451 Research

IMPACT REPORT

LogRhythm 7 capitalizes on Elasticsearch, performance and endpoint response

OCTOBER 22 2015
BY SCOTT CRAWFORD, DAN RAYWOOD (/BIOGRAPHY?EID=870)

With Version 7, LogRhythm has introduced a major update to its SIEM technology offering. The new version incorporates architectural advances designed to significantly improve performance, elastic search to reveal vital information quickly, and new functionality for risk scoring and threat activity mapping to help organizations more accurately prioritize incidents and events. It also features an expansion of the role of SIEM in closing the loop on remediation through expanded automation and enhancements to the LogRhythm SmartResponse framework.

The 451 Take

With its approach to an intuitive interface, ease of adoption and respectable performance, LogRhythm has won a following that has made it a significant challenger to a field of well-established incumbents. With version 7, LogRhythm embraces Elasticsearch to heighten its differentiation. The new release accelerates performance and enhances intuitive search, as well as introduces risk-based scoring and threat mapping to help sharpen analyst insight. LogRhythm 7 also expands endpoint threat response capabilities integrated with monitoring

and alerting to streamline a number of security operations within a single platform. This reflects a growing demand in security not only to make the most of automation, but also to break down silos among security products to improve integration, enhance visibility and deliver more effective response.

Context

Legacy SIEM has often gotten a bad rap for biting off more than it can chew. Many complaints revolve around the sheer number of alerts generated, management requirements, configuration requirements and the people required to run it – not to mention the initial outlay of cost for the technology. With new threats added daily to hundreds of existing attacks, and thousands if not millions of exposures in the typical enterprise, modern data management, search and analytics techniques have become essential. Yet many SIEM platforms hang on to yesterday's approaches, not least because of the impact on critical dependencies in legacy architectures.

This has introduced opportunities for those who challenge the status quo in security information management. LogRhythm gained a following from its recognition of the values of an intuitive, modular approach to building rules and queries, which enhance ease of deployment and use. With its latest version, LogRhythm doubles down on both performance and search with an embrace of Elasticsearch and a fundamental re-architecting of data processing and indexing.

Another frustration often reported by security operations teams is the disconnect between monitoring and alerting, as well as the seamless handoff of significant issues to response and remediation. Trouble ticketing is the typical method for such handoff, but operational platforms such as SIEM rarely engage automation directly in resolving potential issues detected in targeted systems such as endpoints. The siloing of security tools also inhibits the visibility required for security teams to have a clear understanding of the context of risks and threats.

These factors have led not only to an increased interest in automation (further heightened by growing difficulties in sourcing qualified security expertise), but also to the increased introduction of functionality that breaks down traditional boundaries that keep security tools isolated from each other. LogRhythm had previously introduced its SmartResponse automation framework to capitalize on this opportunity, and with version 7, the LogRhythm platform further extends these capabilities.

Product

In its pursuit of the most modern enhancements to the LogRhythm platform, the company has turned to Elasticsearch with a number of positive results delivered in this major upgrade. Elasticsearch allows log management functions to be divided between data processing and indexing, which frees limitations on scaling each. Elasticsearch also provides a significant boost in full-text unstructured search that augments existing LogRhythm contextual search functions, further supporting an intuitive search experience that yields actionable results.

Other performance enhancements in LogRhythm 7 include clustering at the indexing tier that further supports scalability and performance. Active-active HA parallelism increases compute availability, rather than forcing fault tolerance to remain dormant in the face of high processing demands. These improvements have resulted in as much as 300 percent gains in data indexing performance on a per-node basis, according to LogRhythm.

Enhancements in the LogRhythm 7 user experience helps organizations realize these benefits of improved performance and search. The addition of a new risk-based scoring algorithm applied to every event by IP address, location and user simplifies the actionable correlation of context in prioritizing alerts. A new, real-time threat activity map provides a vivid and interactive visualization of geographic threat origins correlated to targets.

One of the more provocative aspects of version 7 is LogRhythm's continued push into response automation at the endpoint. SIEM tools have long incorporated aspects of workflow and ticketing to facilitate the handoff and response tracking. But the addition of more comprehensive security management functionality to a SIEM platform is more recent, and

customer uptake speaks to the need for more direct integration of threat detection and response. SIEM vendors have recently been challenged by new endpoint technologies. The technologies are not only designed specifically to increase visibility and improve defense at the endpoint, but also designed to overcome yet another shortcoming of traditional SIEM in its limitations on handling detailed data from thousands of enterprise endpoints.

LogRhythm responds to these challenges by leveraging enterprise-wide insight to deliver response directly to the endpoint in a platform that integrates both. Extensions to LogRhythm's SmartResponse framework introduced in LogRhythm 7 include a range of pre-configured actions that can be delivered in response to a single alert, as well as centralized management of actions handled remotely. These capabilities enable response actions from ad hoc scanning of a targeted endpoint to quarantine, all delivered from the LogRhythm console without the need to pivot to additional tools.

