Endpoint Security
Managed DNS Protection

Protect devices from Internet threats anytime, anywhere

Domain Name System (DNS) Protection can greatly reduce the effectiveness of ransomware, phishing, botnet, and malware campaigns by blocking known-malicious domains[1]. This important security solution can be used to protect all endpoints, including servers, workstations, and IoT devices. It blocks as much as 88% of Internet-based threats before they hit your network or endpoints[2].

Why should I implement DNS Protection?

Protect against Internet threats Defend against Internet-based threats by blocking and filtering traffic to/from malicious sites, sites infected with malware, or sites with questionable or dangerous content.

Enforce compliance and policy DNS protection offers increased visibility and control over Internet use, which helps you maintain compliance and enforce corporate Internet use policy.

Safeguard remote users Endpoint DNS Protection helps remote devices and users maintain strong security when outside the corporate network.

Why should I choose TPx?

Leading threat intelligence TPx DNS Protection service is powered by Webroot's world-class Threat Intelligence, which is trusted by over 90 network and security technology vendors worldwide to enhance their own solutions.

Flexible deployment options TPx DNS protection can be used to safeguard any device that accesses the Internet. Deploy TPx DNS protection on Windows devices to protect users while on your network or while traveling. Need to protect IoT devices, servers, or devices accessing your Wi-Fi network? Deploying TPx DNS at the network edge allows complete protection regardless of device type.

Fully managed TPx delivers a turn-key solution that leaves you free to run your business. Our team professionally onboards your service and our support team is available 24x7x365 to assist.

[1] Cybersecurity & Infrastructure Security Agency (CISA) [2] Webroot

How It Works

Traffic Redirection Internet-based traffic to/from your endpoints is routed through a secure cloud infrastructure to create a highly secure, resilient, private, and manageable connection to the Internet.

Advanced Filtering Automated filtering blocks requests to undesirable, dangerous, or malicious internet domains. Support for DNS over HTTPS (DoH) is included to increase security through filtering encrypted Internet traffic.

Best-in-class Threat Intelligence Data correlation between domains, URLs, IPs, files, mobile apps, and more provides a comprehensive and continuously updated view of the Internet threat landscape — not just URLs and IPs.

What's Included?

Anytime, Anywhere Protection Individual device agents protect Windows systems and users from Internet threats while on your network or roaming.

Security for Any Device DNS Protection installed on your network gateway protects servers, IoT devices, wireless users, and other systems for comprehensive location-based security.

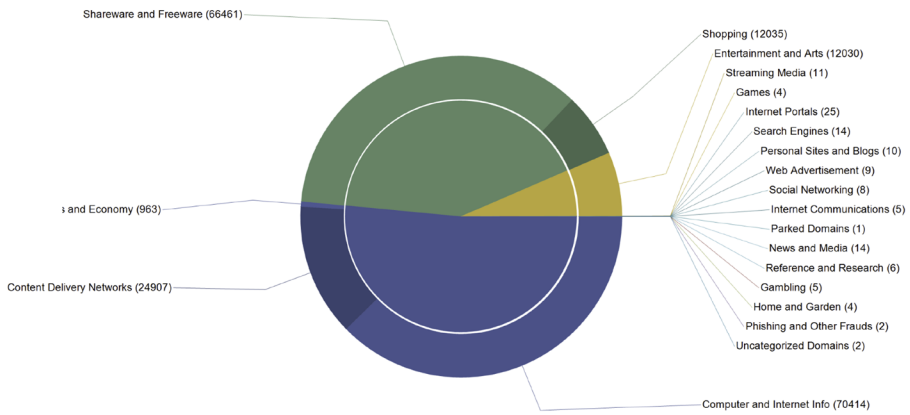
Customized Security Policies DNS protection policies can be customized using TPx recommended templates to address the different security needs of your users.

Monthly Reporting Customers automatically receive a comprehensive monthly report that provides visibility into your organization's Internet use and security.

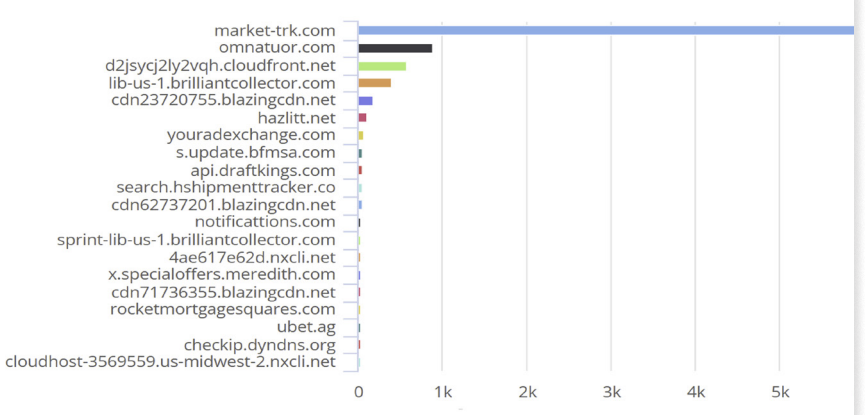
24/7/365 Helpdesk Support You can rely on our experienced resources to ensure that your DNS protection solution remains effective and meets your compliance and policy requirements.

TPx's Managed Detection and Response is powered by WEBROOT an opentext company Webroot BrightCloud® Internet Threat Intelligence

DNS: TOP BLOCKED CATEGORY



DNS: TOP BLOCKED DOMAIN



Managed DNS Protection is an integral part of TPx's security services portfolio for protecting endpoints and users from ransomware and other cyberattacks. Bundling multiple services can increase your overall value and improve your organization's security. Below is our current portfolio of Endpoint and User Security and Management services.

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.	■		
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.	■		
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.	■		
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.	■		
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.		■	
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.		■	
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.		■	
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.			■
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.			■

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.