Channel Partner Cheatsheet

TPX

TPx Overview

- Over 18,000 customers in 49k+ locations nationwide
- Connect & Protect: One-stop shop for communication, collaboration, and managed IT services
- Large enough to get the job done but agile enough to get it done on time
- More than two decades of industry-leading customer service focus
- TPx offers fully managed services that can offload time consuming tasks from IT departments, freeing them up to do other things. Co-management is available for organizations that want to be more hands-on.
- Managed Services solutions use top tier products selected for their features, security, and the stability of the provider

Target Audiences

- CIO, CTO, CFO, Director/Manager of IT, Operations Manager, CEO of small or mid-size business, Office Manager, CISO & Compliance Officer for security services
- Verticals: Healthcare, followed by banking/finance, followed by education, manufacturing, retail, legal/law
- 50-1000 users. Smaller may not be ready to spend and larger may require more hands on / in-house
- Customers that have demonstrated a willingness to invest in technology and security for their business, and are willing to pay for it are the best targets in general

Discovery Questions

Generic Questions

- Can you tell me about your business?
- What is the technology you use today?
- How do you see the growth of your company and the use of technology in the future?
- Do you have an internal IT department, or do you use an MSP?
- What do you like or not like about your existing support?
- Do you have any pending technology projects or initiatives?
- Do you have any pain points or chronic technology issues?
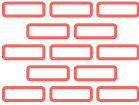
Security Questions

- Do you have a security program that provides a mature security posture?
- How many people work in Information technology? How many in Information Security?
- Have your information security solutions evolved with the move to work-from-home?
- Do you have in-house security or do you outsource? Are you satisfied with your current team/provider?
- Are you worried about cybersecurity?
- Have you read about [security news/article]?
- How does your MSP stay current of new and evolving threats?

Key Resources

Check out tpx.com/channel

- Managed Datasheets (on product pages on tpx.com)
- *YouTube Playlist*
- *Customer Testimonials*
- *Infographics*

Service	Description	Elevator	Features/Benefits	Vendors	Prospect Questions
UCx with Webex	Unified Communications	UCx with Webex transforms the way employees work with a secure, single solution that includes video meetings, whiteboarding, messaging, file sharing, built-in call control functionality and more to increase employee productivity and streamline teamwork.	■ Collaboration: Enables everyone to see/share information to work productively ■ Messaging: Exchange secure messages/share files inside/outside your organization ■ Meetings: Host meetings from anywhere with audio, video and screen sharing ■ Enterprise VoIP: Manage calls, any device, anywhere	Cisco	■ How do you leverage your phone service to grow and keep customers? What other channels do you use to communicate with customers or internal teams? ■ Where do you fall on the UC spectrum? Own it or monthly subscription? Desk phone, softphone, mobility or BYOD? ■ Is your service voice only or does it include apps for presence, chat and click to call? Does it include video meetings? What is max attendee capacity? Does it include team collaboration in the form of persistent workspaces? If not included, what 3rd party app are your teams using? ■ How do you make and receive calls outside of the office and still appear to your clients that you are calling from your business line? ■ What type of tools are your teams using to efficiently collaborate on projects together? ■ How many pps make up your current business communications solution? ■ How secure and reliable is your current business communications solution? ■ Can you tell me about what your business priorities and challenges are when it comes to your phone system requirements? ■ How many CRMs are in use? ■ If you could have whatever you wanted out of a phone system, what are the top features that would allow your teams to work more efficiently?
Managed SD-WAN	Monitoring and management of SD-WAN network	Better network performance, more agility and lower cost	■ Flexible WAN options: WAN and Hybrid WAN ■ WAN optimization ■ Bring your own bandwidth with QoS ■ Application aware customer profiles ■ Active/active continuity including 4G LTE	VMWare Silver Peak Cisco Meraki Fortinet	■ Can you provide a summary of your network topology (HQ, data centers, remote sites, etc.)? What are your requirements for remote user access? ■ Do you have visibility into how your applications are performing? ■ Do you know how your bandwidth is being used? ■ Are your circuits proactively monitored so you are notified when they go down? ■ Do you have any performance or quality issues with your critical applications (like voice applications)? ■ Do you have MPLS in your network? ■ Do you have an existing contract for your network?

Service	Description	Elevator	Features/Benefits	Vendors	Prospect Questions
Managed Firewalls	Monitoring and management of firewalls	Fully customized perimeter security with next-gen firewall	■ Monitoring/management of Next Gen Firewalls ■ Best-in-breed hardware and UTM (Unified Threat Management) features ■ 24/7/365 security team in our SOC will configure, deploy, monitor and manage it for you ■ Comprehensive logging and detailed reporting tools provide exceptional network visibility ■ Managed Detection and Response (MDR) ■ Deep Packet Inspection (DPI)	Fortinet Cisco Meraki	■ What are you using for a firewall now and how old is it? ■ When is your license up for renewal? ■ Are you running UTM features like anti-virus, application control IDS/IPS? ■ How long do you currently maintain your firewall logs? ■ Do you integrate your current firewall with active directory? ■ How often do you backup your configs? ■ Have you ever had a computer get a virus? ■ What are the top applications on your network? ■ How much time do employees spend on social media or streaming? ■ When was your last vulnerability assessment? ■ How are you identifying breaches? ■ Would you know if you are being compromised right now? ■ What is your biggest security concern and is your spending and expertise properly allocated to address it?
Managed Networks	Monitoring and management of core network devices	Remove the burden of monitoring and managing critical LAN infrastructure	■ Monitoring/management of SD-WAN, firewall, switches and Wi-Fi access points ■ Increased performance and productivity with best-in-class solutions ■ Hardware assurance and firmware upgrades ■ Experienced network specialists available 24/7	Cisco Meraki	■ What does your current network infrastructure look like? ■ Do you have times when you notice your network/internet connection is slow? ■ What are the most common apps you run on your network? ■ Have you thought about what might happen if you ever had a serious breach? ■ How old is your current network hardware? ■ How often are you updating the firmware on your network equipment? ■ Would you like to enable your employees to be more mobile in the office?

