NetSPI™

Merger & Acquisition (M&A) Security Testing

Minimize risk and maximize ROI of your investments with NetSPI Merger & Acquisition (M&A) cybersecurity assessment package

The most trusted products, services, and brands are secured by NetSPI

The Challenge

"More than one in three executives surveyed said they have experienced data breaches that can be attributed to M&A activity" – *IBM*[1]

M&A activity expands an organization's attack surface, creating more targets for adversaries to exploit. In today's fast-paced M&A landscape, companies face the critical challenge of thoroughly assessing cybersecurity risks within condensed due diligence timeframes. Decision-makers must quickly identify potential vulnerabilities, misconfigurations, and security gaps in target companies without delaying the transaction process, yet incomplete or rushed security assessments can lead to costly post-acquisition remediation efforts or unexpected liabilities that significantly impact deal value and integration success.

The Solution

NetSPI delivers best-in-class M&A cybersecurity assessments for both due diligence or post-acquisition with unmatched speed in scheduling and execution, beginning assessments with rapid turnaround time. Our proven experience across M&A security testing provides acquisition teams with comprehensive, actionable intelligence including real-time findings (no waiting on final pentest reports), executive readouts and summaries, and necessary release documents — all delivered through the NetSPI Platform. We enable your team to reduce investment risk by revealing the complete cybersecurity risk profile of target companies, empowering more informed decisions throughout the merger and acquisition process.

- Reduce investment risk and enable informed M&A decisions
- Rapid deployment to meet short M&A timelines
- Real-time reporting of actionable findings in The NetSPI Platform

> **"The announcement of a merger, acquisition, or partnership spikes interest among cybercriminals... Bad actors often seize these opportunities to test an organization's systems, data architecture, and access points."**
>
> OliverWyman[2]

[1] IBM, Assessing cyber risk in M&A, Published September 2020.
[2] Cyber Risk Due Diligence,A Game Changer For Healthcare M&A, Published February 2025.

Delivered on The NetSPI Platform:

The NetSPI Platform simplifies M&A security by identifying vulnerabilities, modeling attack paths, and prioritizing risks in real-time. Gain visibility, accelerate remediation, and safeguard assets during mergers and acquisitions.

Application Testing:

✓ Web ✓ Mobile ✓ Thick ✓ API ✓ Virtual

Comprehensive pentesting for web, mobile, thick client, API, and virtual applications uncovers vulnerabilities from both authenticated and anonymous perspectives utilizing manual techniques and automated tools to address multiple attack scenarios effectively.

Network Testing:

✓ Internal ✓ External

Detect vulnerabilities in internet-facing and internal systems with actionable remediation guidance. Combining automated tools and manual testing, risks like misconfigurations, patch issues, and privilege escalation are mitigated using frameworks such as NIST 800-53 and MITRE ATT&CK. Enhance security posture and meet compliance requirements.

Cloud Testing:

✓ AWS ✓ Azure ✓ GCP

Secure cloud environments by leveraging advanced manual and automated testing, uncovering vulnerabilities, misconfigurations, and security risks across AWS, Azure, and GCP platforms. Gain actionable insights to protect assets and ensure compliance.

Secure Code Review:

SAST and SCR services detect vulnerabilities early in the development lifecycle. By using automated tools, manual testing, and reviews, issues like injection attacks, insecure logic, and weak encryption are fixed pre-deployment, saving costs and ensuring compliance.

Kubernetes:

Thorough Kubernetes infrastructure assessments follow NIST 800-53, NSA/CISA hardening standards, and best practices. Identify vulnerabilities, privilege escalation paths, unauthorized data access, and other risks for a comprehensive and controlled evaluation.

AI/ML Testing:

Secure AI-driven systems by identifying risks in LLM models with advanced benchmarking and jailbreaking techniques. Tailored assessments mitigate risks, improve model resilience, and provide actionable insights to protect evolving applications.

External Attack Surface Management (EASM):

Continuous discovery, monitoring, and manual validation of internet-facing assets, exposures, and vulnerabilities. Combining advanced technology and expert validation, reduce risks in real time by identifying shadow IT and prioritizing critical threats.

Cyber Asset Attack Surface Management (CAASM):

Real-time visibility into internal and cloud assets reveals vulnerabilities and security control gaps. CAASM integrates seamlessly with existing tools, delivering contextual insights and enabling effective risk prioritization, compliance, and governance.

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**.