

Extend your Investment in ServiceNow with Incident Resolution Automation

Contents

1
The Reality of IT Incidents

2
ServiceNow Helps IT Organize & Manage Incidents

3
Consequences of Manual Incident Resolution

Can the Promise of Automation Deliver?

4
Implement an Automation Strategy that Fits Your IT Operations Team

Left Shift Incident Resolution Workload

5
Integrate to Automate

React to Change Quicker

Accelerate Incident Resolution with Resolve

7
Conclusion

References

About Us

Businesses rely on IT operations to assure the availability of mission-critical services and infrastructure. ServiceNow is the leader in IT Service Management (ITSM) tools to help improve the communications and service level of enterprise IT organizations. Many enterprises invest in the ServiceNow IT Service Management suite to consolidate IT services into a single system of action, get a real-time view of KPIs for IT agents and managers, and align IT services to the business. When deployed, ServiceNow derives increasing value over time, so optimizing incident management in ServiceNow is an important next step to explore. Ultimately, IT operations teams aim to validate, diagnose, and resolve all incoming tickets as quickly as possible.

The Reality of IT Incidents: Hundreds a Day, with Some Costing Thousands a Minute

IT and customer-impacting incidents occur frequently, with the average organization logging approximately 1,200 per month.ⁱ More than half of IT organizations identified as prepared to support digital services still experience customer-impacting incidents at least weekly.ⁱⁱ Incidents also run the gamut of complexity, from simple password resets all the way to major business service outages. While less impactful incidents typically occur many times per day, even major IT incidents occur as frequently as every other week for a significant fraction of enterprises.ⁱⁱⁱ

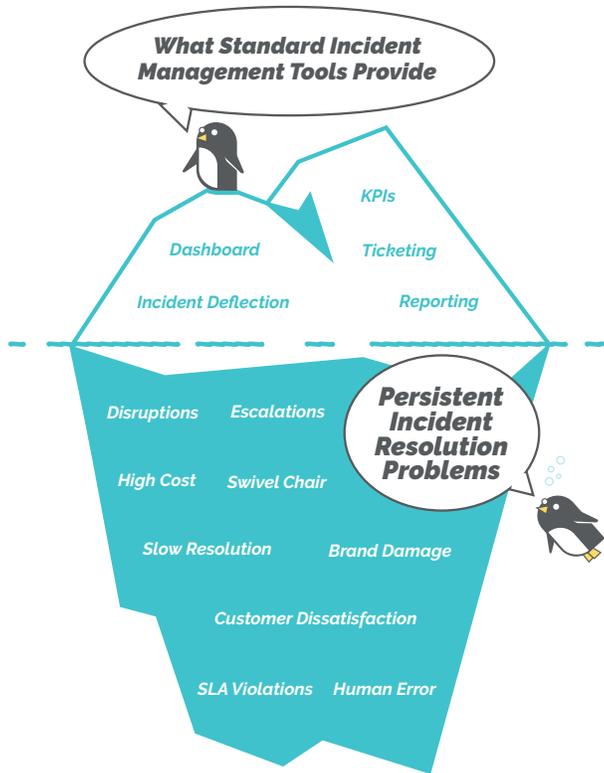
The consequences of downtime to mission-critical applications and systems can be significant, as these incidents:

- » Impede employee productivity
- » Disrupt business operations
- » Prevent businesses from meeting customer SLAs
- » Can even damage brand equity

Nearly three quarters of global enterprises report a past critical incident has caused reputational damage.^{iv}

IT incidents can drive immense costs, damage an enterprise's brand, and even disrupt its revenue-generating ability.

In concrete terms beyond brand equity, almost one in three enterprises reports one hour of IT downtime costs \$1 million or more, with an average cost of downtime of \$8,662 per minute.^v Close to 80% of the cost of downtime is attributed to loss of employee productivity, with the sales organization being the most frequently impacted.^{vi}



ServiceNow Helps IT Organize and Manage Incidents

ServiceNow steps in to help with its Incident Management solution, offering a quality toolkit for: deflecting incidents via a service portal; capturing IT incidents across multiple contact channels; viewing incidents in the broader context of all IT tasks and projects; tracking incident work status; organizing a variety of service-level commitments between providers and customers; and even on-call scheduling. In essence, ServiceNow Incident Management circles an IT incident, connects the team, tracks, and reports to drive better performance for the whole IT operations organization.

