8 Biggest Mistakes

IT Practitioners Make and How to Avoid Them

splunk>
turn data into doing™

Table of Contents

The State of Global IT: It Doesn't Have to be an Uphill Battle

Imagine you're the mythological character Sisyphus, forced to roll a boulder up a hill. When it gets near the top, it always rolls back down, so you have to keep repeating the same futile exercise over and over. If you're an IT professional in charge of a complex, hybrid environment, this scenario probably sounds familiar. Instead of helping move your organization forward, you spend most of your time constantly trying to pinpoint and fix one problem after another (eternally rolling boulders uphill). Adding to the stress, all the pressure is on you to maintain system availability and performance to keep business leaders and customers happy.

You're not alone. Across the world, IT professionals are in charge of an increasing number of servers and data coming in from disparate sources, and they're using way too many monitoring tools to make sense of it all. The 2018 report *Reducing Complexity in IT Infrastructure Monitoring: A Study of Global Organizations* by the Ponemon Institute* sheds light on the challenges of troubleshooting and monitoring cloud and on-premises environments. The Ponemon Institute polled 2,497 IT and IT security practitioners in the United States, the United Kingdom, Germany, France, Australia, Singapore and Japan about their infrastructure monitoring challenges.

When asked about the past year:

- Twenty-four percent said the handling of scale and complexity of IT infrastructure has improved
- Twenty-nine percent said the ability to easily deploy and maintain server monitoring technologies has improved

The Ponemon survey also found that while a significant percentage of IT practitioners are in charge of monitoring over 50 servers, only 33% felt that they could ensure performance and system availability with their current toolset. So how can IT effectively manage increasingly complex, hybrid environments, and what are the major missteps IT organizations can correct to build a more efficient approach to infrastructure monitoring and troubleshooting?

This guide outlines the **8 biggest mistakes IT practitioners make** and provides solutions, key takeaways and real-world examples to help improve IT monitoring and troubleshooting in your organization.

* Reducing Complexity in IT infrastructure Monitoring: A Study of Global Organizations. Ponemon Institute, LLC. Publication date: April 2018

01

Too Many Tools

Seventy percent of IT professionals in the survey said that using data to determine root cause slows them down — ingesting and normalizing data of differing formats and types is tedious and unmanageable, and it's difficult to make real-time decisions. This is often because companies use too many monitoring tools for single layers of their IT stack, such as networks or applications, which creates silos and inefficiencies. When data lives inside one tool but can't access or communicate with data confined to other tools, IT practitioners lose context on what's happening in their environment because they're seeing only a part of the picture.

The Solution

How can companies improve their approach to IT infrastructure monitoring? IT practitioners said the most influential factors when choosing an infrastructure monitoring and troubleshooting strategy are:

- Simplification of IT complexity through consolidation of technologies and systems
- Automation of IT maintenance and management processes

More than ever, it's critical to monitor performance across hybrid architectures with a tool that collects and correlates data from all sources. Multiple, fragmented monitoring solutions don't provide the visibility and intelligence needed to meet business and IT goals. So what's the solution to too many tools and disparate data? The answer is a single, scalable monitoring tool that provides end-to-end operational visibility into hybrid environments. Let's take a look at how two companies solved the problem.

ENGIE

BEFORE: Resolving issues became time-consuming and inefficient for ENGIE because its development and infrastructure teams were using different monitoring tools, which required too much back-and-forth between the two teams.

AFTER: By deploying Splunk Enterprise and Splunk IT Service Intelligence (ITSI), the large energy company gained a holistic view of the health of key business services, faster resolution of business-impacting issues, and improved collaboration between development and infrastructure teams during incident triage.

SMSGlobal

BEFORE: An online service company, SMS Global struggled with information access because many applications were integrated with different devices — such as Cisco network devices and ASA appliances — and every system generated logs in different formats and locations.

AFTER: The company now uses Splunk Enterprise to collect, index and harness operational data across its infrastructure for in-depth, real-time visibility. Compliance reporting that required 10 people and days to complete now takes only one admin and seconds to complete. The company also gained full visibility into its Microsoft Exchange environment with the Splunk App for Microsoft Exchange. SMSGlobal can now monitor email movement across the entire IT infrastructure in real time, cutting the time it used to take to correlate events from firewalls, Exchange or ad logs from days to minutes.

