illumio

EBOOK

Illumio Insights in Action

The incident response playbook for threat hunters, security operations teams, and forensic investigators

Contents

INTRODUCTION
Turning weak signals into action:
why security practitioners rely on Illumio Insight 3

USE CASE 1
Suspecting a threat actor 4

USE CASE 2
Investigating risky traffic before it escalates 7

USE CASE 3
Stopping malicious access fast 10

USE CASE 4
Catching data exfiltration in motion 16

USE CASE 5
Tracking unsanctioned LLM use 21

CONCLUSION
Taking the next step 24

INTRODUCTION

Turning weak signals into action: why security practitioners rely on Illumio Insight

News headlines aside, the most serious cyber threats aren't loud. They hide in normal traffic, using trusted tools and everyday protocols to slip past your defenses. For security analysts, incident responders, and threat hunters, the challenge is clear: spotting the risks of lateral movement, persistence, and data exfiltration before it's too late.

Illumio Insights turns suspicion and weak signals into clear evidence that security teams can act on right away. It answers the most critical questions: Which workloads are at risk? How could attackers move through the environment? Where should they be contained? Armed with these answers, security teams can contain breaches quickly before they escalate, stopping intrusions from turning into cyber disasters.

This guide explores five real-world use cases. It shows how Insights empowers teams to investigate, confirm, and act with confidence. With this clarity, security practitioners can contain threats quickly and protect critical data across hybrid, multi-cloud environments.

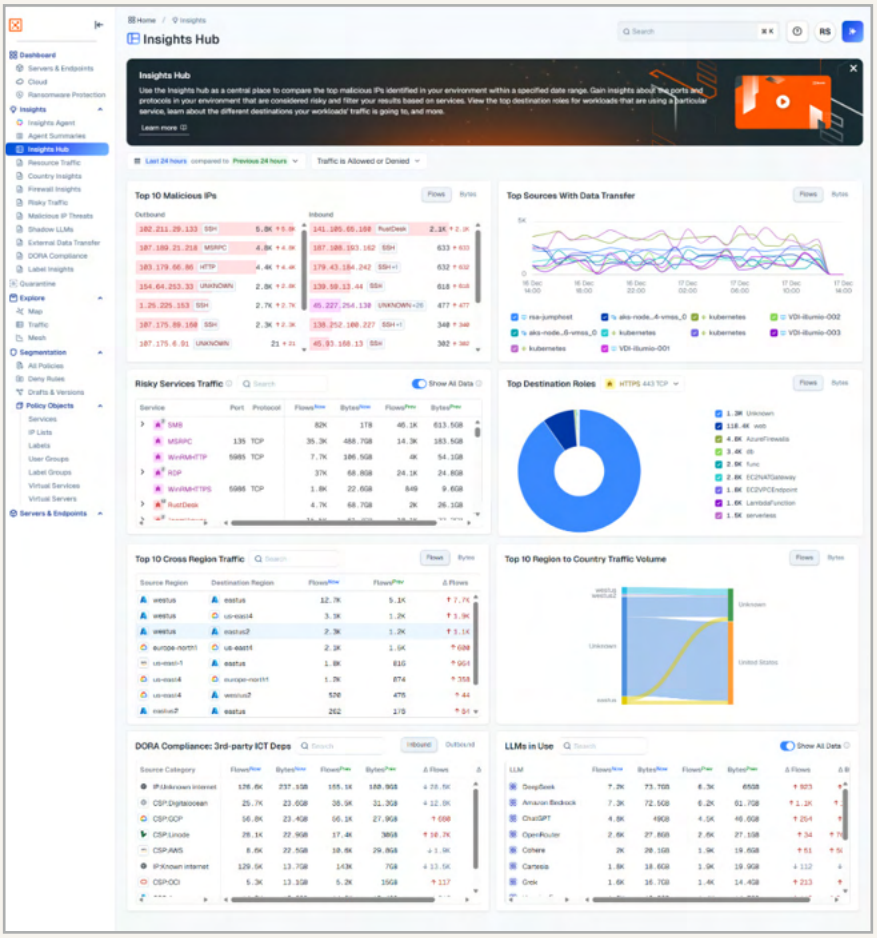

Figure 1: The Illumio Insights Hub: The central place for cyber threat investigation and analysis

USE CASE 1

Suspecting a threat actor

Objective: You suspect a threat actor is targeting your environment. You need to validate that suspicion by detecting behaviors tied to lateral movement, persistence, and privilege abuse.

Security practitioners know that threat actors rarely reveal themselves directly. They leave faint trails.

The breadcrumb could be a sudden spike in SMB connections. Or maybe it's an odd service, such as RustDesk, running where it shouldn't. It might even be unexpected zone-to-zone traffic.

For an analyst, the question isn't just "Is something happening?" It's "Does this activity map to a real adversary's playbook?"

Illumio Insights help security teams pivot from suspicion into evidence. By aligning indicators with known Tactics, Techniques, and Procedures (TTPs), you can confirm whether the unusual traffic is lateral movement, isolate the workloads involved, and determine the blast radius. Instead of guesswork, you can move with confidence from detection to instant breach containment.

Threat hunting in Insights using Agent

With Illumio Insights, even the quietest threats can't hide for long. Now you can customize and automate your insights using the Threat Hunter persona in Insights Agent.

Insights Agent acts as an AI-powered investigation assistant that helps security teams turn weak signals into fast, confident action. It continuously analyzes traffic, behaviors, and risk indicators across hybrid and multi-cloud environments, highlighting where attackers could move, which workloads are exposed, and how threats might spread. By aligning activity to known attacker techniques and prioritizing what matters most, Insights Agent guides analysts from suspicion to evidence — accelerating detection, simplifying investigation, and enabling rapid containment before threats escalate or data is lost.

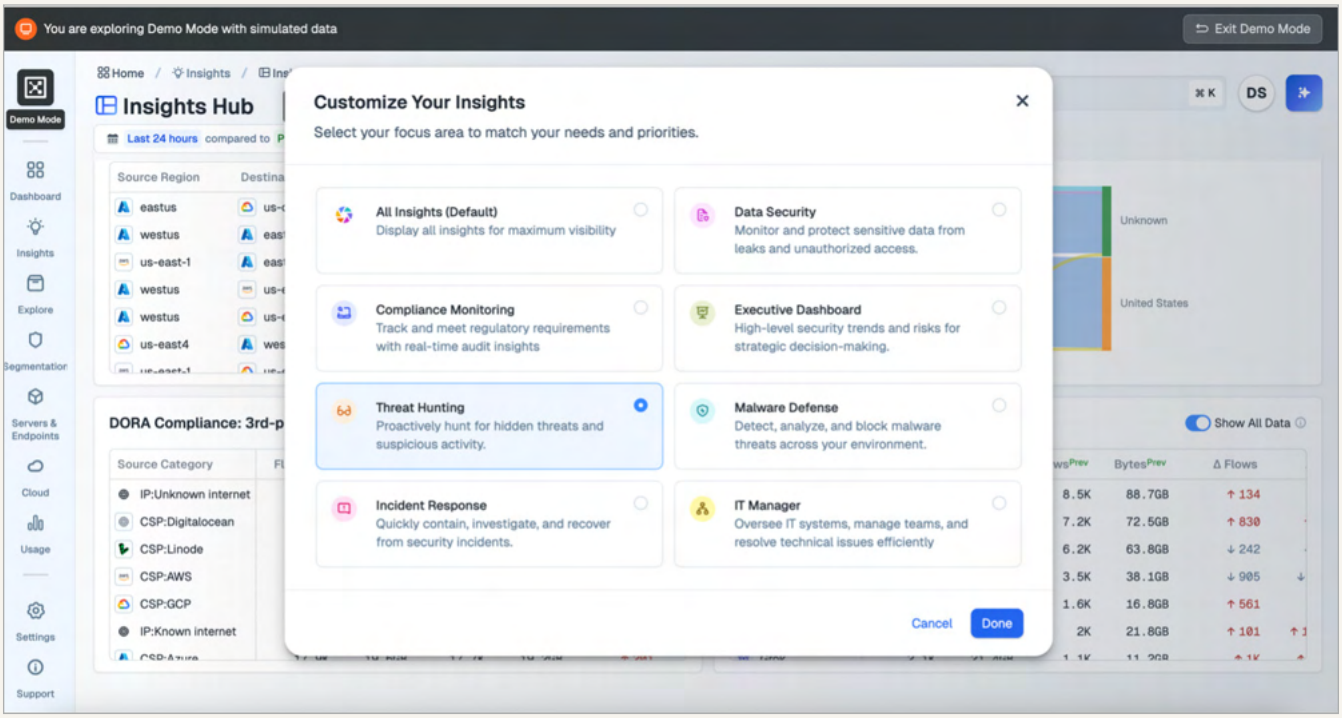

Figure 2: Insights Agent offers customized security capabilities tailored to individual roles and responsibilities.

