RESOLVE SYSTEMS™

Mission Critical IT Incidents: When You Need Resolution, Not Just Data.

Contents

Businesses rely on IT operations to assure the availability of mission-critical services and infrastructure. As systems' uptime and performance are crucial to the success of daily business activity, IT incidents must be identified and mitigated quickly. As such, operations teams employ cutting-edge tools to continually monitor assets. Splunk, the leader in analyzing organizations' big data, offers Splunk Enterprise and Splunk IT Service Intelligence (ITSI) to help IT operations teams proactively monitor critical infrastructure and services; reduce alert fatigue with event correlation and deduplication; and even visualize services and key performance metrics.

IT operations teams are charged with diagnosing and resolving infrastructure and service incidents as quickly as possible. That means optimizing event validation as well as incident diagnosis and resolution starting in Splunk is an important area to explore.

IT Incidents Could Cost Thousands a Minute

IT and customer-impacting incidents occur frequently, with the average organization logging approximately 3,000 per month.[1] The consequences of downtime to mission-critical applications can be significant, as these incidents:

- Impede employee productivity
- Disrupt business operations
- Prevent businesses from meeting customer SLAs
- Damage brand equity

In concrete terms, almost one in three enterprises report an hour of downtime costs $1 million or more, with an average downtime cost of $8,662 per minute.[2] As the stakes are high for managing incidents quickly and efficiently to resolution, many offerings exist in the marketplace to help operations teams identify incidents as early as possible.

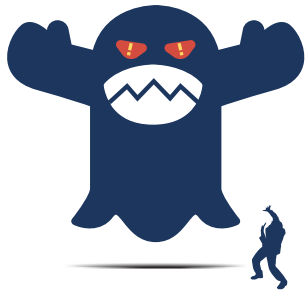
Splunk Helps IT Keep up with the Incident Storm by Monitoring Key Systems to Identify and Prioritize Events

Splunk provides service, device, and application monitoring, as well as event correlation and alerting on top of its industry-leading big data platform. At first glance it appears IT teams' event management needs are fully addressed by Splunk.

Enterprises must not just detect events, but validate, diagnose, and resolve the incidents they identify.

IT operations teams are charged with achieving incident resolution as quickly, reliably, and inexpensively as possible. And not just for simple, everyday events, but also for events with the most complex root causes that signal the most potentially disruptive incidents.

Fighting the Invaders: Incident Resolution is Too Critical for Manual Methods



Even with Splunk quickly detecting events, those events are typically reviewed, validated, and (when they're incidents) resolved manually. This approach is slow and has many dependencies—especially for an event that identifies an incident, as an IT Service Management platform must be involved.

Even with a Splunk installation, IT incidents are commonly resolved manually in the enterprise today.

Manual incident resolution also invites human error. When trying to validate a Splunk event, frontline IT agents must often swivel chair between Splunk and other siloed applications or scripts. The results of their commands are sometimes difficult to understand, and activity data can be lost between tools. Plus, many organizations lack complete or up-to-date standard procedures for frontline agents to validate, diagnose, and resolve incidents. That means agents are often left to interpret command results with only their best judgment as a guide, which is unlikely to deliver the high quality or consistency needed for robust incident resolution.

What's more, frontline agents often typically lack permissions to log into impacted systems or execute necessary diagnostic or remediation actions. This disempowerment causes unnecessary escalations to Level 2 and beyond, even for relatively simple incident types, so more incidents end up waiting for attention from fewer people.

Manual Incident Resolution Means Higher OpEx & Missed Opportunities

Manual incident resolution leads to escalations, which bring heavy burdens to the IT organization. Resolution by Level 2 agents cost nearly three times as much as resolution by frontline agents. Incidents resolved by top-tier resources cost a whopping nine times what a frontline agent-resolved incident does.[3] Escalations also reduce the productivity of Level 2 agents and Subject Matter Experts (SMEs), as these valuable personnel spend time on reactive, incident-related fire-fights rather than value-added projects to foster the broader enterprise.

Manual incident resolution is also slow, and the consequences of slow incident resolution are felt across the business. The longer a major incident takes to resolve:

- The longer and more serious the service impact
- The more likely customer SLAs are violated
- The higher the chances a customer-impacting incident will negatively affect brand equity

In the case of major incidents, IT organizations take half an hour just to assemble the right members into a response team, and the average time to resolve major incidents is nearly six business hours, with the most severe extending well beyond that.[4]

Can the Promise of Automation Deliver?

Clearly, incident resolution is a valuable area to focus improvements that will reduce expensive manual efforts, errors, and escalations. By promptly identifying service events in Splunk and quickly validating, diagnosing, and resolving the incidents they identify, businesses can drastically reduce legal and financial pitfalls; improve customer satisfaction; and mitigate other risks associated with infrastructure or service failures. That's why many IT operations teams are investigating the promise of automation, as well-applied automation can help the organization manage increasing numbers of systems and users without adding costly head count.

