Brought to you by Informa Tech

Publication date:
11 Jan 2024
Author(s):
Rik Turner, Senior Principal Analyst

On the Radar: Censys vertically integrates search and EASM

Summary

Catalyst

Censys offers a search engine for gathering internet intelligence and an external security posture management (EASM) platform, with both of them delivered in software-as-a-service (SaaS) mode. This report focuses on the vendor's EASM offering, called Exposure Management, recognizing that its vertical integration with Censys Search provides differentiation within its market space.

Omdia view

Organizations have seen their external attack surface (i.e., the range of internet-facing assets they own that are susceptible to a cyberattack) expand dramatically in recent years. This is partly the result of increased reliance on digital channels for customer and employee interaction, itself a trend that was supercharged by the recent pandemic. However, the problem is compounded by the rate at which new assets are created in the modern development environment.

EASM is a technology that has arisen to address this situation, offering the ability to discover the full extent of an organization's public-facing digital assets, marry that data with information about the current threat landscape, prioritize any issues detected by their severity, and then suggest remediations. And given the dynamic nature of modern asset creation, discovery must be carried out on an ongoing basis via monitoring of the infrastructure.

The market opportunity for EASM generally is shown by the interest of larger cybersecurity vendors in entering this market, expressed via their readiness to acquire dedicated startups in the space since the beginning of this decade. Censys's opportunity in particular is to highlight the advantages of its vertically

integrated offering, in which highly detailed and accurate scan data power sophisticated asset discovery and risk assessment within the same platform, enabling faster refresh times and more visibility across ports, services, and IP addresses discovered.

Why put Censys on your radar?

Censys's ability to gather and contextualize exposures across the entire internet, combined with logic to assemble a complete inventory of an organization's public-facing digital assets that is itself continuously updated, differentiates its offering from other EASM vendors and makes it worth considering by any enterprise looking to address a burgeoning attack surface.

Market context

As digital transformation has gone into overdrive, so new web pages, versions of applications, and data stores are thrown up at an ever more vertiginous pace, often for test and development purposes or as "trial balloons" for the marketing department to play around with a new concept as it crafts a new campaign. These assets are frequently left abandoned or, as the term of art goes, orphaned once the team behind them has moved on to something else, which in turn expands the attack surface of the organization to which they belong. To quote Censys here, "the cloud has enabled employees outside of traditional IT groups easily to stand up public-facing servers and transfer sensitive data to externally managed providers." Teams can thus become more innovative and agile, but the process also creates blind spots for security teams.

Attack surface management (ASM) is one of the principal manifestations of the proactive wave of security approaches in the market today. The ethos of proactive security is to inspect some aspect of an organization's IT infrastructure, discovering all the assets within that domain, and determining which of them is susceptible to cyberattack. The next step is for the ASM platform to prioritize which of these issues are the most critical, recommend the remedial steps to address them, and, where permitted by the customer, even carry out the remediation in an automated fashion.

The ASM sector falls into two subgroups, which are:

- **Cyber asset attack surface management (CAASM):** This is a somewhat unwieldy term for technology that provides asset visibility, primarily via API integration with existing tools, enabling them to query the consolidated data it brings together, identify the scope of vulnerabilities and gaps in security controls, and remediate issues. It can be thought of as an evolution of traditional asset management technology, specifically designed to address the challenge of security issues within an organization's infrastructure. As such, it relies on permissions to access all the extant asset information in the relevant places, such as change management databases (CMDBs).
- **External attack surface management (EASM)**: This, on the other hand, relies on no such permissions to deliver the continuous discovery, monitoring, evaluation, prioritization, and remediation of attack vectors within an organization's external attack surface, which can be defined as all and any internet-facing assets. Since those assets are all public facing, they can be discovered without reference to any existing repositories of asset data.

Omdia has recently detected some imprecision in the market in terms of the way each side of the divide refers to itself. In particular, vendors in the CAASM space (which Omdia has often felt tempted to call simply "internal" attack surface management) nowadays like to claim the ability to provide a complete inventory of

a customer's assets, both internal **and** external. They explain that the integrations and collaborations they maintain with EASM specialists, meanwhile, are driven by a desire to gather additional external attack surface data for an even more comprehensive view, but insist that they can in fact do without those third-party contributions.

Omdia has its doubts. Indeed, we have often mused about the desirability of an eventual fusion of the two market segments. This would enable the vendors bringing these capabilities together in a single platform to provide a full-service offering. They would also be able to refer to it simply as ASM, which would be a non-trivial advantage in a sector that is awash with acronyms and initialisms.

