Data Security Quick Start

This guide provides some quick and easy steps for you to understand your data security posture, surface the most critical problems, and identify their source.

Before you begin

Make sure that Data Security is configured for your tenant, i.e. your Connector was granted the required permissions and data scans were enabled. Learn more.

Basic workflow

Step 1: Switch to the Data Security view

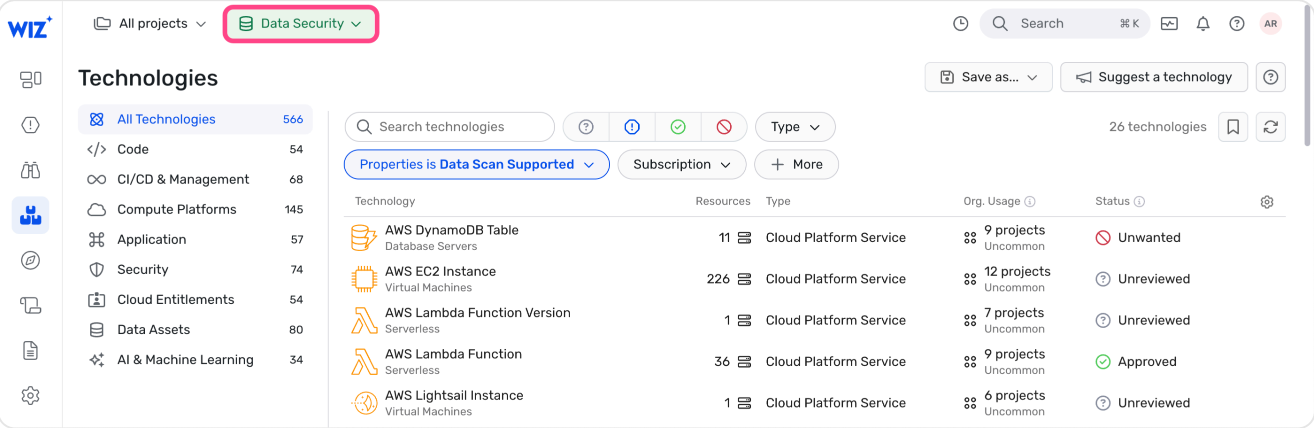
Step 2: Start from the Data Security Board

Step 3: Review and investigate Data Findings

Switch to the Data Security View

Wiz supports custom Views to help you focus on specific risk categories or tasks. When you select the Data Security View, you ensure the portal pages and information you view are relevant to data security. For example, all default menu options such as Boards, Findings, and Technologies, are data-related ones. Learn more about Views.

On any page in Wiz, in the top navigation bar, click View > Data Security.



Technologies

All Technologies	566
Code	54
CI/CD & Management	68
Compute Platforms	145
Application	57
Security	74
Cloud Entitlements	54
Data Assets	80
AI & Machine Learning	34

Technology	Resources	Type	Org. Usage	Status
AWS DynamoDB Table Database Servers	11	Cloud Platform Service	9 projects Uncommon	Unwanted
AWS EC2 Instance Virtual Machines	226	Cloud Platform Service	12 projects Uncommon	Unreviewed
AWS Lambda Function Version Serverless	1	Cloud Platform Service	7 projects Uncommon	Unreviewed
AWS Lambda Function Serverless	36	Cloud Platform Service	9 projects Uncommon	Approved
AWS Lightsail Instance Virtual Machines	1	Cloud Platform Service	6 projects Uncommon	Unreviewed

All menus and pages update to focus on data security. For example, the Inve Technology page lists only the technologies Wiz can scan for sensitive data.

