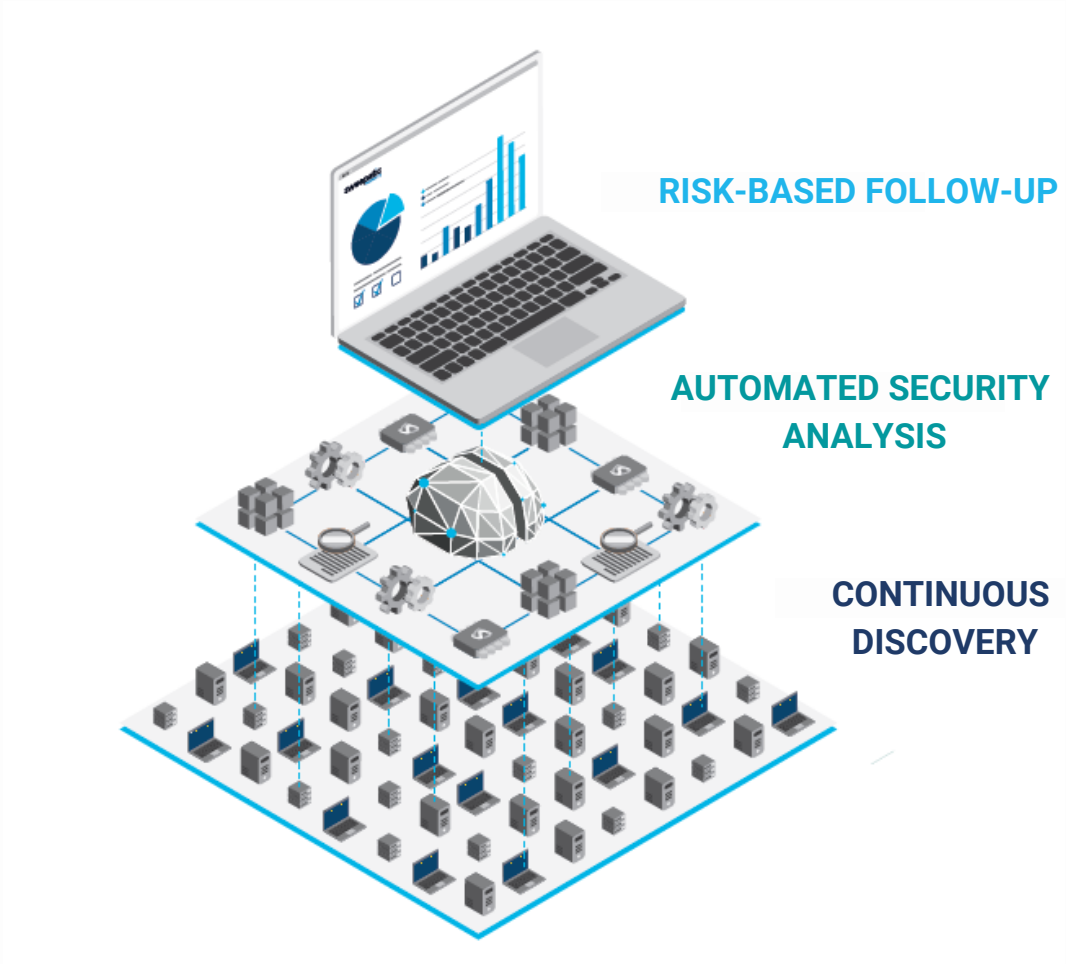
sweepatic SECURITY

Attack Surface Management: Key Features

WHITE PAPER

APRIL 2021



What is Attack Surface Management?

A relatively new cyber security problem space with its own definition has been coined since a few years now: Attack Surface Management or ASM. The term can be confusing or vague without spending some time on a clear definition. In cybersecurity there are many 'surfaces' that can be attacked. So what surface are we talking about?