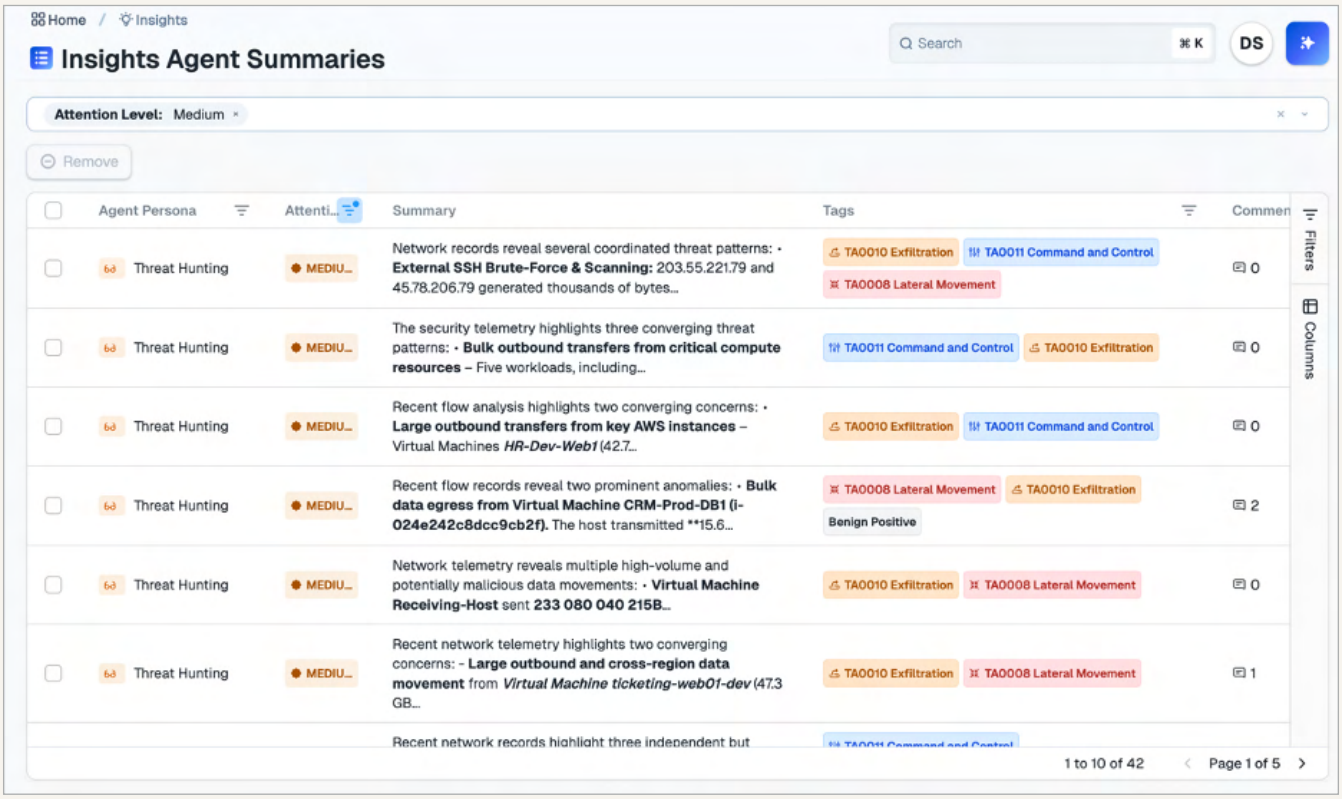

Figure 3: View a summary of active threats, including the needed attention level, and drill down to view more security details.

How to investigate and scope a suspected threat

The following actions can help you investigate suspicious activity, identify impacted systems, and decide when to act:

Map any adversary TTPs:

In **Risky Services Traffic**, filter for Server Messaging Block (SMB) and other protocols commonly used for lateral movement, including unexpected Remote Desktop Protocol (RDP) sessions or remote access tools like RustDesk.

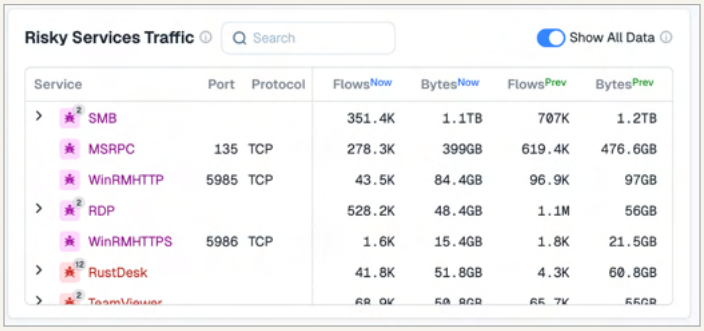

Figure 4: A workflow analysis of potentially risky services and ports

Determine if roles or workloads are being targeted:

Use **Top Destination Roles** to determine which system categories are receiving the most traffic and whether those targets align with normal behavior.

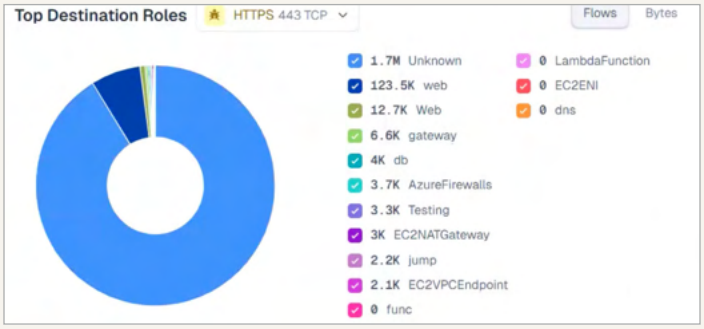

Figure 5: The Top Destination Roles view shows which systems are receiving the most traffic.

Analyze your SMB activity:

In **Risky Traffic**, filter by **SMB** and look for abnormal patterns such as unusually high connections or bytes that are being transferred.

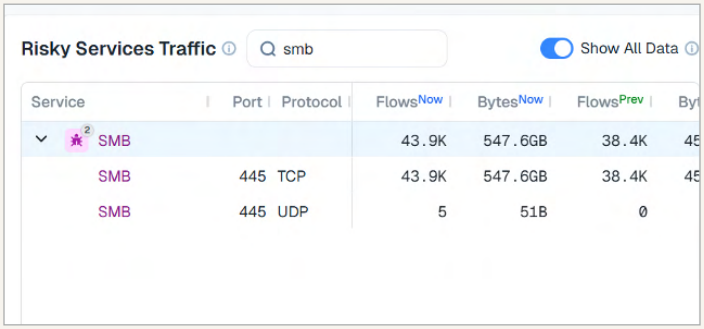

Figure 6: Risky Services traffic filtered by SMB in the last 24 hours

Pinpoint affected workloads:

Check **Top 10 Cross Region Traffic** to determine any systems generating or receiving anomalous traffic.

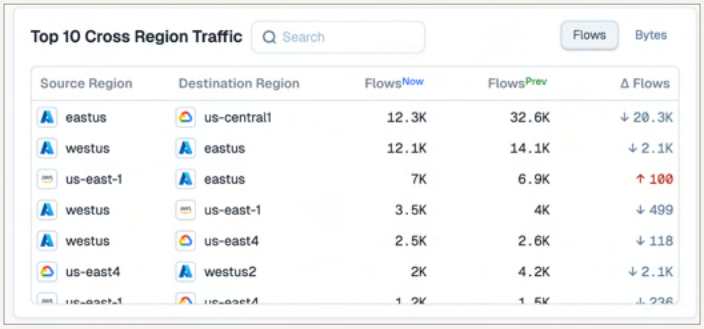

Figure 7: Top 10 Cross Region Traffic showing traffic flow patterns

USE CASE 2

Investigating risky traffic before it escalates

Objective: You need to investigate potentially dangerous traffic. These include risky protocols, connections to malicious IPs, or anomalous patterns that could signal early compromise.

Analysts know risky traffic isn't always malicious, but it's never safe to ignore. Whether it's old protocols like Telnet or SMBv1, remote management tools appearing in unexpected zones, or connections that spike late at night — each one deserves scrutiny. These anomalies are often precursors to privilege escalation or data staging.

With Illumio Insights, teams can hunt from the top down: begin with high-risk protocols, drill into which workloads are talking, and zero in on traffic flows where you need more information. This process turns risky traffic from being just background noise to actionable information.

Here's how to use Insights to turn suspicious connections into clear, actionable intelligence:

1. **Filter by risky protocols:** In **Risky Services Traffic**, select legacy or insecure services such as Telnet, FTP, SMB, or RDP.

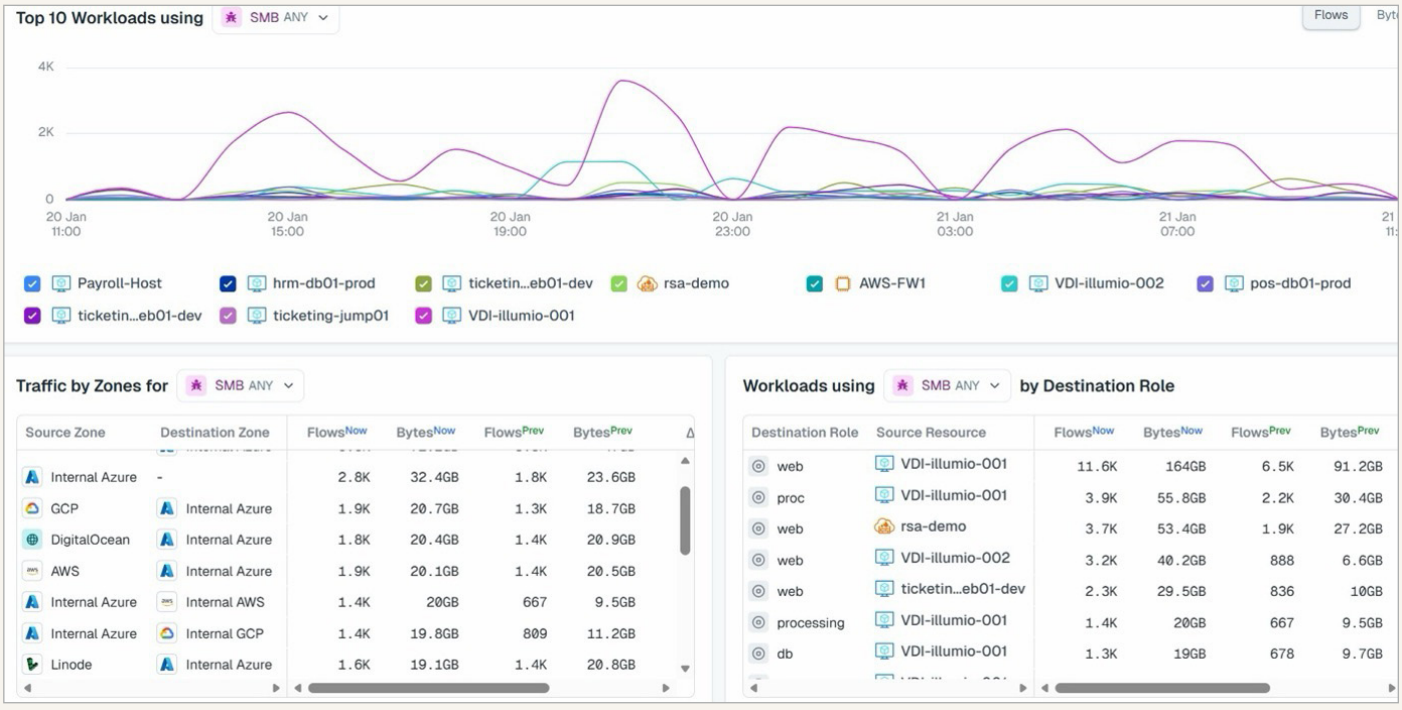

Figure 8: The Risky Services Traffic dashboard

2. **Identify roles and workloads at risk:** Review **Workloads by Destination Role** for exposure.

