


# Raising The Stakes for Attack Surface Management

The first generation of external attack surface management (EASM) products were founded on a single yet powerful premise: security teams cannot protect the assets that they do not know about. This is just as true today as it was when EASM products were first developed.

However, the market has evolved and single-purpose EASM products are no longer sufficient. Now, incorporating threat intelligence is table stakes when it comes to attack surface management solutions.

---

This e-book will discuss the progression of the attack surface management market and explain why the combination of threat intelligence and EASM is essential to effectively mitigating external risks.

A decorative graphic consisting of a cluster of small red and white dots is located in the bottom left corner of the page. The dots are arranged in a somewhat irregular pattern, with some larger dots and some smaller ones. In the bottom right corner, there are large, faint, overlapping circular shapes in shades of green and blue, which appear to be part of a larger design or background element.

# Table Of Contents

---

4	Introduction
5	The Ever-Expanding External Attack Surface
6	Drilling Down On Attack Surface Risks
7	Gain A Continuous View Of The Attacker's Perspective
8	Attack Surface Management: It's A Process
9	Raising the Stakes: Threat Intelligence Mapped To Your Attack Surface
10	Better Together: The Benefits Of Combining Threat Intelligence & EASM
11	The Cyberint Argos™ Platform: Greater Than The Sum Of Its Parts
12	Why Customers Choose Argos™

# Introduction

---

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 become exponentially more hostile in just a few short years. This has shifted the needs of defending security teams at organizations in all industries and regions.

Alongside these developments, the technologies and solutions provided by security vendors have also evolved to combat the latest threats and meet the needs of security teams. External Attack Surface Management solutions have also developed in this regard.

The first generation of EASM solutions automated the processes of asset discovery and asset inventory maintenance. As with most automated solutions, there was great value in these products: they automated a repetitive and tedious process, which saved time and freed up resources so they could be reallocated to focus on other important (and more gratifying) projects.

Many EASM solutions went beyond this simple asset discovery and inventory step to include other capabilities: checking for common risks and vulnerabilities, assigning risk scores, prioritizing issues, and integrating with ticketing systems to simplify remediation efforts and track changes over time.

More recently, the combination of threat intelligence and attack surface management has become the new standard— and for good reasons. The fusion of these two capabilities provides immense value to security teams.

This ebook will discuss the foundational capabilities of EASM solutions, discuss how these technologies and markets are evolving, and explain why the next generation of external risk mitigation platforms will continue to move in this direction while adding in other features, like phishing detection, brand protection, and social media monitoring.

# The Ever-Expanding External Attack Surface

---

Automated EASM products can keep pace with the corporate digital footprint, which is constantly expanding, by continuously discovering and inventorying new assets as soon as they are deployed. New assets are checked for common security errors, vulnerabilities, and other issues.

While EASM products address the challenge of an expanding digital presence, the visibility gap between what is known and what actually exists remains a risk for most organizations. Below are some of the factors that continue to contribute to the severity of this challenge.



## Cloud Migrations

Many organizations operate several cloud environments with different service providers, in addition to legacy on-premise data centers. This expands the breadth of the attack surface and can introduce challenges in tracking all external assets across all environments.



## New Domains & Websites

Organizations are now hosting more domains, subdomains, and websites than ever before. In many cases, new assets are being created and launched by various teams in different regions. This makes it difficult for security personnel to keep visibility on all the new assets being deployed.



## An Increase In Applications

Almost every organization builds and deploys software, whether it's a simple web application, a mobile app, or a specialized SaaS product. In all cases, the app must be deployed and hosted on your organization's infrastructure, so it adds to the scope and complexity of the attack surface.



## Internet-of-Things Devices

Internet-of-Things devices can be hard to track, as it isn't always clear which are connected to corporate networks. In one infamous case, attackers breached a major retailer through its Internet-connected HVAC system. Keeping up with IoT devices is an attack surface challenge.



## Ephemeral Environments

Some environments are designed to be temporary. Microservices create and delete new resources to match demand. Build environments are often used just once. These assets add complexity to the attack surface, especially if an asset is supposed to be decommissioned but is not.

