CYCOGNITO

DATA SHEET

Vulnerability Management with the CyCognito Platform

The CyCognito Platform delivers proactive vulnerability management (VM) so you can eliminate the critical risks sophisticated attackers target first. Unlike other external attack surface management (EASM) and VM solutions, it combines full discovery of your extended IT ecosystem and autonomous, active security testing of your externally-exposed attack surface. Using advanced attacker reconnaissance techniques, the platform discovers assets that are part of your IT external ecosystem, but are unknown or unmanaged by you, and it identifies attackers' paths of least resistance into your environment so you can efficiently eliminate them.

The CyCognito Approach to Proactive Vulnerability Management

Discovery as a Foundation of Proactive Vulnerability Management

In a digitally transformed world, vulnerability management must include all of your attacker-exposed assets — whether on-premises, in the cloud, in your subsidiaries or in partner environments. That's a critical, foundational step and one that traditional VM solutions don't address.

The CyCognito Platform gives you an accurate view of your most critical vulnerabilities because it first discovers your entire external attack surface by taking the attackers' perspective in identifying organizations assets. And just like an attacker searching for exploits we start discovering assets autonomously which does not require any information from organizations to create an asset inventory. Its discovery capabilities go far beyond the known or easily discovered IP ranges of typical EASM tools.

Proactive Vulnerability Management

KEY CAPABILITIES

Focused On What Attackers Target: A 100% focus on what's externally exposed to attackers — intentionally or not — including cloud and affiliate organization environments, using reconnaissance and testing techniques that go far beyond traditional attack surface discovery and VM tools.

Automated Asset Discovery: Automated and comprehensive asset discovery, and attribution of assets to departments and organizations across your extended IT ecosystem, including unknown and unmanaged assets.

Frictionless: 100% SaaS solution with no installation/deployment, no configuration, no authorization, no ongoing management of vulnerability assessment (VA) or VM infrastructure components — all critical for managing risks in subsidiaries, partners, and potential mergers and acquisitions (M&A) targets.

Undetectable: Anonymous, undetected discovery and testing eliminates both configuration of allowlists and alerts from other security solutions in the testing path.

Proactive VM: Unlike other ASM solutions and their passive banner-based risk assessments, and traditional VA solutions that only consider active IPs and vulnerable software, the platform combines automated penetration testing techniques with proactive VM and identifies issues with active and inactive IPs, domains, certificates and configurations.

Prioritized: Provides actionable guidance on what to remediate first, using a risk prioritization engine that factors in business impact and exploitability.

The CyCognito Platform's automatic asset classification and ownership attribution uses intelligent, iterative analysis to take the hassle out of determining who owns assets and what data resides on them. It automatically classifies organizations' attack surface assets by their business context and relationship to organizations. Business context helps organizations understand which assets and what data belong to the right owners in departments or subsidiaries within the organization, the business process associated with those assets, and what risks and attack paths the assets expose. We use entity extraction with natural language processing (NLP) and machine learning (ML) to detect concepts like PII and give customers evidence on how these assets were discovered and an attribution certainty, a metric that indicates how confident the CyCognito Platform is that an asset is rightfully attributed to an organization.

The CyCognito Platform identifies your entire external attack surface and automatically organizes it with capabilities that go far beyond other ASM tools as shown in the chart above. This creates a strong foundation for your external VM requirements.

Comparison Chart

Capabilities for External Attack Surface Management Tools (EASM)	CyCognito	Other EASM Vendors
Scan the internet continuously to discover assets	Yes	No
Fingerprint assets, identifying services, software, text, graphics, attributes, etc.	Yes	No
Automatically associate assets with your organization and subsidiaries	Yes	No
Determine the business context of assets	Yes	No
Identify attack vectors impacting your assets	Yes	No
Prioritize risk based on context and impact	Yes	No
Prescribe methods to remediate risks	Yes	No
Provide easy-to-understand scoring of security posture and change over time	Yes	No

"Always On" Proactive Defense

The CyCognito Platform continuously scans and automatically tests your entire attacker-exposed IT ecosystem to identify your critical risks. This vigilant, proactive and cost-effective defense has clear advantages over the traditional approach of point-in-time vulnerability scanning or penetration testing sparingly applied to a limited segment of your attack surface. As a result of its broad discovery and automated testing, the CyCognito Platform enables dramatically expanded VM coverage of your external attack surface without burdening an already over-extended cybersecurity teams with additional tools to manage, alerts to address or false alarms to muffle.

