

TPx Managed Endpoints

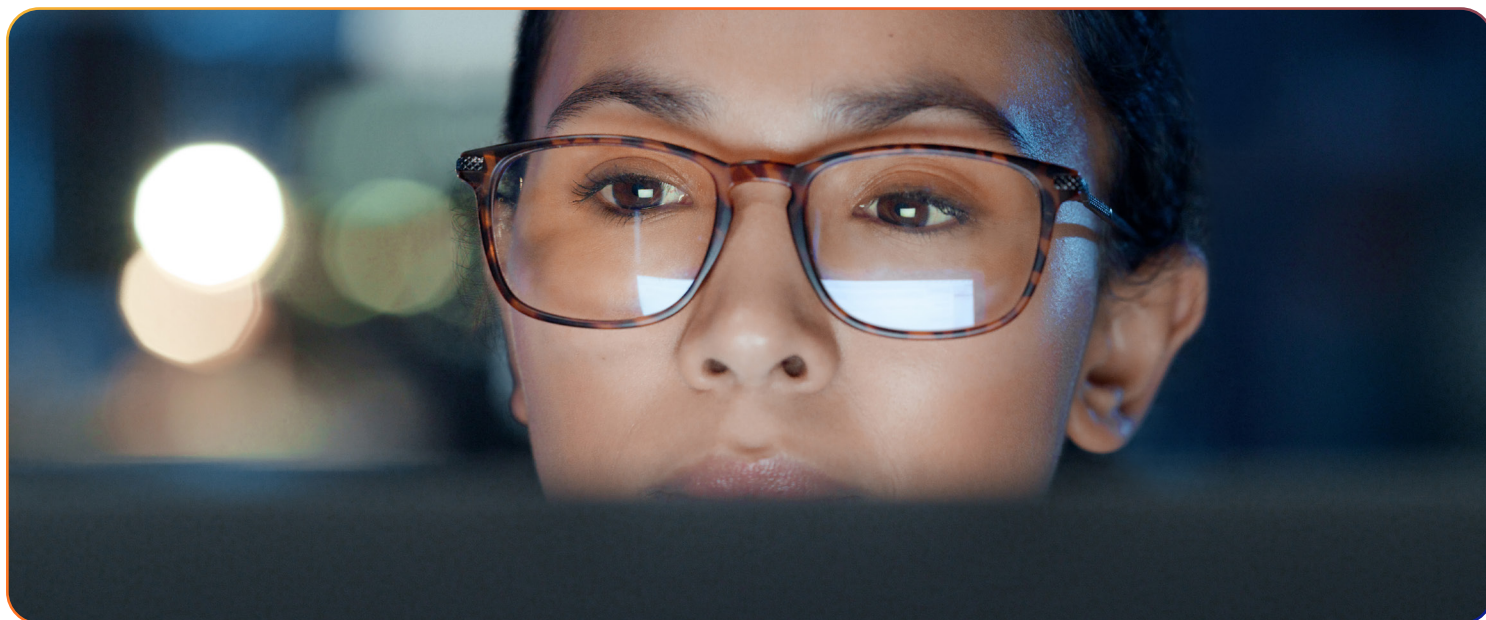
Stronger Protection and Performance,
Minus the IT Headaches



What Is It and Why Do You Need It?

Endpoints (servers, PCs, laptops) are the #1 target for cyberattacks – and also the foundation of productivity for your employees. Without proper management, they introduce risks like unpatched vulnerabilities, malware infections, and costly downtime.

TPx Managed Endpoints unifies endpoint management and endpoint security into one fully managed service. From proactive patching to advanced protection like DNS filtering, phishing simulations, and real-time threat detection, TPx keeps your endpoints secure, compliant, and performing at their best – without overloading your IT team.



Benefits

Benefit	What It Means for You
Stronger Protection	Block malware, phishing, and unsafe connections before they disrupt your business.
Up-to-Date Security	Patches and antivirus updates are applied automatically, lowering risk from outdated systems.
Less Downtime	Problems are caught and fixed quickly – often before they cause interruptions.
Compliance Support	Meet security standards with endpoint controls, logging, and reporting.
24/7 Monitoring & Support	TPx experts oversee your endpoints around the clock and respond to issues right away.
Scales with Your Business	Add or remove endpoints as needed without slowing down IT operations.
Reduced IT Burden	Offload patching, monitoring, and troubleshooting to TPx's team.
Flexible Options	Choose fully managed or co-managed – retain control or hand off entirely.

How It Works



Step 1: Worry-Free Setup

TPx deploys lightweight agents, configures policies, and activates dashboards so your endpoints are ready to go from day one.



Step 2: Secure and Up to Date

Automated patching, next-gen antivirus, and DNS filtering keep systems protected and maintained with less effort from your team.



