ATLASSIAN

The state of incident management report

2021

Table of contents

Executive summary

We conducted Atlassian's first incident management benchmark report in 2020, at the start of the COVID-19 global pandemic. As a result of stay at home orders and health concerns, the world changed quickly and so did consumer habits. With many people spending more time at home than ever before, industries like streaming, food and grocery delivery, and at-home fitness solutions experienced massive growth. This year's report saw the aftermath of extended social distancing and quarantining.

Companies like Delivery Hero and UberEats reported **96%** and **152%** year-over-year growth respectively. Peloton, known for their online courses and spinning bikes saw a 94% jump in subscriptions. In-person visits were replaced with video and phone chats so folks could stay in touch with loved ones. As such Zoom, a video conferencing solution, saw over **300 million** daily meeting participants in April 2020, compared to 10 million in December 2019.

The increase in demand for digital, always-on services meant that companies had to scale, fast. Even companies not traditionally thought of as software companies, were building up their online apps and expanding capacity to keep up. This increased demand on digital, always-on services and had a downstream impact on incident management.

This year's report showed that in 2021, companies are more willing to spend on incident management so they can ensure a positive service experience for their customers. We surfaced many other findings to help you benchmark against your own processes. Here's what you can expect:

- A general observation of incident management processes and practices
- Focus on collaboration and communication preferences
- Discussion around process automation
- Future plans and investments

Downtime costs more than just dollars, it can also cost you quality employees and damage your reputation. Leverage these findings to make sure you're staying ahead of the curve, and investing in future growth. Incident Management is an ever-evolving practice, we can expect incidents to happen, but the key is in a rapid, organized response.

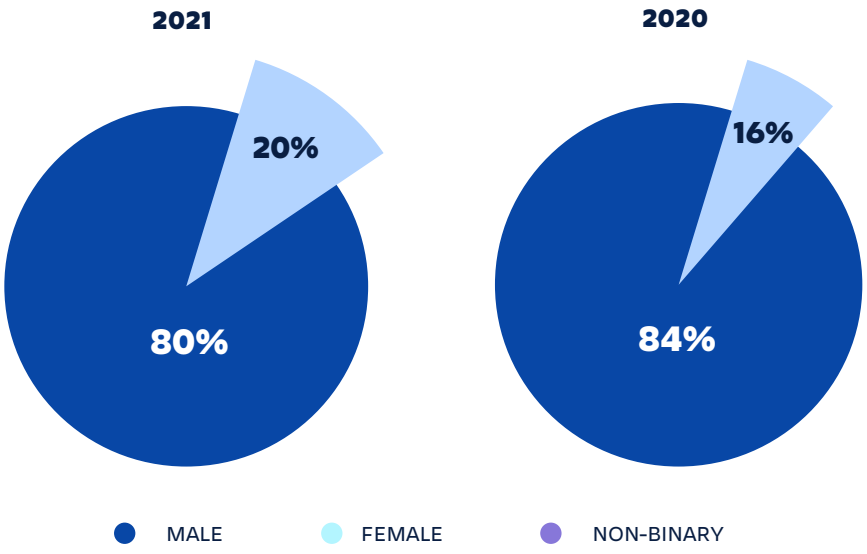
Survey methodology and demographics

Who took the survey?

Atlassian's 2021 State of Incident Management research study surveyed over 500 software developers and IT professionals across the US about IT Service Management (ITSM), with a focus on the practice of Incident Management. The survey was fielded by CITE Research, on behalf of Atlassian and required that respondents were:

- 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

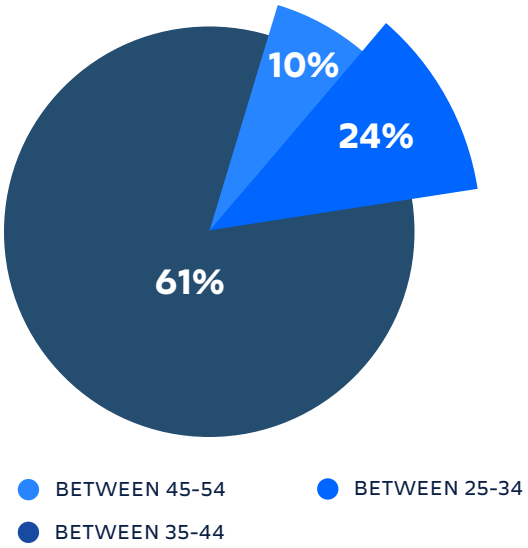
Gender



Only 20% of respondents were women which highlights the gender disparity amongst IT and Dev professionals. We did see a slightly larger disparity last year. While there was a 4% increase in female respondents which is encouraging, it's too small of an increase to make any assumptions. It will be interesting to see if this trend continues next year.

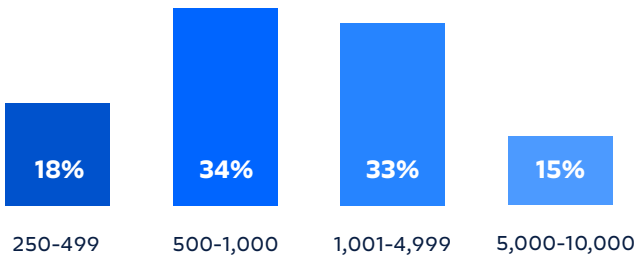
Age

Over 61% of respondents were between 35-44 years of age. Twenty-four percent were 25-34, and only 10% were between 45-54 years of age.



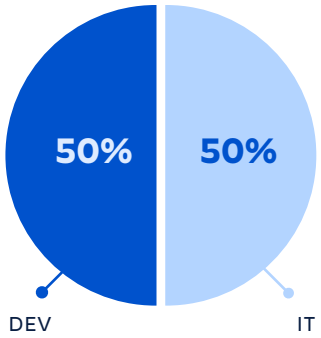
Company Size

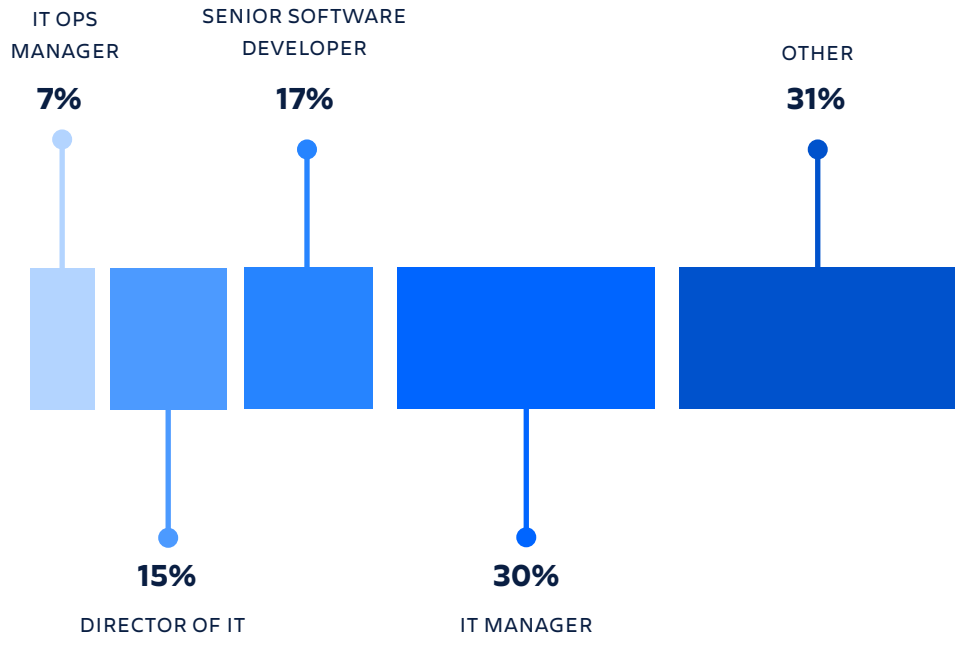
The majority of respondents worked at small to medium sized companies, with 15% working at larger enterprises.



Title and department

Unlike last year's survey, this year's respondents were a 50/50 split between Dev and IT, compared to last year's 78% / 22% split.





01

Perception vs. reality

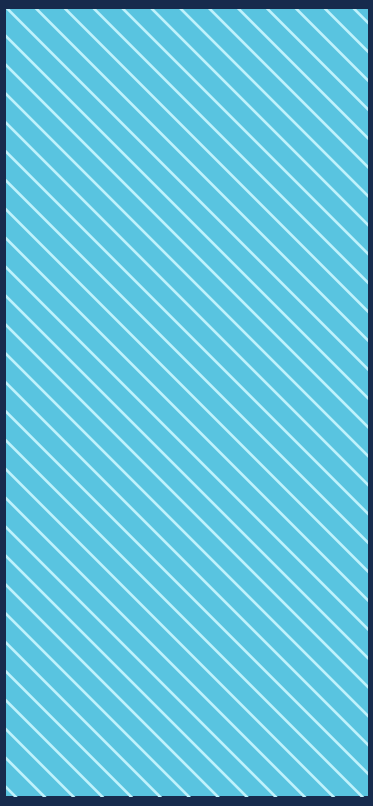
The maturity of the incident management process

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 and automation in at least one aspect of their incident management process.

