Automate incident management across teams with Slack and PagerDuty
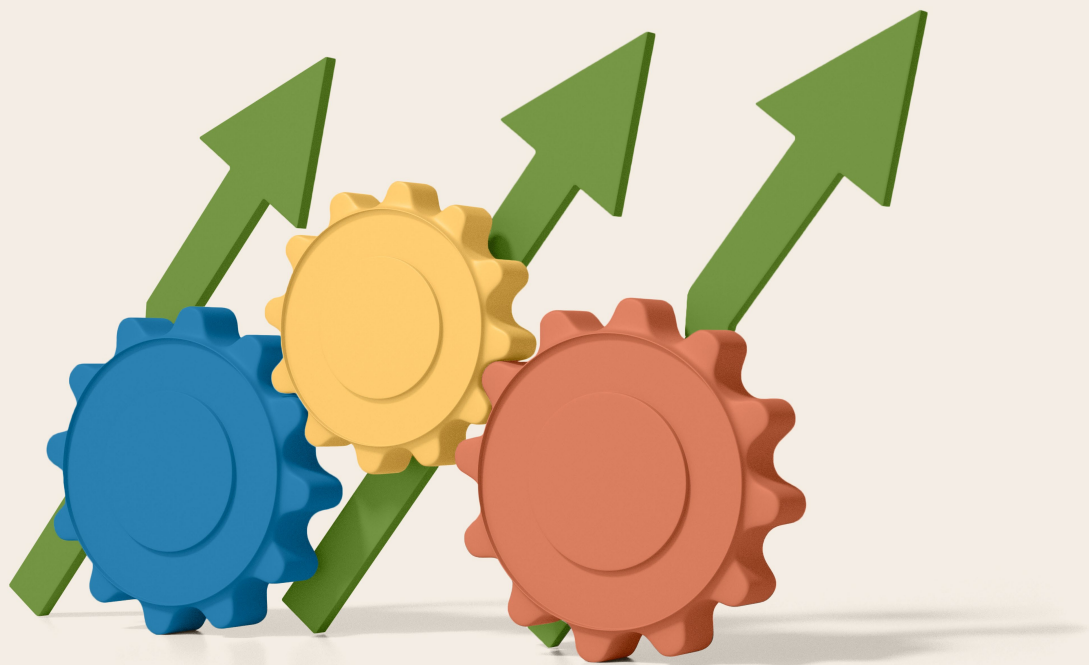
slack | PagerDuty

Table of contents

Introduction

In today's digital world, incidents occurring in customer-facing applications have a wider impact beyond the technical teams who respond to them. Customers demand to know why their tool, app, portal, game or shop is no longer responding. At the same time, internal leadership and line-of-business stakeholders are looking for answers.

While these update requests may be distracting to responders who have to stop what they're doing to give status reports, this cross-functional communication is still required. Communication is a key part of the incident response process, especially with teams adopting hybrid work. Luckily, there's a way to do it so that both sides of the house, technical and non-technical, feel supported and empowered to see the incident through. When used together, PagerDuty and Slack provide an end-to-end approach to managing incidents in real-time, seamlessly coordinating communications and collaboration across teams in an organization. The result? Less stressful incident management experiences and better customer outcomes.

The growing need for incident response automation

There have been many positive advancements lately in technology, tools and DevOps. But with these advancements comes more complexity to the incident management process, such as:

- Changes being released more often
- Distributed microservices creating more complexity and dependencies
- Siloed teams and tools creating confusion and chaos
- Reliance on external cloud providers and vendors

This level of complexity leads to a higher volume, variety and velocity of incidents. These incidents, in turn, can make a huge dent in your company's bottom line. *According to a 2023 survey conducted by IDC*, *the average cost of an hour of downtime/outage can range from $100,000 to $250,000.*[1]

To manage incidents at scale, you need automation and alignment within teams during those that are most critical and time-sensitive.

"Slack has had a dramatic effect on engineering productivity at Riot. We've seen a reduction in iteration cycle and bug-resolution times and increases in feature delivery velocity since moving to Slack."

Bryan Dover
Former Software Engineering Manager and Team Captain of IT Applications, Riot Games

---

[1] IDC, "AIOps and Observability Survey Results: Leadership Drives Trust and Expansion," January 2023

Who needs to know about a critical incident?

