ATLASSIAN

The state of incident management report

2023

Table of contents

Executive summary

Atlassian's first incident benchmark report was conducted in 2020; the findings of the report don't exist in a "tech vacuum" and reflect the trends and challenges that the world was facing as a whole. Prior reports were heavily influenced by the global Covid-19 Pandemic start and peak. This year's results are influenced by the aftermath of the pandemic–during a time when return-to-work initiatives are prevalent, people are tired of being on video chat, and employees are reporting high rates of burnout[1].

While much of the economy was in tumult due to the effects of Covid-19, tech seemed to boom. Whereas, today macroeconomic headwinds have turned the tides[2]. Big tech and start-ups alike are affected by slowed, industry-wide-growth, and even companies like Amazon, Meta, and Google have seen workforce reductions as a result.

Despite economic and workforce challenges, this year's report showed that in 2023, organizations are looking toward automation and Artificial Intelligence (AI) to pick up the slack. The pandemic showed us that time is precious, and many of us want to spend less of it doing what a computer can do for us. Although digital assistants like Alexa, Siri, and Google Assistant have been part of our lives for years, controlling our lights and deejaying our mornings, tools like ChatGPT have made AI feel more tangible for lightening our load at work.

1 Morgan Smith, "Burnout is on the rise worldwide–and Gen Z, young millennials and women are the most stressed," CNBC Make It, Published Tue, Mar 14 2023, Updated Tue, Mar 14 2023, https://www.cnbc.com/2023/03/14/burnout-is-on-the-rise-gen-z-millennials-and-women-are-the-most-stressed.html

Bryan Robinson, "New Outlook On Burnout For 2023: Limitations On What Managers Can Do," Forbes, Feb 7, 2023, https://www.forbes.com/sites/bryanrobinson/2023/02/07/new-outlook-on-burnout-for-2023-limitations-on-what-managers-can-do/?sh=4ba9aea54343

2 Alyssa Stringer, "A comprehensive list of 2023 tech layoffs," Techcrunch, June 28, 2023, https://techcrunch.com/2023/06/28/tech-industry-layoffs-2023/

In addition to a willingness to invest in AI, expect to be able to benchmark your own practices with findings like:

- A general observation of what other organizations' incident management processes look like
- Focus on common pain points
- Discussion around automation
- Future plans and investments in AI

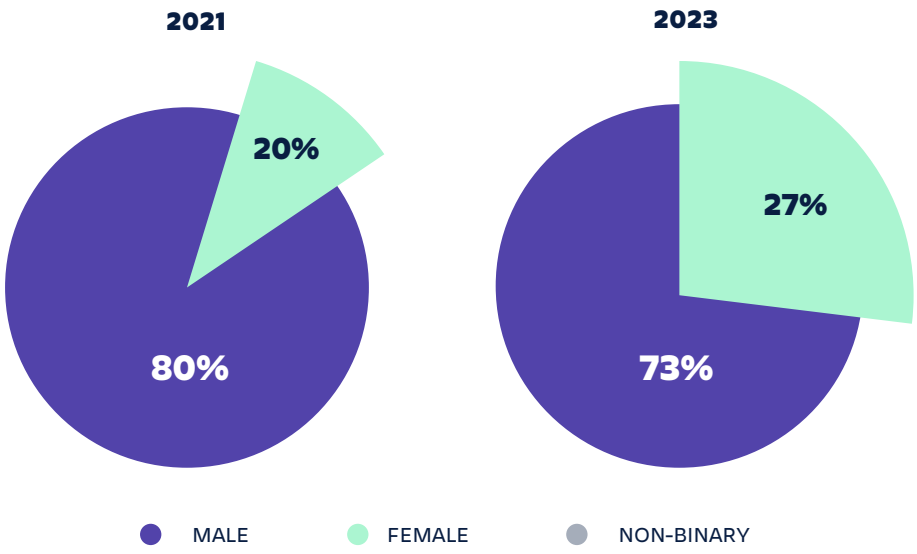
Now that we have a few years of data, we will also provide a year-over-year comparison to surface key changes in investment focus and processes.

Survey methodology and demographics

Who took the survey?

Atlassian's 2023 State of Incident Management research study surveyed over 500 software developers, IT professionals, and IT decision makers (ITDMs) across the US about IT Service Management (ITSM), with a focus on the practice of incident management. This is the third installment; previous surveys were conducted in 2020 and 2021 respectively. All were fielded by CITE Research, on behalf of Atlassian. In 2023, we required that respondents be:

- Employed full time
- In either a software development or IT role
- Working at an organization that practices DevOps
- At manager level or above
- Working at a company of 101+ employees or more

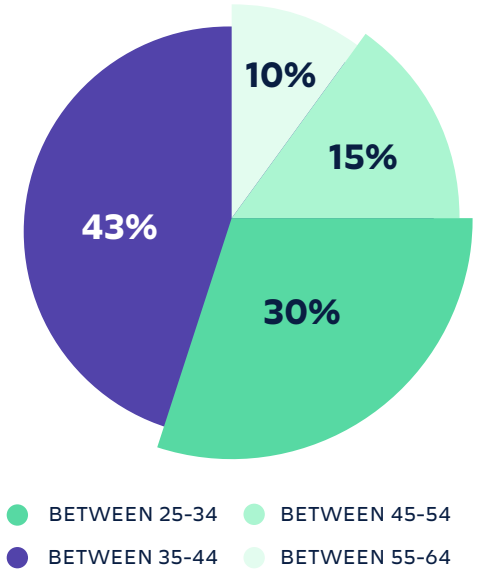


Gender

Only 27% of respondents identified as women, whereas 73% identified as men, which illustrates the gender disparity among IT and Dev professionals. An encouraging trend has emerged that shows the gender disparity is steadily decreasing, with a 4% increase year over year of women respondents. This trend was first identified in 2021, and while we don't have data for 2022, in 2023, there is a marked increase of 7% for female respondents, which may indicate the disparity is continuing to slowly decrease.

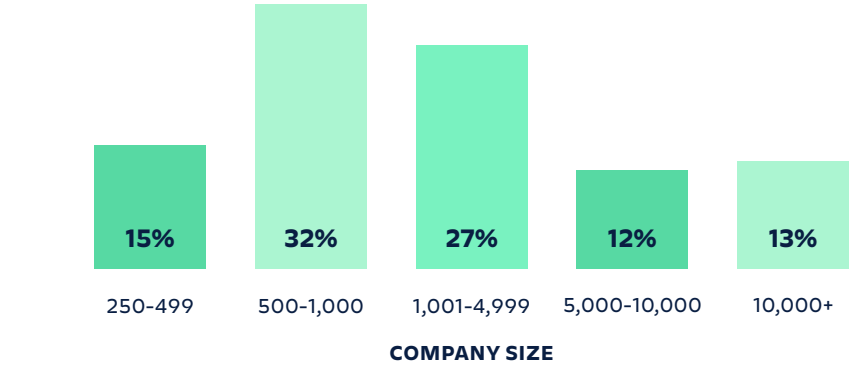
Age

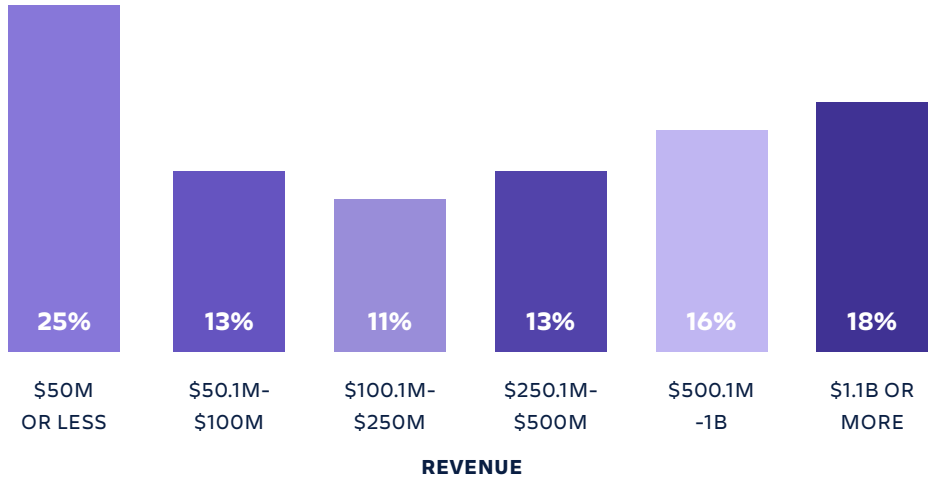
Similar to 2021, the majority of the respondents fell within the 35-44 age range, dissimilar to 2021, this year, folks were more distributed across age ranges, with 30% in the 25-34 range, 15% in the 45-54 range, and 10% in the 55-64 range.



Company size & revenue

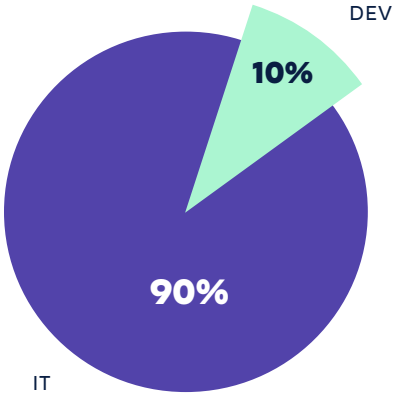
The majority of respondents worked at small- to medium-sized companies, with 25% working at larger enterprises.

