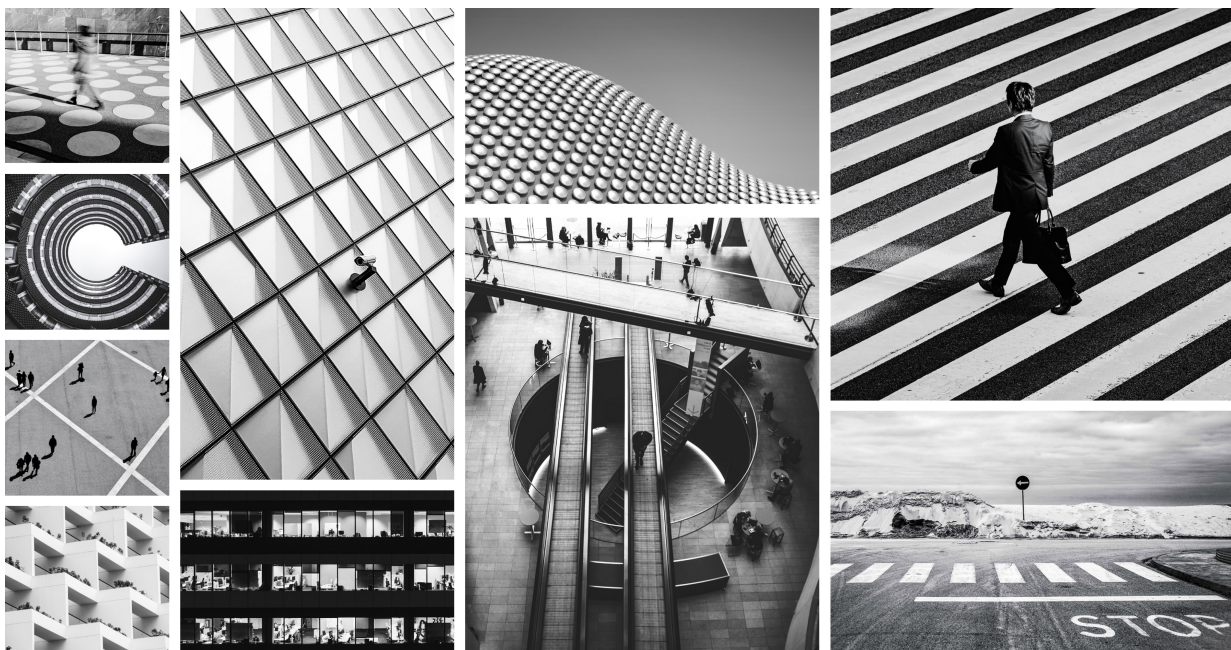




Using the Free Trial



Use this guide to learn about Illumio Insights and onboard your cloud using the free trial process.

Discover the world's first CDR built on an AI security graph

Identify risk, detect attacks, and contain threats in one click with AI cloud detection and response. Get AI-enriched observability at cloud scale — in minutes, not months.

[Explore Insights](#)

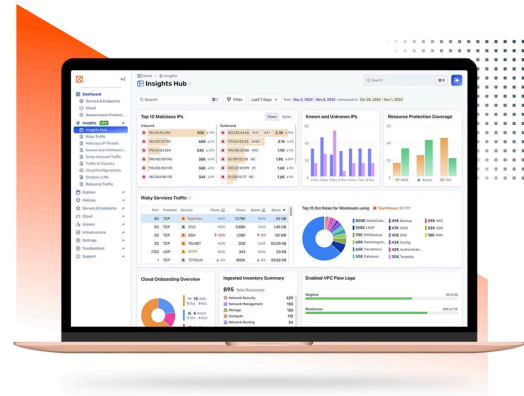


Table of Contents

Before You Begin	4
Checklist for Onboarding Illumio Insights	4
Onboarding Paths	5
Onboarding Path Using the Free Trial from illumio.com	5
Onboarding Path Using a Cloud Marketplace	5
Free Trial Onboarding Steps for Azure	6
Step 1. Start Free Trial	6
Step 2. Onboard Azure	7
Step 3. Explore Illumio Insights	9
Free Trial Onboarding Steps for AWS	9
Step 1. Start Free Trial	9
Step 2. Onboard AWS	9
Step 3. Explore Insights	11
Free Trial Onboarding Steps for GCP	11
Step 1. Start Free Trial	11
Step 2. Onboard GCP	12
Set up Flow Log Access	12
Step 3. Explore Illumio Insights	12
Explore Illumio Insights	13
The Insights Hub	13
Illumio Insights Overviews and Use Cases	13
Resource Traffic	13
Risky Traffic	14
Malicious IP Threats	15
Shadow LLMs	15
External Data Transfer	16
DORA Compliance	16
Country Insights	17
Insights Use Cases	18

Before You Begin

Review this checklist before you begin your onboarding journey.

