CYCOGNITO

SOLUTION BRIEF

Not every security gap is a fire drill. Risks to your business are.

Maximize impact by focusing on fewer risks through precise risk prioritization

Analysts and vendors alike say "you cannot protect assets you don't know about." 67% of organizations surveyed said their externally exposed, unknown assets have been used in a breach.[1] This has led to a crowded market of vendors saying they solve External Attack Surface Management (EASM) yet their attention is only on "discovery" while discovery is a critical step in EASM and uncovering the unknown.

While discovery is a critical step in EASM, you will be set up for failure if you're not detecting and prioritizing the most important risks on those assets. The CyCognito platform is the first EASM solution to perform active security testing of all your external assets to help security and operations teams detect and prioritize their most important risks. Security testing all assets may sound like it will lead to an overwhelming volume of findings. The CyCognito platform addresses that by using tailored tests that increase precision, combined with prioritization based on what poses a business risk. The result is fewer, most urgent risks, enabling you to set realistic and measurable remediation goals for your team.

Continuous, Automated Discovery

Keep up with daily changes to modern IT infrastructure. Automated asset and security issue discovery fueled by machine learning and advanced natural language processing.

Asset Insights and Entity Owner

Deep knowledge about assets with high fidelity insights and automated asset attribution using machine learning to attribute about 95% of assets to their organizational owner including across subsidiaries, partners, and more, viewable in a visual organizational map.

Tested and Validated Accuracy

Industry-leading active testing with global scalability for millions of assets. This provides incredible precision, very low false-positives and verifiable findings you can trust.

Prioritize Real Risks to the Business

Context of your business matters. Prioritize based on importance of the asset to you, exploitability by attackers, and severity of the risk.

Zero-touch Deployment

Just like an attacker, no data input or "seeding", no deployment, no configuration, and no whitelisting or inclusion-listing.

Step-by-Step Remediation Guidance

Actionable remediation steps with deep insight, evidence of assets discovered and risks detected.

Improve MTTR as much as 88%[4]

Automatically distribute remediation guidance through configurable workflows and seamless integrations with ticketing systems, SIEMs, and vulnerability management platforms including ServiceNow, Jira, ZenDesk, Tenable and Splunk.

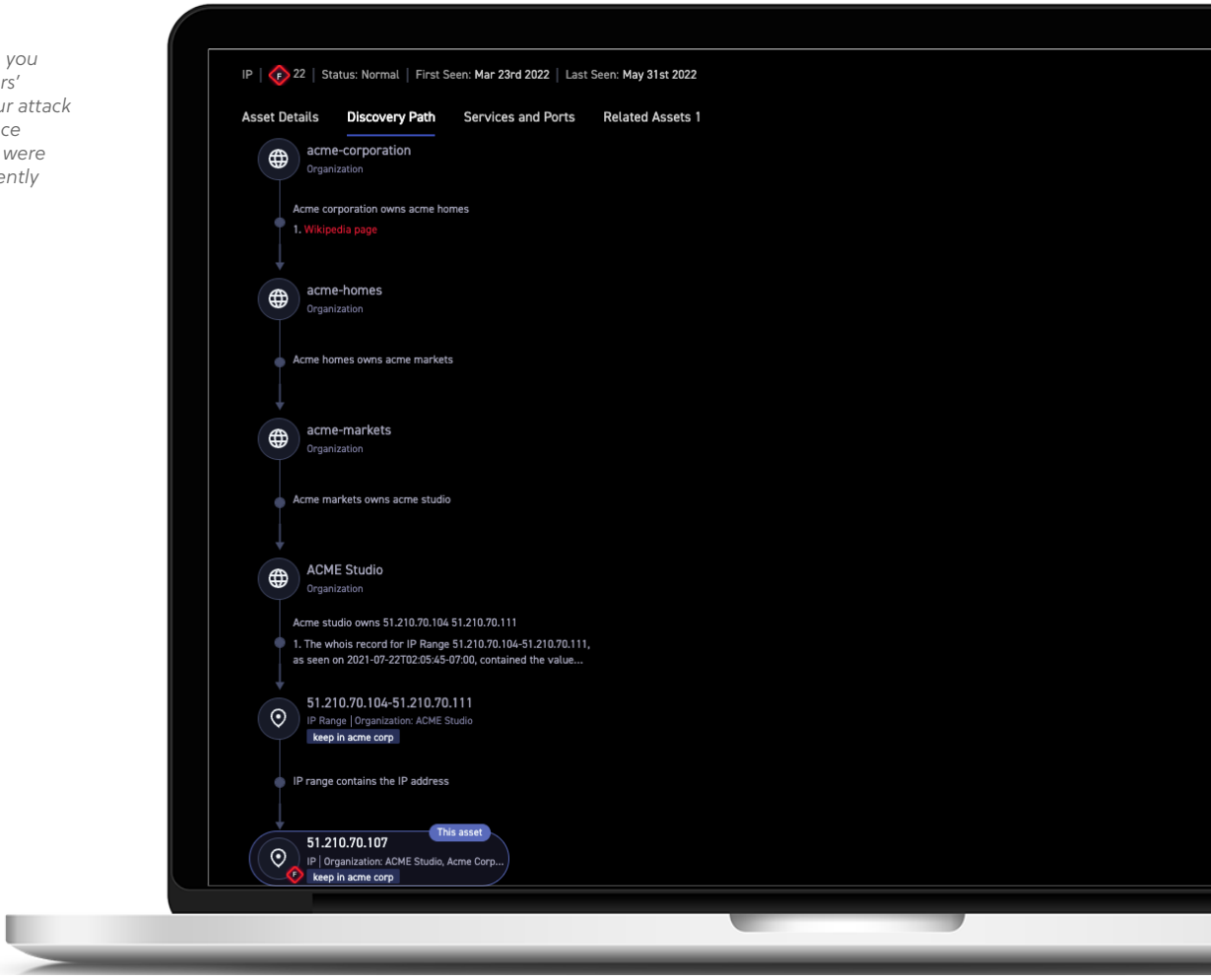
Sprawl of Internet-Facing Assets Makes Testing At Scale a Challenge

