NETENRICH

SEVEN TIMES TO ATTACK YOUR ATTACK SURFACE

TABLE OF CONTENTS

This guide explains seven times to attack your attack surface, what you should investigate and, shore up your attack surface.

Your attack surface is “the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from,” according to the National Institute of Standards and Technology (NIST).

Think of your attack surface as a fast-moving, ever-changing target. With more publicly accessible infrastructure, externally-facing digital assets, access points to those digital assets, and myriad people who have access, the more attractive — and vulnerable — that target can be.

This guide explains seven times you should investigate and, if necessary, shore up your attack surface, specifically when you:

1. Launch or promote cloud- or SaaS-based services
2. Acquire another company
3. Find or suspect shadow IT
4. Assess third-party risk
5. Prepare for a cyber audit
6. Justify your security spend
7. Incur serious breaches

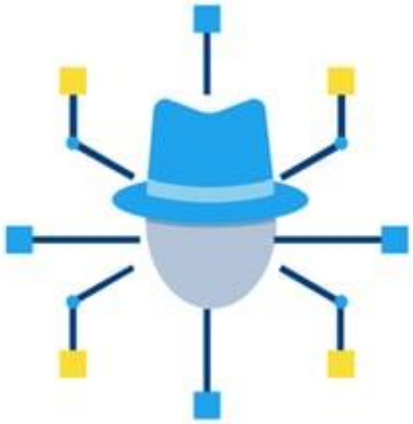
We cover each of these in more detail below. First, let’s cover the basics

What is Attack Surface Management?

Attack Surface Management (ASM) is the continuous discovery, assessment, and mitigation of cyber risk across your attack surface. Keeping your digital attack surface in good shape takes constant vigilance to find and fix vulnerabilities *before you’re attacked.*

ASM is similar to IT asset discovery and asset management, but *ASM views your attack surface from an attacker’s point of view.* Its goal is to identify potentially vulnerable assets and end points that you don’t necessarily know about, that aren’t being monitored on a regular basis, and/or that fall outside of your regular security processes and procedures.

Think like a hacker – continuously



Because your attack surface is dynamic – and so are hackers – your attack surface management solution must be dynamic, agile, and continuous. ASM makes it easy to visualize external risk exposure and severity in one place. It enables security teams to act quickly to address the most critical exposures *before* damage occurs. Thus, attack surface management should be automated, always-on, and near real time.

You likely already have security procedures in place for key assets, such as your company's website. But other elements of your digital attack surface may be hiding

in plain sight, such as old domains, publicly exposed code repositories, and other by-products of digital transformation that make you vulnerable to cyberattacks.

Advanced ASM solutions like Attack Surface Exposure (ASE), part of Resolution Intelligence Cloud® from Netenrich, make discovered vulnerabilities actionable with threat correlation, context, and prioritization to accelerate remediation.

Now that you're thinking like a hacker, let's examine those seven times you should investigate and, if needed, shore up your attack surface.

1. You launch or promote cloud–and SaaS–based

Migrating apps and services from physical systems to the cloud introduces new risk. Security teams face two major challenges:

- lack of visibility
- the dynamic nature of cloud computing.

For example, engineering or DevOps teams may spin up machines in the cloud without thinking through the potential security implications or making IT aware of new cloud instances.

Continuous attack surface monitoring helps you stay on top of exposed or unauthenticated services and publicly exposed storage, even if one or more of your cloud providers has gaps. ASM helps steadily improve best practices, and lets you see what matters as soon as it changes.

> Cyber events like annual sales require servers to scale up fast to dramatically increase capacity. In the absence of impeccable digital hygiene among both clients and providers, these dramatic fluctuations can add substantial risk.

ASM targets the major hazards of cloud migration such as services becoming exposed as hosted cloud infrastructures spin up virtual machines (VMs) and leave them running when they're no longer needed. Multi-cloud environments add to the chaos as a large SaaS provider might operate 90 machines in Google Cloud one day, see that spike to 110 the next day, and drop back down to 80 the day after that.

