

Splunk On-Call

Investigate, collaborate, and resolve incidents faster. Make on-call suck less.

What is Splunk On-Call?

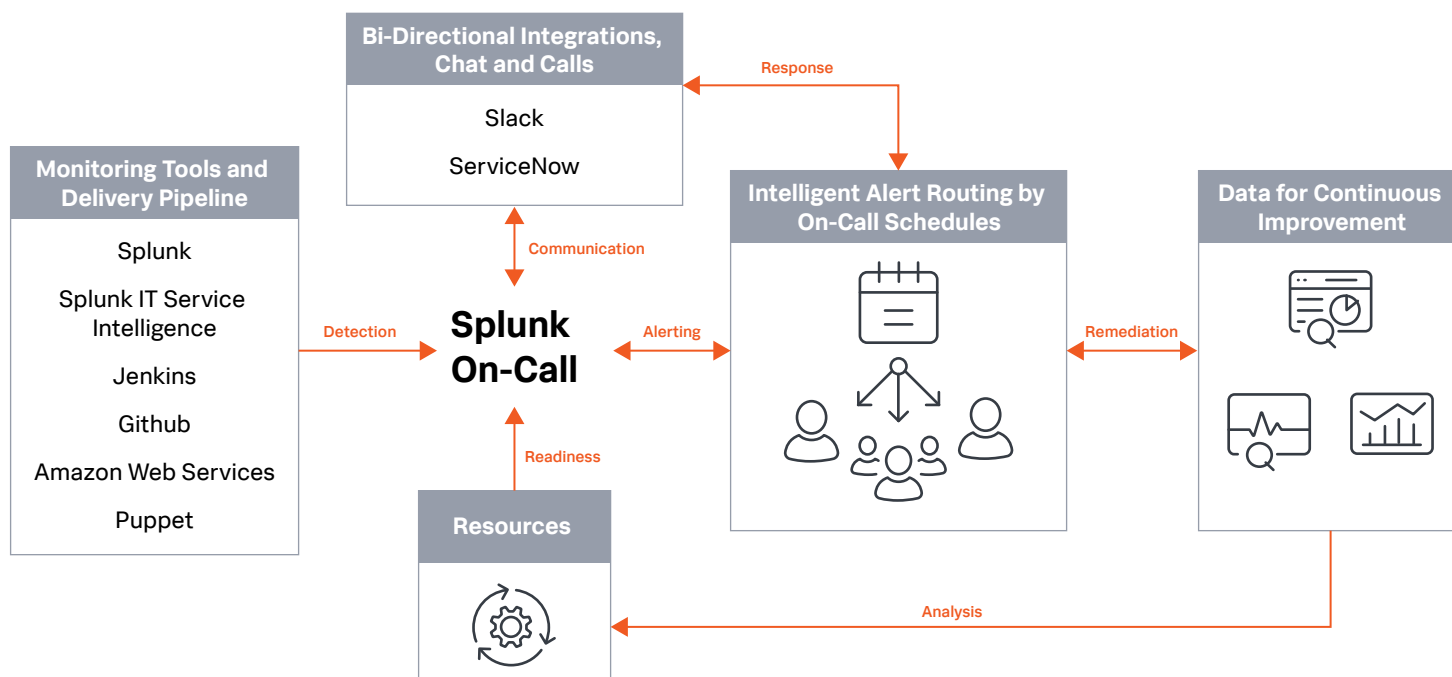
With Splunk, “on-call” isn’t a four-letter word. When application or infrastructure monitoring systems identify issues, Splunk On-Call ingests those alerts and sends them to the correct person based on various on-call schedules. By using Splunk On-Call web and mobile apps, teams understand the holistic health of systems and collaboratively resolve incidents faster, minimizing the impact of downtime.

How Splunk works with On-Call

In essence, Splunk is all about actionable outcomes from vast amounts of data — collecting, analyzing and indexing oceans of it every day. On-Call, on the other hand, is all about *people*.

How this fits into your workflow

When Splunk unearths an issue and triggers an alert, On-Call ingests the alert, appending it with context (e.g., runbooks, annotations, graphs) before automatically routing it to the right person or team. Native chat and built-in Slack integrations make collaboration a breeze. Whether it’s 3:00 p.m. or 3:00 a.m., cross-functional teams have the information they need to solve incidents efficiently.



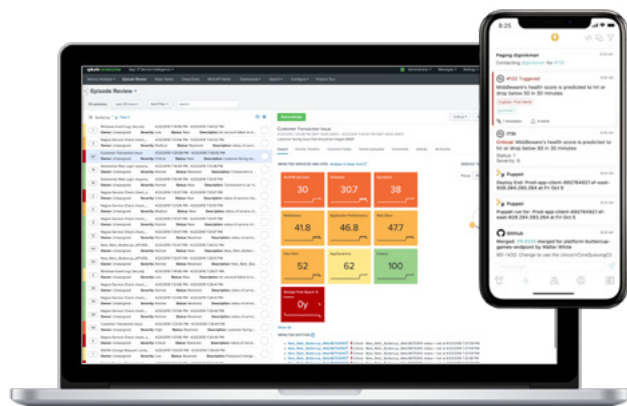
Leveraging AIOps: Splunk IT Service Intelligence (ITSI) + On-Call

Predict and prevent outages

ITSI is a monitoring and analytics solution that uses artificial intelligence (AI) to predict problems, allowing teams to prevent incidents from impacting both revenue and customer experience. When ITSI detects an impending issue and triggers an alert, Splunk On-Call routes the incident to the right expert. On-Call then leverages some machine learning of its own to help responders collaboratively resolve incidents faster.

Reduce alert fatigue

ITSI doesn't just predict and prevent alerts, it generates event episodes (groupings of related events) to help responders not only focus on what really requires attention right now, but also what will require attention in the future. Once ITSI groups events into episodes, On-Call ingests and routes a single incident — not 20 — to on-call engineers, making it much easier for responders to understand dependencies and get to work quickly.



Mapping episodes to incidents.

Centralize monitoring, collaboration and transparency to remediate Splunk issues faster

- **Reduce mean time to resolution:** After Splunk fires an alert, On-Call appends critical context to alerts and sends it to the right expert at the right time, driving high-impact incident resolution.
- **Fast time to value with native Splunk integrations:** With built-in integrations, the Splunk Platform and On-Call connect in moments.
- **Get the most out of Splunk investments:** On-Call displays what types of alerts are most commonly triggered, so teams can see if thresholds are too sensitive — or just right — making it possible to optimize the performance of Splunk investments.
- **Revenue protection:** Increased uptime means positive brand perception and happy customers.
- **Reduce attrition:** Providing engineers with a more positive on-call experience improves collaboration during incidents and reduces burnout.
- **Continuous improvement:** After resolution, Splunk dashboards display incident details to achieve more visibility and drive process improvement.
- **Mobile-led incident response:** Mobile-first approach puts all of the power of Splunk On-Call within a responder's device.

Ready to get started?

Integrating Splunk and On-Call is a breeze. Contact your Splunk representative or start a free, 14-day trial of [Splunk On-Call](#) — no credit card required!



Learn more: www.splunk.com/asksales

www.splunk.com