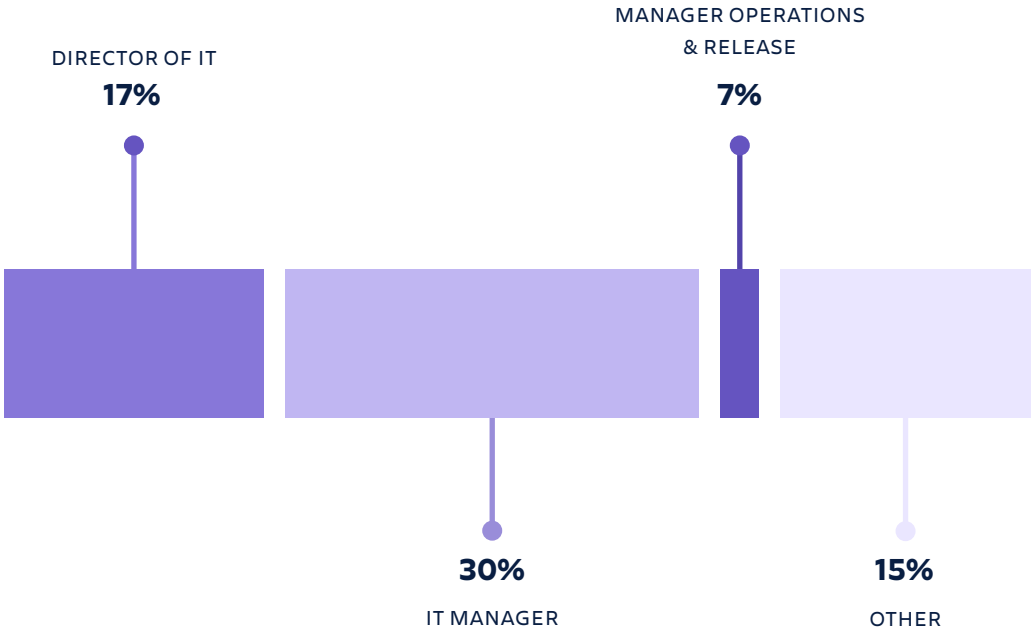




Title and department

In 2021 respondents were split evenly across Dev and IT, 50% each. This year in 2023, 10% of respondents were Dev, and 90% were IT. This is almost the opposite of 2020's results, where 78% were Dev, and 22% were IT. For context, this change was not intentional as respondents are chosen at random, and only move forward in the survey if they work in either Dev or IT.



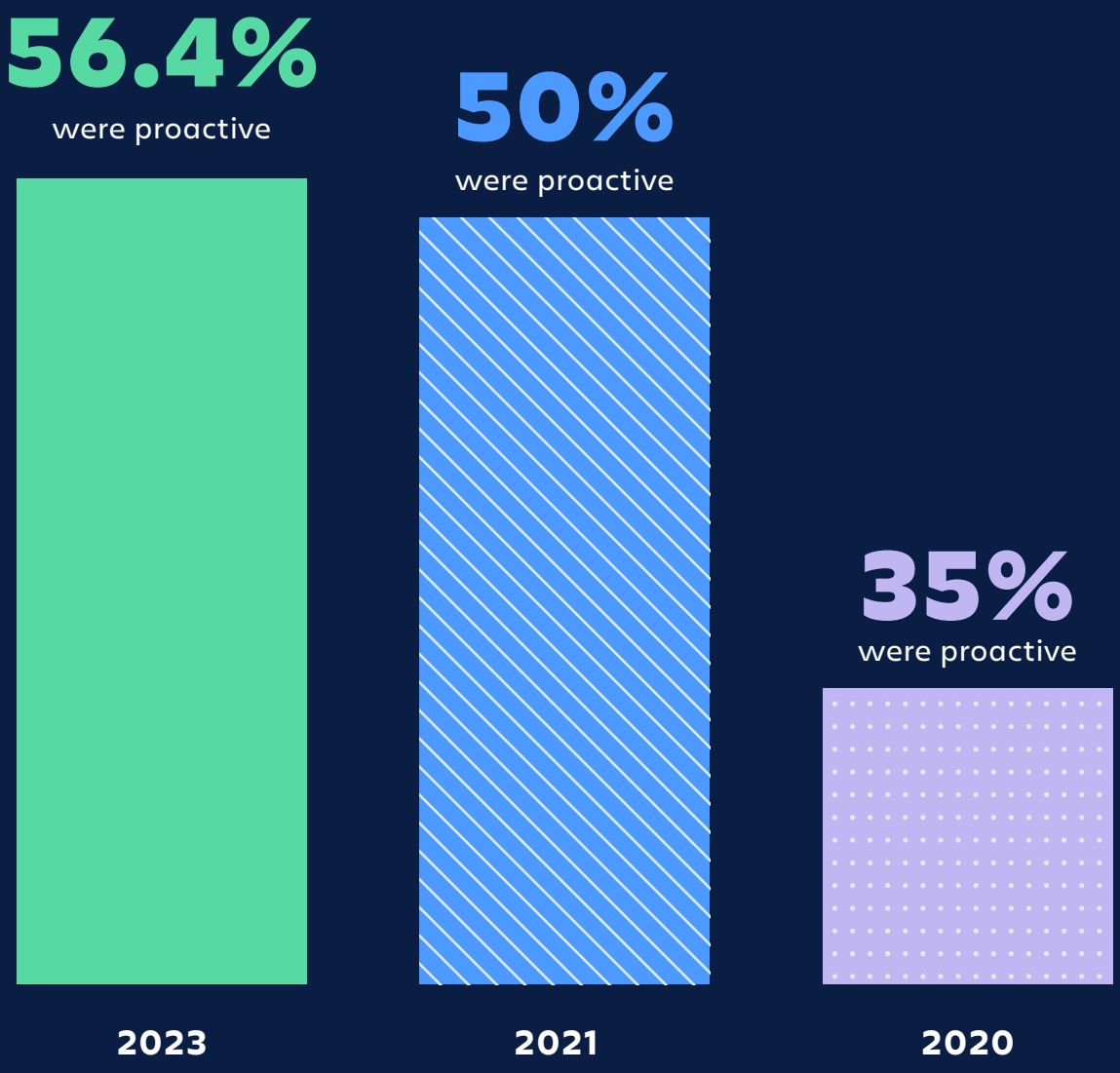


01

Perception vs. reality

The maturity of the incident management process

To define an organization as proactive, we concluded that the use of monitoring, alerting, and communication tools were required, as well as incident response training. In 2023, we expanded the definition to include the use of AI for incident trending, as well as integrated visibility into recent changes.



02

Tools and processes

Frameworks

In prior surveys, we've asked folks to rate how much frameworks like DevOps, Agile, ITIL 4, and Lean influenced their organizations and teams. This year we rephrased the question around frameworks in order to get a better understanding of how people were implementing the various frameworks, and instead asked respondents to describe which frameworks they were using and how.

Similar to previous years, only respondents who practiced DevOps were able to move forward in the survey. Despite the fact that the majority of respondents were in IT, DevOps still took the lead in the most influential framework, as it was mentioned over 270 times in the open text box answers, more than any other framework specified.

Below, see word clouds based on respondents' answers. The larger the word, the more often it was mentioned.

Word cloud from responses to:

Briefly describe in your own words what DevOps is/ how your organization is practicing DevOps.

Word cloud from responses to:

Briefly describe to what extent your organization is influenced by different industry frameworks. For example: ITIL 4, Agile, Lean, DevOps, etc.

EXCERPTS FROM RESPONDENTS' ANSWERS

AGILE

"Agile–we practice agile mostly in teams where we are building new products and scaling them quickly. We practice Lean where we are testing out very new ideas to solve ongoing problems and need feedback as quickly as possible."

DEVOPS

"DevOps is all about the unification and automation of processes, and DevOps engineers are instrumental in combining code, application maintenance, and application management."

ALL FRAMEWORKS

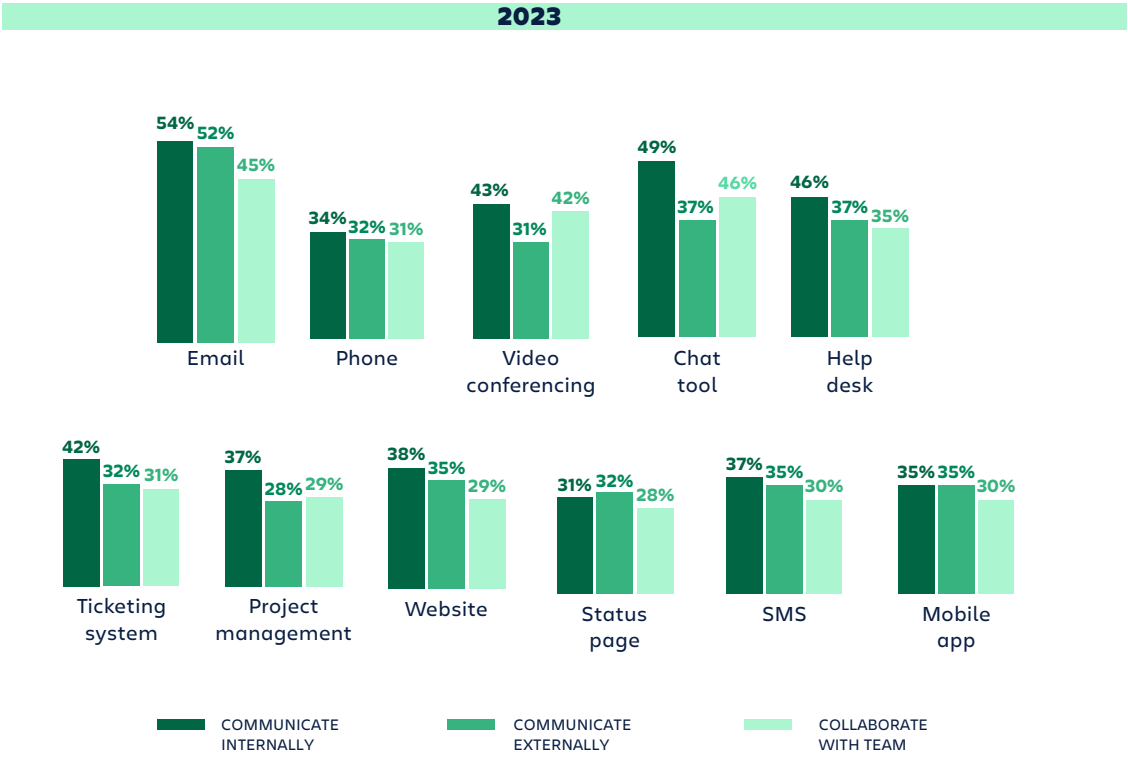
"We are heavily influenced by certain industry frameworks which allowed us to have a foundation to build our systems. These frameworks, particularly Agile, allowed for flexibility that was crucial to our success."

"We utilize these frameworks to acclimate concepts regarding cost, value, and business risk."

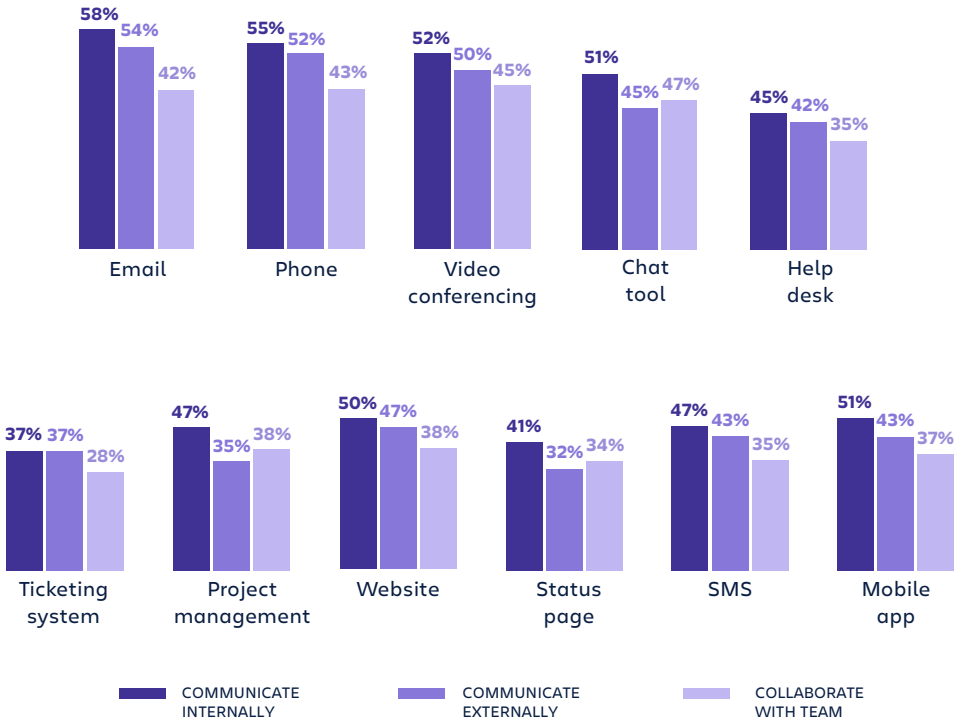
Communication and collaboration

Communication methods appear to be affected by “return-to-work” measures and possibly “video-chat fatigue”–we saw a drop in how many respondents leverage video conferencing for collaboration and internal communication during an incident. Whereas, email remains a key tool for both internal and external communication as well as team collaboration.

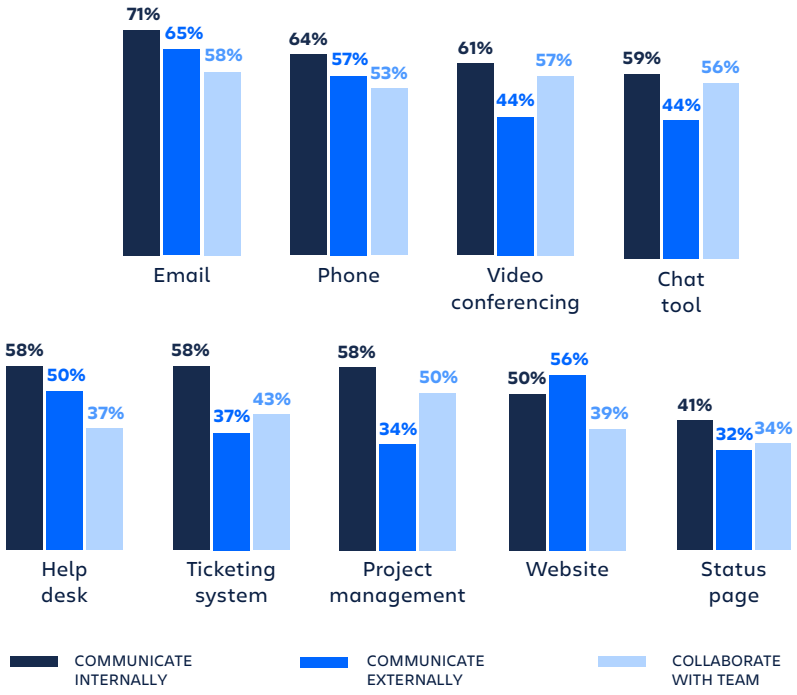
Chat is slightly more favored than email for collaboration, likely due to the immediate nature of messaging. Although consistent with earlier waves, it’s interesting to note that usage of status pages for external communication remains around 30%. Unsurprisingly, phone usage continues to decline, but we will have to wait to see if this trend continues in 2024.



2021


58%
54%
42%
Email
55%
52%
43%
Phone
52%
50%
45%
Video conferencing
51%
45%
47%
Chat tool
45%
42%
35%
Help desk
37%
37%
28%
Ticketing system
47%
35%
38%
Project management
50%
47%
38%
Website
41%
32%
34%
Status page
47%
43%
35%
SMS
51%
43%
37%
Mobile app
COMMUNICATE INTERNALLY
COMMUNICATE EXTERNALLY
COLLABORATE WITH TEAM

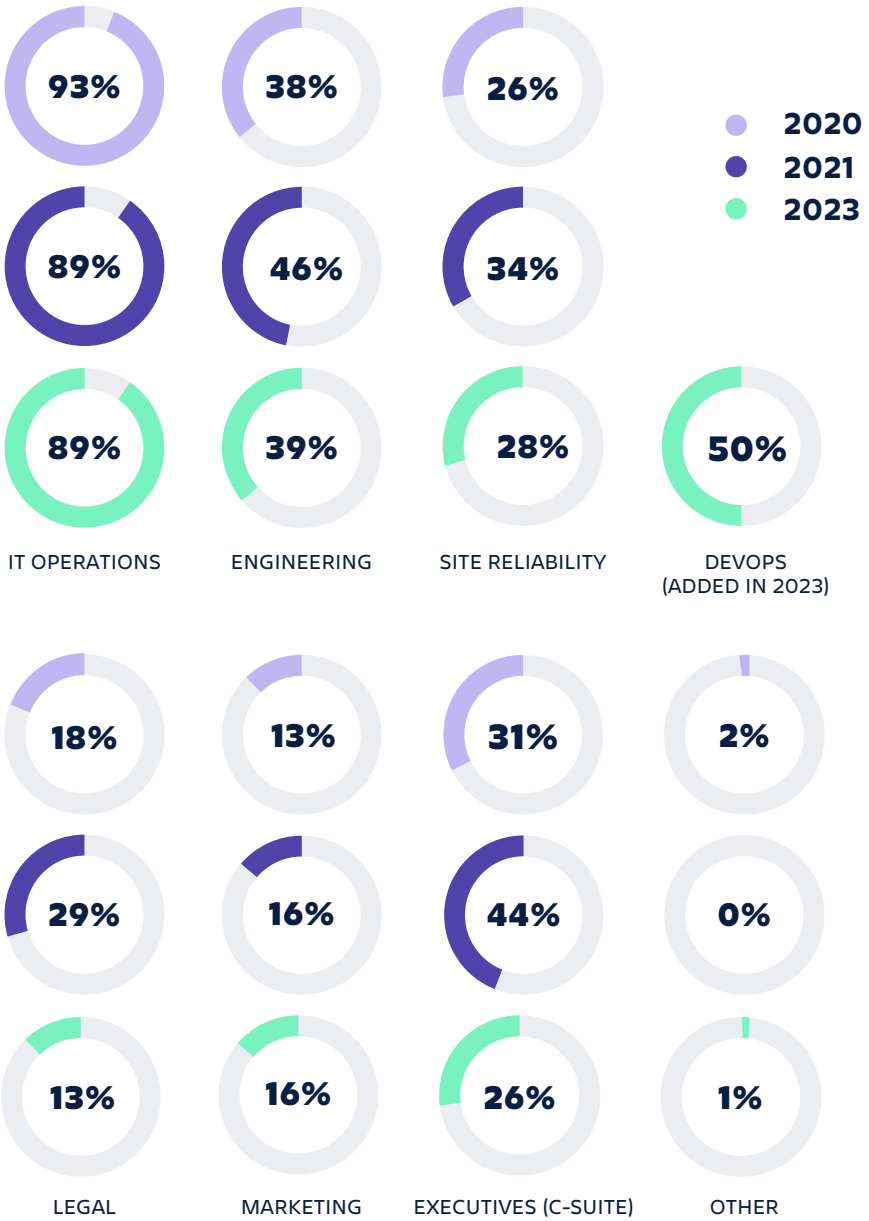
2020


71%
65%
58%
Email
64%
57%
53%
Phone
61%
44%
57%
Video conferencing
59%
44%
56%
Chat tool
58%
50%
37%
Help desk
58%
37%
43%
Ticketing system
58%
34%
50%
Project management
50%
56%
39%
Website
41%
32%
34%
Status page
COMMUNICATE INTERNALLY
COMMUNICATE EXTERNALLY
COLLABORATE WITH TEAM

Who manages incidents?

Consistent with prior years' surveys, IT Operations are still the most heavily involved in incident management. However, it looks like other groups may be stepping back from the incident management process as compared to previous years. Decreases of more than 10% were seen among legal and the C-Suite; we'll have to see if the lack of functional involvement is a trend or a one-off.

One possibility for this decrease is that at peak pandemic, outages received more press. This could explain the increased focus and inclusion of legal, marketing, and C-Suite teams in incident management.



Who goes on call?

Although the majority of respondents identified as being in IT, our results are still on-par with prior years. Ninety-one percent of respondents reported that IT goes on call, as compared to 87% in 2021. At the same time, 49% of respondents reported that developers went on call too, a 14% decrease since 2021. It's key to note that this decrease could simply be due to the fact that in 2023, 91% of respondents were IT, compared to a 50/50 split of IT and Dev respectively, in 2021. Only 1% of those surveyed reported that they don't have an on-call process, results consistent with prior surveys.

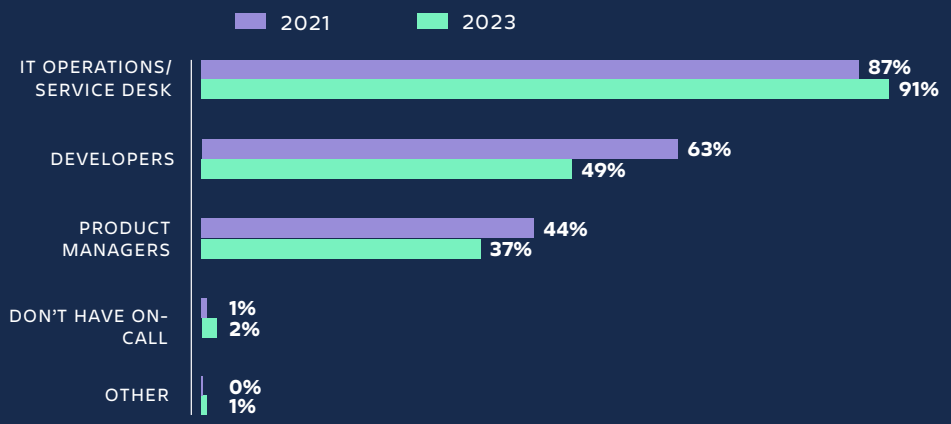
91% IT OPERATIONS/ SERVICE DESK

49% DEVELOPERS

37% PRODUCT MANAGERS

2% DON'T HAVE ON-CALL

1% OTHER



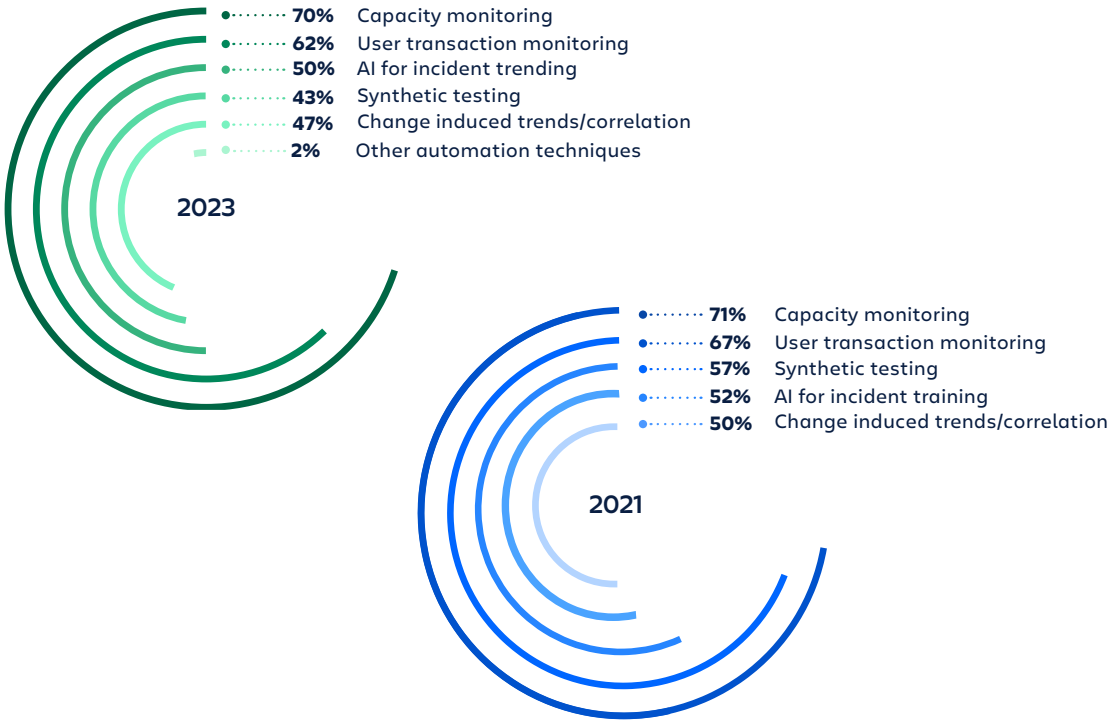
Incident prevention

A strong majority of organizations use procedures, processes, or runbooks for managing incidents (95%). Three in four are using war games or incident management training as well. Those in IT are more likely to report the usage of both of these techniques compared to software developers. Those who have no plans to leverage AI in the future are least likely to engage with these techniques (82% and 36% do so, respectively).

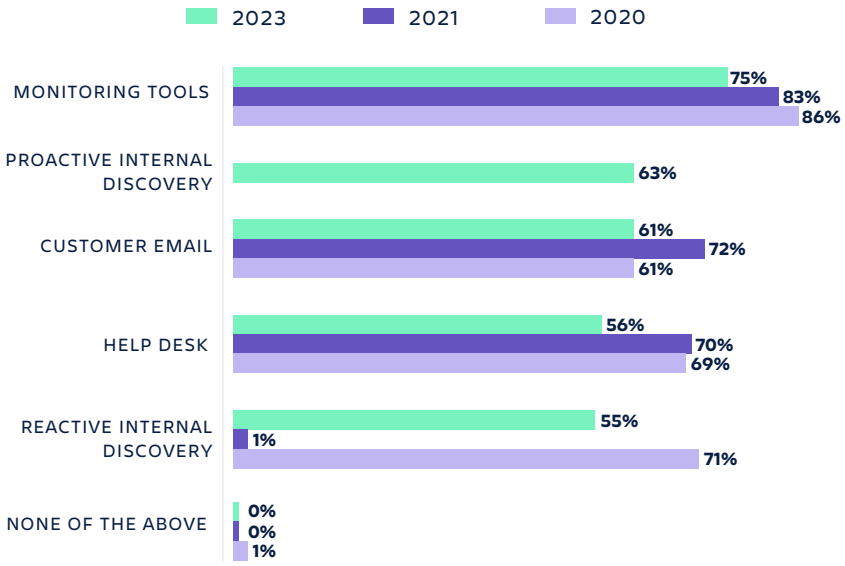
Most are implementing chaos engineering, most commonly through simulating high increases in traffic and simulating failures. On average, respondents use 2.5 of these techniques. While injecting failures of services and causing host failure are less commonplace, four in ten organizations are using these.

