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

Splunk.conf22 Presents Vision for Security and Observability Platform: Key Customer Opportunities

June 29, 2022

By: Katie Norton, Jevin Jensen, Stephen Elliot

IDC's Quick Take

At its annual user conference, .conf22, Splunk introduced new capabilities and feature enhancements across its security, observability, and platform capabilities, focusing on ease of use, scalability, analytics, and adoption expansion. The cadre of announcements suggests Splunk product and engineering teams have made advancements across its portfolio, notably observability, whereby there is continued progress on ease of use and integration of capabilities and data sources to drive faster problem identification and resolution cycle times across teams at various stages of maturation.

Event Highlights

- .conf22 was held in person in Las Vegas, NV and virtually from June 14-16, 2022. Conference attendance was over 13,000 in total, with around 5,000 attending in person. The conference was also the first for Gary Steele, Splunk's new president and CEO.
- Among the new capabilities and features announced by Splunk for both the Splunk Cloud Platform and Splunk Enterprise 9.0 (announced as generally available at.conf22) are:
- Data Manager for Splunk Cloud Platform simplifies the data onboarding experience and provides a hybrid cloud control plane of data flowing into Splunk for Amazon Web Services and Microsoft Azure today, with Google Cloud Platform support available later this summer.
- Ingest Actions allows users to author, preview, and deploy transformation rules at ingest-time including filtering, masking, and routing within the Splunk Platform or to external Amazon S3 storage.
- Splunk Log Observer Connect enables no code visualization and analysis of logs from Splunk Cloud Platform or Splunk Enterprise alongside the metrics and traces from Splunk Observability Cloud
- Edge Processor (in preview) for filtering and masking data at the edge before routing it to Splunk Enterprise, Splunk Cloud, and Amazon S3.
- Synthetic Monitoring is now fully integrated into Splunk Observability Cloud in preview.
- Splunk Incident Intelligence, in preview, is a new team-based event and incident management solution integrated into Splunk Observability Cloud.
- Federated Search is expanded to support search of non-Splunk data, with the addition of searching Amazon S3 buckets in preview.
- A new fully managed cloud service within Splunk Enterprise 9.0, Splunk Assist, allows customers to monitor the security of their Splunk instances, leveraging insights from cloud deployments for recommendations.
- Anomaly Detection Assistant app for Splunk, in beta, uses machine learning to create queries for identifying anomalies in time-series datasets.
- Automated zero trust is now enabled through risk-based alerting in Splunk Enterprise Security, combined with risk-notable playbooks from Splunk SOAR.

- Splunk Cloud Developer Edition, in preview, lets developers create and test their applications being built on, for, or with the Splunk Cloud Platform.

IDC's Point of View

Most of the announcements coming out of.conf22 demonstrate the work Splunk has done over the last year around ease of use, analytics, and integration driving cohesion and faster adoption across its portfolio. The announcements also acknowledge that Splunk customers will continue to be an array of both on-premise and cloud-based hybrid environments.

Splunk's current customer base across security and operations teams provides a foundation where enterprises can build and innovate with speed and agility across common problem, change, and incident management processes that span various teams and disciplines. An outcomes-based, use case approach focused on business value and identifying key metrics that support speed and resiliency are critical to Splunk's customer expansion.

Splunk believes it is uniquely positioned to deliver unified security and observability in an increasingly integrated set of solutions while meeting customers where they are: on-premises, hybrid, cloud, or multi-cloud. Splunk aims to see and ingest data at all layers in a multi-cloud era, including the application, infrastructure, security information and event management/security orchestration automation response (SIEM/SOAR), and other cybersecurity data layers. With its new Data Manager, Splunk promises to be entirely agnostic to future data sources. Customers told IDC they would be in hybrid and multi-cloud models for years to come, so Splunk's approach makes sense.

Splunk's end-to-end visibility and holistic, analytics-based approach to monitoring the entire application and infrastructure stack should reduce troubleshooting and root cause analysis time. Splunk is well known for its Federated Search, which has been further enhanced to make visibility even easier to obtain by searching and analyzing non-Splunk-related data sources.

The importance of a shared data set was confirmed by Sarika Attal, a 14-year veteran of Papa John's Pizza and vice president of enterprise architecture and technology services. Ms. Attal stated, "In the early stages of an incident, it is difficult to say if it's a security issue or operational outage. Having a shared data set (observability and security) helps us understand the root cause."