> *In cybersecurity, the word 'attack surface' is interpreted as the publicly exposed or internet exposed or external exposed IT assets.*

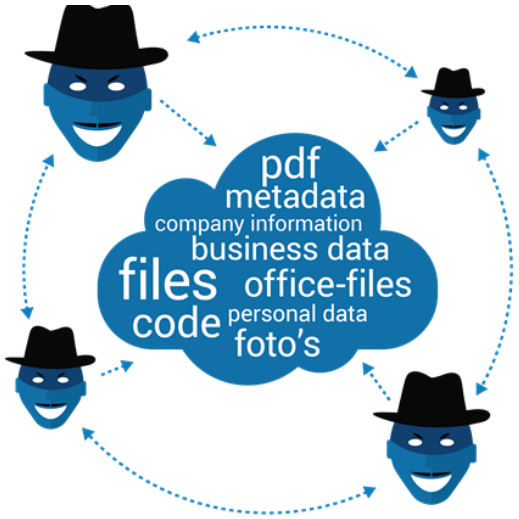
So it can also be translated to 'Internet exposed IT asset security management', but that is too long to be handy, so we shortened it to ASM.

An IT asset can be anything that can help an attacker gain relevant information, usually in order to stage an attack. Assets can be: IP addresses, DNS records, application endpoints, websites, APIs, remote (administrative) access points, databases, encryption details, file sharing services, stolen credentials that are sold on the dark web, etc. The end goal is usually to find vulnerabilities, insecure configurations, data or other issues that can be abused.

Why is a clean attack surface important?

That is simple. The first stage of any attack is the reconnaissance phase.

An attacker will find as much information and weak spots as he can, in order to devise the best attack strategy. He will simulate normal traffic and search queries to gather as much data as possible. The cleaner your attack surface, the more effort he needs to put in. This can result in the attacker moving on to an easier target.



> *Attack surface management is the art of becoming as unattractive as possible for bad actors.*

Why are attack surface management tools valuable?

The attack surface of organizations is becoming ever more complex because of a few key trends:

- The continuous focus on the **digitization** of organizations in order to remain competitive.
- The adoption to the **cloud** and the speed of deployment the cloud brings.
- The **multi-cloud approaches** that many companies follow to optimize.
- The empowerment of non-IT staff to deploy applications online via **SaaS** offerings.
- A workforce that is ever more **mobile** via connect anywhere and use any device tools.
- Cyber security **experts** are limited in time, are expensive and hard to find.
- The **constant evolution of online assets** making bi-yearly vulnerability scanning or other technical cybersecurity assessments way to slow from a risk perspective.

That is why organizations are finding it increasingly difficult to keep track of which IT assets are exposed online and to follow up on the continuous stream of newly deployed assets, both on-premise and across clouds. The biggest challenges are often in mid- to big-size organizations that manage a mix of old and new IT infrastructure which is continuously adapted and upgraded. Big organizations often have different sub-brands with their own IT teams and mandates.

Organization clusters, brands or departments prefer to collaborate on security instead of investing in people and tools in their own silos. In many cases a CISO or a security team comes in with the task to improve security across the holding or organizations. One of the big challenges is to know all the internet exposed IT assets. Talking with the different teams is often too slow and complex and leads to incomplete results that are hard to follow up on. In those cases, an automated and continuous discovery solution would be very valuable.

What are the common use cases for the adoption of an Attack Surface Management solution?

Organizations consider an ASM solution for various reasons. Attack surface reduction is a key cybersecurity tactic. Other common reasons are:

- Detecting **unknown assets**, Shadow IT and Shadow projects in on-premise infra and across clouds.
- Finding **weak spots and risks** that are not discovered by traditional vulnerability scanners.
- **Reducing the internet exposed attack surface**: what is not online, cannot be hacked. It is that simple.
- Assessing risks from **suppliers and IT vendors**.
- Assessing M&A targets and **subsidiary risks**.

