability of your network security framework and traffic flow:

- **VNet routers**
- **Subnets**
- **Workloads (aka hosts)**
- **VNet peering**
- **VPN gateway**
- **Network security group per subnet**
- **Network security group per vNIC**

REDSEAL-AZURE USES

- View all security groups within the VNet and VM.
- See specific firewall rules that apply to Azure VNet instance (VM/host).
- View all Azure instances (hosts/VMs) associated with a particular security group
- Query Azure VNet subnets and view micro-segmentation



REDSEAL MAP OF AZURE VNET TOPOLOGY

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

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

OCTOBER 2018