Aware

Risk Management in Slack:

What the Modern Company Needs to Know

Unlock faster, cheaper, more effective security and search in Slack with Aware

Slack revolutionized the way companies do business. The collaboration platform reduces email by 60% and meetings by 36%, while delivering 49% more productivity.[1]

The numbers speak for themselves

77% of the Fortune 500 use Slack[2]	**12 M+** daily users[3]
1B+ Slack messages sent each week[4]	**2400+** app integrations[5]

What makes Slack so popular with employees and business leaders alike is its ability to cut through red tape, democratize collaboration and unite teams from around the globe. Slack gives employees the freedom to collaborate how they want, with whoever they want. Public and private channels, direct and group messages help to filter out the noise.

And in the click of a button, employees can invite partners and prospects into their Slack environment, share links and documents, and help each other do their best work. Slack offers massive benefits to the modern company that embraces it in the workplace.

But the same freedoms that make Slack so popular also make it near impossible to surface all relevant messages and context with Slack's native search functionality alone.

The size of the problem you face

Your employees want to do their jobs as effectively as possible. That means cutting through processes that slow them down or hold them back. Over a third[6] of employees admit to breaking their organization's data security policies to get their jobs done. Unless they have another easily accessible, secure repository to share confidential information with each other, they're doing it in Slack — in much greater numbers than you might want to think.

	Password Share	Confidential Information
Public Messages	1:262	1:118
Private Messages	1:149	1:135

Aware research from analyzing millions of real collaboration messages shows that 1:166 messages contains sensitive information.

CASE STUDY

IP Leak

Ben has worked for Company X for two years. During that time, he wrote a script that helped Sales colleagues to quickly pull relevant data from LinkedIn, reducing the lifecycle of new deals. After securing a higher position at Company X's main competitor, Ben copied the code into his personal Slack space to easily access it from home and take to his new employer. Because Ben sent the code through a private message to himself, nobody else at Company X had visibility into what Ben had done.

Intelligent compliance monitoring from Aware could have mitigated this IP leak by automatically detecting code in an unsanctioned channel and tombstoning the message immediately, preventing Ben from accessing it.

The hidden cost of the risks in your Slack communications:

Total Number of Employees	**2500**
Average Messages Per Employee Per Day	**23**
Total Daily Messages *(2500*23)*	**57,500**
Total Annual Messages *(57500*260)*	**14.95 M**
Number of Annual Sensitive Messages *(14.95 mil/166 — Aware research shows that 1:166 messages contains sensitive information)*	**90,000**
Average Data Breach Cost Per Record	**$161**[7]
Total Cost of Annual Risk Exposure *(90k*161)*	**$14.5 M**

Imagine these scenarios…

- During litigation, your company is required to produce a complete record of relevant communications from two members of your team.
- A HR complaint alleges several employees have created a private Slack channel where they discuss their coworkers in harassing and discriminatory ways.
- A data subject access request reveals customer PII within your Slack messages. Now your legal team want assurances it was a one-off incident.
- An employee uses Slack to share sensitive files with a colleague who is leaving for your company's top competitor.

How do you currently handle compliance monitoring, search and eDiscovery in Slack?

Where would you start looking for insider threats, unauthorized information sharing, harassment or noncompliance?

How could you be sure you surface everything you need to find?

Every single message an employee types into your Slack environment adds another dollar to your total cost of risk exposure.

Slack retains all data by default. That means unless you actively establish retention policies or a user manually deletes content, Slack will keep every single file uploaded throughout the lifetime of your workspace. Just think what they could contain — proprietary information, confidential business plans and financial projections, customer and client data and more.

Even if you think your employees would never link to or upload that information — how can you be sure? Could you demonstrate to a regulator or potential investor that your Slack environment is free and clear of PII/PCI/PHI, IP or other risks?

CASE STUDY

Payment Card Industry Information

Carla works in the call center of a major telecommunications provider. She accepts customer PCI data, which needs to be entered into a secure system separate from the company's primary customer management system. Because switching between systems takes a long time and makes it harder for her to reach her call quota, Carla saves PCI data in a private Slack channel to batch upload into the system later.

Proactive compliance monitoring from Aware could have alerted the provider to unauthorized PCI data within Slack by detecting regular expressions such as card numbers and zip codes and flagging the content for review.

