Supercharge Your Observability

Real user data for real-time analytics

splunk>

turn data into doing®

Traditional approaches to monitoring fall short.

Particularly as teams modernize, they must monitor and react to:

- Hybrid environments.
- More frequent software changes.
- More telemetry data emitted across fragmented tools.
- More alerts.

Troubleshooting these software systems has never been harder. We'll walk you through some common challenges and the benefits companies experience once they embrace observability.

Average won't cut it

The average organization has dozens of tools to monitor different parts of their stack. Does that sound like a lot? (Hint: it is a lot.)

And, why should we care about how many tools there are?

Hopefully, it's not when a manager is asking about silos and your customers are posting less than flattering tweets about your business. Teams often adopt a disconnected set of tools for monitoring their data.

They are commonly monitoring:

- Infrastructure (cloud providers, owned data centers, networking gear, databases)
- Applications (hundreds of microservices, serverless functions)
- Digital customer experience (real user monitoring data, synthetic monitoring data)

With so many disparate things to keep track of, it's easy to have data silos, blind spots and increased complexity. It's also harder to diagnose cascading issues that may be impacting different parts of your environment. All of these factors increase the likelihood that a critical signal will go unnoticed.

Most monitoring tools weren't built to handle the frequency of changes or the explosion of interactions between components and potential failure scenarios found with modern software. The traditional way monitoring tools are used starts with an engineer getting paged with an alert, logging into their monitoring tool and interpreting dashboards or logs to investigate the problem.

The biggest issue with this approach is that it requires alerts be set up in advance for things that are likely to fail. These days, it's impossible to anticipate every problem or to spot unknowns when you're dependent on human-generated alerts to know what's changing. There are often different monitoring systems for different infrastructure environments (legacy vs cloud-native stacks, for example). And it's hard to diagnose the root cause of problems when you have to manually sift through dashboards to find out what happened and why. Additionally, if some aspect of your application wasn't considered likely to contribute to problems, it may not be emitting data to your alerting system at all.

A new approach to monitoring is needed — one where teams can see all of their data in one place, anticipate emerging problems before customers notice, and know where to look when a problem does occur. The secret to this new approach? Data. Instrument everything and use modern AIOps powered tools to help bring insight to what matters with the visualization of your choice.

Welcome to observability. Here's how to go beyond traditional monitoring — we'll walk through the keys to creating a successful observability practice.

IT departments need a single solution

And that solution should offer holistic monitoring across on-prem, hybrid/multicloud environments, leveraging all data from any source and at any scale. It’s a simple fix, but one that vexes IT teams struggling with legacy systems.

Every company selling an IT monitoring solution talks about their ability to analyze data, but the differentiators are in the details. It’s not just about analyzing data, it’s about what data and where it comes from.

As organizations move to the cloud and modernize their software delivery practices to ship innovation faster and more frequently, there are more services and more changes that need to be monitored in real time.

With no single source of truth for all telemetry data, it’s hard for IT Operations, DevOps and application development teams to understand how infrastructure health and application performance impact the digital customer experience. Fragments of critical data get trapped in siloed tools and, as customer expectations have risen, there’s more pressure to find and fix problems faster, as well as prevent them from occurring. These dynamics lead to four main challenges:

1. Poor uptime, reliability and performance

As the volume of software changes increases, so does the risk of failures. Software teams struggle to meet and exceed service level objectives when deployments break things, when it takes too long to resolve incidents, and when teams lack the proactive insight needed to anticipate and prevent potential problems before they turn into customer-impacting incidents.

2. Operational inefficiency

As monitoring tool sprawl increases with missing context and scattered telemetry silos across tools, blind spots make it harder to efficiently diagnose issues. This is a classic example of too many cooks in the kitchen — this contributes to tribal knowledge with too many people needed to fix problems.

3. Limited visibility into customer experience

When teams can't detect and resolve unexpected performance issues or outages quickly, customers aren't happy — which creates churn and jeopardizes revenue. And when teams can't measure the impact of software changes and are unable to get business context from their telemetry data, they miss out on opportunities to continually improve the experience customers have.

