# What's Lurking Beneath the Surface

## Getting Started with EASM

CHARIOT

# Contents

# Getting Started with External Attack Surface Management

External Attack Surface Management (External ASM, or EASM for short) is a new category of Security Tools that are designed to help defenders identify and manage the machines they have exposed to the Internet. It's an exciting addition to the defender's tool chain, but EASM is still an emerging category of the security market. There will be a lot of shifts in this segment.

In this eBook, our goal is to explain the value proposition of EASM, how it works, and how to evaluate implementation and deployment choices. For example, should you buy into a managed offering or is a self-managed SaaS offering a better fit? Finally, we'll tie it all together with a discussion of what you can (and cannot) expect from EASM.

## Understanding the Value of EASM

At the broadest level, we can understand the goals of External ASM by pulling the acronym apart:

**Attack Surface:** Attack surface is all the different points an unauthorized user (the "attacker") tries to exploit to manipulate or steal data.

**Management:** A good EASM product will help you manage the attack surface in some way, either by helping you track vulnerabilities and exposures, or by helping prioritize the risks that actually matter.

With this understanding, we can better appreciate the value proposition of EASM, which is really three-fold.

1 | **Discovery:** EASM should tell you about assets you didn't know you had. This asset discovery role is crucial and in many ways is the "magic" functionality that makes EASM useful.

2 | **Scanning:** Once EASM has located your assets it's going to allow you to scan them for vulnerabilities. Vulnerability scanning and asset discovery are important to knowing your actual attack surface in detail. In the long-term, however, they are means to an end.

3 | **Prioritization:** EASM should help you prioritize the things it finds. Not all security exposures and vulnerabilities are created equal, and while the open framework for vulnerability scoring (CVSS) is useful it lacks the context stored within your environment. Getting a list of 200 vulnerabilities scattered across dozens of machines is a good start, but having a system warn you that two of them represent a critical business risk is a game changer.

## “Outside-in” vs. “Inside-out” Attack Perspective

Instead of looking at your entire network, EASM vendors take an “outside-in” view of the world, leveraging Open-Source Intelligence (OSINT) to view the system very much like a hacker would. While this sounds great, consulting approaches based solely on an external view of your network do not take advantage of your specialized insider knowledge of the network. Therefore, they can fail to deliver on the full promise of EASM tools for modern cloud environments.

### Outside-in: OSINT

From an outside-in perspective, almost every EASM system in the market uses OSINT to identify assets. Generally, OSINT is a type of intelligence gathering that uses information that can be found in the public domain.

**Broadly, EASM sources of OSINT can include:**

- **DNS**
- **Certificate transparency logs (CTLogs)**
- **IP ranges**
- **Passive tools like DNS database (DNSDB)**
- **Databases of assets like Shodan**
- **Search tools like Google Search**
- **Source code managers like GitHub**
- **Email and social media accounts**

You should be taking advantage of OSINT, because it’s how attackers see your network. However, it’s also only a part of the story. Like an iceberg, the real risk can lurk beneath the surface, inside your cloud, not even linked to your DNS.

> “For EASM to truly be effective, you need both OSINT (outside-in) and cloud integration (inside-out) visibility.”

### Inside-out: Cloud Integration

The right way to handle EASM is to leverage the knowledge and context you have of how the system is structured. For example, if you integrate your cloud environments and allow the EASM solution to pull data about workloads inside the private cloud, it becomes easier to understand which systems actually are connected to the Internet.

Similarly, a storage bucket that isn’t in your DNS is difficult to find, unless you leverage the asset tracking features of the cloud providers you use. Moreover, if you set up your EASM this way it can scan any asset immediately upon integration, which essentially reduces discovery time to zero.

As if all this wasn’t enough, you can also start to add context to your discoveries. A security scanner might have insight into how exploitable a vulnerability is, but it doesn’t know the value of the system it’s looking at. You do. Once you start to account for the value of assets based on your business, your prioritization gets better, and that means you’re able to make better security decisions.

When we look at a real-world example like Log4Shell the limitations of OSINT-only EASM become obvious. The challenge was finding all systems that contain the vulnerable Log4J component. To cause a breach, attackers only needed to get a system to log a line that contains, somewhere within it, specific text. Directly internet-connected systems were not the only ones breached. Systems inside the cloud were affected as well when they processed tainted data.

For EASM to truly be effective, you need both OSINT (outside-in) and cloud integration (inside-out) visibility. We can use cloud integration to understand where these vulnerable components are running, what they are doing, if they are directly reachable, and how important they are. Basically, we've gone from a "security nightmare" to a problem which not only is tractable, but also can be triaged by potential impact. The difference is night and day. Given that you, as a defender, have so few advantages, it would be foolish not to take advantage of the hidden knowledge that you have.

## Buy vs. Build

As you understand the processes around OSINT, you will quickly discover that many parts of an EASM system are available in the open-source community. Discovery tools, for example, are available on sites such as GitHub, and frankly these very same tools are often the mainstay of commercially-available systems. Should you build instead of buy? For 99% of businesses, the answer is likely no.