The key question on many IT operations leaders' minds is:

What's the best way to automate incident resolution with Splunk?

Getting to the answer requires understanding the types of automation available as well as when and how to implement.

The Right Automation Framework to Defeat the Incident Invaders

In pursuit of improved IT incident resolution, many focus exclusively on introducing automation as a wholesale replacement for human activity. This is often referred to as "end-to-end" automation—where automation handles event validation, and incident diagnosis and resolution without any human involvement. Although end-to-end automation can help remove human error and speed up resolution for certain types of incidents, IT teams need to accelerate all events and incidents, including the complex ones.

End-to-End Automation: Automation that handles an event or incident without any human involvement, from validation through diagnosis to resolution

This means other key capabilities are required alongside end-to-end automation.

Use Automation that Works with the Operations Team

IT events span a spectrum of complexity, ranging from simple resource utilization alerts to critical application performance warnings—events signaling that complex and disruptive issues may be unfolding. For example, critical business service outages may involve many layers of applications and infrastructure.

This means operations teams need a strategy to accelerate event validation as well as issue diagnosis and resolution for all kinds of issues, from the simple to the most complex. For less complex incidents, end-

to-end automation can accomplish the entire resolution process with no human interaction. However, challenging incidents affecting mission-critical systems can't be easily addressed by end-to-end automation. In these cases, IT operations teams should employ automation to work *with* the human agent to validate the event and isolate the issue across a broad technology stack.

What Would this Strategy Look Like in Practice?

An effective method would be to provide frontline agents interactive procedures containing human-guided automations to help execute event validation, issue diagnosis, and resolution. An "interactive" procedure is one that helps an agent troubleshoot and investigate a complex event or incident by asking questions and updating itself in response to the agent's answers. That way, the agent can effectively direct any issue down the right path to quicker resolution.

> *Combining interactive procedures with human-guided automations accelerates almost any process.*

As opposed to end-to-end automation, human-guided automation takes care of *individual tasks* in the midst of an agent's larger workflow to save the agent from slow, manual tedium. The combination of these two capabilities means any previously-manual process can be modelled and accelerated. As a result, a frontline agent becomes capable of performing tasks that would traditionally require escalation to Level 2 or beyond.

For a concrete example of these capabilities at work, see the Resolve automation and incident resolution platform.

Interactive Procedure: *A procedure that updates in response to an agent's choices.*

Human-Guided Automation: *Automation that performs a single task in the midst of a larger, human-directed workflow.*

Go From Reactive to Proactive Resolution

A major reason monitoring and event correlation are valuable is they provide early indication of problems in the infrastructure or services. However, an alert typically indicates a system is already out of its expected state. If only one could extend event detection into proactive checks that take immediate action to fix impending issues! That would turn the entire incident life cycle of validation, diagnosis, and resolution from a reactive, post-event endeavor into a proactive, service-assurance process.

While the concept of health checks isn't new, combining health checks with proactive resolution brings significant benefits: As is seen when using a platform like Resolve.

Lowered operational costs

Reduced incident impact

Reduced risk of downtime

Faster issue recovery time

For example, IT operations teams can leverage proactive resolution to regularly check hosts' CPU, memory, and storage utilization; cross-reference vital signs; and take action before any performance degradation. With proactive resolution, many common issues can be avoided, and IT teams can focus on the events that truly require immediate attention.

Build on What's Already Working

The vast majority of IT teams have made inroads or are experimenting today with automation—whether it be scripting, building homegrown solutions, or investing in commercial automation tools. In seeking an automation platform to accelerate event validation and incident resolution, IT operations teams want to avoid losing the value of what they've already built and stored their knowledge in. Plus, an automation platform with the ability to leverage pre-existing automation tools and scripts can help the team get up and running quickly.

Consider the effort you may have put into your existing automation approach. It's sensible to try to preserve as much of that work as possible.

IT wants an automation platform that integrates existing scripts as well as orchestrates previously-installed automation products. Such a platform helps IT operations teams reduce their operating expenses as it makes use of existing investments and simplifies the deployment of new automation (via reuse of existing work product). With this kind of platform, operations teams also avoid the risk typically created by change, as the organization's existing intellectual property is protected, and existing automation integrity is preserved—all capabilities offered by Resolve. Plus, the launch of a new automation platform can create the opportunity to unify existing automation assets.

React to Change Fast as Lightning with High Maintainability

As obsolete procedures or automation can harm the quality of event validation and incident resolution, IT operations should be able to respond quickly to changes in infrastructure and applications. An automation platform therefore needs to enable rapid deployment of new automations and changes to existing automations.