"Active security testing" parallels the behavior of an attacker to uncover overlooked security gaps. Done at-scale across all external-facing assets can find security risks on assets that can put your business in jeopardy. Testing at scale is a challenge for modern IT infrastructure that has become siloed and overly sprawled. IT innfrastructure has busted beyond the confines of perimeter firewalls and now resides in public and private clouds, is owned by subsidiaries or partners, connects to third-parties and is deployed by business functions as shadow IT. Too often organizations settle with testing only 10% to 30% of their infrastructure resulting blind spots that become opportunities for attackers.

Stay Ahead of Your Rapidly Changing Attack Surface

Untested externally-accessible assets can leave exposed a whole host of security issues spanning CVEs and zero-day vulnerabilities, authentication issues and exposed sensitive data. As part of the CyCognito 2022 EASM executive report, organizations and their subsidiaries observed had an average of 5,000 web apps each. These applications are highly susceptible to SQL injection, cross-site scripting, PII exposure, broken authentication and other security issues.[2] External attack surfaces are highly dynamic and it's reported that developers knowingly push vulnerable code at alarming rates.[3] Security and IT operations teams need help to stay ahead of rapid changes especially where they put the business at risk. The CyCognito platform's continuous scanning and active security testing at global scale helps security teams keep pace with security risks to the business and other connected entities including subsidiaries and partners.

The CyCognito platform helps you identify and eliminate attackers' paths of least resistance in your attack surface. It provides the evidence you need, including how risks were discovered, so you can confidently remediate or mitigate issues.



Real Risk, Real Prioritization

The severity of a security issue, be it a highly critical vulnerability or a misconfigured API, should not be a prioritization factor alone. This can result in an abundance of workload with unimportant focus. Understanding context about the asset is crucial, from knowing how valuable it might be to your organization, how valuable it would be to attackers, and how easily attackers could find it and associate it with your organization. The CyCognito platform identifies detailed information about risks by the asset type, such as a router or web server; and how sensitive it is such as if it includes PII, business data or sensitive systems. Context is what helps understand the priority of each security issue found.

Widest and Deepest Attack Surface Discovery

Unknown and unmanaged assets are discovered, identifying risks to the main networks that can originate from seemingly unrelated assets owned by subsidiaries, partners, third parties and even rogue assets directly connected to your organization, sometimes as far as 15 hops away.

Mean Time to Detection & Response

To respond to a security risk, your team needs to validate findings and figure out who owns the asset. Modern IT infrastructure experiences changes every day by various teams including outside entities with connections to your network. Assessing risks, whether with pen testing once per year, or application scanning once per quarter translates to several months or up to a year delay in detection. Unraveling ownership is manual and time consuming. The CyCognito platform's continuous discovery, with as frequent as a daily cadence, helps to stay ahead of a rapidly changing and sprawling network.

The CyCognito platform provides a fully-verifiable, easy-to-navigate, mapped path of discovery for the asset and risk, making the attribution of organizational or departmental ownership simpler. CyCognito findings are trusted by customers. Security teams use these findings as evidence to validate what they share with IT operations teams or outside teams. CyCognito provides step-by-step remediation guidance on how to fix issues and keep operations running. Continuous discovery confirms the successful completion of remediation efforts for IT operations teams. Leaders use the reporting and dashboards to report progress on remediation efforts to senior executives.

What security leaders say about the benefits of the CyCognito Platform

Solve real risks, faster

Automated workflows with integrated technologies, detailed risk alerts and actionable guidance to resolve each issue, speeds the time to resolve business risk.

"It's so valuable to me because it gives me not another problem to solve; it gives me an action plan and you can't put a price on that."

—CISO, Light and Wonder

Security testing at scale

CyCognito eliminates false positives and uncovers misconfigurations, exposed data, and zero-day vulnerabilities using automated security testing that scales globally across all discovered live assets on a continuous basis, up to daily.

"Using CyCognito to be able to test everything to a level on a regular basis makes our penetration testing more effective as far as high value assets."

—CISO at an Asset Management Company

Prioritize risks that matter

Risk prioritization using business context streamlines the process by identifying the most critical issues from thousands. This is based on factors such as vulnerability severity, asset importance, attraction to attackers, and ease of discovery by attackers.

"The CyCognito platform helps me figure out how to distill an overwhelming amount of information and determine what is a risk for our business."

—Chief Privacy and Security Officer, Human API

1 Olksik, J. 2020. "ESG Research Insights Paper: Gaps in Attack Surface Monitoring and Security Testing for Cyber-risk Mitigation". Enterprise Strategy Group, Inc.
2 CyCognito (2022). "Executive Brief: Anybody Got a Map? The Danger of Subsidiary Sprawl and Unknown Unknowns in External Attack Surface Management". CyCognito
3 Barth, B. (2021, May 14). "Developers knowingly push flawed code, doubt build environments are secure". SC Media
4 Fortune 100 customers of CyCognito across industries including hospitality, manufacturing and asset management report 50% to 88% faster remediation times

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