over

50%

were listed as proactive



THIS YEAR

35%

qualified as proactive by our standards

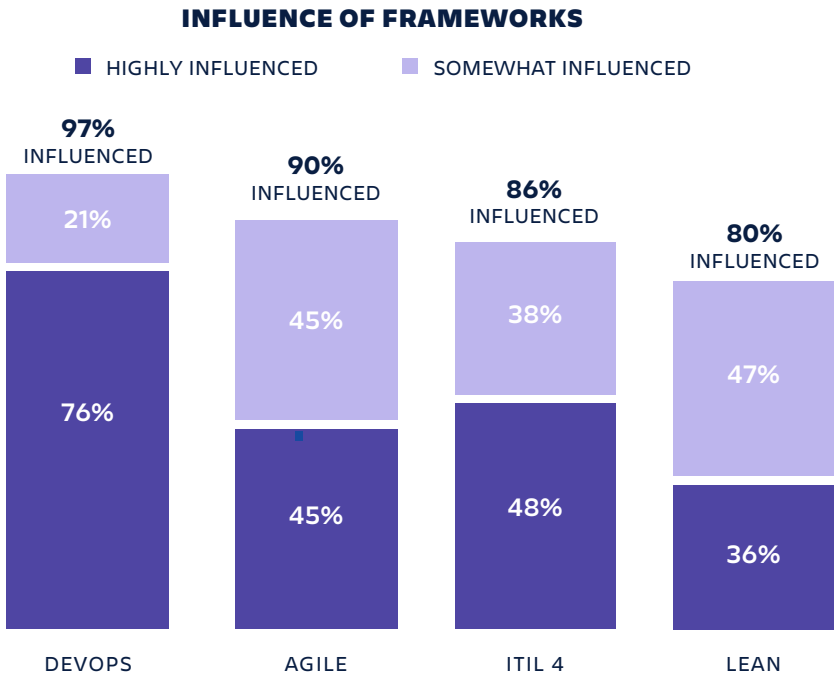
LAST YEAR

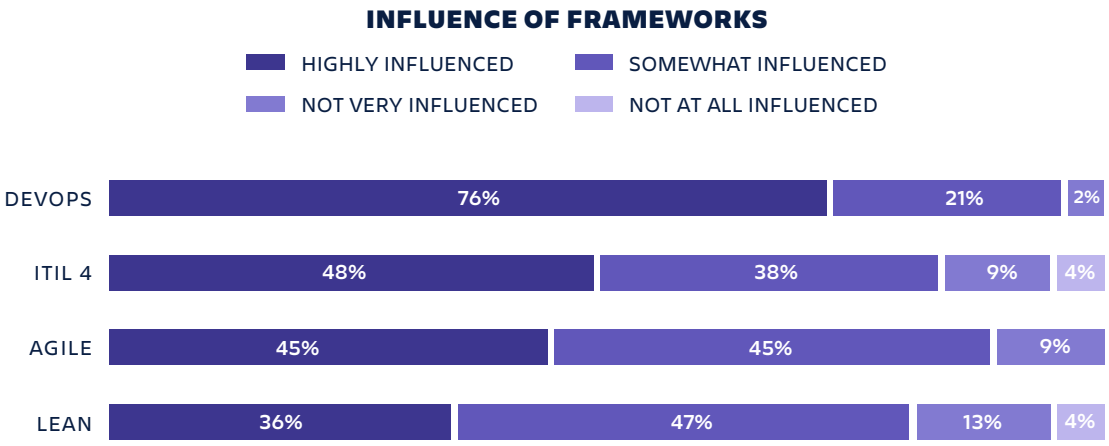
02

Tools and processes

Frameworks

While only respondents who were practicing some form of DevOps moved forward in the survey, we wanted to know which additional frameworks were influential. DevOps took the lead, followed by Agile and ITIL 4. This is especially telling since this year's survey had a 50/50 split between folks who worked in Software Development and IT, versus last year's survey where 78% of people surveyed worked in IT.





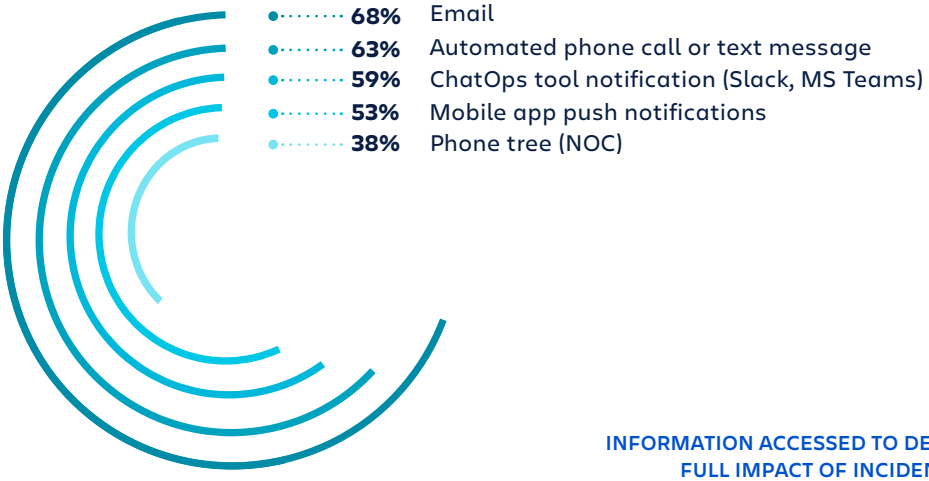
Use of tools during incidents

Incident Discovery

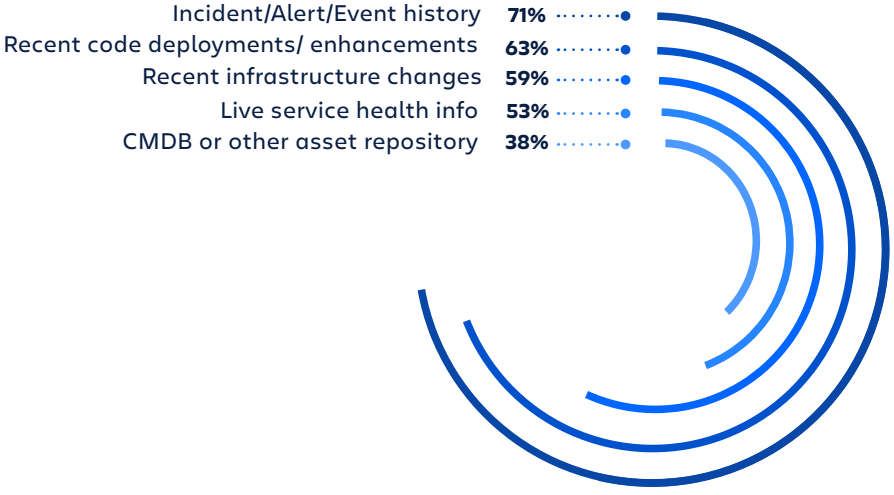
Incident responders are notified through various ways – with two-thirds getting email or automated phone calls or texts. More than half receive a notification via ChatOps tool and/or mobile app. As expected, phone trees and Network Operations Centers are much less common. Practitioners are especially likely to report using email **(72%)** and less likely to report automated call/text **(58%)** as compared to decision makers.

Those that use 5+ tools end-to-end are more likely to use all notification methods tested. To understand the full impact of the incident, responders rely on event history the most, followed by recent code deployments/enhancements.

NOTIFICATIONS OF INCIDENT RESPONDERS

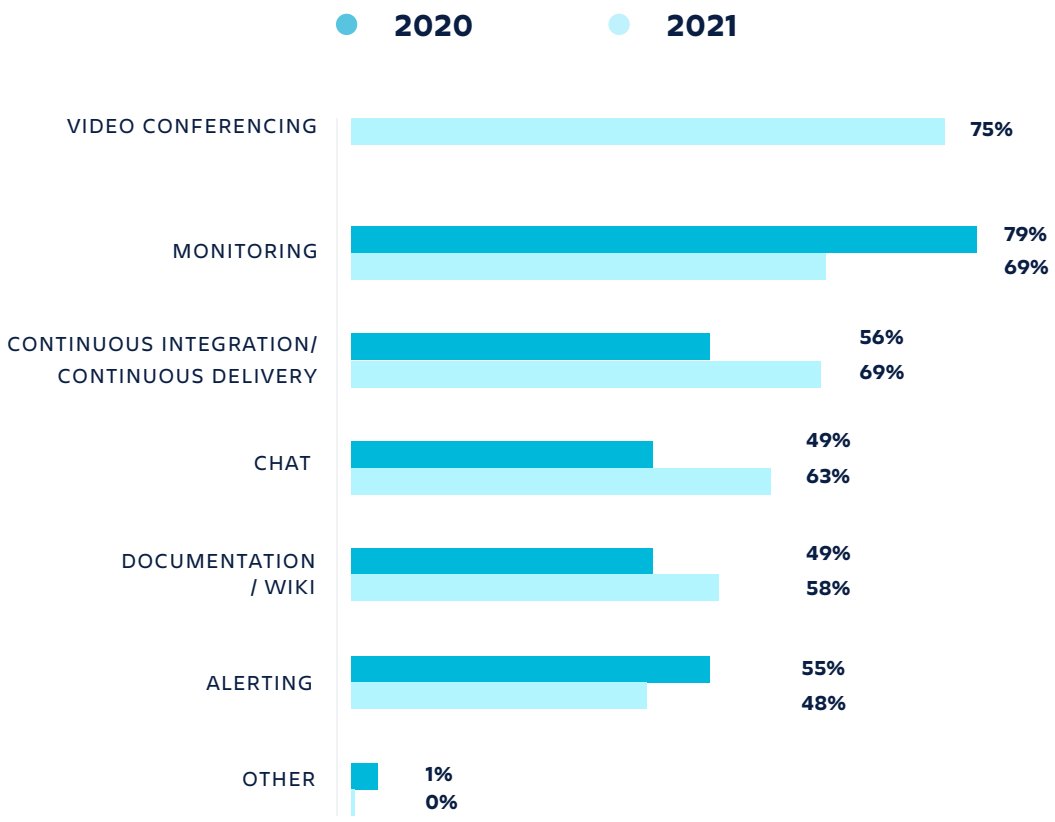


INFORMATION ACCESSED TO DETERMINE FULL IMPACT OF INCIDENT



Use of tooling during the incident

The COVID-19 Pandemic has shifted consumer behavior. Incident management was not untouched by this trend. Video conferencing is now the most used tool throughout the incident management process, followed closely by monitoring, CI/CD tools, and chat.



