NetSPI™

EASM

NetSPI External Attack Surface Management (EASM)

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

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

A mix of automated and manual validation, prioritization, and evidence verification of findings eliminates alert fatigue, further reducing risk and allowing your team to focus on what matters.

Always-on external perimeter security

NetSPI EASM 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), subsidiaries, and more. Additionally, we integrate directly with cloud service providers like AWS, Azure, and GCP to monitor cloud accounts for external-facing IPs and domains.

Our always-on and comprehensive automated scanning against 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 assets are then identified and cataloged, enhancing our visibility into the operational landscape of your network. The always-on approach of NetSPI EASM allows you to know about assets and 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 to each EASM finding. The NetSPI Agents add severity rankings and additional context to their findings, such as location, description, remediation instructions, verification instructions, discovery chains, evidence verification, and more. This saves you and your team time and money, allowing you to tackle other tasks and further reduce risk.

Our EASM testing methodology adheres to frameworks including the NIST 800-53 special publication, Payment Card Industry Data Security Standards (PCI DSS), 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 uses a combination of CVSS scores, EPSS scores, the Center for Information Security (CIS) Benchmarks, PCI DSS requirements, and our internally developed criteria, enhanced by published CVE data and CISA KEV listings to provide actionable context. Using industry standards and proprietary in-house systems 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 and manage them through the remediation life cycle by assigning SLAs and designated remediation owners to vulnerabilities. You can supplement NetSPI's assigned severity with your own rating to customize 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 of your external attack surface assets. By leveraging a blend of commercial, open-source, and proprietary scanning tools, we identify both known and unknown assets, including domains, IP addresses, cloud accounts, ASNs, and more. Our pre-configured and customized tagging system ensures that these findings are organized in a manner that is most beneficial to you and your business. We meticulously inventory, tag, and categorize each asset to facilitate easy review and sorting for your team.

Reporting and trend analysis

Asset repository and dashboards update in real time with a user-friendly UI in The NetSPI Platform so that you can get a clear picture of your external attack surface assets, vulnerabilities, and reporting.

- **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, noise reduction metrics, geographic IP locations, top service ports, and more.
- **Executive Summary Dashboard** is designed for reporting. View summary graphs outlining 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.

Integrations

Seamlessly integrate NetSPI EASM with your existing ticketing, remediation, and security technologies to streamline efforts and save countless hours of manual labor. NetSPI EASM 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 partner with NetSPI, you get a programmatic approach with strategic guidance. Our white glove customer support and advisory programs work together to deliver successful outcomes. Communicate with our NetSPI EASM security experts throughout your engagement to help augment your security team, answer questions, and streamline efforts.

Custom policy 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

NetSPI EASM utilizes scanning technology and human intelligence to visualize your company subsidiaries, divisions, or acquisitions that may be directly or indirectly related. This includes visualizing how they are connected for deeper context. With this level of insight, your team can take a complete, unified approach to managing each individual part. Regardless of an asset's relation to your business, it is critical to be aware of it and protect your organization from any associated risks.

Findings attack path

NetSPI EASM provides powerful visualization, identifying and mapping the potential step-by-step approach to gain access to your environment on tested assets. Graphic representation further contextualizes findings, empowering security teams with possible adversary routes to enhance prioritization and remediate gaps before adversaries can exploit risks.

Severity scoring

Each asset and vulnerability is assigned a severity score to establish a level of risk associated with a finding. NetSPI EASM assigns scores from informational to critical. This provides further context, empowers prioritization, and enables effective resource allocation to tackle the most critical findings first.

Detailed discovery chain

Understand how the NetSPI EASM 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 an asset, then find an exposure on the asset, and then turn that exposure into a vulnerability. This information is made available for each vulnerability discovered so that your team can quickly locate and remediate exposures or vulnerabilities at each step of the exploitation journey.

Perceptual hashing

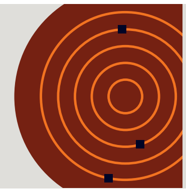
NetSPI EASM routinely takes screenshots of all websites on your global attack surface using perceptual hashing. Perceptual hashing, sometimes referred to as perceptual image hashing or perceptual sorting, analyzes these screenshots and categorizes them based on similar looks, styles, layouts, and images.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

Similar findings

Looking within the details of a finding will also display findings located on other assets that are similar. This capability allows teams to group findings and remediations together easier and faster, streamlining remediations, while also uncovering potential business or security process gaps.

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 way that malicious attackers do, using an external and unauthenticated approach to discovering assets and exposures. NetSPI EASM does not require downloads, specialized configurations, or any other environment changes to begin working. Our EASM security experts work with you for fast and easy onboarding so you and your team can start using NetSPI EASM almost immediately.



Pair NetSPI EASM and CAASM for the complete Attack Surface Management Solution

- **Complete internal and external visibility**
- **Always-on attack surface coverage**
- **Deep asset and vulnerability context**

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), External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), and Breach and Attack Simulation (BAS).

Key: No capability ○ ◔ ◑ ◕ ● Robust capability

FEATURES	VULNERABILITY SCANNERS	SECURITY RATING TOOLS	OTHER EASM VENDORS	NETSPI EASM
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	○	○	○	✓

© 2024 NetSPI LLC | All rights reserved | 09.18.24