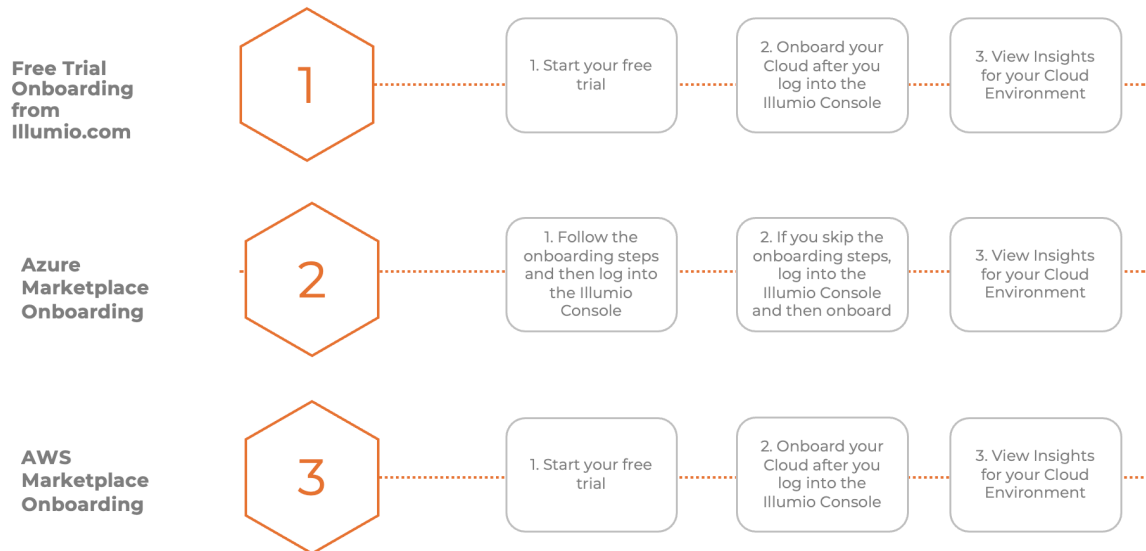
Checklist for Onboarding Illumio Insights

- ☐ Confirm that you have reviewed the permissions set for AWS. See [AWS Permissions](#).
- ☐ Confirm that you have reviewed the permissions set for Azure. See [Azure Permissions](#).
- ☐ Confirm that you have reviewed the permissions set for GCP. See [GCP Permissions](#).

Onboarding Paths

Select the onboarding path based on your cloud environment.

Onboarding Path Using the Free Trial from illumio.com



- See [Free Trial Onboarding Steps for AWS \[9\]](#) from illumio.com
- See [Free Trial Onboarding Steps for Azure \[6\]](#) from illumio.com
- See [Free Trial Onboarding Steps for GCP \[11\]](#) from illumio.com



NOTE

This Getting Started Guide covers the onboarding instructions for the Free Trial only.

Onboarding Path Using a Cloud Marketplace

If you are onboarding using the Azure or AWS Marketplace, see the onboarding instructions in the Marketplace onboarding guides for your clouds.

- See onboarding using Azure Marketplace.
- See onboarding using AWS Marketplace.

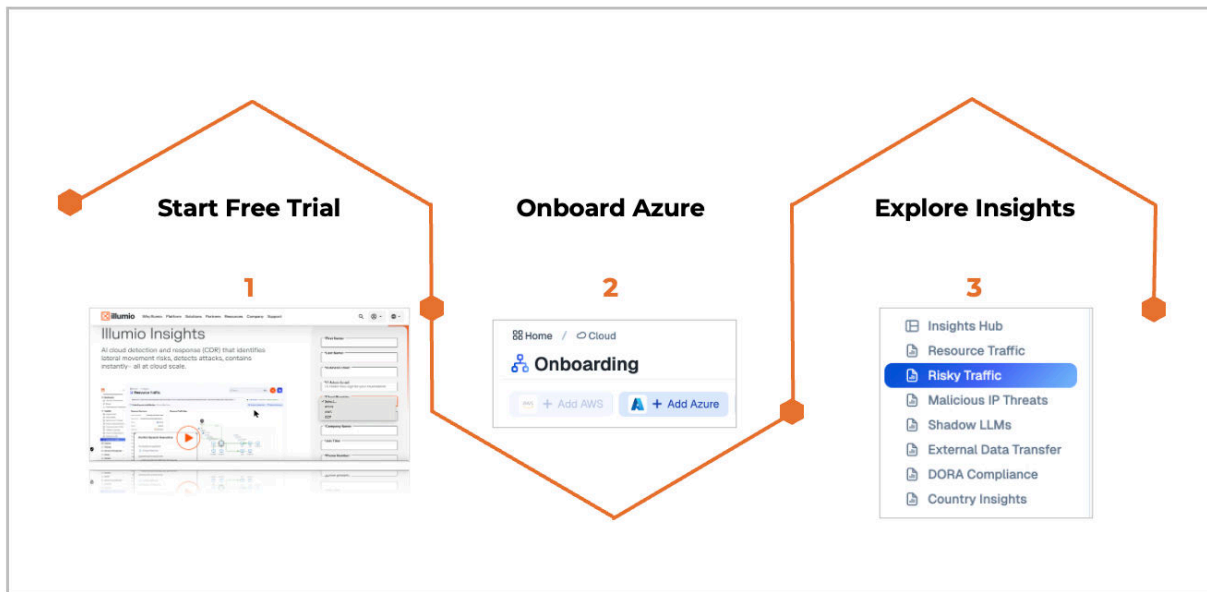


NOTE

Go to docs.illumio.com/s to download and view the Marketplace onboarding instructions for Azure and AWS.

Free Trial Onboarding Steps for Azure

Follow this onboarding path for Azure.




Step 1. Start Free Trial

If you haven't already started your free trial, go to the [Free Trial Insights](#) page first.