ASM finds critical risks that may arise from services that are left unauthenticated, often due to simple misconfigurations. In one real-world situation, Netenrich's Resolution Intelligence Cloud discovered a company's open-source automation server had become exposed leaving the engineering team's continuous integration and deployment pipeline at risk outside the organization.

Employees working remotely may move data to the cloud to collaborate or share information with colleagues. They can inadvertently expose public cloud infrastructure without implementing the proper controls, and without anyone knowing about it. An attacker targeting your company could come across these oversights and start working backwards to map your infrastructure to see what's unauthenticated, and what they can reach.

Finding these misconfigurations as they occur is daunting and time-consuming, if not impossible, without an ASM solution like Resolution Intelligence Cloud.

> Cyber events like annual sales require servers to scale up fast to dramatically increase capacity. In the absence of impeccable digital hygiene among both clients and providers, these dramatic fluctuations can add substantial risk.

2. Your company acquires another company

In most acquisitions, a bigger company acquires a smaller one with less matureyour-company-acquires-another-company cybersecurity defenses and processes. Ideally, during the due diligence period, the security team can assess potential risks of integrating systems and gauge the time and effort needed to do it safely.

While the security team's findings probably won't affect the decision to move forward with the acquisition, they can help inform negotiations around upfront costs and alert CIOs and CTOs to undiscovered or undisclosed breaches that represent brand risk.

ASM helps assess the target company's overall security posture and find major gaps in defenses quickly. ASM can rank critical exposures to focus and fast-track initial clean-up campaigns. Analysts get a running start by simply plugging in and validating the security posture of the new entity and rooting out the nasty surprises, including:

- Issues that have persisted well beyond the normal time to remediate, potentially indicating they may have already suffered a breach without having realized it
- Typo-squatted domains
- Content management system misconfigurations

3. You find or suspect shadow IT

When business users adopt non-IT-approved technology that falls outside of your security protocols, that "shadow IT" can put security at equal to or greater risk than phishing attacks.

For example, your Marketing team or one of its agencies may host web-based events or content, then fail to renew a domain name only to have an adversary hijack the URL and use it in a phishing campaign.

Attack Surface Exposure (ASE) can uncover external digital risk from shadow IT as it appears. The most likely vectors include IP addresses you didn't know were associated with your brand, are part of a block you don't know about, or are hosted by providers not sanctioned by your IT department. For example, your marketing team or one of its agencies hosts web-based content and fails to review a domain name. An adversary hijacks the URL and uses it in a phishing campaign.

> Securing the servers is Amazon's responsibility. Configuring and safeguarding the S3 buckets is the responsibility of the bucket owner. And that seems to be where things go wrong. The S3 buckets come with strong security out of the box. But the owners end up misconfiguring the buckets, leaving their IP addresses wide open on the web for anyone to sniff out, using tools readily available on code repository sites.
>
> - FairInstitute.org

4. You're assessing third-party risk

What you don't know can hurt you. The challenge of third-party risk may be the classic use case for ASM: While you cannot control everything that happens on the internet, you should continually seek it out, monitor it, and address your risk in relation to it.

There may be no direct liability for glitches in another company's defenses, but identifying and addressing third-party risk including your vendors, partners, and other affiliates is a best practice that strengthens your cyber risk posture.

If you suspect you're going to be the focus of a third-party risk assessment, ASM helps you manage exposures that can be used and held against you. Adding ASM and security ratings to regular certifications, pen testing, and SOC2 reports shows stakeholders you're taking a comprehensive and innovative approach to visualizing and shrinking potential exposure. Cybersecurity ratings reflect an organization's overall reputation as a safe company to do business with and rank its performance versus competitors or companies in the same industry. Insight into peer ratings provides value in baselining third-party risk from IP addresses and vulnerabilities, but it does not offer deep technical insight into other aspects of digital risk, such as those associated with cloud and web application exposures described above. Nor can ratings services trace specific IPs of interest to a particular provider without building technical integrations to the other party's systems.

