Compliance for Confluence

Customer Story

ViNotion

Making surveillance smart

Tightening sensitive data controls, complying with ISO 27001, and simplifying DLP best practice.

AppFox

Table of contents

ViNotion, a tech innovator working with sensitive information, needed to confidently automate document classification, tighten access controls, and stay ISO 27001-compliant.

Compliance for Confluence was adopted to meet those needs, helping mitigate the risk of data breaches which can cost hundreds of millions of dollars and the loss of customer trust.*

Customer overview

At a glance

Faced with strict security requirements from clients in highly regulated industries, ViNotion needed a way to manage and protect sensitive information flowing through their Confluence instance - without placing additional burden on time-strapped team members.

Enter **Compliance for Confluence**.

Discover how ViNotion embedded a streamlined, automated solution to classify content, restrict access and maintain compliance with ISO 27001 standards, all while making security practices more intuitive for everyday users.

Customer profile

ViNotion provides advanced Vision AI for real-time image analysis in defense, mobility, and industry. Its customer-base includes government bodies and highly regulated entities for whom data security is especially important.

With a lean operations team managing everything from engineering and project delivery to customer support and device management, efficiency and security aren’t just desirable - they're business-critical.

ViNotion
Making surveillance smart

Industry: Software / SaaS

Founded: 2007

HQ: The Netherlands

Team profile: Compliance officers

Use case: Sensitive data classification and page access control automations at scale for a lean team working with highly confidential information.

The Challenge

ViNotion had long relied on Confluence for documentation and collaboration.
But as the company grew and began working more deeply with sensitive data - from personal customer information to confidential analytical outputs - so did the pressure to secure and control access to this data.

At the same time, the company needed to:

- **Comply with ISO 27001** and internal ISMS standards
- **Prevent accidental data exposure** inside Confluence
- **Reduce administrative overhead** for security controls
- **Simplify and standardize** classification and restrictions for all users
- Replace a legacy on-premise solution with a **cost-effective Cloud alternative**

> According to IBM, **83% of companies will experience a data breach at some point**, and the average cost of a breach in 2023 was **$4.45 million**. Furthermore, recent reports from Gartner, highlight how **70% of data breaches involve internal factors**, often unintentionally.
> As more teams store increasing levels of sensitive data in tools like Confluence, it's **critical to embed access control and classification - directly into the content lifecycle**.

*estimates are based on statistics produced by IBM

The Solution

After reviewing several options, ViNotion selected **Compliance for Confluence** as the solution that best balanced security, usability, and budget.

> *Considering our type of technology and application domain, we are always aiming to* ***improve our security when processing highly sensitive data****, especially with the amount of regulated information flowing through our Confluence spaces.*
> ***We needed to know who could access what, when, and why****. But we didn't want to burden users with more decisions or manual processes.*

It was quickly adopted by both technical administrators and non-technical users, including Security Officers, due to the key benefits it brought:

- **Classification Levels:**
  Pages can be tagged with sensitivity levels (e.g., Internal, Confidential, Restricted)
- **Automated Permission Controls:**
  Based on classification, access restrictions are applied automatically. No guesswork required
- **Ease of Use:**
  A simple UI that lowered the barrier for proactive participation in data protection
- **Cloud-Ready:**
  An ISO-compliant, Cyber Essentials Plus-certified, Cloud Fortified app that filled the gap left by ViNotion's previous Server-based tool whilst also providing Sensitive Data Detection functionality

Using the tool, **Security Officers no longer have to manually lock down pages or interpret policy** every time they write something. The classification levels do the thinking, and the restrictions happen automatically.

ViNotion were also able to **easily embed Compliance for Confluence within the company's onboarding process**, ensuring that data protection is a focus from Day One of an employee's experience, rather than simply an afterthought.

The Result

ViNotion felt the tangible benefits of:

- **Stronger control over access to sensitive data**, aligned with ISO 27001
- **Reduced cognitive load** for users when classifying and securing content
- **Faster onboarding** with security baked directly into documentation workflows
- **A smooth transition to Cloud** after Atlassian's Server sunset
- **One of the most cost-effective compliance solutions** evaluated across the Marketplace

> *“We needed to know who could access what, when, and why – but we didn't want to burden users with more decisions or manual processes.”*

5 ways to make Compliance for Confluence do the work for you

Compliance for Confluence is built to empower both admins and everyday users with automated, intuitive classification and access control. Here’s how to replicate the same results achieved by ViNotion using built-in features, policy automation, and user-friendly workflows.