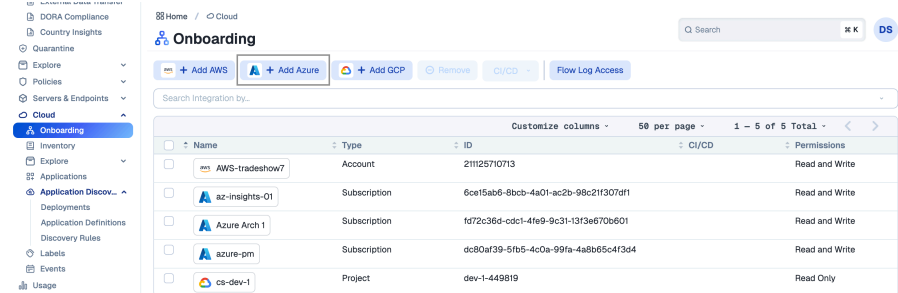
Step 2. Onboard Azure

Onboard Azure



Follow these steps

1. Log into the Illumio Console.
2. Go to **Cloud > Onboarding**.
3. Click **Add > Azure**.



Name	Type	ID	CI/CD	Permissions
AWS-tradeshaw7	Account	21125710713		Read and Write
az-insights-01	Subscription	6ce15ab6-8bcb-4a01-ac2b-98c21f307df1		Read and Write
Azure Arch 1	Subscription	fd72c36d-cdc1-4fe9-9c31-13f3e670b601		Read and Write
azure-pm	Subscription	dc80af39-5fb5-4c0a-99fa-4a8b65c4f3d4		Read and Write
cs-dev-1	Project	dev-1-449819		Read Only

4. Choose Easy onboarding and click Continue.
5. Click Login with Azure to connect your Azure cloud resources. See the detailed sub steps listed next.
6. Setup flow log access for your users.

Login with Azure and Review Permissions

1. Sign into your Azure account with your Azure credentials.
2. On the **Permissions Requested** pane, check **Consent on behalf of your organization** and click **Accept**. This allows the Illumio application's Service Principal to gain **just-in-time access privileges** as the user who is logging in.

API Name	Claim Value	Permission
Azure Resource Manager	user_impersonation	Access Azure Resource Manager as organization users
Microsoft Graph	offline_access	Maintain access to data you have given Illumio access to
Microsoft Graph	openid	Sign users in
Microsoft Graph	profile	View a user's basic profile
Microsoft Graph	User.Read	Sign in and read a user profile

3. In the **Finish Your Azure integration** pane, under **Integration Scope**, select a tenant or subscription to onboard. You can select multiple subscriptions from the **Subscriptions** drop-down list.
4. **Enable VNET Flow Logs.**
5. **Select Read or Write permissions.**
6. **(Optional):** Configure tags and centralize flow storage. Click **View More Settings (Optional)** in the **Enable VNET Flow Logs** pane. **Add Tags**
7. Configure tags for new flow logs and storage accounts. Adding tags helps you meet compliance requirements and enhances search for new resources. To add a tag, click **+ Add Tag**, enter values in the **Tag Key** and **Tag Value** fields and click **Apply Changes**. You can create multiple tags for resources.
See [Use tags to organize your Azure resources and management hierarchy](#).
8. **Centralize Flow Logs .**

9. To centralize flow logs, click the **Centralize Flow Logs** tab, select the subscription where you want to centralize your flow logs, and click **Apply Changes**.

10 Click **Confirm and Continue**.

Permission Type	Permission Name	Notes
Read	Reader-role (Azure-owned role)	This role gives Illumio Cloud permission to read data or resources from your subscription or tenant. This role allows the viewing of all resources but it does not allow modification.
Write	Illumio Network Security Administration (Illumio-created custom role) Illumio Firewall Administrator (Illumio-created custom role)	Allows Illumio to manage Network Security Groups and Azure Firewalls in your Azure environment.
Flow	Storage blob data reader	Allows Illumio to read the contents of storage accounts in your Azure environment.

Set up Flow Log Access for Azure



NOTE

Skip this procedure if you have already performed steps 4 through 9 in the section titled Log in with Azure and Review Permissions previously.

Set up flow log access

Follow these steps



1. In the Illumio Console, go to Onboarding and then click Flow Log Access.
2. Select Azure to grant access to and select Grant Access.
3. Select your service account, provide the service account token, and click Done.



NOTE

If the VPC/NSG flow logs from one account are configured to be stored in S3/storage accounts in another account, then the destination account should be onboarded into Illumio. If the account that owns the S3 bucket is not onboarded, Illumio will not be able to fetch the flow logs of that S3 bucket.

