Brought to you by Informa Tech

OMDIA

Publication date:
22 Nov 2021
Author:
Eric Parizo, Principal Analyst, Security Operations

Splunk cybersecurity strategy analysis: Building an identity as the business-centric SIEM

Omdia view

Summary

Splunk won't be the first vendor to transition its security information and event management (SIEM) solution into a cloud-native, analytics-driven next-generation SIEM (NG-SIEM), but it intends to be the best. At its recent .conf21 virtual conference, the vendor highlighted notable technology advancements in areas including analytics, threat intelligence, and threat response. It reached a critical business pivot point by announcing the long-awaited general availability of workload-based pricing. Even its identity as a cybersecurity vendor is evolving, featuring a new narrative that uniquely casts Splunk as the industry's foremost business-centric threat detection, investigation, and response (TDIR) technology provider.

Splunk seeks new leadership amid revenue transition

Splunk continues to gain momentum in nearly all facets of its business, though admittedly, its fiscal year 2021 revenue was down slightly from the previous year, coming in at $2.23bn. However, the decline can be attributed to its customer base transitioning to its cloud-based platform, Splunk Cloud. That, in turn, affects how Splunk must recognize revenue. A deeper look shows a business fundamentally transforming for the better: total cloud revenue reached $554m, up 77% year-over-year (YoY). Cloud annual recurring revenue (ARR) will be approximately $1.105bn, representing 75% YoY growth as of 3Q22 (ending October 31, 2021).

New or expanded customer accounts in 2021 include California Pizza Kitchen, Nvidia, Okta, Tesco, and Tide, among others. At .conf21, the vendor highlighted strategic relationships with some of the largest organizations in the world, including retailer Walmart and cloud giant Amazon Web Services.

Shortly after .conf21, CEO Doug Merritt announced his resignation, but he will remain in an advisory role as the search for a new CEO begins; he is being replaced in the interim by board chairman and former Salesforce CFO Graham Smith. During Merritt's remarkably successful eight years at the helm, Splunk grew from $302m in revenue in fiscal 2014 to nearly $3bn in ARR in the third quarter of fiscal 2022, not to mention he turned Splunk into one of the most well-known brands in enterprise IT.

Omdia's analysis indicates that the CEO change was precipitated primarily by two factors: the multiyear timeframe needed to fully transition Splunk into a recurring revenue-based business and the company's ongoing struggle to turn a profit. Splunk's preliminary 3Q22 non-GAAP operating margin of negative 14% is believed to be a flashpoint for its larger investors, most notably private equity firm Silver Lake Partners, which in June announced a $1bn investment in Splunk.

While Splunk's investors no doubt desire a new CEO who will accelerate the data platform giant's path to profitability, Omdia believes Merritt's decision to leave Splunk is an unfortunate one. Merritt's decisions on product strategy have been prescient, doubling down on cybersecurity and pushing into observability, a likely future high-growth area of the IT market. He has also overseen a trying yet largely successful multiyear transition away from ingestion-based pricing, a model that proved lucrative but was causing Splunk to be decreasingly competitive in the marketplace.

Omdia believes Splunk is on the right path strategically, and its new CEO would be wise to follow the playbook Merritt has written. Any effort to accelerate its path to profitability by cutting costs or changing key elements of its strategy would risk harming a fundamentally strong business.

Splunk .conf21 announcements

Splunk had no shortage of security-related product announcements at .conf21. Selected highlights include:

- **Workload-based pricing**: Several years in the making, Splunk announced that its workload pricing program, which charges based on the compute power required to run the software, would be made available to all Splunk Cloud customers. The vendor is moving beyond its traditional ingestion-based pricing model, which charges based on the amount of data customers send into Splunk. Ingestion-based pricing has served to unintentionally dissuade customers from utilizing the elastic data storage and compute capacity the cloud offers. Early adopters of workload-based pricing have been able to double or triple their peak daily data ingestion rates while experiencing relative annual cost reductions of up to approximately 40%.
- **Threat intelligence**: Splunk highlighted its May announcement to acquire threat intelligence platform (TIP) vendor TruSTAR and renamed it Splunk Intelligence Management. The move means not only will Splunk Enterprise Security (ES) gain an integrated, cloud-native TIP, but the solution also includes a differentiating capability that allows for vetted threat intelligence to be securely shared among internal and external partners.
- **Analytics**: Splunk has enhanced the Risk-Based Alerting feature of Splunk ES to help customers prioritize important alerts and filter out low-priority ones. Originally announced in 2020, the offering is a resurfacing of a prioritization system that has been in the product for several years. RBA implements a set of rules that seek out activities that are generally associated with adversarial tactics, techniques, and procedures (TTPs) from widely used security frameworks such as MITRE ATT&CK and score findings against a risk index. Notables exceeding defined risk thresholds are automatically prioritized. Additionally, a new preview feature called Behavior Analytics for Splunk Security Cloud complements Splunk ES's correlation-based threat detection using streaming security analytics capabilities to uncover unknown threats and anomalous user and entity behavior.

