

# Next Evolution of Pentesting





## Enhanced Capabilities for Modern Security Challenges

The expanding attack surface and ever-changing perimeter puts your security controls to the test. Gaining and maintaining visibility into all assets, vulnerabilities, and exposures is a noisy, time-consuming challenge. NetSPI is enhancing our penetration testing as a service (PTaaS) to tackle these challenges and provide significantly more value with every engagement. When you purchase a penetration test with NetSPI, you now receive continuous security capabilities that extend far beyond traditional point-in-time testing.

Our enhanced penetration testing combines AI technology, proven processes, and in-house security expertise to deliver a comprehensive approach to securing what matters most to you and your customers. We're introducing significant improvements to provide you with the most advanced penetration testing capabilities available.

## Now Included with Every NetSPI Penetration Test

- Continuous External Monitoring:** Weekly external asset discovery scans and continuous dark web monitoring of up to 2 domains to maintain ongoing visibility of your external attack surface between point-in-time assessments.
- Cloud Security Coverage:** Weekly AWS security configuration scans to identify misconfigurations, vulnerabilities, and exposed endpoints across your cloud infrastructure.
- Self-Service Attack Simulation:** Access to self-service playbook creation and lightweight agent for execution, allowing you to simulate real-world attacks from our extensive library of over 600 attack scenarios, or customize and create your own.

		Other Pentesting Vendors	NetSPI Pentesting
 <b>Testing and Reporting</b>	Program and findings management	X	X
	Remediation testing	X	X
	Trend analysis and real-time dashboards	X	X
	PDF reports	X	X
 <b>Attack Surface Visibility</b>	Asset inventory and deduplication	X	X
	External asset discovery scans (weekly)		X
	AWS security configuration scans (weekly)		X
	Dark web monitoring (up to 2 domains)		X
 <b>Vulnerability Prioritization</b>	Prioritization based on exposure, impact, and exploitability (CVE, CVSS, CPE, EPSS, KEV, and more)	X	X
 <b>Attack Simulation</b>	Self-service playbook creation and lightweight agent for execution		X
	Automated detection verification and coverage reporting		X
	Vendor coverage comparison		X
<b>Integrations</b>	Open API	X	X
	Integrations for assets, vulnerabilities, identities, detective controls, and remediation		X

## Flexible Integration Choices to Fit Your Environment

NetSPI penetration testing integrates seamlessly with your existing security stack. Our integration options ensure that security insights are not only visible but immediately actionable within your current workflows, with the flexibility to customize your setup based on your organization’s specific infrastructure needs.

You can tailor your integration configuration across different capability areas while maintaining comprehensive security coverage. Our open API provides additional flexibility for organizations requiring custom integrations beyond our standard offerings.

### Integration Categories Available

- **Attack Surface Visibility Integration:** Choose up to three complimentary integrations across asset management (AWS, Azure, Jamf, Automox, Microsoft Intune, CrowdStrike Falcon, Microsoft Defender, SentinelOne Singularity), identity management (Okta, JumpCloud, Microsoft Azure Active Directory, Microsoft Active Directory OnPrem), and vulnerability assessment (AWS Cloud Security Configuration Monitoring, Tenable Vulnerability Management API) solutions.
- **Attack Simulation Integration:** All detective control integrations included with unlimited access to Carbon Black Cloud, CrowdStrike Falcon, DefenseStorm GRID, Microsoft Defender, Microsoft Sentinel, SentinelOne Singularity, Splunk Cloud, and Splunk Enterprise.
- **Expedited Remediation Integration:** Choose one complimentary workflow management integration between Jira and ServiceNow for seamless remediation tracking and ticketing system integration.

 <h3>Attack Surface Visibility</h3> <p><i>Choose up to three</i></p> <table border="0"> <tr> <td data-bbox="110 1165 365 1470"> <b>Assets</b> <ul style="list-style-type: none"> <li>• AWS</li> <li>• Azure</li> <li>• Jamf</li> <li>• Automox</li> <li>• Microsoft Intune</li> <li>• CrowdStrike Falcon</li> <li>• Microsoft Defender</li> <li>• SentinelOne Singularity</li> </ul> </td> <td data-bbox="381 1165 698 1354"> <b>Identity</b> <ul style="list-style-type: none"> <li>• Okta</li> <li>• JumpCloud</li> <li>• Microsoft Azure Active Directory</li> <li>• Microsoft Active Directory (OnPrem)</li> </ul> </td> <td data-bbox="714 1165 1036 1312"> <b>Vulnerabilities</b> <ul style="list-style-type: none"> <li>• AWS Cloud Security Configuration Monitoring</li> <li>• Tenable Vulnerability Management API</li> </ul> </td> </tr> </table>	<b>Assets</b> <ul style="list-style-type: none"> <li>• AWS</li> <li>• Azure</li> <li>• Jamf</li> <li>• Automox</li> <li>• Microsoft Intune</li> <li>• CrowdStrike Falcon</li> <li>• Microsoft Defender</li> <li>• SentinelOne Singularity</li> </ul>	<b>Identity</b> <ul style="list-style-type: none"> <li>• Okta</li> <li>• JumpCloud</li> <li>• Microsoft Azure Active Directory</li> <li>• Microsoft Active Directory (OnPrem)</li> </ul>	<b>Vulnerabilities</b> <ul style="list-style-type: none"> <li>• AWS Cloud Security Configuration Monitoring</li> <li>• Tenable Vulnerability Management API</li> </ul>	 <h3>Attack Simulation</h3> <p><i>Included</i></p> <ul style="list-style-type: none"> <li>• Carbon Black Cloud</li> <li>• CrowdStrike Falcon</li> <li>• DefenseStorm GRID</li> <li>• Microsoft Defender</li> <li>• Microsoft Sentinel</li> <li>• SentinelOne</li> <li>• Singularity</li> <li>• Splunk Cloud</li> <li>• Splunk Enterprise</li> </ul>
<b>Assets</b> <ul style="list-style-type: none"> <li>• AWS</li> <li>• Azure</li> <li>• Jamf</li> <li>• Automox</li> <li>• Microsoft Intune</li> <li>• CrowdStrike Falcon</li> <li>• Microsoft Defender</li> <li>• SentinelOne Singularity</li> </ul>	<b>Identity</b> <ul style="list-style-type: none"> <li>• Okta</li> <li>• JumpCloud</li> <li>• Microsoft Azure Active Directory</li> <li>• Microsoft Active Directory (OnPrem)</li> </ul>	<b>Vulnerabilities</b> <ul style="list-style-type: none"> <li>• AWS Cloud Security Configuration Monitoring</li> <li>• Tenable Vulnerability Management API</li> </ul>		
<h3>Expedited Remediation</h3> <p><i>Choose up to one</i></p> <ul style="list-style-type: none"> <li>• Jira</li> <li>• ServiceNow</li> </ul>				

### About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) with its AI-powered platform supported by more than 350 in-house cybersecurity experts. Specializing in 50+ pentest types, attack surface visibility, vulnerability prioritization, and attack simulation, NetSPI delivers security testing with unprecedented clarity, speed, and scale. Trusted by 90% of the top 10 U.S. banks and many Fortune 500 companies, NetSPI sets the standard for modern AI-driven pentesting. Founded in 2001 and headquartered in Minneapolis, MN, NetSPI is available on the AWS Marketplace. Follow us on LinkedIn and X.