ASM lets you see the source of risk from a particular service and quickly drill down to see what's at risk and how to fix it. Having done the hard work of integrating to Google Cloud Platform (GCP), Azure, AWS, and other leading public infrastructures, Resolution Intelligence offers quick context that speeds resolution. ASM complements ratings with actionability as you delve into phishing, typo squatting, and unauthenticated services, some of which are not reflected in risk ratings.

5. You're preparing for a cyber audit

ASM streamlines and fast-tracks the cyber audit process by arming you with proof ofyou-are-preparing-for-a-cyber-audit coverage. Mapping items covered by ASM discovery to specific controls listed in popular cybersecurity frameworks such as NIST 800 or CSF, COBIT (Control Objectives for Information and Related Technologies), and other industry-specific models makes it easier to check the box and go on to the next thing without having to spend more time tracking down evidence.

ASM products like Resolution Intelligence offer precise evidence to satisfy auditors that you're monitoring specific elements of individual frameworks and mounting an aggressive defense overall. Once again, a lot more goes into preparing for an audit, but anything that can help check boxes in multiple areas — and equip you to focus other efforts like vulnerability management — is a definite plus.

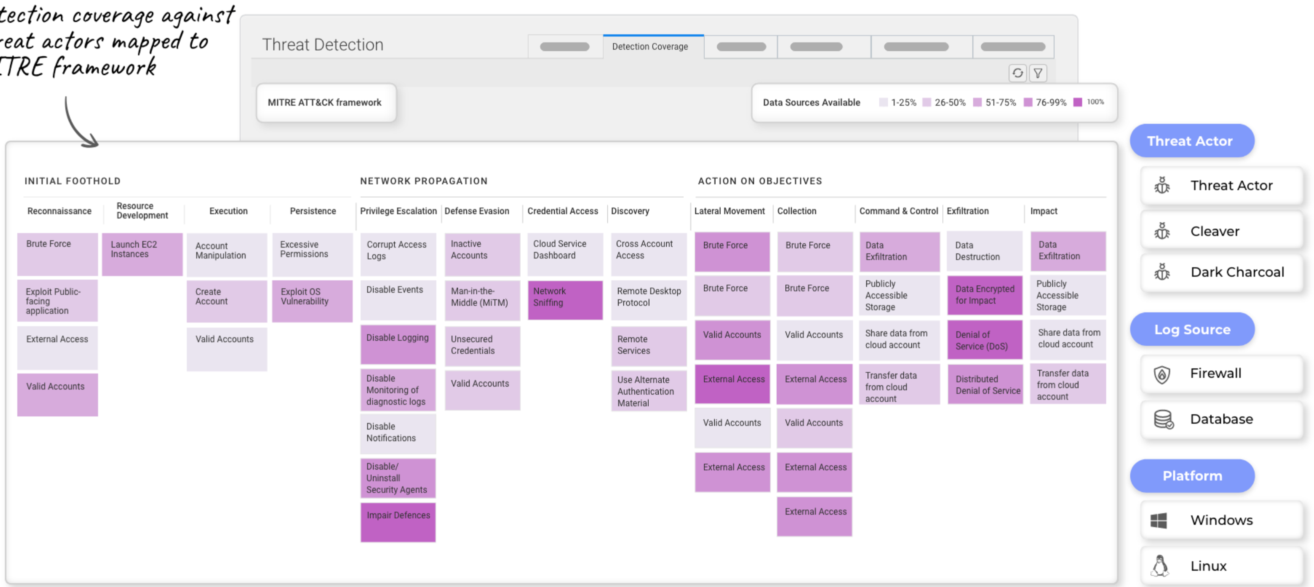
6. You need to justify your security spend

It's harder to justify spending on prevention than action. If nothing happens for a period of time, is that because you were prepared or because hackers were taking it easy? ASM plays a vital role in preventing incidents from happening and delivering ongoing coverage — and it can provide its own cost justification in several ways.

