



Nightfall

Guide to Data Loss Prevention (DLP) in Jira






Data leakage in the context of Jira

The Atlassian ecosystem provides thousands of companies with the ability to collaborate remotely through powerful, feature-rich SaaS applications like Jira. As such tools become the norm across companies, big and small, the amount of sensitive information stored in these systems will increase. This means that organizations need to prioritize minimizing the risk of exposure within cloud environments.

This can be difficult, because most SaaS applications, including Jira, lack any native security functionality, meaning that organizations must rely on processes, policies, and procedures to regulate employee handling of sensitive information and remediate instances where best practices around sensitive data are violated. However, the only way to accomplish this is to maintain the appropriate level of visibility within your SaaS environments in order to keep track of where sensitive data might be and to prohibit employees from sharing it, intentionally or otherwise.

 Add epic /  CS-3

Customer Service Request

 Attach  Add a child issue  Link issue 

Description

Hi I need help completing a customer's purchase their credit card is 4017957436413755

Activity

Show:   

Newest first 

 MO

Add a comment...

Pro tip: press  to comment

How does Jira increase data exposure risk?

SaaS applications like Jira allow for collaboration between a multitude of users. However this high volume of activity, combined with the always-on nature of SaaS systems, can increase the risk that data security best practices aren't followed. This can result in PII, credentials, secrets, and other sensitive information being exposed to the wrong parties.

Within the Atlassian ecosystem, the misconfiguration of sensitive content has led to such information being viewable over the open internet with researchers discovering hundreds of public facing Jira instances among Fortune 500 companies and government agencies.

In a sample of 5,000 Jira Software Cloud sites, there were 273 Jira sites with publicly viewable issues and 1,214 Confluence sites with publicly viewable spaces.



JIRA Misconfiguration Leaks Data of Fortune 500 Companies

By [Ionut Arghire](#) on August 05, 2019

One Misconfig (JIRA) to Leak Them All- Including NASA and Hundreds of Fortune 500 Companies!



[Avinash Jain \(@logicbomb\)](#) Aug 2, 2019 · 7 min read



What is data loss prevention (DLP)?

Data loss prevention is an access control that ensures confidential information is kept on a need-to-know basis. DLP scans for content within messages and files to determine whether an unauthorized disclosure of business-critical information has occurred and can provide automated remediation on the basis of your established data security policies. Additionally, DLP can provide alerts and analytics that help organizations understand risk and employee behavior over time.

Like other always-on, SaaS environments with high volumes of activity, Jira makes violations of data security policies more likely, leading to data leakage risks as well as data compliance violations.

Organizations must implement controls like DLP that will help enforce data security best practices by preventing unauthorized parties from accessing content containing sensitive information.



What risks does Jira introduce?

Unlike traditional productivity and development tools, SaaS and IaaS platforms are always-on systems where any number of contributors share and store business data in environments not owned or managed by an organization's IT department. Without cloud data loss prevention this can easily create scenarios where data policy and security best practices are difficult to maintain or enforce without excessive time or resource commitment.

Key takeaway

Issues, which are the central type of content within Jira, can contain sensitive information inside of text fields or file attachments. A given Jira instance may have hundreds of issues managed across dozens of projects, making it difficult to ensure that sensitive details like API keys in code, customer PII, or other business-critical data remain protected from inappropriate or unauthorized access.

Projects / Customer Service / Project settings

Columns and statuses




Use columns and statuses to define how work progresses on your board. Columns represent the board's workflow, while statuses report the current state.

Assign statuses to board columns

All statuses must be assigned to a column. If you assign multiple statuses to a single column, your team can move work to different statuses within the one board column.

TO DO

IN PROGRESS

Statuses for    Manage workflow

TO DO

IN PROGRESS

What types of data are at risk of exposure in Jira issues?

Credentials & secrets are most frequently exposed in Jira, due to its common use in Agile development projects for product and engineering teams. However, other types of unexpected sensitive data have been identified in Jira by customers using Nightfall. These include:

- API keys & access tokens for third party services, e.g. AWS, Stripe, Twilio, etc.
- Cryptographic keys (SSH, PGP, etc.)
- Certificates (SSL, TLS, etc.)
- Passwords and login credentials
- Database credentials
- UUIDs, cookies, etc.
- Credit card numbers
- Customer PII

The need to identify sensitive data in Jira often arises from a business change, such as merging or separating business units and the subsequent data cleanup. Security leaders should also be aware of their specific industry requirements for compliance, and ensure data security standards are met within Jira — for example, HIPAA compliance may require that protected health information (PHI) is secured within Jira.



