mezmo.com

THE OBSERVABILITY CHALLENGE

ACCESS, SPEED, SECURITY & VALUE

IN SEARCH OF TRUE OBSERVABILITY

INTRODUCTION

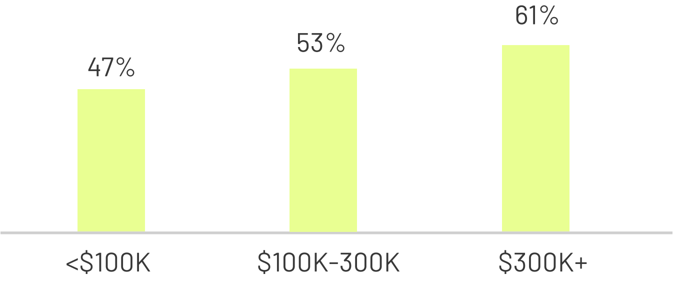
The folks at The Harris Poll wanted to understand the most pervasive pain points around observability. So, they talked to more than 200 engineering professionals who are responsible for observability and log data management at companies across the United States. Their findings are represented in this report.

TRUE OBSERVABILITY IS NOT YET ATTAINABLE

While most (85%) working in this space believe that true observability is possible, for most companies, true observability is not yet attainable. And it is often not for lack of investment. Two thirds of organizations surveyed are currently spending $100K or more annually on observability tools. More than 1-in-3 (38%) are spending $300K or more. Despite this, only about one-quarter (26%) strongly agree that their existing solutions provide true observability. Further, 52% indicate they wish they could use different observability tools – but for the moment are stuck with what they have.

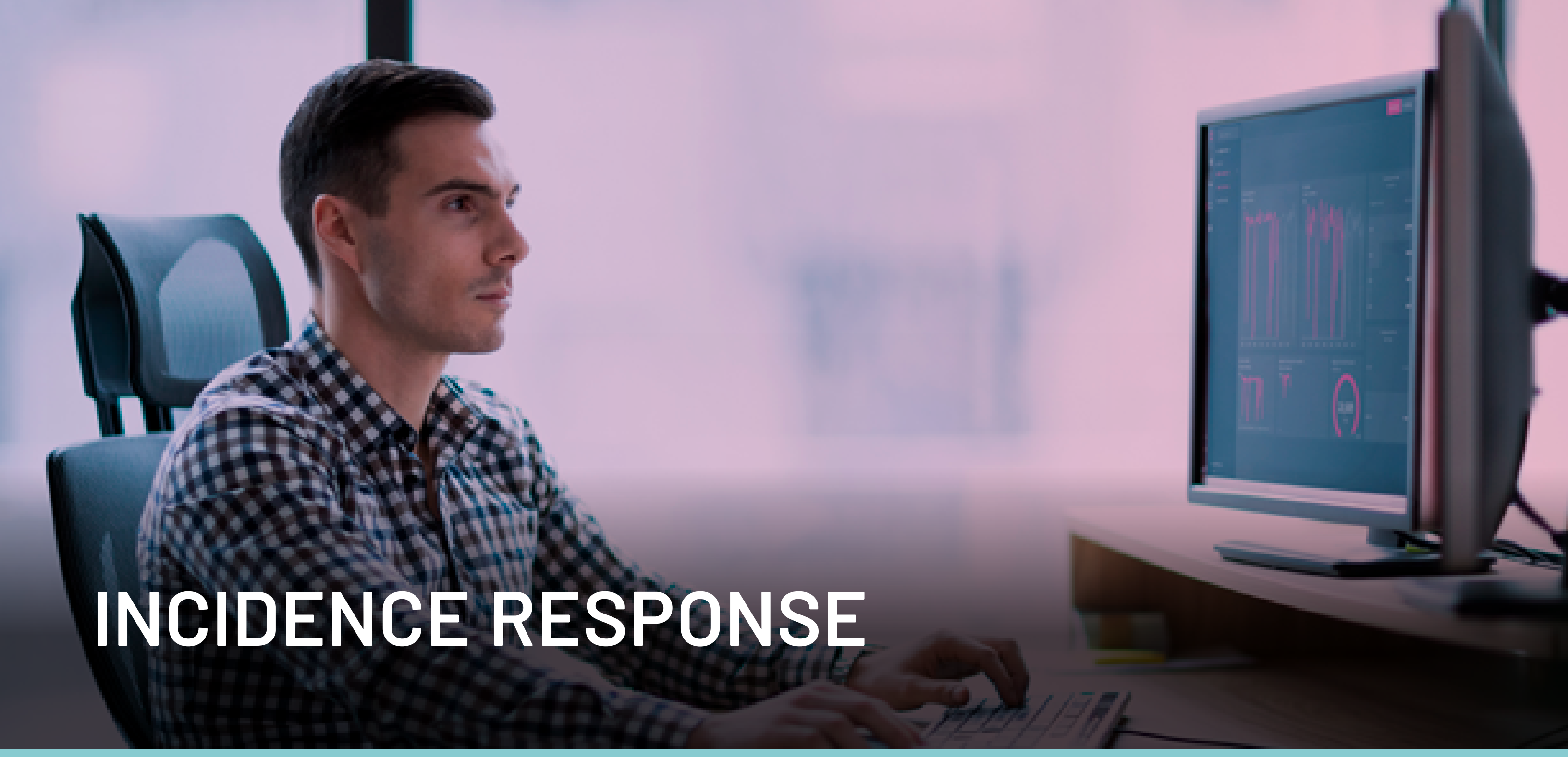
In short, organizations are not getting what they expected from these tools and need this investment to work more effectively.