Detects Attack Vectors, Not Just CVEs

The CyCognito Platform goes beyond the identification of Common Vulnerabilities and Exposures (CVEs) that are the exclusive focus of traditional VM solutions. In addition to CVEs, it uncovers data exposures, misconfigurations and even software zero-day vulnerabilities so that you have a complete view of your attacker-exposed risk. These additional risk areas must be secured to outmaneuver attackers' offensive operations. The platform identifies these attack vectors that legacy solutions miss:

- Inactive IPs
- Insecure/exploitable code
- Abandoned assets
- Subdomain takeovers
- Bypassable authentication mechanisms
- Network architecture flaws
- Default credential vulnerabilities
- SQLi and XSS vulnerabilities
- Exposure of sensitive folders and files
- Certificate trust vulnerabilities
- SaaS platforms takeover risks
- DNS and mail servers hijacking risks
- Web application and database hijacking risks
- and many other attack vectors

Example of a Non-CVE Attack Vector

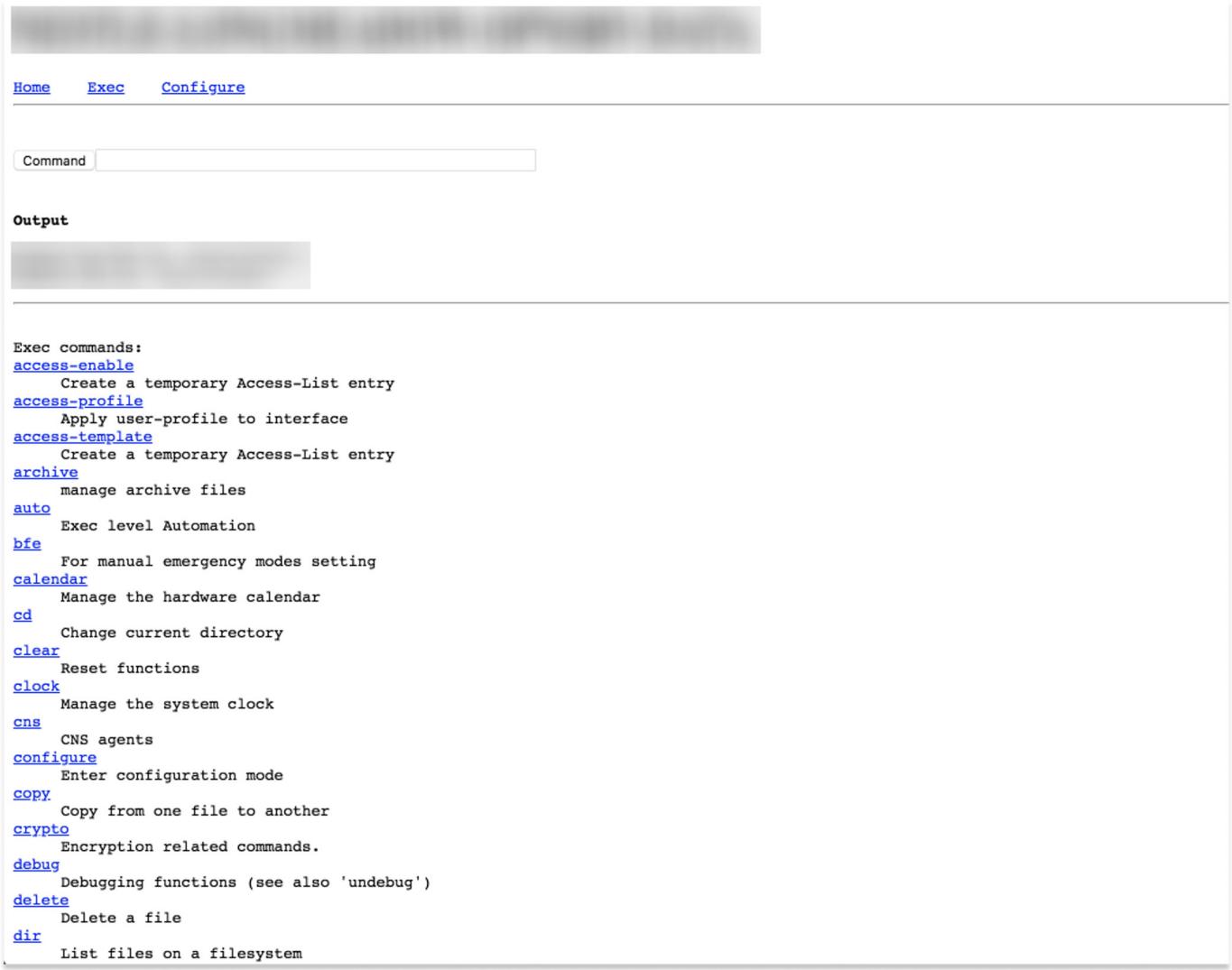

Figure 1: As an example of an attack vector, the platform discovered an exposed, abandoned router whose user interface, shown here, could allow attackers to execute commands remotely.

Automatic Risk Prioritization

The CyCognito Platform automatically identifies and prioritizes your organization's most critical risks, making it easy for security and IT teams to know where to focus immediately. Our unique analysis prioritizes the hundreds or thousands of critical attack vectors down to the handful that account for most of your risk. The platform also determines an overall security grade for the assets in your attack surface so you can keep track of improvement and report back to management.

The platform's automatic risk prioritization is based on:

- Attractiveness to attackers
- Business context
- Discoverability
- Ease of exploitation
- Remediation complexity

Accelerated Remediation, Efficient Validation

The CyCognito Platform decreases the time it takes to remediate risks and validate fixes from months – on average – to days or even hours. For every risk that's identified, the CyCognito Platform provides detailed supporting evidence about the risk, asset ownership and actionable validation guidance with Exploit Intelligence, so security and IT operations teams can focus on remediation instead of research. Our frictionless workflow integration capability connects with the most popular IT technologies, including SIEMs, ITSM, CMDBs, and communications software, to provide CyCognito's intelligence to organization remediation teams. Once external attack surface issues have been addressed, the platform's continuous testing process will efficiently validate your remediation efforts.

Analytics, Trends and Reporting

The analytics and trends features help you extract key insights from your attack surface data and report on them. Dashboards within the CyCognito Platform, customized for your organization's needs, provide impactful, significant metrics that you can share with security leaders and C-level management. For example, the Issues Dashboard visualizes the types of threats you are facing now and the status of threat investigations. These features can help you cut the time spent analyzing and reporting on your progress from hours to minutes.

