



Market Insight Report Reprint

For cloud-native monitoring, most enterprises employ multiple approaches to meet their needs

July 15 2021

by **Liam Rogers, Jay Lyman**

Cloud-native apps have spurred many companies to reexamine their monitoring tooling to see whether it's keeping up with emerging needs. As a result, organizations have taken various approaches to meet their needs, including leveraging their existing monitoring vendors, engaging new ones and building their own tools.

451 Research

S&P Global

Market Intelligence

This report, licensed to Chronosphere.io, 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

Cloud-native applications have introduced new challenges in monitoring as highly distributed microservices-based applications can be complex and the number of interconnected microservices can generate large amounts of telemetry to be stored and analyzed. With the added complexity and differences in architecture, organizations have had to reexamine their approaches to monitoring to ensure they are maintaining visibility across their environments. Our Voice of the Enterprise: DevOps, Workloads & Key Projects survey highlights the benefits and challenges of using cloud-native technologies, as well as how the usage of them has impacted monitoring purchasing decisions.

THE TAKE

Given that there is a relatively even distribution of approaches to procure the tools needed to monitor cloud-native apps and that many organizations are still using multiple approaches, we can infer that many are still assessing their needs and determining the best way to meet them; this may continue to be a mix of options to cover a variety of applications. The fact that many organizations have engaged new vendors indicates that cloud native continues to be an arena where new vendors can differentiate with purpose-built systems designed with cloud-native technologies in mind rather than having to modify or repurpose existing tools and accommodate legacy customer bases. Incumbent monitoring and APM vendors have also made strategic acquisitions to bolster their portfolios, and although this gives them more upselling power, it can also result in large and potentially expensive platforms. However, there are challenges for all vendors in this space given that for technologies such as serverless computing, the default level of visibility can be somewhat predetermined by the cloud providers behind such services. Organizations must balance their ability to collect machine data and also draw meaningful insights from it. Open source software (OSS) will continue to play a significant role even in cases where it is not front and center but rather tooling 'baked into' projects such as Prometheus or integrates would-be standards for data collection such as OpenTelemetry.

Benefits and challenges of cloud-native adoption

There are myriad drivers for the use of containers, Kubernetes and serverless, and primary among them is achieving IT operations efficiency as a benefit of using cloud-native technologies. Other drivers include better developer productivity and application portability. However, organizations must also contend with growing pains as concerns about security and cost persist and can be amplified by complexity, which is a top challenge in its own right (see Figure 1). As more organizations draw on microservices-based architectures supported by newer technologies that are seeing more mainstream adoption, such as Kubernetes and serverless, enterprises have had to contend with new operational challenges. Without adequate tooling or processes in place, the growing complexity of cloud-native apps can be in direct opposition to the desire to maintain visibility and ensure service level objectives.

Figure 1: Cloud-Native Technology Challenges

What are the primary challenges of using cloud-native technology such as containers, Kubernetes or serverless in your organization? Please select all that apply.



