



A Comprehensive
Cybersecurity
Guide for Channel
Partners

FROM THE MANAGED SECURITY EXPERTS AT TPX



Executive Summary

Cybersecurity solutions are a must-have offering for any IT and telecom advisor looking for new ways to increase their monthly recurring revenue (MRR), keep existing clients and provide meaningful non-commoditized services to future-proof their business.

In this Comprehensive Guide to Cybersecurity for Channel Partners, we'll cover why and how your company should offer cybersecurity solutions to your business clients.

Key Takeaways

Tap into Rising Demand

Don't leave easy money on the table by not offering managed security solutions.

Defend Your Client Base

Expand your service offering and sell into your customer base before another agent, MSP, or other poacher beats you to it.

Choose the Right Partner

Choose a cybersecurity partner with the ability to scale with proven technology and the resources to deliver 24/7/365 service.

Focus on Business Outcomes, Not Technology

Impressive-looking dashboards and analytics won't help your end customer if they don't receive the expertise, monitoring and management to combat threats, prevent attacks and remediate breaches.

Table of Contents

Part 1: What is Cybersecurity?

Part 2: Why Should Channel Partners Offer Cybersecurity Solutions?

Part 3: What Cybersecurity Solutions Should Channel Partners Offer?

Part 4: Where Should Channel Partners Begin When Selling Cybersecurity?

Part 5: Which Buyer Personas Should Channel Partners Target for Cybersecurity?

Part 6: What Are Effective Ways to Start Sales Conversations About Cybersecurity?

Part 7: What Are Common Cybersecurity Sales Objections and Responses?

Part 8: How Can Channel Partners Differentiate Their Cybersecurity Offerings?

Part 9: How Can Channel Partners Find Prospective Cybersecurity Clients?

Part 10: What Pitfalls Should Channel Partners Watch Out for When Selling Cybersecurity?

Part 11: Should Channel Partners Insource or Outsource Cybersecurity?

Part 12: What Should Channel Partners Look for in a Cybersecurity Provider?

Part 13: Why Should Channel Partners Consider TPx as Their Cybersecurity Provider?

PART 1:

What is Cybersecurity?

Cybersecurity is an ongoing practice of proactively protecting individuals' and organizations' critical digital systems, networks, communications, applications, data, devices and endpoints (computers, laptops, tablets, smartphones, etc.) from unauthorized external and internal access, use, disclosure, destruction, modification or disruption. Cyberattacks come in many different forms, including:



Malware

Malicious software programs or files that are harmful to a computer user.

Viruses

A common form of malware, which spreads by infecting other programs or files on its own.

Worms

Malware that self-replicates and infects multiple computers, remaining active on infected systems.

Trojan Horses

Malware is frequently disguised as legitimate software.



Ransomware

A subset of malware wherein computer or network data is breached, locked and used to extort a ransom from the victim to regain access to vital data or avoid the publication of sensitive and/or compromising information.



Phishing

A form of fraud wherein an attacker pretends to be a reputable person or source in an email, social media direct message, or SMS text message communication in order to gain access to software platforms, email accounts, passwords, credit card numbers, or other personally-identifying information.



Password Breaches

Unauthorized access to accounts after hackers successfully gain access to user passwords, either through decoding simple passwords, automation software, or gaining direct access to passwords digitally or physically.



Unauthorized Data Collection

Unauthorized access of personal information (e.g., passwords, bank account numbers, social security numbers, credit card information, or other records) stored in websites, online portals, e-commerce stores, or other digital repositories.



Insider Threats

Risk to an organization caused by current or former employees, business partners, or third-party contractors.



Endpoint-delivered Attacks

Attacks that gain access to data and infrastructure through endpoint devices, including computers, tablets, mobile and other devices.

A comprehensive cybersecurity program aims to protect data and infrastructure from cyberattacks and mitigate damages when breaches occur. An effective program encompasses:



Businesses of all sizes are turning to trusted IT and security advisors, including telecom and IT sales agents, to source and deliver fully managed security technology and services from a leading managed services provider (MSP).