Most businesses often trade software cost for speedier time to market. This fact is perfectly illustrated by the rise of "managed" solutions in the cloud world, where a customer pays a premium to use a managed version of an open-source solution. The time saved by allowing an expert to apply best practices to a piece of infrastructure outweighs the increase in cost.

However, if that component is a core part of your business and if you have very specific needs that are very different from others, sometimes it may make sense for you to do it yourself. Similarly, if your environment is highly customized, well-funded, and managed by a mature security organization with a deep bench of OSINT and cloud expertise, then a "build solution" for EASM might be for you.

Even so, for almost all use cases, it would be better to start with a vendor offering and augment it rather than building it out entirely from scratch.

## SaaS or MSSP

When choosing EASM solutions, the most common delivery mechanisms are cloud-based (SaaS) and managed security services providers (MSSPs).

A SaaS-based solution will essentially provide the software you need to get up and running with EASM via the cloud. Its primary advantage is pay-as-you-go models where signing up is a matter of just typing in a credit card and, voila, EASM is running. That simple sign up paired with SaaS systems' ability to scale simply by adding computing power make them relatively low cost to operate. They often are less expensive than MSSPs, which are human intensive. As such, SaaS-based EASM platforms can be a very attractive option.

| Feature | SaaS | Managed Services |
|---|---|---|
| Implementation Complexity | High | Medium |
| Cost of Services | Low | High |
| Prioritization of Issues | Machine Driven | Human Groomed |
| Accuracy of Issues | Medium | Very High |
| Remediation Assistance | Low | High |
| Operational Cost | High | Low |
| Asset Discovery | Good | Great |

Table 1: Differences between SaaS and Managed EASM Solutions

In contrast, the MSSP route is more involved and usually more expensive. Given that it takes - at least initially - a bit more time and money, what are you getting for your hard-earned cash?

First, MSSPs are broad in that they often offer a wide range of services. You can think of some MSSPs as a one-stop-shop for your security needs, and others are specialists who focus on being best-in-class at just one or two services.

Regardless of the size and breadth, a good MSSP will be a genuine extension of your team - whether your in-house security team or your Engineering/IT team in general. Look for an MSSP with very high net promoter (NPS) scores, which measure customer loyalty, and ask them for evidence that their customers love them.

Whereas a SaaS product is tuned for price and scalability, a good MSSP provider should be focusing on the overall quality of the results returned. This is most important when you consider the degree of analysis you will get for your dollar. Can you live with automation, or do you require human-filtered expert insight?

### Should You Invest in EASM?

Whenever considering a new product or service, you should take an honest assessment of your security maturity, because every company is different. To really get the benefit of EASM, we believe that you need to be well into your security journey. If you're not already running endpoint protection and patching software on a regular basis, then EASM is yet another item on your "to do" list. Visibility without action just doesn't help you move the ball up the field.

If, however, you have got a complex cloud environment, and you have  got the basics covered, well, why wouldn't you want to know what's going on? The only possible reason comes down to ROI.

When viewing your security, take a careful note of both factors within your control (visibility, backups, staffing, etc.) and externalities (attacker tactics, techniques, and procedures). Armed with this list, you should be able to identify the most important threats that you do not currently handle (i.e., your largest risk - the composition of impact and likelihood). When you think of the investment required, it's important to think about the trifecta of time, people, and money, not just the dollar cost.

If this analysis reveals that your most pressing risk is related to management of the attack surface, then your decision is made. From here, it is just a matter of picking the right product, deploying it, and getting started. That's what we turn our attention to next.

## What to Look For in EASM

Once you've decided that the benefits of EASM are right for you and it's the next thing on your priority list, it's time to pick your partner. Here, we'll look at some things to look for when selecting your product. The list could be pretty long, so we're going to boil it down to just six points.

### 1 | A Partnership, Not a Product

We will start with a major issue that we've seen in the security world time and time again: you need a partner, not a vendor. So many vendors sing that partnership song, but very few will be there with you when it's all going wrong. We know this is somewhat subjective but trust us when we say that you need to decide if you're getting the partnership you need. The level of partnership does vary based on spend, but if you are entering into a managed service relationship, make sure you know what makes your vendor tick. You need someone in your corner, and the quality of the support and advice you get is as important as the product itself.

How can you tell? Look for customer testimonials. Ask around your network. Do your research, not only on the product but also on the company as a whole.

## 2 | Offensive Security Qualifications

While many of the best people in security have non-traditional backgrounds (in the early days of hacking, almost nobody had a Computer Science degree), experience does matter. Take some time to research the company you're partnering with if you're going the managed route. Attackers are going after your data, so consider the offensive security experience of the MSSP:

- Look for seasoned operators with penetration testing and "red team" skills who can ethically hack vulnerabilities and trace compromise paths to help you prioritize real risk.
- Evaluate how well the security service understands and maps their solution to the MITRE ATT&CK framework. What is the frequency of the partner's contributions to ATT&CK research and techniques?
- Today's attackers are likely to be nation-states as well as individual cybercriminals. A team of security specialists with federal civilian, intelligence, or military backgrounds typically have experience in high-assurance and mission-critical environments.

