A Beginner's Guide to Observability

Seeing everything, everywhere, all at once — and why it matters

splunk>
a CISCO company

In many ways, your organization is similar to a bustling city — complex, growing, and full of moving parts. It's a metropolis of microservices, cloud providers, serverless functions, and third-party APIs. While it may be thriving, chaos could be lurking in the shadows and threatening to upend your success. At any moment, unexpected performance issues or downtime could spell disaster for your business. A critical app could crash, your website could slow to a crawl, or worse — your website could go completely dark during your busiest time of year. In the event of a disaster like this, alarms are blaring, customers are complaining, and your team is scrambling to find answers. You need a hero. That hero is **observability**.

Swooping in to save the day, observability doesn't wear a cape, but it might as well. It illuminates real-time data including logs, metrics, and traces from dark corners of your vast digital ecosystem to help you investigate. It helps you pinpoint the source of the chaos, whether it's a rogue microservice or misbehaving API, and resolve issues before things spiral out of control. And it doesn't stop there — it watches after your organization to make sure you're ready for whatever comes next.

Good news: You don't need to sit around and wait for a disaster before observability can leap into action. In this guide, you'll learn what observability is, how it works, and how your organization can harness its power. We'll share real-world examples, tips, and what to look for in an observability solution.

Everyone — from developers to product managers to customer support teams and even executives — can benefit from the observability mindset. It's not exclusive to site reliability engineers or DevOps teams. It empowers your entire organization to work smarter, move faster, and innovate confidently.

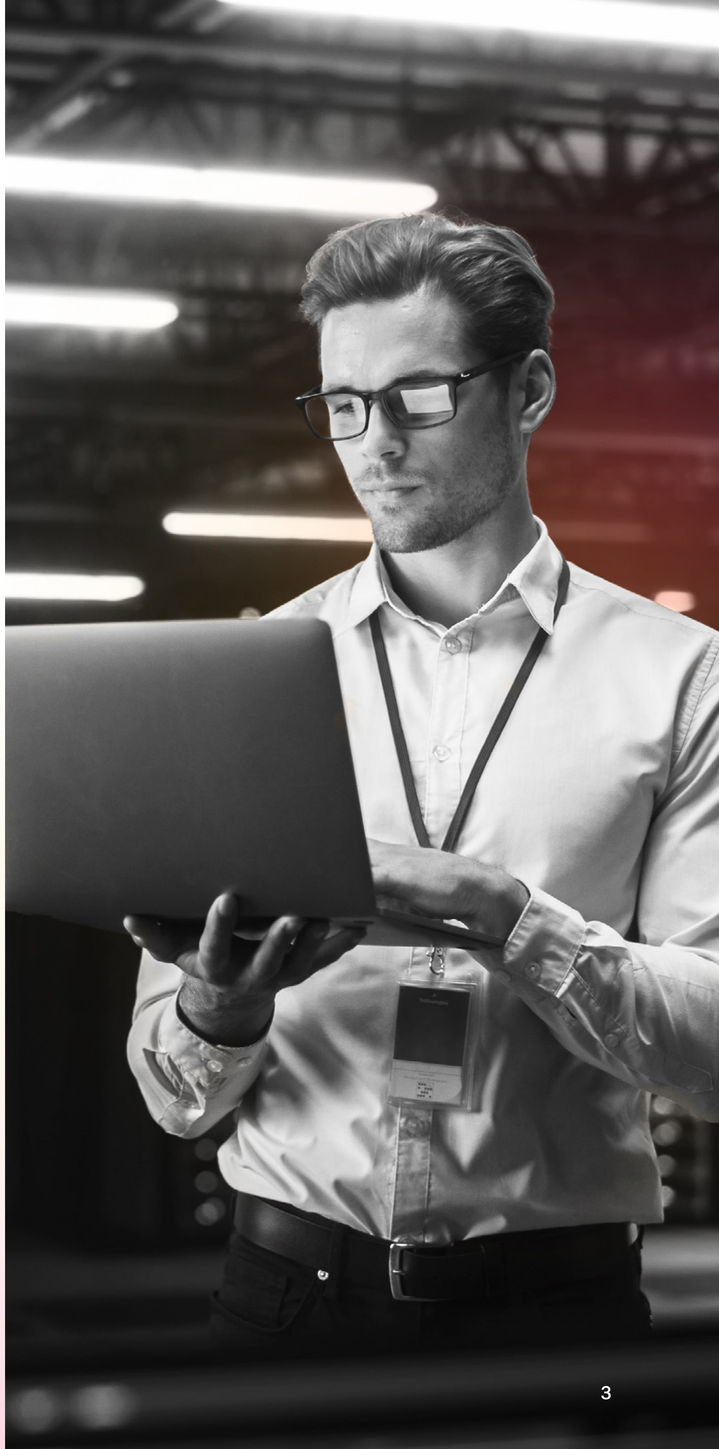
What is observability?