PART 2:

Why Should Channel Partners Offer Cybersecurity Solutions?

Cybersecurity breaches have gone mainstream, rising in frequency and severity, making headlines in media, and striking fear in the hearts of business managers and owners everywhere. Simply put, if you aren't talking about cybersecurity, your competitors will be.

Adding cybersecurity to your portfolio delivers a one-two punch:

1

Cybersecurity locks in customers

Delivering cybersecurity solutions to existing customers broadens your offering, targets their biggest worry and reduces churn.

2

Cybersecurity opens doors to prospects

Cybersecurity is a powerful entry point for conversations with companies that aren't actively looking for other services in your portfolio.

Let's unpack these opportunities.

Customer Retention

Cybersecurity is a stickier solution than most. Whereas customers are easily wooed by lower-priced offerings for commoditized services like voice or Internet access, they're less likely to ditch an effective and proven security solution based on price alone. And since stickiness in one high-performing or high-value solution tends to create stickiness in the other services you deliver, the halo-effect from a security solution can boost revenue retention across your entire portfolio.

Customer Acquisition

Delivering security services is quickly becoming a matter of maintaining your competitiveness. If you specialize in a narrower set of solutions like network access services, you'll start to run into roadblocks. That's because competitors that also sell cybersecurity solutions can become your prospect's single source for network, communications and cybersecurity needs. In this light, failing to develop your cybersecurity practice doesn't only mean missed opportunities for upselling to new clients; it can harm your pipeline and growth prospects.

Further, from the perspective of business evolution, cybersecurity solutions offer a new, fruitful frontier with higher price points and larger margins in a marketplace experiencing race-to-the-bottom pricing and shrinking margins for commoditized access and connectivity solutions.

Finally, channel partners that adopt cybersecurity solutions report "easy" sales to their bases amid a constant stream of free advertising every time a breach makes headlines and reminds their customers of cyberattack risks. Plus, big brand hardware vendors are doing the heavy lifting to educate customers and generate demand.



Cybersecurity Growth is Exploding

"The global cybersecurity market is expected to exceed \$400 billion and grow at over 15% Compound Annual Growth Rate (CAGR) between 2020 and 2026."

Source: Global Market Insights (GMI), 2020

PART 3:

What Cybersecurity Solutions Should Channel Partners Offer?

Your clients need layered protection that addresses multiple touchpoints for all the levels that their staff touches, including:



Network Perimeter



Email Clients



Endpoints



Internet of Things (IoT) Devices



4 Steps on a Cyberattack Path

To determine which security solutions to offer, let's follow the path of a sample cyberattack and correlate the prevention and remediation needs at each point of vulnerability.

STEP 1 Phishing Email Initiates Breach

The majority of cyberattack incidents are initiated by phishing emails, wherein a user clicks on a link in a fraudulent message designed to trick them into revealing sensitive information or enabling the deployment of malicious software on business infrastructure such as ransomware.

SOLUTION Security Awareness Training

Even if your clients have software trying to filter out phishing attacks, they need a total security awareness training program that includes phishing simulations and teaches their employees about cybersecurity, IT best practices and regulatory compliance. Through this program, they'll be able to:

- Expand awareness to reduce threats
- Minimize successful phishing attacks
- Reduce costs by avoiding data breaches

STEP 2

Attack Encounters Firewall

If the human element is breached through phishing, the attack then proceeds to the corporate network, where it can wreak havoc on systems and data.

SOLUTION

Next-generation Firewalls

A firewall creates a barrier around your client's network and monitors traffic in and out based on security rules. A firewall can't protect its network on its own (many companies mistakenly believe it can), but it's still effective. You'll want your clients' systems protected by next-generation firewall (NGFW) technology, which does everything a traditional firewall does but boosts protection through heuristics (analysis using rules, estimates and educated guesses for prediction) or artificial intelligence (AI). Next-generation protection also delivers unified threat management (UTM), which includes:

- Antivirus software
- Intrusion Detection System and Intrusion Prevention System (IDS/IPS)
- Deep packet inspection of SSL traffic
- Safelisting/blocklisting software

PRO TIP: Since cybercriminals don't sleep, you'll want to ensure your clients get a managed firewall offering with monitoring to catch threats 24/7/365.