At first glance it appears the enterprise’s incident management needs are fully addressed by ServiceNow Incident Management. However, consider the actual resolution of the incident. Enterprises aim not just to track and report on incidents, but also resolve them faster, more reliably, and cheaply. And not just for the day-to-day incidents, but also for the most complex and potentially disruptive incidents as well.

Incident Resolution Is Too Critical for Manual Methods

Even with a ServiceNow installation, IT incidents are commonly resolved manually. This approach is slow and has many dependencies. When trying to validate, diagnose, or resolve an incident, frontline agents often must “swivel chair” between ServiceNow and other siloed applications systems. The results of their commands are sometimes difficult to understand and activity data can be lost in the transfer between tools. What’s more, frontline agents typically lack permissions to log into impacted systems or execute necessary diagnostic and remediation actions. This 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 also invites human error. Many IT organizations lack complete or up-to-date standard procedures for frontline agents to validate, diagnose, and resolve incidents. Even if they are able to interpret command results, their best judgment is their only guide.

Best judgment is also relied upon in documenting results and steps taken in the ServiceNow ticket while addressing an incident. As frontline agents are the least experienced members of an IT organization, their best judgment is unlikely to deliver the high quality or consistency needed for robust incident resolution.

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

Consequences: Higher OpEx, Missed Opportunities, and Potential Reputational Damage

All these escalations bring heavy burdens to the IT organization, the most glaring of which is an increased operations expense. When a Level 2 agent or Subject Matter Expert (SME) (e.g., database administrator, network engineer, systems engineer, security professional, etc.) receives an escalation, he must spend time reviewing the ServiceNow ticket and replicating the actions of the frontline agent before he can continue to drive the incident forward. There is a high cost to this individual's time. Incidents resolved by Level 2 agents cost the organization nearly three times as much as those resolved by frontline agents. Incidents resolved by top-tier IT resources cost a whopping nine times what a frontline agent-resolved incident does.^{vii}

Beyond calculable operations cost, escalated incidents also carry significant opportunity cost for the IT organization. Some 60% of organizations say incidents and outages cause IT team disruption and distraction.^{viii} Escalations reduce the productivity of Level 2 agents and SMEs, as these valuable personnel spend time on reactive, incident-related fire-fights rather than value-added projects to foster the broader enterprise. In extreme examples, this effect may even compromise the pace of innovation.

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 to be 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 on average just to assemble the right members into an IT response team, and the average time to resolve major incidents is nearly six business hours, with the most severe extending well beyond that.^{ix}

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 issues and quickly validating, diagnosing, and resolving IT incidents, businesses can drastically reduce legal and financial pitfalls; improve customer satisfaction; and mitigate other risks associated with infrastructure or service failures. This is 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:

How do you approach automation for incident resolution?

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



Faster, Consistent Incident Resolution with Automation

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 an incident without any human involvement all the way from validation through diagnosis to resolution. Although end-to-end automation can help remove human error and speed up resolution for certain types of incidents, IT needs to accelerate all incidents, including the complex ones. This means other key capabilities are required alongside end-to-end automation for maximum acceleration.

Implement an Automation Strategy that Fits Your IT Operations Team

As discussed, IT incidents span a spectrum of complexity, from simple service requests, like creating a user account, to critical business service outages that may involve multiple layers of applications and infrastructure. This means that IT operations needs a strategy to accelerate all incident types, from the simple (server restart, password reset) all the way to the most complex (virtual infrastructure, customer portal) incidents. For simple incidents, end-to-end automation (as seen in offerings like ServiceNow's Orchestration product) can accomplish the entire resolution process with no human interaction. However, challenging incidents affecting mission-critical systems can't easily be addressed by end-to-end automation. In these cases, IT teams should employ automation to work with the human agent to isolate and validate the problem area across a broad technology stack. Complex incidents and incidents affecting mission-critical systems can't be addressed by end-to-end automation.

