CYCOGNITO

DATA SHEET

Discovery and Contextualization

Organizational Reconnaissance | Asset Discovery | Asset Business Context
Asset Attribution | External Risk

Most enterprises have a significant number of unknown digital assets exposed to the internet. Unmanaged and untracked, these assets represent the most common threat vector[1] and form the majority of external risk. Automated asset discovery and contextualization are critical to maintain pace with change[2].

Founded in 2017, CyCognito built the discovery engine in its external attack surface management (EASM) platform to replicate an attacker's thought processes, navigating open source intelligence (OSINT) with an automated reconnaissance workflow based on human logic. The result is an unprecedented view into an organization's business structure and the assets tied to it.

CyCognito Discovery and Contextualization

CyCognito automated discovery and contextualization focuses on five capabilities.

Uncover organizations related to the business

Find internet-exposed assets that are related to these organizations

Attribute the assets to the organizations

Gather intelligence on the internet-exposed assets

Classify and categorize the internet-exposed assets

One of the many values of CyCognito's automated and continuous approach to these five capabilities is that the rule based system operates the same way every time. This leads to consistency, provability and the ability to track and propagate changes at massive scale.

1 Verizon Data Breach Investigation Report (VDBIR), 2022

2 On average 9% per month. Source: CyCognito internal research, 2023

CyCognito's Unique Discovery Approach

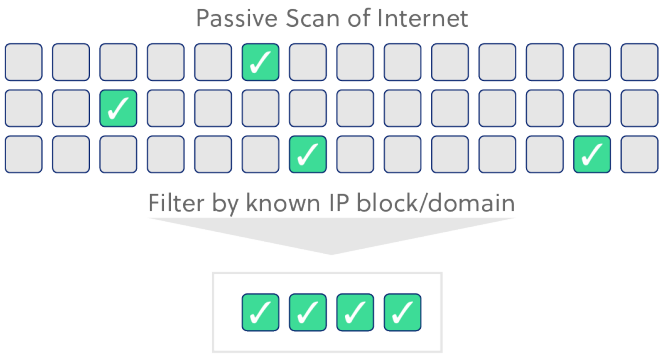
Most ASMs and EASMs scan the internet with passive scanning tools, relying on manually seeded IP blocks to filter for assets and domains. Some EASM solutions go one step further, using DNS enumeration technologies to semi-automate IP address discovery.

CyCognito inverts the asset discovery paradigm. Leveraging dozens of databases, search engines, and websites, CyCognito builds a graph data model that represents your organization's attack surface. Assets and organizations are referenced as nodes and relationships, not a flat database. The graph data model includes machines, applications, cloud instances, and files that attackers can find in their reconnaissance efforts.

CyCognito uses machine learning (ML) and natural language processing (NLP) technologies to scrape web pages, read pdfs, and more. This enables a scalable, highly accurate and low maintenance approach to discovery. Evidence and probability (%) are included with each asset.

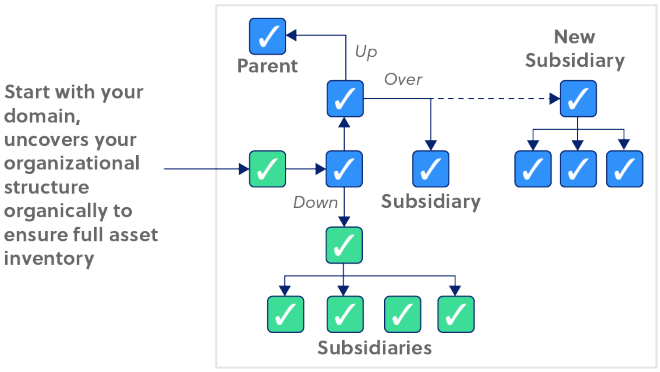
CyCognito is the only platform that auto-identifies organizational business structure. Since most security teams are unaware of the scope of legal entities and brands, this is a critical capability to uncover the company's global attack surface.

