

The Illumio Virtual Advisor AI chatbot helps you understand your risk exposure by using natural language questions to generate quick answers and actions to reduce your risk.

Table of Contents

About the Illumio Virtual Advisor	4
Use IVA	4
Best Practices	5


About the Illumio Virtual Advisor

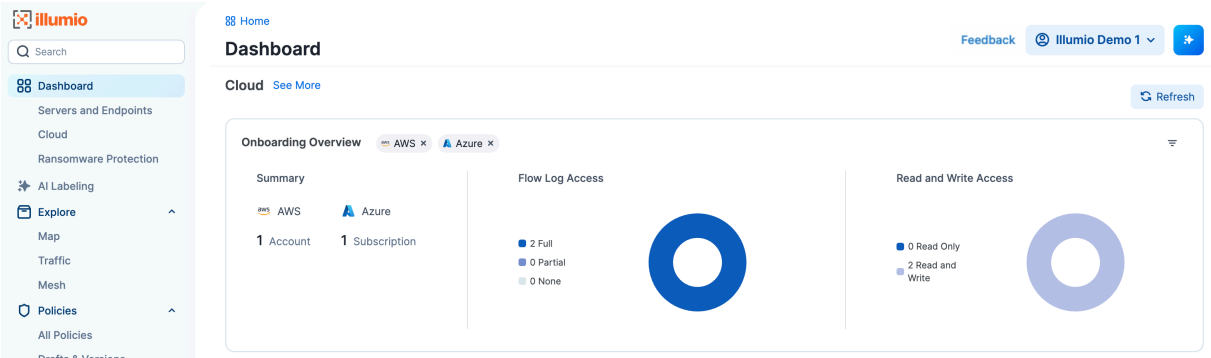
Illumio Virtual Advisor (IVA) helps you understand your risk exposure by using natural language questions to generate quick answers and actions to reduce your risk.

- Use IVA to visualize all traffic from a compromised server so you can take quick action to stop the risk. You can also use IVA to see all traffic from risky ports so you can preempt and prevent breaches.
- Illumio's AI-powered zero trust segmentation helps enhance workload visibility and ensure more proactive segmentation controls so you can stop attacks before they happen
 - Illumio does this with actionable guidance, automated labeling, and robust policy recommendations.
 - By reducing the time and effort required to operate a Zero Trust Segmentation platform, Illumio empowers organizations to respond to the threat of AI-powered attacks by containing spread and getting insights faster.
- Illumio's AI-powered segmentation strengthens cyber resilience by minimizing the attack surface
 - Complex tasks like labeling and policy creation are automated so that you can receive actionable guidance to ensure continuous protection. The internal attack surface is minimized with segments and policies that are identified automatically to protect against threats.

IVA can answer questions related to Illumio products and provide best practices recommendations to improve security based on feedback and questions generated from Illumio support.

Use IVA

1. Click the IVA  located next to your name on the top, right side.
2. Ask general questions in the Chat tab, or ask specific questions about maps and web traffic in the Take Action tab.



The screenshot shows the Illumio Dashboard interface. On the left is a navigation sidebar with options like Dashboard, Servers and Endpoints, Cloud, Ransomware Protection, AI Labeling, Explore, Map, Traffic, Mesh, Policies, All Policies, and Drafts & Versions. The main content area is titled 'Dashboard' and 'Cloud See More'. It features an 'Onboarding Overview' section for AWS and Azure, which includes a 'Summary' card showing 1 Account and 1 Subscription, a 'Flow Log Access' donut chart showing 2 Full, 0 Partial, and 0 None, and a 'Read and Write Access' donut chart showing 0 Read Only and 2 Read and Write.

You can view information in two tabs:

- Chat view: Ask general questions and IVA provides an answer using natural language processing.

Dashboard

Cloud See More

Onboarding Overview AWS x Azure x

Summary: 1 Account (AWS), 1 Subscription (Azure)

Flow Log Access: 2 Full, 0 Partial, 0 None

Read and Write Access: 0 Read Only, 2 Read and Write

Servers and Endpoints See More

Total VENs by Enforcement Mode

- 12 Visibility Only
- 172 Selective

Total VENs by Status / Health

Health: 183 Healthy, 1 Warning

Status: 184 Active

Chat Take Action

What is CloudSecure?