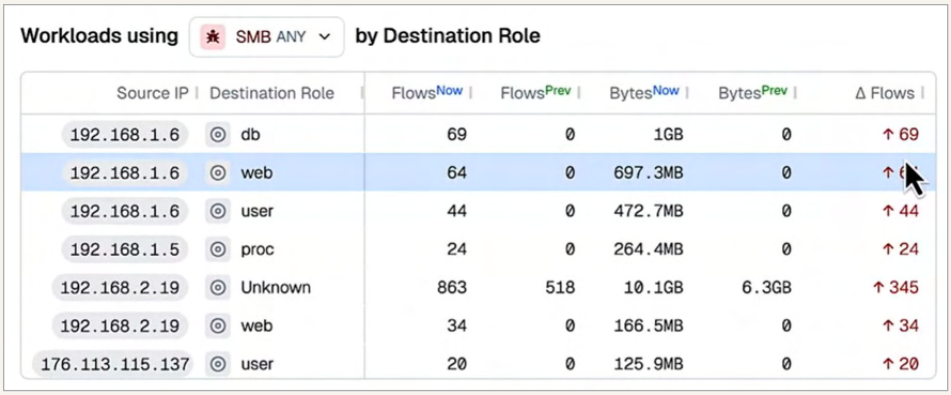

Figure 9: Workloads filtered by SMB traffic sorted by destination source IP and roles

3. **Check exposure:** In **Traffic by Zones**, determine whether risky traffic crosses boundaries, such as leaking externally to the internet, or if large amounts of data are leaving the network.

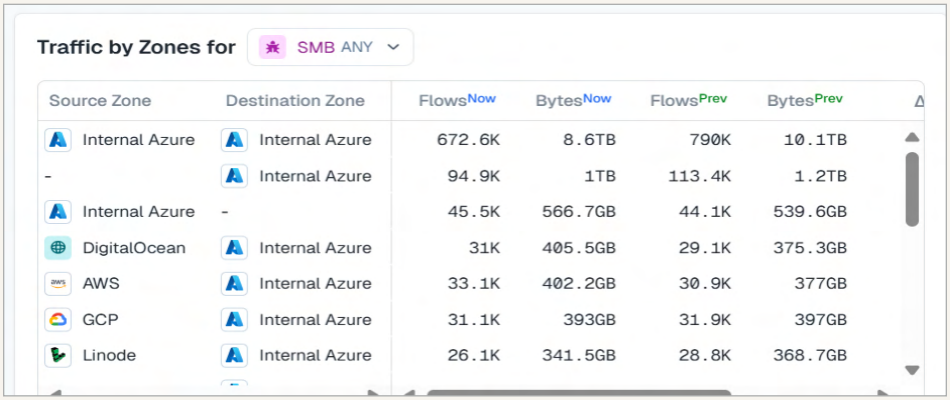

Figure 10: SMB traffic by source and destination zones

4. **If a resource is suspect:** Click the workflow and open the **Resource Traffic Map** to see potential lateral movement.

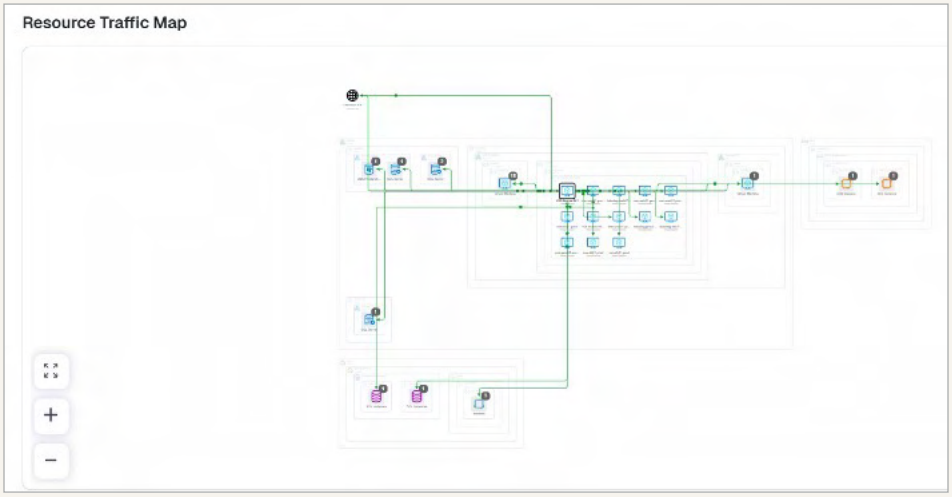

Figure 11: The Resource Traffic Map showing lateral movement paths

5. **Quarantine:** If a resource needs to be isolated, click the **Quarantine** button (currently available only with Azure) and confirm the quarantine.

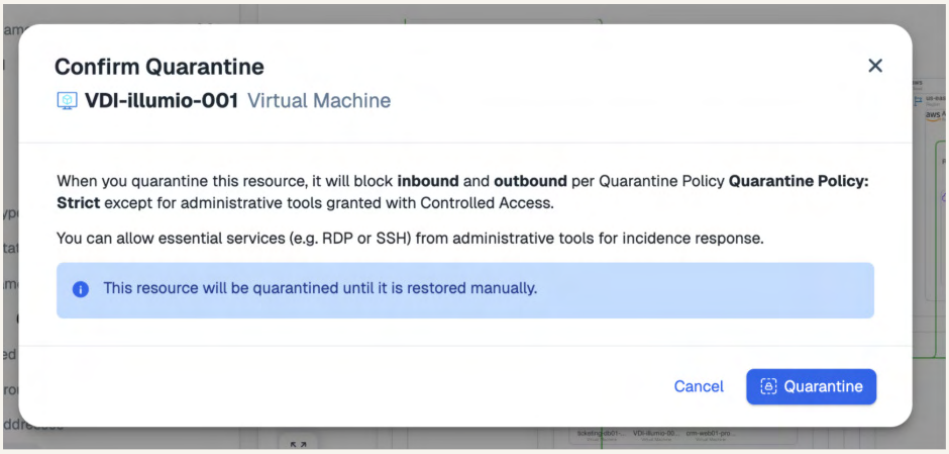

Figure 12: Confirm the compromised workload to be quarantined.

6. Navigate to **Quarantine** on the left panel to see a list of all quarantined resources to take further action.

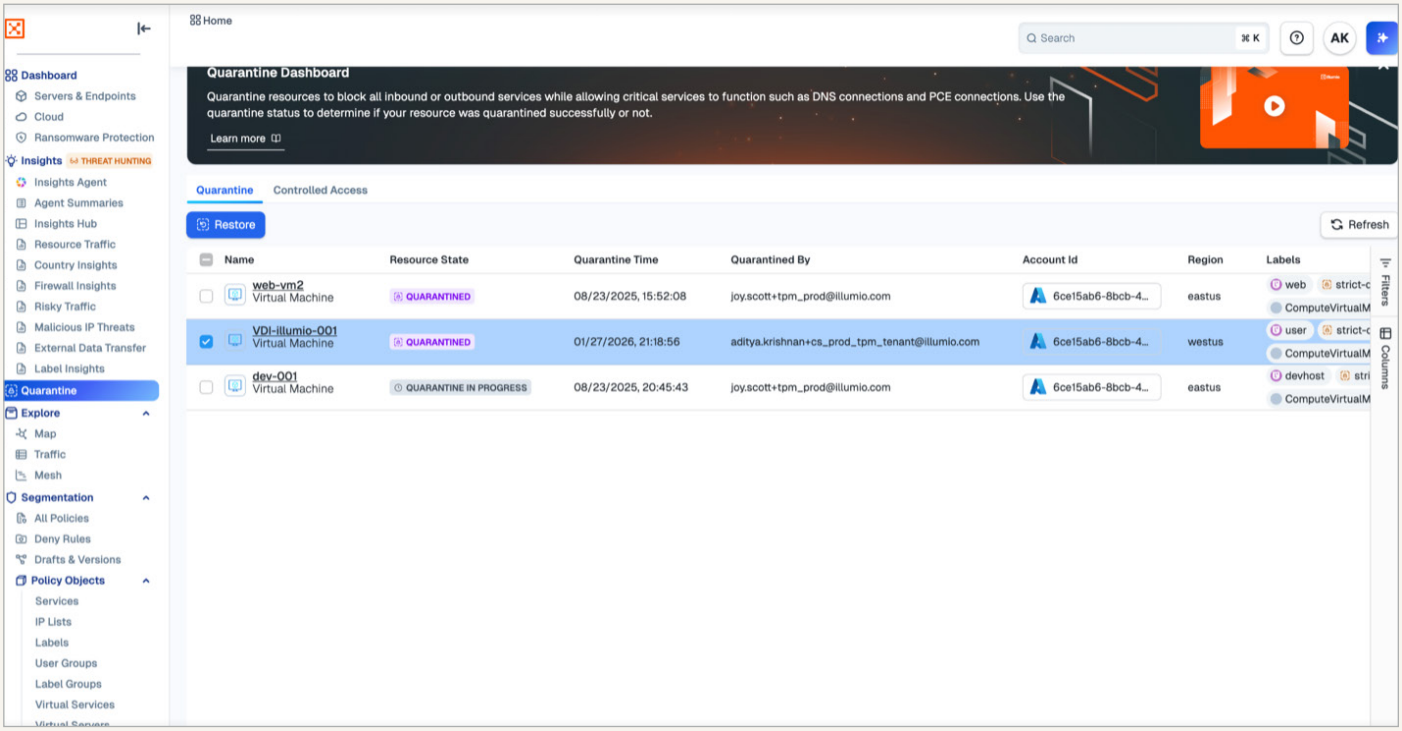

Figure 13: The Quarantine Dashboard

USE CASE 3

Stopping malicious access fast

Objective: You're concerned about inbound access from known malicious IPs or domains and need to scope and stop threats quickly.

