Publication date:
07 Feb 2025
Author(s):
Rik Turner, Senior Principal Analyst

On the Radar: runZero offers an expanding portfolio in exposure management

Summary

Catalyst

runZero is a provider of cyber asset attack surface management (CAASM) technology that is adding functionality to enable a broader offering in attack surface management (ASM) and, ultimately, fully fledged exposure management.

Omdia view

Proactive security approaches have been on the increase since the late 2010s, which is exactly when runZero came into existence. The rationale is that, as the threat landscape has continued to expand and the shortage of skilled security professionals shows no signs of diminishing, the logical way to address the situation is to get out in front of attacks, finding and fixing issues before they are exploited.

CAASM is the more "thorough" side of ASM, so much so that Omdia expects the somewhat easier task of external ASM (EASM; see below) to be subsumed into it over time. Of course, the still broader segment of exposure management is now opening up. Omdia sees runZero as playing a significant role in this emerging market, not least because it goes beyond integration with existing data repositories within the customer's environment, collecting, correlating, analyzing, and prioritizing its own data, as provided by its Explorer scanning engine.

Why put runZero on your radar?

While it started out in the most complex side of ASM, namely the CAASM market, runZero is already expanding into EASM and, over time, its vision is to become a fully fledged exposure management provider. Omdia sees its CAASM backgrounder as being the most solid foundation for such a move, making the vendor a worthwhile candidate for any ASM or exposure management project within an organization.

Market context

ASM is a branch of proactive security; that is, technology that sets out to find issues within an organization's IT infrastructure and address them prior to them being exploited by any threat actor. These issues range from vulnerabilities and misconfigurations and excessive access rights to weak access controls, and so on.

EASM and CAASM

ASM has two subgroups, each with names coined by an analyst firm other than Omdia. They are:

- External attack surface management (EASM), which discovers all the public-facing assets an organization has on the internet, including websites and pages, and S3 buckets, assesses their security posture and provides its security team with visibility into that estate. It also offers recommendations for how to reduce its attack surface; for example, by disactivating some assets or taking others off the public internet. It prioritizes them by their reachability and the criticality of the data processed by, or residing in, them.
- Cyber asset attack surface management (CAASM), which is a rather clumsy denomination for a class of tool that discovers an organization's internal assets, assesses their security posture, and suggests how it might be improved, again with prioritization of the most critical issues.

It would have been better for the analyst firm in question to call this type of technology internal ASM, or IASM, as the comparison between the two would have been more readily understandable. However, some pundits argue that the IASM moniker would have been a misnomer, since it does have some external asset discovery capabilities.

In any case, CAASM is arguably the more demanding of the two fields because, while EASM requires no permissions from the customer to find and identify their internet-facing assets, CAASM must have access rights to, and integrate with, internal systems such as change management databases (CMDBs) and security information and event management (SIEM) platforms to do its job. This frequently entails the CAASM platform being issued credentials for access (although this is not a requirement in runZero's case).

Furthermore, Omdia has long thought that a desirable development would be for the two fields to merge for a single, comprehensive ASM offering, and in this context, we consider runZero's moves to expand its external discovery capabilities both logical and laudable.

Exposure management

To add a further dimension here, an additional market category has emerged in the last couple of years – namely exposure management – which is a still broader umbrella term encompassing even more subgroups. It is applied not only to CAASM and EASM products, but also to:

- Vulnerability management products, and particularly the more risk-based variant, RBVM
- Breach and attack simulation (BAS) tools.

One could even make the argument for the inclusion, within this catch-all term, of the security posture management (SPM) spectrum of technologies, which are applied primarily to cloud environments (e.g., CSPM, SSPM, and DSPM).

Exposure management is clearly the direction in which runZero is headed and, in this context, its CAASM heritage should stand it in good stead in what is proving to be an increasingly crowded space.

Product/service overview

The runZero Platform operates in an agentless fashion and, unusually for the CAASM space, without credentials. It also requires no physical or virtual appliances to be deployed within the customer's infrastructure.