Competition

For competitors already seeing more than they would like of Splunk in the SIEM space, this brings LogRhythm to a new position of functionality that will push the SIEM space on with regard to speed and search. LogRhythm is one of the more competitive vendors in the sector without ownership by a major IT player. Its competitors are either going to have to develop fast to match capabilities, follow the same track with the implementation of elastic search (or equivalent) as well as response integration, or consider targeting alternate opportunities.

LogRhythm's competitors remain those with an eye on enterprise SIEM, primarily HP ArcSight, IBM QRadar and Intel Security's McAfee Enterprise Security Manager – though Splunk and AlienVault are arguably the more innovative contenders on this list. With version 7, LogRhythm takes a step closer to Splunk as a competitor, particularly with the indexing and search capabilities now present in the LogRhythm technology pushing the functionality to greater speeds and getting actionable intelligence from unstructured and machine data, while AlienVault competes in ease of deployment and use as well as integrating a more broadly functional security management platform with SIEM. RSA Security Analytics,

meanwhile, maintains log management functionality, but with the retirement of enVision may skew more towards the former NetWitness portfolio in network forensics and investigation (and may furthermore be distracted for a while by parent EMC's pending merger with Dell).

SIEM vendors across the board – including LogRhythm – face an even broader range of new challengers in security analytics, from behavioral analytics to network threat and breach detection, while plays such as ProtectWise threaten to stand existing security operations platform concepts on their head. Endpoint threat detection, response and Continuous Endpoint Recording (CER) may align with SIEM, but with its SmartResponse framework, LogRhythm offers an alternative to Bit9 + Carbon Black, Crowdstrike Falcon Host, Trend Micro Deep Discovery Endpoint Sensor and other similar plays, with an offering directly integrated with the LogRhythm SIEM.

SWOT Analysis

Strengths

Increased performance and an even more intuitive and responsive elastic search function enhance the appeal of the LogRhythm value proposition, as do enhancements in risk scoring and threat data visualization. The integration of actionable response through the expanded SmartResponse framework, however, may not only be a key differentiator, but also may indicate a future direction for security technologies that would benefit greatly from improved integration with tools across the spectrum of security operations.

Weaknesses

Ultimately, this is still SIEM and it comes with the price tag and task of configuration and management that has followed the functionality around the security sector, though LogRhythm can marshal an appealing differentiation in terms of usability that has served the company well up to now.

Opportunities

LogRhythm has long capitalized on its intuitive interface and (relative to other SIEM competitors) ready deployment to stake out a strong position in what was already a well-entrenched market when the company first debuted. Version 7 ties LogRhythm strongly to Elasticsearch to improve scale, speed and responsive search, expanding its appeal to organizations that see the advantages of such an approach.

Threats

Splunk is the largest relative newcomer to beat in SIEM. LogRhythm clearly has performance, intuitive search and enhanced usability in its sights with today's competitive landscape in mind. However, the field is not limited to other SIEM competitors, with emerging plays in security analytics adding a range of new approaches to the market. LogRhythm is now firmly in bed with Elasticsearch to enhance its position, and will need to keep relations there good given the dependence its new and appealing features have on the technology.

Scott Crawford (/biography?eid=876)

Research Director

Dan Raywood (/biography?eid=870)

Security Analyst

M&A ACTIVITY BY SECTOR

Security / Security management / Enterprise security information management (25) (https://makb.the451group.com/results?basic_selected_sectors=395)

M&A ACTIVITY BY ACQUIRER

ArcSight, Inc. (1) (https://makb.the451group.com/results?basic_acquirers=ArcSight,+Inc.)

Dell Inc. (35) (https://makb.the451group.com/results?basic_acquirers=Dell+Inc.)

EMC Corporation (77) (https://makb.the451group.com/results?basic_acquirers=EMC+Corporation)

Hewlett-Packard Company [aka HP] (71) (https://makb.the451group.com/results?basic_acquirers=Hewlett-Packard+Company [aka HP])

IBM Corporation (151) (https://makb.the451group.com/results?basic_acquirers=IBM+Corporation)

Intel Corporation (74) (https://makb.the451group.com/results?basic_acquirers=Intel+Corporation)

McAfee Inc [fka Network Associates] (22) (https://makb.the451group.com/results?basic_acquirers=McAfee+Inc [fka Network Associates])

RSA Security Inc. [EMC] (8) (https://makb.the451group.com/results?basic_acquirers=RSA+Security Inc. [EMC])

Trend Micro Incorporated (11) (https://makb.the451group.com/results?basic_acquirers=Trend+Micro Incorporated)

Figures shown indicate number of transactions

COMPANY MENTIONS (PRIMARY)

LogRhythm (/search?company=LogRhythm)

COMPANY MENTIONS (OTHER)

AlienVault, ArcSight, Bit9, Carbon Black, CrowdStrike, Dell, EMC, Envision, HP, IBM, Intel, Intel Security, NetWitness, ProtectWise, RSA Security, Splunk, StreamLine, Trend Micro (/search?company=Trend+Micro)

CHANNELS

Networking (/dashboard?view=channel&channel=4)

SECTORS

All / Security / Security management / Enterprise security information management (/search?sector=395)