MARKET NOTE

Highlights from Splunk.conf20: Richer Cloud, Observability, ML, and Security Capabilities to Fuel Data-Driven Innovation

Archana Venkatraman

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Highlights from Splunk.conf20 Event

This IDC Market Note summarizes the key highlights from Splunk's virtual .conf20 event held in October. It assesses how Splunk is extending beyond security and IT insights to add horizontal capabilities around observability, multicloud optimization, and AIOps to help organizations put data strategy at the heart of their digital transformation and innovation.

Key Takeaways

- Splunk has enhanced its Data-to-Everything Platform with new features to improve productivity, insights, and administration for multiple personas including IT, security, and DevOps teams. It has also added cloud-native and multicloud capabilities to the core platform by giving users new ways to implement their data strategy and real-time access to data.
- Splunk has fully embraced cloud in two ways: as a way to better serve its customers through a SaaS model and as a modern digital solution platform to meet the monitoring and management needs of distributed infrastructure, services, data, and applications. This is evident in its collaboration with Google Cloud to provide a single-pane view for security and IT alerting, investigations, and monitoring to detect and remediate potential security threats. It is also fully rearchitecting its platform to make it cloud native.
- Splunk enhanced its Observability Suite with two new products, Splunk Real User Monitoring and Splunk Log Observer. It has also acquired APM vendor Plumbr, network performance monitoring vendor Flowmill, and digital experience monitoring vendor Rigor to further expand its observability portfolio and prepare for the next-generation of observability and troubleshooting needs.
- The million-dollar question for digitally transforming organizations is how to determine the right strategy for applications, cloud adoption, organization vision, and skills. The answer is data-driven insights. Splunk aims to meet this need in a dynamic hybrid multicloud world by delivering cloud capabilities across its Data-to-Everything platform and Security, IT Operations, and Observability Suites.

Source: IDC, 2020

December 2020, IDC #EUR147169320

IN THIS MARKET NOTE

This IDC Market Note summarizes the key highlights from Splunk's virtual.conf20 event held in October. At its annual summit, the vendor showcased its engineering capabilities, business road map, and its own cloud and digital business model transformation. This Market Note assesses how Splunk is extending beyond security and IT insights to add horizontal capabilities around observability, multicloud optimization, and AIOps to help organizations become data driven.

IDC'S POINT OF VIEW

If the pandemic has taught us one lesson it is that digital transformation (DX) is not just a priority — it is an imperative for business resilience, adaptability, and agile innovation. IDC estimates that by 2023, 65% of global GDP will come from products and services of digitally transformed organizations. As enterprises accelerate their DX journeys, they are increasing their investments in innovative and disruptive technologies, newer agile development methodologies, flexible/as-a-service business models, and data-driven insights.

At its.conf20 event, Splunk highlighted how its new capabilities, features, and engineering vision can help organizations succeed in their DX journeys. We look at some of the key highlights from the event in the next sections.

Expansion of Splunk's Data-to-Everything Platform

Splunk's Data-to-Everything Platform is a solution framework that combines multiple products and services to deliver unified data-driven insights. At the heart of this portfolio is the modern data platform — Splunk Enterprise and Splunk Cloud. At the event, the latest, cloud-centric Splunk Enterprise 8.1 was showcased.

The platform helps IT, security, and DevOps professionals ingest any data from any source to investigate, monitor, analyze, and act quickly on the insights. The platform's flagship capabilities include a scalable index, streaming data ingestion, sophisticated (and customizable) ML analytic models, and federated search that uses the Splunk query language for integration across Splunk data and third-party sources. In Splunk Enterprise 8.1 and across multiple Splunk Cloud releases, the vendor has introduced five key capabilities to improve user experience, access and control, performance, metrics store, and workload management. It also announced the beta launch of Splunk Operator for Kubernetes environments (a next-gen platform architecture for operating Splunk Enterprise in containers).

From a user's point of view, new capabilities make it easier to navigate searches. Other enhancements include end-to-end no-code workflows that enable ops teams to visually explore, prepare, and analyze data.

