



# The Guide to Modern Observability

Your observability journey starts here



Fundamentally it's about being able to understand how a complex system works. We work with weather companies monitoring weather stations in the oceans. We've got universities measuring footfall outside buildings and the carbon dioxide levels in lecture halls. From syncing listings for travel agencies to monitoring factory floors — this is all observability.



**Simon Hearne**

Solutions Architect, Elastic



# Four tips

How to maximize this guide in the least amount of time (you're super busy!)

1

Use the **TODO prompts** at the beginning of each section to make your notes.

2

Refer to the **TLDR boxes** at the bottom of each section to help inform those notes.

3

Check out the **red and green flags** to see how potential observability solutions measure up.

4

Download the **POC worksheet** to compile your notes — just like that, you've got a draft proof of concept!

# Table of contents

|                                                                                                               |           |                                                                                           |           |
|---------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------|-----------|
| <b>Unleashing the potential of modern observability</b>                                                       | <b>6</b>  | <b>People: Preparing your team to make the most out of modern observability solutions</b> | <b>35</b> |
| What drives modern observability?                                                                             | 10        | Building your observability maturity for a cloud-native world                             | 39        |
| Inspiring action: Defining your organization's future state                                                   | 15        | Potential impacts to your team's productivity                                             | 42        |
| <b>Organizational strategy: Establishing a vision for the future of your business</b>                         | <b>20</b> | The observability case for customers and executives                                       | 44        |
| Understanding the impact modern observability can have on your specific needs                                 | 23        | <b>Process: Preparing your current operations and workflows for modern observability</b>  | <b>47</b> |
| Assessing the costs involved in cloud migration and modern observability                                      | 26        | Impacts and improvements to your processes                                                | 50        |
| The tradeoffs and challenges between open source, open and extensible, and commercial observability solutions | 29        | Data storage and information lifecycle management                                         | 50        |



# Table of contents (continued)

|                                                                              |           |                                             |           |
|------------------------------------------------------------------------------|-----------|---------------------------------------------|-----------|
| <b>Technology: Preparing your tech capabilities for modern observability</b> | <b>55</b> | <b>Proof of Concept checklist</b>           | <b>69</b> |
| How does open and unified observability impact your current capabilities?    | 57        | <b>Start your observability journey now</b> | <b>70</b> |
| Your observability capabilities evaluation tool                              | 60        |                                             |           |
| <b>Executing your modern observability plan</b>                              | <b>66</b> |                                             |           |
| Preparing for a Proof of Concept (POC), major steps and milestones           | 67        |                                             |           |

# Unleashing the potential of modern observability



In today's insight-driven landscape, everything is data. Everyone is data. Hundreds of millions of impressions are made every day, creating new data points waiting to be ingested by businesses everywhere seeking to deliver data-driven targeted content and services back to you. When done correctly, data analytics is a symbiotic relationship. Organizations collect data and, in return, deliver great user experiences. When done incorrectly, it's a series of unfocused, unactionable loose ends with nowhere to go, signifying nothing.

According to Seagate, “only 32% of data within organizations is actively being put to work today, which leaves an undesirable amount of data taking up space and costing money to store without adding any value.”<sup>1</sup> There's no such thing as too much data — unless it's eating up your budget and letting all your telemetry and data collection work go to waste.

Only  
32%  
of data within  
organizations is  
actively being put  
to work today

<sup>1</sup> Rethink data put more of your business data to work—from edge to cloud, 2020. Seagate.

To get a return on your valuable data and data storage costs, businesses need to move from ingesting data to creating action from it. The potential of your data is boundless — from understanding user journeys and even generative AI training. It's waiting for you to unleash it. **But first, you need to understand it.**

For many businesses handling complex systems and logs upon logs of listless data, this calls for a unified observability solution to provide detailed, actionable insight to turn your data into a dynamic force.

You're here because you know your business needs an observability solution to put your data to work. Perhaps your cloud storage bills from a solutions service provider suddenly tripled overnight. Or you might have heard how a competitor improved time to market, increased efficiency, and grew revenue by implementing a better (read: unified) observability solution.

**Observability applications serve nearly every kind of business. And they affect almost every facet of its operations — its people, processes, and technology. Observability is based on the data your business generates. When an issue arises, the answer is somewhere in the data.**

Say you had an outage. Without adequate observability, your team is subject to another vicious session of finger-pointing. Then, the effect the outage has on your customers might cost you loyalty and trust. Down the line, this costs you revenue.

Then, consider the processes that could be affected. A lack of visibility into internal states and systems means a slower mean time to repair (MTTR), which snowballs into a slower mean time to deployment (MTTD), which inevitably slows down the speed of innovation (and voila, the technology piece). A modern observability solution can help:

- **Improve** team productivity and efficiency by consolidating disparate tools across dynamic environments. This has a direct effect on your operational efficiency.
- **Increase** customer satisfaction, which has a direct effect on your bottom line.

But observability goes beyond addressing the here and now.

When implemented properly, it can get you to a place where understanding your data means a proactive approach to business operations. Having visibility over your past and present operations is just the start. Full spectrum observability means establishing a future vision for your business and actioning your data insights to create proactive solutions. These can range from cybersecurity risk mitigation to using AI and machine learning to speed up innovation. And with increasingly complex networks accomplishing increasingly ambitious goals, your business needs to be multiple steps ahead.

This is why modern observability is built specifically to address today's dynamic architectures and multi-cloud computing environments. Cloud computing has developed to share and store data across distributed networks, so observability has evolved to manage the organizational needs of hyper-accessible, high-volume data across these cloud and hybrid solutions.

This breadth of technology can seem overwhelming for even the most forward-thinking decision-makers. Enter Elastic's Guide to Modern Observability.

By collecting and consolidating all the operational and business data you generate and deploying the right layer of observability on top of it, you can empower your organization and teams to make better decisions for today and tomorrow. We're here to help you understand the many benefits a modern observability solution can offer your organization and the considerations needed to guide your choice of an observability solution. Armed with a roadmap based on a people, processes, technology framework, you can transform your business through unified observability.

**Let's get started.**

## What drives modern observability?

By 2025, global data creation is projected to grow by more than 180 zettabytes (that's 180 x 1000 x 1000 x 1000 terabytes).<sup>2</sup> That's a lot of data. And it can be a gold mine for organizations. It can also drown them. The difference between thriving and sinking? Telling stories.

Data can tell stories about what went wrong and why, what isn't functioning optimally, what is successful and why. But in order for it to do so, it needs context.

Your service desk gets an alert: The traffic on your site has dropped, but your usage on mobile devices has spiked. Data says, "Uh-oh."

So, you pull more data from your website analytics. You discover desktop usage is down, but the distribution of traffic on iPads remains steady.

Data says, "Weird."

So you dig further, and zoom in on where your visitors are coming from. The geo-location data gives you the answer: Users left their desktops to watch a solar eclipse, resulting in a drop in desktop traffic. iPad users presumably went to their windows with their devices, and since their applications were still active, you received a spike in performance because of the change in traffic distribution. (Fun fact, this really happened).

Just like that, your data told you a story — and a true one at that.



<sup>2</sup> "Data growth worldwide 2010-2025", Statista.com, 2023

## Business problems are data problems

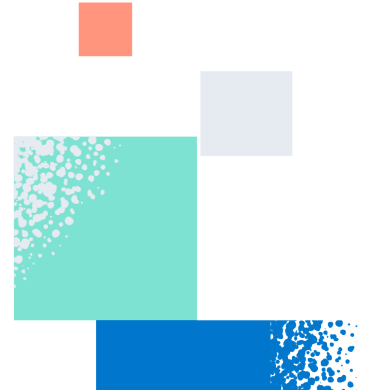
Did your website experience an outage an hour ago? Observability will tell you what happened.

Getting to those disparate sets of data quickly and correlating them in order to get the context and the story they're telling enables you, your team, and your organization to act. (Now in this case, there wasn't anything to do because the alert wasn't the result of an outage, but the actionable insight afforded by the data was: don't panic, everything is fine). In other words, **data, applied to its full potential, drives action.**

Nowadays, getting actionable insights from your data is the gold standard of business operations. But the amount of operational data your business ingests and generates every day is probably overwhelming — and it's growing larger every second. The average enterprise stores more than 71PB of structured and unstructured data on-premises alone, not even including cloud.<sup>3</sup>

In other words, **business problems are data problems.** How do you pinpoint issues, uncover root causes, and perform quick repairs for seamless customer experiences without chaos, sweat, and tears (from your team and your customers)?

An effective observability platform offers a suite of tools that will help find the right signals in that data, allowing you to more quickly address costly outages, monitor application performance, and detect untapped revenue streams.



<sup>3</sup> Meeting the new unstructured storage requirements for digitally transforming enterprises, 2022. IDC. [delltechnologies.com](https://www.delltechnologies.com)

**You want the observability solution you choose to say: We're going to give you that end-to-end view of what that application is doing. When something breaks, we're going to help you fix it quickly. And we're going to apply all kinds of analytics to help you do that in a very smart way. We're not going to give you the haystack. We're going to tell you where the needle is and give you the insights to guide your investigation.**

— **Chris Pozezanac**  
**Principal Solutions Architect, Elastic**

The quantity and velocity of the data your business generates, requires, and processes, creates a complex monitoring environment that can very easily hinder innovation and digital transformation if it's not being used well. Hybrid and multi-cloud environments in particular generate massive amounts of data, much of it siloed in different observability tools – business metrics are in the domain of one team, and performance metrics and logs are in another's domain.

