"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

Dan Foote
Owner/President

What's Inside:

Got IT Problem? - Click Here!

What is a Managed Services Provider?

Is an MSP right for your business?

Managed service providers (MSP)

A managed service provider (MSP) is a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user systems. Small and medium-sized businesses (SMBs), nonprofits and government agencies hire MSPs to perform a defined set of day-to-day management services. These services may include network and infrastructure management, security and monitoring.

MSPs often handle management services on a daily basis so customer organizations can focus on improving their services without worrying about extended system downtimes or service interruptions.

While some MSPs may specialize in specific segments of IT, such as data storage, others focus on specific vertical markets, such as legal, financial services, healthcare or manufacturing. Managed security service providers, for instance, offer specialized types of services, such as remote firewall administration and other security-as-a-service offerings. Often, MSPs perform their tasks remotely over the internet.

The evolution of MSPs began in the 1990s with the emergence of application service providers (ASPs), which offered a level of service for remote application hosting. ASPs helped pave the way for cloud computing and companies that would provide remote support for customers' IT infrastructure.

MSPs initially focused on the remote monitoring and management (RMM) of servers and networks. Over time, they have expanded the scope of their services as a way to differentiate themselves from other providers.

Voice Chat with ChatGPT is now available – even for the free version

The vocal chat feature on ChatGPT was first announced in September 2023, but at that time, it was only available for Premium and Enterprise subscription holders. As of Nov. 21, 2023, the voice chat function is possible for uses by anyone who has ChatGPT.

To use, you'll need to open the latest version of the ChatGPT app on your Android or iOS device. If you're not sure you have the latest version, check for updates. On the app, tap the headphones icon at the bottom of the screen to start a verbal conversation with ChatGPT.

Some things to remember, though:

This AI chatbot is only trained on data through January 2022, so the answers to your questions may be outdated, especially if they're about more current topics.

Also, "hallucinations" are still a possibility. This means that ChatGPT could give you information, quite convincingly, that's just plain wrong.

This is an area of ongoing research and development. The exact features and capabilities may vary, so you should continue to check the latest updates from OpenAI for the most accurate information.

This news about this new talkback feature of ChatGPT was announced on X by Greg Brockman, OpenAI's President and co-founder.

Privacy mode is not so private after all

Some holiday shoppers mistakenly believe that they get tagged by algorithms when they browse for certain items, so they assume that cloaking their identity by putting their browser in Incognito Mode can help them get better prices.

While using Incognito Mode or Apple Safari's Private Mode do offer some benefits, getting a better price isn't one of them. All these stealth modes do is erase your search history and prevent the browser from using cookies to see your browsing history.

This is a great feature for concealing the gifts you're buying your kids, but it won't help you get better prices.

The price of items online is typically based on a several factors that don't have to do with you, individually, or how often you search for a product. Instead, pricing is based on timing, location and how much a company has paid to get the item to the top of the results listing.

A Google representative confirmed that cookies are remembered in the current session in Incognito Mode, but then deleted immediately after closing the browser. If you return in Incognito Mode, you just have to start as a new user without an empty cart.

You should also know that your internet service provider and network administrator still may see what you're searching for.

For instance, when you search for a product in Amazon, even using Private Mode, Amazon is 99.99% sure of who you are, based on the link you clicked, your IP address, your zip code, etc. The company may not know specifically who it is that's searching, but they do know at what home the search is coming from, what operating system you're using, which language is your default, and other details that point to you.

And all that tracking is likely passed on to the company that paid for the ad you clicked on.

Shiny New Gadget Of The Month:

Starlink in Alaska

Starlink now shows full coverage in Alaska and Northern Canada. The Starlink map was recently updated and they have turned on all of Alaska a bit earlier than expected.

Another exciting aspect of this new open coverage area in Alaska up to the polar region is that the Starlink coverage this far north is compliments of Starlink's laser inter-satellite links (Space Lasers). The inter-satellite links allow the Starlink satellites to communicate with each other and cover areas of the world that it's not practical to install ground stations like polar regions and large areas over the open ocean.

Since all of Alaska and Canada are now turned on for complete Starlink coverage, this covers a popular area that many RVers will travel through when traveling from the lower 48 up to Alaska.

Initial reports suggest there is still some tweaking needed to get uninterrupted service in Alaska due to the limited satellite coverage this far north leaving some coverage caps at certain times, but with the current progress already in place, chances are looking good by the summer of 2024 you can stay connected with high speed internet with Starlink from the lower 48 all through Canada into anywhere in Alaska you wish to travel.

907-885-0501

Risk of cyberthreats in hospitals

The costs of cybercrime to any organization can be huge, including financial loss, reputational damage, and inconvenience. But the risks increase exponentially for an organization whose primary mission is helping and saving lives.

For hospitals and other healthcare entities, cyberthreats such as DDoS attack campaigns, AI deepfakes, and major hacking events can disrupt quality service delivery and potentially pose a risk to patient safety.