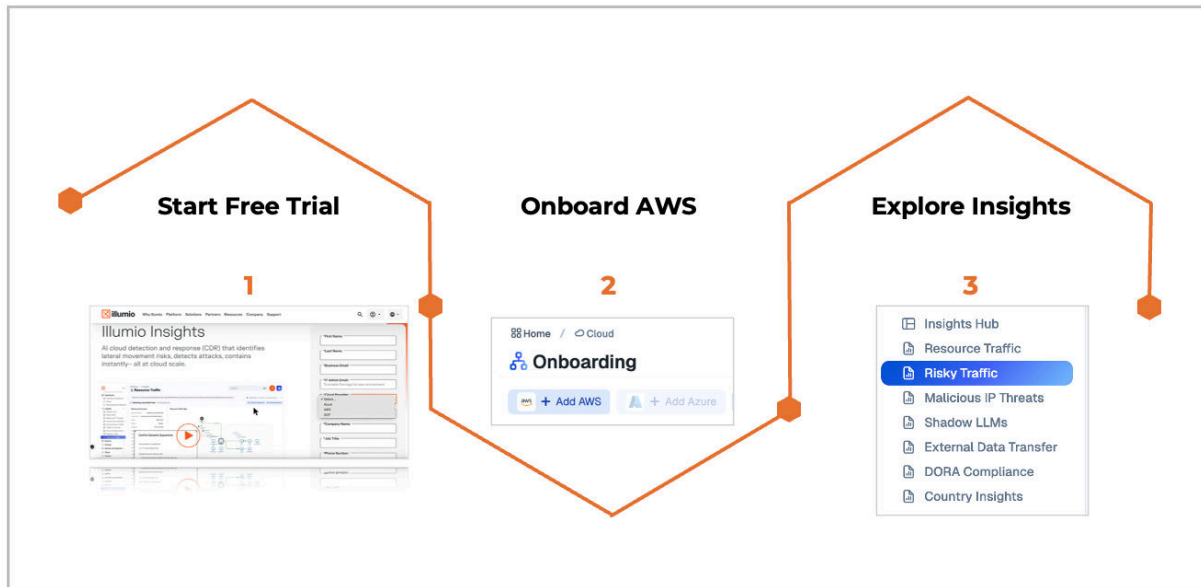
For detailed instructions for setting up your flow logs, see this [topic](#).

Step 3. Explore Illumio Insights

View Illumio Insights in the Console. See [Explore Illumio Insights \[13\]](#).

Free Trial Onboarding Steps for AWS

Follow these free trial onboarding steps for AWS.



Step 1. Start Free Trial

If you haven't already started your free trial, go to the [Free Trial Insights](#) page first.

Step 2. Onboard AWS




NOTE

Easy onboarding is not available for AWS at this time.

Onboard AWS

Follow these steps

1. Log into the Illumio Console.
2. Go to Cloud > Onboarding.
3. Click Add > AWS, fill in the required fields, and click Next.



The screenshot shows the 'Onboard AWS' interface. A red box highlights the 'Add AWS' button in the 'Onboarding' section. The interface includes a progress bar with three steps: 'Connect to AWS', 'Set up Access', and 'Confirm and Save'. The 'Connect to AWS' step is currently active.

Add AWS Cloud Organization

Progress bar: Connect to AWS (active), Set up Access, Confirm and Save

☒ **Organization** RECOMMENDED
Secure an AWS Organization including all its member accounts

☐ **Account**
Secure a specific AWS account

Name
AWS

Root Account ID
543219999999

READ WRITE ACCESS
☒ Yes Illumio has Read and Write access to ensure compliance [Download Permissions](#)

[Cancel](#) [Next >](#)

4. Set up a service account and click Next.

Add AWS Cloud Organization

Progress bar: Connect to AWS (completed), Set up Access (active), Confirm and Save

Service Account
Service Account: TPM-Orion-Tenant

Illumio Cloud Tenant ID
39e868b6-fdfe-4118-b664-a7d4b04728e8

Download Cloud Formation Stack
[Download](#)

[Cancel](#) [< Back](#) [Next >](#)

5. Click Save and Confirm. See [Onboarding AWS Cloud](#) for detailed instructions.

Set up Flow Log Access

Set up flow log access

Follow these steps



1. After you have added your AWS account, go to Onboarding and then click Flow Log Access.
2. Select AWS to grant access to and select Grant Access.
3. Select your service account, provide the service account token, and click Done.



NOTE

In AWS, Illumio supports reading flow logs that are stored in S3 buckets only. Currently, other storage destinations are not supported.

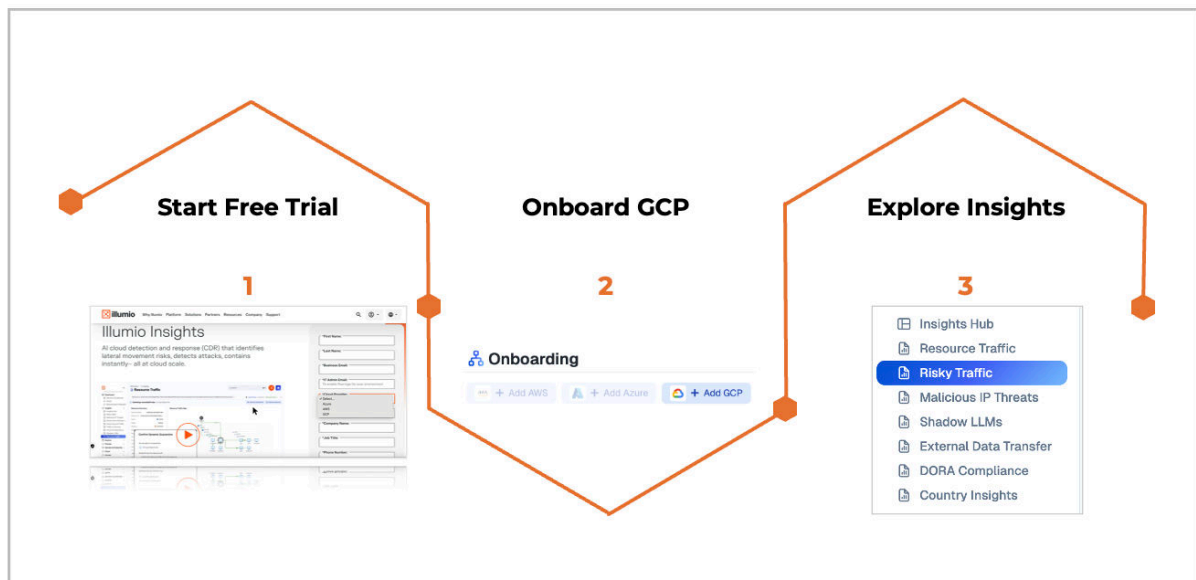
Go here for detailed instructions about [setting up your flow logs](#).

