REPORT REPRINT

IT monitoring meltdown: Just 11% of decision-makers are satisfied with their monitoring tools

AUGUST 06 2020

By Nancy Gohring

In a recent survey, we found that 83% of respondents are either actively seeking new monitoring services or have plans to expand or improve their approaches to monitoring. With only 11% saying they're satisfied, users are demanding new functionality from vendors.

THIS REPORT, LICENSED TO STACKSTATE, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. 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 451 RESEARCH.

451 Research®
Now a Part of
S&P Global Market Intelligence

Introduction

In a study conducted by 451 Research (and commissioned by New Relic) in July, we surveyed 700 people in the US and Europe who primarily make but also influence decisions about monitoring tools for their organizations. We found that 83% of respondents are either actively seeking new monitoring services or have plans to expand or improve their approach to monitoring. With only 11% saying they're satisfied, users are demanding new functionality from vendors, and vendors are responding by offering an array of tools that were commonly provided independently.

451 TAKE

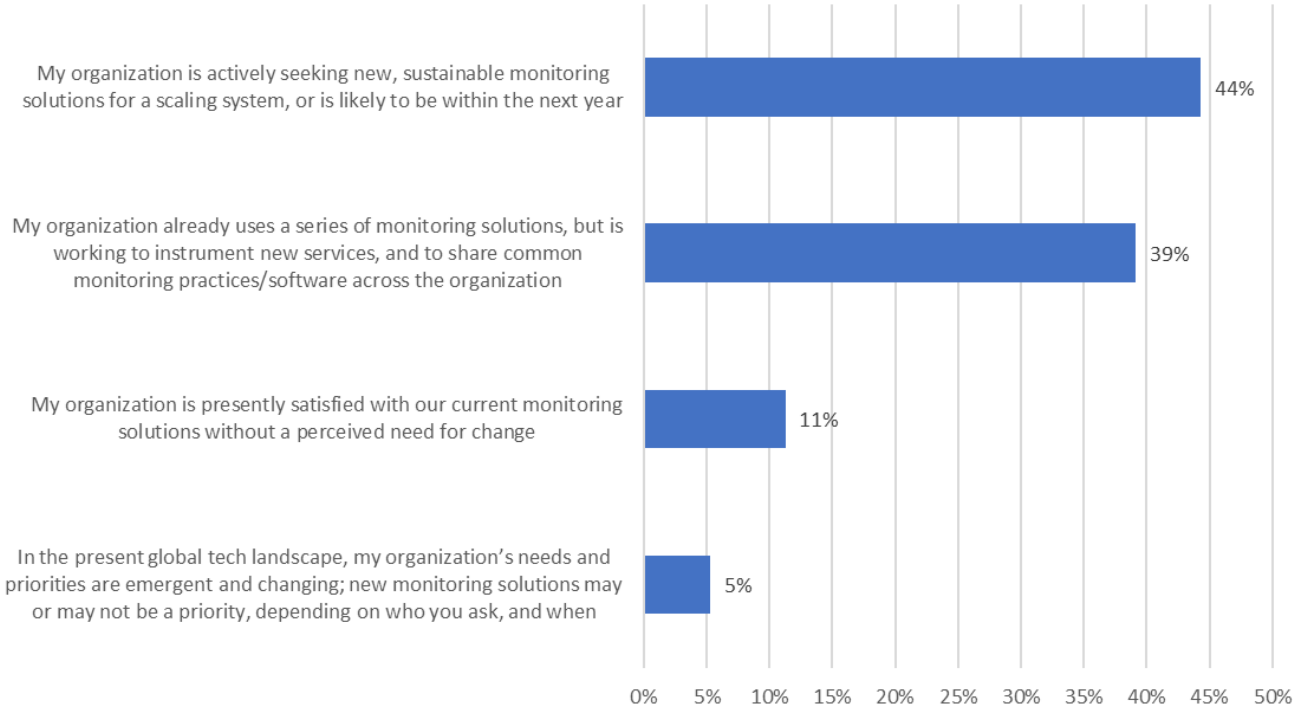
It's a time of significant change for the monitoring industry, driven largely by operations and incident-response challenges that have emerged as a result of the adoption of cloud-native technologies. With 83% of organizations in our recent survey planning to make changes to their monitoring practices, the pressure is on vendors to deliver capabilities that end users feel are lacking in their current tools. The most important capabilities required of monitoring tools used to achieve visibility into cloud-native environments include the ability to collect granular data at scale, flexible data querying functionality, advanced analytics and support for automation techniques. In addition, it has become increasingly clear that organizations have struggled with juggling too many tools that collect and retain data in silos. Users are interested in combining several monitoring functionalities from a single provider to not only reduce tool and vendor management pain but also gain new capabilities.

It's time for a change

In our recent survey, we found that a significant majority of respondents are planning to deploy new monitoring tools or expand their monitoring operations, with very few respondents satisfied with their existing approach to monitoring. Forty-four percent of respondents said they were seeking new monitoring tools or would be within a year, with an additional 39% of respondents planning to monitor new services and share common monitoring approaches across their organizations. Only 11% of respondents said they were satisfied with their current monitoring tools.

