



Splunk Mission Control Takes Off, Supercharging the Security Operations Center

October 22, 2019

New Splunk Security Solutions Help the SOC Turn Data into Business Outcomes

SAN FRANCISCO & LAS VEGAS--(BUSINESS WIRE)--Oct. 22, 2019-- .conf19 – [Splunk Inc.](#) (NASDAQ: SPLK), provider of the Data-to-Everything Platform, today announced new innovations across its Security Operations Suite to modernize and unify the Security Operations Center (SOC). Anchored by the newly launched [Splunk@ Mission Control](#), the Splunk Security Operations Suite makes it easier than ever for security analysts to turn data into doing by managing security across the entire threat lifecycle.

Security analysts around the world are under greater pressure than ever before to investigate, monitor, analyze and act on security threats with data. Splunk Mission Control is a new, cloud solution that connects Splunk SIEM (Splunk Enterprise Security), SOAR (Splunk Phantom) and UEBA (Splunk UBA) products into a single unified analyst experience. Combined, these powerful innovations form the Splunk Security Operations Suite, which allows customers to act on threats and other high-priority security issues through the entire event lifecycle.

With Splunk Mission Control, customers gain a new, unified SOC experience that supports investigation and search across multiple on-premises and cloud-based Splunk Enterprise and Splunk Enterprise Security instances, ChatOps collaboration, case management and automated response, all from a common work surface. This industry-first combination helps to boost productivity and increase efficiency, particularly for customers using hybrid on-premise and cloud-based infrastructures.

“For decades, security analysts have been struggling to keep up with the rising volume of data to help them fight back against emerging cyber threats that can cripple businesses, disrupt governments and impact customer privacy. Today, the industry has grown to recognize that the answers are often sitting right in front of them, within their data,” said Haiyan Song, Senior Vice President and General Manager of Security Markets, Splunk. “Splunk is proud to launch Mission Control to help our customers bring data to every question, decision and action within the SOC, allowing them to dramatically improve the analyst experience and modernize security operations.”

“Starbucks’ security operations team is responsible to defend its customers, partners and the Starbucks brand. Our success is directly dependent on the ability for our team to respond and remediate threats at machine speed,” said Atom Coffman, Manager of Cyber Security Operations, Starbucks. “Leveraging Splunk as a part of Starbucks’ SOC, we are able to automate action and pre-built orchestration workflows, all from one central platform.”

Splunk’s Security Operations Suite Redefines The Analyst Experience

As the volume of security-relevant data continues to grow, so will the importance of technologies that can automate and respond to that data in real-time. In front of a capacity crowd of 11,000 customers and partners at its annual user conference, Splunk also introduced several significant updates across its security portfolio, designed to create the strongest analyst experience and enable detection, defense and action on threats at machine speed:

- **[Splunk Enterprise Security \(ES\) 6.0](#)**: The latest version of Splunk’s flagship security offering, Splunk ES, builds upon its industry-leading SIEM platform. Splunk ES 6.0 introduces new and improved asset and identity framework enhancements, which improves scalability and performance; delivers analytics reporting on investigations; provides out-of-the-box reports of key security metrics; and offers a new integration with Splunk’s Machine Learning Toolkit.
- **[Splunk User Behavior Analytics \(UBA\) 5.0](#)**: Splunk UBA enables SOC teams to build advanced, customized Machine Learning (ML) models for baselining and tracking deviations, based on their security environment and use cases. With Splunk UBA 5.0, customers gain access to new custom use case frameworks, which helps SOC’s build advanced ML models. Splunk UBA 5.0 also introduces new High Availability/Disaster Recovery capabilities and improved device management.
- **[Splunk Phantom 4.6](#)**: Splunk Phantom brings the power of security orchestration, automation and response (SOAR) to your mobile phone. Phantom on Splunk Mobile allows customers to automate repetitive, manual tasks from the palm of their hand, enabling analysts to focus on mission-critical security threats that fuel security operations. Splunk Phantom 4.6 also introduces new open source integration apps, giving developers easy access to Phantom’s source code to extend SOAR to the unique needs of every individual SOC. Find out more about Phantom’s [new user-based pricing](#) on the Splunk website.
- **And More**: Splunk also announced today several new security apps and updates to [Splunk ES Content Update](#), which delivers pre-packaged Security Content to Splunk ES customers. Updates include Splunk Analytics Story Preview, a new Splunkbase app; Cloud Infrastructure Security, new security content which analyzes cloud infrastructure environments; and new open source content, including over 30 new open sourced apps for Splunk Phantom.

“Deploying and scaling a cyber analytics platform is a journey,” said Brent Conran, Chief Information Security Officer, Intel. “We built a new platform based on Splunk and Kafka, and modernized our tools. With the data in the right place and reskilling of our people, we reduced our technical debt and created a force multiplier. Now, we are using machine learning to significantly increase the depth and speed of our cyber intelligence.”

Splunk Mission Control is in beta for early access customers, with general availability coming in the near future. New versions of Splunk ES, Splunk UBA and Splunk Phantom are available today. For more information about [Splunk's Security Operations Suite](#) and how you can turn data into doing, visit the Splunk website.

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

View source version on businesswire.com: <https://www.businesswire.com/news/home/20191022005465/en/>

Source: Splunk Inc.

For more information, please contact:

Media Contact

Bill Bode
Splunk Inc.
press@splunk.com

Investor Contact

Ken Tinsley
Splunk Inc.
ir@splunk.com