- **Research group**: Splunk announced the creation of SURGe, a new cybersecurity research team led by Splunk veteran Ryan Kovar. SURGe will focus on not only creating important security research for Splunk customers by showing the value of Splunk as an analytical tool but also acting as an information resource regarding high-priority cybersecurity events.
- **Threat response**: Splunk SOAR, formerly Phantom, became a cloud-delivered offering in June. At .conf21, it gained a new App Editor, providing a new way to create, edit, and test playbooks, as well as foster improved integration and automation between Splunk SOAR and commonly used third-party tools.
- **Partner program**: The new Splunk Partnerverse Program will debut in February 2022. Its network of more than 2,200 partners will gain access to expanded technical expertise, more detailed core competency demonstration via a new badge system, and improved showcasing of joint customer successes.

Splunk and business-centric threat detection

Though Splunk has been one of the largest vendors by revenue in enterprise cybersecurity for a number of years, it is still largely known as a general-purpose data platform provider. It has yet to be broadly recognized as a leading SOC vendor. Until recently, its challenge in fostering security-centric go-to-market messaging has been that its core value proposition has been somewhat at odds with what contemporary SecOps teams desire. Splunk's unofficial motto, "Leave no data behind," does not necessarily resonate with enterprise cybersecurity buyers who want more simplicity and less noise. Extended Detection and Response (XDR) is emerging as an alternative to the SIEM/SOAR-based SOC stack, in part because organizations want faster results with *less* data.

But there are good reasons why Splunk has found success as the primary SOC tool for many of the largest organizations in the world. And those unique principles—the ability to analyze data at a scale larger than anyone else, explore data relationships more ways than anyone else, and develop deeper, more unique business insights than anyone else—may serve as cybersecurity operations differentiators, but they can be difficult to convey.

Splunk is making a new effort to build its brand in SecOps, and it's doing so by using the very people it's trying to reach: its customers. Leading the charge is Pamela Fusco, Splunk's new CISO. Fusco is a 30-year cybersecurity industry veteran who has held leadership positions at Citigroup, Digex, and Merck after starting her career as a cryptologist for the US Navy and NSA. Fusco wanted to work for Splunk after using the product in multiple organizations and learning its value first-hand. Specifically, she discovered that Splunk could identify threats by not only identifying traditionally anomalous IT events as most SIEMs can, but also by detecting anomalous business activities such as unexpected sales spikes or supply chain disruptions.

The result is an emerging new go-to-market messaging opportunity that positions Splunk as the leader in business-centric threat detection. By leveraging its data platform leadership and demonstrated ability to highlight business insights, the vendor believes it can differentiate by proving it can use data to "learn" how a customer organization operates, identify unusual business events, and correlate them with potential cybersecurity threats. Splunk believes this strategy can build its cybersecurity credibility with C-suite buyers and influencers.

Splunk is nurturing this approach with product development efforts as well, most notably its new Executive Summary Dashboard for Splunk ES. The dashboard surfaces key SecOps program performance indicators, such as mean time to detection/response/resolution, investigations created, and risk-based alerting trends. Splunk is leveraging a key strength, namely to analyze and develop insights from nearly limitless volumes of data and delivering value to CISOs and other senior security and business leaders in the form of data that can assess SOC health and success.

Strategy and analysis: Deliberate approach, superior results

There is little use in overlooking the reality that Splunk is not among the early SIEM vendors that have successfully transitioned to NG-SIEM. Omdia's baseline requirements for NG-SIEM include a cloud-native platform, native ingestion of non-traditional telemetry including threat intelligence, built-in behavioral baselining to supplement rules-based detection, and native incident response capabilities.

However, Splunk's NG-SIEM progress is notable: ES Cloud is a fully cloud-hosted solution; the TruSTAR acquisition enables Splunk to ingest non-traditional telemetry; its analytics-based detections remain a work in progress, but are improving; and Splunk SOAR remains a standalone offering, but integration with Splunk ES is solid and steadily improving. Splunk's next major objective is to bring all these technologies together, along with its Mission Control unified cloud-based management system, as a single NG-SIEM offering, which will be called Splunk Security Cloud.

Splunk also recognizes that its competitive Achilles' heel versus rival SIEM vendors is usability: Splunk ES can deliver outcomes as good or better than any other SOC platform on the market, but the effort required of customers in regard to configuration, data analysis, and ongoing content addition and refinement is often considerably greater than its rivals. But it is making enhancements here as well, such as the advancement of its analytics capabilities, more and better Splunk ES content via SURGe, and a variety of improvements to make its cloud platform more scalable and extensible.

Ultimately, Omdia believes that the combination of analytics, TIP, and SOAR capabilities, once matured and tightly integrated, will position Splunk Security Cloud as a highly competitive NG-SIEM solution. In the meantime, its budding go-to-market efforts around business-centric SOC use cases will foster further competitive momentum that will help Splunk differentiate in the marketplace versus a growing number of NG-SIEM rivals.

Additionally, few realize Splunk is transitioning all aspects of its business to the cloud; not only its products, but also its way of developing them. The vendor's DevOps-based software-development model now allows a vendor that releases an update for its on-premises customers every six months to deliver updates to its cloud-based customers every six weeks. To be clear, a Netflix-style model with multiple daily updates may never be attainable, but its progress represents just the beginning of its efforts to become a faster, more nimble organization at all levels.

Appendix

Further reading

Splunk buys TruStar to beef up its threat intelligence management capabilities (May 2021)

Splunk .conf20 recap: SIEM vendor advances unified SecOps platform, offers friendlier pricing (November 2020)

Fundamentals of Next-Generation Security Information and Event Management (July 2021)

Author

Eric Parizo, Principal Analyst, Cybersecurity Operations

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com