Step 3. Explore Insights

View Illumio Insights in the Console. See [Explore Illumio Insights \[13\]](#).

Free Trial Onboarding Steps for GCP


Follow these free trial onboarding steps for GCP.




Step 1. Start Free Trial


If you haven't already started your free trial, go to the [Free Trial Insights](#) page first.

Step 2. Onboard GCP

Onboard Azure	Follow these steps
	<ol style="list-style-type: none"> 1. Log into the Illumio Console. 2. Go to Cloud > Onboarding. 3. Click Add > GCP. 4. Select Organization, Folder, or Project and enter the required fields based on your selection. 5. Select the Service account, enter the service account token information, and the project ID. 6. Check Cloud Shell Deployment Completed and click Next. 7. Click Save and Confirm. For detailed instructions, see Onboarding GCP. 8. Set up flow log access for your users.

Set up Flow Log Access

Set up flow log access	Follow these steps
	<ol style="list-style-type: none"> 1. In the Illumio Console, go to Onboarding and then click Flow Log Access. 2. Select the GCP account to grant access to and select Grant Access. Grant access by first selecting individual or grouped accounts. 3. Select your service account, provide the service account token, and click Done.



NOTE

To grant access to flow logs stored in a different account than the one you onboarded, you must also onboard the account containing those flow logs.

For detailed instructions about setting up flow logs, see this [topic](#).

Step 3. Explore Illumio Insights

View Illumio Insights in the Console. See [Explore Illumio Insights \[13\]](#).

Explore Illumio Insights

Here's a quick overview of everything you'll find in Illumio Insights.

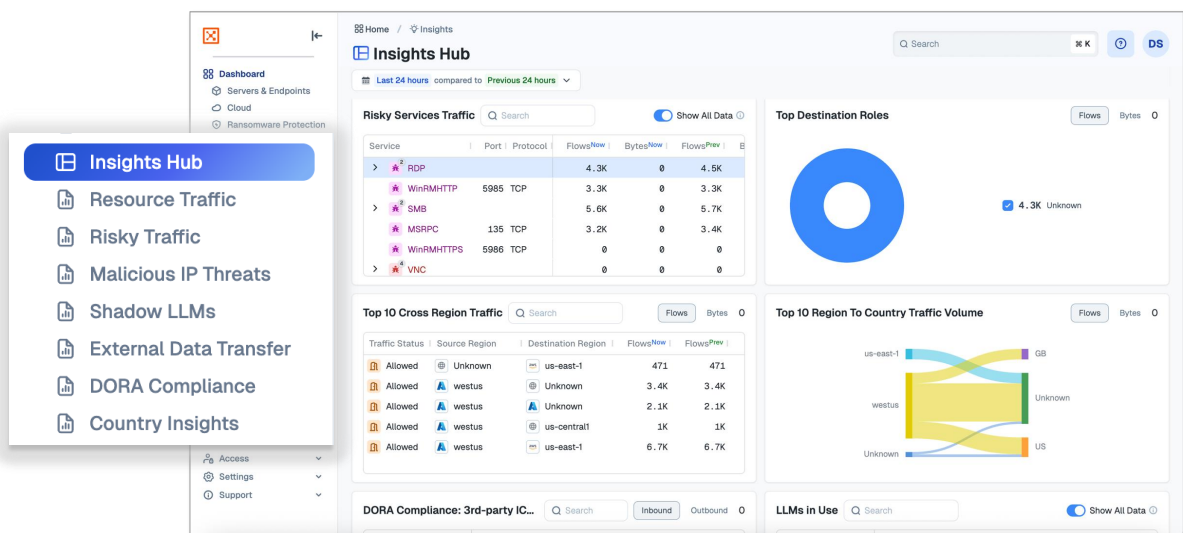
The Insights Hub

The Insights Hub offers a comprehensive overview of lateral movement risk throughout your environment. Use the Insights Hub to pinpoint significant areas of concern quickly and then navigate to the appropriate section for further investigation.

- Overview: [Watch the Insights Hub overview video.](#)
- Use Case: [Watch the Insights Hub use case video.](#)



