e-guide

Atlassian Confluence
Collaboration and Data Security

Ensuring Compliance and Reducing Data Exposure with Automated Data Discovery

SecurEnvoy
A Shearwater Group plc Company

Executive Summary

Collaboration tools, such as Atlassian Confluence make our work life easy and businesses more effective with data sharing. But, at the same time, this easy data-sharing environment also comes with a huge challenge: How do you track and secure sensitive data when the data itself is so easily shared by users?

In this e-Guide, we'll take a look at how it is possible to ensure compliance and reduce the risk of exposing sensitive data by using automated data discovery and remediation.

Automated data discovery reduces the burden on data security teams to carry out manual processes to track data, subsequently lowering the potential for inaccuracies and out-of-date information. The option for real-time remediation by users, made possible with data discovery tools, also ensures that any sensitive data issues can be resolved immediately by the data users themselves.

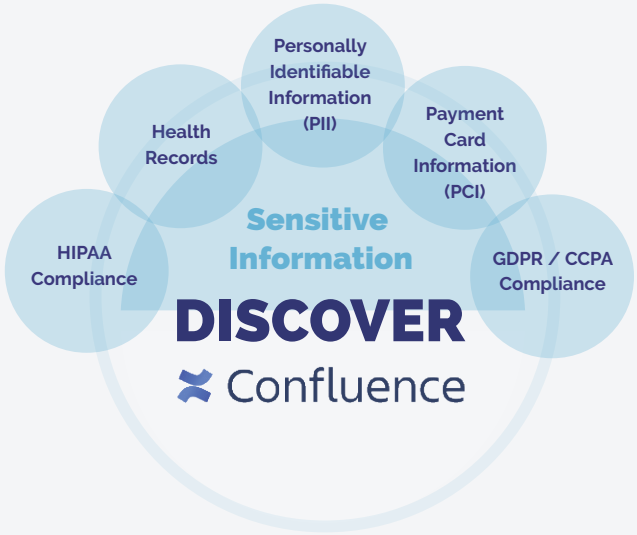
Read on to find out more.

Contents

Do you know what sensitive data is in your Atlassian Confluence?

With the proliferation of data everywhere, collaboration tools, such as Atlassian Confluence have come into their own, making data sharing, storing and tracking incredibly straightforward for organisations, departments and teams. However, the nature of collaboration tools, with their easy data sharing, also means that it is incredibly easy to share sensitive information by mistake. Information shared might be internally sensitive, such as business plans, financial information and project budgets, but also may include sensitive information that is external to the organisation, such as customer data - Personally Identifiable Information (PII), health records, national insurance numbers, and so on.

Keeping track of sensitive data within collaboration tools is not straightforward. Data discovery and tracking tools are not built into Atlassian Confluence and organisations often find themselves resorting to manual processes to find sensitive data, which can be fraught with problems, such as inaccuracies down to human error and a lack of constant sensitive data tracking that could leave companies open to the risk of a data security breach and resulting fines.



Why manual data tracking doesn't work

Checking for sensitive data via a manual process comes with a host of problems, not only the risk of inaccuracies, which can result in costly mistakes from a data protection perspective, but there are also disadvantages from a cost perspective. Setting up a manual process requires a large number of person-hours to perform, the need to take staff away from other tasks, or the recruitment of outside contractors to carry it out. Managing sensitive data is also an ongoing task. Collaboration is dynamic, and the information in Atlassian Confluence is constantly changing, so while a manual audit may be helpful to start, data changes constantly and needs to be tracked constantly.

In this e-book we'll take a look at how tools like SecurEnvoy Data Discovery can help automate this process, making it easy to track sensitive data and reduce the risk of non-compliance with data protection regulations.

Disadvantages of using manual processes for sensitive data tracking

Steps in setting up an automated data discovery process in Atlassian Confluence

1) Data Governance and Compliance – Set up clear policies on how sensitive data should be handled and stored

Whether you are looking to set up a manual or automated process to discover the sensitive data stored in your collaboration software, the first step is always to set up the policies and procedures to manage the sensitive data in your system. Data compliance requirements, such as GDPR, SOX, HIPAA and other industry standards, are the key driver towards establishing rules for data handling, retention and deletion within Atlassian Confluence.

