Vulnerability & Penetration Scanning

Find and Fix Security Weaknesses Before Attackers Exploit Them

Cyber threats evolve daily, and **unpatched vulnerabilities remain one of the biggest security risks.** Studies show that **57% of data breaches** are due to **poor patch management,** with an average time of **102 days** to apply a security patch (Ponemon Institute).

TPx's **Vulnerability & Penetration Scanning** (VPS) provides **automated, intelligence-driven security scanning** to identify **critical weaknesses** in your network before cybercriminals exploit them.

Pinpoint security flaws before attackers find them

Understand the real risk behind vulnerabilities

Prioritize the most critical threats based on industry standards

What Is It & Why You Need It

Most businesses don't know where they are vulnerable—until it's too late. TPx's **Vulnerability & Penetration Scanning Service (VPS)** provides continuous **security scanning** and **risk validation** using automated tools that simulate **how attackers would attempt to exploit your network.**

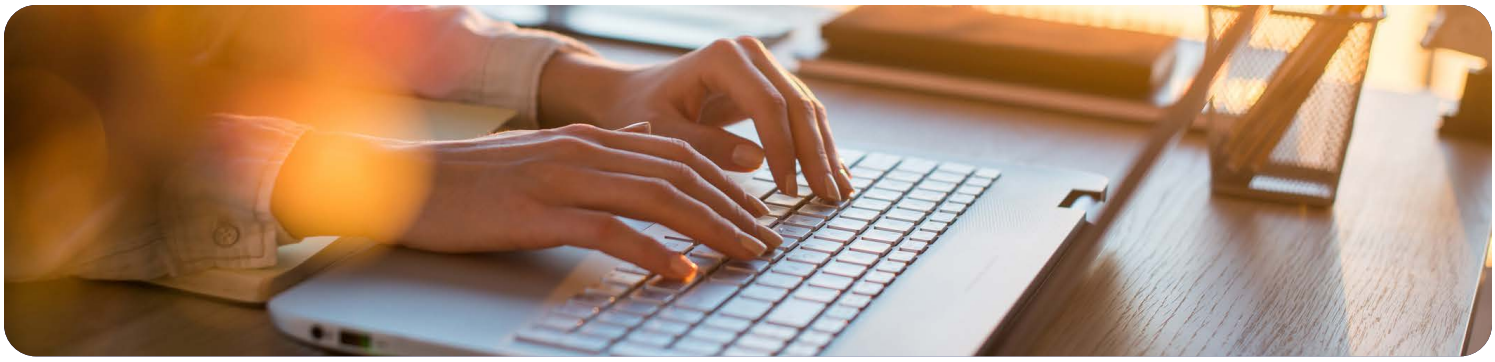
This service is **critical for businesses that:**

- Want to **proactively manage vulnerabilities** instead of reacting to breaches.
- Need to **prioritize security fixes** based on real risk factors.
- Must comply with **industry regulations** like PCI-DSS, HIPAA, and FTC Safeguards.

Not all vulnerabilities pose the same risk. Our automated scans **help you focus on what truly matters.**

Key Benefits

Benefit	What It Means for You
Proactive Risk Reduction	Identify and fix vulnerabilities before attackers exploit them.
Threat-Based Prioritization	Focus on high-risk vulnerabilities, not just generic threats.
Regulatory & Compliance Support	Helps meet PCI-DSS, HIPAA security standards.
Automated Scanning with Expert Analysis	Get accurate, validated security insights—without false alarms.
Comprehensive Security Reporting	Actionable insights for both security teams and executives.
Ongoing Risk Monitoring	Track security improvements over time.



How It Works

1 Vulnerability Scanning

What It Does:

Scans network-connected devices for known security flaws such as:

- Open ports
- Exposed services
- Unpatched software.

How It Helps:

- Uses manually written signatures to detect known vulnerabilities.
- Identifies misconfigurations and software weaknesses.
- Helps organizations prioritize patching and system updates.

2 Automated Penetration Scanning

What It Does:

Simulates automated attacks to validate vulnerabilities found during scanning.

How It Helps:

- Tests if identified vulnerabilities are exploitable in real-world conditions.
- Reduces false positives by eliminating vulnerabilities that pose no real threat.
- Highlights urgent security risks that require immediate action.

Unlike manual penetration testing, this process is fully automated and designed for continuous security monitoring.

3 Optional: Vulnerability Management Plan Review

What It Does:

Evaluates your security program and patching process to ensure best practices are followed.

How It Helps:

- Reviews policies, compliance, and security workflows.
- Identifies gaps between your vulnerability response plan and industry best practices.
- Provides strategic recommendations to strengthen your security posture.

Why TPx?

More Than Just a Scan—A Cybersecurity Partner

TPx doesn't just provide **automated reports**—we provide **real security insights** to help you make **informed decisions** and improve your **defense strategy.**

- **Security Thought Leaders** – Built on **CISSP, NIST, and ISO 27000** best practices.
- **Enterprise-Grade Protection for SMBs** – Advanced security solutions tailored for **any business size**.
- **Actionable Reports with Expert Guidance** – We don't just give you data—we **help you understand what to fix first.**
- **Continuous Risk Monitoring** – Track security **trends and improvements over time.**

Ready to Strengthen Your Cyber Defenses?
Let's talk. Visit TPx.com today.