02

IT and Business Friction

As digital business infrastructure increases in complexity, IT teams feel more pressure than ever to reduce business-impacting incidents. When IT systems fail, the ramifications go beyond the immediate financial loss of downtime — a business could lose customers and jeopardize its reputation, a harsh reality that keeps IT teams up day and night. According to Ponemon's research, 61 percent of IT professionals say that lack of system availability and poor performance creates friction between IT and lines of business.

The Solution

How can an IT team keep business professionals and decision makers happy and on their side? By ensuring 24/7 system availability and high performance, of course. But that's only achievable when IT has the ability to quickly isolate, identify and fix issues before they become a problem. In addition to a solution that allows IT to find the root cause to identify service interruptions, IT and business need to work together to design business and technical requirements in tandem.

Here are some real-world examples of companies that decreased friction between IT and the business.

Micron Technology, Inc.

BEFORE: Growing manufacturing company Micron struggled with production and shipping delays due to its lack of enterprise-wide visibility across the entire IT infrastructure.

AFTER: The company adopted an analytics-driven approach with Splunk to transform its IT operations and business, resulting in a reduction of business-impacting IT incidents by more than 50%, mean-time-to-resolve IT incidents by 32% and the number of major IT incidents by 23%.

Networld Technology Ltd.

BEFORE: The IT team at online services provider Networld Technology was under pressure due to time-consuming data aggregation procedures that delayed business decisions, such as insufficient searching and monitoring for analytics and the lack of a centralized view of sales performance and revenue. Its business team needed to centrally monitor the overall trends of various retail brands, and identify the top products, categories and merchants for business management purposes.

AFTER: With Splunk Enterprise, Networld replaced manual reporting with powerful dashboards that show all of this information in real time and in a user-friendly graphical interface that keeps track of the overall performance of the website. Operations became more efficient due to end-to-end visibility into business processes, and real-time revenue analysis generated new business opportunities.

03

No Way to Easily Identify Root Cause

Across the globe, IT professionals spend their days identifying and fixing server environment problems. Indeed, the Ponemon survey found that the top two challenges of troubleshooting, monitoring and cloud migration are:

- Lack of insights to quickly pinpoint issues and identify the root cause
- Complexity and diversity of IT systems and technology

When IT can't find and fix issues quickly, it has a direct effect on the business.

The Solution

In order for IT to quickly fix problems, they need a monitoring tool that can surface an issue's root cause with an alert about where and why something is wrong. Issue resolution time can be cut in half with a monitoring solution that correlates metrics and logs, and provides visualizations of alerts, trends and logs in one place.

Making sure your monitoring tool can enable those types of actions and resolution planning is critical for success. Read on to learn how two companies succeeded in speeding root cause analysis.

Advanced MD

BEFORE: A cloud-based provider for medical professionals, AdvancedMD lacked visibility into service-related systems when issues occurred, resulting in long detection and remediation times.

AFTER: The company deployed Splunk ITSI to ensure the performance and availability of services, gaining faster MTTR and increased reliability with Splunk's consolidated views into workflows and components.

Hyatt

BEFORE: The hotel chain's online check-in experience wasn't reliable due to a time-consuming troubleshooting process.

AFTER: To speed up detection time, Hyatt adopted Splunk Enterprise and the Machine Learning Toolkit (MLTK) and gained centralized, real-time visibility — dashboards and alerts help the IT team see an issue before a ticket is even opened.

04

The Wrong Skills to Manage Application Complexity

When Ponemon asked IT professionals about the biggest risks to their ability to troubleshoot, monitor and migrate to the cloud:

- Fifty-five percent said the increasing complexity of applications running on infrastructure
- Forty-four percent said a lack of skills and expertise to deal with application complexity

As infrastructure grows and evolves, it becomes increasingly difficult for IT teams to successfully manage, monitor and troubleshoot systems. Couple that with an IT skills gap that makes it difficult for organizations to attract and retain qualified talent, and it becomes clear why IT teams feel nonstop pressure.