Of course, technical teams who can help resolve or are impacted by the issue need to be alerted and updated immediately. During an incident, though, you'll also have several additional audiences who need varying levels of detail about what's happening. It's unlikely that customers will need a deep technical understanding of what's happening behind the scenes. It's also unlikely that executives will be satisfied with short customer-oriented communications. For on-call responders, it's important to tailor your incident-related communications based on your audience. Here are five audiences to keep in mind:

Executives:
Executives are the most common stakeholders asking to be informed of high-priority issues. You'll want to give them the bottom line up front. The most important things they'll care about are customer impact and SLA violations, if applicable to the business. They will expect a regular update on progress and ensure that you have the resources and support you need.

Customer service teams:
These teams are often on the front lines of incidents yet can feel left in the dark about how the resolution process is going. Customer service teams want to communicate with customers about when service will return to normal. It's key to ensure that these teams are among the first to hear about new incident developments, bridge communications between customers and engineering, and foster trust.

Additional technical teams:
Often an incident on a single service affects other teams. They can't actively do anything about it, but they still need to be aware. In high-priority incidents, it may be beneficial to inform them of the customer impact, provide relevant progress updates, and request their assistance.

Customers:
Customer-impacting incidents can erode trust. One way to maintain some of that trust is by openly communicating with customers about incidents that affect them. Strategic customers want more frequent and in-depth updates. The rest of your customer base deserves an acknowledgment update, sharing that there's an incident and that you are working to fix it.

Additional line-of-business teams:
Teams like marketing, sales, legal and finance may need to know about incidents that affect how they conduct business. Marketing may want to stall a campaign that would drive prospects to a broken website. Sales may want to postpone demos. Legal and finance might want to get ahead of SLA penalties.

Slack modernizes the incident command center

Bring teams together quickly to speed up response

Gone are the days of mile-long email threads. Slack unites conversations around code changes and monitoring alerts into topic- or incident-based channels so responders can collaborate and solve incidents faster.

Slack also integrates with Zoom, Microsoft Teams and Webex so your team can quickly video chat and screen share if face-to-face conversations are needed.

For more focused real-time coordination, **huddles** is an audio-first communication channel that allows you to meet with team members within an incident channel to quickly discuss, triage, and take action.

Minimize interruptions and distractions for faster resolution

Communicating and working in Slack reduces interruptions and speeds up time to resolve incidents.

Team members can seamlessly enter and exit channels when they're needed. When a new team member enters a channel, there's no need to brief them, as they can quickly scroll through and catch up on exactly what's happened. Threads within channels cut down on information overload and reduce clutter for the larger group.

With Slack, it's possible to keep stakeholders out of live incident channels, while at the same time ensure they are still in the loop by creating a separate executive channel to provide higher-level updates.

Streamline incident reviews to prevent future incidents

Dedicated incident channels act as a timestamped audit log for completed incidents. There's no need for anyone to take notes while firefighting, since it's easy to quickly scan the channel and pull up everything that happened and how decisions were made.

Channels act as unbiased, objective sources of truth for post-incident reviews. Instead of forgetting who said what in a video call or watching a multi-hour recording, incident channels store all communications in a single place.

Even when incident channels are archived to preserve channel hygiene, anyone with access can continue to search for and share all types of rich content, including URLs, observability data and screenshots all in one place.

"Slack incident channels are often our most valuable sources of data during incident reviews. This data is critical to our Learning from Incidents approach, which requires accurate visibility to observations, actions, observability telemetry, hypotheses, and much more. All of this is indispensable in telling the non-biased story of the incident and sharing more actionable lessons learned."

David Leigh
Distinguished Engineer, Resilience Engineering IBM CIO

PagerDuty unites teams around data

When business-impacting issues strike, PagerDuty ensures you are never caught off guard. The platform collects data signals from all business systems, interprets those signals using machine learning, automatically creates incidents, and engages the right people to accelerate resolution and learning.

PagerDuty proactively manages your digital operations by enabling you to structure your services and teams to detect and resolve major incidents in real time. It also provides key information such as current service health, who's on call, incidents on each service, and more.