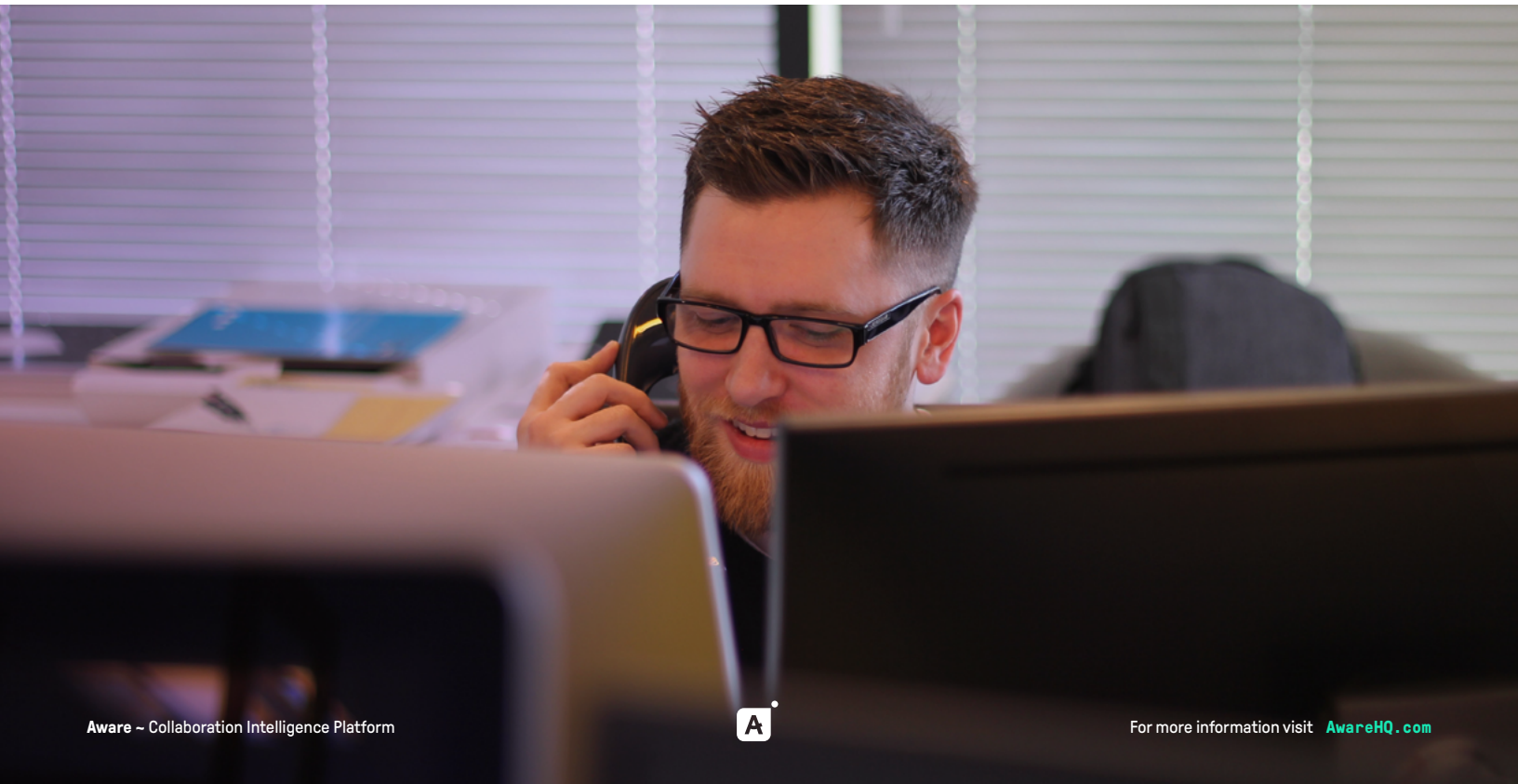
How do you manage risk in Slack?

Handling your Slack risk management needs in-house as they arise seems to make sense on the surface. But what does a reactive internal review entail?

Taking someone away from their regular duties to work on Slack search and eDiscovery is rarely time or cost-effective. Putting an inexperienced worker in charge of producing evidence for courts, regulators or investigators could have disastrous consequences. And in most instances, businesses lack the technological ability to perform eDiscovery or DLP in Slack.

Without Slack Enterprise Grid, for example, the only way to immediately search all of a user's Slack data is to log into their account. That publicizes the investigation and increases the risk of spoilation. And Slack itself will only provide user data to employers after they have approved the legality and necessity of the request.

Ultimately, this stop-gap solution saves the time and cost of hiring for a position that hasn't yet become a full-time need, but it comes at the expense of efficiency, effectiveness and employee morale.



