CYCOGNITO

DATA SHEET

The CyCognito Platform

Go well beyond discovery with external attack surface management that lets you rule your risk.

Reduce Business Risk and Protect Your Attack Surface

The CyCognito platform focuses on what attackers think, see, and do to help you dramatically reduce your overall business risk. With no deployment required, it autonomously discovers and maps your organization's entire external attack surface and identifies the business context of assets. It then tests your attack surface, looking for the path of least resistance—critical points of exposure that attackers can most easily exploit.

The CyCognito platform prioritizes your risks based on attacker interest, discoverability, and exploitability. All of this information is delivered to your operations teams—via our UI and using a broad range of integrations and automated workflows—so they know where to focus immediately. This accelerates remediation by giving your teams the actionable intelligence, evidence, and prescriptive remediation guidance they need.

CORE CAPABILITIES

The CyCognito platform helps you identify, prioritize and eliminate the most critical cyber risks to your organization with:

Attack Surface Discovery & Mapping: CyCognito automatically discovers your organization's structure and internet-exposed assets, eliminating blindspots caused by unknown or forgotten infrastructure and giving security and IT operations teams a single, complete inventory of your digital assets.

Automated Security Testing: With continuous, active security testing of all exposed assets, you can confidently understand the real vulnerabilities in your attack surface. Some issues discovered with active testing include weak and misconfigured encryption protocols and ciphers, login issues, man-in-the-middle attacks, and exposed data.

Integrated Threat and Exploit intelligence: Not every vulnerability is created equal, so CyCognito combines threat intelligence with attack surface vulnerability data to highlight weaknesses in your attack surface that attackers are actively looking to exploit.

Intelligent Remediation Guidance: Operations teams can spend their time fixing issues instead of figuring out how to fix issues with our prescriptive and intelligent remediation planner, remediation guidance, and supporting evidence.

CyCognito Platform Differentiators

The platform automates attacker-style reconnaissance and offensive security techniques to close the gaps left by other security solutions, including legacy attack surface management products, vulnerability scanners, penetration testing, and security ratings services. Unique capabilities of the CyCognito platform include:

01

Global Asset Discovery

Attacker-like reconnaissance discovers unknown, unmanaged, and cloud-based assets as well as those you manage, third-party components, and abandoned environments. The platform's discovery capability offers 3 times the visibility of port scanners.

02

Automated Business Context

A graph data model and intelligent, iterative analysis of your organization and its subsidiaries and business units classifies and o-rganizes assets by their business context and relationship to your organization.

03

Active Testing

Detects data exposures, authentication and encryption weaknesses, misconfigured applications, network architecture flaws, phishing threats and other risks as well as common vulnerabilities and exposures (CVEs).

04

Intelligent Risk Prioritization

Dramatically increases your operational efficiency with an innovative risk scoring system based on an attacker's priorities, as well as threat intelligence about attacks in the wild.

05

Intuitive Reporting

Pre-built dashboards enable quick analysis of attack surface risk, as well as continuously updated progress toward risk reduction goals.

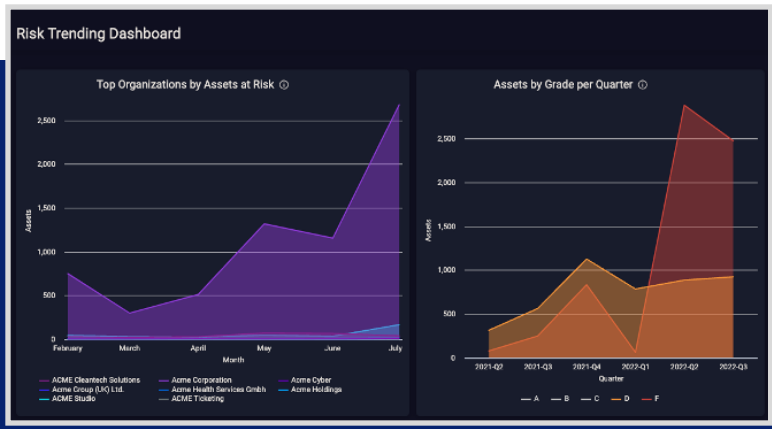

Figure 1. Analyze and report on security posture, including trends, to demonstrate you are managing cyber risk. You can see overall trends as well as trends for asset groups.

Key Use Cases for the CyCognito Platform

Like industry-leading organizations around the globe, you can use the CyCognito platform to:

Automate Attack Surface Management: Identify and manage your attacker-exposed assets with an understanding of their business context and security risks.

Scale External Risk Assessment & Penetration Testing: Augment periodic, narrowly focused testing coverage with continuous, multi-factor testing of your entire external attack surface.

Eliminate Ransomware Attack Vectors: Pinpoint and prioritize critical remote access exposures that attackers can use to plant malware or use for initial access.

M&A Risk Reduction: Evaluate the security risks of your merger or acquisition targets and quickly bring the security posture of acquired entities into alignment with the rest of the organization.

Monitor Subsidiary Risk: Identify and prioritize subsidiary and business unit-level security risks so relevant teams can eliminate them.

Security Self-Assessment: Continuously assess, monitor, and eliminate cybersecurity risk to measure and improve your security posture.