Ninety-nine percent of respondents were using some sort of tool (whether proactive or reactive) to discover incidents. Monitoring tools continue to be the most commonplace, with three in four ITDMs saying they currently use them.

USE OF PROACTIVE INCIDENT TECHNIQUES/TOOLS



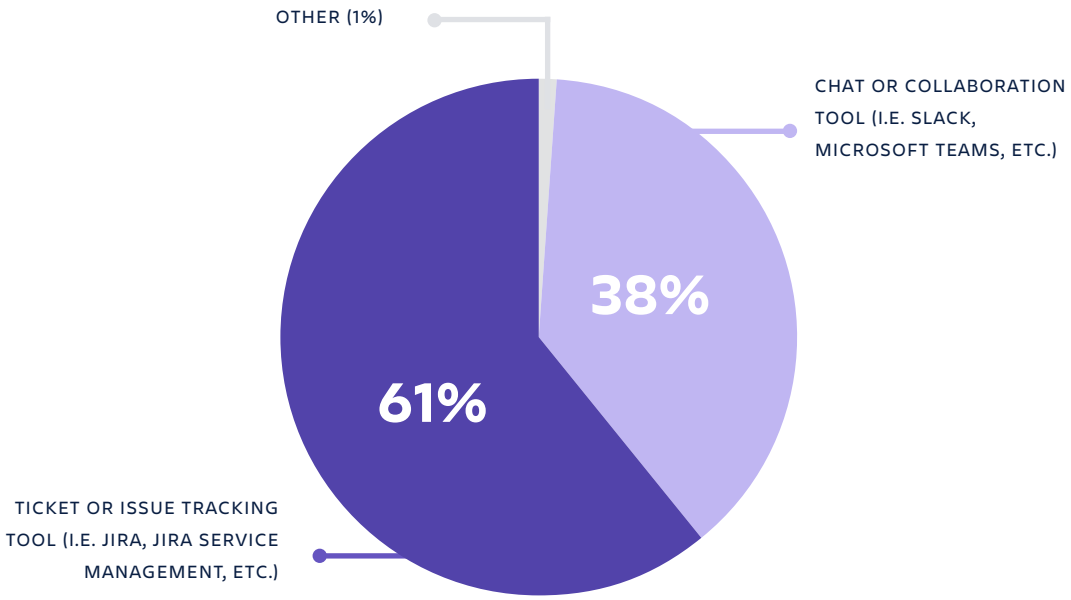
Looking at how incidents are discovered across all methods, it would appear that the trend favoring proactivity is continuing. Monitoring tools are still the most widely used, with internal discovery (proactive) a fast follow at 63%. Customer reported/email discovery remains popular as well.



*Note: We adjusted this question in 2023 to differentiate between proactive internal discovery and reactive internal discovery.

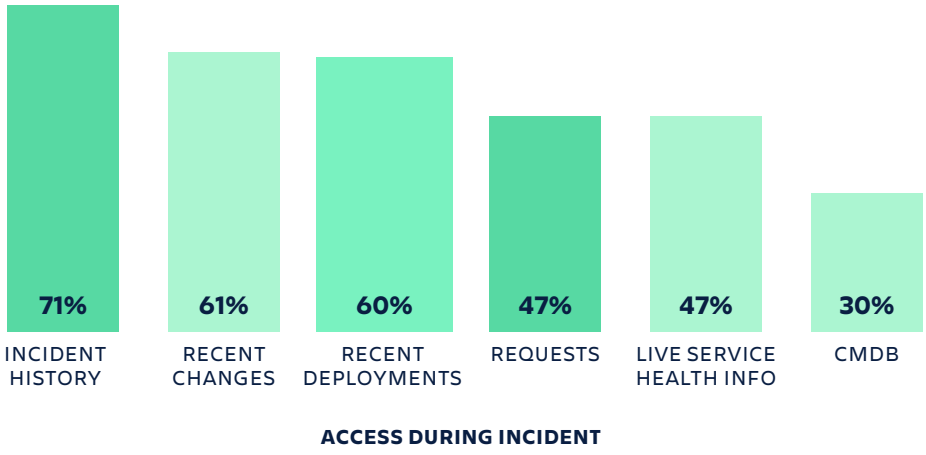
Source of truth during incidents

In 2023, we saw the trend of chat tools being favored as the source of truth during an incident continue. This is a possible indication that ChatOps for issue tracking is still a popular practice among respondents. Approximately a two-thirds majority still say that ticket or issue tracking tools are the source of truth during incidents. This finding is similar to 2021.



Visibility during an incident

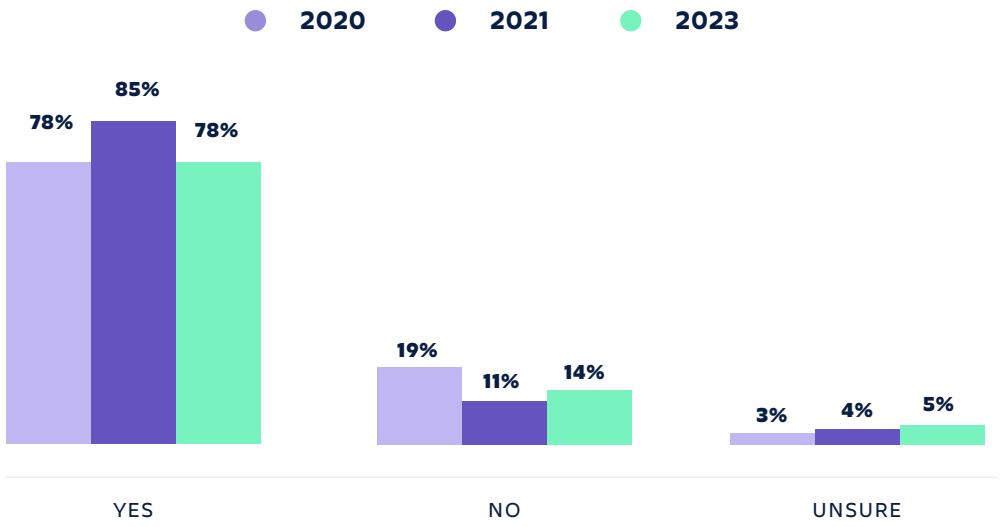
Most organizations access incident history, recent changes, and recent deployments when investigating an incident. Less than half access requests, live service health information, and/or an asset management tool or CMDB. Organizations that are already using AI tools like ChatGPT are more likely to access their CMBD (58%).



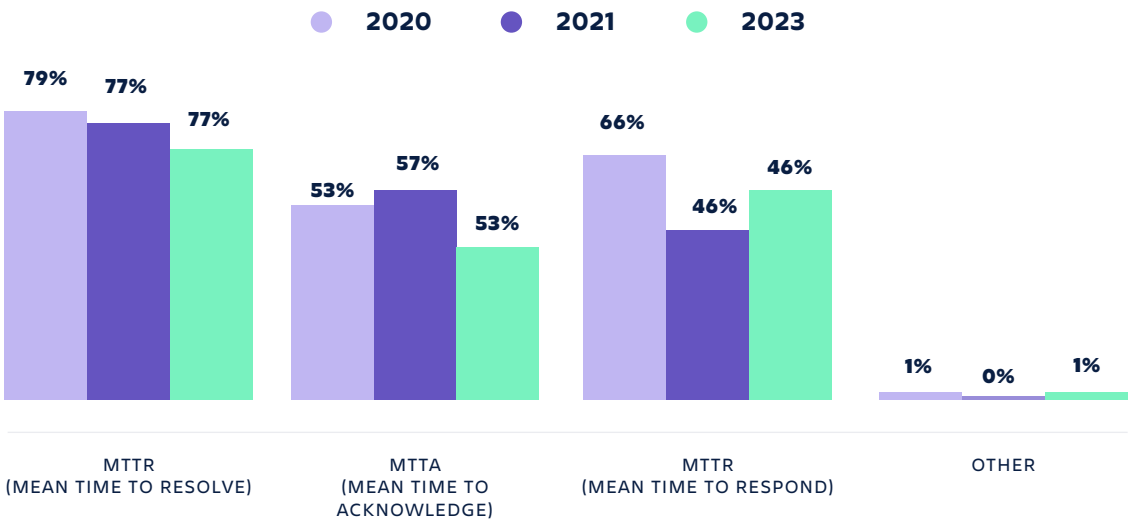
Additionally, 98% of respondents practice change management, with most preferring to refer to it as change enablement. Only one-quarter of ITDMs cited using change advisory board meetings, likely due to most preferring the more agile approach of change enablement.

Measuring success after the incident

Similar to previous findings, most respondents run postmortems or post-incident reviews (PIRs). Those not using AI to trigger incidents are less likely to do postmortems or PIRs (68% do, 22% do not).



Mean time to resolve (MTTR) continues to be the top key performance indicator during incident response. There was a noticeable increase in attention paid to mean time to respond as compared to 2021. We asked respondents to provide an estimate for how much an incident costs their organization. Of those surveyed, 19% didn't measure the cost of incidents, and 39% were unsure what incidents cost them. Among those who did measure cost, incidents were estimated to cost $13,000+ on average. It's important to note that industry size and vertical are important factors that determine the cost of an incident.

