Splunk Security Accelerates Detection and Response with Analytics-Fueled, Automation-Driven and Cloud-Delivered Solutions

October 19, 2021

Splunk Keeps Organizations Secure as Their Cloud Adoption Migration Expands Attack Surface

SAN FRANCISCO & .conf21--(BUSINESS WIRE)--Oct. 19, 2021-- Splunk Inc. (NASDAQ: SPLK), a data platform leader, today announced a series of new product innovations designed to help organizations securely embrace digital transformation by providing the security visibility needed to accelerate time to detection, investigation and response. Led by new enhancements to Splunk Security Cloud and Splunk SOAR, Splunk provides organizations a comprehensive Security Operations Center (SOC) platform with industry-leading intelligence, analytics and automation.

Enterprise security leaders are in the midst of massive digital transformation, which was further accelerated over the last year due to the scale of remote work and cloud computing adoption. At the same time, organizations are confronted with a continuously evolving threat landscape. Many security products are not designed to integrate with one another, so maintaining end-to-end visibility across on-premise, hybrid and cloud environments can be too complex for security teams to handle, which leads to blind spots that attackers can exploit. As a result, SOC's may struggle to quickly detect, investigate and respond to cyberattacks. To address these challenges, Splunk provides an extensive cloud-delivered SOC platform, which is fueled by analytics and driven by automation. With Splunk, organizations can conquer complexity, and defend against threats all the while securely enabling innovation.

"Digital transformation is a top priority for all organizations," said Jane Wong, Vice President of Product Management, Security at Splunk. "However, many security teams lack visibility across their cloud environments, are overwhelmed by alerts and manual tasks and use too many disparate tools. With Splunk, security teams can detect and respond to threats faster, effectively keeping their organizations more secure in the face of an ever-evolving attack surface."

In the face of an ever-expanding array of security tools, technology partnerships continue to be integral to delivering positive security outcomes for organizations. Splunk strengthens customer success through more than 2,400 partner integrations, including Mandiant for enhanced SOC effectiveness , Zscaler for end-to-end zero trust and DTEX for insider threats.

"As global cyberattacks emerge, organizations must have confidence in their ability to detect and respond," said Kevin Mandia, CEO of Mandiant. "Mandiant Incident Responders are on the frontlines and often see emerging threats first. Through our partnership with Splunk, customers have the ability to validate their controls and security operations program to determine how they would fare against a given adversary. In addition, Splunk customers have access to threat intelligence that is backed by Mandiant research, which improves detections in Splunk Enterprise Security."

Splunk Provides End-to-Visibility for Comprehensive Threat Detection

As cloud migration continues, security teams must focus on reducing their time to detect threats to keep their organizations running securely and compliant. With Splunk Security Cloud, coming soon, customers will have access to new, rich visualizations that allow senior leaders to see key metrics and insights into the overall health of their organization's security program. Additionally, Risk-Based Alerting (RBA) enhances threat detection abilities, reduces alert volume, and improves alert prioritization to help drive better outcomes in the SOC.

"At VMware we take a proactive approach to security monitoring, so we require a high level of confidence in our detections along with the context to focus our efforts where it matters most," said Matt Snyder, Advanced Security Analytics Program Lead at VMware. "Splunk's solutions help us reduce false positives, quickly deploy new alerting and take action on the most critical threats."

"Over the last year, our manufacturing clients have faced unique, evolving security challenges," said Kyle Miller, Director at Booz Allen Hamilton and a leader in the firm's Commercial Operational Technology Cybersecurity practice. "Simply put, the manufacturing industry is changing quickly and the sector requires radically new automation, communications and analytics capabilities. With Splunk's security solutions, we have been able to scale our data sources and reduce alert fatigue, allowing our customers to prioritize the alerts that are actionable. Our manufacturing clients can now detect threats earlier and faster than ever before."

Splunk Enhances User Productivity and Increases the Speed of Response with Automation

When seconds can count against a fast-moving adversary, the response to security alerts must be as close to immediate as possible. In August, Splunk SOAR launched an updated visual playbook editor. This feature made it easier to create, edit, implement and scale automated playbooks to help businesses eliminate manual security tasks, and respond to security incidents at machine speed.

