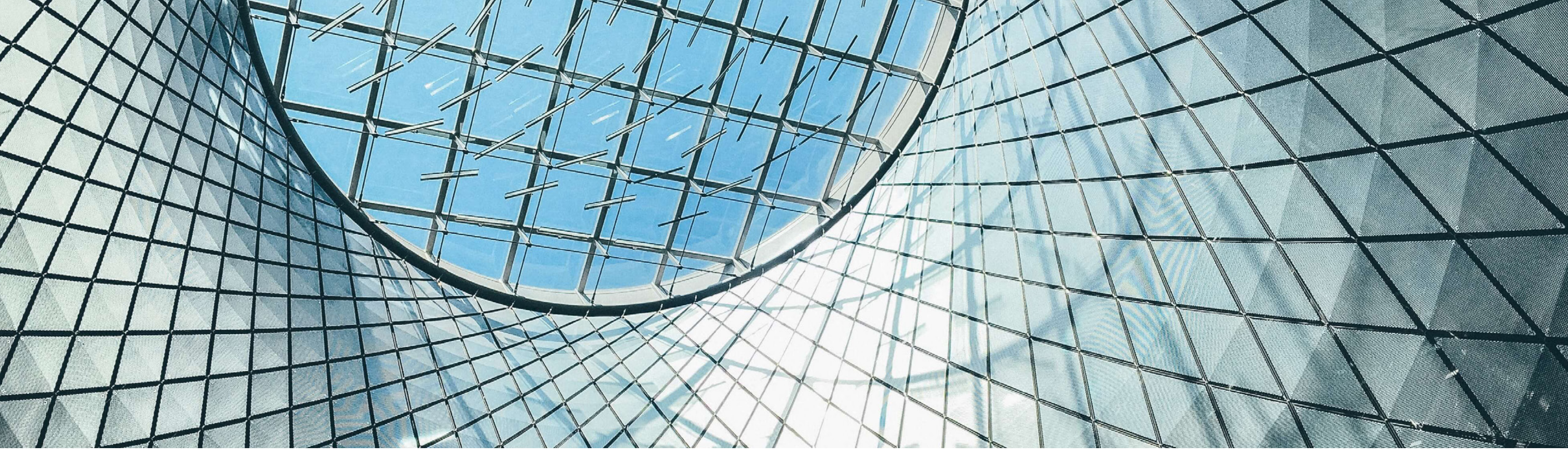


Market Insight Report Reprint

Splunk Enterprise 9.0 launches at .conf22 alongside keynote from new CEO

July 15 2022

by James Sanders

At .conf22, Splunk's annual user conference, new CEO Gary Steele reiterated the company's position as the center of workload observability, touted feature improvements to Splunk Enterprise and Cloud, and explored the influence and importance of security in observability processes.

451 Research

S&P Global
Market Intelligence

Introduction

Observability is the topic du jour among enterprise IT practitioners. The prospect of leveraging AI/machine-learning-aided tools to simplify IT management tasks, including managing more workloads with fewer employees, is undeniably attractive. In practice, actually extracting this value is challenging: A sprawling number of tools from a growing list of vendors, with overlapping feature sets and use cases, as well as inconsistent paths toward integration, has led to a patchwork of software.

This patchwork would not exist without merit – at a minimum, each tool would have some definable utility to at least one product/service team or stakeholder. Splunk Inc. takes a “big tent” approach to observability. While the company has developed observability functionality, it has also been a prodigious acquirer of observability startups, including SignalFX, Omnition, Rigor and Plumbr in recent years. Splunk also touts over 2,500 apps available on Splunkbase for integration of third-party tooling. At .conf22, Splunk’s annual user conference, the company reiterated its position as the center of workload observability, touted feature improvements to Splunk Enterprise and Cloud, and explored the influence and importance of security in observability processes.