How the CyCognito Platform Works

The CyCognito platform performs reconnaissance automatically, using an attacker mindset to build a comprehensive view of your external attack surface. It then guides you and your operations teams on what needs to be fixed immediately to reduce the most risk and eliminate attackers' paths of least resistance into your organization. The platform works without deployment or configuration and does not disrupt business continuity.

Graph Business & Asset Relationships

- Maps your business structure, subsidiaries, acquired companies, cloud environments, and more using machine learning and natural language processing to reveal the full organizational makeup of your attack surface.
- Continuously discovers and fingerprints all of your digital assets with our global discovery network and associates those assets with your organization, even those that might not be clearly or traditionally related.
- Validates discovery data with a complete discovery path to assets, providing proof and reasoning behind why assets were associated with your organization.
- Inventories all of your external digital assets with identifying elements, including IP ranges, web applications, links, URL patterns, headers, banners, certificates, code fragments, deployed software, TLS configuration, related domains, encryption ciphers, and many more.

Automatically Determines Business Context

- Analyzes and classifies your assets based on your organization's structure, whether on-premises or in cloud (IaaS, PaaS, SaaS), technology partner, or subsidiary environments.
- Automatically associates which assets and what data belong to which departments or subsidiaries within your organization, the business processes associated with those assets, and what risks and attack paths the assets expose.

Continuously Tests Security at Scale

- Goes beyond port scanning and simple identification of common vulnerabilities and exposures (CVEs) by automatically and actively testing assets to enumerate, validate, and score attack vectors based on context.
- Identifies all attack vectors that an attacker could use to breach your most critical assets, including non-CVE related weaknesses, like data exposures, misconfigurations, code injection risks, and even zero-day vulnerabilities.
- Tests your entire attack surface, not just the assets and IP ranges that your teams have programmed into a scanner, with automated risk-detection techniques, vulnerability assessment, encryption analysis, and more.

Prioritizes Risks

- Cuts through the noise to reveal the most critical risks that security and IT teams need to fix first.
- Grades risks based on attackers' priorities, business context, discoverability, ease of exploitation, and remediation complexity—including whether there have been attacks in the wild.
- Determines security grades for the entire organization, as well as on asset, business-unit, issue, and region type to help understand where there are weaknesses and to track improvement over time.

Accelerates Remediation

- Saves time for security and IT teams and reduces your window of exposure by automatically providing detailed remediation guidance for each identified risk.
- Provides automated guidance on what to do in order to achieve a desired remediation outcome (such as "raise my overall score from D to B," or "eliminate all Apache vulnerabilities in my customer-facing systems") with Remediation Planner.
- Integrates CyCognito's remediation guidance, planning, and attack surface insights into your existing security stack, including SIEM/SOAR, ticketing, communication and collaboration, GRC, and asset management tools.
- Analyzes and reports on changes and trends in your attack surface, including remediation progress and new issues.

Reduce Risks Across Your IT Ecosystem

CyCognito empowers companies to take full control over their attack surface by uncovering and eliminating the critical security risks they didn't even know existed.

NETWORK SECURITY RISKS: Uncover assets you do not manage or are not aware of, including remotely accessible servers with misconfigured and insecure authentication mechanisms and services

CONFIDENTIALITY RISKS: Reveal weak and misconfigured encryption protocols and ciphers, login issues, man-in-the-middle attacks, and exposed data

APPLICATION SECURITY RISKS: Actively test for insecure code and vulnerable software components that enable attackers to take full control of assets, default credentials, and misconfigurations

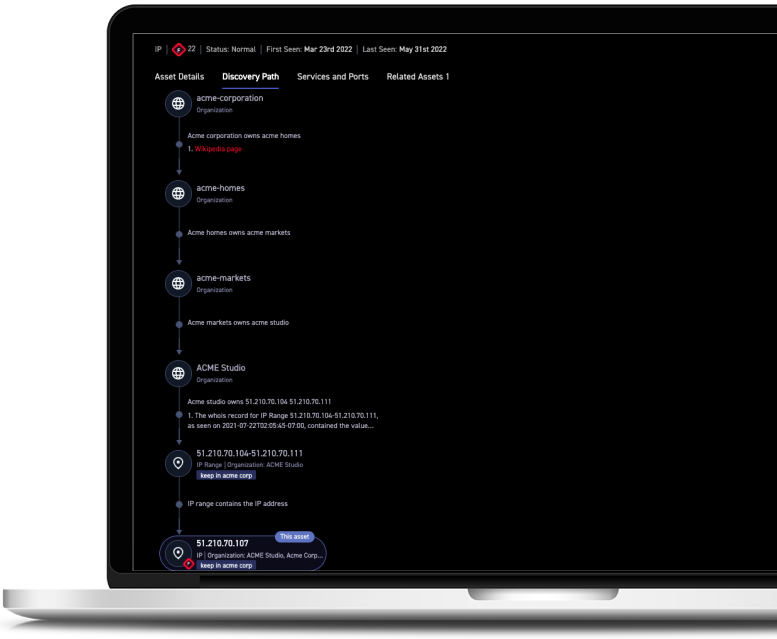

Figure 2. The CyCognito platform helps you identify and eliminate attackers' paths of least resistance in your attack surface. It provides the evidence you need, including how risks were discovered, so you can confidently remediate or mitigate issues.

> **CyCognito came up with more unique and significant findings than any other [vendor]."**
>
> **SC MAGAZINE | April 22, 2021**

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