CYCOGNITO

TECHNICAL DATASHEET

Active Security Testing

Payload-based Active Security Testing ■ Application Security
CyCognito Architecture ■ Technology Comparison

External risk, assessed frequently across the entire asset inventory, is essential to reduce the risk of a breach. Automated active security testing is the only approach that delivers meaningful results that are proven to lower mean time to remediation (MTTR). With CyCognito:

Test for over 25,000 attacks

CyCognito's payload-based active testing provides comprehensive visibility into complex risk, including extensive dynamic application security tests (DAST).

Test your entire external asset inventory

CyCognito's active testing is integrated with the CyCognito asset discovery and contextualization engine. This eliminates visibility gaps and removes manual effort.

Eliminate asset resource impact

CyCognito's active testing is architected as "low and slow" and is monitored carefully. This enables production systems to be tested without impact or need for complex scheduling.

Achieve >90% confidence

CyCognito's active testing has >90% accuracy in identifying risk exposures. This solves the fourth challenge: High accuracy and low false positives lead to confident IT security staff and faster MTTR.

Validate remediation efforts

CyCognito's active testingis automatic and continuous. Only active testing can confidently validate remediation remediation efforts.

Eighty-three percent of breaches involve external actors[1], yet it is common for today's organizations to actively test a fraction of their thousands of external-facing assets.

The result? Large coverage gaps, lack of detail, noise, and exhausted security teams that are busy but missing meaningful external risk issues.

It isn't a surprise that while 70% organizations report having vulnerability assessment solutions, only 30% find their program effective.[2]

1. Source: 2023 Verizon Data Breach Intelligence Report, https://www.verizon.com/business/resources/reports/dbir/

2. Source: https://www.cybersecurity-insiders.com/portfolio/2022-vulnerability-management-report-helpsystems/

OVERVIEW

How CyCognito Active Security Testing Works

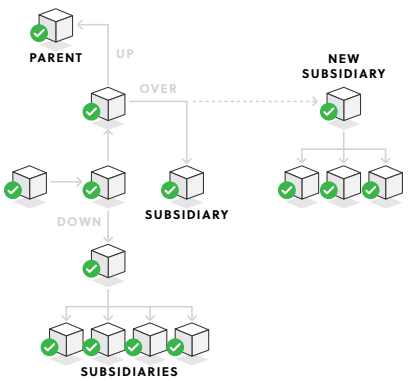
CyCognito's automated, rule based system tests the same way every time, leading to consistency, accuracy and scalability:

1. **External asset inventory and context retrieved** from CyCognito EASM solution
2. **Payloads built to asset specifications** to meet risk detection requirements
3. **Payloads sent to asset** via globally distributed network of CyCognito test systems
4. **Results are validated, compiled and delivered** through user interface and RESTful API

01 External Asset Inventory and Context

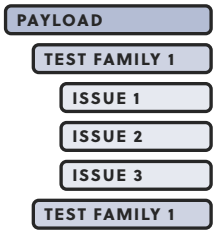
CyCognito active security testing is performed continuously across a dynamically maintained external asset inventory, including assets owned by subsidiaries and 3rd parties.

Integration with the CyCognito discovery engine ensures that the CyCognito test engine has the entire attack surface and full context on every asset, enabling accurate payload development. Examples of asset context include business context, owner, open ports, running services, operating system, and software versions. Testing pre-work is automatic, for example all URLs/ services are captured per web app as context.



02 Payload Development

CyCognito intelligently deploys payloads tailored to asset context. For example, DAST payloads are only applied to web applications. Joomla and Wordpress vulnerability and misconfiguration tests run on CMS environments. Some tests are run on all assets, for example, data exposure.



CyCognito tests for over 25,000 attacks, including validated coverage of 90% of the OWASP Top 10. Test and attack examples include:

- Remote code injection
- SSO/CAPTCHA detection
- WAF detection
- Authentication bypass
- Data exposure detection
- Application misconfigurations (sensitive information disclosure)
- Identify internal business applications
- Cross site scripting (XSS)
- Cross site request forgery (XSRF)
- Weak Javascript libraries
- Exposed remote desktop service (RDP, VNC, etc).
- Weak encryption

CyCognito rigorously evaluates each test prior to deployment to ensure minimum impact. New tests are added frequently with a focus on short turnaround time for newly published zero days and urgent issues.

03 Payload Delivery and Monitoring

CyCognito's network of over 60,000 nodes spread over 100 countries deliver payloads to the asset under test (AUT). Individual tests are distributed across multiple test nodes, from multiple IP addresses, regions and types, to obfuscate the interaction. Whitelisting, input and configuration are not required.

Resource impact levels are monitored carefully, including both load ("bandwidth") and depth (the number of interactions, etc.) even for basic user actions, e.g. fetching a homepage.