CASE STUDY

Spoilation

Jose and Denise have been friends for years. They work for different companies in the same industry. They keep in contact through Slack Connect and share information about the deals they are working to prevent undercutting each other. Jose's company hears about this and initiates a search of his communications. But Jose deletes all his Slack messages with Denise at the end of each day, destroying the record of their communication.

With Aware, the company would retain a complete record of all the messages sent within its Slack environment, preserving everything said between Jose and Denise, including revisions and deletions.

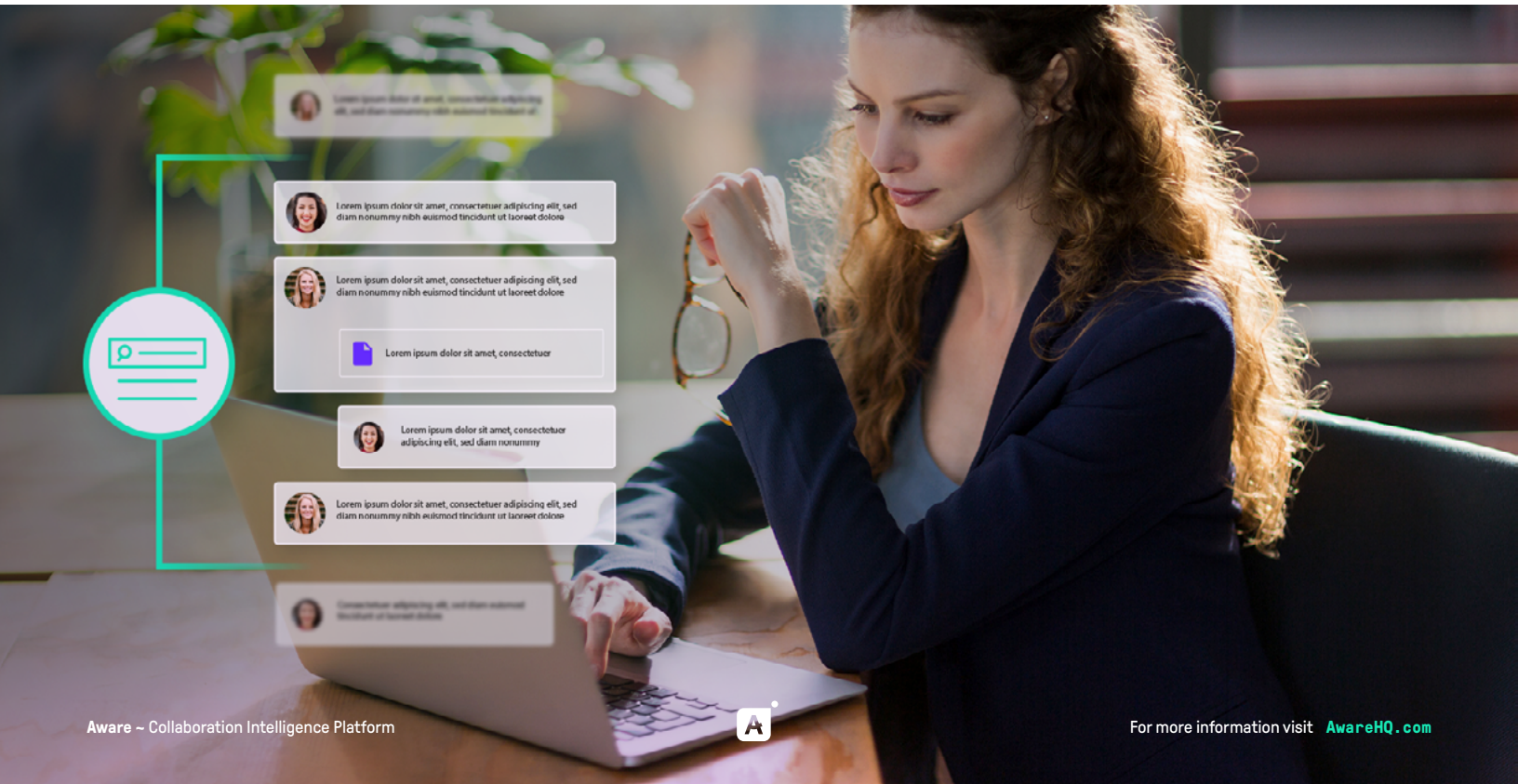
Outsourcing Risk Management

Calling in the experts is an attractive alternative to trying to manage Slack risks internally, but it can be eye-wateringly expensive.

eDiscovery accounts for up to 50% of litigation costs[8] and averages $18,000 per GB.[9] It also begins internally. The company must still provide the relevant data for review, and the less precise the export, the more expensive the process becomes.