2) Ensure Employee Awareness

To err is human. Honest mistakes can be made by users. Lack of awareness can lead to inadvertent or improper data handling practice and individuals may also be unaware of the policies that are in place and violate them accidentally. Once you have established policies and procedures, educating Atlassian Confluence users about the importance of data security and best practices for handling sensitive information is a must.

3) Actively scan for sensitive data with SecurEnvoy Data Discovery

Having a policy in place will help prevent sensitive data from being mishandled and educating users is a good start, but it will not actively find or stop data from being inadvertently posted, nor will you be able to automatically record any potential data handling violations. This is where a tool such as SecurEnvoy Data Discovery can help you understand the sensitive data you have and help you implement policies consistently, reducing the risk of mistakes made via human error.

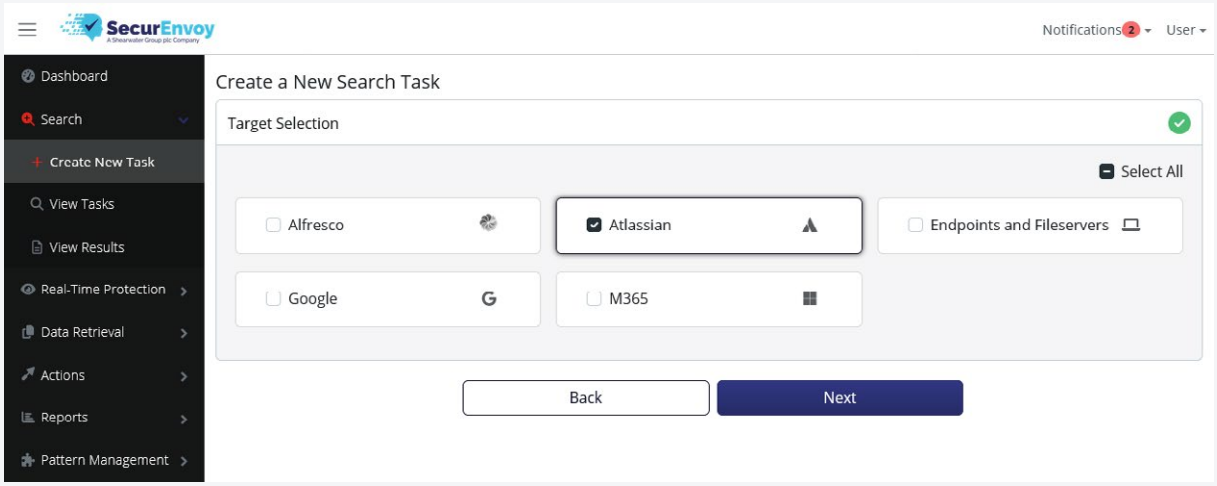
SecurEnvoy Data Discovery enables you to scan for potentially sensitive information in your Atlassian Confluence knowledge bases along with other places where data is held, such as endpoints and file servers.

- Set up your own rules for defining and searching for sensitive data. While SecurEnvoy Data Discovery does provide standard sensitive data types, it also provides the flexibility to define your own specific sensitive data types and set up searches by different project names.
- Mitigate risk – by classifying data according to its sensitivity level and implementing tagging of sensitive data for follow-up action by users
- Improve accuracy – having set up rules (such as finding credit card or national insurance numbers) SecurEnvoy Data Discovery will automatically find them, every time, without the risk of human error.
- Real-time 24 x 7 scanning – to identify sensitive information. Sensitive data scanning that never sleeps!
- Reduce costs – by using automated data audits, rather than time-consuming and costly resources to carry out manual checks.

