NetSPI™

ASM

NetSPI Attack Surface Management

NetSPI ASM uses a combination of human intelligence and a variety of tools to discover, inventory, and manually test known and unknown assets and vulnerabilities on your external attack surface.

Continuous monitoring of your external attack surface alerts you to assets, exposures, and potential vulnerabilities in real time, allowing you to drastically reduce risk.

Manual validation, prioritization, and evidence verification information of findings eliminates alert fatigue, allowing your team to focus on what matters.

Continuous external perimeter scanning

NetSPI ASM uses a combination of commercial, open-source, and proprietary techniques to discover and assess internet-facing assets, including known and unknown IPs, domains, Autonomous System Numbers (ASNs), and more. Additionally, we integrate directly with the cloud service providers AWS, Azure, and GCP to monitor cloud accounts for externally facing IPs and domains.

Our continuous and comprehensive automated scanning against discovered assets consists of full 65535 TCP port scans with both ping and no ping methods, UDP port scanning, and vulnerability assessments for network and web applications. All services on live assets are then identified and cataloged, enhancing our visibility into the operational landscape of your network. The continuous aspect of NetSPI ASM allows you to know about vulnerabilities as soon as they occur to drastically reduce exposure time and risk.

Validation and prioritization

NetSPI's in-house security experts bring over 20 years of penetration testing experience across various practices and industries, utilizing curated knowledge, and a combination of manual and automated review. We add severity rankings and additional context such as location, description, remediation instructions, verification instructions, discovery chains, evidence verification, and more for each finding. This saves you and your team time and money, allowing you to tackle other tasks and further reduce risk.

Our methodology for ASM adheres to frameworks including the NIST 800-53 special publication, Payment Card Industry Data Security Standards (PCI DSS) penetration test requirements and guidelines, and established industry best practices. This ensures a thorough and compliant testing process that leverages our extensive expertise to deliver high-quality results. Furthermore, NetSPI's vulnerability severity rating system prioritizes delivering contextual information. Using a combination of CVSS scores, the Center for Information Security (CIS) Benchmarks, PCI DSS standards, and our internally developed criteria, enhanced by published CVE data and CISA KEV listings. This system allows us to effectively prioritize and manage risks, ensuring that vulnerabilities are addressed efficiently and in alignment with the latest security standards and insights.

Remediation assignments and SLAs

Accelerate remediation efforts by assigning SLAs and designated remediators to vulnerabilities and manage them through the remediation life cycle. You can supplement NetSPI's assigned severity with your own rating allowing further customization of the vulnerability management process. Also, when remediations are complete, you can flag a vulnerability "Ready for Retest" which lets our team know it is time to validate remediations were successful.

Asset discovery

Provide NetSPI with a single domain, and we will discover and inventory the rest. Using our combination of commercial, open-source, and proprietary scanning tools, we discover known and unknown assets such as domains, IP addresses, cloud accounts, ASNs, and more. Pre-configured and customized tagging ensures findings are organized in the most impactful way to you and your business. We inventory, tag, and categorize them to deliver easy review and sorting for your team.

Reporting and trend analysis

Dashboards update in real time with a clean UI in a single platform so that you can get a clear picture of your external attack surface assets, vulnerabilities, and report over time with ease.

- **Attack Surface Dashboard** is designed for managing your attack surface. It provides information on Team Activity, Live IP, Live Domain, Open Port, and Management Port changes. Here you can also find Vulnerability Severity summaries, Geographic IP Locations, Top Service Ports, and more.
- **Executive Summary Dashboard** is designed for reporting. Here you can find summary graphs displaying asset vulnerability status, top vulnerabilities, expiring SSL/TLS certificates, and more. Adjustable timeframes allow you to use this for weekly team meetings, monthly management meetings, or even quarterly board reporting.
- **Signal Dashboard** highlights the amount of data generated by ASM, reviewed by the ASM security experts, and alerted to you. Our goal is to reduce as much noise as possible to allow your team to focus on what matters and let us handle the rest.

Integrations

Seamlessly integrate NetSPI ASM with your existing technology stack to streamline efforts and save countless hours of manual labor. NetSPI ASM integrates with ticketing systems, asset management tools, vulnerability scanners, and more for easy, improved time to remediation. You can also use an API to instantly connect the tools you use with simple integration guides – no coding needed. All integrations and API connections are included at no additional cost.

Program management

When you work with NetSPI, you get a programmatic approach with strategic guidance. Our white glove customer support and advisory programs work together to help deliver successful outcomes. Our dedicated NetSPI ASM security experts are comprised of in-house pentesters that help augment your security team and prioritize what matters most for remediation.

Custom vulnerability triggers

Create customized alerts for the events you care about, such as domains being discovered, certificates expiring, management ports being publicly available, and more. Receive daily, weekly, or monthly updates based on your preference. Vulnerability triggers allow you to know about the scenarios that you want to know about, when you want to know about them.

Company hierarchy view

Visualize your company subsidiaries, divisions, or acquisitions that may be directly or indirectly related. NetSPI ASM utilizes scanning technology and human intelligence to discover each part of your organization and how they are connected to each other. This allows your teams to take a complete, unified approach to managing each individual part. Regardless of its relation to your business, it is critical to be aware of it and protect your organization from any associated risks.

