ATLASSIAN

The state of incident management report 2024

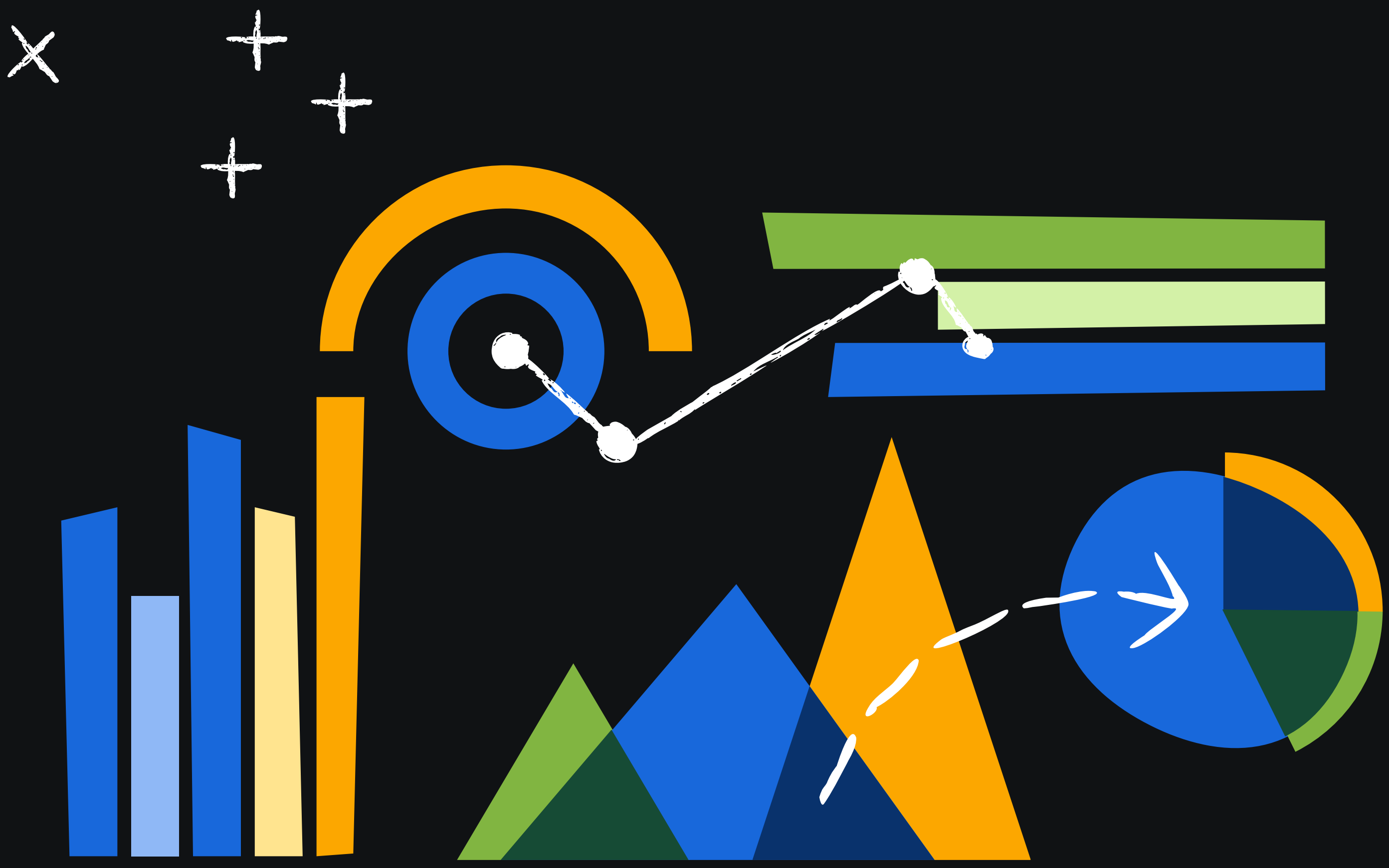


Table of Contents

Executive summary

This year brings us to the fourth year of Atlassian's incident benchmark report.

A lot has changed since our inaugural report in 2020. Video conferencing usage has skyrocketed, gone down, and back up again. Return to office initiatives are still looming for companies that hold their physical campuses dear. Tech stocks seemed to "recover" after a notable slump[1,2] and inflation appears to be leveling out[3]. All these signals that "all is well" (or, will be) might be the reason we saw a large increase in tool usage this year.

Tech is a funny business, the stocks are doing well but reductions in force, mass lay-offs and downsizing is still plaguing the industry, although the impact seems to have slowed[4]. Many of us are still waiting for artificial intelligence (AI) to deliver on its promise to either replace us all or make our jobs fun again. But what does all this mean for incident management?

Although folks are still skeptical about the security of AI tooling, they are more willing to invest and find it ever-important. In addition to taking the temperature on AI you can also expect to benchmark your own process with findings across:

- Companies' overall incident management processes
- Common pain points and opportunities for improvement
- How automation is being leveraged to make incident response easier
- Where the industry is focusing for future investment
- Year over year comparisons and identified trends

SOURCES:

1. **CNBC: Tech stocks just wrapped up one of their best years in past two decades after 2022 slump**

2. **US News & World Report: 10 Best Tech Stocks to Buy for 2024**

3. **Statista: Monthly 12-month inflation rate in the United States from July 2020 to July 2024**

4. **CNBC: Laid-off techies face 'sense of impending doom' with job cuts at highest since dot-com crash**

Survey methodology and demographics

Who took the survey?

As we've done since its inception, Atlassian's 2024 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 fourth installment; previous surveys were conducted in 2020, 2021, and 2023 respectively. All were fielded by CITE Research, on behalf of Atlassian. In 2024, 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 23% of respondents identified as women, whereas 76% identified as men. This is a 4% fall in women respondents over last year. The gender disparity among IT and Dev professionals is nothing new, however we had previously identified a trend of increasing female respondents. One percent of respondents identified as non-binary, which is 1% more than last year. It will be interesting to see if this is a continuing trend as tech companies continue to embrace diversity.

2021	2023	2024
Male 80%	Male 73%	Men 76%
Female 20%	Female 27%	Women 23%
	Non-Binary 0%	Non-Binary 1%

In 2024 we changed terminology to be more inclusive.

Age

Consistent with previous years, the majority of respondents continue to fall within the 35-44 age range. We also see the trend of more distribution across age ranges continuing from 2023 with 15% in 18-24, 22% 25-34, and 17% in 45-54.

Age range	2023	2024
18-24	1%	15%
25-34	30%	*22%*
35-44	43%	39%
45-54	15%	17%
55-64	10%	6%
65 or older	--	2%

Company size and revenue

The majority of respondents worked at small-to-medium sized companies with 25% working at larger enterprises. In 2024 40% of companies brought in $1.1B or more in revenue each year, this is more than double the respondents of 2023.

Company size	2023	2024
Less than 500	15%	10%
More than 500	32%	90%
1,001-4,999	27%	--
5,000-10,000	12%	--
10,000+	13%	--

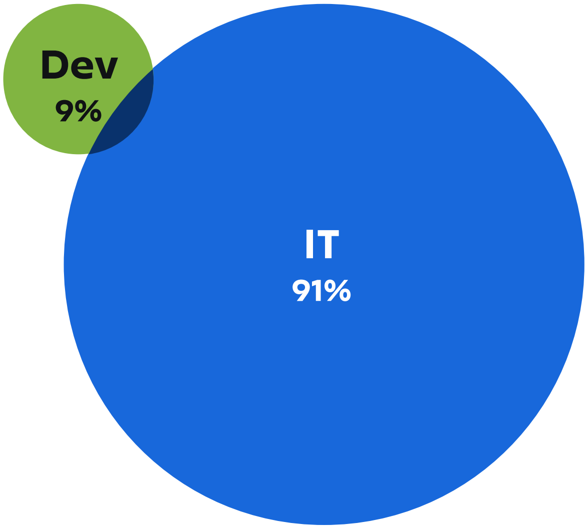
Revenue	2023	2024
$50M or less	25%	21%
$50.1M - $100M	13%	9%
$100.1M - $250M	11%	7%
$250.1M - $500M	13%	8%
$500.1M - $1B	16%	15%
$1.1B or more	--	40%

Title and department

In 2024, respondent titles are largely on par with last year's report, with 91% of respondents in IT, and 9% in a developer role. Last year's survey had a 90% and 10% split, respectively.

