xmatters

Incident Management Software Buying Guide

Introduction

Ideally, IT incidents would never happen. The reality is that they do — and more frequently than any site reliability engineering (SRE) or DevOps team would like. In fact, **research indicates** some teams spend up to 80 percent of their time just addressing incidents instead of focusing on building and improving their systems and software.

Every technical manager or CTO must assume incidents will occur and plan accordingly. Just as effective monitoring is invaluable for tracking and evaluating your application stack's performance, a solid incident management tool is essential for tracking and evaluating your incident response.

Whether your applications run on-premises or in the cloud, downtime and other incidents are costly. Even subtle incidents, such as slow-loading forms and unreliable buttons, chip away at your bottom line. If customers can't use your service or your platform doesn't perform to their expectations, you risk upsetting and losing them. You may lose money from not meeting your customers' service level agreements or failing to deliver a great customer experience. Also, troubleshooting and mitigating failures or outages adds runtime and management costs.

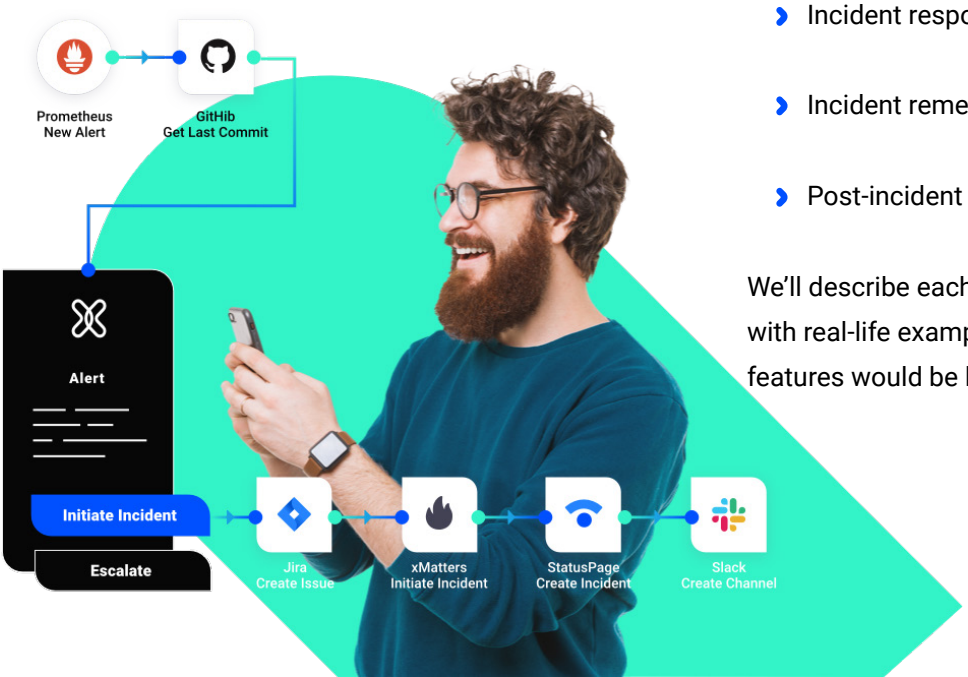
These days, technical teams move quickly, using a vast (and growing) toolbox to deliver reliable digital services. As teams enlist these tools to create a better customer experience, it becomes more challenging to track everything. They need another tool to help juggle it all.

Incident management software helps you recognize, respond to, and remediate incidents quickly, then analyze the incident to learn what went wrong and prevent future, similar incidents. You just need to decide which software is right for your team.

Throughout this guide, we'll explore what to look for when choosing an incident management solution, and we'll use xMatters to demonstrate the concepts we're discussing. While we think xMatters is great, we admit we're a bit biased. There is no one-size-fits-all incident management solution, and the ideal choice for your organization depends on your specific needs.

