Hydrolix Security Data Layer Gives Security Teams Instant Access to Full-Fidelity Telemetry Without Breaking Budgets

Security Data Layer complements existing SIEM investments and delivers up to 9x faster investigation queries

Hydrolix.io

PORTLAND, OR, UNITED STATES, July 30, 2026 /EINPresswire.com/ -- Hydrolix, the real-time data platform for internet-scale operations, today announced the Hydrolix Security Data Layer. Hydrolix serves as the data layer beneath modern SIEM and agentic SecOps platforms, connecting through MCP where applicable and delivering native integrations for federated environments like Splunk.

> We built the Security Data Layer so security teams can investigate and remediate incidents faster, with full-fidelity data, without blowing up their budget to keep it."
>
> *Michael Cucchi, Chief Product and Marketing Officer at Hydrolix*

Hydrolix gives security teams and MSSPs a purpose-built home for the high-volume telemetry that they can no longer afford to retain in their SIEMs, keeping all data hot, fully searchable in seconds, and available for investigations and audits regardless of age. The solution fits into existing threat detection and investigation stacks through a tight integration with security pipeline provider Monad, purpose built for next-generation agentic security operations.

Security investigations increasingly fail not because analysts lack skill or tooling, but because the evidence they need is gone by the time they go looking for it. Faced with rising data volumes and SIEM costs that scale with ingest, security teams routinely shorten retention windows, sample telemetry, or archive data into cold storage, decisions that reduce costs today but eliminate tomorrow's evidence. When a security investigation stretches back weeks or months, as many now do, analysts often discover the data they need no longer exists or takes hours to rehydrate. Without that evidence, investigations become slower, less conclusive, and harder to use to prevent future attacks. Without that

evidence, investigations become slower, less conclusive, and harder to use to prevent future attacks.

Michael Cucchi, Chief Product and Marketing Officer, Hydrolix

The Hydrolix Security Data Layer is designed to close that gap. It sits underneath the existing security stack, not in place of it, ingesting petabyte volumes of telemetry, compressing it by up to 50x, storing it in the customer's own cloud, and keeping it immediately queryable at any age. Security teams keep using the SIEM and analyst tools they already know for detection and day-to-day workflows; the difference is that when an investigation reaches back six months or two years, the data is still there and still fast to search, and available when analysts need to establish root cause, determine the full scope of an incident, and confirm it has been contained.

"The industry has spent years making security smarter with better detections, better analytics, and now overlaying AI," said Michael Cucchi, Chief Product and Marketing Officer at Hydrolix. "But none of that matters if the evidence and source of truth was deleted six months ago because storing it became too expensive. We built the Security Data Layer so security teams can investigate and remediate incidents faster, with full-fidelity data, without blowing up their budget to keep it. That means faster investigations, faster root cause, and faster resolutions. This isn't about replacing the SIEM; it's about augmenting your existing data architecture, keeping the tools you already trust and federating your data to leverage best-in-class where you need it."

To validate the approach, Hydrolix worked with RAD, one of Europe's leading managed security service providers, and critical technology partners like Cisco/Splunk and Monad on a real-world evaluation rather than a synthetic benchmark. Using approximately two million real Palo Alto firewall log events, Monad’s collectors and data pipeline, and RAD's own production detection logic, the RAD team retained the telemetry in Hydrolix for low-cost, full-fidelity storage before retained the telemetry in Hydrolix for low-cost, full-fidelity storage and used the Hydrolix Search for Splunk connector for querying.

For the broad correlation searches that define threat hunting and incident response, Hydrolix returned results in 1.6 seconds. Hydrolix achieved those results with column indexing intentionally disabled, a deliberately conservative test configuration. The findings show that for Splunk users, Hydrolix can serve as the security data layer for fast querying, full fidelity, long-term, cost-effective data retention, and minimizing the MTTR, while they continue using Splunk

for monitoring, analysis, and insights, without sacrificing the historical context needed for complex investigations.

"As an MSSP, every customer expects us to reconstruct what happened, even if the incident started months earlier," said Daniele Ricci, Head of Strategic Consulting at RAD. "Retention had become a business decision instead of a security decision. We wanted to know whether organizations really had to choose between affordability and effective investigations and whether we could give every customer a longer history without significantly increasing costs. Based on what we saw, the answer was yes: we could keep more data and still get analysts to root cause faster, all from inside the Splunk interface they already use."

RAD's testing also confirmed that Splunk remains faster for highly targeted, single-record lookups, exactly what it was built to optimize for. But long-running investigations rarely hinge on finding one log entry; they succeed or fail based on how quickly analysts can correlate activity across weeks or months of historical telemetry, which is where the Security Data Layer is designed to help.

Hydrolix is explicit that the Security Data Layer is not a SIEM replacement. Analysts continue to work in Splunk or the detection and response tools they already rely on; Hydrolix simply becomes the high-volume data layer underneath, fed by Monad's broad network of over 340 integrations. The combination feeds those tools full-fidelity, sub-second-searchable data at a fraction of the cost of storing it all in the SIEM directly. Organizations can send high-volume sources — firewall, network flow, DNS, EDR, proxy, and cloud logs — to Hydrolix while keeping their existing detections, dashboards, and workflows unchanged, ensuring that months or years of telemetry remain immediately available whenever an investigation demands it.

"Retention shouldn't be the thing security teams have to compromise on to keep their SIEM bill under control," said Christian Almenar, CEO and Co-founder at Monad. "With Hydrolix, teams send their SIEM the high-value data their detections actually run on. The full record goes to storage built for real-time scale. Nothing gets sampled or thrown away to make the budget work. That gives investigators the complete evidence they need to understand what happened, determine whether the threat has been contained, and prevent it from happening again."

The Hydrolix Security Data Layer is available now. Hydrolix and Monad experts, including Hydrolix CEO and Co-founder Marty Kagan, will be on site at Black Hat USA for interviews about this topic. Book a meeting here.

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. For more information, visit hydrolix.io.

Media Contact(s):
Abby Ross
Head of Corporate Communications, Hydrolix

Stacey Barker
Jade Umbrella PR
+1 323-833-8358
email us here