Service	Description	Elevator	Features/Benefits	Vendors	Prospect Questions
Managed Endpoints	Performance and security solutions for server and workstation environments	Healthy, secure and well-performing IT systems	■ Automated patch management across all servers and workstations ■ 24/7 monitoring/alerting ■ Asset management and scheduled reporting ■ Advanced, integrated anti-malware and anti-virus technology ■ Cost reduction and peak performance with automation and extensive patch library ■ Managed Detection and Response (MDR) ■ Inbox Detection and Response (IDR) ■ Security Awareness Training (SAT)	Datto RMM Webroot Secure Anywhere GoSecure Infosec Institute InfoSecIQ Webroot DNS Protection	■ Are you concerned about the security of your network and exposure to ransomware and other security threats? ■ What tools and processes do you use to ensure servers and workstations are being patched? ■ How do you validate that patches have been completed properly and in a timely manner? ■ What anti-virus software are you using? ■ Is it "next-generation anti-virus"? ■ What EDR software and Managed Detection and Response (MDR) services are you using to proactively identify, block, and recover from advanced cyberattacks? ■ Who is maintaining and administering all your management and security tools to ensure they continue to provide optimal value? ■ What do you have in place to minimize phishing?
Managed Backups & Disaster Recovery	Data backup and disaster recovery	Fast local backups/restores using best-in-class hybrid BDR technology	■ Managed backup and disaster recovery (in the cloud and on-premises) ■ 1-year and Infinite Cloud backup retention options ■ Recover to virtualized servers on backup appliance or in the cloud ■ Bare metal and file-level restore capabilities ■ Ransomware scanning of backups	Datto	■ How long can you afford to be down before getting your systems and data back up and running? ■ How much data can you afford to lose in the event of a failure? ■ What is your current backup solution? ■ Is someone diligently reviewing your backup jobs for success? ■ Is someone consistently testing data recovery? ■ Are you concerned about ransomware and other security threats?
Managed Datacenters	Colocation for all of your IT infrastructure	Efficient way to ensure IT systems, apps and data are available 24/7/365	■ 24/7/365 professional support and access including remote hands ■ Multiple redundancy layers for 100% up time ■ Access to high capacity Internet and MPLS networking		■ Do you have all your IT in-house or do you outsource? ■ Does your business have compliance requirements? ■ Will data transfer requirements demand greater bandwidth? ■ Do you want to lower datacenter expenses? ■ Have your own datacenter? Looking to move to a virtualized environment? ■ Are you running eCommerce applications on your network? ■ Do you have workplace mobility requirements? Do you run any internal business critical applications?

Service	Description	Elevator	Features/Benefits	Vendors	Prospect Questions
Managed Microsoft 365	Microsoft 365 services and support	More productive, collaborative and secure teams	■ Microsoft 365 managed and billed by TPx ■ Administrative technical support and escalations to Microsoft ■ Unlimited cloud backups of Microsoft 365's Exchange, OneDrive, and SharePoint data ■ Managed portal administration of Microsoft 365 Tenant		■ Do you have all your IT in-house or do you outsource? ■ Does your business have compliance requirements? ■ Will data transfer requirements demand greater bandwidth? ■ Are you looking to lower your datacenter expenses? ■ Do you have your own datacenter? ■ Are you looking to move to a virtualized environment? ■ Is security a concern when it comes to your data? ■ Are you running eCommerce applications on your network? ■ Do you have any workplace mobility requirements? ■ Do you anticipate your company growing or expanding? ■ Do you run any internal business critical applications?
Security Advisory Services	■ Cybersecurity Gap Assessment ■ Network Vulnerability & Penetration Scanning ■ Network Security Assessment ■ Wireless Security Assessment ■ Ransomware Readiness Assessment ■ Customized Advisory Assessment	Comprehensive security consulting services to help improve your security posture and protect your business	■ Target high-impact areas for reducing risk ■ Identify gaps in your monitoring and reporting capabilities ■ Fully document your network assets and architecture ■ Secure your WFH and remote access infrastructure ■ Develop roadmap for corporate security initiatives ■ Identify exploitable vulnerabilities in your infrastructure ■ Uncover asset misconfigurations that could lead to poor performance or data loss ■ Defensible position to ELT/Board when asked "are we protected"? ■ Analytical approach to requesting & spending security budget		■ When was the last time you had a security audit? ■ When did you perform your last vulnerability scan? ■ How do you prioritize your patching and upgrade activities? ■ How often does it take you to patch identified vulnerabilities? ■ How protected do you feel against ransomware attacks? ■ Do you know when your network devices are scheduled to go End-of-Support/End-of-Life? ■ When was the last time you performed a scan of open ports on your outward-facing assets? ■ Do you track successful/unsuccessful login attempts to your systems? ■ How do you prevent unauthorized users from accessing your Wi-Fi network? ■ What wireless encryption protocols do you use? ■ Do you have a documented BYOD policy? ■ Do you have an Incident Response plan to follow in case of a breach? ■ How do you make sure only authorized employees access your most sensitive data? ■ Do you need to demonstrate and prove compliance (PCI, HIPAA, FISMA, CMMC, etc.)? ■ Are your security standards, processes, and procedures documented? ■ Are your backup and disaster recovery procedures documented? ■ Is security documentation up to date? Distributed to appropriate personnel?

