Service Specific Terms

MSx Endpoints

Effective 7.1.2024

These Service Specific Terms are incorporated into each applicable Service Order, and collectively with the General Terms and Conditions, form the Agreement between the Parties. Any capitalized terms not defined herein have the meaning given to them elsewhere in the Agreement.

A. Service Description – MSx Endpoints

"**MSx Endpoints**" is TPx's Managed Endpoints Solution, that provides unified performance and security management across a customer's server and workstation environments. It is designed to keep our clients' supported systems healthy, secure, and working optimally. The Service Features and other Entitlements included in the MSx Endpoints Services are further described in the sections below.

B. Supported Third-Party Product(s) & Technical Features; Portal Access

TPx currently offers its MSx Endpoints Service utilizing Software from the following Third-Party Product Providers:

Software:

- Datto
- Webroot
- GoSecure
- Infosec Institute

Technical Features. Certain features that are inherent to the Third-Party Product(s) ("**Technical Features**") may augment or limit the availability of Add-On Service Features. TPx supports all Technical Features requisite to deliver the Managed Service and Add-On Service Features detailed herein, but may not support all Technical Features offered by a particular Third-Party Product Provider.

Portal Access. User access may be provided to the Datto graphical user interface (the GUI or "**Portal**") for Customer's authorized users. The software used for a Portal is dependent on the respective Third-Party Product Provider. TPx will provision read/write Portal access where Customer has purchased the Core (self-managed) Service Level, or where Customer requests co-management at the Optimum or Secure Service Levels. Please note that there are additional Service Specific Terms in Section G below associated with Self and Co-Management of the Services.

C. Standard Service Onboarding; Initial Configuration & Account Enablement

Standard Service Onboarding. As a separate non-recurring Professional Services charge, TPx will provide project management and enablement services as required to implement and configure the Technical Features and provision access to Customer's authorized users. Standard service onboarding is offered during TPx regular business hours. Custom service onboarding may be required for certain deployments, which must be agreed to between the parties in a separate statement of work.

D. Managed Service Levels; Service Feature Availability

Service Levels. MSx Endpoints is offered at four service levels for qualified Windows devices: (i) Core; (ii) Optimum; (iii) Secure, and (iv) Secure Endpoint Bundle. The Core Service Level is designed for Customers looking for basic security service through self-management, including Next-Generation Antivirus software, and patching for Windows Operating Systems and Select third party applications leveraging Remote Monitoring and Management (RMM). The Optimum Service Level is designed for Customers looking for additional support including remote monitoring, management, troubleshooting and repair from TPx on top of the Core Services. The Secure Service Level adds several high-value security features that are designed to materially reduce the risk or impact of a cyber incident to the Optimum services. Finally, the Secure Endpoint Bundle is designed for customers that want to provide their own system patching and administrative support but want to leverage TPx for the additional high-value security services that we offer. The availability of Service Features for each Service Level is detailed in Table 1 below.

Table 1. Managed Service Feature Availability.

Legend: "**I**" – Included; "**MRC$**" – available with additional recurring cost; "**NRC$**" – available with additional Professional Services charges.

Managed Service Feature	**Description**	**Service Level**			
		Core	**Optimum**	**Secure**	**Secure Endpoint Bundle**
Datto RMM	DATTO RMM (Remote Monitoring and Management) allows TPx to monitor, alert and report on important KPIs affecting the health, performance and security of supported systems; remotely and securely access supported systems, deploy patches, schedule maintenance jobs and manage certain TPx provided Software.	**I**	**I**	**I**	**N/A**
Webroot NGAV	Webroot SecureAnywhere is a leading Next-Generation Antivirus (NGAV) software that delivers enterprise-class endpoint protection to protect against viruses, malware, and other security threats.	**I**	**I**	**I**	**I**
GoSecure MDR	GoSecure Titan Managed Detection and Response (MDR) provides comprehensive real-time detection and response to security events across all supported endpoints. By proactively detecting indicators of compromise, and automating alerting and mitigation, MDR can minimize the damage from identified security events and stop potential breaches.	**MRC$**	**MRC$**	**I**	**I**
Webroot DNS	Webroot SecureAnywhere includes an optional Secure DNS feature. When enabled all Internet requests are filtered through a powerful cloud security solution to block Internet-borne threats and help enforce company Internet use policy.	**MRC$**	**MRC$**	**I**	**I**
Online Security Awareness Training	Infosec IQ is an online Security Awareness Training platform that TPx leverages to create and schedule training campaigns and phishing simulations, and track & report on campaign and user statistics.	**MRC$**	**MRC$**	**I**	**I**
Self Service RMM Access	TPx provides and manages access to the RMM platform for Customer's authorized users. Customer access allows for limited functionality that includes remote control, and system audit & visibility.	**N/A**	**I**	**I**	**MRC$**
Lifecycle Management	TPx provides proactive reporting and communication of End-of-Life status on covered devices. Service includes Hardware warranty expiration as well as manufacturer End-of-Support status for Operating Systems and select applications. Post warranty hardware support packages, for covered servers, are available at additional cost.	**I**	**I**	**I**	**N/A**
Managed Patching for Supported Operating Systems	TPx provides managed, automated patching of supported Windows Operating Systems. Service includes operational and security patches remotely applied per TPx recommended practice. Patch status monitoring and reporting is also included.	**NRC$**	**I**	**I**	**N/A**