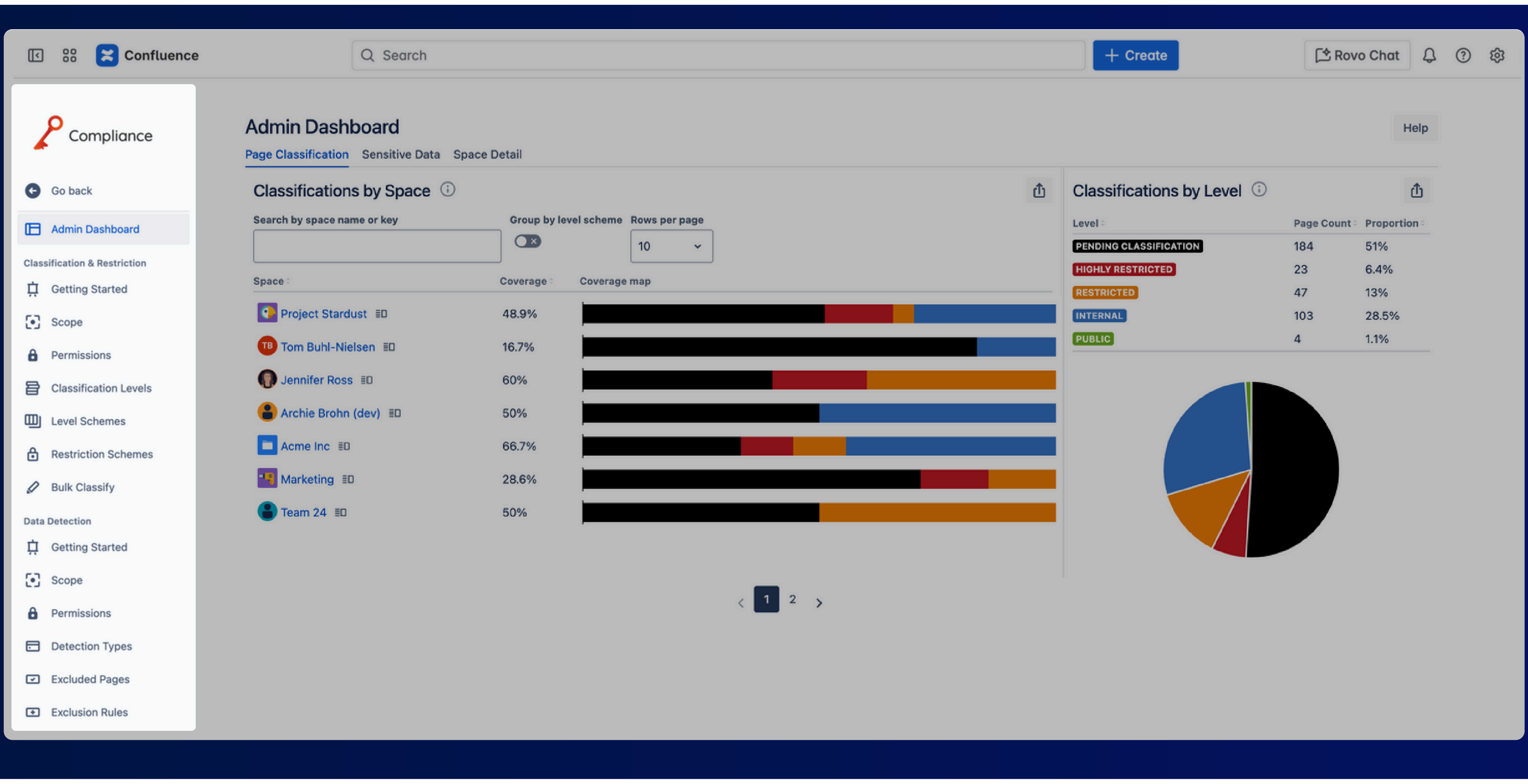
Install and open and the app

1. Install Compliance for Confluence from the Atlassian Marketplace.

2. As a space or Confluence admin, access the workflow builder via:
   - Global Settings → Compliance Configuration

From here, you can:

- Define classification levels
- Set up permission rules
- Enable Sensitive Data Detection
- View audit trails and export compliance logs



Admin Dashboard

Classifications by Space

Space	Coverage	Coverage map
Project Stardust	48.9%	
Tom Buhl-Nielsen	16.7%	
Jennifer Ross	60%	
Archie Brohn (dev)	50%	
Acme Inc	66.7%	
Marketing	28.6%	
Team 24	50%	

Classifications by Level

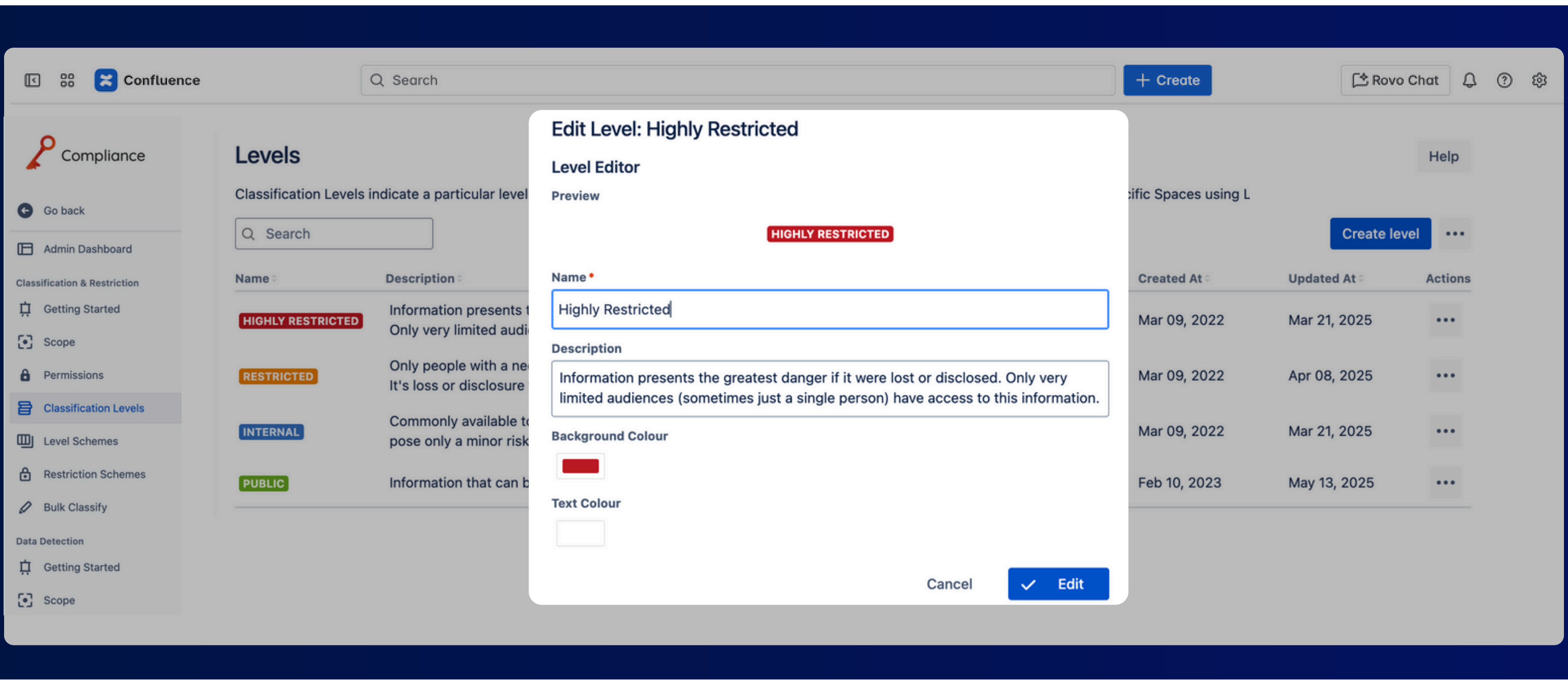
Level	Page Count	Proportion
PENDING CLASSIFICATION	184	51%
HIGHLY RESTRICTED	23	6.4%
RESTRICTED	47	13%
INTERNAL	103	28.5%
PUBLIC	4	1.1%

1. Define Your Classification Levels

Classification levels allow you to clearly label a page based on sensitivity, and even further, depending on the type of document it is.

