REDSEAL

CASE STUDY

Leading energy provider closes critical security gaps faster with true clarity on exposures and risks

Overview

As one of the largest energy producers in the United States, this Fortune 500 power generation company provides essential electrical services to businesses and consumers coast-to-coast. The company maintains a diverse fleet of electric generation and energy storage facilities. Cybersecurity attacks and technology systems failures pose significant risks to this critical infrastructure—and the lives and livelihoods that depend on it.

Cybersecurity leaders for the generation fleet are keenly aware of their responsibility to, as they say, “protect our way of life.” They rely on RedSeal to stay informed, proactive, and prepared. With a complex IT/OT environment to defend, the team puts as much—if not more—focus on anticipating threats and uncovering security gaps as they do on understanding the assets, configurations, and controls currently in place. The RedSeal platform empowers the entire organization with a holistic, big-picture view of their ecosystem, as well as the ability to zero-in quickly on the real risks to the business.

Removing the blinders, seeing the whole picture

With the company for over 30 years, the senior director of cybersecurity considers RedSeal a force multiplier for their entire cyber program. He and his diligent team of security managers, analysts, and engineers engaged with RedSeal to gain a level of network visibility and understanding they could not achieve with other tools.

“Our previous product was very limited in the analysis that it could do,” the senior director explained. Our previous product did not provide the broad visibility across the entirety of the companies environment. RedSeal looks at all pathways and helps us evaluate both North-South risk but also very importantly East-West risk as well.

The RedSeal platform integrates with IT/OT infrastructure across the company’s nationwide fleet of power plants, each with different systems and vintages of equipment from the past three decades. It also hooks into other security solutions from vendors such as Palo Alto Networks, Tenable, and Zscaler. RedSeal ingests data about every asset, configuration, vulnerability, firewall rule, interface, and more to model the entire environment. Then, it analyzes all access paths—both direct and indirect—to assess exposures and prioritize risks.

“Compared to the speed and usability of the previous tool, RedSeal is light years better,” added a senior analyst on the team. “Within two months of bringing in RedSeal, we had complete network maps of all our sites for compliance, covering more than 1,300 assets. That is the fastest and easiest we’ve ever done it, and it just keeps getting easier.”

“Within two months of bringing in RedSeal, we had complete network maps of all our sites for compliance, covering more than 1,300 assets. That is the fastest and easiest we’ve ever done it, and it just keeps getting easier.”

Above and beyond compliance

As an energy provider, the company is required to comply with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards, among others. On an annual basis, the security team submits drawings that document assets and controls in place, including firewalls for electronic access control. RedSeal helps us meet our compliance obligations with greatly reduced effort. More importantly, it helps us ensure that our segregation strategy has not drifted from our intended outcome. We can validate that all connections are understood and that they are authorized.

Cyber security posture drift is a real risk and it's critical that we know our networks are secured as we intended them to be. From a security perspective, the National Institute of Standards and Technology’s Cybersecurity Framework (NIST CSF) has been a guiding force for cybersecurity efforts.

But the senior director notes that, as with many frameworks, they deliver outcomes and not the specific ways to achieve. We have to identify what we will do to achieve these objectives from his point of view, knowing what good looks like and the using tools like RedSeal to verify is a key component of their cyber security program. "A focus on compliance can lead to missing the target of security", the senior director commented. "We want to be compliant and secure. RedSeal helps us to achieve this goal."

"Except for where we don't"

RedSeal's ability to analyze the entire environment proactively against best practices and policies is instrumental in helping the team catch any unintended exposures before they become problems. The platform identified numerous issues in the first year alone, including misconfigured devices, routing enabled for decommissioned devices, unknown subnets, unmapped network segments, and more than 50 firewall rules that were no longer needed or effective.

The senior director emphasizes the importance of the work they do and credits the passion and expertise of his team—in partnership with RedSeal's Professional Services staff—for the success they have achieved to date with the RedSeal platform. But he also acknowledges the imperfect and ongoing nature of the work in an environment where technologies and threats are constantly changing.

"I say all the time that we do good work, except for where we don't," he said. "We're blocking access to the internet… except for where we don't. We have intermediary devices… except for where we don't. RedSeal highlights those exceptions—that drift that happens over time. It makes us question our assumptions, rather than just feeling good about everything because we think we're good. That is a key part of the value that RedSeal provides."

Risk storytelling

The cybersecurity team treats each power plant as if it were its own business, providing centralized services with strict rules about access between plants and to and from the corporate network. Meanwhile, the people operating the plants tend to be very self-sufficient, continually looking for ways to make the plant run more efficiently or reliably. This includes installing new systems or physically plugging in cables, oftentimes without involving the cybersecurity team. With RedSeal, the cybersecurity team can detect, visualize, and explain how an action taken at a plant impacts security or creates additional, downstream risks that the business may or may not deem acceptable.

"Our role is to help the business understand our security posture, and RedSeal provides the building blocks for those stories we need to tell," the senior director noted. "We are a storytelling organization. If we identify a risk, we need to tell a story about it, not just throw out data or facts. RedSeal provides critical context that the business needs in order to make the ultimate decision about whether we live with the risk or not."

The senior cybersecurity manager appreciates RedSeal's ability to assess and prioritize risks based on actual exposure—not just highlighting what vulnerabilities exist with what severity scores, but showing where they are exposed and how they could be exploited. This is especially critical in a real-time production environment where taking systems offline for patching is not always possible. RedSeal ensures the team is focused on addressing real risks and not wasting time on vulnerabilities that pose no real threat.

"RedSeal gives us the ability to triage those CVEs in a way that helps us get to the real problems quicker," the manager said. "We've never really, truly, been able to do that before. With RedSeal, we validate everything. We know that an asset has these vulnerabilities and this amount of exposure. That level of detail is crucial for effective storytelling."

"RedSeal provides critical context that the business needs in order to make the ultimate decision about whether we live with the risk or not."

While initial efforts focused primarily on plants' perimeter controls and preventing exposures from external sources, the company now looks to RedSeal for insights into exposures from internal sources and within the corporate network as well.

A successful partnership

The RedSeal Professional Services team has been working closely with the generation cybersecurity team from day one in a managed services capacity. While initial efforts focused primarily on plants' perimeter controls and preventing exposures from external sources, the company now looks to RedSeal for insights into exposures from internal sources and within the corporate network as well.

"We always think in terms of what's now, next, or never," said the senior director. "RedSeal has already helped us identify and tackle our 'now's —the biggest risks to our power generation facilities. As for other risks we identify, only the business can decide what's next or never. There may be some risks that the plants or the company are willing to accept and actively manage."

"That's why this partnership is so successful," he continued. "RedSeal brings their expertise in their platform and how to maximize its value, and we bring our expertise on the environment and our business, and together we solve problems faster. We are defining what good looks like and constantly evaluating whether we are there."

Everyone on the cybersecurity team values the partnership, citing RedSeal's collaborative approach, responsiveness to product requests, and willingness to address the company's unique challenges and edge use cases. There is always work to be done, but RedSeal has proven invaluable in improving visibility, proactively remediating and mitigating risks, and streamlining compliance in this complex, critical infrastructure environment.

Learn more

RedSeal, a leader in cybersecurity and proactive exposure management, delivers proactive, actionable insights to close defensive gaps across hybrid environments. RedSeal continually discovers all resources, connectivity, and exposures, creating a single, comprehensive model—a network digital twin.

Contact RedSeal to learn more or request a demo today.