Why is data loss prevention (DLP) essential for protecting data in Jira?

Aside from Nightfall, there are no mature cloud-native DLP products for Jira. Atlassian does not have a native DLP product, and many CASBs cannot support Atlassian apps.

With Nightfall, you can flexibly configure multiple different DLP policies, and apply them to particular locations within Jira. This leads to a prioritized and optimized DLP approach, with reduced false positives and noise.

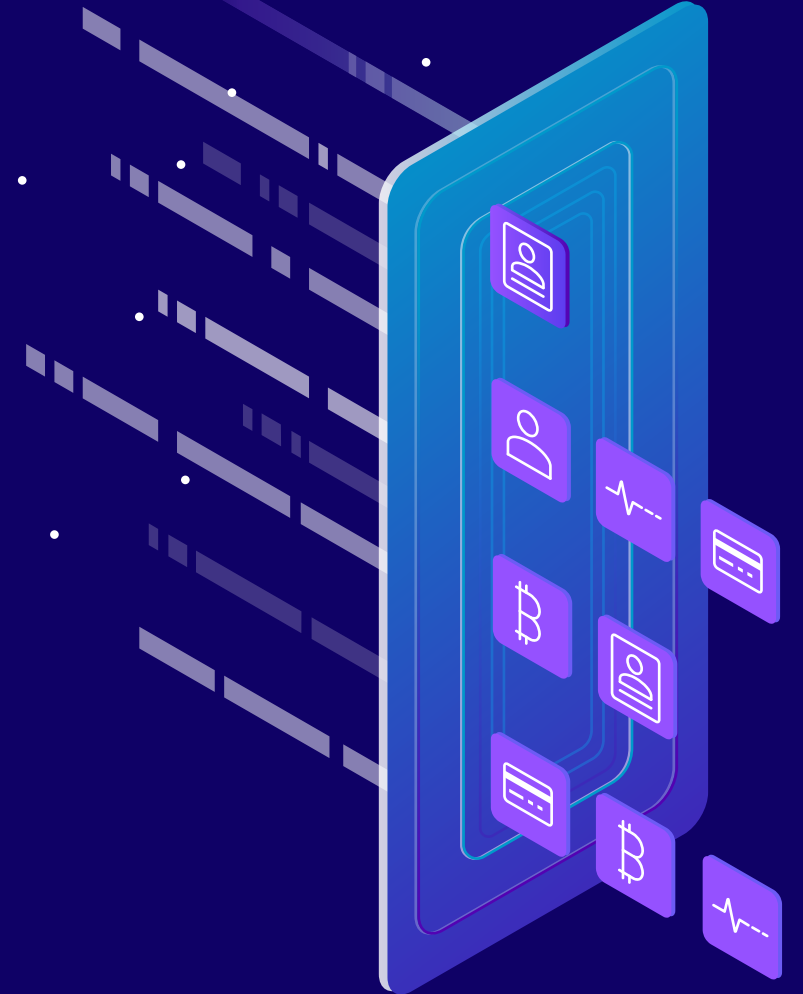
With Nightfall, users can create multiple detection rules that specify whether data is deemed sensitive in any instance, or whether it is deemed sensitive only in combination with other data. This provides granular control over the organization's unique definition of what constitutes sensitive data, further reducing false positives and noisy alerts.



How does DLP work?

DLP helps organizations:

- Discover sensitive data within designated environments.
- Classify data on the basis of predefined token types, like PHI, PII, and other industry standard sensitive data types.
- Protect data with manual or automated redaction, quarantine, or deletion of offending content.



What is Nightfall?

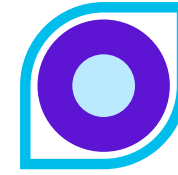
Nightfall is a platform to discover, classify, and protect sensitive data across cloud SaaS & cloud infrastructure. Nightfall supports compliance efforts with a number of industry standards like PCI-DSS, GDPR, HIPAA, CCPA, and more. Additionally, Jira is just one of the many platforms Nightfall secures. You can protect data across all your SaaS apps with our native integrations for Confluence as well as Slack, GitHub, and more — or build completely custom solutions for other systems with the Nightfall Developer Platform.

Nightfall works by continuously monitoring data changes in cloud applications, and classifying that data with machine learning. Data marked as sensitive can be automatically quarantined, deleted, and redacted with workflows.