Go to **Compliance Configuration → Classifications**, then:

- Click **Create level**
- Create labels such as *Public, Internal, Confidential, Restricted*
- Assign visibility rules per level:
  - Who can view/edit
  - Which user groups have override permissions
  - Whether users will be prompted to classify a page before publishing
- Empower users to add Classification Levels directly into pages using the interactive page classification lozenge in the top left of any Confluence page



Edit Level: Highly Restricted

Level Editor

Preview

HIGHLY RESTRICTED

Name *: Highly Restricted

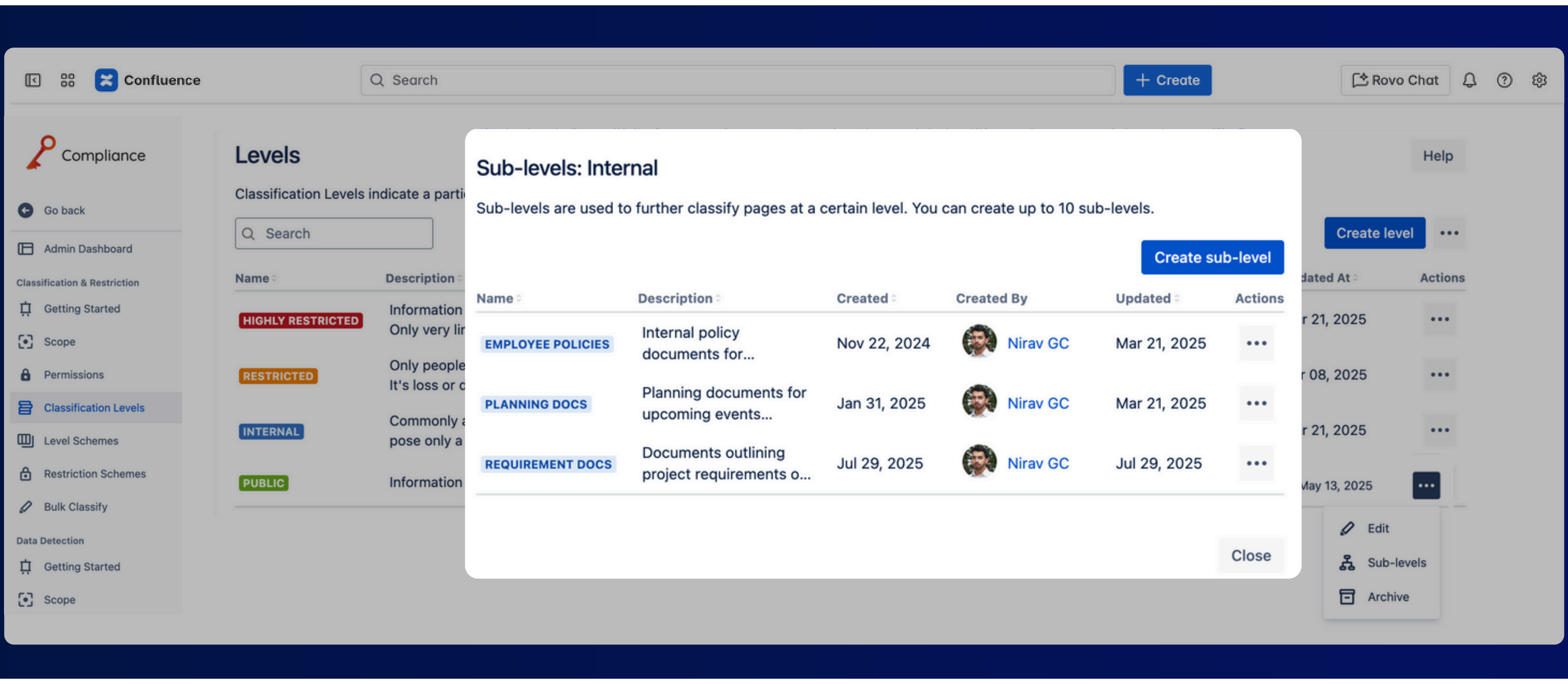
Description: Information presents the greatest danger if it were lost or disclosed. Only very limited audiences (sometimes just a single person) have access to this information.

Background Colour: 🟥

Text Colour: □

Cancel | ✓ Edit

Optional: Create Sub-levels within a specific level for an extra layer of information and granularity *(eg. Internal > Employee Policies)*



Sub-levels: Internal

Sub-levels are used to further classify pages at a certain level. You can create up to 10 sub-levels.

Create sub-level

Name	Description	Created	Created By	Updated	Actions
EMPLOYEE POLICIES	Internal policy documents for...	Nov 22, 2024	Nirav GC	Mar 21, 2025	•••
PLANNING DOCS	Planning documents for upcoming events...	Jan 31, 2025	Nirav GC	Mar 21, 2025	•••
REQUIREMENT DOCS	Documents outlining project requirements o...	Jul 29, 2025	Nirav GC	Jul 29, 2025	•••

