Brought to you by Informa Tech

Author(s):
Fernando Montenegro, Senior Principal Analyst, Cybersecurity

Absolute acquires Syxsense as it continues to expand its platform

Omdia view

Summary

Recently, Absolute Security announced the acquisition of Syxsense, a vulnerability and endpoint management vendor, for an undisclosed amount. Absolute Security, now owned by Crosspoint Capital Partners, has about 750 employees and a strong presence in Canada, EMEA, and APAC, with expansion underway in LATAM. Absolute was taken private in 2023. Syxsense is based in California and has approximately 75 employees.

Before this acquisition, Absolute Security had two main offerings: its origins are in providing endpoint security via firmware-embedded security capabilities, plus an offering of secure access capabilities it acquired with the purchase of NetMotion in 2021. Absolute Security's firmware capabilities have been embedded in just over 600 hundred million devices worldwide, and the company has positioned its offerings as increasing resilience for mission-critical systems.

Syxsense had been focused on patch management and vulnerability management. This includes vulnerability scanning and remediation across multiple platforms, including Windows, Linux, Mac, and mobile. The offering includes risk-based analysis and high degrees of automation.

Another step toward a broader platform

This acquisition is interesting as it touches on different trends we continue to observe.

Primarily, it shows how Absolute Security is navigating growing its approach beyond the firmware-based endpoint persistence capabilities that were foundational for the company. These capabilities allowed customers to recover key systems more easily using robust firmware capabilities, but they were primarily “reactive.” The acquisition of Netmotion gave the company a more "active" role in terms of now running a remote access service for mission-critical devices. Now, the Syxsense acquisition gives it a "proactive" component as it aims to help customers proactively address patching and vulnerability concerns.

Omdia defines proactive security as technologies (including those provided as services) that enable organizations to seek out and mitigate likely threats before they pose a danger to the extended IT environment. Proactive security allows enterprises the opportunity to consistently and programmatically address the specific circumstances—unknown IT assets, vulnerable software, misconfigurations, and the like—that lead to unknown and unexpected threats to the enterprise.

The move also counts toward the tendency we have observed of vendors aggregating their security offerings within more of a "platform" approach. According to our research, end users prefer rationalizing the number of security tools they use. That said, the journey toward rationalization is not a straight one: only a small fraction of respondents to Omdia's 2024 Cybersecurity DecisionMaker survey indicated they had a decrease in the number of security tools used in their environments.

One more aspect that is worth exploring in this acquisition is that Absolute Security has positioned its broader strategy around resilience, with a goal of focusing on end-user organizations that have particularly critical endpoints distributed across remote and hybrid workers to protect. The proposed approach is that rather than having customers put together “generic” security tooling into a cohesive package, Absolute can cover a broad set of endpoint needs – visibility, control, recovery, access, hygiene, and more.

Moving forward, it’s good to consider rethinking boundaries

For Absolute Security, the company must now navigate the challenge of positioning its resilience-centered offering vis-a-vis the traditional mindset of how organizations build their endpoint security stack. Although all organizations should be focused on resilience, the company is likely to find more success focusing on specific use cases around industries where resilience is critical, including but not limited to transportation, education, healthcare, government, banking, and others, rather than a generic offering.

For enterprise buyers, this deal gives them one more option for a more specialized offer. Is this the time to think about a more platform-centric approach to security? If so, what are the merits of a more generic cybersecurity platform versus one providing more focus? In the case of Absolute’s offering, this means patch management, remote access, response and recovery, and resilience for critical tooling.

For cybersecurity vendors, the question becomes whether there are opportunities to pursue a more focused approach, such as Absolute Security’s "resilience"-centric one. This is likely to require vendors to build—or partner with those who already have—deeper knowledge of the many mission-critical environments.

Appendix

Further reading

Fundamentals of Proactive Security (September 2023)

Author

Fernando Montenegro, 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