SINGLE DIGITS™
OUTSOURCED IT BUYERS GUIDE

Communities Need 24/7/365 IT Support and Cybersecurity Challenges

END USER SUPPORT

End User Device Management

Our desktop support approach is holistic, involving full hardware patch management to make sure your computers have the most up to date security patches and mitigating threats using Microsoft Defender. We also have remote access support so agents can assist when you are at the community or working from home. Ability to submit requests from your workstation and automate reporting so you know the status of your technology environment conveniently in one report.

Software

- Microsoft Suite, Outlook, Word, Excel, etc
- Daily Data Backup for Business Continuity
- Mobile Device Management (BYOD/Tablets)

Hardware Purchasing and Support

- Dell laptops and desktops
- Managed printers including scan to email functionality
- Nurse cart equipment support

COST/BENEFIT

Hired Employee vs Managed Service Provider

IT Manager On-Site

- $32–$44/hour with a 24x7x365 support expectation
- $66K–$91K annually or $5,500 - $7,600 monthly, without overtime assumptions
- If burnout is your style, repeat with a new hire again in 6-9 months

Managed Service Provider

- On-site team member can actually take a night/weekend off
- Residents and staff get the support they need, anytime at a 10-20% lower cost
- You eliminate unexpected OT or IT costs that fall outside of their scope.
- You're not hiring (again) in six months when burnout wins.

CYBERSECURITY

Threat Vectors

SaaS Scanning

With the amount of services that a community uses on a daily basis that is through Internet portals, the need for scanning links prior to allowing access to a site is critical to stop potential malware

Vulnerability Management

Regularly scheduled scans of network devices and end user equipment to detect and remediate any threats

Email Scanning

Identify threats upon receipt and scan attachments for any suspicious characteristics with proper mitigation

End User Training

People are the weakest link in any organization. Customized monthly security training to improve awareness and example phishing exercises improves end user detection to avoid potential breaches

Wealth of Knowledge and Experience

You are partnering with a team that is detecting and mitigating thousands of threats and learning from each one of them. Compared to one employee that will have limited experience and may miss or elongate the mitigation process due to a lack of exposure.