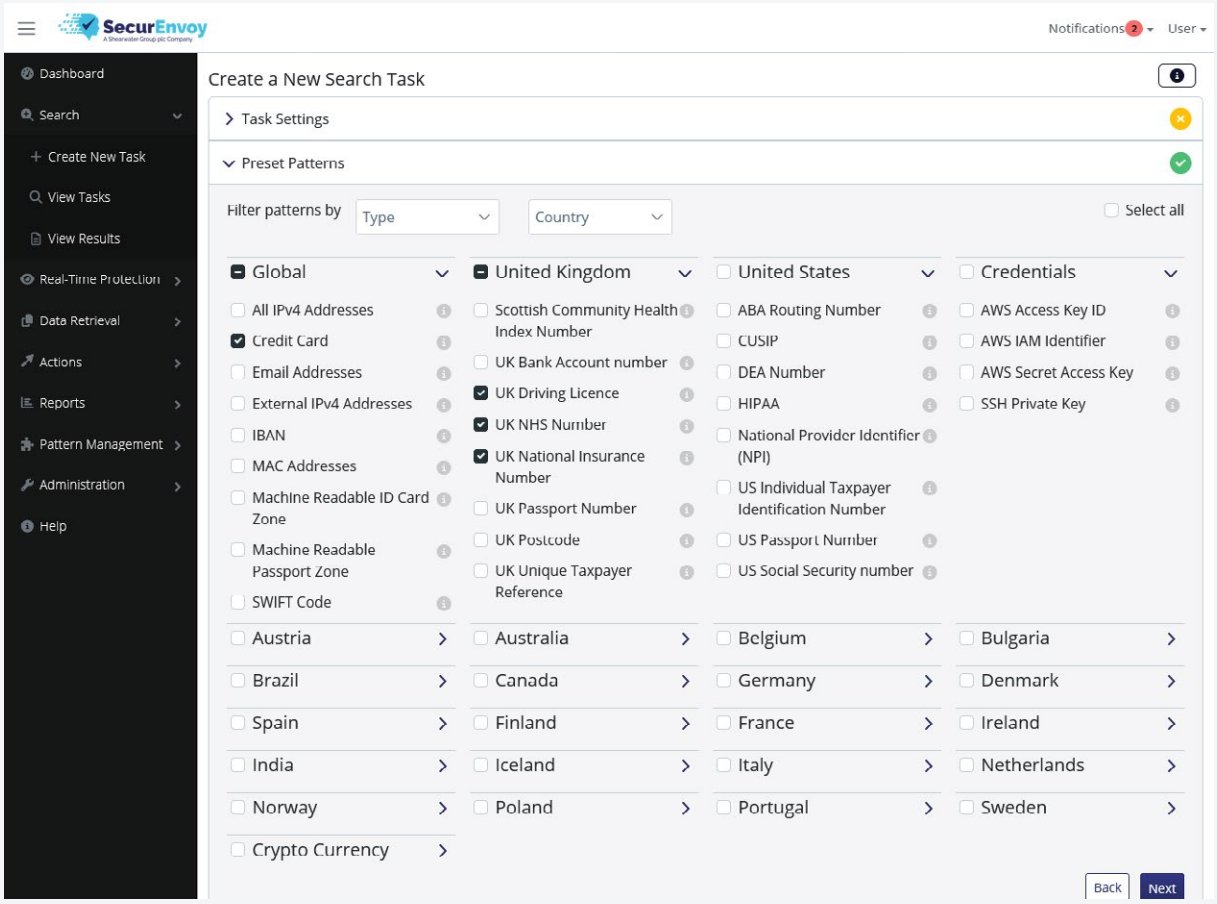
Learn how an International bank reduced their costs by 93% with SecurEnvoy Data Discovery >