English ▲

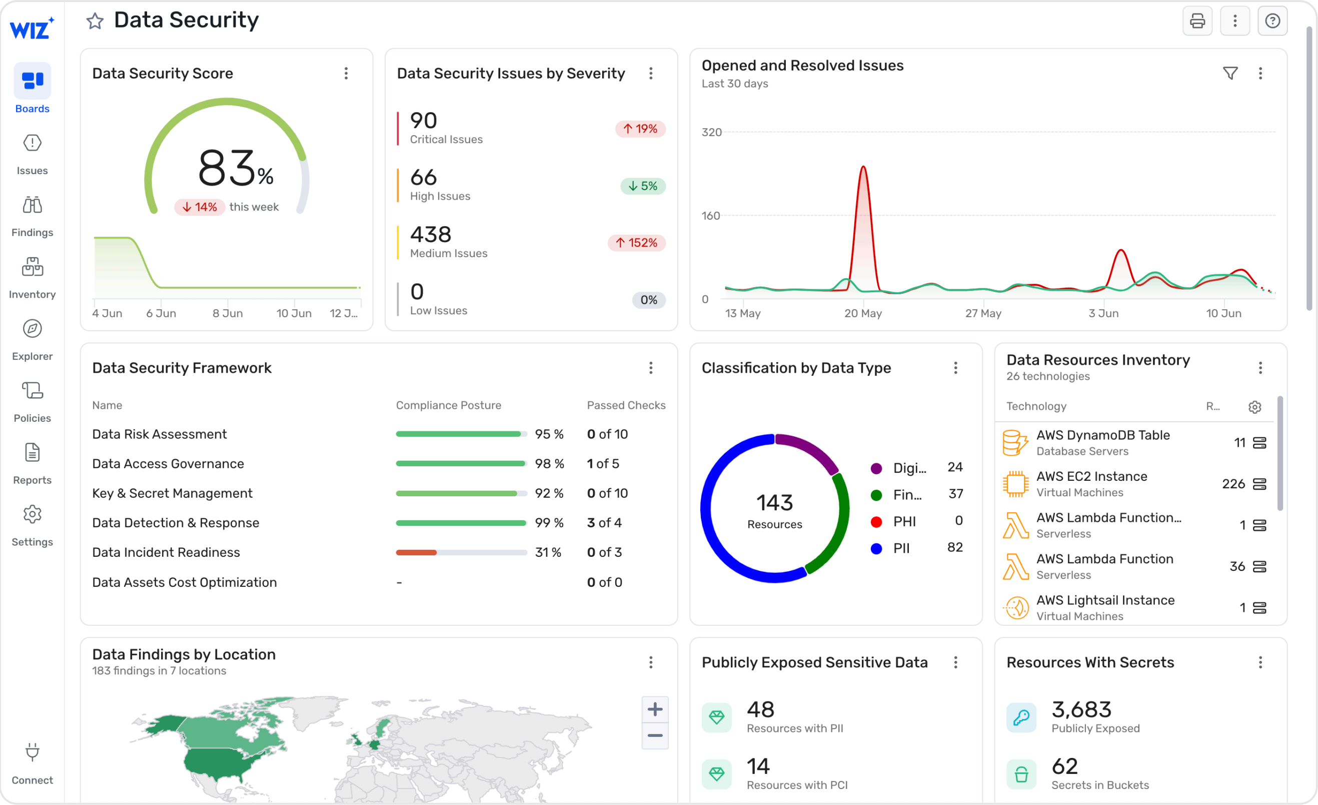
Start from the Data Security Board

The Data Security Board is the best place to start any data-related investigation, as it provides a high-level and visual overview of the most important questions, such as:

- What is my overall data security posture?
- What are my critical Issues?
- Which resources are most vulnerable?
- In which regions is my sensitive data located?

Once you identify the question that interests you, click the corresponding widget to start your investigation. Then you can add more filters and drill down to locate the source of the problem.