% WISH THEY HAD DIFFERENT OBSERVABILITY TOOLS



RELIANCE ON LOG DATA

Log data is critical to tracking performance of applications and capacity resources, informing product improvements and to flag hacking or other unauthorized entry. Nearly nine in ten companies (86%) indicate they rely on their log data for these efforts. However, existing solutions on this front are not always successful. Fewer than half are very satisfied with their ability to use log data for any one of these purposes. Additionally, this use case for log data has the lowest satisfaction rates of any tested. Other pain points include ingesting a variety of log types into a standard format (32% cite this) and ingesting logs into multiple tools for different use cases (30%).



INCIDENCE RESPONSE

ENTERPRISES REPORT THAT INCIDENCE RESPONSE EFFORTS ARE LAGGING

Enterprises report that incidence response efforts are sub-optimal as when tools are applied, outcomes generated fall short of expectations. Issues stem from three key areas – the logging tools in place are not seen as easy to use, collaboration with colleagues on multiple teams is difficult, and there are challenges with routing security events.

Challenges with ease of use are more commonly cited by senior leaders (VP or above) with 82% of this cohort indicating response time is hindered because tools are not easy to use (vs. 64% in Manager roles and 61% among Directors). Also, those newer to their role are more likely than longer tenured employees to cite this as a challenge. These audiences may be less familiar with the tools, and as such, are not as easily able to navigate them.

In terms of collaboration challenges – these appear to exist across the organization, with all levels of seniority, tenure and co. size consistently agreeing on this as a challenge. The tools do not successfully enable multiple stakeholders across use cases.

On the security front, most organizations indicate they are confident that they can see security events in real time – only 1-in-10 say they do not have this visibility. Nearly all, 83%, agree that this visibility is critical in delivering faster incidence response. However, routing of the security events is a bigger pain point. Unlike ease of use, we see an inverse relationship between this challenge and level of seniority. Managers are most likely to indicate security routing is a challenge, followed by Directors and finally senior leadership.

66% of organizations say that they spend more time trying to resolve issues because their logging tools are **not easy to use.**

67% of organizations say that they spend more time trying to resolve issues because it is **difficult to collaborate** with colleagues & other teams.

58% of organizations say that **routing of security events** is a **challenge** for their teams.

SECURITY THREATS VS BUDGET

ON THE BIGGEST CHALLENGES LOG DATA POSES...

"It is always about data privacy and data management; cybersecurity is a big problem facing any organization that uses network information that can be easily tampered with."

"Cost is usually our biggest challenge."

LIMITING LOGS INGESTED

Security threats are at an all time high, but many companies can't afford to store the data to ensure a fast incidence response. More than half of organizations (57%) indicate that they limit the amount of logs they ingest or store due to costs. This rationing due to budgets means that a majority (63%) also say that sometimes they don't have the logs they need to troubleshoot or debug systems or an application because the needed logs were not retained.

This is a bit more common in large organizations (1000+ employees) at 68% vs. midmarket organizations (100-999 employees) at 59%. Interestingly, those with larger observability budgets are also more likely to report limiting the amount of logs ingested/stored due to costs. 68% of those spending $300K+ on observability vs. 53% of those with smaller budgets report this.

LIMITING VOLUME TO SIEM

Organizations are also limiting the amount of data that enters SIEM systems due to cost. Over half (55%) of enterprises are limiting this. The result of this rationing is that most (61%) indicate that limiting the volume ingested into SIEM systems slows their incident response.

EXPENSIVE & LAGGING SECURITY SOLUTIONS

A NEED FOR BETTER SECURITY SOLUTIONS

Organizations are also increasingly fed up with expensive and laggy security solutions. There are four primary pain points. First is system latency. More than half of organizations (59%) say that the volume of logs they currently send to their SIEM results in system latency. Managers are more likely than senior leaders to note this pain point.

The second pain point relates to cost. One-in-three (33%) say that the volume of logs they send to their SIEM results in cost overruns. Data suggest that this challenge affects companies of all sizes equally.

