# HOSPITAL EFFECTIVELY SECURES THEIR CLOUD ENVIRONMENT

## Background

In addition to other disruptions, the pandemic has accelerated the healthcare sector's migration to cloud computing. Increasing numbers of healthcare IT solutions take advantage of the advantages of cloud usage, including improved storage, flexibility, and data scalability. In addition, more and more healthcare providers are providing virtual consultations. These changes have brought cloud and cybersecurity concerns to the forefront while the healthcare regulatory environment has grown even more stringent.

## A Hospital in a Large U.S. Healthcare System

The pandemic forced RedSeal's customer, a 312-bed hospital, like many others, to speed up their digital transformation. This meant migrating to the cloud where possible and delivering remote and virtual services quickly and effectively. Their public cloud of choice was AWS, which they leveraged fast, quickly seeing benefits.

The hospital faced some obstacles: their IT department lacked cloud skills and they had a hard time finding eligible hires with those skills. In addition, their network was flat, lacking segmentation and effective policy implementation.

## The Top-of-Mind Cloud Security Concerns

The hospital was concerned about potentially high-cost security issues:

- **Data leakage/exfiltration** – Protect themselves from unauthorized movement of data outside the hospital, whether accidental or deliberate. When this happens, hospitals frequently only discover the data leak after days, weeks or longer. Damage can include reputation, lost patient trust and fines.
- **Non-compliance** – Not adhering to mandatory regulations or cybersecurity frameworks (such as PCI-DSS, HIPAA and NIST) can result in costly penalties. Patients, referring doctors and staff might perceive that the hospital isn't serious about security.
- **Cloud team collaboration/staffing shortages** – Cloud operations and development are frequently distributed across and organization. This can aggravate an already critical shortage of security people with cloud platform know-how.
- **Ransomware** – Preventing ransomware attacks that would encrypt their data and systems. Avoiding having to pay ransoms to regain access or to protect their stolen data, such as

sensitive HIPAA-protected patient information, from being publicly posted or permanently locked.

## RedSeal Solution

The hospital security team wanted to understand what resources they had in their environments, how those resources are connected and could be accessed or exposed to the internet, and the accompanying risk. They determined their most critical issue was challenge as not knowing which of their resources were unintentionally exposed to the internet and that they needed a cloud security solution. They chose RedSeal.

### AWS VPC Inventory

The team believed they had 2 or 3 AWS VPCs. RedSeal found more than 200 VPCs in the network. Most of the VPCs had subnets without instances running in them. Some VPCs were empty. This revelation was in itself, "*worth the price of admission."*

### Shadow IT

RedSeal helped the team discover a number of previously unknown connections from the hospital's on-premise infrastructure to the AWS cloud, representing a serious potential for exploitation and breach. It turned out that one of the hospital's business units wanted to move quickly and had set up their own AWS environment.


### Routes Through the Firewall

The hospital security team had a policy that all access from their AWS cloud must pass through a Palo Alto Networks firewall. Within a short time, RedSeal helped the team discover that many of the connections weren't --. another potential exploitation or breach waiting to happen.

## Critical Resources Escaping

The security team's own best practices dictated that network security groups and network ACLs would be set up to prevent assets labeled critical from passing through. Unfortunately, RedSeal helped the team discover that critical assets were getting through, and they were able to identify the security policy gaps allowing it. The team re-segmented their cloud network and reset their cloud network security policies – and validated it with RedSeal.

## Vulnerabilities from Cloud Resources

The hospital uses NIST CVSS scores to determine which vulnerabilities are high priority. RedSeal quickly showed them that a CVSS rating by itself wasn't sufficient to determine priority. Access is important. Lower-scoring vulnerabilities that are directly exposed to the internet need to be the highest-priority. They are now assessing each vulnerability in its network context; exposed to the internet or not.

### Business Impact

- Provided accurate inventory and connectivity data to demonstrate potential access and exposure.
- Gained visibility of all VPCs.
- Identified shadow IT activity and reined it in.
- Discovered connections not being routed through firewalls and remediated.
- Discovered assets labeled critical 'escaping' due to policy flaws and corrected them
- Determined vulnerability priority based on both CVVSS and exposure to the internet.

*RedSeal's cloud security solution accurately locates resources unintentionally exposed to the internet and brings all your network environments-- public clouds, private clouds and on premise -- into one comprehensive, dynamic visualization. RedSeal's experienced cloud security advisors are available to assess your environment and show you how you can improve your cloud security.*

*Please email:* ***info@redseal.net*** *or call* ***+1-(408) 641-2200****.*