SUMMARY DATASHEET

Automated Security Testing

Network Infrastructure and Web Applications Across On-Prem and Cloud

Eighty-three percent of breaches involve external actors[1]. A robust risk reduction strategy requires frequent testing of your full external asset inventory. However, managing tests for thousands of assets, scattered across multiple regions, using siloed tools run by different teams, makes this goal practically unachievable.

CyCognito Automated Security Testing (AST) solves this challenge by running continuously, without manual input, seeds or configuration. AST supplies your teams with critical test results that are central to all manual risk analysis activities

Coverage

YOUR FULL EXTERNAL ASSET INVENTORY

Close risk gaps by testing all exposed infrastructure and web apps, both on-prem and in the cloud. CyCognito automates discovery and recon for all exposed IT and third-party assets.

Accuracy

ACHIEVE >95% CONFIDENCE

High accuracy means less noise and deeper, more meaningful results. With fewer false positives, your team can focus on real vulnerabilities rather than false alarms, reducing time to remediation by more than 60%.

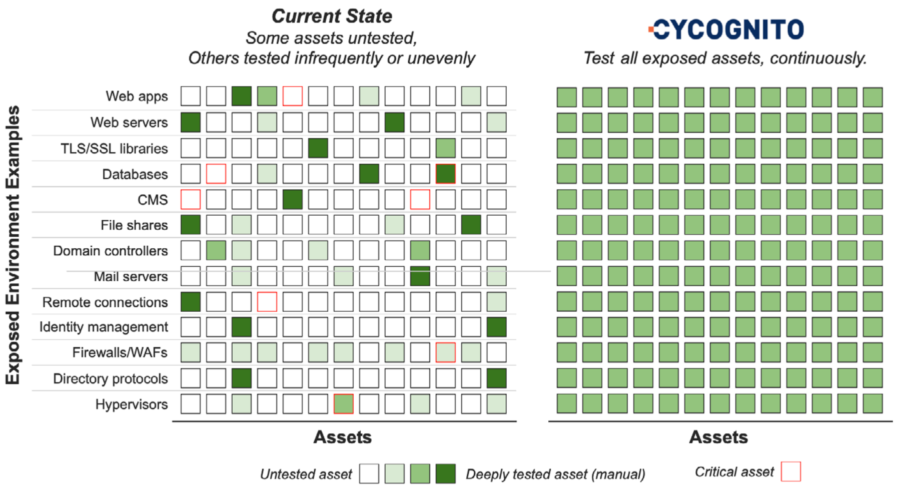
Frequency

CONTINUOUS, AUTOMATED TESTING

CyCognito network and web application tests are curated for safety. Test selection, configuration and monitoring is fully automated, instant scans can be initiated any time.

Reach Your Ideal Security Testing Goals

Security testing teams often reduce test scope due to lack of time, test tool complexity and visibility gaps. CyCognito closes these gaps by providing fully automated testing, delivered as a service.



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

How CyCognito Security Testing Works

CyCognito's automated, rule-based test architecture delivers consistency, accuracy and scale:

- **Retrieve external assets and context** – Delivered by CyCognito Attack Surface Management (ASM)
- **Assign test payloads** – Asset context informs payload assignment and test configuration
- **Schedule and deliver tests** – Tests delivered through 60,000+ globally distributed test nodes
- **Validate and compile results** – Prioritized issues and evidence via user interface, integration and API

CyCognito tests for tens of thousands of attacks, including coverage of the majority of OWASP Top 10. Tests include:

- SSH using weak credentials
- 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.

Eliminate Risk Gaps, Automatically

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

Gaps in your security testing program are likely more than simply missed assets. Infrequent testing and low test accuracy are also gaps, and can be just as bad or worse.

CyCognito removes the barriers to reaching your ideal security testing goals, providing deep insight with no manual effort.

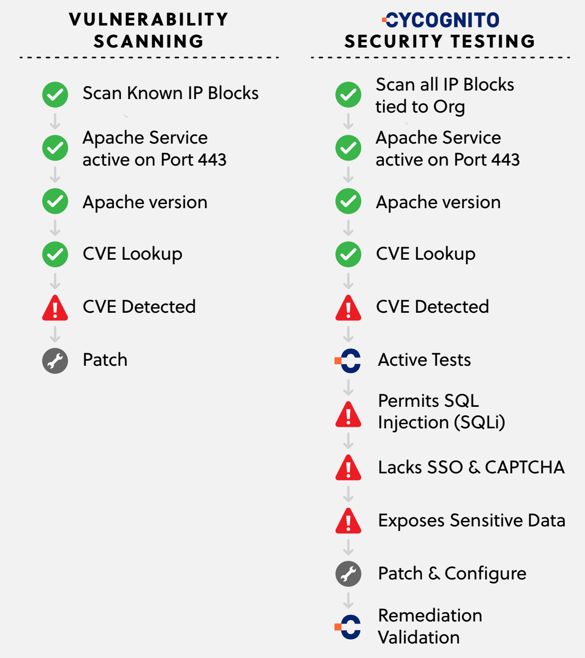
Use CyCognito's security testing gap calculator for visibility into your current testing deployments: https://www.cycognito.com/security-gap-calculator/

Find Out More

Don't just scan. Test.

CyCognito's fully automated active testing reduces an operationally complex test workflow to a simple service model. Your security teams work at their fullest potential on issues that matter. To learn how the CyCognito platform uniquely helps you identify and prioritize issues in your exposed IT ecosystem, visit cycognito.com.

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



VULNERABILITY SCANNING

- ✓ Scan Known IP Blocks
- ✓ Apache Service active on Port 443
- ✓ Apache version
- ✓ CVE Lookup
- ⚠ CVE Detected
- Patch

CYCOGNITO SECURITY TESTING

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