- Detecting **external risk** from data hosted outside of the organizations' infrastructure. Like the stolen credentials on the dark web and from cybersquatting activities that abuse their brand.
- **Saving time and expensive cybersecurity resources** by automating the manual work that needs to be done when patching together insights obtained from freely available Open Sourcing scanning tools (OSINT).
- **Collaborating on security**: An attack surface management (ASM) solution gives a security overview across departments and brands. Different profiles can access the platform to get the info they need and follow up on risks in their domain. Everyone sees the results, both the actions taken by themselves and others, which can motivate everyone for the common goal. The management can easily follow up on key metrics.

What is the difference between an attack surface scanner and a vulnerability scanner?

Many people wonder how an ASM scanner is different from a traditional vulnerability scanner. Some examples are listed below.

1. **Internet facing only**: an ASM solution is specialized in discovering the internet facing risk exposure.

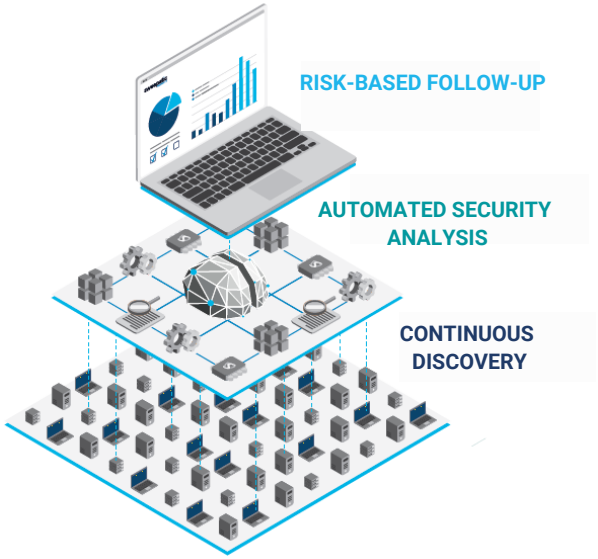
2. **Discovers unknowns**: a vulnerability scanner focuses on known assets by starting from a list of known IP addresses or known cloud providers. ASM scanners specialize in the discovery of both known and unknown assets based on DNS information and not IP addresses. They don't need a lot of input to get started.

3. **Assesses more than only software vulnerabilities**: a vulnerability scanner only looks for software vulnerabilities and is an expert in finding them all. The scans can even go into a real attack mode depending on how aggressive the scan is executed. As such, it automates part of the manual work of a penetration tester. Care must be taken when using aggressive scans as they can damage systems or even bring them down.

   An attack surface solution **simulates normal internet traffic** and is by default safe to use. It finds more than only software vulnerabilities. It can discover IP addresses that were unknown, so they can be added to the vulnerability scanners' list.

What are the key features of an Attack Surface Management platform?

ASM empowers cybersecurity professionals by reducing much of the heavy manual labor so they can focus on actually solving the issues instead of finding them.



Technically skilled professionals know how to use the broad set of available open source scanning tools and security testing scripts, but correlating and storing all the returned data and conclusions is not an easy thing to do. An ASM platform is heavily automated and should be easy to set up and get started.

An ASM solution typically has three key features:

- Continuous discovery
- Automated security analysis
- Risk-based follow-up

1

Continuous discovery

The purpose of the ASM solution is to automate the discovery of your assets. It should be able to start based on your primary domain (ex. mycompany.com), or a list of primary domains for bigger organizations. There should be no need to provide IP addresses to get started.
Adding additional IP ranges should however be supported for special use cases where the discovery techniques cannot help out. An ASM solution will use an intelligent search algorithm to build a map of your assets with minimal input and limited false positives.
The discovery process is continuous and each scan will find assets that will trigger new scans. Because it is continuous, newly deployed or removed assets will be detected and reported on a weekly basis.