Can you give me an example of ports and pathways that I would need to block?

How can I write an outbound any rule?

I'm sorry, but as a virtual assistant, I don't have access to specific data about your system. However, Illumio identifies several services as risky, including HTTP (TCP port 80), LLNMR (UDP port 5355), NFS (TCP/UDP port 2049), RDP (TCP/UDP port 3389), MSFRPC (TCP port 135), SMB (TCP/UDP port 445), SSH (TCP/UDP port 22), and others. I recommend reviewing your system's open ports and comparing them to Illumio's list of risky services for a more accurate assessment.

What are my risky ports?

Is RDP a ransomware vulnerable port? Can you clarify?

Yes, the Remote Desktop Protocol (RDP) which operates on TCP/UDP port 3389 is indeed considered a high-risk service. Ransomware attackers often exploit vulnerabilities in exposed RDP servers to gain unauthorized access. Therefore, Illumio recommends mapping all RDP servers and connections, identifying nonessential

Ask anything

- Take Action view: This applies to questions related to Maps and Traffic only. For example, "Show me all web traffic in my production environment for the past week." Based on your input, IVA will set appropriate filters such as specific ports and generate web traffic data.

Dashboard

Cloud See More

Onboarding Overview AWS x Azure x

Summary: 1 Account (AWS), 1 Subscription (Azure)

Flow Log Access: 2 Full, 0 Partial, 0 None

Read and Write Access: 0 Read Only, 2 Read and Write

Servers and Endpoints See More

Total VENs by Enforcement Mode

- 12 Visibility Only
- 172 Selective

Total VENs by Status / Health

Health: 183 Healthy, 1 Warning

Status: 184 Active

Chat Take Action

Show me traffic on admin ports (port 22 and 3389)

I've successfully applied filters to display traffic associated with a set of specific ports. These ports are typically known for being risky and include: 21, 23, 25, 80, 110, 135, 139, 143, 443, 445, 1433, 1521, 3306, 3389, 5432, 5500, 5800, and 5900.

I successfully analyzed the traffic for the past month to determine if any of your PCI compliant workloads are communicating with non-PCI compliant workloads. I did this by applying filters to the traffic data, specifically looking at the source and destination labels to identify which workloads are PCI compliant.

I've successfully filtered and loaded traffic data for admin ports 22 and 3389.

Show me traffic in risky ports

Are any of my PCI compliant workloads talking to non-PCI compliant workloads?

Are any of my PCI compliant workloads talking to non-PCI compliant workloads?

I've successfully checked if any of your PCI compliant workloads are communicating with non-PCI

Ask anything

Best Practices

- Ask questions in the Support tab, not in the Take Action tab, and vice versa
- Ask questions related to Illumio or information security

- Ask questions related to the feature you have active in the UI. Asking Core-related questions while you are in a Servers and Endpoints feature will give you inaccurate answers.
- Use the Take Action tab for things related to the feature you have active in the UI. For Servers and Endpoints, the Take Action tab is available on the Map and Traffic pages. For Core, the Take action tab is available on the Cloud Map and Traffic pages.
- Ask questions that are 50 words or fewer in length
- Ask no more than seven questions per minute, per tenant, for best performance
- Filters support AND with the following terms:
 - Cloud Map and Cloud Traffic:
 - Cloud
 - Regions
 - Account ID
 - Resource Type
 - Maps and Traffic (Servers and Endpoint):
 - Source: labels
 - Destination: labels
 - Service port and protocol
 - Time Range

**NOTE**

Transparency Notice: Illumio confirms that Customer Data processed through the Illumio Virtual Advisor feature (IVA) will not be commingled with the data of other customers. It will remain logically separated to ensure data integrity and confidentiality and will not be used to train a large language model.

Customer Data will only be used within the bounds of the customer's instance and strictly for the purpose of the Company providing the IVA feature to Customer. This includes the operation, maintenance, support, and improvement of IVA, but does not include use for any other purposes without Customer's explicit consent.

The Customer agrees that any output of IVA is merely a suggestion or recommendation to be taken under advisement by the Customer and must be independently reviewed, verified, and assessed for accuracy by the Customer.