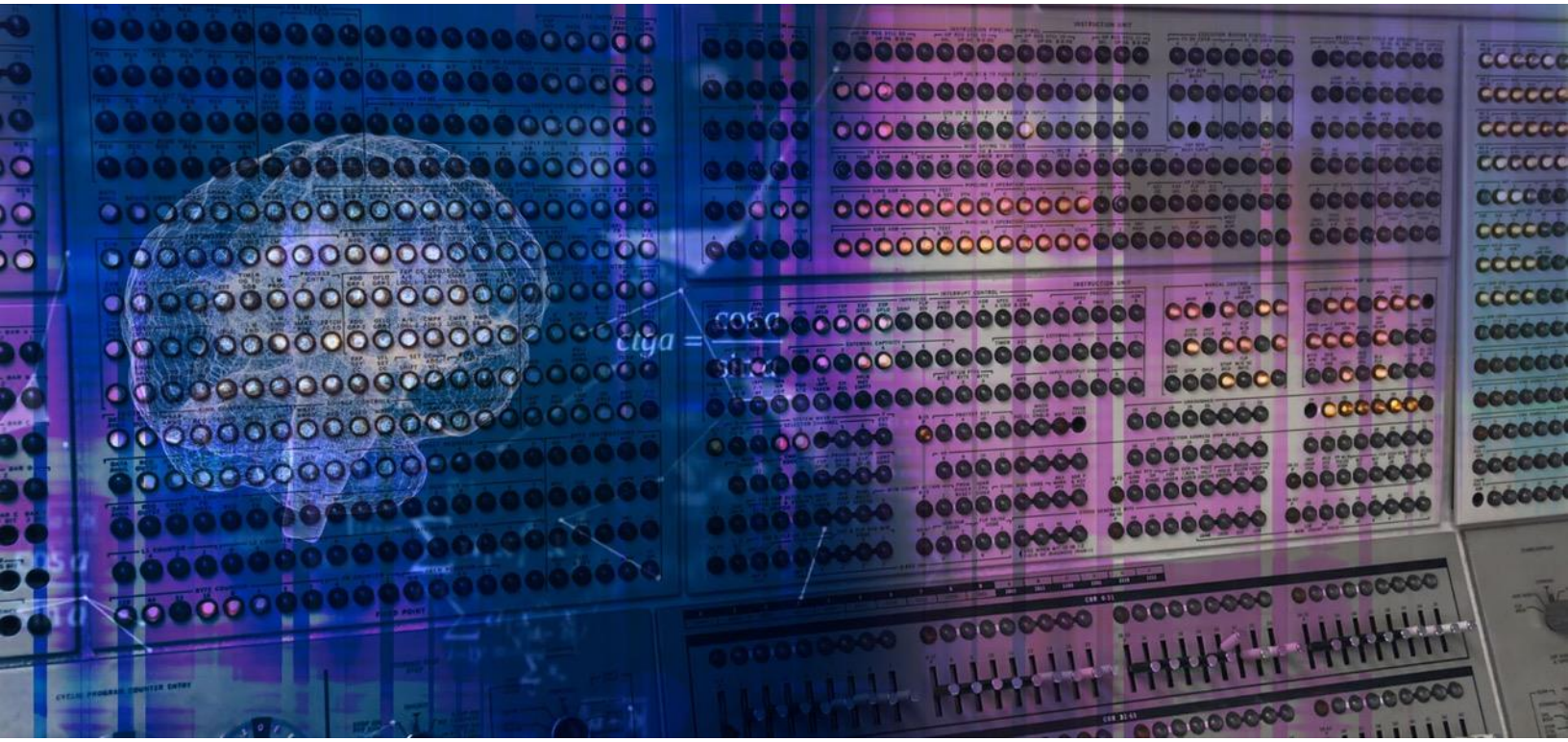

BrainBlog

Splunk: Combining Full Stack Observability and Cybersecurity for Today's Hybrid Organizations

Jason Bloomberg

President, Intellyx

June 2022

The Splunk annual .conf customer conference returned to the Las Vegas strip in June 2022 after two years virtual. The five thousand-strong, fully vaccinated, largely unmasked crowd underscored the fact that big tech conferences are roaring back.

Today, Splunk offers a cloud-centric data platform that provides the end-to-end data that both ops and security people need to manage IT performance and cybersecurity threats, respectively.

For Splunk old-timers and newbies alike, the company has transformed its approach to the enterprise marketplace. From its cloud platform to its revamped pricing model to the strategic synergies across IT ops, DevOps and cybersecurity, Splunk has reinvented itself for the digital era.

The Kinder, Gentler Splunk

After getting its start in the log management business, Splunk has spent several years rounding out its offering for IT operations, DevOps and cybersecurity personnel.