These piecemeal data points, particularly when they're accessible only to certain departments or divisions, result in imperfect or incorrect insights into your operations.

For example, the swivel-chair phenomenon: What happens when your CRM tool provides you with one set of data that is contradicted by the numbers provided by your APM tool? (Hint: it's not good.) Decision-makers are forced to alternate between different sources of “truth” in order to gain insight into their business, and those data silos result in too much noise and often conflicting signals.

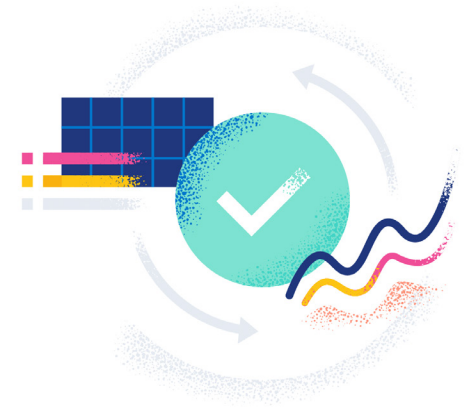


Aside from silos, the sheer amount of data to parse through manually makes the task extremely time and labor-intensive. This results in blind spots in your digital delivery system. With all that data, how can you possibly have blind spots? It's more likely than you think, especially if your company is still using disparate, legacy monitoring tools that don't provide the right insights or visibility into this new, complicated, cloud-first world.

With the amount of data generated per minute — gigabytes per minute, per domain — automation is required to collect and operationalize this data at scale. Artificial intelligence for IT operations (AIOps) and machine learning (ML) enhanced observability enables faster response times and drives better responses from automation and your team.

You're collecting information from all your verticals — business, marketing, operations, IT — but are unable to correlate the information without hours of painstaking work. On average, about 66% of repair time is dedicated to identifying the issue.<sup>4</sup> What, when, where, why, and who's in charge?

There's no efficient way to get to the root cause of suboptimal uptime on your website, or what's causing things to break down, or the core issues affecting performance. You're not getting real value from all that data, because you're unable to consolidate it and integrate it with business data to understand true impact. Moreover, your ability to achieve specific business outcomes can be slowed down or made more difficult because of trade-offs between performance and cost. You either have to pay a lot to have the data readily available, or store it in economical tiers which are slower.



About  
..... 66%

of repair time  
is dedicated  
to identifying  
the issue

<sup>4</sup> Simic, Bojan. "2022 State of Managing IT Performance - Key Takeaways", Digital Enterprise Journal

Observability is about your business's past, present, and future.

## Past

**Did your website experience an outage an hour ago?** Observability will tell you what happened.

## Present

**Is your business operating at peak efficiency?**

Are your services all functioning the way they should? Observability will give you tools to understand and improve.

## Future

**Are there opportunities for future growth that you're missing?** Observability will enable those insights.



TL;DR: What drives modern observability?

Data.

The terabytes upon terabytes generated and ingested by your organization on a monthly basis are a dead weight if not prioritized and interpreted – and actionable. In order to do that — to draw meaning from your data — you need a modern observability solution that enables you to correlate disparate data sets, monitor application performance, pinpoint issues, perform AI- and ML-powered analytics to speed up root cause analysis, troubleshooting, and ultimately get to a proactive operational stance. A place where the insights you gain from your data influence revenue-driven business decisions.

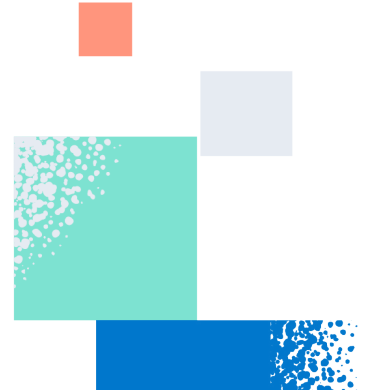
## Inspiring Action: Defining your business's future state

Imagine what would be possible if your business could discover actionable insights from all the data you collect, no matter where it's being collected. The ability to understand the real impacts of real-time data creates benefits that accrue in every aspect of a company's operations.

By moving your team onto a single data platform and tool that democratizes access to insights, you could empower your team to work smarter, not harder. The time normally spent reacting to issues, looking for the reasons behind an outage, and parsing through disparate datasets would free up. You could reorganize your resources into a more efficient machine that can focus on delivery and innovation. Growth possibilities and more. This is where modern observability comes in.

**Observability offers a business predictability – in spending, in operations, in development time – and scalability.**

— **Brian Retzbach**  
**Regional Vice President, Elastic**





## Tool consolidation

As we've discussed, data silos not only create inefficiencies but also hinder a holistic understanding of your business. The right observability solution enables tool consolidation to eliminate business blindspots by uniting multiple monitoring capabilities in a single tool. No more swivel-chair-related eye strain and en-masse mental fatigue. Distributed, complex cloud applications demand a unified and consistent tool to simplify their day-to-day management.

More effective tools empower your staff to be more efficient. Reducing the number of tools your team uses and deprecating unused tools helps everyone do more with less. Provided you support your team with the training to use a common platform, tool consolidation will inevitably increase productivity. And these productivity gains quickly translate into savings for your company.

## Faster fixes

A consolidated tool, or a correlated view into what went wrong, helps reduce the time spent troubleshooting. And it's a magic elixir: reducing MTTR means that both your engineering team and your customers can get back to normal more quickly. With fewer outages, your customer gets the experience that they deserve.

When your team doesn't have a unified observability solution, it can take hours to parse what's broken. And even when the anomaly is detected, what about the root cause analysis and resolution process? Many teams get stuck trying to figure out who owns what before they even get to fixing the issue.

Not with a unified approach.

## Supporting cloud-native transformation

In a cloud native environment, you benefit from the efficiencies afforded by containers and serverless computing. This architecture can support and scale your microservices and containers and help you deploy and run reliable applications. This approach offers many advantages, like improved scalability, faster time-to-market, and cloud cost efficiencies. It also creates a data-rich, and data-diverse complex environment, generating even more metrics, logs, and traces.

The disadvantage? Without an effective observability solution in place, it's difficult to understand how each of those microservices is working as a whole, identify choke points — especially when working with containers — and gain holistic insight. The data generated in this environment requires the context of the wider system in order to be valuable. A unified observability solution does just that. It gives you a system-wide view so you can pinpoint issues, correlate them to data across multiple sources, and take action.

## Performance optimization

Observability helps improve system resilience, as well as the use of IT and cloud resources. You can be more efficient, which means you can be more productive and focus on what matters: delivery and innovation. In other words, observability can empower your team to take a proactive approach to their performance.

Add AI to the equation, and you're talking about next-level optimization. Data can now help answer third-, fourth-, and fifth-level questions — not just what happened, but why did it happen? Where did it happen? How does this compare to previous events? Are the challenges similar, or different?

Taking it a step further, AIOps leverages the power, speed, and automation of AI for IT operations, such as observability. It offers teams the ability to perform root-cause analyses of complex problems and use predictive analytics to proactively prevent problems before they happen. And with generative AI now on the scene, we are just looking at the tip of the iceberg!



## Predictability

A modern observability solution ultimately affords your organization predictability in your operations, in your development time, and in your spend. Each of these business pillars is interconnected: getting predictability in one affects predictability in the next. Some vendors might get you up and running quickly, and their pricing models might seem predictable because they are familiar, but depending on what you use and how you use your observability tool, you might be looking at unexpected overages. Predictable spend starts with resource-based pricing that is transparent. Once your observability solution is up and running, it should help optimize your resource use, and in turn, stabilize the predictability of your spending.

## User experience and flexibility

The best observability solution should be a customizable solution that meets your unique use cases and addresses your specific pain points, while also remaining flexible enough to anticipate your business's needs six months, or six years from now. You want it to have the integrations and connectors for the sources you're using today, and for the services you'll want to use in the future. A solution that offers you predictability in spending, operations, and development time empowers you and your organization to prepare for the future.

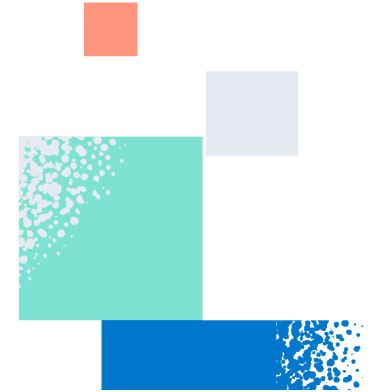
Equally important for achieving flexibility: no (minimal) vendor lock-in. You want a vendor who can support you when your needs change — because they will change — and who can offer you a solution based on open standards and its inherent flexibility.





## TL;DR

A unified observability solution provides current solutions and benefits: consolidating multiple monitoring tools into one, reducing mean time to repair and increasing team efficiency, supporting your cloud transformations, and optimizing performance which means higher productivity and returns. A unified observability solution also provides support for future functionality.