Other notable findings include the significant increase in usage of Continuous Integration, Continuous Delivery (CI/CD), chat and documentation tools since 2020. Adding CI/CD tooling to the incident management process could indicate that as companies' processes mature, they're seeking ways to be more proactive and shorten incident resolution time. These findings also speak to the need for an integrated tool chain for seamless incident response, reporting, and follow-up. But this could be the result of having a larger Dev audience responding to the survey this year, as compared to last year.

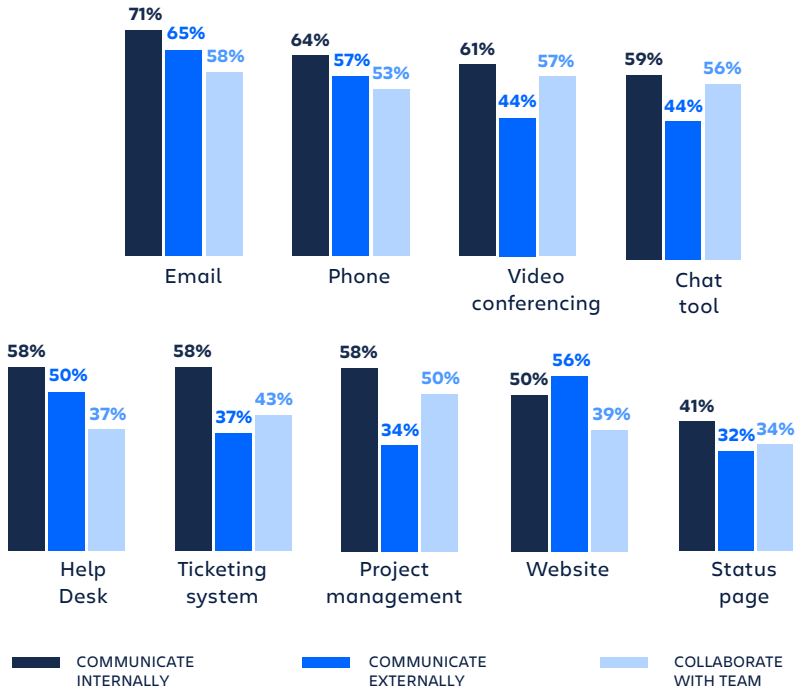
On average, organizations use 3.8 tools throughout the end-to-end incident management process. Decision-makers (4.0) report higher tool usage than practitioners (3.6). This is down from 2020's findings of 5.2 tools to communicate internally, 4.2 to communicate externally, and 4.3 to collaborate with their team during an incident. Since various data points indicate a more mature incident process, it's likely the reduction in tooling is a result of streamlining and consolidating.

Communication and collaboration

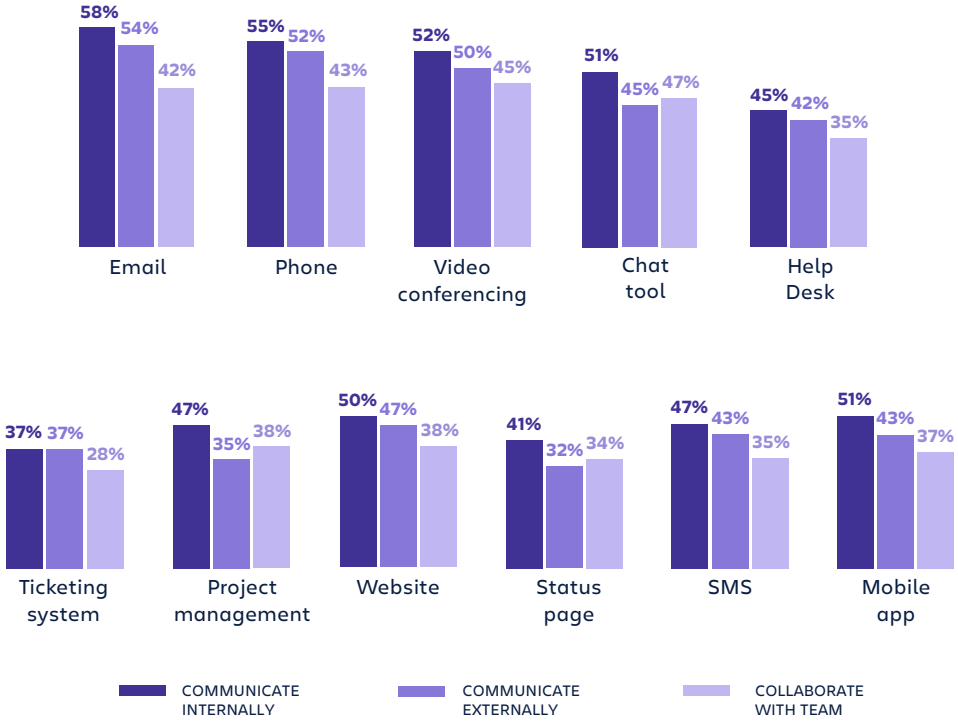
Email is still the most used tool for communication and collaboration but usage decreased by 11-16% over last year. According to the answers respondents gave, software developers may be shifting to chat, using it most for team collaboration (54%) – and nearly as much as email for internal communication (56%). This highlights the demand for ITSM tooling with deep ChatOps integrations.

Another finding that stands out, despite the fact that incident management tooling has increased, usage of nearly all communication tools has gone down since 2020. This could be an indication of communication/screen fatigue as a result of the pandemic, or point to the fact that most respondents are using more integrated tooling with clear audit trails and actionable information, putting less burden on the need for communication.

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

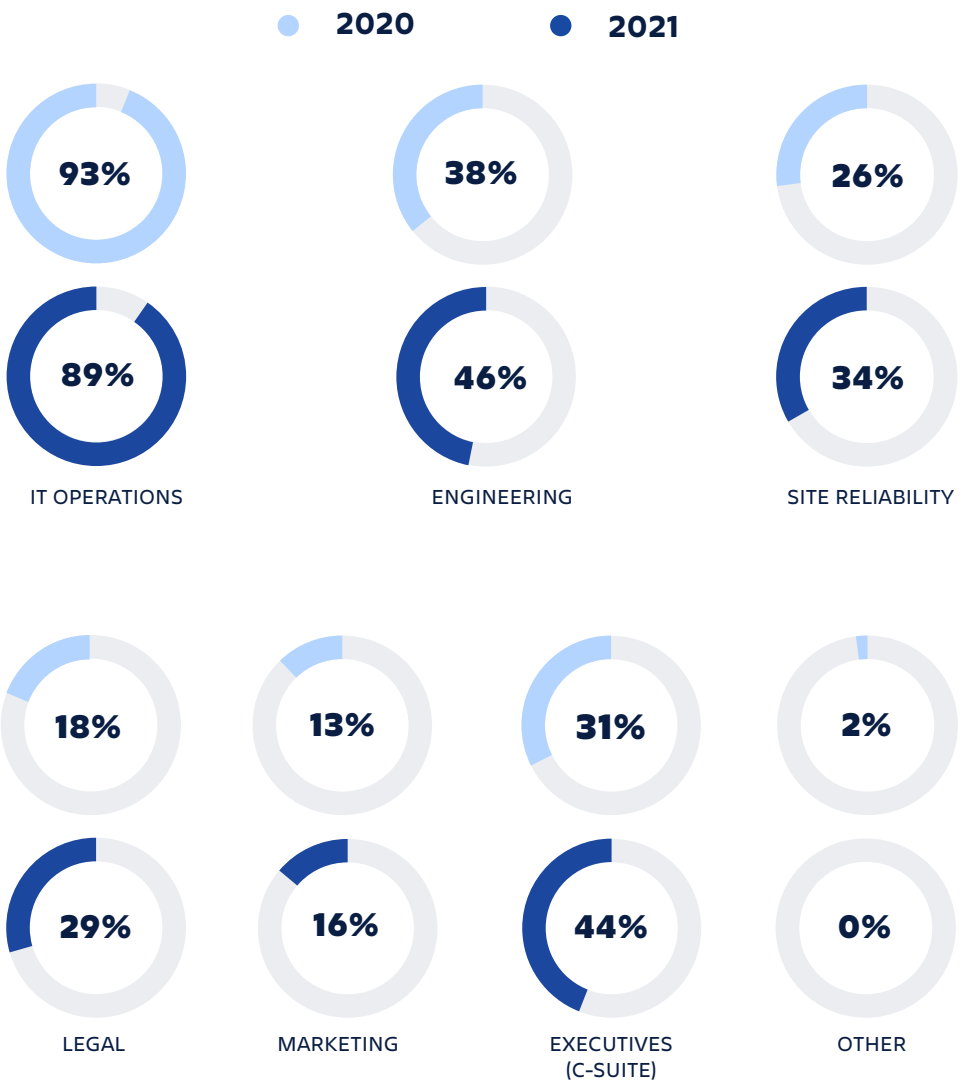
2021


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

Who manages incidents?

Last year's survey found that IT Operations were the most heavily involved in Incident Management, this is still true. But involvement has increased notably across the board – with more involvement from Marketing, Legal, and Executives. This cross-functional involvement could mean there is more focus on transparency and communication with all stakeholders.