Solutions Architects

Service	Questions

Managed SD-WAN

General

- Does client have 3rd party apps?
- Does client require custom routing?
- Does client need SNMP. If so, what is the IP address?
- Does client need Netflow. If so, what is the IP address?
- Will client self-manage?
- Any special notes?

Per location

- What will total Internet bandwidth be at that location?
- Does client need bandwidth Boost (Y/N)?
- Does client need 1 to 1 NATs?
- Does client need IPv6?
- Does client need multicast?
- If client using 3rd party MPLS, do they have BGP with that provider?
- Does client have BGP, EIGRP, or RIP towards LAN?
- Is inbound failover needed for NTA/PAT?
- Any circuits traditional MPLS circuits (private IPs)?
- Does client need multiple VRFs / segmentation?
- Does client need public IPs?
- Is a circuit available? If yes, is it provided by TPx and if not, who is the provider?
- Does client need Boost?
- Does client need a rack?
- Is device in parallel?
- Does client want TPx to manage OTT circuit?
- Which transports used (DIA, HSIA, OTT, TPx 4G, TPx DS1, TPx EoX, TPx OneNet, MPLS)?
- What products options does client need (DIA, SmartVoice, Private Segment, UCx, High Availability, Public IPs)?
- Override management IP? If so, what is the IP address?

Does client need any of the following (if so, collect details for each):

- VLAN interfaces
- Interface, port type, default IP & subnet, VLAN, VLAN native (Y/N), Segment (1), Advertise (Y/N)
- WAN interfaces
- Interface, IP & subnet, gateway, VLAN, addressing type (static, DHCP)
- DHCP
- VLAN, type, pool/relay agent, DNS, options, actions
- NAT (1:1)
- Name, outside IP, Interface, inside IP, outbound traffic (Y/N), protocol (GRE, ICMP, TCP, UDP), remote IP & subnet, port range, segment (Global, Internet, Voice)
- Port forwards
- Name, protocol (TCP, UDP), Interface, port, LAN IP, LAN port, remote IP & subnet, segment (1)
- Static routes
- Source & subnet, destination, segment (1)
- Dynamic OSPF routing
- Area, interface, notes, segment (1)
- Dynamic BGP routing
- Local as, remote as, local IP, remote IP, notes, segment (1)
- Firewall rules
- Deny/allow, name, source IP & subnet, destination IP & subnet, segment (1)
- QoS
- Application, queue (high, med, low), segment (1) Segments: Global, Internet, Voice

Product SKUs

- East coast only: Managed WAN Bundle
- Central & west coast: Managed WAN

Service | Questions

Managed Firewalls

General

- Does client need to self-manage firewall?
- Any special notes?

For each location that is to get a firewall:

- Is a circuit available? If yes, is it provided by TPx and if not, who is the provider?
- What will the total Internet bandwidth be at that location?
- How many users are at that location?
- How many remote VPN users will there be?
- Do they have an existing firewall and if so, what brand is it?
- Where is the firewall to be physically located (TPx datacenter, client site, other)?
- Does client require Managed WAN or OneNet MPLS, if so, how many sites?

Does client have Wireless services (Y/N)?

- If yes, will TPx manage the current WiFi (Y/N)? If yes, are the current Access Points FortiAP's and what models are they (Y/N)?
- If no, but client needs WIFI, how many FortiAP wireless access points (WAP) will they require? (note: TPx does not conduct WIFI surveys, run cable to or install WAPs. TPx will configure wireless profiles and manage WAPs from the firewall only. Please be prepared to adjust and/or switch configurations as needed).

Does client need any of the following:

- Antivirus (Y/N)?
- Antispam (Y/N)?
- Web Filtering (Y/N)?
- IDS/IPS - Intrusion Detection/Prevention (Y/N)?
- Application Monitoring (Y/N)?
- High Availability (Y/N)? (Additional hardware costs apply)
- Should firewall use network directory for user authentication? If so, should it use FortiGate Single Sign On (FSSO)?
- Site to Site VPNs (Y/N)?

Does client need any of the following (if so, collect details for each):

- External Interfaces
- Public DHCP (Y/N)?
- Priority
- IP address and subnet
- Default gateway
- Description
- Alias
- Internal Interfaces
- Priority
- IP address and subnet
- Default gateway
- Description
- Alias
- Guest network (Y/N)?
- DHCP
- Interface
- DHCP range

Product SKUs

- East coast only: Managed Firewall Bundle
- Central & west coast: Managed Firewall

Managed Endpoints	

Initial Qualification for Servers

- Does client have Windows based servers (Y/N)?

- Does client need TPx to Administer and/or troubleshoot and repair their servers (Y/N)? If yes, does client want TPx to administer and/or troubleshoot and repair their servers (Y/N)?