We saw notably increased participation from IT Managers and Directors of IT. Last year, they represented 30% and 17% of respondents, respectively. But this year, IT Managers represented 39% of respondents, while Directors of IT represented 35% of respondents.

Similar to last year, we also collected data from respondents in C-Level roles, which represented 8% of 2024 survey takers.



Title	Percentage
Director of IT	35%
Manager of Operations and Release	3%
IT Manager	39%
Other	15%
C-Level (CIO, CTO)	8%

Chapter 01

Perception vs. reality

The maturity of incident management processes

We define a “proactive” organization as one that:

- Makes use of monitoring, alerting, and communication tools
- Facilitates formal incident response training
- Uses AI for incident trending, and integrated visibility into recent changes (added in 2023)

In 2024, we saw the largest increase in proactivity since our 2021 report; rates of proactive responders are up 12% since last year. That falls just behind the increase observed in our 2021 report, which showed a 15% increase in proactive responders year over year.

Year	Percentage of proactive responders
2020	35%
2021	50%
2023	56%
2024	68%

ATLASSIAN

Chapter 02

Tools and processes

Frameworks

We asked folks which frameworks they were using to do their work and listed DevOps, Agile, ITIL 4 and Lean as options. In 2023, we reworded the question to dig deeper into how these frameworks were being applied. As a reminder, only respondents who practice DevOps were represented in the survey.

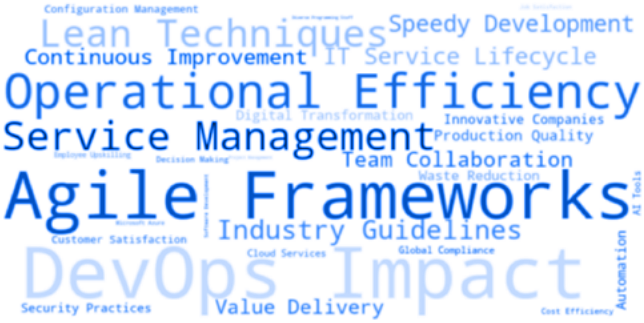
This year, DevOps and Agile took the lead as the most influential frameworks. When surveyed about how they were applying these frameworks, respondents said they leveraged frameworks because they were a way to deliver value faster. They emphasized that teamwork and collaboration were key benefits of following DevOps and Agile.

Excerpts from respondent's answers:

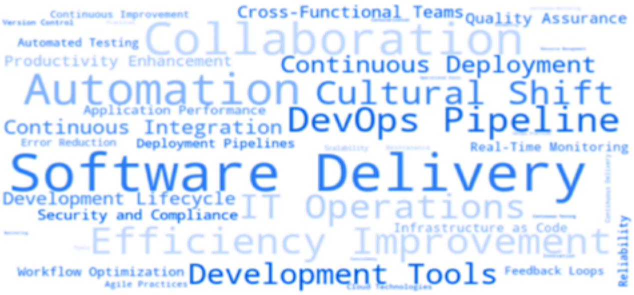
> “DevOps is a cultural movement that combines development, quality assurance, and operations into a single process. It allows us to track the performance and stability of our systems in real-time.”
>
> **SURVEY RESPONDENT**

> “It has been highly influential for us to keep up with the increasing pace of business and technology change. It helps us with speedy development through developing and delivering the features of apps in smaller functional units.”
>
> **SURVEY RESPONDENT**

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.

Communication and collaboration

The way we communicate at work is consistently influenced by cultural shifts. As social media becomes pervasive, so does contactless grocery delivery, automated billing, and online restaurant reservations.

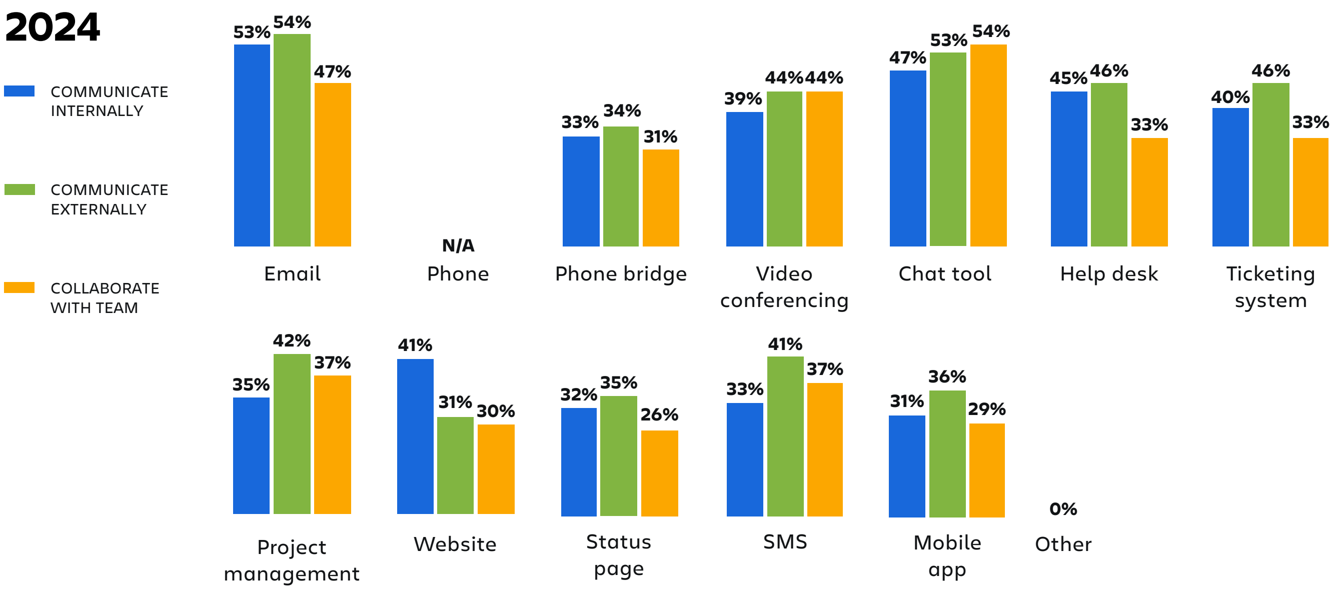
Remember landlines? Only 1/4 of workers in the U.S. still have a desk phone, which explains why "phones" or phone bridges are still among the least-used tools for communication. Old but faithful, email is still holding strong as the go-to method for external communication, likely due to its reliability and ease of use.

In 2023, we saw a marked drop in the use of video conferencing for collaboration and internal communication during an incident. Interestingly enough: this was also coupled with an increase in frustration around communication during incidents. That may be why video conferencing is back on the upswing this year, increasing 2% over last year as a team communication method.

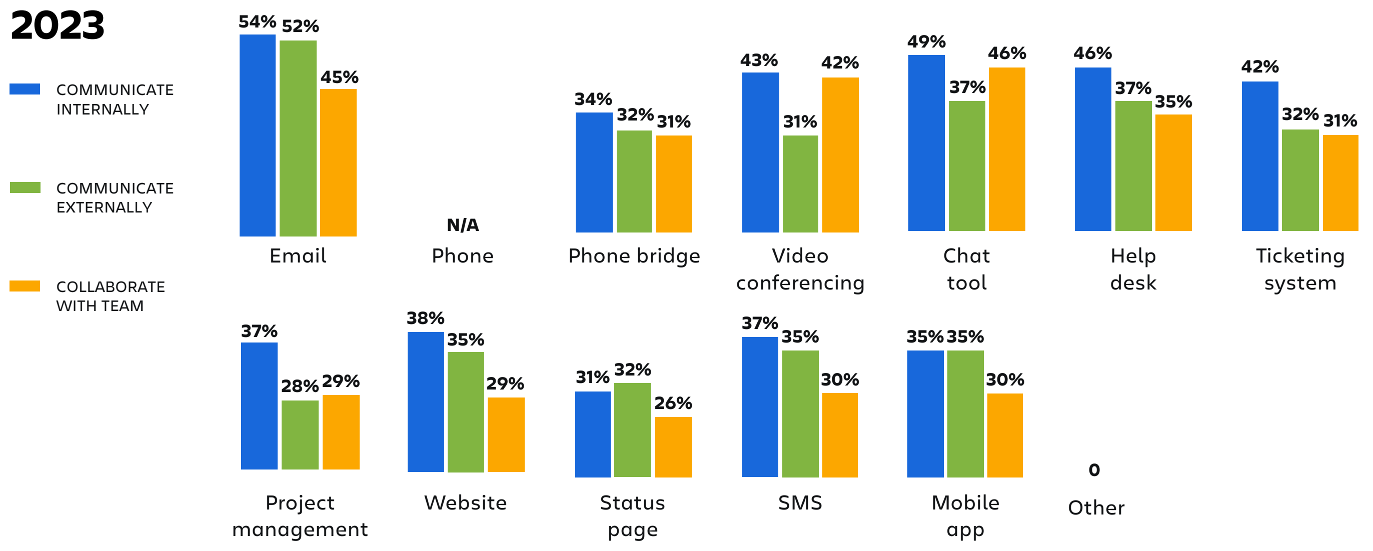
We also saw a huge jump in video conferencing as a communication method for external communication. It will be interesting to see if this trend continues in 2025.