Which of the Following Models Best Characterizes Your Company's Current Monitoring Status?

Source: 451 Research, custom study commissioned by New Relic (N=700)



The shift to cloud-native technologies and practices is spurring this period of significant change in the monitoring industry. As organizations deploy technologies like cloud, containers, Kubernetes and service mesh, their application and infrastructure environments become significantly complex. Not only are applications and infrastructure composed of many more components, those components may be dynamic, running for very short periods of time.

Each of the components of this dynamic environment generates operations data, as does the communications between the services that make up these distributed applications, resulting in a much larger volume of IT operations data than that generated by traditional applications. To learn that a performance problem is occuring and quickly and accurately identify the cause of a problem, teams must collect and analyze this potentially enormous volume of data. This new reality requires a new approach to monitoring that in many cases includes new monitoring tools.

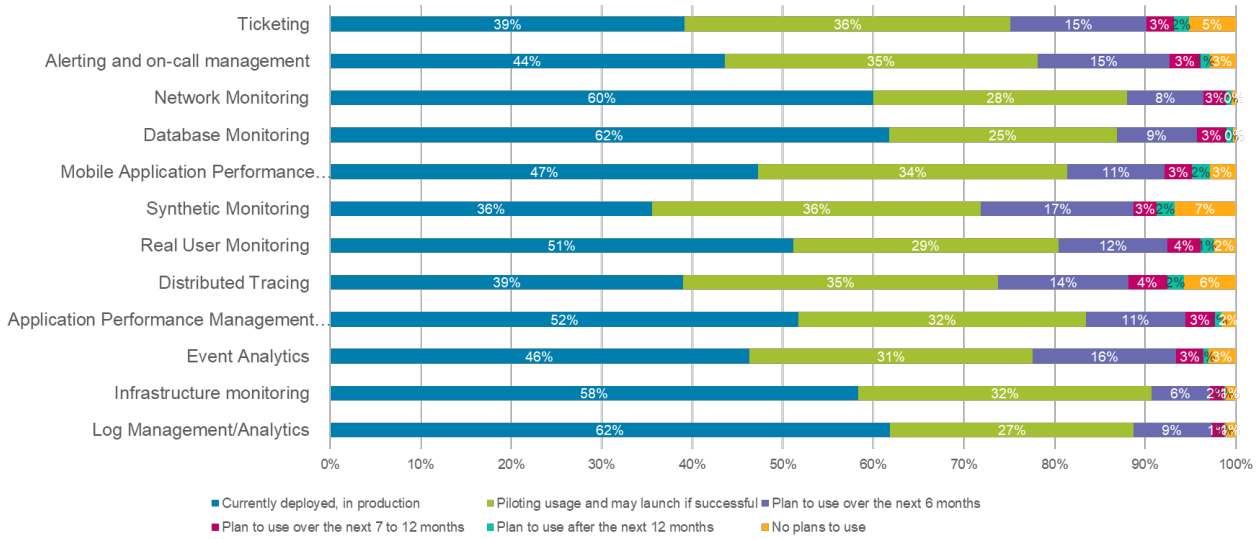
However, new tools should not necessarily mean additional tools. We commonly hear from organizations that face a number of important challenges because they are juggling too many tools that collect and analyze only a subset of relevant operations data.

Now what?

Our recent survey indicates that users either already have or plan to implement a very wide array of monitoring functionalities. We asked respondents about their use of 12 different types of commonly used monitoring and incident response tools, and found strong current and planned adoption of all 12. The percentage of respondents who had no plans to deploy the tools was remarkably small, with network monitoring and database monitoring each registering zero respondents with no plans to deploy, and log management and infrastructure monitoring with only 1% each with no plans to deploy.

Which of the Following Best Characterizes Your Adoption of the Following Monitoring Tools at Your Company?

Source: 451 Research, custom study commissioned by New Relic (N=700)



These results do not indicate that respondents necessarily plan to use a different tool from a different vendor for each function, and we would recommend that organizations consider using tools that offer multiple functions. It's increasingly possible to do so, with many of the larger vendors expanding horizontally over the past few years to deliver several types of tools. In fact, among the top 10 vendors by revenue in this sector, all have offerings in six or more of the categories we track, with two delivering in eight categories, according to our research.

Integrated tools can solve a few challenges for organizations. One is that they simplify vendor and tool management. More importantly, integrated tools have the potential to deliver new capabilities that can address some of the problems that commonly plague organizations that are adopting cloud-native technologies. One of the most common integrations we've seen over the past few years is infrastructure monitoring and log analytics, where a user discovers that a problem is occurring via the metrics-centric infrastructure monitoring functionality but can view within the same visualization relevant logs that may help pinpoint the root cause of the problem.

Those capabilities are increasingly combined with distributed tracing data, which can help narrow down trouble spots and contribute to detailed topology maps. Modern tools can run sophisticated analytics across metrics, distributed traces, logs and events to group together related issues and guide users to the source of a problem and how to solve it. Such functionality can have a significant impact on incident response by reducing or eliminating alert storms and decreasing the time it takes to identify and fix performance issues.