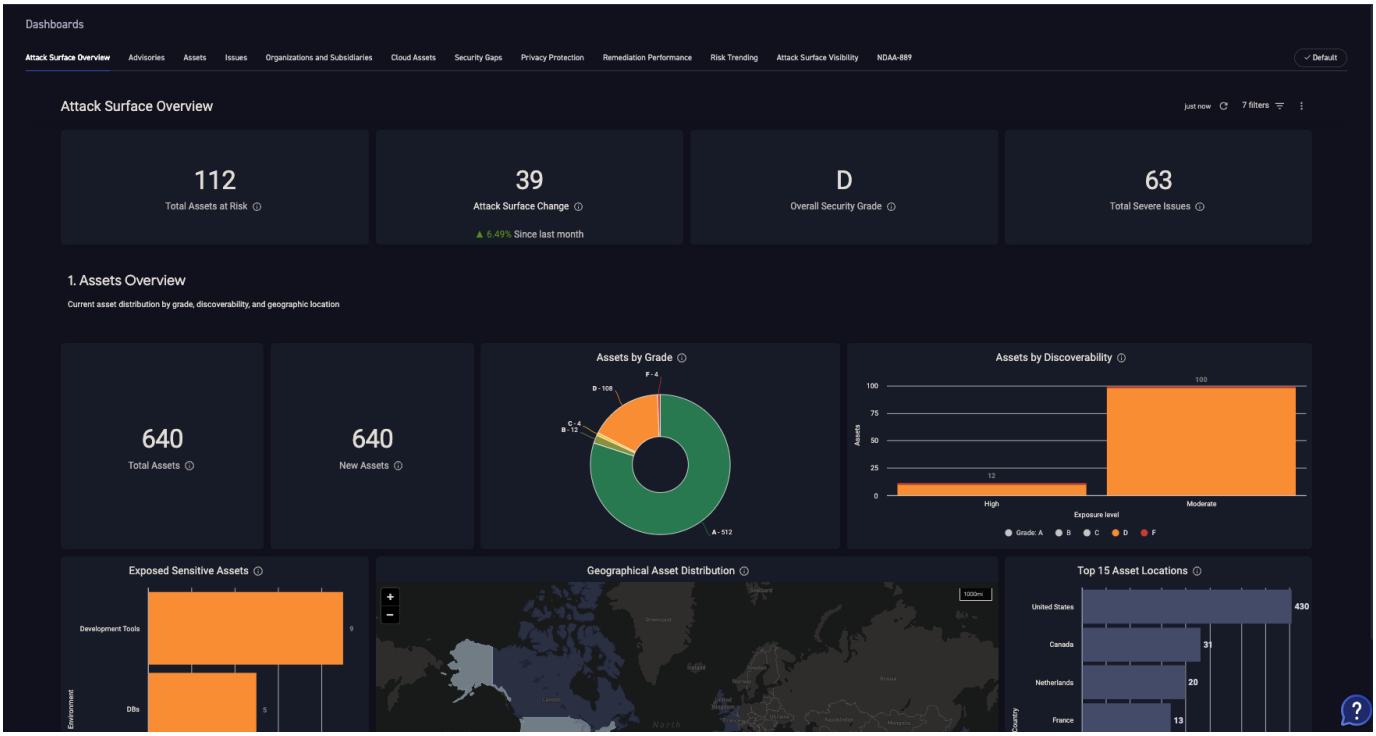

Figure 2: The CyCognito Platform helps you analyze overall trends in your attack surface as well as trends per each asset group.