Observability is the ability to ask and answer any question about your business or application at any time, no matter how complex your infrastructure. It also covers you in the case of unknown unknowns, where you're not actively asking questions. The process includes instrumenting systems and applications to collect data such as metrics, traces, and logs, then sending this data to a system that can analyze and provide actionable insights. While monitoring is an important part of observability, observability is more than monitoring. Instead of passively tracking predefined metrics to alert you when something is wrong, observability actively helps you uncover root causes by analyzing the internal state of your systems. It's like having X-ray vision for your digital infrastructure.

In the event that something does go wrong, like a checkout page failing during the biggest sales day of the year, your team won't be stuck struggling to connect the dots and watching helplessly as customers abandon their carts. With observability, you can detect a problem or slowdown before it impacts your customers, look at the right log to identify the source of the issue, and resolve the problem within minutes — before customers ever even notice.

Observability is a mindset that grows and evolves over time — it isn't just a tool or a feature you can plug in overnight. A big part of it is designing simple systems that your team can easily understand, troubleshoot, and improve. By building applications with instrumentation baked in from the ground up, you can solve problems quickly and efficiently.

In a world where complexity is inevitable and downtime is not an option, observability is your organization's superhero.



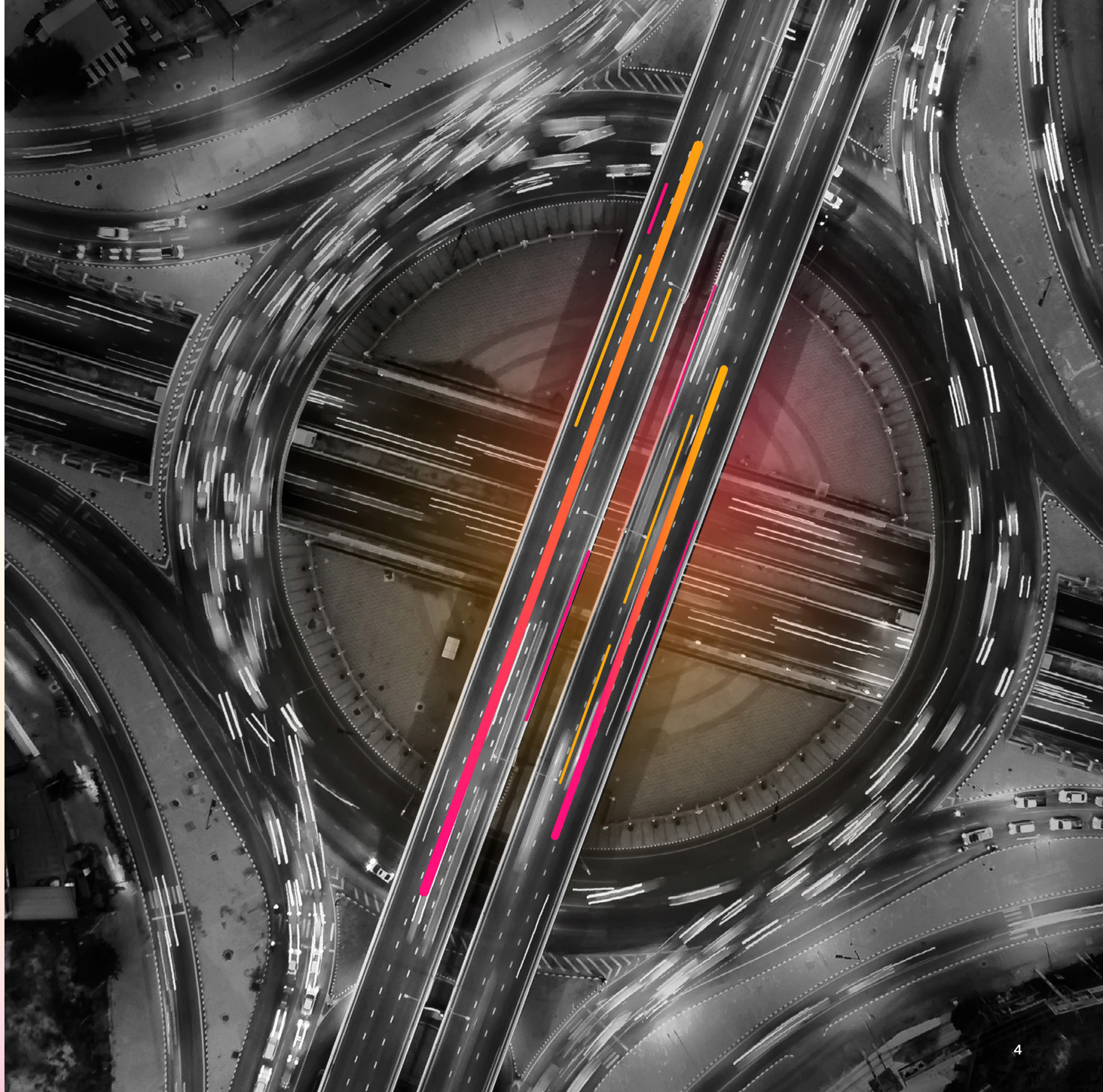
Why observability?

Observability enables you to reduce time spent firefighting to seize innovation opportunities. It ensures you're not just reacting to problems, but driving lasting improvements. A mindset shift from monitoring to observability protects your team from painstakingly firefighting individual issues. Instead, you're empowered to optimize the system as a whole.

