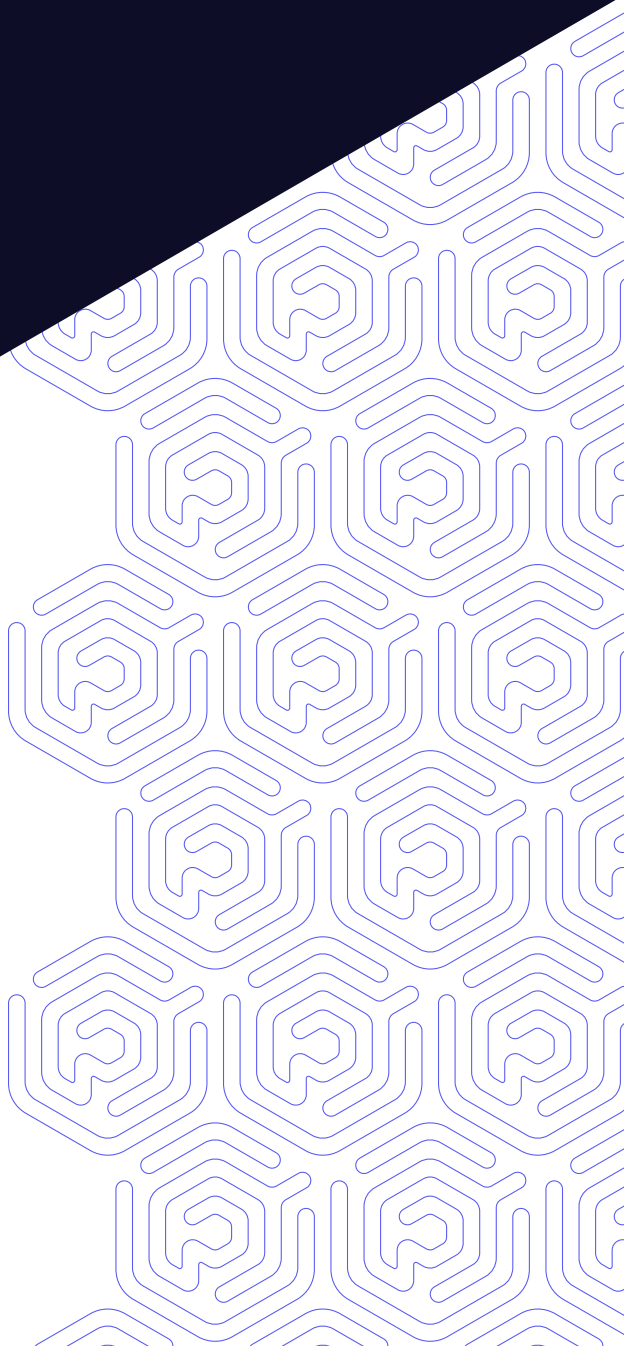
WHITE PAPER

# What's Lurking Beneath the Surface?

## A CISO's Guide to Choosing an EASM Vendor



praetorian

# Getting Started with External Attack Surface Management

INSIDE THIS REPORT



External Attack Surface Management (External ASM, or EASM) is a new category of Security Tools that help defenders identify and manage the systems 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. We expect to see 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 employment 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. **Discover** 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 immediately useful.

2. **Scan** 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. **Prioritize** 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

Many 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 instead of looking at your entire network. 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

Almost every EASM system in the market uses OSINT to identify assets and gain an outside-in perspective. Generally, OSINT is a type of intelligence gathering that uses information from the public domain.

→
Broadly, EASM sources of OSINT can include

- DNS
- Certifcate 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 Git Hub
- 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.

## Inside-Out: Cloud Integration

The way to maximize the impact of EASM is to leverage your knowledge and context of how the system is structured. For example, if you integrate EASM with your cloud environments and allow it to pull data about workloads inside the private cloud, you will more easily 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 related system. You do. Once you start to account for the value of assets based on your business, your prioritization improves. That means you're able to make better security decisions.

### You Need Both for Maximum Impact: Real World Example

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

This is an excellent example of why, **for EASM to be truly effective, you need both OSINT (outside-in) and cloud integration (inside-out) visibility.**

With a combined approach using our EASM solution, once we found vulnerabilities we could use cloud integration to understand where they were running, what they were doing, if they were directly reachable, and how important they were. Basically, combining the two approaches took us from a "security nightmare" to a problem which not only was tractable, but also could 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 probably is 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, doing it yourself may make sense. 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.

## What Type of Product

When choosing EASM solutions, the most common delivery mechanisms are risk-rating platforms, cloud-based applications (SaaS), and managed security services providers (MSSPs). Most risk-rating platforms' primary advantage is that they offer pay-as-you-go models where signing up is a matter of just typing in a credit card and, voila, EASM is running. They are low cost to operate, but the ROI also is low because the findings are less accurate and the vendors do not offer prioritization or remediation assistance.

