



Guide to Data Loss Prevention (DLP) on Slack

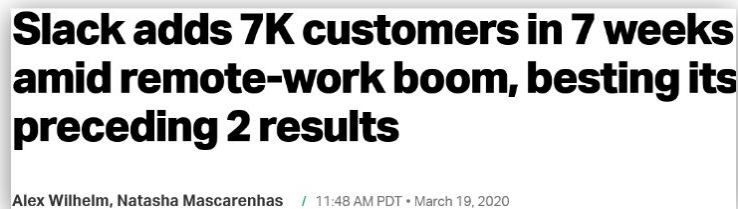
How to implement data loss prevention (DLP) on Slack, and detect leakage of sensitive data across any Slack workspace.



Data leakage in context of Slack

Slack has become an integral to business and enterprise operations, with millions of employees spending on **9 or more hours** connected to the application¹.

The always-on nature of SaaS applications combined with high volume of activity in Slack workspaces introduces new opportunities for sensitive data leaks within companies.



1. [“Not all Daily Active Users are created equal: Work is fueled by true engagement”](#) - Slack Blog



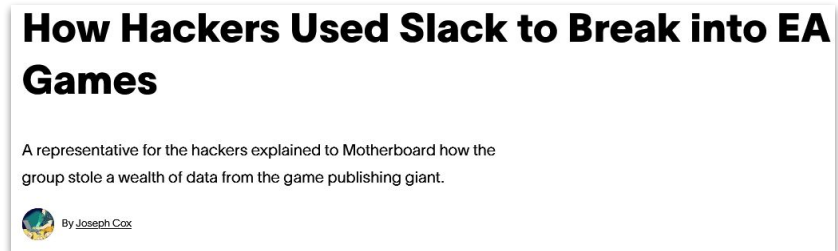
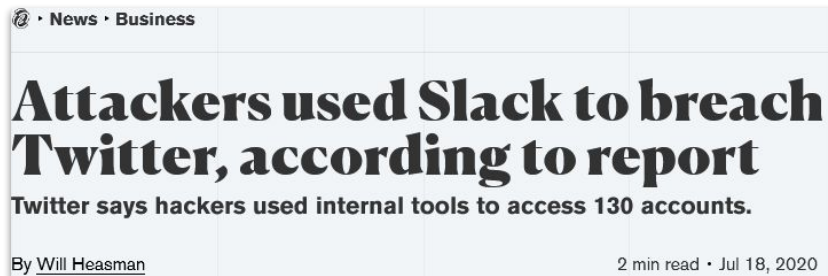
What can contribute to data exposure risk in Slack?

- Slack environments present challenges for ensuring infosec best practices are followed:
 - **Slack connect channels** introduce users from outside your organization who many not know or follow policies.
 - **Slack guest accounts** must be provisioned appropriately, with access to the right channels and assets being maintained across their lifetime.
 - **Private channels** create visibility constraints for security teams.
 - **File attachments** create complexity by expanding the number of places where data can live as well as the types of sensitive data they must look for.
 - **Retention policies** must be actively managed in accordance to compliance and security policies and practices.



What are the consequences of data exposure risks?

- **Historical security risks:** Sensitive data may already be stored in your environment and could be accessed at any time by anyone.
- **Real-time security risks:** Sensitive data can be shared and seen in real-time within your environment by unauthorized persons.



Best practices for protecting sensitive data in Slack

1. Enforce a **consistent channel creation process** that complements business objectives and security policies
2. Streamline Slack security with automated features like **message and file retention time limits** that map to your risk management & compliance strategies
3. **Identify engaged stakeholders** who will serve as Slack admins and aid employee education
4. Invest in technologies like **cloud data loss prevention (DLP)**



What is Data Loss Prevention (DLP)?

