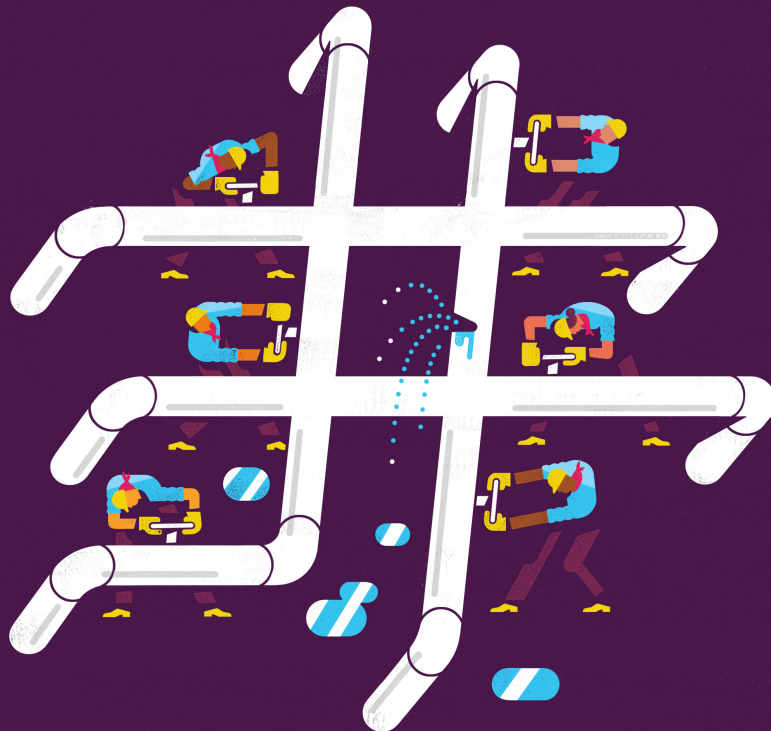


Transform your incident command center

Minimize chaos, resolve problems faster and
prevent future incidents with Slack



Command center 101:

1. Introduction: Make sense of all the noise	3
2. Alert and respond in real time	5
Mitigate, monitor and manage	5
Monitoring tools	5
Incident response tools	6
Service management tools	7
Sync up and talk it out	8
3. Automate and simplify your response	9
Organize each incident before it escalates	10
Protect sensitive data	11
4. Keep information organized and minimize distractions	12
Set channel topics, pin updates and start threads	13
5. Accelerate incident reviews	16
6. Get started right now	19



1. Make sense of all the noise

You're humming along on a Tuesday morning when you get a ping about an incident. The usual feelings of panic, adrenaline and stress sink in. From the looks of it, you know there will be pressure on all sides to fix this quickly—from your team and boss to the executives and business stakeholders.

Not to mention customers, whose expectations align with a digital world that's open 24/7. Indeed, no issue is too small to cause frustration, from a small line of broken code to site-wide outages. The data analytics company Splunk reports that many companies experience incidents like these more than once a week, with each offense costing more than \$100,000—rounding out to roughly \$500,000 lost each month.

Million-dollar mistakes

50%

of outages cause substantial financial, operational and reputational damage

62%

of businesses report losing more than \$100,000 for each severe downtime, with 15% losing over \$1 million

Source: Uptime Institute's 2021 Global Data Center Survey (via [Facility Executive](#))

Disparate email threads, instant messages and video calls create unnecessary silos and convolute efforts to mitigate the incident. Getting the right people involved is slow-going, and you have to share an update every time someone new joins the conversation, derailing your troubleshooting efforts. Transparency is nonexistent, and scattered data only feeds the chaos.



1. Make sense of all the noise

If and when you fix the problem, you have to wait to get the entire group in a meeting to cobble together a postmortem story across teams, emails, video recordings and messages. Preventative measures and lessons learned often take weeks to implement, and your engineers get pulled off important projects to spend unnecessary time debriefing your Ops team. Everyone is stressed, frustrated and exhausted due to wasted time and costs, and slow resolutions.

Every incident is unique, extraordinary and often unpredictable. But the good news is that you and your teams can tackle incidents with less stress, minimal chaos and fewer interruptions with Slack. Whether yours is a fast-growing 2,000-person company like Iress or a Fortune 50 company like Target, **Slack transforms incident management right out of the box, acting as a single command center for detection, containment and post-incident analysis.**

Preventing incidents with automation

“Before Slack, we had 10 to 20 release incidents a month due to miscommunication. Now we automatically communicate big release changes in Slack, and it’s been four months without incident.”



