Splunk Security for Hybrid and Multicloud Infrastructures

Key Benefits

- **Adopt, operationalize and secure** multiple cloud technologies across your infrastructure
- **Conduct effective security investigations and analysis** across multicloud services
- **Gain better visibility across multicloud environments** for better investigation, alerting, remediation and reporting
- **Normalize and manage data** across hybrid and cloud infrastructure to better analyze and detect threats
- **Control costs and scale security** as demands of the business grow

With cloud adoption increasingly on the rise, businesses have started to transition to hybrid and multicloud environments at an incredible rate. Multicloud specifically — which consists of two or more cloud services within a single architecture — has become so popular that a significant majority of enterprises have a multicloud strategy, according to reports from both Gartner and Flexera.

But as more and more organizations turn to multicloud infrastructures, the demand to upgrade and implement a cloud security strategy becomes more pressing. Inevitably, the cloud adds a growing attack surface, with a new set of data streams, applications and services to manage and secure. This has magnified the need for better end-to-end visibility across environments, to better identify, investigate and respond to internal and external threats in real time.

Enter Splunk

It's never been more important to create a strong unified cloud security strategy — and it's never been more difficult. Splunk's security operations suite helps SOC teams operationalize data across hybrid and multicloud environments for enhanced visibility. This comprehensive view enables customers to more quickly monitor, investigate, analyze and detect threats across multicloud environments, helping strengthen their cloud security posture by providing a consolidated environment in which multiple teams can see a complete picture of the infrastructure.

Splunk's analytics-driven solutions provide a comprehensive approach to cybersecurity in the multicloud, bringing together data across environments to build a successful unified security posture. Splunk enables customers to normalize and manage critical data across various cloud service providers (CSPs) — including AWS, Azure and GCP — as well as platforms, applications and product implementations to better detect and prevent cloud security vulnerabilities and threats.

Splunk Capabilities

Gain visibility across multicloud environments

A multicloud ecosystem is diverse — spanning across multiple vendors, applications and systems. But companies who adopt a multicloud strategy need visibility across their infrastructure to quickly identify potential threats and mitigate risk. Splunk provides security analysts with a single view of all systems by centralizing the data, findings from raw event data, CSP native security tools or a cloud management platform. This unified view enables analysts to more efficiently validate, contextualize and prioritize alerts, reducing time to incident detection, streamlining investigations and responding rapidly.

Flexibility and tools for auditing across multiple cloud providers

Monitoring and auditing with one tool while troubleshooting with another can be needlessly complex, making security become a blocker and slow down teams addressing critical issues. Splunk can be built cloud-first to scale quickly, ingest any data from any cloud while replacing a multitude of tools with one simple solution. This can help to eliminate silos, enable fast release cycles and improve overall operational efficiency, while still allowing for multiple simultaneous required capabilities.

Monitor, investigate and detect vulnerabilities and misconfigurations

With the data platform and continuous monitoring established, security teams can seek out known threats and other threat indicators, including suspicious traffic patterns and anomalous activity that deviates from established baselines. Splunk security solutions are vendor agnostic, and the unified view they provide can help teams quickly detect and investigate vulnerabilities and misconfigurations across multiple cloud services for remediation.

Continuous monitoring can help to ensure adherence to compliance mandates, and by leveraging Splunk the security team can proactively respond when needed. Splunk provides an entire library of detections against the security-relevant data from the cloud platforms, through both freely available applications like Splunk Security Essentials and Enterprise Security Content Update, as well as premium solutions like Splunk Enterprise Security.

Realize the cost benefits and maximize your ROI

Gaining the value of seeing events across multicloud and hybrid environments reduces overall cost, increases agility and mitigates risk, by enabling teams to focus their time on high value tasks and continuous SOC maturity growth. Organizations can monitor spend in real time, forecast costs and identify inefficiencies when and as they occur. They can then confidently transition security operations to increase business demand and lower upfront costs.

20-14609-SPLK-SplunkSecurityforHybridandMulticloudInfrastructures-103-SG