Attackers don't just probe once. They persist. Frontline security often sees repeated attacks from the same malicious IPs trying to blend into normal traffic. The challenge is to separate noise from true malicious access and quickly identify where those IPs are connecting inside your environment.

Illumio Insights makes this triage fast. It surfaces known-bad IPs, maps flows to workloads, and overlays geography through the Global Threat Map. This shows analysts which connections matter and allows them to cut off malicious access before it escalates.

Cutting off malicious access in Insights

Here's how to use Insights to cut through false positives, confirm malicious access, and contain threats before attackers can gain a foothold:

1. **Surface malicious connections:** In Insights Hub, select **Malicious IP Threats** to display known-bad IPs and domains.

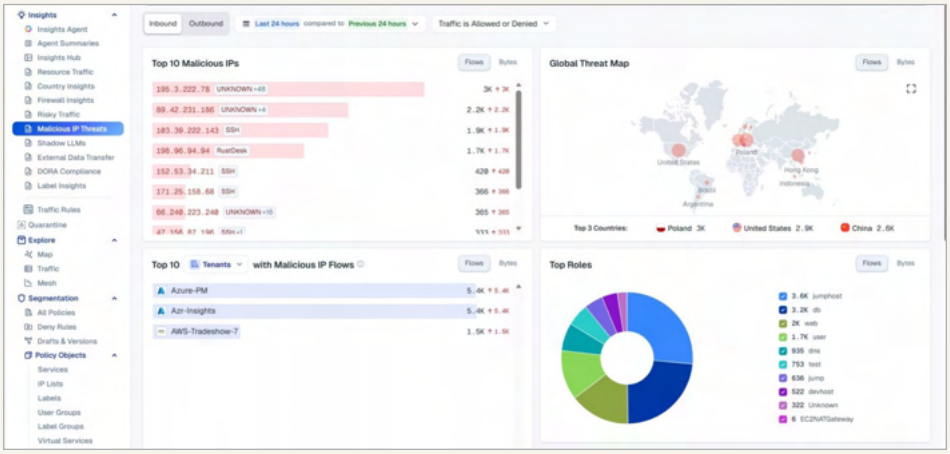

Figure 14: The Malicious IP Threats dashboard

2. **Prioritize indicators of compromise (IOCs):** Review the **Top 10 Malicious IPs** and **Top 10 services used in malicious IP communications** to focus on the most relevant threats.

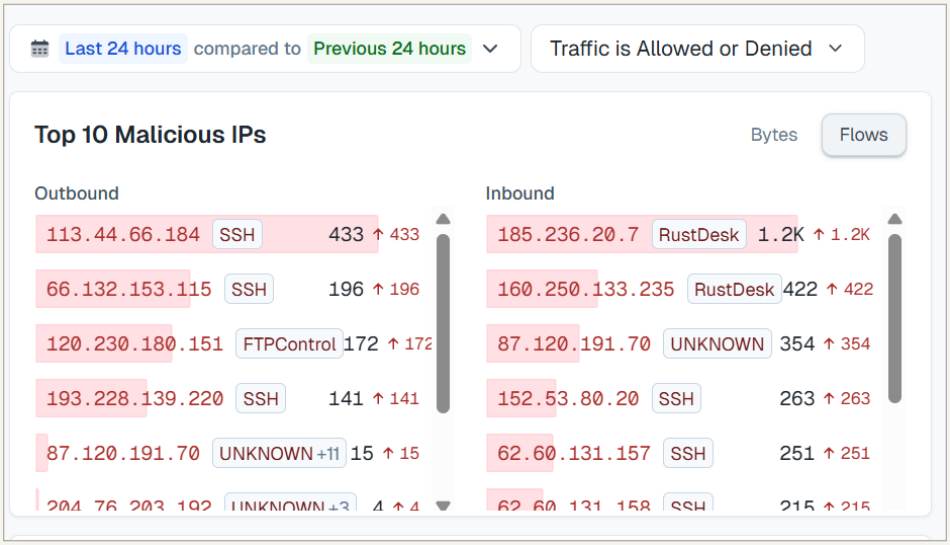

Figure 15: The Top 10 Malicious IPs showing inbound and outbound traffic

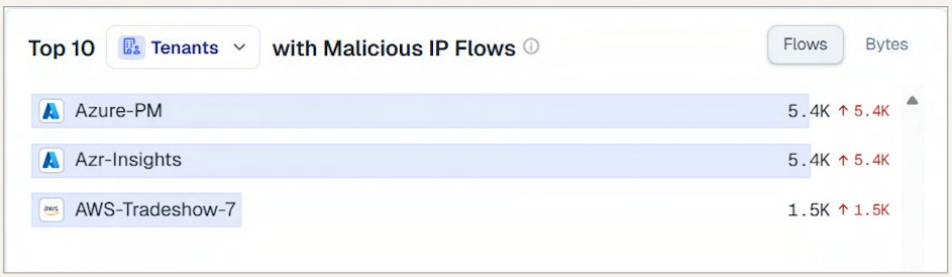

Figure 16: The Top 10 Services with Malicious IP Flows

3. **Scope affected workloads:** In the **Resource Traffic Map**, visualize workloads communicating with malicious IPs.

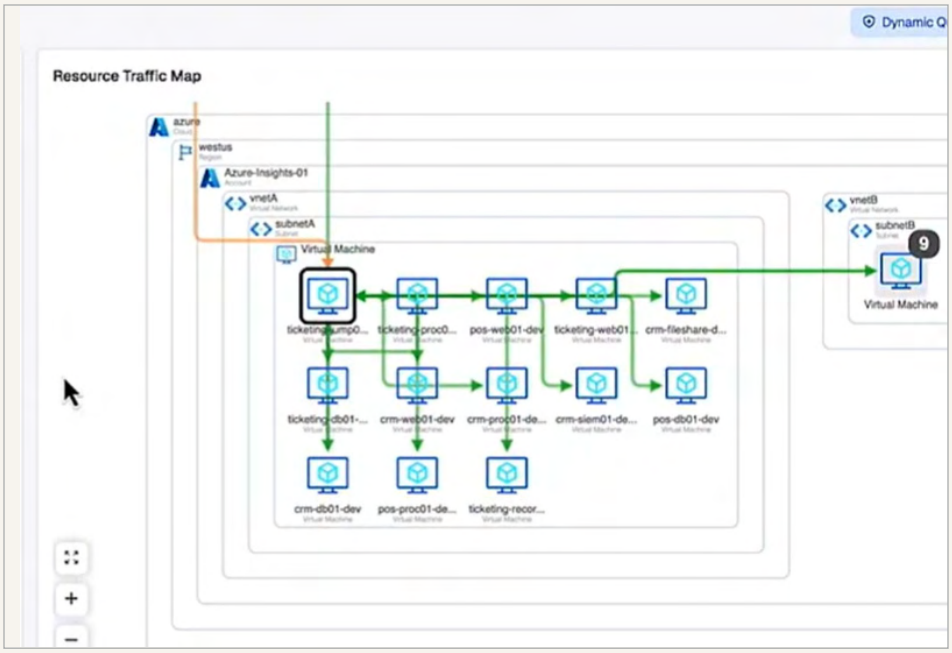

Figure 17: The Resource Traffic Map showing workloads communicating with malicious IPs

4. **Add geographic context:** Use the **Global Threat Map** to view regions where malicious connections originate.

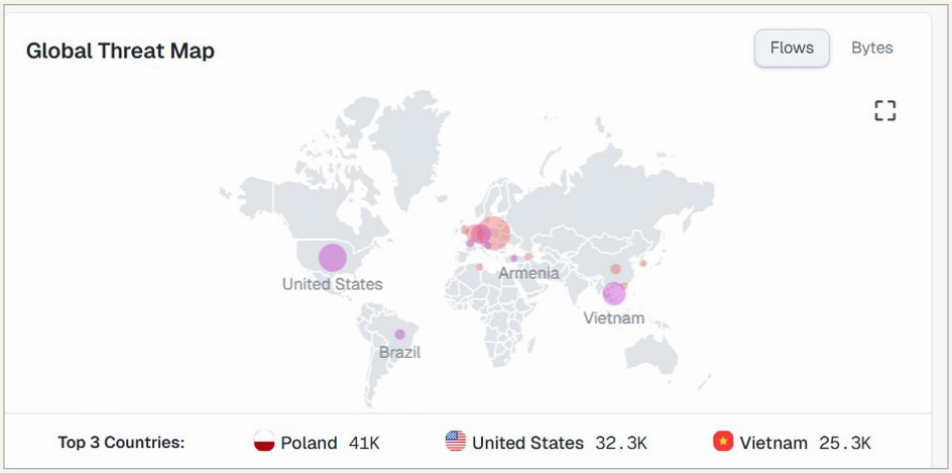

Figure 18: Global Threat Map showing which countries are originating malicious IPs

5. **Inspect detailed flows:** In **Traffic Query Results**, analyze source IPs, zones, ports, services destinations for anomalous traffic.

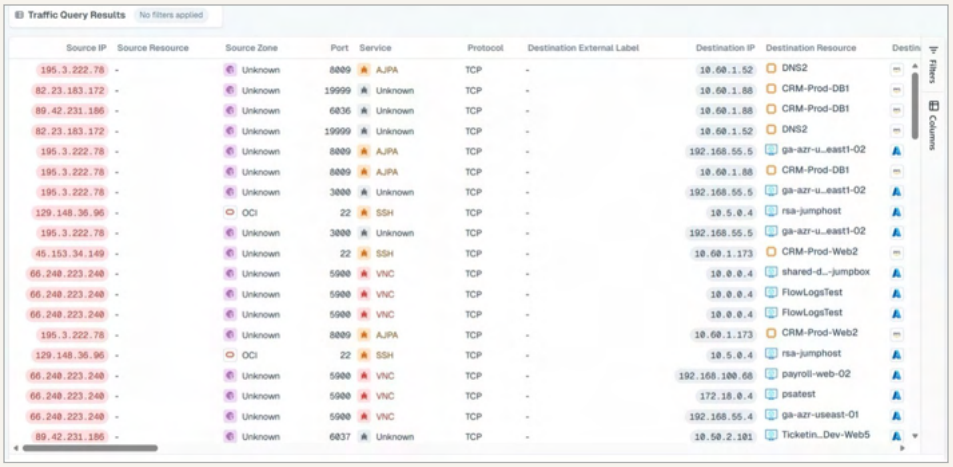

Figure 19: The Traffic Query Results panel

6. **Map potential spread:** Select the **Communications Map** to see if compromised workloads are talking laterally.