Also similar to 2020, IT professionals are more likely to report IT operations involvement (92% vs. 85% of software developers), while Software Developers are more likely to report Engineering involvement (54% vs. 38% of IT professionals).



Who goes on call?

This year IT is still on-call the most with **87%** of survey respondents reporting that IT goes on-call. At the same time, **63%** of respondents reported that Developers were on call too. Only 1% of those surveyed do not have an on-call procedure, and the majority have automated the schedule process through a tool, like Opsgenie. Eighteen percent of respondents are still using manual processes like spreadsheets. Last year, only **93%** of respondents had an on-call process, versus **99%** this year.

WHO GOES ON CALL

87% IT OPERATIONS/ SERVICE DESK

63% DEVELOPERS

44% PRODUCT MANAGERS

1% DON'T HAVE ON-CALL

HOW ON-CALL SCHEDULES ARE CREATED

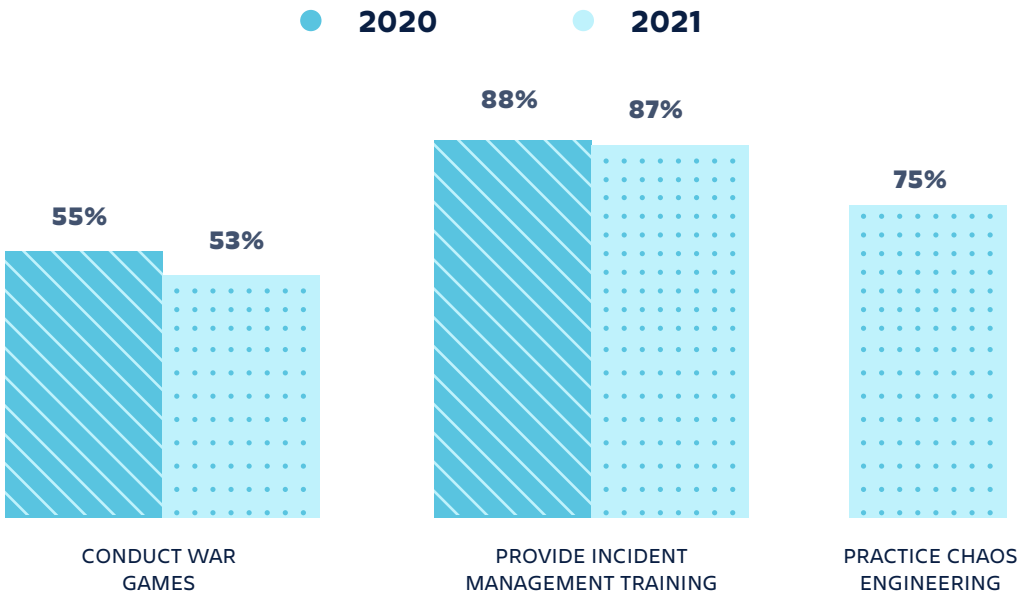
64% AUTOMATED PROCESS THROUGH A TOOL (LIKE OPSGENIE)

18% SPREADSHEET

17% HR TOOLING/ SCHEDULING

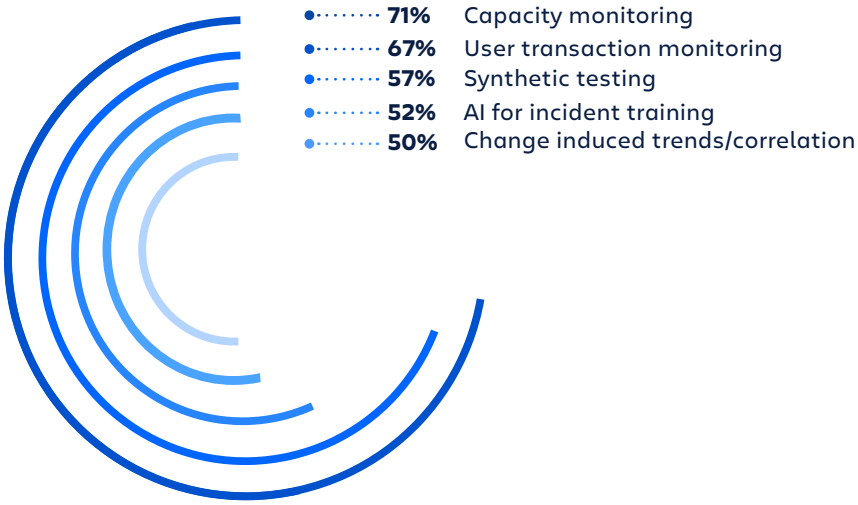
Incident prevention

The majority of organizations **(87%)** provide incident management training. Slightly less reported conducting war games than last year. This year we also asked about Chaos Engineering, which **75%** of respondents participate in. The more tools an organization uses for the end-to-end incident process the more likely they were to engage in war games, chaos engineering, and incident management training.

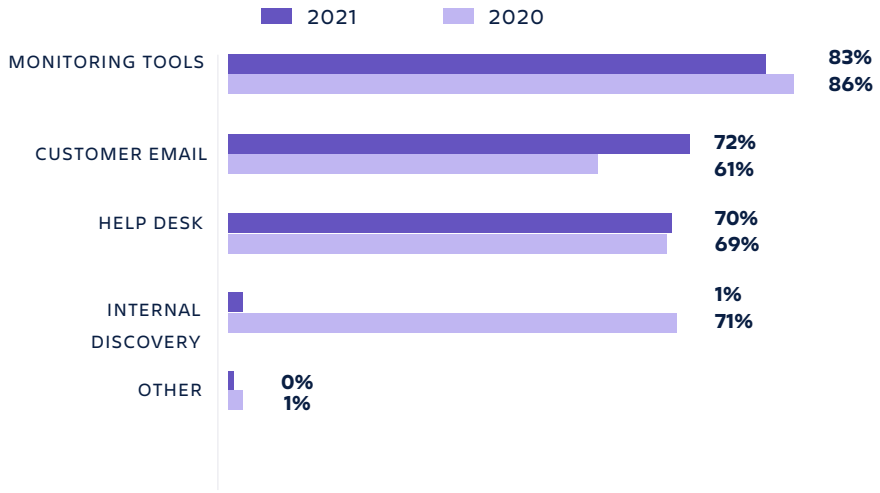


Proactive incident management tools are the norm, with more than 50% using all techniques tested. Capacity monitoring and user transaction monitoring are the most common. Organizations that use AI to trigger incidents are statistically much more likely to report usage of all proactive techniques tested (with the exception of user transaction monitoring, where the difference is directional). Those who use 5+ tools end-to-end are also significantly more likely to use all tools tested. This could indicate that AI is utilized by more mature companies, or that AI empowers these organizations to be more proactive.

USE OF PROACTIVE INCIDENT TECHNIQUES/TOOLS



Similarly to 2020, monitoring tools are used by the majority to discover incidents. Internal discovery has decreased, but this is likely due to a wording change in the questionnaire. In 2020, we referred to “internal/employee discovery” as opposed to internal discovery in 2021.

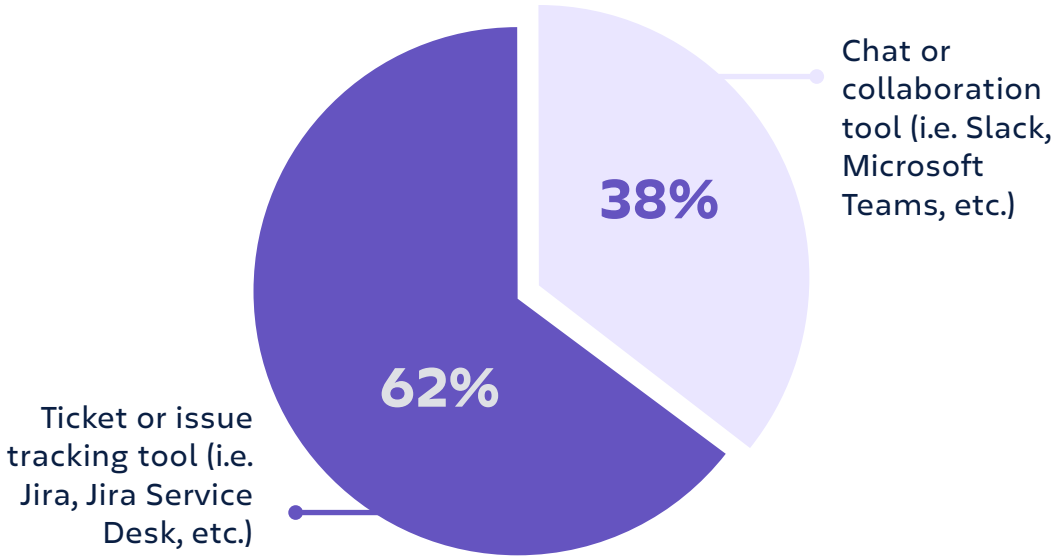


Source of truth during incidents

A two-thirds majority say that ticket or issue tracking tools are the source of truth during incidents. Those who use AI to trigger incidents are especially likely to say the tracking tool is the source of truth (64%) compared to those who don't use AI (50%).