- Does client want TPx to deploy and manage our next generation antivirus software (Y/N)?

Technical Qualification for Servers

- What server Operating Systems are in use (2003 or older, 2008, 2008 R2, 2012, 2012 R2, 2016, or unknown)?

- How many Windows servers are to be supported by TPx?

- Does client need TPx to support any of these applications on their servers: MS Exchange (Email), MS RDS/TSE (Remote Access), MS SQL (Database), other application (specify)?

- How many Windows servers running these applications?

- Are servers covered by a hardware support contract (Y/N)?

- Has SA explained requirement for all servers to be covered under a hardware support agreement (Y/N)?

Technical Qualification for Workstations

- Does client have Windows based workstations (Y/N)?

- Does client need TPx to administer and/or troubleshoot and Repair their workstations (Y/N)? If yes:

- Does client want TPx to deploy and manage our next generation antivirus software (Y/N)?

- Does the Client need service on Apple Workstations (Y/N)? If yes, How many Apple workstations are to be supported by TPx? (note: support is currently limited to best effort remote control troubleshooting and configuration assistance)

- Does client need service on Linux workstations (Y/N)? (note: TPx supports SuSE Linux Enterprise 11 and 12, Red Hat Enterprise 6 and 7, and Ubuntu 12.04 LTS and 16.04 LTS)

Technical Qualification for Workstations

- What versions of Windows are currently installed?

- How many Windows workstation are to be supported by TPx?

- Does client need 3rd party application support (Y/N)? If yes, then provide as much info as possible: (ideally, application name, version, manufacturer, and contact details)
Note: customer must have an active vendor support contract for 3rd party application support

- Are workstations covered by a hardware support contract (Y/N)?

Product SKUs

- All locations: Managed Endpoints

Service	Questions	Service	Questions
Managed Datacenters	■ Does datacenter need to be in client's geographic area (Y/N)? If so, how far will it encompass (miles)?	**Managed Networks**	Engineering questions are the same as for Managed WAN and Managed Firewalls.

Managed Datacenters

- Does datacenter need to be in client's geographic area (Y/N)? If so, how far will it encompass (miles)?
- Is client looking for a manned site (Y/N)?
- Are video security cameras important to client (Y/N)?
- Does client need sites with UPS or will they bring their own?
- Does client require a cage? If yes, what size (10x10, 10x20, 10x30, or 10x40)?
- How many Us will client need? (note: a cabinet is 42 Us)
- Does client anticipate needing another cabinet within the next 12 months (Y/N)?
- Does client have their own router/firewall (Y/N)?
- Would client like to review our selection of managed Cisco and/or Fortinet firewalls (Y/N)?
- What connectivity does client require (TPx/3rd party)?
- Does client require layer 1 or 2 redundancy for the internet connection (Y/N)?
- How many IPs does client need? (note: only applies to TPx connectivity)
- How much bandwidth does client need? (note: for TPx circuit, specify Mbps or Gbps, for 3rd party circuit, specify copper <300 Mbps, copper > 300 Mbps, or fiber)
- Does client require meter power (Y/N)?
- What voltage/amperage does client need (120/20, 120/30, 208/20, 208/30)?
- Does client need DC power (Y/N)?
- Is client a financial or medical business (Y/N)?
- Does client need an SSAE audited location (Y/N)?
- How many remote hands/month does client anticipate requesting?
- Will client need use of a crash cart with monitor, keyboard, and mouse (Y/N)?
- How many access badges will client need for their staff?
- Will client need to temporarily store any equipment (Y/N)?
- Any special notes?

Product SKUs

- East coast only: Managed Firewall Bundle
- Central & west coast: Managed Firewall

Managed Networks

Engineering questions are the same as for Managed WAN and Managed Firewalls.

For MS Series (for each location):

- Does client need Power over Ethernet (POE)?
- How many ports does client need?

For MS Series (for each location):

- All locations: Managed Networks

Service	Questions	Service	Questions
Managed Backups	▪ What service level is client interested in (Core/Optimum)?	**Managed Microsoft 365**	▪ Is client currently using Office 365 (Y/N)?
	n Is client interested in Managed Endpoints (Y/N)?		n What Office 365 licensing plan does client want (business, enterprise, or non-profit)? (note: TPx currently can't sell government or education licenses, but we can still offer Managed for O365 – The client would have to purchase licenses directly from Microsoft)
	n How long should backups be retained (1 year or infinite)?		
	For each location that is to get a backup device:		
	▪ How many devices does client want backed up?		n How many Office 365 users does client have or need?
	n What is the total used space on all devices to be backed up (in TB)?		n Are all production email users already on Office 365 (Y/N)?
	n What is the anticipated annual storage growth rate?		n Will TPx administer client's Office 365 environment (Y/N)?
	n How many devices does client estimate will be added over the next 18 months?		n Does client need to be able to recover deleted files and emails (Y/N)? If so, what backup retention do they need (Indefinite, 1 yr, 2 yrs, 3 yrs, 4 yrs, 5 yrs, or opt-out)?
	n Does client want to use the local server virtualization feature?		
	n Does client want encryption for the data stored on the local backup appliance?		For MS Series (for each location):
	n Will the backup appliance be rack mounted?		▪ All locations: Managed for Office 365
	n Does client have 10 GB Ethernet ports available to connect the backup appliance to their LAN?		
	n What is the Internet upload speed at this location?		
	n Is client able to provide a device inventory?		
	n Any special notes?		
	Product SKUs		
	▪ All locations: Managed Backup		