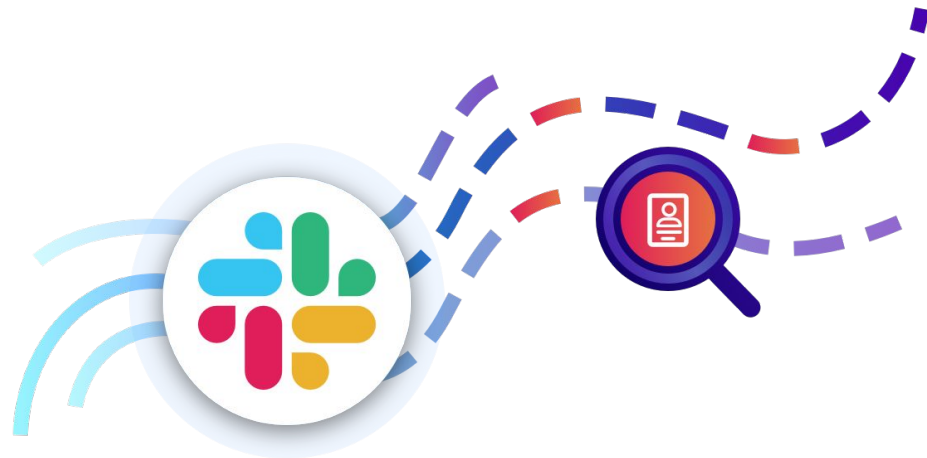
DLP ensures confidential or sensitive information (like credit card and social security numbers) isn't shared outside of Slack by scanning for content within messages and files that break predefined policies.



How does Slack benefit from DLP?

Collaborative SaaS applications like Slack create environments where data policy and security best practices are difficult to maintain or enforce without an excessive time or resource commitment.

Data loss prevention helps provides companies with a feasible alternative to address this problem.



Does Slack have DLP functionality built-in?



No, Slack relies on third-party apps (like Nightfall) to provide DLP functionality in Slack. Nightfall is a Slack DLP partner.

Designed for



Nightfall™

nightfall.ai/integrations/slack

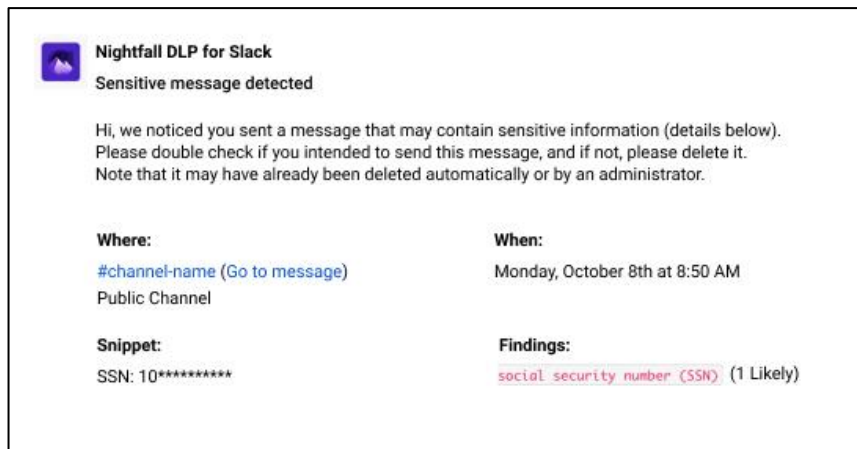


How do I implement DLP on Slack?

Nightfall's Slack bot can be added in seconds to your Slack account.

No additional set up, tuning, or installed agents are required.

Request a free trial with us.



Does Nightfall's bot work on any Slack plan?

Yes, Nightfall works on any Slack plan:

Nightfall Pro is designed for Slack Free, Standard, and Plus plans. Scan all public channels. Learn more [here](#).

Nightfall Enterprise is designed for Slack Enterprise plans. Scan the entire Slack organization via Slack's Discovery API. Learn more [here](#).



Available in



Nightfall[™]

nightfall.ai/integrations/slack



Case Study: Aaron's, Inc.

(NYSE: AAN)

Stuart Lane, Information Security Engineer

Industry: Retail

Employees: 12,000+

Use Cases: DLP, policy enforcement, toxicity filtering

Aaron's[®]



“Nightfall has allowed us to automate the detection and response of DLP in Slack. This has alleviated an impossible task of manually monitoring the platform.”



