



Data curation remains Splunk's "Mission Control" and its central value statement, as it expands to the hybrid cloud

June 27, 2022

By: [Michelle Abraham](#), [Christopher Kissel](#)

IDC's Quick Take

Splunk held its first in person annual user conference since 2019 from June 13-16, 2022. Several new platform announcements were made that will be helpful to Splunk Security customers and fit Splunk's philosophy of "no data left behind."

Event Highlights

Splunk .conf22 can be viewed as something of a stabilizing effect for Splunk the company. Splunk has two relatively new important C-level executives—in July 2021, Splunk hired Garth Fort to be its Senior Vice President and Chief Product Officer, and on April 1, 2022, Gary Steele was brought on to be its CEO.

Splunk is also at the tail-end of two large company initiatives. Since late 2019, Splunk has actively encouraged its customer base to move from enterprise licensing to software-as-a-service (SaaS)/workload-based model. The transition from enterprise licensing is aptly named the 'valley of death' and Splunk has transitioned the vast majority to the more favorable SaaS model. Additionally, in May 2021, Splunk acquired TruSTAR which helped with cloud-native visibility and threat detection. For Splunk, the challenge was to create a mesh for Splunk tools, Splunk SOAR and TruSTAR capabilities and these platforms now have a common architecture.

Even as things change, one important fundamental defines Splunk at its root. The company was founded on the idea that a customer can throw unstructured data at Splunk and its platforms and derive contextualized data and meaningful business analysis. And, as a corollary, the quality of search is the soul of security information and event management (SIEM). Splunk made several announcements about additions to Splunk Enterprise 9.0, new search capabilities, and expansion to visibility in storage to help organizations achieve resilience across Security and IT infrastructures.

Customers were excited about the expanded Federated Search capability for hybrid cloud environments and for AWS S3 storage (currently in preview) making it easier to search across cloud and on-premises storage, allowing customers to keep data where it makes most sense economically while still allowing it to be searched for investigations and threat hunting from a single pane of glass without the need to ingest it into Splunk. Splunk plans to add other data storage options in the future.

SmartStore has been expanded beyond AWS to Azure, offering customers the ability to cache data in native Azure blob storage while still helping customers save money on data storage or ingest cost, giving more options for data they want to keep in case it is needed. SmartStore saves customers money and offers assurance with this "just in case" data storage option for data that is not regularly part of a threat detection workflow.

Ingest Actions enables the routing and filtering of data to a predetermined location either in the Splunk Platform, AWS S3 storage, and other customer storage options. Security practitioners can decide if an

entire dataset should be ingested into Splunk to be correlated and analyzed now or if should be stored for later potential investigations. Rules may be set to filter or mask sensitive data, or forward critical parts of the log data to one place while other, less critical items can be stored elsewhere.

Splunk SURGe is the initiative developed to support security teams during the initial incident review of emerging threats (we note its great tagline ‘a blue collar for the blue team’). In talking with Ryan Kovar leader of SURGe, IDC learned that our idea of what happens in a ransomware attack is different from what we initially thought. Ostensibly, a Lockbit 2.0 attack may infect (encrypt) every file in a midsized company within 4 minutes of detonation. Ransomware would seem to be hit it and get it. However, generally attackers have dwell time on the network of at least a week before initiating an attack, so security teams have more time to detect ransomware before encryption than after that process has started.

IDC's Point of View

From IDC’s SOC tools survey from November 2021, the most important feature when considering a SIEM platform is to work with data stored in many locations according to 25.9% of respondents. Federated search will answer this need as more and more storage options are added by Splunk.

One of the top challenges for survey respondents is that ingesting all data into the SIEM makes it too expensive. Splunk’s workload pricing helps as well as SmartStore and Ingest Actions allowing customers to take advantage of lower cost storage options elsewhere to save data they do not need now but may in the future. It eliminates the need to choose what to save and what to throw away.

Providing more options for data storage also helps customers meet data and privacy regulations in place today as well as those that may be important in the future.

Naturally, IDC asked about eXtended Detection and Response (XDR) and what it meant to Splunk. XDR is a potential competitive threat to SIEM and to Splunk. On its upside, XDR will combine the fast detections from endpoint detection and response, with log management, threat intelligence, and with SOAR as a lithe integrated platform. On the downside of XDR, if too many technologies are integrated, it too could become bogged down. In truth, Splunk took the longer attitude that if it were executing on its partnerships, its platforms, its DevOps strategies, its Splunkbase app store, and its Mission Control (the dashboard and the workflows within it), Splunk would be fine. Splunk considers XDR to be one of the many tools to feed into its SIEM giving broader visibility across an organization’s entire security ecosystem.

Data is the DNA of Splunk, but the term data is evolving. If we thought about data as recently as five years ago, in general, we were thinking about on-premises, networking logs, and flatter security architectures. The game is changing. Data residency requirements must be considered. New key management schema means that data in transit cannot be monitored in real-time (at least as full packets) and insights need to be derived from data lakes. By manner of speaking, data lakes themselves can be useful for individual companies to curate, index, and configure to prove compliance, streamline business use cases, and observe the efficacy of its zero-trust policies. The need for quick telemetry from data will be at the heart of 5G technologies. The ballyhooed convergence of IT and Operational Technology (OT) is complicated because OT often has proprietary languages and protocols.

Splunk seems in tune with these paradigms. Insights must lead to business outcomes, security, and also IT outcomes. Configuring the network and developing the right access policies is an ongoing battle. However, the network exists to host data, and data drive applications. Blue blazers never go out of style, and the fine detail work of data curation for observability and security remains noble work.

Subscriptions Covered:

[SIEM, Vulnerability Management and Compliance, Tier 2 SOC Analytics](#)

Please contact the IDC Hotline at 800.343.4952, ext.7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC or Industry Insights service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices. Copyright 2022 IDC. Reproduction is forbidden unless authorized. All rights reserved.