Data Security Tutorials

The following scenarios provide step-by-step instructions to help you understand a few key ways we want you to use Wiz to detect and address your data discovery risks:

- See an example of a Data Finding in Wiz
- Identify sensitive data in a specific region
- Find all public buckets with sensitive Data Findings
- Identify public buckets with secrets susceptible to lateral movement
- Identify data lineage
- Assess your data security compliance posture
- Identify potentially sensitive data in VCS repositories

For a more abstract discussion of data identification and analysis, see the How Wiz Works page on Data Security.

See an example of a Data Finding in Wiz

The simplest way would be to set up a dry-run for sensitive data scanning on a public S3 bucket, as that does not require making any changes to your connector permissions or tenant setup:

1. Download a Parquet or CSV example file which contains fictive sensitive data.
2. Save it to a public S3 bucket included in your cloud scanning.
3. Wiz will scan your bucket during the next workload scan, which occurs daily.
4. Once the data is detected, use this query to see the Data Findings in Wiz.

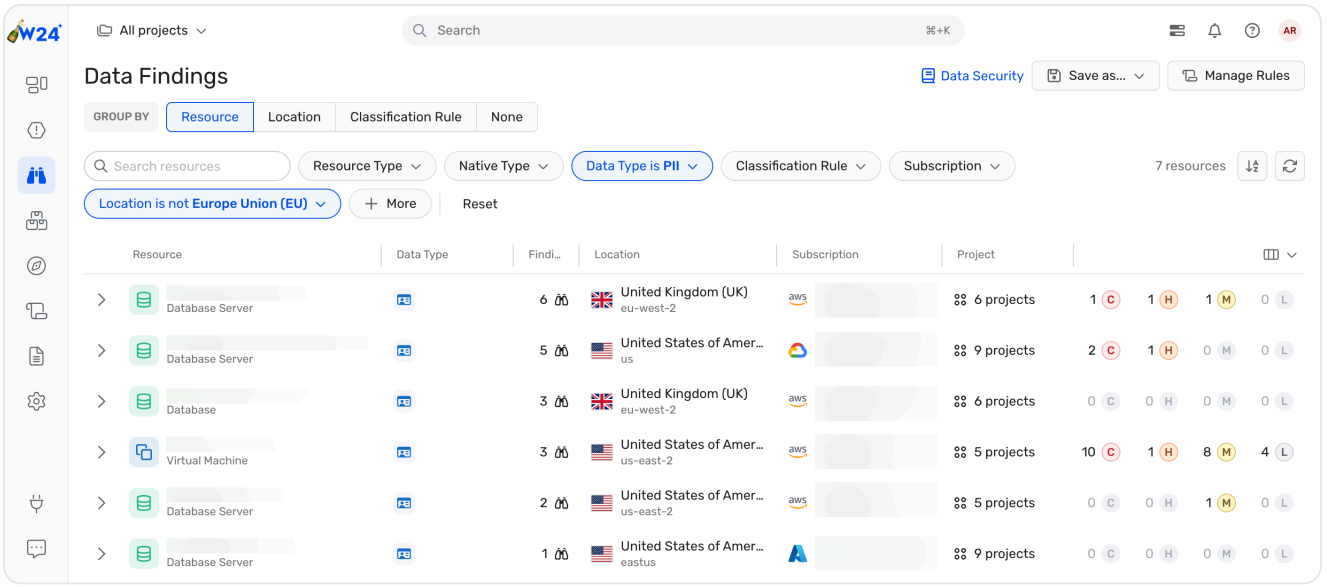
Identify sensitive data in a specific region

One of the GDPR requirements is to ensure all your data is located in a specific region. Using the Data Findings Explorer, you can view all the Data Findings Wiz detected in your environment and filter by region.

For example, view all your PII outside of Europe:

1. Go to the Findings > Data Findings page.
2. From the Data Type filter, select PII (direct link).

3. From the Location filter, change the condition to is not and select EU (direct link).
4. Review the list of all detected PII findings by resource. Click a resource to see what type of PII was detected, an example, and more.



