



Market Insight Report Reprint

Coverage Initiation: Pentera looks to change how enterprises test and validate their cybersecurity posture

July 2 2021

by **Aaron Sherrill**

The vendor is aiming to end the perpetual lag in testing, detection, remediation and mitigation with its automated security validation platform. By converging and automating multiple testing approaches into a single platform, Pentera says it provides full visibility of attack operations and respective root vulnerabilities.

451 Research

S&P Global

Market Intelligence

This report, licensed to Pentera, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

Organizations leverage a range of security testing approaches, methodologies and technologies to validate their security postures, discover deficiencies, and evaluate the effectiveness of their security controls, policies and operations. Comprehensive testing often requires a combination of penetration testing, vulnerability scans, red team exercises, and other assessments to gain visibility across the entire IT ecosystem in light of evolving cyberthreats. However, these periodic tests often only provide point-in-time snapshots of an enterprise's security posture, unable to offer a continuous evaluation of the organization's cyber defenses, processes and controls. This intermittent testing approach, often driven by compliance mandates, is a critical shortcoming due to the increasingly agile, dynamic and fluid digital landscape of modern organizations.

Pentera (formally known as Pcysys) is aiming to end the perpetual lag in testing, detection, remediation and mitigation with its automated security validation platform. By converging and automating multiple testing approaches into a single platform, the company says it provides full visibility of attack operations and respective root vulnerabilities, continuously assessing the organization's resiliency against real attacks and enabling security teams to focus on remediations that have the greatest impact.

THE TAKE

Validating the organization's security posture and effectiveness should not be a lone annual event. Nor should organizations wait until an attack or other malicious event occurs to discover the effectiveness of their security investments, processes, operations and security service providers. However, manually testing the effectiveness of an organization's security posture tends to be a cumbersome process, requiring resources and expertise that is lacking in many organizations. And while traditional annual penetration testing engagements, vulnerability assessments, and security audits can help with risk identification, they only offer a point-in-time snapshot of an organization's security posture.

Automated, continuous testing platforms and services, like those offered by Pentera, can provide organizations with ongoing evaluation of their security posture and resilience, enabling the remediation of root vulnerabilities before an attack strikes. Pentera's goal of converging multiple testing frameworks into a single agentless platform could be advantageous, offering organizations assurances of their security readiness to meet a variety of use cases and needs.

Context

Founded in 2015 by CTO Arik Liberzon and chairman Arik Faingold, Pentera made its market debut in 2018, led by CEO Amitai Ratzon. With over 150 employees based out of offices in Israel, the UK, Germany, Switzerland, Italy, France, Spain, Australia and the US, the company claims that it has 350 customers across a wide variety of industries, including finance, healthcare, retail, technology and energy. Pentera reports that it has been adding more than 50 customers per quarter, a number it expects to increase substantially in the coming quarters as it begins to scale sales and marketing efforts.

Formally known as Pcysys, the vendor changed its name to Pentera in mid-2021, aligning with the name of its flagship platform offering. It has raised over \$40m to date, including a \$25m series B in September 2020. The round was led by US-based venture capital and private equity firm Insight Partners along with existing investors Awz Ventures and The Blackstone Group.

According to Pentera, few data breaches and security incidents are a result of the latest zero-day vulnerabilities. Rather, successful compromise and ransomware attacks are most often due to misconfigured security controls, unpatched vulnerabilities, excessive privileges, and a lack of segmentation. The firm has found that most organizations are missing a scalable way to continuously assess their security posture and efficacy from an adversarial point-of-view.

Pentera is aiming to empower security teams to combat these challenges with its automated security testing platform. Conducting automated attacks that leverage adversarial tactics and techniques, aligned with the MITRE ATT&CK framework, the company says it safely provides security teams with visibility into how attackers and ransomware threats can exploit their IT ecosystem, helping organizations identify weaknesses, prioritize remediations, and uncover cybersecurity risks.