The Insights Hub: An Overview Demo

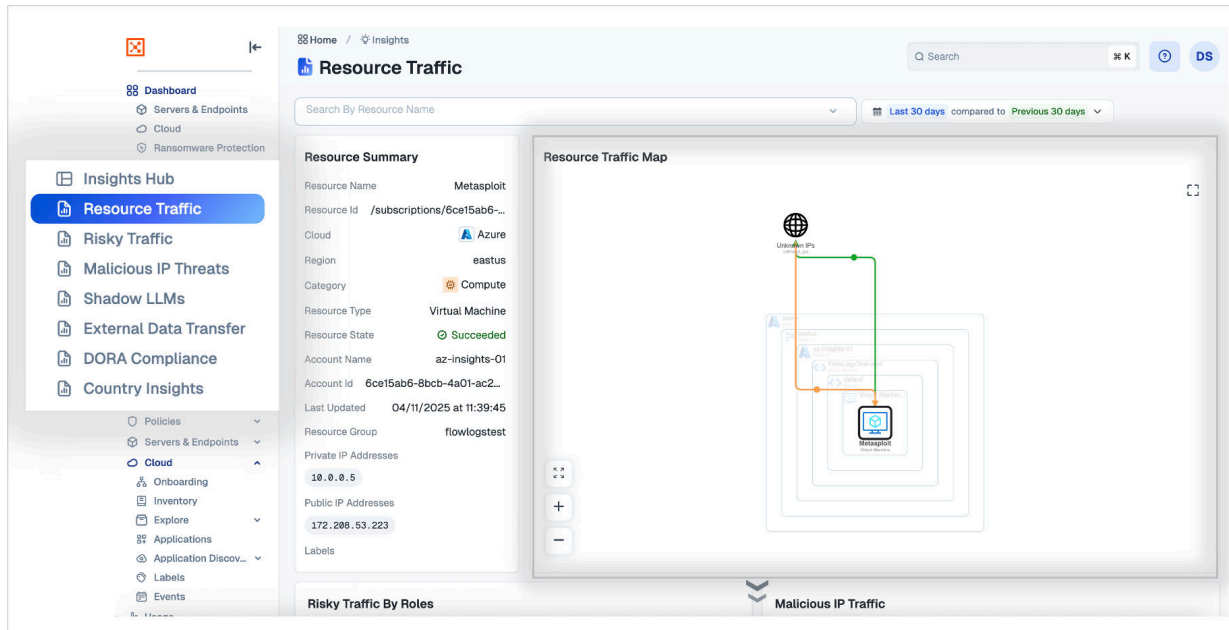


Illumio Insights Overviews and Use Cases

Resource Traffic

The Resource Traffic dashboard allows you to examine a single resource in detail. You can access all related metadata, resources connected to it, and see in real time what it's directly interacting with—visualized through the Resource Traffic Map. Other widgets on this page help you identify if it has been engaging with malicious IPs, attempting external data transfers, or using potentially risky protocols.

[Watch the overview video.](#)

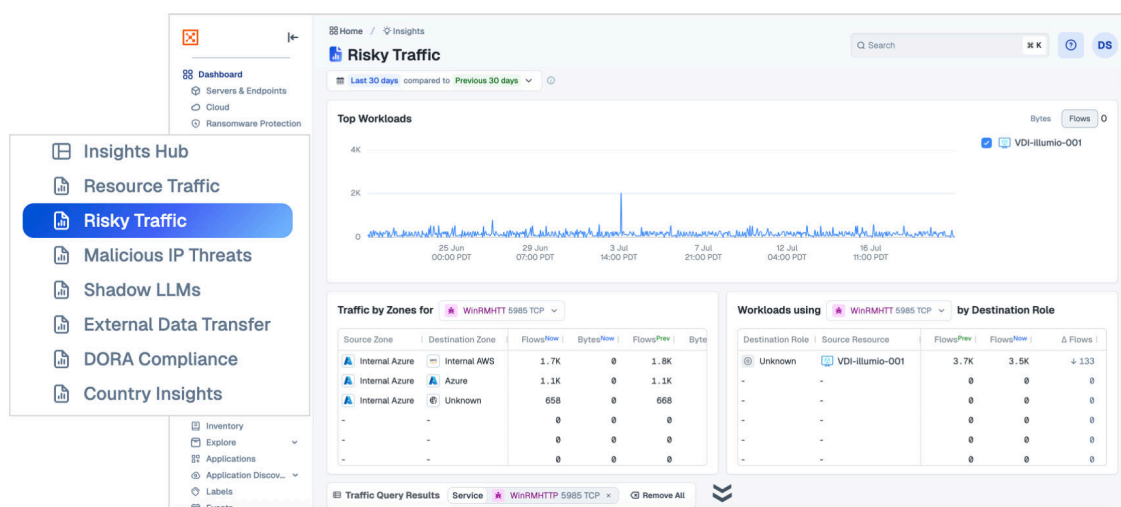


Risky Traffic

The Risky Traffic dashboard focuses investigation on the use of potentially dangerous ports and protocols in your environment—these are services that attackers are known to exploit for lateral movement.

When you select any protocol from the “Risky Services Traffic” widget, it updates all other widgets on the page to show data related to that protocol. From there, you can review specific types of workloads that participated in this traffic, review activity patterns, see zone and account traversal, and more.

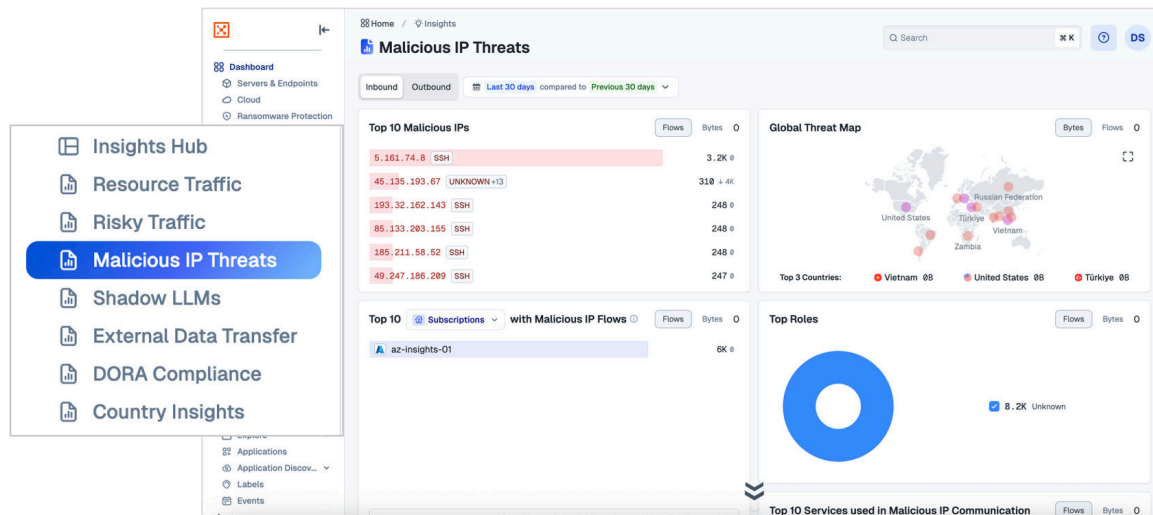
[Watch the overview video.](#)