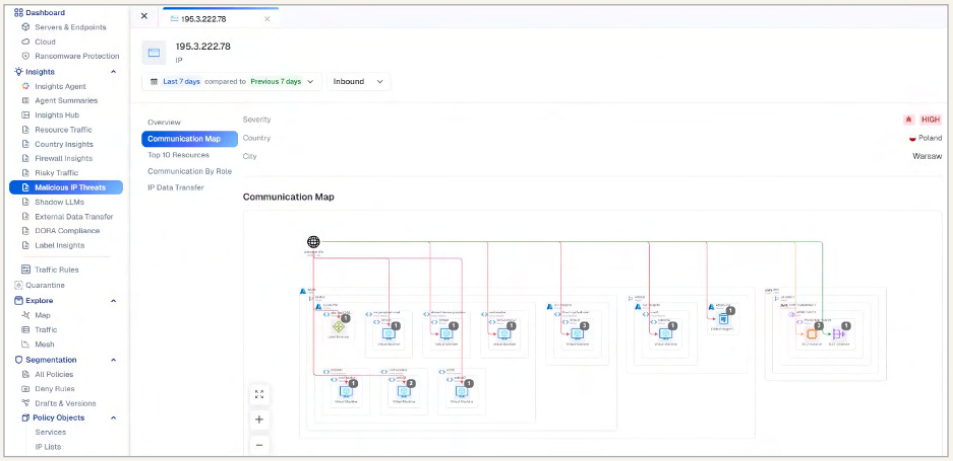

Figure 20: The Communications Map showing communication between workloads

7. **Contain quickly:** If malicious access is confirmed, select the compromised workloads workflow and quarantine.

8. **If a resource is suspect:** Click the workflow, which will take you to the **Resource Traffic Map** to see potential lateral movement.

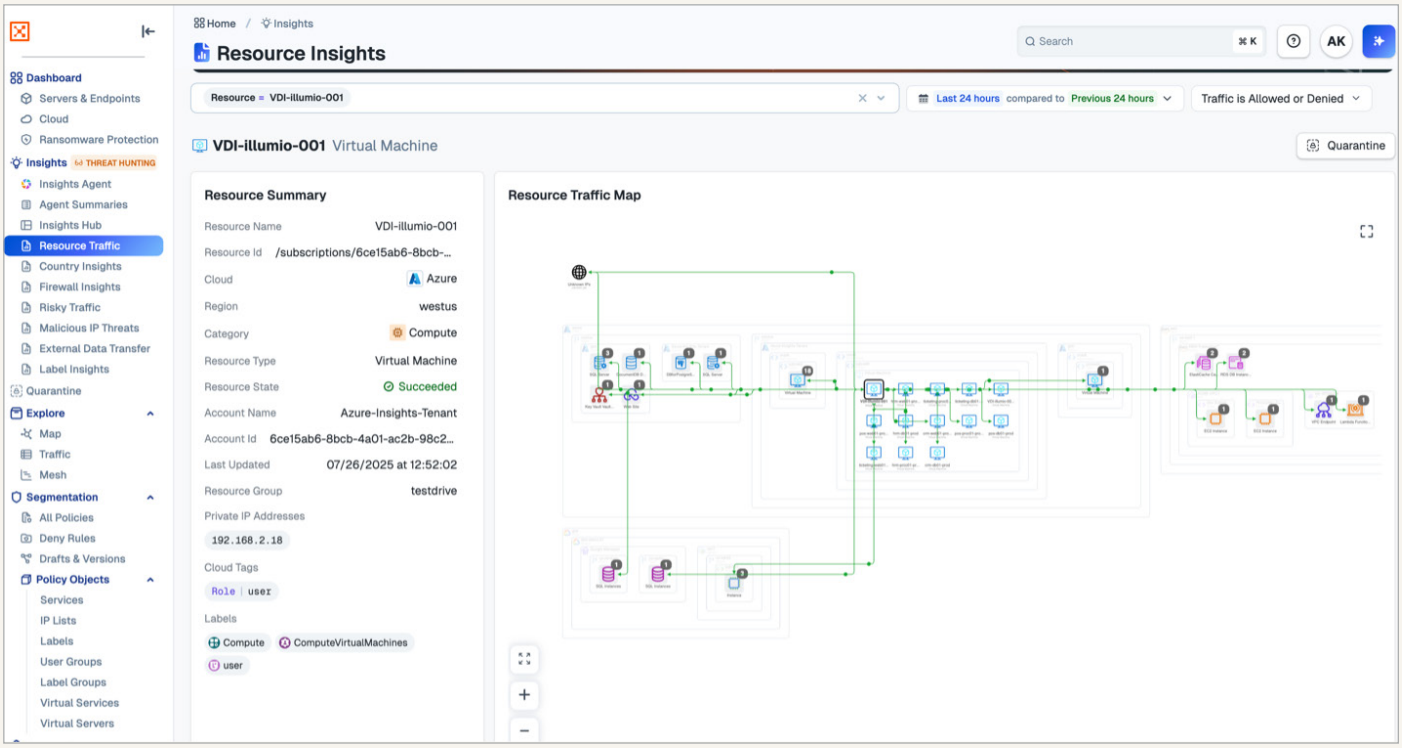

Figure 21: The Resource Traffic Map showing lateral movement paths

9. **Quarantine:** If a resource needs to be isolated, click the **Quarantine** button (currently available only with Azure) and confirm the quarantine.

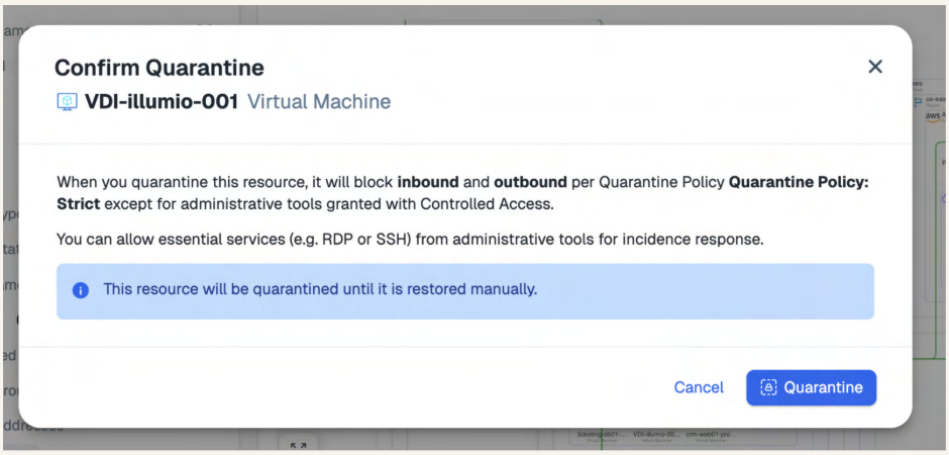

Figure 22: Confirm the compromised workload to be quarantined.

10. Navigate to **Quarantine** on the left panel to see a list of all quarantined resources to take further action.

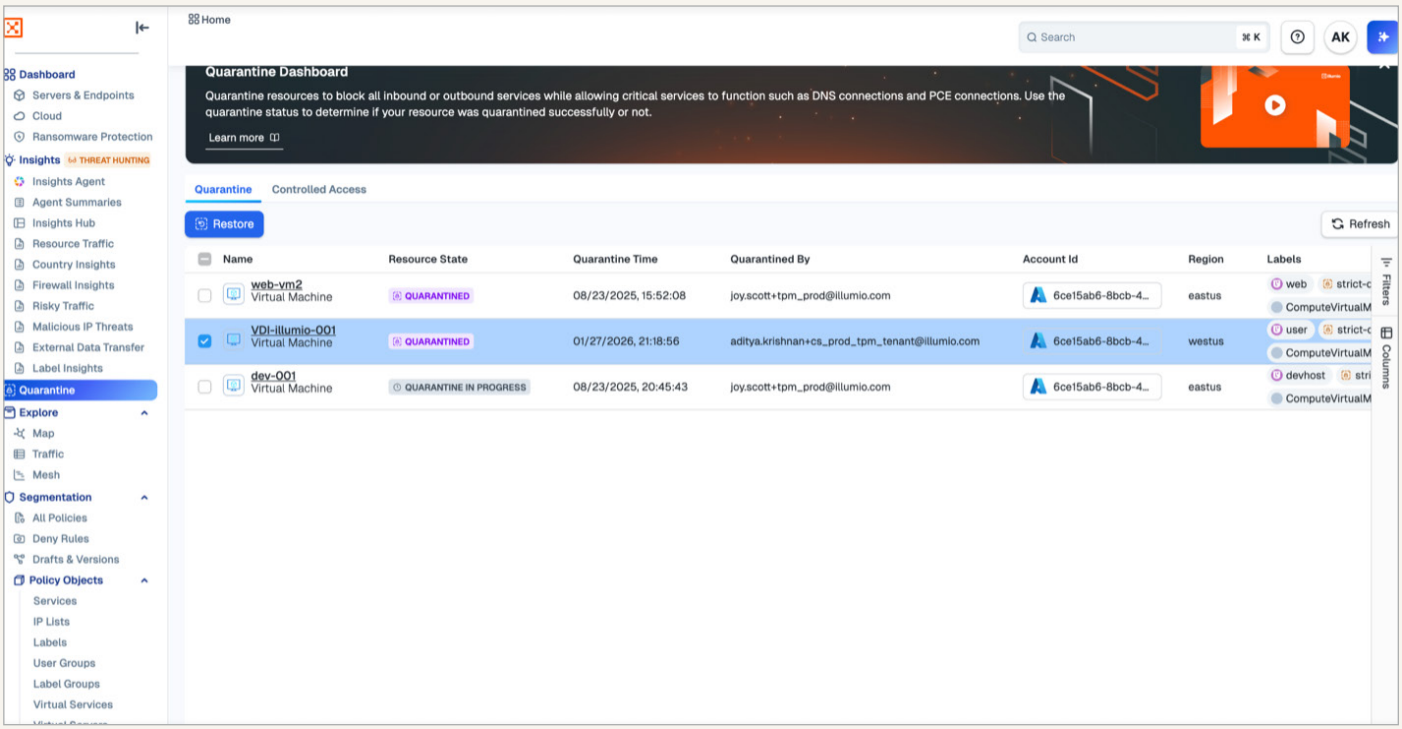

Figure 23: The Quarantine Dashboard

USE CASE 4

Catching data exfiltration in motion

Objective: You suspect potential data exfiltration and need to investigate large transfers, outbound destinations, and responsible workloads.