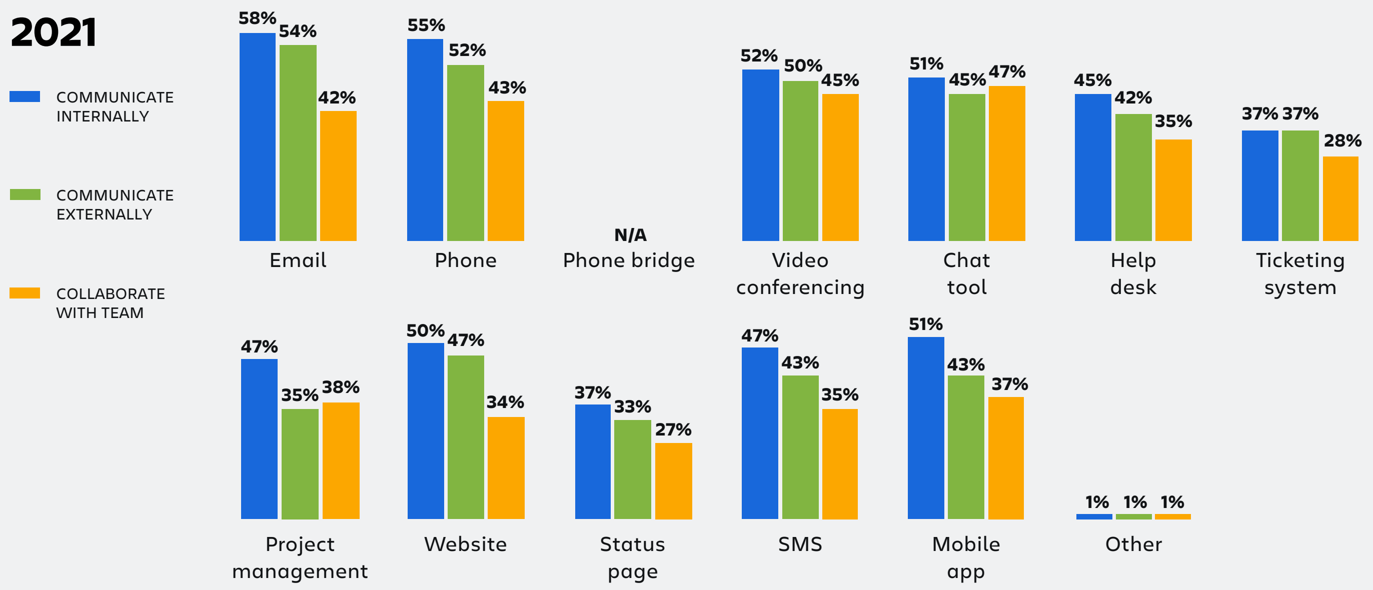
This year chat established itself as the most used medium across the board for internal and external communication, as well as team collaboration. The immediacy of chat, along with the lower pressure is hard to pass up: after all, you don't need to get video-call ready to answer a chat ping. Not to mention, tools like Slack and Microsoft Teams also offer the option for live calls if needed. Perhaps surprisingly video conferencing for external communication increased 13% this year. Respondents also relied on ticketing and help desk systems for external communications, likely using banner announcements to communicate systems' status and request deflection.

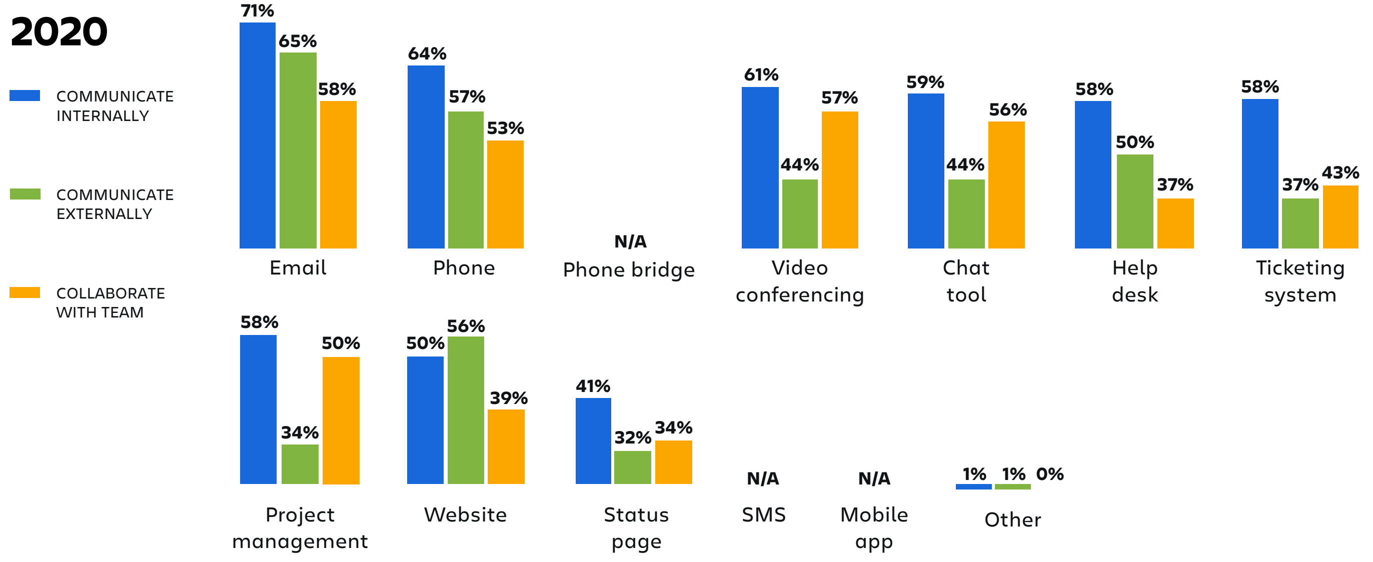
COLLABORATION AND COMMUNICATION TOOLS USE



Categories marked "N/A" indicate they were not included in the survey for that year.







