E-BOOK
2019

# MSPS
# A GUIDE TO GETTING STARTED IN CYBERSECURITY

untangle

# CHAPTER 1: INTRODUCTION

## 1. THE MANAGED SERVICES PROVIDERS MARKET

The managed IT Services market continues to show year on year growth. As IT infrastructure is improving productivity, companies are choosing to engage with service providers to pick up the slack left by their in-house IT departments. According to ***Markets and Markets***, the industry will grow at a 9.3% Compound Annual Growth Rate between 2018 and 2023.

Managed Services Providers (MSPs) and Managed Security Service Providers (MSSPs) are specialist IT firms that provide both on-site deployed systems and remote managed services. Of these two service types, on-site deployed services will gain the larger market share over the next four years.

A report released by ***Forrester Research*** lists the three main industry trends that will affect MSPs and MSSPs in the future as outsourcing, cloud deployment, and system automation. Companies who use their services say they are choosing their service providers mainly based on the associated costs, the level of expertise (both in hardware and in software), and business process knowledge. For small-and-medium businesses (SMBs), it is also essential that service providers can handle end-to-end IT projects.

Companies may be wary of trusting third-party service providers with their data and access to their systems. It may be necessary to ensure prospective MSPs and MSSPs comply with frameworks like SSAE-16 or AT101 (repackaged as SOC 1 and SOC 2 Reports).

## 2. NEW PLAYERS ARE EMERGING

Value-Added Resellers (VARs) traditionally sold hardware systems to companies, which may also have included a software element. They are similar to MSPs and MSSPs in that they possess the technical expertise to serve a customer’s needs. Many VARs may even receive requests from their current customers to include services like a firewall or network monitoring, and instead of outsourcing the demand, now choose to provide it themselves. Either they have the expertise, or they partner with an expert service provider already.

These similarities mean many VARs are actively changing their business model to that of an MSP. It requires a relatively small shift in focus from delivering a technical product to providing a technical service. Implementing a customer service process model and improving the support services offered by a VAR goes a long way to moving into the MSP space.

VARs have years of technical expertise delivering hardware systems to their customers while making use of service providers themselves. They can easily expand their offerings to include a complete end-to-end solution, something customers desire more often.

## 3. IT MSP STATISTICS ARE MOSTLY FAVORABLE

The demand for Technology and Managed IT Services is growing daily. From large enterprises to small and medium companies, everybody is dependent on the latest technology systems to succeed in the business world. IT budgets rarely increase though, so companies are always looking to do more while spending less.

With MSPs and MSSPs at the forefront of this technology drive, the industry has favorable forecasts for the future.

**Some vital statistics on the industry include:**

- Overall IT Industry growth expected to be 5% per year
- Of all the digital data in use today, 90% was created in the last two years
- Annually 75% of SMBs will outsource some of their IT requirements to MSPs
- New customers will make up 48% of the market's growth
- Machine Learning, Blockchain, and the Internet of Things (IoT) are the leading new technologies
- Top skills sought by customers are for Data Management and IoT

There are still challenges facing the industry though. Foremost of which is the skills gap in the sector. IT firms are recruiting the best technicians and engineers, but the rapid rate at which new technology is developed requires additional skills and training to be provided to existing IT staff members.

Additionally, maintaining systems that are becoming more complex every year is consuming a more substantial portion of IT budgets for companies, capping their expenditures.

## 4. SOLUTIONS FOR SMALL-TO-MEDIUM BUSINESS

MSPs/MSSPs are becoming more critical to SMBs as they seek to grow and thrive in their respective markets. Having their IT needs catered to in-house has become expensive and laborious. Both resources and equipment (including technical expertise) can quickly become outdated and upgrades to new systems slow due to operational constraints.

A smart solution to the above problem is to farm out a larger portion of the operational IT systems to a service provider.

**The primary services requested are:**

- Storage, backup, and disaster recovery services
- Network Monitoring (Firewalls, Intrusion Detection and Prevention Systems)
- Security (Antivirus and Malware protection)
- VOIP Telephony services
- Software-as-a-Service (Saas)

Knowing what SMBs need makes it possible for MSPs and MSSPs to bundle solutions that specifically cater to small-and-medium businesses. Their budgets can therefore cover their IT needs, while upgrades and automating additional business tasks remains possible without causing as many operational disruptions.