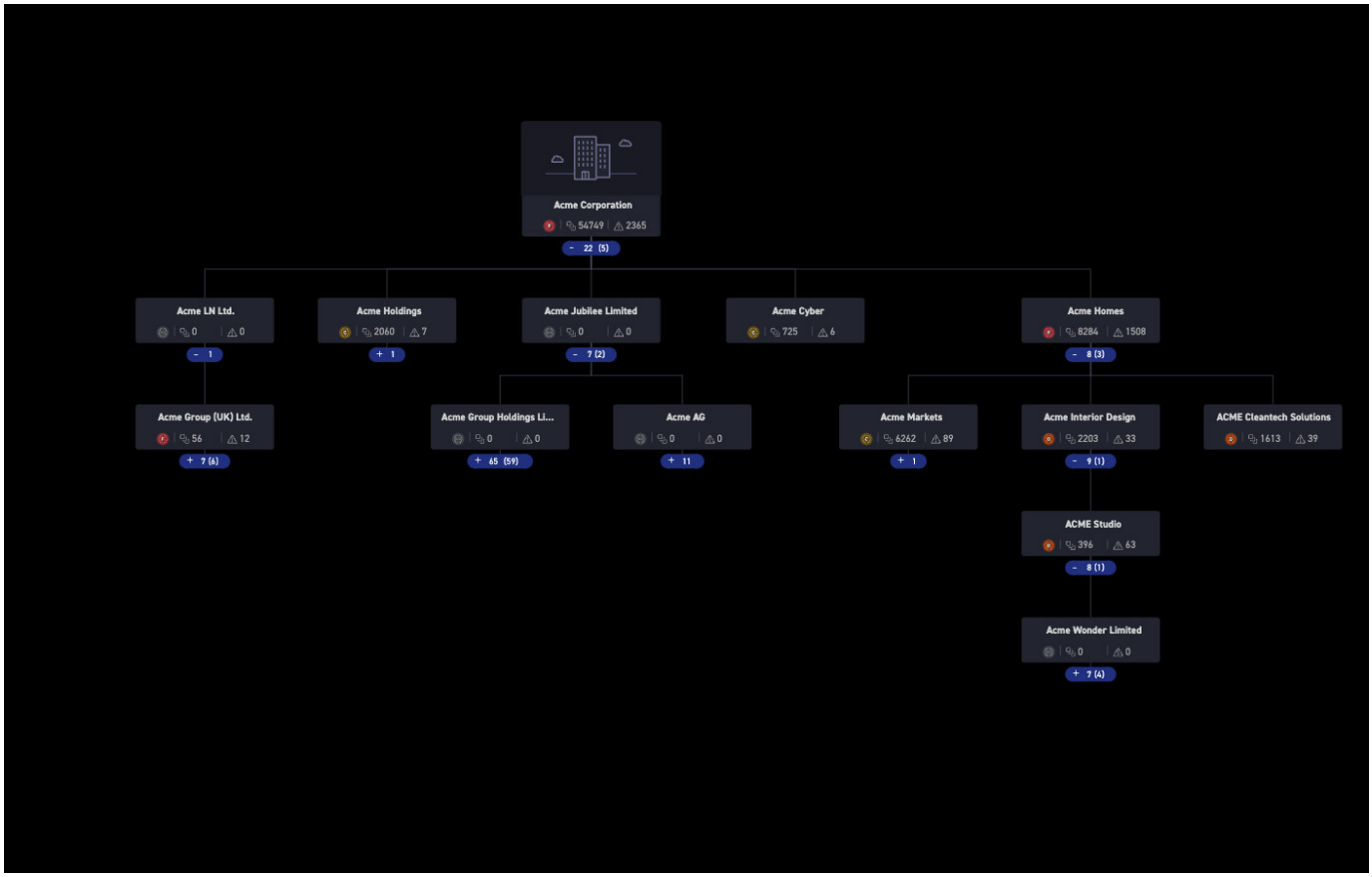

Figure 3: *The CyCognito Platform helps you analyze overall trends in your attack surface as well as trends per each asset group.*

