June 27, 2017

Splunk Introduces Splunk Insights for Ransomware

New Offering Delivers Analytics-Driven Ransomware Solution with User-based Pricing

SAN FRANCISCO--(BUSINESS WIRE)-- Splunk Inc. (NASDAQ: SPLK), provider of the leading software platform for real-time Operational Intelligence, today announced Splunk® Insights for Ransomware, a new offering that delivers organizations a complete analytics solution to manage ransomware threats. Splunk Insights for Ransomware offers Splunk Enterprise capabilities with user-based pricing and gives organizations real-time insights for proactive assessment and rapid investigation of potential ransomware threats. User-based, tiered pricing for the offering is available for organizations with up to 1000 employees*. For more information on Splunk Insights for Ransomware, please visit the Splunk website.

In today's evolving threat landscape, maintaining security posture is critical to fighting ransomware, but day-to-day security hygiene is difficult for many smaller organizations constrained by limited resources, budget and time. Splunk Insights for Ransomware is designed to help these organizations with a broad, analytics-driven approach at a low cost and from a centralized platform.

"In today's threat landscape, the definition of critical infrastructure has expanded from electricity, water and gas to include IT infrastructures. During the WannaCry response, Splunk saw the need for a cost-effective ransomware offering that delivers a centralized point of visibility into potential ransomware activities and threats," said Haiyan Song, senior vice president of security markets, Splunk. "Splunk Insights for Ransomware allows us to deliver a way for small teams to combat the big problem of malware in real time. We are proud to provide a clear path for those customers to take full advantage of Splunk solutions to protect their business from ransomware."

Splunk Customers Defending Against Ransomware

"Children's Discovery Museum, like any organization, must protect itself against ransomware and phishing/spearphishing attacks to keep our critical systems safe and in operation. To compare this to natural disasters, when WannaCry emerged, we used Splunk software to detect the ‘tsunami' of the attack, from the first waves to the water receding, before the big wave, and take action against the threat in under five minutes," said Gregg Daly, principal engineer, Children's Discovery Museum. "We use Splunk software to monitor our email and DNS security, and we've done layered behavioral and characteristics studies through Splunk software. As a result we were able to see a user notification of a suspicious attachment and quickly investigate to learn an attack was in progress. Splunk's easy-to-navigate view across all of our data, devices and applications, combined with our data-driven transport rules, enabled us to automatically defend our systems against WannaCry."

"Northwestern University uses Splunk software to help our security team detect threats so we can deliver consistent services and protect critical data for staff, faculty and students. Splunk enables us to search for threat indicators across our systems on the fly, without having to generate cumbersome reports or manually sift through data in source systems," said Tom Murphy, CISO, Northwestern University. "With Splunk our security analysts can pivot and view new sets of data from a single source as investigations evolve. In the case of WannaCry, we used statistical models and visualizations from Splunk Enterprise to maintain a comprehensive, real-time view of network activity that might be associated with ransomware, to help detect and prevent any damage from occurring."

For more information on the Splunk Insights for Ransomware offer and pricing details, please visit the Splunk website.

**The License Capacity for Splunk Enterprise for Ransomware is based on the Number of Ransomware Monitored Accounts. "Number of Ransomware Monitored Accounts" means the number of user and system accounts in Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) or any similar service that is used to authenticate users inside the network.*

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. More

than 13,000 customers in over 110 countries use Splunk solutions in the cloud and on-premises. Join millions of passionate users by trying Splunk software for free: http://www.splunk.com/free-trials.

Social Media: Twitter | LinkedIn | YouTube | Facebook

View source version on businesswire.com: http://www.businesswire.com/news/home/20170627006323/en/

Media Contact
Splunk Inc.
Jacinda Mein, 415-266-3990
jacinda@splunk.com
or
Investor Contact
Splunk Inc.
Ken Tinsley, 415-848-8476
ktinsley@splunk.com

Source: Splunk Inc.

News Provided by Acquire Media