Antoine Millet
Head of IT operations
Veepee



2. Alert and respond in real time

Integrate monitoring and incident response tools

Having all your tools and communication in the same place enables a faster response and eliminates the time and distraction costs of context switching. To reduce each event's impact on both customers and the company, teams can leverage Slack's **automation capabilities** to quickly respond to issues and shorten incident resolution time.

Mitigate, monitor and manage

By using automation tools and integrations to create a central location where all stakeholders can quickly view relevant context, your teams have the power not only to shorten the incident but to reduce its potential impact. Plus, when your people can still use the tools they prefer, they're inspired to contribute more, increasing the likelihood of cross-department collaboration.

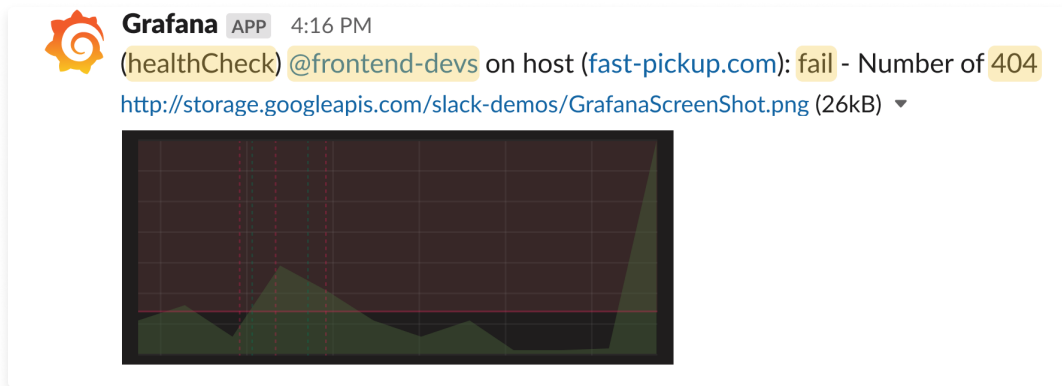
Monitoring tools

Real-time alerts give teams visibility to triage and take action.

- **Ensure even the smallest incidents don't slip through the cracks** by automatically piping critical alerts and notifications directly into Slack channels with [Grafana](#). Collaborate across teams to quickly resolve issues.



2. Alert and respond in real time



- **Track system-wide activity** with **Datadog** notifications. If needed, declare an incident with the `/datadog` incident slash command, which will open a modal directly inside Slack and automatically create a dedicated Slack channel.
- **Make it easier for your teams to manage pretty much any operational activity**, from monitoring and system management to CI/CD workflows with **AWS Chatbot**.
- **Stay on top of potential risks** to applications, services and infrastructure with **Dynatrace's** problem-notification integrations, which enable DevOps teams to respond swiftly to service failures and requests.
- **Find and fix problems faster** with **New Relic** by giving developers, engineers, operations and management a clear view of what's happening in your software environments.

Incident response tools

Speed up incident response by getting the right people in the right place quickly.

- With **PagerDuty**, you can **seamlessly manage and track situations before they escalate**, using Slack to connect all the right stakeholders. Proactive notifications and status dashboards **bridge communication gaps** found among dispersed teams.
- Plan ahead for service disruptions and **stay in control** during inevitable incidents with **Opsgenie**, which helps your team design actionable alerts, manage on-call schedules and escalations, and **facilitate communication to enable resolution**.
- The bi-directional **VictorOps** integration gives your engineers **visibility into the entire payload of your incidents**. Send notifications for incident actions and **notify teammates of on-call shift changes** right in a designated Slack channel.



2. Alert and respond in real time

Service management tools

Give your support team the context they need to assess customer impact by connecting support and service tickets to your incident data and response workflow.

- With **Salesforce Service Cloud**, you can **easily manage swarms with cross-functional experts** and send messages posted in Slack directly to the associated Salesforce records.

The screenshot shows a Slack channel named "# billing-support-team". A message from the "Service" app at 12:42 PM states: "A new Case has been assigned to the billing-support team queue". Below the message, it says "Case | 938771" with two buttons: "View Case" and "Take Case Ownership".