THE TAKE

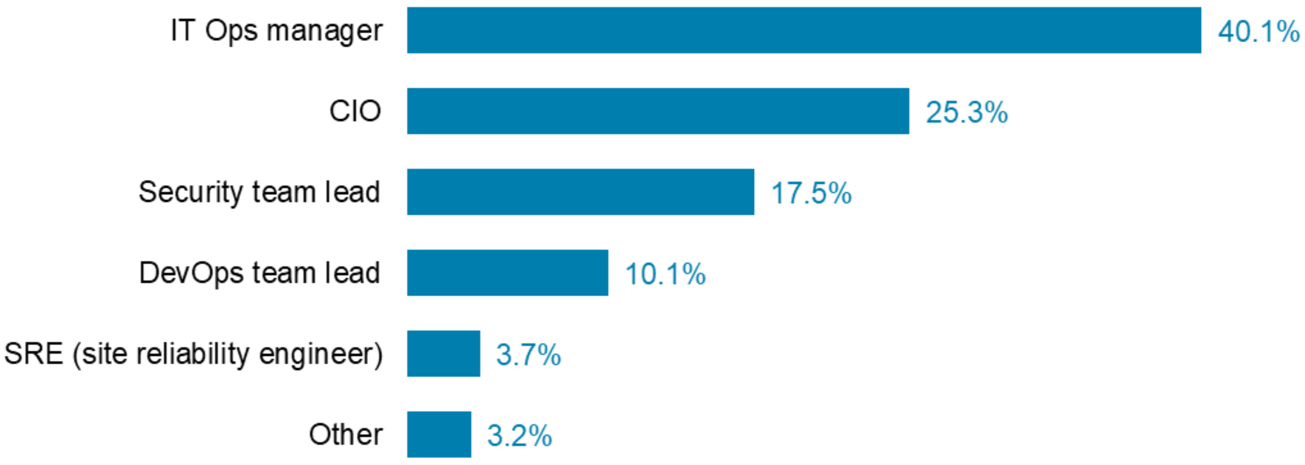
Splunk has the distinction of being an entrenched player in observability. While this implies (and occasionally begets) the ability to shape a market, it also puts Splunk in the position of being a lightning rod for competition. With the appointment of new CEO Gary Steele and a leaner executive team, Splunk has an opportunity to transcend, not pivot, from the cloud transition plans put in place several years prior. Building a bigger tent to include security practitioners, in addition to the development and operations practitioners it already courts, requires a willingness to compete with erstwhile partners across a number of different fields, as well as clear and repeated messaging about the value of centralizing and processing the same set of data once, with tools relevant to different enterprise IT roles. Splunk positions this as a “unified security and observability platform.”

Context

CEO Steele is taking an active role, backed with a leaner executive team after the exit of former CEO Doug Merritt in November 2021. Chief growth officer Teresa Carlson and president of products and technology Shawn Bice also left the company, and neither of these roles will be backfilled. Steele, who had been in the CEO role for two months as of .conf22, previously served as founding CEO of Proofpoint since 2002. This security influence can be seen in an increased emphasis in security functionality across Splunk’s product portfolio.

Splunk claims security functionality is important for workload observability, and that gaining visibility into whether an application is running performantly and securely draws on the same data. Security team leaders are generally not the decision makers for buying observability tools, however. While 43% influenced buying decisions, according to 451 Research’s Cloud Native, Observability survey, only 18% of security team leaders were primarily responsible for buying decisions for observability tools.

Buying Decisions for Observability Tools



Q. Who in your organization is primarily responsible for buying decisions for observability tools?

Base: All respondents, abbreviated fielding (n=217)

Source: 451 Research's Voice of the Enterprise: Cloud Native, Observability 2022

While some renewed interest in, and emphasis on, security outcomes is a likely consequence of having a CEO with a security background, planning and designing for the needs of Splunk's core constituency of IT operations professionals should remain at the forefront.

Separately, it was reported that Cisco offered $20 billion to purchase Splunk in February 2022 prior to Steele joining the company, which would have been a record-setting acquisition in the already notably M&A-heavy application and infrastructure performance monitoring (AIPM) market. For Splunk, this deal appears to be in the rearview mirror following Steele's appointment and a 7.5% stake purchased by private equity firm Hellman & Friedman in March 2022.

Strategy

Directionally, Splunk appears to be charting a course toward increasing the variety of enterprise roles/personas that its products are relevant for – expanding beyond developer and operations positions to include security practitioners, while touting the cost savings of ingesting data once in one tool, rather than relying on a multitude of vendors for different contexts or outcomes.

Splunk is also embracing developer enablement and engagement as a greater priority, casting developers as the hero, and providing the latitude to pick up the product and see outcomes from it without being bombarded by sales motions, a strategy supported by our data noted above.

Observability

Over 50 enhancements to the Splunk platform were announced and released at .conf22, notably Data Manager for Splunk Cloud Platform to provide more granular control over data ingested by Splunk. This functionality is available now for AWS and Azure, with GCP support promised for later this summer.

Ingest Actions effectively acts as a data pipelining product, providing "filtering, masking and routing" of data bound for Splunk or AWS S3 storage. For Splunk Enterprise users, SmartStore support was extended to Azure (bringing it to parity with AWS and GCP), providing cost savings by disaggregating compute from storage. Splunk claims this can reduce operating costs by up to 70% while retaining full data fidelity. These features chiefly take aim at Cribl – which, among other data pipelining offerings, is the most vocal about using pipelining to reduce Splunk bills.

Splunk Log Observer Connect enables no code visualization and analysis of log data from Splunk Cloud Platform or Splunk Enterprise, alongside the metrics, traces and events from Splunk Observability Cloud. This functionality was released to general availability for Splunk Enterprise users this January.