Ultimately, your business is only as strong as your ability to understand and respond to problems. Observability helps you confidently and quickly answer critical questions like:

- Why is my application running slower than usual?
- How is a particular system issue impacting customers directly? Are there particular groups of customers who are affected more than others?
- What trends can I pinpoint to fuel future growth?

Competition is stiff in the tech world, and reactive troubleshooting simply won't cut it. You need observability to give you deep visibility into every layer of your digital environment.



Key benefits of observability

Observability drives success for your business, your tech, your employees, and your customers. Here are some reasons why it's so transformative:

- **It provides a comprehensive understanding of complex systems.** Modern applications consist of dozens or hundreds of microservices, serverless functions, and third-party integrations. Observability helps untangle the complexity, offering a clear picture of how everything works together.
- **It helps solve problems faster and reduce MTTR (mean time to resolution).** When something breaks, observability empowers teams to quickly pinpoint root causes instead of wasting hours sifting through logs or dashboards.
- **It enables smarter planning for code releases and capacity.** With a clear view of system behavior, teams can better predict potential issues and make informed decisions about scaling, resource allocation, and release timing.
- **It guides more insightful incident reviews.** Observability helps you identify patterns and system behaviors, helping you learn more from incidents and prevent future problems.
- **It boosts uptime and performance.** Observability ensures teams can proactively address issues before they affect customers, leading to more reliable systems.
- **It makes customers happier and increases revenue.** Great performance and minimal disruptions lead to better customer satisfaction, retention, and ultimately, a healthier bottom line.
- **It gives you a better understanding of your overall business, not just digital applications.** As systems become more interconnected, tech and business leaders need real-time, actionable insights that connect performance to outcomes.