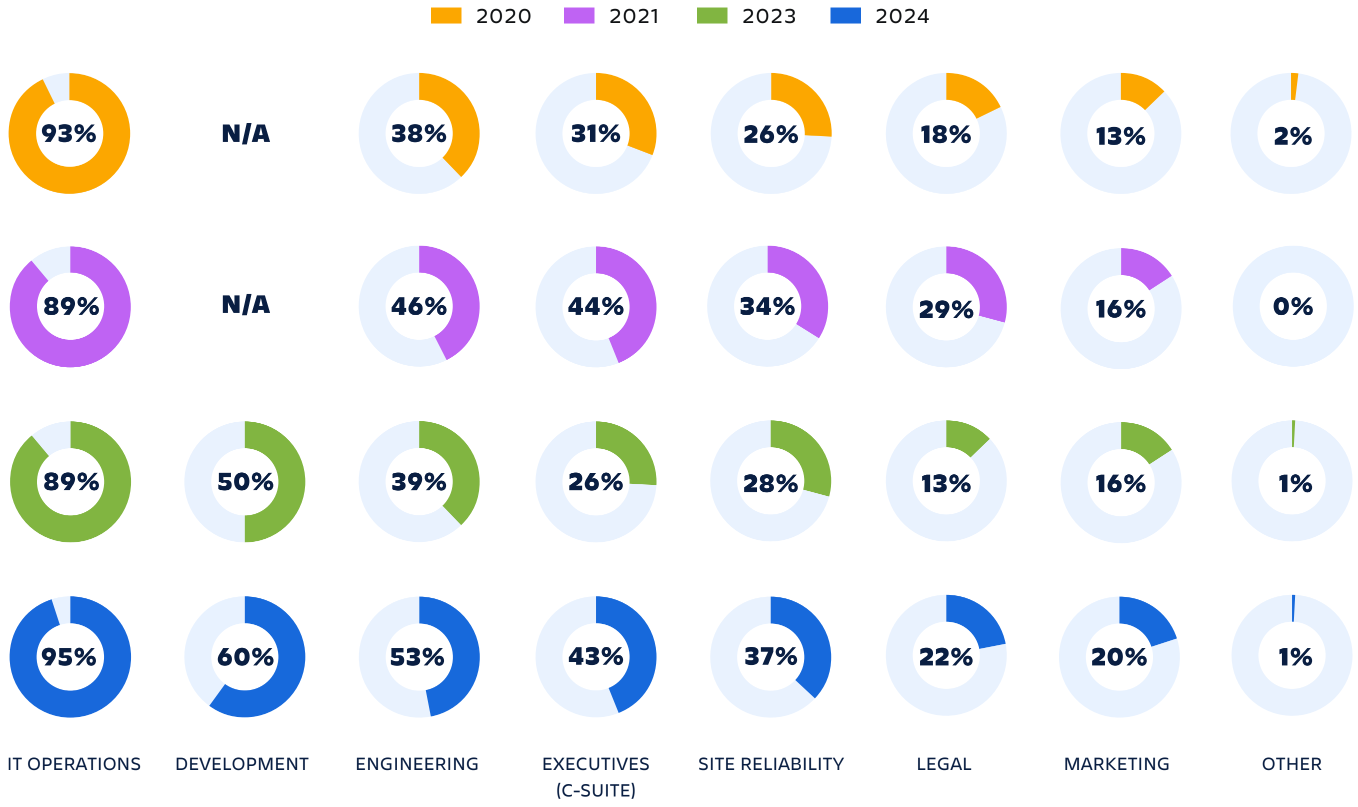
Categories marked "N/A" indicate they were not included in the survey for that year.

Who manages incidents?

Holding consistent since 2020, IT Operations are still the most heavily involved in incident management. In 2021, we saw teams outside of IT Ops and Dev involved in incident response, likely due to the added pressure on infrastructure as a result of the pandemic. However, this trend seemed to peter out until this year.

In 2024, we saw a statistically significant increase of the C-Suite and Legal getting involved in incident management as well as a small increase in Marketing involvement (4%). Companies could be trying to get ahead of the added threat that technology like AI, deep fakes, world-wide inflation, and a reported increase in cyber attacks and data breaches.[5]

TEAMS INVOLVED IN MANAGING INCIDENTS

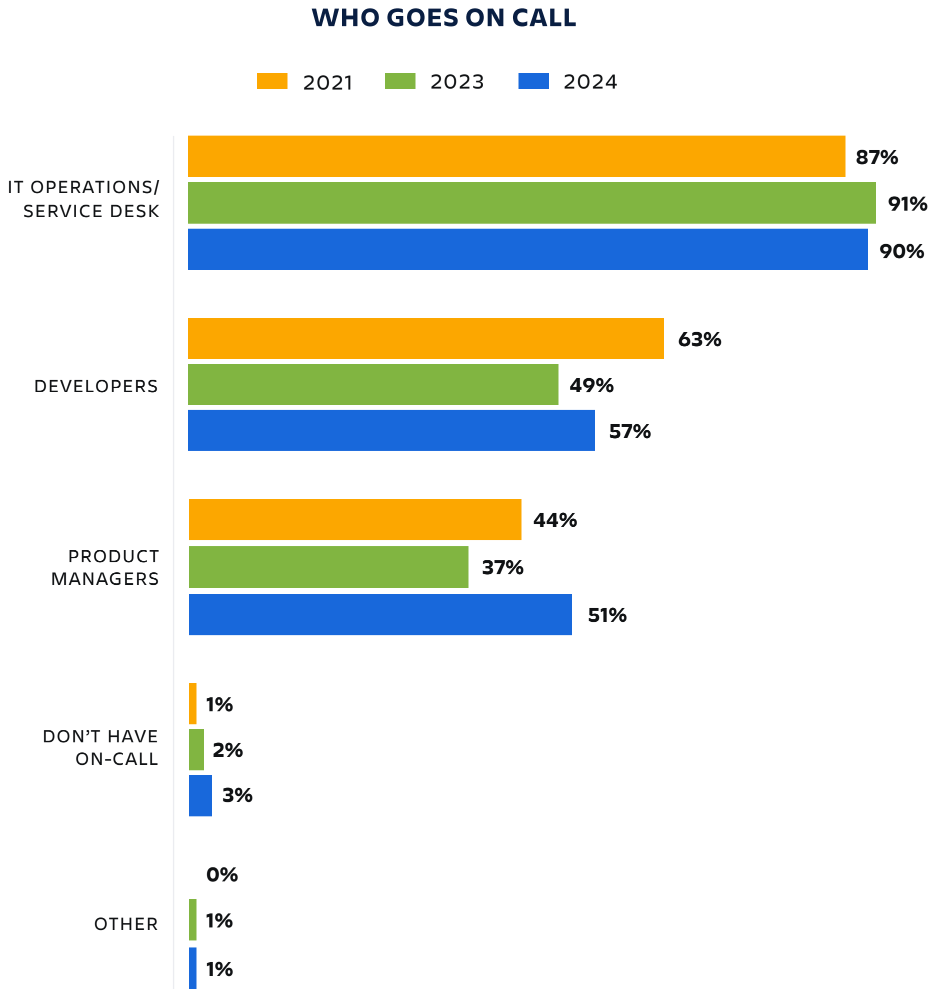


Categories marked "N/A" indicate they were not included in the survey for that year.

[5] IBM Cost of a Data Breach Report 2023

Who goes on call?

Similar to previous waves of research, IT still represents the majority of who goes on call. However, there was a marked increase (8%) of on-call Developers, and a 14% increase in Product Managers going on-call. A slight increase (from 1% to 3%) in respondents reported not having on-call in their organization.



Incident prevention

On par with last year, 97% percent of organizations have procedures, processes, or runbooks in place for managing incidents. Seventy-eight percent are using wargames or incident management training, which is a slight increase over last year (75%). Those using AI are more likely to use both procedures and wargames training than those not using AI.

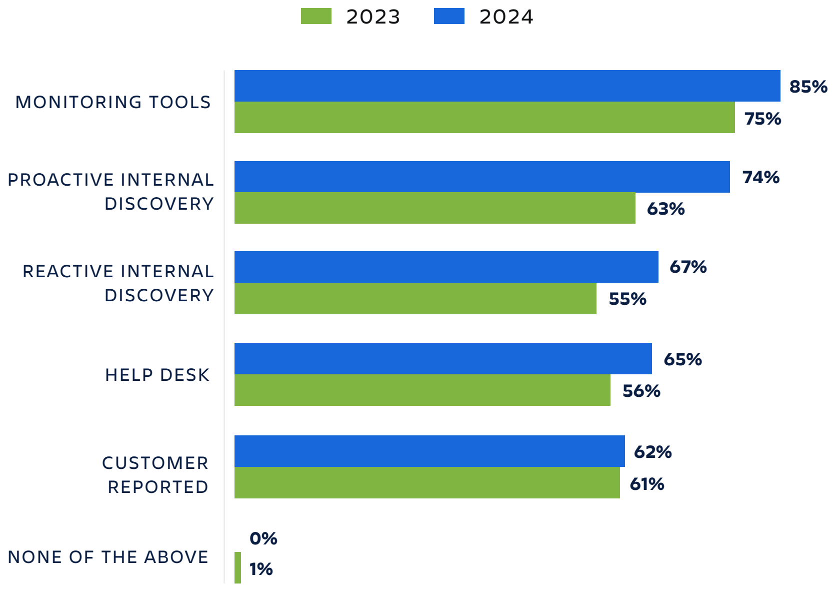
This year, we also saw a significant increase in use of proactive techniques. Similar to previous waves of research, capacity monitoring is the top proactive incident tool utilized by organizations. And now, AI for incident trending has now become equally common as user transaction monitoring. While synthetic testing was used in over half of organizations, those where Developers are held accountable for incidents were significantly more likely to use it (63%).