# CHAPTER 2: MOVING INTO CYBERSECURITY CAN BE DAUNTING

For MSPs who are starting to look at offering complete and secure solutions for their customer's IT headaches, their first glance at cybersecurity can be confusing. The technical jargon can be off-putting. The solution offerings can seem over the top or insufficient for their needs. To unpack all the requirements without specific technical knowledge can be time-consuming and frustrating for administrators.

## 1. CHOOSING THE RIGHT SOLUTIONS

If you've already received requests to provide security solutions to your customers, you'll have a good idea of what it is they need. Similarly, by using a vendor with comprehensive industry knowledge, they would be able to advise you where your current offerings fall short and how best to extend them.

**A comprehensive cybersecurity solution will primarily include:**

- Next-Generation Firewalls
- Mobile Cybersecurity (software controls specific to mobile network-enabled devices)
- Real-time Alerting

- Enforcing password policies (revoking and forcing password changes regularly)
- Data backups and virus protection
- Multifactor Identification and Authentication

Due to the rapid increase in cyberattacks, it is critical that as an MSP you have the right alerting tools in place to protect clients and their networks. Finding out too late that a phishing email slipped through or a device began acting suspiciously can lead to a breach and devastating results for you and your client. MSPs should ensure that the solutions they choose have 24/7 alerting engines that can be integrated into their Remote Monitoring and Management (RMM) or apps like PagerDuty or Slack.

## 2. MSPS TO MSSPS – SECURITY-SPECIFIC SOLUTIONS

An MSP may want to include security services or start making use of security-specific service providers to augment its customer offerings. This makes sense as MSSPs focus exclusively on data and network safety. They provide state-of-the-art firewalls boosted with Intrusion Prevention and Detection Systems (IPDS) that are sophisticated enough to prevent real-time attacks.

Similarly, if you are a VAR thinking of aligning your business model with that of an MSP, it makes sense to include cybersecurity services for your customers at the earliest opportunity. By proactively sourcing solutions that cater to your customers' security needs, you can become the one-stop-shop for both hardware products and managed IT cybersecurity solutions.

Adding managed security services to your portfolio will also increase your revenue stream and improve your client relationships. The managed security services market will grow to more than $35 billion in 2020. As an MSSP, you are the security professional protecting clients from major data breach threats like phishing, malware, trojans, and work proactively with the client to ensure all systems and devices are adequately protected.

## 3. EVALUATING SOLUTIONS

When determining which solutions to add to your MSP portfolio to offer MSSP services, you can get bogged down with the amount of options to choose from. Follow these tips to ensure you select the right vendor that can benefit your business and clients.

- **Find a Comprehensive Solution** - You don't want a solution that only addresses a few aspects of network security. Solutions should have threat and malware protection as well as block phishing and hacking attempts. Look for solutions that also encompass cyber threat intelligence to protect against emerging and unknown threats.

- **Price is Important** - Many of your customer will probably not be able to afford high-end solutions, which is the reason they are coming to you for help. Make sure the solution you choose has SMB pricing in mind so you can pass those savings on to the client.

- **Alerts & Reporting are Critical** - Being able to easily pull reports to determine the root cause of an attack or showcase compliance efforts for those clients with egulations to abide by is a critical feature you should look for when deciding on a network security vendor to partner with. A solution with real-time alerts is also crucial if you want to patch a vulnerability or stop a threat from reaching users.

- **Cloud Options** - Everyone is moving to the cloud, and your customers will be curious about this option too. Choose a solution that has cloud-based options that can scale as you grow.

Whatever solution you choose, it will be important that it can integrate with current technologies and software applications. The most significant benefit of doing this is the convenience you offer to your customers. They will not have to seek additional service providers to ensure their overall security. That simplifies their lives and boosts your attractiveness for any future business needs they may have.

# CHAPTER 3: FOCUSING YOUR SECURITY REQUIREMENTS

If you're an MSP seeking to extend your offerings to include security services, choosing the right vendor will be of critical importance. You will need to know what security components your customers require and how your service provider can deliver them.

