

# Attack Surface Management (ASM)

**Inventory, contextualize, and prioritize assets and vulnerabilities on your internal and external attack surface when you pair NetSPI EASM and NetSPI CAASM**

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

## The challenge




Only 17% of organizations can clearly identify and inventory a majority (95% or more) of their assets.<sup>1</sup>

Organizations are struggling to manage their expanding attack surface as technological environments become more complex and dispersed across on-prem, cloud, and SaaS solutions. While tools like configuration management databases (CMDB), asset discovery (AD), and scanners can be useful, they each offer only partial insights. These tools can be cumbersome to switch between, and often result in manual errors and gaps in information. Organizations require a solution that offers a comprehensive, real-time view of both internal and external attack surface assets and vulnerabilities.

## The solution

NetSPI External Attack Surface Management (EASM) and NetSPI Cyber Asset Attack Surface Management (CAASM), used together, delivers a complete attack surface management solution seamlessly on The NetSPI Platform.

NetSPI EASM delivers always-on external perimeter security, leveraging people, processes, and technology to uncover both known and unknown assets, while validating and prioritizing vulnerabilities. NetSPI CAASM offers real-time visibility across users, applications, devices, and clouds, mapping and correlating assets within your technology stack to identify risks and coverage gaps. Together, these products deliver internal and external asset and risk visibility, always-on coverage, and deep data context to empower security teams.

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



<sup>1</sup>Gartner: Innovation Insight: Attack Surface Management, Published: 09 April 2024



## Comprehensive asset visibility

**Gain a single, complete, and accurate view of your entire attack surface**

Inventory both internal and external attack surface assets and vulnerabilities by pairing NetSPI EASM and NetSPI CAASM. Identify and map assets as they are added to your environment, eliminating manual discovery efforts and maintaining an accurate list for you and your team.

- 360-degree attack surface visibility
- Real-time asset inventory, tagging, categorization, and querying
- In-depth risk and exposure management, prioritization, and validation



## Always-on coverage

**Identify assets, vulnerabilities, and coverage gaps in real-time**

EASM and CAASM always-on monitoring capabilities ensure your internal and external attack surfaces are protected around the clock. Real-time updates and 24/7/365 monitoring allow you to inventory assets and tackle vulnerabilities as they arise, minimizing the window of opportunity for attackers and significantly reducing risk.

- Always-on internal and external attack surface monitoring
- Real-time asset and vulnerability updates
- Automated and manual verification and de-duplication



## Actionable context and visualization

**Streamline prioritization and remediation throughout your environment**

Gain needed asset and vulnerability context throughout your entire attack surface to implement informed decision-making, prioritization, and resource allocation. View descriptions, severity, potential routes attackers could take, and the consequences of exploitation, all on The NetSPI Platform.

- Visualize asset relationships and potential exploit impacts
- View potential adversary attack routes and impact
- Simplified attack surface reporting and trend analysis

## 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).