Close

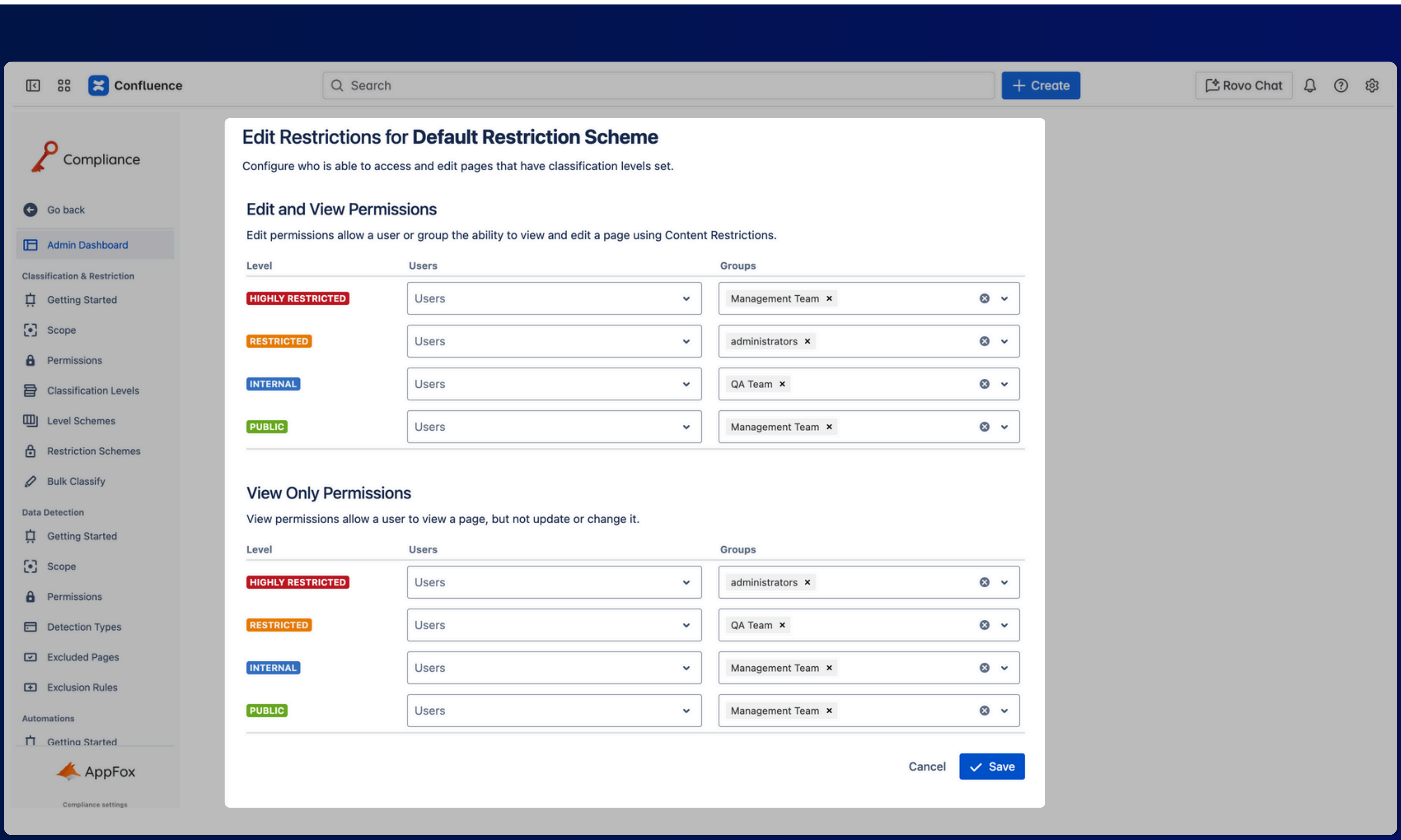
2. Automate Access Controls

Once classification levels are created, configure automatic access control:

- Navigate to **Restriction schemes**
- Set **restriction rules** based on Confluence user groups
  - Example: Only members of “Security Team” can view “Restricted” pages
- Configure **page edit restrictions** if needed

This ensures users can’t accidentally overshare sensitive data, even if they’re unaware of policy.

No need to rely on individuals to manually restrict content; it happens automatically based on their classification.



Edit Restrictions for **Default Restriction Scheme**

Configure who is able to access and edit pages that have classification levels set.

Edit and View Permissions

Edit permissions allow a user or group the ability to view and edit a page using Content Restrictions.

Level	Users	Groups
HIGHLY RESTRICTED	Users	Management Team ×
RESTRICTED	Users	administrators ×
INTERNAL	Users	QA Team ×
PUBLIC	Users	Management Team ×

View Only Permissions

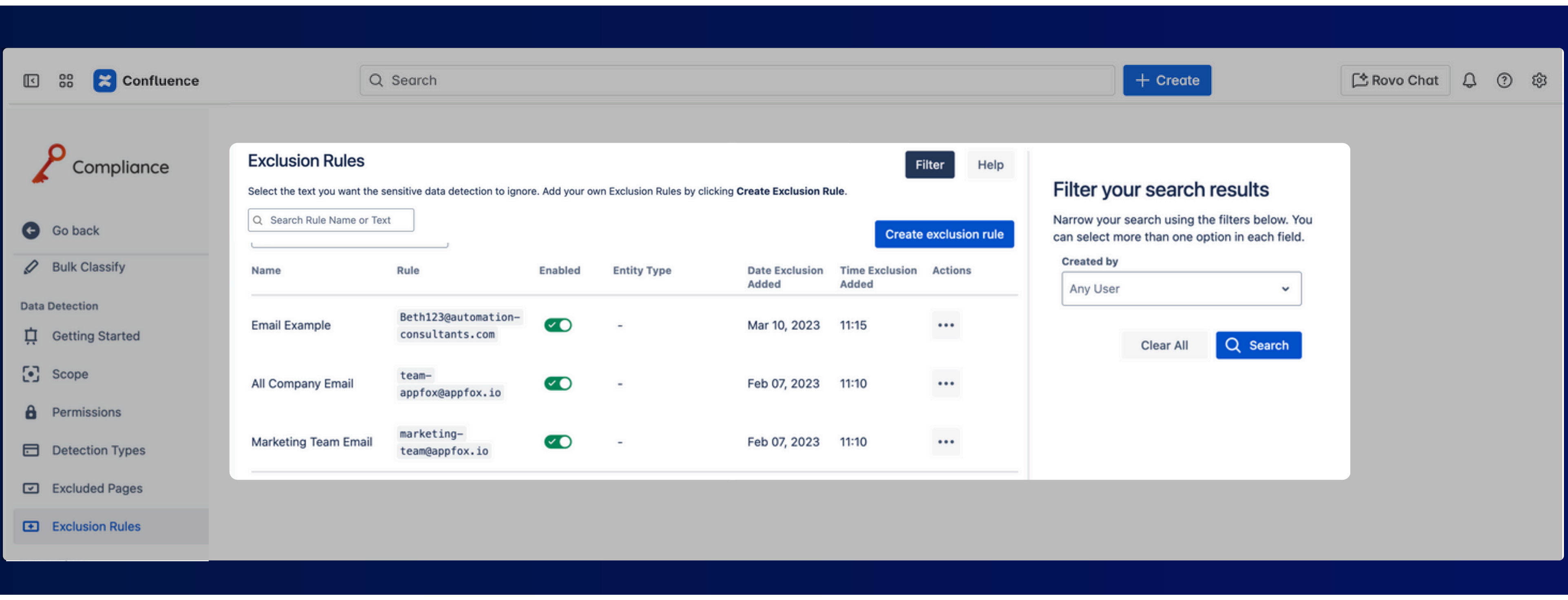
View permissions allow a user to view a page, but not update or change it.