Preparing your business for such a transformation might appear daunting, but in fact, through ample preparation and a clear proof of concept, the journey towards a modern observability solution doesn't have to be disruptive.

**We're going to show you how.** Every section of this guide has a worksheet for you to make notes in, so you can think through your proof of concept, plan it, map it, and prepare for the next steps — making the change to help your business gain insight and visibility into a cloud-first world.

# Organizational strategy – Establishing a vision for the future of your business



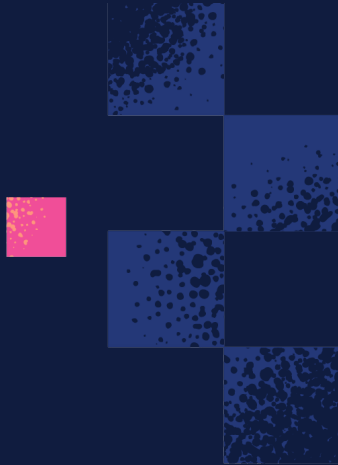
**TO DO:** Define your organizational goals. Refer to the future state you imagined earlier to set your organizational goalposts. Set SMART goals quarterly, bi-annually or annually in function of those goal posts. Outline how greater visibility and insights can help you get there.

## SMART

(acronym for specific, measurable, achievable, relevant, and time-bound)

Your business is always changing. Different types of outages and emergencies may have led you to adopt different tools over time. The first and greatest challenge of all might be getting strong leadership to have a vision and drive value from an observability solution that is implemented. That means setting organizational goalposts, training your teams, staying on top of the technology, and keeping an eye on the future.





Reversing a decision to move forward with the wrong platform, or a platform that cannot sustain your company's inevitable changes, is costly and incredibly difficult. Nobody wants to have to go back to the C-suite to ask for more money. When you choose an observability platform, you're making a choice that will define your organization for years to come. While you're addressing a current issue, it's always useful to maintain a forward-thinking point of view.

Thinking ahead to that future state prompts you to consider a solution that can help you achieve your 2-year plan or your 5-year plan. This might seem daunting, but observability can help you use data to actually determine what that looks like — and back it up with evidence. Returns like growth, innovation, and predictable pricing make it worth the effort.

## Define your organizational goals.

What are you looking to achieve in 6 months, 12 months, 24 months? Refer to the ideal state to set your organizational goal posts.

Ideal State:

6 Months from now:

12 Months from now:

# Understanding the impact modern observability can have on your organization

So you know why you need an observability solution, and you know that transitioning to unified observability can be intimidating — especially for the C-suite. You're talking longer term, significant investment, some potential restructuring... Who wouldn't get cold feet?

**Bottom line:** It is a big deal, and there's no reason to sugarcoat it. Focus instead on the positive business impacts downstream. Here are some talking points  to help you sweeten your pitch.

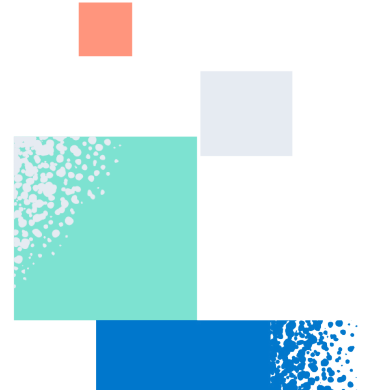
## Improving time to market

Consider this scenario: You validate your infrastructure with observability so you know it can take the resource load of a new application. The result? It's on the market faster, with fewer issues.

Now, say you run into issues. You've got a holistic observability solution that can help you pinpoint exactly what happened, address the issue faster, fine-tune the application, and boom — you're back on the market.

## Streamlined workflows for DevOps teams

Data correlation happens automatically with an observability solution, taking the load and the back-and-forth off of DevOps. A platform your organization trusts will eliminate unnecessary war rooms and allow your teams to focus on value-add performance and innovation.



## Improved customer satisfaction

Unified observability allows your organization to address outages faster, and to prevent them from happening at all. When your team can dedicate their time to performance and innovation, your customer benefits. Better functionality, faster response times, quicker repairs, mean you're meeting your SLOs and SLAs. In other words, customer needs are met — and that means happy customers.

## Measurable revenue-impact (ROI)

Observability has an important impact on revenue. When you improve how your team operates, and how your operations run, there is real money savings — not just cost avoidance. Not sure about that? Check out this case study. Proof in the pudding, if you will.



# Case Study: DISH Media

**DISH Media, a subsidiary of leading U.S. satellite and set-top box broadcaster DISH Network, was faced with translating data intelligence from 7.5 million subscribers across 25 million devices. It needed a hands-off observability platform that could handle high volumes of data, and consolidate and contain the data without manual analysis.**



## Before

Before implementing Elastic Observability, DISH Media was working with several tools and multiple teams of developers were charged with manually aggregating data and generating reports, plus responding to technical issues and raising red flags. As a business focused on growing and adapting, **DISH decided it needed to automate its data analytics process** to put more energy into innovation rather than reactive response.



## After

Implementing Elastic Observability gave the company a full spectrum solution with big revenue results. By automating the analytics process using AI and machine learning, **DISH Media eliminated the need for manual toil while also exponentially increasing the speed and accuracy of its data collection efforts.** Productivity skyrocketed as teams that were previously charged with data collection could focus on new, future-focused ventures.



Different areas of the company now have the data insights they need to engage and interact with each other in ways that boost agility, efficiency, and innovation. We're a faster and smarter and faster business now with Elastic.

---

**John Haskell**

Head of  
engineering,  
DISH Media

[Read the full story](#)

## Assessing the costs involved in modern observability

Every business has unique needs: some urgently need to address a recurring pain point, others need to deepen their visibility across the board, and some are ready to correlate IT operations to business outcomes. The costs involved in achieving modern observability follow the same range of variety.



### How does the current open source observability ecosystem impact your transition to unified observability?

Often, the biggest challenge is mapping what is deployed across the whole estate. You need to figure out what is being spent in aggregate across your teams, appreciate the value of what is deployed, and identify opportunities for improvement. Despite the savings and flexibility an open source ecosystem offers teams for scaling development and deployment, consolidating your estate across a unified platform with consistent dashboards may feel a bit out of reach.

The first step to assessing the costs involved is assessing your current environment, and zeroing in on your current goals and future goals for a modern observability solution.

You can factor in the cost of a consultant whose sole responsibility will be to assess your environment, or you can budget time for you and your teams.

While assessing your deployments to get a fair cost estimate may be the most challenging part of undertaking the transformation to unified observability, teaming up with a vendor who will guide you through a trial to understand your data ingestion and retention needs will ease the load. Bonus points if this is an assessment that happens over a limited term that is long enough to give you accurate insights (think 6 to 12 months).

## So, how does pricing work?

Know this: observability is not limited to a single line item or even a cost calculator, though that is often how it will be quoted. Pricing for a solution will vary depending on a host of factors: your needs, what hosting cloud provider/s you use (AWS, Google Cloud, Azure), ingest data volume, users, nodes or objects monitored, memory, or CPU used, data transfer volumes, data storage costs, and more. Different vendors will have different approaches to

pricing. And everyone on this journey, from change agents like you to developers, executives, engineers, and data analysts are all after the same prize: predictability. While the ever-changing nature of cloud-based technologies affords an inherent level of unpredictability, you shouldn't give up on the goal to get predictability, especially when it comes to budget and spending. Some billing models for your consideration:

**Licenses:** Some vendors will sell you a license to their platform. You make a minimum annual spend commitment and then consume that commitment. This is not a predictable spend.

**Subscription model:** This might be the most popular and widespread billing model because it is familiar (thank you, Netflix) to most. Subscription models sometimes tout turnkey pricing. Billed annually, they may be a predictable upfront spend but quickly become unpredictable as you work towards observability maturity.

**Pay-for-what-you-use:** Vendors will charge based on data ingestion and retention policies. Though it might seem a more complex billing model than a license or a turnkey model, it is the billing model that affords you the most predictable spend in the long run along with options to help you manage your spend.

# Red flags

**Some pricing factors aren't necessarily exposed on an order form.** A common scenario in the market is to commit to US\$500K, but end up doubling the spend. Why? A variety of components aren't reflected in what procurement sees, because they might be unknowns at the time the deals are structured. This is in part due to an honest lack of predictability, but it can also be a sales tactic from vendors to close a deal.

**Not all your data is valuable.** Not all your data is going to give you the insights you need. A pricing model that forces you to limit your data ingestion or adjust its granularity upfront makes it a challenge to explore and understand what data is of long-term value to your team and operations.

# Green flags

**If you make peace with the fact that there will be some variance due to the nature of your ever-changing environment,** which results in a lack of predictability, then you can go after the next best thing: **transparency**. Assessing costs with a vendor who can guide you through unknowns, and who is transparent about common unknowns is the gold standard.

**Understand what the premiums and penalties are** for overages because it's very easy to overlook them, and even easier to exceed those limits. Again, a vendor who is transparent with you about what a surge in traffic or a change in operations might look like on an invoice is what you're after.