The Solution

How can organizations ensure their IT teams are able to effectively troubleshoot, monitor and migrate to the cloud? A solid plan that takes future growth into account is necessary for smooth IT operations. Business and IT need to work together to create an IT environment roadmap, followed by a talent strategy that aligns to that plan. Be sure to:

- Identify skills gaps and adjust hiring
- Identify and train qualified employees for advancement
- Include succession planning for inevitable changes

05

Lack of Visibility Throughout Cloud Migration

What's the biggest cloud migration headache? Sixty-eight percent of IT practitioners said that ensuring application performance and availability throughout cloud migration caused the most stress. Over half said both cost and the inability to monitor and troubleshoot applications were their biggest pain points.

As infrastructure increases in complexity, the core responsibilities of IT to monitor and measure remain the same. So how can IT achieve infrastructure visibility and workload insights when performance data spans diverse environments?

The Solution

It's critical to monitor performance across hybrid architectures with a monitoring solution that collects and correlates data from every location. Full visibility is needed throughout the migration process, so choose an end-to-end monitoring tool that allows you to establish a pre-migration baseline, mid-migration insights and post-migration success. Before cloud migration, measure the baseline user experience and performance, and define acceptable post-migration levels. To accurately validate a migration's success, use the same monitoring tool throughout the migration process. A unified tool can analyze centralized data and provide better insights from dashboards and reports.

REI

BEFORE: When REI wanted to extend its security posture to include edge protection of its Amazon Virtual Private Clouds (VPCs) as it migrated applications to Amazon Web Services (AWS), the company realized it needed to gain edge protection and close a security gap during cloud migration by ensuring real-time visibility across applications, services and security infrastructure.

AFTER: REI deployed Splunk Cloud and Amazon GuardDuty service across its hybrid environment and has seen benefits including end-to-end security visibility during AWS cloud migration and real-time insight into potential threats.

TrueCar

BEFORE: TrueCar, a digital automotive marketplace, was using an open-source log management tool that took many hours to maintain.

AFTER: When the company switched to Splunk Cloud, it freed up the infrastructure team's time so they could tackle other problems. The team now relies on Splunk Cloud for monitoring all core infrastructure and application delivery across the organization. Dashboards provide visibility into AWS billing, enabling the team to better control costs and allocate resources effectively throughout cloud migration without needing to manage the infrastructure.

When it comes to migration expense, cost management tools offer current and historical instance usage and show unused resources. But it's vital to have full infrastructure economics for strong resource forecasts and intelligent migration decisions. For more information on creating an effective migration strategy, including predicting and managing costs, see the guide How to Get Your Cloud Migration Strategy Right.

06

Overwhelmed by Data Silos

As infrastructure evolves into a mix of mainframe, client-server, virtualized, serverless and hybrid cloud, the potential for silos and blind spots increases. When Ponemon asked IT professionals about the greatest difficulties of managing IT infrastructure, complexity and diversity of IT systems and technology was highest on the list.

Infrastructure complexity affects IT's ability to quickly determine root cause of an issue. When asked about challenges faced when trying to determine root cause, 63 percent of IT practitioners said that ingesting data from different formats and making sense of it to diagnose and determine root cause is problematic, while 56% said they weren't even sure what data was relevant for specific problems that arise.

The Solution

To avoid silos and banish blind spots, IT needs a single infrastructure monitoring and troubleshooting solution that can ingest and correlate data from any source. Instead of separate monitoring and log analytics tools, a single solution that unifies and correlates metrics and logs will speed up root cause identification. Let's take a look at how two companies solved their data silo problems.

Leidos

BEFORE: The IT team at science and technology solutions leader Leidos struggled to find and fix glitches before customer experience was negatively affected, because they had to find patterns and trends in siloed data and triage a flood of events spanning more than 120 IT services.

AFTER: After adopting Splunk, the company was able to see data across its entire service stack, consolidate events from a heterogeneous IT environment, detect and suppress duplicate alerts, clear solved alerts and distill them down to actionable events. Splunk helps the company boil 3,500 to 5,000 daily alerts down to roughly 50 tickets for network and data center operations to act on.

Micron

BEFORE: Micron found it difficult to maintain service quality to remain competitive because data silos limited the ability to identify, resolve and prevent IT issues.

AFTER: The technology company adopted an analytics-driven approach with Splunk to transform its IT operations and business, which dramatically reduced time-to-resolve and number of IT incidents. Real-time visibility now enables engineering teams to share data and expertise, and a new IT operations strategy enables the company to catch issues early to avoid business impacts.