Service   Feature Matrix

UCx with Webex

UCX WITH WEBEX

Webex Collaboration Features

Description	UCx with Webex			
	Softphone	Business	Pro	Elite
	Softphone only	Add chat, join meetings	Complete collaboration[1]	Highest level collaboration[2]
Voice and video conferencing		■	■	■
Call escalation to meeting		Spaces	Spaces	Spaces
Space participants		5000	5000	5000
Space meeting capacity		25	100	300
Space meeting recording				■
PMR[3] capacity		n/a	100	1000
Call in audio #		Spaces	■	■
Desktop & app screen sharing		■	■	■
File sharing		Spaces	Spaces	Spaces
Full screen view		■	■	■
Gallery view		■	■	■
Join as meeting participant		■	■	■
Messaging with Teams/Spaces		■	■	■
Multi-party chat		■	■	■
Scheduled meetings		■	■	■
Presence		■	■	■
Whiteboarding/annotation		Spaces	Spaces	Spaces
User web portal		■	■	■
Virtual desktop (VDI) support		■	■	■
Virtual backgrounds		■	■	■
Web guest experience			■	■
Calendar integration (Outlook/Google)			■	■

Enhanced Collaboration Features

	UCx with Webex			
	Softphone	Business	Pro	Elite
Floor control				■
Lock meeting				■
Presenter/password protection				PMR
Recordings (cloud)				PMR
Remote desktop control				PMR
Breakout rooms				PMR
Transcriptions				PMR
Message storage		2GB	5GB	10GB
Cloud recording storage (PMR)				10GB
Years stored		3	3	5

Enterprise VoIP Group Calling

	Softphone	Business	Pro	Elite
Barge-in exempt	■	■	■	■
Call waiting	■	■	■	■
Caller ID	■	■	■	■
Caller ID delivery blocking	■	■	■	■
Call park/pickup	■	■	■	■
Historical reporting	■	■	■	■
Intercept user	■	■	■	■
Music on hold	■	■	■	■

[1] Join and host meetings
[2] Host large groups or advanced meetings
[3] Personal meeting room

■ Feature available in both Spaces & PMR
Spaces Feature only available in Space Meetings
PMR Feature only available in Personal Meeting Room

TPX

UCx with Webex

UCX WITH WEBEX

Enterprise VoIP Calling Features	UCx with Webex			
	Softphone	Business	Pro	Elite
3 Way calling	■	■	■	■
Anonymous call rejection	■	■	■	■
Anywhere	■	■	■	■
Call forward always, busy, no answer, selective	■	■	■	■
Call forward not reachable	■	■	■	■
Call history	■	■	■	■
Call hold	■	■	■	■
Call notify	■	■	■	■
Call pull	■	■	■	■
Call transfer	■	■	■	■
Do not disturb	■	■	■	■
Hoteling login/logout	■	■	■	■
Last call return	■	■	■	■
Last number redial	■	■	■	■
N-way calling	■	■	■	■
Personal phone directory	■	■	■	■
Sequential ring	■	■	■	■
Simultaneous ring	■	■	■	■
SMS	■	■	■	■
Speed dial	■	■	■	■
Video calling	■	■	■	■
Voicemail	■	■	■	■
Voicemail to email	■	■	■	■

Supported Phone Features	UCx with Webex			
	Softphone	Business	Pro	Elite
Busy lamp field		■	■	■
Push to talk		■	■	■
Shared call appearance		■	■	■

Service

**Managed
SD-WAN**

Feature Matrix

Service Availability

24/7/365 Support	■

Administrative Services

Multi Services Router (MSR) Monitoring & Alerting	■
VPN Tunnels Monitoring & Alerting	■
CPC/OTT Monitoring and Alerting	■
Hardware Assurance/Equipment RMA	■
Configuration Management	■

Features

Compliance	■
Physical and Virtual MSR options	■
Static routes or dynamic routing protocols such as BGP and OSPF supported	■
Orchestrator Access	■
Multiple circuit design options	■
MPLS Integration	■
Routing Policies	■
Two-Factor Authentication	■
Third Party Vendor Support	■
High Availability	■
Clustering	■
TPx 4G Connectivity	■
Inbound Internet Failover Public IPs	■
Nonstandard Managed WAN IPSec Tunnels	■
Boost	■

Installation Options

Remote Installation	■
Professional Installation	■
Expedited Implementation	■

Service

**Managed
Networks**

Feature Matrix

Available Features	Core	Optimum
24/7/375 Support	■	■
24x7 Monitoring		■
Configuration Management	+	■
Configuration Backup	■	■
Firmware Research and Upgrades	+	■
Hardware Assurance/Equipment	■	■
Troubleshooting	+	■
Product Licensing	■	■
Administrative Portal	■	■
Device Reporting	+	
DASH Portal	■	■

Service

**Managed
Datacenter**

Feature Matrix

Technology Deployed

24/7/365 Datacenter Management	■
Guaranteed 99.99% Network Availability	■
Security and Compliance	■
Geographic Redundancy	■
Facility Redundancy	■
Customer Workspace Available	■
Multiple Space Options	■

■ Included – monthly cost
☐ Available – monthly cost
+ Available – time & materials cost

