Cyberint

4 Key Considerations Before Renewing Your EASM Solution

The external attack surface management market is just a few years old. But in this short time frame, much has changed. The threat landscape has grown exponentially and shifted the needs of cybersecurity teams at organizations in all industries and regions. Before renewing with your current provider, it's worth taking a moment to consider your satisfaction, goals, and alternatives.

Can EASM address all external exposure use cases now– and in the future?

The External Attack Surface Management (EASM) contract renewal period is a perfect time for re-assessing how EASM fits into current and future needs and objectives.

Goals may include streamlining your security stack, integrating EASM into other cybersecurity programs, and maximizing ROI in terms of cybersecurity as well as business operations. It's also worth evaluating satisfaction whether your current solution has kept pace with the technological developments in the market.

The list below contains 4 key considerations to think about during your contract review, coupled with actionable questions that will help you determine whether you should renew your EASM contract– and if not, what to do next.

01/

Coverage

As digital life expands, so does the size of your external attack surface, the prevalence of vulnerabilities, and the level of risk you must address.

By implementing advanced converging technologies and methodologies, organizations can improve their attack surface coverage beyond the perimeter and provide their teams broader visibility and into external risk exposures beyond the perimeter.

Questions to ask yourself:

1. Does my EASM solution feature the most advanced coverage of my external IT assets?
2. How fast and effective is my EASM solution in discovering and validating my new assets as they are deployed?
3. Does my EASM solution offer coverage beyond the perimeter with threat intelligence to provide coverage for use cases like leaked credentials and malware infections, or do I need another point solution?

02/

Fidelity

Organizations are struggling with noise. If your EASM solution is picking up assets that aren't yours, you may end up with useless alerts regarding someone else's problems.

By converging advanced technologies, methodologies, and service models, organizations can minimize false-positives and provide their teams the focus needed to improve efficiency and performance, resulting in elevated cybersecurity and optimal posture.

Questions to ask yourself:

1. How does my EASM solution reduce false-positives findings?
2. Can my EASM solution deliver focus on scale according to my needs?
3. Does my EASM solution have built-in expert assistance?

Cyberint

03/

Confidence

External attack surface management solutions often output alerts and actionable insights designed to help cybersecurity teams better detect, protect and investigate external risk.

Such insights need to be backed up by confidence levels and possible audit trails to ensure they are as reliable as they are accurate.

Questions to ask yourself:

1. How does my EASM solution provider determine if a certain finding is relevant?
2. What evidence can my EASM solution provide to back up the accuracy of insights?
3. Does my EASM solution add context to alerts to make it easier to address them and resolve the issue?

04/

End-to-end solution

External attack surface management products should go one step further than merely providing visibility on risks and issues.

An exceptional EASM solution should provide contextualized alerts and integrations with your current stack to accelerate response, investigation, and remediation. EASM vendors should serve as an extension to your in-house capabilities, helping to not only identify risks but eliminate them.

Questions to ask yourself:

1. Does my EASM solution integrate with my other security solutions?
2. What is the scope of services and supporting capabilities my EASM solution provider offers?
3. Can they provide concrete evidence and quantitative data regarding their success rate?

What's next after EASM?

EASM provides value in many areas. However, in order to get maximum value from your external attack surface management solution, you need additional, complimenting capabilities.