What to Look for in an Incident Management Tool

First and foremost, look for an incident management tool that helps you automate your workflows. When incidents occur, your solution should be able to automatically create tickets with relevant information from your monitoring platform, then notify relevant parties. And, of course, it should also help mitigate the incident, minimizing the effort and cost of restoring your system or application to a healthy state.



When your incident management tool captures information, you can further analyze and learn from the incident. This continuous learning helps you gradually improve your systems, prevent future incidents, and create a better customer experience.

You may be tempted to build homegrown incident management tools and processes since your internal operations and development teams know their platforms best. However, consider the extra time and cost to build and maintain such a platform. This takes time away from managing the production environment and preventing (or fixing) problems. These in-house solutions don't always scale well and often lack features that existing products provide out of the box.

With that in mind, let's explore key features of an effective incident management tool, based on the core phases of incident recovery:

- Incident recognition
- Incident response
- Incident remediation
- Post-incident analysis

We'll describe each phase in more detail, complemented with real-life examples of which incident management features would be helpful in that situation.

Incident Recognition

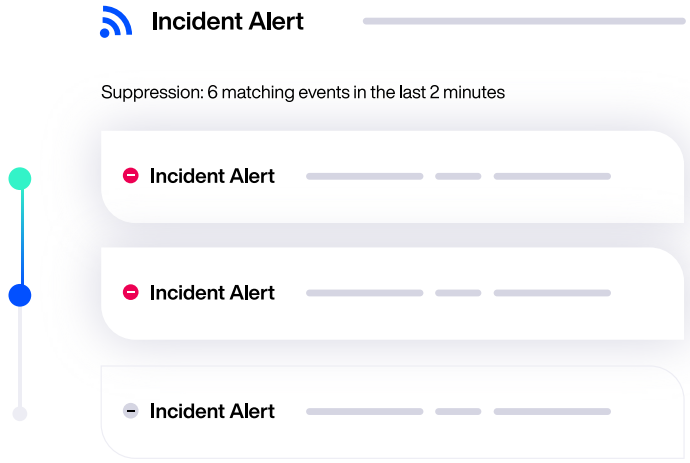
One way your monitoring systems cooperate with your incident management solution is by recognizing incidents as early as possible. When your technical teams don't have a clear view of what's happening with the application or system, they can't take any action to resolve the incident.

Monitoring alone isn't enough. While we wouldn't recommend running any environment without proper end-to-end monitoring in place, monitoring tools tend to capture everything, generating so much data that it's almost impossible to separate incident signals from monitoring noise. It can be a nightmare to find data in this information overload, causing teams to neglect the monitoring data.

Having said that, monitoring tools can provide your incident management platform with the data it needs to recognize that an incident is occurring. These monitoring tools include:

- Application performance management (APM) services like New Relic and Dynatrace that focus on monitoring applications deployed on-premises or in the cloud.
- Microservice and container monitoring solutions like Prometheus that store data in a time-series database.
- Log management services like Loggly or Logz.io typically store detailed diagnostic information.

While these monitoring tools are useful, they're also reactive. When things go sideways, monitoring tools may overwhelm your team with a flood of alerts. This makes it challenging to pick out the important messages that will help avert disaster.



Instead of waiting until a catastrophe is well underway, good incident management software should integrate with monitoring tools to detect incidents early and automatically. Look for an incident management platform that can receive data from a wide variety of monitoring and alerting tools simultaneously and use it to recognize incidents early. Effective incident management software uses signal intelligence to filter the signal from the noise, and delivers smart notifications with relevant information to the people who can take action.

To ensure the tooling you choose can ingest all application performance data, no matter the source, look for a tool with an extensive list of integrations.