Level	Users	Groups
HIGHLY RESTRICTED	Users	administrators ×
RESTRICTED	Users	QA Team ×
INTERNAL	Users	Management Team ×
PUBLIC	Users	Management Team ×

3. Enable Sensitive Data Detection

Prevention is better than the cure. To catch risks early, turn on **Sensitive Data Detection:**

- Go to **Compliance Configuration → Sensitive Data Detection**
- Enable **exclusion rules** to automatically scan for:
  - Email addresses
  - Personal names
  - Credit card numbers
  - Customizable regex patterns (e.g., internal ID formats)



Exclusion Rules

Select the text you want the sensitive data detection to ignore. Add your own Exclusion Rules by clicking **Create Exclusion Rule**.

Name	Rule	Enabled	Entity Type	Date Exclusion Added	Time Exclusion Added	Actions
Email Example	`Beth123@automation-consultants.com`	✓	-	Mar 10, 2023	11:15	···
All Company Email	`team-appfox@appfox.io`	✓	-	Feb 07, 2023	11:10	···
Marketing Team Email	`marketing-team@appfox.io`	✓	-	Feb 07, 2023	11:10	···

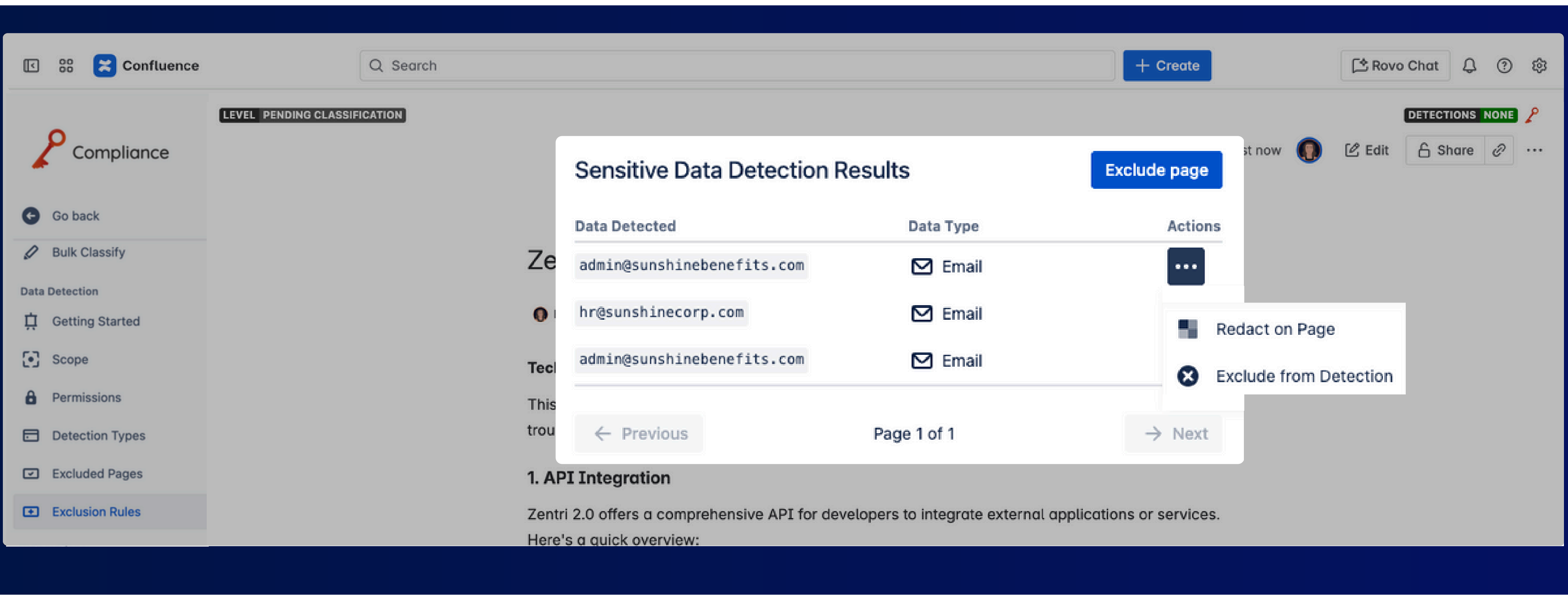
Filter your search results

Narrow your search using the filters below. You can select more than one option in each field.

Created by: Any User

Pages containing these patterns will be flagged automatically and, using the Automation Rules function, can be set up to also:

- Alert the page author
- Immediately add a classification level to a page containing sensitive data
- Set up email notifications for compliance officers
- Redact confidential data from a page the moment it is detected



Sensitive Data Detection Results

Data Detected	Data Type	Actions
`admin@sunshinebenefits.com`	Email	···
`hr@sunshinecorp.com`	Email	
`admin@sunshinebenefits.com`	Email	