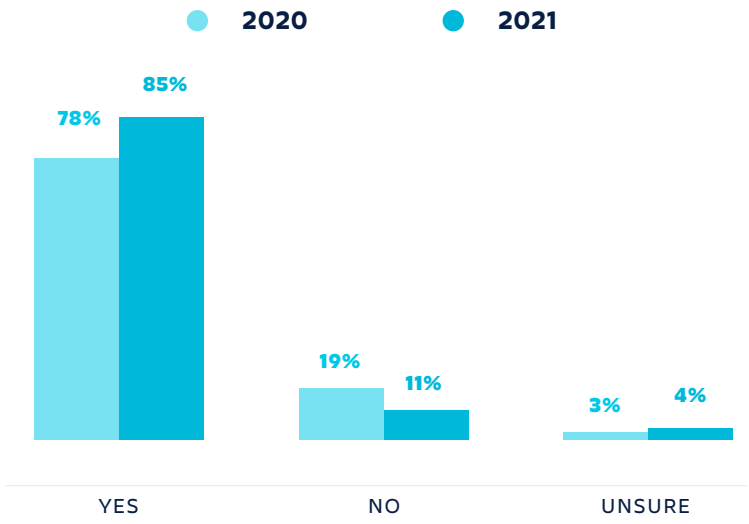
In 2020, 88% were using an issue tracking tool like Jira or Jira Service Management as a source of truth with 65% using a chat or collaboration tool. In 2021, 62% leveraged an issue tracking tool as their source of truth, while 38% used a chat or collaboration tool like Slack or Microsoft Teams. We can't say for sure what caused the shift, but it seems that more and more ChatOps tools are being leveraged for issue tracking.

SOURCE OF TRUTH DURING INCIDENTS

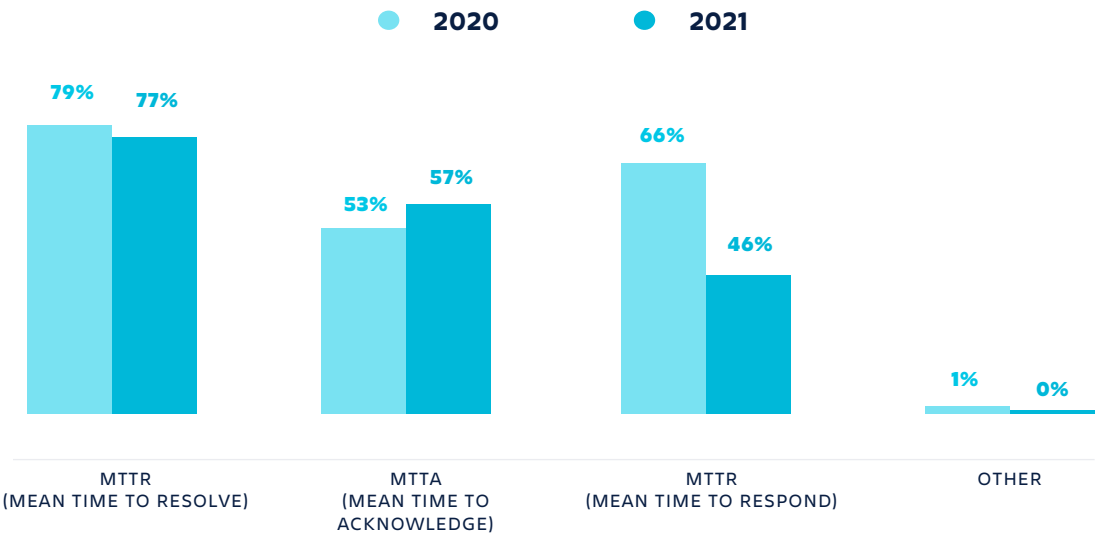


Measuring success after the incident

Similar to last year's findings most run postmortems on incidents. Those who use AI are especially likely to do so (89%). This could speak to the overall maturity of their processes, or indicate that leveraging AI may automate this process for them.



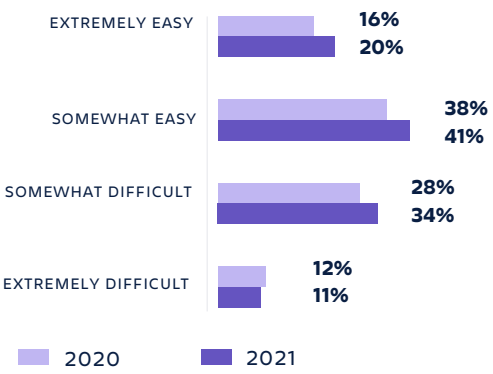
The top measure of success is still mean time to resolve. There is a noticeable decrease in folks paying attention to mean time to respond compared to last year. We asked respondents to provide an estimate for how much each incident costs their organization, the average cost per incident based on their answers comes to $14,985. A study by Gartner found the average cost of downtime to be $5,600 per minute, but cost can vary depending on the size and vertical of a company.



03

Areas for improvement

Main pain points



When asked if it was difficult to get stakeholders involved 61% said it was easy and 39% said it was difficult. Respondents who reported using 5+ tools end-to-end, said they were responsible for both development and operations.

The biggest issue in the incident management process is a lack of full visibility across IT infrastructure. As can be expected, those with fewer end-to-end tools (0-4) are more likely to cite this as a problem (28%).

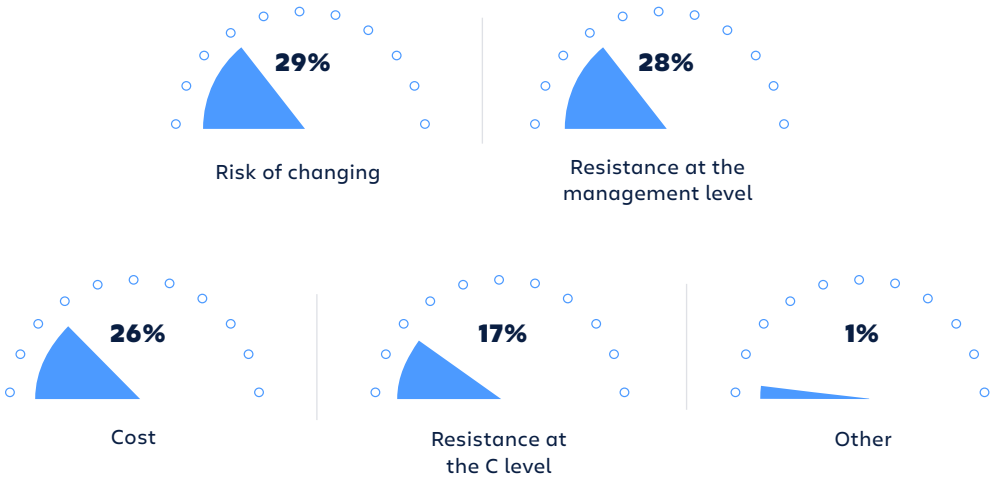
BIGGEST PAIN POINT IN INCIDENT MANAGEMENT

Lack of full visibility across IT infrastructure	24%
Lack of coordination across departments	11%
Lack of integration with a chat tool (Slack, Microsoft Teams)	11%
Lack of context during an incident	11%
Ill-defined processes	11%
Lack of change management /change records	11%
Lack of plans to address incidents	10%
Lack of automated responses	9%
Other (please specify)	1%

Barriers to change

We wanted to get an idea of what respondents felt prevented change, or were barriers to improving the process. Respondents cited change risk, management resistance, and cost as the most prominent – with c-level resistance being less of a concern.

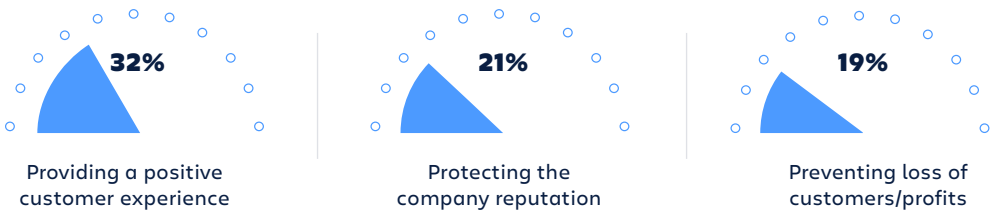
BARRIERS TO IM IMPROVEMENT OR CHANGES



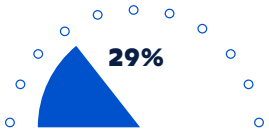
What influences change?

Overall the main driver to adapting a quality incident management process is providing a positive customer experience, followed by protecting the company reputation with loss of profit being the lowest factor. Software Developers place slightly more importance on preventing loss of customers/profits than IT professionals (23% say this is a driver, compared to only 15% of IT professionals).

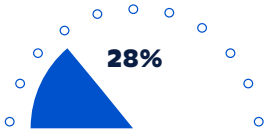
TOP DRIVERS OF INCIDENT MANAGEMENT



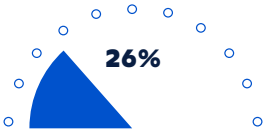
TOP BARRIERS TO INCIDENT MANAGEMENT IMPROVEMENT OR CHANGES



Risk of changing

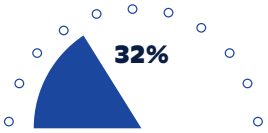


Resistance at the management level

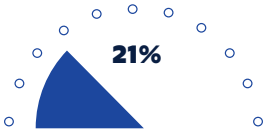


Cost

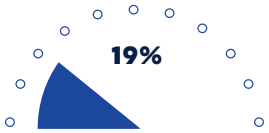
DRIVERS OF INCIDENT MANAGEMENT



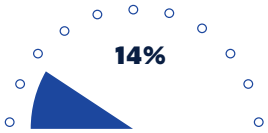
Providing a positive customer experience