# Drilling Down On Attack Surface Risks

---

As the attack surface grows, there are myriad external issues that can lead to a breach of a corporate system or network. These risks are not new but they are persistent concerns, as the attack surface is constantly expanding and changing shape. A single shadow IT asset with an exploitable open port or an old CVE can lead to a devastating breach.

Because these external risks are still frequently utilized as attack vectors for bad actors, EASM solutions both old and new identify these kinds of issues. Here are some of the most critical risks that can be found in the external attack surface.



## Shadow IT

You can't protect the assets that you don't know about. It's essential to identify shadow IT, old infrastructure, and unauthorized assets, so you can bring them all into compliance.



## Hijackable Domains

Errors in DNS records can make it possible for threat actors to hijack a domain or subdomain, allowing them to send traffic to the IP address of their choosing.



## Open Exploitable Ports

Open remote access ports— like SSH (port 22) and RDP (port 3389)— present massive risks when not properly secured. These ports should only be open temporarily and when absolutely needed.



## High-Risk Vulnerabilities

It's common to have vulnerabilities in your external software and services but the risks increase exponentially when the CVEs in your attack surface are actively being exploited in the wild.



## Exposed Databases & Cloud Storage

Human error sometimes causes databases and cloud storage buckets to be exposed to the public Internet. Detecting these errors as quickly as possible is critical to avoiding a data breach.

# Gain A Continuous View Of The Attacker's Perspective

---

The first stage of an attack is reconnaissance. Threat actors will use open source tools and techniques— from search engines and DNS records to port scanners and network mapping tools— to learn every inch of your external security perimeter. If there is a gap in your defenses, they will immediately get to work in exploiting it.

To protect your organization, you need to look at your infrastructure through the eyes of an attacker. If you were targeting your own organization, where would you start? By finding the soft spots that offer the best opportunity to successfully breach the network.

There are existing techniques that try to find these weaknesses and vulnerabilities. Consider penetration tests, which allow skilled hackers to play the role of threat actors and try to break into your network. However, these tests are point-in-time assessments that are often performed just once or twice per year, so they cannot continuously identify new risks as they appear.

To give another example: vulnerability scanners. While these tools provide plenty of value, they cannot operate without a full IP whitelist. In other words, you must tell the program exactly which assets to scan. This means they cannot detect shadow IT or misconfigurations, which is a real limitation when security teams are trying to keep up with an expanding attack surface.

EASM solutions were designed to detect unknown assets, map out the attack surface, and identify potential issues in a continuous, ongoing manner. Continuous visibility is a major benefit that adds value in addition to the time saved by automating the external asset discovery and inventory process. This automated and continuous functionality continues to be one of the primary value drivers of EASM solutions.

# Attack Surface Management: It's A Process

---

It's often said that cybersecurity is about people, processes, and technology. While there are technologies that help, it's important to remember that attack surface management falls firmly into the process category. As mentioned earlier in the e-book, many of the steps in the EASM process can be automated, making the process much easier and faster for security teams.

It's also worth pointing out that attack surface management is not a new process. In years past, this process would simply be performed manually and managed in spreadsheets. Analysts would hunt for domains, subdomains, IP addresses, servers, and software that they did not know about. If they found a shadow IT asset, they would simply add it to the list.

Now, with IT infrastructures becoming so large and complex, it's no longer practical to perform this process manually. Even if you tried, it would likely become prohibitively expensive, as you would need to dedicate several full-time resources to this project.

As with other important but tedious duties, managing an IT asset inventory is a task best left to automation. External Attack Surface Management solutions were first developed to conduct the asset discovery process, create an asset inventory, identify common issues, and assign risk scores to issues and assets. The automation saves time, enabling security teams to receive alerts about high-risk issues so they can immediately address them before they lead to an incident.



# Raising the Stakes: Threat Intelligence Mapped To Your Attack Surface

Over the past few years, the External Attack Surface Management market has evolved quickly. Many EASM products are now integrated into a larger offering, most often a threat intelligence solution. This has become so common that it's now table stakes: external attack surface management without threat intelligence is an incomplete solution.