Federated Search was expanded as a highlight of the .conf22 keynote to allow searches to traverse Amazon S3 buckets, with additional data sources forthcoming. Federated Search, introduced in 2021, originally provided the ability to search across multiple Splunk Cloud and on-premises environments. This functionality keeps practitioners inside the Splunk interface, rather than context-switching to AWS CloudWatch to view logs generated by that service. It also acts as an additional lever for cost control, since data in external sources exposed to Federated Search is not ingested before use.

Security

Just as Splunk has been a prodigious acquirer of observability startups, significant M&A activity prior to Steele joining as CEO informs its security product portfolio. Splunk Mission Control, launched in 2019, unifies Splunk Enterprise Security, Splunk Intelligence Management (incorporating TruSTAR, acquired in 2021) and Splunk SOAR (incorporating Phantom, acquired in 2018) to offer data collection and enrichment and threat detection, as well as event triage and response.

Splunk Enterprise Security offers the functionality expected of any SIEM. It provides dashboards and reports tailored to different roles/levels in an organization, from executive summaries to practitioner-focused case summaries, as well as an overall Cloud Security dashboard, informed by data from both on-premises and multicloud environments. Splunk touts over 150 out-of-the-box detections developed by Splunk Threat Research to better inform multicloud security postures.

Security feature additions announced at .conf22 included Anomaly Detection Assistant, which aims to help security practitioners (and non-security IT personnel) identify potential problems by using ML to create queries that surface anomalies in time-series data sets. Risk-based alerting was added to Splunk Enterprise Security, which can be used to triage alerts, surfacing high-fidelity alerts and group related events, and minimizing lower-importance alerts to reduce alert fatigue in aggregate. When used in conjunction with risk-notable playbooks in Splunk SOAR, enterprises can automate containment and response tasks to security events, which can be built in a visual (low-/no-code) playbook editor.

Products

Splunk is continuing support for its traditional/on-premises product Splunk Enterprise, although the company touted the rapid release of features for Splunk Cloud, which has a release cadence of 4-6 weeks.

New at .conf22, Splunk Cloud Developer edition is intended for partners, third-party developers, and ISVs to develop applications for release on the Splunkbase app store. This free service – backed with sample data for testing purposes – could prove useful for bolstering Splunk's integration ecosystem. Similarly, Splunk Assist provides management insights previously exclusive to Splunk Cloud, for improved outcomes in security, performance and compliance.

Customers and partners

Splunk claimed a 40% increase in data ingested year over year, arriving at 1.7 PB for 2021, against which 16 million synthetic tests were run by customers. Further, it claims a total of 2,400 partners to date. Reference clients at .conf22 included New York-Presbyterian Hospital, Brazilian banking firm Nubank, payment processor Stripe, outdoor goods retailer REI, pizza franchise Papa John's, and beverage company Heineken N.V. Splunk also touted a content pack for ServiceNow; this integration was announced in late February.

Competition

Splunk's broad product portfolio puts it in competition with nearly every vendor in 451 Research's Application and Infrastructure Performance Monitoring Market Forecast, insofar as some component/product of Splunk overlaps in feature or scope with vendors pursuing APM, infrastructure monitoring, log management, real user monitoring, synthetic monitoring, event correlation, and/or alerting.

Most notably, these include New Relic Inc., Dynatrace Inc., Datadog Inc., Sumo Logic Inc., Elastic N.V., Cisco AppDynamics, IBM Corp. (chiefly Lightstep), VMware Inc. (chiefly Tanzu), Grafana, SolarWinds Corp., and startups including Mezmo (formerly LogDNA), Chronosphere and Honeycomb. Notably, Era Software and ChaosSearch are also aiming to provide cost-sensitive log management (cf. Splunk Federated Search), while Cribl targets total Splunk cost reduction acting as a data intermediary.

AWS, GCP and Azure are growing in observability features and market share, although these (and Splunk's aforementioned competitors) work with and build on top of public cloud platforms, making the relationship as much cooperative as competitive.

SWOT Analysis

STRENGTHS Splunk is well entrenched among enterprises, and is redoubling its efforts in observability through strategic M&A and support of OpenTelemetry, as well as a continuing focus on Splunk Cloud, emphasizing the benefits of SaaS.	**WEAKNESSES** Splunk retains a reputation for being expensive, despite the advances and enhancements made in rationalizing its own billing practices. Communicating these changes, as well as the fitness of Splunk for SMBs in addition to enterprises, is advisable.
OPPORTUNITIES With the security background of newly appointed CEO Gary Steele, the company is well positioned to use its established foothold in SIEM to build out broader and deeper security offerings relevant to security practitioners.	**THREATS** Splunk's recent expansion into on-call management, and ongoing expansion into security, is likely to bring it into competition with vendors that have historically been partners. Splunk is likely to face vocal competition in the markets where it plays.

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

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.