What would this optimal strategy look like in practice? An effective method would be to provide agents interactive procedures containing targeted automations to help execute incident validation, diagnosis, and resolution. An "interactive" procedure is one that helps an agent troubleshoot and investigate a complex incident by asking questions and updating itself in response to the agent's answers. That way, the agent can effectively direct the incident down the right path to a quicker resolution.

Targeted automation is the opposite of end-to-end automation, as a targeted automation takes care of a single task 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.

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

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

Left Shift the Incident Resolution Workload

As escalations are harmful to both the IT organization and the broader enterprise, IT operations should seek to reduce escalations (often referred to as "left shifting" work) to achieve the fastest incident resolution at the lowest cost. Automation can assist in this aim by proactively testing systems to identify and remediate issues before they have a business impact.

With such a platform in place, the IT organization will see a reduction in escalations and increased team morale.

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

Left Shift: Push work to the lowest-tier resource available; i.e., from L2 to L1, and from L1 to automation.

Integrate to Automate

Automation does not occur in a vacuum. IT operations teams need an incident resolution automation platform that can readily interoperate with their existing IT systems and infrastructure. Resolution actions will likely include making controlled changes to connected assets and systems to fix identified problems and may require the platform to stitch together data from multiple IT management applications, the CMDB, network topology, and other tools to help with both human and automated decision making.

React to Change Quicker with High Maintainability

As obsolete procedures or automations can harm the quality of incident resolution, IT operations should be able to respond quickly to changes in infrastructure, applications, and business process services. This means an incident resolution automation platform should enable rapid deployment of new automations and changes to existing automations.

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

Development of new automated processes accelerates with a library of pre-built automations, building blocks, and connections to 3rd-party systems. As every organization's environment is unique, non-developer IT operations SMEs should be enabled to quickly build and edit automations. This enablement not only saves IT operations from having to wait on support from an external development team, it's also a way of retaining and implementing IT experts' tribal knowledge.

Accelerate Incident Resolution with Resolve

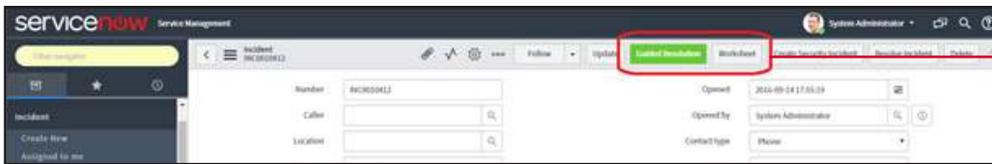
These key capabilities can be brought to IT operations' ServiceNow implementation with Resolve.

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

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

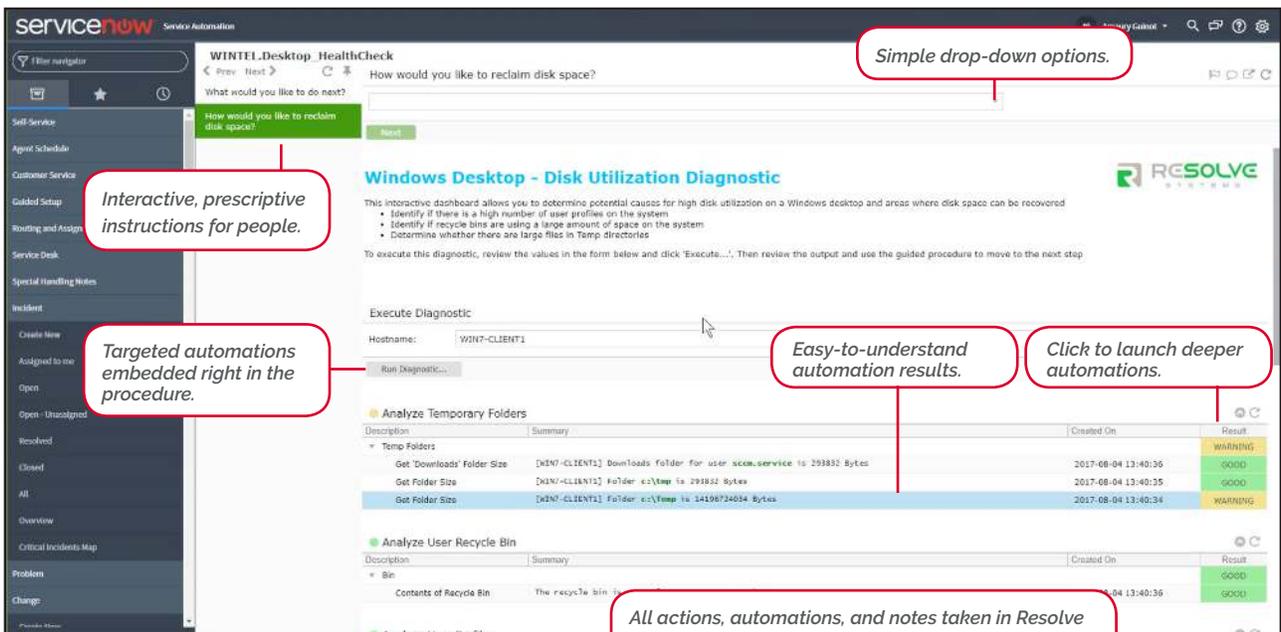
The largest global enterprises have deployed Resolve, as the platform stands up to the most demanding requirements of performance and scale. Resolve, certified by ServiceNow, provides an integrated experience to help extend organizations' investments in ServiceNow's Incident Management.

