NETSPI™

Attack Surface Management

ASM

Detect unknown and potentially vulnerable public-facing assets before bad actors do with continuous penetration testing and attack surface management.

IDENTIFY & PROTECT
THE UNKNOWN

The global attack surface is growing faster than we know. Today, security leaders and technical teams are challenged by the lack of visibility into their internet-facing assets, unknowingly leaving numerous network entry points susceptible to exploit.

SC Labs' analysis of the external attack surface management category suggests that high-profile breaches such as Equifax, Buffer, Cottage Health System, and the persistent Log4j incidents all follow a similar pattern: There was a risky public exposure that organizations were not aware of.

Without proper visibility, inventory, and understanding of your external attack surface, you cannot have peace of mind that your organization is secure. "You don't know what you don't know" is NetSPI's attack surface management mantra. By identifying all assets through continuous pentesting – from network assets to credentials exposed on GitHub to assets found on the dark web – you gain the ability to better secure your attack surface and ultimately reduce your risk.

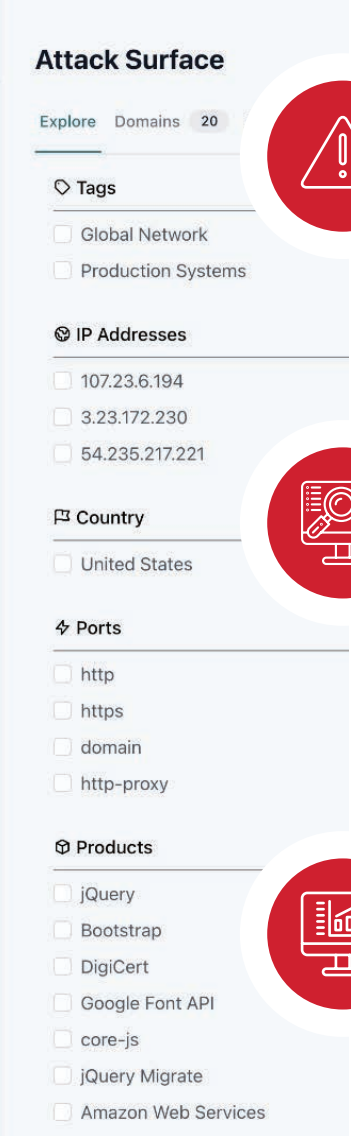
ASM

NETSPI'S
ATTACK SURFACE MANAGEMENT

What it IS	What it ISN'T
An automated, dynamic technology platform enriched by our global, human pentesting team	A siloed service or technology; rather you get the ASM technology enabled by our experts
Continuous pentesting to identify and inventory your known and unknown internet-facing assets	A noisy vulnerability scanner – NetSPI's tests are targeted to only alert you when a high-risk asset is found within your attack surface
A solution to shadow IT and asset management challenges	A Configuration Management Database (CMDB) – but we do integrate with CMDBs and help keep them up to date
An opportunity to focus and supplement your network penetration testing strategy	A replacement for vulnerability management tools nor manual penetration testing – Attack Surface Management fills an existing gap between the two

THE HUMAN IMPACT

Modern attack surface management requires the human touch to help provide context around assets that could cause the most harm to your business. That's why NetSPI's human expertise is an essential component of our service. Here are three core ways to leverage our Attack Surface Management security consultants:



Exposure Triaging

If NetSPI or your internal team notices an asset that looks risky on the surface, our team will jump in to manually investigate for exposures (vulnerabilities, technologies, exposed public data, etc.). Tapping into our pentesting and red teaming roots, we help organizations determine risk levels and prioritize your remediation efforts.

ASM Reviews

On a cadence that makes sense for your organization, we will schedule a review of your attack surface. During the meetings, your NetSPI team will provide insights into the assets and details that should matter most. Our insights are based on intelligence gathered from thousands of comprehensive pentests and our deep-rooted understanding of TTPs used by real attackers.

Improve your Pentests

Attack surface management informs your external penetration testing teams to drive the most comprehensive results. It identifies key areas that warrant further testing and enables your team to focus on manual testing techniques to find business-critical vulnerabilities tools often miss. Plus, you'll have a direct line to the top pentesting organization in the world: NetSPI.

