CYCOGNITO

SOLUTION BRIEF

IS YOUR VULNERABILITY MANAGEMENT SOLUTION A MATCH FOR TODAY'S THREAT ENVIRONMENT?

Evaluate Its Effectiveness with These Five Key Questions

Organizations typically turn to security testing to uncover potential risks and attack vectors, and one "go to" solution is their vulnerability management (VM) platform. It's no secret that attacker techniques have dramatically improved in scalability and effectiveness in the last decade and that the area to be guarded — your attack surface — has been reshaped by your IT transformation. But legacy VM solutions, created some 20 years ago, haven't been upgraded to address today's extended IT ecosystems. While their methods may be adequate for internal scanning, they are not designed to uncover your externally-exposed assets that harbor the hidden risks that creative, sophisticated attackers target first.

Here are five questions to ask yourself to determine if your vulnerability management solution is adequate to help you proactively defend your attacker-exposed IT ecosystem:

01 Is your VM platform addressing your entire attacker-exposed IT ecosystem?

Your VM solution can't assess what it can't see. In order to fully assess risks in your extended IT ecosystem, your VM process must begin with an accurate view that includes assets that are part of your organization, even if they are unknown or unmanaged by you.

Vulnerability assessment (VA) solutions review active IP addresses and only the IP ranges you have directed them to look for. But your actual attack surface that attackers are surveilling includes both active and inactive IPs, abandoned assets, domains, subdomains, certificates and web applications. Attackers also focus on your assets that are externally exposed via cloud, subsidiary, partner and third-party environments.

If your VM solution has an incomplete view of your attack surface because your VA solution, penetration tests and other tools have limited visibility, it will only have an incomplete view of your attacker-exposed risk.

02 Does your VM solution discover a full range of risks across your IT ecosystem — well beyond what software versions are out-of-date and which patches are needed?

Vulnerability scanners focus on identifying tens of thousands of Common Vulnerabilities and Exposures (CVEs). Matching scans of your organization against a CVE list will identify out-of-date software that needs patching and other common issues. With so many CVEs in the typical vulnerability scanner database, it's understandable why you might feel that your organization is being thoroughly assessed when you are presented with a long list of findings.

But CVEs are not enough to assess all of your attack surface risks. Your organization also needs to detect potential issues with the following to outmaneuver attackers' offensive operations:

- inactive IPs
- insecure/exploitable code
- abandoned asset vulnerabilities
- bypassable authentication mechanisms
- misconfigured cloud components
- network architecture flaws
- default credential vulnerabilities
- software vulnerabilities
- web application vulnerabilities
- certificate trust vulnerabilities
- SaaS platforms takeover risks
- data exposures
- DNS and mail server hijacking risks
- web application and database hijacking risks
- and many other attack vectors

Because vulnerability scanners don't address all of these issues, organizations will layer on one or more point-products designed to address some of these, and services such as penetration testing. The result is a difficult-to-manage patchwork that creates risk visibility gaps.

03 Does your VM platform help you prioritize the many thousands of risks that an externally-focused vulnerability scanner (and other tools) will uncover?

As noted above, vulnerability scanners are focused on matching known vulnerabilities to your assets. For a large enterprise, a vulnerability scan will identify an overwhelming volume of vulnerabilities in your attack surface based on CVEs alone. The volume is overwhelming even to the most seasoned security team. And experienced team members know that their vulnerability list is only the start of the process. They must spend dozens of hours per month prioritizing risks because CVEs are not evaluated by the lens of your organization and whether the vulnerability actually exists for you in the way that you have deployed the software.

Ask yourself if your security team would be more effective if your VM solution identified the vulnerabilities that are most critical to your organization, in the context of which assets are most important to your organization, and which assets are most attractive and easily accessible to attackers.

04 Does your VM solution give you actionable remediation guidance supported by research for risks beyond CVEs and help you validate your remediation?

Since vulnerability scanners focus on CVEs, they don't typically offer actionable remediation guidance for risks beyond the CVE list. Ask yourself if actionable remediation guidance for all the issues identified in your attack surface would save your security team time and effort when remediating.

And does your VM solution provide efficient validation and reporting that, in fact, the remediations have achieved their purpose? This is an important and time-consuming part of the process.

05 Is your VM process continuous?

In addition to the fact that vulnerability management solutions can't assess assets they can't find, most organizations aren't scanning and testing their entire IT ecosystem due to cost concerns around the staffing requirements alone. Continuously scanning and testing your entire IT ecosystem for vulnerabilities and other potential attack vectors 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.

Attackers won't respect a periodic scanning cadence, your VM solution has to be "always on" to offer proactive defense.

Compare the CyCognito Platform to Traditional VM

		VM Only	CyCognito
Capabilities	Automates unbiased scoping of scan targets		✓
	Automates contextualized grouping by subsidiaries, environments, and platforms		✓
	Frictionless, no-noise vulnerability management		✓
	Prioritizes risk based on asset discoverability, attractiveness and exploitability		✓
	Automates and continuously rescans and reports on fixed issues		✓
	Evaluates subsidiaries, third parties, and M&A candidates		✓

To learn more about how the CyCognito platform goes far beyond traditional vulnerability management solutions, visit ***cycognito.com***.

If you have already adopted the CyCognito platform for vulnerability management, you know that your answers to the above questions are "Yes."

The CyCognito platform uniquely delivers:

- The essential vulnerability management foundation of full discovery of your extended IT ecosystem, including assets that are part of your IT ecosystem, but are unknown or unmanaged by you.
- Detection and testing of attack vectors across your entire attacker-exposed IT ecosystem, going well beyond CVEs, including data exposures, misconfigurations and even software zero-day vulnerabilities.
- Prioritization of the attack vectors in your IT ecosystem based on what could impact your organization most from a cybersecurity risk perspective.
- Actionable remediation guidance and reporting to accelerate your remediation and validation.
- Continuous scanning and testing of your entire IT ecosystem, detecting new assets, vulnerabilities and other potential attack vectors.

CYCOGNITO
420 Florence Street
Palo Alto, CA 94301
cycognito.com

CyCognito is solving one of the most fundamental business problems in cybersecurity: the need to understand how attackers view your organization, where they are most likely to break in, and how you can eliminate that risk.

© CYCOGNITO INC. ALL RIGHTS RESERVED. 101620