STEP 3**Attack Reaches Endpoints**

Continuing along the path of our sample attack, your client has endpoints in the form of servers and workstations that are usually the most vulnerable points of their networks. Typically, a phishing email does the most damage by exploiting a vulnerability in an endpoint somewhere in the network.

SOLUTION**Endpoint Detection & Response (EDR)**

EDR platforms monitor traffic, detect problems and remediate some incidents. Managed EDR adds 24/7/365 monitoring and remediation by security analysts from a security operations center (SOC).

Through EDR, your clients' will get the benefits of:

- 24/7/365 protection
- Next-gen antivirus
- Improved system reliability and performance
- Reduced downtime
- Increased employee productivity

STEP 4**Data & Systems Are Breached**

Finally, the attack could be successful and result in your client losing data and system integrity.

SOLUTION**Data Backup & Disaster Recovery**

On-premises and cloud-based backups of your clients' data will shield them from some of the effects of ransomware, viruses and malware. They'll provide your clients with the means to recover their data and systems quickly and efficiently to mitigate the damage done by the attack.



Today's
cybersecurity
solutions are
affordable,
especially
considering
the average
cost of a
data breach
in 2020 was
\$3.86 million.

Managed Services is the Only Way to Go

Implementing the solutions in our sample attack above is an excellent start for your clients, but it's not over once they've installed the tech. Security solutions need to be:

- Continuously monitored and maintained around the clock
- Properly configured to keep all systems up-to-date
- Managed by professionals that live-eat-and-breathe cybersecurity

Case in point: In 2019, [one of the largest breaches in history occurred](#) at Capital One Financial due to a misconfigured firewall. The breach exposed the personal information — including social security and bank account numbers — of more than 106 million people.

Don't Forget Cloud Apps

Cybersecurity solutions are applicable both on-premises, remote and work-from-home (WFH) locations, and cloud environments. Your clients' cloud resources, including third-party applications, need to be protected as if they're part of their own networks.

Take, for example, the Microsoft Office 365 suite of products [used by more than a million companies worldwide, 731,000 of which are right here in the United States.](#) Configuring and securing your clients' Microsoft Office 365 business accounts is vital to reducing risk, and joining forces with a Microsoft Certified Partner like TPx adds this all-important element to your clients' security.

PART 4:

Where Should Channel Partners Begin When Selling Cybersecurity?

IT and telecom agents have been selling complex technology like network access, data centers, phone systems and SaaS applications for years. Yet, cybersecurity solutions can seem like a different animal and have a reputation for being “complicated to sell” because of the engineering involved and potentially high stakes for getting it wrong. But selling security doesn’t have to be scary. MSPs like TPx can help you navigate it.

After you pick the right cybersecurity provider to team up with, use the following strategies to ease into cybersecurity sales:



Talk to Your Existing Customers.

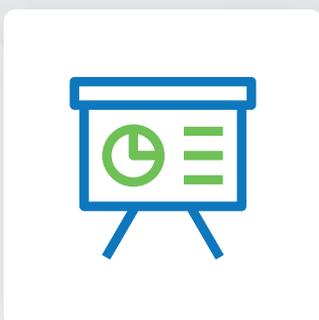
Start with sales and marketing campaigns to raise awareness with your customers that you have a cybersecurity practice. Remember, if your customers don’t have a solution already, they’re thinking about one. The time to move is now before a competitor poaches the opportunity from you.



Ask Customers How They're Handling Security.

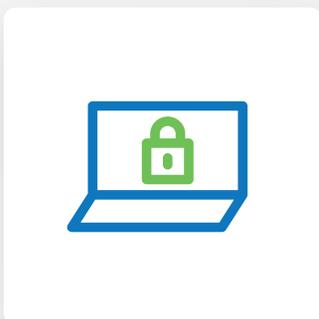
Open conversations with customers using simple, direct questions, like “How are you keeping your business safe from cyberattacks?”

