



A Primer for External Attack Surface Management (EASM)

Table of contents

What is External Attack Surface Management?

Why it's important to monitor your external attack surface?

Why are EASM tools valuable?

What are the common use cases for an EASM solution?

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

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

1. Continuous discovery

Asset elements that can be discovered:

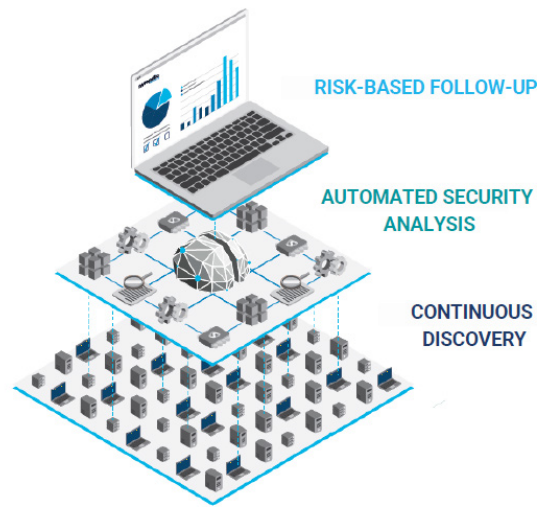
2. Automated security analysis

Typical security issues found:

3. Risk-based prioritization and reporting

Get Started with Outpost24's External Attack Surface Management Solution





What is External Attack Surface Management?

An emerging cybersecurity solution space with its own definition has been coined in recent years: Attack Surface Management or ASM. Gartner, Forrester and other industry analysts have described the term in recent reports, adding the word 'external' to indicate the outside-in perspective of these solutions. The term External Attack Surface Management (EASM) can however be confusing or vague without a clear definition. In cybersecurity there are many 'surfaces' that can be attacked. So what kind of attack surface are we talking about?

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

An IT asset can be anything that can help an attacker gain unauthorized access, build a foothold and penetrate critical systems 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, or stolen credentials that are sold on the dark web, etc. The end goal is usually to find vulnerabilities, misconfigurations, exposed data or other security issues that can be abused.

Why it's important to monitor your external attack surface?

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

An attacker will find as much information and weakspots as they can, in order to devise the best entry point and attack strategy. They will simulate normal traffic and search queries to gather as much data as possible. The 'cleaner' your attack surface is, the harder it is for attackers to find a way in. This can result in the attacker moving on to an easier target.

EASM is a foundational component of continuous threat exposure management (CTEM) programs because it supports the first three phases of CTEM: scoping, discovery and prioritization.

Gartner, Competitive Landscape: External Attack Surface Management 2023

Why are EASM tools valuable?

The attack surface of organizations is becoming ever more complex due to digital transformation:

- The continuous focus on the **digitization** of organizations in order to remain competitive.
- The adoption of **cloud technologies** and the speed of deployment the cloud brings.
- The **multi-cloud approaches** that many companies use to be fast and remain flexible.
- The empowerment of non-IT staff to deploy applications online via **SaaS offerings**.
- A **remote and hybrid workforce** that connect anywhere and use any device tools.
- Cyber security **experts** are limited in time, expensive and hard to find.
- **Enterprise IT infrastructure and systems** are in constant flux, making bi-yearly vulnerability scanning or other technical cybersecurity assessments way to slow as attackers are quick to exploit new vulnerabilities.

That is why organizations are finding it increasingly difficult to keep track of which IT assets are exposed online and pose the biggest risk, both on-premise and across the clouds. The biggest challenges are often in midsize to large organizations that manage a mix of old and new IT infrastructure which is continuously adapted and upgraded. Large organizations often struggle with visibility across 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. One of the big challenges is to know all the internet exposed IT assets in your environment. Talking with the different teams is often too slow and leads to incomplete results that doesn't paint the full picture. That's why, an automated and continuous attack surface discovery solution has become all the more important.

What are the common use cases for an EASM solution?