Non-developer IT operations experts need tools to quickly build and edit automations

For example, with Resolve, a library of pre-built automations, building blocks, and connections to 3rd-party systems accelerates the development and deployment of new automated processes. As every organization's environment is unique, IT operations SMEs need tools to help them quickly build and edit automations without support from an external engineering team. This enablement not only makes waiting on outside help unnecessary, it's also a way of retaining and implementing IT experts' knowledge. Giving the operations team this power requires:

- Reusable automation content
- User-friendly graphical automation- and process-building tools
- Quick and easy knowledge capture

IT operations teams armed with these tools reap significant cost savings, as fewer resources are required in the construction or editing of automations, and the time to develop automations is cut down substantially. Further, the organization retains tribal knowledge as processes and automations. These automations are easily maintained and thus much less likely to become obsolete.

Accelerate Incident Resolution with Resolve

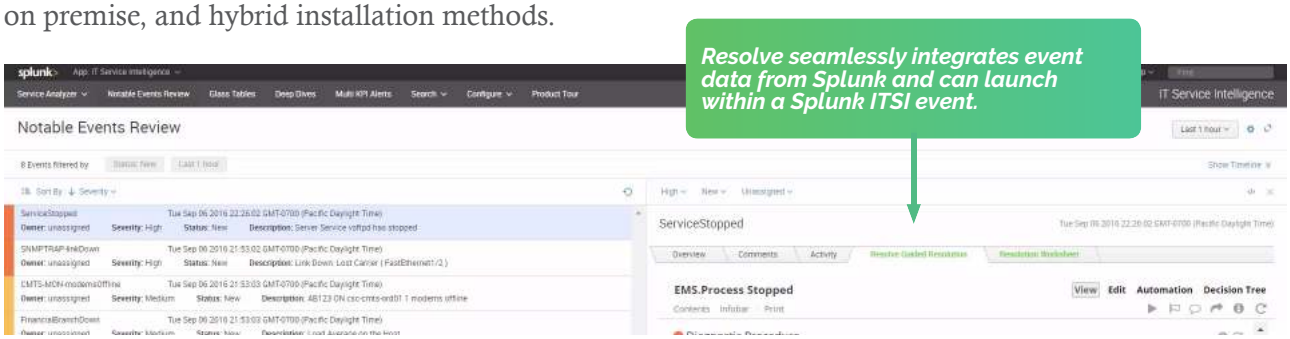
Resolve brings these key capabilities to IT operations' Splunk implementations.

Resolve is an industry-leading software platform for resolving IT incidents at scale, with the lowest cost and mean time to resolution.

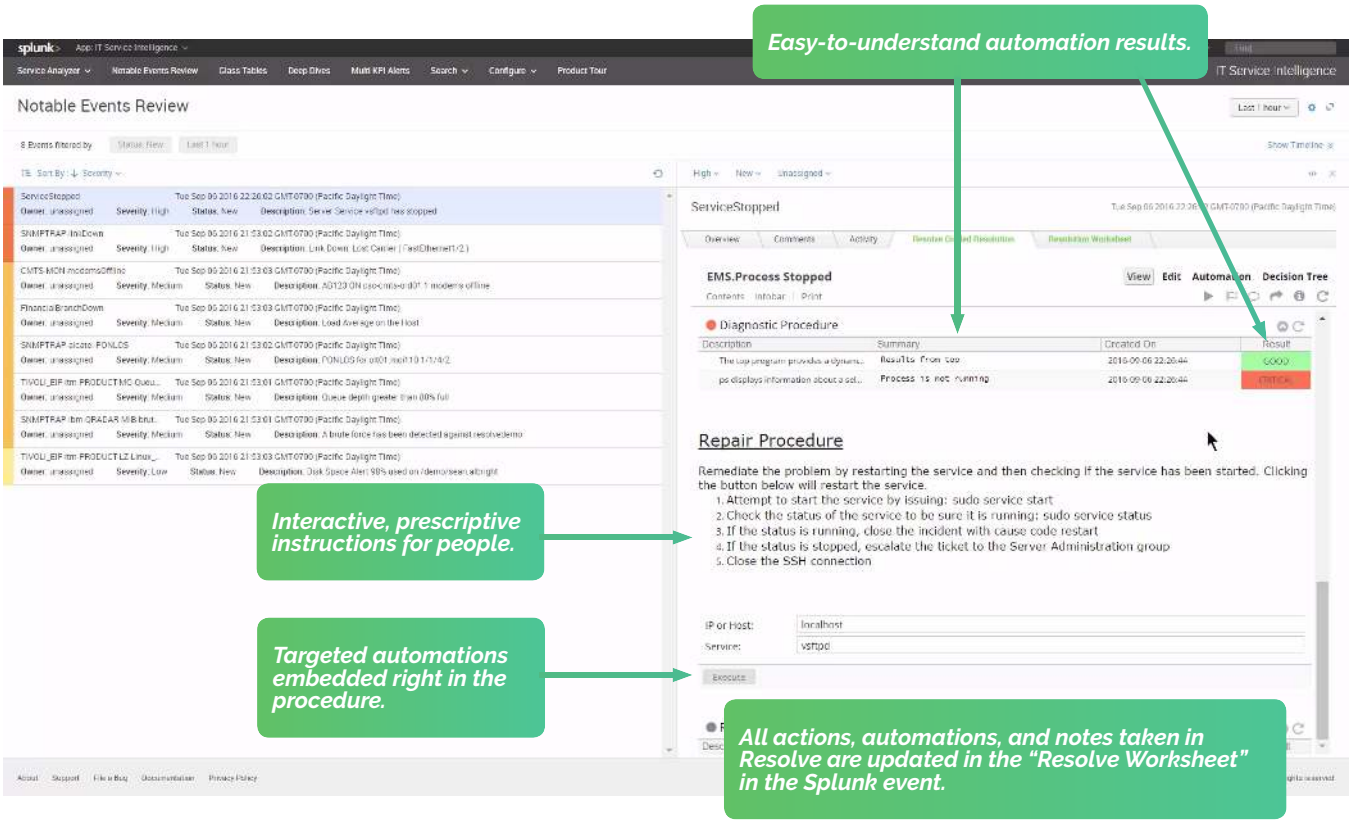
Resolve accomplishes this by fully automating event validation, and incident diagnosis and resolution wherever possible. When human intervention is required, Resolve provides frontline agents interactive, context-specific procedures and embedded, human-guided automations to speed activity and reduce escalations to Level 2 agents or expensive SMEs.