- Most small and medium businesses (SMBs) will tell you they use antivirus software. Antivirus isn't enough and likely never was.
- Some will say they have firewalls, which also isn't enough.
- Many will admit that they're not sure.
- Larger customers with IT personnel may have more protections in place, though it's likely to be chronically outdated and not up to today's cybersecurity demands.



Ask Customers About Security Awareness Training.

Since most successful attacks start from phishing, ask your customers if they have a security awareness training program in place and engage them in a conversation that walks through the 4 Steps in the Path of a Cyberattack (see Part 3). This process will help your customers understand all their points of vulnerability, and you uncover the holes in their defenses.



Bring in Your Trusted Cybersecurity Provider.

From this point, now that you have a conversation going, it's time to bring in your trusted cybersecurity provider to handle the rest of the sales process, including scoping out the full opportunity and engineering a solution for your client's unique circumstances.

That's it! If your security provider can't or won't take the reins to engineer a solution and help you close the deal, find a better match.

PART 5:

Which Buyer Personas Should Channel Partners Target for Cybersecurity?

Buyer personas for your ideal decision-maker vary based on company size. In TPx's experience, there are three groups of decision-makers based on employee headcount:

< 100

Employees

A headcount of less than 100 usually means you're working with a senior business leader at the company (e.g., the business owner or a member of the C-suite). If there is an IT director, they are typically a generalist about all things IT. They fulfill multiple functions, wear lots of hats and spend most of their time putting out fires. They're not cybersecurity experts by any stretch; they are most likely system network admins who are out of their depth in managing cybersecurity on their own.

Note: SMBs may outsource their entire IT departments, so an existing third-party company may feel threatened by your presence. TPx has experience navigating these delicate relationships and defusing concerns over scope creep into another vendor's turf.

100 to 500

Employees

In this segment, the decision-maker usually is an IT manager with in-house staff. However, they're not necessarily security experts and are unlikely to have a security operations center (SOC). More often than not, they're open to – and even *welcome* – assistance with cybersecurity.

500+

Employees

For medium-to-large enterprise customers, the decision-maker typically is an educated cybersecurity expert or manager who reports up to a chief information security officer (CISO) or chief information officer (CIO). These larger organizations may run their own SOC. Their issue is the lack of the breadth and depth of staff to manage high volumes of inbound alerts around the clock. A vendor like TPx can help manage all those alerts, report to, and advise the client's team on issues that need attention.

Note: You may have noticed that we didn't segment by vertical. That's because cybersecurity solutions can benefit any company, and the need for them exists across all industries.

PART 6:

What Are Effective Ways to Start Sales Conversations About Cybersecurity?

The most important point to remember is that you don't have to be a security expert to sell cybersecurity. All you need to do to get started is ask a few questions about how your prospect's business is being secured today. Then record the answers to share with your cybersecurity provider.

Cybersecurity Sales Discovery Questions

What does your business do?

WHY ASK: Ensure you understand their business goals and pain points, especially if you're familiar with their vertical industry.

What does your current network infrastructure look like?

WHY ASK: You first want to understand what technology they are currently using and then look for potential gaps. If they don't mention a firewall or backup service, you have a clear opening to talk about that.

Do you have firewalls, switches, and/or wireless access points? Which vendors do you use?

WHY ASK: Finding out which vendors they are currently using may position you to talk about replacing systems from lesser-known vendors with better known, higher-ranked solutions from vendors that TPx supports.

How old are your existing network security systems?

WHY ASK: We replace our cell phones every year or two because the new ones are so much better. If a customer's equipment is more than five years old, talk to them about the need for aging infrastructure to be changed, just like cell phones, to avoid bottlenecks and performance issues.

Is this a new location?

WHY ASK: New locations require all new infrastructure. We can help with everything from SD-WAN, to firewalls, to network switches to Wi-Fi. We'll set it all up and manage it turnkey or hand the keys to the customer to manage themselves with assistance from us as needed.

Do you have support contracts on your infrastructure? When are they up for renewal?

