CASE STUDY | WATER TREATMENT

One annual assessment was never going to be enough.

How a Southeastern U.S. water treatment facility built a repeatable program to find, prioritize, and fix security risk.



IMPACT AT A GLANCE

- Security policy framework formalized across 13 areas
- Vulnerabilities ranked by risk and business impact
- Controls validated through hands-on penetration testing

VERTICAL

Water treatment and distribution, critical infrastructure

ENVIRONMENT

Corporate IT, operational technology (OT), remote access, and third-party systems

SECURITY GAPS EXPOSED

- Security policies and procedures not yet formalized
- Limited visibility into vulnerabilities across IT and OT
- No real-world test of whether controls would hold
- Thin internal security staffing

REDZONE CONTINUUM FOCUS

Continuous Intelligence
Continuous Posture

The Challenge

The facility ran essential treatment and distribution operations on a mix of corporate IT, OT, remote access, and third-party technology. Controls were in place, but policies were informal, visibility into vulnerabilities was limited, and no one had tested whether an attacker could actually get through. Leadership wanted more than a report. They wanted a team that would help them understand the risk and fix it.

The Approach

Passpoint Security, now part of RedZone, ran the work as one program instead of four separate projects. The team strengthened policies across 13 areas, from access control to incident response. Vulnerability scanning covered systems, applications, network devices, and configurations, with every finding ranked by risk. Penetration testers then worked from an attacker's perspective to see whether weaknesses could be chained together to escalate privileges or move laterally, using AI-assisted analysis with human oversight and validation throughout.

Why This Matters for Utilities

Utilities face rising ransomware and cyberattack activity, often on aging technology with thin security staffing. A once-a-year assessment can't keep up when threats, systems, and people change constantly. What protects a water system is the ability to keep finding, prioritizing, and fixing risk. That's the capability this facility built.

Results

13
Policy areas strengthened

Ranked
Findings prioritized by risk

Ongoing
Security Model, Not Annual

- Clear view of vulnerabilities and potential attack paths across the environment
- Repeatable process for identifying, prioritizing, and remediating vulnerabilities
- Leadership briefed on cyber risk and the specific steps needed to reduce it

THE REDZONE CONTINUUM ANSWER

Continuous Intelligence + Continuous Posture

Continuous Intelligence keeps testing security controls the way an attacker would. Continuous Posture keeps vulnerabilities found, ranked, and fixed between tests instead of piling up until the next annual assessment.

RedZone brings Managed IT, Cybersecurity, Cloud, Compliance, and Technology Strategy together under one accountable partner for utilities and public sector organizations where uptime, public safety, and community trust are the mission. Confidence in the technology your business depends on.

BOOK A MEETING