IDC LINK

Splunk Launches Full-Stack Observability Cloud Service to Address Hybrid and Multicloud Operational Complexity

May 12, 2021

By: Archana Venkatraman

IDC's Quick Take

Splunk has brought together a suite of tools including infrastructure monitoring, application performance management, user monitoring, incident response, log observer, and synthetic monitoring to deliver a full-stack Observability Cloud. As organizations accelerate hybrid and multicloud journeys and application modernization, an observability-defined cloud strategy can help derisk the journey.

Product Announcement Highlights

Splunk has made its unified Observability Cloud generally available as a service to empower IT, site reliability engineers (SREs), and DevOps teams with metrics, traces, and logs to troubleshoot the complexities in hybrid, multicloud environments.

IDC's Point of View

Cloud adoption is central to digital innovation but cloud adoption is becoming hugely multifaceted.

In conversations with IDC, organizations talk about cloud strategies ranging from public cloud, hybrid cloud, multicloud, connected cloud architectures, distributed cloud environments, and edge clouds.

Likewise, the application landscape is becoming multifaceted with organizations managing a whole array of applications from traditional apps to cloud-native, containerized apps, to serverless and edge apps. In addition, DevOps teams use various strategies such as microservices and application modernization tools.

As a result, the operational challenges that need to be tackled by infrastructure operations teams and SREs have increased exponentially. Modern technologies such as containers, microservices architectures, and cloud-native workloads are introducing a near constant stream of updates. This is making IT management, resilience, security, resource allocation, and cost optimization difficult to predict and manage. It is no surprise that at least 20% of cloud spending is believed to be wasted, according to IDC's research.

The huge increase in infrastructure and application complexity calls for a paradigm shift in how organizations address it. Using point tools for individual needs such as APM, infrastructure monitoring and troubleshooting, security management, and log data can result in blind spots and different stakeholders not having a single version of truth to work with. Not having access to real-time data about the health of infrastructure, security, and applications can be detrimental. As one customer at the May 5 Splunk Observability Cloud customer roundtable said, "Without telemetry, you are really flying blind."

Splunk's full-stack Observability Cloud comes at a time when many organizations are ready to pivot to full-stack observability, data-driven diagnostics, and automation, and the ability to do all of this at scale.

Splunk has unified multiple platforms including infrastructure monitoring, application performance management, real user monitoring, synthetic monitoring, log investigation, and incident response as part of the Observability Cloud service for end-to-end visibility.

Not All Observability Platforms Are Equal

As observability becomes the holy grail of cloud and application management, the space is fast getting overcrowded with infrastructure vendors, cloud vendors, management providers, and niche APM vendors all offering observability capabilities.

But IDC believes Splunk differentiates its observability portfolio with some unique strategies, engineering capabilities, and technologies:

- Splunk Observability Cloud and its other observability portfolio are developed natively based on open source standards. It uses the OpenTelemetry data collector to enable customers to instrument once, ingest data at scale without loss of context, and avoid vendor lock-in. Customers relying on observability insist on the value of standardization and freedom from vendor lock-in. With OpenTelemetry, Splunk can drive standardization in its customers' environments so they don't have to manually correlate data through multiple tools. Standardization around open source is also reassuring for customers who expect more dynamic IT environments and the addition of technologies such as containers at scale.
- Its popular NoSample, full-fidelity data ingestion and real-time streaming analytics and scale reduce alert noise with accurate problem detection and alerting, pointing users to the likely source of problems to improve recovery.
- Enterprise-grade features deliver centralized management over usage and costs, templatized best practices, and automation and observability as code.
- Splunk offers full-stack visibility across infrastructure, applications, users, and business processes, from the user to the back end.
- Splunk's Synthetic Monitoring is a service developed using Rigor technology, which Splunk acquired last year. The service helps to improve uptime and performance of APIs, service endpoints, business transactions, performance of web applications, and user flows.
- The shift from data-volume-based pricing to easy-to-understand pricing for full-stack observability can help tie investments to business value.
- Splunk offers the ability to cater to multiple personas, including IT, cloud center of excellence, DevOps, SREs, operations, and security teams.

As next steps, Splunk should provide a clear road map for its existing customers to adopt its newly launched observability as a service. It should also consider how it will add other technologies in its portfolio, especially network performance monitoring (Flowmill) into Observability Cloud. IDC's research shows that nearly half of cloud journeys are unsuccessful because of security and network configuration issues. Splunk will be able to derisk cloud migration strategies by adding network monitoring to its Observability Cloud service.

Another key requirement for Splunk will be to first articulate how Observability ties into AIOps because AIOps is now high on SREs' agendas. In the long run, while enriching its portfolio, it needs to look sideways to align with key AIOps features such as self-healing.

Derisk Your Future Cloud and Infrastructure Strategies

IDC believes adopting an observability-defined approach to manage IT complexity can ensure consistent SLAs, cost control, resilience, and compliance across the board.

Businesses are under real pressure to ensure that their cloud migration, application modernization, DevOps strategies, and modern security architectures are all successful. The million-dollar question is how to determine the right strategy for cloud adoption, application modernization, and agile development. The answer is observability and data-driven insights that can have a positive impact on IT operations, IT management, cybersecurity, operations, and business resilience.

One Splunk Observability customer is able to cut its mean time to resolution (MTTR) from 30 minutes to under 5 minutes. Observability helped it to improve operational efficiency, collaboration, and troubleshooting.

IDC predicts that by 2023, 75% of Global 2000 IT organizations will adopt automated operations practices, including observability and AIOps, to succeed in their digital journeys. Splunk is well placed to deliver business value to these organizations that take an observability-defined approach to IT and operational resilience.

Subscriptions Covered:
European Cloud Data Management Strategies

Please contact the IDC Hotline at 800.343.4952, ext.7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC or Industry Insights service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices. Copyright 2021 IDC. Reproduction is forbidden unless authorized. All rights reserved.