

# Attack Surface Management

PLATFORM DRIVEN. **HUMAN DELIVERED.**

Utilizing automated technology and expert human penetration testers to continuously discover, test and prioritize your global attack surface.

## 1. DISCOVER

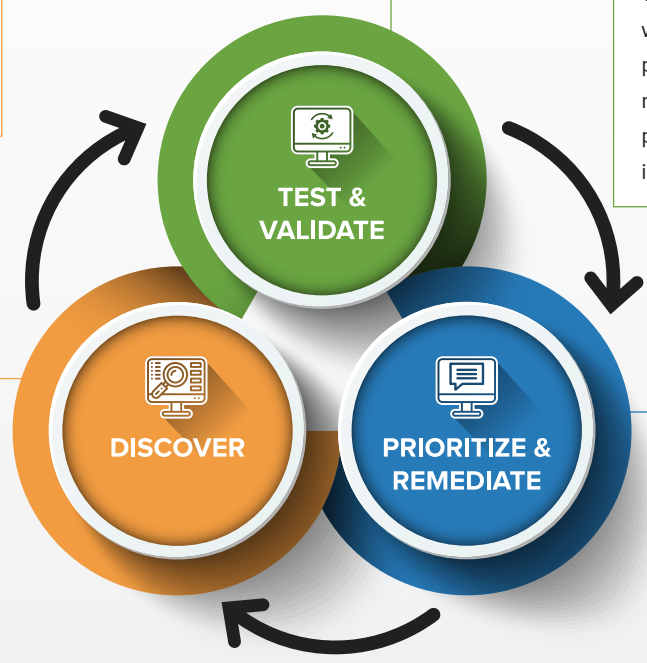
We use our exclusive technology to continuously scan your entire attack surface, mapping known and unknown assets within the primary company, subsidiaries, third-party vendors and more.

## 2. TEST & VALIDATE





We pair our technology with expert human penetration testers to manually validate and prioritize vulnerabilities in real time.

## 3. PRIORITIZE & REMEDIATE





Finally, we accelerate remediation by providing detailed discovery chains, bi-directional remediation guidance, and open API implementation.



### SOC TEAM CHALLENGES:

-  Rapidly changing attack surface
-  Alert Fatigue
-  Increasing workloads & limited staff
-  Lack of visibility

### HOW NETSPI'S ASM SOLVES THESE CHALLENGES:

-  Continuous monitoring
-  Manual exposure validation
-  Detailed discovery chains & access to global cybersecurity experts
-  Discovery of all known and unknown assets over time

## NETSPI ASM

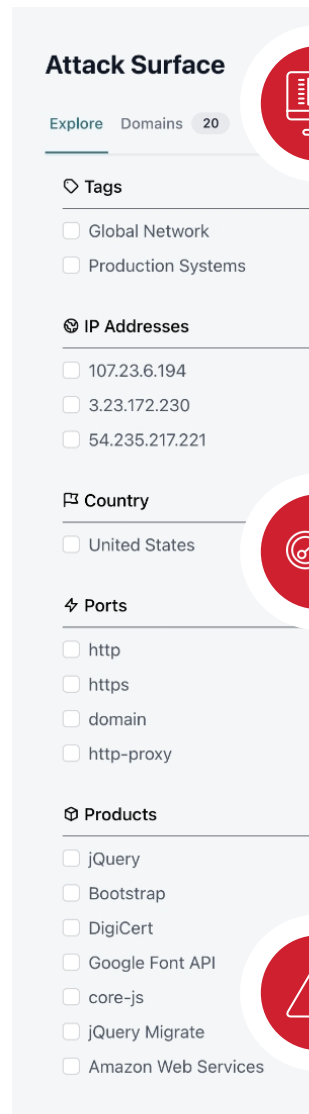
### KEY BENEFITS:

- Always-on, continuous penetration testing
- Asset discovery and monitoring
- Third party vendor discovery
- Manual pentest, triage and exposure validation
- Real-time exposure alerts
- Simplified company and subsidiary asset management
- Improved visibility, tracking and reduction of attack surfaces
- Open API integration

## WHY NETSPI?

NetSPI is the leader in enterprise security testing and attack surface management, partnering 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. NetSPI offers Penetration Testing as a Service (PTaaS) through its Resolve™ penetration testing and vulnerability management platform. Its experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces, historically testing over one million assets to find four million unique vulnerabilities. NetSPI, a KKR and Ten Eleven Ventures portfolio company, is headquartered in Minneapolis, MN, with global offices across the U.S., Canada, the UK, and India.

## NETSPI'S EXCLUSIVE HUMAN IMPACT



**Attack Surface**

Explore Domains 20

**Tags**

- Global Network
- Production Systems

**IP Addresses**

- 107.23.6.194
- 3.23.172.230
- 54.235.217.221

**Country**

- United States

**Ports**

- http
- https
- domain
- http-proxy

**Products**

- jQuery
- Bootstrap
- DigiCert
- Google Font API
- core-js
- jQuery Migrate
- Amazon Web Services



### Improved Penetration Testing

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.



### Project Team Review

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.



### Exposure Triaging

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

CONNECT WITH US  
TO LEARN MORE ABOUT  
**ATTACK SURFACE MANAGEMENT!**

<https://www.netspi.com/attack-surface-management>