After getting its start in the log management business, Splunk has spent several years rounding out its offering for IT operations, DevOps and cybersecurity personnel. Revamping its pricing model, however, has proven to be an essential component of the company's transformation.

Revamping its pricing model, however, has proven to be an essential component of the company's transformation.

For most of its history, Splunk offered on-premises technology and charged for it via 'ingest pricing' – that is, pricing based upon the volume quantity of telemetry data customers wished to process and store.

This 'more data, more money' approach forced customers to make decisions about what and how many data they'd feed into Splunk, thus facing a tradeoff between the business value in the data with the expense of using the product.

Splunk expanded its pricing model to workload-based pricing in 2021. Customers are now finding that they are far more comfortable leveraging Splunk with more of their data. "Customers should be leveraging all their data," explains Spiros Xanthos, Senior Vice President and General Manager of Observability for Splunk. "They shouldn't be thinking that they can't use data because they can't afford to."

Splunk has also recently combined its on-premises and cloud-based offerings into a unified platform for customers managing the complexity of hybrid cloud environments. Shifting its emphasis to the cloud works hand-in-hand with the new pricing model, as cloud providers are able to take on much of the responsibility for storing data while Splunk focuses on the analytics applied to the data for security, IT and DevOps.

Leveraging the leading clouds to store large data sets leverages their immense efficiencies of scale – a no-brainer for today's cloud-centric enterprises. Amazon S3 is particularly well-suited for this purpose, and Splunk's improved Federated Search capabilities can now search across hybrid data stores that include S3 in the mix.

Leadership from Logs to Observability

Splunk has been so well established as a log management leader that the company risked being typecast in the role. To avoid this pitfall, it has successfully expanded its IT ops focus to the full breadth of the modern DevOps observability story, adding metrics and traces to its focus on log files.

Splunk's ability to provide end-to-end visibility across complex, hybrid IT landscapes, combined with its leadership in the open-source Open Telemetry project, give credence to Splunk's position as an observability leader.

Splunk positions its observability offerings as 'full stack,' as they include infrastructure monitoring, application performance monitoring, and AIOps. Furthermore, these tools work across hybrid IT, from legacy applications and systems to cloud-based services to cloud native, microservices-based applications running on Kubernetes.

Splunk positions its observability offerings as 'full stack,' as they include infrastructure monitoring, application performance monitoring, and AIOps. Furthermore, these tools work across hybrid IT, from legacy applications and systems to cloud-based services to cloud native, microservices-based applications running on Kubernetes.

Bringing Security and Observability Together

While the roles and challenges of IT operations, DevOps and cybersecurity professionals are different, they can all benefit from full visibility into the observability data that Splunk collects, processes, and displays.

For Splunk, however, more than data connects the ops and security worlds. Fundamentally, both teams are responsible for managing risk: ops people dealing with availability and reliability risks, and the security team focusing on cyber threats.

Splunk leverages its observability capabilities combined with industry standard risk frameworks to create a risk index for each cybersecurity issue. This risk-based alerting approach not only quantifies cybersecurity risks, but it also automatically prioritizes them.

This automatic prioritization of risk is also an important tool in an IT operator's toolbelt. Chasing down and fixing every single issue in the production environment would be too costly and time-consuming. Instead, operators must prioritize issues by the risk they present to their organization, just as security analysts do.

Splunk's end-to-end visibility, therefore, empowers both the ops and cybersecurity teams to leverage the same data sets to accomplish corresponding business goals: measuring and prioritizing the risk to the organization in order to determine the right course of action for any issue that presents itself.

The Intellyx Take

Bringing observability and security together into one holistic set of tools helps Splunk customers raise the technical focus of IT ops, DevOps and cybersecurity personnel to a broader business concern for managing risk.

Many Splunk customers are taking this business context one step further, where line-of-business personnel are leveraging Splunk insights to better manage their businesses overall.

This increased business focus is especially important for those digital organizations who have long since realized that while software empowers their business, data are the currency that delivers value to customers.

About the Author: Jason Bloomberg

Jason Bloomberg is a leading IT industry analyst, author, keynote speaker, and globally recognized expert on multiple disruptive trends in enterprise technology and digital transformation.

He is founder and president of Digital Transformation analyst firm Intellyx. He is a leading social amplifier in Onalytica's Who's Who in Cloud? For 2022, and he is ranked among the top nine low-code analysts on the Influencer50 Low-Code50 Study for 2019, #5 on Onalytica's list of top Digital Transformation influencers for 2018, and #15 on Jax's list of top DevOps influencers for 2017.

Mr. Bloomberg is the author or coauthor of five books, including *Low-Code for Dummies*, published in 2019.

About Splunk

Splunk Inc. (NASDAQ: SPLK) helps organizations around the world turn data into doing. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale.