Visibility is essential for **cloud security**

Managing a secure cloud requires continuous monitoring of all relevant data for meaningful insights

Ashok Sankar
Director of Industry Marketing, Public Sector and Education, Splunk

THE CORONAVIRUS PANDEMIC and the rapid shift to remote work have made agencies realize that they cannot continue relying on legacy applications. The pandemic has thrust cloud adoption into the spotlight and made it an imperative.

Although cloud services offer many benefits — including agility, enhanced citizen experience and reduced cost of operations — many agencies lack confidence and have been reluctant to undertake this journey. Security and visibility have always been cited as primary challenges with any cloud deployment or modernization initiative.

The gold standard for cloud security

The nature of an agency's mission, data protection needs and other requirements suggest that multi-cloud and hybrid environments will be the norm. As we migrate to these new locales, there is an exponential deluge of data scattered across multiple systems and endpoints. It is critical that agencies have granular visibility into all the devices, workloads and applications running across these environments so that they can gain operational and security insights. The fidelity of data is another crucial factor because without it any technology has its limits and decisions may not ensure successful outcomes.

To allay any fears about security, FedRAMP, a standardized framework for security assessments, was introduced. It has grown to be the gold standard for cloud security today. Authorized cloud services ensure that all mandated federal security measures are met and can even accelerate an agency authority to operate due to the "do once, use many times" approach. Access to granular data enables continuous monitoring of the cloud service, resulting in a better security posture and enabling timely risk-based decisions.

Splunk drives confidence in security

Splunk, an analytics-driven platform that employs AI and machine learning, is ideally suited to tackle the complexities of cloud security. It can not only aggregate data regardless of scale, format and volume from any source, but it also automates the process of sifting through mountains of telemetry data and correlating the relevant entities to find critical insights in real time, thereby reducing the burden on security analysts.

Given the disparate nature of data generated across this heterogenous environment, it offers a "single pane of glass" to present contextual views across all environments and gain holistic situational awareness critical to making confident decisions and driving actions. With enhanced visibility, agencies can accelerate security posture assessments, ensure compliance through continuous monitoring, automate responses to prevent threats and expedite investigations. Agencies can proactively address threats and manage risk with the ability to identify anomalous network traffic, prioritize security investigations, and automate policy changes and updates based on malicious activity. ■

Ashok Sankar is director of industry marketing for public sector and education at Splunk.