PRAETORIAN

WHITE PAPER

What's Lurking Beneath the Surface?

A CISO's Guide to Choosing an EASM Vendor

INSIDE THIS REPORT

INTRODUCTION

Getting Started with External Attack Surface Management

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 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

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 by tracking 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.

3. **Prioritize**

   EASM should help you prioritize the things it finds. Not all security exposures and vulnerabilities are created equal. Getting a list of 200 vulnerabilities is a good start, but having a system warn you that two represent critical business risk is a game changer.

ATTACK PERSPECTIVE

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.

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, Databases of assets like Shodan, Certificate transparency logs (CTLogs), Search tools like Google Search, IP ranges, Source code managers like GitHub, Passive tools like DNS database (DNSDB), 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.

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.

IMPLEMENTATION

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.

PRODUCT TYPES

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.

EASM Solution Comparison

Feature	Risk-Rating Platform	SaaS	Managed Services
Implementation Complexity	Low	High	Medium
Cost of Services	Low	Low	Very High
Prioritization of Issues	Low	Medium	Very High
Accuracy of Issues	Low	Medium	High
Remediation Assistance	Low	Low	High
Operational Cost	Low	High	Low
Asset Discovery	Low	Good	Great

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.

INVESTMENT DECISION

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.

VENDOR SELECTION

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.

Offensive Security Qualifications

While many of the best people in security have non-traditional backgrounds, 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:

- **Seasoned team** - Look for operators with penetration testing and "red team" skills
- **Framework familiarity** - Evaluate MITRE ATT&CK framework understanding
- **Adversarial backgrounds** - Teams with federal, intelligence, or military experience

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 an ongoing solution.

The attack lifecycle commonly consists of four phases:

1. **Identify**
   Continuously discover known and unknown internet-facing and cloud assets
2. **Attack**
   Exploit vulnerabilities to signal what truly matters and prioritize risk mitigation
3. **Detect**
   Ensure your security program can detect and respond to real-world attacks
4. **Prevent**
   Stop future occurrences through automation and policy management

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–should be non-negotiable.

Efficacy & Risk Prioritization

The real measure of a security program is material risk reduction. 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.

GETTING STARTED

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.

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.

FINAL THOUGHTS

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.

www.praetorian.com | info@praetorian.com