Rapid7’s Alcide acquisition continues the vendor’s aggressive expansion of a strategy focused on cloud-native application security platform functions. Security and risk management leaders must evaluate the impact of this and prior acquisitions on their application security tool portfolios.

Get the full story
This content is part of a larger body of research on this topic.

Magic Quadrant for Application Security Testing

Key Background
Rapid7 announced on 1 February 2021 it had acquired Alcide, a Kubernetes-centric cloud security vendor based in Tel Aviv. Rapid7 reported a purchase price of $50 million, subject to unspecified adjustments. Alcide continues to operate as a stand-alone entity. However, technology from the firm has been combined with that from previous Rapid7 acquisitions, leading to the July 2021 release of a new product, InsightCloudSec, under the Rapid7 brand.

The acquisition is the third in an effort to expand the company’s application security portfolio beyond more traditional boundaries. With its InsightAppSec DAST offering — complemented by vulnerability assessment tools such as InsightVM, Metasploit and Nexpose — Rapid7 has been a long-term, successful competitor in application security. The Alcide acquisition, combined with the purchase of DivvyCloud (a CSPM vendor acquired in May of 2020 for $145 million) and tCell (a RASP solution purchased for an undisclosed sum in October 2018), provides Rapid7 with the elements of a cloud-native application protection platform (CNAPP) offering.
Considerations for Technology and Service Selection

This research is intended to provide relevant contextual information to help you consider and prepare for potential future risk or advantage. It is not a reevaluation of providers, but rather an update based on publicly available information at a certain point in time. Because the results of corporate reorganizations typically change and evolve over time, Gartner analysts will continue to monitor these changes. The next annual update of the Magic Quadrant will reflect the potential impact(s) that we determine the corporate reorganization may have on provider positions.

We encourage you to use this perspective in conjunction with the existing Magic Quadrant as you consider initial resources for provider evaluations and decision-making. As you assess your unique business and technical requirements, always supplement this research with scheduled analyst inquiries to help you and begin to gain insight on further developments, before making any decision.

Provider- and Market-Agnostic Analysis

Customers of both Rapid7 and Alcide should undertake standard measures to anticipate and mitigate potential disruptions to operations.

Potential impacts on or risks to customers:

- Support issues are a common effect of ownership changes. Budget for and shortlist supplementary resources to address support inconsistencies.
- Be alert for reductions in new product development in favor of capability and technology alignment and integration.
- Track changes in the vendor and channel sales organization. Compare vendor feedback with other sources, including competitive vendors, resellers and integrators, as well as independent advice such as industry peer groups and Gartner analysts in specific areas of expertise.

Risk mitigation strategies and tactics to consider:

- Develop contingency plans that allow your organization to continue in business if a critical supplier is unable or unwilling to deliver its services or solutions.
- Identify the services, solutions and suppliers that should require contingency plans based on their business criticality and the potential disruption.
Keep close tabs on the vendor product roadmap, and ensure the vendor is meeting its communicated release dates with committed product features.

Use change and uncertainty as a procurement advantage during sales or renewal negotiations by making it clear that there is an unknown impact from the acquisition.

Market-Level Analysis

This transaction is significant in the context of the application security market in that it reinforces significant shifts in how organizations view application security as they transition to DevSecOps. Conceptually, a DevOps team (or a higher-level value stream or product organization) consists of a comprehensive array of individuals and resources needed to design, build, deliver and operate an application or service — including security. And, as noted in previous Gartner research on cloud-native application security platforms, in these environments, “rather than treat development and runtime as separate problems — secured and scanned with a collection of separate tools — enterprises should treat security and compliance as a continuum across development and operations, and seek to consolidate tools where possible.”

In reality, a relatively small percentage of organizations have actually progressed to that level of integration, with the vast majority of organizations still in a transitory phase of migration. For example, 20% of all the contacted respondents for Gartner’s Enabling Cloud Native DevSecOps Survey \(^1\) indicated they’ve achieved production status in implementing a DevSecOps pipeline. That means nearly four out of five respondents are either in transition (27%) or still piloting (15%), or not involved/unsure (16%). As a consequence, markets for security tools focused on development (e.g., application security testing, software composition analysis) and cloud application security (e.g., cloud security posture management and cloud workload protection) are essentially distinct, although overlap is seen among some vendors. Rapid7’s acquisitions are another step in that evolution.
As the transition to DevSecOps occurs, we see other trends affecting the market in ways that make a converged solution, similar to the one offered by Rapid7, of interest to a broader set of buyers. First, the technical nature of cloud native applications relies heavily on the concept of infrastructure as code, where operating environments and supporting services are instantiated in a cloud environment by way of scripts and configuration files. These are frequently written — and security tested — by developers in the context of the programming and build environments. This makes developers responsible for additional infrastructure beyond the application, a responsibility that extends into the runtime environment. Scanning tools capable of spotting security issues with these artifacts show increased interest. Similarly, scanning of container images for security problems is another function that is moving into the development phase.

