Brought to you by Informa Tech
OMDIA

Publication date:
30 Sep 2022
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: Cyberpion offers a platform to reduce external attack surfaces

Summary

Catalyst

Cyberpion is a provider of external attack surface management (EASM) technology, which aims to reduce an organization's exposure to any cyber threats on the internet, including the ability to reduce risk automatically. This can range from web applications, mail servers, cloud, and other internet-facing assets, belonging to the organization itself and to those of its business partners, as well as supply chain relationships, kill chains, unowned and uncontrolled assets. Cyberpion delivers its technology in software-as-a-service (SaaS) mode.

Omdia view

EASM is definitely on a lot of enterprises' minds at the moment, as they feel the need to regain control of their internet-facing assets (i.e., enforce security policies on them). There are a large number of vendors offering technology to do so, and part of the challenge faced by Cyberpion is to establish its name in this market, with a differentiated profile for what it offers vis-à-vis the competition.

This is particularly the case with regard to the likes of Palo Alto Networks, Microsoft, IBM, and Tenable, all of whom have acquired vendors in this segment and have considerably deeper pockets when it comes to marketing their wares.

That said, Omdia sees Cyberpion as well placed to carve out a share of this expanding market, given the breadth of its current offering and its plans for where it needs to take its technology next.

Why put Cyberpion on your radar?

Cyberpion offers a platform providing comprehensive external attack surface management for internet-facing assets including web applications, SaaS services, cloud, networks, infrastructure, and more. It will also be expanding its platform into API attack surface in 2023, giving customers an opportunity to influence its technology roadmap.

Market context

While cybersecurity technology develops in multiple directions, Omdia identifies three broad eras characterized by different approaches to threats. First was the preventative era, where antivirus (AV) vendors waited for a "patient zero" to be infected, then quickly developed a "signature" for the virus, distributing it to all their customers so that their instance of the AV software would recognize it and block it from entering their infrastructure.

That approach worked well for a couple of decades, but as the threat landscape mushroomed through the end of the millennium, the AV industry struggled to keep up, and the efficacy of signatures waned. By the end of the first decade of this century, there was a need for a new approach, which was when the reactive era began, in which a breach was assumed, and the focus turned to detecting and responding to the threat as quickly as possible. Starting endpoint with endpoint detection and response (EDR), the approach soon expanded to networks (NDR) and beyond, leading to the evolution of extended detection and response platforms, or XDR. The idea here is for individual silos of security technology from endpoint, network, cloud, email, and beyond to feed telemetry to a common XDR "brain" in the back end (typically a data lake where machine learning algorithms can perform analytics). Decisions are then taken on remedial action and instructions are sent back to the individual silos for enforcement.

The reactive approach held sway for much of the last decade, but in the last couple of years Omdia has detected the rise of a series of technologies that embody a third "wave" of cybersecurity, in what we are calling the proactive era. These are platforms that seek to identify issues (vulnerabilities, misconfigurations, excessive access rights, etc.) and address them before any attack has taken place, thereby reducing the workload of the reactive technologies that are still essential in any security arsenal.

Unlike XDR for the reactive world, there is currently no single initialism or acronym for proactive security. The spectrum of proactive technologies range from

- traditional ones that have enjoyed a new lease of life, such as vulnerability and patch management, through
- breach and attack simulation (BAS, aka incident simulation and testing, or IST),
- cloud-specific platforms such as cloud security posture management (CSPM),
- SaaS security posture management (SSPM),
- and cloud permissions management (CPM, aka cloud infrastructure entitlement management, or CIEM), to attack surface management (ASM).

EASM is a subset of ASM, in that it deals only with the external attack surface, defined as the sum of the assets that are accessible on the public internet. These are initially assets belonging to the organization itself (e.g., network devices and services, web applications, and mobile apps) that the development or marketing

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

team have delivered as part of an ongoing project. However, they can extend to the internet assets of its partners and suppliers, which can serve as an on-ramp for an attack on the organization itself.