4. Curbed innovation and growth

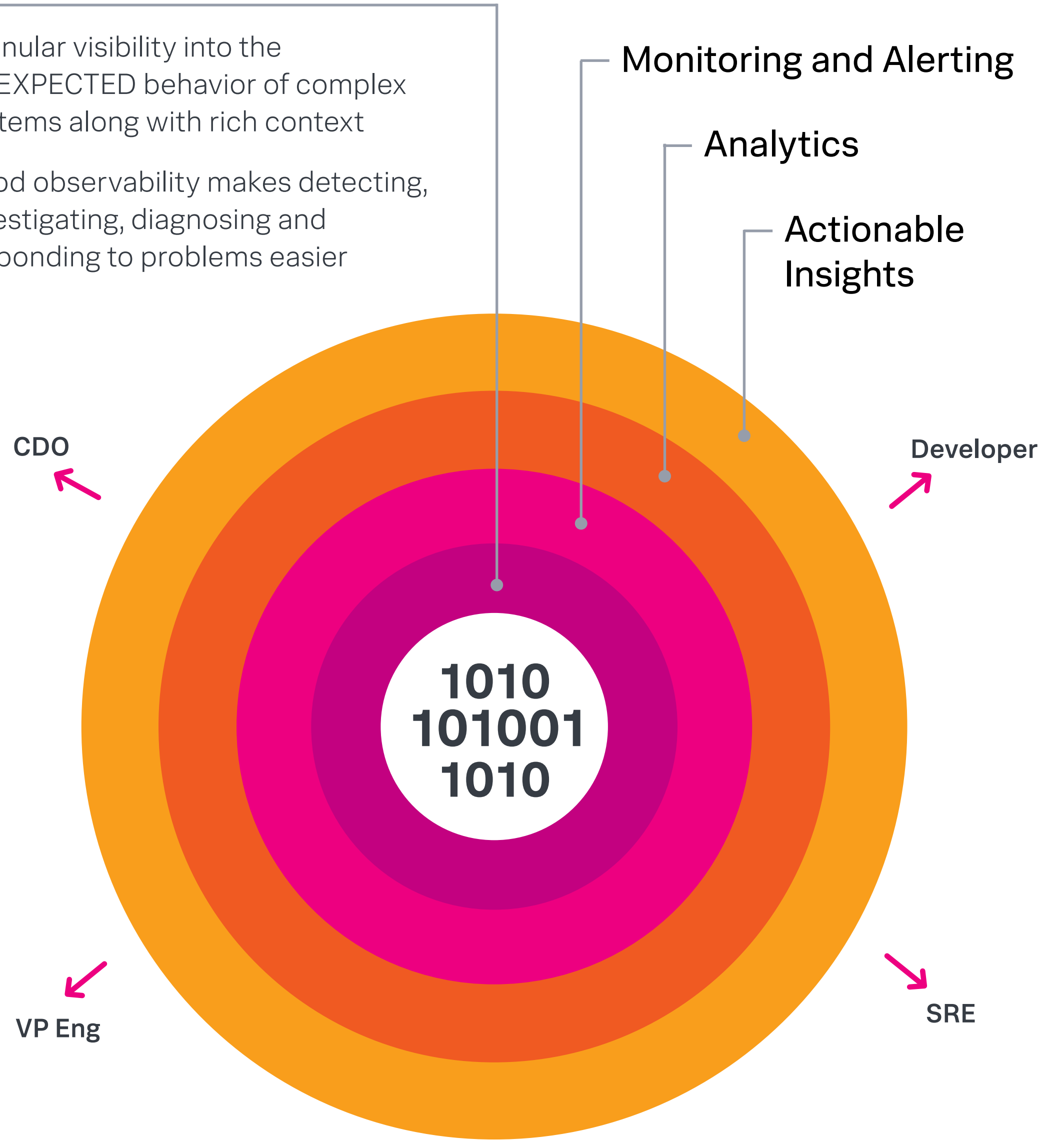
An inability to quickly respond and adapt to changing market conditions and get new innovation to market can result in missed opportunities, lost market share, inability to attract and retain top talent and lack of growth.

But it's not all bad news. An observability platform addresses these challenges.