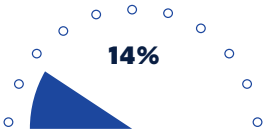
Protecting the company reputation



Preventing loss of customers/profits



Compliance and auditing



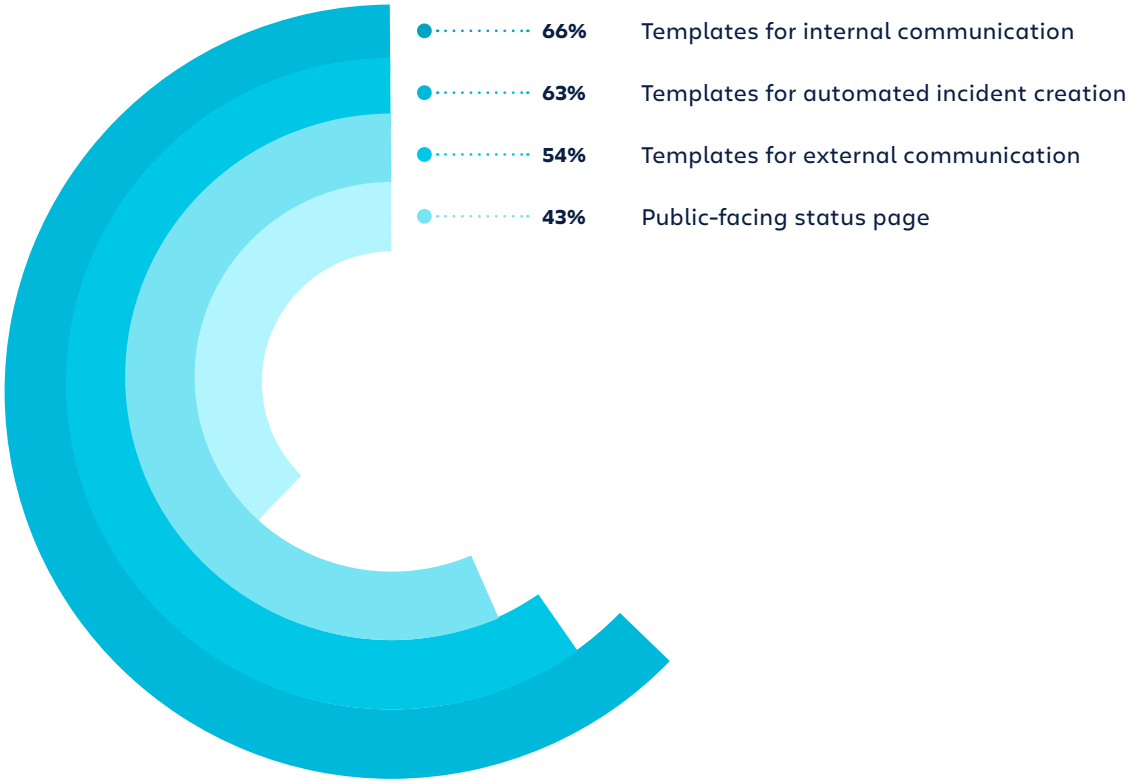
Company culture & philosophy

04

Increased focus on automation

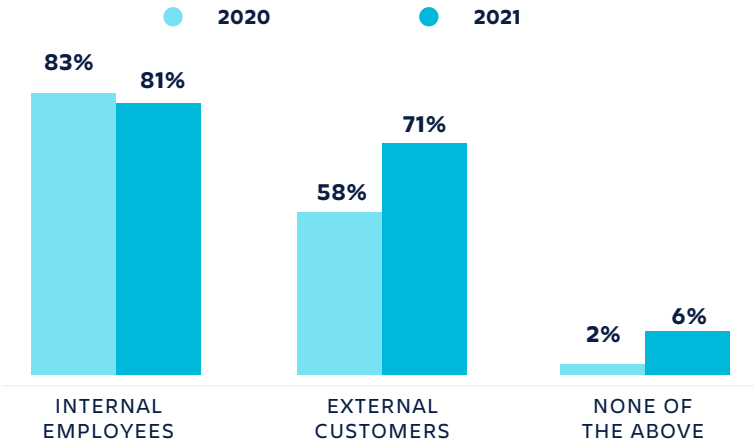
Automation

It's no surprise that automation continues to be a big focus, especially for internal communication and incident creation. More than half have automated templates for external communication as well. Decision-makers are more likely than practitioners to report automation of templates for internal communication (71%) and external communication (58%). Those who report using 5+ tools end-to-end are more likely to have automated. It's no surprise that those who automate incident creation with templates (68%) also report that it's easier to get stakeholders involved.

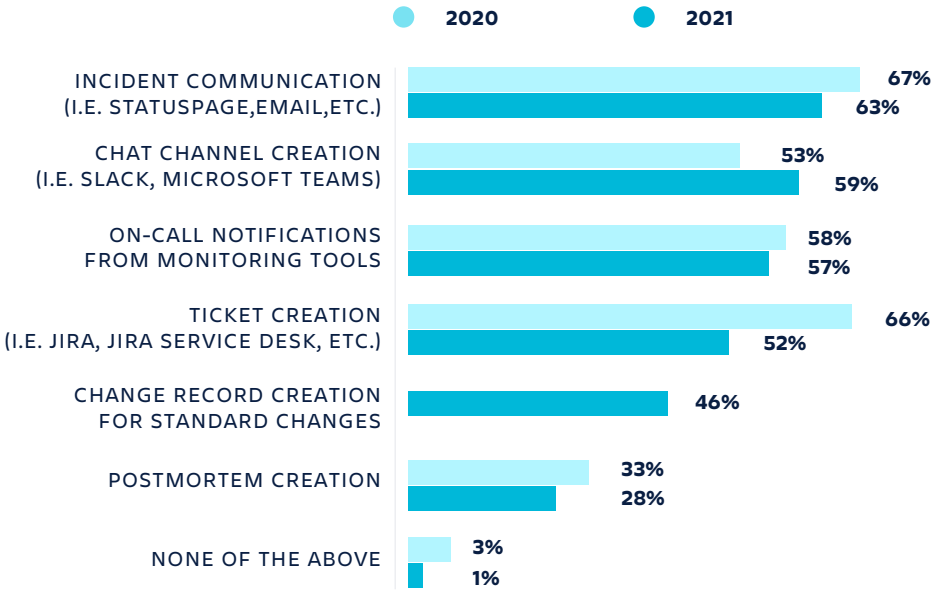


The automation of ticket creation has decreased significantly, from 66% in 2020, to 52% in 2021. One possibility for this decrease, is that oftentimes when automating ticket creation, it's not implemented or filtered properly which leads to a lot of noise. Organizations that use 5+ tools are more likely to automate all communications and processes tested. Those who report easy stakeholder communication are more likely to report automated communication with internal employees (85%) and automated processes for on-call notifications (62%), incident communications (68%), and chat channel creation (62%).

AUTOMATED INCIDENT COMMUNICATIONS

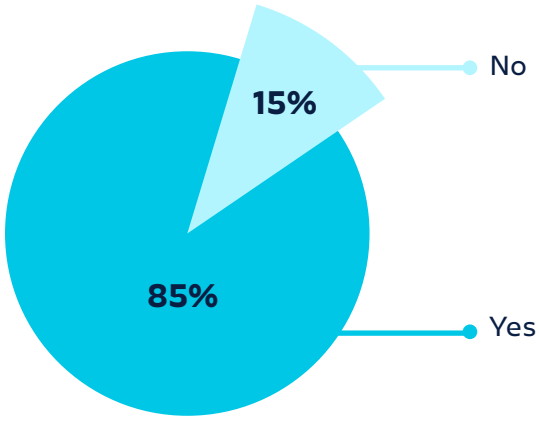


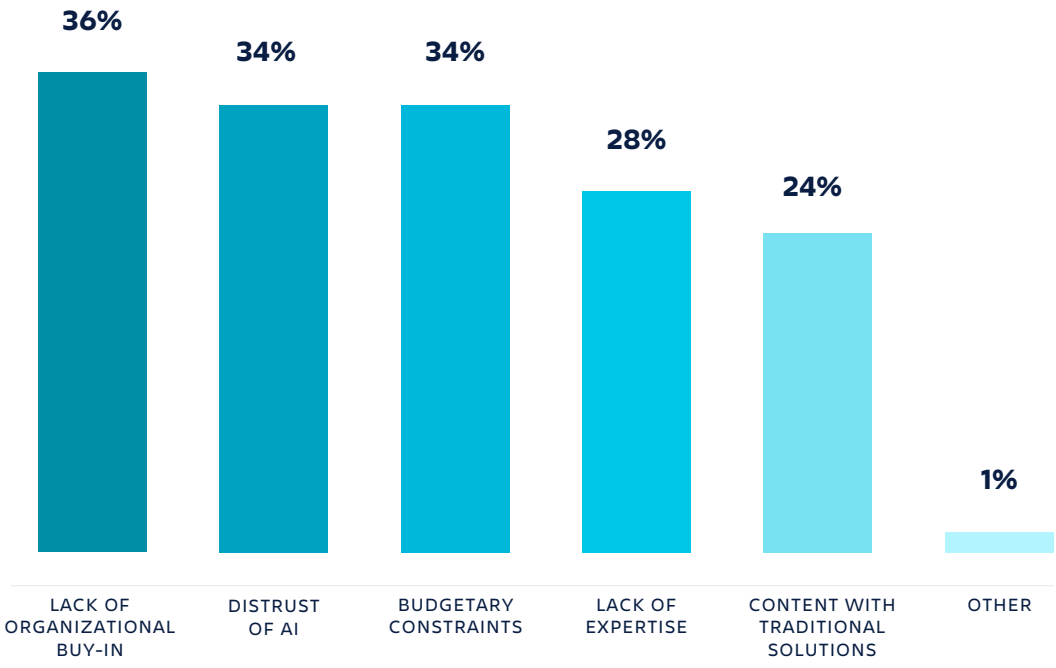
AUTOMATED INCIDENT MANAGEMENT PROCESSES



The vast majority of respondents reported leveraging a tool that uses AI to trigger incidents.

- 85% report using on incident management tool leverages AI to trigger incidents.
- Of those who do not use a tool, lack of organizational buy-in, budgetary constraints, and lack of expertise are the top barriers.