Product/service overview

The Censys Internet Map represents the ground truth internet intelligence that powers Censys and is the foundation of what Censys delivers to its customers. Its proprietary scanning engine scans the internet to gather and correlate information on the current threat landscape. The company's Exposure Management platform integrates vertically with Censys Search, using the same internet scan data and refining it to a subset that represents an organization's public-facing digital assets.

Like all EASM products, Exposure Management starts with the discovery of an organization's entire estate of internet-facing assets. It then uses the internet intelligence provided by Censys Search to identify critical exposures, assigning them severity scores to enable the customer to mitigate the most serious risks, using around 300 risk "fingerprints" to assess severity and determine priorities. This is a differentiator for Censys in the EASM market, where most of its competitors use third-party scan data for this purpose.

Beyond the initial discovery process, the platform continues to scan for changes both to the customer's infrastructure (i.e., new assets and vulnerabilities) and to the threat landscape, providing daily coverage across the organization's known and unknown attack surfaces.

Rapid Response and integrations

Censys also offers Rapid Response programs for customers, whereby it undertakes to prioritize and communicate emergency vulnerabilities to its security team within 24 hours of disclosure via the platform's web interface.

In addition to its own dashboard and reporting capabilities, it has API-based integration vulnerability management tools Qualys and Tenable, as well as the likes of ServiceNow for ITSM and Splunk's SIEM platform, all designed to streamline a customer's response activities.

Adding a GenAI tool for ASM and threat hunting

Generative AI (GenAI) penetrated the popular consciousness in 2023, thanks to OpenAI's launch of the ChatGPT facility giving all and sundry the opportunity to experiment with the technology. The world of cybersecurity, and particularly the SecOps domain, is feeling the impact, with Microsoft being just one of many vendors launching capabilities in this area, with its Security Copilot offering.

Aware of this trend, at the end of the year, Censys announced a beta program for an AI-based capability called CensysGPT. As its name suggests, this tool leverages GPT large language models to help customers build queries, enhancing their ability to conduct cyber reconnaissance operations. The GenAI tool is designed to speed users' paths to insights into hosts or certificates on the internet, streamlining the process and allowing for more proactive threat hunting and exposure management. It does this by making suggestions for queries to be typed into the Exposure Management platform, such as:

- Russian hosts running RDP or FTP
- Services in Brazil with the html title “Index of /”.

Company information

Background

Censys was founded in 2017 by Chief Scientist Zakir Durumeric and a group who had met in academia. The company’s platform evolved from ZMap, an internet scanner created by Durumeric during his PhD studies at the University of Michigan.

The first product to go on general availability in 2017 was **Censys Search**, which is itself an evolution of ZMap and is still available as a standalone capability. Its core premise is that the entire internet can be scanned, providing a source of extensive information about advanced threat actors.

This also led to the development of a second product, **Exposure Management**, which is Censys’s EASM product. Becoming generally available in 2019, Exposure Management is where the threat landscape data from Search is correlated with information about a customer’s exposed assets, and severity scores are assigned to help prioritize remedial actions.

Censys has raised a total of $128.1m in funding, most recently announcing a $50m Series C round in October 2023, led by Decibel Partners, GV, Greylock, and Intel Capital, with new investors Ascension Ventures, Four Rivers, and accounts managed by Hamilton Lane. It also unveiled $25m in debt funding, led by SVB Capital, Silicon Valley Bank, a division of First Citizens Bank.

Current position

Censys offers both its products in a series of pricing tiers:

- Community is a free product for single users to get acquainted with the technology, enabling them to carry out 250 monthly queries delivering up to 10 pages of results. From there they graduate to:
- Solo, which costs either $69 a month or $745 a year, with 500 monthly queries, 25 pages of results, and additional features such as basic support.
- Teams is a subscription for up to five users that costs $499 a month, with an allowance of 3,750 monthly queries and 50 pages of results. A significant additional feature here is SSO and SAML support.
- Pro is for groups of 10 or more people, with 25,000 monthly queries, one month of historical data, and unlimited pages of results.
- Advanced tier offers organizations 150,000 monthly queries with up to six months of historical scan data and unlimited pages of results.
- Premium is available for organizations that benefit from large quantities of monthly queries and need up to a year of history to track threat actor changes.

