Market Insight Report Reprint

Graylog takes log management to the cloud and aims at SIEM in the midmarket

November 9 2021

by Liam Rogers

Log management vendor Graylog has released a SaaS version of its enterprise product as well as a new security offering. With additional funding onboard, the vendor is aiming to further establish itself with security teams looking for SIEM tooling.

451 Research

S&P Global
Market Intelligence

Introduction

Graylog commercializes the open source log management project of the same name, catering enterprise licenses to IT ops, DevOps and security teams. Over the course of 2021, the vendor has added several new products: Graylog Cloud, a SaaS version of the enterprise platform; Open Insights to support open source installations; and most recently Graylog Security. Additionally, the company took in a fresh round of funding to fuel its expansion efforts.

THE TAKE

While observability and uniting logs, metrics and traces are pervasive in conversations surrounding log management, Graylog is an example of a vendor that has chosen to focus on excelling in a few areas rather than trying to compete in them all. Log management and SIEM have become a nexus between the trend of observability on the operations side and XDR on the security side, and Graylog aims to capitalize on this by providing a refined log management platform developed with security use cases in mind. To that end, Graylog anticipates partnering with security providers that want to delve into XDR and need a robust log management system. Because the company is built around the open source project created by its founder, it benefits from the growing base of free users that it now aims to capitalize on via the addition of Open Insights.

Context

Graylog as an open source project began in 2009 with commercial support products being offered in 2013. The vendor is headquartered in Houston with personnel in Hamburg, where founder Lennart Koopmann started the project. Currently, the company has 85 employees and in June it raised $18m in funding from new investors Harbert Growth Partners and Piper Sandler, taking total funding to $27m. Graylog says it has 350 on-premises customers and 10 customers for the newer cloud service, which are in the 20 to 200GB ingested per day range. The vendor says it will continue to support on-premises enterprise users but expects that the SaaS version will drive the most interest for new customers as well as existing customers looking to offload management.

Strategy

One challenge facing Graylog has been converting free users to enterprise licensees, and Open Insights is targeted at Graylog's 50,000 free open source installations. Once enabled, the subscription-based Open Insights automatically provides health and performance monitoring capabilities, which also enables the vendor to provide a base level of technical support and optimization recommendations to unlicensed users. This provides a better experience for users and paves the way for discussions about more hands-on support for those that are ingesting tens or hundreds of TBs a day, indicating that some free users are potentially already surpassing ingest volumes of existing Graylog Cloud customers and doing so without support. The vendor acknowledges that 15 to 20% of Graylog OSS installs are in home lab-type scenarios and are unlikely to be candidates for later enterprise deals, but Open Insights is also a way for Graylog to gain a better perspective on which users, based on consumption, are good candidates for support discussions and conversion to Graylog Cloud.

Products

Graylog's products now include Graylog Enterprise, Graylog Cloud, Graylog Security, Graylog Illuminate and Open Insights. The SaaS version, Graylog Cloud, has the majority of the same features as the on-premises enterprise version and gives users 90 days of retention for hot data and one year of archiving. Graylog has also incorporated a number of UI and user experience updates to the enterprise platform. Among these updates are UI personalization options for VAR or MSP customers, and potentially future XDR partners that want to bake Graylog into their platforms and have it be visually cohesive. Version 4.1 also added Log View, an interface for customizing how logs are parsed to make investigating patterns and viewing logs simpler.

Graylog Security builds on Graylog Enterprise but tailors the user experience and features to security analysts to speed investigations. The security product is aimed at the SIEM market with the goal of providing a streamlined, less noisy and less expensive option that can appeal to midmarket customers as well as to enterprise customers. One aspect of the security product is user and entity behavior analytics, where Graylog leverages machine learning tuned for over 50 security use cases to improve anomaly detection and reduce noise. This includes using machine learning to analyze data to surface events related to common security concerns such as authentication to a new host, web policy violations and file modification spikes, among others. Users can turn off certain use cases if they don't want data to be analyzed for them or don't want to be alerted on them to reduce noise.

Larger enterprises are more likely to have SIEM in use so there is opportunity in the midmarket for organizations that may not have adopted it for cost concerns. Additionally, there is interest in AI augmentation for SIEM tooling. In 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020 study, 41% of organizations using SIEM cited the integration of advanced analysis methods including machine learning and/or behavioral analytics as being very important.

Competition

There is no shortage of competition for Graylog since it competes with myriad log management vendors that also cater to SIEM, including Splunk, Elastic, Sumo Logic, Datadog, Devo, Humio (Crowdstrike), Logz.io and LogRhythm. As more vendors in APM and infrastructure monitoring take on log management to round out their observability platforms, the competition will only increase. Security vendors that compete in SIEM include the likes of FireEye and Rapid7, although Graylog aspires to partner rather than compete with security vendors and MSSPs that want to offer SIEM and XDR to their customers.

SWOT Analysis

STRENGTHS

The open source project at the core of Graylog's enterprise offering has had time to mature and has built up a community of users; with the introduction of its cloud offering, the vendor has provided heavy users of the free tier a path for offloading management and getting support.

WEAKNESSES

Graylog is still a relatively lesser-known vendor in the crowded log management space and the majority of its users are not paying customers.

OPPORTUNITIES

Many vendors in observability have turned their sights to security teams as a growing market opportunity. By focusing on log management and SIEM, Graylog has positioned itself to ideally build partnerships with some security providers rather than compete more directly with them.

THREATS

Growing adoption of observability has resulted in more incumbent vendors in adjacent sectors entering the space and there is more competition than ever over larger enterprise log management customers.

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

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.