Market Insight Report Reprint

# Splunk offers a steady stream of enhancements to observability cloud, along with pricing flexibility

December 3 2021

by Liam Rogers

Having successfully integrated past acquisitions into its Observability Cloud, the vendor continues to offer enhancements to capabilities spanning APM, RUM and security, along with quality-of-life features such as mobile access. At its Splunk .conf21 event, there was a bevy of updates announced to both its observability and security services.

451 Research

S&P Global
Market Intelligence

## Introduction

There was a bevy of updates at Splunk .conf21 to both its observability and security services. This included continuous profiling for APM, real-user monitoring (RUM) for mobile apps, integration of Splunk Log Observer and Splunk Enterprise, a new app editor for Splunk SOAR, and Splunk Intelligence Management (we will cover more on the .conf21 security announcements in a subsequent report).

Additionally, Splunk is offering workload-based pricing to help customers retain data more cost-effectively. Splunk's updates are numerous, and the organization continues to see growth in its cloud business – but despite the flurry of activity, the recent turnover in leadership means Splunk will also need to reestablish its vision for the future.

## THE TAKE

Splunk is an established player and commands significant market share in this sector; however, this also results in it often being the target of other vendors. The competition continues to try to carve out market share based on promises of cost savings. In this sense, it is Splunk's game to lose as a host of vendors take aim at its sizeable customer base, but the continued expansion of capabilities across its services would indicate the vendor is more than willing to go toe-to-toe with a range of competitors in log management and beyond.

Splunk APM is still a relatively newer component of Splunk, and a number of the recent updates bolster the utility of Splunk APM's service map, functionality that's relevant given the complexity of many modern applications. The expansions in security as well as the integration between Log Observer and Splunk Enterprise show that the vendor is eager to make good on its aim to cater to a wider range of audiences, and to let them tap into the data their organizations are already collecting in Splunk. Simultaneously, workload-based pricing will give customers an incentive to allow more users to funnel data into the Splunk platform with lessened scrutiny, and without incurring the potential wrath of ingest-based costs.

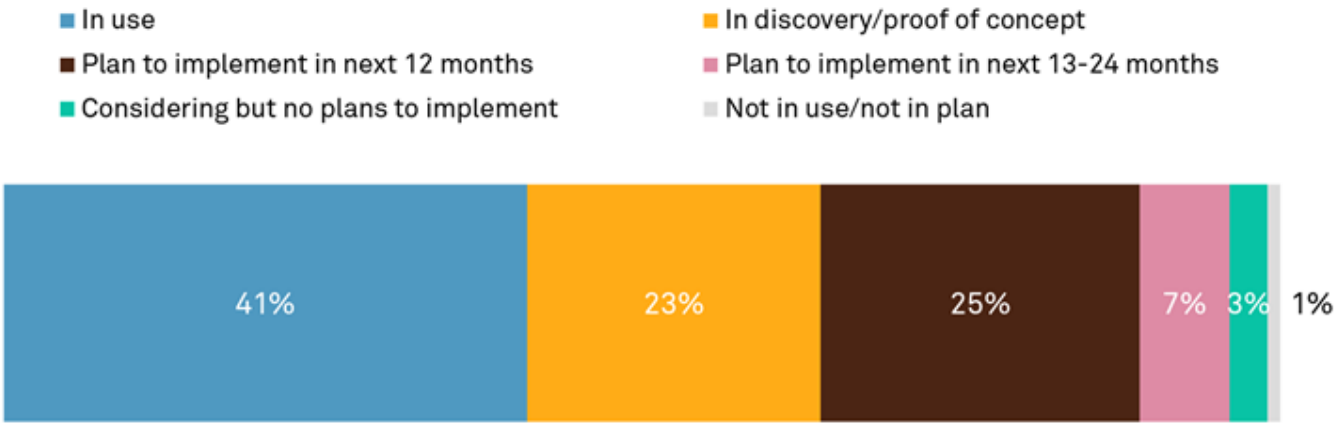
## Context

Splunk's Q2 FY 2022 earnings showed growth in ARR, with cloud ARR at $976m, up from $568m in Q2 FY 2021. Although Splunk continues to see gains in the cloud, where it is putting much of its effort, the on-premises business still makes up the majority, with noncloud ARR at $1,656m in Q2. After six years, Splunk CEO Doug Merritt recently stepped down, with board of directors chair Graham Smith stepping into the role in an interim capacity.

This follows the departure of CTO Tim Tully earlier this year, and the turnover at the executive level will likely raise eyebrows among some customers. Additionally, in June, the company received a $1bn investment from private equity firm Silver Lake, with chairman Ken Hao gaining a seat on Splunk's board of directors. Regarding ESG, Splunk has been progressive about developing and articulating its strategy. Recently, the company announced a commitment to achieving net-zero greenhouse gas emissions by 2050.

In 451 Research's Voice of the Enterprise: DevOps, Organizational Dynamics study, 41% of organizations say they have already adopted observability (see figure below). While there is still confusion around what constitutes observability, the 1% of organizations saying it's not in their plans is testament to the drive toward widespread adoption. Currently, larger enterprises are also more likely to have adopted observability, and these kinds of organizations often already have a myriad of tools in their environment to form the foundation of their observability strategies, especially as vendors expand the breadth of their capabilities.