## 1. COVERING THE BASICS

A firewall remains an essential security control that every organization needs. Apart from physical firewalls installed on-site, virtual firewalls can keep track of traffic originating externally or internally on the network (helping to identify advanced persistent threats). A comprehensive solution will likely include both these components, and should also consider cloud deployment options.

Similarly, firewalls are only as good as their threat definitions, so having integration with advanced threat intelligence will also be required. Remote management and endpoint visibility are just as important.

Securing your customer's system is easier if you collaborate with specialists who are ahead of the curve and proactive in dealing with cybersecurity.

## 2. CHOOSING A CYBERSECURITY PARTNER

**Key considerations when selecting a cybersecurity partner will include:**

- Deployment and implementation requirements
- Industry knowledge and expertise
- Support and remote management capabilities
- System customization and integration features

The items above should all form part of the assessment before choosing a partner. The best cybersecurity solutions will consider these pain points and eliminate most of them for you.

## 3. UNTANGLE'S CYBERSECURITY OFFERINGS

NG Firewall, Untangle's award-winning product, is a software solution that can be downloaded and run on your hardware, in a virtual environment, or in the public cloud via Amazon Web Services or Microsoft Azure, giving you ultimate flexibility as to how you deploy. Because it's software-based, it's also easy to integrate into the RMM solution of your choice.

Easily manage all of our NG Firewall deployments from our cloud-based, centralized management: Untangle Command Center. Command Center allows access to your deployments with ease and convenience from any browser. And because it’s cloud-based, you avoid slow, cumbersome, on-premises hardware deployments.

Integration with Malwarebytes provides threat visibility across all managed networks and endpoints, ensuring consistent and comprehensive security protection.

Untangle offers a range of network security solutions that can help managed services providers build out their product portfolios or jump into the rapidly growing network security space.

## 4. UNTANGLE’S PARTNER PROGRAM BENEFITS

**When joining Untangle’s Partner Program, you will get:**

- Highly competitive discounts on products
- Quick registration of critical deals
- Expert technical support and account management
- Recurring revenue stream with subscription services
- Optional, turnkey product rebranding via Branding Manager
- Control over the deployment of hardware (Yours or ours)
- Decreased time-to-market with freemium NG Firewall and cloud-based Command Center

Additionally, Untangle offers Partner Program Benefits to enable MSPs, and MSSPs get the best deals for their customers.

**These benefits include:**

- Software and hardware discounts
- Additional savings with deal registration
- Discounts on live support
- Cloud-based remote management capabilities included free of charge
- Partner portal access
- Listing in the partner directory

As a partner, you will be eligible to receive training and certification from Untangle-U. You will also be able to co-brand your resources, receive demo licenses, and be part of the promotions program.

In an industry where many customers feel they are one breach away from disaster, having a cybersecurity solution may just give you the edge over your competitors. By choosing to partner with Untangle, your customers will know you have their networks and data secured.

# LINKS

**Markets and Markets**

- https://www.marketsandmarkets.com/PressReleases/managed-services.asp

**Forrester Research**

- https://www.crn.com/news/managed-services/managed-services-market-the-three-key-trends-impacting-msps

**VARs to MSPs**

- https://searchitchannel.techtarget.com/tip/VARs-How-to-become-a-managed-services-provider
- https://blog.storagecraft.com/tips-moving-var-msp/

**MSP Statistics**

- https://www.sherweb.com/blog/msp-it-industry-statistics-2018/

**SMB Growth**

- https://www.uswired.com/2018/03/smb-needs-msp/

**Right MSP Approach to SMB Market**

- https://www.computerweekly.com/microscope/news/252447844/Taking-the-right-MSP-approach-to-the-SMB-market
- https://www.businesswire.com/news/home/20160329006196/en/Global-Managed-Security-Services-MSS-Market-Grow

## ABOUT US

Untangle is the most trusted name in solutions specifically designed to help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Untangle’s Network Security Framework provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. Untangle’s award-winning products are trusted by over 40,000 customers and protect millions of people and their devices. Untangle is committed to bringing open, innovative and interoperable solutions to its customers through its rapidly growing ecosystem of technology, managed services, and distribution partners worldwide. Untangle is headquartered in San Jose, California.

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at **sales@untangle.com**.