FUELING SECURITY: HOW A FORTUNE 500 UTILITY STAYS AHEAD OF EMERGING THREATS

CUSTOMER SNAPSHOT

INDUSTRY	Energy and Utilities
CUSTOMER	Fortune 500 organization managing critical infrastructure spanning the power grid, natural gas distribution, and energy generation.
SERVICES PROVIDED	Attack Surface Management

> "Bishop Fox's constant effort to maintain testing for both old and newly identified exploits stands out. Every day new vulnerabilities and threats come out, so having a development team dedicated to creating that testing is invaluable."
>
> — **SR. SECURITY MANAGER**

THE CHALLENGE:

With subsidiaries spread across multiple U.S. states and a wide range of technologies in use, the energy provider lacked full visibility into its external attack surface. The offensive security team needed a continuous, validated view of its external perimeter to meet NERC CIP and TSA requirements and proactively defend against real-world threats.

Meeting these obligations while continuing to protect customers and maintain reliable service required more than manual processes or reactive scans. They needed continuous, validated insight into their perimeter.

SECURITY CHALLENGES

- Maintain a current, accurate inventory of public-facing assets
- Identify vulnerabilities that internal tools may miss
- Support compliance with federal cybersecurity mandates
- Act quickly on exposures with confidence
- Report clearly on program maturity to leadership

> "We really needed to build a solid asset inventory and be able to identify vulnerabilities and exploits through the techniques that attackers use."
>
> — **SR. SECURITY MANAGER**

THE SOLUTION

The energy company selected Bishop Fox's fully managed service for Attack Surface Management as its first dedicated investment for tracking externally facing systems and vulnerabilities. What began as a technical implementation quickly evolved into a trusted partnership with the Bishop Fox team becoming advisors in the energy provider's growing security program over the last five years.

The company considers the service a cornerstone of its proactive security strategy. Unlike a tool, the service is delivered by tech-enabled security experts who validate asset ownership, as well as verify the exploitability and business impact of all exposures. As a result, the team can act confidently on real findings and avoid alert fatigue.

GOALS OF THE ENGAGEMENT

- Focus on validated, actionable findings
- Discover shadow assets and unknown exposures
- Prioritize efforts based on confirmed business impact
- Receive expert support through ad hoc analysis and quarterly reviews

"No news is good news, but it's easy to forget that. The service reviews help shine a light on everything happening in the background. All the work that's usually invisible."

— **SR. SECURITY MANAGER**

THE OUTCOME

The Bishop Fox managed service has delivered high-impact results across both daily operations and critical response scenarios. It gives the security team a real-time view of its external perimeter, enabling them to maintain a trustworthy asset inventory and respond quickly to new threats.

That value became especially evident when Bishop Fox detected and immediately flagged a critical vulnerability in one of the company's operational monitoring systems. It was an exposure that, if left unaddressed, could have posed serious risk to infrastructure reliability.

KEY RESULTS

- 3-hour response from detection to remediation for a critical vulnerability
- Accurate, up-to-date external visibility across multiple states and subsidiaries
- Continuous monitoring of vulnerabilities and emerging threats with human validation to eliminate noise
- Support for NERC CIP and TSA compliance
- Quarterly reporting for leadership alignment and transparency

"We got the alert, pulled the report, spun up a tiger team, and brought in Bishop Fox within the hour. Within three hours, we'd identified the issue and put a solution in motion."

— **SR. SECURITY MANAGER**