IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

IT Executive Focus: Splunk .conf20: Record Attendees and High Product Interest Set Up Transformational Customer Opportunities

December 09, 2020

By: Stephen Elliot

IDC's Quick Take

Splunk recently had their annual customer conference with a record 30,000 virtual attendees. There were several key product announcements at the event targeting DevOps, IT Operations, and Security, teams. In addition, the company recently released Q3FY21 financial results, reporting revenues 11% below expectations at $559m, but reporting continued strength at 80% growth in cloud revenues that reached $145m, and ARR reaching a record $2B. Finally, the company continued to grow through acquisitions, announcing Flowmill (network performance monitoring), Rigor (synthetic monitoring/optimization), and Plumbr (real user monitoring/code profiling/advanced instrumentation) to extend its Observability capabilities. The company has 444 customers with ARR of $1 million or more. Finally, customer interest in the Splunk portfolio is high, as attendee levels at the conference and with virtual demand generation events indicate.

Product Announcement Highlights

Key product announcements included:

Splunk Platform

Introduction of Splunk Machine Learning Environment and updates to the foundational technology:

- Splunk Machine Learning Environment (SMLE): SMLE is a new, dedicated solution that makes it easier to build and operationalize machine learning models and algorithms. SMLE simplifies the end-to-end machine learning lifecycle and provides faster time to production with rapid deployment, centralized model management, and automated monitoring at scale.
- Splunk Data Stream Processor 1.2 (DSP): DSP helps customers expand their data streaming capabilities for multi-cloud environments including Google Cloud and Azure Event Hub. Splunk DSP enriches data with ML functionality, minimizing compute load and making downstream searches more accurate.
- Splunk Connected Experiences: Splunk Connected Experiences updates help customers get their data insights from anywhere via Splunk AR, Splunk TV and Splunk VR.

IT Operations

- Splunk Service Intelligence for SAP solutions: Splunk Service Intelligence for SAP solutions enables existing and new ITSI customers to gain a high-level view into the health of their services, as well as a deeper dive into different incidents so they can monitor, triage, resolve and report on mission-critical business services. Splunk Service Intelligence for SAP solutions, now in controlled availability, couples the power of AI-based monitoring, with SAP technology stacks, creating end-to-end visibility across both the SAP and entire IT environment.

- Splunk IT Service Intelligence (ITSI): The latest version of Splunk IT Service Intelligence gives teams end-to-end visibility, operational efficiency and business intelligence so organizations can predict incidents before they impact customers, whether their deployment is cloud-based or on-premises. Splunk ITSI can correlate and apply ML to all data, for real-time performance monitoring, predictive analytics, intelligent alerting and integrated incident management using enhanced service monitoring dashboards to better understand business impact.
- Splunk Infrastructure Monitoring Add-On: Splunk Infrastructure Monitoring Add-On is now generally available and allows organizations to seamlessly collect and integrate Splunk Infrastructure Monitoring (formerly SignalFx Infrastructure Monitoring) metrics data with the Splunk Data-to-Everything Platform and into Splunk ITSI.

Observability

- Splunk Observability Suite: The Splunk Observability Suite brings together solutions for infrastructure monitoring, application performance monitoring, digital experience monitoring, log investigation and incident response into a single, tightly integrated suite of products. It leverages no sample streaming, full-fidelity ingestion, and sophisticated machine-learning capabilities to collect and correlate across all metric, trace, and log data in real-time.
- Splunk Log Observer: Splunk Log Observer brings Splunk logs to cloud-centric site reliability engineers, DevOps engineers and developers. Entirely cloud-based, it deploys within minutes and offers out-of-the-box integrations with popular cloud services for fast time-to-value and provides a point-and-click search for rapid log exploration. Splunk Log Observer works with Splunk Infrastructure Monitoring and Splunk Application Performance Monitoring (APM) for context-rich, unified monitoring, troubleshooting and investigation.
- Splunk Real User Monitoring: With Splunk Real User Monitoring, Splunk extends its monitoring capabilities helping organizations understand and optimize the digital experiences and user journeys of their end customers. Splunk User Monitoring leverages the same capabilities of Splunk APM with OpenTelemetry standard for data collection, NoSample full-fidelity data ingestion, real-time streaming architecture, and AI-driven analytics for directed troubleshooting.