Managed Firewall

Feature Matrix

Service Features	Core	Optimum	Secure
24/7/365 Support Center	■	■	■
Base Administrative Features			
PCI and HIPAA Compliance	■	■	■
24/7 Firewall Monitoring		■	■
(Product) Licensing	■	■	■
Mgmt of Manufacturer Support/ Response	+	■	■
Hardware Assurance/Equipment RMA	+	■	■
Configuration Management	+	■	■
Firewall Configuration Backup & Storage		■	■
Troubleshooting	+	■	■
Firmware Research and Upgrades	+	■	■
Firewall Vulnerability Patching	+	■	■
Log Retention	40 days □	120 days □	365 days
Reporting	+	All template reports	Custom reports
Firewall Access	Read/write	Default read only	Default read only
Solution Features			
SD-WAN	+	■	■
Gateway Anti-Virus	+	■	■
Web Filtering	+	■	■
Application Control	+	■	■
Intrusion Prevention (IDS/IPS)	+	■	■
SSL Deep Packet Inspection		■	■
Traffic Shaping	+	■	■
Policy Scheduling	+	■	■

Solution Features (cont.)	Core	Optimum	Secure
Site-to-Site IPsec VPN Tunnels	Limit 5	■	■
SSL-VPN for Remote Users	Limit 20 No Limit with AD	Limit 20 No Limit with AD	Limit 20 No Limit with AD
Routing	+	■	■
Single Sign On	+	■	■
Portal	■	■	■
Managed Detection Response — SOC Active Log Monitoring	□	n/a	■
Threat Intelligence	n/a	n/a	■
Data Leak Prevention (DLP)	n/a	n/a	■
Sandboxing	□	n/a	■
Monthly Vulnerability Scan	□	□	■
Web Application Firewall	n/a	n/a	■
Add-on Features			
Wireless Access Point (Wi-Fi) Management	+	□	□
Switch Management	+	□	□
Firewall Accessories	□	□	□
High Availability	□	□	□
2-Factor Authentication	□	□	□
4G Failover	□	□	□
Third Party Vendor Support	□	□	□

■ Included – monthly cost
□ Available – monthly cost
+ Available – time & materials cost

Feature Matrix

Technology Deployed	Core	Optimum	Secure	Secure Bundle
Remote Monitoring and Management Agent (RMM)	■	■	■	
Next Generation Anti-virus Agent (NGAV)	■	■	■	■
Endpoint Detection and Response Agent (EDR)			■	■
Endpoint DNS Protection Agent			■	■

Administrative And Support Services Provided

	Core	Optimum	Secure	Secure Bundle
24/7 Monitoring and Alerting	■	■	■	
Automated Patch Management	■	■	■	
RMM Portal Access	■	■	■	
Scheduled Standard Reporting	■	■	■	
On-Demand Reporting	■	■	■	
System Lifecycle Management	■	■	■	
Remote System Administration		■	■	
Remote Troubleshooting & Remediation of Software		■	■	
Remote Troubleshooting and Hardware Ticket Management		■	■	
Peripherals Troubleshooting		■	■	
Security Patch Management	■	■	■	

Security Services Provided

	Core	Optimum	Secure	Secure Bundle
Antivirus Software Mgmt	■	■	■	■
Endpoint AV/AM Deep Scan Assistance	+	■	■	■
MDR			■	■
Peripherals Troubleshooting		■	■	
Security Patch Management	■	■	■	

Security Services Provided (cont.)

Technology Deployed	Core	Optimum	Secure	Secure Bundle
Managed Endpoint DNS Protection			■	■
Security Awareness Training			■	■

Add-on Services

	Core	Optimum	Secure	Secure Bundle
Inbox Detection and Response	□	□	□	□
Active Directory Server Add-on		□	□	
Remote Desktop Services Add-on		□	□	
Microsoft Exchange/SQL Server Add-on		□	□	
Network DNS Protection			□	□
Endpoint AV/AM Remediation	+	+	+	+
On-Site Troubleshooting Assistance	+	+	+	+

■ Included – monthly cost

□ Available – monthly cost

+ Available – time & materials cost

* TPx support resources are available 24x7x365 for all service levels by contacting the support center via phone, email, or online ticket

Service: Managed Backup & Disaster Recovery

Feature Matrix

Available Features	Core	Optimum
Customer Support Center	8am - 8pm ET	24/7
Hybrid On-Premises Backup Device + Cloud Backup Solution	■	■
Off-Site Retention of Backups to Cloud Environment	■	■
Backup Screenshot Verification	■	■
Fast Failback Bare Metal Restore	■	■
Disaster Recovery Virtualization	■	■
Bandwidth Optimization	■	■
Device and Cloud Audit Reports	■	■
Ongoing Maintenance and Rapid Replace		■
Self-Service Backup Administration	■	■
Managed-Managed Backup Administration	+	■
Proactive Monitoring and Reporting for Backup Job Failures	+	■
Configuration of Backup Jobs	+	■
Config. of Exchange/SQL Aware Backups	+	■
Configuration of Ransomware Detection	+	■
Re-initiate Backup Jobs in the Event of a Backup Job Failure	+	■
Recovery of FILE/FOLDER from Backups	+	■
Backup Restore Assistance	+	■
Disaster Recovery Virtualization	+	■
On-Site Troubleshooting Assistance	+	+