Ze

Tec

This

trou

1. API Integration

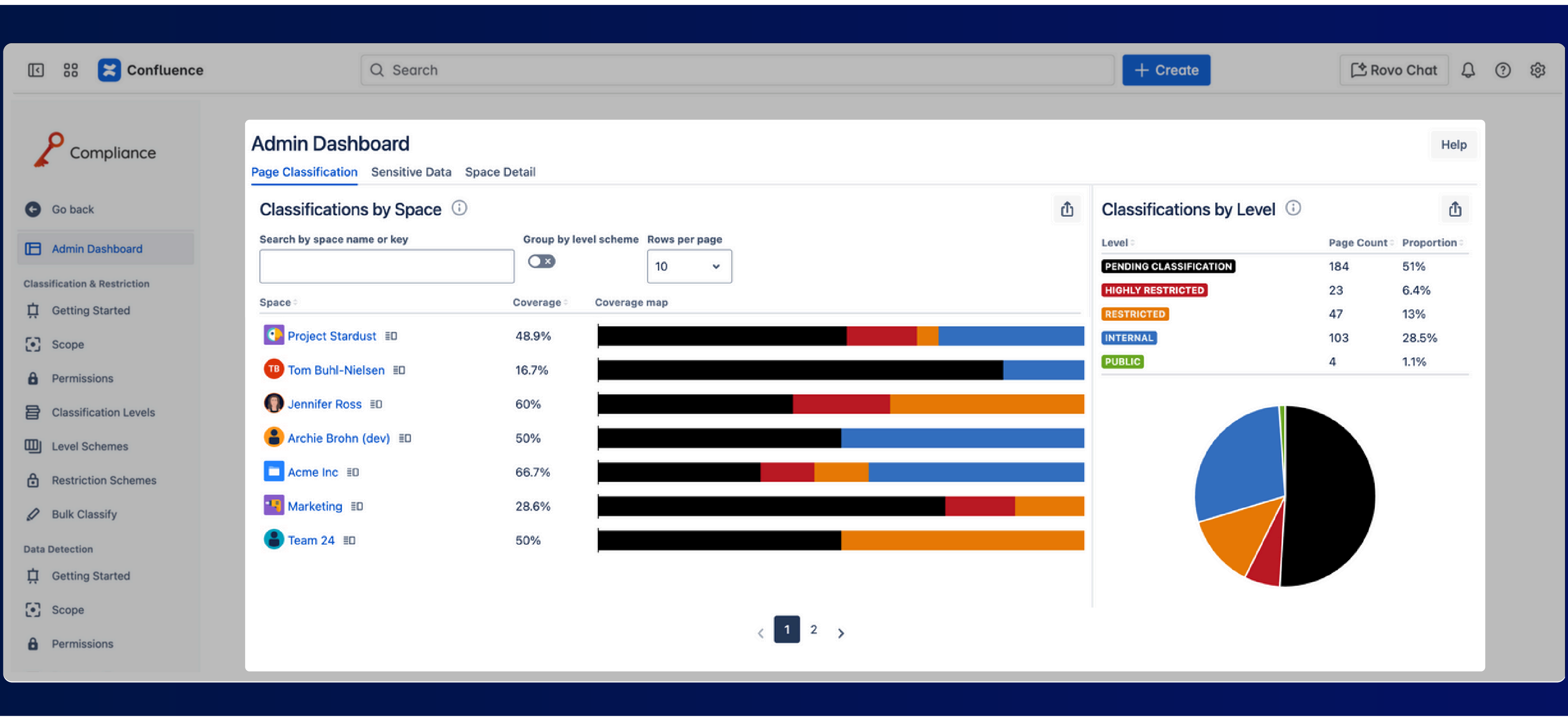
Zentri 2.0 offers a comprehensive API for developers to integrate external applications or services. Here's a quick overview:

4. Monitor Compliance & Export Audit Logs

Maintain visibility and prove compliance with built-in logs and tracking tools.

Go to **Compliance Configuration → Audit Log**, where you can:

- View classification history per page
- See who made classification changes and when
- Export logs in CSV format for ISO 27001 audits or internal reviews



Admin Dashboard

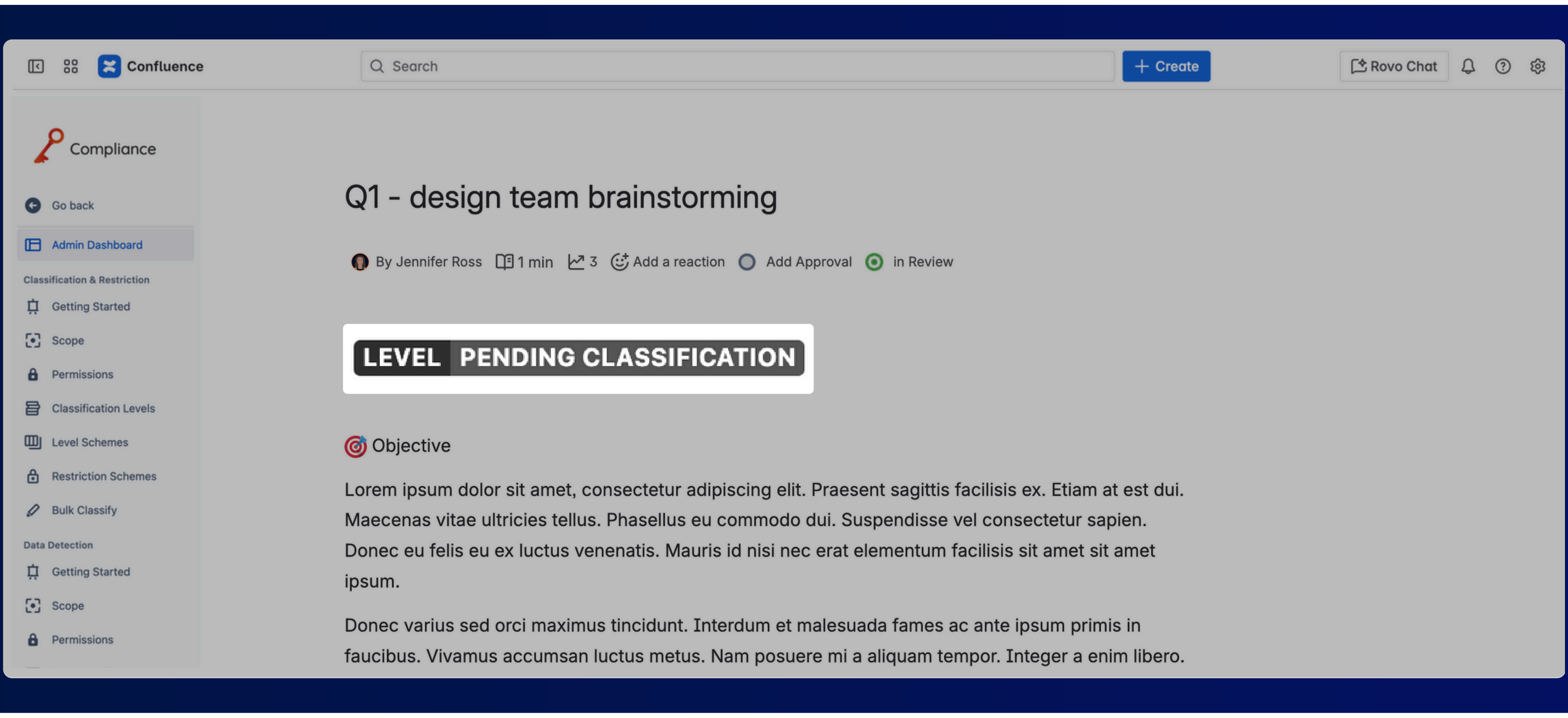
Classifications by Space

Space	Coverage	Coverage map
Project Stardust	48.9%	
Tom Buhl-Nielsen	16.7%	
Jennifer Ross	60%	
Archie Brohn (dev)	50%	
Acme Inc	66.7%	
Marketing	28.6%	
Team 24	50%	

Classifications by Level

Level	Page Count	Proportion
PENDING CLASSIFICATION	184	51%
HIGHLY RESTRICTED	23	6.4%
RESTRICTED	47	13%
INTERNAL	103	28.5%
PUBLIC	4	1.1%

You can also enable **Compliance Macros** to display classification metadata directly on pages (e.g., in footers or headers), making audit readiness part of the user experience.