ASM dashboards should demonstrate a steadily shrinking attack surface. They can show that you've got things covered during predictable spikes (such as during holiday shopping seasons), market fluctuations, and event registration. That means fewer opportunities for breaches to happen and greater ability to detect and respond faster if they do. Over time, you can demonstrate that you're reducing exposure — and work. You can compare results to industry standards for companies like yours and seek out cost metrics for specific, known intrusions.

Resolution Intelligence Cloud maps your security posture to the MITRE ATT&CK® framework so you can identify and remedy detection gaps, in general and in relation to specific, known threat actors, saving you time and preventing threat exposure.

Detection coverage against threat actors mapped to MITRE framework



Threat Detection

Detection Coverage

MITRE ATT&CK framework

Data Sources Available ▢ 1-25% ▢ 26-50% ▢ 51-75% ▢ 76-99% ■ 100%

INITIAL FOOTHOLD				NETWORK PROPAGATION				ACTION ON OBJECTIVES				
Reconnaissance	Resource Development	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Brute Force	Launch EC2 Instances	Account Manipulation	Excessive Permissions	Corrupt Access Logs	Inactive Accounts	Cloud Service Dashboard	Cross Account Access	Brute Force	Brute Force	Data Exfiltration	Data Destruction	Data Exfiltration
Exploit Public-facing application		Create Account	Exploit OS Vulnerability	Disable Events	Man-in-the-Middle (MiTM)	Network Sniffing	Remote Desktop Protocol	Brute Force	Brute Force	Publicly Accessible Storage	Data Encrypted for Impact	Publicly Accessible Storage
External Access		Valid Accounts		Disable Logging	Unsecured Credentials		Remote Services	Valid Accounts	Valid Accounts	Share data from cloud account	Denial of Service (DoS)	Share data from cloud account
Valid Accounts				Disable Monitoring of diagnostic logs	Valid Accounts		Use Alternate Authentication Material	External Access	External Access	Transfer data from cloud account	Distributed Denial of Service	Transfer data from cloud account
				Disable Notifications				Valid Accounts	Valid Accounts			
				Disable/ Uninstall Security Agents				External Access	External Access			
				Impair Defences					External Access			

Threat Actor

Threat Actor

Cleaver

Dark Charcoal

Log Source

Firewall

Database

Platform

Windows

Linux

7. You've had a serious breach

We saved the worst for last. When you've had a serious breach, you're under the microscope. As incident response (IR) winds down and things inch back to normal, it's worth the effort to dissect the initial infection or attack vector, and understand why it occurred and how long it existed. Once you understand what happened, you can take steps to prevent the a similar breach by limiting your attack surface exposure.

For example, Resolution Intelligence not only finds vulnerabilities in your attack surface exposure, it also identifies risky behaviors that can indicate attacks and prioritizes them based on criticality, but ranks it in terms of criticality based on the likelihood of it being used against you. In one real-world scenario, Resolution Intelligence discovered code that had been left exposed in a Github repository for nearly two years, with API keys embedded.

The aftermath of a breach is an obvious time to re-assess how to avoid future breaches. If you don't have continuous external risk assessment in place, this is the perfect time to make the case for adding ASM to your security best practices.

The continuous nature of ASM represents a major step in becoming more predictive and proactive, ultimately saving time and money – and reducing the impact of future breaches.

8. Bonus!

When should you attack your attack surface? Now.

Hackers need only to find one attack vector one time to take you down. ASM should happen continuously because your attack surface changes on a continuous basis, often without you realizing it.

Any business event that involves monitoring for continuity should include a comprehensive cybersecurity assessment featuring attack surface management. Done right, ASM gets smarter over time. Moreover, it eliminates manual processes that can prevent essential investigations from taking place, and it avoids wasted or duplicated efforts.

Schedule a secure operations assessment with a **Netenrich security expert** to learn how Resolution Intelligence Cloud helps you manage your attack surface and minimize your cybersecurity risk exposure.

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.

Why ASE from Netenrich

Plug-and-play onboarding

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.

Zero downtime

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.

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.