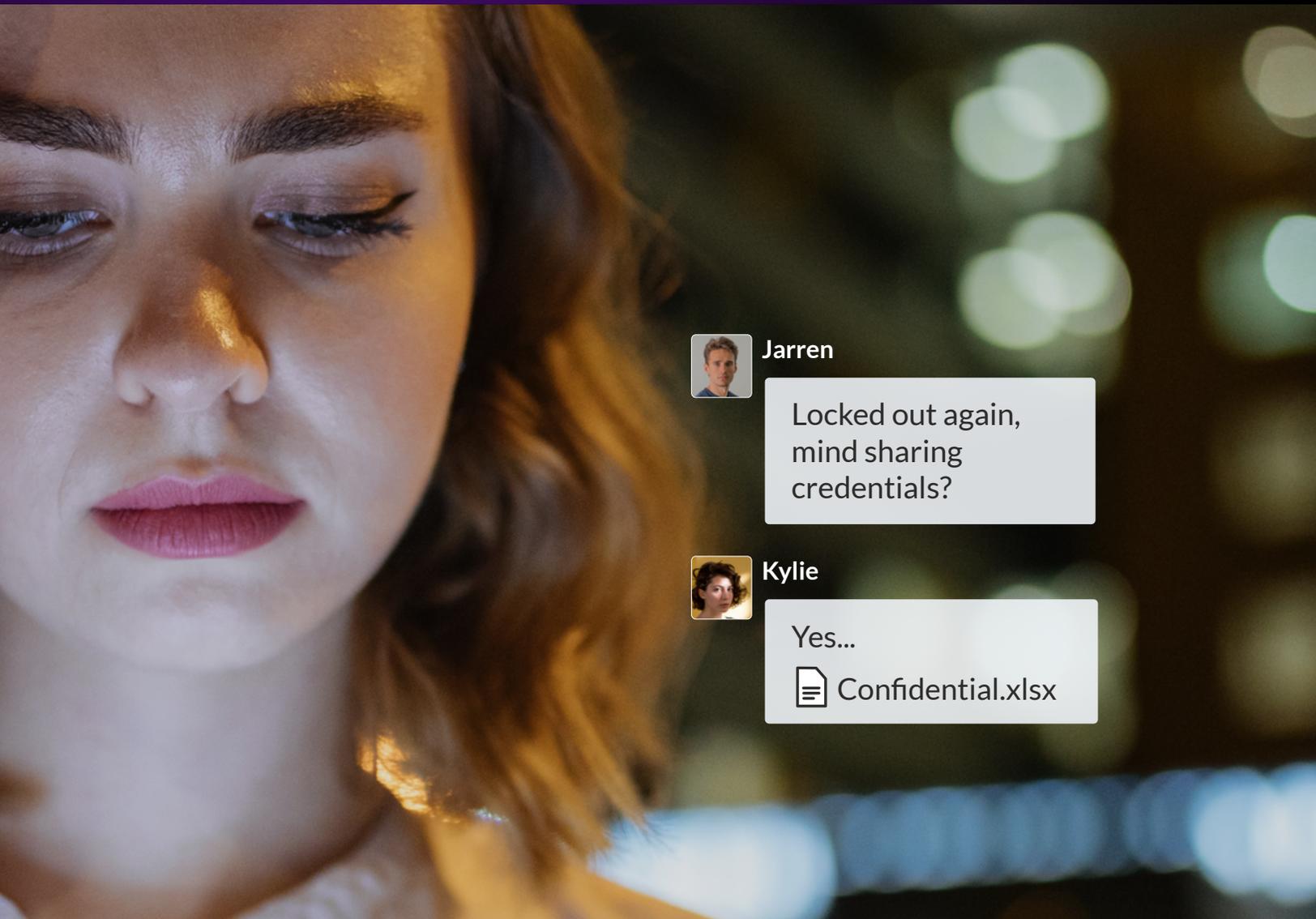


Aware

WHITEPAPER

MITIGATE DATA RISKS IN SLACK

Compliance Monitoring, DLP and Search for Slack



Jarren

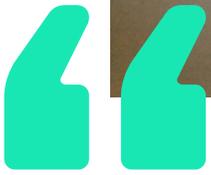
Locked out again,
mind sharing
credentials?



Kylie

Yes...

 Confidential.xlsx



When people have the chance to work flexibly, 87 percent of them take it.

McKinsey

¹ McKinsey's American Opportunity Survey 3rd Edition

In today's diverse, hybrid workplaces, organizations frequently turn to messaging and collaboration tools like Slack to meet the growing need for productivity and knowledge sharing. It's a need that exploded during the pandemic but continues to be more relevant than ever. In 2022, McKinsey found that 58% of Americans can work remote at least one day a week, and more than a third can work fully remote.¹

Slack reported in 2019 that paid users spend upwards of 9 hours per business day connected to the app, including 90 minutes of active work. That number is likely much higher today. Innovative organizations use platforms like Slack to support every type of work: synchronous and asynchronous, in-person, hybrid and fully remote, across multiple functions, multiple organizations and within single teams.