The core capabilities of an EASM platform are:

- Asset Discovery
- Vulnerability Assessment
- Prioritization by risk
- Actions for Remediation

It is also imperative that all these activities are performed on a continuous basis, given the dynamic nature of organizations' external attack surface in the era of cloudified application infrastructures and working-from-anywhere, new developed apps and services, consumption of SaaS and even mergers and acquisition rate.

It is worth pointing out here that the exact definitions in the ASM space are still in flux. Omdia tends to think of EASM as one dimension and a subset, with the other being the rather hazy cyber asset ASM (CAASM). Cyberpion on the other hand asserts that EASM is in fact a superset of ASM, or at least will trend to become so in the longer term.

Whether or not that comes to pass, it is certainly the case that EASM has gained a higher profile of late, with considerable M&A activity as more vendors seek to move into the market. The reason for this is that there is scarcely a business activity today that doesn't change the external attack surface in some way, making EASM increasingly critical to every organization.

Product/service overview

The key benefit of an EASM platform is that it should enable an organization to visualize its external attack surface as a threat actor would and thereby also to take remedial action, prioritizing the most important changes that need to be made to bolster its defenses.

The Cyberpion Platform is entirely non-intrusive, in that it takes a customer's primary domain name, which is where its scanning will start, from its email address. From there, its discovery engine uses machine learning and data science technologies to discover:

- all the relevant subdomains under that domain
- IP addresses and IP blocks
- third-party connections to it through supply chain and other business relationships
- Web applications, mail servers, cloud infrastructure, DNS, PKI
- so-called dangling DNS, which is where a DNS record points to a resource that isn't available, such that the record itself should have been removed from an organization's DNS zone, failure to do so resulting in the possibility of subdomain takeover and
- for broader context, it continually maps the internet itself to understand the threat landscape.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Cyberpion begins its discovery process with the customer's main domain. It uses multiple techniques to identify assets, including:

- mapping DNS and web connections,
- cloud and internet indexing, and
- public data sources.

In this process it identifies subsidiaries and brands. For each one it identifies all domains and subdomains, IP addresses and IP blocks, and managed domains. Discovery extends beyond internet-facing assets to the connected digital supply chains the customer organization depends on (Cyberpion tends to use the term "hyper-connected" to underscore the degree of interconnectedness the world has reached by now).

This process enables Cyberpion to maximize coverage and reduce false positives. The vendor argues that its approach is fundamentally different from generic scan technologies such as Shodan (a freemium search engine for internet-connected devices) because they face the hard attribution task of determining who an asset belongs to from an endless list of possibilities. By contrast, Cyberpion's machine learning discovery has to determine whether an asset belongs to its customer, with a yes/no answer. It uses machine learning asset models to reach this conclusion.

These activities enable Cyberpion to build a complete external-facing asset inventory for the customer, or as the vendor refers to it, an outside-in view of an organization's public-facing digital footprint. Once it has that inventory, the Platform's vulnerability assessment engine considers not only the type of asset, but also its importance and how it is connected to the organization.

Utilizing a proprietary multi-layered assessment approach, vulnerabilities are examined for the risk they present as well as their exploitability. The vendor argues that this not only reduces false positives but provides the customer with insights into which vulnerabilities are the greatest threat and should be prioritized immediately.

Beyond that, the Platform provides the customer's security team with suggested steps to mitigate or remediate vulnerabilities via Active Protection, which is a growing set of technologies and techniques that enable it to remediate issues and break kill chains for customers.

Company information

Background

Cyberpion was founded in 2016 by CEO Nethanel Gelernter, Chief Business Officer Ran Nahmias, and Chief Engineer and VP of R&D, Ori Engelberg. Gelernter has a Phd in computer science and cybersecurity, and was previously a university professor, as well as working as a security researcher at ethical hacking company KayHut and earlier in his career, a software engineer at Microsoft. Nahmias held various executive roles at security heavyweight Check Point. Meanwhile Engelberg was previously a researcher at Bar-Ilan University.

