



DIFFERENCE BETWEEN ATTACK SURFACE VS. ATTACK VECTOR





TABLE OF CONTENTS

<u>Introduction</u>	<u>3</u>
<u>What is an attack surface?</u>	<u>3</u>
<u>What is an attack vector?</u>	<u>3</u>
<u>What is attack surface exposure?</u>	<u>4</u>





People often get the terms **attack surface**, and attack vector confused. Though these terms are related, they hold a different meaning altogether.

What is an attack surface?

Attack surface is the sum of all the touchpoints on your network where an adversary can attempt to gain entry across your hardware, software, cloud, and network components. These components can include:

- Managed and unmanaged devices
- Cloud storage and apps
- IoT devices
- Wi-Fi access points and routers
- Servers
- VPN
- Firewalls
- SaaS solutions
- Third-party vendors, and more.

An organization's **attack surface** constantly expands and shape-shifts in both physical and digital dimensions, making it quite a task to manage it. However, organizations can **reduce the risk** to their attack surface with continuous mapping and real-time visibility.

What is an attack vector?

An **attack vector** is the actual method that a threat actor uses to breach or infiltrate your network.

Attack vectors may target weaknesses in your security and overall infrastructure, or they may even target the people in your organization.

Some of the most used attack vectors are:

- Man-in-the-middle
- Compromised credentials


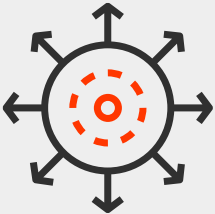


- Weak and stolen credentials
- Malicious insider
- Missing or poor encryption
- **Misconfiguration**
- **Ransomware**
- **Phishing**
- **Spear-phishing**
- Zero-day vulnerability
- Physical theft
- Misused trust relationships

What is Attack Surface Exposure?

Through continuous monitoring, Resolution Intelligence Cloud's Attack Surface Exposure (ASE) feature lets you find — and act fast to fix — hidden risks across your digital exposure on domains, certificates, **open ports**, vulnerabilities, misconfigurations, and more. ASE can also help start-ups, mid-markets, and enterprises demystify security beyond the perimeter with enterprise-grade, outside-in security delivered via Netenrich's Resolution Intelligence platform.

I Why ASE from Netenrich

	<p>Plug-and-play onboarding</p> <p>ASE requires minimal effort to onboard. You can quickly and easily ingest any data you need from any source and begin monitoring — and managing — your attack surface to get ahead of hackers and other threats.</p>
	<p>Zero downtime</p> <p>ASE continuously and non-intrusively scans your attack surface to discover your publicly exposed digital footprints — something point-in-time exercises like pen tests and red teaming can't do. It also escalates anything that needs your immediate attention.</p>



Proprietary **threat** intelligence

We built our global threat intelligence service from the ground up to work natively with our security solutions, including ASE and Intelligent SOC (ISOC). Leverage our intelligence to prioritize risks and keep ahead of threat actors in your industry and geography.



Collaborative **risk** mitigation

Fix risks right now by contacting our bench of cybersecurity experts via chat, e-mail, and phone. Put effective security controls in place and scale your security operations with our ISOC solution at a fraction of the cost to run your own.

In Netenrich

Attack Surface Exposure (ASE) offers continuous **attack surface** monitoring to detect bad actors and vulnerabilities in an organization's digital or physical surfaces. ASE maps incidents and attacks to the following categories and can generate numerous records per day, per customer on any of these.

Threats

A cyber threat is any malicious activity that aims to compromise the security and integrity of computer systems, networks, or data. Threats can take various forms, such as hacking, malware, phishing, ransomware, and denial-of-service (DoS) attacks, and have severe consequences, ranging from financial losses and reputational damage to the theft of sensitive information and the disruption of critical infrastructures.

Bad actors could launch, for example, a DoS attack to cripple a power grid or transportation system simply by cutting a fiber-optic cable or they could exploit vulnerabilities in a Domain Name System (DNS) to intercept communications or redirect users to fraudulent websites.

Brand Exposures

Bad actors can damage an organization's reputation by posting malicious content on fake websites and social media platforms or selling counterfeit products on



digital marketplaces and application stores. But how do they get started? They've got plenty of choices, including:

- **Email breaches.** Email inboxes are a treasure trove for cybercriminals; and unauthorized access to sensitive information stored in emails has the potential to wreak havoc, not only potentially compromising privacy but also exposing individuals and enterprises to identity theft, phishing scams, and other malicious activities.
- **Cloud storage.** An attacker can easily gain access to public-cloud storage and cause irreparable damage or steal valuable data if the storage company has not prioritized security and, for example, lacks proper data **governance** or robust credentials.
- **Typo-squatted domains.** Typo squatted domains, also known as URL hijacking, are deceptive websites created with slight misspellings of popular domain names to trick unsuspecting users into clicking on them. Hackers often use them for phishing attacks and malware distribution.
- **Code repositories.** Since code repositories are accessible to multiple users, they present an easy route for threat actors to gain unauthorized access to intellectual property. For example, if developers inadvertently upload proprietary or sensitive code, it can be exposed to the public domain, which can then potentially cause copyright infringement or competitive advantage issues.
- **Expired or soon-to-expire domains.** When a domain expires, it becomes available for anyone to register, including cybercriminals. Attackers can take advantage of an expiring domain to gain access to confidential data or use it for malicious purposes. For example, they can create fake websites that mimic legitimate ones to trick unsuspecting users into sharing personal information or downloading malware. That's why it's crucial for domain owners to renew their domains on time or take necessary precautions to prevent their expired domains from falling into the wrong hands.
- **Subdomain takeovers.** Attackers look to take control of inactive or misconfigured website subdomains, which they can use to steal sensitive data, launch phishing attacks, or redirect users to malicious websites.

Misconfigurations

Misconfiguring servers, laptops, and desktop ports open the door for attackers to gain access and steal data. For example, if an attacker discovers that a directory listing is not disabled on a server, he can simply list directories to find and



execute any file. Other areas where bad actors can look for misconfigurations include:

- **Web applications.** When it comes to web apps, default settings may seem convenient. However, it's important to understand why you should avoid using them — not least of which is the fact that attackers can easily exploit them. By customizing settings instead, you can help ensure that your web app operates in the most effective and secure manner possible.
- **Service identification.** Most security scanners include a robust service identification engine that's capable of detecting more than 90 different application protocols. However, with less robust engines, threats can easily creep in.
- **Service authentication.** Authentication technology controls access by checking whether a user's credentials match those in a database of authorized users or in a data authentication server. Hackers can easily exploit poor credentials, such as easily guessed passwords.
- **Expired or soon-to-expire certificates.** Websites work intermittently with the use of SSL certificates installed on a network. Expiring or expired certificates can prevent services hosted on a website from functioning correctly, which can then affect running secure transactions.
- **Self-signed certificates.** Users issues these public key certificates on their own behalf as opposed to having a certificate authority (CA) issue them. Unfortunately, attackers can use self-signed certificates to gain access control over a network.

Vulnerabilities

A vulnerability is a weakness or flaw in a system, network, or software that a threat actor can exploit to gain unauthorized access, steal sensitive information, or disrupt normal operations. Vulnerabilities can exist in various forms, including:

- **Vulnerable services.** Services with weak credentials and open ports on servers.
- **Vulnerable content management systems.** While content management systems play a crucial role in simplifying website creation and maintenance, they can also expose sensitive data and open the door for malicious attacks if they have outdated software and plugins, weak passwords, and improper access controls.