**Current Observability Adoption**




Q. What best describes your organization's adoption of observability (i.e., collection and analysis of data logs, metrics and traces)?
Base: All respondents (n=492)
Source: 451 Research's Voice of the Enterprise: DevOps, Organizational Dynamics 2021

## APM and RUM enhancements

Splunk APM saw the addition of AlwaysOn Profiling and Database Visibility. AlwaysOn Profiling provides, as the name implies, continuous code profiling for faster resource optimization and troubleshooting of performance issues. Functionally, it captures call stack data from runtime to augment spans and traces, as well as provide more detailed performance information. This data is then visualized alongside Splunk APM's service graph as well as in a 'flame graph' menu where call stacks are organized by time range.

Customers can toggle the profiling on and off, and will be more likely to use it for new code being pushed to production, with the capability turned off after refinements are made. Splunk is one of the vendors heavily involved in the open source OpenTelemetry (OTel) project within the Cloud Native Computing Foundation, and has made native support for OTel a part of its services. The company does have its own OTel distribution and SDK distributions, for ease of support. This OTel distribution is used as the continuous data collection method for the AlwaysOn profiler (OTel standards are used in other Splunk services as well).

AlwaysOn profiling is currently in preview, and planned to be generally available by the end of the year. Splunk APM has added more granular query performance visibility and data aggregation for SQL-based databases to identify slow queries and resulting latency. Given the proliferation of databases – ranging from larger enterprise databases to smaller ones underlying microservices-based apps – there is value in collecting more detailed telemetry without having to instrument it within the database itself. The new database visibility enhancements for Splunk APM are currently in preview. Finally, Splunk RUM went into general availability in May. At the time, it only supported web applications, but now it includes Android and iOS mobile apps.

## Observability updates and integrations

Two updates to improve the accessibility and user experience of the observability platform include the integration of Splunk Log Observer and Splunk Enterprise, and the addition of Observability Cloud for mobile. The Log Observer and Enterprise integration allows customers to use the more intuitive Log Observer UI to analyze any logs stored in the enterprise product. Telemetry can be centralized in the enterprise platform, but debugging can be performed via the Log Observer UI, which is designed to be accessible for personas from DevOps to SREs.

Observability Cloud for mobile does what it advertises – provides an app for iOS and Android devices where users can quickly view alerts and dashboards. Given Splunk's expansion into on-call management, the ability to equip on-call engineers with another way to access dashboards is a synergistic addition.

## Pricing flexibility

Splunk also announced the availability of workload pricing for Splunk Cloud. Workload-based pricing is not a new addition to Splunk, but the vendor is bringing it to the fore at a time when data collection and retention costs have become a growing pain for customers. In this pricing model, customers are not charged based on data ingest but instead based on usage of data; effectively, compute resources become the variable that is metered.

For data that is searched less frequently, the workload-based pricing can prove more cost-effective. Customers will be able to switch pricing models as needed. So as new workloads become more understood and predictable, it may be advantageous to switch from ingest to workload-based pricing for less critical applications, without having to forego retaining that data, or make large volumes searchable without having to pay massive ingest costs.

If Splunk is successful in getting tools in the hands of a wider set of personas within organizations, it becomes more economical for teams spanning DevOps, IT ops and security to send data to Splunk in a way where simply collecting the data will not impact cost as greatly as if it were billed on volume ingested.

## Competition

Splunk has no shortage of competition in observability, given that its platform spans log management, infrastructure monitoring, APM, RUM and synthetic monitoring. These include Elastic, Cisco (including AppDynamics), IBM (including Lightstep), Sumo Logic, VMware, Datadog, Grafana, SolarWinds, Dynatrace and New Relic, in addition to smaller companies such as Honeycomb, Chronosphere and LogDNA. Elastic recently acquired Optimyze to add continuous profiling capabilities to its platform.

Datadog and SolarWinds both provide database monitoring capabilities. Vendors such as Era Software (fka EraDB) and ChaosSearch are among those aiming to offer more cost-conscious log management compared to incumbent vendors, and Cribl also targets log data cost reduction with its platform, although Splunk's workload-based cloud pricing is intended to offer similar cost savings. AWS, GCP and Azure are growing their market share, but many of the vendors mentioned here (Splunk included) work with and build on top of public cloud services, so competition is tempered by cooperation.

In security, competition is largely around SIEM, which includes vendors large and small from observability and security such as Elastic, Sumo Logic, IBM, RSA Security, Datadog, Devo, Logz.io, FireEye, Rapid7, Humio (Crowdstrike), LogRhythm and Graylog.

## SWOT Analysis

### STRENGTHS

Splunk is well established in market share, and its acquisitions in recent years reinforced the foundation for its capable cloud platform. With its emphasis on OpenTelemetry, the vendor continues to strengthen its appeal for growing cloud-native workloads.

### WEAKNESSES

Splunk is still executing on the shift to the cloud and the vision of its previous execs. It will need to begin charting the next leg of its journey to ensure it doesn't lose ground to the competition.

### OPPORTUNITIES

Security has become a hot topic among observability vendors vying to capture new market share, and given Splunk's established foothold with security teams via SIEM, there is plenty of runway for newer offerings.

### THREATS

While its continued expansion improves stickiness with customers, Splunk has also brought itself into competition with some vendors that have historically been partners, and the vendor will continue to face fierce competition from all sides.

**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