Service: Managed Office 365

Feature Matrix

Available Features	Core	Optimum
Customer Support Center Providing Remote Support	8am - 8pm ET	24/7
Customer Account Setup in TPx's Azure CSP Portal	■	■
Billing Management	■	■
Technical Support Management & Escalation	■	■
Domain Association and Branding	■	■
User Account Management	+	■
Policy Settings Management	+	■
Groups and Resources Management	+	■
Security & Compliance Center Administration	+	■
Site Collections Management	+	■
Channel and Video Administrator Management	+	■
Skype for Business Configuration	+	■
Managed Cloud Backup	+	■

■ Included – monthly cost
□ Available – monthly cost
+ Available – time & materials cost

Solutions Highlights

Managed WAN

Initially, TPx only offered VMware because it was the best-in-class product and because TPx could do things with it that it couldn't do with others. TPx later added Silver Peak because of demand. Both VMware and Silver Peak offer:

- Sub-second failover
- Dynamic path selection
- Link steering and remediation
- Forward Error Correction (FEC)
- Jitter buffering
- Circuit aggregation (up to 4 circuits)
- Two-factor authentication
- Third party vendor support, high availability, and 4G failover options available

VMware

TPx's VMware based SD-WAN remains TPx's best-in-class solution and because TPx owns the VMware gateways it uses and those gateways are on TPx's own telecommunications backbone, that allowed TPx to enable inbound internet failover, which only a few providers can offer.

Note: inbound internet failover is available on only VMware

Additional features:

- Clustering (use of multiple devices to increase bandwidth)
- Non-standard IPSec tunnels
- Private segmentation
- Work for home Segmentation
- PCI and HIPPA complaint
- Physical and Virtual MSR options

Silver Peak

Certain Silver Peak models have an optional "Boost" available, which increases circuit bandwidth by compressing data prior to transmission. Additional features:

- Fail to Wire
- Layer 2 Bridge mode

Managed Firewall

For Managed firewall, TPx uses FortiGate firewalls and FortiAP WI-FI access points, both from Fortinet. FortiGate firewalls have been a leader in Gartner's magic quadrant for firewalls for a number of years.

FortiGate firewalls:

- Offer a complete Unified Threat Management (UTM) solution, including anti-virus, intrusion protection (IDS/IPS), web filtering, application control, and SSL DPI (Secure Socket Layer Deep Packet Inspection) (SSL is an internet encryption protocol)
- Are the only firewalls using custom processors designed to operate as firewalls. Everyone else uses general processors that are programmed to operate as firewalls. The difference is that FortiGate firewalls are hardware firewalls, while others have a software layer that makes them a firewall. Using the same processor power, hardware is always faster than software.
- Were amongst the first to offer SSL DPI. SSL DPI provides greater security by decrypting and scanning SSL encrypted packets. This is critical as more and more mal-intended sites and individuals have been using SSL for their sites and to distribute their malware. Any firewall that does not have SSL DPI will not be able to detect or block such malware.

In addition, FortiGate firewalls support SD-WAN. However they do not have:

- Forward Error Correction
- Jitter buffering
- Inbound failover

As a result, SD-WAN on FortiGate should be considered SD-WAN *Light*.

Datto RMM[1]

Datto RMM is the remote management platform used by TPx to manage endpoints remotely, but customers can also have access to the platform so they can remotely manage endpoints themselves if they want to.

Keeping endpoints up to date is critical. For Windows servers, workstations, and laptops, Datto RMM manages the deployment of TPx's anti-virus solution, and deploys updates and security patches for Windows, anti-virus software, and most major software packages.

The Datto's RMM solution installs a small agent on each server, workstation, or laptop which is used to communicate securely with the device. The agent allows TPx support engineers to remotely take control of an endpoint when appropriate via a secure VPN. The agent also gathers details about each device and monitors many, including:

- Status of the anti-virus
- CPU usage
- Size and space used and available on Hard disks & Solid-State Drives (SSDs)
- File and folder sizes
- Memory usage
- Network usage
- Processes that are running
- SNMP

Any details gathered or monitored can be viewed directly in the platform or in reports, making the platform an inventory system for all endpoints placed under its management.

In 2020, Datto RMM was rated best RMM/PSA platform by CRN.

Webroot

SecureAnywhere[1]

SecureAnywhere is a next generation anti-virus/anti-malware (NGAV) that is currently the smallest and fastest NGAV on the market.

It is supported by Webroot's worldwide threat intelligence, so as new threats are identified and solutions are created to protect against them, those details and solutions are propagated world-wide to all Webroot users.

In 2021, SecureAnywhere was again a PC Magazine Editor's choice (for the 22nd time).

DNS Protection[2]

Provides web filtering for endpoints.

Like Webroot SecureAnyware, Webroot DNS protection is also supported by Webroot's worldwide threat intelligence. Webroot scans the Internet 3 times daily to identify and track sites that contain malware or that harbor hackers and other mal-intended people.

G2 Grid lists Webroot's DNS Protection as a market leader for 2022.

GoSecure EDR/MDR[2]

GoSecure's EDR is an AI based Endpoint Detection and Response (EDR) agent that, on Windows systems, is one of two options currently on the market that operates at the Kernel level or operating system level. Others operate at the service or application levels, which don't have as much access to core system components. As a result, it can detect and respond to threats others can't.

When a threat is detected, the EDR agent will isolate the endpoint from the network and launch an AI based auto-remediation process. If the remediation is successful, the endpoint is put back on the network. If not, then an Alert is raised in TPx's SOC requesting manual remediation (TPx has a 15 minute SLA for the manual remediation once the alert has been received). Once an alert has been received, Manual Detection and Response (MDR) takes effect. That's when a cybersecurity engineer works to manually remediate a threat.