Today, Splunk is releasing a new Splunk SOAR App Editor, which provides a new way to edit, test, and create SOAR apps. This provides easy integration and automation between Splunk SOAR and commonly used third-party tools. Furthermore, there are more than 350 Splunk SOAR apps now available on Splunkbase, Splunk's extensive ecosystem of partner and community-built technical integrations, which provides customers with a one-stop shop to extend the power of SOAR.

Outsmart Tomorrow's Threats with the Best Intelligence and Research

Splunk is providing new, additional sources of intelligence to identify threats faster to better secure the enterprise. Following the acquisition of TruSTAR earlier this year, Splunk considerably expanded its intelligence marketplace sources. Today, Splunk announced that TruSTAR is now Splunk Intelligence Management, which enables customers to operationalize all sources of security intelligence across their ecosystem of teams, tools and

partners, and directly delivers insights into Splunk Enterprise Security and Splunk SOAR.

In addition, Splunk has launched SURGe, an elite team of cybersecurity experts that will provide technical guidance during high-profile, time-sensitive cyberattacks. This team is dedicated to researching, responding, and educating on the threats that impact the world. As a trusted advisor, SURGe offers further support to security teams with response guides and in-depth analyses in the form of research papers and webinars. Organizations can rely on SURGe to provide appropriate context and timely recommendations so they can navigate global security incidents with confidence and intelligence.

"SURGe is your partner during high profile security incidents," said Ryan Kovar, Distinguished Security Strategist at Splunk. "In the face of new cyberattacks, like Kaseya or SolarWinds, SURGe empowers blue teams by providing contextual awareness. We're here to provide details like who is behind a major cyberattack, details on the techniques being used and its implementation. We'll also show you how to apply our trusted security research in your response workflow so that you can quickly identify exploits and act on it."

Today, SURGe published their inaugural SURGe research paper, which explores several methodologies for identifying potential abnormal SSL/TLS communications specifically around supply chain compromise using multiple Splunk commands and queries and open source data sources.

For more information on .conf21 announcements, visit the Splunk .conf21 website.

Safe Harbor Statement

This press release contains forward-looking statements that involve risks and uncertainties, including statements regarding Splunk's security products and services, including Splunk Security Cloud, Splunk SOAR, Splunk Intelligence Management and SURGe, cybersecurity, and information about Splunk's roadmap outlines and general product direction. We undertake no obligation either to develop the features or functionalities described (in preview or beta, which are used interchangeably) or to include any such feature or functionality in a future release. There are a significant number of factors that could cause actual results to differ materially from statements made in this press release, including: risks associated with Splunk's rapid growth, particularly outside of the United States; Splunk's inability to realize value from its significant investments in the company's business, including product and service innovations and through acquisitions; Splunk's shift from sales of licenses to sales of cloud services which impacts the timing of revenue and margins; a shift from generally invoicing multi-year contracts upfront to invoicing on an annual basis, which impacts cash collections; Splunk's transition to a multi-product software and services business; Splunk's inability to successfully integrate acquired businesses and technologies; Splunk's inability to service its debt obligations or other adverse effects related to the company's convertible notes; the emergence of new COVID-19 variants such as the Delta variant, the impact of new variants such as the Delta variant and related public health measures on our business, as well as the impact of new variants such as the Delta variant on the overall economic environment, including customer buying capacity, urgency and patterns; and general market, political, economic, business and competitive market conditions.

Additional information on potential factors that could affect Splunk's financial results is included in the company's Quarterly Report on Form 10-Q for the fiscal quarter ended July 31, 2021, which is on file with the U.S. Securities and Exchange Commission ("SEC") and Splunk's other filings with the SEC. Splunk does not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

About Splunk Inc.

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.

View source version on businesswire.com: https://www.businesswire.com/news/home/20211019005375/en/

Media Contact
Emil Hanscom
Splunk Inc.
press@splunk.com

Investor Contact
Ken Tinsley
Splunk Inc.
ir@splunk.com

Source: Splunk