Splunk Enterprise Transformation with Azure

A Cloud-based Data Analytics solution for Agencies to take advantage of objective, data-driven insights

splunk> | Microsoft | Cloud offering by: carahsoft.

Public Sector Agencies

Splunk Enterprise on Azure helps customers improve mission outcomes, make effective use of ever-limited funding, protect critical assets and drive modernization

Challenges	Ideal Solution	Desired Outcomes
Without access to monitoring and troubleshooting tools, agencies are missing important metrics such as performance, uptime, and availability.	Splunk on Azure turns machine data into answers. This means agencies now have a tool to perform continuous diagnostics and mitigation (CDM), including monitoring for unauthorized access and employing advanced threat detection techniques to combat cyber-threats in real time.	Splunk on Azure is the easiest way to aggregate, analyze and get answers from your machine data. It also provides visibility into existing applications and metrics, allowing agencies to better understand what resources are being used and to what extent.
Machine data is real time, messy and unpredictable. It comes from so many different sources and in so many unpredictable formats, that it's difficult to collect, and even more challenging to make sense of or take action on.	Splunk on Azure makes it possible to see the answers that are buried in that chaotic data. Real-time insights that agencies use to solve its problems, to find new opportunities, to do its job and mission more effectively.	This cloud-based, real-time data analytics platform helps accelerate modernization initiatives. Armed with data-driven insights, agencies can quickly make confident decisions and take action.

Availability

Azure Commercial	Azure Government	Azure Gov. Secret	Azure Gov. Top Secret
Data up to DoD IL2/FedRAMP High	Data up to DoD IL5/FedRAMP High	Data up to DoD IL6	 ICD 503 – In Progress

splunk> | Microsoft | carahsoft

Splunk Enterprise on Azure - Features

A Cloud-based, real-time data analytics platform offering enterprise-grade availability and scalability to support the collection of hundreds of terabytes of data per day from workloads residing on-premises, in the Cloud, or across hybrid environments.

Investigate	Monitor	Analyze	Act
Overcome resource limitations, identify and investigate abnormalities and predict issues before impact with AI/ML technologies.	Automate compliance monitoring to ease audits, enable self-reporting and ensure a passing scorecard while enhancing security posture and proactively managing risk.	Ensure successful modernization to analyze with granular visibility into migration processes and rationalizing applications.	Ensure optimal performance, uptime and availability of systems and applications by closing any visibility gaps to act across any environment — cloud, on-premises or hybrid.

Splunk on Azure makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and mission results.

Splunk Enterprise on Azure - Solution

Turn data into answers with intuitive machine learning powered analytics

Solution Alignment

Real-Time Visibility	Data Source Agnostic	AI & Machine Learning
Automate the collection, indexing and alerting of machine data that's critical to your operations.	Uncover the actionable insights from all your data — no matter the source or format.	Leverage artificial intelligence and machine learning for predictive and proactive business decisions.

Turn Data Into Doing - Ingest data from different sources including systems, devices and interactions, and turn that data into meaningful business outcomes across your organization.

Customer Success Story

Fairfax County, Virginia

"Previously, reporting to leadership was difficult because everything was manual. My staff would spend countless hours, probably two weeks' worth of work, to get me a summary report of our cybersecurity stance. Now, with the Splunk platform, I have real-time access and can give an overall security posture to my leadership to let them know when we have issues."

- Mike Dent, Chief Information Security Officer

- Win in 2019
- Compliance & Security, State and Local East

https://www.splunk.com/pdfs/customer-success-stories/splunk-at-fairfax-county.pdf

Win Results

Achieved significant cost savings by reducing data center hardware footprint as well as allowed for repurposing full-time equivalents (FTEs) away from managing infrastructure and towards more value-added tasks

Replaced time-consuming, two-week security reporting with real-time reporting to leadership

Proactively supports more than 50 county agencies and protects the data of over 1.1 million citizens

Thank You

AzureMP@Carahsoft.com

splunk> | Microsoft | Cloud offering by: carahsoft.