TPx	**Service Specific Terms** ***Managed Endpoint Security***	**Effective 8.3.2026**

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 – Managed Endpoint Security

"**Managed Endpoint Security**" is TPx's Managed Endpoint Security Solution, that provides AI driven Endpoint Detection and Response (EDR) platform with behavioral threat detection, advanced investigation capabilities, and automated response actions. The available Managed Detection and Response (MDR) service provides 24x7 security analyst monitoring, threat investigation, proactive threat hunting, and coordinated response. The Service Features and other Entitlements included in the Managed Endpoint Security Services are further described in the sections below.

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

TPx currently offers its Managed Endpoint Security Service utilizing Software from the following Third-Party Product Providers:

Software:

- SentinelOne

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 is provided to the 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 or administrator level Portal access based on Solution Tier and Customer user roles. 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 Solution Tiers; Service Feature Availability

Solution Tiers. Managed Endpoint Security is offered with two solution tiers (i) Standard, and (ii) Advanced. Optional add-ons are available to expand security capabilities based on customer needs. The Standard Solution Tier is designed for Customers looking for endpoint threat detection and automated responses through self-management; the Advanced Solution Tier is designed for Customers looking for 24x7 security analyst monitoring, threat investigation, proactive threat hunting, and coordinated response on top of the Standard Solution Tier. The availability of Service Features for each Solution Tier is detailed in Table 1 below.

Table 1. Managed Service Feature Availability.

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

Managed Service Feature	Description	Solution Tier	
		Standard	Advanced
SentinelOne EDR	SentinelOne Singularity Complete EDR for workstations includes behavioral AI threat detection to detect suspicious and malicious events on the endpoint. Storyline attack correlation to link related events into a single attack narrative to support investigations. Protection policies that can autonomously kill, quarantine, remediate, or rollback processes or files in response to a threat.	I	I
SentinelOne Cloud Workload Security	SentinelOne Singularity Complete Cloud Workload Security expands EDR capabilities to servers delivering real-time threat detection and response for cloud workloads. Cloud Workload Security detects and stops runtime threats and provides the ability to respond with autonomous mitigation actions.	I	I
30-day Data Retention	SentinelOne 30-Day Data Retention provides 30 days of searchable endpoint telemetry data for threat hunting, incident investigation, IOC validation, and forensic analysis within the SentinelOne platform.	I	I
SentinelOne Purple AI Foundations	SentinelOne Purple AI Foundations streamlines threat investigations with AI-enriched alert summaries, natural language querying of endpoint telemetry, and a conversational user experience for technical support.	I	I
Management Portal Access	TPx provides and manages access to the Endpoint Security platform management portal. Administrative access is provided for Standard Solution Teir Customers needing self-management or read/write access for Advanced Solution Tier customers leveraging MDR services.	I	I
Lifecycle Management	TPx provides proactive reporting and communication of new releases and end-of-life status on software components.	I	I
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
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
Firmware Management	TPx monitors platform maintenance and confirms release updates. TPx will initiate endpoint agent software upgrades from the Endpoint Security platform. Agent upgrade issues will need to be reported to Technical Support.	I	I