While seeing through walls and predicting the future may seem far-fetched, observability is the next best thing — and organizations are reaping the benefits. Having a leading observability practice results in fewer outages, faster problem-solving, and a stronger return on investment, not to mention the peace of mind that your team can defeat any villain that comes their way.

Roadmap to observability

So, how can you put the superpowers of observability into practice at your organization? The core foundation of observability is based on data, a reliable platform, AI and ML capabilities, and insight into metrics and data sources. Let's explore.

Key data types needed for effective observability

These specific types of data are fundamental for building an observability practice.

Logs/events

Logs/events are immutable records of discrete events that happen over time. Common event sources include:

- System and server logs (syslog, journald)
- Firewall and intrusion detection system logs
- Social media feeds (Twitter, etc.)
- Application, platform and server logs (log4j, log4net, Apache, MySQL, AWS)

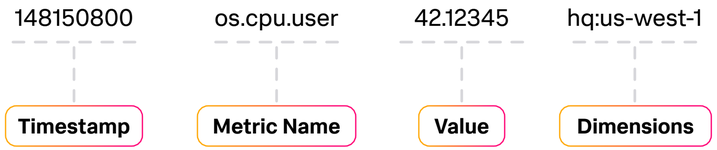
Metrics and dimensions

Metrics are numbers that describe a particular process or activity, measured over intervals of time. They provide the foundational data you need to understand your systems, applications, and business performance. Common sources of metrics include:

- System metrics (CPU, memory, disk)
- Infrastructure metrics (AWS CloudWatch, Azure Monitor, Kubernetes Metrics Server)
- Web tracking scripts (Google Analytics, Digital Experience Management)
- Application agents/collectors (APM, error tracking)
- Business metrics (revenue, customer sign-ups, bounce rate, cart abandonment)

What are dimensions, and why do they matter?

Metrics alone don't tell the full story — they need dimensions to provide context. Dimensions are attributes or labels that you attach to metrics to add specificity and context. Think of them as the "who," "what," and "where" that give your metrics meaning. For example, a raw metric like "CPU usage" becomes significantly more actionable when paired with dimensions like region (e.g., "us-east-1"), application name (e.g., "checkout-service"), or instance ID (e.g., "i-123456789").



By layering in dimensions, you can slice and dice your metrics to answer precise questions, such as:

- How is one specific user's transaction performing?
- Are big spenders more affected by an outage than other customers?
- What's the bounce rate for users in a particular geographic region?

Dimensions enable you to go beyond high-level averages and unlock granular insights that directly tie system performance to business outcomes.

The role of cardinality

Understanding cardinality is key to making the most of dimensions. Cardinality refers to the number of unique combinations of dimensions and their values in your dataset. For example, if you track metrics like "response time" and add dimensions like user ID, region, and device type, the possible combinations (or cardinality) can quickly grow into the thousands, millions, or even billions.

High cardinality is powerful because it allows you to ask highly specific questions of your data, such as:

- What's the average response time for premium users accessing the app from mobile devices in the US East region?
- How many failed transactions occurred for user IDs associated with VIP customer accounts?

High cardinality does have its challenges, like increased storage and computational overhead. That's why observability platforms that excel in handling high-cardinality data stand apart — they allow you to uncover critical insights without compromising performance or usability.

In summary, metrics tell you what's happening, but dimensions and cardinality reveal why it's happening and to whom it matters most. They allow you to make data-driven decisions that improve uptime, user experience, and revenue — and are essential to mastering observability.

Traces

Specific parts of a user's journey are collected into traces, showing which services were invoked, which containers/hosts/instances they were running on, and what the results of each call were.