Data exfiltration is the attacker's payday. Analysts know it rarely looks like a single giant data dump. It often trickles over time, hidden inside normal data flows. The red flags include:

- Large byte counts showing unusual workloads
- Data headed to geographies with no business need
- Outbound transfers to AI/LLM services that are not sanctioned by policy

Illumio Insights brings exfil attempts into focus. It combines byte and flow counts, drilling into source workloads and analyzing destination categories and locations. This context helps analysts confirm and cut off leaks before the data walks out the door.

Spotting data exfiltration in Insights

With Insights, even stealthy exfil attempts can't hide for long. Here's how to use Illumio Insights to uncover data exfiltration in progress:

1. Select the **External Data Transfer** dashboard.

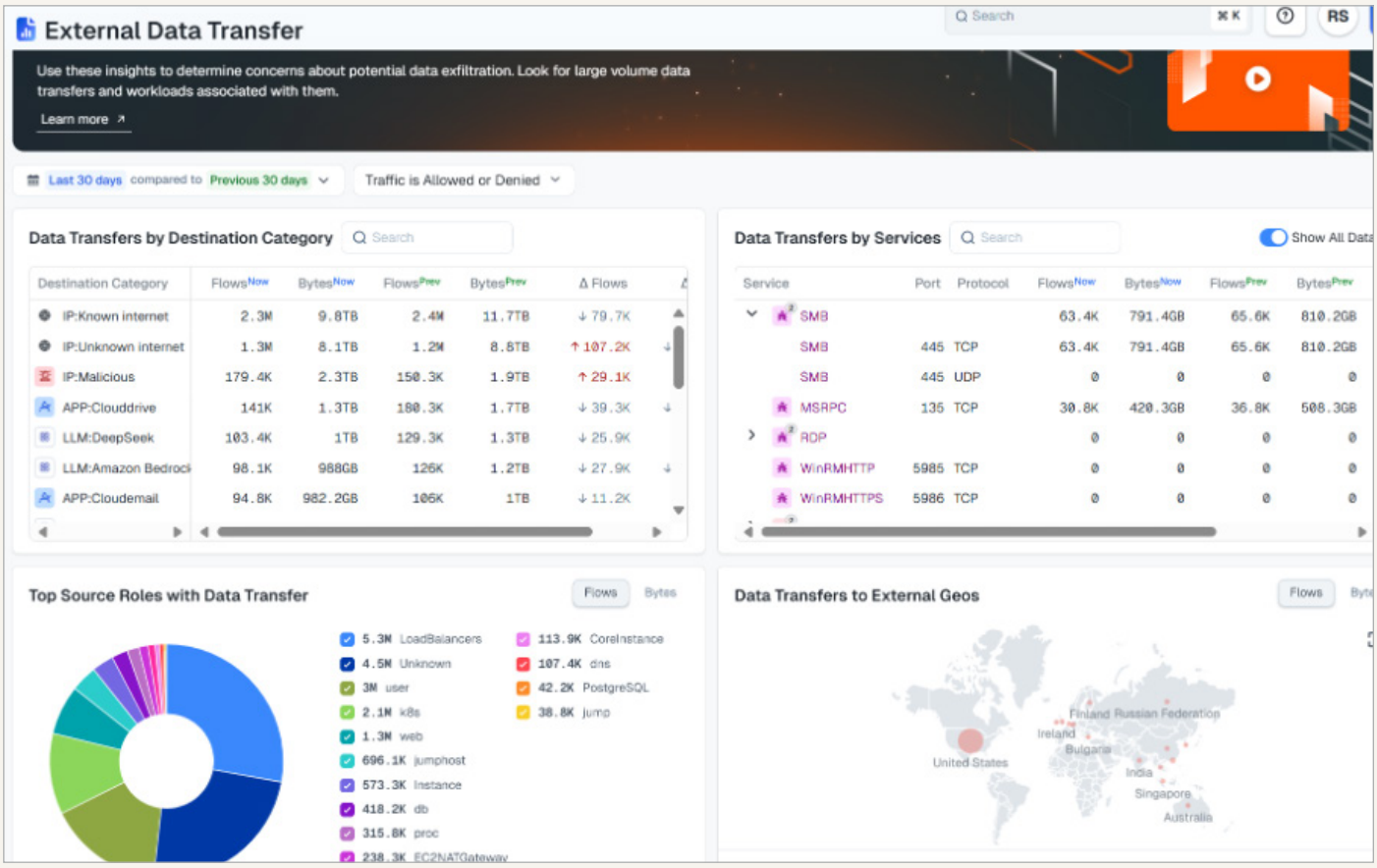

Figure 24: The External Data Transfer dashboard

2. **Confirm outbound transfers:** In the **External Data Transfers** dashboard, you can surface anomalous outbound activity.

3. **Identify destinations:** In **Data Transfers by Destination Category**, see whether data is flowing to CSPs, AI services, or unsanctioned endpoints.

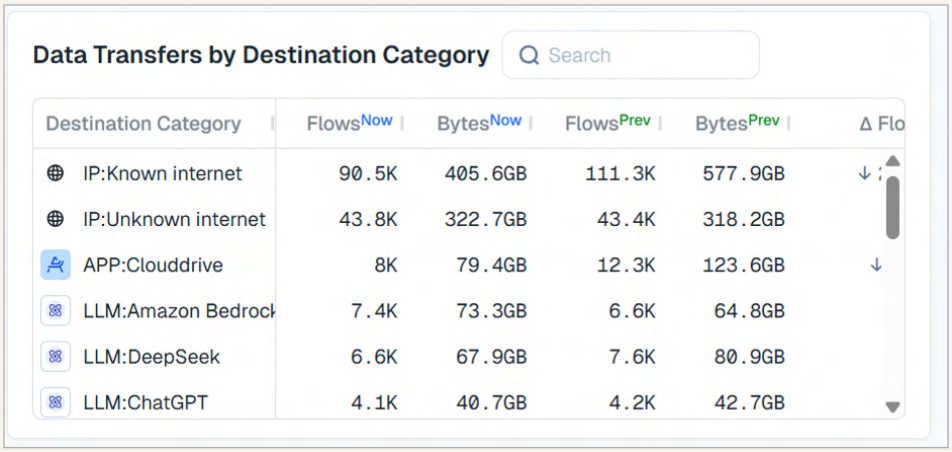

Figure 25: Data Transfer by Destination Category dashboard with views of flows and bytes

4. **Analyze transfer methods:** In **Data Transfers by Services**, check which protocols and services are in use, such as HTTPS, SFTP, and tunneling.

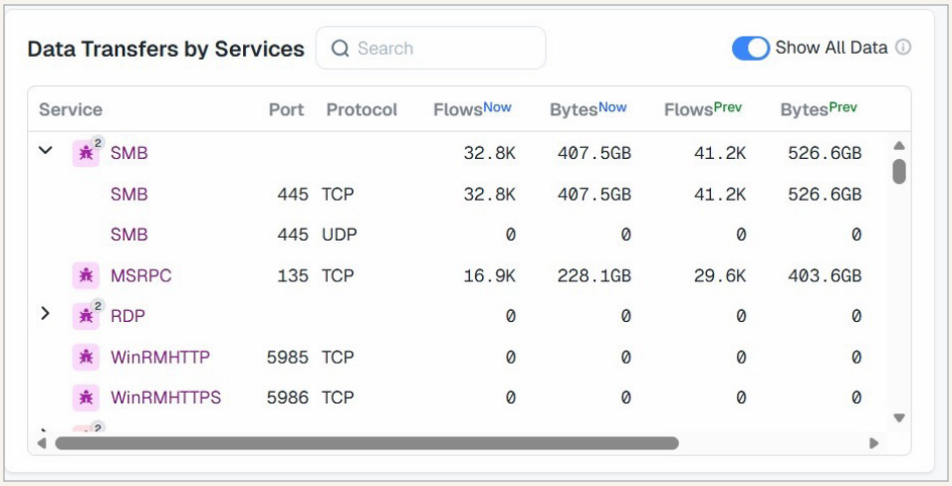

Figure 26: The data that is being transferred by services

5. **Compare volume vs. frequency:** Contrast bytes transferred vs. number of flows to detect stealthy exfil (such as many small flows or single large bursts).

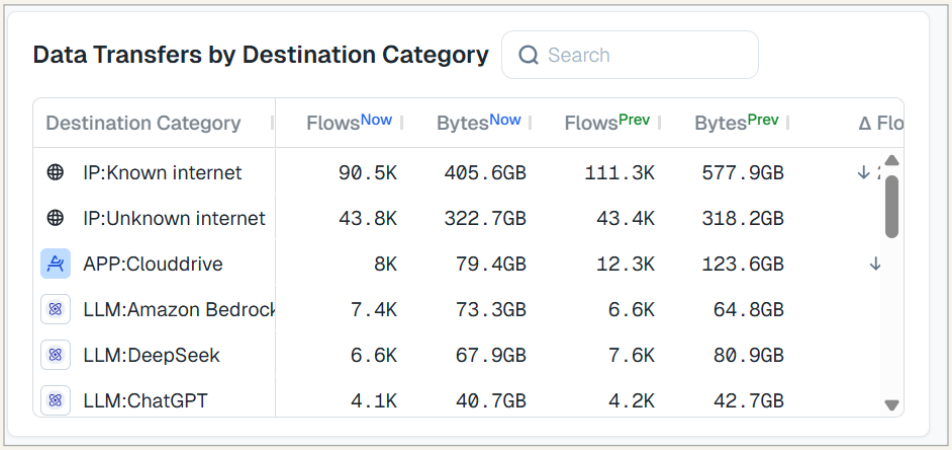

Figure 27: Data Transfer by Destination Category dashboard

6. **Add geographic analysis:** In **Data Transfers to External Geos** and **Traffic Activity Across Countries** check location details; hover or expand for information about the destination.