It works by deploying a lightweight scan engine known as a runZero Explorer in each network segment to be monitored within an organization's IT environment. The runZero Platform integrates with any existing CMDBs, endpoint detection and response (EDR), and vulnerability management tools running within the infrastructure, enabling it to collect data from them, but crucially it performs its own active scanning for both network and asset discovery. It carries out this scan of both IT and OT systems within the customer environment, allegedly without any hit to the performance of their infrastructure.

runZero attributes this ability to its approach of deploying incremental probes that enable it to develop comprehensive fingerprints of the systems monitored, analyzing each device against a library of around 800 attributes. Its objective is to gain a deep understanding of the assets in the environment and detect the potential for any zero-day attacks.

Rapid response and ongoing exposure identification

The platform also has a feature called runZero Rapid Response, which helps users identify and respond to emerging threats to their network, as well as the presence of noncompliant systems in the environment. This includes unpatched and end-of-life software no longer supported by its supplier, plus endpoints that are not running the customer's preferred EDR technology. runZero provides:

- Pre-built queries that users can run to pinpoint exposures without rescanning, including native detection for categories of exposures that are beyond the scope of traditional vulnerability scanners
- Outlier analysis, which both analyzes and provides a criticality score for assets that are unique within the network
- Vulnerability data that can be imported, prioritized, and validated, with the possibility of customers creating their own vulnerabilities
- Asset inventory, which can be used in conjunction with vulnerability management tools to find impacted assets
- Fingerprinting to enrich vulnerability scan results with asset and network data.

In order to prioritize issues for remedial action, runZero combines input from the customer themselves (i.e., what they have tagged as critical) with the result of machine learning algorithms it uses to model what constitutes normal behavior and outliers, plus the network context.

Passive scanning

In September 2023 runZero expanded its platform with the addition of a passive data collection capability, explaining that while active scans typically provide better information, passive sampling can be useful on networks where scanning is not permitted, as well as for finding new hosts on a network. The capability was developed primarily to meet the needs of customers with OT infrastructure, where active scanning is not an option for a combination of operational and safety reasons.

While a single Explorer can only operate in active or passive mode at any one time, customers can schedule scan tasks for an Explorer with passive sampling enabled, such that the system will ensure that the scans still run: when the Explorer has no active tasks assigned, it will go back to passive sampling.

Company information

Background

runZero was founded as Rumble Network Discovery in 2018 by its CEO, HD Moore. He is best known as the creator of Metasploit, the open source tool for developing and executing exploit code against a remote target machine, which was acquired by vulnerability management vendor Rapid7 in 2009. His most recent previous role was VP of Research and Development at Atredis Partners, where he spent almost four years and contributed to custom projects that included advanced penetration testing, binary analysis, software development, and applied research. Prior to that, Moore spent six years at Rapid7, where he rose to the rank of Chief Research Officer.

runZero has raised in excess of $50m over three funding rounds. Five months after a $15m Series A round in March 2022, led by Decibel Partners, the company rebranded as runZero.

Current position

The runZero Platform can be delivered in software-as-a-service (SaaS) mode or deployed on the customer's premises. It also supports an air-gapped mode of deployment, which is particularly important for OT environments and governmental entities.

runZero's charging mechanism for its technology is an annual subscription based on a per-asset fee, with discounts as the number of assets moves into higher tiers. The vendor has a wide range of customers paying anywhere between $5,000 and millions of dollars a year. It has no particular target vertical, given that its technology is inherently horizontal in its application, with customers in:

- High tech
- Financial services
- Manufacturing
- Automotive
- Retail

- Higher education
- Telecom
- US federal government.

The one proviso runZero does make is that it is not best suited to companies that are 100% cloud in their infrastructure (i.e., the so-called cloud native or "born in the cloud" companies). However, it does have a number of organizations with hybrid environments.

The vendor currently has approximately 500 paying customers of all different sizes and, since it offered a free Community Edition of the platform from April 2020 (originally called Rumble Starter Edition), it has a further 18,000 users registered there, with the freemium marketing mode affording ample opportunities for upsell.

As for its geographical split, while North America makes up the lion's share of its customer base, runZero says that around 20% of customers are in Europe, as well as a few in Australia and New Zealand. The company launched an international partner program in November 2022 and has operated a data center in Germany since mid-2024 to comply with the data sovereignty requirements of the European Union.

