Nightfall

Guide to Data Loss Prevention (DLP) for Asana

How to implement data loss prevention (DLP) within Asana to manage data exposure risk and maintain compliance

Data leakage in context of Asana

Today, more than 130,000 organizations use Asana for project management and communication.

As such, Asana is a high-volume collaboration tool where some of the world's largest organizations store unstructured sensitive data about a wide variety of topics that may include proprietary information like source code, personal information for customers & employees, secrets and credentials for private systems, and more.

In order to address this potential risk, organizations need to educate employees about what information can safely be shared in Asana, via a detailed data security policy that can be enforced with tools like Cloud DLP.

Nightfall™

nightfall.ai/solutions/product/asana

What can contribute to data exposure risk in Asana?

- Always-on SaaS environments like Asana present unique challenges for ensuring infosec best practices are followed:
  - Without the proper tools, security teams lack visibility into the types of sensitive data stored or shared in Asana Projects, **including within images, documents, and other types of file attachments**. This can make it difficult to audit for compliance or data exposure risk.
  - Organizations may lack **dedicated stakeholders** explicitly responsible for understanding how security policies and best practices should inform Asana security settings. Including authentication settings, guest account settings, deprovisioning processes, and default content privacy settings.
  - Employees may add **third-party integrations** or bots with read and/or write privileges that can add or access data in Asana.
- This necessitates that security teams have access to tools that provide the visibility to see what data is shared within Asana.

Nightfall™

nightfall.ai/solutions/product/asana

What are the consequences of data exposure risks?

- **Historical Data Compliance violations**. Without knowledge of what employees have shared and are storing in Asana, it's difficult to validate organizational compliance posture for industry regulations like HIPAA, PCI DSS, and more.
- **Privilege escalation risk.** In addition to compliance violations, security teams need to validate that secrets, credentials, and data that can be used to access other accounts/environments are not being stored in Asana.

Nightfall™

nightfall.ai/solutions/product/asana

Best practices for protecting sensitive data in Asana

1. **Identify engaged stakeholders** who are Asana experts and make sensitive data protection in Asana a top priority by using security and compliance policies to determine the appropriate security configurations and user best practices.

2. Implement the **appropriate security & privacy configurations** for your Asana instance based on your compliance and security policies (multifactor authentication, team privacy settings, SSO, etc.) and ensure employees are educated on the importance of maintaining these configurations.

3. Invest in technologies like **cloud data loss prevention** (DLP) to enforce **consistent sensitive data protection policies across all your cloud applications** from a centralized product. DLP can also streamline Asana security across orgs to **discover sensitive data, enforce protection controls and continually meet compliance** requirements.

Nightfall™

nightfall.ai/solutions/product/asana

What is Data Loss Prevention (DLP)?

DLP ensures confidential or sensitive information (like credit card and social security numbers) isn't exposed within Asana by scanning for content in any files and fields

Nightfall™

nightfall.ai/solutions/product/asana

How does Asana benefit from DLP?

High-volume, collaborative SaaS applications like Asana, with enormous amounts of sensitive data, create environments where data privacy 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 by automating the detection of data policy violations.

Nightfall™

nightfall.ai/solutions/product/asana

Does Asana have DLP functionality built-in?

No. Nightfall is the first and only DLP solution available today within the Asana ecosystem.