WHY ASK: When a support contract is up for renewal, it's an excellent time to consider a hardware refresh. If your clients use TPx, we'll handle the license renewals going forward, so they don't have to worry about them. Also, our monthly payments are much easier for businesses to manage than significant, one-time expenses every year or so.

How much would a day of downtime cost you? Two days? More?

WHY ASK: This question helps you to communicate the economic costs of remediation versus prevention.

When is your firewall license up for renewal?

WHY ASK: If a license is up for renewal in the next year or so, it's time to talk about a hardware refresh for a better-performing firewall—usually for a similar cost to the license renewal.

Suppose they move to a managed firewall service with a provider like TPx. In that case, they won't need to worry about license renewals again and not have to front expensive purchases during renewal. We spread hardware and licensing costs over easy-to-manage, predictable monthly payments. (If a vendor increases license prices, the customer won't see the increase.)

Does your business have a security compliance need?

WHY ASK: Your clients may need to comply with Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), or National Institute of Standards and Technology (NIST) requirements. To help your clients stay in compliance, you can recommend networking and cybersecurity solutions in consultation with a trusted cybersecurity provider like TPx.

Have you ever experienced a hack, virus, malware, or other security incidents?

WHY ASK: Everyone likes to tell their story, so this question gets them talking and can get a stalled conversation going. This question also drives home the negative impacts of a cyberattack. Learning how they resolved issues (or didn't) can help you better understand the resources at their disposal.

Are you comfortable with your current security posture?

WHY ASK: This question helps you get at the gut feeling the prospect has about whether they could withstand an attack today. A "no" answer provides an entry point to set up a meeting with a provider like TPx.



When you're the first advisor talking to a client or prospect about cybersecurity, you may get the business for that reason alone.



When you're the first advisor talking to a client or prospect about cybersecurity, you may get the business for that reason alone. Your clients are already worried about cybersecurity but may not have gotten around to address it (or may not know where to start). Think of it like going to the dentist—you'll put it off over and over because more pressing things come up, but if the dentist calls, you're likely to act. The same principle applies to business situations—especially those involving new technology adoption.

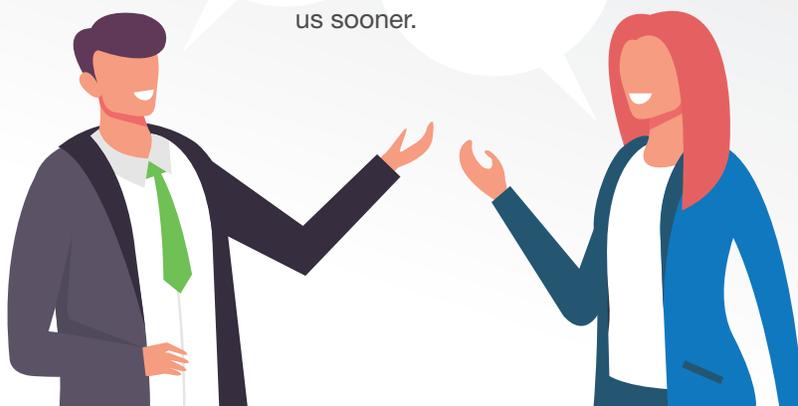
PART 7:

What Are Common Cybersecurity Sales Objections and Responses?

“I don’t see the value in a managed security service.”

Unless your prospect happens to work for a large enterprise with its own SOC, you can explain to them that they’ve been dodging bullets. It’s just a matter of time until they become a victim of an attack that causes significant financial and reputational damage with their customers (often due to legal disclosure requirements around breaches and potential data exposure).

The unfortunate reality is that the best sales tool is when a breach incident occurs. Plenty of TPx’s customers turned to us after they experienced a damaging breach and wished they’d engaged with us sooner.



“I already have cybersecurity today.”

“I have a guy.”

“I use XYZ tools.”