Managed Patching for Supported Third Party Applications	TPx plans and executes system updates on TPx included software as part of a proactive maintenance and performance management process. Changes are made based on the manufacturer's recommendations and TPx recommended practice.	**I**	**I**	**I**	**N/A**
Configuration Management – Initiated by TPx	TPx plans and executes system configuration changes on TPx included and supported software as part of a proactive maintenance and performance management process. Changes are made based on the manufacturer's recommendations and TPx recommended practice.	**I**	**I**	**I**	**I**
Configuration Management – Approved by TPx	TPx plans and executes system configuration changes that are requested by the customer and have been approved by TPx.	**I**	**I**	**I**	**N/A**

Table 2. Add-On Service Features. The service features below are available as add-ons and do not form a part of the Services unless they are expressly included as separate line items on the Service Order.

Add-on Managed Service Feature	**Description**	**Service Level**			
		Core	**Optimum**	**Secure**	**Secure Endpoint Bundle**
Managed Services for Microsoft Server Applications	TPx provides applicable Managed Services for specific named Microsoft Applications running on Servers. Includes Active Directory, Exchange, and SQL.	**MRC$**	**MRC$**	**MRC$**	**N/A**

Stand Alone Services. TPx provides Online Security Awareness Training, Webroot DNS, and GoSecure MDR services as stand-alone offers. If contracted for any of these services as stand-alone offers the service and technical features provided are limited to those specifically included with those offers.

E. KPIs & Support Priority Levels

The KPIs for monitoring, alerting, and reporting are as set forth in the table below. TPx will treat an incident that is either triggered by an alert or raised by Customer through a support case associated with each KPI based on the assigned Support Priority Level, as defined within the Service Level Agreement found at www.tpx.com/terms/service_level_agreement.

Table 3. KPIs and Support Priority Levels.

KPI	**Monitoring**	**Alerting**	**Description**
Antivirus Status Monitor	X	X	The Datto RMM Agent can be instructed to alert when no antivirus product is detected, or it has a certain status. For information on which antivirus products are detected refer to Antivirus Detection.
CPU Monitor - Servers	X	X	Physical device status indicating whether it is connected to the network and monitoring platform.

Disk Usage Monitor - Server 97%	X	X	Low disk space on a device can result in poor performance, application problems and eventually user complaints when they cannot save any more data. If the available space on your hard drive drops below a certain threshold, the device may not be reliable anymore.
Application Error	X	X	Applies for Event Codes 1000 and 1001. Event ID 1000 is application shutdown. Event ID 1001 indicates a crash.
Memory Monitor - Server	X	X	There are times when a device may get slow, freeze, fail to start certain programs, or even restarts while a user is working on it. One reason may be the device's high memory usage. Monitoring the devices memory performance may help proactively address further issues.
Online Status Monitor - Servers	X	X	A device with the Datto RMM Agent installed normally checks in with the RMM Portal every 90 seconds. If it does not (for example, due to a power outage or a network outage), Datto RMM sees this device as offline and alerts. This is particularly useful for servers as they should never go offline without an Administrator knowing.
Threat Alert	See below	See below	See below
Urgent	X	X	Urgent Priority events monitor and alert on a compromised endpoint with no EDR Mitigation, CNC activation, Ransomware, or malware.
High	X	X	High Priority events monitor and alert on Compromised endpoints with EDR Mitigation, Communication with a malicious site, Malicious files found on an endpoint, or a malicious email found.
Medium	X	X	Medium priority events monitor and alert on communication with a phishing site, potential credential compromise, exploit attempts, and higher threat policy violations.
Low	X		Low priority events monitor potentially unwanted programs/Adware, Credentials visible in plain text, and policy violations. To reduce noise, Low priority events have their alerts suppressed.

F. <u>Service Commencement & Delivery; Initial Service Term & Billing</u>

TPx endeavors to initiate the Standard Service Onboarding process by contacting Customer within five (5) business days of the mutual execution of the applicable Service Order. During the Standard Service Onboarding process, the Parties will mutually agree to a targeted Service Commencement and Service Delivery Date, as evidenced in writing (email sufficient).

For MSx Endpoints:

Service Commencement means that TPx has placed the order with the respective Third-Party Product Provider(s) for the Equipment and Software (as applicable), or has otherwise assigned the Equipment in inventory to Customer’s order.