CyCognito tests are unauthenticated (also called non-credentialed); at no time do CyCognito active tests modify or compromise a customer asset.

04 Results Validated, Compiled and Delivered

Test results are continuously validated, collected and delivered to the CyCognito multi-tenant architecture for access via UI and API.

The CyCognito prioritization engine combines the test results with exploit intelligence and business context to rank issues for remediations.

3. See CyCognito Discovery & Contextualization technical datasheet for more information

REAL-WORLD EXAMPLE

Why Active Testing is Required for External Risk Detection

You need to know if your externally facing web application is at risk. How does CyCognito active security testing compare to unauthenticated vulnerability scanning?

WEB APP: Vulnerability scanning stops at web server CVEs. Active testing will uncover advanced risk, including exposed sensitive data.

VULNERABILITY SCANNING	CYCOGNITO SECURITY TESTING
Scan Known IP Blocks	Scan all IP Blocks tied to Org
Apache Service active on Port 443	Apache Service active on Port 443
Apache version	Apache version
CVE Lookup	CVE Lookup
CVE Detected	CVE Detected
Patch	Active Tests
	Permits SQL Injection (SQLi)
	Lacks SSO & CAPTCHA
	Exposes Sensitive Data
	Patch & Configure
	Remediation Validation

Technology Comparison

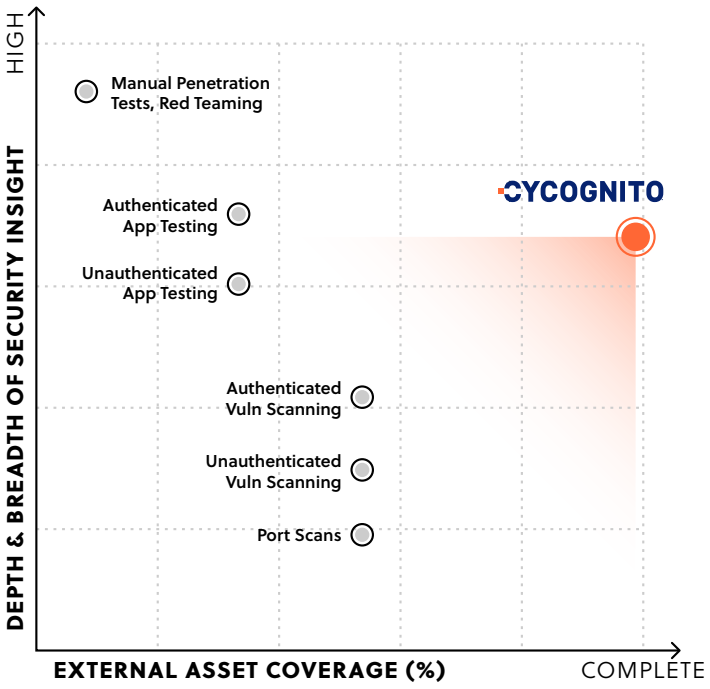
Organizations need security technologies that reduce complexity while providing accurate and meaningful results.

Even high insight across 50% of assets leaves significant gaps. You need full test coverage.

Various technologies provide varying degrees of insight. However, due to limitations in design and increasingly manual effort/cost, they tend to be applied to fewer assets.

CyCognito removes the barriers to full active security testing, providing high-security insight with no manual effort.

What level of security insight do you require?



CyCognito Security Testing vs. Traditional Approaches

Traditional approaches rely on passive scanning techniques and work from incomplete asset inventories.

CyCognito's comprehensive testing and architecture scales to Fortune 10 organization requirements.

Feature	Traditional ASM/EASM/SRS/TPRM	CyCognito
Risk detection	Scanning technology (port scanning)	Active testing and scanning technologies
App Testing	None	Full suite of application security testing, including DAST
Scope	Limited to a portion of external assets, found on pre-configured IP ranges and domains.	Dynamically integrated with full external asset inventory, tied to CyCognito's org reconnaissance and discovery
Accuracy	Low confidence port scanning data along with CVSS leads to excessive noise	Active testing enables complex interactions that uncovers risk beyond vulnerabilities at >90% confidence.
Frequency	Multiple cadences available	Automated active testing delivered continuously
Scale	Manual steps and physical infrastructure requirements make it difficult to scale to enterprise-sized organizations	SaaS delivery model proven to scale to millions of assets, at Fortune 10 organizations
Complexity	High management effort	Continuous active tests delivered frictionlessly. Delivered as a service, without management or configuration.
Remediation validation	None	Validates remediation efforts with active tests
Evidence collection	Lacks attribution and risk detection evidence	Automated evidence collection for all test results

FIND OUT MORE

Don't just scan. Test.

CyCognito's fully automated active testing reduces an operationally complex workflow to a simple service model. Your SecOps team works at its- fullest potential on issues that matter.

Scalable, continuous, and comprehensive active security testing – **only from CyCognito**.

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