External reviews are also subject to the timelines of third parties. That means even a simple case could take months — and many thousands of dollars — to complete. In the meantime, what additional risk has entered your Slack workspace, and how do you take a proactive approach to containing it when you're so far behind? Outsourced Slack risk management will never put the company ahead of controlling the risks Slack contains.

There is another way.



Proactive Risk Management for Slack from Aware

Aware is an AI-powered collaboration intelligence platform that provides comprehensive compliance monitoring, search and discovery across all channels and message types, quickly surfacing relevant data — including revisions and deletions.

The Aware platform connects to Slack via native APIs and webhooks with no IT lift needed. Data is continuously uploaded in real time and normalized for faster, more effective risk management.

Aware empowers organizations to perform eDiscovery, early case assessment and root cause analysis quickly and effectively, without outsourcing and without extensive training requirements. The intuitive platform enables contextualized oversight of your entire Slack environment, including private groups and direct messages. Continuous uploading to an immutable archive provides a complete record of all communications, including revisions and deletions.

Aware was purpose-built for collaboration, meaning it understands the unique nuances of your Slack dataset. Other risk management tools treat collaboration messages like email threads, often losing critical context in the process. Aware normalizes collaboration data while preserving context, then deploys artificial intelligence and machine learning enhancements that speed up eDiscovery while increasing the relevancy of results.

Aware is a one-stop solution to faster, better and more cost-effective risk management in Slack.

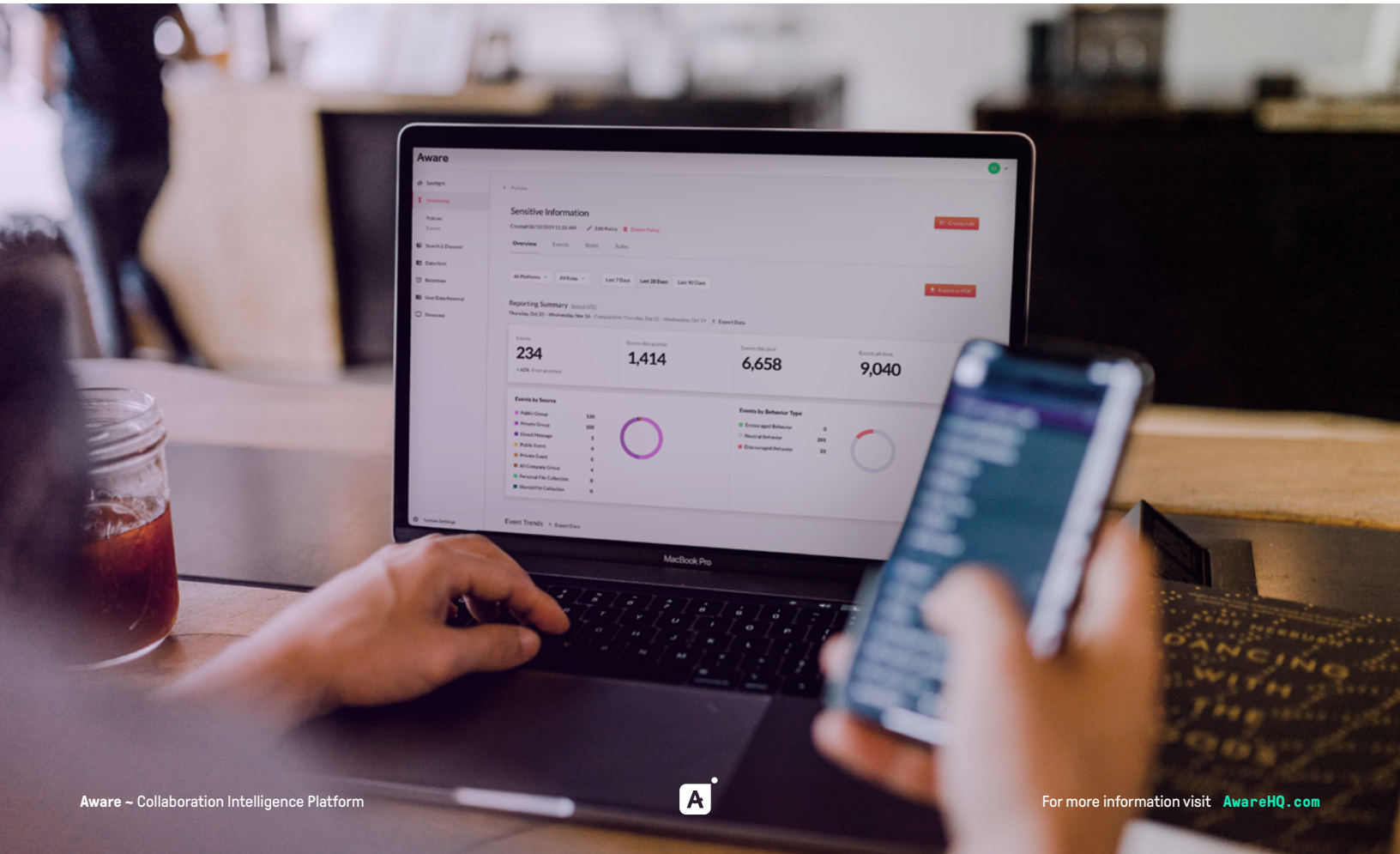
- Search by message author, keyword or regex
- Refine results by date/time, message type, attachments and more
- Get complete, holistic oversight with contextualized search results
- AI-powered federated search reduces timescales from days to minutes
- Apply industry-leading natural language programming to explore sentiment and toxicity
- Purpose-built for the unique data that lives in Slack, including reactions, attachments, threads and more
- AI/ML collaboration-specific filters accelerate information finding and increase results accuracy
- Designed to perform investigative searches for multiple use cases
- Effortlessly implement legal holds and custom retention policies in a click
- Automate real-time compliance monitoring and analysis
- Immediately notify business stakeholders when sensitive information is uploaded
- Tombstone messages within Slack to limit the spread of restricted data