Malicious IP Threats

The Malicious IP Threats dashboard shows activity between known malicious IPs and your environment. It displays the top talkers, the locations of these malicious IPs worldwide, as well as specific accounts, workloads, and protocols that are being targeted.

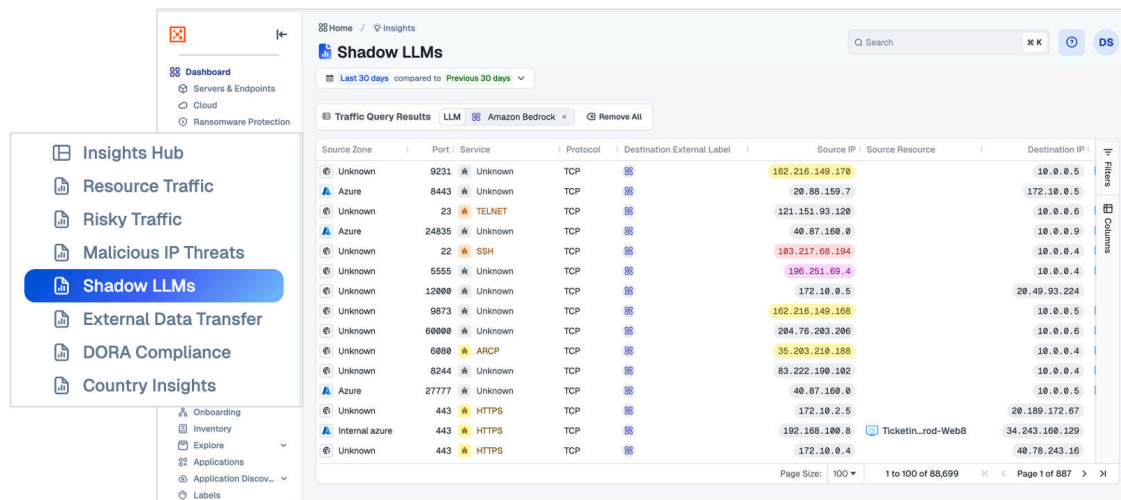
[Watch the overview video.](#)



Shadow LLMs

Use the Shadow LLMs dashboard to see which publicly accessible LLM services your resources are accessing and exchanging data with. You can view the specific LLMs being used, the accounts associated with this activity, and the resources involved in the access.

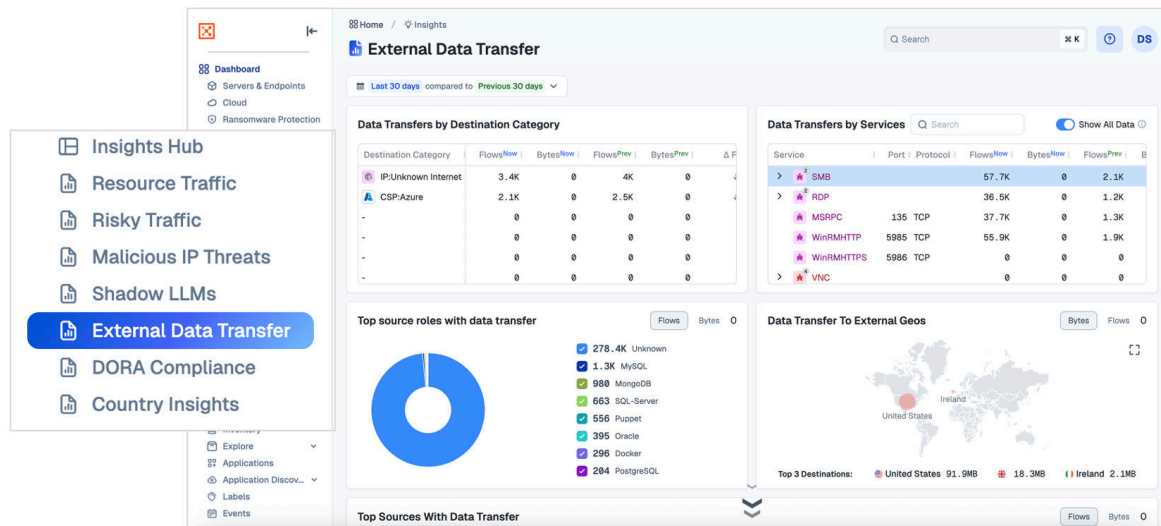
[Watch the overview video.](#)



External Data Transfer

The External Data Transfer dashboard highlights data leaving your environment for destinations on the internet. You can see where your data is being sent, which protocols are used for the transfer, and details about specific workloads and workload types involved.