LinkedIn can help here, as well as your People Ops/HR teams. Bring them in and have them assess the qualifications of the people you are relying on to keep your business safe. In a managed service, you should be as fussy about the qualifications of the team as you would be about your key hires.

## 3 | Attack Lifecycle Vision and Positioning

When you buy a product or a service, you are going on a journey with that company, it's not transactional, like buying a cup of coffee; instead, both parties invest time and money for, in an ideal world, a journey. You need to make sure that your vendor can deliver on where they're promising to take you. It's a cliché in sales that customers buy the vision but use the product. That can be fine - but make sure your new partner has a solid path toward realization of that vision.

The attack lifecycle commonly consists of four phases: identify, attack, detect, and prevent. Does your partner cover all the bases?

**Identify:** continuously discover known and unknown internet-facing and cloud assets

**Attack:** exploit vulnerabilities to signal what truly matters and prioritize risk mitigation

**Detect:** ensure your security program can detect and respond to real-world attacks

**Prevent:** stop future occurrences through automation and policy management

Even if your vendor of choice has a strong ability to deliver on their vision, their vision should align with yours. There are lots of ways to "do" security; make sure that you're going on the journey that aligns with your direction and worldview.

## 4 | Inside-Out Asset Discovery is a Must

This should go without saying, but it's actually rarer than you would think. Make sure that your vendor has a *really* good story about cloud integration and explore how their service makes use of it. Integration is easy; truly leveraging that data is another matter. You need a product that can fully leverage the few advantages you have over the attacker. Because of that, having robust integrations - encompassing source code repositories like GitHub, public cloud providers, container registries, agile and development tools like Jira, and other CI/CD workflows - and a way to demonstrate the types of detection they enable should be non-negotiable.

## 5 | Efficacy

It feels very strange to have "efficacy" near the end of the list, but as is so often the case, the real measure of a security program is risk reduction. Being a percentage point better at finding an obscure vulnerability is less impactful than you might think. With that said, and with all other things being equal, you obviously want the absolute highest efficacy money can buy. Just remember it's not the whole story.

## 6 | Risk Prioritization

So, you've made up your mind, you've placed your order - you're ready. Your product is selected, you've got your budget wrangled, and you're about to hit the "start" button. Here we consider the things you should keep in mind right before you turn on your EASM solution for the first time.

The very first thing you need to be ready for is the scans will very likely find vulnerabilities. That's okay - in fact, it's very much a good thing. Your new EASM solution didn't create them, it just found them, and now you can deal with them.

If you've gone the managed service route, see what kind of input and advice you can get from your security partner. It's likely they've seen this before lots of times and can help you prioritize. That word is really important here: you cannot and should not jump in and think you have to fix all this tomorrow. It's about triage:  Do the most important first, and you'll be better off. Try and do them all at once, and it'll likely feel like more trouble than it's worth.

You'll very likely be getting a security scorecard or board level metrics of some kind. It's also worth managing upward a little bit. Any time you turn the light into the dusty corners of your network, it can be scary. The important thing to communicate is that this is reality and the right measure is that you're getting better with each step. Even if the results aren't what you want, it's important to communicate clearly with the team that this is the path toward safety.

# Conclusion

As we have discussed, EASM is a powerful defensive technique that can dramatically improve the cybersecurity stance of the business. Moreover, correctly implemented it becomes a business accelerator, not a hurdle.

Getting the right partner for delivery, whether as a managed service or SaaS offering is critical, and we hope that this guide has provided the orientation you need to make the very best decision for your business. There is no such thing as a "universal" solution that's right for everyone; instead, you need to consider the factors that make your business unique and the constraints with which you work. If it's time and people, a managed approach is best for you; conversely, if you are limited entirely by budget, then a SaaS solution can be a cost-effective way of realizing the promise of EASM.

By increasing your understanding of the value proposition and how it is realized, you'll be able to operate more effectively. At the end of the day, that is what it's all about: happy and safe businesses that can advance quickly with their business objectives while managing security risk based on business need.

### Ready to Discover Exposures?

Let's get started with a demo.

praetorian

## About Praetorian

Praetorian delivers the only end-to-end security platform and managed service that acts like attackers to protect customers. As an extension of your security team, Praetorian helps enterprises achieve business resilience by continuously discovering assets, contextualizing their relationship and import, pinpointing vectors of compromise, and personalizing protection to remediate future risk. Engage with Praetorian offensive security engineers and experts to locate your critical exposures and continuously validate your cybersecurity program. Follow at www.praetorian.com or Twitter and LinkedIn.