Step 3: Threats Detected and Stopped Early

Advanced monitoring tools and TPx's 24/7 security experts catch suspicious activity quickly and act to contain it.



Step 4: Faster Fixes, Less Downtime

Continuous endpoint health checks let TPx resolve issues remotely before they disrupt your users or business.

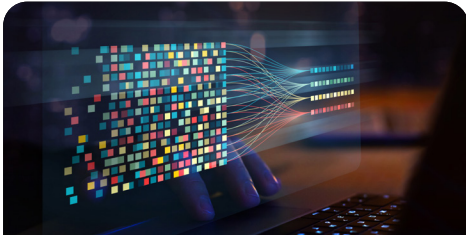


Step 5: Smarter Planning, Stronger Resilience

Regular reporting and lifecycle insights give you a clear view of endpoint health, helping you plan ahead and protect your investments.

Why TPx?

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our expert consultants, well versed in Information Security Standards like HIPAA, NIST, and ISO 27000, leverage extensive experience in strategic and operational solutions to ensure robust, nationwide security for our clients.



Complete Endpoint Management

From patching to policy enforcement, TPx keeps endpoints secure and up to date.



Expert Security Oversight

Our team monitors threats, applies protections, and responds to issues before they spread.



One Partner for IT & Security

Simplify vendor sprawl by consolidating endpoint management and protection with TPx.



Cost-Efficient Protection

Predictable service pricing that reduces the hidden costs of downtime or unmanaged risks.



Peace of Mind

Rest easy knowing every endpoint is managed and secured by experienced professionals.

“We’re impressed with their systematic approach ... they are a trustworthy partner that delivers cost-effective results”

**- Jaz Jackson
Executive Administrator,
Grower’s Secret**

How TPx Helped Grower’s Secret Strengthen Security

Grower’s Secret, a 17-employee company spanning Hawaii and California, turned to TPx to tackle growing phishing threats and a lack of internal security resources. By deploying Managed Endpoints and Security Awareness Training, TPx delivered continuous monitoring, patching, and phishing simulations that eliminated incidents and strengthened defenses – freeing the team to focus on their business.



Solution Overview

Service Features	Description	Endpoint Management	Endpoint Security	User Security
Monitoring, Alerting, and Reporting	TPx provides automated monitoring and alerting and scheduled reports for device availability, health and performance, and inventory. Monitoring and alerting are per TPx's recommended practices. Alerts are received and actionable by either TPx or the customer, based on service level.	Yellow	White	White
System Patching	TPx provides managed, automated patching of operating systems and select third-party applications. Service includes operational and security patches remotely applied per TPx recommended practice. Patch status monitoring and reporting are also included.	Yellow	White	White
Remote System Support	TPx provides 24/7 troubleshooting and repair of covered devices. Service includes proactive support based on TPx recommended practice and responsive support for customer requests or identified alerts. Remote Systems support features may be included in the fixed monthly charge or billable based on the chosen service level.	Yellow	White	White
Lifecycle Management	TPx provides proactive reporting and communication of end-of-life status on covered servers. Service includes hardware warranty expiration as well as manufacturer end-of-support status for operating systems and select applications. Post-warranty hardware support packages are available at additional cost.	Yellow	White	White
Managed NGAV	TPx provides managed Next-Generation Antivirus support. Service includes the use and management of the NGAV software as well as monitoring, alerting, and reporting on NGAV status. Virus remediation is available as a billable service	White	Orange	White
Endpoint Managed Detection and Response	TPx provides MDR services to identify and prevent advanced security attacks. The service includes the use and management of leading EDR software, SaaS platform hosting, SOC threat hunting, alert response, and event mitigation with an industry-leading 15-minute response time.	White	Orange	White
DNS Protection	TPx provides DNS Protection for covered devices to combat Internet-born threats and enforce Internet usage policy. Service includes the use and management of the DNS Agent software, configuration of security policies, and monitoring and reporting on browsing activity and security events.	White	Orange	White
Security Awareness Training	TPx provides automated Security Awareness Training campaigns. Service includes campaign setup, ongoing phishing simulations, and monthly training courses delivered automatically to enrolled users. Scheduled reporting of campaign status and activity is also included.	White	White	Blue
Inbox Detection and Response	TPx Inbox Detection and Response service allows users to easily report potential phishing emails. Reported emails are quarantined then scanned by software and SOC personnel to identify threats. Within just a few minutes, safe emails are returned to the users' inbox and all instances of malicious emails are automatically removed from all other users' mailboxes.	White	White	Blue

All service features are available in pre-packaged solution bundles to meet a variety of use cases. Endpoint Security and User Security service features are also available as stand-alone offerings.

Take control of your endpoints – before attackers do.

See how TPx Managed Endpoints simplifies IT, strengthens defenses, and keeps your business running.

Schedule your **free cybersecurity discovery session** today at www.TPx.com!