September 28, 2016

Splunk Expands Adaptive Response Initiative to Strengthen Enterprise Security

Organizations to Demonstrate New Capabilities at .conf2016

SAN FRANCISCO & ORLANDO, Fla.--(BUSINESS WIRE)-- **.conf2016 -** Splunk Inc. (NASDAQ: SPLK), provider of the leading software platform for real-time Operational Intelligence, today announced the expansion of the Adaptive Response Initiative. The initiative, announced earlier this year, brings together leading vendors, leveraging end-to-end context and automated response to help organizations better combat advanced attacks through a unified defense. Acalvio, Anomali, Cisco, CrowdStrike, DomainTools, ForeScout, Okta, Proofpoint, Qualys, Recorded Future and Symantec have now joined the Splunk initiative, bringing together many new capabilities to enterprise security.

"More and more organizations are embracing Splunk® Enterprise Security (ES) as the nerve center of their Security Operations Center (SOC). It is important that we enable collaborative architectures so our customers can extend analytics-driven decisions across a multi-vendor security technology stack," said Haiyan Song, senior vice president of security markets, Splunk. "Splunk welcomes the new participants of the Adaptive Response Initiative and is excited to deliver the new framework in Splunk ES. This helps the security industry to work closer together while helping organizations to leverage intelligence and automation to better defend against attacks."

Advanced cyber adversaries are continuously leveraging new attack methods that span multiple domains, launching devastating attacks that often leave enterprises vulnerable. Despite advancements in security technologies, most solutions are not designed to work together out-of-the-box, making it challenging to coordinate a response. By leveraging adaptive security architecture, the Adaptive Response framework in Splunk ES provides end-to-end context and automated response across twenty of the world's leading security technologies - enabling customers to quickly detect threats and execute response.

"The pace and variety of today's cyberattacks combined with a wide range of security tools in the typical enterprise make for a daunting challenge for security professionals. For real visibility and a truly actionable approach, enterprises demand a level of multi-vendor integration across silos and tools that goes beyond the efforts of the past," said Scott Crawford, research director of Information Security, 451 Research. "The Adaptive Response capabilities in Splunk Enterprise Security provide the centerpiece of a flexible, ecosystem-driven approach to combat advanced attacks through a more coordinated, automated response."

New Participants Respond to Adaptive Response Initiative:

- **Acalvio:** "Splunk and Acalvio share a common strategic and technical vision - to help customers get precise and timely detection, and automated resolution of threats," said Ram Varadarajan, co-founder and CEO, Acalvio Technologies. "Our patented Deception 2.0 technology, when integrated with the Adaptive Response framework in Splunk ES, delivers a compelling solution to help organizations detect malicious activity quickly. We are thrilled to be working with Splunk to provide this strategically important defense technique in an efficient and cost-effective way."
- **Anomali:** "Anomali is committed to making threat intelligence actionable across customer environments. Our joint customers look to integrate threat intelligence into Splunk ES for immediate and seamless access to a wealth of information on indicators of compromise," said Asad Baheri, director of business development, Anomali. "Splunk's Adaptive Response Initiative is an ideal way to deliver this high-value information to enable customers to investigate and respond to security threats efficiently and comprehensively."
- **Cisco:** "Cisco is pleased to expand our collaboration with Splunk by coupling our integrated threat defense portfolio with Adaptive Response," said Jeff Samuels, vice president of security marketing, Cisco. "To defend against aggressive adversaries we must streamline remediation by making security simple, open and automated. By integrating Adaptive Response with Cisco's open platforms such as ISE (Identity Services Engine) and Cisco Umbrella Investigate, mutual customers have the tools to help respond to threats throughout the network and in the cloud in real time, enabling protection everywhere."
- **Crowdstrike:** "Organizations are hungry for actionable intelligence and information that can help stop breaches from advanced attackers," said Upesh Patel, vice president of business development, CrowdStrike. "We are pleased to join Splunk's Adaptive Response Initiative to help defend against cyberattacks faster than ever. Integration of CrowdStrike

Falcon with Splunk ES within the Adaptive Response framework helps provide our mutual customers the visibility and notification to respond to today's rapidly evolving threats."

