REDSEAL

REGIONAL U.S. HEALTHCARE PROVIDER

SITUATION

To avoid increased fees from credit card companies, the security team needed to pass their PCI audit—quickly. Unfortunately, the team is short staffed and so busy they haven't been able to create standard operating procedures. The security team had other concerns, too. They needed to ensure that their unpatchable medical devices remained protected and behind firewalls. And, they wanted to be more proactive about security rather than just react to alerts.

- Small team with no standard procedures.
- Needed to:
  - Pass PCI audit.
  - Be more proactive about security.
  - Ensure unpatchable medical devices are behind firewalls.
  - Improve patching prioritization.

REDSEAL SOLUTION

RedSeal professional services created a customized policy for PCI segmentation on this network. They discovered a lot of access the security team didn't know they had. In fact, some so surprising, they believed it to be "impossible." Next, RedSeal allowed the team to visualize their network by site. They could see what was on their network and how it was connected. Then, RedSeal professional services imported vulnerability scan results—from both Qualys and CrowdStrike. Combining this with RedSeal's knowledge of the network showed the security team which vulnerabilities represented the most risk to their network. They could prioritize patching based on both criticality and risk.

- A customized PCI segmentation policy.
- Topology map allowing network visualization by site.
- Network information lets team prioritize patching on criticality and risk.

RESULTS

RedSeal worked closely with the security team until they passed their PCI audit. RedSeal's ongoing understanding of their network allows the team to see their network by site—and to be aware of any changes. They can actively see and manage their network's segmentation and make sure those medical devices remain protected and the policy is enforced. The security team's patching program continues to be informed by RedSeal's network knowledge, increasing their confidence that they're mitigating the most important things first. RedSeal is showing them if the asset could be directly accessed from an untrusted network—as well as where an attacker could reach, if that asset were compromised. RedSeal professional services will continue to support the team by providing managed services in more areas.

- RedSeal found a lot of access security team didn't know they had, but professional services worked with them to pass the PCI audit.
- Network context continues to help prioritize patching
- RedSeal network knowledge allows security team to group and visualize devices and endpoints by site.
- RedSeal will provide managed services in more areas.