Overlaid on the right is a "Begin Swarming" modal. It contains the following fields and options:

- Name Swarm Channel:** # swarm-case-9328771
- Help needed (optional):** Unusual spike in chargebacks for Capricorn Coffee
- What's this swarm about?:** (Empty text field)
- Record to Swarm Around:** 9328771 (with a close icon)
- Expert Finder:** Payments (with a close icon) and Credit Card Processing (with a close icon)
- Swarm Owner:** Jessica Alcala (with a close icon)
- Start Swarm:** (Green button)

- **ServiceNow** helps you create custom incident workflows and customize alerts for record changes in Slack channels. **Search and share records**, and take action as necessary.
- The **Jira Service Management** integration allows your teams to create and preview issues in Slack, **fetching the key details they need to stay focused**. Powerful filtering to selected channels, projects, issue types and priorities cuts out the clutter.



Find resolutions 75% faster

“[With Slack,] we’ve reduced the mean time to resolution to under five minutes. It’s been phenomenally successful in a very short period of time.”



Paul Whyte

Former head of systems engineering
Vodafone

It previously took the telecommunications company 15 to 20 minutes to find the root cause of incidents. After switching to Slack, the team dramatically reduced its mean time to resolution, in part due to Slack’s PagerDuty integration.

Sync up and talk it out

To stay nimble and facilitate painless communication, your support teams can automatically spin up meetings as needed using the [Zoom](#), [Microsoft Teams](#) or [Webex](#) integrations in Slack.

If video chatting isn’t your cup of tea, you can re-create quick discussions with **Slack Huddles**, a lightweight, audio-first way to communicate inside an incident channel. When a huddle is open, any member of the channel or DM can come and go as they please. Anyone present can share their screen, and others can draw on it. There’s also an option for live captioning (just make sure you share back key findings and decisions in the main incident channel so everyone has visibility).





3. Automate and simplify your response


Customize shortcuts any way you want

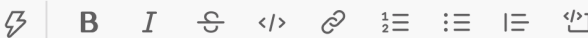
Slash commands act as shortcuts for specific actions in Slack. Depending on what you need, these commands can initiate simple message responses, kick-start complex workflows or summon integrations with external services. If you don't see a shortcut that fits your team's needs, you can include custom slash commands as part of a Slack app created for your workspace.

A slash command also has the power to spin up a **dedicated incident channel** in Slack and post a message with relevant documentation links. You can standardize channel naming to let employees know a channel's purpose from the get-go, increase discoverability and encourage cross-team collaboration.

 **Zoom** APP 3:01 PM
A Zoom meeting has started
Join the call to meet the response team.
[Join](#)

 **Incident Bot** APP 3:15 PM
This incident is **Paused**

 **Harry Boone** 3:15 PM
set the channel topic: State: Paused, **S1** S1, 🚨 @Harry Boone





3. Automate and simplify your response

While there are a variety of ways to scale incident channels as issues grow, channels are even helpful when they're used for only a short period of time by a handful of people. These single-purpose channels isolate important conversations and help everyone focus on quickly mitigating issues.

Everything in its place

“We have a custom integration that spins up a Slack channel with the ticket number and automatically starts a Zoom call for key stakeholders. Engineers don’t have to answer calls or monitor another tool. They see everything in real time in Slack.”



Matt Davis
Principal engineer
Red Ventures

The media company’s telephony team averages millions of calls per day, which meant Davis often woke up to 100,000-plus emails if something blew up overnight. Now it’s all streamlined in Slack.

Organize each incident before it escalates

Even with the best intentions, someone looking to report an incident can unintentionally cause information silos and create confusion around prioritization, stifling productivity. With Slack’s **Workflow Builder**, anyone can quickly submit a form in a centralized channel to report a potential incident. The details are then properly organized and automatically shared with the designated team channel to assess severity and take action.



3. Automate and simplify your response

Some other handy ways to use Workflow Builder for incident management:

- **Security:** Data security or privacy incident reporting
- **Operations:** Frontline worker incident management
- **Facilities:** Office workspace issues or health notifications
- **Product:** Incident triaging and post-incident reviews
- **Customers:** Report issues in-channel with [Slack Connect](#)

There's a bot for that

Taking the power of automations one step further, you can use the **Slack API** to build your own custom bot with a face, name and personality, just like a human colleague. Every organization has its own incident management process, and custom apps complement unique processes, toolsets and communication styles.