Observability

Granular visibility into the UNEXPECTED behavior of complex systems along with rich context

Good observability makes detecting, investigating, diagnosing and responding to problems easier



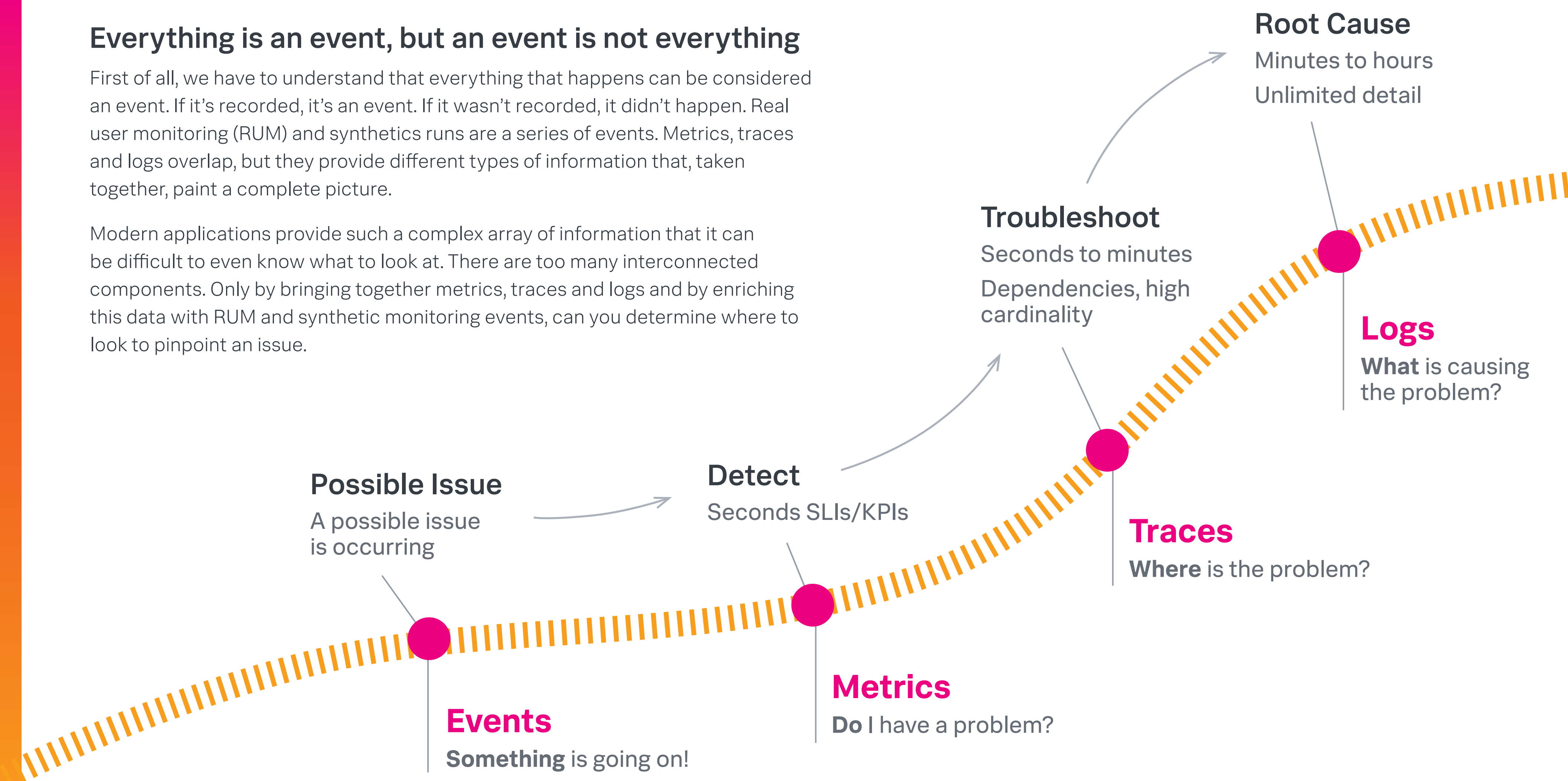
THE THREE PILLARS OF OBSERVABILITY:

Metrics, logs and traces

Everything is an event, but an event is not everything

First of all, we have to understand that everything that happens can be considered an event. If it's recorded, it's an event. If it wasn't recorded, it didn't happen. Real user monitoring (RUM) and synthetics runs are a series of events. Metrics, traces and logs overlap, but they provide different types of information that, taken together, paint a complete picture.

Modern applications provide such a complex array of information that it can be difficult to even know what to look at. There are too many interconnected components. Only by bringing together metrics, traces and logs and by enriching this data with RUM and synthetic monitoring events, can you determine where to look to pinpoint an issue.