**Resource-based pricing.** It might require a runway to iron out exactly how much in resources you need, but you want to work with a vendor who can guide you in that direction. The outcome? Once you've identified and created a baseline of your resource usage, you get predictability in costs for the long haul.





## The politics of observability costs

At an organizational level, another hurdle to overcome might be the siloed division of purviews, responsibilities, and budgets. Observability touches every department in your organization — whether they know, or care. This might mean that you will have to navigate some political challenges to implement a unified observability solution. Some departments might have certain budget allocations for observability or monitoring, while other departments might be capped and require a resource reshuffle. While this is very much a case-by-case situation, it is a common scenario. Don't let it get you down. You're not alone. If anything, this type of challenge makes the case for modern observability even stronger: opportunities to streamline spending and ditch unnecessary costs in sprawled monitoring efforts become possible. Take that to the C-suite.

## Choosing between open source and commercial observability solutions

**Fork in the road:** one signpost reads “open source”, the other says “commercial vendor.” Which way to go? Is one path better than the other? **Both choices are valid, but let's compare.**

As an organization, you can choose from a variety of commercial observability tools. Generally, these will enable you to scale quickly and offer access to out-of-the-box integrations, automation and professional support. From a user experience perspective, you get up and running more quickly, but trade that for vendor lock-in and limited flexibility for the future, which comes into play one year or two years down the road.

On the other hand, you might set off to build your own observability solution with open-source tools, such as OpenTelemetry (OTel), Loki, Fluentd, Prometheus, or OpsTrace, to name a few. Consider: You will need to bring together a few of these tools in order to ensure that you are getting the visibility and capabilities a commercial solution can provide. While this option guarantees

flexibility since there is no vendor lock-in, you're trading access to expert support for community know-how for maintenance, updates, solutioning, and trading a quick "install and run" for a significant period of development time for the initial deployment and ongoing maintenance.

So while a commercial observability solution might limit you to specific use cases either due to capability specialization, or because of budgetary constraints (maybe

it costs too much to correlate IT operations to business metrics because of their billing model), you might be limited capabilities-wise with a DIY solution due to resource constraints, i.e. your team isn't big enough to spend the time required to build and implement the solution for maximum positive impact.

Now consider another option — a third signpost?! — **open and extensible** commercial software. It's a full stack observability solution built on open standards data collection

(such as OpenTelemetry), with readily accessible data, and open machine learning models, that allows you to customize your observability solution to meet your use cases for today and tomorrow. It's a handsome alternative to building from scratch or getting locked in with a more traditional vendor. You get both a dedicated support team and an established community support network along with crowd-sourced resources as well as professional services teams that support your customization needs.



## Open source

Build your own observability solution with a flexible, DIY approach and no vendor lock-in.

## Commercial vendor

Get your observability running fast with an out-of-the-box solution offering scalability and support.

## Open and extensible

A full stack observability solution built on open standards data collection, allowing for customization.



**People don't want to be locked into a specific solution – they want to be flexible. They want to be able to adopt new technologies when they want to, at their own pace, and know that it's not all going to be gone tomorrow. The open source community really helps bake in all of those advantages.**

— Brian Retzbach

## Cost effectiveness of open standard, and open and extendible software

The biggest advantage of going with open standards such as OpenTelemetry for your observability data architecture (ingest, schema) is no vendor lock-in, meaning it is relatively easy to switch to a new vendor if your current vendor increases the price.

That's right — flexibility.



## Ahem, what is OpenTelemetry?

Thanks for asking! OpenTelemetry is an open source observability framework that enables development teams to generate, process, and transmit telemetry data in a single, unified format. Telemetry data is the umbrella term for your logs, traces, and metrics, which are the data pillars of observability solutions. OpenTelemetry can accommodate changes to your systems, back ends, and processes, so you're never locked into a single platform, solution, or contract, allowing your organization to expand and adapt as your technology needs evolve. That independence and flexibility means you can base your business decisions on what's best for your bottom line and customers — not the limitations of your technology. OpenTelemetry is the future of observability.

The cost-effectiveness of using open and extensible software, which offers you open data (you own your data), based on open standards, and the ability to extend the solution to integrate with all your tools, comes back to the notion that every business use case is unique. Your observability solution should be tailored to your needs, and going with an open standards-based observability solution is an excellent way to do just that. While a simple proof of concept may work for your more common use cases, it rarely prepares you for a future state, real-life events, and new technologies that are just on the horizon.

Taking an open and extensible route might prove a double-edged sword at the beginning. The flexibility can mean it takes longer to set up — the paradox of choice, if you will. But once it's up and running, an open and extensible solution ends up being more cost-effective because it enables you to evolve and future-proof your solution in the direction your business scales, especially if you're only paying for the resources you use. Think thick brush and hills for a few miles and a progressive easing of the trek on your observability journey.



## How does a vendor's stability and size impact your transition? How can the right vendor enable it?

The more established a vendor, the more robust the professional support. Every case is unique, but the bigger and more mature the vendor, the larger its community, and the wider its experience in problem-solving unique cases. In other words, a vendor's stability and size will influence how reliable its service and consulting arms are. Funny image, sure, but on the road to unified observability, everyone needs a helping hand.



# Red flags

**A solution that has limited interoperability with other tools and platforms may not be able to support your future use cases or technology ecosystem.** Lack of flexibility and lack of adherence to open standards isn't worth the spend — it'll be a sunk cost. Open APIs and open standards are key because they will enable future use cases.

# Green flags

**Data nerds:** You want to work with a vendor who will help you understand your data so you can get real, actionable insights from it. You don't just want information, you want your data to give you real meaning that is relevant to your team's and organization's goals.

**Help from the machines:** Observability is all about actioning the avalanche of data generated daily. This requires tools that can properly analyze huge volumes of data so that you can get true value from it. Think AIOps and ML.

**Access to a community:** This may not be so much for the C-suite, as it is for the technicians and practitioners on your team who will be interacting with the nuts and bolts of the technology every day. Having a community — and the ability to communicate with them easily — is an invaluable tool for continuous improvement.



## TL;DR

The digital environment is ever-changing. Your use cases are unique to your organization and your observability solution should be designed to meet those needs — even those that you don't know about yet. Getting to that state means asking how your organization is currently affected by the lack of observability and what it will gain from end-to-end observability. Transitioning from a piecemeal observability solution to a unified one comes with a set of cost considerations that are specific to your organization, but as a rule you want to achieve two things: predictable spending and implementing a future-proof solution.

In order to do that, you want to maximize interoperability and avoid vendor lock-in. This strategy affords you freedom from their sudden price increases, and the independence and flexibility to customize a solution to meet your needs now, and in the future. Meaning, you can base your business decisions on what's best for your bottom line and your customers, rather than the limitations of your technology. And that, change agent, bodes for blue skies ahead.

# People: Prepare your team for making the most out of modern observability solutions



**TO DO:** Identify the people who will be affected by this transformation, and how they will be impacted. Consider your DevOps team, your IT team, and your project managers. And don't forget about your customers, your execs, and other key stakeholders.

---

It's time to get your team and business stakeholders on board. An observability solution has a cascading effect on the organization – it also touches different teams in your organization: DevOps, IT, project managers, executives, and customers.

**Identify the people who will be affected by this transition, and how they will be impacted.**

Consider your DevOps team, your IT team, your project managers, but don't forget about your customers, your execs, and so on.

People affected:

---

---

---

The effect:

---

---

---

How to facilitate a smooth transition:

---

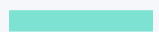
---

---





When I see clients successfully implement an observability strategy, it becomes fun for them. It's about empowering teams to be competitive, to be engaged, to have metrics that they can improve upon and celebrate. Being able to democratize data like that across an organization brings people together to work toward a common goal.



**Simon Hearne**

Solutions Architect, Elastic



In spite of being a wide net to cast, it is worth your time to think through how the observability transformation will affect each of these groups of people — because it will. This thought exercise should lead you toward another inevitability: reorganization.

## Showdown: the specialist vs. the generalist

There are two types of IT analysts in this world: specialists and generalists. An individual can be both, but if you have a small team a generalist usually takes on observability duties. They're collecting logs, analyzing logs, making sure things are running properly — and also doing application performance monitoring (APM). This is your swivel-chair analyst.

Larger teams have room for specialists, though smaller teams are also trending towards specialization. With the right tools, specialists can ask deeper questions: What are people doing in the app that we didn't expect? What are certain types of requests or searches that we didn't plan for? These questions cascade into what your developer team is doing. The same can be true for front-end teams. They can monitor with synthetics and ask questions like, "What if a customer clicks on this 28 times? Will the site crash?"

With the right observability solution, you can empower your generalist to delve deeper and be proactive, and your specialists to break down their silos and work together more effectively. A unified observability platform will be foundational to making your staff more productive

## Showdown



### The specialist

- Hone in on a niche
- Ask deeper questions
- Track specific results
- Collaborate with specific teams



### The generalist

- Overall visibility
- Collect and analyze logs
- Collaborate with all teams
- Application performance monitoring (APM)

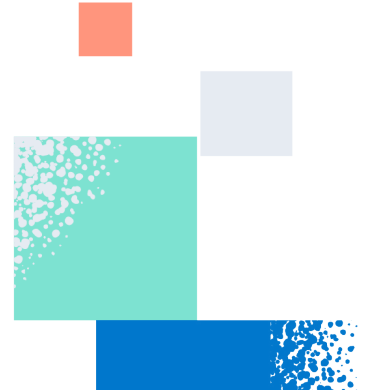
as it provides both breadth and depth for the people on your team. And it goes further than that: bringing your team together around a new, common platform gives them ownership over their work and shared responsibility so they can truly invest in their success and the organization's success.