PagerDuty harnesses signals from your organization's digital data by integrating with your ecosystem (offering over 700 pre-built integrations and plug-ins), aggregating and transforming data into real-time insight and action. Machine-learning algorithms automatically reduce noise, create context and offer recommendations so you can focus on the events that matter.

PagerDuty engages the right teams of experts who can rapidly resolve critical issues and drives coordinated business responses with stakeholders in real time through proactive notifications and status dashboards.

PagerDuty leverages a unique combination of human and machine data, along with integrated automation, to enhance performance. This means you can automate routine response plays and runbooks to shift operations from ticket time to machine time.

It's important that the incident response team communicates and collaborates with the customer service team. Too often customer service teams can become isolated from other teams within a business, making it difficult to access the necessary information to provide the best customer service.
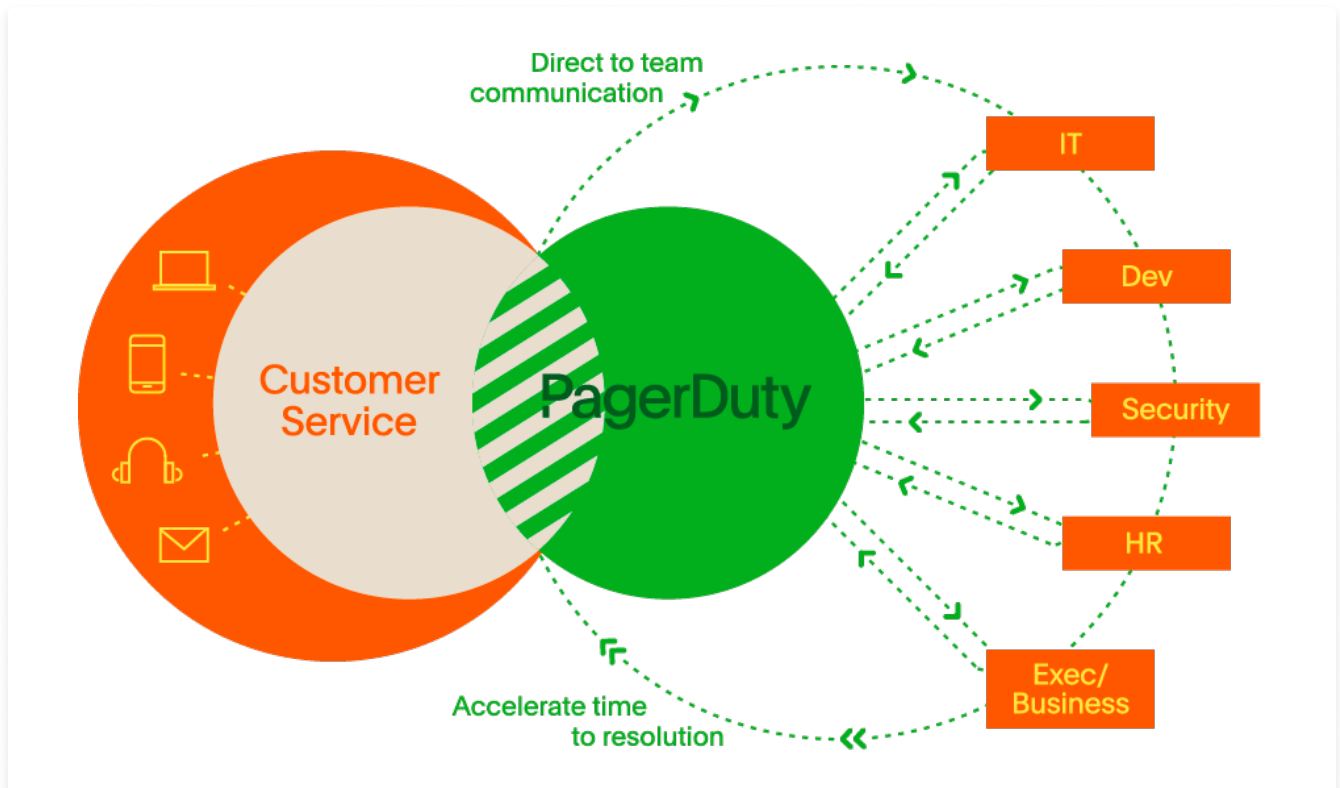
Incorporating tools like Slack and PagerDuty into the customer service team's process helps break down those barriers by providing them with the same information as developers and incident responders. By linking customer service cases to incidents in PagerDuty, the team can better understand the impact of an incident on customers. Additionally, using Slack and PagerDuty can allow for real-time communication and information sharing between teams, resulting in faster response times and more satisfied customers.