Q1 - design team brainstorming

LEVEL PENDING CLASSIFICATION

Objective

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent sagittis facilisis ex. Etiam at est dui. Maecenas vitae ultricies tellus. Phasellus eu commodo dui. Suspendisse vel consectetur sapien. Donec eu felis eu ex luctus venenatis. Mauris id nisi nec erat elementum facilisis sit amet sit amet ipsum.

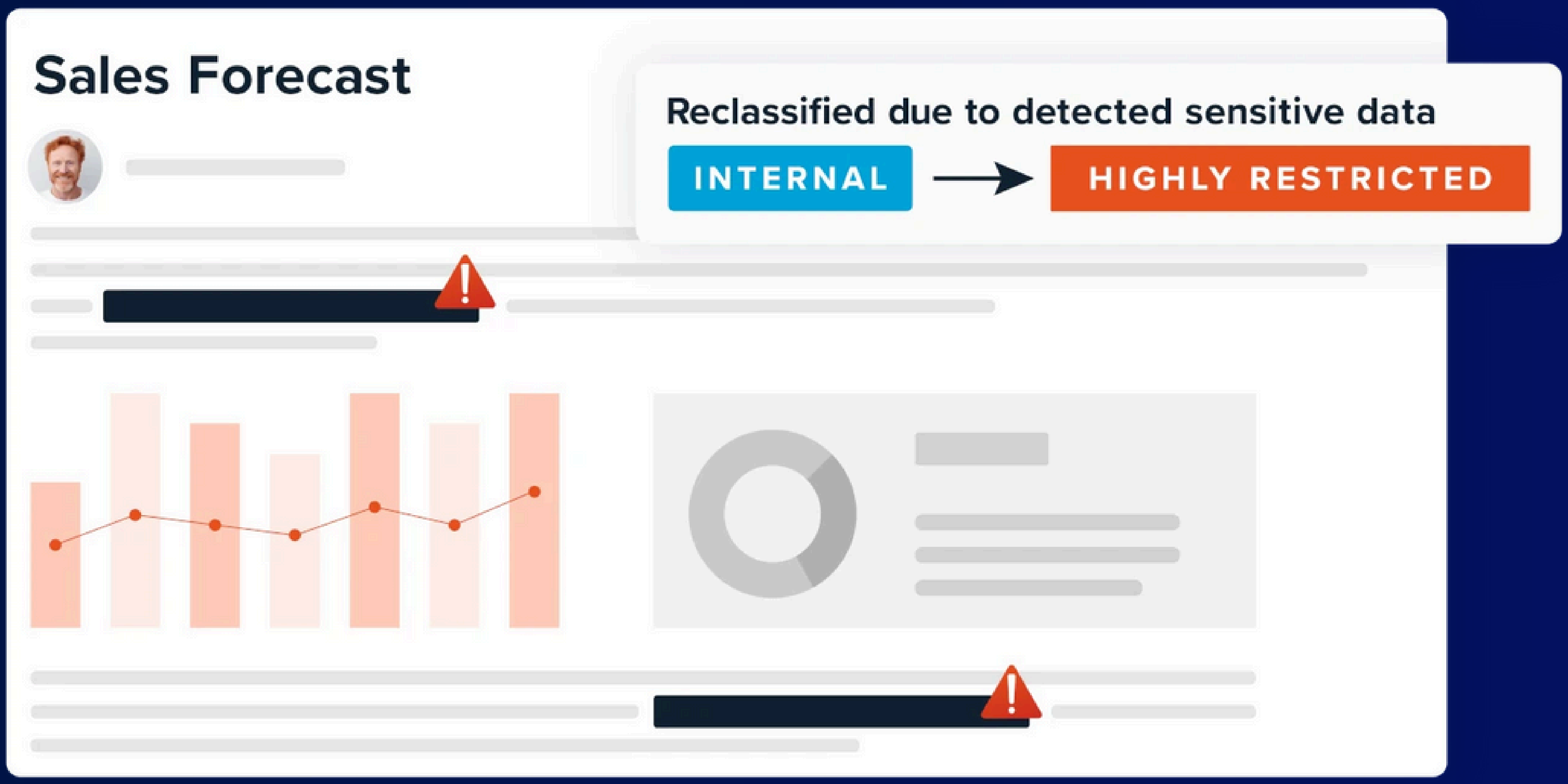
Donec varius sed orci maximus tincidunt. Interdum et malesuada fames ac ante ipsum primis in faucibus. Vivamus accumsan luctus metus. Nam posuere mi a aliquam tempor. Integer a enim libero.

5. Embed Compliance in Templates and Onboarding

To replicate ViNotion’s success in baking compliance into team workflows:

- Create Confluence page templates with pre-inserted classification macros
- Include usage notes in the template to guide employees on selecting the correct level
- Use **Confluence onboarding tasks** to walk new hires through:
  - How to classify content
  - Why it's important
  - Who to contact with questions

When every page starts with the right structure and classification logic, governance becomes second nature.



Built for growth, customization and peace of mind

As your organization grows, your compliance needs will evolve. Compliance for Confluence grows with you.

Update classifications, rules, and user group settings anytime - all changes apply automatically to affected content across your instance.