[Watch the overview video.](#)

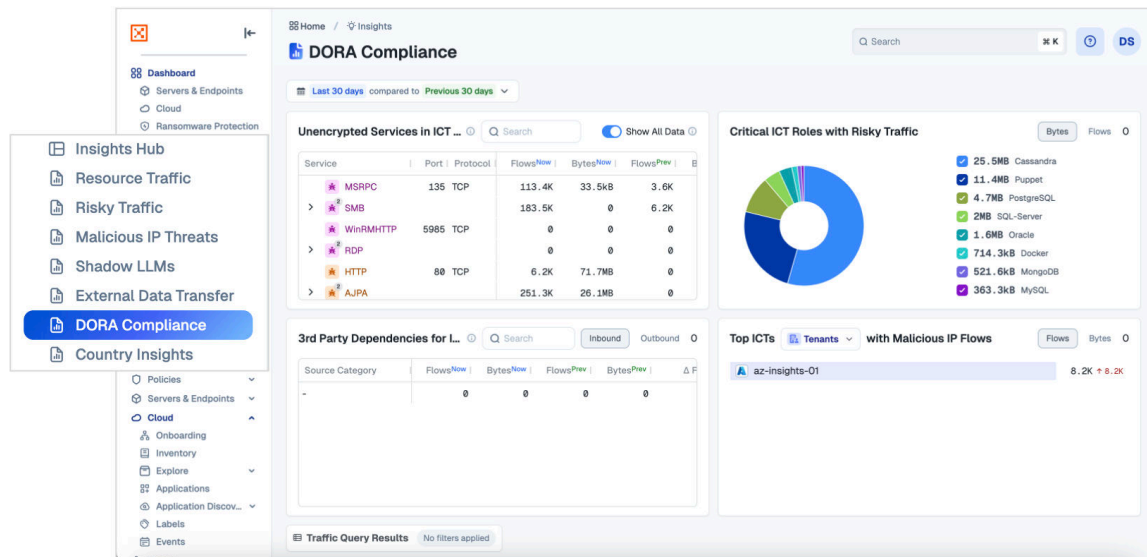


DORA Compliance

One of the main requirements of the EU's Digital Operational Resilience Act (DORA) is monitoring risks related to franchise-critical Information and Communication Technology (ICT)

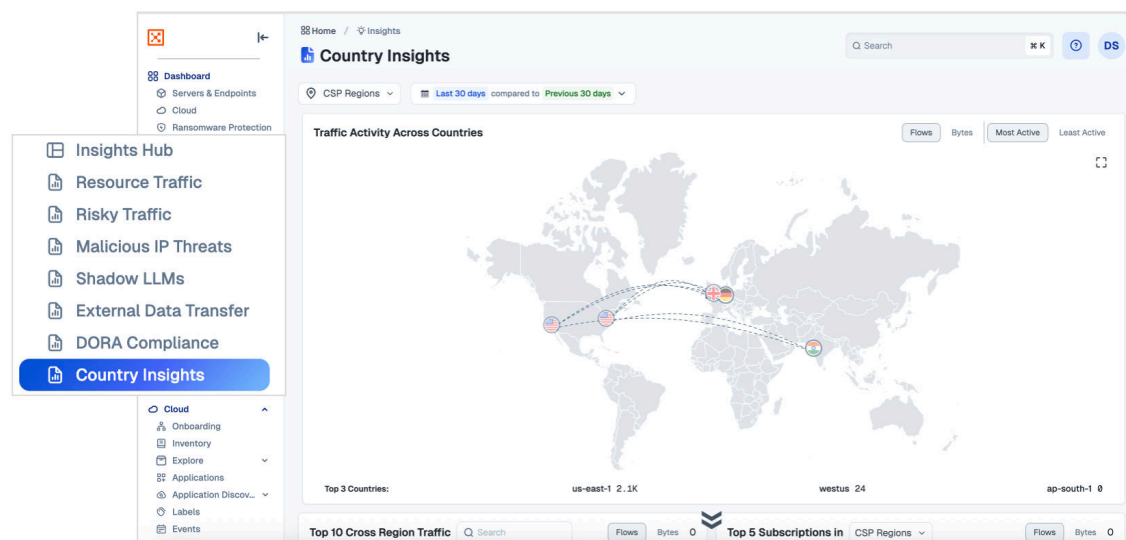
systems. The DORA Compliance dashboard combines important widgets from other Insights dashboards into a single view to assist with monitoring, detection, response, and reporting needs of DORA.

[Watch the overview video.](#)



Country Insights

Use Country Insights to monitor global traffic and spot suspicious patterns in unexpected regions. Filter traffic by Cloud Service Provider (CSP) regions—such as Northern Europe AWS data centers—to analyze traffic origins and detect risky connections.



Insights Use Cases

Now that you're familiar with what's available in Insights, here are some common use cases to help you explore further.

- Investigate the use of unauthorized ports and protocols.
[Watch the Resource Traffic use case video.](#)
- Explore possible lateral movement by a threat actor.
[Watch the Risky Traffic use case video.](#)
- Inspect activity related to known malicious IPs.
[Watch the Malicious IP Threats use case video.](#)
- Identify use of public LLMs.
[Watch the Shadow LLMs use case video.](#)
- Check for possible data exfiltration.
[Watch the External Data Transfer use case video.](#)