Dashboards and Reporting	The Endpoint Security platform provides Customers through a combination of dashboards, platform reporting or scheduled executive reports. Additional incident reporting is available for Advanced Solution Tier customers.	**I**	**I**
Technical Support	TPx provides Technical Support for the platform and endpoint agent software. Problem identification, analysis, initial diagnosis, and troubleshooting will be performed in an effort to resolve the problem.	**I**	**I**
24x7 MDR Monitoring	The SentinelOne MDR team of threat detection and response experts provide 24x7 monitoring of EDR threat alerts detected on the endpoint and generated in the Endpoint Security platform.		**I**
Analyst-led Triage and Investigation	The MDR team will triage false positive alerts and investigate confirmed threats and unusual or complex alerts. Analyst notes will be added to the alert visible within the Endpoint Security platform.		**I**
MDR Response Actions	The MDR team will respond to security incidents following the approved MDR Response Policies that define the response authority provided by the Customer. The mitigation actions the MDR team is permitted to take will include incident containment, incident eradication, and tuning.		**I**
Incident Escalation Coordination	TPx coordinates escalated incidents that require additional information to assist in an investigation, Customer approvals for response actions, or recommended remediation steps following an incident.		**I**
Incident Based Configuration Changes	TPx executes system configuration changes recommended by TPx or the MDR team as part of an identified incident recommended remediation.		**I**
Proactive Threat Hunting	The MDR team performs proactive threat hunting to identify otherwise undetected malicious activity within your environment. Confirmed hunt findings are published in the Endpoint Security platform to review the details of the hunt finding and related threat intelligence.		**I**
Quarterly Business Reviews	TPx review of policy effectiveness and alert trends to identify recurring risks, false positives, and opportunities for tuning. Various reports and performance metrics including MTTR will be reviewed to inform technical or business stakeholders.		**I**

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**	**Solution Tier**	
		Standard	**Advanced**
Purple AI SOC Analyst	Purple AI SOC Analyst enhances the Standard Solution Tier by providing AI-powered security investigation assistance that helps internal IT and security teams investigate alerts more quickly and efficiently. Using natural language queries and autonomous investigation capabilities, Purple AI gathers evidence, provides contextual analysis, and delivers actionable findings, enabling customers to accelerate threat investigations and improve analyst productivity while maintaining full control over response decisions.	**MRC$**	**N/A**

Network Discovery	Network Discovery extends endpoint visibility by identifying managed and unmanaged devices connected to the customer's network. By continuously discovering assets that may not yet be protected, organizations can improve asset inventory accuracy, identify security coverage gaps, and strengthen their overall endpoint security posture.	**MRC$**	**MRC$**
Vulnerability Management	Vulnerability Management includes and builds on Network Discovery by continuously identifying, assessing, and prioritizing vulnerabilities across managed assets. The solution provides centralized visibility into endpoint risk, helping organizations focus remediation efforts on the most critical exposures, improve cyber hygiene, and reduce overall attack surface through risk-based vulnerability management.	**MRC$**	**MRC$**

E. KPIs & Support Priority Levels

The KPIs for EDR monitoring, alerting, and reporting are as set forth in the table below. Alerts generated in the Endpoint Security platform are a result of suspicious or malicious threats detected on one or more endpoints. Alerts are assigned a Severity Level that shows the potential impact of the threat. Alert Severity Levels are shown in Table 3. Additional Alert details can be found in the Endpoint Security platform management portal to assist in Customer analysis of the alert.

Table 3. EDR Alert Severity Levels.

KPI	Monitoring	Alerting	Reporting	Description
Critical	X	X	X	Imminent or ongoing threat with potential for catastrophic impact (e.g. Ransomware Detected).
High	X	X	X	Significant potential impact (e.g. API Abuse for Data Theft detected).
Medium	X	X	X	Moderate potential impact (e.g. Direct Syscall From PEB Trap Library detected).
Low	X	X	X	Minor potential impact (e.g. Domain Controller Discovery detected).
Info	X	X	X	No indicative of a threat (e.g. SGID Set With Chmod detected).

The Advanced Solution Tier, including 24x7 MDR Monitoring, will involve the MDR team reviewing all EDR threat alerts. Confirmed threats will be investigated and if they are identified as suspected malicious activity that poses a security risk to an organization's data or systems an incident will be escalated. Escalated incidents will be assigned an Incident Severity Level shown in Table 4. TPx will treat incidents through a support case associated with the assigned Support Priority Level, as defined within the Service Level Agreement found at https://www.tpx.com/legal/sla/.

Table 4. MDR Escalated Incident Severity Levels.

