



# THE ULTIMATE GUIDE TO ATTACK SURFACE

---





# TABLE OF CONTENTS

---

<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">What is attack surface?</a>	<a href="#">3</a>
<a href="#">What to protect in your attack surface?</a>	<a href="#">4</a>
<a href="#">How to map your attack surface?</a>	<a href="#">5</a>
<a href="#">Steps to map your attack surface:</a>	<a href="#">5</a>
<a href="#">How can real-time visibility protect your attack surface?</a>	<a href="#">7</a>
<a href="#">What is Attack Surface Exposure?</a>	<a href="#">8</a>
<a href="#">Getting started with Attack Surface Exposure</a>	<a href="#">9</a>





The attack surface is the sum of all internet-facing digital assets, hardware, software, and applications that can be exploited to carry out cyber-attacks.

In September 2017, the world saw one of the worst data breaches in history. Equifax Inc. — one of the three, largest consumer credit reporting agencies in the world — announced a data breach that compromised the personal information of 147 million people.

The information included first and last names, social security numbers, birthdates, addresses, and in some instances, driver's license and credit card numbers. Dealing with this incident cost Equifax a staggering \$1.4 billion+ in legal fees.

The incident came in as one of the most critical reminders of a simple fact when it comes to modern cybersecurity: a slight lapse in monitoring of your attack surface could cause immense damage to your organization.

## What is attack surface?

Your attack surface is the sum of all internet-facing digital assets, hardware, software, and applications that can be exploited to carry out cyber-attacks. Potential, security-risk loopholes exist across cloud, network, and on-premises. The smaller your attack surface, the stronger your security. Your attack surface can include:

- **Known assets:** websites, servers, firewalls, endpoints, storage, and apps (cloud and on-premises).
- **Unknown assets:** abandoned and orphaned sites, domains, servers, and IT infrastructure.
- **Internet of Things (IoT) devices:** point-of-sale devices, physical security equipment (locks, cameras, alarms, and more),
- **Brandjacked assets:** typo-squatted domains, lookalike domains, and apps.
- **Vendors and services:** verified and unauthenticated access to assets gained by third-party and fourth-party services.
- **Dark-web artifacts:** assets, email database, and data records exposed in the hidden corners of dark web.

Because of the ongoing shift towards digital transformation, the size of the attack surface has grown immensely. So much so that the IT teams struggle to map the exact size of the attack surface and keep themselves secure.

Gartner had estimated that by 2020, 30% of data breaches would result from shadow IT assets or vulnerabilities related to undocumented attack surfaces.



These numbers will only increase with the adoption of digital transformation. As such, the need for efficient attack surface management is higher than ever before. A robust attack surface management solution can provide extensive attack surface analysis to help manage risk.

**Jon Oltsik**, the ESG senior principal analyst and fellow, puts it best:

"You can't manage what you can't measure. By discovering and monitoring these assets, security professionals can then find the 'path of least resistance' those hackers may use as a doorway to penetrate corporate networks and commence a cyber-attack. Armed with this intelligence, security teams can close the gaps, fine-tune security controls, and develop countermeasures."

## What to protect in your attack surface?

Malicious actors continually hunt for ways to break into your organization. It is essential to know everything that can add to your attack surface. Find all the ways that your infrastructure is exposed and vulnerable to attack, and then prioritize activities that help make that attack surface smaller. Key categories of digital assets that need protection include:

- Websites (domains and sub-domains), services, and APIs
- Email addresses found in breached databases
- Open or misconfigured ports, email servers, databases
- Expiring or abandoned certificates
- Vulnerability exposures
- Public-cloud storage and code repositories, such as GitHub, BitBucket, and GitLab
- Abandoned servers, sites, domains, pages
- Asset access to third-party and fourth-party vendors

This seems obvious, right? However, a report shared by *Security Magazine* shows that even the most prominent companies do not know what they are dealing with:



- 68% of organizations surveyed experienced an attack that originated from an unmanaged or poorly managed company asset.
- A whopping 98% of organizations said that testing is a top 10 security issue, while only 43% admitted to regular pen-testing.
- 50% of organizations do not include software-as-a-service (SaaS) applications and public-cloud workloads in their attack surface.

## How to map our attack surface?

Comprehensive attack surface evaluation and analysis can help you create your parameters and limit the opportunities available to cybercriminals.

Here is how to map your attack surface once you have planned and scoped out your organizational perimeter.

## Steps to map your attack surface:

### Step #1: Perform application discovery

The first step is application discovery to understand what critical web apps you own and where they are exposed. This can be difficult due to the significant amount of shadow IT in large organizations. So, instead of bombarding your team with false positives, it is a far more reasonable approach to focus on assessing the risk level of business-critical web apps first.

### Step #2: Check code usage

Some code languages are more exposed than others, and as new versions are released, this will organically fix the issues. Using insecure and old code to develop your website will lead to a host of easily exploitable vulnerabilities for hackers to take advantage of.