Incident Response

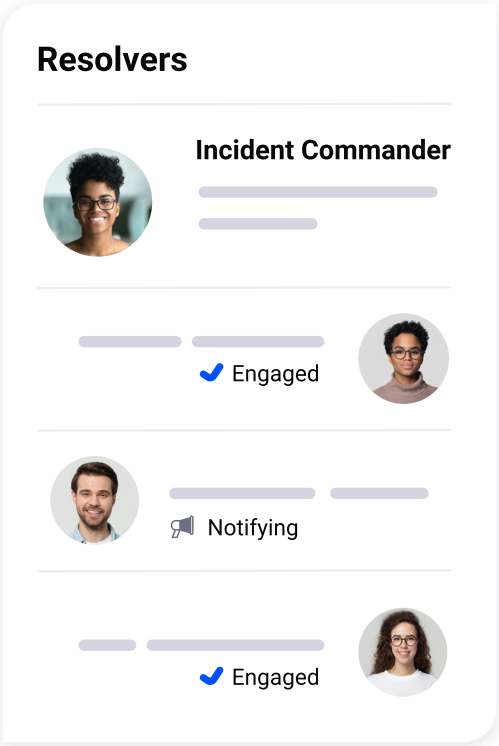
Once a tool recognizes an incident, someone or something must notify the correct people. But how should this happen, and what does it mean to notify the correct people? Effective **on-call management** is the key to quick incident response. Your incident management software should provide on-call management by automatically:

1. Handling scheduling, shift management, rotation, and incident escalation.
2. Quickly identifying who is responsible for incident response at any given day and time.
3. Adding and dismissing resolvers to bring in the right people as an incident progresses.

Once key responders are identified, your incident management software should engage them, either directly or by opening tickets via integrations with workflow automation tools such as ServiceNow or Jira. If the primary on-call responder is not available, a good incident management application should automatically escalate the notification to the secondary on-call responder, and so on, until it reaches someone who confirms they are ready to take action.

Some incident management platforms provide **workflow automation templates** to optimize incident response. For example, you might create a workflow to ensure that when the platform generates an automatic ticket, it also pulls up several key pieces of information, such as source system, impacted application, and key responder or responding team in the "assigned to" field.

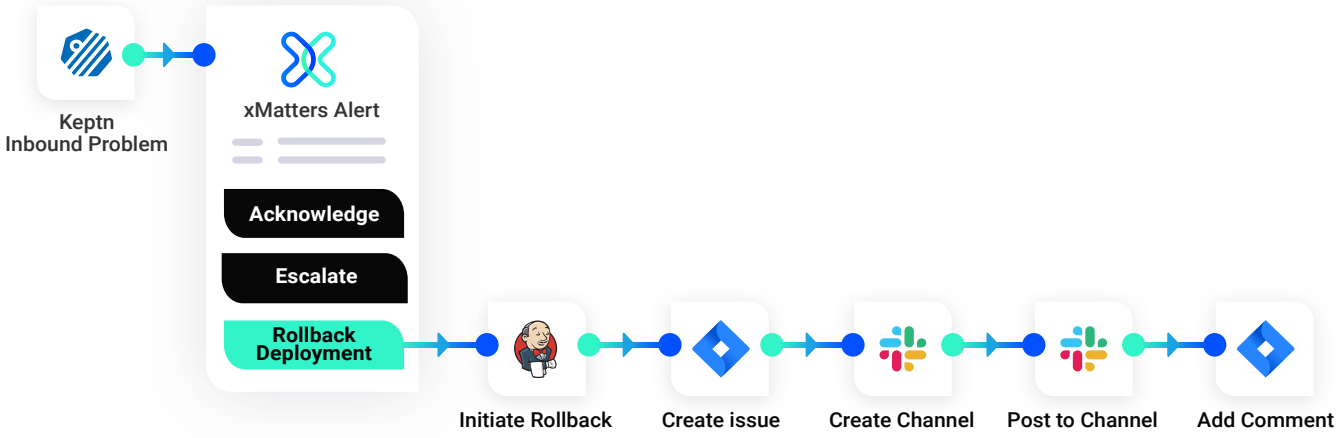
Above all, your incident response tool should be quick — it should begin engaging resolvers immediately after an incident is detected.