Slack and PagerDuty help you resolve incidents faster

PagerDuty's Slack integration is designed to continuously improve and expand the way Slack users work.

Ops and DevOps teams depend on an increasingly large number of tools each day. While each tool serves a purpose, toggling between apps to get the context or perform simple tasks can reduce agility and focus, especially when dealing with a complex incident.

64%
of workers report spending 30 minutes or more each day simply switching between apps. That half hour of lost productivity adds up to more than 130 hours annually.

Source: "The State of Work," Slack

The PagerDuty integration helps teams create, reassign, add responders, escalate, and gather more context about a PagerDuty incident—all from within Slack. There's no need to switch between apps; it's all in front of them. Incident responders can also deploy scriptable diagnostics and remediation with **Automated Actions** directly from Slack.

"The team also integrated PagerDuty with Slack, allowing responders to easily turn a Slack message into a PagerDuty incident with a slash command. If multiple services are impacted or responders from distributed teams are required to resolve an issue, the Slack integration makes it easy for the on-call engineer to create a conference bridge and pull in the right response team."

Manish Jain
Director of Engineering, BukuWarung

Let's walk through the lifecycle of an incident created, managed and solved exclusively within Slack using the PagerDuty Slack app:

As the central nervous system of an organization's digital operations, PagerDuty collects those incoming signals and alerts from various observability tools (e.g. Dynatrace, Datadog, New Relic), groups and correlates incidents and, when necessary, creates a new incident. PagerDuty assembles the incident responders, and the right subject-matter experts arm them with information such as related incidents and recent changes.

During collaboration, incident responders can quickly turn a Slack message into a PagerDuty incident with a Slack workflow or **trigger** a slash command and launch an **incident card** to create a new incident.

Incident responders can view who's on call and quickly **assign or add** the right response team and available responders directly from Slack.