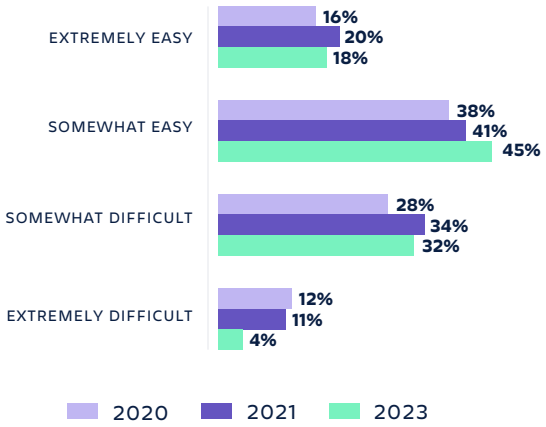


03

Areas for improvement

Main pain points

Similar to previous surveys, most respondents found it easy to get stakeholders involved (63%), whereas 36% found it difficult. Notably, those not using AI to trigger incidents (45%), find it significantly more difficult to get stakeholders involved than those who do.



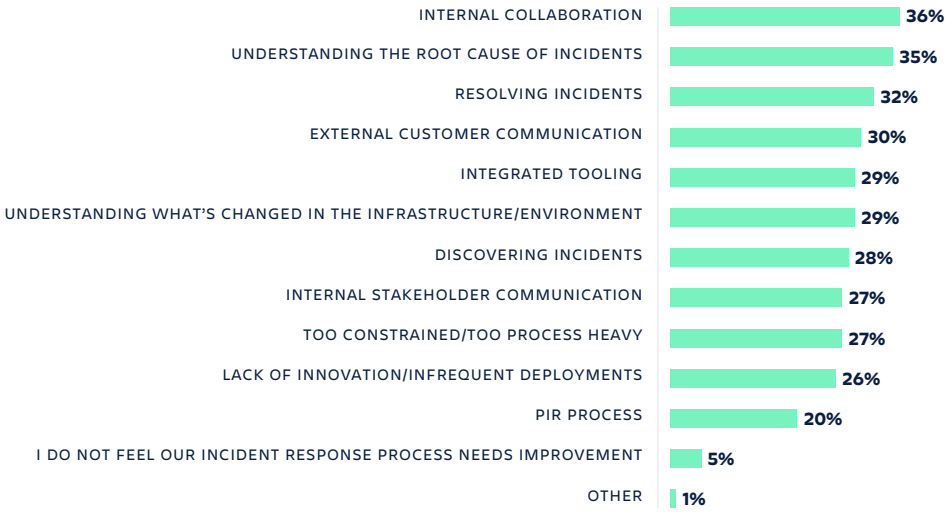
The most significant pain point in the incident management process continues to be a lack of full visibility across IT infrastructure. However, since 2021, lack of coordination has been on the rise, with 20% citing this as a pain point in 2023, as opposed to 11% in 2021. Those in software development are more likely to feel that lack of context is a top pain point (22%). Many respondents do have plans to invest in tooling like CMDBs, Wikis, and others that should help alleviate this pain point.

BIGGEST PAIN POINT IN INCIDENT MANAGEMENT

Lack of full visibility across IT infrastructure	23%
Lack of coordination across departments	20%
Lack of context during an incident	13%
Ill-defined processes	9%
Lack of change management /change records	9%
Lack of plans to address incidents	9%
Lack of automated responses	9%
Lack of integration with a chat tool (Slack, Microsoft Teams)	8%
Other (please specify)	1%

The top areas that ITDMs feel need immediate improvement include internal collaboration and understanding the root cause of incidents. The latter is especially an area of concern among software developers (50%). Only 5% of respondents did not feel that their incident management process needed improvement. A possible reason for this could be that communication is now more distributed amongst various tools, versus in 2021, when video conferencing was the dominant channel.

AREAS NEEDING IMMEDIATE IMPROVEMENT



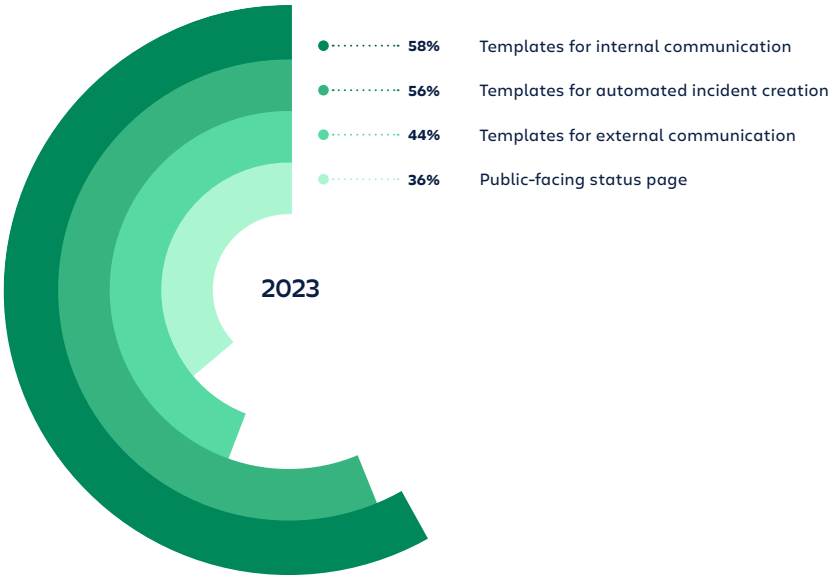
Six-in-ten organizations (58%) hold developers accountable for deployments that cause incidents, while 25% cite practicing blameless postmortems as the reason they don't. Ninety-four percent agree that Dev and Ops teams have full visibility into what they need to do their jobs effectively while minimizing disruption. Segments who are significantly more likely to agree include those currently using AI tools like ChatGPT, those who use AI to trigger incidents, and those who hold developers accountable for incidents.

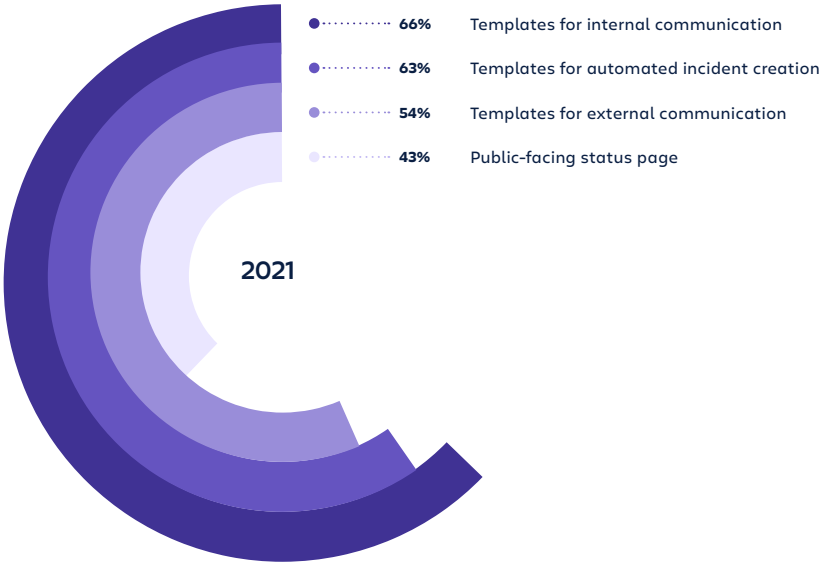
04

The role of automation, AI, and ChatGPT

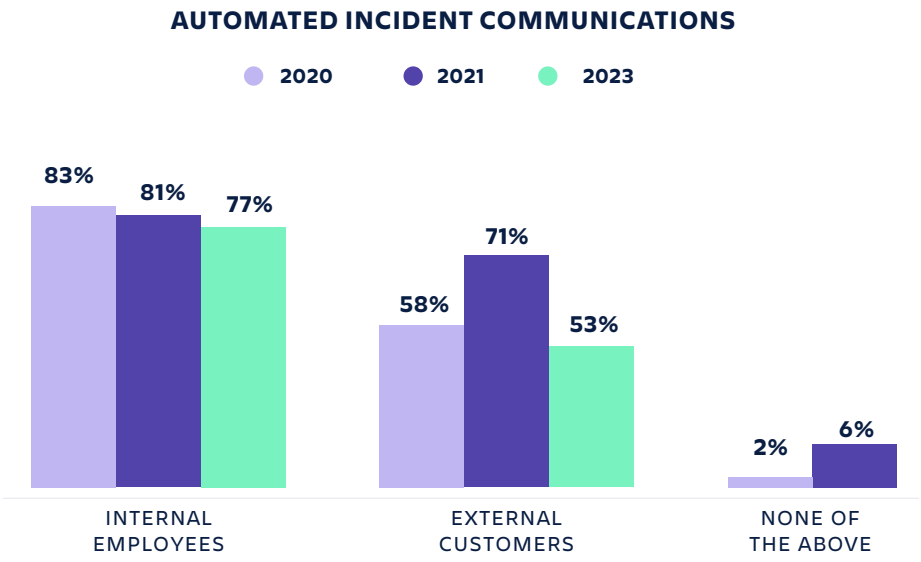
Automation

Automation remains a priority in the incident management process. Eight-in-ten organizations are automating incident communications with their internal employees. There does appear to be a drop in automation of communications to external customers in 2023, with results more in line with levels we saw in 2020. Around 77% of internal communications with employees are automated, whereas external communication comes in around 53%, with both percentages decreasing since 2021.