Incident Remediation

Notifying on-call responders and responsible teams is a good start, but it doesn't solve the problem. Good incident management software should distill and consolidate incident information into concise reports so responders can quickly determine what's wrong and decide on remediation steps.

Earlier, we discussed how a flood of monitoring data can slow down incident recognition. Too much information is even worse at the incident remediation stage. Before incident responders can resolve an incident, your teams need to know exactly why it's happening — and that's tough to do if they have to wade through dozens of pages of monitoring data, hundreds of alerts, and thousands of log entries.



Good incident management software should [cut through the noise and block redundant alerts] so teams can focus on fixing issues fast. What's better is taking it a step further by offering one-click mitigation options based on an automated workflow for the type of incident that's occurring.

Of course, automated workflows only help if your teams use them, so it's important that your software's workflow design and implementation tools are user-friendly. If they're a pain to use, they won't be used. If you're curious about what's possible, [xMatters code-free workflow builder Flow Designer] is the current gold standard in automated incident workflow design.

To illustrate all of this, let's look at an example. Imagine your continuous integration and continuous delivery (CI/CD) system builds and deploys on every commit, and now a commit and deploy cycle is causing an outage. Your incident management software should enable responders to trigger a rollback to the last successful commit, possibly by a single button click.

Using [xMatters], this workflow may look as follows:

- A third-party monitoring tool detects a problem and sends a signal to xMatters
- This triggers an alert in xMatters to identify the problem and opens a Jira ticket
- The incident response action kicks off and informs on-call responders, who acknowledge the problem
- Based on the problem's severity, xMatters offers responders the option of rolling back to the previously deployed version of the app with a single click of a button
- When a responder taps the button, xMatters triggers an Ansible task causing the CI/CD system to roll back to the previous version
- xMatters sends a resolution notification to a specific channel on Slack
- xMatters marks the incident as resolved

Post-Incident Analysis

An incident doesn't disappear as soon as it's resolved. Both management and engineers need to understand what went wrong, so good incident management software should help your team perform post-incident analysis and create detailed **post-incident reports** showing:

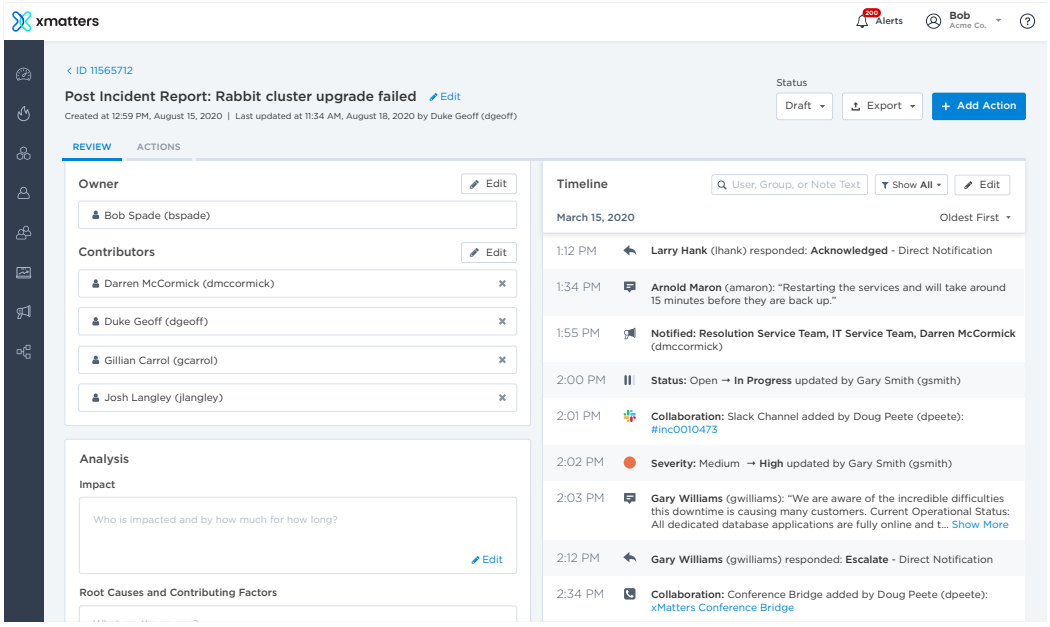
- When the incident was identified
- Who responded to it
- How quickly it was resolved

