CYCOGNITO

PRODUCT DATASHEET

CyCognito Cloud Connector

Attack Surface Insight, Tailored to the Cloud

Finding and Testing Cloud Assets is Challenging

Whether it's through Amazon's AWS, Microsoft Azure, or Google's GCP, 94% of enterprises are using cloud services to support their business. The speed and simplicity of new cloud environments makes it challenging to maintain visibility, particularly in multi-cloud environments.

Because cloud assets frequently change, yearly or quarterly tests often fail to identify current risks and vulnerabilities affecting these environments. Passive tests don't go deep enough, missing more complex issues that attackers could easily exploit.

Introducing the CyCognito Cloud Connector

The CyCognito Cloud Connector retrieves assets and metadata from Amazon AWS, Microsoft Azure, and Google GCP cloud environments. Once these external-facing IP addresses and domains are ingested, CyCognito automatically incorporates them into the discovery, contextualization, and attribution process.

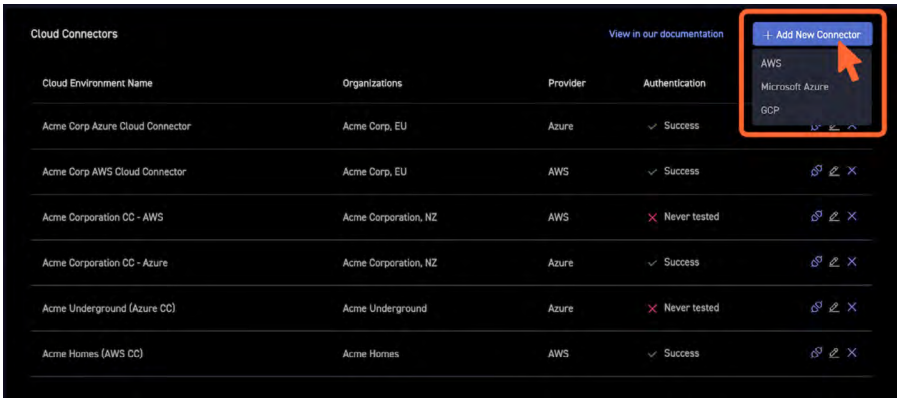

Figure 1: The Cloud Connector menu with the "Add New Connectors" button highlighted as it appears in the CyCognito platform. There is no limit to the number of cloud environments that can be connected to the CyCognito platform for monitoring.

CYCOGNITO CLOUD CONNECTOR FEATURES

- Unlimited cloud connectors
- No installation, no deployment
- Automatic, continuous coverage of all external cloud assets
- Easy to use, no dedicated employee necessary
- Immediate visibility
- Active testing of all external cloud assets
- Available now for Azure, AWS, and GCP

With CyCognito, you'll have continuous visibility and comprehensive risk assessments of all cloud assets, regardless of cloud service provider or ownership within your organization.

Simple Set-up

A set-up wizard walks users through the process of connecting an unlimited number of cloud connectors for Azure, AWS, or GCP. Documentation on the cloud connector creation process can also be found in the CyCognito Knowledge Base, along with step-by-step instructions and guidelines on information to have on hand before beginning the set-up process.

CyCognito's Cloud Connector does not require installation or deployment, just read-only permissions to the metadata of your organization's cloud assets with internet-facing network interfaces.

Instant Visibility

While CyCognito's platform automatically finds and analyzes cloud assets, we wanted to give organizations crystal clear visibility into the external assets in their cloud environments. Once CyCognito identifies new cloud assets, these assets will be automatically added to your dashboard. Assets that were already discovered by CyCognito will be updated with additional cloud metadata.

CyCognito actively tests these cloud assets, identifying potential vulnerabilities and the risks associated with them.

Rigorous Active Testing

Assets discovered by these cloud connectors are fully incorporated into the CyCognito active testing process. Open source, commercial and proprietary active testing engines run a full suite of tailored tests based on asset type and services, carefully monitored to avoid impact. This information, combined with asset context and threat intelligence, is used to build the unique CyCognito severity scores for all cloud assets in your environments.

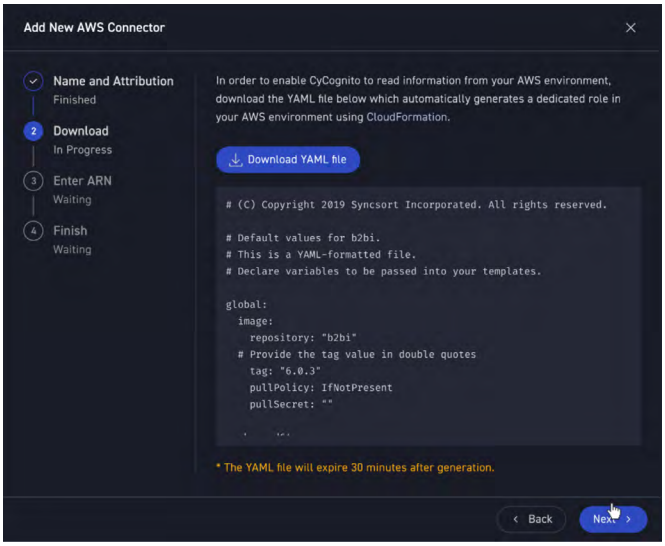

Figure 2: The CyCognito platform features an easy-to-use set-up wizard that connects AWS, Azure, and GCP cloud environments for monitoring.

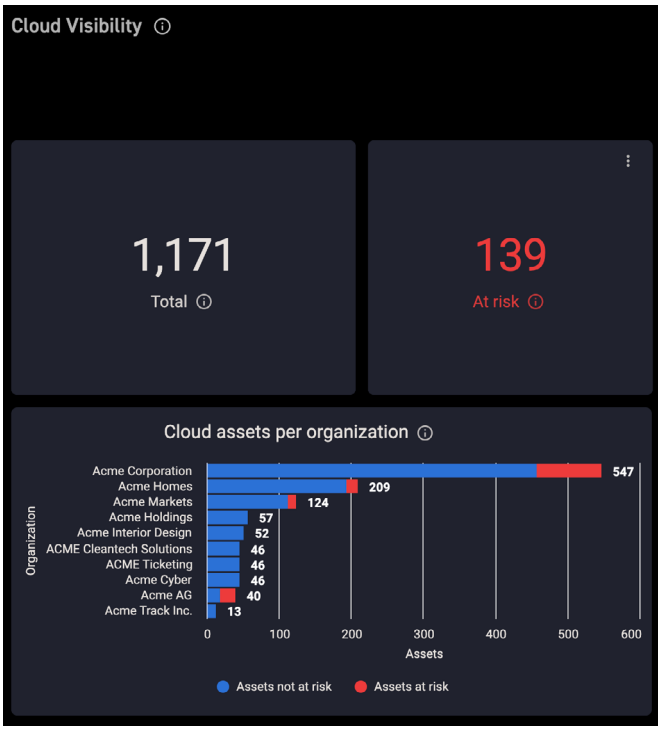

Figure 3: Cloud assets are fully incorporated into the CyCognito platform. Specific risks to cloud assets and environments can be viewed in the Cloud Visibility Dashboard.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO