Attack Surface Protection

KEY VALUE

- Identify and reclaim unknown assets, services and shadow IT in order to ensure it is properly managed in the future
- Pinpoint and remediate vulnerabilities in all of your assets across your attack surface, before any incident occurs
- Minimize risk by reducing the amount of time vulnerabilities in your attack surface are exposed, using the automated, periodic scans
- Automated alerts inform you of any changes to your attack surface, eliminating the need for manual checking
- API integration can expedite the communication and remediation process in order to reduce exposure time and efforts
- Extend your monitoring capabilities to the cyber underground in order to identify a new class of threats that would otherwise remain undetected
- Take proactive steps to ensure this new class of threat cannot impact on your organization and its continued operation

Attack Surface Protection

An organization's attack surface is the collective term for all the internet-facing assets that could be vulnerable to unauthorized access or attacks. Keeping this surface as protected as possible should be the focus of all organizations. Intel 471's 'Attack Surface Protection' is the name for our suite of solutions, each geared for different users at different stages in their attack surface journey.

Understanding which solution is right for you

- ***Attack Surface Discovery (ASD)***

Attack Surface Discovery is designed for pentesters or those organizations who are just embarking on this journey. It allows you to take a snapshot of an organization's digital footprint at a single point in time. You can discover all of an organization's internet facing assets, whether hosted in-house, in the cloud, under the control of IT or not (shadow IT). Known as 'Asset Discovery', it's ideal for better understanding the attack surface, which is critical if you want to implement actions to reduce risk: you can't fix what you can't see.

- ***Attack Surface Management (ASM)***

Building on the functionality of our Discovery solution, Attack Surface Management takes it to the next level: ongoing monitoring and alerting. With new vulnerabilities and data sources emerging all the time, and the ever changing nature of your internet facing assets, a one time scan is not enough to stay on top of security gaps in your digital footprint. Attack Surface Management helps by regular, automated scanning of your attack surface to provide ongoing monitoring and immediate alerting to any changes or new vulnerabilities identified. Attack Surface Management is API enabled, ensuring that it can work in conjunction with other systems to expedite the communication and remediation of potential vulnerabilities and minimize the amount of time your attack surface is exposed.

- **Attack Surface Intelligence (ASI)**

Attack Surface Intelligence adds an entirely new dimension to our solution offering, whilst retaining all the functionality of the other packages. Attack Surface Intelligence allows organizations to extend their monitoring to the cyber underground, a remarkable benefit only available from a premier CTI provider, like Intel 471. We use our unparalleled cyber threat intel data as an early warning sign for our customers, identifying in real-time when relevant and critical threats appear in the cyber underground. No amount of Attack Surface Management can prevent all data leaks, so taking proactive measures to identify this new level of threat and using it to inform your vulnerability patching is essential.

sales@intel471.com

Attack Surface Discovery

- Understand and map an organization's attack surface at a single point in time
- Identify the known and highlight the unknown components of that attack surface
- Locate any potential vulnerabilities across the attack surface
- Ideal for pentesters and for organizations searching for a cost-effective, introductory solution

Attack Surface Management

- *All the functionality of Attack Surface Discovery, plus…*
- Track and map your attack surface and pick up on security gaps immediately by scheduling regular, automatic scans
- Configure automated alerts to stay continuously informed of relevant changes
- Compare scans using the comparison function to easily track differences over time, measure change, and report on KPIs
- API integration allows you to implement orchestration

Attack Surface Intelligence

- *All the functionality of Attack Surface Management, plus…*
- Extend attack surface monitoring into the cyber underground with Intel 471's unparalleled cyber threat intelligence
- Unique use of cyber underground intel as an early warning system for your organization
- Identify in real-time when relevant and critical information appears in the underground that could compromise your attack surface
- Use this intelligence to inform your vulnerability patching and overall security posture.
- Identify a new level of threat that could never be detected through Attack Surface Management alone

Turbo-charging traditional ASM

Intel 471 has attack surface solutions that will grow with your capabilities and appetite. Attack Surface Intelligence takes attack surface monitoring to a whole new level by offering visibility of threats that could never be detected through traditional ASM offerings. The blurring of an organization's digital 'perimeter' is inevitable, because of cloud computing, BYOD and remote working, and carries inherent risks. No attack surface is impregnable and organizations need to look beyond their walls to understand what threats exist. By combining traditional ASM with our cyber underground intelligence, we help organizations work proactively to mitigate potential threats in real-time. Providing attack surface solutions is a natural progression of our offering, as our reach into the underground is inimitable, we know what threat actors are saying, how they operate and what vulnerabilities they look to exploit. We use this unique knowledge to focus on and prioritize the most relevant and critical threats to your organization. Depending on where you are in your Attack Surface journey, we have a solution for you. We're offering you the opportunity to take control of your digital footprint and even go a step further in tackling cyber threats.

sales@intel471.com