NetSPI™

Cyber Asset Attack Surface Management (CAASM)

Discover and monitor assets, security controls coverage gaps, and enable risk-based remediation in real-time across your entire attack surface.

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

The Challenge

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 spend many hours manually trying to identify and monitor known, unknown, or forgotten assets and their related risk. Current asset identification, management, and monitoring processes and tooling, although helpful, only provide part of the picture and are often static, manual, and error prone. The longer assets are unknown or poorly managed, the greater the risk due to vulnerabilities and improper patch management. Organizations need a solution that provides complete internal asset and risk view in real time.

The Solution

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

- Discover and monitor internal and cloud assets
- Map security control coverage and discover gaps
- Prioritize remediation guidance focused on asset and compliance risk

> **"When the CrowdStrike incident happened, I knew I had 43 impacted machines within 15 seconds... How do I know that? Because we have CrowdStrike integrated with NetSPI CAASM."**
>
> Brian Markham,
> CISO, EAB Global

[1] Enterprise Strategy Group (ESG) by TechTarget: Research Report: Security Hygiene and Posture Management Remains Decentralized and Complex

NetSPI™

Gain a Holistic View of Known and Unknown Internal Assets and Their Related Risk

Gain complete visibility of internal assets in your environment 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 their security control coverage and risk.

- Identify known and unknown assets and their related risk
- Enable risk-based remediation through policy engine and contextualized findings
- Gain visibility to security control coverage gaps such as endpoint detection deployment

Map Security Control Coverage and Discover Gaps

Identify and inventory internal attack surface exposures, vulnerabilities, and control coverage with deep context.

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 vulnerabilities and risks.

- Identify vulnerabilities, coverage gaps, and inconsistencies in real-time
- Gain validated and prioritized findings with severity and risk scoring for each asset
- Dynamic internal asset capture and visibility

Enable Risk-Based Prioritization and Remediation

Protect your most valuable assets and align your organization with ease.

Leverage policy engine and contextualized findings to create a comprehensive risk picture for security and IT teams throughout your internal attack surface. Gain the visibility you need to comply with, report on, and keep pace with what matters most.

- Streamline reporting on what matters most
- Discover compliance, governance, and audit gaps
- Integrate with clouds, networks, IAM, MDR, vulnerability management, and more

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.