Written by Alice Marshall
22 May 2019

The LogRhythm NextGen security information and event management (SIEM) platform takes to the cloud with the promise of full security monitoring, management and automation functionality only in SaaS form.

According to the company, LogRhythm Cloud is the full-fat SIEM platform, with the full breadth of log management, security analytics and out-of-the-box support for compliance automation and advanced threat detection. It also includes full security orchestration, automation and response (SOAR) capabilities, and a critical component in enabling security operations teams to reduce enterprise mean time to detect (MTTD) and mean time to respond (MTTR).

The LogRhythm Cloud user experience promises end-to-end workflow designed for speed, from alarm triage to threat neutralisation. Embedded SOAR capabilities deliver automation, consistency and measurability, while the vendor takes care of infrastructure management, software updates, 24x7 health monitoring and content updates.

“We designed LogRhythm Cloud to deliver customers our full breadth of battle-tested NextGen SIEM platform capabilities when it comes to detecting advanced threats and ensuring the most rapid response possible,” the company adds. “Unlike some other vendor solutions, which are functionally limited when compared to their on-prem offering, LogRhythm Cloud provides the same feature set and user experience our customers have come to love and rely on. We are confident LogRhythm Cloud is the most complete and powerful NextGen SIEM-as-a-service offering in the market today.”

Go The LogRhythm NextGen SIEM Platform Moves to the Cloud