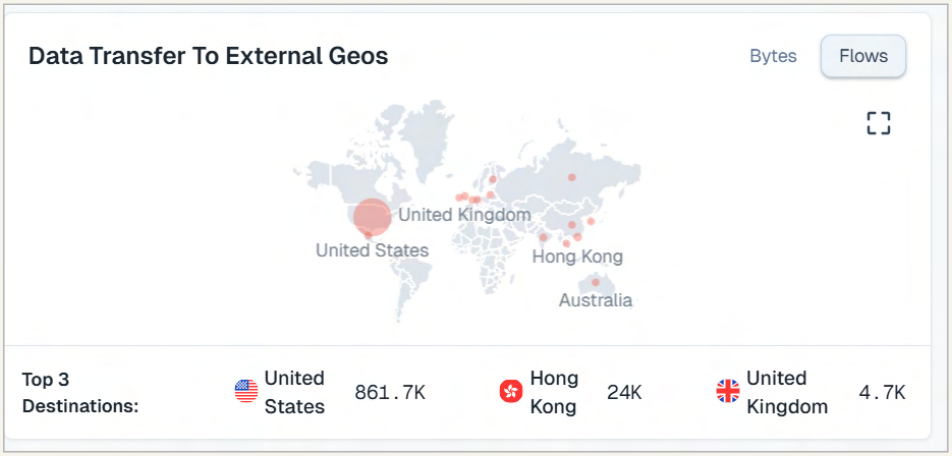

Figure 28: View external data transfer by country

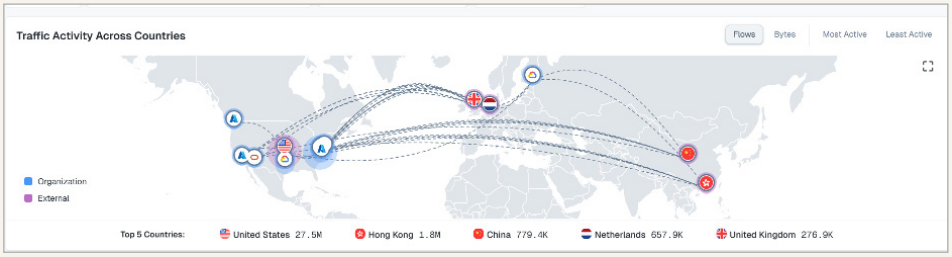

Figure 29: The Traffic Activity Across Countries dashboard

7. **If a resource is suspect:** Click the workflow, which will take you to the **Resource Traffic Map** to see potential lateral movement.

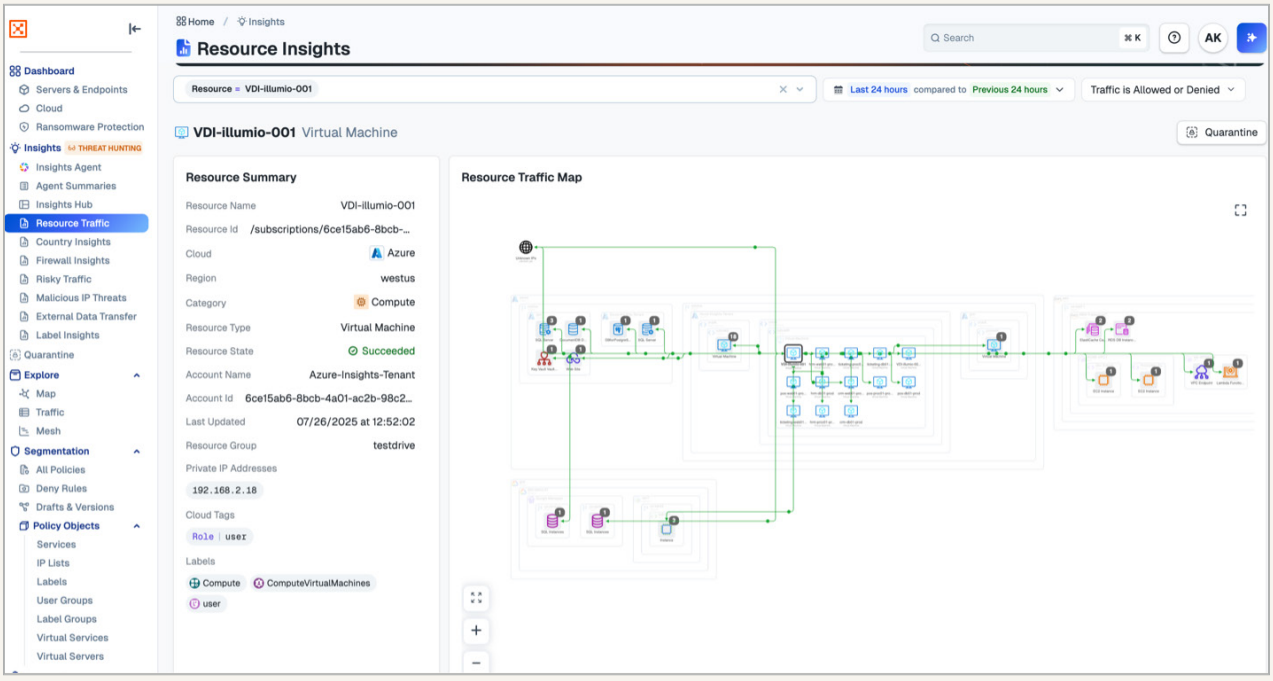

Figure 30: The Resource Traffic Map showing lateral movement paths

8. **Quarantine**: If a resource needs to be isolated, click the **Quarantine** button (currently available only with Azure) and confirm the quarantine.

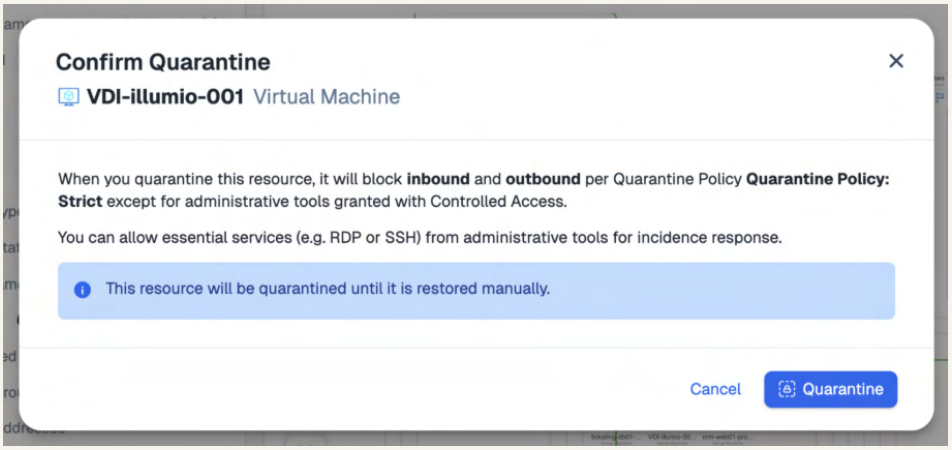

Figure 31: Confirm compromised workloads to be quarantined

9. Navigate to **Quarantine** on the left panel to see a list of all quarantined resources to take further action.

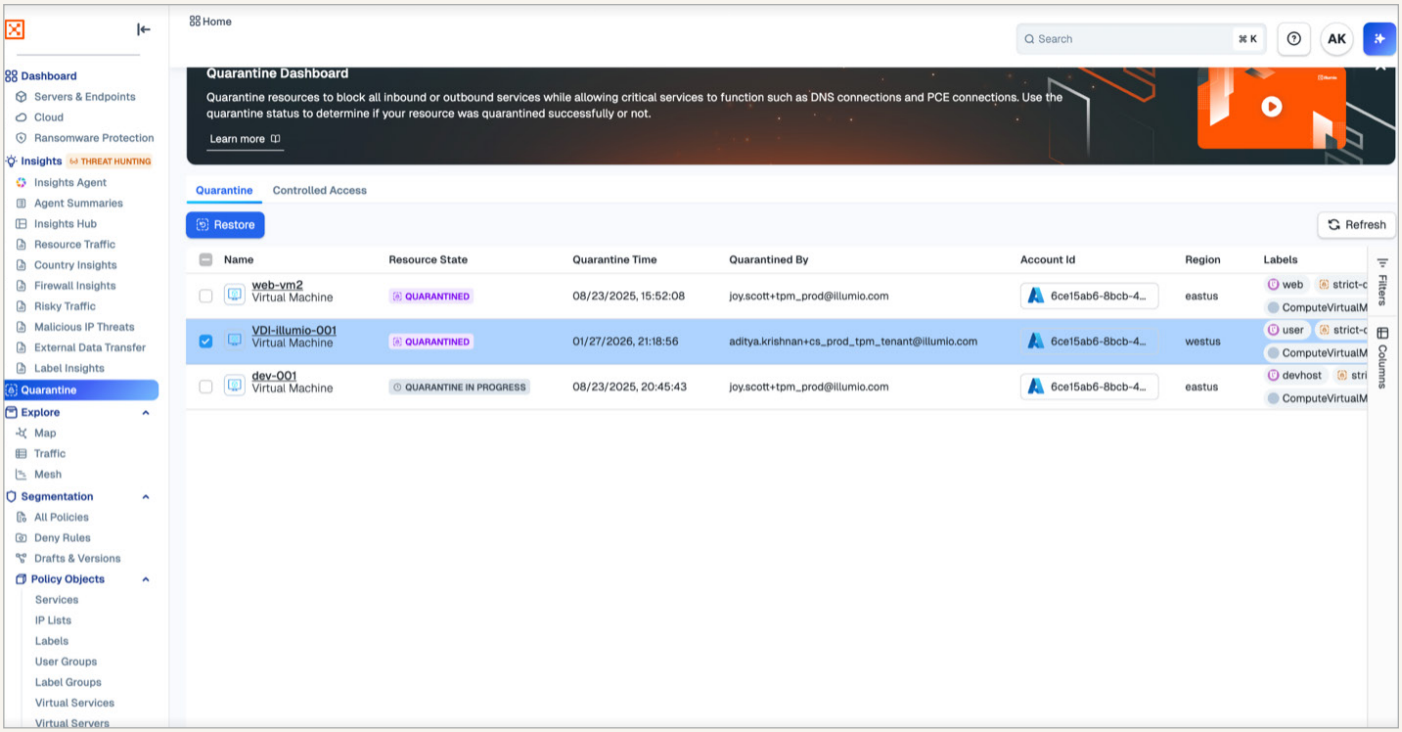

Figure 32: The Quarantine Dashboard

USE CASE 5

Tracking unsanctioned LLM use

Objective: You need to identify and investigate traffic from workloads accessing AI tools that are not sanctioned or approved.

