CUSTOMER SUCESS STORY

sysdig

Sysdig builds security software for containers, Kubernetes, and cloud services, helping DevOps teams secure their cloud-native environments

Users

DevOps Engineers, Developers and SREs

Industry

Software / DevSecOps

Website

www.sysdig.com

The results

- 80% faster access to logs, significantly reducing Mean Time to Resolution (MTTR)
- Holistic visibility into all systems and applications
- Cross-team accessibility, empowering every engineer to interact with logs
- Compliance-ready logging, supporting SOC 2 Type 2, PCI-DSS Level 1, HIPAA, GDPR, and CCPA

> With Mezmo, anyone at Sysdig can easily access and interact with log data—no complex identity management required.
>
> - Mark Breitung, Senior DevOps Engineer

sysdig

mezmo

Sysdig gains Kubernetes observability and 80% faster log access

The challenge

Sysdig initially relied on a custom-built observability solution to manage and analyze logs. The company's DevOps team used syslog to aggregate logs into an S3 bucket hosted in the Amazon cloud. Then, the team deployed Athena, an Amazon cloud service, to process log data. This approach was an effective way to collect logs and store them in the cloud. However, it fell far short of delivering full observability. The Sysdig team's ability to query log data using Athena was limited, and there was no efficient way to customize queries for different types of logs, such as server logs and Kubernetes logs. The solution was also unwieldy to manage. It was "crazy town," according to Breitung, because it relied on a mishmash of open source tooling and Amazon cloud services, making it difficult for the team to quickly track down critical information and gain holistic visibility into its systems. Worst of all, the logs that the team aggregated into S3 buckets were difficult for most team members to access. Although in theory the logs were accessible to anyone, the tools necessary to process and analyze them were too complex for the team to use efficiently in practice. The custom-built solution "got us a check box telling us that our logs were there, but I don't think anyone actually used it," Breitung explained.

The solution

The shortcomings of the initial logging solution used by Sysdig pushed the team to search for a better solution, which they found in Mezmo. For Sysdig, Mezmo offered an array of benefits. Most obviously, Mezmo allowed the DevOps team to replace its complex log management stack with a unified solution that provides log aggregation, processing, and management through a single tool while still allowing the team to keep its log data in the cloud. But Mezmo did much more than simplify the logging solution stack. Another critical point of value is Mezmo's Kubernetes Enrichment feature, which provides native, out-of-the-box support for displaying Kubernetes events and metrics data alongside log data. This means the Sysdig team can gain visibility into their Kubernetes clusters without writing extensive custom queries or managing Kubernetes metrics separately from other observability data. Mezmo's built-in alerting features are also important.

They enable the Sysdig team to write nuanced alerts that trigger notifications based not merely on simplistic metrics and thresholds but also on contextual data. “We can say in Mezmo, ‘Send me an alert if X thing happens more than five times in a minute,’” Breitung said. “This is helpful when our backend doesn’t have a metric yet,” but the team nonetheless wants to configure alerts for certain types of events or patterns. The graphing tools within Mezmo, too, stood out to the Sysdig team. With graphing, DevOps engineers can create rich visualizations to help them interpret log data, using whichever method suits them best: A line graph, a histogram, or a pie graph. Mezmo’s archiving features also help Sysdig manage its historical log data efficiently. With Mezmo, the Sysdig team can still archive log data in the Amazon cloud using S3, as it did with its original logging solution. The archiving experience in Mezmo, however, is simpler to manage and easier to automate. It also ensures that archived logs remain searchable, even if they are housed on a low-cost cloud storage service. Finally and most importantly, Mezmo simplifies log access. With Mezmo, anyone with a Sysdig email address can easily access and interact with log data, Breitung said. He added that there is no need to manage complex user identities in the Amazon cloud, unlike when working with Athena. Ultimately, Mezmo helped the Sysdig team to achieve an 80 percent improvement in the time it takes to access and use log data. By extension, the team has significantly reduced its Mean Time to Resolution (MTTR), ensuring that it can quickly and efficiently troubleshoot problems in production systems.

The results speak for themselves:

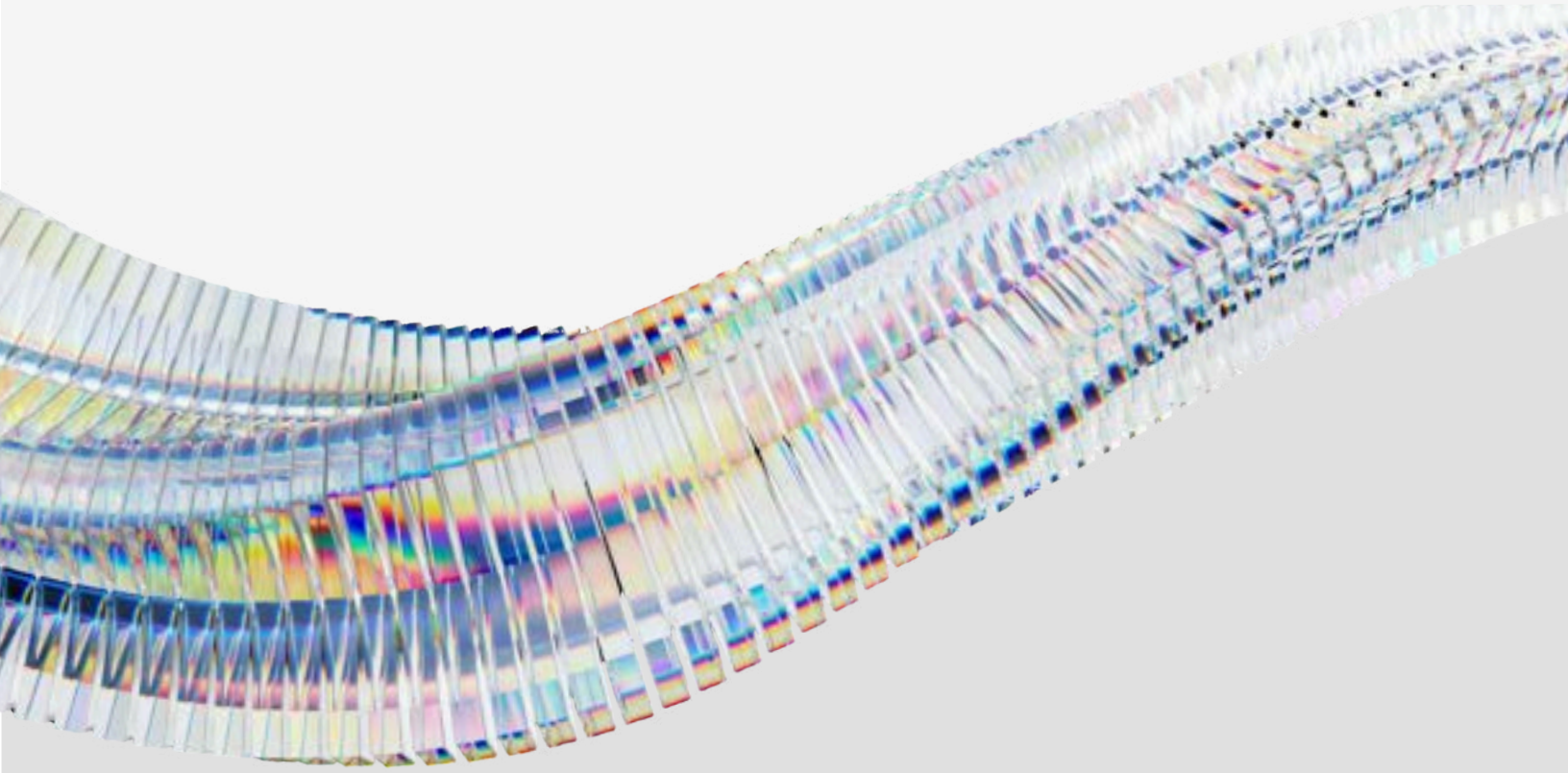
- 80% faster access to logs, significantly reducing MTTR
- Holistic visibility into all systems and applications
- Cross-team accessibility
- Compliance-ready logging, supporting SOC 2 Type 2, PCI-DSS Level 1, HIPAA, GDPR, and CCPA

sysdig

mezmo

A foundation for the future

For the Sysdig DevOps team, Mezmo has greatly simplified log management and delivered critical observability into complex systems like Kubernetes, which few other log management solutions support natively. At the same time, Mezmo ensures that everyone on the Sysdig team can access visibility insights whenever they need to. That helps the Sysdig team achieve the same level of operational observability into its systems that Sysdig provides to its customers through its security observability solutions.



About Sysdig:

Sysdig is a cloud-native security and monitoring company that empowers organizations to confidently run containers, Kubernetes, and cloud infrastructure at scale. Built on open source roots, the Sysdig platform delivers runtime threat detection, vulnerability & compliance management, and deep visibility across cloud workloads, services, and identities. With a focus on minimizing “security blind spots” while enabling agile DevOps workflows, Sysdig helps both security and engineering teams detect, respond, and prevent threats in real time without compromising innovation.

About Mezmo:

Mezmo is the leader in intelligent telemetry orchestration, empowering platform teams and developers to control, understand, and act on their telemetry data in real time, reducing costs, accelerating troubleshooting, and enabling innovation at scale. The AI-powered solution combines continuous profiling, intuitive live stream search, responsive, dynamic routing, and stateful in-stream aggregation to deliver enhanced visibility, compliance, and cost optimization. The company has been recognized as one of the fastest-growing companies in the U.S by Inc. 5000 and Deloitte Fast 500.