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 known incident types and out-of-the-box integrations to key IT systems. It also offers a low-code automation builder and graphical development tools for building automations and interactive guidance. Resolve even supports SaaS, on premise, and hybrid installation methods.



Resolve seamlessly integrates ticket data from ServiceNow and launches from a single click within a ServiceNow incident

- » As soon as an incident or request is submitted in ServiceNow, Resolve can trigger an associated automation or process
- » Resolve routes incidents and events to the appropriate execution based on the context and contents of the ServiceNow ticket



Conclusion

As incidents continue to pile up on IT operations teams and cost organizations huge sums of money, IT service management leaders like ServiceNow step in to help IT organize and manage the onslaught of incidents. IT leaders seek to resolve incidents faster and more efficiently, and automation is key to this initiative. Achieving success with incident resolution automation hinges on having a comprehensive automation strategy that left-shifts workload, along with an eye to integrating automation into the infrastructure and ensuring high maintainability.

Resolve compliments ServiceNow in these crucial areas and speeds responses to even the most complex IT incidents, helping IT operations teams maintain critical service continuity and reduce operations costs.



References

1. <https://www.splunk.com/pdfs/white-papers/damage-control-the-impact-of-critical-it-incidents.pdf>
2. <https://iqm711pa7bn3d42rc278rat5-wpengine.netdna-ssl.com/assets/report-digital-operations.pdf>
3. Ibid.
4. <https://www.splunk.com/pdfs/white-papers/damage-control-the-impact-of-critical-it-incidents.pdf>
5. <https://techbeacon.com/20-it-ops-stats-matter> and <https://italerting.com/state-of-incident-management/>
6. <https://www.opsgenie.com/blog/facing-downtime-in-it-operations> and <https://iqm711pa7bn3d42rc278rat5-wpengine.netdna-ssl.com/assets/report-digital-operations.pdf>
7. <https://www.metricnet.com/benchmark-2014-global-results-for-desktop-support/>
8. <https://italerting.com/state-of-incident-management/>
9. Ibid and <https://www.splunk.com/pdfs/white-papers/damage-control-the-impact-of-critical-it-incidents.pdf>

About Resolve Systems

Resolve Systems is the global leader in providing a single platform for enterprise-wide incident response, automation and process orchestration for Security Operations, IT Operations, Network Operations and service desk teams.

Resolve accelerates incident response and resolution by supplying engineers with partially or fully customized human-guided automations, powerful real-time incident collaboration and the omnipresence to orchestrate existing systems, across silos.

Headquartered in Irvine, California, USA with operations in EMEA and APAC, **Resolve Systems** works with nearly 100 of the largest global firms and 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 \$13 billion and invested in nearly 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](#).



North American Headquarters
2302 Martin Street
Suite 225
Irvine, CA 92612
T: +1.949.325.0120

EMEA Headquarters
60 Cannon St
Suite 119
London EC4N 6LY, UK
T: +44 (20) 37432123

Asia Pacific Headquarters
1 Fullerton Road
#02-01, One Fullerton
Singapore 049213
T: +65 6832 5513