### Step #3: Identify page distribution

The more pages your website has, the more risks there are. As such, you must find all pages and uncover vulnerabilities at all levels. You can also restrict access to specific actions or pages using user levels set up by the administrator. This is critical in keeping the bad guys out.



## Step #4: Input Vectors

Having too many input fields in your web applications exposes you to the risk of an XSS attack. Find the number of input vectors in your attack surface and assess their criticality and risk.

## Step #5: Active Contents

As soon as an application runs scripts, the attack surface may increase depending on how the scripts have been implemented. If a website has been developed using several active content technologies, it could uncontrollably expand the attack surface. Some of the examples of active contents are website polling forms, opt-ins, animated GIFs, maps, JavaScript applications, streaming videos, audio applications, embedded objects, features that rely on browser plug-ins, and more.

## Step #6: Cookie Usage

Cookies are necessary for real-time application security, which they achieve by monitoring session activity and keeping malicious actors away from unauthorized zones.

Now that you have gone through all these steps, you will need to correlate the results in a way that best suits your risk posture. Some of the factors to keep in mind are:

- **Criticality:** Check if the asset in question is business-critical and could harm your organization and revenues if attacked. Defining these weak points will help you understand the business-criticality level of the application.
- **Update Frequency:** Not all applications are updated regularly and remain static with little intervention. Some need dynamic maintenance, making them more vulnerable with time. Finding the update frequency of applications will help to more accurately determine the risk.

When you consider all these factors, you will get a proper blueprint of your attack surface, helping you gauge your overall weaknesses and risk score. You'll be able to decide to shut down an app if it is no longer being used and focus your vulnerability assessment and remediation efforts on the areas that pose the highest risk for your organization.

Once you have mapped your attack surface and found the high-risk areas, you must focus on entry points, such as interfaces in your system that allow anonymous and public access. You could be exposed to the following:



- Network-facing code
- Web forms
- Files from outside your network
- Interfaces that are backward-compatible with other systems
- Custom APIs
- Security code dealing with cryptography, authentication, authorization

Operational controls like network firewalls, application firewalls, and intrusion detection systems can help you immensely. Maintaining multiple versions of an application and leaving features redundant or leaving old, backup copies and unused code increase your attack surface significantly.

Keep your actual attack surface close to your theoretical version by controlling your source code and exercising robust change management.

## How can real-time visibility protect your attack surface?

If you cannot see chinks in your armor, you will not be able to manage it. Legacy strategies like audits and pen tests tend to miss the vulnerabilities that crawl up across your dynamic threat landscape. This is where real-time visibility comes in — to give you around-the-clock monitoring, completely hands-off. Real-time visibility into your attack surface helps you in the following ways:

- **It eliminates the need for new scans**

A lot can change within a matter of few hours in your threat landscape. Having a static risk assessment program could make you miss serious vulnerabilities that might crop up any time in your attack surface. Getting prompt and updated intel without requiring any news scans could save you the crucial time to find your adversaries.

- **It improves time to respond and remediate**

Real-time visibility into your attack surface means you plug the holes before a risk is exploited and leads to major losses. Mitigating risk in advance ensures you have enhanced productivity, reliable security operations, and a higher ROI (return on investments) eventually. Advanced attack surface management offered by Netenrich brings in threat correlation capabilities for proactive risk management.



By drawing on the latest threat intelligence, it helps you predict attacks before they occur. Such intelligence allows you to focus more on corrective measures instead of research.

- **It ensures consistent, complete, and updated security**


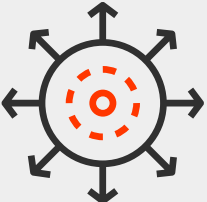
To have a consistently robust security posture, you need to manage and resolve threats at the speed they arise. Real-time visibility ensures you take prompt action when something needs your attention, such as changes to critical assets, expiring or expired certificates, brand impersonation incidents, third-party risk, and more. A real-time attack surface view is an excellent tool for easy and always-on monitoring.

Companies these days are spending millions of dollars across a wide range of solutions but struggle to gain even limited visibility into their entire attack surface. Turns out, these organizations too often focus only on assets they already know exist. As such, most don't have a good idea what their attack surface really looks like.

## 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><b>Plug-and-play onboarding</b></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><b>Zero downtime</b></p> <p>ASE continuously and non-intrusively scans your attack surface to discover your publicly exposed digital footprints — something</p>





point-in-time exercises like pen tests and red teaming can't do. It also escalates anything that needs your immediate attention.



### 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.

## Getting started with Attack Surface Exposure

Learn more about how **Resolution Intelligence Cloud™** offers:

- Attack surface scans
- Access to the ASE intelligence portal and dashboards
- Expert analyst insights to address your most critical risks first

Discover the full power of Netenrich's Threat + Attack Surface Exposure.

## 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.