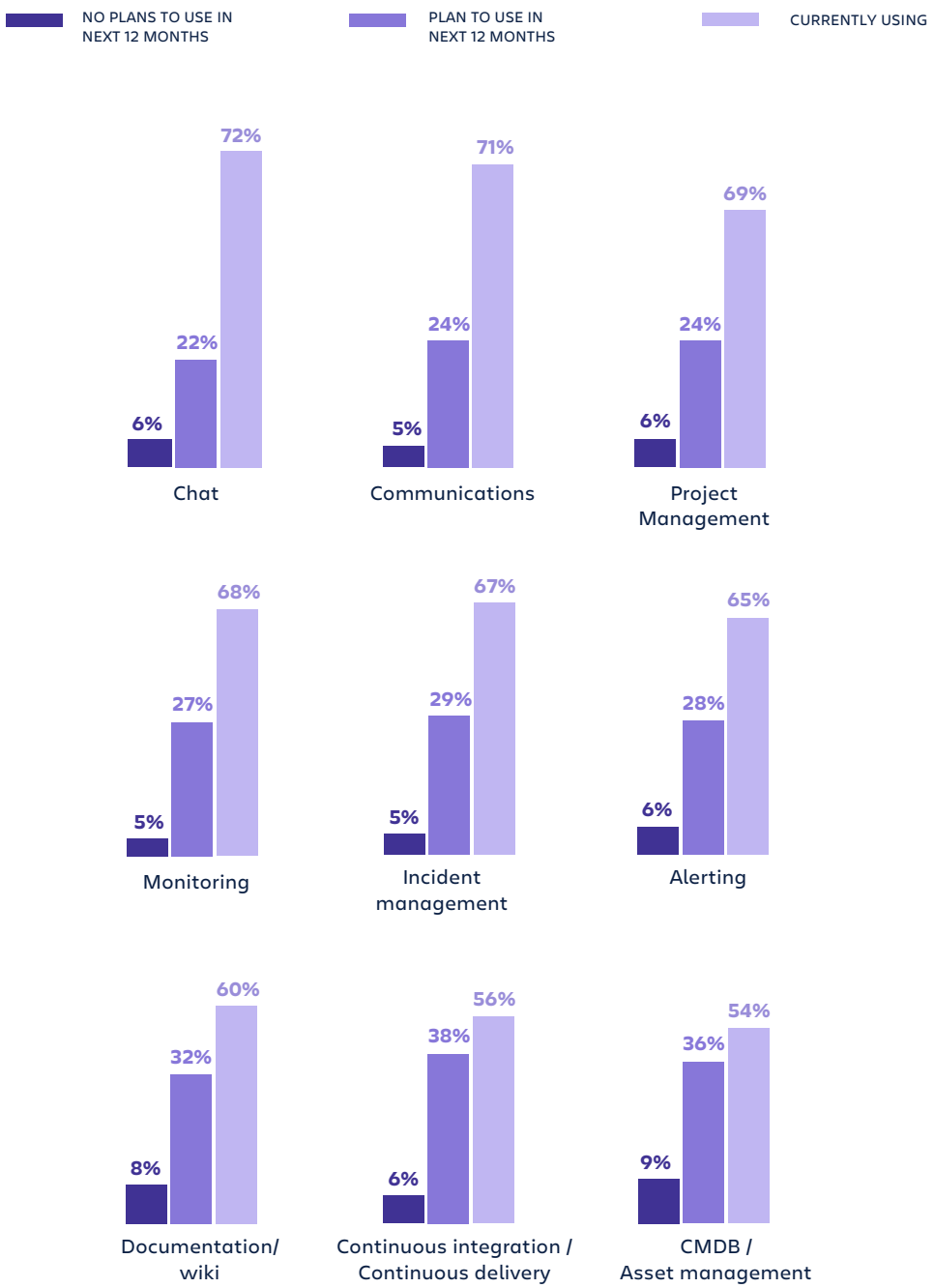


05

What's next?

Tools used, versus tools planned

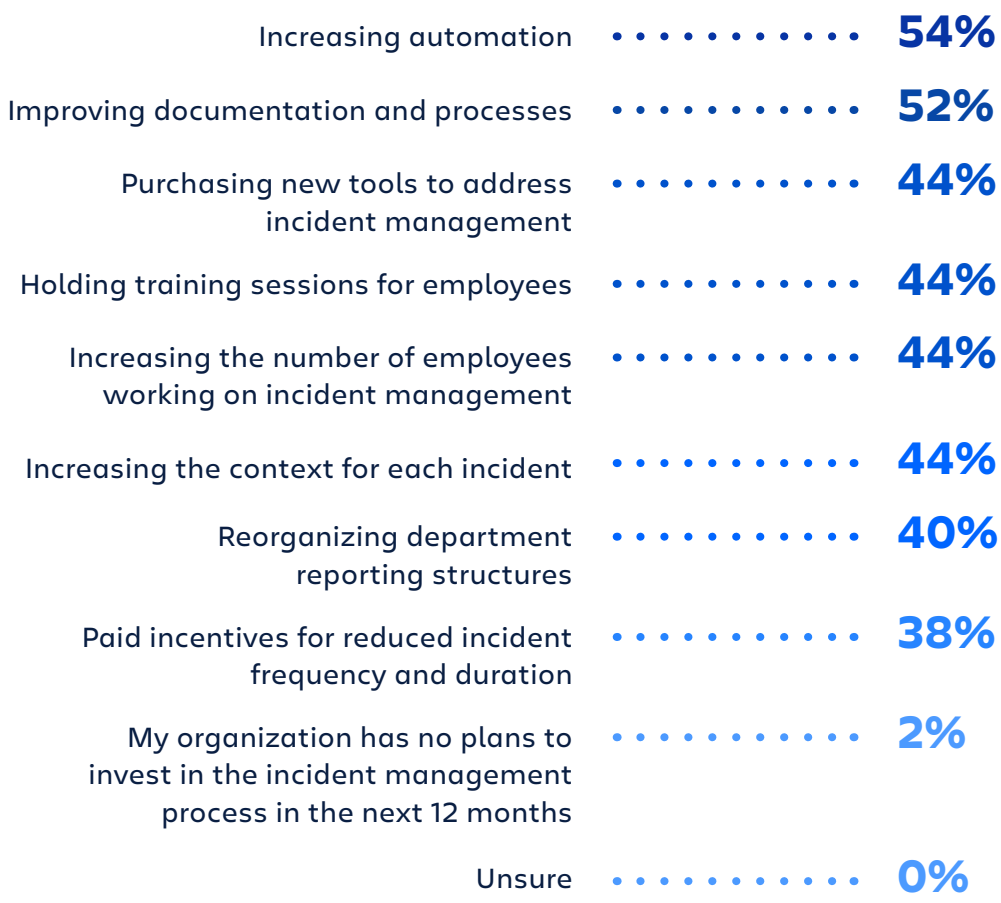
Two-thirds or more of organizations report using the following tools currently: alerting, incident management, monitoring, project management, communications, and chat. Of those who do not use tools currently, most plan to within the next 12 months.



What's next for incident management?

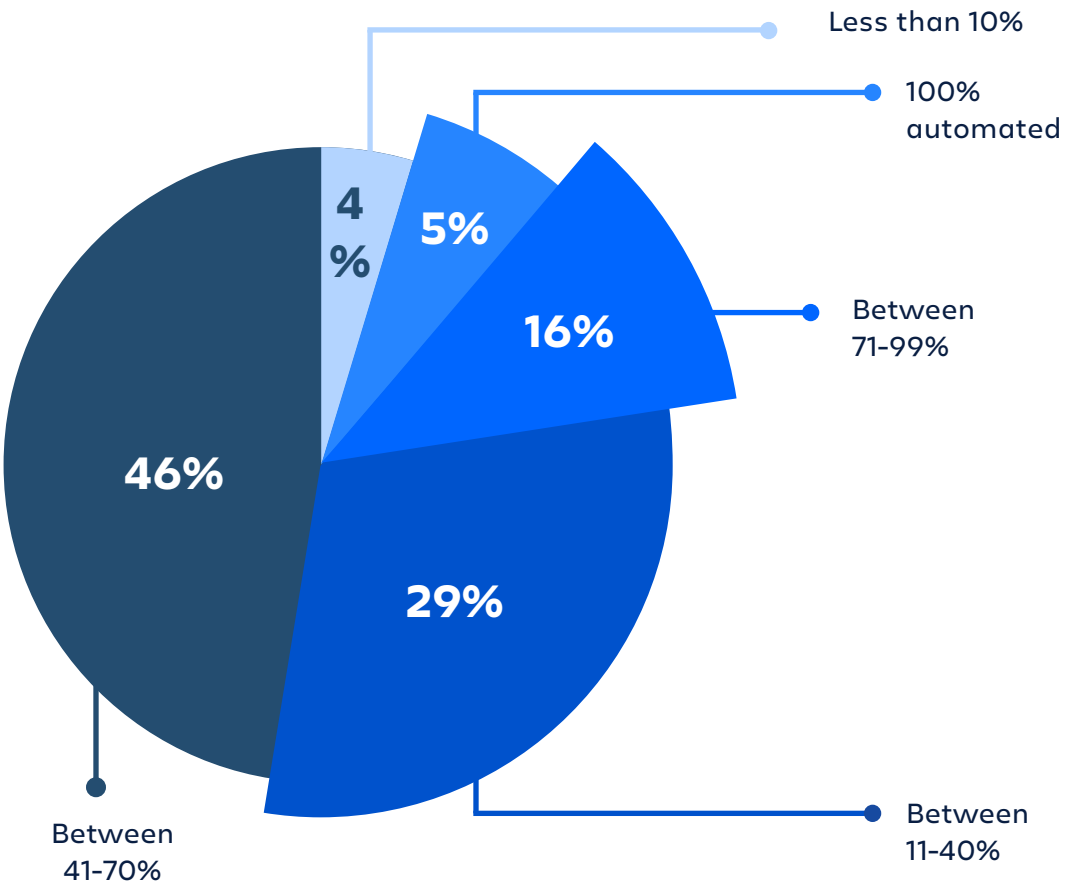
Looking ahead organization are prioritizing increasing automation (54%), and improving documentation and processes (52%). Both of these tactics can cut down on incident resolution time, which supports the finding that mean time to resolve is currently the most used metric for success. Organizations using 5+ end-to-end tools are more likely to invest in all areas the survey asked about. It's no surprise that organizations with higher revenues of $100.1M+ are especially likely to purchase new tools (49%), as they have the resources to do so.

