THE MANAGED ADVANTAGE

A Proactive Approach to Operational Support

How a managed services provider can extend your team's capabilities efficiently and effectively.

inflexion point

HOW WE EVOLVED TO MEET THE NEEDS OF OUR CLIENTS

We didn't set out to offer "managed services." We just answered a client's call for help.

One of our earliest customers, a multi-site operator, needed coverage they couldn't staff for — nights, weekends, critical issues — and we stepped in to help. Over time, that relationship grew into something more structured: remote monitoring, dashboards, patching, and 24/7 support.

That's how our managed services began — not as a product, but as a solution to real-world needs. And we've seen the same demand emerge across life sciences, food and beverage, and critical infrastructure.

This isn't about replacing your team. It's about reinforcing it — with the visibility, redundancy, and expertise needed to stay ahead. As systems evolve and uptime expectations grow, support must be proactive, strategic, and scalable.

This guide unpacks managed services — when it works, why it matters, and how to tell if it's time to stop going it alone.

MIKE CIGNARELLA
VP of Managed Services,
InflexionPoint

inflexion point

Six Signs Your Current Operations Model Is Holding You Back

Not everything in operations fails with a bang. Sometimes, your support model just kind of… wears out. Quietly. Slowly. Until one day it's obvious you've been duct-taping your way through issues that needed real solutions.

Six signs your current operations model is holding you back:

1. You're Always Playing Catch-Up

If your support strategy is basically "wait until it breaks," you're not alone—but you're also not really supported. Constant firefighting means your team's energy is spent reacting, not improving.

2. Updates Keep Getting Delayed

Whether it's patching, upgrades, or vulnerability scans, the "we'll do it next quarter" mindset is a huge risk. Especially when those delays stack up across multiple facilities.

3. Your Team's Tapped Out

Smart people can only carry so much. When they're covering too many systems, working after-hours, or Googling their way through unfamiliar platforms, it's not sustainable—and burnout is just around the corner.

4. Every Site Feels Like a Different Planet

Different hardware. Different support contacts. Different documentation (if it even exists). If your sites don't run the same playbook, you're probably dealing with inconsistency, duplication, and missed opportunities.

5. The System's Running... But It's Not Performing

Laggy dashboards, missing alarms, and "we've always done it this way" problems don't trigger alarms—but they eat away at productivity and visibility all the same.

6. Workarounds Are the Norm

If operators are regularly bypassing standard procedures just to get through the day, that's not resourceful—it's risky. It usually points to weak support, unclear ownership, or outdated systems.

Practical Tip:
Audit the last six months of support tickets

- How many were preventable with proactive monitoring or patching?
- How long did it take to resolve each one?
- Who handled it - and what would have happened if they weren't available?

What 250 Support Tickets a Month *Really* Looks Like

If you've never had to manage hundreds of support tickets a month, it probably sounds like chaos. And if you have had to manage that load? You already know: it's not just about volume — it's about how fast things get sorted, how many repeat issues you see, and whether you're putting out fires or actually solving problems.

When we first started supporting multiple remote sites for one of our earliest managed services customers, it didn't take long before we were fielding 250+ tickets every month. These weren't all big, dramatic failures. Most were small but important — things like patching schedules, backup alerts, configuration tweaks, CVE monitoring, or someone needing to escalate a PLC issue in the middle of the night.

But they all mattered. And they added up fast.

