



UNLEASH THE
POTENTIAL OF
YOUR WORKFORCE

WorkJam Digital Loss Prevention

Safeguard sensitive information, stay compliant, and protect your business from data breaches and liabilities.



Fact: data breaches are expensive. IBM estimatesⁱ that the average data breach costs \$3.86 million, and it typically takes 280 days to identify and confine data breaches.

But beyond the upfront financial costs of these incidents, businesses have to reckon with even more expensive consequences: a blow to the organization's reputation and loss of customer trust.

Data breaches are something you want to prevent at all costs, and your organization has probably already deployed firewalls and multilayered authentication to its internal systems so that no one can *get in* and breach data, but what about your digital workplace or communications platforms?

- What about employees who use sanctioned workplace solutions?
- What if they are using un-sanctioned communications solutions?
- How can you keep your sensitive and customer data internal?

While this task may seem difficult and complicated when you have thousands of frontline employees spread out across the country (or the world), **WorkJam Digital Loss Prevention (DLP)** makes protecting your data surprisingly easy.

HOW WORKJAM DIGITAL LOSS PREVENTION WORKS

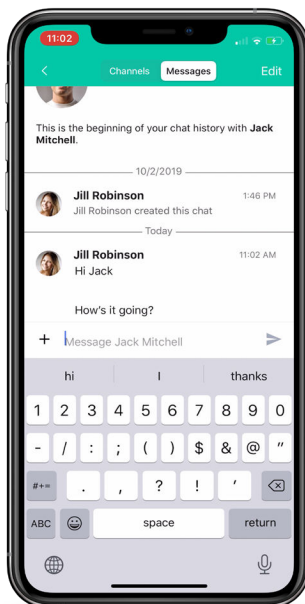
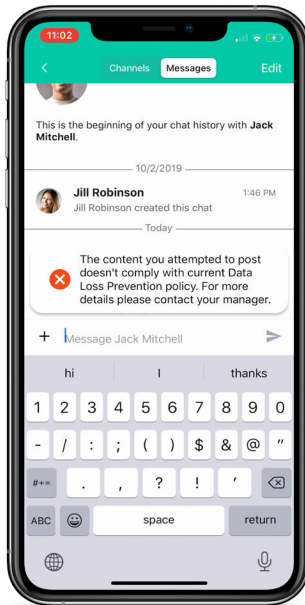
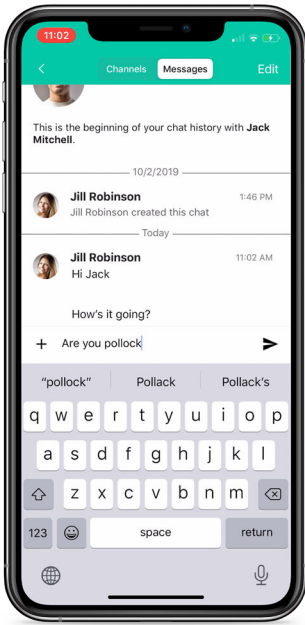
WorkJam's DLP module helps keep your data secure by preventing sensitive information from being shared on your communication platform. When team members attempt to send restricted data or information through posts or direct messages, WorkJam automatically blocks the message and prevents it from being shared over your network.

WorkJam stops sensitive data from leaking, reducing the possibility of it being shared over direct message and chat.

Automatically detect and redact 120 data types. WorkJam Digital Loss Prevention can recognize and block certain types of information from being sent on your network. Such data types include:

- Drivers license numbers
- Social security numbers
- Credit card numbers
- IMEI Hardware IDs
- Bank Routing Numbers
- Employer Identification Numbers
- Passports
- MAC Addresses
- Phone Numbers
- Swift Codes

There are a total of 120 data typesⁱⁱ that can be used, including many country-specific data sets.



Specify the information you don't want being shared. DLP also enables you to add words and phrases to your "block list." Confidential client data or details about unreleased products are just a few examples of information that WorkJam can safeguard for you.

Works for images and PDF files.

WorkJam Digital Loss Prevention can scan images and PDF files. For example, the system can automatically recognize images of credit cards and stop employees from sharing them. As for PDFs, WorkJam can scan the content of these documents for sensitive information and prevent users from sending them using your communications platform.