The January 2020 ICSA Labs test report shows that GoSecure's EDR solution detected 100% of threats thrown at it with only 9 false positives and 6 consecutive quarterly test cycles successfully passed.

The January 2022 ICSA Labs test report shows that GoSecure's EDR solution detected 95.2% of threats thrown at it with 0 false positives, and 14 consecutive quarterly test cycles successfully passed.

InfoSec IQ[2]

Users are still the #1 source of incidents, as a result, Security Awareness Training (SA) is a critical component of cybersecurity.

TPx configured its implementation of InfoSec IQ to be 100% in accordance with the National Institute of Standards and Technology's (NIST) 800-50 recommendations, which recommend a continuous security awareness training program that covers specific topics for 9 months of the year and leaves the topics for the remaining 3 months up the organization.

InfoSec IQ was awarded Cyber Defense Magazine's 2021 Infosec award as Security Awareness Training Market Leader and has received many other awards.

Depending on the service level, TPx provides a remote management platform, next generation anti-virus (NGAV), Endpoint Detection and Response (EDR), Manual Detection and Response (MDR), DNS Protection, and Security Awareness Training (SAT).

[1] included with Core, Optimum, and Secure)

[2] Included with Secure and available stand-alone)

Managed Networks

MX Firewalls

MS Switches

MR Wireless Access Points

Three Cisco Meraki product lines make up Managed Networks:

- MX series firewalls
- MS series smart switches
- MR series Wireless Access Points (WAPs)

MX firewalls are popular because of their cost relative to their features. However, they lack certain security features, so they are not recommended for high security environments (finance, legal, health care, etc.):

- No application monitoring
- No SSL-DPI – As more and more mal-intended sites and individuals use SSL, this is a serious security hole.
- No generation of syslogs that can be monitored. Syslogs, also known as event logs, are where threats are identified on firewalls. Those logs can be forwarded to a Security Information and Event Management (SIEM) system, which is software most Security Operations Centers (SOCs) use to monitor firewalls for threats.

MX firewalls also support SD-WAN, but they lack advanced SD-WAN features:

- No Forward Error Correction
- No jitter buffering
- No inbound failover
- No dynamic routing
- No per packet steering
- No inbound Quality of Service (QoS)
- No brown out monitoring and remediation
- No circuit quality monitoring

MS switches are remotely managed switches with:

- Layer 7 visibility
- Real-time QoS
- Cable test
- Remote packet capture
- Port security
- DHCP server
- Port isolation

Add-on services include:

- Layer 3 switching
- Modular power
- Switch stacking

MR WAPs are remotely managed with:

- Traffic shaping policies
- Wireless intrusion protection (WIPS)
- Interference detection
- Location analytics

Add-on services include:

- Splash page
- Access point installation (does not include heat mapping, cabling, coverage design, hardware selection, or hardware placement).
- Power Over Ethernet injector

Managed Backups

TPx's Backup and Disaster Recovery (BDR) solution is based on Datto's backup systems. Key features that set Datto's backup solution apart:

- It uses the ZFS file system, which is a versioning file system. This allows Datto's backups to keep multiple versions of files, making it easier to recover specific versions of files. It also is much faster at accessing backups since the file system can be browsed like a hard disk.

- Inverse chain technology improves reliability of backups. In traditional backup systems, intermediate backups are chained, meaning for a particular backup to be good, the previous backup must also be good. If for any reason, one backup is corrupted, then all intermediate backups that come after it will not be useable until the next full backup. Datto's Inverse Chain technology renders each backup independent of others, so if one of them is corrupted, the others will still be fully functional.

- Built-in ransomware detection. When ransomware installs itself on a system, it usually goes dormant for a while, it's there, but it's not active. The reason for that is to ensure that ransomware gets backed up with everything else, so if the organization tries to restore files from a backup following activation of the ransomware, the ransomware also gets restored. Datto detects ransomware within backups, making it easier to locate the last clean system restore point.

- Local backups can be encrypted with AES encryption, and cloud backups are always encrypted using AES and SSL during both transmission and cloud storage.

- Instant virtualization of failed systems either locally on the Datto device or in the cloud. A failed server can literally be back up and running in the time it takes to start it as a virtual server, whether on the Datto device or in the cloud, and in most cases, that will be in minutes, not hours or days.

- One of the areas many organizations have issues with is verifying backups (ensuring backups are clean and usable), which is a time-consuming process. Datto's backup solution has built-in screenshot verification. After backing up a device, Datto's solution can launch a virtual instance of that device (with networking disabled) to ensure it gets to the login screen. In addition, it can check for specific services and can even launch scripts (such as a script to ensure a particular database is up and running and is accessible).

The ZFS file system, inverse chain technology, ransomware detection, instant virtualization, and screenshot verification are each game changing features in themselves, but when combined into a single BDR solution, they put Datto's BDR solution far ahead of the competition.

General IT Consulting Services

Advisory Services consultants are well versed in many IT areas and technologies and can provide customers general IT consulting services tailored to their needs. Here are just a few:

- Hardware installations
- Software installation or upgrades
- Microsoft Exchange upgrades
- Office 365 or Microsoft 365 security reviews
- Project management
- Cybersecurity documentation