**Observability isn't just going to help a business operate better, but it's also going to help people provide receipts for their own success. Executives don't want to just hear that you're doing a good job, they want to see data. Observability is a great way to put real numbers behind the improvements that you're responsible for.**

— Stephen Shepperd  
Senior Manager, Solutions Architecture, Elastic

## Building your observability maturity for a cloud-native world

Once you've outlined possible ways to reorganize, you can start planning how to set yourself and your team up for a successful migration to unified observability. Reaching observability maturity isn't a one-and-done process. It takes place over time, it is something you and your team continue to move towards. Evaluating maturity begins with people and culture. They are at the core of your organization, so setting them on the path to achieving observability maturity is how your processes and technology follow suit.



To do so, consider the importance of these strategies to prepare your team for modern observability.

## Build centers of excellence

It's important to front-load adoption with training. Budget in training — it's an invaluable piece of the puzzle. It's what will enable the tool's primary users to thrive, deliver results, and ultimately, ensure that your leaders see the return on their investment.

Once your tool is in place, ensure that you keep a regular training cadence. Within a single year, you might see an entire engineering staff rotation. For this reason, training refreshers ought to happen for however long you invest in a given technology.

You might also consider offering your team professional observability-related training and certifications. An observability vendor with an established training program helps you get your staff up to speed and can help you find additional talent as your organization grows. From public classes to private corporate classes, training and knowledge transfer is crucial for the success of a modern observability effort.

**Sometimes we see businesses don't want to build in training and education. They'll say, 'My team is super smart and savvy. They can figure it out.' Six months later, they'll reach out and ask for training. And it's not even disruptive or time intensive. We're talking about two or three day workshops held quarterly or biannually. And that training goes a long way in ensuring that businesses are getting everything they need from that observability platform.**

---

**Brian Retzbach**

## Establish best practices

Setting up an observability solution is an endeavor, but it doesn't have to be disruptive. Normally, the new system will be installed to run parallel to the old one, as you phase the old system out. To avoid unnecessary confusion and frustration, establish best practices. Instruct your team to always start with the new system during this transition period. If something is missing, report back and use the old system. As painful as this may be, this period will help you identify and document gaps, and patch them.

## Institute team knowledge and experience sharing culture

Part of any successful change is culture. (How did Crocs become fashionable and cool? Cultural shift.) The same is true within your team. Are your functional teams siloed? Is there limited access to observability dashboards, and are a handful of SMEs the sole guardians of key expertise? What's the experience like for new hires? Are they empowered to get on board quickly and contribute, because of the robust training they have received? All of these questions relate to your team culture.

You want to shift your team culture by breaking down data and consequently, knowledge silos. Finger-pointing turns instead into shared responsibility and a no-blame-ocracy. Cross-functional teams are strongly aligned and have self-serve access to observability data, documentation, and tooling, which enables team members to make autonomous decisions.

Creating a space that values communication for troubleshooting and supporting colleagues will give your team ownership over the transition and most importantly, buy-in — two birds, one stone. This way, the solution gets up and running faster.



## Possible impacts on your team's productivity to look out for

### Red flags

**Anticipate resistance and fatigue from your team:**

Possible scenarios like, "I could do this on the old system in one click and now I can't." "How is this different from the last solution we implemented and are now stuck un-implementing?" "I don't have the time or energy for this."

**Be cognizant that a lot of change all at once is**

**overwhelming:** A major technology transition also means additional responsibilities tacked onto already full workloads.

### Green flags

**Prepare your team for the long haul:** Implementing an observability solution, like any other new technology, will require more time and energy from your team.

**Upfront training time:** Your team should spend time understanding the tool, how to use it, and how to gain the most value from it.

**Evaluation time:** Your team and the vendor need to evaluate what data is going to be most valuable and how much of it you are generating.

**Migration time:** Depending on how much data and what kind of data you have, factor in migration time.



Coming to your team with a plan that factors in the extra hours, flags possible hurdles, and gives them a clear understanding of the benefits this transformation brings can help quell resistance and get their buy-in.

## The impact doesn't have to be sudden

Equally concerned about the additional lift, the disruption of workflows, the resistance, and the fatigue? The impact of the transition doesn't have to be abrupt. The transition can (and will likely) span over several months giving everyone — yourself included — much-needed breathing room. Focus on addressing a specific pain point first, and keep problem-solving, one issue at a time. This way, your team stays focused and on task and maintains clear stakes in the process. Soon, issues become opportunities instead: your team can go from being reactive to being proactive.

**The expansive nature of observability can be a blessing and a curse. So it's important to stay hyper-focused on what you're looking to solve for right now. Let's address a specific pain point first, and not try to boil the ocean. And as an organization matures, the product should mature alongside it.**

— Stephen Shepperd

## The observability case for customers (and executives)

You've charted the obvious people impacted by a transition to unified observability: your DevOps team, your IT team — and the tool's end-users. But two other sets of people deserve your attention too: your customers and company's executives.

The executive team will be your purse strings for this transformation. They will be impacted by it through their investment. So let's talk about the return.

Unified observability has a cascading effect on your business. Say your e-commerce site experiences an outage on Cyber Monday. It goes without saying that this disruption negatively impacts your customers, and adversely affects your revenue. If your site is down for 10 minutes on a day that has 2.5 times the online shopping activity of a regular day, it's easy to say that those 10 minutes were 2.5 times more disruptive than they would have been on a normal day for 2.5 times your usual volume of customers. That's a significant revenue loss.

Your observability solution is piecemeal, your tools and teams are siloed? Your team will likely spend precious time (time is money, after all) contacting the person who is in charge of this data stream, to then contact another person who is in charge of another signal, to then figure out who owns what and how to go about fixing it.





# Case Study: UK Betting Company

**UK Betting Company is one of the most popular sites for sports betting on the English Premier League, the Grand National, and even giant events like Wimbledon.**



## Before

There are two main concerns for any betting platform: it has to be fast, and it has to be fair. To make sure its site was speedy and the betting process was seamless, UK Betting Company needed a flexible observability solution to manage fast-growing, unpredictable log volumes. UK Betting Company's Infrastructure Platforms team was seeking a system solution to manage enormous capacity loads without compromising the user experience, and the team's efficiency.



## After

With Elastic Observability, AIOps spots and stops fraudulent behavior by analyzing user patterns. If there is a need for human intervention, Elastic's observability tool seamlessly connects to Slack to alert a UK Betting Company specialist to review the activity instantly. With easy implementation, dynamic pricing, and real-time results, Elastic Observability transformed the betting process for the UK Betting Company's in-house team and its users.



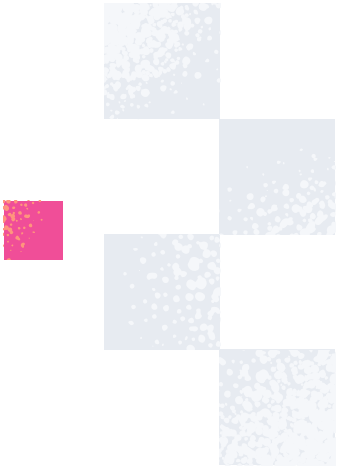
By using Elastic Observability, we've reduced overall fraudulent activity by 84%, helping to save the business more than \$5 million annually.

**Fraud Strategy  
Manager, UK  
Betting Company**

[Read the full story](#)

Having an observability solution where your tools are consolidated and signals come into a single application where you can correlate them enables you to quickly pinpoint what caused the outage, and means that your mean MTTR is that much faster.

And what does that mean? Happier customers. Happier customers generally mean better revenue and a stronger brand. So naturally, happier customers mean happier executives.



## TL;DR

People are at the core of your organization. Observability — modern, unified observability — starts with you and your team. And it affects everyone in your organization and anyone interacting with your organization.

In order to benefit from the effects of unified observability — detecting untapped revenue streams, supporting rapid DevOps initiatives, reducing workloads, reducing costly outages, boosting productivity and team morale — you have to front-load adoption with training, establish best practices, consider how to reorganize your team for improved efficiency, and institute a culture that favors collaboration, autonomy, knowledge-sharing and ownership over the processes. Getting buy-in upfront from your team is key to a successful transformation.

# Process: Preparing your current operations and workflows for modern observability



**TO DO:** Identify which business operations and processes will be impacted by the transition. Outline what will be improved and what common pitfalls to avoid.

---

Once you've spent the time reviewing how the people of your organization will be impacted, you can move on to the next part: the processes. As you now know, transitioning to modern observability doesn't have to be disruptive. While it is a process that happens over time and with support, it will nonetheless affect the processes and workflows of the people on your team who are using the tool every day.