Possible Issue
A possible issue is occurring

Detect
Seconds SLIs/KPIs

Troubleshoot
Seconds to minutes

Dependencies, high cardinality

Root Cause
Minutes to hours

Unlimited detail

Events
Something is going on!

Metrics
Do I have a problem?

Traces
Where is the problem?

Logs
What is causing the problem?

Splunk is a complete observability solution

How is observability not monitoring?

Monitoring tells you something is wrong, but it doesn't tell you why it's wrong. Monitoring setups also can only monitor things you've already thought could be problematic (your 'known knowns'). If you didn't think to instrument the component in question in advance, you can't monitor it. What's worse, if you have a problem and decide to add monitoring to it, you still don't have the historical data about how

the component performed. Also, monitoring requires special attention before you even know what could go wrong — you have to instrument specific things and set up specific alerts about them. This takes time and is prone to errors.

No matter how well-instrumented your monitoring solution is, it still doesn't let you explore your business. Looking into 'unknown unknowns' isn't possible with a classic monitoring system, because the data simply doesn't exist for you to evaluate. Adding in key business metrics and analyzing the effect your application availability and performance has on them is generally not supported or is poorly supported in traditional monitoring.

Real-user data is almost never included in monitoring systems, which is absurd, because the entire point of what we do in web applications is delivering user experience.

While most observability vendors have focused on either cloud-native or on-premise deployments, Splunk has built out a comprehensive monitoring approach that spans both environments, as well as the key services that support these environments. With Splunk, you have no blind spots in your monitoring. This is end-to-end visibility across a hybrid technology landscape.

Why Splunk?

Splunk detects problems before customers notice, before those angry tweets start hammering your notifications. Splunk analyzes patterns from telemetry and events to identify concerning performance issues and can predict when issues might impact service availability. Taken together, including business context, organizations can anticipate and proactively address problems, reducing downtime and poor performance.

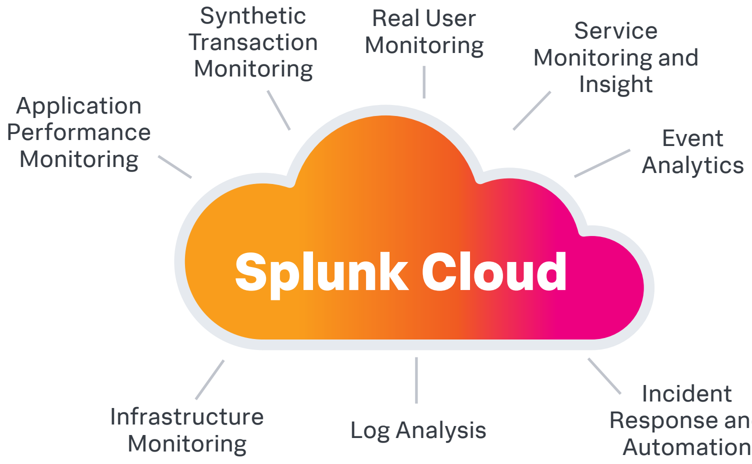
Splunk empowers developers, SREs and IT Ops teams to quickly investigate issues and answer questions of their observability data. With Splunk, ML can aggregate what would be hundreds of alerts in other platforms into a single event episode to provide more effective ways to begin investigations. Based on previous incidents, Splunk can recommend ideal responders for problems, and interesting and anomalous data is highlighted. Users can quickly pivot from problem awareness to identifying the reasons behind the problem. With directed troubleshooting, there are no dead-ends in your investigations.

Splunk is the industry's only analytics-driven, multicloud monitoring and observability solution for all environments. Splunk gives you the speed, scale and insights you need to master your IT challenges. Splunk is the only solution that allows you to:

- Pinpoint root cause with speedy real-time troubleshooting, find and fix issues as soon as they arise and get to resolution in just seconds.
- Correlate data from multiple data sources in multiple formats from multiple tools and get actionable insights in one solution.
- Get insights fast from across your entire environment, whether you're onprem, hybrid, multicloud or using containers and microservices.
- Get started quickly and easily with hundreds of out-of-the-box integrations, pre-built charts and dashboards, and automatic service discovery.
- Drive value faster for your organization with easy-to-use, high-performance monitoring and troubleshooting that enables you to quickly detect and resolve issues.
- Reduce cost and complexity by consolidating monitoring tools and standardizing on the market-leading data platform.
- Future-proof your investment with a comprehensive, scalable and flexible data-driven solution that grows with your organization.
- Analyze and correlate data for valuable insights that reduce event noise and predict future degradation.