Embedding ML and Democratizing IT for Practitioners

The new Splunk Machine Learning Environment (SMLE), currently in beta in Splunk Cloud, will help organizations build and operationalize machine-learning models and algorithms to get value from data at scale in Splunk. In addition, the new Data Stream Processor 1.2 helps customers expand their data streaming capabilities to both transform and analyze data sourced from and routed across multiple cloud environments.

IDC believes that adding features that automate and simplify the ML life cycle and accelerate time to production with rapid deployment, centralized model management, and automated monitoring at scale can make analytics and data science accessible to organizations of all sizes and skills.

Cloud and Multicloud as First-Class Citizens

At.conf20, Splunk reiterated its commitment to cloud – to better serve its customers through a set of SaaS offerings and also as a growth lever for the business to provide observability services around monitoring, troubleshooting, and optimization of complex cloud environments that need to be included in an organization's data strategy. It has shifted to a cloud-centric delivery model for its entire portfolio, under which:

- A growing number of offerings, such as the Observability Suite, are available only as a service
- Other capabilities that are delivered both as a service and as customer-deployed software are delivered primarily in the as-a-service offerings; because of Splunk's cloud-first strategy for delivery model, certain capabilities are included as software product options (after they have been proven in the cloud) to meet some customers' specific on-prem needs
- Its as-a-service offerings include pricing and packaging structures aligned to cloud business models

What further lends credibility to its cloud-native strategy is its commitment to rearchitect the core Splunk Cloud platform for the cloud rather than simply adding a SaaS layer on top.

"To rebuild for the cloud, we have made 30% code changes in 12 months and write 500K+ lines of code per year," said Chief Product Officer Sendur Sellakumar. Rearchitecting the core platform for cloud has enabled Splunk to release 50 new capabilities in Splunk Cloud in 9 months, showing that it has increased the velocity and value of its services in line with cloud-native expectations.

All capabilities of Splunk Cloud are now also available on Google Cloud, providing a single-pane view for security and IT alerting, investigations, and monitoring to detect and remediate potential security threats. Users can leverage integrations with Google Cloud for monitoring and managing cloud services, containers, applications, and infrastructure.

IDC believes that with enhancements in Splunk Cloud and Splunk Enterprise, as well as deeper integration with Google Cloud, the vendor has increased its relevance in the multicloud-centric era. Cloud is the future of digital infrastructure and IDC predicts that by the end of 2021, 80% of enterprises will put a mechanism in place to shift to cloud-centric digital infrastructure twice as fast as before the pandemic.

Adding multicloud capabilities gives its users flexibility to deploy, manage, and access their data platform from anywhere. It is no surprise that in its FY21 3Q (ended October 31) its cloud revenues were up 80% YoY and cloud ARR was up 71% YoY.

IDC's research shows that 62% of organizations are committed to multicloud environments but top challenges in making multicloud journeys successful included difficulties with building common control workflow (58%), driving common security policy (55%), a lack of unified monitoring and management (55%), and application migration (50%).

In conversations with IDC, enterprises admit the complexities and management overheads of using domain-specific tools to manage multicloud environments. IDC believes Splunk, with its multicloud monitoring capabilities, has the potential to provide end-to-end visibility and data-driven insights for applications, infrastructure, and team performance.

Another highlight is the new features in Splunk's Security Operations suite to help companies derisk their cloud migration strategies and accelerate the cloud journeys. The features enable security teams to take their security operations to the cloud and modernize and unify them. Customers can plug in Splunk SIEM, SOAR, and other third-party security technologies into Splunk Mission Control for real-time, contextual visibility, control, and workflow across their entire security infrastructure.

Richer Observability Portfolio

Splunk has expanded its Observability portfolio with three key acquisitions around network performance monitoring (Flowmill), application performance monitoring (Plumbr), and digital experience monitoring (Rigor).