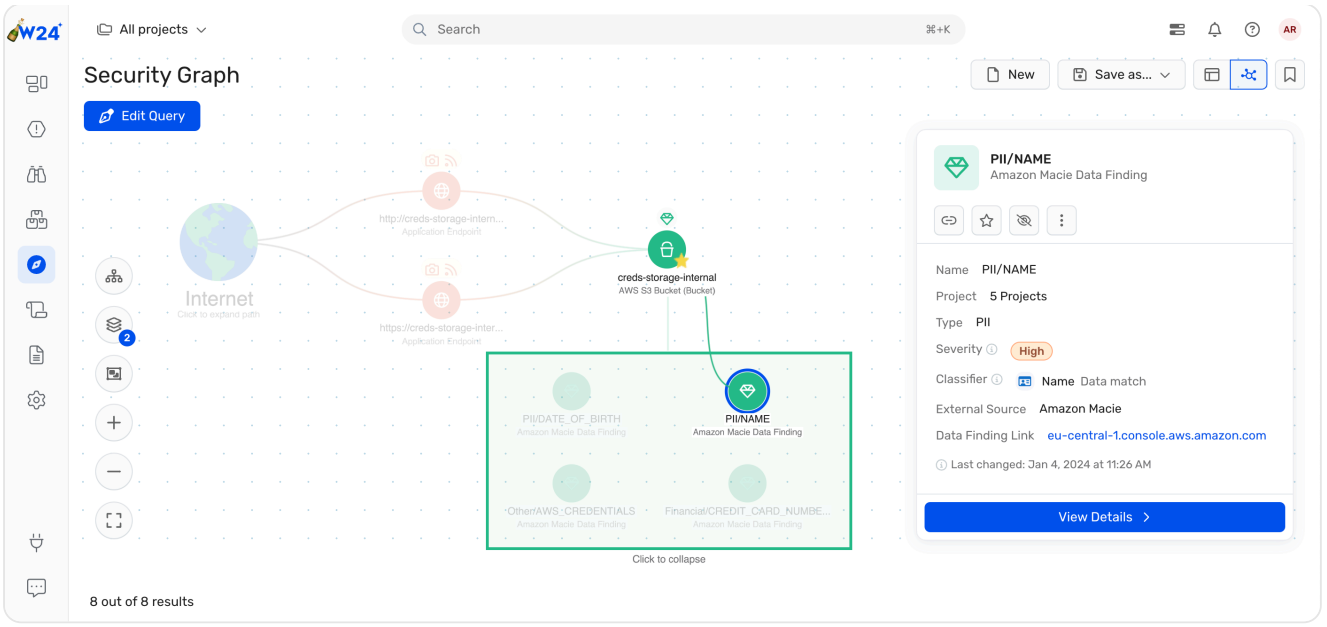
5. (Optional) After you've addressed all these findings, wait for the next Wiz workload scan to complete (up to 24 hours) and revist the Data Findings Explorer to ensure that no PII is hosted outside of Europe.

Find all public buckets with sensitive Data Findings

Wiz uses Data Classification Rules to identify sensitive data.

1. Use this query to identify externally exposed S3 buckets where Wiz has detected sensitive data.
2. Review the findings:

- Click a finding object on the graph to open the details drawer and review the finding category, rule ID, and more.