For example, Netflix integrated a suite of various crisis management tools into a custom Slack app called [Dispatch](#). The app was so successful within Netflix that it open-sourced it so other companies could automate their own incident management processes.

Protect sensitive data

For large-scale or complex incidents or those that might contain sensitive data—say, a health organization working with patients—companies can create private channels that follow the same naming convention as the main channel. With the “**share message**” feature, employees can copy key messages from the main incident channel to these auxiliary channels as needed, where conversations involving sensitive data can occur with a pre-approved subset of people.

For added security, **Slack Enterprise Grid** has the option for multiple workspaces, and each workspace can have different access controls (i.e., different people who are allowed to access it). This way, everyone at the company might be allowed in your Main workspace, but only a subset of people would have access to a Sensitive Data workspace. This is critical for those vendors and partners you work with most often, making it not only more secure but easier to administer and manage.



4. Keep information organized and minimize distractions

Increase focus during troubleshooting for faster resolution

To build proper team structure and bring in the right people at the right time to solve an incident, it can be helpful to designate an **incident commander**, or IC.

The role of the incident commander

“The role of an Incident Commander (IC) is like that of an orchestra conductor, coordinating and directing the work of the team. During an incident, everyone working on the incident works for the Incident Commander, regardless of their titles in the organization. The Incident Commander sets the overall direction and specific priorities of the incident response; if tough choices need to be made during an incident, the Incident Commander is the person who makes them.

Although seemingly old-fashioned, this command-and-control approach helps mitigate and resolve major incidents as quickly and efficiently as possible. It’s similar to the structure used by fire departments and other emergency response agencies that routinely deal with emergencies, day in and day out.”



Brent Chapman
Principal consultant
Great Circle Associates

Brent Chapman helps online businesses prepare for, respond to and learn from emergencies, working from a strong background in IT infrastructure and SRE. He developed the incident management practices for both Google and Slack, which both companies still depend on.

Once there’s a designated incident channel, the IC starts pulling in subject-matter experts who can investigate, troubleshoot and deploy technical fixes. Much like you @mention any other member of your workspace, you can @mention a **user group** to pull an entire team into a channel at once—and then collaborate with whoever’s available.



4. Keep information organized and minimize distractions

Often, when you're in the middle of troubleshooting, every new person who joins interrupts the conversation to get caught up, derailing the solution. This is amplified during major incidents, with everyone trying to make sense of the noise, side conversations and final decisions. With Slack, every newcomer can quickly scan the channel history to get a summary and full context, eliminating disruptions and streamlining the process.

Set channel topics, pin updates and start threads

The IC might also pull in a customer-experience-team liaison to connect engineers with high-value impacted customers and an executive-team liaison for high-profile or urgent incidents. From there, a **channel topic**, which is visible at the top of the incident channel, helps keep new responders up to speed and can serve to identify both severity and status.

The IC can also take advantage of a **pinned message** to provide the team with a quick snapshot of the most essential information or pressing needs. Pinned messages stay in the conversation header and are accessible to all members of the channel. You can also add bookmarks and folders to organize useful links and easily update any content as needed to make sure everyone has the latest intel.

inc-043-mobile

• Severity: S1 S1

Today ▾

Timestamps

- Start of issue: 4/29/2021 6:53:09 AM
- First automated alert: 4/29/2021 6:53:09 AM
- First human report: 4/29/2021 6:53:09 AM
- Start of Incident Response: 4/29/2021 6:53:09 AM
- All Clear was called on 4/29/2021 at 1:44:57 PM

Summary

Service unavailable in multiple geographies. Working the with provider to determine if the last patch update caused the issue.

Edit

1

Lisa Zhang 10:55 AM

Is there a reason this is a Sev1, even though there seems to be no customer impact?

