NetSPI™

AI-Enabled Penetration Testing

Stay Ahead of AI-Driven Threats

The Challenge

As threat actors increasingly leverage AI to scale attacks and enhance effectiveness, the demands on security teams grow exponentially. Staying ahead requires more precision, time, and resources than ever before. The most effective way to counter these evolving threats is to embrace AI yourself—proactively securing your organization while automating workflows.

The Solution

NetSPI's unique blend of people, process, and technology prepares organizations to securely adopt AI. Our AI-powered platform and expert-led AI/ML security services enable faster innovation without introducing new risks.

AI/ML Penetration Testing

With more applications and SaaS providers adopting LLM capabilities, security and privacy risks are rising. Without proper evaluation, users may manipulate LLMs, expose sensitive data, generate unauthorized content, or trigger unintended actions. Application updates and model changes make regular testing essential.

NetSPI helps organizations proactively secure AI through three core offerings: LLM web application testing to uncover evolving vulnerabilities, benchmarking and jailbreaking assessments to measure resilience and track security trends, and customized AI testing that evaluates data pipelines, algorithms, adversarial risks such as model extraction, inference, and evasion. By combining advanced adversarial testing methodologies with expert analysis, NetSPI enables organizations to confidently adopt and scale AI while minimizing risk.

Learn More

NetSPI™

AI-Enabled Platform

Modern penetration testing demands both speed and precision as environments grow more complex and attackers scale operations with automation. Traditional manual testing alone can't keep pace. That's why NetSPI embeds AI throughout the testing lifecycle—to accelerate analysis, streamline workflows, validate remediation, and reduce manual effort.

While our expert testers remain at the core of every engagement, we use the latest and most modern technologies, including AI-based solutions, to make testing faster, smarter, and more effective. By integrating AI across our product development and throughout the pentesting engagement lifecycle, we boost efficiency, enhance quality, and deliver impactful solutions that keep pace with modern threats.

NetSPI has developed AI-powered tools that enhance both the customer and tester experience. Our expert testers use advanced in-house capabilities like the **LLM benchmarking tool**, which automates AI model evaluation and jailbreak testing to generate measurable insights on susceptibility and bias; a credential manager that streamlines large-scale credential validation across web and network engagements; and a voice cloning tool for realistic, authorized vishing simulations. For customers, our AI chatbot provides instant access to documentation and insights, making it easier to find answers and understand results.

Together, automation, human expertise, and privacy-by-design make NetSPI the most effective penetration testing solution in the modern AI landscape—built to move faster, deliver high quality results, and drive meaningful impact for our customers and our teams alike.

Learn More

You Deserve The NetSPI Advantage

Human Driven

- **350+ pentesters**
- **Employed, not outsourced**
- **Wide domain expertise**

AI-Enabled

- **Consistent quality**
- **Deep visibility**
- **Transparent results**

Modern Pentesting

- **Use case driven**
- **Friction-free**
- **Built for today's threats**

About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) and leads the industry in modern pentesting. Combining world-class security professionals with AI and automation, NetSPI delivers clarity, speed, and scale across 50+ pentest types, attack surface management, and vulnerability prioritization. The NetSPI platform streamlines workflows and accelerates remediation, enabling our experts to focus on deep dive testing that uncovers vulnerabilities others miss. Trusted by the top 10 U.S. banks and Fortune 500 companies worldwide, NetSPI has been driving security innovation since 2001. NetSPI is headquartered in Minneapolis, MN, and available on **AWS Marketplace**. Follow us on **LinkedIn** and **X**.