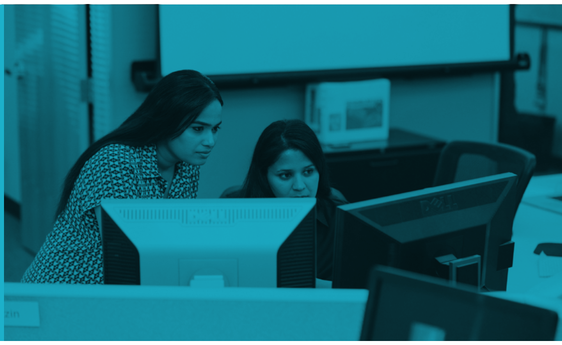
REDSEAL AT WORK: HEALTHCARE

REDSEAL

A LARGE U.S. RESEARCH HOSPITAL



SITUATION

At a large research hospital, the security team members didn't have enough information to do their jobs. The security team was small, and they lacked visibility into their network. They knew a new hospital would come online but they didn't know when. They'd heard that some groups were working with AWS instances, but they didn't know where or how many. They just didn't know what they didn't know. So, they asked RedSeal to show them what's on their network, how it's connected and the associated risk.

- Small security staff that didn't know.
  - What's on the network.
  - When new sites or cloud subnets go live.
  - How everything connects.
  - What's connected to compromised hosts.

REDSEAL SOLUTION

RedSeal Professional Services began by pulling in data from the SolarWinds NCM. Then, they had RedSeal calculate all paths across the network and determine what was on the hospital's network. They found AWS VPCs and, to everyone's surprise, Google Cloud VPCs. Further, they discovered network devices missing from SolarWinds which they used to make SolarWinds more accurate.

Next, they organized the network by site, so the security team could see all traffic paths between facilities. They were able to find and include the new facility and will be able to minimize exposure when the hospital acquires another group. With RedSeal's cloud visibility capabilities, the security team can also visualize their cloud-based environments and see the interactions with their physical assets – all without tracking down other people for information.

When the hospital's vulnerability management team asked for help prioritizing vulnerabilities identified by Rapid7, RedSeal professional services imported Rapid7 data. First, RedSeal identified some unscanned subnets. Then, RedSeal added network context to Rapid7's prioritization, showing the team which vulnerabilities represented the most risk to their network. This is based on how accessible the vulnerability is to untrusted networks and where an attacker can go once they compromise that machine.

- RedSeal professional services installed the RedSeal platform, bringing in information from SolarWinds NCM, AWS, Google Cloud Platform and Rapid7.
- Set up to continuously discover network changes.
- The security team implemented RedSeal managed services to augment their staff and continue to improve their security posture.

RESULTS

Now, the security team has a network inventory that is updated daily, including what’s in the AWS and Google clouds. They can see connectivity between facilities and identify any new facilities or subnets. RedSeal continues to add inventory information back into SolarWinds. RedSeal’s understanding of how things are connected adds to the picture SolarWinds provides and allows RedSeal to prioritize Rapid7's vulnerability data based on access paths in their network.

RedSeal helped when a sister facility was compromised. The security team needed to know if the threat could reach into their network. Within minutes, RedSeal was able to reassure them that no access paths existed.

The security team implemented RedSeal managed services to augment their staff and continue to improve their security posture.

- **Security team sees what’s on their network.**
- **Has a topology map organized by facility.**
- **Sees connectivity between facilities.**
- **RedSeal updates SolarWinds NCM.**
- **New facilities are immediately visible.**
- **RedSeal verifies Rapid7 scans as intended.**
- **Mitigation prioritized on network risk.**
- **Team knows within minutes if network is accessible from a compromise.**