The Most Common EASM Approach



A flat, unranked list of some assets

CyCognito Approach



Full context, business structure and asset inventory

CyCognito Contextualization

Gathering asset context requires substantial human effort[3]. CyCognito's automated and continuous contextualization provides what your team needs, when they need it, and makes it available via API and UI.

Organizational Reconnaissance and Attribution

Many organizations have less than 30%[4] of their known attack surface assets attributed to an owner in their configuration management database (CMDB). This makes it difficult to find the team responsible for fixing an issue and also identifying the internal asset for further investigation.

CyCognito knows the user of an external asset discovery tool doesn't necessarily have the inputs to uncover the breadth of an organization's infrastructure. The CyCognito platform automatically uncovers these inputs and applies the organizational attribution context to each asset. The result – IT security teams spend more time remediating and considerably less time researching.

Asset Business Context

Business context is critical for prioritizing external risk. Without it, security teams are left with thousands of "potential critical issues" since they do not know how the business uses the asset and its criticality to the business. This does not scale and increases mean time to resolution (MTTR).

CyCognito platform uncovers the context required to make appropriate prioritization decisions, including ecommerce services, personally identifiable information (PII) collection, internal business applications, DevOps instances, sensitive data, and more.

3 On average 4 - 10 hours per asset, as per CyCognito internal research and dialog with large enterprises.

4 Source: CyCognito internal research and dialog with enterprise organizations

CyCognito added context include:

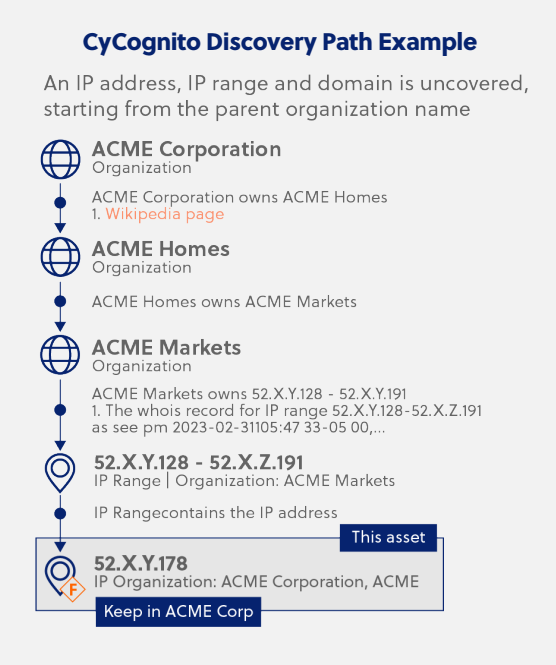
- **Asset type:** Domains, servers, web applications, services, certificates, etc.
- **Technology:** Asset state, DNS resolve evidence, asset relationship, etc.
- **Unique metadata:** Attractiveness to attackers, discoverability, PII collection, sensitive data, related applications, etc.

Without business context, IT security teams are left making assumptions for issue prioritization, or using generic severity scores which are typically not relevant to business priorities.

Discovery Path and Evidence Collection
Asset relationships are complex. CyCognito's unique graph data model enables IT security teams to rapidly consume asset context and associated connections.

The CyCognito discovery path includes comprehensive details. Evidence is included for every step; links, URL patterns, headers, banners, certificates, code fragments, deployed software, TLS configuration, related domains, encryption ciphers, even screenshots of applications. Data is available via RESTful API, UI and pre-built integrations.

CyCognito automated discovery leverages an extensive list of OSINT sources, for example SEC filings, Crunchbase, Wikipedia, investor relations materials, Google, and more. The OSINT source is always included as evidence.