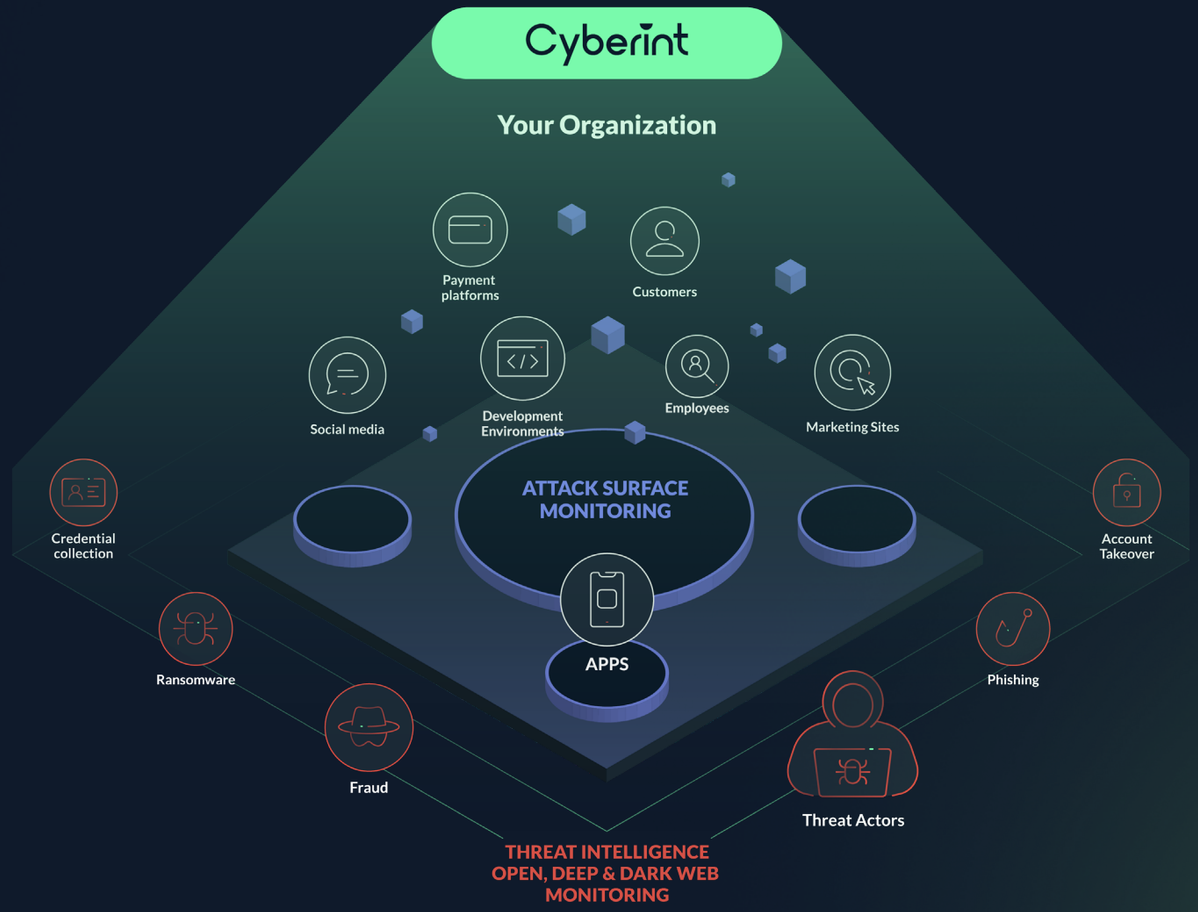
One option is to purchase and integrate additional point solutions such as Threat intelligence and Digital Risk Protection Services.

A better option is to implement a natively integrated solution that converges all capabilities into one powerful solution. This provides **impactful intelligence**.

Cyberint

What is impactful intelligence?

Cyberint's Argos is a platform that converges digital risk protection, threat intelligence, and attack surface management functionalities into a unified service, providing organizations with extensive visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, it allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier on the cyber killchain.



For intelligence to be impactful it needs to be:

Accurate

Actionable

Cost effective

Relevant

How impactful intelligence modernizes risk visibility and exposure mitigation

01/ Coverage

Cyberint's solution helps prevent, detect, and investigate dozens of use cases such as phishing, fraud, ransomware, malware, data leakage, account takeovers, brand abuse, intellectual property infringement, and more.

02/ Fidelity

Upon completion of EASM autonomous discovery, the relevant threat intelligence—sourced from the open, deep and dark web– is mapped to your organization's external assets, resulting in focused, actionable intelligence since it's tailored to your attack surface. Cyberint's intelligence team helps sanitize the data and triage alerts. This sets you and your team on a path to zero false-positives. This human-machine power combo results in unparalleled relevance, eliminates alert fatigue, and keeps teams laser-focused on the right actions to minimize external cyber risks.

03/ Confidence

For each and every finding, Argos includes a confidence level attribute, providing a probability estimate on the relevance of the alert and the accuracy of the risk assessment. Cyberint's intelligence team then verifies, validates, and, if needed, further investigates, before surfacing the finding. This results in high fidelity data that allows your team to efficiently prioritize and remediate the issue.

04/ End-to-end

Advanced automation is supplemented by human expertise everywhere needed– from contextualizing intel, all the way to taking actions such as takedowns and proactively engaging with threat actors under aliases/avatars. The sheer number of takedowns Cyberint does every month, combined with the expertise of its analyst and customer success teams, has turned the company into a source-of-truth for vendors, completing your takedown requests faster.

Cyberint

Impactful intelligence vs. EASM

External Attack Surface Management is only one part of impactful intelligence. Organizations wishing to achieve total visibility and maximize prevention and remediation of external risk exposures need to also leverage digital risk protection and real-time threat intelligence.

Capability	Use Cases	Limitations	Impactful intelligence - the native fusion of EASM, DRPS, TI
Standalone DRPS product	Brand protection; social media monitoring; phishing protection	Provides coverage for abuse of trademarks and logos, but does not discover or monitor the attack surface.	A fully integrated solution to provide coverage for all external risks. Threat intelligence is mapped to the customer's digital footprint, including both external IT assets as well as brand trademarks, to provide targeted, actionable, and extremely high-fidelity alerts.
Standalone EASM product	External IT asset discovery and management; issue and CVE detection; risk assessment	Discovers shadow IT, misconfigurations, and other errors in the security perimeter, but ignores all other external risks.	
Standalone threat intelligence product	Deep & dark web monitoring; malware intelligence; leaked data detection; compromised credentials detection	Provides valuable threat intelligence but may lack relevance, as it isn't mapped to the organization's digital footprint	

Getting started with Cyberint

Argos is the first platform natively fusing digital risk protection, threat intelligence, and external attack surface management. Using Argos, customers can better prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities and more, ensuring continuous external protection from cyber threats.

> Get started