

NetSPI and Synack: Continuous Offensive Security at AI Scale

What has closed, and what is not changing?

NetSPI and Synack have officially closed their merger, bringing together two complementary approaches to offensive security. NetSPI contributes a large in-house testing organization, specialist coverage for legacy and physical technology, attack surface management and breach and attack simulation. Synack contributes Sara AI Pentesting, a vetted global researcher community, continuous and point-in-time PTaaS and human validation of exploitability.

Nothing changes for existing engagements as a result of the close. Testing cadence, scope, platform access and points of contact stay the same, and customers and partners should continue working with their current representatives.

The Combination at a Glance

Transaction Closed: Definitive agreement announced September 2, 2026. The merger officially closed in October 2026, following customary closing conditions and regulatory approvals.

Combined Scale: More than 13 million hours of real-world offensive security testing, over \$200 million in combined revenue and nearly 40 years of combined operating history.

Human Depth: 350+ NetSPI in-house pentesters and 1,500+ vetted Synack Red Team researchers, two different delivery models rather than one larger pool.

Testing Breadth: 50+ NetSPI penetration testing types, plus Synack continuous and point-in-time PTaaS across modern attack surfaces and Synack Advanced Services.

Federal Posture: The Synack security testing platform is FedRAMP Moderate Authorized. This authorization applies specifically to the Synack platform, remains unchanged by the merger, and does not extend to NetSPI products or any future combined offering.

No Change Today: Existing cadence, scope, platform access and points of contact stay the same.

Why the combination matters for security teams

Cover more of the attack surface

Both companies test modern applications, APIs, cloud, infrastructure and AI systems. NetSPI adds specialist depth across mainframe, hardware, IoT and OT. Synack adds continuous testing and a global researcher community. Together that is a wider set of assets and technology types that can enter an assurance program,

Multiply expertise with AI

Purpose-built and agentic AI expand what expert testers can reach. Sara AI Pentesting runs real-world attacks at a scale traditional pentesting cannot match, and findings are validated by human experts. The point is augmentation. Neither company positions AI as a replacement for expert judgment.

Prove what is actually exploitable

Scanner output and attack surface data tell you where exposure might be. They do not tell you what an adversary can reach and use. Human-validated exploitability, security control evidence and remediation context give teams a defensible basis for what to fix first.

Operate continuously without losing depth

Continuous testing keeps changing surfaces under recurring scrutiny, while specialist, compliance and point-in-time assessments stay where the technology, risk or regulation demands them. The two models are complementary, not alternatives.

Connect exposure to action

Asset visibility, prioritization, offensive testing, defensive control validation, remediation and retesting belong in one flow. NetSPI integrates penetration testing, attack surface management and breach and attack simulation. Synack connects asset discovery, validated findings, patch verification and reporting. The combination is intended

About NetSPI+Synack

NetSPI+Synack is a leader in continuous offensive security, combining elite human expertise with agentic AI to help organizations identify, validate, prioritize, and remediate exploitable risk. Its platform delivers continuous, expert-validated testing across the attack surface at enterprise scale, giving security teams the clarity to distinguish vulnerability noise from what represents real risk. With global reach and more than 13 million hours of real-world offensive testing experience, NetSPI+Synack serves many of the world's largest enterprises and government organizations with one ambition: nothing left to exploit.

"Organizations need validated findings they can trust, backed by security professionals who understand exploitability, context and business risk."

NETSPI AND SYNACK MERGER ANNOUNCEMENT, SEPTEMBER 2026

For partners:

Continue to transact through your current Synack or NetSPI partner motion and your existing representative. No combined SKU, pricing or channel program has been announced. Your partner manager can help map customer attack surface, coverage gaps and specialist requirements to the broader offensive security story.

Read the joint announcement at netspi.com/netspi-and-synack/ or the full [press release](#).

NetSPI and Synack have officially closed their merger. The transaction was announced on September 2, 2026 and closed in October 2026, following customary closing conditions and regulatory approvals. The combined company continues to honor existing customer and partner engagements, with cadence, scope, platform access and points of contact unchanged. A product integration roadmap has not yet been published.

**Talk to your account team to learn what the
NetSPI + Synack merger means for you.**

How NetSPI and Synack Complement Each Other

NetSPI Today	Synack Today
Human offensive talent	
350+ in-house pentesters, positioned as an extension of the customer's team.	1,500+ vetted Synack Red Team researchers in a global research community.
AI-enabled pentesting	
An AI-accelerated platform with agentic MCP integrations, supporting discovery through validation. July 2026 added Continuous Web Application, Continuous AI and Continuous Internal Penetration Testing, plus Continuous AI Findings Validation, which applies expert human judgment to the output of AI-driven tooling.	Sara AI Pentesting, generally available since May 2026. Sara runs real-world attacks against the same scoped assessment a human researcher would use, at a fraction of the credit cost, and every finding is validated by human experts before it reaches the customer.
Application and infrastructure testing <i>(comparable coverage on both sides)</i>	
Web, API, mobile, thick and virtual applications, internal and external networks, AWS, Azure and GCP, and AI/ML.	The same surfaces, delivered point in time or continuously: web applications, APIs, mobile, cloud, hosts, internal environments and AI/LLM systems.
Specialist and advanced testing	
z/OS mainframe, hardware systems, automotive, medical devices, IoT, ATMs and OT, plus Kubernetes, wireless, LLM and source code review.	Advanced Services, delivered by the Synack Red Team: attack surface analysis, cloud testing, focused research, security benchmarks, compliance and vulnerability checklists, CVE missions and mission retests.
Attack surface visibility	
360-degree monitoring of internal and external assets, cloud misconfigurations, dark web exposures, and fraudulent domains.	Attack Surface Discovery and Asset Insights: inventory, fingerprinting, testing history and vulnerability context to decide what to test next.
Control and exposure validation <i>(NetSPI adds breach and attack simulation)</i>	
Breach and attack simulation across endpoint, network, SIEM and related defensive controls.	Human-led and agentic testing that proves which weaknesses are exploitable, with exploit evidence, remediation guidance and patch verification.
Workflow and remediation <i>(closely comparable)</i>	
A platform centralizing penetration testing, attack surface management and breach and attack simulation, with vulnerability prioritization.	Discovery, validated findings, vulnerability management, patch verification and reporting, with coverage analytics and the Attacker Resistance Score.