EASM solutions should be considered as part of a broader vulnerability and threat management effort aimed at discovering and managing internal- and external-facing assets and their potential vulnerabilities:

- Detecting **unknown and unmanaged assets**, Shadow IT and projects on-premise and across the cloud.
- Providing an external outside in view of your security **weak spots and risks** that cannot be discovered by traditional vulnerability scanners.
- **Reducing the internet exposed attack surface**: You can't protect what you don't know. 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.
- **Save time and money** by automating the manual work that needs to be done when patching together insights obtained from freely available open source scanning tools (OSINT).
- **Enhance security collaboration**: An external attack surface management solution gives a security overview across departments and brands. Empower business units with security insights and mitigate risks in their domain. The management can easily follow up on key metrics.

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

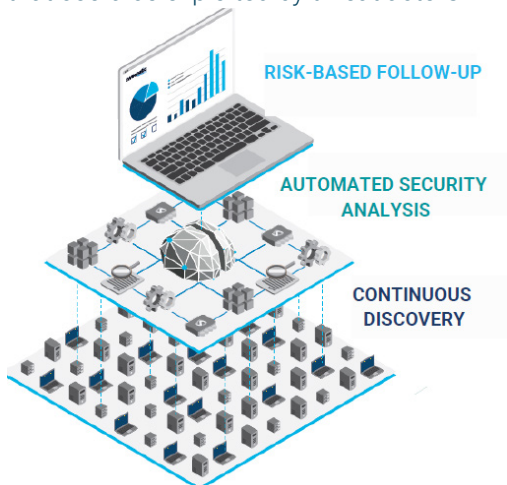
Many people wonder how an EASM scanner is different from a traditional vulnerability scanner.

1. **Internet facing only:** An EASM solution specializes in discovering the internet facing risk exposure.
2. **Discover the unknowns:** A vulnerability scanner focuses on known assets by assessing a list of known IP addresses or known cloud providers. EASM scanners discover 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. **Assess more than 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 external 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 External Attack Surface Management platform?

EASM empowers cybersecurity professionals by discovering internet-facing enterprise assets and systems and exposures that could be exploited by threat actors.



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 too time consuming and complex.

An EASM platform is heavily automated and should be easy to set up and get started.

An EASM solution typically has three key features:

- Continuous discovery
- Automated security analysis
- Risk-based reporting

1. Continuous discovery

The purpose of the EASM solution is to automate the discovery of your external assets. Start with your primary domain (ex. mycompany.com), or a list of primary domains for bigger organizations. Outpost24's EASM solution uses 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 finds assets that will trigger new scans. Because it is continuous, newly deployed or removed assets will be automatically detected and reported on a weekly basis.

Asset elements that can be discovered:

- All DNS records
- All related IP addresses
- WHOIS or DNS registration info
- Geolocations 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, DBs, remote access, file shares, 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](#), the Cyber Kill Chain starts with the reconnaissance phase. Hackers today run well-organized criminal enterprises that use the best automation tools available to them. Your EASM tool must be continuous to keep up.

Typical security issues 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-like websites that abuse your brand.

3. Risk-based prioritization and reporting

Outpost24's EASM solution prioritizes the found issues out of the box with a built-in risk-based engine.

With new vulnerabilities appearing on an hourly and daily basis, the goal is to fix the biggest issues across your infrastructure. Not all assets have the same value to an organization.

Our solution provides action plans on the mitigation of prioritized threats as well as integration with solutions such as ticketing systems, security orchestration, automation, and response (SOAR) solutions.

An EASM solution will typically give a risk score and a trendline over time so management can follow up on the evolution of risk reduction and the outstanding issues.

As resources are always limited most organizations will use the risk score to prioritize their remediation effort based on their risk tolerance level. Organizations can also see how they are scoring within the average of their industry calculated from peers that are also on the platform.

Get Started with Outpost24's External Attack Surface Management Solution

Our customers leverage the Sweepatic Platform's discovery capability to **continuously identify 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 prioritize 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 with real-time alerts.

[Get a free trial or a personalized demo](#)

About Outpost24

The Outpost24 group is pioneering cyber risk management with vulnerability management, application security testing, threat intelligence and access management – in a single solution. Over 2,500 customers in more than 65 countries trust Outpost24's unified solution to identify vulnerabilities, monitor external threats and reduce the attack surface with speed and confidence.

Delivered through our cloud platform with powerful automation supported by our cyber security experts, Outpost24 enables organizations to improve business outcomes by focusing on the cyber risk that matters.

 outpost24.com

 info@outpost24.com

 twitter.com/outpost24

 linkedin.com/outpost24