Sample Size = 547
Base: All respondents

Source: 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2021

How enterprises are responding to emerging needs

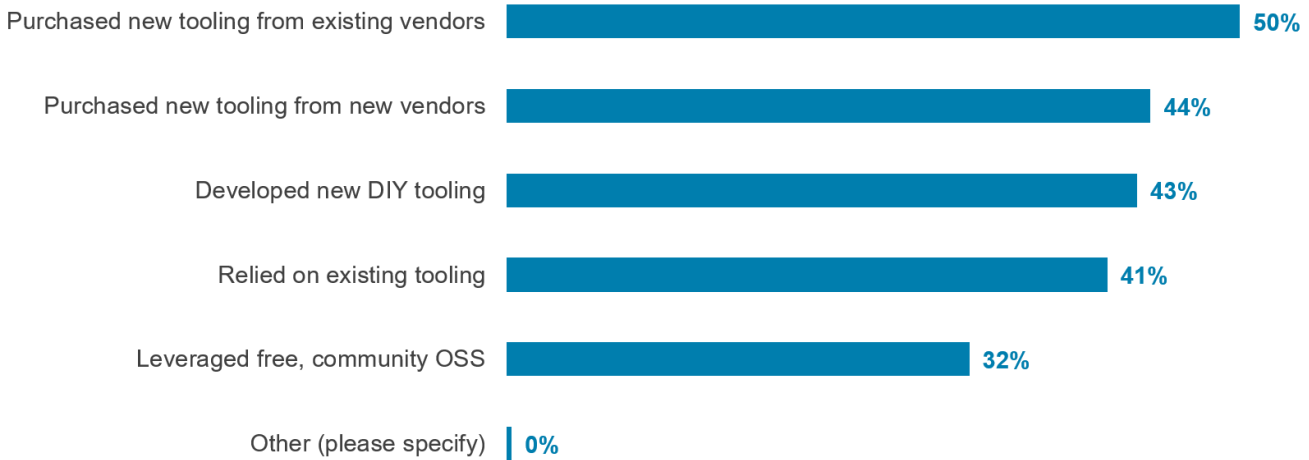
To respond to emerging and changing monitoring needs, enterprises have employed multiple approaches such as leveraging existing vendors, new vendors, open source software and even creating DIY tooling (see Figure 2). Many organizations have turned to more than one of the aforementioned options at a time: 32% of respondents are leveraging just one, 36% are using two, and 25% are using three (with the remaining 7% using four or more).

It's no surprise that organizations are turning to existing vendors for emerging needs, and 50% of respondents cited that they have done so. Large vendors in the observability space have been quick to demonstrate their ability to accommodate cloud-native applications, and previous data has shown that customers prefer to source as much tooling from a single vendor as possible. For example, 451's Voice of the Enterprise: Storage, Transformation data shows that 83% of organizations prefer to buy monitoring and incident response tools from a single vendor when possible. This preference is partially driven by the desire to consolidate the number of disparate tools being deployed in environments to reduce complexity and drive down cost, but it's also due to the logistical simplicity of purchasing from a vendor with which the organization already has an established relationship.

Since incumbent vendors have largely expanded their portfolios through acquisition to span logs, metrics and traces in an effort to offer holistic or 'full stack' observability platforms, it is now feasible for customers to attain more functionality from existing vendors than they would have been able to in the past. For example, DataDog and Splunk are among incumbent vendors offering wide-reaching and integrated portfolios. They are also among the market leaders in terms of revenue in the monitoring and logging subsegment of our Market Monitor application container ecosystem market sizing.

Figure 2: Purchasing Behavior Related to Monitoring Cloud-Native Apps

How has your organization responded to the monitoring needs of cloud-native applications? Please select all that apply.



Sample Size = 542
 Base: All respondents

Source: 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2021

Keeping tool sprawl in check is likely similar motivation for the 41% of organizations that are effectively making do with what they have in place as more vendors update existing tooling to integrate with the likes of Kubernetes and Prometheus or, in the case of serverless, package functionality into AWS Lambda extensions. AppDynamics (Cisco), DataDog, Dynatrace, New Relic and Splunk are among vendors that have released Lambda extensions as a way to extend functionality of their platform (more details on this will be in an upcoming Spotlight report on serverless monitoring).

The relatively high number of organizations purchasing from new vendors (44%) highlights the notion that despite the expanding portfolios of incumbent players and the desire to reduce tool sprawl, customers are still interested in a best-of-breed approach when necessary. Startups such as Lumigo and Chronosphere aim to show customers that newer technologies can best be met by more recently engineered products that have been purpose-built with cloud native in mind – Lumigo and Chronosphere are focused on AWS Lambda and Prometheus, respectively.

A few additional data points stand out. For example, organizations in the financial vertical were half as likely to use free OSS – only 15% of those respondents cited doing so. With the proliferation of OSS such as Prometheus and FleuntD (Cloud Native Computing Foundation projects), we expect that many organizations using vendor-supported or even DIY tooling are drawing on pieces of OSS to some degree since usage of Prometheus will underpin Kubernetes monitoring tools from many vendors. For organizations that have adopted DevOps across 100% of their organization, development of DIY tooling was much more likely at 51%, compared to 34% of organizations with just some adoption of DevOps. However, this may also be an indicator of the scale of cloud-native apps in those organizations because a 'roll your own' approach can quickly become costly and time-consuming to manage, and these organizations may in time opt for support from vendors.

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.