🔀 illumio

Illumio Insights

Cloud detection and response built on an AI security graph

You can't secure what you don't understand

As more organizations rely on the cloud, it's important to take a proactive approach to security. That means being able to see potential attack paths and prioritize high-risk threats.

Without this, security teams can get overwhelmed with alerts, miss the most critical issues, and struggle to stay ahead of breaches.

- Many attacks still go unnoticed. <u>Nearly half</u> of organizations say they can't quickly identify and contain cyberattacks.
- Keeping cloud environments secure is more complex than ever. Cloud systems are always changing, which makes it tough to keep constant, consistent oversight.

Cloud security is urgent. In the past few years, <u>98%</u> of organizations have suffered cloud data breaches. Traditional security methods can't keep up with today's fast-changing, hybrid environments.

Illumio Insights bridges this gap. Built for cloud scale, Insights helps security teams quickly detect and contain risks.

- Get complete, real-time observability. Map your hybrid, multi-cloud attack surface and understand risk in real time.
- Identify and stop lateral movement. Get better context and flow data that show how attackers might move across cloud resources.
- Streamline detection and prioritize response. Designed for hyperscale, Insights manages cloud traffic volumes from a centralized hub, so you get critical information faster.

Key benefits

Complete observability

Gain full context of all resources, flows, and workloads with Al-powered classification and labeling — all within minutes. No hardware or agents required.

Smarter threat detection

Turn raw traffic data into clear, useful insights to accelerate threat detection and analysis. Spot threats faster and make fast, informed response decisions.

Prioritized response

Proactively identify and close high-risk attack paths. Reactively block real-time lateral movement. Reduce your attack surface.

Reliable threat detection and response

Illumio Insights uses AI to help security teams spot threats quickly — often just minutes after setup. It gives defenders a real-time view of suspicious activity and shows how traffic flows across environments, including apps, workloads, user roles, and cloud providers.

By combining AI context and threat data, security teams can rapidly hunt for threats and make informed choices. Reduce risks and eliminate potential threats with confidence.



How it works

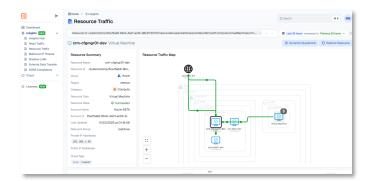
Illumio Insights is the first cloud detection and response (CDR) solution built on an AI security graph. A key part of our breach containment platform, Insights can observe and protect every workload and resource across hybrid and multi-cloud environments.

Insights visualizes dangerous traffic and behavior and prioritizes lateral movement risks across environments, helping teams quickly detect and respond to breaches.

Fast, easy setup at cloud scale. Get insights powered by an AI security graph across millions of workloads in minutes, made possible by a push-button, agentless deployment.

8		8 Home / 4		ub 🌼						Q. Search		xk 🤹 🚺
Dashboard Servers & Endpoints Cloud		Q. Search			¥/	♥ Filter	Last 7 di	ays 👻 from N	ov 2, 2024 - Nov 8, 2024 con	pared to Oct 26, 2024 - N	av 1, 2024	
Ransomware Protect	ti_	Top 10 M	alicious II	2g				Flows Dynes	Known and Unkno	wn IPa	Resource Prote	tion Coverage
🔆 Insights 🔤	~	Intraund				bound			80		10	
🗄 Insights Hub		* 98.142	95.254	80K		102.133.44.54	6 1531 12	2.3K + 10N				
 Risky Traffic Malicious IP Threats 		* 124.221	127.90	60K	1 8% R	179.60.123.45	5 8080	2.1K +2%	40		40	
Known and Unknow	1	* 172.96.1	37.224	54K	- 20% A	195 150 22 8	8 443	196 + 45		1 A A A	-	
Cross Account Traffi	0	* 198.165	159,145	386	+15	62.109.121.50	80	19K ± 22N	20		20	
Traffic to Country		115.236		366		203 25 123 9		1.05 + 05	20			
Cloud Configuration		10.24		346		91200.12.77		1.0K + 05				
Shadow LLMs B Resource Traffic		A 190.764	CIUTUTIZ	348	••••	V1200(12))	80	1.0K + 0h	0 2 Nov 3 Nov 4 Nov 5 N	ov 6 Nov 7 Nov 8 Nov	0 😁 AWS 🔺	Azure O OCI
Explore	-											
O Policies	~	Risky Ser	vices Tra	iffic ©								
Servers & Endpoints	~	Port	Protocol	Service	Flows 🖀	Flows	Dytes 🔏	Dytes -	Top 15 Dst Roles for W	orkloads using 🏽 🗎 Team	Viewer 80 TCP	
Cloud	~	80	TCP	A TeamVie	NEW	13.79K	NEW	52 GB		850K GlobalCata	AQK Backup	29K NES
2 ₈ Access	~	53	TCP	A DNS	NEW	5.65K	NEW	1.45 GB		100K LDAP	47K ISCSI	22K EDR
Infrastructure	~	22	TCP	A SSH	† 20%	1.05K	T 8%	20 MB		70K EMCBackup	45K DNS	18K PAM
Settings	~	23	TCP	A TELNET	NEW	202	NEW	55.09 KB		68K DataIntegrat.	43K Syslog	
Troubleshoot	~	1723	UDP	A PPTP	NEW	343	NEW	33 KB		65K Trendmicro	42K Authenticati	
Support	~		TCP	TCPM.IX	1 8%	800k	4.8%	29.02 KB		50K Database	30K Tenadata	

Unmatched threat detection. With AI observability, uncover hidden threats and attack paths faster. Significantly reduce the mean time to detect (MTTD) breaches.



One-click breach containment. Immediately neutralize potential risks and reduce the mean time to respond (MTTR) to breaches.

× +	88Home / Oinsights				
a	Resource Traffic	Q Search	×× RN		
Boundary Construction Cons	Necorre III: //ution/store/botfaile-Bito-4a01-acite-Bitoff301rt1/vecorredinopa/testime/providen/MonoshLibrego		Last 24 hours: compared to: Previous 24 hours: O Dynamic Quarantine D Restore Resource		
	Resource Summary Resource Farme crm-ctgrrgi01-dev	·			
	Resource 34 //subscriptione//Boel/Sabel-Boo. Cloud A Aparte Regio westes Compared and Compared				
	Category Control Countering this resource will: Resource State Resource Stat				
	Account IS 60at5iab6-8bc0-4a02v-9L Last Updated IN/03/2025 at 01:05:08 Resource Will remain in guarantine until explicitly restored	1 Vitas Martine			
	Private P Addresses Cancel © Quarant 382.108.1.49	tree			
	Public P Addresses + Cloud Tage - Cloud Tage -				

Our AI security graph

Illumio Insights and Illumio Segmentation are integral components of our breach containment platform, the first built on an AI security graph.

Illumio Insights helps organizations quickly identify risk, detect attacks, and contain threats with a single click. It empowers security teams to protect critical assets and respond instantly. Insights and Segmentation work together to identify and mitigate risks, contain attacks, and improve your cyber resilience.

See what you've been missing

Get the observability you need to contain the breach.

illumio.com/illumio-insights

About Illumio



Illumio is the leader in breach and ransomware containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by the Illumio AI Security Graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

Copyright © 2025 Illumio, Inc. All rights reserved. Illumio[®] is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.