CYCOGNITO

SOLUTION GUIDE

CRITICAL CAPABILITIES FOR EXTERNAL ATTACK SURFACE MANAGEMENT

Every business is a digital business. And because of that, you have an ever-expanding IT presence exposed to the entire world via the internet. Your internet-exposed assets and their potential risks define your external attack surface.

This paper evaluates different external attack surface management (EASM) capabilities that serve the needs of the business, enable digital transformation, and securely connect your organization to your customers, employees and partners through the internet. Specifically, the capabilities of a true external attack surface management solution should provide:

01
Accurate inventory of every internet-exposed asset and business relationship across your organization

02
Asset context to help identify business owner, function and purpose

03
Continuous testing at scale to uncover all risks across your entire external attack surface

04
Prioritization of risk based on meaningful evaluation of several factors

05
Accelerated remediation with actionable guidance, efficient validation and streamlined workflows

LET'S EXAMINE EACH OF THESE POINTS BELOW

01 IDENTIFY AND INVENTORY INTERNET-EXPOSED ASSETS & BUSINESS RELATIONSHIPS

The foundation of security is knowing what you have so you know what to protect. However, most security teams are working off of asset inventories and business maps, including all subsidiaries and business units, that are out of date and incomplete. These gaps are often due to manual processes, human error and the ease with which assets can be procured or spun up, especially in the cloud.

Many organizations augment manual processes by using tools that monitor their internal networks for unknown or previously unseen devices that should be in their inventory. But these technologies do not have the ability to discover assets which may be connected directly to the internet and not a part of the internal networks being monitored. This is especially important for assets in the cloud.

An external attack surface management solution should be able to automate this external discovery and provide an inventory of everything that belongs to your organization, including your acquired companies and joint ventures, that is connected directly to the internet. That's critical because you must prioritize those exposures and vulnerabilities that can be accessed directly by attackers.

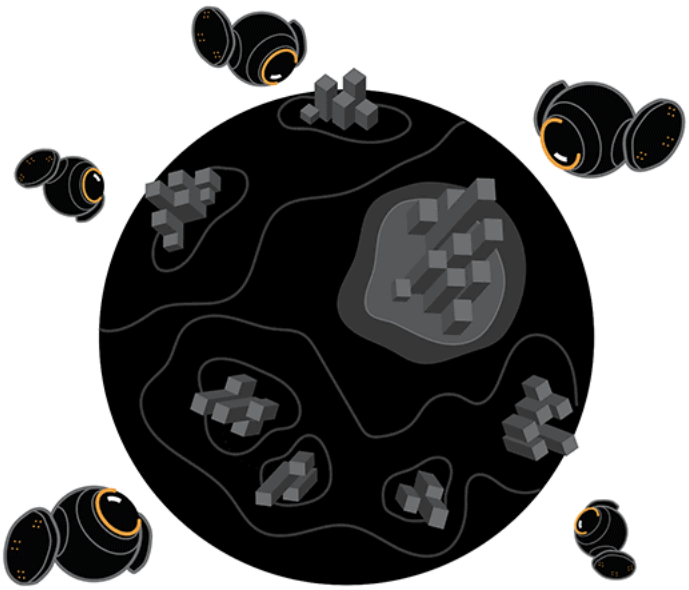

Figure 1. The first step is to understand the scope of your business, including all subsidiaries and business units, and the breadth of your external attack surface.

02 BUSINESS CONTEXT MATTERS

The depth of information ASM vendors discover or create about your assets is another key item to consider when evaluating platforms, especially with the goal of reducing your attack vectors efficiently and effectively.

Security teams need the context of incidents and issues that they're presented with. Given security team staffing constraints, organizations need all the security intelligence they can get. By providing deep insight into what triggered an alert, how that system is connected into your organization, and what group is responsible for it, your security teams can operate faster and with less manual effort to determine context around incidents.

Different groups within an organization may have different risk tolerances given their business function, initiatives or leadership. In addition, different assets and attack paths may be more attractive to attackers based on the data and business processes associated with those attack paths. This means that the attack surface risk of different areas of the business can be different from one another.

Once your internet-connected assets are understood at this depth, prioritization and system-level remediation or evaluation of enterprise-wide policies can begin.

You Need More Than Just IP Information

Every business will always have systems connected to the internet. That's the nature of IT and digital transformation. They need to understand:

- Which systems are visible to attackers?
- Do those systems expose attack paths to attackers?
- Is there vulnerable software running on exposed systems?
- Do I have expired certificates?
- What is the business purpose of the system?
- What other systems are connected to this system?