If prospects give you answers like these, don't worry! Here are some follow-up questions you can ask to keep the conversation going without being a security expert:

- How do you know that you're getting the right value from that service? Do you get reports? Do you have visibility into how the solutions are performing?
- Does your team have the right skill sets or breadth and depth of resources to address your requirements in a reasonable amount of time?
- How does your internal IT staff keep up with changes and requirements in the market?
- If you manage the technology in-house, when was the last time your staff logged into the security applications and monitored them?
- Do you know right now whether or not you can recover your data backups?
- Do you have a dedicated resource monitoring your network 24/7/365, or only 8 a.m. to 5 p.m. Monday through Friday?
- If you do have dedicated employees watching your network 24/7/365, how much does that cost you monthly?
- If you outsourced cybersecurity management (e.g., managing firewalls, monitoring the network, patch management, managed detection and response alerts and remediation, etc.), could your internal IT resources be better used for projects that build value for your organization?
- We often find companies think they're protected but discover they aren't when it's too late, and there's been a catastrophic breach. Do you want to make sure you're not in that situation?

PART 8:

How Can Channel Partners Differentiate Their Cybersecurity Offerings?

There are more than a thousand cybersecurity solutions on the market, but here's how you can set your solution apart:

Offer a single-source provider.

A managed services provider (MSP) with a broad swath of solutions in cybersecurity and networking, communications, and collaboration gives your customers access to support and expertise that spans their entire infrastructure, leading to a faster resolution to any issue that comes up.

Propose solutions that proactively remediate threats and attacks.

Companies don't need more alerts, alarms and notifications from applications that detect problems; they need fast and intelligent resolutions to those problems. Choose to work with a company that has remediation capabilities through holistic solutions like Managed Detection & Response (MDR).

Help future-proof client operations by aligning with a larger provider.

You can suggest a regional or local MSP, but they'll struggle to support solutions for your client with a nationwide presence or for those who plan to expand their businesses beyond their local markets. A larger provider like TPx already has the infrastructure in place to support large enterprises and can help your clients seamlessly scale as they grow.

Recommend a provider with the purchasing power to pass cost savings on to your customers.

In the MSP world, being smaller does not mean being cheaper. In fact, smaller MSPs may have to charge your customers more for cybersecurity because they don't have volume-based sourcing deals that larger MSPs can leverage to deliver cutting-edge services affordably. Connecting your clients with a larger MSP not only provides scalability but cost savings as well, delivering wins on both fronts.

PART 9:

How Can Channel Partners Uncover Prospective Cybersecurity Clients?



Center the Conversation on Benefits

The most effective method of prospecting and selling cybersecurity is by centering the conversation on the benefits for the business, not the technology solutions themselves. The benefits to customers include:

- Protecting their business better
- Gaining increased visibility and control around what is happening on their network
- Minimizing downtime with 24/7 support
- Boosting productivity
- Saving time and money via outsourcing
- Ensuring compliance with regulations like PCI, HIPAA, NIST and more

Tweak Your Message for IT Decision Makers

If you're having a sales discussion with an IT department or executive, focus on IT-related pain points such as:

- How IT resources get often caught up in fighting fires instead of advancing the business
- How your solution complements and supports the company's IT department (it doesn't displace people)
- How managed security solutions can free up IT teams in their personal lives, with benefits like taking vacations without worrying about incidents that occur while they're away
- Demonstrating the costs of outsourcing versus building and staffing round-the-clock security teams
- The difficulty in finding and keeping skilled talent
- The costs of training existing IT employees on cybersecurity solutions



PART 10:

What Pitfalls Should Channel Partners Watch Out for When Selling Cybersecurity?

The top three pitfalls to avoid when selling cybersecurity services include:

PITFALL 1: Focusing on Tech, Not Value

Focusing on the technology itself instead of results is a surefire way for your sales conversations to become lost in translation. Let your cybersecurity provider handle the technical discussions.

PITFALL 2: Quoting Prices Upfront When Comparing Inequivalent Solutions

Right out of the gate, prospects may ask you questions like, “Can you manage my endpoints? How much is it? I’m looking at Company X right now for \$8.99 per endpoint a month. How much do you charge?”

That’s a challenging question to answer because of varying service levels among MSPs. Company X, in this example, only quotes the cost of its software. Management of that software with incident response and proactive service cost extra.