Ninety-nine percent of respondents report using monitoring tools, with 86% relying on monitoring tools to discover incidents. Proactive internal discovery is up 11% over last year, with 73% of respondents now using this method. Other than "customer reported," IT Decision makers are significantly more likely to report using all channels for incident discovery.

USE OF PROACTIVE INCIDENT TECHNIQUES/TOOLS

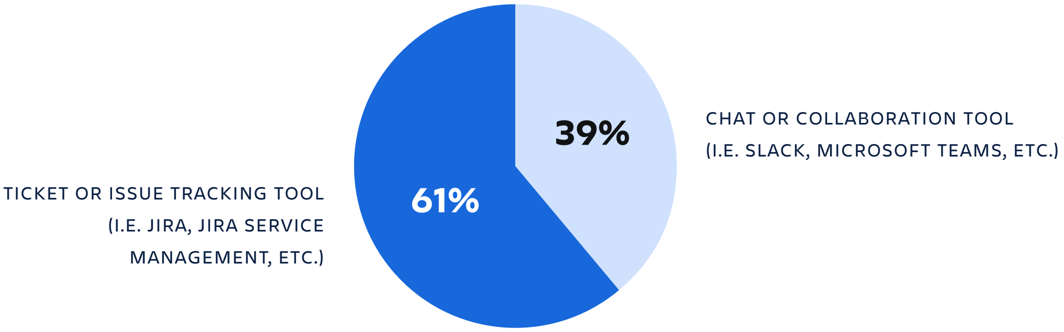
	2023	2024	
●	70%	80%	Capacity monitoring
●	50%	74%	AI for incident trending
●	62%	73%	User transaction monitoring
●	47%	59%	Incident trends/correlation
●	43%	56%	Synthetic testing
●	2%	0%	Other automation techniques

CHANNELS USED TO DISCOVER INCIDENTS



Source of truth during incidents

While chat tools are the source of truth for 39% of respondents, 61% still prefer to leverage their ticketing or ITSM system instead. Tools like Slack or Microsoft Teams alone can't fulfill the need for detailed logging and reporting like Jira Service Management, BMC Remedy, or ServiceNow can but their immediacy and accessibility is unmatched. This is likely why ChatOps is woven into the incident response process, but not the source of truth for most respondents.

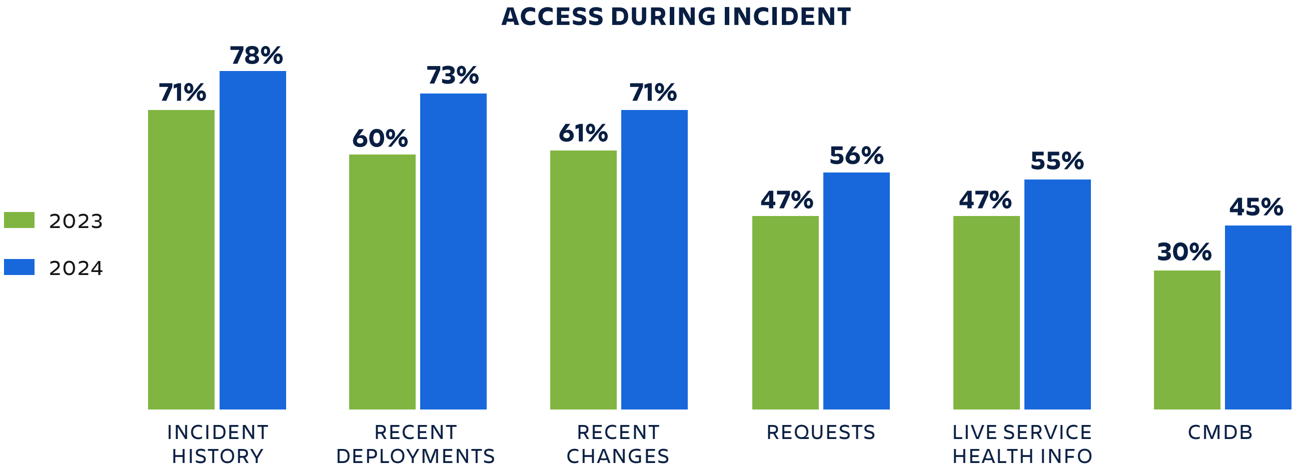


Visibility during an incident

Monitoring/logging, chat, deployment, and incident management/response tools remain the most commonly used tools. Compared to 2023, respondents are significantly more likely to report leveraging all tools tested. Over 70% of organizations are able to access incident history, recent deployments, or recent changes for context during incident response.

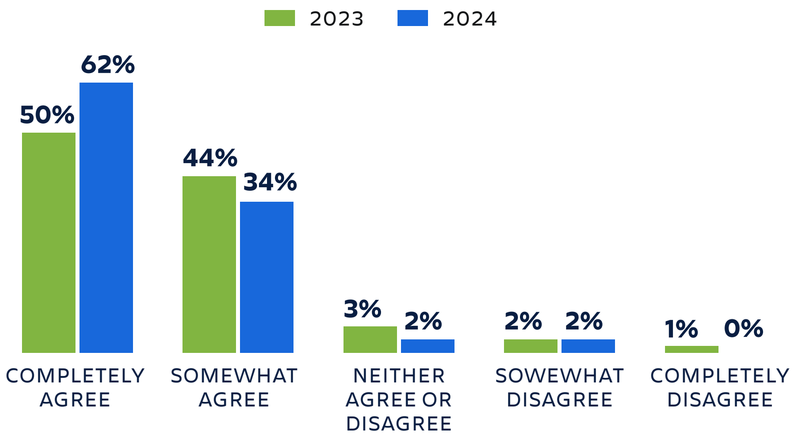
While organizations are significantly more likely to report access to all records/information types tested compared to last wave, respondents reported access to each at similar rates to last year, with CMDB as the least likely to be accessible during an incident. This could be due to the size of organizations that are responding to the survey, or due to the maturity of their incident management process.

Also surprising: only 55% of respondents have access to live service health information.



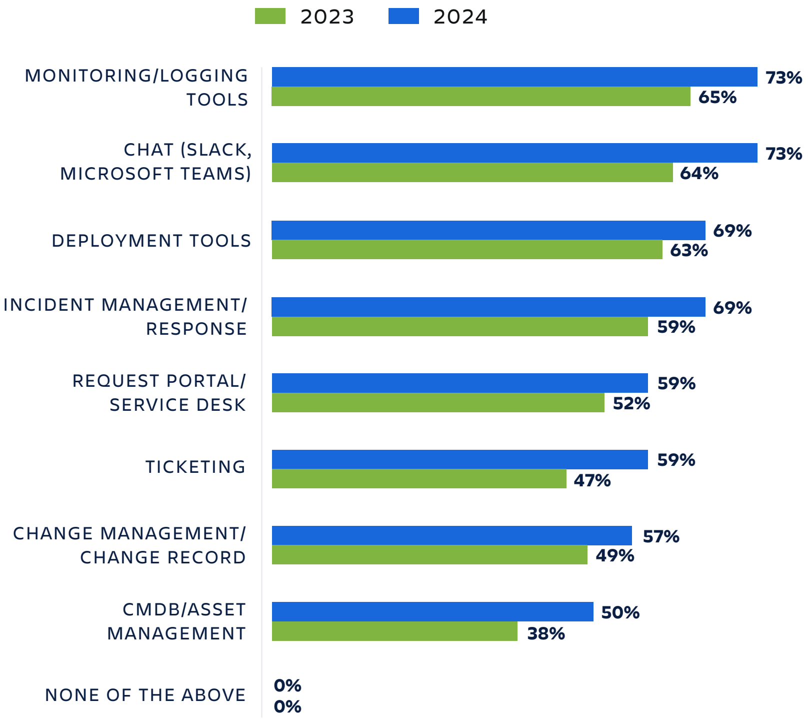
However, 96% of respondents feel that Dev and Ops teams have the visibility they need to do their jobs effectively while minimizing disruption. Those that are leveraging AI to trigger incidents (66%) and organizations that are currently using AI (68%) are especially likely to feel that Dev and Ops teams have the visibility they need, possibly signifying the benefits of AI in this context. It should be noted that IT decision makers are more likely to agree with this sentiment and the majority of respondents were in IT, which could color the results.