4 replies Last reply today at 11:36 AM

Zoe Maxwell 11:00 AM

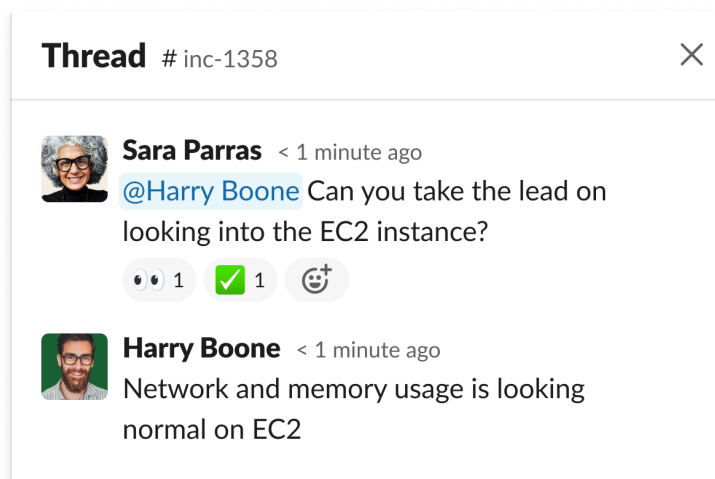
Seeing too many things hardcoded...need to address after we fix

7 replies Last reply today at 12:11 PM



4. Keep information organized and minimize distractions

With the appropriate response team at hand, the IC can assign clear actions, and new responders can get up to speed by scrolling up to see previous discussions and decisions. When every second counts, emoji reactions make it easy to scan for status updates. Teams align on which emoji indicates what, like eyes 👁️ to signify “I’m looking at this”, *thumbs up* 👍 to say “I agree”, and *checkmark* ✅ to indicate “This is done.” They can even create their own incident-specific emoji to further customize the response.



As we all know, emergencies rarely wait for the 9-to-5 window, so this gives everyone involved a quick holistic view of all communication, even during off-hours on mobile devices. Other stakeholders can follow along in the channel and see what fixes are being implemented and when without slowing down the process.

Emoji can also delineate who is working on what; for example, the IC could mark themselves with a *helmet* 🛑 symbol, both in their status and in the channel description, so others can see at a glance who’s running point. For teams with multiple incidents running simultaneously, an IC can name which one they’re responsible for in their user status, which anyone can view by simply hovering over their status emoji.

To avoid cluttering the main channel, **threads** help you create organized discussions around specific messages. You can spin a thread off any message as a powerful way to provide a quick and easy place for parallel investigations and to focus on a particular subject. This also ensures you don’t flood the channel with every single message (and response).



4. Keep information organized and minimize distractions

The screenshot shows a Slack interface. On the left, a pinned message from Lisa Zhang states: "We have determined that the issue was caused by an unanticipated spike in our servers. We are working with our cloud provider and marketing team to see how the short-term. Next update will be in 15 minutes." Below this is a PagerDuty alert for a high request response time on the Shopping Cart API. The alert includes details like assigned person (Lisa Zhang), urgency (Low), and a meeting URL. A thread on the right shows a discussion between Sara Parras, Harry Boone, and Zoe Maxwell about an EC2 instance issue. Harry Boone mentions network and memory usage, while Zoe Maxwell notes some bugs in Jira. The thread ends with Harry Boone stating everything is behaving as expected.

Communication made easy

"We've been able to take all of the engineers and focus them on getting the problem solved, as opposed to having to tear off someone's time to just handle communications."



Jay Kline
Director of technology—engineering enablement
Target

At Target, Slack is the central hub for engineering communications and troubleshooting. During incidents, a proactive bot sends updates to relevant stakeholders, allowing response teams to stay focused on finding solutions.



5. Accelerate incident reviews

Use emoji to mark important follow-ups

By default, dedicated incident channels provide a timestamped audit trail of the events for future reference. With the full context, teams can explain issues during customer meetings and postmortem discussions—and share the knowledge with colleagues to prevent similar situations in the future.

Using a specific emoji, like the *lightbulb* 💡, the response team can easily flag any message they'd like to include in a review: timestamped discussions, screenshots, metrics and logs from monitoring tools, links to relevant systems and dashboards, and resulting decisions. Using the **Reacji Channeler app**, users can leverage their chosen emoji to automatically route all of their flagged messages to a dedicated incident review channel.

For example, let's say someone shares a concern with the current runbook for database restarts in the incident channel: if they tag it with a particular reacji, like the *lightbulb* 💡 we just mentioned, this shares that message in a previously designated channel, Google Sheet or project management tool like Jira or Asana. It's an app you can install and use out of the box, no code required.



Leave a trace

“The Slack channel serves as a kind of audit trail. We use these incident channels as the root of our analysis for our postmortems, and what’s great is there’s no guesswork because we all have that history right there.”



