Query

# Unlocking CrowdStrike Data with Query Search

## Overview

**Query** brings all of your CrowdStrike data together and puts it **instantly at your fingertips** in a visual, context-rich graph. It unifies and allows a **single search field to access data** across your security and other technology **without need for data movement, centralization, or rearchitecture.**

## The Problem

With over **70% of attacks originating at an endpoint,** CrowdStrike, the leading Endpoint Detection and Response (EDR) tool, is a key control for strong security operations. CrowdStrike is optimized to **detect attacks in real-time,** and does an excellent job of doing so. However, **novel attacks can occur without triggering the system,** leaving the user with **days or weeks of vulnerability** until a patch or update enables protection against the new threat.

CrowdStrike offers variable data retention periods, **ranging from 15-90 days,** depending on the type of data and the specifics of your contract. This can mean understanding an incident requires **searching both current CrowdStrike data resident in the application,** as well as older, **historical records that are no longer in the application. This presents two major challenges:**

### Expensive Storage

With CrowdStrike only storing recent telemetry data, **historical data must be moved and stored elsewhere.** CrowdStrike data could be stored directly in your SIEM in order to continue to have the data available to security operators. But with the amount of data created and the high cost of SIEM storage, **the cost is prohibitive; typically an extra $400,000 a year per 10,000 employees.**

CrowdStrike can also be stored in **less expensive cloud storage solutions like Amazon S3 Buckets.** This is **much more cost effective, around $20,000 annually,** but leads to our second problem.

### Limited Usability

While **Amazon S3 Buckets make the most sense** from a cost perspective, they make it **much more difficult to use the data.**

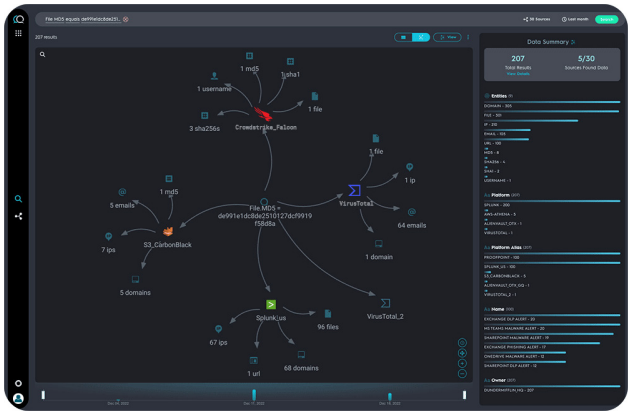
**Search and/or retrieval is difficult for the archived data** — analysts will have to download the files and then rely on doing raw text searches to find results.

Once the results have been found, the analyst will have to **manually put the results into context**. Integrating the two different data sets is manual and challenging, **requiring a different set of skills than typically found in a security operator.**

## The Solution

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.**



- **Flexible Control** - Allows you to decide where and how CrowdStrike data is stored, so you can reduce cost without compromising on security response effectiveness or efficiency.
- **Enhanced Visibility** - Enriches search results with context from other distributed security relevant data — from both security systems and relevant non-security systems — without needing to move or transform data ahead of time.
- **Improved Effectiveness** - Visualizes data linkage and context to allow operators to quickly orient and act; eliminating alert fatigue and providing additional understanding and situational awareness.
- **Greater Speed** - Quickly enables operators to pivot from one question to the next; reducing time to investigate and respond to minutes instead of hours.

> "Before Query we were moving the same security data across AWS four different times. Now we leave the data in the native systems and search it as needed. Game changer."
>
> - F1000 Financial Services

## How It Works

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

Amazon S3
(or other cloud services)
CrowdStrike
Other Relevant Systems

Query **manages...**

API Integrations
Search Translations
Normalization of Results

Your team **gets...**

More Visibility
Expanded Context
Reduced Storage Costs