AGREEMENT: OUR DEV AND OPS TEAMS HAVE FULL VISIBILITY INTO WHAT THEY NEED TO DO THEIR JOBS EFFECTIVELY WHILE MINIMIZING DISRUPTION



Additionally, most organizations are leveraging a change management practice (97%) with most referring to it as change enablement (86%). Surprisingly, 53% are leveraging some form of change advisory board, which is a 25% increase over last year.

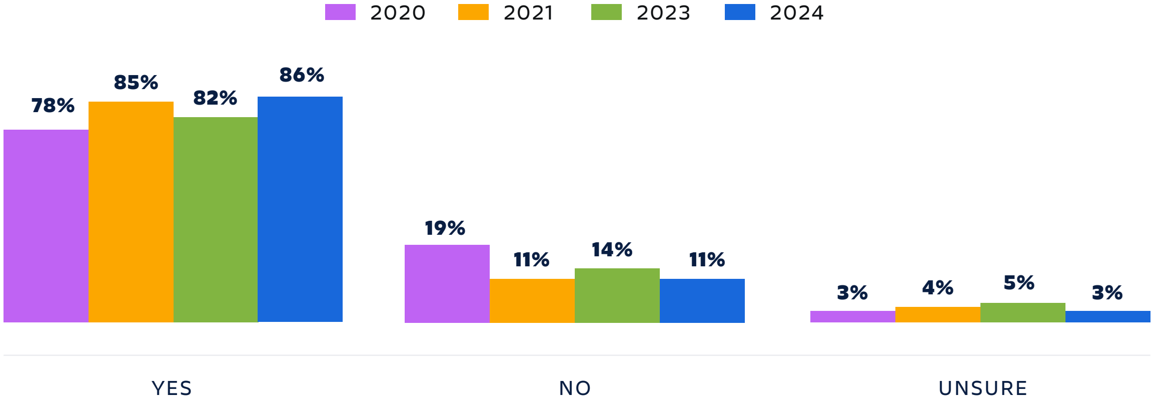
TOOLS CURRENTLY LEVERAGING



Measuring success after the incident

Consistent with prior research, most respondents are running postmortem or post-incident reviews (PIR) after an incident. Those not using AI to trigger incidents are less likely to do post mortems or PIRs: 68% do, 22% do not. This is likely a sign of the maturity of their incident management process.

POSTMORTEMS ON INCIDENTS

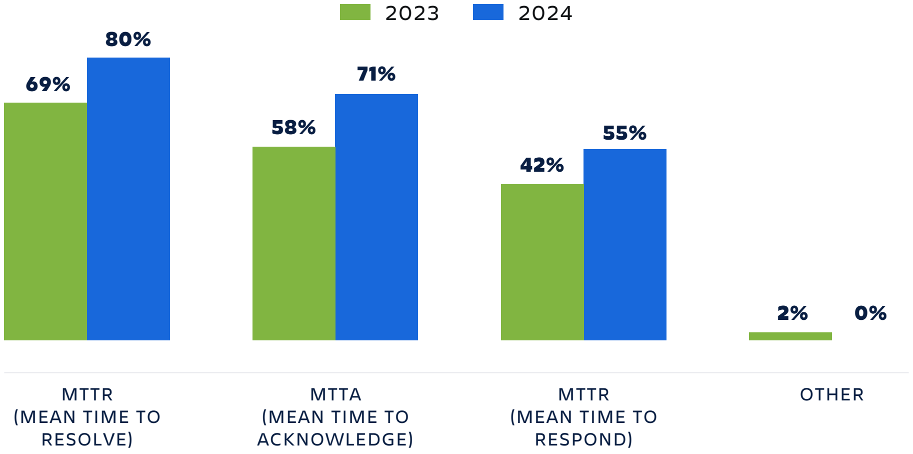


Mean time to resolve (MTTR) continues to be the most popular performance indicator for incident response. This metric has only continued to gain popularity as a performance indicator since our initial survey in 2021.

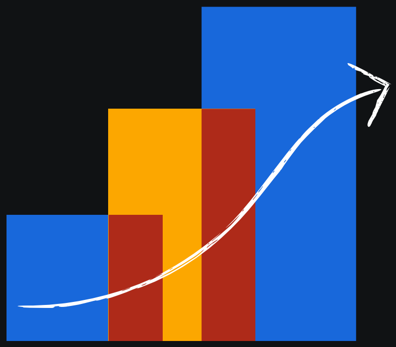
While MTTR remains the most common performance indicator, usage of all metrics is up significantly since last year. Respondents were asked to provide an estimate for how much an incident costs their organization. Fifty percent estimate that incidents cost their organization more than $500, while 39% of respondents are unsure of the cost, and 20% don't measure the cost associated with incidents. The cost of an incident can vary greatly depending on the duration, industry, and company size. The incident cost question is used to determine what percentage of organizations are using this as a metric.

When it comes to accountability, 7 in 10 organizations hold their developers accountable for deployments that cause incidents, while 22% practice blameless post mortems.

METRICS TO DETERMINE SUCCESS



ATLASSIAN



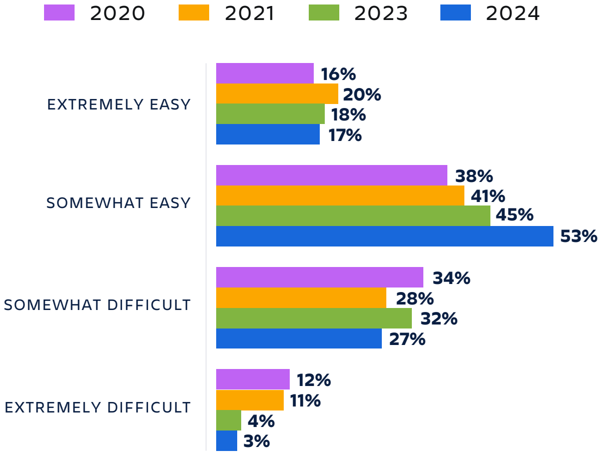
Chapter 03

Areas of improvement

Main pain points

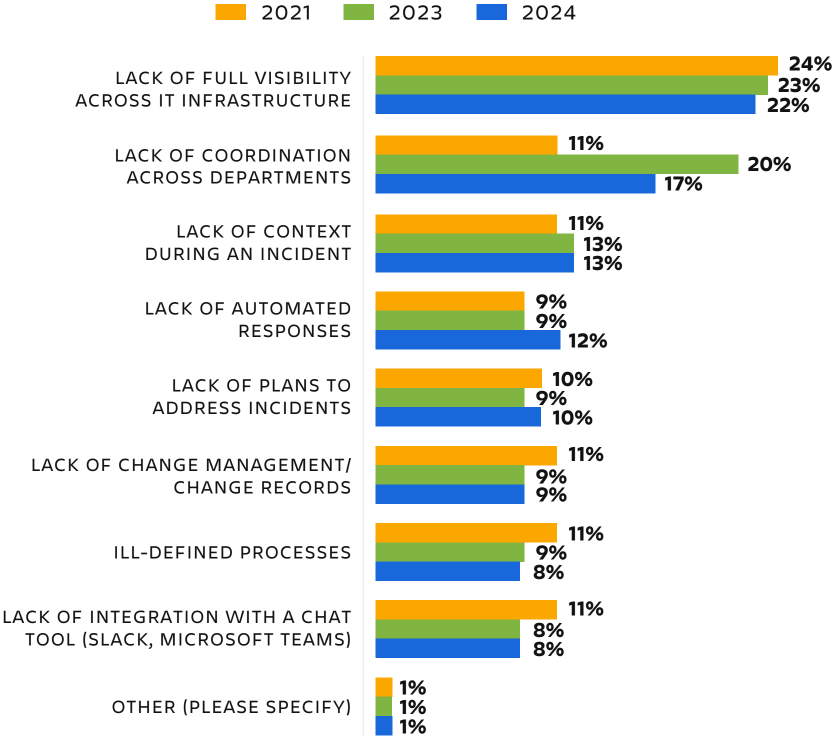
On a positive note, most respondents found it easy to get the right stakeholders involved during an incident; 70% reported it was easy to bring in the right teammates, whereas 30% found it difficult. Those who found it difficult to get the right stakeholders involved were less likely to hold developers accountable for incidents (37%) and were also less likely to be using AI to trigger incidents.