Types of data sources

The following are types of data sources that have evolved over the years — all important in achieving observability:

- Network flow data: router/switch counters, firewall logs, etc.
- Virtual servers: VM Logs, ESXi Logs, etc.
- Cloud services: AWS data sources such as EC2, EMR, S3, etc.
- Docker: logging driver, syslog, apps logs, container metrics, etc.
- Containers and microservice architectures: container and microservices logs, container metrics and events, etc.
- Third-party services: SaaS, FaaS, serverless, etc.
- Control systems: vCenter, Kubernetes, etc.
- Dev automation: Jenkins, Sonarcube, etc.
- Infra orchestration: Chef, Puppet, Ansible, etc.
- Signals from mobile devices: product adoption, users and clients, feature adoption, etc.
- Metrics for business analytics: app data, HTTP events, SFA/CRM
- Signals from social sentiment analytics: analyzing tweets over time
- Customer experience analytics: app logs, business process logs, call detail records, etc.
- Message buses and middleware

Core capabilities of an observability platform

The good news is that so much data exists; the challenge is aggregating and gaining insight from all of it. That's where an observability platform comes in — to facilitate shared learnings, enable collaborative incident response, support development with data, and foster intelligent operations. But observability isn't about buying a shiny product and expecting instant success. It's a journey, requiring the right tools and the right approach to unlock its full power. The rewards — like lightning-fast problem resolution, bulletproof reliability, and game-changing business outcomes — are well worth the effort.

Look for a system that can do the following:

Collect all data

Your observability platform needs to see across all stacks, technologies, and environments. Think of this as the omniscience superpower. The platform should grant visibility into everything, including cloud-native (containers, cloud, serverless), traditional (self-hosted, on-premises, monoliths), and all languages and frameworks you use. All of this data then needs to be aggregated and visible in one place.

Analyze and de-duplicate

Your observability platform needs to be able to separate valuable signals from the noise, like a superhero with enhanced perception. It should store statistics about your data at ingest time to get to alerts and insights faster, and detect outliers or other anomalies automatically. This will help your team identify problems at hyperspeed, zeroing in on what's most important.

Add context

Next, the platform needs to show the responding engineer what they need to fix the problem quickly and efficiently. They should be able to view data related to incidents in one click, keeping downtime to a minimum. This context will also help them determine the effects of code deployments on key metrics.

Utilize AI and ML

The data you need to answer questions about your business is massive, and realistically, it's a vast world that no human can realistically keep up with. That's where AI assistants and large language models (LLMs) save the day, providing the superpowers you need to make sense of it all.

The best observability systems use LLMs and machine learning (ML) to get a handle on your past and present, giving you crystal-clear insights into what's going on with your services and applications. They also help you look around the corner and predict what's likely to happen next. By processing all that historical and real-time data, these models dish out predictions, insights, and help you find root cause faster than ever.

With advances in AI, you can:

- Reduce event clutter and false positives with multivariate anomaly detection
- Automatically conceal duplicate events to focus on relevant ones and reducing alert storms
- Easily sift through vast amounts of events by filtering, tagging and sorting
- Enrich and add context to events to make them informative and actionable
- Speed and simplify investigations and workflows
- Make better decisions with deeper visibility and understanding of the environment

Get data in seamlessly

OpenTelemetry (OTel) is the industry-standard way to collect and export telemetry data for observability. Backed by the Cloud Native Computing Foundation (CNCF) and supported by a thriving developer community, OTel simplifies how organizations gather traces, metrics, and logs across their systems. Its open, vendor-neutral framework ensures flexibility while avoiding lock-in.

What makes OpenTelemetry so compelling is its widespread adoption and seamless integration with many popular open-source tools and platforms. It's designed to work across diverse environments — whether you're monitoring cloud services, microservices, containers, or legacy systems — making it the easiest way to standardize and centralize your data collection.

By adopting OpenTelemetry, you're aligning with the leading open-source standard, future-proofing your observability practice, and tapping into a powerful ecosystem built to reduce complexity and deliver better insights. It's the simplest way to get your data in and make observability work for you.