1. On the Boards > Data Security page, click any widget to display more information.



Data Security Framework

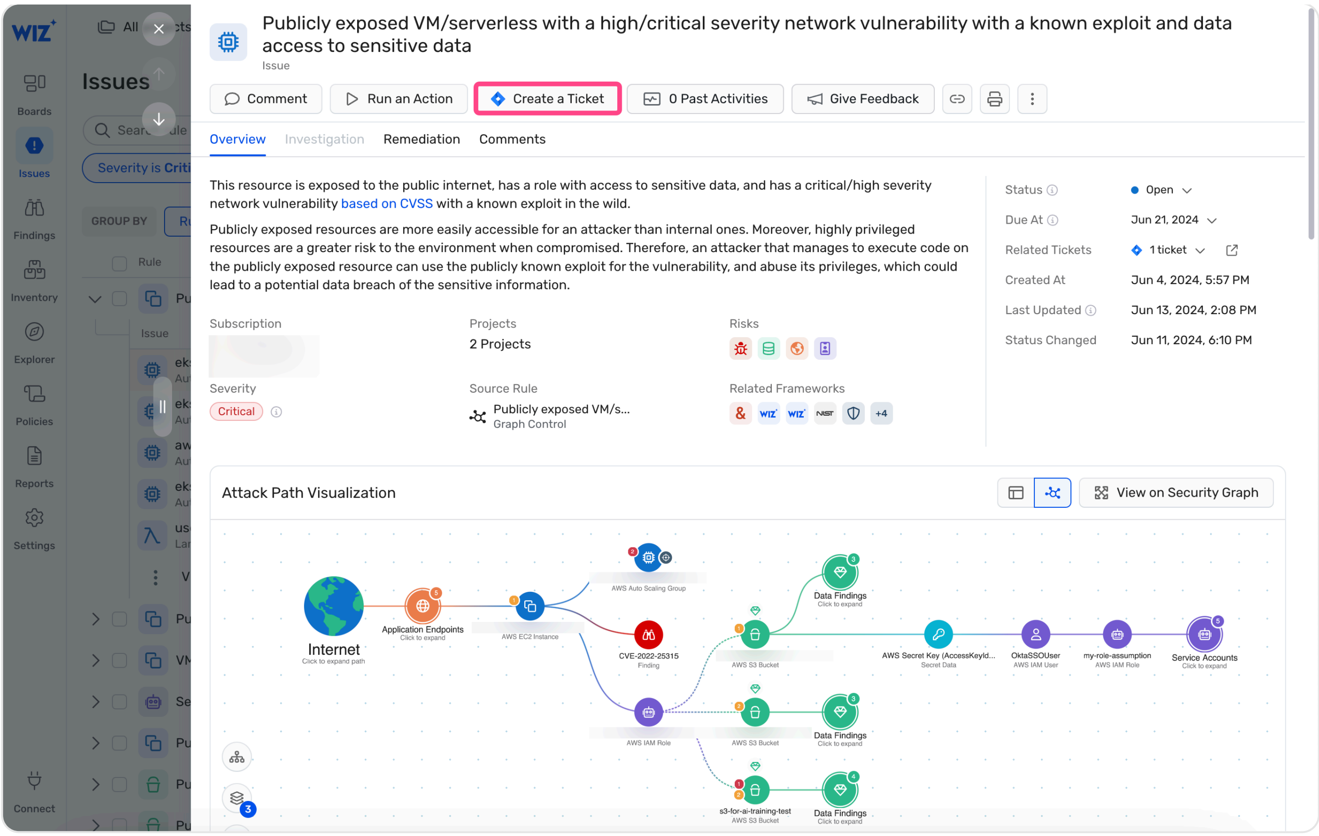
Name	Compliance Posture	Passed Checks
Data Risk Assessment	95 %	0 of 10
Data Access Governance	98 %	1 of 5
Key & Secret Management	92 %	0 of 10
Data Detection & Response	99 %	3 of 4
Data Incident Readiness	31 %	0 of 3
Data Assets Cost Optimization	-	0 of 0

Data Resources Inventory
26 technologies

Technology	R...
AWS DynamoDB Table Database Servers	11
AWS EC2 Instance Virtual Machines	226
AWS Lambda Function... Serverless	1
AWS Lambda Function Serverless	36
AWS Lightsail Instance Virtual Machines	1

2. For example, explore your critical Issues directly from the Data Security Issues by Severity widget.
3. By default, the Issues are grouped by the Data Classification Rule that generated them. You can change the grouping and add more filters to focus on specific Issues. If you've identified an Issue that needs to be reviewed by a colleague, you can open its details drawer and Create a ticket directly from the Wiz portal.

