Indiana sanitary district slashes monthly IT spend by 35% while gaining nonstop cybersecurity SOC monitoring and 24/7 NOC services.

The Situation

Facing spiraling subscription invoices, limited daytime support and an aging control network, a fifty-person sanitary district in Indiana saw its managed service contract eating capital it needed for a looming plant-wide SCADA modernization. Adding pressure, rival local providers were courting the district while internal leadership explored do-it-yourself tooling, so any replacement partner had to prove immediate hard savings, deeper security coverage and zero head-count growth from day one.

Customer

Regional Sanitary District, Indiana, five sites, fifty employees, seventy endpoints

Problem

Wrote monthly checks exceeding nine thousand dollars for licensing, monitoring and help-desk work that rarely arrived, all while operating without 24-hour SOC eyes on critical plant systems infrastructure

Solution

Marathon trimmed unused seats, took over the existing BCDR solution, deployed Huntress EDR through Datto RMM and layered continuous NOC oversight

Results

Monthly outlay fell to under six thousand dollars, patch windows dropped below ten minutes, security alerts flow around the clock and reclaimed bandwidth lets staff focus on the district's SCADA migration roadmap

"Now every invoice matches a service we need & the numbers finally add up."

Cost & License Optimization

Marathon performed a forensic review of every invoice, license receipt and renewal notice on the district's books. The team discovered overlapping security subscriptions, duplicate Microsoft plans, a block of help-desk hours that had been untouched for months and EDR agents outnumbered actual workstations by nearly forty percent.

First, we rebuilt the licensing profile from the ground up. These changes alone shaved $600 off the monthly Microsoft line.

Next in line came security optimization. The district traded SentinelOne licenses for Huntress Managed EDR and ITDR, bundling 24-hour SOC response for both endpoints and Microsoft 365 Identity activity. At under eight dollars per endpoint, the Huntress bundle enhanced protection while freeing $900 each month. Add-in removal of unused help-desk blocks and the cost-of-ownership curve bent downward by an additional $1700.

"Seeing the side-by-side spreadsheet was a wake-up call. We were paying premium prices for empty seats & nobody challenged the math until Marathon walked through every line item, showing where money was hiding. "

---

24 × 7 Security & NOC Coverage

Once budget leaks were sealed, the focus turned to uptime, replacing reactive troubleshooting with automated, around-the-clock monitoring and patching. Leveraging Huntress' EDR and best-of-breed Kaseya toolsets, Marathon provided fully managed NOC & SOC services, backed by 24/7 Operations Center and expert security analysts, effectively providing the benefits of an in-house service without the overhead.

“The EDR & NOC consoles tell me exactly what happened, when it happened & what was already done about it. If a server reboots outside the patch window, I receive a text before anyone calls. The Meraki switches report temperature & fan health in real time while Marathon’s NOC team resolves most alerts before I even open the ticket queue. It feels like adding staff without adding salaries for a department that runs lean by necessity these days anyway.”

Results / Benefits

35 percent Lower Monthly IT Spend

Reducing 35% from monthly budget was not an exercise in slashing features, it was about eliminating waste. The district still enjoys Microsoft 365, enterprise backup, endpoint detection and proactive monitoring, yet pays greater than $3,000 less every month, freeing public funds for infrastructure the community can see and trust.

Time Back for Core Projects

NOC automation collapsed patch windows from hours to minutes, a shift that liberated evenings and weekends for the plant’s tiny IT crew. Help-desk escalations dropped by 38% because issues are resolved before users notice them. Instead of juggling tickets, the team now spends its time mapping new SCADA sensors, testing failover procedures and working with engineering on predictive maintenance dashboards that promise even more operational resilience for the utility.

Future-Proof Security Posture

With licensed headroom, a live SOC and reliable backups already in place, the district is positioned to bolt on future capabilities without renegotiating its contract. Marathon’s modular model means threat intelligence, compliance reporting or additional plant sites can be added as projects demand, turning a once bloated agreement into an agile platform that grows only when value is clear for taxpayers and staff.

FORMAL REFERENCE AVAILABLE UPON REQUEST