Detailed discovery chain

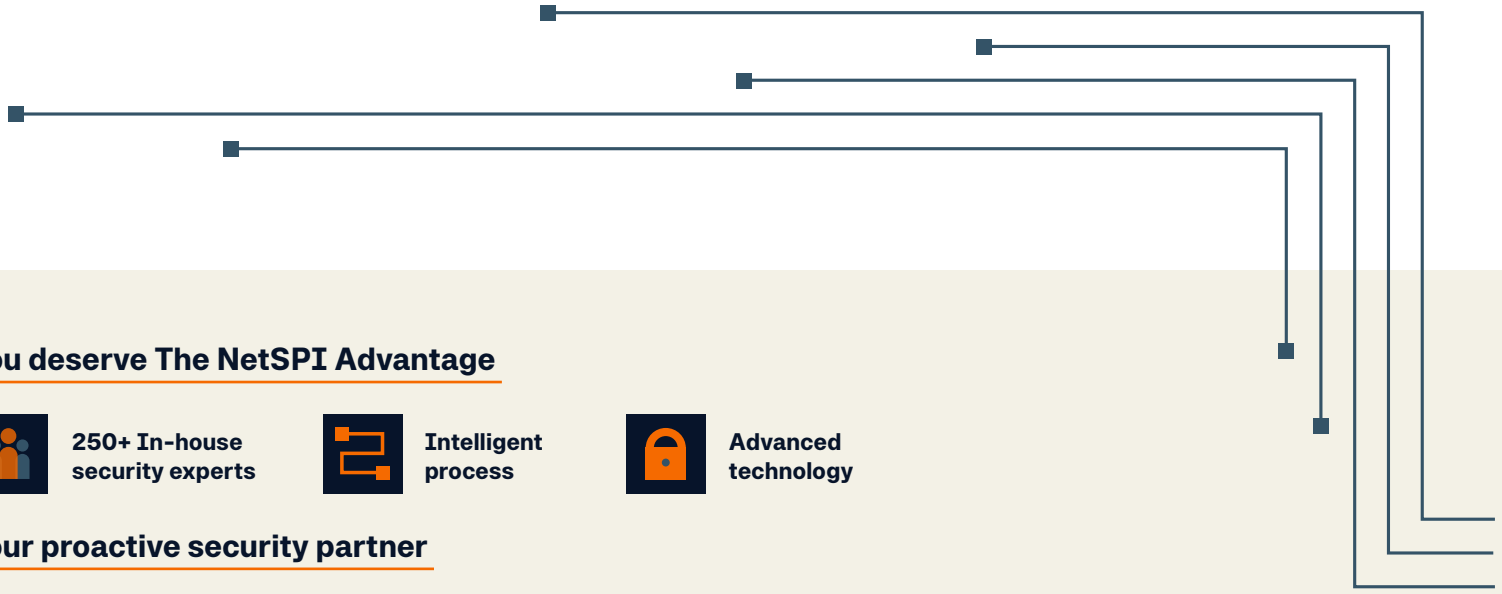
Understand how the NetSPI ASM security experts were able to discover and exploit a vulnerability with step-by-step visualization. This evidence verification shows how a user was able to discover as asset, then find an exposure on the asset, and then turn that exposure into a vulnerability. This information is made available for each discovered vulnerability so that your team can quickly locate and remediate exposures or vulnerabilities at each step of the exploitation journey.

Perceptual hashing

NetSPI ASM routinely takes screenshots of all websites on your global attack surface using perceptual hashing. Perceptual hashing, sometimes referred to as perceptual image hashing or perceptual sorting, analyzes these screenshots and categorizes them based on similar looks, styles, layouts, and images. These groups of screenshots are then reviewed by NetSPI ASM security experts to identify trends in your network or find outliers of websites running on your perimeter, and then notify your team.

No setup or specialized systems required

All we need is one domain, and your company will be on its way to improved security. We scan your external perimeter in the same ways that malicious attackers do, using an external and unauthenticated approach, to discovering assets and exposures. NetSPI ASM does not require downloads, specialized configurations, or any other environment changes to begin working. Our ASM security experts work with you for fast and easy onboarding so you and your team can start using NetSPI ASM almost immediately, delivering a fast time to value.



You deserve The NetSPI Advantage

250+ In-house security experts

Intelligent process

Advanced technology

Your proactive security partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), Attack Surface Management (ASM), and Breach and Attack Simulation (BAS).

NetSPI™

Key: No capability ○ ◔ ◑ ◕ ● Robust capability

FEATURES	VULNERABILITY SCANNERS	SECURITY RATING TOOLS	OTHER ASM VENDORS	NETSPI ASM
SCANNING				
Scan tools	Commercial open source	Commercial open source	Commercial open source proprietary	Commercial open source proprietary
Scan depth	Medium	Shallow	Medium	Deep
Scanning activation	Manual	Manual	Automated	Automated
Scanning frequency	On-demand	Variable	Variable	Continuous
Asset discovery	○	◔	◑	◕
Vulnerability discovery	◕	◔	◑	●
VULNERABILITY MANAGEMENT				
Real-time vulnerability reporting	●	●	●	●
Human finding validation	○	○	◔	●
Vulnerability deduplication	◔	○	◔	●
Finding prioritization	◑	◑	◑	◕
Severity scoring	◑	◑	◕	●
False positive tuning	◔	◑	◑	●
Custom tagging	○	◕	◕	◕
Findings context	◔	◔	◑	●
Asset attribution	○	◔	◕	◕
Asset contextualization	◔	◔	◑	◑
Custom remediation SLAs	○	○	○	●
Remediation testing	○	○	◔	●
REPORTING				
Reporting frequency	On-demand	On-demand	On-demand	Instant
PDF/CSV report	✓	✓	✓	✓
Annual NetSPI platform access	○	○	○	✓
HUMAN DELIVERED				
Dedicated project manager	○	○	○	✓
Dedicated solutions architect	○	○	○	✓
Dedicated client delivery manager	○	○	○	✓
Security expert support	○	○	○	✓
INTEGRATIONS				
Integration capabilities	○	○	○	Jira, Service Now, Microsoft Teams, Azure Sentinel, Github, and over 1,000 more
API	○	○	○	✓