KPI	Monitoring	Alerting	Reporting	Description
High Severity Incident	X	X	X	A threat that has not yet been fully mitigated and continues to pose an active risk to your organization (e.g. An attacker has established persistence in your environment).
Low Severity Incident	X	X	X	A threat that has not yet been fully mitigated but does not pose an active risk to your organization (e.g. Attacker tool discovered on system but not executed).
Request for Information	X	X	X	The MDR team has a question about suspicious activity in your environment.
Exclusion / Informational	X	X	X	The MDR team is recommending exclusions or policy overrides to prevent benign activity from triggering additional details.

F. Service Commencement & Delivery; Initial Service Term & Billing

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 Managed Endpoint Security:

The **Initial Service Term** will begin on the date of Service Commencement for the respective service location and continue through the Term identified in the applicable Service Order. Billing for the Service will coincide with the beginning of the Initial Service Term.

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 or Software 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. Where Customer unreasonably delays the Service Delivery or otherwise fails to fulfill its obligations under Article VI of the General Terms and Conditions the target Service Delivery date may be delayed.

G. Additional Service Specific Terms

1. **User Access and Service Co-Management.** Where TPx provides user access or administrative roles 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. Customer also takes full responsibility for any additional users provided access to the Service. Additional Labor Charges or Professional Service Charges may be incurred to rectify degradation in the Service Quality or security resulting in actions taken by the customer through customer management.

2. **Subscription Adding Users/Licenses**.

- Customer agrees to subscribe to the number of users set forth in the applicable Service Order ("Subscribed Users"). TPx will invoice Customer for the full number of Subscribed Users beginning in the first billing month.

- Customer may increase Users at any time; however, reductions are not permitted during the Term identified on the applicable Service Order. TPx will periodically reconcile the number of active users accessing the Service ("Active Users"). Customer may exceed the Subscribed Users by up to twenty percent (20%), rounded to the nearest five (5) users ("Tolerance Threshold"). Any Active Users in excess of the Tolerance Threshold will be deemed authorized and will be automatically billed at the applicable per-user rate effective as of the first month in which such excess occurs.
- TPx will provide Customer with written notice of any administrative adjustment to the Subscribed Users, which may be provided via a support ticket, customer portal notification, or email. Such notice is for informational purposes only and does not require Customer approval. F. Service Commencement & Delivery; Initial Service Term & Billing

3. **Log Ingestion Overages.** Customers are allotted a fixed Log Ingestion of 10GB per Customer site per day for any configured Marketplace integrations within the Endpoint Security platform management portal. Customer acknowledges and agrees that TPx will not permit an average daily usage of more than 10GB within a 30-day period. Any Log Ingesting in excess of the allotted amount, shall be deemed accepted by Customer and may be billed by TPx as usage based overage charges, after which customers may receive an invoice for overages.
4. **Supported Agent Versions**. Customer acknowledges that the Managed Detection and Response (MDR) Service requires all in-scope endpoints, servers, virtual machines, cloud workloads, and other protected assets to run a SentinelOne agent version that is supported by SentinelOne. TPx shall have no responsibility or liability for any degradation of service, service limitations, missed detections, delayed responses, incomplete investigations, inability to perform response actions, or security incidents resulting from Customer's failure to maintain supported agent versions.
5. **Third-Party Security Technologies**. Customer acknowledges that the Services rely in part on third-party security technologies provided by independent vendors. TPx does not develop, control, or materially alter such technologies and shall not be responsible for defects, vulnerabilities, outages, or failures arising from such third-party products except to the extent caused by TPx's own negligence in service delivery.
6. **No Guarantee of Threat Prevention**. Customer acknowledges that cybersecurity threats are constantly evolving and that no security solution or managed security service can guarantee the detection, prevention, or remediation of all threats, vulnerabilities, or incidents. TPx does not guarantee that the Services or any underlying security technology will prevent unauthorized access, data loss, or security breaches.
7. **Security Policy Configurations.** As a part of the Service, TPx establishes and maintains recommended security configurations, including but not limited to Endpoint Protection Policies, Agent Security Settings, MDR Response Policies, and other security-related configurations (collectively "Security Policies"). Customer may request modifications, exclusions, or disabling of specific Security Policies. Customer acknowledges and agrees that such modifications may reduce the effectiveness of threat detection, prevention, investigation, containment, remediation, and other security capabilities of the Service. TPx shall not be responsible for any degradation of Service arising from Customer-requested modifications to the default Security Policies.
8. **Incident Response Limitations.** Unless expressly included in a separate written agreement, the Services do not include full incident response, forensic investigation, legal response coordination, or breach remediation. TPx's role is limited to alerting and reasonable response actions as defined in the applicable service description.