The last three tiers are collectively referred to as the enterprise packages and, in the context of the EASM platform, require a meeting with the sales team to determine bespoke pricing, based on several factors, the main one being the size of the attack surface.

The pricing model for Search is based on the number of queries carried out and results delivered, going up in tranches as shown above. Meanwhile, for Exposure Management, the vendor charges a subscription based on the number of assets under management, meaning the number of IP addresses, hosts, web entities, domains, or internet-facing apps it discovers and then monitors on an ongoing basis.

Censys says it already has around 312,000 individual users for its commercial products, of whom 12,000–15,000 are active each month. Its customer base includes over 50% of the Fortune 500, and it adds that many tech vendors that are classified as its competitors in EASM, such as Mandiant, Microsoft, CrowdStrike, and Recorded Future, are also customers. Furthermore, a number of major banks use Exposure Management in combination with competing EASM platforms.

In terms of its broader competitive landscape, Censys sees its closest competitor on the Search side as Shodan, which also has a freemium approach and tiered pricing models up to Corporate level. Meanwhile, in EASM, there are of course the heavyweights that have moved into the space via M&A, but the vendor it sees most frequently is EASM startup CyCognito.

Future plans

Censys is already in the threat hunting and EASM markets with its current products, and it will continue to invest in its offerings to increase their appeal to those market segments.

The current free version of Search is set for enhancements in 2024, positioning it as a platform for teams of all sizes, as well as beefing up its threat hunting credentials, with a view to helping customers use Censys more effectively. The technology already covers machine learning-based discovery of services across all the possible 65,535 TCP port numbers, the entire IPv4 namespace, and is expanding its coverage of IPv6.

Key facts

Table 1: Data sheet: Censys

Product/service name	1) Censys Search 2) Exposure Management	**Product classification**	Internet search EASM
Version number	n/a (entirely SaaS)	**Release date**	1) 2017 2) 2019
Industries covered	All	**Geographies covered**	North America South America Western Europe Japan Australia and New Zealand
Relevant company sizes	Enterprises (typically, companies with a security operations center and threat hunting capabilities) and government agencies	**Licensing options**	Monthly or annual subscriptions, based on: 1) Number of queries and results 2) Assets under management
URL	https://censys.com/	**Routes to market**	1) Direct 2) Channel partners
Company headquarters	Ann Arbor, Michigan, US	**Number of employees**	140

Source: Omdia

Analyst comment

The fact that Censys comes from a background in search technology for gathering internet intelligence, and that it continues to offer a commercial product in that area, gives it a couple of clear differentiators vis-à-vis its competitors in EASM.

From an operational perspective, its search gives it a depth of information on which the EASM platform can draw for the purpose of assessing the size and gravity of a customer's attack surface. By contrast, other EASM vendors can discover their customers' assets, but rely on open source intelligence and/or commercial threat intel feeds to gauge the severity of the issues they have found within an organization's public-facing digital estate. This inevitably slows the refresh rate of that intel.

Meanwhile, on a commercial level, Censys continues to compete in the internet scanning market, which provides it with a revenue source separate from its efforts in EASM, affording it the time to perfect its technology offering in that segment free from the pressure of immediate profitability there.

The challenges the vendor faces in EASM, meanwhile, stem from the flurry of M&A activity in the sector over the last few years, meaning there are a number of major names or tech heavyweights already in the space.

The landgrab started in 2020, when Palo Alto Networks acquired EASM specialist Expanse. The following year, Mandiant (then part of FireEye but now owned by Google) bought Intrigue and Microsoft bought RiskIQ. Since then, they have been joined in the fray by:

- IBM (who bought Randori)
- CrowdStrike (Reposify)
- Tenable (Bit Discovery)
- Recorded Future (SecurityTrails)
- Darktrace (Cybersprint).

All of these M&A deals happened in 2022, and the buyers are all companies with deep pockets to mount marketing campaigns and spread awareness of their EASM capabilities.

As such, it behooves Censys to raise its own profile in this market, alerting potential customers not only to its presence but also its technical differentiation, and how this can be beneficial for the management of their security posture.

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.

Further reading

Identity attack surface management (IASM) edges into cyber parlance (January 2024)

Fundamentals of Proactive Security (September 2023)

On the Radar: Axonius offers cyber asset attack and SaaS management with a common data model (July 2023)

On the Radar: JupiterOne delivers CAASM and continuous compliance from a single platform (June 2023)

On the Radar: IONIX offers a platform to reduce external attack surfaces (September 2022)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

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