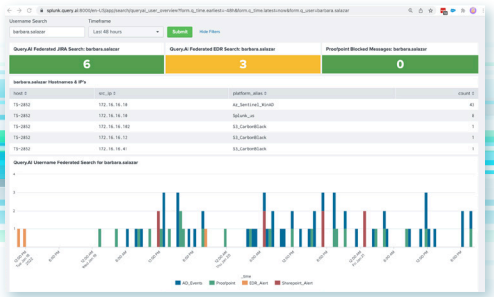
Query.ai

Datasheet

Query.AI Federated Search for Splunk

Supercharge your Splunk® and improve the speed and accuracy of your cybersecurity investigations



If your high-performing security operations team leverages the power of Splunk to detect, investigate and respond to complex threats in your organization's environment, then they know the pain of the "swivel chair challenge." That's the manual and time-consuming process typically required to gain access and insights into crucial data located outside of your Splunk platform.

Your team needs an easy, efficient and cost-effective way to access data across your full cybersecurity ecosystem, which likely has between 50 to 75 discrete products that operate in the cloud, third-party SaaS, and on-prem.

The Solution: Query.AI Federated Search for Splunk

Query.AI Federated Search for Splunk unlocks access to and value from cybersecurity data wherever it is stored, regardless of vendor or technology, without requiring centralization. The app plugs into disparate security technologies quickly and easily using APIs and displays real–time and historical data in your Splunk platform. By leveraging the Query.AI app, you can empower your people to make timely and accurate security investigations decisions with high confidence in the outcomes.

Key Benefits

Access and search across your data silos

Better address security threats with centralized access to decentralized data that resides outside your Splunk platform, without any data movement or transfer.

Increase team efficiency

Automate previously manual and time-consuming investigation processes, directly within Splunk, without ripping and replacing existing technologies.

Maintain operational rhythm

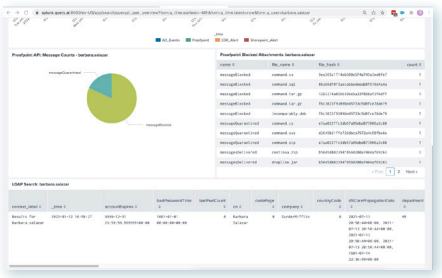
Plug the Query.AI app into existing Splunk workflows and realize greater efficiencies from your security operational processes.

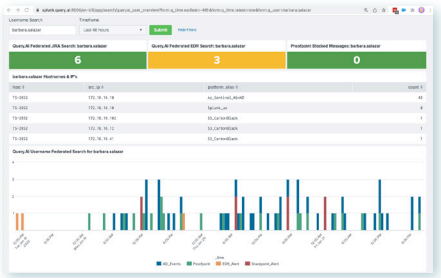
Retain control of your indexed Splunk data

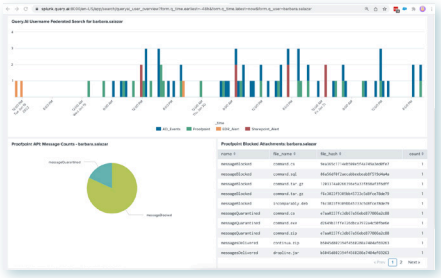
Access data across your environment and maintain flexibility and control to decide if you want to persist any returned data to your Splunk platform.

Key Features

Seamless integration	Install the Query.AI app using **simple, plug-and-play integration** that ensures **unified operation with your Splunk platform**, and enables **central management of your security investigations** across your infrastructure.
Centralized access to your data silos	Extend your Splunk platform with access to **investigate your siloed data** across your **cloud, third-party SaaS,** and **on-prem environments**, without transferring or moving the data.
Federated search	Run **federated searches** across 150 of the most widely used enterprise technologies from **within your familiar Splunk interface**, giving you insights from the data you need to **quickly and accurately** complete your investigations.
Unified Query Language	Conduct simultaneous searches across multiple data silos with our **Unified Query Language (UQL)** which is similar to Splunk's Search Processing Language (SPL), so there's **no additional learning curve for your team.**
Enriched Splunk console	Get more value from your Splunk console by enriching them with **real-time and historical views** into data that resides **outside of your Splunk platform**, giving you a complete picture of your decentralized environment.







Learn More

To learn more about **Query.AI Federated Search for Splunk**, please watch this video or request a live demo.