English ▲



Publicly exposed VM/serverless with a high/critical severity network vulnerability with a known exploit and data access to sensitive data

Issue

This resource is exposed to the public internet, has a role with access to sensitive data, and has a critical/high severity network vulnerability based on CVSS with a known exploit in the wild.

Publicly exposed resources are more easily accessible for an attacker than internal ones. Moreover, highly privileged resources are a greater risk to the environment when compromised. Therefore, an attacker that manages to execute code on the publicly exposed resource can use the publicly known exploit for the vulnerability, and abuse its privileges, which could lead to a potential data breach of the sensitive information.

Subscription

Projects: 2 Projects

Risks

Severity: Critical

Source Rule: Publicly exposed VM/s... Graph Control

Related Frameworks: +4

Status: Open

Due At: Jun 21, 2024

Related Tickets: 1 ticket

Created At: Jun 4, 2024, 5:57 PM

Last Updated: Jun 13, 2024, 2:08 PM

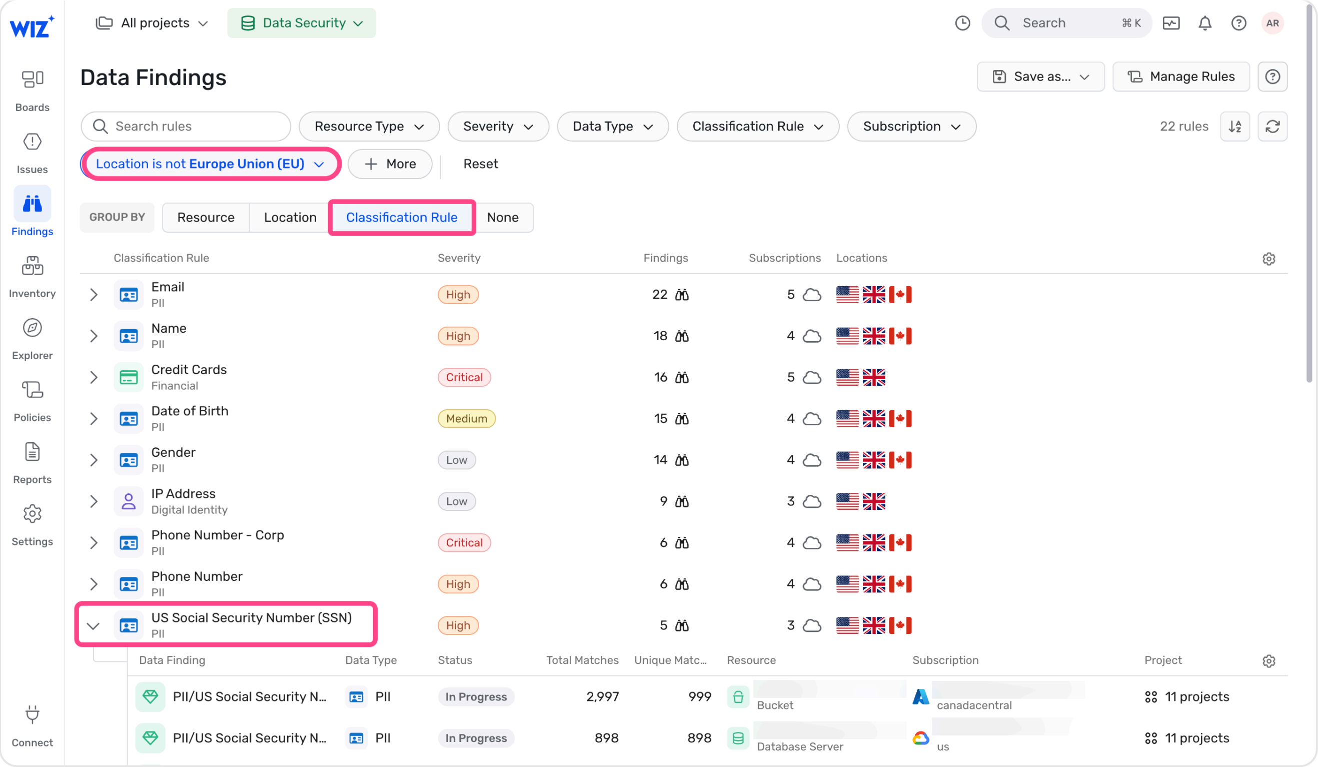
Status Changed: Jun 11, 2024, 6:10 PM