07

No Plans for System Failure

Most companies aren't prepared to respond to interruptions or loss of service. According to the Ponemon study, only 29% of IT practitioners said their organization has:

- Documented workflows and automated processes to follow when a system failure occurs
- The ability to pinpoint problems early because of the adoption of automation and current monitoring tool sets

The longer it takes to resolve an incident, the longer customers suffer through poor customer experiences and organizations suffer negative business impacts, like loss of revenue. Without documented, ready-to-execute incident management plans, organizations spend precious resolution time responding to potentially recurring issues rather than reflecting and learning.

The Solution

Organizations need to prepare for the worst by putting an IT system failure contingency plan in place. Ownership and responsibilities should be clearly defined, and IT should document a plan for each potential technology failure scenario.

It's vital to continually test a system contingency plan to make sure it works, and keep in mind that any contingency plan will need to be refined as infrastructure changes. It's imperative to deliver the right information to the right person — or teams — at the right time.

08

Relying on Manual Processes

All over the world, IT teams spend too much time on manual tasks such as performing searches, managing daily logs, troubleshooting issues, creating analysis and compliance reports and more. Lack of visibility across the entire infrastructure is forcing IT teams to perform time-consuming manual processes in a reactive state. Only 30 percent of IT practitioners say their organization proactively gathers information from various intelligence sources to understand what the issues are before an outage.

In addition to resource allocation challenges, relying on manual processes results in longer mean time to resolution (MTTR), which can negatively affect customer experience and create friction between IT and the business.

The Solution

So how can IT move from reactive to proactive? Infrastructure monitoring complexity can be reduced with monitoring tools that allow for monitoring and troubleshooting in the cloud or an on-premises environment. When it comes to the feature that IT professionals desire the most in a monitoring solution, it's no surprise that 87% of IT practitioners said they want automated, machine learning-based investigations that enable them to quickly and easily find trends and root causes. Other key features to look for in a monitoring solution are that it can be used across teams, use cases and hybrid environments, and that installation and deployment is easy.

In addition to helping IT spend more time making improvements instead of fixing what's broken, implementing automation and operational analytics will improve the ability to deliver projects within budget, according to 51% of IT practitioners. Forty-six percent said it will improve their ability to deliver projects on schedule, while 45% said it will improve their ability to maintain service quality.

Moving from from a state of reactive monitoring to proactive, real-time monitoring is achievable with the right tool, as the companies mentioned next learned.

SONIFI

BEFORE: A technology integrator that services the hospitality and healthcare industries, SONIFI needed a solution for manual and tedious processes that made it difficult to make data-informed decisions.

AFTER: Since deploying Splunk Enterprise and taking advantage of new features, including metrics and event annotation, SONIFI has seen an annual savings of $85,000 by centralizing reports and implementing more efficient processes, a $100,000 monthly savings thanks to new insights into its billing decisions, and a reduction in reporting time from days to minutes.

ROKT

BEFORE: The IT team at online services company ROKT was spending hours manually managing its diversified range of logs, such as user, access, load balancer, CloudTrail, system, customer and transaction logs.

AFTER: Splunk has refined log management for the company. As a centralized log analysis tool for machine-generated data as well as unstructured and structured data, it enables IT managers to automatically index, correlate and monitor all logs across virtual and non-virtual environments from a single location, turning manual searches into automated real-time alerts, graphical reports and intuitive dashboards with only a few mouse clicks. What took the team hours to finish has now become minutes of computer operation, allowing the business to further grow and scale.

What Does IT Actually Do … and What Should IT Actually Be Doing?

With so many servers, applications and events to monitor, IT professionals are overwhelmed trying to meet performance and availability expectations. They're also being asked to meet business requirements, to build and deliver everything faster, and to make it higher quality and more efficient across the entire structure. And, they're supposed to do all that with fewer resources — most on-premises and cloud IT budgets aren't likely to increase over the next year, according to responses to the Ponemon survey.

When you consider that IT is responsible for managing large portfolios comprised of increasingly complex and stacked technologies, answering to business, fulfilling service requests and fixing problems in production when things break, it becomes clear that it's difficult for IT to meet organizational demands without changing their approach from purely reactive monitoring to proactive — or even predictive — monitoring.