Additionally, artificial intelligence and machine learning (AI/ML) are playing an increasingly important role across Splunk's platform. Splunk expanding use of AI/ML aims to optimize the enormous scale of data many of its customers ingest. By filtering out the repetitive, known, or other 'noise' data from the Splunk dashboards, customers can more quickly find actual incidents and resolve them sooner. In addition, AI/ML can spot new or anomalous data in a sea of 'normal' data, ensuring operations teams can prioritize incidents more efficiently.

Synthetics monitoring continues to be a component of any observability strategy. Splunk Synthetic Monitoring, a capability added through the October 2020 acquisition of Rigor, was announced as now fully integrated into Splunk Observability Cloud. Splunk is no stranger to adding capabilities through acquisitions. IDC's Decoding DevOps Market Merger and Acquisition Activity, 2011–2021 identified Splunk among 17 vendors that completed ten or more mergers or acquisitions over the 11 years tracked (IDC #US48994922, April 2022). A growth-by-acquisition strategy can effectively obtain new capabilities and talent, increase market share and assets, and facilitate access to capital and new markets, often

faster than organic growth. But acquired technology can be challenging to integrate. As Splunk continues to pursue a unified observability and security platform, full integration of new products such as Synthetic Monitoring becomes increasingly important.

Splunk Incident Intelligence further reflects the company's recognition of the importance of integration across its platform. Currently in preview, Incident Intelligence is the company's next generation event and incident response product that is integrated natively with Splunk Observability Cloud. Splunk already has an incident response tool in Splunk On-Call (a capability added from the acquisition of VictorOps in 2018). This solution provides a migration path for customers using Splunk On-Call and continues the market compression between event and incident response processes.

The surface area and complexity of infrastructure to be monitored and secured have exploded as cloud-native application models gain traction. An IDC survey identified mapping and fixing relationships between services and data as the top challenge for software development and delivery organizations regarding the observability of containers and microservices operations (see U.S. Accelerated Application Delivery Survey, IDC #US47924622, January 2022).

Log Observer Connect acknowledges multi-cloud infrastructure's complexity by bringing log data from Splunk Enterprise or Splunk Cloud into a single Observability Cloud interface alongside metrics and traces for a complete Observability data set, providing a comprehensive view and the context needed to fix issues more quickly. IDC sees this feature as key for Splunk as they continue to increase their product adoption by developers, SREs, and DevOps teams who can benefit from seeing the impact changes to their application are having in production. Teams operating with the "you build it, you run it" mantra need contextual telemetry data to make decisions around the building and troubleshooting their applications. The no-code interface is also critical in making the feature easy to adopt by personas who may not be avid users of Splunk Enterprise or Splunk Cloud Platform.

IT Executive Recommendations

- Existing Splunk customers should evaluate the latest features of version 9.0. Splunk Cloud Platform will automatically receive this newest version soon. Splunk Enterprise customers running on-premises will need to assess the timing and benefit of upgrades to their business, especially the new Data Manager and Federated Search.
- Many customers at.conf22 who migrated to the Splunk Cloud Platform noted they had also migrated to the workload pricing model, which moves away from data ingest-type licenses and gives customers great flexibility to import more and varied data. Enterprises should consider this licensing model to grow complete observability visibility.
- Customers of Splunk using only security without an observability solution should evaluate Splunk's Observability Cloud. Customers looking to consolidate tools may benefit from bringing these large data sets together.
- Open source, specifically OpenTelemetry, is becoming the default way to collect a full stack of digital experience, application infrastructure, and observability data. Regardless of which observability solution an enterprise selects, they should ensure it supports OpenTelemetry at a minimum. Among other ease of deployment features, Splunk's distribution of OpenTelemetry also adds the ability to instrument a JAVA application without requiring developer changes.
- On-premises Splunk Enterprise customers should evaluate migrating to the Splunk Cloud Platform. Splunk's Cloud Migration Assessment (SCMA) app is a free tool to assist the on-

premises customer in migrating to their cloud offering. Splunk professional services are also available for an additional fee.

- Customers should consider their relationship with Splunk, specifically on moving from a transactional relationship to a strategic platform relationship that utilizes the solution set to drive business returns on speed, time to market, and resiliency. Work with Splunk to create a bridge across teams working on related challenges (i.e., Security and Operations).

Subscriptions Covered:

DevOps Analytics, Practices and Automation, Enterprise System Management Observability and AIOps Software, Intelligent CloudOps Markets and Opportunities