Splunk provides the most comprehensive, robust and flexible troubleshooting and monitoring solution across on-prem, hybrid/multicloud environments at any scale. Splunk is recognized by leading analysts as the best solution in the market for ITIM and ITOM, as well as a leader in cloud observability solutions. Based on OpenTelemetry standards, Splunk delivers enterprise performance and scale as well as centralized management of teams, usage and costs without fear of vendor lock-in..

The Most Comprehensive Set of Observability Capabilities


Synthetic Transaction Monitoring
Real User Monitoring
Service Monitoring and Insight
Application Performance Monitoring
Event Analytics
Splunk Cloud
Infrastructure Monitoring
Log Analysis
Incident Response and Automation

METRICS • TRACES • LOGS

On-Prem | Hybrid Cloud | Multicloud

Splunk® Infrastructure Monitoring

Monitor infrastructure and services of any size, at any scale from on-premise to the hybrid cloud. With Splunk Infrastructure Monitoring, it's simple to auto-instrument the entire tech stack for high-resolution visibility with no blind spots. Start real-time metrics monitoring in minutes for custom metrics and a fast pivot to related content. With actionable alerts in seconds, reduce noise and direct your troubleshooting using AI-powered contextual insights. Put your trust in a patented, streaming architecture that's purpose built to concurrently process hundreds of thousands of metrics time series per detector. Resolve service outages quickly with automated and predictive analytics.

Splunk Application Performance Monitoring

Get insight into cloud-native, microservice and monolithic applications, and gain visibility into performance and trace data — with any cloud environment and with existing infrastructure.

> **“We're alerted to issues in seconds, compared to a 10-minute latency with our previous solution. This allows us to get in and fix issues before they have a downstream effect for the officers using the platform.”**
>
> Kevin Heins
> DevOps Technical Lead, Mark43

Splunk Log Observer

Speed up time to clue and time to resolve with log analysis across your technology stack — anything that emits data. With Splunk Log Observer, you can view logs from key DevOps sources in minutes, optimize data sources and workflows, all in one place and with no code. Rapidly explore context-rich logs with a point-and-click experience, usable by SREs, engineers and developers.

> **“Splunk captures all the logs, metrics and traces in a way that allows us to understand any event across our platform, so we can ask questions and get answers.”**
>
> Matt Coddington
> Senior Director of Devops Engineering at Care.com

Splunk Real User Monitoring (RUM)

Improve customer experience on web, iOS and Android apps with full-fidelity session capture and end-to-end tracing. Understand unified web and app performance across every transaction, resource and third-party dependency.

> **“Splunk RUM helped find an extra two to three seconds of delay in interactivity on a page load. We've recently had glowing customer testimonials on improvements we've made.”**
>
> John Rousseau
> VP Technical Operations at OnShape

Splunk Synthetic Monitoring

Detect and resolve issues more quickly by simulating user transactions worldwide, with multiple browser and connectivity types. Get automated suggestions to increase performance and reliability, and get more informed on your applications' health. Splunk Synthetic Monitoring makes it effortless to deliver outstanding web app experiences.

> **We've decreased load time by 30% with Splunk® Synthetic Monitoring helping eliminate customer-facing issues and optimize web performance.**
>
> Tom Wilson
> Principal Engineer at Blue Apron

Splunk On-Call

Empower teams with automated incident response that gets incidents and alerts to the right teams before it's too late. Reduce mean time to acknowledgement and resolution (MTTA and MTTR), and improve collaboration across all groups. A complete ChatOps experience and integration with existing tools and reporting. Engineers can work with the tools they're most comfortable with, and blameless reviews are enabled by incidents being aggregated in one place.

> **In 12 months, our mean time to acknowledge came down from 4 hours to 20 minutes. Now we're 3 years in, and we're under 2 minutes.**
>
> Earl Diem
> IT Operations Manager, PSCU

Troubleshoot customer-facing issues. Optimize performance on web and mobile.