Security

- Splunk Mission Control: Splunk Mission Control, a cloud-native, unified security operations platform that brings together security data, analytics and operations has introduced the Splunk Mission Control Plug-In Framework. This new framework allows customers to combine their Splunk security tools and non-Splunk security tools, such as endpoint security, network security, cloud security posture and threat intelligence technologies, from a common, cloud-native work surface.
- Splunk Enterprise Security and Splunk User Behavior Analytics: The newest version of Splunk's industry-defining SIEM solution - Spunk ES - now offers new, native risk-based alerts that help SOCs further refine the fidelity and priority of notable events. Splunk ES's risk-based alerting feature reduces the quantity of alerts while increasing their quality; and enables detection of complex threats.
- Splunk Phantom: New updates to Splunk's security orchestration, automation and response (SOAR) solution helps customers automate more of their security operations, allowing SOCs to scale automation. New "custom functions" in Splunk Phantom makes playbook creation and

execution faster and easier. Security analysts can reuse custom code blocks across multiple playbooks and introduce complex data objects into the playbook execution path.

IDC's Point of View

Splunk continues to expand its customer base in enterprise accounts across security, IT operations, and observability users and teams. The more recent entrance into Observability started in earnest with the announced acquisitions of SignalFX and Omnition in August and September 2019. Recent deals continue to show that Splunk can sell across teams, using specific use cases to gain access and attaching products that expand the value proposition of its platform. With the recent acquisitions in the observability pillar, selling across buying centers across the account base will involve new buyers to Splunk; examples include digital experience management teams, web application teams, and DevOps and SRE teams that require full visibility into the end user digital experience. In addition, their anchor in enterprise security and IT operations buyers must also use the same go to market strategy.

IT organizations are transforming their organizational constructs and processes; balancing both traditional and modern application architectures with Agile development practices and Dev/Sec/Ops and SRE practices. Splunk offers solutions to manage both models for on premises and SaaS delivered, while using the Platform and associated analytics models to address silo-based problems for security, operations, and observability teams. IDC continues to hear from IT executives that the compression of operational processes with development processes is a long-term journey; and tools must be able to serve both sets of buyers with contextual interfaces, easy to use technology, and extensive integrations. The role of analytics is increasingly important as the rising levels of complexity is making manual capabilities more difficult to scale in a timely fashion.

Splunk has a unique portfolio that resides on several key factors; data collection depth and high data cardinality, patented analytics capabilities, process automation and integration, business impact assessment, and cross IT team adoption spanning security, IT operations, and observability and Dev/Ops teams. Sales execution will need to focus on these buying centers, understanding and communicating each unique value proposition, and positioning the platform value for each team. Selling the notion that the sum of its parts is more valuable than singular capabilities is increasingly critical. Part of the discussion must focus on the level of process and organizational maturity for each customer to upsell solutions and determine fit. A customer journey-oriented sales focus will be a key factor in winning deals as is the need to elevate the value proposition to business outcomes that address cost containment and reduction, time to market, speed, and/or improved efficiencies that deliver better customer experiences.

The recently updated pricing model has helped customers focus on business outcomes and not as much on data ingestion; providing data tiers with clear workload pricing packages, upgrade pricing, developer licenses, and training/PS and education capabilities for both on premise and Cloud capabilities across the portfolio. In addition, a growing customer success program (called Service 360) that includes a dedicated customer success manager, ongoing coaching, and business value reviews is being well received. Customers like the improved pricing transparency and predictability, and customer support that delivers a focus on business outcomes and adoption success.

Splunk is also in some early accounts as it relates to the idea of Dev/Sec/Ops transformations; introducing the theme of application security, audit, and compliance requirements into the software development lifecycle. Most often it addresses how developers should include security such as

application scanning, vulnerability assessment at the code level, and general information access and collaboration before production into the SDLC. It's still early, but some financial services, healthcare, and retailers are investing into this idea. These solutions must be easy to use and integrated into existing development processes (i.e. CI/CD), while driving more collaboration across teams. IT executives often ask how a technology can make these processes faster, easier, and more efficient.

IT Executive Recommendations

- Have a clear understanding of how the Splunk platform plays a role in applying analytics across the product suites and identify the types of models that best fit the business challenge and objectives. Discuss patents and where they are applied in analytic models, and what they address.
- Consider the on-ramps for observability solutions for DevOps and Dev/Sec/Ops use cases; different stakeholders across website or digital ownership, operations, security, and development should be brought in to consider end to end solutions.
- Executives should consider the focus on IT Operations transformation and its intersection points with security and DevOps teams and tools; improving business outcomes like customer experience, time to market, NPS, and cost reduction are important metrics to define early.
- Customers continue to migrate from on-premise to Cloud based Splunk solutions. For these customers, consider buying implementation and migration blueprints and frameworks to speed deployment and adoption.

Subscriptions Covered:
Cloud Management Software, Enterprise System Management Software, IT Service Management and Client Virtualization Software, Software-Defined Compute