DIFFICULTY GETTING STAKEHOLDERS INVOLVED AFTER INCIDENT IS DISCOVERED



Like the previous two reports, lack of full visibility across IT infrastructure remains the largest pain point. And given respondents' tool usage, that makes sense: roughly 60% of respondents are not leveraging a CMDB, which provides important infrastructure context in the face of an incident, which may explain why lack of infrastructure context is cited as a pain point.

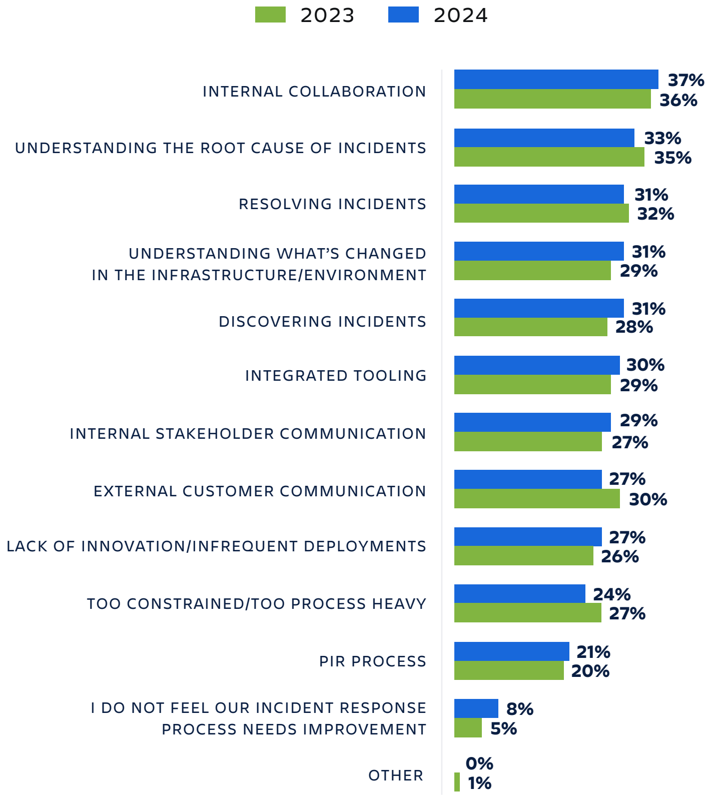
BIGGEST PAIN POINT IN INCIDENT MANAGEMENT



Coordination across departments is also a source of frustration, plaguing 17% of respondents. Those in software development are significantly more likely to feel that ill-defined processes are a pain point (19%). Understanding the root cause of incidents, resolving incidents, understanding changes, and proactively discovering incidents also remain concerns.

Communication with external stakeholders was also a notable pain point. Only 8% feel their incident processes don't need any improvement. This is likely due to the spirit of continual improvement among the frameworks respondents are following (like DevOps, Agile, and Lean).

AREAS NEEDING IMMEDIATE IMPROVEMENT



ATLASSIAN

Chapter 04

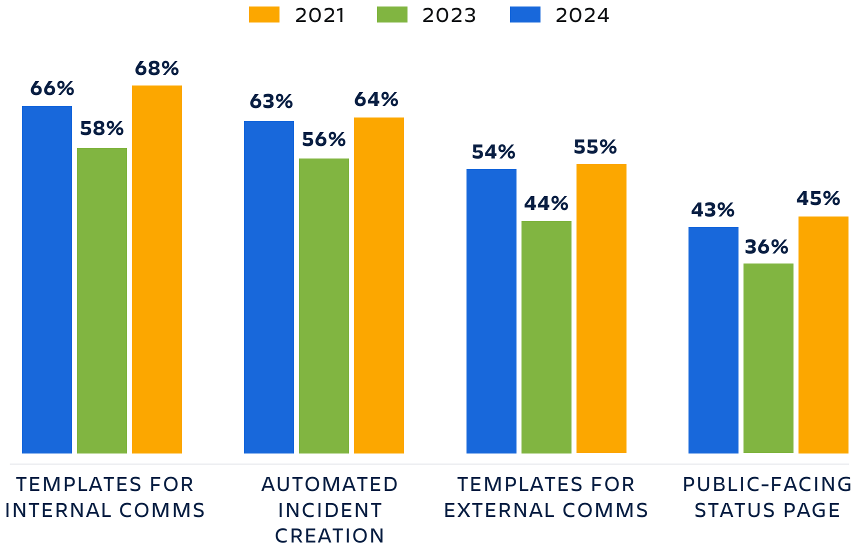
The role of automation, AI, and innovation

Automation

The use of automation increased significantly across almost all areas surveyed. Incident communications and issue/incident creation were the most commonly automated processes, as they were in previous years. IT decision makers reported an increase in usage of tools like templates and public-facing status pages after dropping in the last wave of research. The preference to automate internal incident communications is still prevalent, and over 50% of respondents report automating external communications.

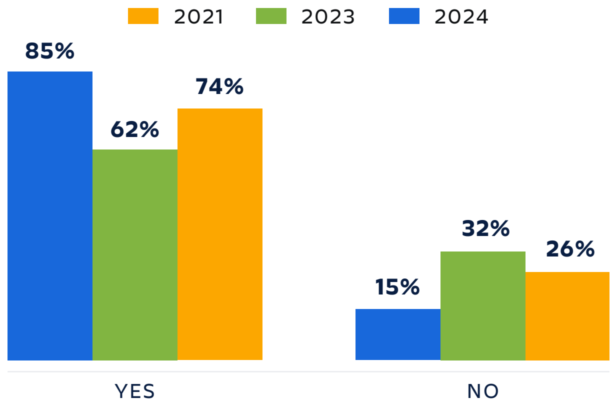
In 2024, 38% percent reported automating change record creation, which is close to 2023's findings of 36%. Post mortem creation remains the least of the automated processes.

LEVERAGING TO AUTOMATE INCIDENT COMMUNICATIONS



Usage of AI to trigger incidents is also up significantly, inching back toward 2021 levels after temporarily dipping in 2023. Software developers are more likely to report that they are not using an AI incident management tool (35%). While the reason is not clear, early adopters of AI in 2021 may have been disappointed with the results, reduced usage in 2023 and picked it back up in 2024 when the technology was more mature. We'll have to see if adoption holds steady next year.

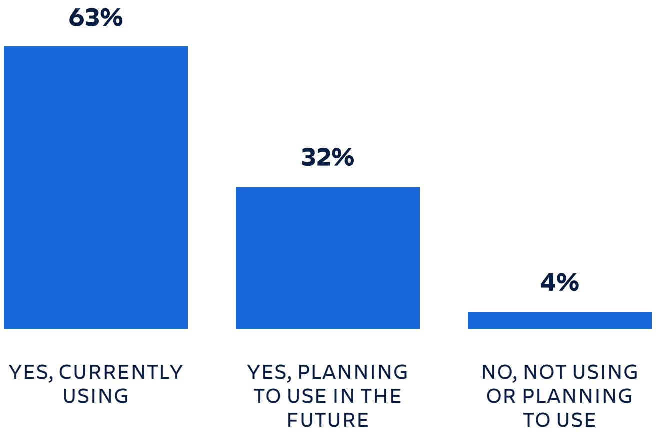
USING INCIDENT MANAGEMENT TOOL THAT LEVERAGES AI TO TRIGGER INCIDENTS



Artificial intelligence

When it comes to AI, nearly all organizations surveyed are currently using it (63%) or plan to use it in the future (34%) to enhance their incident response. This is a 21% increase in AI usage for incident response in just one year. Those who say it's easy to get stakeholders involved in incident management (69%) are more likely to report the usage of AI tooling.

