CYCOGNITO

SOLUTION BRIEF

# Active Testing vs. Passive Scanning to Detect Attack Surface Risk

While many organizations have adopted a shift left approach to integrating security in their software development lifecycle (SDLC) and have deployed protection technologies throughout their infrastructure, the fact remains that at any time there are 100's if not 1,000's of digital assets[1] that have bypassed an organization's formal pre-production test regimen, are unknown, or unprotected.

Gartner research states "unpatchable security issues will increase from 10% to over 50% of overall risk by 2026"[2]. Externally exposed assets represent the most easily accessible threat vector[3] and vulnerabilities on these assets are top priority for remediation.

## Passive Scanning vs. Active Testing in EASM

Many external attack surface management (EASM) solutions depend on passive scanning techniques to build asset inventories and identify common vulnerabilities. However, when used alone, this approach does more harm than good, resulting in asset gaps, low context, high false positives and overall lack of meaningful insight. Active testing is necessary for complete visibility into external risk.

| | | |
|---|---|---|
| **Passive Scanning** | OSINT \| DNS \| Network monitoring<br>Network mappping \| Port scanning | "No touch"/"light touch" techniques used to obtain port state. Most EASM solutions stop at passive scanning, resulting in incomplete asset inventories based on manually entered IP ranges. Passive scanning can be used to alert on possible presence of some CVEs (with high false positives). |
| **Active Scanning** | Advanced testing engine(s) to identify critical risk: web applications, networks, confidentiality, reputation + more | Interactive testing techniques used by select EASMs to build high confidence asset inventories, advanced risk assessment and vulnerability identification, remediation validation and more. |

Passive scanning tools range in interaction with an asset from zero ("no touch") to limited ("light touch"). Active testing uses advanced techniques that can involve repeated interaction with the target asset.

1 Examples from CyCognito internal research (2023) include infrastructure, DevOps tools, forgotten marketing websites, APIs, data sharing platforms, and cloud resources (directories, services)

2 Gartner "Predicts 2023: Enterprises Must Expand From Threat to Exposure Management" December 2022

3 Verizon Data Breach Investigation Report (VDBIR), 2022

## Passive Scanning

Passive scanning techniques are used in most, if not all, EASM products. "No touch" passive scanning techniques use open-source intelligence (OSINT) such as DNS enumeration through tools such as dig[4] or host[4], network monitoring through tools such as Wireshark. It may also involve parsing pre-existing active reconnaissance results.

"Light touch" passive scanning include command-line resources like netcat[4] (nc) as well as open-source network mappers like nmap[4] or port scanners like masscan[4]. This approach requires seeding the tools with IP ranges, which is then used to identify port state (open/closed/filtered) and more.

These tools can build a basic list of externally exposed assets and alert on the possible presence of common vulnerabilities and exposures (CVEs).

- **To keep speed high and impact low**, port scanners use only the initial response presented within the protocol handshake, called "banner grabbing".
- **Banners can be incomplete or incorrect** due to misconfiguration or system instability; Software versions (CPEs) developed solely from banners are best estimates.
- **CVEs mapped from CPEs are "assumed to be present"** since port scanners are unable to provide validation. This introduces in accuracy (e.g., a patch may not be reflected in the banner) and noise (as much as 70% false positives[5]).
- **Port scanners use CVSS[6] severity ratings for prioritization** which often do not align with business priorities; it is common for so-called critical issues to not pose measurable risk[7].
- **Port scanners cannot detect most attack surface risks**, including most software vulnerabilities (e.g., BlueKeep), web application vulnerabilities (e.g., SQL injection), sensitive data exposure (e.g., personally identifiable information, or PII), or many other issues.

Port scanning isn't just a "nice, basic way to perform EASM", it's actually risky, **problematic, noisy, and sometimes painful**.

### OSINT
### The (often underutilized) Attackers Perspective

While OSINT is a leading source of insight used by attackers, **only select EASMs utilize it to its full extent**.

Most EASM require manually entered IP ranges to build asset inventories. Modern EASMs leverage OSINT to **perform organizational reconnaissance** and dynamically build public facing IP blocks.

Asset inventories and CVEs obtained solely from port scanners should be viewed as **incomplete and low confidence results**.

## Active Testing

Active test engines interact repeatedly with a digital asset to reach success criteria defined by the test methodology. Commercial and open-source active testing tools are available, such as OpenVAS and Burp Suite.

Active testing is required for meaningful risk detection and management because:

**Most external risk is invisible to port scanners**

- Active tests evaluate the entire session for anomalous behavior, not just protocol handshake information; any vulnerability, weakness, or risk on any digital asset type can be uncovered through active testing.
- Active tests provide complete visibility into attack surface risk, such as susceptibility to SQL injection attacks, use of default logins in webforms, replication of complex manipulations to reveal non-obvious sensitive data exposure, vulnerable shared libraries, security misconfigurations, and more. Only active testing can detect 9 of the OWASP Top 10, for example.

**High accuracy is non-negotiable**

- Active testing has >90% accuracy in identifying vulnerabilities; this is the minimum level of confidence required for organizations to assign human staff to resolve issues.
- Active testing validates that a running service aligns to protocol banner information, building a vulnerability list based on what is running, not just what the banner describes.

**Without context, remediation is orders of magnitude more difficult**

- Active testing reveals context that is relevant to the organization's environment. For example, the same vulnerability on a database server and a random "empty" server should not have the same prioritization (a nuance that port scanning based EASM technologies cannot overcome outside of manual effort, which is not scalable).
- It is common for IT security teams to discover the vulnerability and IT operations teams to remediate it. Active testing produces issue evidence that significantly speeds remediation efforts and builds cross-functional team trust.