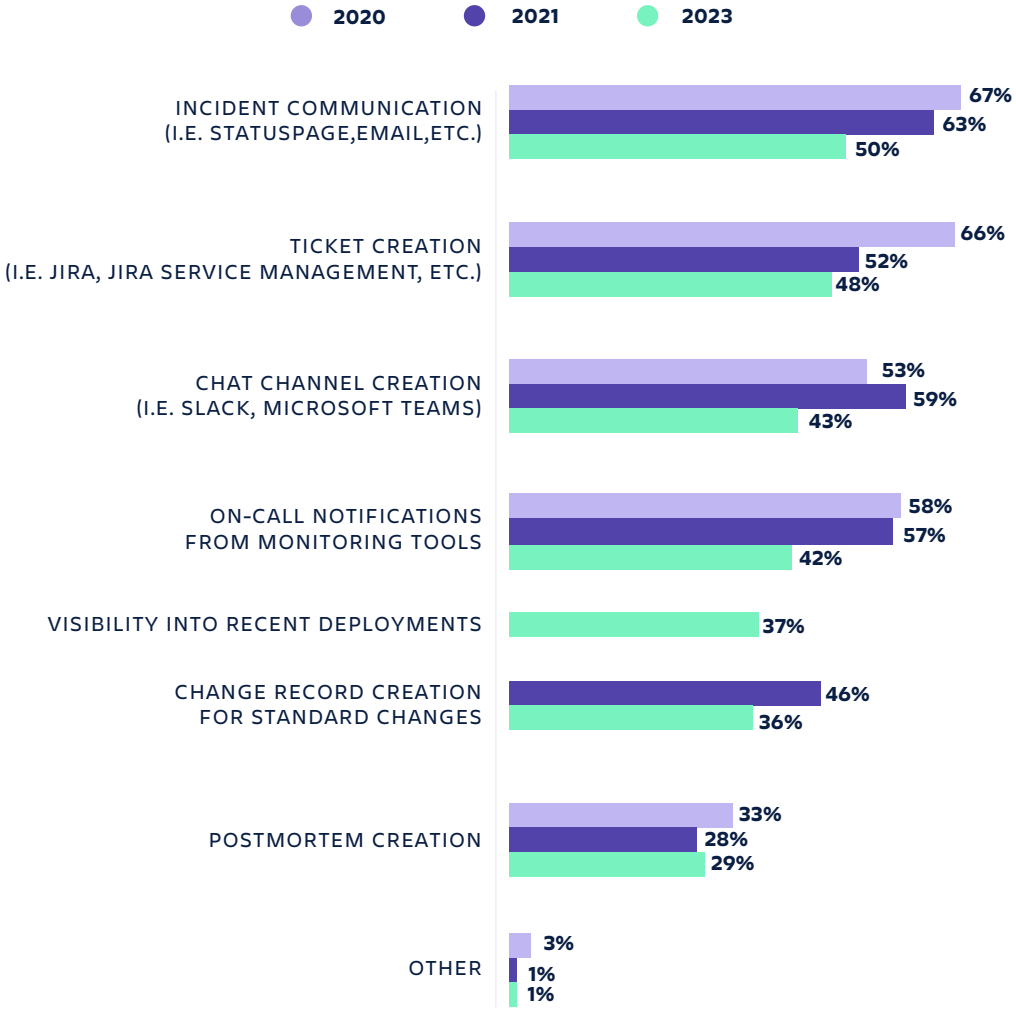




Organizations are most often automating incident communications and issue/incident creation. Postmortem/PIR creation automation is only utilized by three in ten ITDMs, indicating usage has room to grow. Identification of affected CI and/or service is also automated by less than one-third of organizations. It's no surprise that organizations that use AI to trigger incidents and organizations that currently use AI tools like ChatGPT are more likely to automate most areas of the incident management process, indicating that their processes are more mature.

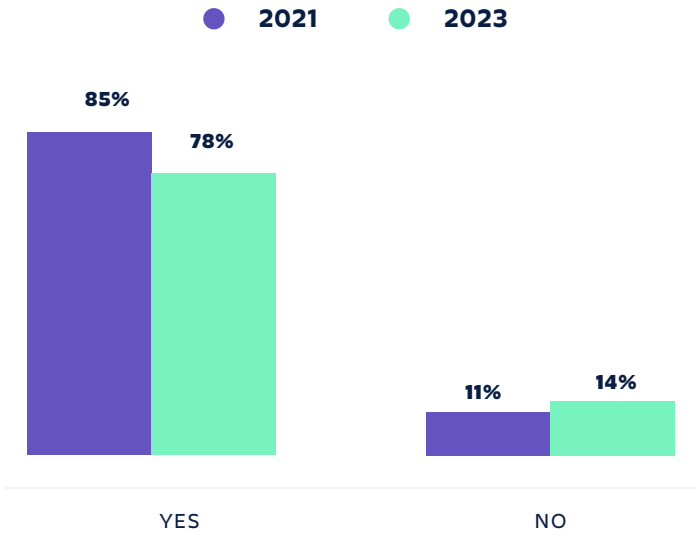


AUTOMATED INCIDENT MANAGEMENT PROCESSES



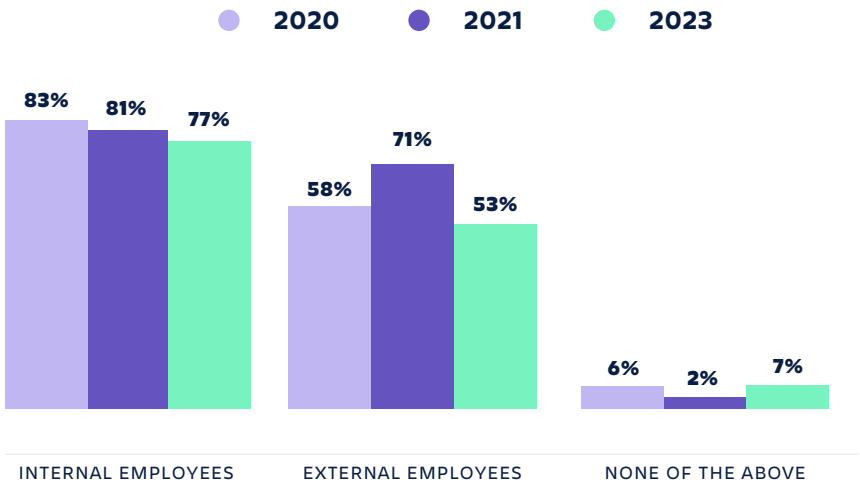
Usage of AI to trigger incidents has fallen since the last wave; 62% of respondents indicated using AI to trigger incidents versus 85% in 2021. The reasons for this are unclear, and whether this is a trend has yet to be determined. Software developers are more likely to report not using AI to create incidents. Fifty percent of respondents report using AI for incident trending purposes; this is still a majority, although it's on a slight decline from 2021 (57%).

USING IM TOOL THAT LEVERAGES AI TO TRIGGER INCIDENTS



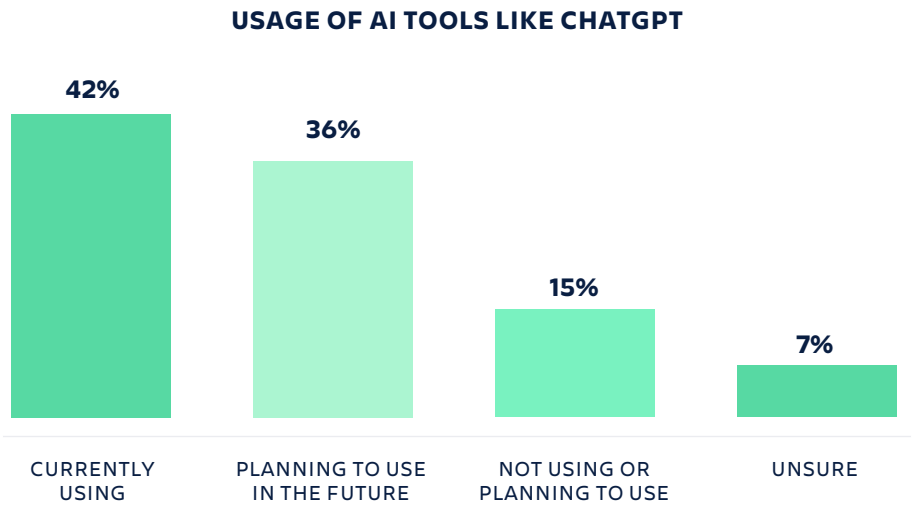
Automation of communications also fell. In 2023, respondents automating internal communications fell around 10% as compared to 2021. Those automating external communications dropped even more to 53% in 2023 versus 71% in 2021.