Here are the three top cyberthreats that hospitals and other healthcare organizations face:

- **Ransomware:** Healthcare organizations continue to be targeted as the number one sector in the ransomware space. These attacks, by individuals and nation-state actors seeking patient data, can disrupt hospital operations and lead to significant financial losses.

- **Phishing and Spear Phishing**: Ransomware arracks are common due to their effectiveness in gaining initial access to healthcare networks, as well as their low cost for cybercriminals. Cybersecurity professionals recommend using a sophisticated email gateway solution augmented by DMARC capability to help authenticate and mitigate these attacks.

- **Third-Party / Partner Breaches:** Data breaches involving third-party partners can expose sensitive patient information, which can lead to identity theft and fraud, increased cost for the hospital to remediate these damages, and significant disruptions in healthcare operations. On the cybersecurity front, third-party vendors can provide an entry point for further attacks into the hospital's network.

Healthcare entities are focusing on ways to strengthen their defenses against these threats, as well as how to respond and recover from them if breaches do occur.

As in any other organization, cybersecurity has got to be a team fight, involving every leader in the organization, from administrators to CEOs, who much become familiar with these risks and be responsible for implementing best standard practices.

The Future of Social Media

The industry trend seems to be separating social media into entertainment feeds and private channels for chat. Social media used to be a means for connecting friends with friends, but that purpose seems to be going away. It has instead evolved to connect you with people you don't actually know in real life, similar to what tv has always been.

A handful of accounts create most of the content while everyone else acts as the audience, mostly there to enjoy said content. Thus, social media is looking a lot like mass media, having content created with high-production values.

The future of social media, experts predict, is that it will become another avenue for public entertainment. It will end up looking like flipping from one cable channel to another, they say. **This means the rise of a new kind of entertainment professional: The Creator.** A creator is anyone who records or makes something that goes viral on the internet. Instagram, TikTok, and other social media platforms, have become avenues for these young creators to practice their art.

To assist these young creators, a new business has formed - Creator Talent Management Agencies, which get involved with creators and musicians at the early stages of their careers to help them develop their brand, plan content, understand different platforms, and connect them with potentially lucrative brand deals.

As social media and its audiences gravitate toward more professional content, those who are good at making content with high-production values will thrive.

On the formerly social platforms, whether content is coming from creators with better equipment and more skills or Hollywood studios testing the waters, doesn't matter. In the end, it will all look the same to the consumer. Advertisers, too, appreciate the convenience of tv, because people are never more suggestable than when lulled into a sort of mindlessness.

But tidbits that people used to share on social media are not going away, they've just been relegated to private group chats.

Meta is following the broader industry trend of making the public messages more professional entertainment feeds, while connecting individuals primarily through private messaging.

Today, the terms _cloud service provider_ and _managed service provider_ are sometimes used synonymously when the provider's service is supported by a service-level agreement (SLA) and is delivered over the internet.

What are the types of MSPs?

The types of managed service providers can differ depending on the criteria chosen to categorize them. For example, if a business chooses to organize MSPs by the size of their target customers and how much responsibility they take on, MSPs can be organized in the following way:

Pure-play MSPs. These tend to be smaller providers that focus on monitoring networks and application performance. They offer their own native services that focus mainly on reporting and alerts.

Staffing legacy MSPs. These MSPs generally target midlevel organizations and Fortune 500 companies and often offer a wide range of services, including monitoring, reporting, and software installation and upgrades.

High-level MSPs. These consist of small and large providers that enable their clients to outsource as much of their IT processes as needed. Typically, high-level MSPs offer a wide range of services.

MSPs can also be categorized by the type of services they offer:

Monitoring. These MSPs offer real-time monitoring software for different applications, network devices, servers or websites.

Remote support. These MSPs offer cloud-based software, support remote devices and remotely troubleshoot technical issues.

Proactive support. These MSPs perform preventative maintenance to stay ahead of any device or network issues that could arise.

Centralized management. These MSPs provide a management console for complex networks, remote monitoring, patch management and security software.

Scheduled maintenance. These MSPs offer organizations regularly scheduled network maintenance.

Simplified billing. These MSPs handle invoicing, payments and budgeting via a billing management system.

What are the benefits of managed service providers?

Benefits of managed service providers include the following:

Help an organization fill staff shortages. If an organization lacks workers, it can outsource some of its tasks to the MSP.

Provide expertise. Hiring a reputable MSP provides an organization with access to expert resources.

Provide business continuity. An SLA documents the MSP's obligations to the business to prepare for or recover from a disaster.

Provide constant network monitoring. Many MSPs offer 24/7 monitoring services using network monitoring tools that offer system visibility and cloud management.

Improve security. Some MSPs provide security software and awareness training.

Improve cost efficiency. If numerous unplanned repairs are needed, paying a fixed monthly charge can be more cost-effective than paying hourly. While the MSP handles the day-to-day management services, customer organizations can focus on improving their services.