The first step to managing the transition effectively is ensuring that you understand the steps involved in the transition. In most cases the process begins like this:

## Step 0

### **Training**

You'll want to start training your team using a sample of data. Ingest it, then work with the vendor or an expert to train your staff on how to look at it and how to enable it. As part of this training, you can test customizing the data. This is the opportunity to understand which customizations are most valuable to your team and their operations.

## Step 1

### **Instrumentation**

The vendor will spend some time observing your environment and the data in it. In this phase, you will install the necessary agents and integrations to get your data into the right platform.

## Step 2

### **Data customization**

Once the data is on the right platform — and this is best done not all at once, so your staff can get a solid grasp of the process — you begin customizing the data, transforming it, or 'molding' it to your specific needs, based on what you learned in the tests performed during the training phase. Build out the desired visualizations and dashboards so you can understand what is happening in your environment at a glance.

## Step 3

### Measure impact

The data you customized will give you insights. Act on them. What's more, measure the impact of these actions. This is a crucial and often overlooked step in the adoption of an observability solution. Measuring impact and developing KPIs enables you to fine-tune your tool and processes, and provide success receipts to your team and higher-ups. To do so, implement performance indicators and metrics that are relevant to your business. They might be related to performance, to productivity, to service delivery, or to revenue conversion.

## Step 4

### Monitor and improve

Then, we might say sit back, relax, and watch it all flow, but your continued involvement as a change agent is required. It's in your best interest to maintain an executive touchpoint with your observability vendor to ensure that you are making the most of your solution. Then, you can kick your feet up and appreciate the impacts and improvement to your process.



### The part before Step 0 – data discovery

Many organizations don't have a clear understanding of all the components and technologies used in their environment. If you don't either, don't fret, you're not alone. Don't know how much data is being generated so can't figure out your data ingestion needs? Again, you're not alone.

Bring your team leaders into the discussion, getting their feedback and their estimates. They're on the front lines. At this stage, you're on a discovery mission. Any and all information is valuable for sizing your deployment. Need additional help? Some observability vendors can provide this service to support your POC.

## Impacts and improvements to your processes

Depending on your situation, the impacts to your processes might not be felt much — that's the ideal state. For that to be the case, there are several things to consider, from how a new tool integrates with your existing processes to data management capabilities. To provide receipts of your success, you'll need to measure the impacts and improvements to your processes.

### Managing the transition to a new tool

Your team and resources will be impacted by both the transition and the completed migration to modern observability. Consider:



**Is the process compatible** with your current continuous integration/continuous deployment (CI/CD) toolchain? The transition should be tailored to your specific constraints and needs for your developer team before an application hits production.



**Does your entire team get access** to training and tools that provide common information, or a single source of truth? Democratizing access to information vital to repairs, and access to the tools

that provide this information helps expedite root cause analysis (RCA).



**Does the tool integrate easily** with alerting and service desk tools? You don't want to add unnecessary processes to your team's already stacked workload.



**Does the tool automate** the triage process? This helps reduce MTTR, which means your team can focus on delivery and innovation.



**Does your current environment support** AI and ML integrations? These capabilities are key for automation, which enables your team to work efficiently. Bonus: It's how you achieve observability maturity.

## Data storage and information lifecycle management

When looking into an observability solution, you will consider how much data you want to store and will need to store. But don't forget the importance of data sovereignty and compliance. Depending on your geo-location, what data can you store and where?

# Green flags

**Data ownership:** You should own your own data and you should be able to access it whenever you want, without proprietary tools and at no additional cost.

**Guidance on compliance:** It's important to have a vendor who has a firm grasp of compliance complexities. There are GDPR and geo-location-specific needs, and the rules are ever-changing.

**Data flexibility:** You want to bring in all your data. That means structured, unstructured, and semi-structured — be it operational data (logs, metrics, traces, events, etc.) or custom business data. Find out whether the vendor can handle the different types of data you need..

**Data access:** Look for a vendor that gives you the ability to search and apply analytics across all your data, even across boundaries, without needing to rehydrate your data from archival storage. In other words, you want a vendor who can give you access to all your data in minutes, not days.

## Measure service delivery improvements through improved metrics, KPIs, SLAs, and SLOs

Different businesses will measure improvements, well ... differently. But consider these metrics as you outline KPIs, SLAs, and SLOs:



**Revenue conversion:** With an observability tool in place, you can see what metrics are driving revenue up — or down. Say your e-commerce site is down for a minute. That equals x amount of dollars lost. If you can quickly pinpoint why it was down, and get it fixed, you reduce the loss.



**Operational efficiency and tool consolidation:** By consolidating tools, you are increasing operational efficiency. Everything is in one place, accessible to the people who are keeping things running. A single source of truth simplifies everything you do.



**Staff efficiency and cross-team collaboration:** Tool consolidation and unified context also affect your staff's efficiency and ability to collaborate. You can do more with fewer war-room sessions. Say it normally takes 10 minutes to troubleshoot an issue. With your observability solution in place, it takes five minutes. That's a 50% productivity gain on the MTTR. Time is money and a unified observability platform will save you time. Over the long run, staff efficiency enables the reallocation of resources from tactical fixes to strategic initiatives.



# Case Study: Glencore

**Glencore, a global energy trading company based in London, New York, and Singapore, uses a mixture of in-house and COTS applications to trade, optimize, and schedule oil, gas, and power transactions across multiple markets.**



## Before

While emerging energy trading technologies are constantly changing the landscape, responsive systems are necessary to deploy new features and applications. Plus, working across multiple markets in such a global field, real-time tracking is crucial for issue resolution and up-to-date response times. With so much data to log and analyze, Glencore wanted a full-spectrum solution that allowed for greater visibility. Its time-sensitive operations required real-time access to data and constant updates on performance and availability issues.



## After

Elastic currently supports Glencore's development, testing, quality assurance, and user acceptance testing functions in one cluster. In another cluster, they focus on production and business applications. Having the data and analytics on hand makes Glencore more proactive, rather than reactive, resulting in increased production speed and better customer service. This mitigates revenue loss and bolsters the performance of business-critical applications.



Elastic gives our DevOps team the speed and visibility to fix issues while maximizing our trading application performance. It means we can more proactively respond to general service issues, but also lower-level difficulties where reference data is missing. It's a significant step up in our support capabilities.

---

**James Lamb**

Head of DevOps,  
Glencore UK Ltd

[Read the full story](#)



## TL;DR

A unified observability solution may or may not have a felt impact on your processes for two reasons. The first is that every business case is unique: where you are in your journey to unified observability, what specific pain points you need to address in the now, what your team culture currently is — all of these aspects and more, will influence which processes are impacted by your observability solution, and how.

The second reason you won't feel a seismic shift in your processes: the process of adopting unified observability doesn't need to be disruptive, nor sudden. It happens over time, with support. (Good on you for budgeting that in!) Part of the considerations at this stage are data-related, too. Does the vendor insist that all your data go to them? Do you own all of your data? Does the vendor help you meet geo-compliance requirements? All of these questions have repercussions on your processes — do you have to wait and pay to access historical data required for an audit? Do you spend unnecessary resources on ensuring compliance?

The answers to these questions should also be part of how you measure process improvements. It benefits everyone to have success receipts on improvements in operational efficiency, team productivity and collaboration, and to see how all of that impacts revenue conversion.

# Technology: Preparing your tech capabilities for modern observability



**TO DO:** Define what technology you need to adopt your observability solution, and what changes your current technology and tools will undergo when you adopt your solution. Identify crucial points in your adoption timeline to set tool onboarding, training, and launch deadlines.

---

**Identify which business operations and processes will be impacted by the transition.**

Outline what will be improved, and what common pitfalls to avoid.

Operations affected:

---

---

---

Improvements:

---

---

---

Pitfalls to avoid:

---

---

---

## How does open and unified observability impact your current capabilities?

Observability is the process of understanding complex systems — from e-commerce to financial institutions to manufacturing. It applies to everything.

Getting your tech ready for modern observability requires you to review why you need it and understand the current gaps in your capabilities. What data can't you correlate? What's a recurring issue or use case that takes time to resolve? The best solution will begin by addressing a primary pain point, getting that right, and then growing into a unified solution — you're not going for the whole cake in one bite. One slice at a time.

Think of landing and expanding, one observability capability at a time now that you've got a unified platform to lean on. You'll go from simply monitoring to addressing visibility gaps and improving team dynamics. Then, you'll eliminate silos by democratizing access to tools and data. Eventually, you'll get to tying business data objectives, refining processes, and doing so by leveraging cutting-edge tech. This process will look slightly different in every business context due to a



## Achieving observability maturity

There are different stages of observability. The final destination? A modern, unified observability solution that leverages the power of AIOps, generative AI, and ML — which enables you not only to monitor and understand past and present states but also empowers you to take a more proactive approach to continually improve your future state. That's the direction you want to head towards. But there are important pit stops along the way, important steps you don't want to skip.

variety of factors: budgets, size of enterprise, available resources, current capabilities, and business priorities.

## Compatibility and open standards

When choosing a tool, consider your current ecosystem. Will native OpenTelemetry technologies help you avoid vendor lock-in? Is there value in an open and extensible platform to integrate with other mission-critical tools and data sources?