For SOC teams, unsanctioned AI usage isn't just a policy violation — it's a data leakage risk. Analysts must know whether workloads are pushing sensitive data to public LLMs like OpenAI, Anthropic, or other APIs outside approved channels. Attackers can also exploit LLM endpoints to stage data collection or mask exfiltration.

Illumio Insights helps teams spot these connections by categorizing traffic to LLM destinations, mapping flows, and determining whether workloads are sending unusual volumes of data. It's about turning a vague "shadow AI" concern into a concrete list of systems and connections that can be shut down as needed.

Tracking AI tools in Insights

With Insights, shadow AI doesn't stay in the shadows. Here's how to use Illumio Insights to detect unsanctioned AI traffic, identify which workloads are at risk, and shut down unauthorized connections before data leaves your control:

1. **Detect LLM traffic:** Select **Shadow LLMs**.

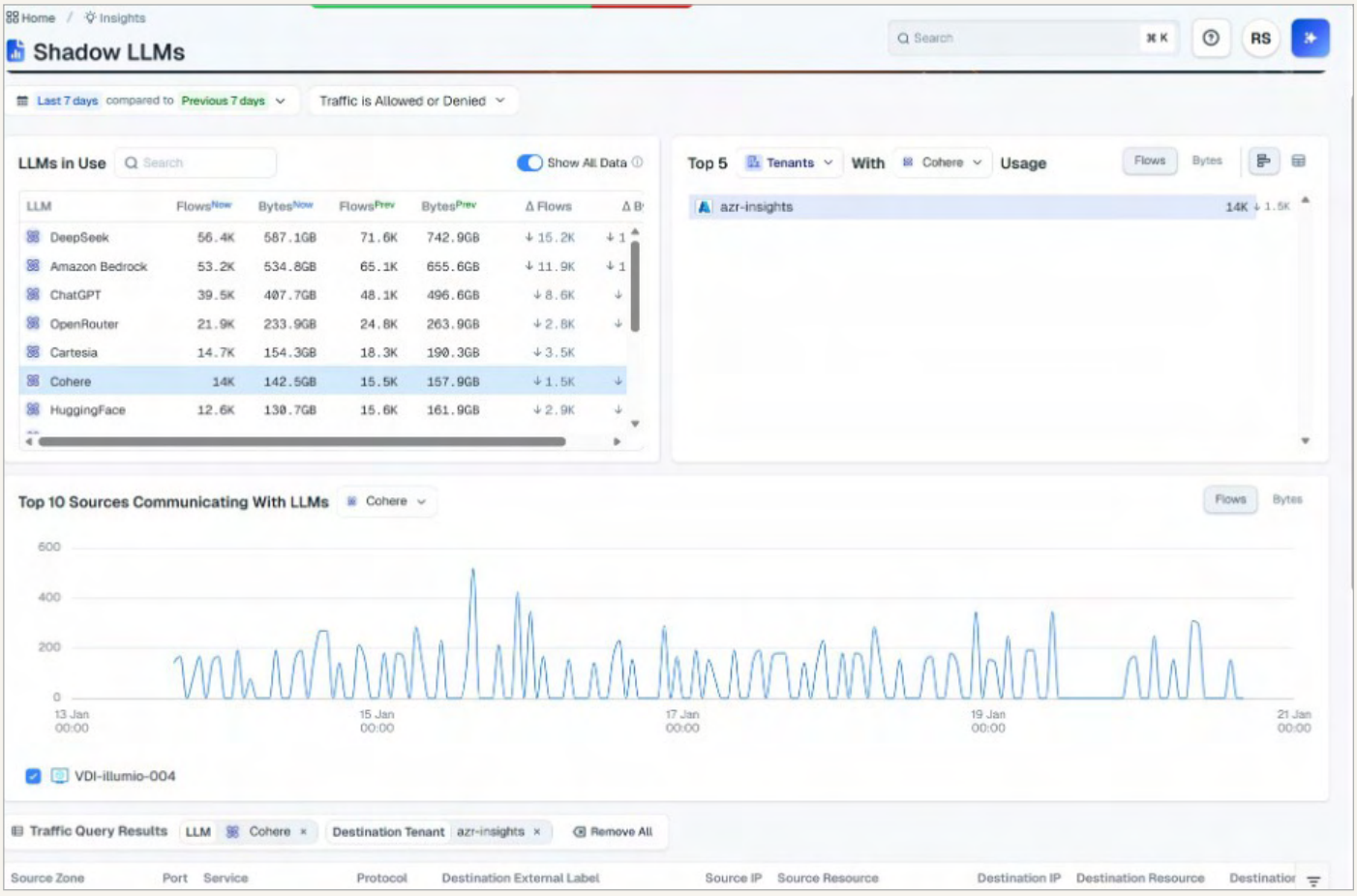

Figure 33: The Shadow LLM dashboard

2. **Scope LLM usage:** Identify connections to any unsanctioned LLM endpoints such as Grok, ChatGPT, Claude, and Gemini.

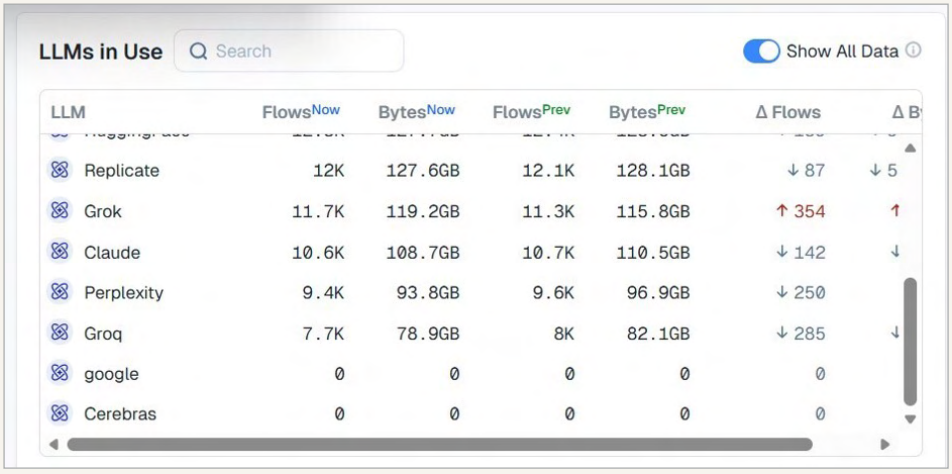

Figure 34: Observe unsanctioned LLMs and usage

3. **Investigate subscriptions:** In the **Top 10 Sources Communicating with LLMs**, select **Grok** for the workflows and bytes volume by date.

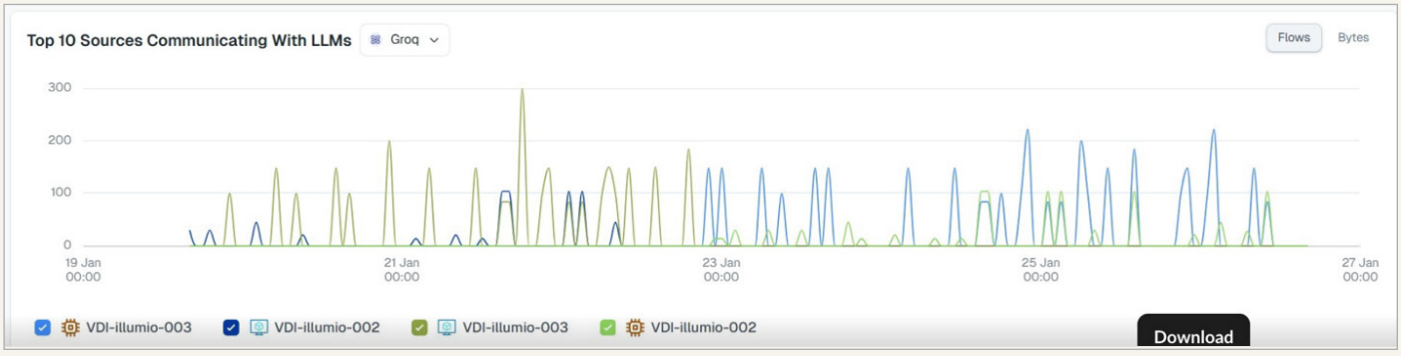

Figure 35: Sources communicating with Grok LLM

4. **Escalate for enforcement:** Confirm unsanctioned LLM use and select to quarantine.

CONCLUSION

Taking the next step

Modern attackers don't wait, and neither should you.

Illumio Insights turns faint signals into clear evidence and complex environments into actionable maps of risk. See every connection, understand every move, and contain every threat — faster than attackers can adapt.

From lateral movement to data exfiltration and unsanctioned AI use, Insights gives your SOC the clarity and control to contain breaches quickly before they escalate, stopping small intrusions from turning into cyber disasters.

Start your free 14-day trial today

illumio.com/insights-free-trial

Try a sandboxed environment using demo data and your own workflows for a real-world experience.