Third-Party Terms.

- ***SentinelOne.*** All services, software and hardware warranties associated with SentinelOne Third-Party Products are governed by SentinelOne's terms and policies applicable to the Portal and the Managed Services Flow Down Terms https://www.sentinelone.com/legal/master-subscription-agreement/ or other website as designated by SentinelOne.

H. Managed Services Flow Down Terms

Customer and TPx have entered an agreement ("Solution Terms") where TPX is providing managed security services for the Customer ("Services"). This Managed Services – Flow Down Terms, ("Flow Down Terms Attachment") shall be made part of the Solution Terms between TPx and Customer, and where this Flow Down Terms Attachment and Solution Terms conflict, this Flow Down Terms Attachment shall control. TPx has licensed SentinelOne's platform including its malware protection, detection and remediation solutions, endpoint detection and response solutions, device discovery and control solutions, and other solutions and enhancements thereto offered by SentinelOne over time, ("Solutions") from SentinelOne, Inc. and is using the Solutions in its provision of Services.

1. **All Claims between TPx and Customer.** Customer agrees that it will bring all claims under this Agreement as well as any claims arising out of its related use of Solution against TPX and will not make any claim directly against SentinelOne. Customer agrees that SentinelOne has no obligation or liability to Customer under this agreement.
2. **Solution Use.** Customer may only use Solutions for its internal business security and operations, in accordance with the Documentation in conjunction with the Services.

3. **Restrictions on Use.** Customer may not do any of the following: (i) modify, disclose, alter, translate or create derivative works of the Solutions (or any components thereof) or any accompanying Documentation; (ii) license, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Solutions (or any components thereof) or any Documentation; (iii) use the Solutions for commercial or business uses not contemplated in Services such as offering Solutions to the benefit of other third-parties, Solution may only be used as directly related to Customer's internal business operations and in conformity with the Documentation; (iv) use the Solutions in violation of any laws or regulations, including, without limitation, to store or transmit infringing, libelous or otherwise unlawful or tortious material, or material in violation of third-party privacy rights; (v) use the Solutions to store, transmit or test for any viruses, software routines or other code designed to permit unauthorized access, disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (vi) probe, scan or test the efficacy or vulnerability of the Solutions, or take any action in an effort to circumvent or undermine the Solutions, except for the legitimate testing of the Solutions in coordination with TPX and SentinelOne, in connection with considering a subscription to the Solutions as licensed herein; (vii) attempt or actually disassemble, decompile or reverse engineer, copy, frame or mirror any part or content of the Solutions, or otherwise derive any of the Solutions' source code; (viii) access, test, and/or use the Solutions in any way to build a competitive product or service, or copy any features or functions of the Solutions; (ix) interfere with or disrupt the integrity or performance of the Solutions; (x) attempt to gain unauthorized access to the Solutions or their related systems or networks; (xi) disclose to any third party or publish in any media any performance information or analysis relating to the Solutions; (xii) fail to maintain all copyright, trademark and proprietary notices on the Solutions and any permitted copy thereof; or (xiii) cause or permit any Solutions user or third party to do any of the foregoing.