Plumbr offers byte code instrumentation, real user monitoring, and deep application performance insights for enterprise applications, while Rigor provides synthetics monitoring and web optimization tools to enhance user experiences in digital channels. The combination of these technologies with Splunk's existing Observability Suite can help it to provide seamless, end-to-end observability experience across hybrid multicloud environments and modern application architectures. Splunk also announced Splunk Log Observer, which brings the power of Splunk logs to site reliability engineers, DevOps engineers, and developers, while Splunk Real User Monitoring extends its monitoring capabilities to help organizations understand and optimize the digital experiences of their customers.

Conclusion: Writing the Next Chapter

It is becoming clear from these new capabilities that Splunk is aggressively investing in three key areas:

- **Expanding its Data-to-Everything vision to include modern architectures such as hybrid multicloud, cloud-native, and container environments.** As infrastructure gets distributed, so do applications and for most organizations connecting the data silos is a key priority to make informed decisions. Data processing needs are becoming complex in the dynamic, heterogeneous infrastructure and applications world. Splunk's transformation to go beyond logs to meet the data needs of new-age decision makers – including infrastructure teams, workload owners, DevOps teams, SREs, and CloudSecOps – can help establish it as the go-to data platform for all enterprise needs.
- **Embracing the cloud.** The conversations around cloud are moving from "or" to "and," and most organizations are embracing hybrid multicloud environments. As cloud becomes the de facto IT architecture of a digital enterprise, cloud is no longer just a destination – it is an experience, an operating model. Customers are evaluating cloud for all types of workloads – traditional workloads, cloud-native workloads, and even transforming workloads making hybrid multicloud a natural evolution. Challenges and blind spots in dynamic hybrid multicloud environments are inevitable, and organizations need to make a paradigm shift in how they monitor the dynamic infrastructure and use the insights to succeed in their digital initiatives.
- **Readying itself for the "observability and monitoring revolution."** IDC believes that in the dynamic cloud-native world, organizations need a unified platform that provides not just diagnostics but continuous observability of applications, data, and infrastructure assets. This is critical to ensure every aspect of IT is resilient, secure, and optimized. Splunk's new observability capabilities, along with its AIOps, ITOps, and incident response features, and the newly acquired technologies from Plumbr, Rigor, and Flowmill, are well suited for the observability revolution in the hybrid multicloud era.

Recommendations

Splunk has a strong head start in the observability space but it needs to be mindful that many vendors — be it infrastructure vendors, cloud providers, or niche APM vendors — are all moving into delivering observability capabilities. Splunk needs to keep up the momentum of innovation and continue building deeper infrastructure, SaaS, security, and application integrations to maintain its competitive edge. It should also aggressively target newer personas and teams such as cloud center of excellence teams, DataOps teams, DevOps teams, and SREs.

It is clear that many large enterprises are evaluating Splunk's platform to get visibility into their IT environment and turn that data into action. Recent customers include organizations from around the world such as Bass Pro Shops, Carvana, Clemson University, E.ON, Founders Federal Credit Union, Herbalife Nutrition, HSBC Group, Idaho National Laboratory, Intrado, James Paget University Hospitals — NHS Foundation Trust, National University of Singapore, Nu Skin, Ocado Group, Toyota Systems Corporation, and TripActions.

Businesses undergoing digital transformation are under real pressure to make sure their cloud migration, application modernization, DevOps strategies, and next-gen security architecture realize the expected business outcomes. The million-dollar question is how to determine the right strategy for your applications, your organization's vision, and your skills. The answer is data-driven insights. Data is essentially the glue for application modernization. A powerful data-driven strategy can make application modernization journeys successful.

"Digital transformation is about joining the dots and making faster, informed, and better decisions. Splunk enables us to democratize access to data," said Chris Taylor, VP of Digital Accelerator at Airbus, speaking at.conf20. Airbus has 200 data sources in the Splunk platform and has a data strategy for its IT operations, IT management, cybersecurity, operations, and business resilience.

Having tangible data to inform this journey is paramount for success. Splunk, with its Data-to-Everything vision, is well placed to ensure organizations' DX success.

LEARN MORE

Synopsis

This IDC Market Note summarizes the key highlights from Splunk's virtual.conf20 event held in October. At this annual summit, the vendor showcased its engineering capabilities, business road map, and its own cloud and digital business model transformation.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com