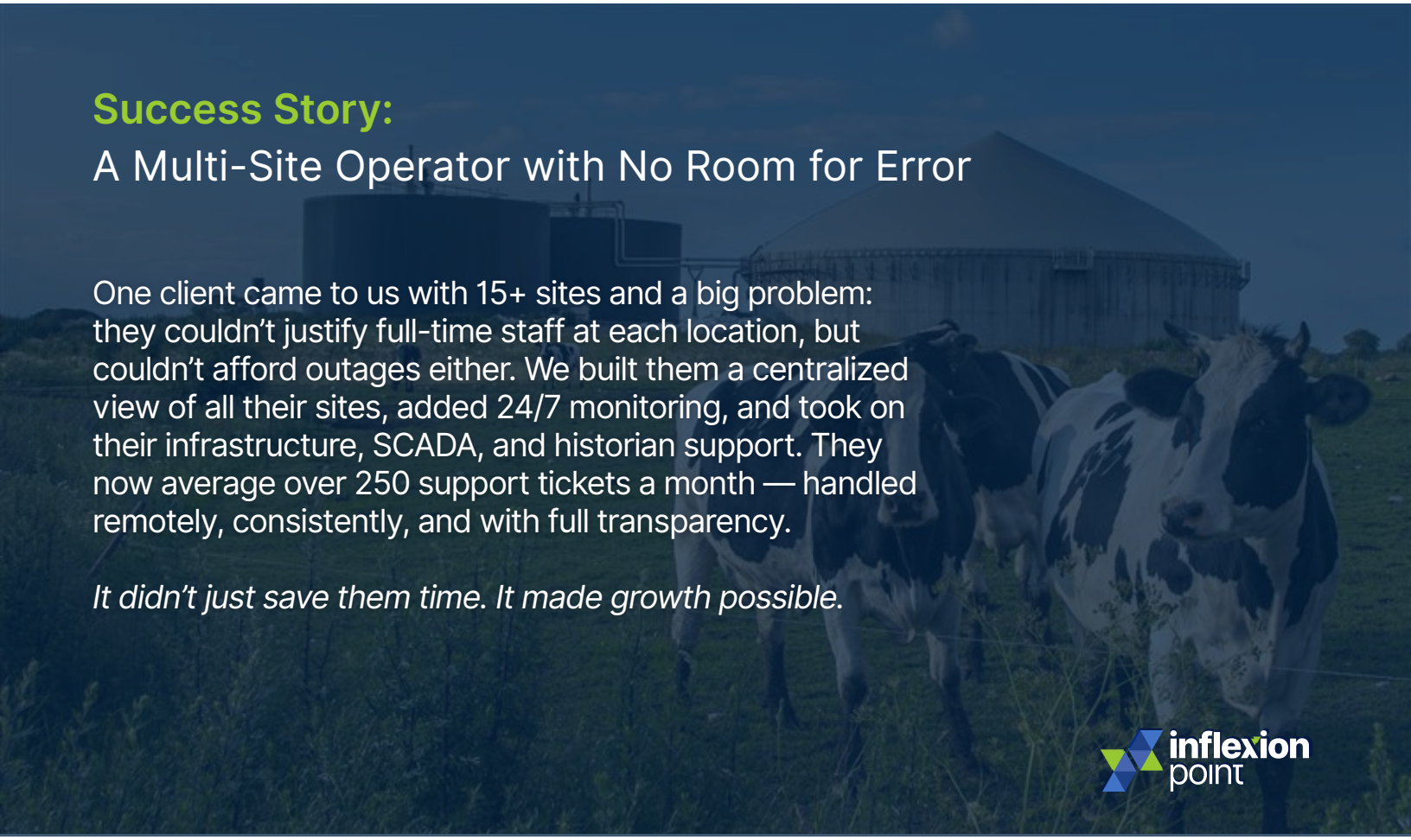
What saved us — and our client — was structure.

The Difference Between Scrambling and Systemizing

- Daily backups and verification
- Quarterly patching (scheduled, not reactive)
- Real-time CVE monitoring with remediation plans
- Asset and vulnerability management — so we knew what was running where, and what needed attention
- Clear escalation paths for when something went sideways
- Root cause analysis baked into every ticket — not just closing it out and hoping for the best

What A Systematic Approach Actually Enables

- A control system update doesn't stall for weeks because no one's free
- A minor alarm doesn't snowball into downtime
- A cyber threat doesn't sneak in because patching "wasn't urgent"
- Sites can scale without needing to hire a whole new team



Success Story:

A Multi-Site Operator with No Room for Error

One client came to us with 15+ sites and a big problem: they couldn't justify full-time staff at each location, but couldn't afford outages either. We built them a centralized view of all their sites, added 24/7 monitoring, and took on their infrastructure, SCADA, and historian support. They now average over 250 support tickets a month — handled remotely, consistently, and with full transparency.

It didn't just save them time. It made growth possible.

inflexion point

Holistic OT Support: It's Not Just IT with a Hard Hat

A lot of people assume OT support is just IT in a hard hat. And honestly? That's part of the problem.