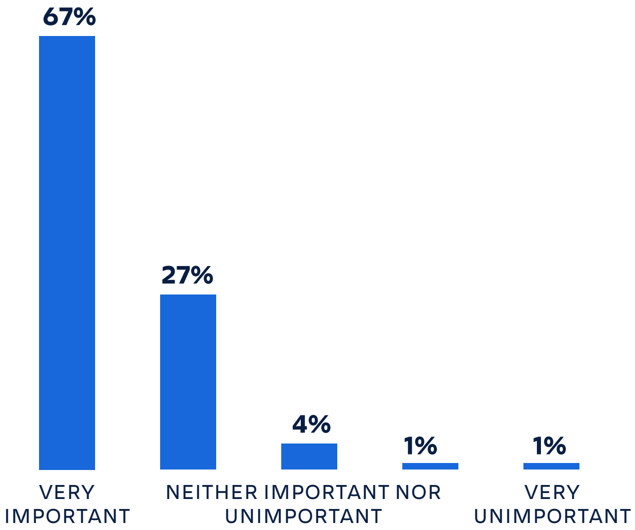
USAGE OF AI TOOLS TO RESPOND MORE QUICKLY TO INCIDENTS



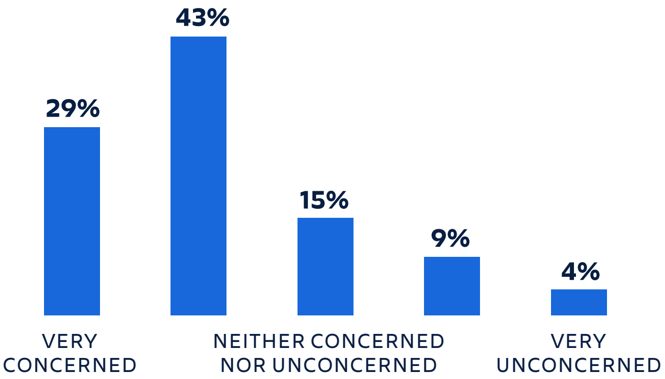
Ninety-four percent of ITDMs feel that investing in AI is important, and two-thirds feel it's very important for their organizations. Based on survey results, higher-level employees are especially likely to consider investing in AI important (88%).

Although most respondents recognize the importance and benefits of using AI, many also cite concern around security risks associated with AI, though it should be noted that results skew toward a more moderate level of concern

IMPORTANCE OF INVESTMENT IN AI FOR HANDLING INCIDENTS



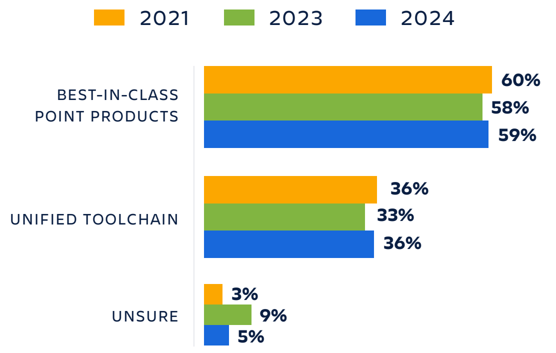
CONCERN ABOUT SECURITY RISKS ASSOCIATED WITH AI TOOLS



Tools used, versus tools planned

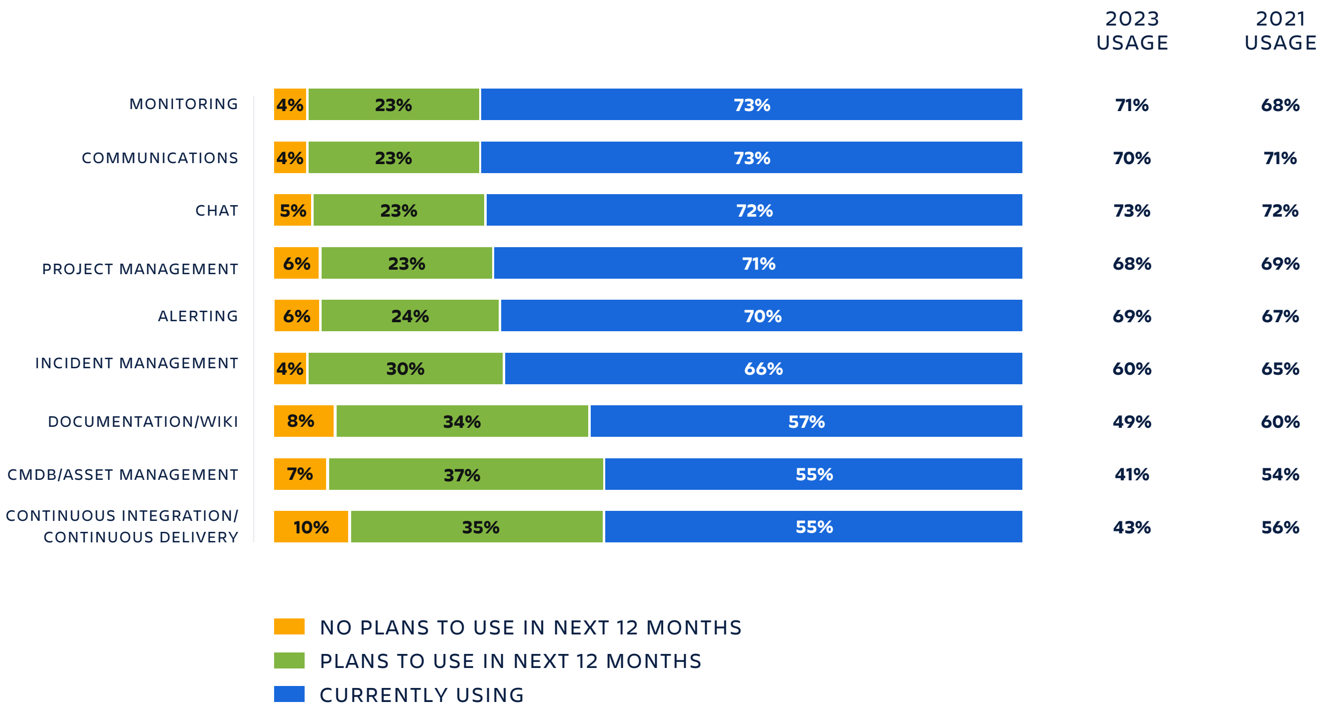
Although tool usage is up across the board compared to last year, six in ten respondents prefer to handle incidents with best-in-class products over a unified toolchain. On par with last year, one in ten don't have a preference.

PREFERRED WAY TO HANDLE INCIDENTS



The majority of organizations are using some combination of chat, monitoring, communications, incident management, project management, and alerting tools. Last year, less than half were using documentation or a wiki, a CI/CD tool, and/or a CMDB. This year, over half of respondents report using all three of these tools.

TOOL USAGE AND PLANS TO USE



Looking ahead, what's next in incident management?

As AI continues to mature and the "hype-cycle" dies down, it will be exciting to see where it gets woven throughout the incident management practice. This year's results saw a spike in the number and type of tools that organizations were using as part of their response. We will have to see if this trend continues in 2025 as AI becomes more prominent across ITSM.

Last year, we questioned if email would finally be dethroned, and if video conferencing would make a return. Well, while video conferencing is on the rise to quell those pesky communication problems, it doesn't look like email is going anywhere.

Based on industry trends and survey responses next year we'll likely see:

- Increased usage of CMDB and Wikis
- Richer AI features like alert grouping, noise reduction, and incident prediction
- Virtual agents in the incident management process

Stay tuned to see if AI writes this report next year, or if we're all back to using wax candles and parchment paper. Need more incident management info? Take a look at our additional resources below:

- **Incident Management for High Velocity Teams**
- **[Video] Incident Management Highlights**
- **[Video] AI as Your Teammate**

Previous years' reports can be found here:

- **State of Incident Management Report 2023**
- **State of Incident Mangement Report 2021**
- **State of Incident Management Report 2020**

ATLASSIAN

Unleash the potential of every team.

Atlassian unleashes the potential of every team. Our agile & DevOps, IT service management, and work management software helps teams organize, discuss, and complete shared work. The majority of the Fortune 500 and over 300,000 companies of all sizes worldwide - including NASA, Audi, Kiva, Deutsche Bank, and Dropbox - rely on our solutions to help their teams work better together and deliver quality results on time. Learn more about our products, including Jira, Confluence, and Jira Service Management at Atlassian.com.