

Hydrolix improves all phases of the game development lifecycle

REAL-TIME LOG ANALYTICS | FASTER INSIGHTS | LOWER COST | RETAIN HOT DATA LONGER

Hydrolix manages and analyzes high-performance, affordable log data streams at all scales of operation—from early game development to launch day and beyond. Some of the biggest studios rely on Hydrolix for observability, security, real user monitoring (RUM), and build high-quality ML models.



GAME DEVELOPMENT

Lower the cost of delivering high-quality games

- › Identify bugs >10 seconds
- › Load testing
- › Keep all logs to reproduce issues
- › Trace complex sequences of events

USER TESTING

Improve performance and polish gameplay

- › UX performance optimization
- › Identify issues with third-party integrations
- › Analyze user choices and preferences
- › Train AI models for gameplay and personalization

DAY ONE/LAUNCH DAY

Monitor and improve end-user experience

- › RUM and network performance monitoring
- › Real-time DDoS detection and remediation
- › Multi-CDN load balancing

POST-LAUNCH DAILY OPERATIONS

Smooth operations, better gameplay, more revenue

- › Find and fix issues before they impact users
- › Capture more user data for better AI models
- › Increase revenue for ad-driven games



USE CASE SPOTLIGHT

Launch Day DDoS Attack



Launch day is finally here after years of development and millions of dollars spent. Social media is enthusiastic, anticipation is building, and the lobby is filling up. All that's left is to deliver the software to an eager public without a hitch.

But not everyone wants launch day to be a success, and unbeknownst to your team, a volumetric DDoS attack has started. As downloads start and traffic begins to mount, evidence of performance issues emerges. Mean time to first byte (TTFB) rises, as do HTTP 408 Request Time Out errors. But is this a DDoS attack or just the result of a successful launch?

The pressure is on your team since any performance issue can turn anticipation into anger, buzz into angry social media posts, and incur substantial reputational and financial damage.

Enter Hydrolix: Designed for High-Volume Log Analytics

A typical observability platform would struggle to discern good traffic from bad. Unlike Hydrolix, which can process millions of events per second while providing highly granular insights within seconds of ingest, they can take minutes to provide answers. These are minutes you don't have when a DDoS attack is underway.

Using Hydrolix, you can ingest logs from multiple sources—AWS Cloudfront, WAF, Akamai, Fastly, Qwilt, and other CDNs—get counts on errors and associate them with IP ranges, all within a few seconds. It may not sound dramatic, but you can then quickly take other mitigation steps, such as updating WAF rules, before attacks take your servers down.

Armed with Hydrolix, you can deliver a smooth launch day event, maximize revenue, and bolster your brand reputation.

[Read how Akamai's Hydrolix-powered observability solution, TrafficPeak, saved leading Nordic retailer Elkjøp's Black Friday from a DDoS attack.](#)

Hydrolix for AWS



Hydrolix for AWS is a managed observability service for origin to edge service products.

For Amazon CloudFront, WAF, and Elemental logs.

Hydrolix for Akamai



TrafficPeak is an observability solution for Akamai Connected Cloud, powered by Hydrolix.

For DS2, SIEM, DNS, and multi-CDN logs.

Hydrolix for Splunk



Keep your Splunk dashboards, use Hydrolix to massively reduce the cost to store and query log files.

Available on all major cloud platforms.

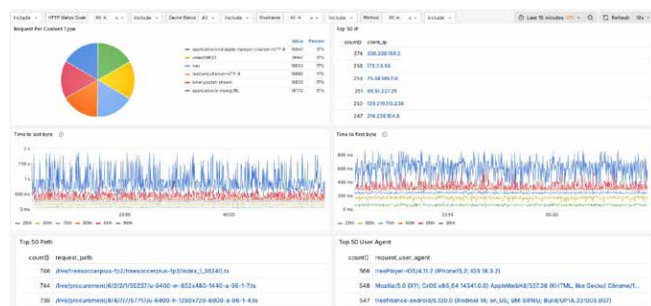
Build with Hydrolix



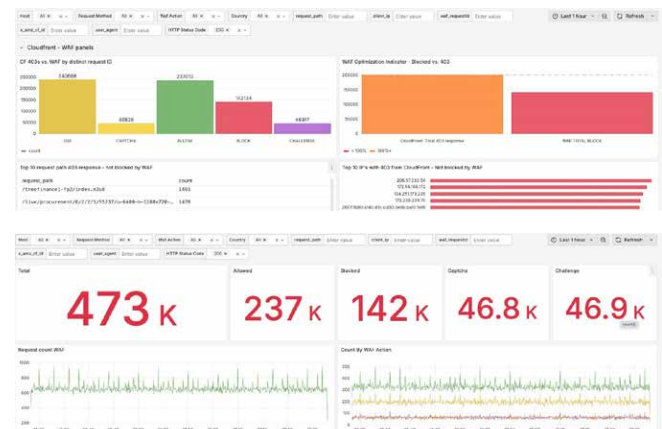
A fully-managed Hydrolix streaming data lake for high-volume log data. Save on cloud costs.

Available on all major cloud platforms.

EXAMPLES



Amazon CloudFront: Summary tables and alerts for cache miss rates, HTTP status code counts, error codes by region, FBL/LBL.



WAF: Monitor for malicious traffic, alert within seconds, and change rules from "count" to "block."

LEARN MORE AT [HYDROLIX.IO](https://hydrolix.io)