Alongside this key information, the post-incident report should also include detailed information from the incident itself or other incidents involved. This may include the resolution team or individual and the responsible owner. It should also clearly identify the incident's impact, the root cause with as much detail as possible (such as screenshots and log files), and the exact path to resolution.

Lessons learned can help technical teams understand the root cause and how to prevent the same issue in the future. This can be both technical and procedural. For example, your incident management software should let stakeholders make notes like "We need to provide more documentation on the system we are using" or "A handover training session from the Dev team to the Ops team can shorten time to resolution." Post-incident analysis may even indicate ways to improve the customer experience beyond simply fixing problems.

An incident timeline is an essential source of information during incident response. The incident management tool may represent this information as a summarized or extra-detailed field via a toggle in the incident report — but regardless of exactly how it's presented, it should be available. See the xMatters **Incident Timeline** for an example of what to look for.

Parties beyond the technical team may need to view the incident report. In addition to providing this report in the interface, the incident management tool should be able to export a PDF or Markdown email attachment.



xMatters Post-Incident Report allows users to share key information and understanding about why an incident occurred, how resolvers responded, and what preventive actions can be taken to ensure it doesn't happen again.

Scale, Compliance, and Internationalization

Although the overall incident management flow should be similar for any organization, your exact incident management needs likely vary depending on your company's size.

A small organization (or small technical team) might be fine with the base capabilities of a free, cloud-based software-as-a-service (SaaS) solution. Larger enterprises may have several different teams with different needs. Incident frequency and platform complexity may also drive the need for a scalable incident management solution, both in the number of users it supports and the number of incidents it can handle. There may be different license levels, ranging from free (basic features for a limited number of users) to enterprise (complete features with a per-user cost.)

Another aspect to consider is compliance. Certain compliance regulations may guide or force you to follow specific requirements. For instance, a finance organization must follow different privacy and security regulations than a manufacturing plant. Some organizations must seek ISO-certified solutions for security and risk management to meet their regulatory requirements. Even two organizations in the same industry may be bound by different compliance regulations based on their location, such as the European General Data Protection Regulation (**GDPR**) and American Federal Risk and Authorization Management Program (**FedRamp**).

IT departments may be in different locations around the world, with different languages and cultures. Global enterprises need a reliable, globally available platform to ensure all locations get the notifications and information they need to quickly and effectively manage incidents as a team.

You may need a language other than English, or multiple languages, for incident management reporting. A language barrier between teams can slow response and mitigation time, with misconceptions and confusion about resolutions presented in the incident reports. An incident management tool that supports multiple languages and takes time zone differences into account may be necessary for international teams.

Wrapping up

Choosing an incident management software can be daunting, with so many options available. In this buyer's guide, we looked at the key factors to consider when choosing incident management software, such as automation, separating signal from noise, notifying the right people, providing actionable remediation steps, and helping analyze postmortem reports.

Your team may have specific needs, such as scalability, compliance, global coverage, and support for different time zones and languages. Choose not just the best incident response tool in the market but the best incident response tool for you. Hopefully, this guide helps you think about critical factors to consider when looking at all the available tools.

Consider **scheduling an xMatters demo** to learn more about our adaptive approach to incident management. Our xPerts can show you the software in action and answer your questions, helping you decide if xMatters is the right incident management tool for you.

xmatters.com

Copyright 2021 xMatters. All rights reserved. All other products and brand names are trademarks or registered trademarks of their respective holders.