## The role of AI in improving your capabilities

While there is much you can achieve before you apply AI to your observability solution, the technology is an important consideration and component of an end-to-end solution. AIOps enables anomaly detection across all your user, application, and infrastructure data with minimal configuration work (if the vendor offers the option). Built-in machine learning can automatically correlate anomalies to downstream data and dependencies. This empowers your teams to quickly find the root cause of an issue and expedite debugging. Ultimately, AI and ML are the (not-so) secret weapons in your observability arsenal. An observability solution that has these capabilities improves productivity for your developers, SREs, and DevOps teams.

## Common gaps in capabilities

It's likely that you lack visibility into complex cloud-native technologies. If you're using serverless functions, you probably have visibility gaps because there is a vendor between you and the servers. If you're using Kubernetes to run containers, you run into the same issue. Ephemeral container runtimes also have an impact on your visibility, what they afford you in agile development, they cost you on effective monitoring. Favoring scalability, event-based architectures make it more difficult to track transactions, and to see correlations between datasets to resolve issues. AI can help you fill in the bigger picture and make connections.

Not sure about AI?

# Case Study: BPCE-IT

**As the second-largest banking group in France, BPCE is committed to the digital transformation of its subsidiaries and services. Gleaning actionable analytics from high volumes of data allows BPCE to provide high-quality service and develop even more ways to bank with BPCE.**



## Before

BPCE collects up to 10TB of application data a day. With this formidable log volume and ambitious data goals, BPCE-IT (the independent IT entity serving all subsidiaries of the BPCE Group) set out to create a unique solution to meet its unique needs. It was particularly attracted to AIOps, hoping to implement automation technology to centralize data and utilize the power of analysis and machine learning.



## After

BPCE-IT created an Elastic-based monitoring system named THEIA to optimize its usage of data and implement AIOps. THEIA, built and run on Elastic, allows BPCE-IT to manage its interconnected applications, which run on multiple servers. THEIA uses AIOps and machine learning to give teams visibility of the entire complex ecosystem, making it easier to spot anomalies, tighten security, and ensure complete confidentiality.



By combining a strong ingestion capability with machine learning analytics, we knew we could deliver new experiences to our users and help teams to collectively improve their analytics capability and quality of service. Elastic Observability provided a powerful and scalable solution to monitor all our data and get value quickly.

---

**Antoine Chevalier**

Head of data for ops, BPCE-IT

[Read the full story](#)

## Your observability capabilities evaluation tool

By this point, you have a clear understanding of what you want to accomplish organizationally, who will be impacted, and which processes will change. You know what you need. You have a clearer sense of how to get there. Now, you have to choose your observability solution — your superpower, if you will.

As for its capabilities, it should fulfill the following core use cases:

### Monitor and respond to system performance

Your observability tool should enable your IT team to debug and monitor application performance, and get insights about the health of your services and systems. For your DevOps team, an observability tool helps monitor everything from average response times for any operation, to what's causing uptime issues. In addition to this, your observability tool can point you to what services need tuning, or how certain changes might have affected application performance and latency. When data is correlated, an observability solution can inform you of your user experience, so you can keep a close eye on your SLOs.

### Increase business performance and improve productivity

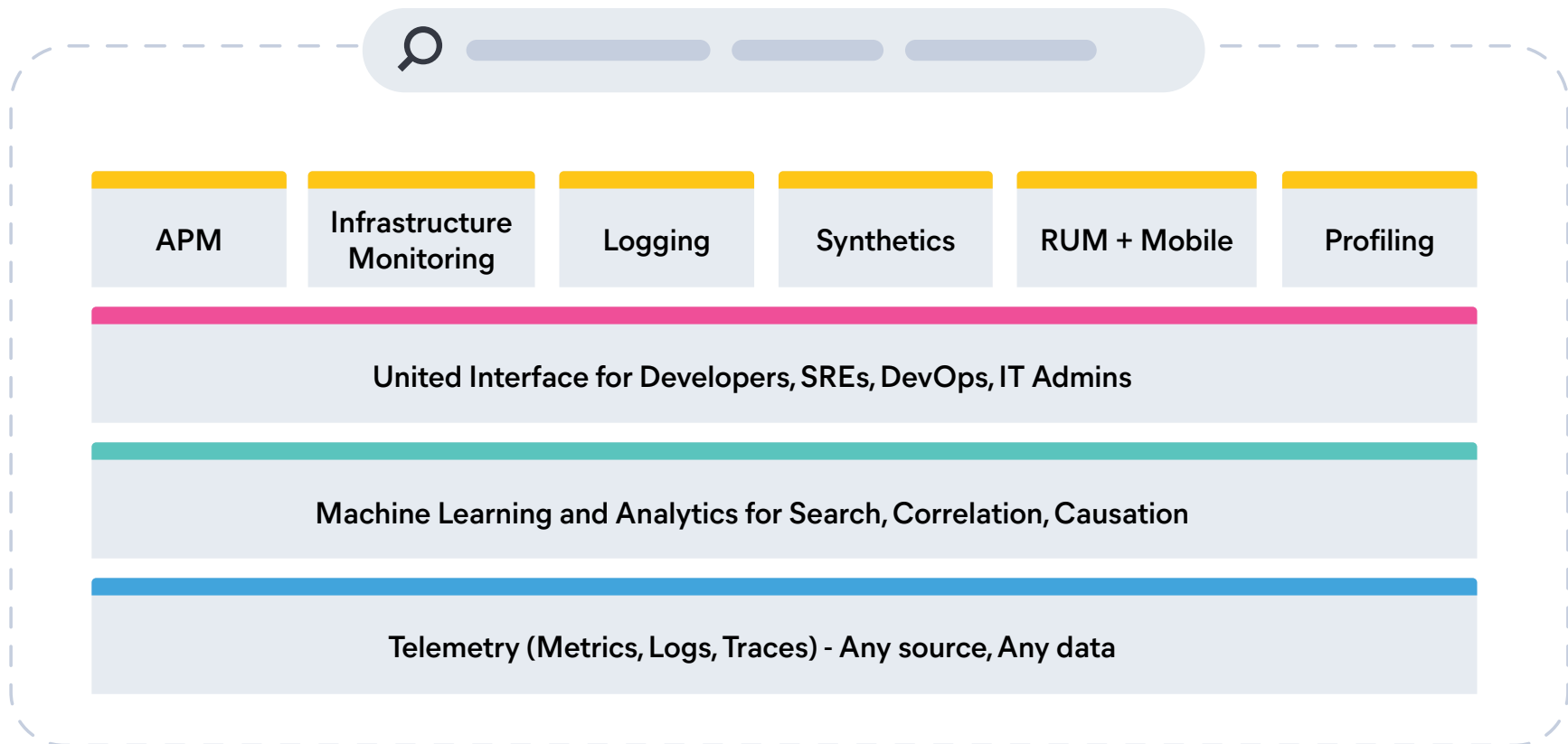
When you correlate business data with operational data, you get actionable insights that empower you to improve your business performance. Getting cross-system visibility means getting a holistic view of your entire ecosystem. That results in faster incident resolution, which inevitably means more efficient operations. More efficient operations look like streamlined processes and increased productivity, which in turn lead to quicker revenue conversion.

### Enable digital and cloud transformation

The right observability tool ensures that you can scale without losing sleep over potential issues like downtime, costly outages, and so on. Full-stack observability is necessary during migrations or new product launches — it's what gives you the confidence that your systems are running reliably. In a dynamic environment, like a microservice-centric infrastructure, an observability tool gives you crucial, full visibility into the dependencies inherent to these complex systems.



Below is what a unified observability platform might look like.



At a basic level, your observability platform should enable: increased productivity, operational efficiency, revenue conversion, and a future-proofed architecture. To get that, look for a tool that has these features:



**Real-time insights and multi-signal data**

**aggregation:** You need your tool to provide you with real-time information on what's happening in your environment and your digital delivery system. A tool that can correlate data from multiple signals and diverse sources into a single platform is vital. This is a key step to improving your MTTR and MTTRD.



**Interactive visualization:** We all love a good, easy-to-use dashboard. A great observability tool empowers you to take action from your data by helping you make sense of your data as a human. And how does it do that? Dashboards. You want a tool that has out-of-the-box dashboards and that also gives you the ability to build and customize your own — so you can make the most of the tool, and meet your unique needs and use cases.



**Search capabilities:** Being able to use your tool to search for information is crucial. You want to be able to perform ad hoc investigations and analyses,

and search capabilities are where the difference is made. Search, explore, drill down, and determine root causes faster.



**Application Performance Monitoring (APM):**

With APM capabilities, your observability tool can help you accelerate your software development lifecycle. End-to-end distributed tracing — from your cloud services to your microservices to your serverless functions, and beyond — helps your team improve code quality.



**Log monitoring:** An observability tool, at its core, is built on log monitoring. So it has to do it right, and it has to do it well. You want your tool to easily deploy log monitoring, to detect patterns and outliers with anomaly detection, and to enable you to deploy and manage your logs — structured and unstructured.



