CUSTOMER STORY

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

Like many others, the pandemic forced RedSeal's customer, a 312-bed hospital to accelerate 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 Cloud Security Concerns

- **Data leakage/exfiltration**
  They needed to protect themselves from unauthorized movement of data outside the hospital, whether accidental or deliberate. Often when this happens hospitals only discover the data leak after days, weeks or longer. The resulting damage can include weakened reputation, lost patient trust and fines.
- **Non-compliance**
  It was crititcal to adhere to mandatory regulations or cybersecurity frameworks (such as PCI-DSS, HIPAA and NIST) or else face costly penalties. In addition, patients, referring doctors and staff can view non-compliance as a lax attitude toward security.
- **Cloud team collaboration/staffing shortages**
  Maintaining security requires the right staff. 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**
  Healthcare data breaches are on the rise. Preventing ransomware attacks that would encrypt their data and systems was a neccessity. Paying ransoms to regain access or avoid public release or to protect their stolen data - including sensitive HIPAA-protected patient information - had to avoided at all costs.

REDSEAL

RedSeal Solution

The hospital security team wanted to understand what resources they had in their environments, how those resources are connected, what could be accessed or exposed to the internet, and the accompanying risk. They determined their most critical issue was knowing which of their resources were unintentionally exposed to the internet. They knew they needed the right cloud security solution to help. 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. As often happens, in the race to the cloud one of the hospital's business units had set up their own AWS environment without informing anyone.

Routes Through the Firewall

The hospital security team had set 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 unfortunately, many of the connections weren't doing so. Ensuring visibility into all connections is critical.

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 in fact getting through. After identifying 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 demonstrated that a CVSS rating alone 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

- Established accurate inventory and connectivity data exposing potential unintended access and exposure
- Gained visibility of all VPCs
- Identified shadow IT activity and eliminated the risk
- Remediated risk of connections not being routed through firewalls
- Stopped critical assets from "escaping" due to policy flaws
- Properly prioritized vulnerability based on both CVVSS and exposure to the internet

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