What is Nightfall?

- Nightfall is a platform to discover, classify, and protect sensitive data across cloud SaaS & data infrastructure via machine learning.
- Nightfall's Slack bot helps you instantly add DLP functionality to Slack.
- The bot detects sensitive data in files & messages in real-time. Get alerted & take remediative action directly within Slack.
- Nightfall supports compliance efforts with PCI, GDPR, HIPAA, CCPA, SOX, and many others.



How does Nightfall work?



Discover: Continuously monitor sensitive data that is flowing into and out of files & messages in Slack.



Classify: Machine learning classifies your sensitive data & PII automatically, without prior tuning or tagging, so nothing gets missed.



Protect: Setup automated DLP workflows for quarantines, deletions, redaction of sensitive content in messages, alerts, coaching, and more - saving you time and keeping your business safe.



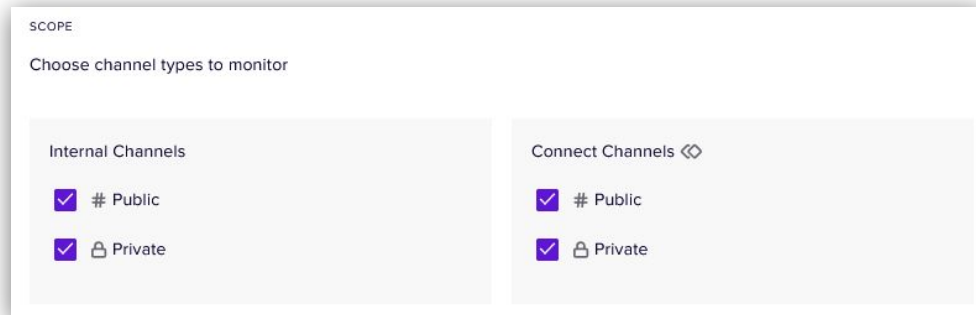
Key Benefits

Get started now for free - no setup or tuning required.

Leverage 150+ pre-tuned, standard detectors of PII out of the box.

Configure detection settings to fine-tune the conditions and contexts that trigger Nightfall detectors.

Apply policies with a high level of granularity in Slack. Including within DMs & Slack Connect channels.



Enterprise-Grade Security

- **Does not store or track sensitive findings**, only non-identifying metadata is gathered to improve accuracy.
- TLS 1.2+ and AES 256 encryption.
- Fully hosted on AWS and GCP.










Detectors

10M

Average # instances of
sensitive data classified
per month

Types of Detectors

-  Standard PII & Names
-  ID Numbers
-  Finance & PCI
-  Network & Geographical Addresses
-  Health & PHI
-  Credentials & Secrets
-  Custom Regexes & Word Lists



File Scanning Capabilities

Nightfall can scan 100+ file types, including images using optical character recognition

COMMON FILE TYPES



Plaintext



Google Drive file types



Open Office



Microsoft Office



Adobe PDF



HTML



XML



Images

... and many more!



Customer: Bluecore

Brent Lassi, CISO

Industry: SaaS, Retail Marketing Services

Use Cases: DLP, policy enforcement



“Nightfall helps us prove to our customers that we have a high level of hygiene diligence. Our clients want to know that we're responsibly managing their data.”



Case Study: Galileo Health

Michael Supon, Head of Security and Compliance

Industry: Healthcare

Employees: 55

Use Cases: HIPAA compliance, DLP,
credentials/secrets detection

galileo^o



“Nightfall’s ease of setup and accuracy of identified data are both on point.
Nightfall has eased our collective mind.”

Nightfall[™]
nightfall.ai/integrations/slack



How do I get started?

To get started with Nightfall, request a demo or free trial or email us at sales@nightfall.ai with any questions.

Request a demo or free trial

Not ready yet? Learn more at www.nightfall.ai or contact us at sales@nightfall.ai.