Employ essential tools

There are many solutions that can help you get insights from the overwhelming volume of disparate data from all the sources listed above. You'll likely find that you need the following tools to gain a full, end-to-end picture of your application:

Tool	Use
Infrastructure monitoring	Determine the health and performance of the hosts, containers, and overall environment your applications run on.
Application performance monitoring	Investigate the behavior of your application at the service level. Determine where calls are going and how they perform.
Real user monitoring	Understand the experience of real users by collecting data from browsers about how your site performs and looks. Isolate issues from the frontend or backend.
Synthetic monitoring	Measure the impact that releases, third-party APIs and network issues have on the performance and reliability of your app.
Logs	Dig deeper into "the why behind the what" when issues occur. Figure out how to remediate the issues quickly.
Incident response	Alert the right team the first time to fix the issue and provide them with the data they need to succeed in doing so, all in one place.Reduce the risk of application security exposure with real-time threat detection and prevention.

Built for complexity

Modern tech environments often feel like a labyrinth of complexity. Microservices, containers, hyperscalers, and hybrid clouds accelerate innovation but also make it harder to see what's really going on. Without the right tools, it can be easy to feel lost.

Your observability solution should act as your guiding light, cutting through the fog and making sense of it all. It should be able to:

Monitor everything
Your observability platform should grant you crystal-clear visibility into your entire ecosystem, no matter where your infrastructure and applications live. It should pinpoint root causes, provide crucial context, and generate automated insights to catch problems before they snowball into disasters.

Foster team collaboration
Your observability solution should break down silos, ensuring that every stakeholder has access to the data that matters. It should alert the right people the first time and empower your team to act quickly and work together seamlessly.

Automate the routine, master the complex
Free your team from the burden of repetitive tasks by automating the mundane. Your platform should not only save time but also orchestrate complex processes, helping you focus on what truly matters — like driving your business forward.

Why Splunk Observability Cloud?

Splunk Observability Cloud is the all-seeing superhero your business needs to realize the full potential of observability. With Splunk, you gain real-time, high-fidelity insights into your systems — no sampling, no blind spots. It's like having laser vision that captures every critical data point, from user IDs to transactions, enabling you to uncover granular insights that make all the difference. Plus, it's secure and scalable, so you can trust that your data is safe as you navigate the complexities of your digital universe.

Splunk doesn't just stop at tracking technical metrics — it's a bridge between system performance and business outcomes. In today's always-on world, where every delay or outage ripples through customer experiences and bottom lines, Splunk helps you connect the dots. After all, observability problems are business problems. From pinpointing the root cause of a slowdown to quantifying its revenue impact, Splunk transforms challenges into opportunities.