Thomas Lawless

Lead engineer, STSM - CIO

Developer Experience at IBM

Lawless and his team also use Slack Connect with providers of the various services they use. He’s found that most companies are happy to share a private Slack channel across their organizations so they can talk about problems and questions they might have, saving them a lot of back and forth.

Once companies resolve an incident, an effective post-incident review ensures that it doesn’t happen again. Fortunately, you can organize your entire incident response to inform this review with little extra legwork.

The ability to **archive** channels means the historical record is preserved and can be searched and referenced to identify patterns and onboard new engineers more effectively; this also helps your team tame channel sprawl so you can zero in on what matters most. When the incident review is complete, they can share the final report and related tickets back to the dedicated incident channel, where it’s neatly stored alongside all the relevant context.



5. Accelerate incident reviews

Stay agile

“Slack enables us to look back and examine production incidents, where things have gone wrong, and analyze what happened and how we can improve in the future, which is fundamental to agile development and continuous improvement.”



Clifford Bailey
Head of Partnership Management for APAC
Ocado Group

The online supermarket's central operations team monitors a Slack channel where they're notified when changes are made to hundreds of systems across the company. By integrating their DevOps deployment systems with Slack's simple API, everyone knows what's going on, wherever they are.

#support 🔔

PagerDuty APP 12:44 PM Today ▾

Acknowledged #3847 Shopping Cart API: Request Response Time is High for prod - (95th percentile > 250 ms on average during the last 10m)

Assigned: [Lisa Zhang](#) Triggered by: [Datadog](#)

↓ Low Urgency

Service: [Customer experience](#) Meeting URL: [Join Meeting](#)

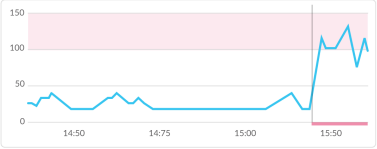
Incident Description: Shopping Cart API: Request Response Time is High for prod - (95th percentile > 250 ms on average during the last 10m)

[Link to metric](#)

Custom Details:

query
avg[last_10m/avgshopping_cart_result_duration_msec.95percentile[aws_er:prod] > 250

1 Acknowledged by Lisa Zhang (@Lisa Zhang) | Today at 12:50 PM (13kB) ▾



Acknowledge Resolve More actions... ▾



6. Get started right now

When incidents take longer to resolve, the disruption grows exponentially. With a digital HQ where employees can take swift, efficient action and keep stakeholders informed, they're able to shorten the incident *and* reduce its impact, not only for your customers and your bottom line but for your hardworking engineering team.

Faster resolutions, happier customers

"Slack has allowed us to really provide the experience we want to deliver. The satisfaction of the customer always goes up, and the overall resolution time goes down."



Jon Brummel

Senior manager of premier support
Zendesk

While every team's needs will be different, we hope this serves as a guide along your journey to build a digital command center that equips your employees to take a proactive approach and collaborate in real time with an open and extensible platform that evolves with them.



6. Get started right now

To hit the ground running, here's a quick-start checklist

1. For faster responses and visibility, pull relevant monitoring and paging alerts into Slack channels.
2. Use dedicated incident channels to document key findings, major decisions, metrics and logs, ensuring anyone who joins can gain context without disrupting progress.
3. Pin the latest update to the top of the incident channel and share it with other channels so everyone outside the incident stays up to date.

"The highest value is that people know exactly what's going on without having to ask and can see everything in a very centralized place: Slack."



Andrew Cunningham

Delivery lead

Tyro

Without the burden of siloed and redundant email chains, endless games of phone tag and isolated tools that don't speak to one another, your teams will be able to navigate any high-pressure scenario that comes along. [#]



About Slack

Slack is your Digital HQ—a place where work flows between your people, systems, partners and customers. Slack breaks down communication silos inside and beyond your organization by bringing teams and tools together around common goals, projects and processes in channels and in Slack Connect. It removes the limits of physical walls, giving people the flexibility to do their best work where, when and how they prefer with huddles and clips. And it empowers everyone to automate common tasks with apps and workflows. In the digital-first era, Slack makes work simpler, more pleasant and more productive.



The preceding information is intended for informational purposes only, and not as a binding commitment. Please do not rely on this information in making your purchasing decisions. The development, release and timing of any products, features or functionality remain at the sole discretion of Slack, and are subject to change.