Access to detailed reports on data loss prevention. DLP automatically generates reports that allow administrators to review and audit violations by users. These reports are available as Excel files and contain the following information:

- Log Number - Sequential
- Timestamp
- IP address
- Username
- Location - Store
- Action taken by the user
- Action taken by DLP

BENEFITS OF WORKJAM DIGITAL LOSS PREVENTION TO YOUR ORGANIZATION

Protect sensitive data. The primary benefit of DLP is it allows you to easily safeguard sensitive information. From confidential company, vendor, and customer data to personal employee details, WorkJam helps you keep your sensitive data under wraps.

Stay compliant with privacy laws and regulations. GDPR. GLBA. CCPA. Privacy and data and protection laws are constantly being introduced and updated. Failing to comply with regulations may lead to costly and damaging lawsuits. WorkJam Digital Loss Prevention makes compliance simple by automatically protecting the data of your company, employees, and customers – ultimately reducing liability for your organization.

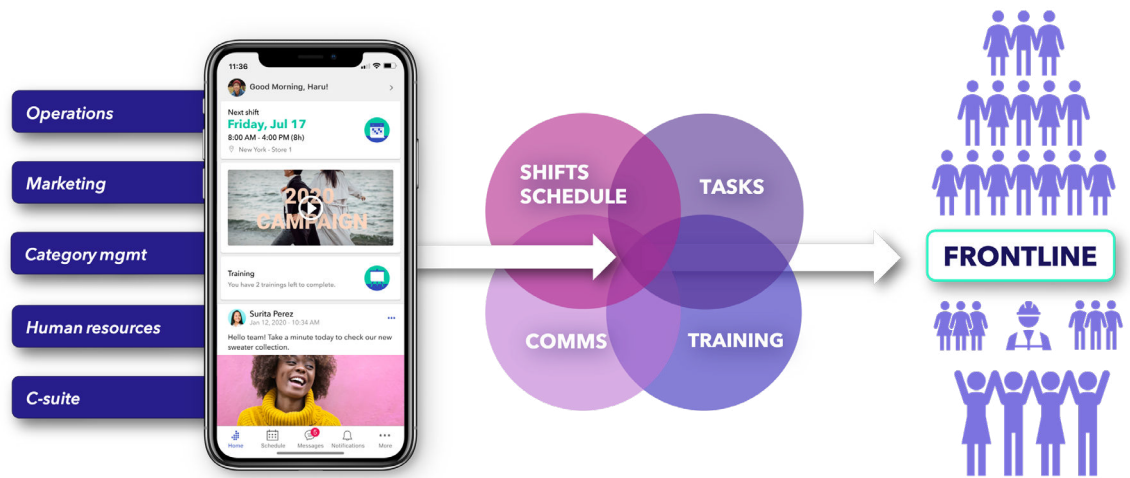
Gain insights into the security and privacy practices of your organization. What are the common types of sensitive information that people are prone to sharing? Are employees mindful of the data they're sending, or do you need to conduct training on privacy protection? With WorkJam's reports, you can glean insights into the state of privacy and security in your organization so you can improve your existing processes and continue to keep data safe

IS SHADOW IT PUTTING YOUR COMPANY AT RISK?

If you don't currently have a corporate digital workplace or sanctioned communications platform in place, you know your employees are probably using their devices with unsanctioned applications to share information such as public email accounts, WhatsApp chat apps, and others. WorkJam recently released a white paper on the subject, but the bottom line is that WorkJam is a digital workplace solution that your employees will want to use, and given we are one of the few digital workplace solutions with a digital loss prevention option, you will want them on WorkJam.



UNLEASH THE
POTENTIAL OF
YOUR WORKFORCE



DON'T WAIT TO SAFEGUARD YOUR DATA

As organizations and consumers continue to adopt digital solutions and apps, the need to protect sensitive data is more important than ever. In a highly competitive business landscape, you simply cannot afford to get hit with a data breach and lose time, money – and, more importantly – customer trust.



Sources

- 1 <https://www.ibm.com/security/data-breach>
- 2 <https://cloud.google.com/dlp/docs/infotypes-reference>

Schedule a demo of **WorkJam** today and
see how we help you unleash the potential of your workforce

Request a Demo