Future plans

Building on its CAASM foundation, runZero has rapidly expanded beyond asset inventory into EASM and is adding new exposure management capabilities on an ongoing basis. runZero already provides visibility into devices across the entire environment – from the cloud to the network core and everything in between. Because the solution does not depend on agents or credentialed scans, runZero secures a significant portion of the attack surface that is often missed by other tools.

Additionally, runZero has recently released new "inside-out" attack surface management features, combining internal and external perspectives to uncover internal assets unintentionally exposed to the public – a unique capability that sets runZero apart from externally focused attack surface management tools.

Looking ahead, runZero is focused on helping organizations prioritize closing the gaps that are most critical. This includes identifying misconfigurations and vulnerabilities that are both likely to be exploited by attackers and put high-value targets at risk.

runZero is also introducing a new top-level paradigm for assessing and remediating risks. This approach highlights exposures that could be exploited in real-world attacks and aggregates related assets, services, or entities into actionable findings. For example, instead of a daunting list of all vulnerabilities, runZero helps teams focus on critical issues such as misconfigured applications that are accessible from the internet, enabling faster, more targeted remediation efforts.

runZero's innovation extends to its fingerprinting capabilities, which now encompass an even broader range of unconventional and vertical-specific equipment, including OT, IoT, and other unmanaged assets increasingly connected to IT infrastructure. This forward-looking approach supports its vision of becoming a complete exposure management platform – empowering organizations to discover exposures across their entire attack surface, prioritize the most critical threats, and close the window on exploitability faster than ever.

Key facts

Table 1: Data sheet: runZero

Product/service name	The runZero Platform	**Product classification**	CAASM/ASM/exposure management
Version number	n/a	**Release date**	October 2019
Industries covered	High tech, financial services, manufacturing, automotive, retail, higher education, telecoms, and government	**Geographies covered**	North America, Europe, and Asia Pacific
Relevant company sizes	All	**Licensing options**	Subscription based on the number of assets
URL	www.runZero.com	**Routes to market**	Direct and channel, including MSSP
Company headquarters	Austin, Texas, US	**Number of employees**	±75

Source: Omdia

Analyst comment

Proactive security, in all the various firms described above, has been a leitmotiv of the cyber industry since the latter part of the 2010s. However, it has gathered pace in the last few years thanks to the expansion of corporate infrastructures (i.e., cloud, remote working, and IoT), the ongoing skills shortage, and the potential for automation, at least of the most mundane tasks, that artificial intelligence (AI) has brought to the party.

CAASM is arguably the harder end of the ASM spectrum, as demonstrated by the fact that there were, for a few years, new EASM vendors popping up every few weeks, whereas the CAASM competitive landscape is more restricted. There was also a glut of M&A activity in EASM, since that capability can be added more easily to a broader security offering such as a cloud-native application protection platform (CNAPP), whereas CAASM is a more complex undertaking that tends to remain standalone. Indeed, Omdia has often wondered why the CAASM vendors themselves have not been more aggressive in adding EASM capabilities to their products.

The fact that runZero is doing just that, and indeed plans to go further by evolving its product into full exposure management, is a salutary development, and Omdia will be accompanying that process as it goes forward. Given the lack of definition of what exactly constitutes exposure management at the moment, there is an opportunity for runZero to establish its credentials in this still nascent market, explaining and articulating how CAASM + EASM + vulnerability management + breach and attack simulation (BAS) (and

possibly one or two more capabilities such as pen-testing as a service, also known as PTaaS), represent the core components for any such offering.

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

Proactive Security: Data-driven Analysis (March 2024)

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*vv (June 2023)

On the Radar: KeyCaliber delivers cyber asset attack surface management based on telemetry (February 2023)

On the Radar: Sevco offers real-time asset inventory with a SaaS platform (March 2022)

On the Radar: Qualys Cybersecurity Asset Management (CSAM) helps discover and manage cybersecurity risks in IT assets (October 2021)

"Microsoft dives into Proactive Security, gives competitors heartburn with new exposure management solution" (December 2024)

"Rapid7 bags CAASM vendor Noetic while activists press for broader change" (July 2024)

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 TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, 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 TechTarget 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 TechTarget 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 TechTarget 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