1. Choose the service

2. Add the right responder to address an incident
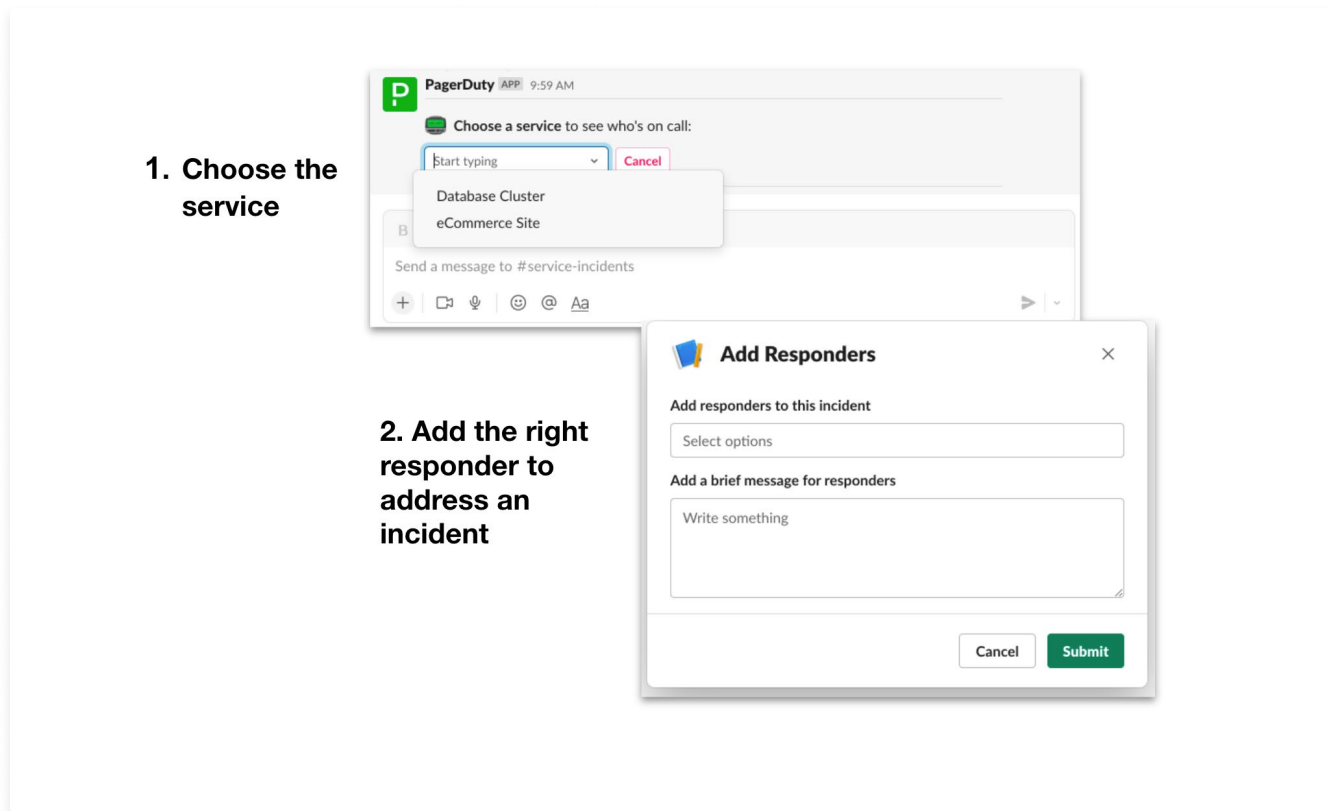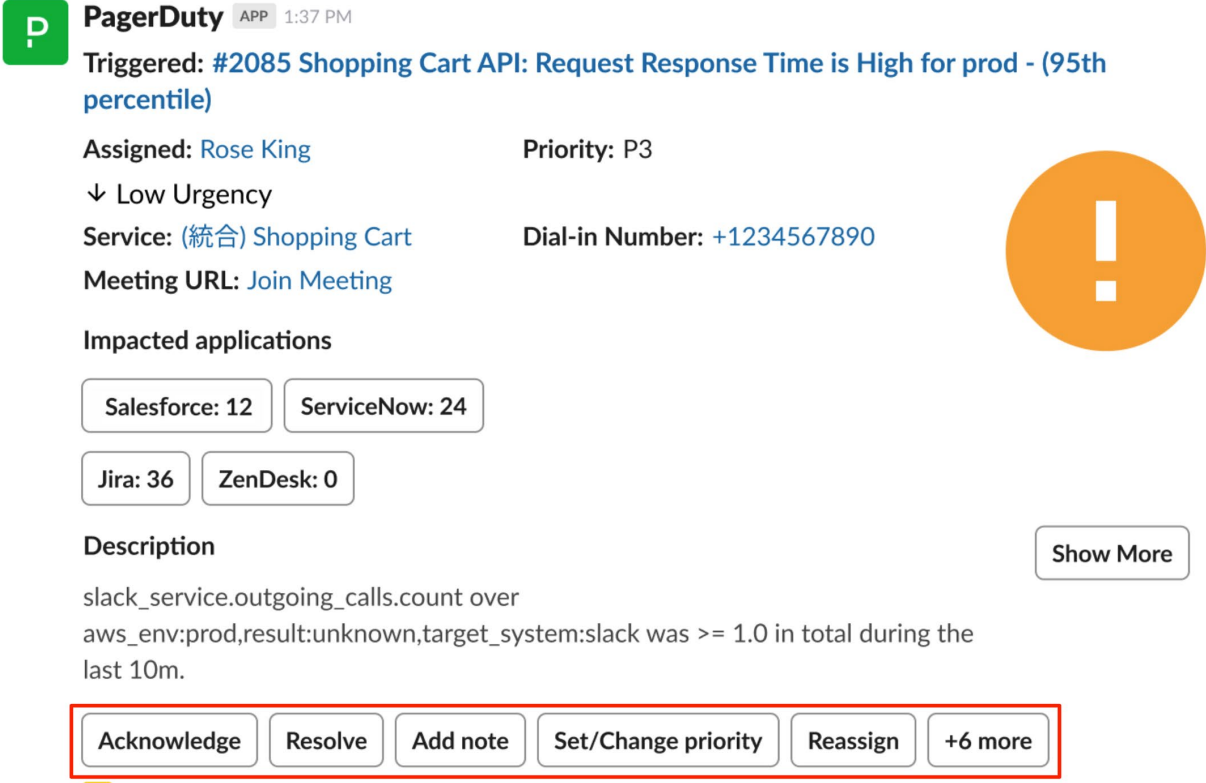
Incident responders can let teammates know they are on it by **acknowledging** the incident and stopping the escalation policy within the incident card.