Without understanding the competitive offer, you could waste time chasing an unrealistic price point for a fully managed service offered by TPx that may have higher service levels and be less expensive with all inputs factored in.

Since it can be challenging to recover from a perceived upfront pricing disparity, it’s essential to reframe customer expectations right away.

Instead of quoting a price, commit to a bill analysis. “We’re always competitive, but I can’t answer that exact question until we analyze your bill. Usually, fees in that range cover only part of what you need. We’ll run an analysis and give you an apples-to-apples comparison.”

PITFALL 3: Being Viewed as a Replacement to Existing IT Departments

If your prospect has an existing IT department or is outsourcing IT to a third-party vendor, you may be viewed as a threat to continued salaries and retainer contracts. As discussed earlier, it’s vital to frame your presence as supporting – not replacing – IT personnel.

PART 11:

Should Channel Partners Insource or Outsource Cybersecurity?

The debate over do-it-yourself (DIY) or outsourced business models apply to any service offering. Still, it's especially relevant in managed cybersecurity, thanks to the highly specialized expertise and costly infrastructure required to do the job well.

Consider these questions before developing home-grown solutions:

- **Do you have the capital to build out a SOC?**

A SOC is a seven-figure investment. One of the benefits of being an agent in the first place is that you're selling someone else's technology and letting them take on the overhead required to support those solutions.

- **Can you hire the right security experts?**

Do you know where to find experts? Can you afford them? Cybersecurity is a specialized field, with shrinking talent pools and soaring compensation to match. Can you hire enough experts to meet 24/7 demand?

- **Can you afford to staff 24/7/365?**

Your clients' networks are most vulnerable at night and on the weekends when their staffs are off the premises, not working, and unlikely to notice breaches. To provide adequate protection, you'll need to pay experts to spend their nights and weekends at your SOC, which doesn't come cheap. And if you can't afford it, can you realistically sell a "9/5/261" managed security service?

- **Can you keep personnel?**

Every industry has turnover, but as a small fledgling security provider, what do you do when one of your hard-to-source network engineers leaves, and suddenly your service capacity suffers (perhaps for months) while you scramble to find a competent replacement?

The bottom line is that scaling a DIY model for an agent partner or small MSP is extraordinarily difficult to achieve. Teaming up with an established cybersecurity provider like TPx provides scale and takes away the financial burden and operational headaches so you can focus on taking care of your customers and growing your business.

PART 12:

What Should Channel Partners Look for in a Cybersecurity Provider?

To pick the right MSP, you'll need to assess the breadth and depth of their resources, especially around personnel. **Key questions to ask before trusting an MSP with your customers include:**

- How deep and current is their knowledge?
- How long have they been in business?
- How long does it take them to solve for issues? Can they solve a problem in 5 minutes that would have taken a less experienced provider 30 minutes?
- What tools and solutions to your client's security requirements do they have available? Do they have a wide array of technology to address security at every point in your customer's network? Do they understand how to keep your client compliant with industry- and vertical-specific regulations?
- Are they large enough to deliver reliable 24/7/365 support?
- Are their agreements and contract terms reasonable?
- If they need to troubleshoot an issue, do they have remote desktop access as part of their infrastructure, or do they need to dispatch an engineer to the client location?
- What compensation do they offer? What are the commission rates? What MRR can you expect on each deal? Do they offer SPIFFs, and if so, do they pay well, and are they realistic to achieve?
- Will they bring in resources to help you sell? Do they offer dedicated personnel who engineer solutions and co-sell with you to get your deals across the finish line?

PART 13:

Why Should Channel Partners Choose TPx as Their Cybersecurity Vendor?

When you join forces with TPx as your go-to cybersecurity provider, you can leverage TPx subject matter experts in the sales process to create the right solution for your clients, including:

- Product Specialists
- Solution Architects
- Managed Services Evangelists
- Network and Security Engineers

We'll take care of all the technical questions and deep dive into solving your clients' needs. All we ask is that you make the introduction; we'll handle the rest — making you look good to your customers throughout the process.

