



Beyond Visibility: Turn Guided Insights into Action for Greater Digital Resilience

Insights from Splunk and Logicalis

Bring context to every alert, everywhere with Splunk and Logicalis

Duplicate and irrelevant alerts across today’s sprawling IT infrastructure make it hard to triage and respond, and to understand how incidents are impacting the business. And, there are a lot of alerts. The volume and lack of actionable insights can quickly lead to staff burnout.

With deep visibility and context into the health and performance of all IT assets and entities, teams can reduce alert noise and prioritize issues based on business impact — sparing them unnecessary false leads and toil. Today’s organizations need a single, live view

of all critical IT assets, entities, and applications so ITOps and engineering teams have the context necessary to troubleshoot problems more effectively.

Splunk Observability and Logicalis help organisations detect threats and issues with context to improve digital resilience.



Only 58% of CIOs feel confident identifying security or performance gaps. Those with stronger visibility and integrated tools can pinpoint issues faster, reducing time lost to false signals and blind spots.

Logicalis 2025 CIO Report
Logicalis



Reduce alert noise



Debug problems in microservices

Don't just see alerts — make sense of them

It's hard for ITOps teams to make sense of what is happening in their environment, much less find and fix issues, when they are drowning in alerts. Tool sprawl and the continued exponential growth of IT and business systems data make this worse. Teams can't find and fix issues. Instead, they spend their time jumping between tools, leading to frustration, lost revenue, and higher costs.

Yet, for over 20 years, ITOps teams have been using event and incident management tools alongside monitoring tools. This accumulation of tools, along with siloed teams and data, creates an onslaught of alerts, many of which are duplicate, and makes it extremely difficult to understand signals from noise. And that results in more unplanned downtime, reactive response, and staff burnout, which has real cost for the business as customer experience suffers.

Leveraging both machine learning and rules-/policy-based correlation, Splunk ITSI can help reduce alert noise by more than 90%.

Splunk and Splunk help ITOps teams manage alerts, avoid downtime, and improve efficiency.

- **Position alerts all in one place:** With data source agnostic inputs, ITOps teams can quickly and easily onboard Splunk and third-party monitoring data into Splunk IT Service Intelligence (ITSI) using data integrations and content packs.
- **Reduce alert noise and group related alerts:** Reducing alert noise can happen in two ways — better alert hygiene with more accurate alerts and grouping related alerts. With Splunk ITSI, leverage root cause analysis to visually correlate services to underlying infrastructure and drill down on specific data to identify root causes.
- **Provide efficient incident response with directed troubleshooting:** With alerts grouped and prioritized, teams can see service impact and use Splunk ITSI Episode Review to find probable root cause on the event timeline. Splunk ITSI machine learning-powered Predictive Analytics capabilities and dashboards trigger alerts based on business KPIs with proprietary algorithms to detect service degradations 30 minutes before they create an issue.

57%

Over half of respondents to the Splunk State of Observability 2024 report say alert fatigue is either somewhat or highly problematic.

Swiftly navigate changes to the application environment

Customers want perfection. But, identifying — and fixing — issues in microservices can become a lengthy and difficult process. When planned or unplanned change causes an issue, engineering teams need to know how it impacts customer experience or other key business metrics. But, in most cases, monitoring solutions cannot give them that kind of visibility.

Engineers often rely on aggregated telemetry, but this data and its respective alerts are frequently tied only to application golden signals, like latency, traffic, errors, and saturation, or infrastructure metrics. But without tying telemetry data to key business metrics, it's extremely hard to prioritize alerts. Since change is constant in the application environment, engineers should be alerted when it impacts key business priorities and be able to zoom in on the performance of key workflows.

Engineers need guided insights that let them take action to:

- **Get granular and accurate alerts on service issues:** Apply custom metrics to improve detection and isolation of problems in service.
- **Monitor the performance of key workflows:** Group together any combination of microservices that align to key functions.
- **Isolate which service, infrastructure, or business logic is causing a problem:** Leverage OpenTelemetry to easily code in any tag for microservices.
- **Debug issues with unified telemetry and visibility for each service:** Bring together all the telemetry data that engineers need to tackle an issue.
- **Diagnose accurate root cause within service infrastructure:** Easily understand issues across your hybrid IT estate, including infrastructure, the network, and apps.
- **Empower advanced troubleshooting use cases:** Log Observer Connect automatically pulls relevant logs from the Splunk Platform so engineering teams and developers can view the logs in context to metrics, infrastructure, and traces to more easily identify the root cause of issues.
- **Gain complete business visibility regardless of architecture:** Discover a unified experience with shared context through the combination of Splunk ITSI, AppDynamics, Observability Cloud, and the Splunk Platform.

59% of CIOs believe vendor solutions are too complex, and many are turning toward more unified approaches that reduce tool sprawl and make core data and performance management easier to control.

Logicalis 2025 CIO Report

Evaluate your alert landscape

Can you guess how many/what percentage of alerts each day are non-actionable?

Understanding how much time your team is spending on going through non-actionable alerts is a critical first step. If less than 60% of alerts are important, there's room for improvement.

Do you have any form of correlation in place to group and prioritize alerts?

Your team could benefit from having all their events — enriched with relevant context — in one place without jumping between tools.

How many people are required to resolve issues today?

You know the saying: Two's company, three's a crowd. An explosion of dependencies in cloud-native environments means no single engineer has the ability to contextualize and resolve an issue. As a result, more people are required when an issue occurs, increasing overhead costs and reducing the amount of time spent on building new code. Your team can benefit from guided insights that deliver needed context to solve quickly.

How do you currently get an understanding of the business impact that performance issues have across your microservice-based apps?

Your team could benefit from tying telemetry data to key business metrics so engineers are alerted when changes in an application environment impacts key business priorities.

Do your engineers have all the telemetry data they need in one place?

Your developers need telemetry data to debug issues in their services. If they have all the relevant metrics, traces, and logs on one dashboard, they can optimize performance.



Gain valuable, guided insights with Splunk and Logicalis

ITOps and engineering teams need context and guided insights to achieve digital resilience at scale. Splunk and Logicalis help detect threats and issues with context to:



Reduce alert noise



Debug problems in microservices

Teams can prioritize issues based on business impact while reducing alert noise to focus on what really matters.

Let’s drive digital resilience forward together.



Learn more: www.splunk.com/asksales
www.uki.logicalis.com

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2025 Splunk LLC. All rights reserved.

Legal information for Logicalis, including policies, terms and conditions, and regulatory statements, can be found on the Logicalis UK & Ireland Legal page at <https://www.uki.logicalis.com/about-us/legal>.



According to the Logicalis CIO Report, the organisations that thrive are those that use insight to fuel innovation. Leaders who unlock the value of their data won’t just keep up - they’ll define what comes next.

Logicalis 2025 CIO Report
Logicalis