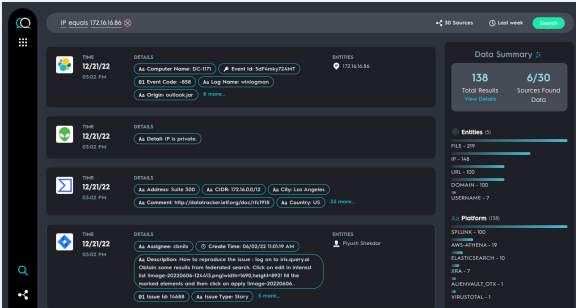
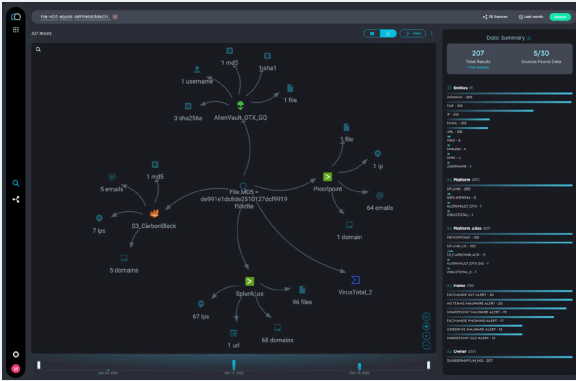




Query Federated Search for Cyber Security Teams

Get answers from your security data without the need to centralize it.



“Query vastly reduces the time and effort required for my security investigations by making it easy to access and understand the data I need, when I need it.”

– F1000 Financial Services

Overview

Query Federated Search

Query is a cloud-native federated search solution that enables security teams to search relevant security data wherever it is stored, perform faster suspicious activity, incident response and threat hunting investigations, and reduce the cost of storing security data. With Query, you leave your data where it resides, including cloud services, SaaS applications, and on-premise infrastructure. Query manages API integrations, search translation, and normalization of results.

POWERFUL SEARCH

Search your data without moving it

Security data is everywhere. Centralizing everything takes prep work, time you don't have, and a hefty budget. Some data is better left where it is and accessed in real-time when you need it. Do you have data in multiple SIEMs, data lakes, cloud storage, SaaS apps, and on-prem apps?

Query gives you the power to search and get answers from your data, wherever it resides.

Accurate Answers Fast

You have questions, we have answers.

Get the answers you need in security investigations, threat hunting, and incident response. Gain context from more data sources; not just your SIEM or data lake.

Query delivers access to real-time and historical data sources to enable your team to quickly decide and act.

Take Control of Your Costs

Increase visibility, not your SIEM bill

Technology environments are always changing & expanding.

Query gives you the flexibility to choose what to centralize and what to leave in place. You no longer need to compromise and always have access to the data you need.

How It Works



Leave your data in **your technologies...**

Cloud Services
SaaS Apps
On-prem Infrastructure



Query **manages...**

API Integrations
Search Translations
Normalization of Results



Your team **gets...**

More Visibility
Expanded Context
Fast Answers & Insights

The Query platform provides real-time, centralized insights from decentralized data so you can accelerate cybersecurity related searches, investigations, and threat hunting, resulting in more empowered and effective security teams.

Who Are We?

Cybersecurity data is now everywhere. Traditional tools rely on centralizing logs, alerts, and other data that security operators may need to investigate issues, hunt for threats, and defend the environment. Query Federated Search gives security teams access to the data and answers they need without the cost, complexity, and compliance challenges resulting from moving and storing vast amounts of data. Query uses APIs to access data across your SaaS, cloud, and on-prem technology systems; unlocking answers and visual insights from your data, where it resides. Learn more at query.ai.