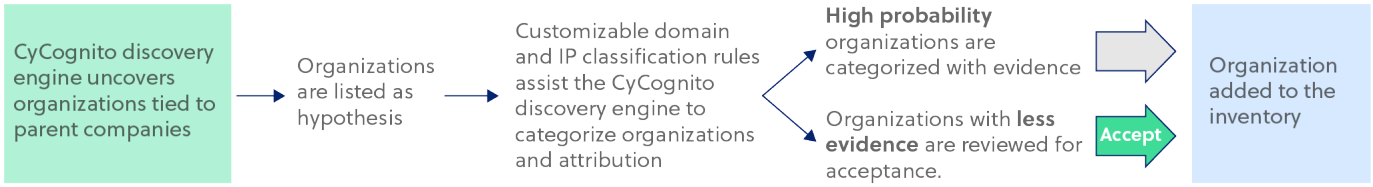


CyCognito Discovery: How it Works and Where it Looks

CyCognito discovery and contextualization is more than a technical exercise involving DNS enumeration and a domain name. Discovery performed properly is a **decision tree**, using logic, probability, OSINT, and careful investigation.

CyCognito automates the asset discovery workflow with an interconnected global network of over 60,000 endpoints. CyCognito *hypotheses* act as logical statements to describe discoverable relationships between asset inventory objects. They represent the human thought process, which is complicated and error prone to complete manually at scale.

As evidence of relationships between entities is uncovered and populates the graph data model, high probability hypotheses are accepted automatically and lower probability reviewed by CyCognito analysts. An example of hypothesis workflow for attribution is shown below.



CyCognito hypotheses probabilities are visible in the CyCognito UI. CyCognito identifies digital assets that include web applications, IP addresses, certificates and domains. Web applications are identified both by HTTP/HTTPS and API. Once an asset is added to the asset inventory it is fingerprinted for unique identification by the system.

Where CyCognito looks for Assets
The external facing digital edge of an organization varies widely; some parts heavily regulated and others unmanaged and uncontrolled. Subsidiaries, interconnected companies, joint ventures, partners, cloud environments, etc. all may store digital assets owned by the organization. All are uncovered with the CyCognito platform.

Cloud resources are particularly dynamic. CyCognito's cloud connector authenticates to customers' cloud environments to identify, classify, and test external cloud assets. The cloud connector fetches public facing assets across major service models: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS).

Comparison of CyCognito Discovery to Commodity Solutions

Legacy ASM, commodity EASM and open-source tools typically do not have the scalability, accuracy, completeness and timeliness of enterprise-grade modern EASM.

	Commodity ASM / Open Source Approach	CyCognito
Scope	Manual inputs with known data (IP address ranges, etc.) seeds discovery. Limited to searching in what is programmed, not uncovered.	Progressive organizational reconnaissance automatically reveals scope and structure for asset discovery. Subsidiaries, business units, partners, cloud services, and more.
Scale	Challenged to scale to enterprise-sized attack surfaces due to manual workflows and configuration, resulting in large gaps and delay.	Fully automated, proven with millions of assets at Fortune 10 organizations.
Accuracy	High noise/gaps due to heavy use of passive reconnaissance techniques and lack of organizational visibility	Multiple discovery engines validate discovered assets, relationships and organizations result in high accuracy. Assets are fingerprinted uniquely.
Complexity	Manual, analyst entered data (IP's, domains) requires continuous maintenance.	Frictionless - no input, installation, configuration, or whitelisting needed.
Organization structure mapping	Lacks organizational and business context; device-only approach focuses on known IP ranges and customer-registered domains.	Automated organizational reconnaissance uncover business scope organically, using open source intelligence and progressive tooling.
Evidence collection	Lacks automated attribution and risk detection evidence collection, leading to substantial manual validation and data augmentation effort.	Automated evidence collection saves significant time/money on validation, reduces MTTR, and builds trust with cross-functional teams.
Frequency	Multiple cadence options. New data is often limited to the available analyst time for review and update.	Continuous

About CyCognito

CyCognito is a cloud-native software-as-a-service that was built to meet the external risk requirements of the largest and most complex organizations. Discovery & Contextualization, Security Testing and Prioritization & Remediation are the foundational elements of the CyCognito platform.

Scalable, continuous, and comprehensive asset discovery – only from CyCognito.

To discuss CyCognito's security testing capabilities or a demonstration of CyCognito, please reach out to to your CyCognito account representative, or email us at **info@cycognito.com**.

CYCOGNITO