OT environments are not just another department on the network. They're physical, they're real-time, and they don't forgive mistakes. You're not rebooting someone's laptop — you're touching equipment that runs a plant, controls gas flow, or manages regulated production. Stakes are high, systems are sensitive, and timelines are tight.

We've seen well-meaning IT teams accidentally take entire lines down. Or deploy patches that mess with SCADA stability. Or miss a key alarm because it wasn't in a language they speak.

That's why holistic OT support isn't a nice-to-have. It's a must.

So, What Does Holistic OT Support *Actually* Cover?

- SCADA, HMI, and Historian Support
- PLC Support and Troubleshooting
- Infrastructure + Network Awareness
- Custom Applications
- Cross-Discipline Engineers

> Supporting compliance frameworks like NERC CIP and FDA 21 CFR Part 11 is second nature to our team - we're used to working within change control, audit trails, and strict documentation standards.

Why It Matters

You don't want four different vendors pointing fingers. You don't want your controls guy saying, "That's an IT thing," while the IT team says, "That's OT's problem." You want someone who sees the whole picture and owns the outcome.

inflexion point

IT Help Desk vs OT Support Partner

Feature	IT Help Desk	OT Support Partner
Scope	User endpoints, email, VPN	PLCs, SCADA, HMIs, Infrastructure
Priority	Tickets by queue	Critical uptime and compliance
Change Control	Often ignored	Fully embedded in process
Context	Office environments	Regulated / Industrial Environments

Practical Tip:
Map Your Dependencies

- List your key operational tools (HMI, SCADA, PLCs, Historian, etc.)
- For each one, write down what it *depends on* - network, VM, OS, backups, patches, custom scripts
- Then ask: who owns support for each of those pieces? If the answer is “a mix of people, and we hope they talk to each other” – that’s a gap.

From Firefighting to Foresight

Most OT teams don't start out firefighting. But over time, the pileups happen: outdated patches, undocumented fixes, tribal knowledge that walks out the door, alerts that get ignored because they're always going off. Eventually, everything feels urgent—and nothing feels strategic.

That's the trap. And it's exactly what managed services are designed to break.

Proactive Support Means Better Ops

- Data-Driven Reporting
- Root Cause Analysis
- Patch Schedules That Stick
- Built-In Continuous Improvement

The Shift:

From Panic to Planning

We've seen it happen:

- Plants that finally got their alert storm under control.
- Teams that stopped manually restarting things every Friday.
- Operators that stopped fearing audits because the reports were already built it.

Practical Tip:

Create a simple report each month with these columns:

- ☑ Ticket Category (infrastructure, SCADA, network, alarms, etc.)
- ☑ Role Needed to Resolve
- ☑ Time Spent Resolving
- ☑ Repeat Issue Count
- ☑ Root Cause (if known)

inflexion point

Why Modern Operations Demand More Than In-House IT

Smart operators aren't choosing managed services for convenience. They're choosing them because complexity, compliance, and continuity demand more than internal teams can sustainably deliver. When you weigh predictable costs against unpredictable downtime, specialized expertise without the burden of full-time overhead, and the ability to refocus internal teams on strategic improvements instead of routine upkeep—the decision becomes clearer.

Build vs Buy

Add up the cost of:

1. One full-time SCADA expert
2. Coverage for after-hours and vacations
3. Ongoing training & compliance updates
4. Licenses, monitoring tools and infrastructure redundancy

Then compare it to a single, flat monthly fee. That's the logic driving today's shift to managed support

Make the Smart Move Before You're Forced To

You don't need a system failure to know something's not working.

Maybe your team is stretched too thin. Maybe patches are getting delayed. Maybe support just isn't consistent across sites—or across shifts. These aren't dramatic failures. But they add up. And they get expensive.

The good news? You don't have to overhaul everything. You just have to stop doing it alone.

We built our managed services offering the same way we approach every system—by listening to what clients actually need, then designing for it. Now, whether it's backup monitoring or full-blown critical care, we've got a model that fits.

Smart operators aren't waiting for a crisis to make a change. They're planning for scale, designing for uptime, and partnering with teams that can grow with them.

We'd love to be that team for you.

inflexion point