UTOPIC software

MSP

Preserve. Protect. Recover!

BECOMING A TRUSTED ADVISOR

Helping your clients prevent unforseen expenses: improve quality of service while reducing costs

(813) 444-2231
partner@utopicsoftware.com
www.utopicsoftware.com

"Seek first to understand and then to be understood."

-Steven Covey

The 7 Habits of Highly Effective People

As a service provider of any kind, the ultimate compliment is to be considered a "trusted advisor" by your client. But this status is more than simply getting a good reference or getting a customer to renew their annual contract. By its very title, a trusted advisor is an ***outside insider*** for a company: a consultant depended upon by an organization to provide valuable insight on how a company can best achieve its stated ***and latent*** goals.

For managed service providers, whose very purpose is to ensure various IT infrastructure and applications provide the expected results and value for the client, to become a trusted advisor means you have the responsibility to continually identify and implement ways to improve performance, anticipate challenges

The difference between an **expert** and a **trusted advisor** comes down to a single attribute: an expert provides good answers. A trusted advisor asks good questions.




Becoming a trusted advisor

and constantly adapt to the transformative nature of technology.

Sounds easy enough. That *is* what you do, right? Whether you provide network support, security, help desk or a variety of other key services doesn't immediately raise you to the level of trusted advisor. It simply means you provide an important service…and we assume you provide it very well.

Part of the trusted advisor's job description is not only to improve performance, but to do so at the maximum level for minimal costs. The transition from service provider to trusted advisor means you are looking out for your client's best interest, and not just service they can buy. To accomplish this, MSPs must address one of the biggest cost burdens that can affect the relationship: break/fix issues.

The labor required to manage this portion of the relationship is the biggest drain on margin. Regardless of whether a client purchased full coverage for a monthly fee, use a capped block of hours or pay out of pocket for each issue, somebody's margin is affected when things go sideways. It's either money (margin) out of the MSPs pocket or out of the clients.

It's not that issues arise, it's just that the ***labor required to address problems is unpredictable***. It could be a five minute fix or something that takes an application or network offline for an extended period of time while troubleshooting, fix planning and solution are applied.

Nothing erodes trusted advisor status faster than money. This is not to say an MSP should operate as a non-profit, but there are **ways to proactively and automatically confront the break/fix issue without either side having to dig deep into profit margin**. And, more importantly, provide a reliable means to attack unforeseen issues that eat time, upset productivity, and force reprioritization of potential revenue generating services. This is the road to trusted advisor status.

The ability to break out of "*firefighter mode*," is the first step to creating lasting value for clients. The less time spent with your hair on fire, the more you can concentrate on tasks that support client business

(and add to an MSP partner's credibility and differentiation). For many MSPs services surround 6 general areas of coverage

1. Network Support
2. Backup and Recovery
3. Security
4. End User Support/Help Desk
5. Compliance
6. Extra consulting services

The one constant through each of these services are the likelihood that break/fix will occur sooner or later. The ability to mitigate the risk associated with these problems and the labor required to properly diagnose and repair them can by automated configuration.

This doesn't suggest a simple recovery tool. Instead of applying hours diagnosing and repairing, **systems can self-heal upon reboot**. It takes the client's ideal image and removes the service issue. It's simple. It's automatic. And it removes problems that would otherwise require manual intervention and desk side visits.

Of course this doesn't solve every problem, but if it can remove 60-70% of user-inflicted issues like changing critical settings, downloading malicious viruses, making unauthorized application changes, deleting necessary dll files, disabling BITS, and thousand other actions that compromise infrastructure integrity, not only are significant dollars saved, uptime and asset availability increased, but expensive personnel time is saved for higher value tasks.

There are several other benefits an MSP achieves by including automated self-healing as part of an overall package.

Scheduled vs variable labor: Labor costs take a huge bite out of the scope of service--especially when it comes to break/fix issues. An MSP and their client can create more fiscally stable relationship through precision budgeting. The client knows how much is going to pay each and every month and the MSP

gains the stable recurring revenue. By using configuration automation and optimization, MSPs can reduce the specter of additional pass-along costs to the client or avoid absorbing the additional expensive labor costs. Now the conversation can ***move from "how much" to "how to improve***" (*from reactive to proactive*).

Expand geographic reach: Many MSPs operate as regional entities because they do not have the personnel or the budget to adequately cover a larger (or even national) territory. From a cost perspective, self-healing eliminates a great many client visits. Typical on-site services like device restoration, no longer require a warm body in the room. This, in turn, reduces the need to travel and out-of-pocket time and costs. Without having to hop in a car or plane, you can provide effective service to a wider circle of clientele. Now when you visit a client, it is to provide proactive intellectual value and consulting expertise…or simply take them to dinner to thank them for the business.

Help Desk reduction: Resources show that by self-healing and rebooting to an ideal state eliminates more than 34% of all inbound help desk issues without manual intervention. If you consider that very time the help desk phone rings, it's $20 (based on nat'l average). For more serious issues such as catastrophic device failure, infected operating systems/applications, unauthorized downloads, the cost is obviously greater--and not just in terms of tech/admin intervention, but lost productivity and potential loss of client trust. This doesn't include scheduled maintenance tasks such as patching, updating and migration—which in itself requires a significant time and resource commitment. By adding a self-healing component to your existing slate of offerings, it reduces the number of help desk calls and, more importantly, allows an MSPs help desk pros to **uncover root causes rather than continually fix the symptoms**.

Removal of malicious changes: Through maliciousness or carelessness, your client's network is under constant attack from botnets, malware, viruses and a variety of other negative impact influences. Although automatic configuration and reimaging can't prevent Stan from sales downloading a suspect

app or prevent organized element in Eastern Europe from worming into a system, the continuous maintenance and reapplication of an ideal state can prevent lingering damage. Any time an unauthorized outside influence tries to change a registry, attach itself to a file, or embed itself in a supported application, the system rejects these modifications in favor of the ideal state…in real time. From an MSP perspective, this avoids the downtime needed to cleanse a network and helps preserve the continuity of critical information.

Of the six general service areas mentioned, it is obvious how configuration/recovery/repair/ reimage automation can helps issues related to the network, backup and end users, however some question the value to those who provide security and compliance services. The answer is simple. Although not a traditional security solution, it not only demonstrates control over network assets (as required in SANS, HIPAA, PCI and others), but enables the operating environment running smooth over the course of the lifecycle.

Because a trusted advisor is more interested in a long term relationship than any short term gains, it is imperative that MSPs find and propose new and innovative solutions to include within their base services. If clients consider a MSPs service as a commodity, then it is very simple to find another provider.

The difference between an expert and a trusted advisor really comes down to a single attribute: an expert provides good answers. A trusted advisor asks good questions. *Can you reduce costs while increasing your quality of service?*

Let us prove it!

Schedule a demo today