Post-implementation, your clients will have access to these same talent resources, monitoring their network 24/7/365 from our cybersecurity operations centers.

Plus, TPx is a well-known leader in the channel, delivering industry-leading support, commissions and SPIFFs.



Team Up The Way You Want

TPx doesn't offer a one-size-fits-all partner program. You can team up with TPx in three different ways to meet your business goals:



Become an Independent Agent

In this performance-based program, you'll earn generous monthly recurring commissions, with your earning capacity only limited by how fast you sell.



Work with a Master Agency

Take advantage of a master agent's expertise, resources, training and tools. Negotiate terms directly with your preferred master agent. TPx works with all major masters, including Avant, TBI, Intelisys, Sandler Partners, Telarus, MicroCorp, AppSmart and more.



Provide Customer Referrals

Simply refer business to us and let us do the work. You make money for the referral and leave all the heavy lifting to us. Choose from either upfront or residual-based commission programs.

Why Team Up with TPx

Dedicated Channel Team

TPx's channel team will help you design, price and present the best solution to your customers. Our channel sales coordinators will take care of all the paperwork and order entry. And our agent help desk provides the support you need for anything from customers to commissions.

Guaranteed Customer Satisfaction

TPx provides your customers with an industry-best 100% service level agreement (SLA).

Sales Training & Enablement Tools

In addition to getting access to our technical experts pre- and post-sale, we provide onboarding training, sales training and product training for all channel partners. Plus, we provide sales enablement tools and collateral, including co-branded datasheets, presentations and sales scripts.

Commissions & Sales

We offer one of the most aggressive and competitive compensation packages in the IT and telecom industry. Throughout the year, we offer special SPIFFs and sales contests, increasing your compensation and opportunities to earn rewards like trips to top destinations.

Why Choose TPx for Your Clients

At [TPx](#), we have the products, services, experience and certification to keep your clients' networks safe and running smoothly:



Single-source Provider

We solve the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella.



Buying Power & Cost Savings

We have the IT solutions, staff and experience to deliver cybersecurity effectively and within budget. We use our buying power to pass on the savings to your clients.



Certified & Vetted

We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, AWS, SMC and more.



Digital Transformation

We modernize your clients' IT and communications while minimizing their risk from cyber threats.



Enterprise-Class & White-Glove Support

With 23,000 clients in 50,000+ locations, we're big enough to get the job done and small enough to be agile.



Customized Solutions

Your clients can mix and match our portfolio of managed security, IT and communications solutions to best suit their needs.

TPx is Your One-stop Shop for Managed Security Services

Managed Detection & Response (MDR)

Discover, prevent and recover from cyber threats faster. TPx's MDR helps you identify more threats, reduce attack dwell time, and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.

Endpoint Management & Security

TPx helps keep your clients' servers and workstations healthy, secure and performing optimally. Our endpoint security service leverages Remote Monitoring and Management (RMM), Patch Management and Security. We provide 24/7/365 service with expert support and security analysts.

Next-Generation Firewall (NGFW)

The firewall is the first line of defense in protecting your clients from Internet-based threats. Firewalls block today's advanced threats while also providing secure access, visibility and control to help your clients be more productive.

Backup & Disaster Recovery (BDR)

We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet your clients' recovery objectives.

Unified Threat Management (UTM)

TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.

Email Security

Whether it's protecting against email-based cyberattacks like phishing or ensuring sensitive information doesn't fall into the wrong hands, we can help your clients navigate the email security challenge.

DNS Protection

We protect systems and users from malicious websites using leading DNS protection software. Windows devices are protected on the corporate network and while traveling. Network-based DNS protection covers BYOD, guest wireless, and non-Windows devices to deliver comprehensive DNS security and reduce your clients' risk of attack.

Security Awareness Training

Users are your clients' last line of defense. The more they know, the less prone they are to fall victim to a phishing scam or other security incident. Our service includes monthly phishing simulations and Security Awareness Training courses with automated reporting to track your clients' results.



Interested in Becoming a Channel Partner?

[CONTACT US TODAY](#)