Review and investigate Data Findings

Wiz helps you explore high-level questions like "Where do I have PII outside Europe?" and then drill down by data type, severity, and more.

1. Go to the Findings > Data Findings page.
2. Review all the Data Findings detected in your environment, grouped by the resource they were detected on by default.
3. Use the various filters and grouping options to explore. For example, to locate your PII outside of Europe:
    i. Change to Group By Location.
    ii. Add a Location is not EU filter.
4. Review what type of data is located where. You can also group by Classification Rule and easily identify the type of data that resides outside of Europe. For example, having your organization's US Social Security Numbers (SSN) outside of Europe could be something you'd want to address right away.

English ▲



All projects · Data Security

Search ⌘K

Data Findings

Save as… · Manage Rules

Search rules · Resource Type · Severity · Data Type · Classification Rule · Subscription · 22 rules

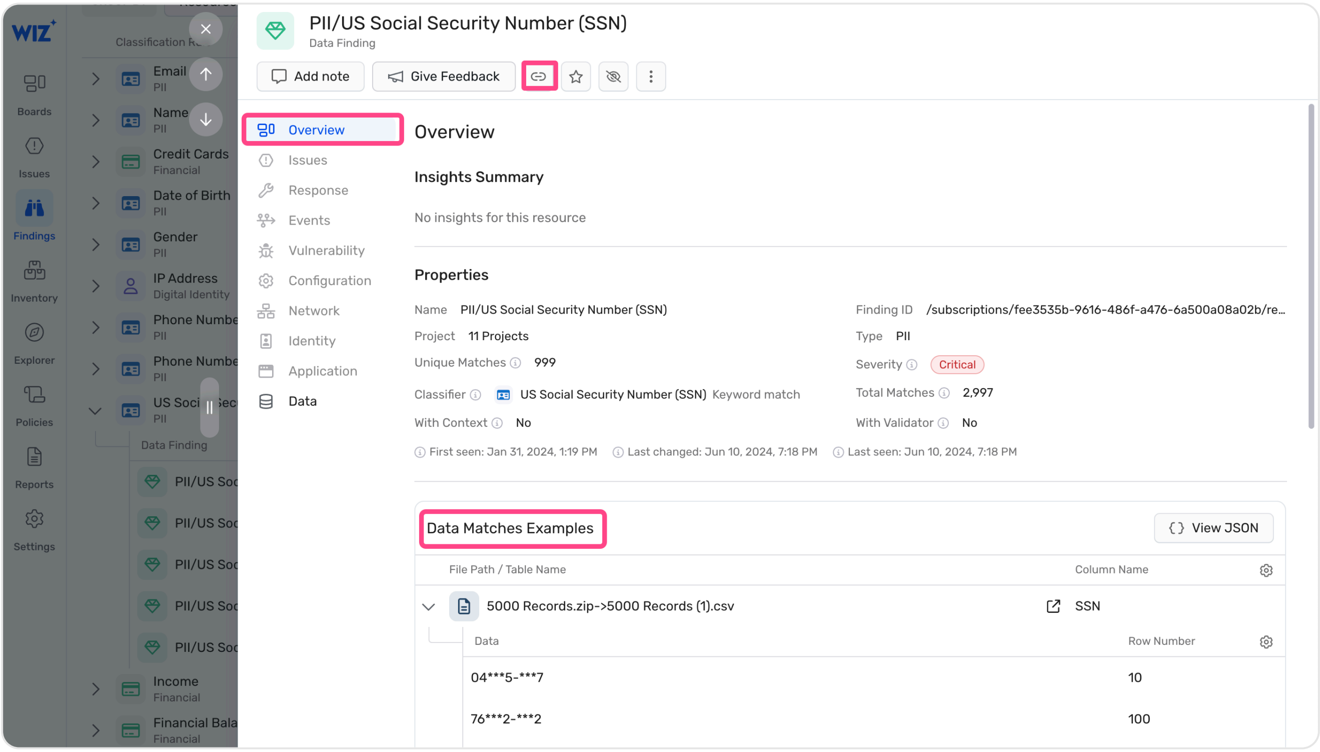
Location is not Europe Union (EU) · + More · Reset