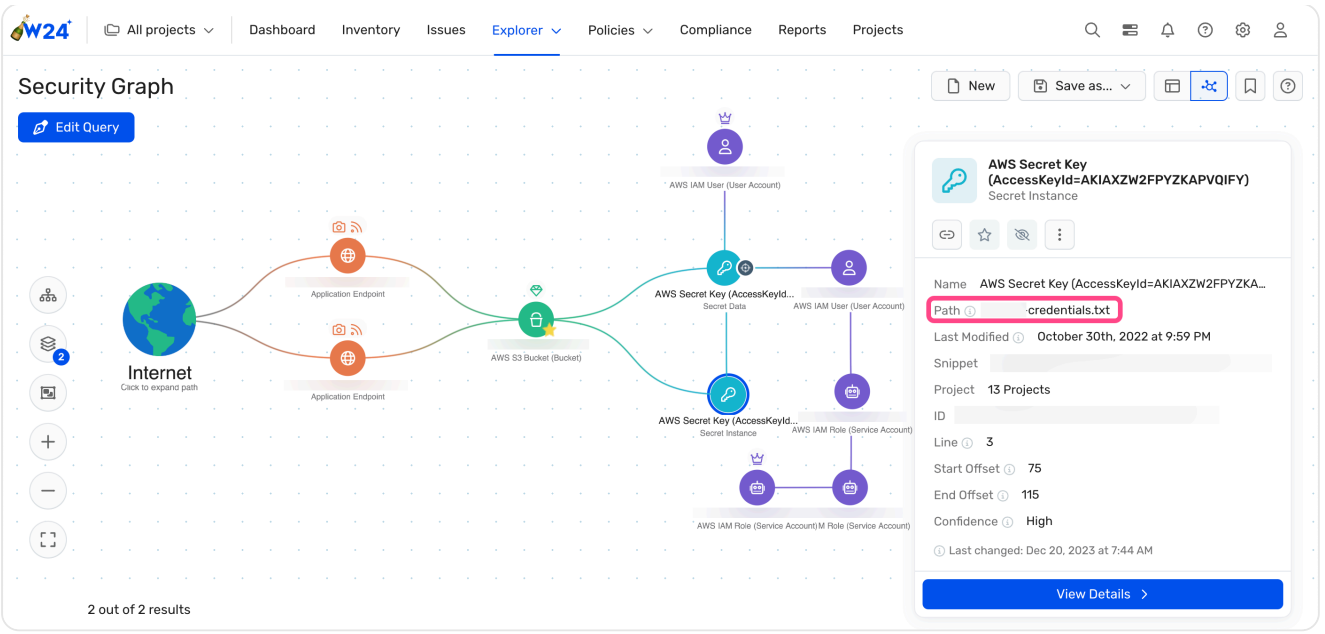
- Click View examples to see an example of the detected findings, such as redacted email addresses or credit card numbers, along with their location in the file.

> - Wiz stores and displays only metadata. The actual details are not stored in Wiz.
> - Wiz does not display examples for Data Findings ingested by a third party tool.

3. Narrow down your search query to focus only on a specific data category by clicking `+`. For example to locate only PII findings, select Category and search for "PII". Switch back to Table view and inspect the findings to decide which files or buckets need to be removed.

Identify public buckets with secrets susceptible to lateral movement

1. Use this query to identify externally exposed S3 buckets with secrets.
2. Add the Lateral Movement path to the graph (click Layers > Lateral Movement) to identify which exposed secrets could be potentially abused by a malicious actor to move around your environment.
3. Review the secret properties to gain a better understanding of the potential impact of the risk. You can also verify the presence of the secret in the bucket:

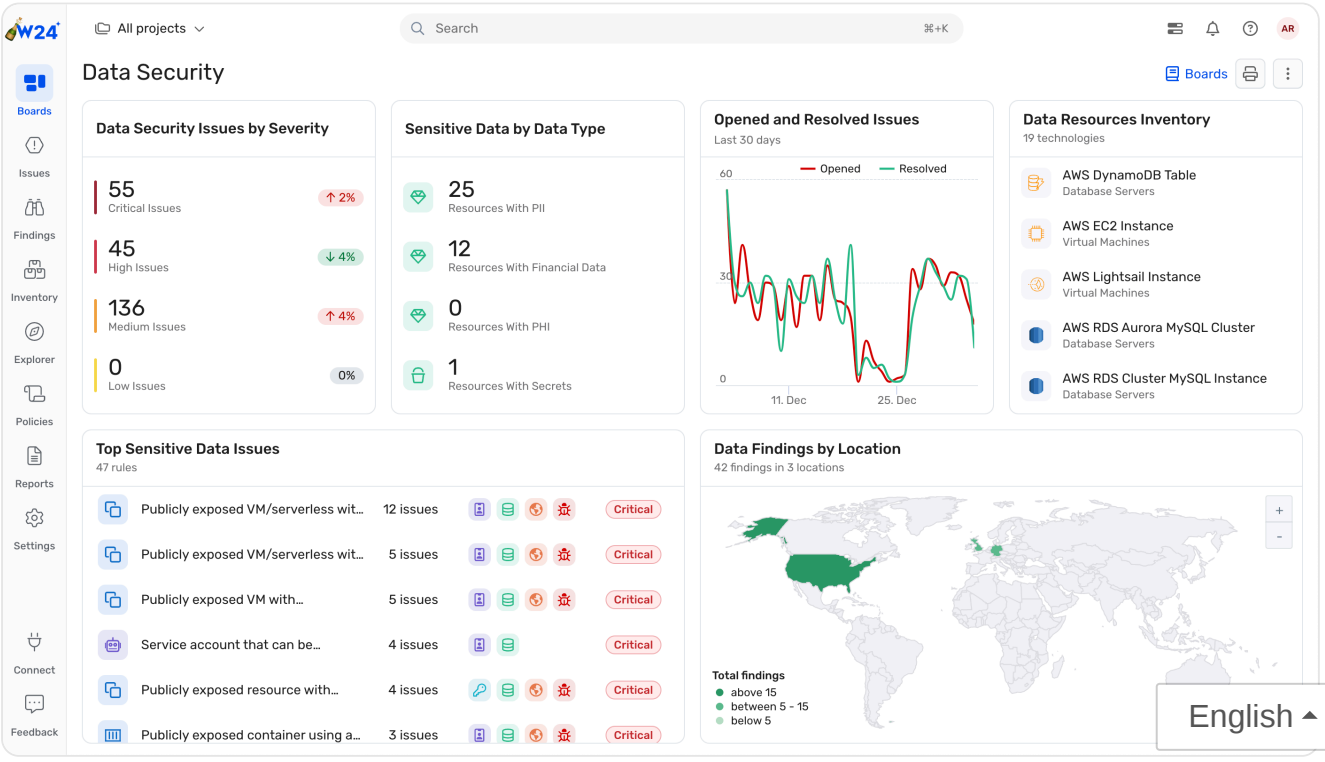


- Click the Secret Instance object to open the details drawer and locate the file path where the secret is located within the bucket (e.g. `credentials.txt`).
- Next, click the Application Endpoint object to open the details drawer, and click on the linkable Name to view the bucket data.
- Search for the file path within the bucket and remove the secret from the exposed bucket.

Identify data lineage

Data can be unintentionally copied between environments, regions, or clouds. To search for sensitive data across subscriptions for example,

1. Go to the Data Security board.



2. Scroll down to the Sensitive Data Across Subscriptions widget and click the widget name to view all detected resources (direct link).
3. Switch to Graph View and inspect the findings:

- Which subscriptions is the data associated with?
- Do you see a subscription which should not contain sensitive data?
- What is the shared schema and is it sensitive for your organization?

4. Fix the problem by removing the data from the resource(s) where it should not exist.

Assess your data security compliance posture

Wiz provides an out-of-the-box Data Security framework, covering areas such as Data Risk Assessment, Data Access Governance, Data Incident Readiness, and more. Wiz also supports other compliance frameworks related to sensitive data storage and management, such as PCI DSS, HIPAA, HITRUST CSF, NIST SP 800 53, NIST 800-171, ISO/IEC 27001, and SOC 2.

> Compliance frameworks can be enabled (or disabled) on the Reports > Compliance Frameworks page.

1. Go to the Data Security board.

2. Review the Data Security Framework widget, which displays Wiz's built-in framework. Click it to drill-down into the individual categories and Controls to identify and resolve the problems detected in your environment.
3. Scroll down to the DSOn Compliance Scores widget to review your posture based on external frameworks.
4. For example, the ISO/IEC 27001 requires that sensitive personal data (PII) will not be stored on resources that are exposed to the public internet. Select the ISO/IEC 27001 framework. (direct link).
5. Let's look for example at a Control that can help you identify data assets with sensitive personal data can be accessed by all (direct link).

6. Review the various Data Findings and remediate the issues in order to be compliant.

Identify potentially sensitive data in VCS repositories

> To block pull requests that contain sensitive data, enable event-triggered scanning for the version control Connector; follow the instructions of the first solution here. You can also apply custom CI/CD policies.

1. Go to the Findings > Version Control Scans page.
2. At the top, click Finding Type > Sensitive Data (direct link).

Updated about 1 month ago

← Data Security Coverage

How Data Classification Works →