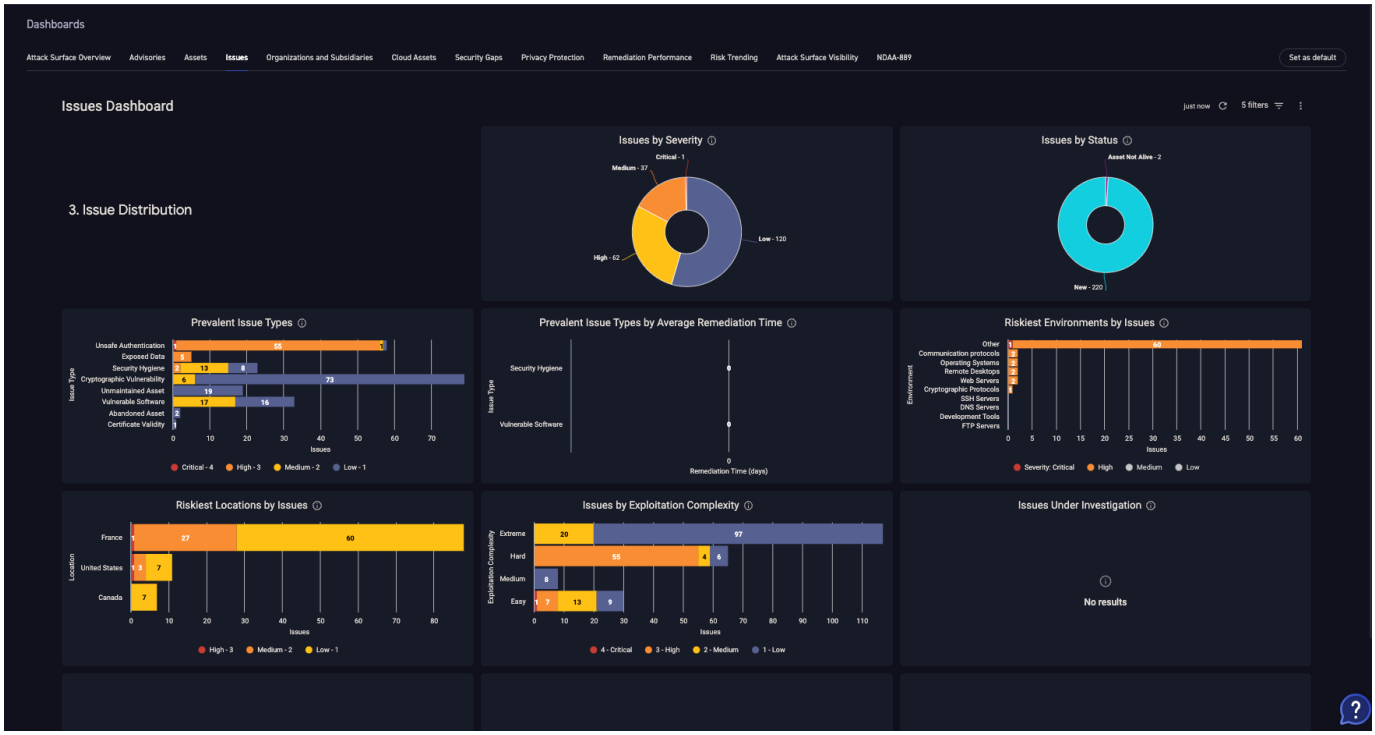

Figure 4: *The CyCognito Platform automatically prioritizes your organization's most critical risks, so your security team knows what to focus on first.*

CyCognito Platform Vulnerability Management

CyCognito Platform Vulnerability Management – a Proactive Approach

The CyCognito Platform detects contemporary cybersecurity exposures that other solutions don't address. See the chart below for the advantages that CyCognito proactive vulnerability management capabilities offer for your external vulnerability management requirements.

	Other VM Solutions	CyCognito Proactive VM
Discovery	Agents (software, cloud extensions) Appliances (cloud or physical)	SaaS with no configuration or deployment
Reconfiguration Of Other Security Solutions	Yes, requires allowlist configurations	Not required, scans cannoted be detected
Scan Types	Authenticated and Unauthenticated	Unathenticated only
Targets	Customer-configured IP address ranges	All exposes assets, including domains and certificates that are owned by or related to your organization whether known or unknown and located on-premise or in cloud, shoudn't be exposes to the internet
Attack Vectors	Focused exclusively on CVEs	Detects CVEs, data explosure, misconfigurations, zero-day vulnerabilities, and assets that are abandoned or shouldn't be exposes to the internet
Prioritization	Static scores Common Vulnerability Scoring System (CVSS),manually configured, incomplete configuration management database (CMDB), third-party prioritization products	Automated determination of business relevance and attractiveness of assets to attackers, along with discoverability, impact, and ease of exploitation
Quantity Of Critical Unauthenticated CVE Detections	Comparable across market-leading VM vendors	On par with, or better than, market-leading VM
New Signature Release Timing	Assured with service-level agreement (ASM)	Assured with SLA

The CyCognito Platform is purpose-built to help you stay ahead of contemporary cybersecurity risks. To learn more about how it gives you an advantage over attackers, visit cycognito.com.

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