

Cyber Asset Attack Surface Management (CAASM)

Inventory assets, find contextual relationships, and identify blind spots in security coverage and risks in real-time across your internal attack surface




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

The challenge

Organizations spend many hours manually trying to solve challenges of identifying and monitoring assets and associated risks because of static, manual, error prone, methodologies. Configuration management databases, combined with manual methods and other tools, are common ways to perform asset identification, management, and monitoring. Although helpful, they only provide part of the picture. In fact, 50% of security professionals said it is difficult to keep up with security hygiene and posture management due to growth and frequent changes in their attack surface.¹ Organizations need a solution that provides a complete internal asset and vulnerability view in real time.

The solution

NetSPI CAASM gives you visibility across users, applications, devices, and clouds so you can view your assets in real time, find contextual relationships, and identify risks. Extensive integration capabilities inventory, map, and correlate assets within your technology stack, identifying vulnerabilities, coverage gaps, and more. Finally, dashboards visualize internal attack surface data to enable action for your teams.

-  Complete internal asset visibility and contextualization
-  Real-time vulnerability and risk mapping
-  Enable teams with actionable asset and risk information

“The precision and speed with which we can now manage and analyze our IT assets have not only boosted our confidence in data accuracy but also significantly elevated our compliance and risk management capabilities. It’s not just a tool; it’s a game-changer”

Jeff Saginor
CTO, EJP Capital



Gain a holistic view of internal assets and their interconnectivity **Obtain complete visibility of internal assets using our pre-built connectors.**

Achieve an inventory of assets that update in real-time as they are added, changed, or removed from your environment, along with deep data contextualization on how they are connected to other assets and risk.

- Centralize internal attack surface asset inventory
- Visualize asset context and connections
- Aggregate, ingest, and deduplicate asset information in real time



Identify, validate, and prioritize attack surface exposures and vulnerabilities **Gain internal attack surface coverage and context to streamline remediations.**

Security experts purchase solutions that only provide part of the picture. NetSPI CAASM provides a complete, real-time view of your internal assets along with their related exposures and vulnerabilities.

- Identify vulnerabilities, coverage gaps, and inconsistencies in real-time
- Discover how asset vulnerabilities affect other assets (blast radius)
- Dynamic internal asset capture and visibility



Accelerate reporting and audit compliance **Protect your most valuable assets and align your organization with ease**

Create a comprehensive risk picture for security and IT teams to work together with leadership, governance, and compliance teams. Gain the visibility you need to comply with, report on, and keep pace with what matters most.

- Create reporting on what matters most
- Discover compliance, governance, and audit gaps
- Streamline IT compliance, governance, audit, and other reporting

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