Service Delivery means that TPx has completed the Standard Service Onboarding and otherwise delivered the Service, which is available for Customer's use.

The **Initial Service Term** will begin on the date of Service Delivery for each respective Service Location, and continue through the Term identified in the applicable Service Order. TPx will generally accommodate small changes to the target Service Delivery Date; however, where Customer unreasonably delays the Service Delivery or otherwise fails to fulfill its obligations under Article VI of the General Terms and Conditions preventing TPx from completing Service Delivery on the target Service Delivery date, then the Initial Service Term will begin on the target Service Delivery Date. Billing for the Service will coincide with the beginning of the Initial Service Term.

G. Additional Service Specific Terms

1. **Customer Self-Management or Co-Management.** Where TPx provisions read/write or administrative user access to the Customer in the Portal, Customer will have access to modify and otherwise reconfigure Technical Features and other aspects of the Services ("***Customer Management***"). Customer takes full responsibility and TPx disclaims all liability associated with any degradation in the Service quality or security resulting from actions taken by Customer through Customer Management.

2. **Managed Patching for Operating Systems.** TPx applies patches to Supported Operating Systems or Supported third-party systems as part of Incident Management if recommended by the manufacturer or if identified as a part of an incident remediation plan. System Patching is included with Core, Optimum and Secure service levels. Incident-based system patches are performed at TPx's sole discretion and may require a system reboot to fully implement the system patch. Certain patching services may need to be scheduled during a maintenance window to minimize the impact on the affected customer or affected endpoint.

3. **Datto RMM 3rd Party Application Patching Support.** 3rd Party Applications may be considered for support at TPx sole discretion and will be categorized as follows:

    a. **Full Support –** TPx delivers automated patching, uninstall/reinstall, remote troubleshooting, vendor escalation and support case management (applications in this category typically include select Microsoft applications).

    b. **Limited support –** TPx delivers patching and uninstall/reinstall services. Some applications in this category can be automatically and proactively patched using Datto RMM and are notated by Datto.

    c. **Unsupported -** TPx does not include support for Unsupported applications as part of the standard monthly recurring service and charges.

4. **Datto RMM ComStore 3rd party Applications & Scripts.** TPx does not support DattoRMM ComStore Applications and Scripts. These are not updated or maintained by Datto, and are generated from 3rd parties within the Datto Ecosystem.

5. **Operating System Support.** TPx supports Microsoft operating system versions that are fully supported by the manufacturer, as notated on the Microsoft Product Lifecycle site. VMWare, ESXi, Apple MacOS, and Linux systems are limited support, and are best effort.

6. **Service Dependencies; Third-Party Products.** Enrolled endpoint devices are required to be under an applicable maintenance or support agreement as a Service Dependency for the MSx Endpoints Service. Third party maintenance and support agreements may be available through TPx as an Add-On Service. All endpoint devices, regardless of whether they are acquired through TPx, will be considered Excluded Products. Except for TPx responsibilities expressly set forth herein, Customer remains exclusively responsible for the Excluded Products. For avoidance of doubt, except as exclusively set forth in the subsection below, TPx does not support or manage any endpoint hardware issues.

7. **Managed Endpoints Hardware Support.** TPx provides remote troubleshooting and management to resolve identified hardware issues on supported endpoints under both the Optimum and Secure Service levels. Where applicable to resolve an incident, TPx will open a warranty repair service case with the manufacturer or third-party hardware maintenance or support provider. TPx services related to hardware support herein is limited to warranty repair/replace tickets, and any performance thereafter is provided by the manufacturer or third-party maintenance or support provider.

Third-Party Terms.

- ***Datto/Kaseya.*** All services, software and hardware warranties associated with Datto Third-Party Products are governed by Kaseya's policies, currently stated at https://www.datto.com/legal/datto-business-management-services-terms-of-use/ or other website as designated by Kaseya. Portal Access is provided to Customer as an authorized user under the license or subscription rights granted by the respective Third-Party Product Provider to TPx. No pass-through EULAs or other Third-Party Terms are required to utilize Portal Access; however, Customer must adhere to all provisions of the Agreement, including, without limitation TPx's Acceptable Use Policy.

- ***GoSecure .*** All services and software associated with GoSecure Third Party products are governed by GoSecure's policies currently stated at https://www.gosecure.ai/wp-content/uploads/GoSecure_EULA.pdf or other website as designated by GoSecure
- ***Webroot/OpenText.*** All services and software associated with Webroot Third Party products are governed by Opentext's policies currently stated at https://www-cdn.webroot.com/4716/6922/1022/Webroot-Consumer-Terms-and-Conditions-v.2022.11.23.pdf or other website as designated by OpenText
- ***Infosec.*** All services and software associated with Infosec are governed by Infosec's policies currently stated at https://www.infosecinstitute.com/infosec-license-agreement/ or other website as designated by Infosec.