A SaaS-based solution will provide the software you need to get up and running with EASM via the cloud. The implementation is very complex and expensive, but once integrated the SaaS systems' ability to scale by adding computing power makes them relatively low cost to operate. As such, SaaS-based EASM platforms can be a very attractive option.

| Feature | Risk-Rating Platform | SaaS | Managed Services |
|---|---|---|---|
| **Implementation Complexity** | Low | High | Medium |
| **Cost of Services** | Low | Low | High |
| **Prioritization of Issues** | Low | Medium | Very High |
| **Accuracy of Issues** | Low | Medium | Very High |
| **Remediation Assistance** | Low | Low | High |
| **Operational Cost** | Low | High | Low |
| **Asset Discovery** | Low | 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 would you be 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 a very high net promoter score (NPS), which measures 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 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?

Every company is different, so whenever you are considering a new product or service you should take an honest assessment of your security maturity. To really get the benefit of EASM, we believe that you need to be well into your security journey. If you have a complex cloud environment and you cover basics such as endpoint protection and regular software patching, you also need to understand your attack surface.

Given the dynamic nature of securing systems based on microservices, cloud infrastructure, and APIs, the ability to identify and close gaps in your perimeter has become a necessity. That being the case, why would an organization like yours debate whether to invest in EASM? It comes down to the metrics and KPI used to measure the efficacy of your overall program.

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. What you define as your largest risk should combine your assessment 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, your focus will be on 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, the next step is to pick your partner. Here, we'll discuss six things to look for when selecting your solution.

## A Partnership, Not a Product

We will start with a major issue that we've seen in the security world time and time again: So many vendors sing the partnership song, but very few will be there with you when it's all going wrong. You need a partner, not a vendor, to maximize your ROI from EASM. 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. Trust us when we say 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 if a vendor will be a good partner? Look for customer testimonials. Ask around your network. Do your research, not only on the product but also on the company as a whole.

## 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, particularly if you're going the managed route. Attackers are going after your data, so consider the following indicators of an MSSP's offensive security experience:

- **Seasoned team** 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.

- **Framework familiarity** 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? Do they simultaneously allow for the likelihood of attacks that fall outside the framework?
- **Adversarial backgrounds** Today's attackers are likely to include 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 and/or HR team. Bring them into your decision making process and have them assess the qualifications of the people you are relying on to keep your business safe. When selecting a managed service, you should be as fussy about the qualifications of the vendor's team as you would be about your key hires.

## Attack Lifecycle Vision and Positioning

When you buy a cybersecurity product or a service, you are establishing a partnership with the vendor. It's not transactional, like buying a cup of coffee; instead, both parties invest time and money to create, in an ideal world, an ongoing solution. You need to make sure that your vendor can deliver on that solution even (especially) during events like Log4Shell. One sales cliche states that customers buy the vision but use the product. That can be fine, but make sure your new partner has a viable path toward realization of that vision.

The attack lifecycle commonly consists of four phases–identify, attack, detect, and prevent, which we have defined below:

- **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

Does your partner's technology cover all the bases? Alternately, do they offer a human-driven approach to supporting your team from discovery through to prevention?

Even if your vendor of choice has a strong ability to deliver on their vision, you need to verify that it aligns with yours. There are lots of ways to "do" security; make sure that you're committing to a solution and partnership that aligns with your direction and worldview.

## Inside-Out Asset Discovery is a Must

Cloud misconfigurations and hard-coded secrets can lead to internet-facing vulnerabilities that attackers can use to gain a foothold for lateral access to other parts of your network. Despite that, inside-out asset discovery is rarer than you would think. Robust integrations–encompassing source code repositories like GitHub, public cloud providers, container registries, agile development tools like Jira, and other CI/CD workflows–and a way to demonstrate the types of detection they enable should be non-negotiable.

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; accessing the telemetry necessary to accelerate your prioritization and remediation workflows is exceedingly difficult. You need a product that can fully leverage the few advantages you have over the attacker, and provide you context for your strategic decisions.

## Efficacy

It feels very strange to have "efficacy" near the end of the list, but the real measure of a security program is material 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.

## Risk Prioritization

As we mentioned previously, finding vulnerabilities doesn't reduce material risk. Acting to mitigate the most critical vulnerabilities does. When selecting a partner, consider how clearly their solution will communicate the relative priority of findings. If you're looking

at a SaaS product, will you be able to set up the dashboard to take into account your business risk and inside-out knowledge? Similarly, if you're leaning toward an MSSP will the vendor's extension of your team be able to accurately prioritize the findings?

# Before You Dive In

So, you've selected your product, you've wrangled your budget, 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 that 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. They've most likely seen a similarly sized collection of initial findings before and can help you prioritize. You cannot and should not jump in and think you have to fix everything tomorrow. It's about triage: do the most important first, and you'll be more secure and realize a ROI. Try and do them all at once, and it'll likely feel like more trouble than it's worth.

We also strongly suggest you develop a plan for managing upward a little bit. Any time you turn the light into the dusty corners of your network, it can be scary. You'll very likely be getting a security scorecard or board level metrics of some kind. The important things to communicate when presenting this information are that this is reality and the best metric moving forward is material risk reduction with each step. Even if the results aren't what you want, the most important point to emphasize with your board (and your team, for that matter) is 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 your business. Moreover, when 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 comes to fruition, 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 their business needs.

**Ready to Discover Exposures? Let's get started with a demo.**