What should IT really be focused on?

- Avoiding outages
- Improving customer experience
- Providing agility and adapting to ever-changing business needs

So how can IT become less reactive and more proactive? Switching from reactive monitoring and troubleshooting to proactive becomes possible with an analytics-driven monitoring solution such as Splunk, which allows for intelligent investigations to speed up root cause analysis.

Transforming IT: Speeding Detection, Investigation and Resolution With Proactive Monitoring

At Splunk, we hear from one customer after another that constantly changing demands require a new approach to infrastructure monitoring. From financial services to healthcare, manufacturing, telecommunications, even technology — IT teams in every industry we work with struggle with lack of visibility and insight across the entire infrastructure, tedious investigations and slow mean time to resolution.

What Customers Say About Infrastructure Monitoring Challenges		
Monitoring and Troubleshooting in Silos	Increasing Complexity Makes It Harder to Find and Fix Problems	Spending Too Much Time Administering Monitoring Software
"Why am I monitoring with one tool and troubleshooting with another?"	"Applications keep getting more complex and I'm required to monitor more than ever and find problems faster!"	"We don't have enough resources to buy and maintain complex monitoring tools."

How can Splunk help solve infrastructure monitoring pain points?

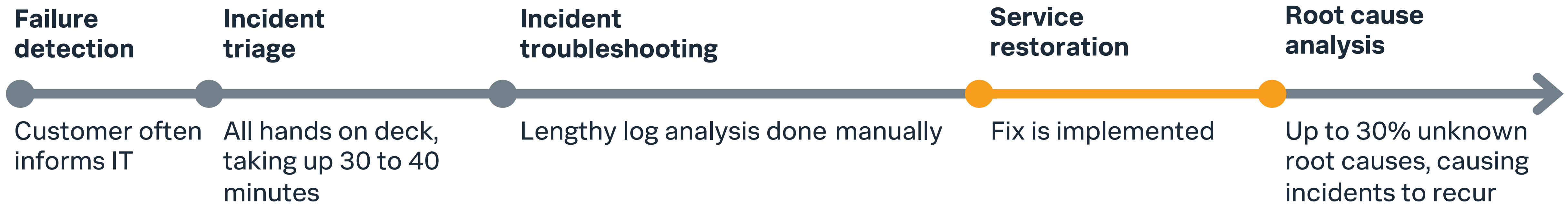
Our customers have experienced significant improvements in monitoring and troubleshooting with Splunk, including:

- Improved detection times
- Faster triage and investigation
- Service restored more quickly
- Faster root cause analysis so they can document trends in incident response and plan accordingly

Splunk customers also see cost savings related to infrastructure capacity utilization and are able to find gaps of efficiency instead of just troubleshooting.

