Managed Firewalls

Expertise | Passion | Technology

Security artisans bring expertise, passion, and technology to cybersecurity.

Cybersecurity technology is meaningless unless properly configured, monitored, and maintained

Outdated software and unmanaged devices leave your company open to cyber threats. Erroneous configurations give hackers a way around your security assets.

The TPx team and its group of highly trained security professionals will configure, deploy, manage, and monitor your next generation firewall (NGFW) to help protect your business from cyber threats.

Our people defending your business and your people

TPx Managed Firewall service shields organizations and their employees with enterprise-grade security for a fraction of the cost of a single security analyst. The service includes certified security analysts who combine human intelligence with AI and threat intelligence driven data to find and terminate threats before they impact your business.

Our cybersecurity experts manage and monitor your firewall and when threats are found, they immediately take action to

We can provide a co-managed solution that allows TPx to work closely with your IT team through a common change management system and process.

neutralize them. While in-house solutions can take years and hundreds of thousands of dollars to develop to full maturity, our rapidly deployed service offers immediate value and added safeguards for businesses. You may know firewalls for security and their ability to block today's advanced threats, but with Managed Firewalls, the benefits go far beyond that. Secure access, visibility and control are major advantages that can help your business be more productive.

Secure Access SD-WAN enables organizations to leverage multiple transport services (e.g. broadband internet, 5G, etc.) to connect users securely and economically to applications and each other, while a Virtual Private Network (VPN) connects remote workers.

Visibility With detailed reporting by TPx, know what is happening on your network — from the top applications running and the top websites being visited, down to which users are on the VPN.

Control Once you know what is happening on your network, you can take action to control your network, so your productivity is maximized. Want to stop bandwidth and time-draining applications like video streaming? The choice and control are in your hands.

75% of SMBs could not continue operating if they were hit with ransomware.
- 2021 CNBC | Momentive Q3 Small Business Survey

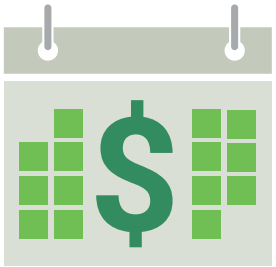
Managed Detection and Response

Managed Firewalls with Managed Detection and Response does more than block suspicious IP addresses and preconfigured static signatures, it augments existing firewall controls with dedicated security analysts who combine context, deep security understanding and expertise with today's advanced technology to make data actionable. We detect the threats other technologies miss. But it isn't enough to just detect threats. When a breach happens or an attack is transpiring, response time is critical, as is knowing how to respond. We know and treat your network like our own and this allows us to orchestrate a rapid, coordinated, and effective response to threats ensuring your business thrives and your people are better protected.

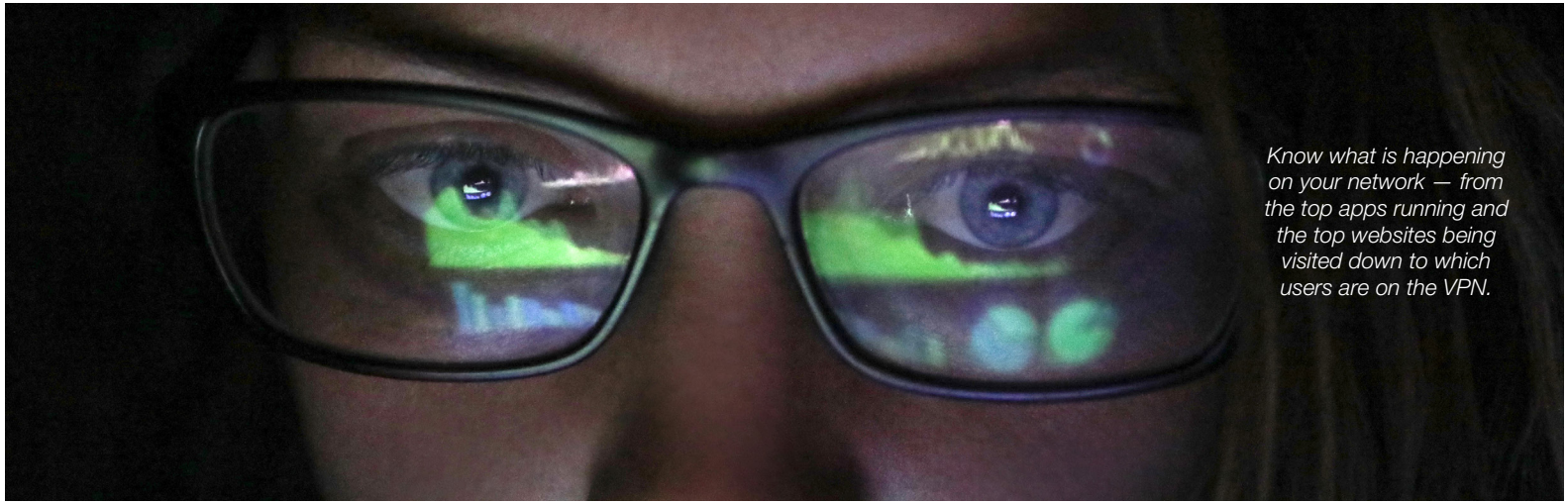
Avoid business debilitating threats

Our managed firewall solution will help you:

