CybelAngel

External Attack Surface Guide:

Maximize protection, minimize costs

CONTENTS

UP YOUR GAME.
Downsize your toolstack.

CybelAngel, the broadest External Attack Surface suite

In the current sluggish economic environment, large enterprises are under pressure to reduce costs and streamline operations.

> In a recent Gartner Survey it showed that **75% of organizations are pursuing security vendor consolidation** up from 29% in 2020.*

CybelAngel is a comprehensive cybersecurity solution that enables companies to eliminate overlapping vendors and save money, whilst benefiting from both best-of-suite and best-of-breed External Attack Surface Management capabilities.

In this ebook, you'll find relevant information to help you with the following questions:

1. What should you be looking at when building and optimizing your External Attack Surface Management tool stack.
2. How CybelAngel is a relevant option for a stand-alone solution covering every relevant EASM use case.
3. Finally, what are the benefits you can expect by switching from a multi-vendor to a single pane-of-glass approach, including cost savings and efficiency.

REQUEST A DEMO

*Source: https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022

External Attack Surface Management
Scope and challenges

> In today's digital landscape, protecting your external attack surface has become more critical than ever.

External attack surface management (EASM) encompasses a combination of processes and technology aimed at safeguarding any digital or "smart" technology that connects to the internet. This includes interconnected assets like mobile apps, IoT devices, hybrid cloud infrastructure, websites, operational technologies, and even BYOD devices.

In our latest study, we have detected over 70 billion exposed files containing corporate secrets and personal information, accessible on the web without authentication. With over 800,000 leaking databases, the significance of proper configuration cannot be overstated. We also observed a rise in ransomware attacks, with 116,000 ransomed servers identified.

These statistics are just to name a few and **highlight the amount of risks organizations face everyday.**

Our latest study detected

70 BILLION
exposed files

800,000+
leaking databases

116,000
ransomed servers identified

The goal of EASM is to actively and continually **identify and address publicly-facing assets or exposed data** that could potentially allow unauthorized access to your business-critical digital systems.

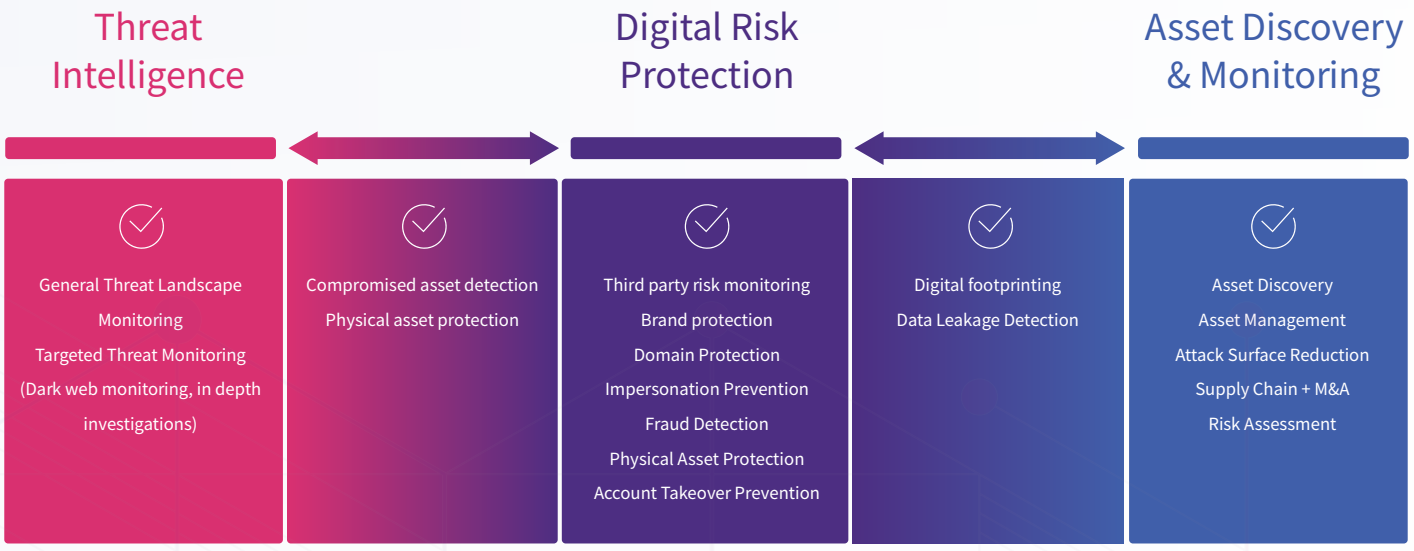
Our definition of EASM is to cover 3 pillars:

Asset Discovery & Monitoring

Digital Risk Protection

Threat Intelligence

The usual response is most of the time to be equipped with a multitude of tools to cover all risks and potential use cases. It makes sense but also poses its own set of problems. Multiple vendors also means multiple onboarding, potential overlapping, technical complexity and often a loss of efficiency. **What if you could have just one?**



One-stop-shop platform to cover all External Attack Surface Management use cases.

CybelAngel has been recognized by Forrester as the only solution able to efficiently cover all of these use cases.

Providers	Physical asset protection	Brand and domain reputation or impersonation protection	Attack surface discovery and management	Fraud and counterfeit detection	Third party risk monitoring
Accenture					●
Claroty			●		
CybelAngel	●	●	●	●	●
Cybersixgill		●			
Everbridge	●	●			●
Flashpoint	●	●		●	
Forntinet		●	●		
Google			●		
IBM			●		
LookingGlass Cyber			●		
NSFOCUS			●		●
QI-ANXIN			●		
Rapid7		●	●		●

Asset Discovery & Monitoring

What is Asset Discovery Monitoring?