They can view details and manage escalations, allowing them to understand everything about an incident and **reassign** or **escalate** when needed.

Once an incident is declared, a **dedicated incident channel** can be auto created and on-call responders are automatically invited to join. This process can be automated via PagerDuty's priority-based Incident Workflows or manually triggered via the incident notification card.

Incident responders can quickly collaborate, review and post internal stakeholder updates from the incident Slack notification card. At the same time, stakeholders can view incident updates and status from a **dedicated stakeholder channel**. This minimizes responder interruptions and increases business health visibility.

PagerDuty streamlines customer service by integrating with systems such as Salesforce Service Cloud, delivering real-time notifications and updates directly to customer service (CS) agents through the PagerDuty status page in their Service Cloud console. This ensures that CS agents are aware of any impacted services and can link incidents to cases via PagerDuty within Service Cloud incident management. PagerDuty's ability to update ticket status in ITSM/ticketing systems allows for a seamless flow from customer service to incident consolidation and back-end IT ticketing.

Rather than trying to figure out who to pull in for additional support and determining if there's actually a problem, incident responders can diagnose and remediate with **Automation Actions**, which allow them to invoke scriptable, **Automated Diagnostics** and remediation actions directly from Slack. By automating these investigative and debugging tasks, incident management teams can:

- Reduce escalations to scarce experts by designing paths to provide the first responders with information that would typically be manually gathered
- Distribute subject-matter expertise across response teams
- Invoke secure automation behind firewalls and VPCs
- Troubleshoot and resolve faster without a human-assisted action required
- Improve the speed of enablement to new engineers and ensure optimal efficiency at all levels of the incident response organization

Once resolved, responders can **close the incident**, add a closing note, and send a resolution note as a stakeholder update—all of this without leaving Slack.

Throughout the incident, PagerDuty posted valuable incident data, such as timestamped diagnostics, remediation actions taken, and major status updates. Conversations and threads in the channel help fill in the rest of the details. So the post-incident reviewer can now simply scan the incident channel to eliminate the guesswork of exactly what happened.

Finally, to prevent future issues, tickets and actions can be created and assigned directly from Slack by selecting specific messages or typing a simple slash command. This ensures that engineering and operations teams stay accountable and continuously reduce risk for the entire organization.

Get started with Slack and PagerDuty

Together, Slack and PagerDuty are your incident management dream team. Their integration provides responders with incident action and prompt resolution right where they work. By integrating PagerDuty's powerful real-time operations platform into Slack, your team can streamline incident remediation and keep customers happy.

Learn more about PagerDuty's integration with Slack and **get started here**.

About Slack

Slack is on a mission to make people's working lives simpler, more pleasant and more productive. It is the productivity platform for customer companies that improves performance by empowering everyone with no-code automation, making search and knowledge sharing seamless, and keeping teams connected and engaged as they move work forward together. As part of Salesforce, Slack is deeply integrated into the Salesforce Customer 360, supercharging productivity across sales, service and marketing teams. To learn more and get started with Slack for free, visit **slack.com** or connect with us **@SlackHQ.**

About PagerDuty

PagerDuty is a leader in digital operations management. In an always-on world, organizations of all sizes trust PagerDuty to help them deliver a better digital experience to their customers, every time. Teams use PagerDuty to identify issues and opportunities in real time and bring together the right people to fix problems faster and prevent them in the future. Notable customers include Cisco, DocuSign, Doordash, Electronic Arts, Genentech, Shopify, Zoom, and more. To learn more and try PagerDuty for free, visit **www.pagerduty.com**. Follow our **blog** and connect with us on **Twitter**, **LinkedIn**, **YouTube** and **Facebook**.