ATTACK SURFACE MANAGEMENT IN ACTION

- Continuous/always-on penetration testing
- M&A due diligence
- Asset discovery and monitoring
- Attack surface reduction
- External asset management
- Third party vendor discovery
- Risk prioritization and validation
- Monitoring cloud workloads
- Dark web exposures

ATTACK SURFACE MANAGEMENT **FEATURES**

A DYNAMIC TECHNOLOGY PLATFORM

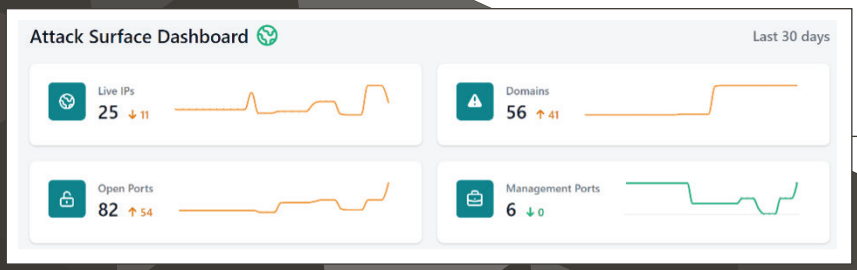
NetSPI's Attack Surface Management is enabled by an automated technology platform, accessible via an easy-to-use web application. The platform provides an interactive interface for continuous pentesting and efficient attack surface management.

SIMPLE SET UP

Provide us with your email address and we can run a full scan of your external network, identifying assets that may put your organization at risk of a cybersecurity breach. Provide us with additional information on your known domains and IPs to improve your results.

TRACK AND TREND DATA OVER TIME

Track your assets over time and measure your ability to protect and manage your attack surface via the platform dashboard.



ATTACK SURFACE MANAGEMENT FEATURES

ALWAYS-ON, CONTINUOUS PENTESTING

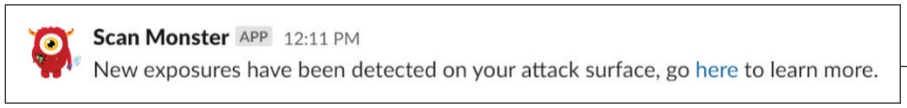
The platform interface is intuitive and driven by our powerful automated scan orchestration technology, Scan Monster, which has been utilized on the front lines of our pentesting engagements for years. Take comfort in the fact that the ASM platform is working continuously in the background, 24/7, 365 to provide you with the most comprehensive visibility of your external attack surface.

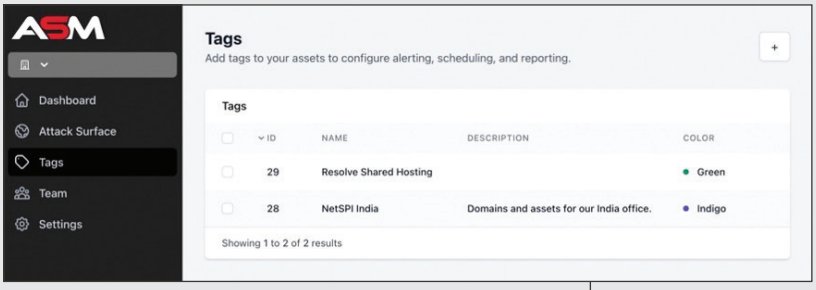
UNDERSTAND YOUR ASSETS

With every asset, we identify a broad spectrum of information – including but not limited to domains, DNS records, IP addresses, ports, products, and certificates. This information helps our penetration testers determine where they should focus their manual efforts.

REAL-TIME ALERTS

Scan Monster, your guide to NetSPI's Attack Surface Management platform, will alert you of high-risk assets in real-time through Slack and Teams integrations, email notifications, or in-platform alerts.





ATTACK SURFACE MANAGEMENT **FEATURES**

DOMAIN DISCOVERY

We discover domains through a multitude of automated and manual methods, including but not limited to public databases, SSL/TLS certificate parsing, subdomain brute forcing, and DNS record searching.

OSINT

Among our other discovery techniques, we leverage open source intelligence (OSINT) to identify publicly available data sources such as business entities, IP addresses, domains, employee information, and sensitive company data.

TAGGING

Use tagging to group assets together and create a risk view of your attack surface. Provide metadata about your assets, like whether they are hosted in an on-prem datacenter or in the cloud or what business processes they are associated with, to help drive prioritization and focus on the assets that are most important to your organization.

ATTACK SURFACE MANAGEMENT FEATURES

EXPOSED PORTS

Investigate your global attack surface for outliers and exposed ports.

GETTING **STARTED**

GAIN VISIBILITY INTO YOUR EXTERNAL ATTACK SURFACE TODAY.

Reach out to your NetSPI team to get started with Attack Surface Management.

sales@netspi.com

612-465-8880

ASM

ABOUT NETSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest healthcare companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve™ platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.