Analysis of the data is difficult due to the sheer volume. One-in-three (32%) of enterprises say that the volume of logs they currently send to their SIEM makes it hard to separate the signal from the noise.

This pain point is more common in mid-market organizations (100-999 employees) than in enterprise organizations (1000+ employees) at 38% vs. 27%.

Lastly, 39% of organizations report dropping of data – further complicating security matters.

Directly streaming log data into a SIEM may help with some of these challenges. More than 80% of enterprises are interested in the ability to stream log data to other services – and more than half (55%) would be interested in streaming log data directly to their SIEM service.
On an open-end basis, benefits cited included "better latency", "improved response time", "reduction of data storage costs" and "an extra layer of security recovery".

[Other top destinations for streaming log data include data access and automation platforms (63%), analytics platforms (66%), data warehouses (59%) or data lake (41%).]

ON MANAGING MULTIPLE TOOLS

"The biggest challenge is managing to select optimal tools within budget constraints."

"Every tool promises the moon but can't deliver when it comes to developing a process, so we end up with a lot of tools and processes."

USE OF MULTIPLE TOOLS & SPIKING DATA STORAGE NEEDS ARE ALSO DRIVING COSTS...

The average enterprise is using 3 or more tools (3.82 to be exact) to access their log data today. Not surprisingly, those enterprises spending the most on observability are also using the most tools. Those spending $300K+ are using 4.68 tools on average, versus 3.20 for those with budgets under $300K.

Spiking data needs are also driving organizations to look for ways to reduce their costs. Many are considering variable retention. 72% of enterprises are currently using variable retention functionality – and most agree (89%) feel the feature would be useful to their organization. Nearly half of those using this functionality (47%) indicate that the biggest benefit is reduced overall cost of operation.

Rehydration/re-ingestion from cold storage back to a useable interface is another feature that 91% of organizations indicate would be useful – but only 45% are currently using. While there are clear security benefits to this functionality – one-in three (36%) cite cost savings as the biggest benefit.

TEAMS ARE TALKING MORE THAN EVER – CROSS FUNCTIONALITY IS KEY

In addition to thinking about budgets when selecting tools, enterprises are also focused on cross-functional usage. On average, log data is accessed by 3.49 teams most commonly IT Operations, DevOps/Developers and Security. Given this, it is unsurprising that 82% of organizations indicate that multiple stakeholders need access to the same data. As such, balancing the need for data/insights with budgets, security and current levels of collaboration is key in helping organizations make the most of their log data.

"The biggest challenge is managing to select optimal tools within budget constraints."

IN CLOSING

Organizations need to drive more value from their logs. Most are deploying multiple tools at a significant cost but are unable to drive the needed outcomes. Finding tools that are effective across multiple stakeholders and use cases is challenging, as are finding tools that balance the need for strong security with budget realities. Further, there is an opportunity cost for all of the time spent managing sub-optimal observability tools.

Organizations should be asking themselves, 'What else could I be doing if I didn't have to spend time on this? What if the tools were easier to use? What if they better facilitated collaboration? What if they provided better security solutions? And all within budget?' For information on how one company is addressing these questions, visit Mezmo.com.

Want to learn more?
Reach out to outreach@mezmo.com

ABOUT MEZMO

Mezmo is a comprehensive platform to control all of your log data. Mezmo fuels massive productivity gains for modern engineering teams at hyper-growth startups and Fortune 500 companies, including Asics, Better.com, Sysdig, and 6 River Systems.

Since 2018, Mezmo has been the sole logging provider for IBM Cloud, where it partners to drive innovation in observability at hyperscale. The company has been recognized as one of Forbes' Cloud 100 Rising Stars, EMA's Top 3 Observability Tools, Gartner's Top 25 Enterprise Software Startups to Watch, and Deloitte's Technology Fast 500™.

ABOUT THE HARRIS POLL

The Harris Poll is a global consulting and market research firm that strives to reveal the authentic values of modern society to inspire leaders to create a better tomorrow. It works with clients in three primary areas: building twenty-first-century corporate reputation, crafting brand strategy and performance tracking, and earning organic media through public relations research.

One of the longest running surveys in the U.S., The Harris Poll has tracked public opinion, motivations and social sentiment since 1963, and is now part of Stagwell, the challenger holding company built to transform marketing.

Research was conducted by The Harris Poll among N=202 IT or Engineering professionals with responsibility for observability and log data management. All respondents are US-based full-time employees within organizations with 100+ employees, and all are Managers or above within their organization. Data was collected September 29, 2021 through October 17, 2021.

mezmo.com

Thank You

Sales Contact:	outreach@mezmo.com
Support Contact:	support@mezmo.com
Media Inquiries:	press@mezmo.com