How to build a search in SecurEnvoy Data Discovery

Create Search in Atlassian

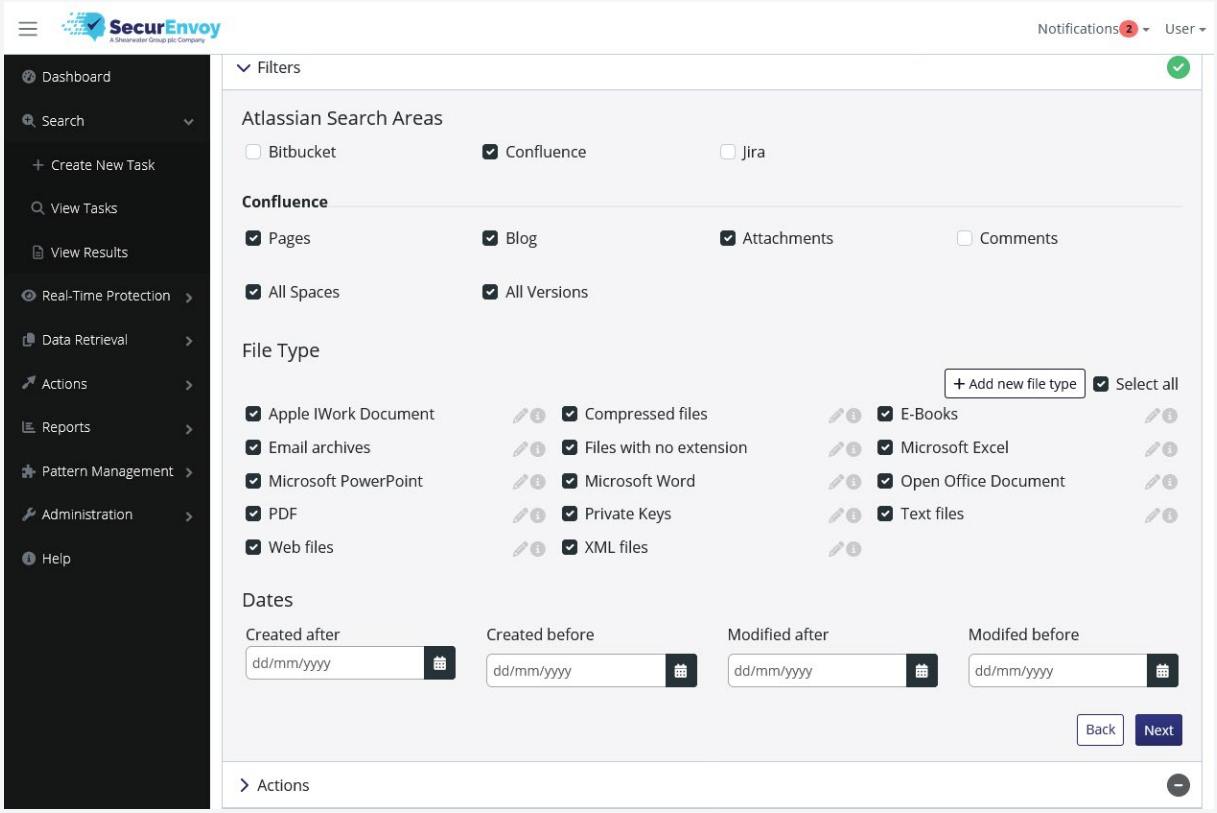


Select Data Types



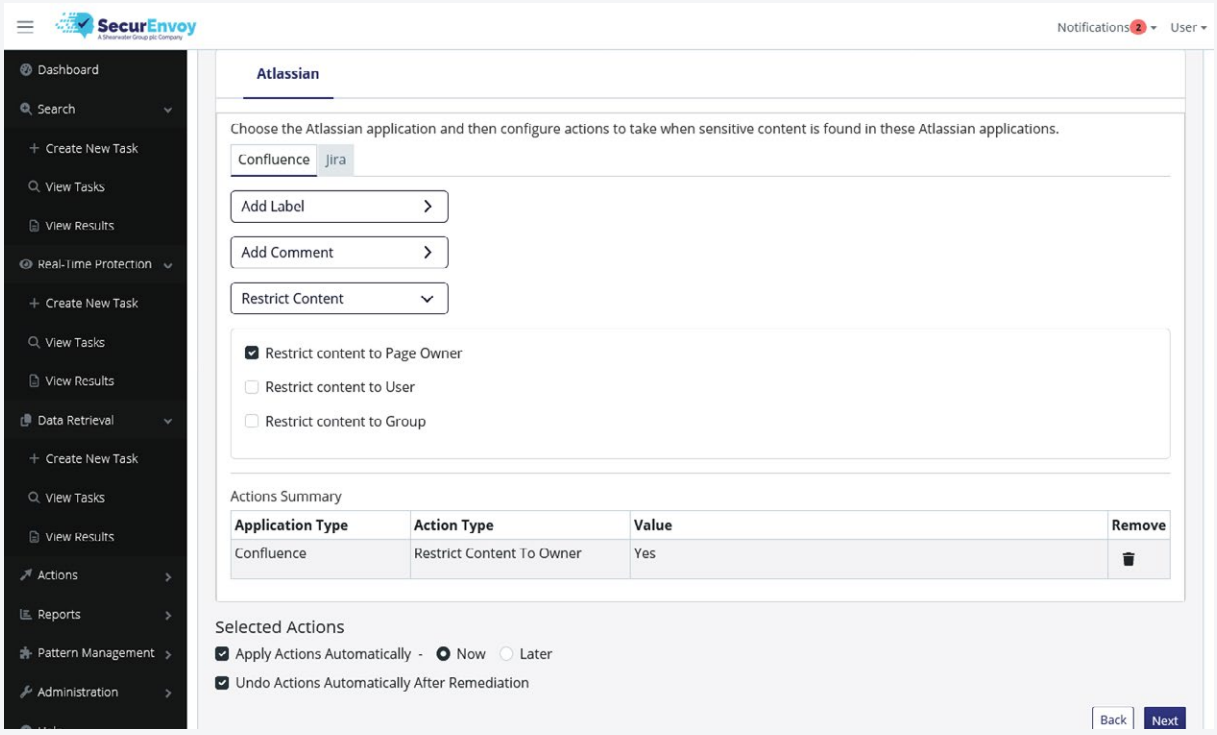
Select from a range of sensitive data including Personally Identifiable Information (PII), Payment Card Information (PCI), Intellectual Property (IP), HIPAA, and GDPR-related information. You also have the flexibility to include your own custom search terms.