AUTOMATED INCIDENT COMMUNICATIONS



ChatGPT & AI

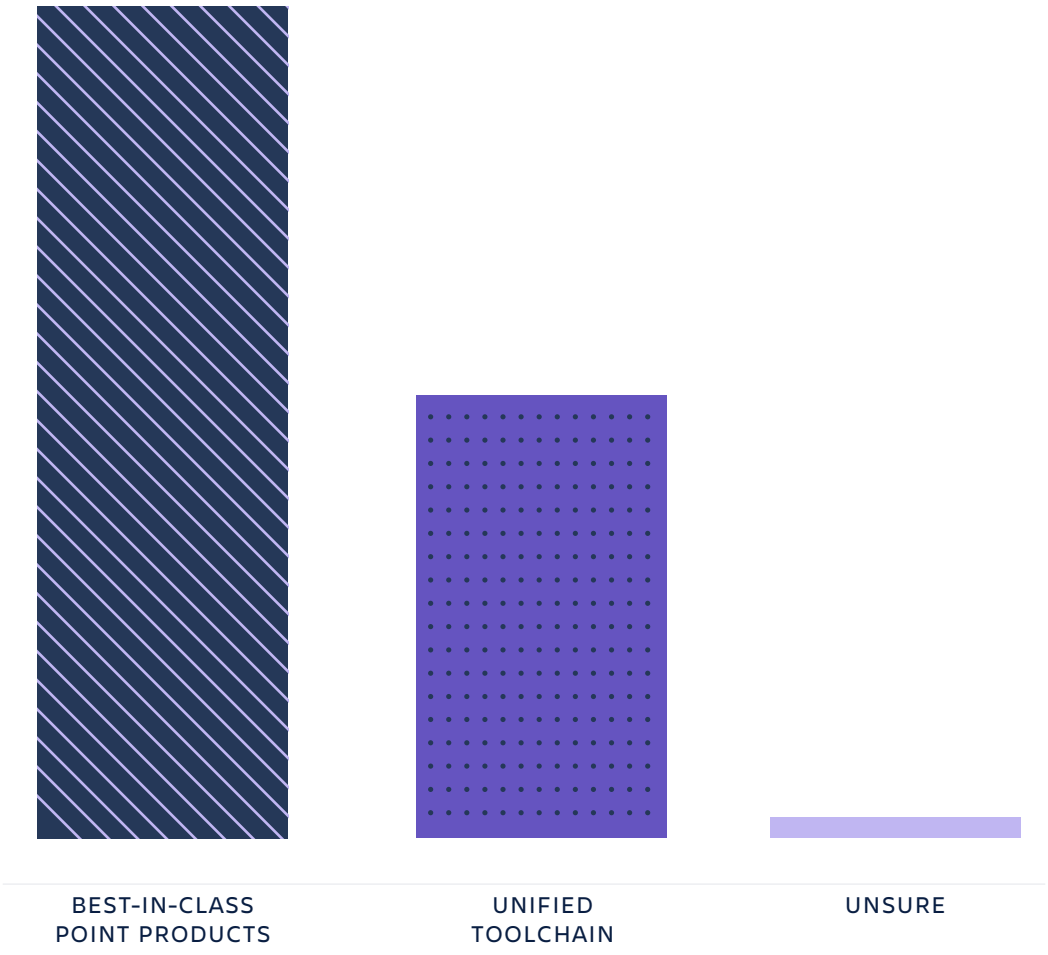
A strong majority currently use or plan to use AI tools like ChatGPT in the near future. Eight in ten are currently using AI, with 36% planning to use it in the near future. Those not planning to use AI also do not automate incident creation.



Eighty-three percent of ITDMS feel that investment in AI for handling incidents is important, with those in higher positions considering it especially important. Despite the willingness to use AI, security remains a top-of-mind concern, 32% are very concerned, and 25% are somewhat concerned. Those at organizations who have no plans to use AI are more likely to use chat (84%), change management/change record (66%), ticketing (65%), and request portal/service desk (65%).

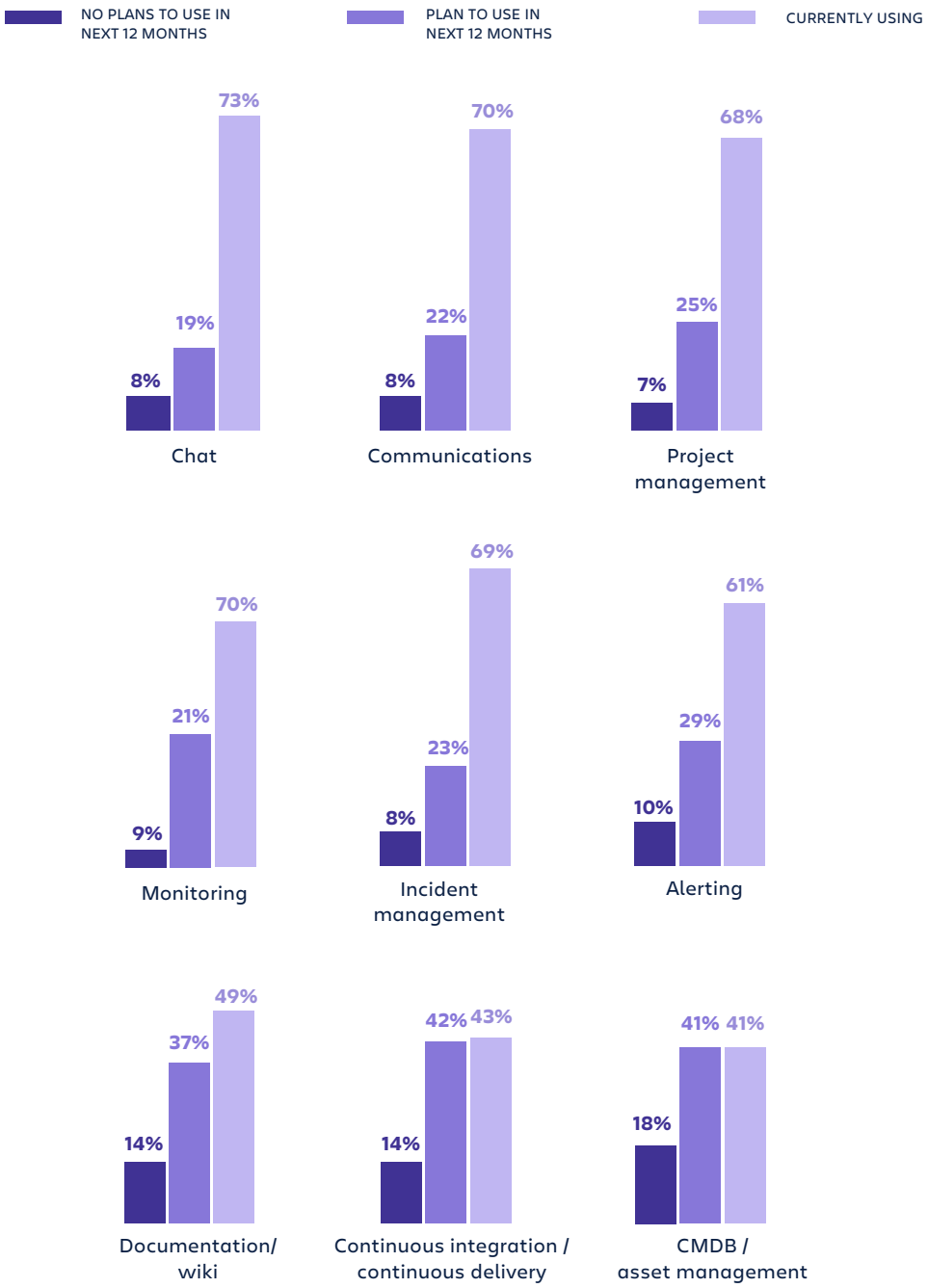
Tools used, versus tools planned

Like in 2021, six in ten prefer to handle incidents with best-in-class point products over a unified toolchain. Notably, now one in ten are uncertain which they prefer, which is slightly more than in 2021.



The majority of organizations are using some combination of chat, monitoring, communications, incident management, project management, and alerting. Less than half are using documentation/wiki, CI/CD and/or CMDB. However, it's important to note that most of those who are not currently using these tools plan to do so within the next year.

TOOL USAGE AND PLANS TO USE



Looking ahead: What's next for incident management?

In addition to increased investment in AI and automation (with a healthy dose of skepticism toward security), other trends to look out for in 2023 include:

- Prioritizing wikis
- Investing in CI/CD tooling
- Focussing on asset and configuration management

This is no surprise as all of the above increase visibility across IT infrastructure and support enhanced cross-functional collaboration, two of the main pain points felt by respondents during an incident. Communication trends will also be an interesting topic to watch. Will video conferencing make a return? Will another communication tool finally displace email? Stay tuned until the next benchmark report and take a look at some additional resources listed below.

Want to dig deeper?

www.atlassian.com/incident-management

Have questions?

Contact us at sales@atlassian.com

ATLASSIAN