

Managed IT Services

**Predictable IT. Fewer Surprises.
One Partner Who Owns the Outcome.**

AI raised the bar for IT security, and the model most organizations are running was not built for it. Western Computer replaces fragmented, reactive IT with one accountable partner across your users, devices, identity, and access security. Western runs both your IT and the Dynamics ERP your business depends on, so one partner owns the outcome, and you stop chasing vendors when something breaks.

TWO LEVELS OF PROTECTION. ONE DECISION.

Built for organizations with 10 to 200 users

STANDARD PROTECTION

Your day-to-day foundation

- **Support:** remote help desk and Microsoft 365 support, plus onboarding and offboarding
- **Protect:** proactive monitoring, software updates, and Microsoft 365 backup
- **Secure:** threat detection on every managed device, anti-phishing email filtering, and multi-factor and risky sign-in monitoring
- **Plan:** monthly reporting and an annual planning session
- **Document:** Cyber Liability Essentials, with an incident response plan, security and AI acceptable-use policies, and audit-ready evidence

ADVANCED PROTECTION

Everything in Standard, plus:

- **Managed detection and response:** an analyst triages threats and coordinates containment
- **Identity and Microsoft 365 security review:** risky sign-ins, privileged role changes, multi-factor gaps
- **Posture review:** backup and patch checks with remediation priorities
- **Executive reporting:** monthly trend review and a quarterly business review
- **Security awareness training:** simulated phishing that teaches your people to spot attacks

Support runs 8 a.m. to 8 p.m. ET on both levels. Security tooling monitors continuously; analyst triage happens within coverage hours. Work beyond the managed scope (projects, server administration, vendor management, on-site visits, formal compliance) is quoted as a fixed fee and approved first.

5 REASONS ORGANIZATIONS MAKE THE SWITCH

1. If ransomware hit tonight, there is no written response plan.
2. You back things up, but no one checks whether the backups actually worked.
3. A small team stretched across security, cloud, compliance, and AI has little time left for strategic projects.
4. When something breaks, you chase multiple vendors and no one owns the outcome.
5. Audit and compliance readiness is constant upkeep, not a last-minute scramble.

Which Level Fits?

Choose Advanced Protection if an auditor, cyber insurer, or customer security questionnaire wants **proof your controls are watched and acted on**, you've had a security incident or near-miss, or **the same problems keep coming back**. Formal compliance projects are scoped separately.



Customer Quote

"Western Computer's IT services have been a trusted partner for Dutch Farms. Western is responsive, knowledgeable, and proactive in keeping our systems running smoothly."

— Len DeYoung, Internal IT Admin, Dutch Farms

Identity and email are the front door for attackers, and the risks Standard alone was not built to stop:

67% have seen a spike in identity-related incidents	51% were hit by business email compromise in the past year	68% cannot respond before attackers establish persistence
--	---	--

Source: Huntress 2025 Managed ITDR Report

WHY WESTERN: WE RUN BOTH

Most IT providers manage servers, networks, and devices. Western also understands how they connect to your Dynamics ERP, so we manage IT around how your business runs.

START WITH A COMPLIMENTARY 26-MINUTE IT AND SECURITY RISK REVIEW:

See exactly where you stand before committing to a path. One structured conversation, an internal security scan, and a one-page readout within 5 business days. **The next step is your call.**

Microsoft Inner Circle for AI Business Solutions, 2026/2027, three years running.