Top 4 IT Ops Value Drivers

BEFORE SPLUNK



Failure detection

Customer often informs IT

Incident triage

All hands on deck, taking up 30 to 40 minutes

Incident troubleshooting

Lengthy log analysis done manually

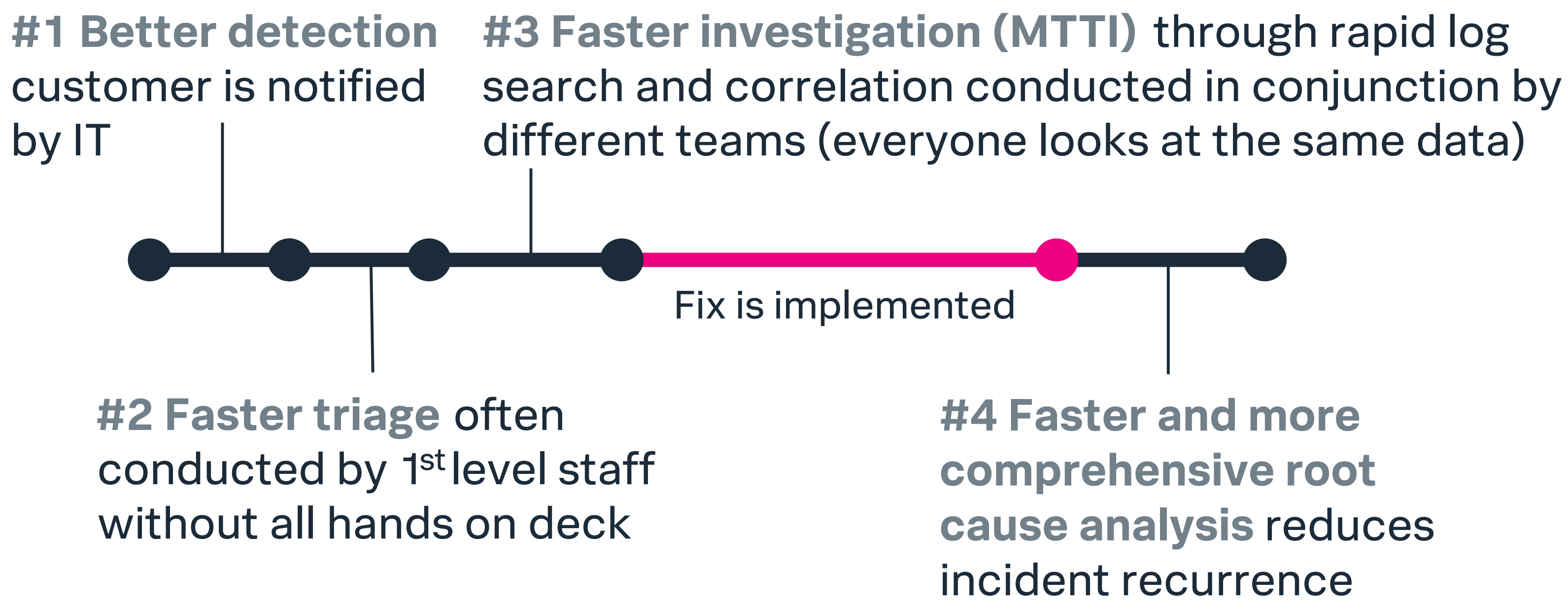
Service restoration

Fix is implemented

Root cause analysis

Up to 30% unknown root causes, causing incidents to recur

WITH SPLUNK



#1 Better detection customer is notified by IT

#3 Faster investigation (MTTI) through rapid log search and correlation conducted in conjunction by different teams (everyone looks at the same data)

Fix is implemented

#2 Faster triage often conducted by 1st level staff without all hands on deck

#4 Faster and more comprehensive root cause analysis reduces incident recurrence

Customer Feedback:

- **15-45%** reduction in high priority incidents
- **70-90%** reduction in incident investigation time
- **67-82%** reduction in business impact
- **5-20%** increase in infrastructure capacity utilization

The Splunk Solution

Splunk offers Splunk® Infrastructure Monitoring, a market-leading service for observability and monitoring in the cloud — private, public or hybrid/multicloud. The Splunk solution visualizes and analyzes performance metrics through streaming analytics across infrastructure, services and applications — including AWS, Linux, Windows and Kubernetes environments — in real time so DevOps, SRE and platform teams can know what's happening before it's too late. The all-in-one user experience correlates data from any source and at any scale from across the entire IT tech stack to provide comprehensive out-of-the-box experiences. Powered by AI and machine learning capabilities, the easy to use, customizable solution will deliver lower MTTD and MTTR in seconds — all through a point-and-click user experience.

Get started with a free trial of Splunk Infrastructure Monitoring to see capabilities, such as:

- Open, flexible data collection
- Cloud API integration with AWS, Azure, GCP and PCF
- Wrappers for serverless functions
- Fully automated Kubernetes monitoring
- Real-time visualization
- Intelligent problem detection and more

> "Real-time monitoring from Splunk lets us support police officers by ensuring they don't have to worry about their tools being down when they're responding to a call in the field; keeping them and the communities they serve safe."
>
> — **DevOps Technical Lead,** Mark43

Conclusion

From lack of visibility during cloud migration to reliance on manual processes, organizations face an uphill battle when it comes to monitoring and managing hybrid and multicloud environments. It's clear that IT needs a solution that will enable them to effectively manage increasingly complex environments — one that will transform operations from reactive to proactive and predictive.

It's easy to get started with Splunk:

Access the free trial for Splunk Infrastructure Monitoring and get started today.

splunk>
turn data into doing™