Increased Adoption Leaves Organizations Exposed

While Slack excels at connecting today's digital workforce, the platform wasn't designed to handle the operational, data governance complexities of modern businesses. As a CIO or CISO, you're tasked with protecting the organization against data risks, including the data that lives within Slack.



SENSITIVE INFORMATION

How do you know that PCI, PII or other sensitive information doesn't live in Slack messages?



EXTERNAL AUDIENCES

How do you prevent external audiences (including guest access or Slack Connect) from gaining inadvertent (or purposeful) access to sensitive data?



REPUTATIONAL DAMAGE

How do you ensure that bad behavior doesn't happen within Slack, potentially leading to massive organizational culture and reputational damage?



WORKPLACE INCIDENTS

What happens if an incident comes to light? How do you conduct eDiscovery or internal forensics on the data living in Slack?

Most organizations using tools like Slack face these same challenges. With the volume of data living in Slack at an all-time high, IT leaders like you need a way to protect your organization's best interests and easily satisfy legal, compliance AND information security.



Humans are always the weakest link in the chain

Deborah Wheeler,
CISO at Delta Airlines

Urgency in Closing the Gaps

In a recent webinar on, Deborah Wheeler, CISO at Delta Airlines, commented that humans are always the weakest link in the chain. Someone either did something they shouldn't have done, or someone didn't do something they should have done.

Human behavior is difficult to predict and the chatty, real-time nature of conversations in Slack make it all too easy for one bad apple—or one honest mistake—to put your organization at risk. This is why you need to address these challenges, now.



SECURITY LEADERS FEEL UNPREPARED

A 2021 study by IDG stated that 90% of security leaders believe they're falling short in addressing cyber risk and listed the top three priorities for the next 12 months as:

- Better preparation for the next unexpected security incident
- Increased protection for sensitive and confidential data
- Improved security awareness of end-users

THIRD-PARTY PROTECTION

Gartner says 52% of legal & compliance leaders are more concerned about third-party cybersecurity risk than they were before the pandemic.

REDUCING REMOTE RISK

According to Malwarebytes, remote workers caused a security breach in 20% of organizations.



How Forward-Thinking Companies Solve These Challenges

Innovative companies adopt platforms such as Aware, which offers best-in-class technology to understand and make sense of all the human interactions happening in the organization, for a variety of use cases including:

- Information Management
- Data Protection
- Organizational and Behavior Insights

Technology is constantly innovating. As leading technology providers focus on business productivity and efficiencies, choosing a third-party solution, such as Aware, brings security and compliance expertise to collaboration datasets and services while enabling organizations to take advantage of the latest functionality of their tools.

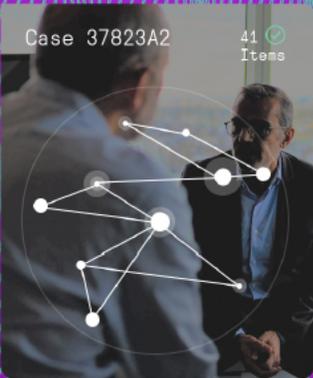
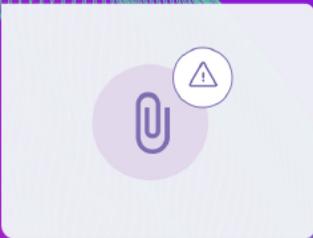
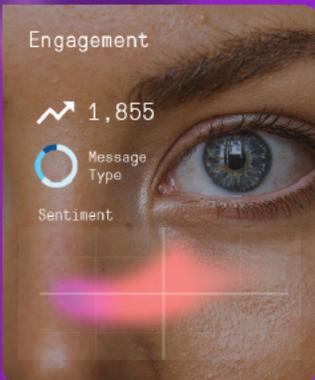
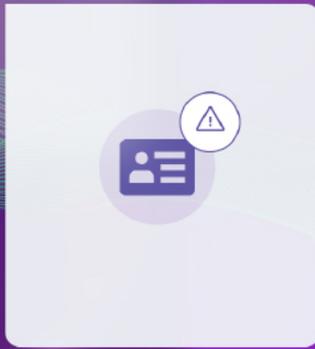
“Aware is by far one of the best partners to work with”

“We always recommend Aware for compliance capabilities”

“With Aware we can collaborate with confidence”

DLP/COMPLIANCE MONITORING AND EDISCOVERY

Aware is the Only Vendor That Offers Both.



Compliance Monitoring & DLP

- AI-driven human behavior anomalies
- Compliance and acceptable use
- HIPAA and PHI sharing
- PII
- Secrets sharing
- PCI and credit card data

Internal Forensics, Search & Discover

- Find, flag and export the data you need using Advanced filtering options, including ML/NLP analysis, reducing the amount of data produced
- Begin capturing, enriching and searching immediately



More than a Vendor, We're a Partner.

At Aware, we're dedicated to innovating with our customers to offer best-in-breed solutions that manage the ever-changing landscape of collaboration data. Request your personalized demo at [AwareHQ.com](https://www.awarehq.com)

Aware

MAKE SENSE OF YOUR COLLABORATION DATA