Market Insight Report Reprint

Security at Splunk .conf21: new functionalities, partnerships and expertise

December 2 2021

by Scott Crawford, Megan Goodwin

From its origins as a disruptor in operations monitoring across a range of domains, Splunk has achieved a strong market position that faces challenges on multiple fronts. Security remains a pillar of its strategy, and at .conf21, this commitment was manifest in multiple announcements.

451 Research

S&P Global
Market Intelligence

This report, licensed to Splunk, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

Splunk kicked off the 2021 edition of its annual .conf event by announcing new products and enhancements, and new partnerships. Security additions and evolutions were also a focus. Splunk revealed a strengthened security analytics capacity by tying new offerings and updates to its existing foundation. Cloud – both for Splunk's customers as well as a venue for its own offerings – remains a priority, but the company still has challenges to face.

THE TAKE

Splunk highlighted its continued growth and cloud transition, emphasized its further push into observability, and in its key market of security called out its focus on increasing detection, investigation and accelerated response. Since .conf20 the company has acquired TruSTAR to better facilitate the integration of threat intelligence into Splunk's offerings for security operations. Splunk acknowledged its role in security market trends toward broadening the reach of security operations by calling out integration with multiple technologies, data sources and customer paths to action, in the vein of XDR. Splunk revealed that it has deepened its partnerships both in terms of the nature of partners and its high number of total partnerships, and has signaled its openness to more.

Established security operations technologies are facing challenges from emerging segments such as XDR, while Splunk continues to navigate its transition to a 'cloud first' provider. There were changes in leadership and personnel, including the recently announced departure of CEO Doug Merritt, made public after .conf21. This puts Splunk at a crossroads, but the company could take on the challenge if it can capitalize on its established and loyal customer base, successfully attack longstanding pricing concerns, and make the most of its advantage as one of the more flexible approaches to managing operational data across a wide spectrum of fields.

Details

Security and observability were among the main focal points at .conf21, with observability concentrating on six aspects: monitoring infrastructure, application performance, user experience, automated incident response, business service insights and 'AIOps.' Splunk revealed layers of security and tooling by sharing tactics that revolve around SIEM, Security Orchestration Automation and Response (SOAR), behavioral analytics and threat intelligence management. Splunk also announced its partnership with Accenture, integrating the company's deep tech knowledge with Splunk's platforms. Splunk highlighted partnerships with Mandiant, DTEX, and Zscaler, taking an additional step to broaden its security outreach. Mandiant's emphasis has been its combination of incident response and intelligence expertise, coupled with a portfolio of relatively recent entrants in the security market, such as continuous and automated security controls validation and XDR. Splunk offers a well-established security operations platform, bridging security analytics with more recent tactics and a common interest in threat intelligence. Offering an enhanced SOC visibility, the partnership with Mandiant presents an app for Splunk Enterprise to help control teams determine the configuration of control points as attacks emerge and to validate that Splunk is receiving the events from the tested control points, and to ensure that Enterprise Security is sending alerts. Connected with SIEM, Enterprise Security can send alerts and identify attacks, enabling teams in a security operations center to respond.