Let's drill down on what exactly it means to map threat intelligence to an organization's attack surface. As we've already discussed in this e-book, the external attack surface is made up of many components—among them, an organization's domains, subdomains, IP addresses, and so on.

Tailoring threat intelligence to an organization's attack surface means correlating the organization's assets with all of the intelligence items collected to see if there are any matches. For example, threat intelligence services discover credential dumps on the dark web. When attack surface management is added into the mix, an organization can receive immediate notifications if credentials to one of their domains appear in the credential dump (e.g. the username jane.doe@examplecustomer.com and the corresponding password are leaked).

In addition to identifying relevant leaked credentials, the intersection of threat intelligence helps organizations get visibility on threats like mentions in threat actor communities, data leakages, malware infections, and more.



## Compromised Credentials

Detect leaked credentials for both customers and employees.



## Targeted Chatter On The Dark Web

Discover when your organization is being mentioned in closed threat actor forums.



## Data Leakages

Identify data leakages, from source code and other IP to sensitive internal data and PII.



## Malware Infections

Receive alerts if your organization or domains appear in malware logs on the dark web.



# Better Together: The Benefits Of Combining Threat Intelligence & EASM

---

The benefits of combining threat intelligence and attack surface management are somewhat intuitive. To see the added value of this duo, let's consider what each capability looks like independently.

On one hand, we have threat intelligence. This data is extremely valuable, but if it isn't correlated to an organization's external attack surface, then it's little more than a library of information that lacks relevance and context. Which intelligence items are important? Which items represent real threats? Without correlating the data to an organization's digital footprint, it's very hard to know the answers to those questions.

On the other hand, we have attack surface management solutions. These are also very valuable on their own, but they only look at issues in an organization's external IT infrastructure: misconfigurations, open ports, expired SSL certificates, high-risk CVEs, and so on. Standalone attack surface management solutions miss all the other external threats, from brand abuse on phishing sites and fake social media profiles to dark web threats like stolen credentials and data leakages.

The combination of threat intelligence and attack surface management provides several major benefits. First, it results in targeted, actionable alerts that can be quickly addressed by security teams. Second, because organizations only receive intelligence tailored to their digital footprint, the alerts are very high-fidelity and contain few false positives. Finally, pairing threat intelligence with EASM identifies urgent risks and threats that may not be easily identified by either solution independently.

# The Cyberint Argos™ Platform: Greater Than The Sum Of Its Parts










Traditionally, the “external attack surface” is thought of strictly in terms of an organization’s external IT assets: domains, subdomains, IP addresses, SSL certificates, externally-visible software and services, etc.

While this heuristic is useful, we all know that, in reality, the attack surface does not start and stop with an organization’s IT assets. An organization must also protect brands, trademarks, and sensitive data.

Because an organization must protect its brands from abuse and impersonation– such as phishing sites, fraudulent social media profiles, and malicious applications– these assets must also be considered part of the attack surface. This is where digital risk protection services come into play. After incorporating threat intelligence, the next step in the progression of EASM solutions will be to bring digital risk protection services into the fold.

The Cyberint Argos platform natively combines all three capabilities: threat intelligence, external attack surface management, and digital risk protection services. By providing all of this functionality in a single powerful platform, Cyberint gives customers visibility on every kind of external risk relevant to the organization’s infrastructure, data, and brands.

The fusion of these 3 capabilities provides complete coverage for an array of use cases, making it a simple, easy-to-use platform that is greater than the sum of its parts.

 <b>Data Leakages</b>	 <b>Brand Abuse</b>	 <b>Shadow IT</b>
 <b>Malware Infections</b>	 <b>Phishing</b>	 <b>Misconfigurations</b>
 <b>Dark Web Chatter</b>	 <b>Social Media Impersonation</b>	 <b>High-Risk CVEs</b>

# Why Customers Choose Argos™

---



“Because we’re a small team, the Cyberint analysts are like an extension of us, which really helps from a risk management standpoint.”

Evans Duvall, Cyber Security Engineer, Terex

[Read more in the customer case study.](#)



“We realized that Cyberint was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web.”

Benjamin Bachmann, Head of Group Information Security, Ströer

[Read more in the customer case study.](#)

## About Cyberint

Cyberint’s impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.