GROUP BY: Resource · Location · Classification Rule · None

Classification Rule	Severity	Findings	Subscriptions	Locations
Email PII	High	22	5	🇺🇸 🇬🇧 🇨🇦
Name PII	High	18	4	🇺🇸 🇬🇧 🇨🇦
Credit Cards Financial	Critical	16	5	🇺🇸 🇬🇧
Date of Birth PII	Medium	15	4	🇺🇸 🇬🇧 🇨🇦
Gender PII	Low	14	4	🇺🇸 🇬🇧 🇨🇦
IP Address Digital Identity	Low	9	3	🇺🇸 🇬🇧
Phone Number - Corp PII	Critical	6	4	🇺🇸 🇬🇧 🇨🇦
Phone Number PII	High	6	4	🇺🇸 🇬🇧 🇨🇦
US Social Security Number (SSN) PII	High	5	3	🇺🇸 🇬🇧 🇨🇦

Data Finding	Data Type	Status	Total Matches	Unique Matc...	Resource	Subscription	Project
PII/US Social Security N...	PII	In Progress	2,997	999	[redacted] Bucket	[redacted] canadacentral	11 projects
PII/US Social Security N...	PII	In Progress	898	898	[redacted] Database Server	[redacted] us	11 projects

5. Verify the identified data. Click a Data Finding to open its details drawer. You can see a redacted example of the sensitive data that was detected, the resource it was detected on, the subscription it is associated with, and more.



PII/US Social Security Number (SSN)
Data Finding

Add note · Give Feedback

Overview

Insights Summary

No insights for this resource

Properties

Name PII/US Social Security Number (SSN)

Finding ID /subscriptions/fee3535b-9616-486f-a476-6a500a08a02b/re...

Project 11 Projects

Type PII

Unique Matches 999

Severity Critical

Classifier US Social Security Number (SSN) Keyword match

Total Matches 2,997

With Context No

With Validator No

First seen: Jan 31, 2024, 1:19 PM · Last changed: Jun 10, 2024, 7:18 PM · Last seen: Jun 10, 2024, 7:18 PM

Data Matches Examples · View JSON

File Path / Table Name	Column Name
5000 Records.zip->5000 Records (1).csv	SSN

Data	Row Number
04***5-***7	10
76***2-***2	100

6. You can share this information directly from the Wiz portal by copying the link address on the top bar. For example, send this to your organization's data protection officer.

Advanced Workflows

English ▲

Now that we've covered the basics, refer to our Data Security tutorials for more step-by-step walkthroughs.

Updated about 1 month ago

← Configure Data Security

Data Security Coverage →

Did this page help you? Yes No

English