TROUBLESHOOT
Proactively find and fix performance issues

VIZUALIZE
Quickly understand customer experience

OPTIMIZE PERFORMANCE
Best practices to improve performance and UX

Observability: Analysts and customers speak

When Splunk and researchers at ESG surveyed ITOps and developer teams from 525 organizations worldwide, we found that established leaders with the best observability practices are four and a half times more likely to report strong success with digital transformation and nearly three times as likely to enjoy better visibility into application performance.

That's a lot to gain — but what does it look like in practice?

For 2021 unicorn Quantum Metric, it looks like 96% faster app development, better capacity planning and more reliable customer experiences through Splunk® Observability Cloud. And for Blue Apron, it's 30% faster site load time, fewer customer-facing issues and better web performance.

With Splunk's full-fidelity tracing and no sampling, Care.com benefits from better visibility into its complex containerized infrastructure, which has reduced MTTR from an hour to less than 10 minutes while accelerating feature releases. Lenovo relies on Observability Cloud as an enterprise-grade solution for ensuring 100% uptime amid huge spikes in web traffic, while Build.com uses the platform to understand exactly how new features or content impacts performance and load times.

The Splunk Observability Cloud helps us see clearly into our complex environment, allowing us to act based on data so we can deliver on our mission to help customers build better products, faster.

Glenn Trattner, Chief Operating Officer, Quantum Metric

CUSTOMER STORY: BLUE APRON

Just as Blue Apron makes it easy for everyone to achieve culinary success at home, through Splunk Web Optimization, an extension of Splunk Synthetic Monitoring, engineering teams of all sizes can identify defects and receive step-by-step directions on how to address any hang-ups with speed and ease.

Tom Wilson, principal engineer at Blue Apron, shared how his team leverages Splunk Synthetic Monitoring: “We have seen two big benefits from using Splunk Web Optimization. The heart of it is the dead-simple suggestions on how to improve our website by telling us what is broken, why it is broken, and what we should do to fix it.” The simple, step-by-step instructions on how to improve their site’s performance has helped Blue Apron respond to defects quickly and accurately.

The second benefit is the knowledge base, which includes how-to guides and best practices. “We are starting to elevate performance as a skill set within the team; the knowledge base — in particular, its explanations on best practices — has been incredibly helpful in doing so,” says Wilson.

Reduced weight of homepage
from 25MB to 4MB

30% faster
site load time

Better site performance
by fixing defects faster

> **We’ve decreased load time by 30% with Splunk® Synthetic Monitoring helping eliminate customer-facing issues and optimize web performance. ”**
>
> Tom Wilson
> Principal Engineer, Blue Apron

Conclusion

There is a reason you're always being told you need to stay on top of your data. The reason is simple, and you probably know it already. The volume of data you need to monitor and understand as an IT professional will continue to grow and grow. The pace of change will only increase. The key to your value as an IT professional lies in your ability to stay ahead of these changes and help drive business success. Observability provides the best technology to help you make your tasks as easy, efficient and effective as possible.

A big advantage of Splunk Observability Cloud is that all of our observability components (Application Performance Monitoring, Infrastructure Monitoring, Real-User Monitoring, Synthetic Monitoring, and Log Observer) are built on the industry-standard open framework of OpenTelemetry. Getting started with OpenTelemetry sets you up for long-term success in an observability journey. You do the work of instrumenting your applications only one time, and from there, you can take your data anywhere. We hope you'd keep using it with Splunk, but you can take it to most other commercial vendors or to open-source or homegrown solutions as well. Ownership of your data is a fundamental principle at Splunk and OpenTelemetry is our expression of that commitment.

To recap:

- **Metrics, traces and logs provide us data on the operation of our infrastructure, services and applications.**
- **Each piece fills a unique need for different use cases.**
- **Each piece works together to give us the complete picture.**
- **Together, they give us holistic visibility for monitoring, analysis and response to changes in our environments.**

Based on OpenTelemetry standards, Splunk delivers enterprise performance and scale as well as centralized management of teams, usage and costs without fear of vendor lock-in. See how a fictional e-commerce site benefits from Splunk Observability Cloud in this short demo, or check out the 12 Immutable Rules for Observability.

Learn More

22-23319-Splunk-Supercharge Your Observability-EB-108

splunk>®

turn data into doing®