The vendor has raised a total of $35.3m in venture funding, most recently announcing a $27m Series A round in March 2022, led by U.S. Venture Partners, with participation from existing investors Team8 Capital and Hyperwise Ventures.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Current position

The Cyberpion Platform is a SaaS offering that is charged for as an annual subscription, with the size of the subscription calculated on a per-tracked asset basis. Approximately half of Cyberpion's customers are from outside North America.

Cyberpion adopts a channel-first approach for its go-to-market strategy and currently has a couple of dozen channel partners signed up, in the form of VARs and MSSPs.

The ASM market is a busy one, particularly its EASM segment, with multiple vendors large and small. Two of the most significant competitors that Cyberpion sees with great frequency are Palo Alto Networks (the result of its 2020 acquisition of ASM specialist Expanse) and Microsoft (since it bought RiskIQ in July 2021. There is considerable ongoing M&A activity in this market, as larger cybersecurity players buy dedicated start-ups to add EASM to their portfolios.

Future plans

On Cyberpion's roadmap for 2023 is the extension of its discovery capabilities from the applications to APIs, enabling the Cyberpion Platform to discover key assets such as active, zombie, and shadow APIs that are mismanaged and can expose sensitive data to the public internet, a common occurrence that can have serious consequences.

While its current technology is agentless, requiring zero deployment of any componentry on the customer's infrastructure, the vendor anticipates that the extension of its capabilities to the cloud in order to discover and inventory shadow IT assets residing there will require at least read-only access rights to be granted.

Key facts

Table 1: Data sheet: Cyberpion

Product/Service name	Cyberpion Platform	**Product classification**	External attack surface management (EASM)
Version number	N/A	**Release date**	2019
Industries covered	Financial, Insurance, Retail, Higher Ed, Critical Infrastructure, Media, Telco	**Geographies covered**	NA, EMEA
Relevant company sizes	Primarily Enterprise, some midsize	**Licensing options**	SaaS pricing, based on number of assets
URL	https://www.cyberpion.com	**Routes to market**	Channel-first model including MSSP's
Company headquarters	San Mateo, CA	**Number of employees**	60

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Source: Omdia

Analyst comment

ASM generally, and EASM in particular, has enjoyed a considerable increase in its profile within the broader cyber market over the last couple of years, in part thanks to the impact on the world of work of the coronavirus pandemic. Essentially, COVID turbocharged existing digital transformation projects as well as fomenting new ones, not only driving millions of knowledge workers into working from home, many of them from the first time, but also accelerating the cloudification of enterprise apps. As Omdia puts it, the pandemic drove digital dominance in the global economy far beyond its previous level.

Thus, the rate at which new corporate assets find their way onto the Web has increased apace, with decreased central control by IT. Marketing teams, developers, and other business units now stand up new websites and webpages rapidly, often unbeknown to their IT departments, which obviously represents a challenge from a security perspective.

The first hurdle in bringing so much shadow IT within the purview of the corporate IT and security teams is, of course, establishing visibility into what internet-facing infrastructure the organization actually has in place at any moment. And of course, shadow IT is just one of the problems addressed by EASM. As Cyberpion argues, every business activity, shadow or not, alters, changes, or otherwise expands the enterprise attack surface in unseen, uncontrolled and unpredictable ways. Hence the importance of discovery as the first task of any EASM platform.

Beyond that, customers need prioritization of the findings of the discovery process, with an analytics engine considering the criticality of the issues the platform has identified, and armed with the prioritized list, making recommendations for how those issues can be addressed.

Cyberpion performs all these functions and so is well placed to grow its customer base and market presence, provided it can make its voice heard over noisier competitors with larger marketing budgets.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com