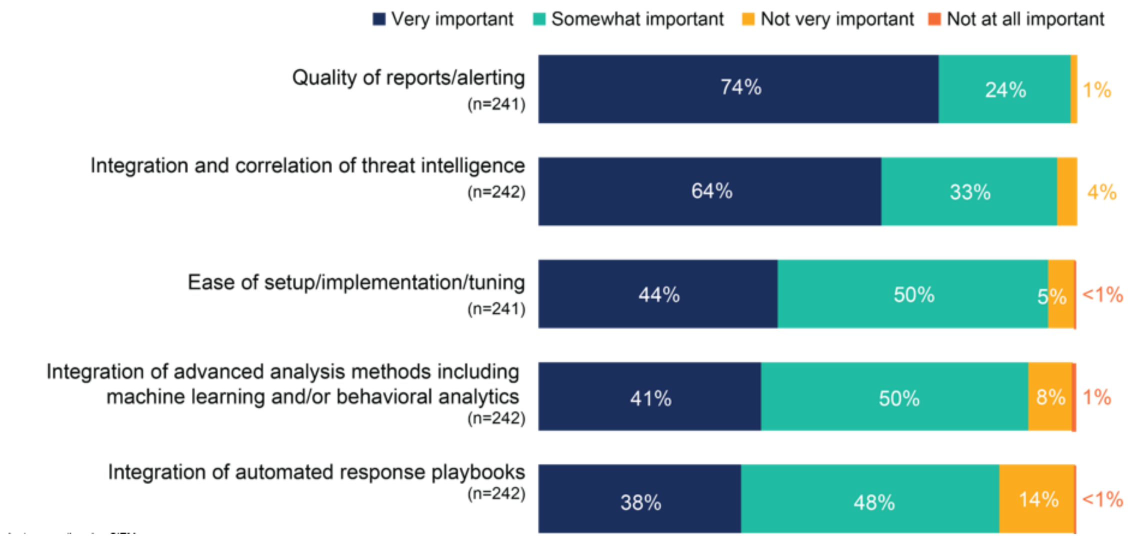
The partnership with DTEX, meanwhile, augments Splunk's security analytics and operations portfolio, which includes Splunk User Behavior Analytics (UBA), with DTEX's distinctive view of human activity, including an approach to data loss prevention (DLP). DTEX expands visibility to threats from an insider perspective by monitoring endpoint behavior and running analytics on endpoint logs. The observed data is then recorded and sent into Splunk.

©Copyright 2021 S&P Global Market Intelligence. All Rights Reserved.

Splunk’s partnership with Zscaler complements the latter’s approach to end-to-end connectivity, security measures and access controls across and beyond enterprise networks with cloud-to-cloud log streaming, API-level integration with SOAR, tracking individual access patterns that may be indicative of threats, and analytics integrated with Splunk Enterprise Security. This addresses a major enterprise concern about network visibility at a time when enterprise IT architectures have become extended to ‘work from anywhere,’ and increasing communications encryption heightens visibility challenges across links.

Of Splunk’s recent acquisitions, most notable for security was TruSTAR, which has become Spunk’s Intelligence Management technology and will soon be integrated with Splunk Enterprise Security. It concentrates on alert prioritization and ease of use in sharing threat intelligence across teams, tools and sharing partners, and creates areas of vetted sources for sharing enclaved data. This speaks to a primary interest among organizations using SIEM, where 451 Research’s Voice of the Enterprise data indicates that the integration and correlation of threat intelligence is second only to the quality of reporting and alerts.

Most Important Attributes to Organizations When Selecting an SIEM Vendor



Q. How would you rate the level of importance of each of the following attributes when selecting an SIEM vendor?

Base: Respondents currently using SIEM

Source: 451 Research’s Voice of the Enterprise: Information Security, Vendor Evaluations 2020

Splunk’s involvement with the practitioner community goes back to its roots as a highly adaptable tool for simplifying alerting and monitoring on a wide range of operational data management through the application of search. In security, Splunk amplified its support for security practitioners at .conf21 by introducing its SURGe Team, consisting of security experts, threat researchers and advisors, concentrated on guiding Splunk users’ response to cyberattacks. The team offers advisory work and research publications to expand public knowledge on the swift handling of incidents because there is often a notable gap between an emerging attack and rapid response. Following the company’s June announcement of the Splunk Security Analytics, which offers automated updates, risk-based alerting (RBA) and deeper analytics, Splunk introduced a simplified interface to its SOAR technology at .conf21. Formerly Splunk Phantom, Splunk SOAR is Splunk’s visual playbook editor that allows for optimization of security operations processes and tactics through automation. SOAR playbooks are structured in a modular format and allow for automation at scale, optimizing the human aspect of security operations and increasing response time and capability.

Overall, Splunk continues to serve its security customers with a range of functionality, now further augmented with both expertise (as with SURGe), product functionality and partnerships with leading providers. The company faces a growing range of competitors in multiple domains while the technologies it serves continue to evolve and expand – but Splunk can still call on a strong position in the market to help it navigate an increasingly complex future.

©Copyright 2021 S&P Global Market Intelligence. All Rights Reserved.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2021 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.