TPx Managed Endpoint Security

Stronger Endpoint Protection. Faster Response. Managed by TPx.

What is It and Why Do You Need It?

Endpoints are one of the most common entry points for cyberattacks. Traditional antivirus can leave gaps in visibility, and many IT teams don't have the time or bandwidth to investigate every alert.

TPx Managed Endpoint Security combines SentinelOne-powered endpoint protection with TPx-managed service delivery to help detect suspicious activity sooner, reduce the burden of alert investigation, and support faster containment.

Benefits

Benefit	What It Means for You
Greater Visibility	See suspicious endpoint activity earlier with SentinelOne-powered Endpoint Detection & Response (EDR).
Faster Threat Detection	Behavioral AI detection helps identify suspicious activity that traditional antivirus may miss.
Ransomware Readiness	Supports ransomware containment and rollback on eligible systems where available.
Flexible Response Options	Choose Standard solution tier when your team manages response, or Advanced solution tier when you need analysts to monitor and respond.
Reduced Alert Burden	Helps your team avoid unmanaged alert backlogs and focus on higher-value IT priorities.
24/7 Analyst-Led Investigation	SentinelOne Managed Detection & Response (MDR) analysts investigate, triage, and coordinate response around the clock (Advanced solution tier only)

How It Works

Step 1: Choose the Right Solution Tier

TPx helps align the solution to your team's needs. Choose Standard solution tier (EDR) if your team can review alerts and manage response. Choose Advanced solution tier (EDR + MDR) if you need 24/7 analyst-led investigation and response support.

Step 2: Configure Endpoint Protection Platform

TPx configures the SentinelOne-powered platform, aligns service settings, and helps prepare your endpoint environment for protection. Your team coordinates agent deployment unless a separate managed deployment service is contracted.

Step 3: Detect Suspicious Activity Sooner

SentinelOne EDR continuously monitors endpoint behavior for signs of malware, ransomware, and other suspicious activity. Behavioral AI detection and attack correlation help provide context so threats can be understood faster.

Step 4: Respond Based on Your Solution Tier

With Standard solution tier (EDR), your team reviews alerts and takes response action using the tools and visibility provided. With Advanced solution tier (EDR + MDR), SentinelOne MDR analysts monitor 24/7, investigate alerts, triage threats, and execute approved response actions.

Step 5: Stay Informed and in Control

TPx manages the service experience, including technical support, escalation coordination, and customer communication. Advanced solution tier also includes quarterly business reviews with service reporting.

Why TPx?

Endpoint security works better when strong technology is paired with a service partner behind it. TPx combines SentinelOne-powered protection with managed support giving your team added expertise, coordinated service management, and flexible control based on the solution tier you choose.

Trusted Experience at Scale

TPx supports thousands of businesses nationwide and manages more than 10,000 endpoints, bringing practical experience across the IT environments our customers rely on every day.

Expertise that Extends Your Team

Your team stays focused on business priorities while TPx provides practical guidance, technical know-how, and a clear path for support. You get added endpoint security expertise without giving up visibility or control.

Transparency and Communication

TPx keeps communication organized when platform support or escalation is needed, so your team knows who is involved and where things stand. With the Advanced solution tier, quarterly business reviews provide a regular checkpoint to review trends, notable activity, and opportunities for optimization.

The Right Balance of Support and Control

Your team stays in control of business decisions and response authority, while TPx helps manage the service around the level of support you choose.

How TPx Helped JF&CS Strength Stability and Security

Jewish Family & Children's Service of Greater Boston supports 14,000 to 15,000 clients each year, with critical services ranging from telehealth and behavioral health to elder support and residential programs. As its digital needs grew, JF&CS turned to TPx to help a lean IT team build a more scalable, secure, and reliable environment. With managed firewall and endpoint services, TPx helped improve visibility, reduce day-to-day IT strain, and build a more scalable foundation for delivering essential services.

Better Together: Endpoint Security + Endpoint Management

Managed Endpoint Security and Endpoint Management are separate services, but together they help organizations keep devices healthy while improving threat detection, visibility, and response. Managed Endpoint Security helps detect, investigate, and respond to endpoint threats. Endpoint Management helps keep devices maintained, patched, monitored, and performing reliably.

Together, they provide more consistent endpoint coverage, smoother agent deployment and validation, better visibility across managed devices, and stronger coordination between IT operations and security response.

Solution Overview

Every organization has different security needs. TPx offers two solution tiers so you can choose the level of protection and managed support that best fits your team.

The Standard solution tier (EDR) is best for organizations that have internal IT or security staff who can review alerts, investigate threats, and make response decisions, but need stronger endpoint visibility and detection tools to support them.

The Advanced solution tier (EDR + MDR) is best for organizations that need endpoint protection but do not have the internal capacity to monitor, investigate, and respond to threats 24/7.

Service Feature	Description	Standard Solution Tier (EDR)	Advanced Solution Tier (EDR+MDR)
Singularity Endpoint	SentinelOne Complete EDR license for endpoint detection and response.	✓	✓
Behavioral AI Detection	Detects suspicious activity based on behavior patterns, not just known signatures.	✓	✓
Storyline Attack Correlation	Links related endpoint events into a single attack narrative to support faster investigation.	✓	✓
Purple AI Foundations	AI-assisted investigation, alert summarization, and context enrichment.	✓	✓
Cloud Workload Security for Servers	Workload protection for server environments.	✓	✓

Service Feature	Description	Standard Solution Tier (EDR)	Advanced Solution Tier (EDR+MDR)
Reporting and Dashboards	Visibility into endpoint security activity and service status.	✓	✓
TPx Platform Configuration and Support	TPx configures and manages the platform and provides technical support.	✓	✓
24/7 MDR Monitoring	SentinelOne MDR analysts monitor endpoint alerts around the clock.		✓
Analyst-Led Investigation and Triage	Human analysts investigate alerts and triage threats.		✓
Proactive Threat Hunting	Analysts proactively search for hidden threats in the endpoint environment.		✓
Incident Coordination	TPx coordinates communication and escalation during security incidents.		✓
Quarterly Business Reviews	Service reporting and review with TPx.		✓

Add-On Managed Service Feature	Description	Standard Solution Tier	Advanced Solution Tier
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$

Take control of cyber threats before they disrupt your business.

See how TPx Managed Endpoint Security helps improve cyber threat visibility, support faster containment, and reduce the burden on your IT team.