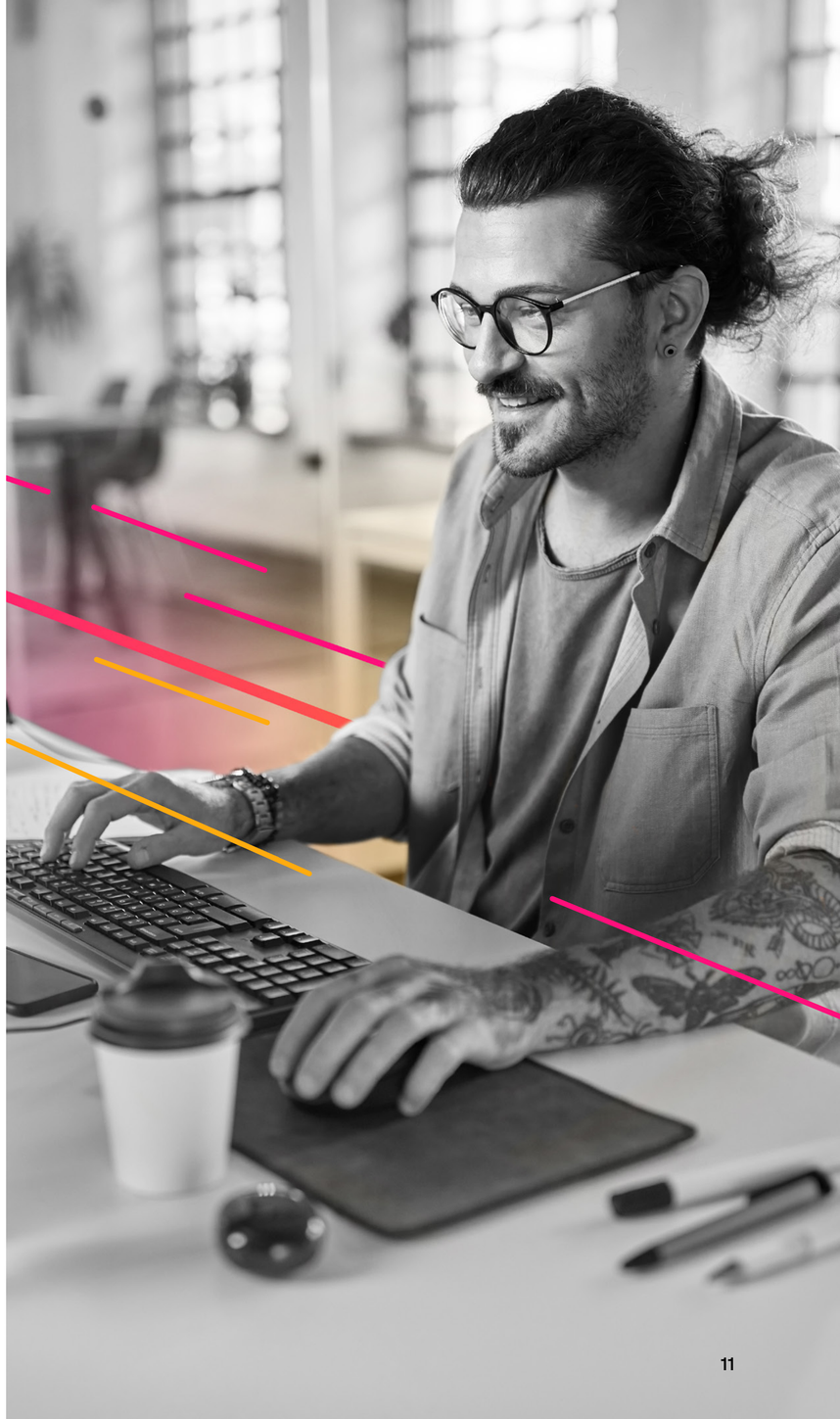
Splunk Observability Cloud bundles all the tools you need (like infrastructure monitoring, application performance monitoring, real user monitoring, synthetic monitoring, log exploration, and incident response) into one powerful platform. It consolidates data across any environment, whether you're running traditional on-prem systems, serverless functions, or cutting-edge cloud-native architectures — ensuring you never miss a critical detail, no matter how complex your ecosystem becomes.

And when things inevitably go wrong, Splunk Observability helps save the day. No more wading through endless logs. Now, you can trace the issue back to its source in just a few clicks. Splunk takes this a step further by helping you see the real-world impact on your customers, providing insights into their actual experiences and recommending ways to enhance them.

Splunk Observability Cloud is built on OpenTelemetry, the industry standard for instrumentation, and Splunk is a major contributor to the project. OpenTelemetry will help you future-proof your observability practice, ensuring your systems are equipped to handle whatever comes next. With more projects adopting this standard, you'll even find new applications pre-instrumented and ready to deliver insights right out of the box.

Splunk Observability in action

The following case studies present real customer data and results from organizations using Splunk's Observability Cloud products.



Spotlight

Rappi

Number one Latin American e-commerce company Rappi's hockey-stick growth, combined with the adoption of containers and microservices across 6,000+ hosts, strained their legacy monitoring platform, which lacked sophisticated and granular analytics, resulting in long delays to deliver alerts. After adopting Splunk Observability Cloud, Rappi:

Gained real-time observability across their environment.