Nightfall's best-in-class DLP includes machine learning based optical character recognition (OCR) for unstructured data, enterprise-grade security, and high accuracy detection via deep learning — all within a single pane of glass, with an intuitive UI for configuring policies.

Key benefits

- Leverage pre-tuned, machine-learning trained detectors out of the box.
- Customizable, configurable, and flexible DLP for all your Confluence Pages and Spaces.
- Deploy a targeted remediation strategy with comprehensive, context-rich scan results that contain direct links to violations in Jira.



Discover

Continuously monitor data that is flowing into and out of data silos.



Classify

Machine learning classifies sensitive data & PII automatically



Protect

Automated workflows for quarantine, deletion, redaction, alerts, and more.



What are the key features of Nightfall DLP for Jira?

Nightfall helps organizations manage DLP in Jira with these features:

- **Setup in minutes.** Quickly and easily connect Nightfall to your Jira in minutes with our out of the box integration.
- **Apply different detection rules to every Project.** Discover sensitive data across all Jira projects. Different rules can be applied to different Jira projects, allowing you to have further control over when and where Nightfall detects specific types of sensitive data.
- **Fully customize your scans.** Configure granular Detection Rules and set confidence levels within the Nightfall dashboard to determine which data is considered sensitive, either standalone or in combination with other data. Build flexible data detection policies based on custom data detectors (e.g. regexes & word lists) and multiple policies to target your DLP scans to certain locations or timeframes.
- **Detail-rich notifications.** Context-rich notifications allow you to see exactly when and where violations occur. Receive notifications in Slack, email, or to a SIEM via webhook. From each alert you can manually redact or delete violations and notify offending users. Alternatively, leverage Nightfall workflows to automate remediation.
- **Dozens of machine-learning detectors.** Nightfall's robust detection engine leverages dozens of detectors, including our proprietary machine-learning trained detectors to detect a wide range of sensitive content types such as standard PII (names, ID numbers, financial information, and addresses) credentials & secrets, custom regexes & word lists, and more.

Jira

Policies Settings

Nightfall will scan your organization's Jira for policy violations in real-time and will send alerts to the alert channels configured in your Jira's **Settings**.

Last updated	Policy name	Detection rule(s)
15 July 2020	Secrets & Credentials Scan engineering projects for secrets	Secrets and Credentials
10 July 2020	High-risk PII Scan all of Jira for high-risk PII.	General PII

What types of data can Nightfall detect?

Nightfall's broad set of machine learning trained detectors accurately scan & classify data that developers stream to our API. We classify an average of 8M instances of sensitive data per month, providing best-in-class accuracy on structured and unstructured data alike. Find tokens in strings, documents, images, and a wide range of file types, including Google proprietary files types. Here are a few examples:



Standard PII: Age, Credit Card Number, Email, Ethnic Group, Name, Location, Phone Number



Health: ICD, FDA, DEA, NPI, DOB, US Health Insurance Claim Number, British Columbia Personal Health Number, Ontario Health Insurance Plan, Quebec Health Insurance Number



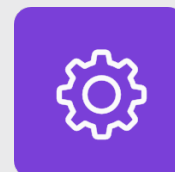
Finance: IBAN, SWIFT, CUSIP, Routing Numbers, US Employer ID, Canada Bank Account



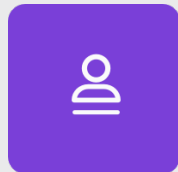
Secrets: Cryptographic Key, API Key, Randomly Generated Token, Database Connection String, Cloud Credentials



Network: IP Address, IMEI Hardware ID, MAC Address



Custom: API Keys (without test keys), Application UUIDs, 12 Digit Number, Name with Email, AWS Access Key, Profanity, Regexes, Word Lists, and more



IDs: Driver's License Number, Taxpayer ID, Passport Number, Social Security Number, Vehicle ID, France CNI, France INSEE, France Passport, German Identity, Ireland PPSN, Ireland Passport, Canada Drivers License, Canada Government ID, Canada Passport, Canada Permanent Resident, Canada Social Insurance

Want to learn more about Nightfall?

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

[Request a demo](#)

About Nightfall

Nightfall is the industry's first cloud-native DLP platform that discovers, classifies, and protects data via machine learning. Nightfall is designed to work with popular SaaS applications like [Slack](#), [Google Drive](#), & [GitHub](#) as well as IaaS platforms like [AWS](#). Developers can build custom solutions in any SaaS app with the [Nightfall Developer Platform](#).



Nightfall