Typical asset elements that will be discovered:

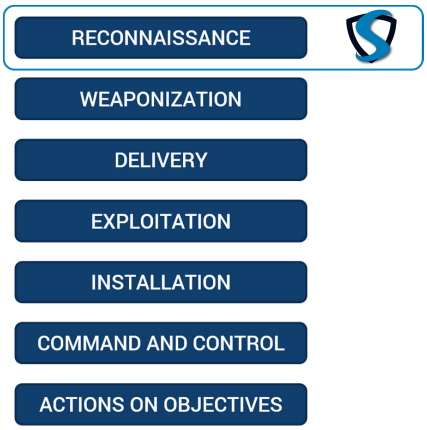
- All DNS records
- All related IP addresses
- WHOIS or DNS registration info
- Geo locations of the asset
- Hosting providers in charge of the asset
- All open ports
- All used SSL/TLS certificates and their details
- Email systems
- DNS systems
- Applications like: websites, emails, DB's, remote access, fileshares, etc.
- Software versions used across discovered assets and applications
- Login pages

2

Automated security analysis

Based on what was discovered, additional verifications are done to determine where security issues can be found.

As explained by SANS Security Awareness, the Cyber Kill Chain model involves 7 steps an attack follows. Every attack starts with a reconnaissance phase. Hackers today run well-organized criminal enterprises that heavily automate and have the best tools available to them. If you are not automating yourself, you are fighting an uneven battle.



Source: SANS, Cyber Kill Chain

Typical security issues that can be found:

- Software vulnerabilities based on discovered software version information.
- Insecure email configuration settings, like missing or wrong SPF, DMARC, DKIM settings.
- Weak encryption, like the usage of very old and insecure SSL/TLS encryption protocols.
- Unsecured DNS setups that don't support DNS SEC.
- Default installs, like a web server that shows a default page after initial install.
- Error codes, like HTTP response errors, an indication of a misconfigured or obsolete website.
- IP blacklisting & reputation issues.
- Unencrypted login pages, leading to password theft.
- Unnecessary exposed services, like databases and dangerous remote admin protocols (e.g. Telnet, RDP & VNC).
- Stolen credentials: alerts based on recently disclosed stolen credentials for your organization.
- Phishing & cybersquatting websites, like look-a-like websites that abuse your brand.

3

Risk-based follow-up

An ASM solution will prioritize the found issues out of the box with a built-in risk-based engine. This is an excellent first start for any organization.

The first goal is to fix the biggest issues across your infrastructure. It is important to fix big holes on less important systems as hackers focus on these to get a foot in the door after which they will laterally move to the real interesting production systems and data. This is exactly what happens in a ransomware attack where one weak system/user is hacked after which many other assets will follow.

Not all assets have the same value to an organization. Organizations that have fixed the big issues across all systems can further prioritize their alerts by further tagging or sorting them according to their priorities.

> *An ASM solution will typically give a risk score and a trend line over time so management can follow up on the evolution of the work done and the remaining risk.*

As resources are always limited, it is likely that most organizations will settle on an acceptable remaining risk score. Ideally the organization can see how they are scoring within the average of their industry calculated from peers that are also on the platform.

Sweepatic is an Attack Surface Management Solution

Our customers leverage the Sweepatic Platform's discovery capability to **continuously find known and unknown IT assets**. Additionally they use our platform to **follow up on a prioritized list of security issues** discovered.

On top of our powerful discovery engine, we automatically inspect and report on **security issues** like vulnerabilities, misconfigurations in email/DNS/Web, weak encryption, expired and weak SSL certificates, exposed databases and file shares, exposed administrative access and much more.

To schedule your **personalized demo** with one of our Sweepatic experts, visit our website or reach out to us via info@sweepatic.com.

Sweepatic is an exciting young cybersecurity company, rapidly growing from start-up to scale-up. Our Sweepatic platform delivers attack surface management to our customers and partners, proactively protecting them from cyberattacks. Sweepatic has its headquarters in Leuven, Belgium, and is backed by eCapital, a leading German venture capital firm.

Request your demo

sweepatic.com/demo

Sweepatic | Kapeldreef 60, 3001 Leuven, Belgium | info@sweepatic.com | www.sweepatic.com