Select File Types



Real time sensitive data discovery can be performed on unstructured data in Atlassian solutions, in the cloud, data centre or on a server.

Define Remediation Actions



WATCH SECURENVOY DATA DISCOVERY IN ACTION >

Take control of data remediation in Atlassian Confluence

Data Users are notified of sensitive data in real-time for immediate action

- **Real-time Alerts and Audit Trails** – instant notifications and detailed audits are provided to data owners for immediate awareness and action
- **Automated User Remediation** – Prompt alerting mechanisms are coupled with streamlined remediation processes.

Managing the remediation process

- **Streamlined Permission Management** – Integrated access control enables efficient revoking and reinstatement of permissions before and after remediation to ensure seamless workflow continuity.
- **Deferred Actions** – A timeline can be set for permissions remediation, allowing users to address issues before access restrictions are enforced.
- **Adjustable scan intensity** – With customisable settings you can manage the scan load to prevent overwhelming data resources and to ensure that normal operations remain undisturbed.

SecurEnvoy Data Discovery– a comprehensive sensitive data discovery, monitoring, user remediation solution

SecurEnvoy Data Discovery for Atlassian Confluence lightens the load of monitoring and managing sensitive data and remediating issues with:

Data Discovery and Monitoring
✓ Tracks new and edited content. Configurable up to and including all spaces, all pages, all blogs, all attachments, all comments, and all versions.

Data Extraction
✓ User-friendly dashboard and executive reporting.

Data Migration
✓ Locate your data easily, ready for migrating to the cloud.

Data Protection
✓ Restrict content and security levels.

Data User Remediation
✓ Data users are notified of sensitive data issues in real-time for immediate action to be taken.

Conclusion

Collaborative features in Atlassian Confluence, such as shared workspaces are an integral part of how we work today, but these same features can increase the risk of unauthorised access to data or accidental exposure of sensitive information. Balancing the need for collaboration with the need to protect sensitive data is difficult to achieve without tools that can automate the data discovery and remediation processes,

With SecurEnvoy Data Discovery for Atlassian Confluence, you don't have to compromise on data security.

Learn more about SecurEnvoy Data Discovery for:

Atlassian Jira >
Atlassian Bitbucket >

SecurEnvoy
A Shearwater Group plc Company

The SecurEnvoy Zero Trust Access Solution

The SecurEnvoy Zero Tust Access Solution allows organisations to provide verifiable trust in every action taken.

By providing the identity of the user, the device and the data they are working on you can monitor and prove exactly who is doing what at any time.

Let's Talk

Talk to our experts today for a No-hassle, No Obligation Consultation.

support@securenvoy.com
securenvoy.com
linkedin.com/company/securenvoy
twitter.com/securenvoy