STRATEGIES ORGANIZATIONS WILL INVEST IN WITHIN THE NEXT YEAR



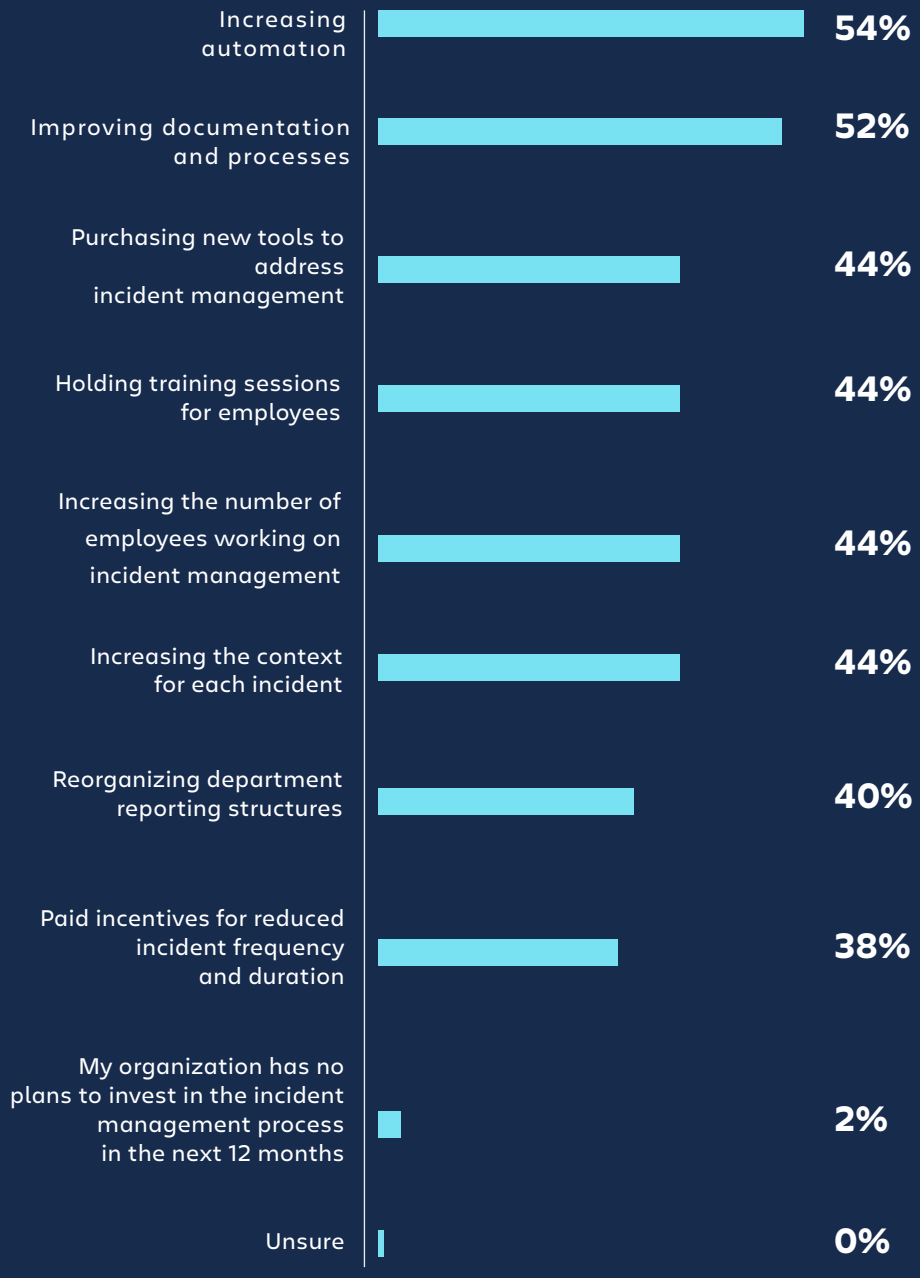
INCIDENT MANAGEMENT PROCESS AUTOMATION

12 MONTHS FROM NOW



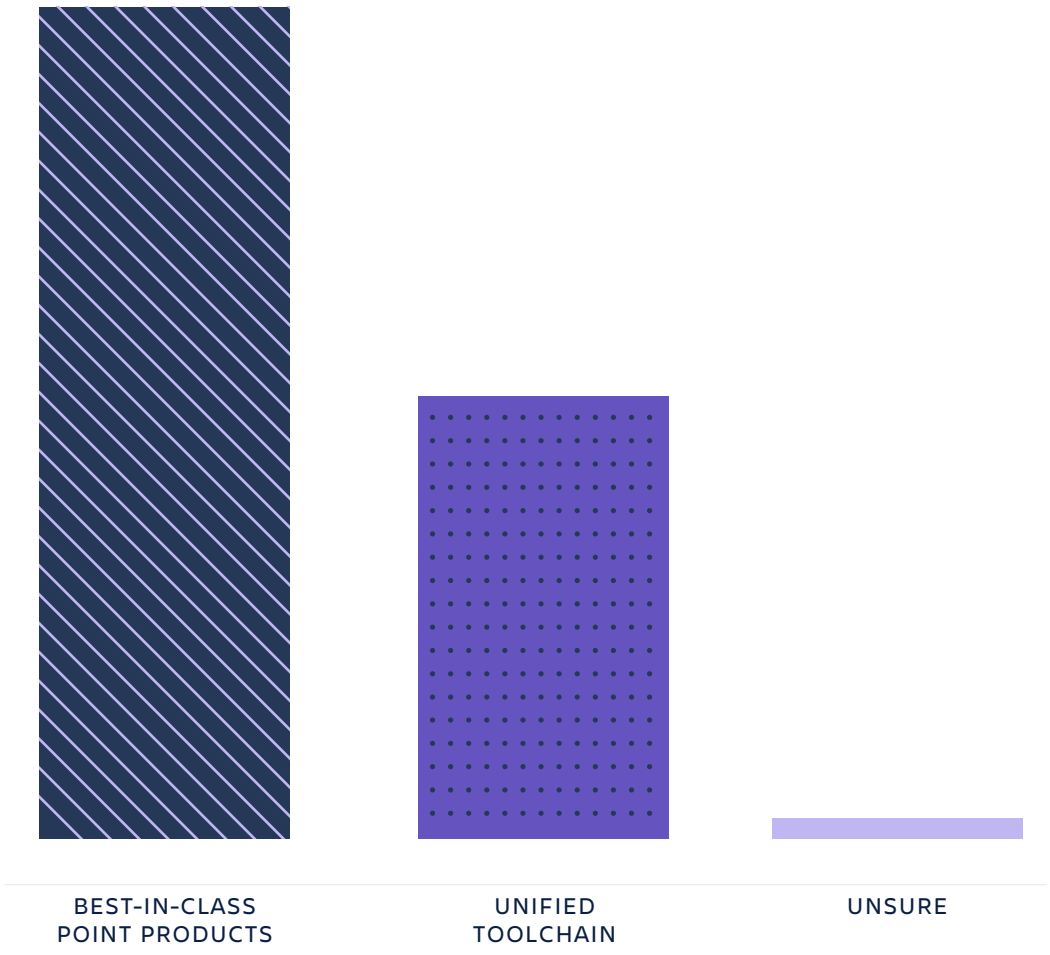
* This chart shows what percentage of processes respondents plan to automate.

Organizations will focus on automation of incident management in the future, but few expect to reach over **70%** automation.



While increasing automation in the incident management process emerges as the top strategic plan for the next year, only 5% expect a fully automated process within the next 12 months. Most expect between 11-40% (29%) or 41-70% (46%) automation in the next year.

Six-in-ten prefer best-in-class point products over unified toolchain to handle incidents. Those who are responsible for both developing and operations are especially likely to prefer best-in-class (66%). This means that they are more likely to choose different products that integrate well together, rather than choosing a single product that does it all.



In conclusion

Now, with two years of incident management benchmarking data to reflect on it's safe to say that there's a large focus on maturing the incident management process, mostly driven by providing a good customer experience. While demand placed on infrastructure and online exploded due to folks spending more time than ever at home, it also increased the need and rapidity for which organizations needed to digitally transform and scale.

Key trends to look out for in 2021 are changes in collaboration methods and an even larger emphasis on automation. While this year's more even split between IT folks and Dev folks as respondents certainly contributed to some of the changes we saw reported, like the decrease in use of monitoring tools, and ticketing as a source of truth, most of our key findings were not a surprise. As we emerge from this pandemic and folks slowly have the option to return to the office, it will be interesting to see what impact that has on our communication and consumer habits.

Want to dig deeper?

www.atlassian.com/incident-management

Have questions?

Contact us at sales@atlassian.com

ATLASSIAN