Designed for asana

Nightfall™

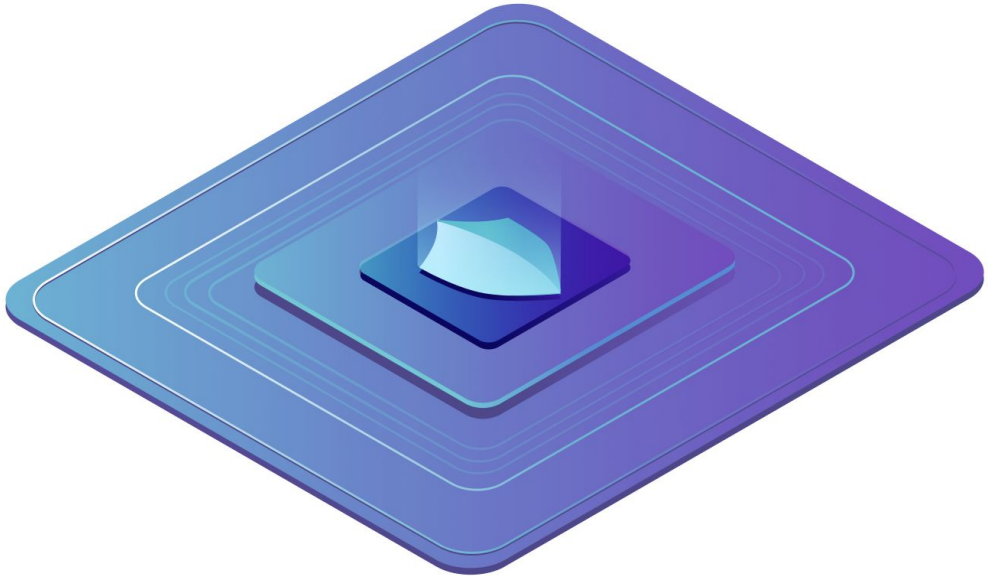
nightfall.ai/solutions/product/asana

How do I implement DLP in Asana?

Grant access to your Asana org via OAuth 2.0. Nightfall's API based integration can start scanning selected objects in seconds.

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

Request a free trial with us.



Nightfall™

nightfall.ai/solutions/product/asana

What is Nightfall?

- Nightfall is a platform to discover, classify, and protect sensitive data across cloud SaaS & data infrastructure via machine learning.
- Nightfall supports compliance efforts with PCI, GDPR, HIPAA, CCPA, SOX, and many others.

Nightfall™

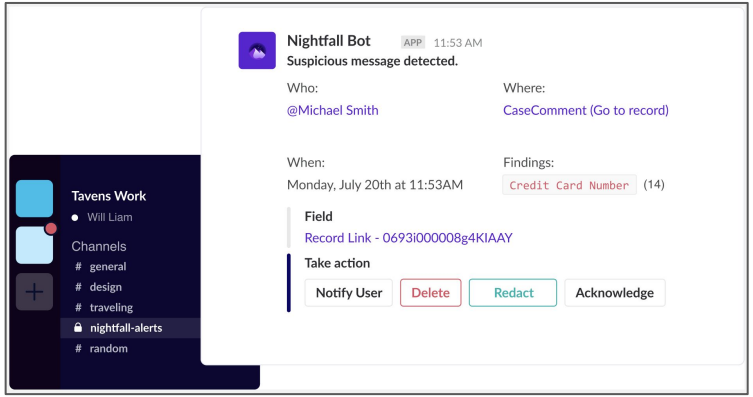
nightfall.ai/solutions/product/asana

Key Benefits

Easy to use with low overhead. Get started now for free - no setup or tuning required.

Leverage multiple pre-tuned, standard detectors of PII out of the box. Including detection for: PHI, PCI, secrets, credentials, and more.

Native support for multiple apps, so it's easy to implement a consistent data protection policy.



Nightfall™

nightfall.ai/solutions/product/asana

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.

Nightfall™

nightfall.ai/solutions/product/asana

Detectors

16M

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

Nightfall™

nightfall.ai/solutions/product/asana

File Scanning Capabilities

Nightfall can scan common many 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

Standard, custom objects, fields ... and many more!

Nightfall™

nightfall.ai/solutions/product/asana

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.”

Nightfall™

nightfall.ai/solutions/product/asana

Case Study: Galileo Health

galileo

Michael Supon, Head of Security and Compliance

Industry: Healthcare

Employees: 55

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

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

Nightfall™

nightfall.ai/solutions/product/asana

How do I get started?

To get started with Nightfall for Asana, schedule time with our product team by choosing a slot that works for you or email us at sales@nightfall.ai with any questions.

Request a discovery call

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

Nightfall™

nightfall.ai/solutions/product/asana