REDSEAL

CASE STUDY

Streamlining NERC CIP Compliance and Cybersecurity with RedSeal

CHALLENGE

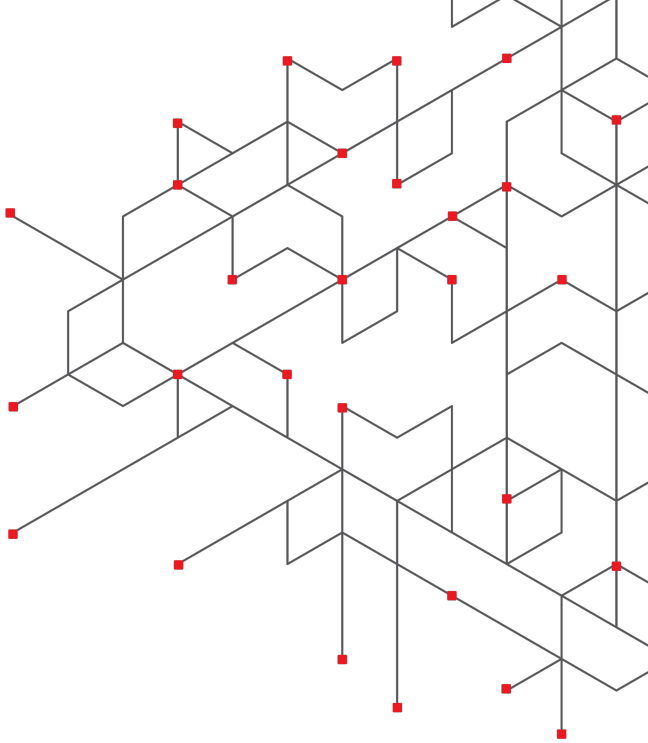
NERC CIP mandates a comprehensive set of security requirements to protect critical cyber assets essential to North America's bulk electric system. The company faced significant challenges in managing these requirements, including ensuring the security of electronic perimeters, managing firewall rules, and performing labor-intensive tasks such as logical segmentation and firewall rule analysis.

To effectively meet these standards, the company needed a solution to visualize its network as a whole, automate routine processes, and ensure that security was embedded in daily operations.

SOLUTION

The company implemented RedSeal as part of its NERC CIP version 5 program. The platform quickly became an integral part of its daily security and compliance operations, starting with firewall rule evaluation and logical segmentation.

Over time, the company expanded its use of RedSeal to streamline a range of cybersecurity and compliance processes.



"Using RedSeal reduced the time it takes us to evaluate our systems for specific vulnerabilities from one person/month to 15 minutes. We can spend our time on mitigation, rather than assessment."

-Director, NERC CIP Operations, Cybersecurity

Key uses included:

- **Firewall rule business justification:** Simplified evaluation and documentation of firewall rules, ensuring compliance with NERC CIP's business justification requirement.
- **Logical segmentation:** Increased security by isolating critical control systems, reducing the risk of cyber-attacks spreading across the network. This also lowered the company's compliance obligations by reducing risk ratings.
- **Firewall rule change monitoring:** Automated monitoring of firewall rule changes, alerting teams to any exceptions to pre-approved logical segmentation policies.
- **Vulnerability evaluation:** RedSeal's network modeling assessed vulnerabilities based on actual risk, allowing the company to prioritize mitigation efforts and reduce time spent on assessments.

RESULTS

RedSeal's ability to model and assess risks in real-time has empowered the company to maintain audit readiness while efficiently mitigating critical vulnerabilities. By implementing RedSeal, the company significantly improved:

- **Vulnerability assessment:** Using RedSeal, the company reduced the time to evaluate vulnerabilities from one person/month to just 15 minutes, enabling the team to focus on mitigation rather than assessment.
- **Audit readiness:** RedSeal's automation and reporting capabilities greatly reduced the time and effort required to prepare for NERC CIP audits, ensuring compliance at any time.
- **Cybersecurity response times:** The company used RedSeal to quickly assess vulnerabilities during the 2017 WannaCry ransomware attack, reducing assessment time from a month to 15 minutes. The integration with Tenable further allowed teams to prioritize vulnerabilities based on their exposure and severity.
- **Ongoing automation:** As the company matured its processes, RedSeal enabled ongoing automation of manual processes, improving efficiency and reducing the risk of human error.

Contact RedSeal to learn more or request a demo today.