Monitor Compliance & Export Audit Logs

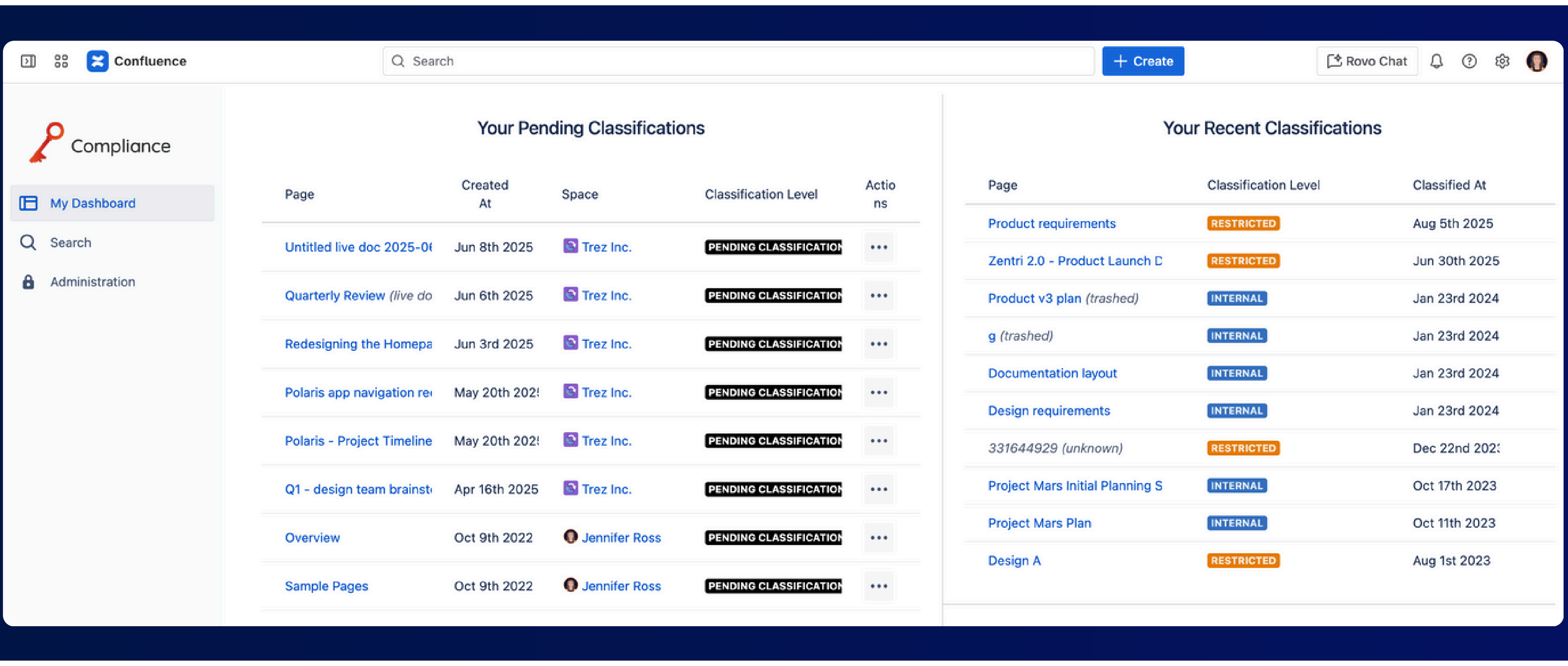
The **Compliance Dashboard** and **Search tools** make it easy to track real-time usage across your instance and refine internal policies or training based on actual data.

Understand at a glance where there is room for improvement

Head to **Apps → Compliance → Dashboard** to get a snapshot of adoption across your spaces. You'll see:

- Number of classified pages per level (e.g., how many are marked Internal, Confidential, Restricted)
- Breakdown by space, helping you identify teams who need support
- Unclassified content, so you can encourage owners to update tags
- Trends over time, showing how classification adoption is evolving

This makes it easy to spot gaps in classification coverage and build targeted training sessions.



Your Pending Classifications

Page	Created At	Space	Classification Level	Actions
Untitled live doc 2025-0(	Jun 8th 2025	Trez Inc.	PENDING CLASSIFICATION	•••
Quarterly Review *(live do*	Jun 6th 2025	Trez Inc.	PENDING CLASSIFICATION	•••
Redesigning the Homepa	Jun 3rd 2025	Trez Inc.	PENDING CLASSIFICATION	•••
Polaris app navigation re	May 20th 202!	Trez Inc.	PENDING CLASSIFICATION	•••
Polaris - Project Timeline	May 20th 202!	Trez Inc.	PENDING CLASSIFICATION	•••
Q1 - design team brainst	Apr 16th 2025	Trez Inc.	PENDING CLASSIFICATION	•••
Overview	Oct 9th 2022	Jennifer Ross	PENDING CLASSIFICATION	•••
Sample Pages	Oct 9th 2022	Jennifer Ross	PENDING CLASSIFICATION	•••

Your Recent Classifications

Page	Classification Level	Classified At
Product requirements	RESTRICTED	Aug 5th 2025
Zentri 2.0 - Product Launch C	RESTRICTED	Jun 30th 2025
Product v3 plan *(trashed)*	INTERNAL	Jan 23rd 2024
g *(trashed)*	INTERNAL	Jan 23rd 2024
Documentation layout	INTERNAL	Jan 23rd 2024
Design requirements	INTERNAL	Jan 23rd 2024
331644929 (unknown)	RESTRICTED	Dec 22nd 202:
Project Mars Initial Planning S	INTERNAL	Oct 17th 2023
Project Mars Plan	INTERNAL	Oct 11th 2023
Design A	RESTRICTED	Aug 1st 2023

Identify all different kinds of usage patterns

Go to Apps → Compliance → Search to dig deeper:

- Filter pages by classification level, creator, last modified date, or space
- Identify pages that were recently downgraded or are missing restrictions
- Monitor whether certain users or teams are over-relying on public/default classifications

Check whether people are applying the right level of classification, detect inconsistent security behavior across teams, and provide guidance to contributors before issues arise.

Take it a step further...

By combining dashboard trends and granular search filters, admins and Security Officers can see how users are engaging with Compliance for Confluence, and where they're struggling.

This enables you to:

- Adjust onboarding materials to focus on the most misunderstood areas
- Proactively coach teams that haven't adopted key practices
- Create feedback loops between policy, documentation, and behavior

No guesswork - just actionable visibility into how well your compliance policies are landing across the business.

Ready to revolutionize the way you use Confluence?

Stay aligned with standards like **ISO 27001**, **automate content classification, and keep sensitive information protected** without slowing your teams down.

Start your free 30-day trial of Compliance for Confluence as today.