- **DomainTools:** "Many organizations struggle to analyze their DNS and proxy logs. Adaptive Response changes that," said Tim Chen, CEO, DomainTools. "By combining data from DomainTools' proprietary reputation scoring engine into Splunk ES, organizations can automate alerts and take immediate action to block threats they found with DomainTools data. We're very pleased to join forces with Splunk to help provide this mutual value to our customers."
- **ForeScout:** "ForeScout is excited to join the Adaptive Response Initiative and help limit data breaches through better validated and automated response to threats such as anomalous access and compromised devices," said Rob Greer, chief marketing officer and senior vice president of products, ForeScout. "ForeScout CounterACT and Splunk ES together provide in-depth endpoint and network intelligence in a manner that can help prioritize and mitigate associated incidents and threats with automated response capabilities."
- **Okta:** "At Okta, we know that automation is essential for CXOs as data and services multiply across the enterprise," said Chuck Fontana, vice president of corporate and business development, Okta. "Joining Splunk in the Adaptive Response Initiative fits into our mission to empower enterprises to work securely. The combination of Splunk ES and Okta enables our customers to better strengthen their security posture by utilizing identity management and access data within a broader analytics-driven approach to security."
- **Proofpoint**: "At Proofpoint, we're big believers in the value of both strong ecosystem integrations and orchestrating rapid responses to security incidents," said Ryan Kalember, senior vice president of cybersecurity strategy, Proofpoint. "We're excited to build on our existing threat intelligence integrations with Splunk solutions via the Adaptive Response Initiative to enable additional hunting and response use cases in Splunk ES."
- **Qualys:** "Qualys is happy to provide a vulnerability prioritization option via Splunk's Adaptive Response Initiative," said Jeffrey Leggett, director, cloud services, API and integrations, Qualys. "By automatically tagging high severity vulnerabilities in the Qualys Web Application Security App for Splunk, remediation teams can more quickly focus on vulnerabilities that need immediate attention."
- **Recorded Future**: "Security teams want better, faster and easier ways to defend their organizations from attack. Through Splunk's Adaptive Response Initiative, Recorded Future can automatically enrich IOCs with real-time threat intelligence collected across the entire web and analyzed in Splunk ES," said Christopher Ahlberg, co-founder and CEO, Recorded Future. "As a result, analysts are more productive and empowered to make decisions faster. We're excited to be a part of this initiative and can't wait to deliver this to our mutual customers."
- **Symantec:** "We are excited to be working with Splunk in this critical area of cybersecurity," said Peter Doggart, vice president of Blue Coat business development, Symantec. "Securing a new world of devices, networks and applications is core to the Symantec mission, and doing so with maximum efficiency will be important as we see a widening skills shortage in IT security. Splunk Adaptive Response has the power to help reduce workload on customer SOC teams by speeding up decision making and associated actions through automation."

Previously announced and founding organizations in the Adaptive Response Initiative include Carbon Black, CyberArk, Fortinet, Palo Alto Networks, Phantom, Tanium, ThreatConnect and Ziften.

For more information and a complete list of security technologies involved in the Adaptive Response Initiative, visit the Splunk website.

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 provides the enterprise machine data fabric that drives digital transformation. More than 12,000 customers in over 110 countries use Splunk in the cloud and on-premises. Join millions of passionate users by trying Splunk 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/20160928005351/en/

Media Contact
Splunk Inc.

Jacinda Mein, 415-420-0026
jmein@splunk.com
or
Investor Contact
Splunk Inc.
Ken Tinsley, 415-848-8476
ktinsley@splunk.com

Source: Splunk Inc.