03 TEST SECURITY CONTINUOUSLY AT SCALE

Attackers will choose “the path of least resistance” into your organization. Most often, that’s a path that goes through an asset that your IT and security teams don’t see, have forgotten about or don’t manage. While organizations are becoming better at protecting against popular attack techniques like phishing or misused credentials, attackers are always looking for new ways into your infrastructure that you aren’t monitoring. This leaves attackers free to wreak their havoc, often unnoticed.

Going beyond just identifying common vulnerabilities and exposures (CVEs) to truly uncover all attack vectors that attackers could use, including misconfigurations, data exposures and zero-day vulnerabilities, modern external attack surface management solutions can give defenders an advantage. And the best EASM solutions do this continuously, not just periodically to meet the needs of compliance mandates.

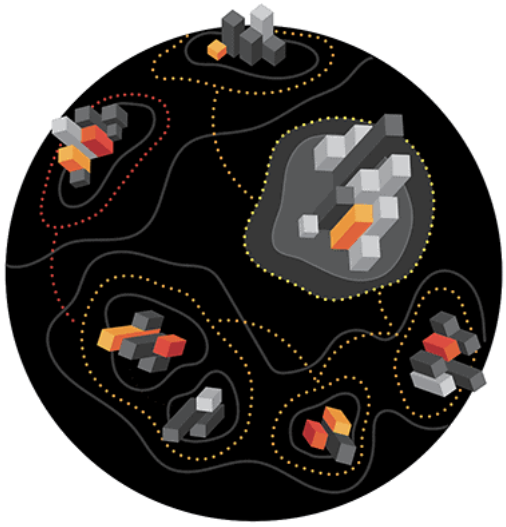

Figure 2. External attack surface management solutions that see all possible attack vectors, as the CyCognito platform does, help organizations eliminate security gaps before attackers can exploit them.

04 INTELLIGENT RISK PRIORITIZATION

Most of an organization’s risk is generated by a very small handful of security gaps. Many ASM vendors will provide details of an exposure, but they leave it up to the analyst or engineer to figure out how to sift through the noise and determine which security gaps expose the organization to the most risk . This leaves many resolutions up to subjective decisions, and often requires laborious, manual effort to review all details of a security gap.

A more efficient way to quickly prioritize the riskiest attack vectors for remediation is to utilize an automated solution that uses meaningful data on things like attackers’ priorities, the discoverability of an asset or exposure, the ease of exploitation, the complexity of remediation, and business context of what is exposed to identify the most critical risks.

Figure 3. An EASM product needs to collect information about your assets – across your entire IT ecosystem – and prioritize risks based upon business context and other factors.

05 ACCELERATE REMEDIATION WITH AUTOMATED GUIDANCE

Guidance, validation and streamlined workflows speed up the time to resolve issues and incidents. With a prioritized list of risks, the next step is to communicate that information quickly and seamlessly to the teams that remediate or mitigate the risk. Clear, detailed and actionable remediation guidance and exploit intelligence offer security and IT teams a clear path forward to fix an exposure and lower the organization's risk.

Because organizations employ many tools along the path from identification, evaluation, prioritization to remediation of a risk, powerful EASM platforms should include workflow capabilities that connect seamlessly into the most popular IT technologies, sending intelligence to remediation teams via the established communications pathways.

Finally, before work can be considered complete – the patch, change in configuration, or compensating control should be validated to ensure that the exposure has been addressed and the risk is gone.

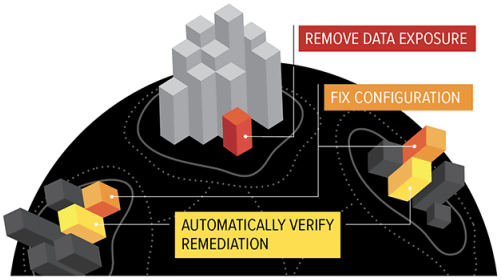

Figure 4. An effective EASM solution can accelerate remediation by providing details about how to resolve an issue.

CONCLUSION

Adopting external attack surface management as a process that helps you understand and continually reduce your organization's risk exposure enables growth and digital transformation.

CyCognito has introduced a platform with this concept in mind. The CyCognito platform helps your IT and security teams reduce the number of attack vectors while also providing perspective and visibility into your organization's IT risk. It does so with the understanding that there will always be business assets that are exposed, but that comprehensive awareness is key to improving your security posture.

To learn more about the market leading external attack surface management capabilities of the CyCognito platform, visit cycognito.com/attack-surface-protection.

CYCOGNITO

420 Florence Street
Palo Alto, CA 94301
cycognito.com

CyCognito provides solutions that identify and eliminate shadow risk: risk that IT and security teams are blind to, but sophisticated attackers actively target. The CyCognito platform is a fully automated next-generation security risk assessment solution that enables leading companies to discover, understand, prioritize and eliminate their organization's shadow risk wherever it is, including cloud, partner and subsidiary environments.