The largest global enterprises have deployed Resolve as the platform stands up to the most demanding requirements of performance and scale. The Resolve add-ons for both Splunk Enterprise and Splunk IT Service Intelligence, available on Splunkbase, provide integrated functionality to drive increased operational efficiency and faster resolution through Splunk.

To achieve quick time to value and quick time to market with new or edited automations, Resolve offers an extensive library of pre-built automations and procedures for common event and incident types as well as pre-built integrations to key IT systems. It also offers a low-code automation builder, parsing wizard, and graphical development tools for building both automations and interactive guidance. Resolve supports SaaS, on premise, and hybrid installation methods.



- A Splunk correlation search triggers Resolve, which starts an associated automation or process to validate, diagnose, and even resolve the issue
- Resolve capabilities appear within Splunk ITSI, so agents have instant access to Resolve's validation and diagnostics, and they can easily engage Resolve's interactive resolution



Conclusion

As alerts continue to deluge IT operations teams, and incidents cost organizations huge sums of money, Big Data leader Splunk has stepped in to sift through the onslaught to correlate, organize, and prioritize events into useful insights. For IT leaders seeking to validate and diagnose events, as well as resolve incidents faster and more efficiently, automation is crucial for keeping mission-critical systems and applications available. Achieving success with event automation in Splunk hinges on having a comprehensive automation strategy, along with the ability to proactively resolve issues and integrate existing tools while also ensuring high maintainability.

Resolve compliments Splunk in these crucial areas and speeds response to even the most complex IT events and incidents, helping IT operations teams maintain critical performance and service continuity, as well as reduce risk and operations costs.

References

1. https://www.splunk.com/pdfs/white-papers/damage-control-the-impact-of-critical-it-incidents.pdf
2. https://techbeacon.com/20-it-ops-stats-matter and https://italerting.com/state-of-incident-management/
3. Ibid and https://www.splunk.com/pdfs/white-papers/damage-control-the-impact-of-critical-it-incidents.pdf

About Resolve Systems

Proven to scale and support the largest and most complex enterprise environments, Resolve Systems is the global leader in delivering incident response and resolution, fully focused on orchestration, automation and incident resolution to help customers address all aspects of the incident response lifecycle. Resolve Systems' focus on human-guided, end-to-end automations makes it the only solution flexible enough to address the full spectrum of use cases whether it be for IT, network or security operations.

Headquartered in Irvine, California, USA, with a global footprint, Resolve Systems is majority owned by funds affiliated with Insight Venture Partners, a leading global private equity and venture capital firm investing in high-growth technology and software companies.

About Insight Venture Partners

Insight Venture Partners is a leading global venture capital and private equity firm investing in high-growth technology and software companies that are driving transformative change in their industries. Founded in 1995, Insight has raised more than $23 billion and invested in excess of 300 companies worldwide. Our mission is to find, fund and work successfully with visionary executives, providing them with practical, hands-on growth expertise to foster long-term success.

For more information on Insight and all of its investments, visit www.insightpartners.com or follow us on Twitter.