- Fortify your security posture
- Limit downtime due to network outages or crippling cyber attacks
- Meet your compliance challenges
- Free up resources to focus on business-driving initiatives
- Enable productivity with safe, secure, high-performance communications with partners, suppliers, customers, and remote employees
- Realize the immediate value of your security investment



For businesses that have cybersecurity measures in place, or are developing a plan, the most popular forms of protection are antivirus software (58%), firewalls (49%), VPNs (44%), password management tools (39%), and secure payment processing tools (38%).
- 2022 Digital.com Survey



Know what is happening on your network — from the top apps running and the top websites being visited down to which users are on the VPN.

Protect investments

We ensure businesses realize the full value of their firewall investments and we help protect their critical assets by providing:

- Continuously trained, seasoned security professionals
- 24/7 health monitoring and troubleshooting
- Customized device configuration and tuning
- Updates and patch management
- Log retention and reporting
- Licensing
- Hardware assurance
- Configuration backup and storage

HIPAA and PCI Compliant

Our people and processes undergo the scrutiny of third-party audits to ensure we meet and exceed HIPAA and PCI industry standards.

Solution features include:

- Managed detection and response
- Threat intelligence
- Sandboxing
- Vulnerability scans
- SD-WAN
- Anti-virus
- Web filtering
- Application control
- Intrusion prevention
- SSL deep packet inspection
- Web application firewall
- Data leak prevention
- Traffic shaping
- Policy scheduling
- Site to site IPsec
- Active directory integration
- VPNs with 2-factor authentication
- 5G/4G failover
- Third-party access vendor support
- Wireless access point and switch integration and management

For SMBs, the average cost of downtime in 2019 was $141,000.

Our people and processes undergo the scrutiny of third-party audits to ensure we meet and exceed HIPAA and PCI industry standards.

Service Descriptions

Managed Firewalls

All base administrative features available for Managed Firewalls are supported in all the service tiers. The onboarding and implementation processes for all service levels are identical. The difference between the service levels lies in how the changes to the equipment profile are managed, feature availability, and the amount of monitoring provided.

Managed Firewalls: Core — Customer Administrative Responsibility
Managed Firewalls: Optimum & Secure — TPx Administrative Responsibility
Managed Firewalls: Optimum & Secure — TPx and Customer Shared Administrative Responsibility

Service Features	Core	Optimum	Secure
24/7/365 Support Center	■	■	■
Base Administrative Features			
PCI and HIPAA Compliance	■	■	■
24/7 Firewall Monitoring		■	■
Product Licensing	■	■	■
Mgmt of Manufacturer Support/Response	+	■	■
Hardware Assurance/Equipment RMA	+	■	■
Configuration Management	+	■	■
Firewall Configuration Backup and Storage		■	■
Troubleshooting	+	■	■
Firmware Research and Upgrades	+	■	■
Firewall Vulnerability Patching	+	■	■
Log Retention	40 days □	120 days □	365 days ■
Reporting	+	All template reports	Custom reports
Firewall Access	Read/ write	Default read-only	Default read-only
Solution Features			
SD-WAN	+	■	■
Gateway Anti-Virus	+	■	■
Web Filtering	+	■	■
Application Control	+	■	■
Intrusion Prevention (IDS/IPS)	+	■	■
SSL Deep Packet Inspection		■	■
Traffic Shaping	+	■	■
Policy Scheduling	+	■	■

Solution Features (cont.)	Core	Optimum	Secure
Site-to-Site IPsec VPN Tunnels	Limit 5	■	■
SSL-VPN for Remote Users	Limit 20 No Limit with AD	Limit 20 No Limit with AD	Limit 20 No Limit with AD
Routing	+	■	■
Single Sign-On	+	■	■
Portal	■	■	■
Managed Detection & Response — SOC Active Log Monitoring	n/a	n/a	■
Threat Intelligence	n/a	n/a	■
Data Leak Prevention (DLP)	n/a	n/a	■
Sandboxing	□	n/a	■
Monthly Vulnerability Scan	□	□	■
Web Application Firewall	n/a	n/a	■
Add-on Features			
Wireless Access Point (Wi-Fi) Management	+	□	□
Switch Management	+	□	□
Firewall Accessories	□	□	□
High Availability	□	□	□
2-Factor Authentication	□	□	□
5G/4G Failover	□	□	□
Third-Party Vendor Support	□	□	□

■ *Included – monthly cost*
□ *Available – additional cost*
\+ *Included – (time & materials costs for post-install support)*

TPX.COM