NetSPI™

CAASM

NetSPI Cyber Asset Attack Surface Management (CAASM)

NetSPI Cyber Asset Attack Surface Management (CAASM) is designed to provide organizations with real-time visibility, analysis, and contextualization of internal digital assets in cloud and SaaS environments. This enables internal asset identification, risk-based remediation, and control gap identification in real-time, reducing the likelihood of cyberattacks and enhancing security posture. NetSPI CAASM integrates with dispersed IT and Security tools, aggregating data into a single location for deduplication, contextualization, and prioritization.

NetSPI CAASM equips organizations with an automated, proactive security tool and partner to enable Continuous Threat Exposure Management (CTEM) through discovery, inventory, and prioritization of assets and security risks associated with their internal-facing digital assets.

Key Use Cases for NetSPI CAASM Include:

- Build a consolidated view of your distributed assets to track known and previously unknown assets
- Add business context to your assets through automatic tagging based on customizable rules
- Enable risk-based remediation and quickly identify high risk assets and vulnerabilities
- Discover security control and SaaS offering coverage gaps
- Enhance the organization's ability to prevent breaches Improve an organization's security posture
- Reduce noise through patented asset deduplication methodology
- Enable streamlined reporting and decision making

Automated Asset Discovery, Inventory, and Mapping

NetSPI CAASM delivers real-time, comprehensive visibility across your internal attack surface through extensive API integrations with existing security tools. The platform can be leveraged to maintain real-time asset relationships and dependencies, automatically capturing and inventorying assets as they're added, changed, or removed from your environment, enabling dynamic asset identification of both known and unknown resources across users, applications, devices, and cloud infrastructure.

The platform provides holistic asset type coverage spanning industrial control systems, mobile devices, cloud resources, applications, and user identities through its elastic data ontology. This comprehensive cataloging creates a unified view of your complete attack surface, regardless of asset type or location.

Asset De-duplication

NetSPI CAASM patented deduplication methodology leverages multi-attribute matching algorithms and entity resolution that extends beyond basic hostname/IP matching to eliminate redundant asset data across disparate security tools, providing a single source of truth for your inventory. The system employs fuzzy logic matching against multiple identifiers, system characteristics, and behavioral patterns to achieve industry leading accuracy. This process enhances data quality, reduces security noise, and increases assurance and confidence in your security posture by preventing duplicate entries from skewing risk calculations.

Security Tool Coverage

Map security control deployment across your asset inventory, identifying where security controls have been properly implemented and where gaps exist. The system calculates real-time control coverage metrics at both asset and subnet levels using a distributed control assessment engine. This capability provides immediate visibility into which security systems (like EDR) have been deployed to which assets, enabling teams to quickly identify inconsistencies and control gaps across the entire attack surface and streamline compliance efforts.

Vulnerability Detection and Prioritization

NetSPI CAASM ingests vulnerability data from integrated security tools, correlating these findings with asset data to validate and prioritize remediation efforts. Identifying risks that might be missed by individual scanners, NetSPI CAASM provides risk-based vulnerability prioritization and deeply contextualized findings consolidated from disparate systems, helping security teams focus on the most critical issues first.

Risk Scoring and Contextual Insights

Using a multi-factor risk quantification model that combines vulnerability severity, asset criticality, exposure metrics, and business context through its knowledge graph architecture, NetSPI CAASM provides contextual understanding of how assets relate to other systems, users, and the broader environment. This contextual data enhances risk scoring by considering not just vulnerability severity but also asset importance, relations, and potential impact during security incidents.

Global Search

The platform features powerful querying capabilities that enable security teams to immediately locate and analyze assets, vulnerabilities, and related controls across the entire environment. This global search functionality allows teams to respond to emerging threats in seconds.

See how NetSPI CAASM Global Search capability streamlined EAB Global's response during the CrowdStrike incident to uncover 43 impacted machines in 15-seconds.

Agentless Approach

NetSPI CAASM operates entirely agentlessly (except for optional virtual appliances for on-premises integration), eliminating deployment overhead while enabling rapid implementation and immediate value. This approach allows organizations to connect technologies to CAASM within minutes and begin collecting information immediately without requiring endpoint agent installation.

Integrations

The platform offers agentless integrations with your existing technology stack, ensuring end-to-end visibility without installing new software. NetSPI CAASM connects seamlessly with security tools through pre-built connectors, creating a unified view of assets, vulnerabilities, and controls.

NetSPI CAASM integrates with common Cloud, IAM, MDR, UEM, and VM tooling, including but not limited to:

- **Microsoft AD:** Comprehensive integration with Microsoft Active Directory for identity and access management visibility
- **Microsoft Azure:** Deep visibility into Azure cloud resources, configurations, and security controls
- **AWS:** Expansive AWS cloud resource discovery and risk assessment capabilities
- **Crowdstrike Falcon:** Integration with Falcon endpoint protection for device security posture
- **Splunk:** Connection to Splunk SIEM data for comprehensive security event correlation
- **Tenable Vulnerability Management:** Incorporation of Tenable vulnerability scan results for a unified risk view

Comprehensive Reporting and Dashboarding Capabilities

The platform visualizes attack surface data through dashboards tailored to provide value for each role, from junior analysts to executives. These dashboards enable stakeholders to immediately answer questions, visualize potential impact of vulnerabilities, and prioritize resources based on real-time data.

- **Overview Dashboard:** Provides a high-level view of the entire attack surface, including asset counts, vulnerability trends, and control coverage metrics
- **Cloud Dashboard:** Offers specialized visualization of cloud infrastructure assets, risks, and security posture across cloud environments

Tagging

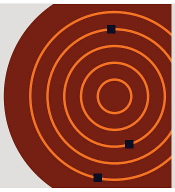
The platform supports comprehensive asset tagging capabilities, enabling organizations to categorize and organize assets based on custom criteria. This functionality enhances search, reporting, and risk assessment capabilities by allowing teams to quickly filter and analyze assets based on relevant attributes.

Asset Lineage

NetSPI CAASM tracks relationships between assets through its knowledge graph, providing visual representation of asset connections and dependencies. This lineage mapping enables security teams to understand how assets relate to each other, facilitating impact analysis and remediation planning.

Data Export

The platform supports flexible data export capabilities, including JSON, CSV, and more, allowing security teams to extract asset, vulnerability, and control data for integration with other security processes or tools. This functionality enables organizations to leverage NetSPI CAASM data in broader security workflows and reporting.



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

300+ In-House Security Experts

Intelligent Processes

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) as a Service.