Reduced the MTTR in production from five minutes to seconds.

Accessed more complex data analytics and better metrics correlation, reducing MTTR.

Grew confident in their continued migration to a microservices and serverless architecture, including ECS, Kubernetes and AWS Lambda (100+ services).

We're all attuned to the potential business impact of downtime, so we're grateful that Splunk Observability helps us be proactive about reliability and resilience with end-to-end visibility into our environment.

— Jose Felipe Lopez, Engineering Manager, Rappi

Spotlight

TRAVELPORT

Operating in over 165 countries with up to 201 billion itineraries priced daily, Travelport relied on a complex mix of observability tools to monitor product health and performance. The company needed monitoring tools that worked smarter, not harder, and they turned to Splunk Observability Cloud. The team worked with a Splunk Assigned Expert for strategic guidance, ensuring support for its key customer-facing product and achieved:

75% reduction in MTTD.

Exceeded uptime goal, delivering better customer experience.

95% reduction in false positives with Splunk Observability Cloud.

Top-line revenue is at risk every minute we're not fully up and running. Splunk's Assigned Expert rolled up their sleeves and found a way to optimize our environment to better respond to disruptions.

— Ed Hubbard, Director of Site Reliability and Monitoring, Travelport

Spotlight

velera

For Velera credit union clients, uptime is the most important service level agreement (SLA). But achieving Velera's 99.995% target requires sophisticated infrastructure monitoring — especially given the organization's cloud-based environment that orchestrates dozens of business-critical microservices. With Splunk, Velera saw these key outcomes:

Accelerated mean time to repair (MTTR) to <15 minutes.

3 billion transactions per month run 300% faster.

Delivered consistent 99.95% uptime.

The results were amazing. Switching on Splunk AppDynamics for Application Performance Monitoring was like walking into a room and turning the lights on.

— Earl Diem, Vice President, Operations Engineering, Velera

Spotlight

Agero

Agero had always relied on sophisticated tooling internally for its call center agents. But the company wanted to make them more observable and offer a fully digital, transparent experience to better pinpoint locations, dispatch vehicles, and provide the help customers needed when they were in an accident or stranded on the road. That's where Splunk came in, allowing Agero to modernize and deliver a 100% digital, agentless experience to drivers in need. With Splunk, Agero experienced:

100% digital, agentless experience now available to customers.

18-point higher net promoter score over non-digital experiences.

5% YOY increase in availability.

In an industry where phone calls are the standard, Splunk's observability solutions have helped us modernize to deliver a 100% digital, agentless experience to our drivers in need of roadside assistance.

— Billy Macdonald, Senior Director, DevOps, Agero

Key takeaways

Here's what you should remember as you embark on your observability journey:

Observability conquers complexity.

It gives you the power to make sense of modern architectures and solve problems before they impact your business.

It's a mindset, not just a tool.

Observability extends beyond traditional monitoring to help you uncover insights and answer questions you didn't even know to ask.

It empowers everyone.

Observability isn't just for engineers. Developers, product managers, customer support teams, and even executives can all benefit from the visibility and insights it provides.

It drives results.

With observability, you'll reduce downtime, improve user experiences, and make data-driven decisions that propel your business forward.

Splunk Observability helps you see everything, everywhere, all at once.

Splunk Observability Cloud is like a transformative force that turns complexity into opportunity, helping you deliver world-class digital experiences and stay ahead of the competition.

What’s next?

Ready to find your observability superpowers? To start, commit to the observability mindset: a focus on visibility, collaboration, and automation. Next, find a solution like Splunk Observability Cloud, which provides the tools to monitor every layer of your system and respond to incidents with precision. Learn what makes Splunk a leading observability platform in this report.

splunk>
a CISCO company

25_CMP_ebook_a-beginners-guide-to-observability_v8