Platform

Pentera is driving toward converging the capabilities and benefits of breach and attack simulation, vulnerability assessments, penetration testing, and risk-based vulnerability management into a single platform. Its platform features a wide range of capabilities, including network reconnaissance, vulnerability assessments, penetration testing, data hygiene assessments, data leakage testing, lateral movement testing, and privilege escalation testing, to name a few.

The platform evaluates and tests cloud, on-premises and hybrid environments, including end-user and IoT devices and applications. Security teams have the flexibility to take the testing approach that best fits their organization's needs, selecting the time, characteristics and testing model based on individual use cases. With both on-premises and cloud-based options, and no agents to install, Pentera says testing new environments can begin quickly with no prior knowledge of the environment.

The vendor offers security teams insights into their security posture improvement over time, detailing both the strengths and weaknesses of the environment, pinpointing misconfigured security controls, and validating security policies. This visibility highlights the impact that security investments have made on the organization's resilience and where additional investments may be needed. Pentera also helps security teams prioritize remediation of risk-bearing gaps, ensuring that time, effort and resources are allocated to the most impactful areas.

Pentera's recently released RansomwareReady framework allows organizations to safely emulate the disruptive ransomware strains such as REvil and Maze to test their network's resilience. Security teams are given visibility to the complete attack vector of vulnerabilities and lateral pathways that ransomware is most likely to take to target critical assets and disrupt operations. This visibility enables CISOs to inoculate their organizations against ransomware attacks before they occur.

While the company has primarily sold directly to enterprises, it is also partnering with managed security service providers (MSSPs) to go to market. By empowering MSSPs to add automated security validation services to their portfolios, Pentera says it sees MSSPs as a significant opportunity for growth.

Competition

Interest in on-demand, continuous, automated security validation and testing is growing as enterprises seek to eliminate weaknesses in their security posture before attackers can exploit them. The market for automated security testing is still relatively new, with vendors adopting a variety of approaches that will compete both directly and indirectly with Pentera for market share.

The vendor's main competition comes from traditional service-based penetration testing firms that have established long-term relationships with customers over the past decade. These include vendors like Accenture, EY, A-LIGN, Deloitte, Coalfire, Nettitude and Netragard. Pentera may vie with legacy breach and attack simulation providers like SafeBreach, AttackIQ, Picus Security, XM Cyber, Threatcare (acquired by ReliaQuest), Cymulate and Verodin (acquired by Mandiant), as well as automated red teaming providers, including Randori, SCYTHE and BreachBits. Differentiators in the broader market tend to revolve around the architectural methods and tactics of each – agent vs. agentless, simulated vs. authentic attack testing, testing production systems vs. testing designated testing systems, and continuous automated testing vs. scheduled traditional testing.

SWOT Analysis

<p>STRENGTHS</p> <p>Pentera's automated security validation platform provides organizations with a proactive, adversarial perspective of their IT ecosystems. The convergence of testing approaches should enable enterprises to continuously identify and close security gaps across a broader attack surface while also helping them prioritize remediation efforts and resources.</p>	<p>WEAKNESSES</p> <p>Automated security validation is a growing area of interest among organizations of every size and industry, fueling both startups and M&A. While the recent name change should be beneficial for the company, it will need to invest in broader marketing efforts to gain recognition in an expanding sector that encompasses a wide range of firms taking a variety of approaches to security testing and validation. Pentera could also benefit from boosting its testing capabilities to include external attack surface testing and custom application testing.</p>
<p>OPPORTUNITIES</p> <p>Expanding partnerships, especially with MSPs, MSSPs and MDR providers, could help broaden Pentera's market reach and be a force multiplier in its customer expansion efforts.</p>	<p>THREATS</p> <p>While continuous and automated security testing is becoming increasingly pivotal, especially in light of recent well-publicized attacks and breaches, many organizations may be reluctant to leave their traditional testing partners and embrace a more modern approach to security testing.</p>

CONTACTS

The Americas

+1 877 863 1306

market.intelligence@spglobal.com

Europe, Middle East & Africa

+44 20 7176 1234

market.intelligence@spglobal.com

Asia-Pacific

+852 2533 3565

market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2021 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.