**Infrastructure monitoring:** Your cloud infrastructure is complex, so you need an observability tool that can ingest and store time-series data and metrics, making it simple to understand with logical and intuitive visualizations of your environment.



**Real user monitoring:** Customer experience and satisfaction are external keys to the success of your business. So look for an observability tool that can give you all the insights on your users: get full visibility on their interactions, get metrics on user performance, and trace user experience across their entire journey. You want to be able to analyze data by URL, operating system, browser, and location.



**Synthetic monitoring:** While you need innovation to keep your organization relevant and competitive, innovation needs a little help from synthetic monitoring. Look for a tool that enables you to simulate, track, and visualize the performance of your critical user journeys, systematically.



**Application profiling:** You want to know what happens in your system at the kernel and I code level? Look for an observability tool that can enable low overhead and frictionless deployment of profiling capabilities and that is compatible with a broad ecosystem of languages (Python, Java, Rust, C/C++, Go, Rust, etc.) and works with all the major containerization and orchestration frameworks.



You know that there are a broad range of observability vendors out there. We've discussed the advantages of going with more established vendors (better support and consulting capabilities) and explored the tradeoffs between commercial, open, and extensible solutions, and building yours from scratch. Whichever direction you choose, keep these green flags handy and top of mind.

# Green flags

**Unified, full-stack capabilities are crucial in the long run.** While deploying observability can be a multi-year initiative, knowing your vendor can provide the basic capabilities of a full-stack platform enabling you to future-proof your observability solution.

**Consider the scalability of the solution:** Is it suited to larger complex environments and architectures? Will it be able to affordably scale and grow with your business?

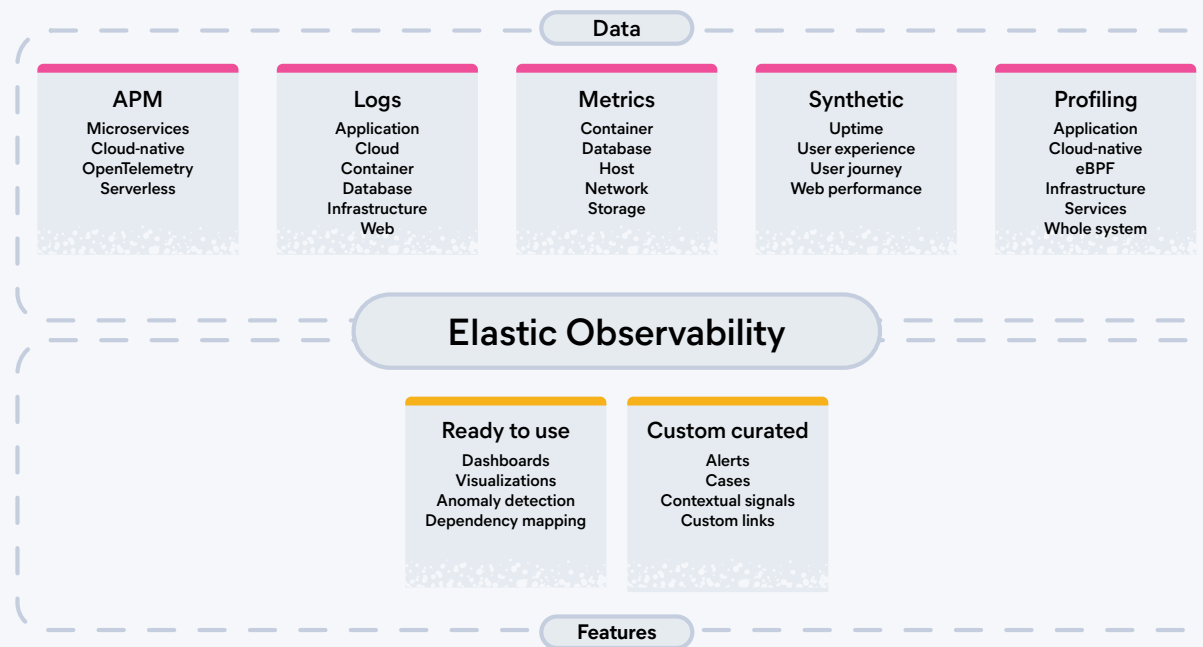
**You need a solution that leverages AI from both a traditional AIOps perspective and also around the future: generative AI.** The benefits can include help coping with overwhelming amounts of data, extracting needles from haystacks, reducing MTTD, reducing MTTR, finding unknown unknowns, surfacing root causes, providing context and correlation across disparate data sets, and curating relevant information that is accurate and business-specific.

**Dig into information regarding vendor lock-in and switching costs.** Ask about the ability to access your historical data. You should be able to do so without extra spend.



**Look for a solution that provides service maps and can keep an inventory of your applications/technologies.** UI is an important part of efficiency. Make sure that the solution truly simplifies the complex.

**Be sure that your vendor can support you in navigating compliance.** Based on your geo-location, what data can you store? For how long and for how much?



Oh! And one more, very important and very overlooked thing to do when shopping for an observability solution: Talk to the vendor's customers for references. Ask them what their experience is and has been from day to day use, to billing and beyond. It's a sure way to pick a solution for unified observability that is right for you and the future of your organization.

Think of it like picking a university: you're about to invest (if you're in the U.S.) a considerable amount of money into the next three to four years of your life. You're not

just looking at what classes you're going to take — let's call these our tool capabilities in this analogy. You're also looking at who the professors are — they're the observability experts who help you along your journey — what the student body is like, what the extracurriculars are, what the parties are like, and so on. That's your customer service, your point people, the perks you get for usage, and the community at large. What's one of the things you do to get a good sense of all that extra stuff? You talk to an alum for a first-hand account. The same goes for your observability solution.

# Executing your modern observability plan



## How to

[Download your proof of concept worksheet.](#) Put all your ideas down in one place.

---

If you've been making notes along the way, congratulations! You have a draft proof of concept on your hands! This is the part where you clean it up, and get it ready for the higher-ups.

## Preparing for a POC, major steps, and milestones

Bring all your notes together and organize them in this order:

1

**Identify your organizational milestones, metrics, and KPIs**

2

**Identify your stakeholders and impacted team members; outline the impacts**

3

**Identify the processes impacted; key use cases, edge use cases, outline**

4

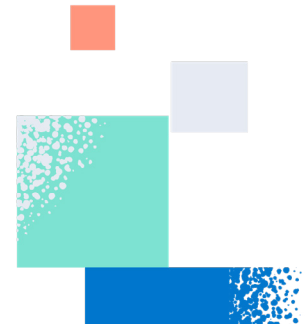
**Identify the impacted capabilities; outline the capabilities the solution will provide**

### Pull together a team of change agents

A journey is nothing without campaign members — pull together a team of change agents, and assign clear responsibilities to everyone. Refer back to your list of stakeholders and impacted team members: getting them on board will be crucial to the success of this operation.

### Set up a short list of vendors

Consider writing up a tear sheet or creating an evaluation scorecard to compare different observability solutions. Understand the key use cases that your current solution currently handles or could use improvement on. Talk to your network, google some names, and list their offerings as preparation for your upcoming proof of concept.



## Set up a project plan for POC

Your POC doesn't have to come together in a day! Give yourself a timeline to put it together. Involve your team of change agents. Keep your organizational milestones in mind as deadline goalposts.

Remember the considered impacts on your team and set deliverables and action dates accordingly.

## Read out

When you're ready to present, set the scene. Start with the pain point — how did you get to make this proof of concept? Then, present the solution.





# Checklist for Proof of Concept

## Review that you've covered all the angles:

---

**Organization:** What you're aiming for

**People:** Who is impacted

**Processes:** What is impacted

**Technological capabilities:** What you need the technology to provide

## Make sure you've covered these capabilities:

---

**Scalability and flexibility:** Customizable solution that fits all your use cases, today and tomorrow.

**Unified, full-stack:** Capture all your logs, metrics, and traces in a single intelligence platform to get complete visibility across your ecosystem.

**AIOps, generative AI and comprehensive analytics:** Empower your team to get real value out of your data and improve operational efficiency.

**On-premises and cloud-based deployments** in dozens of supported regions across AWS, GCP, and Azure: It's a solution that seamlessly integrates with your current ecosystem.

# Start your observability journey

**Well, change agent, you've got your gear. You're dressed for the journey, and a little better equipped than when you started.**

We've talked about data, and how the right end-to-end observability solution is what stands between you and actionable insights drawn from your data. We've explored what a unified observability solution means at the organizational level — what positive impacts this kind of solution can have in your present and your future. We've discussed the importance of putting people first when undertaking this vital transformation, and how to prepare them for the changes so they are empowered by them, rather than alienated. We've touched on your processes: how they will be improved, what disruptions to plan for, and how to pace yourself and your team during adoption. We've reviewed the technological aspect — the impacts on your current capabilities and the must-haves when shopping for the right observability tool.

Undertaking this transformation starts with a single step. Now that you're done reading our guide, you've taken it! You've got a draft proof of concept in your hands, a resource to guide you through further research — don't forget to talk to other vendor users, customers, and alumni for nuggets of truth. So if you're ready for the next step, we've got an Elastic Observability Maturity Model for you.

**Take the maturity assessment ►**

Thank you.

