DNS Protection

Your First Line of Defense Against Internet Threats

What Is It and Why Do You Need It?

Every Internet connection begins with a DNS request — and that's exactly where cybercriminals strike. DNS-based attacks are fast, silent, and can slip past even well-configured firewalls, which only inspect traffic once it reaches your network. Think of DNS Protection as security that works before the firewall, blocking dangerous destinations at the source, not at the gate.

TPx DNS Protection acts as a secure, cloud-based filter between your users and the web. By analyzing every DNS request in real time, it blocks malicious or unwanted sites before a connection is ever made, stopping threats at the network edge before they cause harm.

Delivered as a **fully managed service**, DNS Protection safeguards all your users and devices — on-site, remote, or mobile — without adding administrative burden. It helps enforce compliance, increase productivity, and strengthen your security posture with a simple, scalable layer of defense.

Benefits

Benefit	What It Means for You
Stops threats before they spread	Blocks malicious, phishing, and command-and-control sites at the DNS layer — keeping threats off your network.
Protects users everywhere	Extends security to remote and hybrid workers through lightweight agents and network-based controls.
Strengthens compliance and control	Enforces acceptable use and regulatory policies with customizable filtering and clear reporting.
Boosts productivity	Filters out risky or time-wasting sites, helping teams stay focused and secure.
Reduces IT workload	Fully managed by TPx — we handle setup, monitoring, and maintenance so your team doesn't have to.
Delivers clear insight	Monthly reports show top threats and blocked activity to guide smarter security decisions.

How It Works

Step 1: Quick Deployment – TPx installs lightweight DNS agents or configures your network for DNS routing — with zero disruption to users.

Step 2: Intelligent Threat Detection – All DNS requests are routed through TPx's secure, cloud-based filtering system powered by **Webroot® Threat Intelligence**, identifying and blocking known malicious domains instantly.

Step 3: Policy Enforcement & Web Filtering – Administrators can apply customizable rules for acceptable use, compliance, and content filtering to meet business and regulatory needs.

Step 4: Continuous Monitoring & Reporting – TPx monitors DNS activity 24/7 and provides regular reports summarizing blocked threats, trends, and compliance performance.

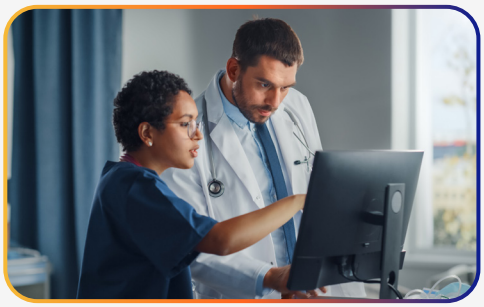
Why TPx?

Powered by Webroot® Threat Intelligence

Trusted by over 90 security vendors worldwide for real-time, high-accuracy threat detection.

Fully Managed Service

TPx handles setup, monitoring, and updates to keep you protected without added complexity.

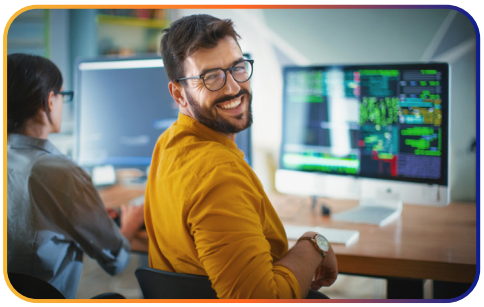


Customizable Policies

Tailor Internet access controls and threat-blocking rules to your unique organizational needs.

One Partner for IT & Security

Strengthen your security stack with TPx-managed solutions for endpoints, firewalls, and email defense.



Protect Every Connection

Every device, user, and Internet request is a potential entry point for attackers. TPx DNS Protection closes that gap with intelligent, proactive, and fully managed defense.

Don’t wait for the next phishing campaign or malicious redirect to hit your business.

Visit TPx.com today to see how DNS Protection can strengthen your first line of defense.