WIZ + 🔀 illumio



Executive summary of the integration

Illumio CloudSecure provides Zero Trust Segmentation to public cloud applications and workloads. Together, Wiz Cloud Security Platform with Illumio CloudSecure ensures enhanced visibility into cloud environments and robust threat detection capabilities. The integration facilitates proactively mapping detected misconfigurations and vulnerabilities to the cloud object metadata, application deployments, and traffic flow telemetry data between workloads to apply Zero Trust Segmentation policies. This means organizations can implement granular access controls based on real-time threat intelligence, thereby minimizing the attack surface and automatically containing potential breaches.

🛌 Market challenge

Security leaders must constantly ensure their teams can quickly contain attacks in fast-changing cloud environments where attackers try every trick in the book to gain access and move around. However, organizations need more visibility into the traffic flows and threats because applications and workloads constantly spin up and down.

Better Together

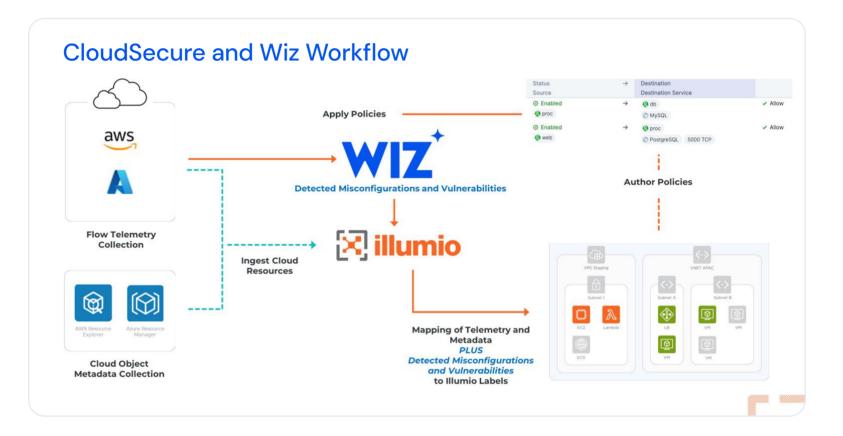
Wiz will scan cloud resources for vulnerabilities and other issues. When it finds a critical security issue, it applies tags to identify the risk on the resource. Illumio CloudSecure will then import that tag and map it to an Illumio label. If a tag is marked as a "vulnerability," it will trigger Illumio to map "vulnerability" to an Illumio label and apply policy based on that label to isolate the device. Illumio CloudSecure maps detected misconfigurations and vulnerabilities from Wiz to the cloud object metadata, application deployments, and traffic flow telemetry data. Illumio can create deny rules whenever a "vulnerability" label applies to a host. These deny rules will kick in and isolate that workload from, for example, being able to connect via HTTP or SSH to anything else. Illumio CloudSecure automatically applies a security policy to mitigate risk and close security gaps before malicious actors can exploit them.

illumio	88 Home > Cloud > Applications	🔀 illumio	88 Home > Cloud > Applications
	Ticketing Feedback ② Jeff St		Ticketing Feedback ② Jef
• Map		• Map	
Traffic	Filter by Production ~	Traffic	Filter by Production ~
Mesh	Summary Inventory Traffic Mep Policy	Mesh	Summary Inventory Traffic Map Policy
Reports	Resource Filter Cloud Resources by	Reports	🔞 Add 🗸 📀 Remove 👒 Disable 🗸 Enable 💿
Workloads	Nasource Price Cloud Resources by-	Workloads	C AGE C C HEMONE C DISABLE C ENSILE
Pairing Profiles	Traffic Last 2 Hours Fiter Traffic by	Pairing Profiles	Verride Deny Rules (2)
Applications	Cloud: Select one Y Just was	Applications	Provision Status No. Status Source Destination
Policies	CIDUC Select OIN * BMS and Citizen	Policies	Destination Service
 Rulesets & Rules 	20052226/248141	Rulesets & Rules	1 © Enabled O Vuin-Found-Open STicketing
Deny Rules	T areast 1 or early 1	Deny Rules	O HTTPS O SSH
 Drafts & Versions 		 Drafts & Versions 	2 © Enabled Ticketing Ticketing
Policy Objects ~		Policy Objects ~	© NetBIOS
O Cloud		O Cloud	Allow Rules (5)
Onboarding	Arrighos Missico m.	Onboarding	
Inventory		Inventory	Provision Status No. Status Source Destination Destination Service
Explore		Explore	1 © Enabled O Ticketing O Ticketing
• Map	Tichtering Status	• Map	C HTTP
Traffic		Traffic	
Applications	Tourng Pro Tourng Pro Tourng Pro	Applications	2 ⊘ Enabled @ web @ web ⊘ HTTPS
Application Discovery ~	Morea Ga. More Ga. More Ga.	Application Discovery ~	
Tag to Label Mapping		Tag to Label Mapping	3 © Enabled @ proc @ db
Policies	Ticketing-Pro Toketing-Pro Toketing-Pro Toketing-Pro Toketing-Pro Toketing-Pro Toketing-Pro Toketing-Pro Toketing-Pro	Policies	© Mysol
Audit Events		Audit Events	4 ⊘ Enabled ♀ web
Settings ~	a	Settings ~	5000 TCP
Usage		Usage	5 O Enabled C Ticketing Ticketing
			© SSH



Benefits of the integration

- Enhanced visibility: Organizations benefit from leveraging visibility and context into security issues across cloud environments to apply proactive segmentation controls.
- **Improved vulnerability management:** The integration improves vulnerability management by detecting misconfigurations and vulnerabilities and adding application deployment and traffic flow telemetry data between workloads.
- Faster breach containment: The ability to implement granular access controls based on real-time threat intelligence minimizes the attack surface and automatically contains potential breaches.



About Illumio

About Illumio Illumio, the Zero Trust Segmentation Company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks.

About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.