While examples of overlaps in products and functions are relatively common, they’re generally limited in scope. For example, a CWPP tool might well offer container security scanning, and CSPM offerings frequently include infrastructure as code (IaC) checks. But, in many cases, these remain cloud security tools purchased by operations or cloud security teams. Likewise, application security testing tools have begun to offer similar capabilities, but focused on the needs of, and sold to, application security teams. As the market moves forward, we will see these distinctions fall away, creating demand for converged solutions.

As further evidence of this trend, we can point to the shift in budget for application security tools from traditional security groups to application development and DevOps teams. In the previously cited cloud-native security study, 32% of respondents indicated security was the budgetholder for security tools (across both development and operations). The combination of DevOps and application development with budget authority has grown to 26% — from nearly zero two to three years ago.

1 Gartner’s Enabling Cloud-Native DevSecOps Survey was conducted online from 12 through 21 May 2021, to identify the emerging governing structures, security owners, technologies used and the current challenges in the DevSecOps pipeline to secure cloud-native applications. In total, 85 IT and business leaders with involvement in DevSecOps initiatives participated in the survey; 82 were from Gartner’s IT and Business Leaders Research Circle — a Gartner-managed panel — and three were from an external sample. Participants from North America (44%), EMEA region (35%), Asia/Pacific (8%) and Latin America (13%) responded to the survey.

The survey was developed collaboratively by a team of Gartner analysts, and was reviewed, tested and administered by Gartner’s Research Data and Analytics team.
Disclaimer: The results of this study represent the respondent base, not the market as a whole.

Provider-Level Analysis

Rapid7’s traditional strengths in dynamic application security testing remain relevant. Forty percent of respondents to a Gartner survey on enabling cloud-native application security report using DAST to secure cloud-native applications. However, the technology’s core strength — assessment of web-based applications — will be increasingly less relevant in an environment where web applications become far more complex and difficult to test. They will be supplanted by mobile and other types of applications and their supporting technologies, such as APIs, microservices, containers and serverless computing.

The acquisition of Alcide — and DivvyCloud and tCell before it — positions Rapid7 across a much broader swath of the application security market landscape. As a result, the company joins a small number of traditional application security testing vendors in offering broader cloud-native application security capabilities and faces a much larger competitive challenge from cloud vendors who’ve begun to reach into the development side of the market. For current and prospective buyers in a market where customers tend to prefer to acquire solutions from vendors with more comprehensive portfolios, the combination is potentially attractive. This is particularly true for the large portion of the market that remains in transition to cloud-native applications and is still focused on more traditional tools such as DAST. Nevertheless, Rapid7’s limited support for broader AST technologies (e.g., SAST, SCA) will hobble the firm competitively.

The relatively rapid availability of a consolidated cloud security product within the Rapid7 portfolio is a promising sign, suggesting the company intends to fully leverage its investments. However, as with any strategy, much comes down to execution. As with any acquisition, and as noted above, customers must heighten their attention to matters such as product sales and support, areas that are frequently disrupted in such transactions.

Especially for current Alcide customers (and DivvyCloud and tCell before them), close attention to both the overall direction of the product roadmap and the company’s ability to deliver on existing commitments should be carefully scrutinized. While both Alcide and DivvyCloud continue to operate in a semiautonomous manner, Rapid7’s clear direction is to move toward the consolidated InsightCloudSec product. Given the company’s vision, organizations must monitor both products and prepare contingency plans to minimize operational and business disruptions as the Alcide products are integrated into the Rapid7 portfolio.
Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Magic Quadrant for Application Security Testing

Innovation Insight for Cloud-Native Application Protection Platforms

A Guidance Framework for Establishing and Maturing an Application Security Program

Survey Analysis: Enabling Cloud-Native DevSecOps

How to Plan for and Respond to a Strategic Vendor’s Merger, Acquisition, or Divestiture

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."