Despite its value, **many organizations perform a fraction of available active security tests** on a subset of their external asset inventory.

4 Publically available manual (man) pages for the listed tools; dig, host, netcat, nmap, masscan
5 Based on 2022 CyCognito internal research across its services and dialog with vulnerability management teams at enterprise organizations.
6 https://nvd.nist.gov/vuln-metrics/cvss
7 Read more in CyCognito's post "One month in: CyCognito looks at Spring4Shell", May 2022

## Navigating EASM Product Hype

EASM products vary widely in capabilities. Unfortunately, vendors use similar terminology to describe their technologies. "Scan", "test", "assess", "classify", "discover", "context" and "attackers perspective" are often used. This makes it difficult to discern which EASM products use which techniques and to what extent.

For example, an EASM vendor may claim **asset discovery**, but rely on human input for IP address ranges or CVE targets.

**Or asset classification**, but provide only banner information and IP address.

**Or application testing**, but only perform a small fraction of tests on a subset of assets.

**Automation is a common hidden layer**; some EASM may automate some tasks, but lack full automation.

Incomplete asset context, manual data augmentation, discovery inputs, and CVSS-based severity scores are indicators of gaps in the EASM technology stack that result in **wasted time for IT security teams**.

| EASM Phase | EASM Type | | |
|---|---|---|---|
| | Basic | Legacy | Modern |
| **Passive Scanning** | | | |
| Domain/subdomain identification | ○ | ◑ | ✓ |
| Organizational business structure mapping | ○ | ○ | ✓ |
| Asset discovery | ◔ | ◑ | ✓ |
| Asset classification | ○ | ◑ | ✓ |
| Asset ownership | ○ | ○ | ✓ |
| CVE assessment | ○ | ◑ | ✓ |
| **Active Scanning** | | | |
| Extended CVE identification | ○ | ○ | ✓ |
| Web application risk | ○ | ○ | ✓ |
| Network risk | ○ | ○ | ✓ |
| Confidentiality risk | ○ | ○ | ✓ |
| Reputation risk | ○ | ○ | ✓ |
| Remediation validation | ○ | ○ | ✓ |

## Why Most EASMs Stop At Passive Scanning

Active tests uncover considerably more risk, with higher confidence, than passive or techniques. Yet most EASM vendors rely solely on passive scanning data for asset discovery, classification and identification of CVEs. Why?

- **Most EASM products on the market are legacy ASM** – Reconnaissance was the primary technology available when these products emerged and retooling a legacy service with new test engines for modern use cases is difficult.
- **Network mappers/port scanners are inexpensive and easy to run** – Active tests involve deeper interaction, lengthier sessions and more tests. Active test engines require more resources to run and monitoring to prevent disruption.
- **Why fix what is (believed) not broken?** – The lower cost and simplicity of a passive-scanning-only approach enables many EASM vendors to offer limited asset discovery and risk assessment content that they can communicate as value.

Consumers pay for the difference with inventory gaps, risk gaps and high false positives during real-world use.

| | Passive Scanning | Active Scanning |
|---|---|---|
| **PROs** | ■ Dual purpose - asset discovery, basic CVEs<br>■ Fast execution, low impact<br>■ Inexpensive | ■ Complete attack vector coverage<br>■ High accuracy<br>■ Validates remediation efforts |
| **CONs** | ■ Noisy/high false positives<br>■ Low accuracy<br>■ Limited attack vector coverage | ■ Potential slower test execution<br>■ Higher testing cost<br>■ Potential target resource impact |

## CyCognito's Approach to Security Testing

CyCognito performs passive and active testing across an organization's entire external asset inventory, automatically and continuously. This high fidelity multi-faceted approach is the only way to understand the true path of least resistance and enable IT security teams to reduce the risk of attack.

We remove the manual steps that **slow your team down** and provide defensible, evidence-based guidance to **speed them up**. A breakout of CyCognito's technology stack is illustrated below, with weekly, bi-weekly and monthly scanning cadences available.

**External Attack Surface Discovery**

- Build map of **organizational business structure**
- Identify **domains** and **subdomains** owned by parent and subsidiaries
- Identify **certificates** & **IP ranges** tied to domains/ subdomains
- Identify active ports on CyCognito supplied external IP addresses
- Identify software versions and classify **web applications**
- Add context to assets: owner, type, CVE mapping, etc.

**Active Testing**

- Web application testing
- Network security testing
- Confidentiality testing
- Reputation testing
- Remediation validation, validate active reconnaissance results + *more*

**CyCognito Passive Reconnaissance Engine**

CyCognito's proprietary passive reconnaissance engine leverages natural language processing (NLP), machine learning (ML) and OSINT to dynamically uncover organizational business structure, domains, sub-domains, IP ranges, and more. This approach provides more complete asset detection and attribution

**CyCognito Active Reconnaissance Engine**

Open source and commercial toolsets combined with proprietary technologies take CyCognito sourced IP ranges and assesses asset state, and adds deep context, including ownership and classification. Potential CVEs are identified for the active testing engine validate.

**CyCognito Active Testing Engine**

Open source, commercial and proprietary active testing engines run a full suite of tailored tests based on asset type and services, carefully monitored to avoid impact. This information, combined with asset context and threat intelligence, is sued to build the unique CyCognito severity scores.

# Scalable, continuous, and comprehensive security testing across your full inventory of external assets – only from CyCognito.

To discuss CyCognito's security testing capabilities or a demonstration of CyCognito, please reach out to to your CyCognito account representative, or email us at **info@cycognito.com**.

CYCOGNITO