Why you need a Slack risk management solution

In recent years, there has been increased legal and regulatory interest in Slack data. Courts know that businesses are holding critical conversations within collaboration, and regulators are clamping down on companies that fail to manage their datasets. Even threat actors are wise to the treasure trove of information that Slack messages contain.

The need to regulate your Slack environment is more pressing than ever, and demand for risk management capabilities in Slack increases by the day. Whether to resolve internal conflicts, to demonstrate adherence to compliance policies, or to respond to legal demands, it is essential for the modern company to be able to access Slack data and extract relevant information in as little time as possible.

- Regulatory fines for failing to control collaboration have exceeded $1.8B since December 2021[10]
- The Twitter lawsuit against Elon Musk saw Musk demanding Slack discovery from 42 different custodians[11]
- Prior court rulings determined that the high cost of collaboration eDiscovery does not constitute an "undue burden" during discovery[12]
- A spate of recent cybersecurity threats have led to the FTC announcing it is considering strengthening consent decree regulations[13]
- The hacker who breached Uber in September 2022 targeted and exfiltrated company Slack messages[14]



Aware

Aware + Slack = Proactive threat detection for your entire organization

Aware helps organizations to unlock deeper insights into employee experience, sentiment and toxicity by analyzing aggregate Slack data. Our algorithms understand “normal” for each organization and shine headlights onto areas of increased threat risk.

Using Aware, businesses can transition from reactive to proactive risk management for Slack, surfacing risks as they appear in collaboration — before they become a problem. Get real-time notifications when employees upload restricted files, talk about confidential projects in public channels or break acceptable use policies. Automate the removal of messages that violate internal policies and streamline all your Slack search and discover processes from a single platform that was purpose-built to make your job easier.

Contact us today to learn more about how Aware can help you reduce your risk surface area within Slack and other places where your employees collaborate, visit **AwareHQ.com**

SOURCES

[1] https://slack.com/engage-users

[2] https://slack.com/blog/transformation/fortune-100-rely-slack-connect-build-digital-hq

[3] https://mashable.com/article/slack-redesign

[4] https://www.sec.gov/Archives/edgar/data/1764925/000162828019007428/slacks-1a3.htm#sC9C346D78943772D97FB567D8BF6BBDD

[5] https://slack.com/integrations

[6] https://track.g2.com/resources/shadow-it-statistics

[7] IBM Cost of a Data Breach Report 2021

[8] Zapproved, "Analyzing the True Cost of eDiscovery"

[9] RAND Institute for Civil Justice, "Where the Money Goes"

[10] https://www.nytimes.com/2022/09/27/business/banks-fined-texting-sec.html

[11] https://www.law.com/delbizcourt/2022/09/08/partial-access-to-slack-text-messages-granted-in-twitter-musk-discovery-row/?slreturn=20221022162224

[12] https://app.ediscoveryassistant.com/case_law/32595-benebone-v-pet-qwerks

[13] https://www.axios.com/2022/09/27/federal-trade-commission-consent-decree-cybersecurity

[14] https://www.uber.com/newsroom/security-update/