STROZ FRIEDBERG
A LevelBlue Company

SERVICE BRIEF

Network Penetration Testing

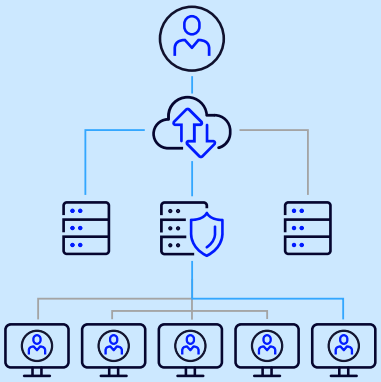
STROZ FRIEDBERG
A LevelBlue Company

Stroz Friedberg's Network Penetration Testing Services

Stroz Friedberg's Network Penetration Testing services evaluate networks using the same Tactics, Techniques, and Procedures ("TTPs") that an attacker would likely use to identify and exploit vulnerabilities.

The goal of Stroz Friedberg's Network Penetration Testing is to simulate the actions of a malicious attacker, aiming to gain unauthorized access to critical systems and sensitive data. Additionally, it assesses security best practices and identifies common vulnerabilities. The results offer an assessment of the potential risks posed to the environment.

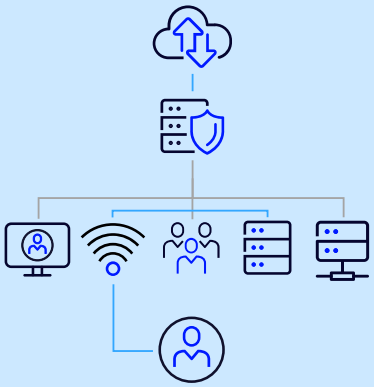
1 External



External Network Penetration Testing

The Stroz Friedberg team specializes in internet-facing infrastructure, hosts, services, and applications. Our team simulates an attacker aiming to breach perimeter controls and access the internal network and sensitive data.

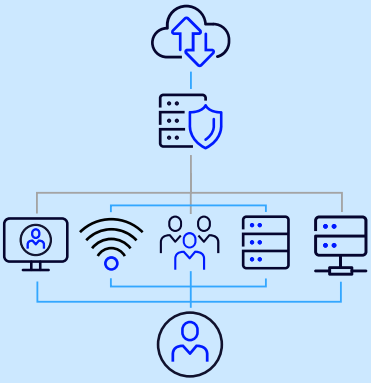
2 Wireless



Wireless Penetration Testing

This testing is designed to evaluate wireless networks for both common and sophisticated security vulnerabilities, including access point discovery, RF signal range testing, traffic analysis, vulnerability profiling, vulnerability exploitation, rogue device detection, encryption evaluation, weak authentication methods, and insecure configurations.

3 Internal



Internal Network Penetration Testing

This testing simulates an attacker who has already gained access and is moving laterally within the network. While many organizations focus on hardening the external perimeter, many attacks originate from phishing, insider threats, zero-day exploits, or other attacks that bypass external security controls to gain access to the internal network. Results from internal penetration testing help harden the internal environment to aid in defending against such attacks.

STROZ FRIEDBERG
A LevelBlue Company

About Stroz Friedberg

Stroz Friedberg, a LevelBlue company, delivers intelligence-driven digital risk management with expert-led services designed for adaptive resilience.

With over 25 years of leading the resolution of the most complex, high-stakes digital risk issues, we manage the entire digital risk lifecycle – from cyber threats and insider risks to IP theft and regulatory compliance. Our approach combines managed security services with expert analysis and strategy, supported by threat intelligence gathered from thousands of engagements across various industries.

We translate complex technical and legal risks into actionable strategies, helping CISOs and legal teams turn digital risks into board-ready insights. Our comprehensive services include managed cyber defense, digital forensics and incident response, trade secret protection, expert witness support, threat intelligence, security strategy and governance, attack path mapping and testing, and resilience engineering.

Operating as one trusted partner, we align technical precision with business priorities to protect critical assets, adapt to evolving threats, and maximize ROI through proven outcomes. Through LevelBlue's portfolio, these specialized services integrate seamlessly with 24/7 managed security operations and AI-driven threat detection for comprehensive digital risk protection.

Cybersecurity. Simplified.

levelblue.com/strozfriedberg