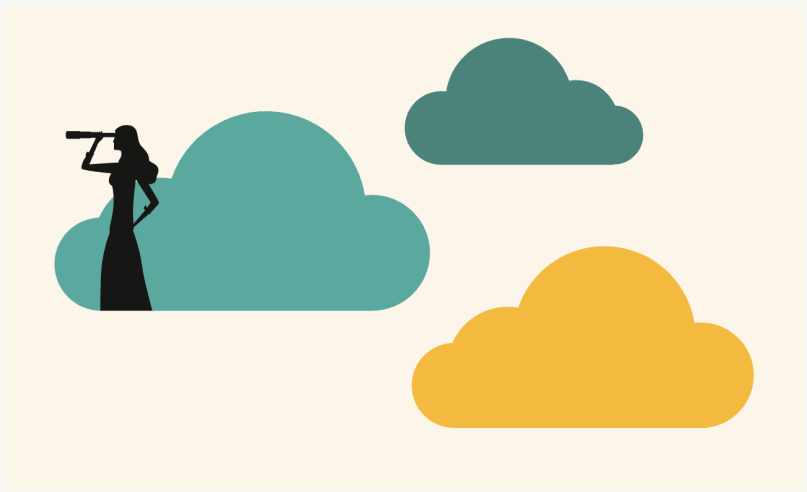
Hydrolix Search for Splunk Eliminates SIEM Retention Blind Spots

Now available in the Splunk app store, Hydrolix Search for Splunk lets security analysts investigate across complete, always-hot data directly from Splunk.



Hydrolix Search for Splunk

PORTLAND, OR, UNITED STATES, June 16, 2026 /EINPresswire.com/ -- Hydrolix, the real-time data platform for operational intelligence at internet scale, today announced Hydrolix Search for Splunk, available in the Splunk app store. The app gives security teams the ability to retain and query 15+ months of complete, unsampled telemetry. This includes high-volume sources like CDN logs, that most SIEM environments can't afford to collect and store, directly from the Splunk interface using standard SPL queries, without retraining analysts or rebuilding workflows. By making CDN and edge telemetry operationally searchable inside Splunk, teams can investigate credential stuffing campaigns, distributed bot activity, token reuse, and reconnaissance behavior that often disappear inside short SIEM retention windows.

> We keep all data hot, queryable in seconds, and accessible directly from the Splunk interface analysts already know. The faster you can get answers, the faster you can stop the threat."
>
> *Ashley Vassell, Senior Product Manager, Hydrolix*

For most security organizations, Splunk is the operational center of gravity. But its cost structure creates a painful compromise. As telemetry volumes grow, teams are forced to choose between storing enough data to investigate incidents properly and staying within budget. The result is shortened retention windows, cold storage that takes hours to rehydrate, and entire categories of high-value telemetry, particularly CDN logs, that never make it into the SIEM at all. The SIEM industry normalized this pattern and called it data management, although it's an investigation liability.

When an incident occurs, analysts are often working with an incomplete picture. Twelve hours into an active investigation, the attacker's trail runs through CDN logs from six weeks ago – logs

that were either deleted on a retention schedule or buried in cold storage behind a rehydration workflow that takes hours and sometimes days to complete. Root-cause analysis stalls, patterns go undetected, and investigations close without full confidence in the findings. Cold storage introduces delays that make archived data effectively unavailable during active investigations.

Ashley Vassell, Senior Product Manager, Hydrolix

Hydrolix.io

Buying more Splunk licenses doesn't solve the underlying economics; it scales the same cost problem faster. Hydrolix Search for Splunk addresses the problem at the infrastructure level. Hydrolix acts as a hot data fabric alongside Splunk, storing high-volume telemetry outside Splunk and executing SPL searches against that data directly from the Splunk interface. Organizations retain 15+ months of complete, full-fidelity telemetry, with every event and field stored exactly as it arrived, and query it in seconds on petabytes of data directly from Splunk using SPL. Because Hydrolix keeps all data hot, there are no cold storage tiers and no rehydration delays. Queries return fast regardless of whether the data is from yesterday or 15 months ago.

Since Hydrolix Search for Splunk is available in the Splunk app store, it's straightforward for Splunk users to extend their existing environment without replacing tools, retraining analysts, or migrating workflows. Analysts continue using the SPL queries, dashboards, and detections they already rely on. Hydrolix removes the data constraints that have limited what those queries can reach. Companies receive up to 10x lower TCO compared with retaining the same data inside Splunk alone.

"Security investigations live and die by the speed and completeness of the data available," said Ashley Vassell, Senior Product Manager, Hydrolix. "When analysts are waiting on rehydration or working without CDN telemetry because it was too expensive to ingest, they're not just slowing down; they're operating blind. Hydrolix Search for Splunk was built to close that gap. We keep all

data hot, queryable in seconds, and accessible directly from the Splunk interface analysts already know. The faster you can get answers, the faster you can stop the threat."

The initial release of Hydrolix Search for Splunk includes three capabilities designed to support large-scale, high-velocity security investigations:

1) HTTP Streaming for Massive Result Sets: Investigative queries now stream results progressively in real time, eliminating timeouts and memory failures common when pulling high-volume datasets from Splunk.

2) Native Summary Table Integration: Column inference and aggregation for summary tables enable sub-second performance on petabyte-scale datasets, with filters working directly on pre-aggregated data.

3) In-App Schema Discovery with hdxdescribe: Analysts browse tables and view schemas directly within the Splunk interface, removing the need to consult external documentation and accelerating time-to-insight during active investigations.

Hydrolix Search for Splunk is designed for security operations teams, including CISOs, SOC leaders, security analysts, and threat hunters who rely on Splunk and need access to complete, searchable telemetry across longer time horizons. It is particularly valuable for organizations managing CDN, web, network, and infrastructure telemetry at scale, where the volume and cost of traditional SIEM ingestion have historically forced teams to sample, archive, or exclude data entirely.

Hydrolix Search for Splunk is available now in the Splunk app store. Organizations interested in seeing the app in action can connect with a Hydrolix solutions engineer at hydrolix.io.

About Hydrolix: Hydrolix is a Portland, Oregon-based real-time data platform for operational intelligence at internet scale. Founded in 2018, Hydrolix addresses the two scale barriers facing observability and security platforms: global scale and real-time performance. The platform delivers real-time analytics that get you insights in seconds across globally distributed data at internet scale—from servers and microservices to AI agents—while enabling years of retention through next-generation compression. Trusted by Fox, ABC, and Paramount for mission-critical live events, Hydrolix has grown to over 650 customers globally in just 24 months.

Media Contact(s):
Abby Ross
Head of Corporate Communications, Hydrolix
abby@hydrolix.io

Stacey Barker
Jade Umbrella PR

+ +1 323-833-8358
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
X