Asset discovery and monitoring allows you to i**dentify and manage risks associated with your internet-facing assets and systems**, like unsanctioned employee devices, Shadow IT, old marketing website, forgotten cloud instance.

CybelAngel's Asset Discovery & Monitoring platform helps :

Having full visibility on your external-facing assets :

One of the major challenges faced by organizations implementing Asset Discovery Monitoring is to get only a partial view of publicly facing assets. CybelAngel technology offers the **most exhaustive inventory** in the industry, to make sure you find all your shadow IT. Our innovative approach detects unknown assets through two effective methods. Firstly, we employ **keyword-matching across diverse sources**, including banners and SSL certificates, ensuring comprehensive coverage. Secondly, we excel at **pivoting from known assets to unveil interconnected unknown assets**, uncovering hidden risks.

Focusing your team through asset prioritization for remediation:

All Incidents are first scanned for threats related to open ports, and vulnerabilities, and rated based on the severity of the exposure. CybelAngel leverages **severity scores, as well as analyst expertise** - an augmented intelligence approach - to cater reports to business risk specific to customers.

Acting fast to secure assets

before bad actors get through daily monitoring (getting alerted when a new thread emerges), **Asset detail** (uncover details including IP address, threat level, registrar, related assets and more to decide on the best remediation next steps), **Automate your workflows** (updating your CMDB and boost VM programs through API integration)

Digital Risk Protection

What is Digital Risk Protection System?

A critical component in safeguarding an organization's digital activities against the growing threats in today's interconnected landscape, like account takeover, typosquatting, hacktivism, phishing, data leakage and more.

CybelAngel's DRPS offers a full coverage to prevent digital risks :

Data Breach Prevention:
Monitor, detect, and secure publicly-accessible sensitive data before they are breached.

Domain protection:
Monitor, detect, and take down malicious domains to keep your brand secure

Account takeover prevention:
Monitor and detect critical credentials leaks before they are compromised.

One of the primary challenges faced in digital risk protection is the ability to translate alerts into meaningful actions, CybelAngel helps you stay efficient managing only true positives.

"With the triage work done by CybelAngel analysts, we have a very low false positive rate and are only alerted on what really matters, so that our SOC team can respond quickly to any possible exposure."

Olivier Thonnard,
Director of Global Security Operations at Amadeus

Threat Intelligence Contextualization

What is Threat Intelligence?

Threat Intelligence can and should give an organization a comprehensive view of the threat landscape you are challenged with. Cyber Threat Intelligence can help understand the **attack surface from a digital and physical view.**

The entire CybelAngel External Attack Surface Management suite can give strategic, tactical and operational intelligence on threats. This allows companies to prioritize based on risk, understand gaps, and be proactive versus reactive.

If your TI program is focused on the dark web only, you are missing the visibility on the majority of your attack surface.

CybelAngel's Threat Intelligence approach consists of:

Threat Intelligence Contextualization

CybelAngel detects **335,000 Deep & Dark Web posts every day** and tracks activities across social networks, criminal environments, forums, messaging apps, and specific channels like Twitter, Facebook, Reddit, and more.

Relying on Cybercrime experts

Our Research and Analysis of Cyber Threats team (REACT) is composed of **cybercrime experts** working on advanced threat intelligence reports, investigations, and answering to customers' enquiries related to Dark Web activities and Threat actors.

How many vendors are you currently using to cover all of these use cases?

By having a platform solution that covers a wide range of cybersecurity needs, large enterprises can remove some overlapping or less efficient vendors. This streamlining of vendors allows them to save money and maintain a more effective security program.

Choosing CybelAngel helps you decrease your Total Cost of Ownership by:

- Simplifying administrative overhead
- Facilitating integration and setup.
- Reduce SOC team fatigue.

The benefits of having one single suite

Reduce administrative overhead:

On top of the technical validation, implementing a contract with a vendor takes a lot of time specifically when managing sensitive information. As a buyer, you may ask a detailed list of questions and requirements that you need to audit for each of the vendors you are working with.

CybelAngel works with some of the worlds best MSSP's. Speed up procurement by going through your local MSSP.

Working with multiple vendors means multiple contacts and multiple touch points, which can be time consuming. At CybelAngel, your customer success manager is your **unique touchpoint** that you can contact when you have any questions or when setting up recurring Executive Business Reviews. No tedious ticketing system, you have a question, just ask your CSM.

Facilitating integration and setup:

One tool equals one set up which is particularly easy at CybelAngel. As a SaaS platform that covers the full EASM Value chain, you set up and maintain a unique list of keywords.

Also thanks to CybelAgel's APIs, off-the-shelf connectors, no-code automation, and solutions architects available at your fingertips, **100's of integrations are available through CybelAngel's** Connect Studio. You can seamlessly Integrate with SIEM, TI, and SOAR tools and facilitate collaboration processes.

Reduce SOC team fatigue:

Thanks to CybelAngel Machine Learning Models, only pre-investigated and verified security issues reach your SOC team.

We provide one unique format of contextualized incident reports with confirmed attribution, tailored to your specific requirements.

Moreover, CybelAngel's **analysts are dedicated experts who already know your organization and your challenges better than anyone**. With their expertise, they discarded a staggering 7.5 million alerts in 2022, ensuring only the most relevant and actionable information reaches you to avoid any alert fatigue.

REQUEST YOUR CUSTOM DEMO NOW