CYCOGNITO

SOLUTION GUIDE

Understanding the Technology: External Attack Surface Management (EASM) & Breach and Attack Simulation (BAS)

Overview

External Attack Surface Management and Breach and Attack Simulation are two security operations technologies that are getting a lot of attention for their ability to improve security posture. Security professionals naturally want to understand how they relate to each other, and which one an organization should deploy first. This guide explores those topics and provides recommendations.

Preventing Breaches

Large organizations spend tens of millions of dollars on a myriad of security solutions trying to secure their complex enterprises. To ensure they are getting the most from their investments, security leaders have long sought ways to validate and bolster organizational security postures. However, as we see nearly daily, companies are still getting breached. Why is that?

The simple answer is that defenders must be right 100% of the time while attackers only need to find one path into an organization's IT ecosystem. The longer answer is that security leaders are faced with trying to manage the risk of an ever-growing and evolving attack surface with too many disparate technologies, too few people resources, and the constant threat of the real-world impacts of a breach. That's why it's more important than ever to select the right technology to address current needs.

It's imperative to understand the external attack surface and its risks to enable organizations to know what areas need attention and focus immediately, and which can be prioritized for later follow-up. That makes EASM a natural technology to apply ahead of BAS solutions, as BAS tools are designed to be aimed at known areas of potential security risk.

Here are some key differences between the two approaches:

It's imperative to understand the external attack surface and its risks to know what areas need attention and focus immediately, and which can be prioritized later. That makes EASM a natural technology to apply ahead of BAS solutions.

Comparison Chart

Capability	BAS	EASM
Automated discovery of assets belonging to all entities related to the organization (such as subsidiaries, business units, connected partners, cloud resources, etc.)	No	Yes
Automated attribution of assets that are discovered to the organization itself, a related entity or another probable owner	No	Yes
Security testing of all assets, not limited to (or primarily focused on) security devices and measures	No	Yes
Security testing for a broad range of issues that are not limited to specific threats and known attack sequences	No	Yes
Prioritization of what to remediate immediately based on a comprehensive view of the organization's entire attacker-exposed IT ecosystem	No	Yes
Ability to simulate lateral movement across an internal network by leveraging a scripted Metasploit agent	Yes	No
Triggers security rules, producing alerts that validate you are being tested	Yes	No
Exploits vulnerabilities	Yes	No

Breach and Attack Simulation (BAS)

What is BAS?

Gartner defines BAS technologies as tools "that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement and data exfiltration) against enterprise infrastructure, using software agents, virtual machines and other means." BAS has gained traction in the security testing and validation space, and Gartner has written favorably about the category.

> BAS will not help you identify where breaches are likely to occur across your entire external attack surface so that you can prevent them, so if you're looking for that kind of solution, EASM is a better option.

Why you may be considering BAS

The premise behind BAS is appealing: what if you could gain insights into how your security infrastructure stacks up against the techniques attackers employ in the real world? And what if you could access these insights continuously, rather than in a report that's delivered two to four weeks after a one-time engagement (as is typically the case with a penetration test)?

In theory, BAS sounds like it would be able to help security operations teams focus on the highest-priority vulnerabilities and areas of greatest concern. However, BAS actually lacks the full context of the attack surface required to do that. BAS solutions are better used once an organization has a comprehensive view of their areas of greatest risk.

4 Things to consider when looking at BAS Solutions for posture management

01 BAS primarily tests security assets

These products usually test security-related assets such as web application firewalls, secure email gateways and web gateways that are both external-facing and inside the organizational network perimeter. They typically do not test assets that are not part of the security infrastructure (e.g., web applications).

02 BAS has limited visibility

BAS solutions will only inspect what you tell them to inspect: you'll need to configure the tool to look at the specific assets that you think are most important. BAS cannot help you determine which assets most need testing. If you aren't aware of the existence of an asset, then a BAS product won't be either.

03 BAS operates without business context

Even products that do what vendors tout as "asset discovery" do so only within a limited range that's been preconfigured, such as on a specific subnet. By their nature, BAS tools only look for exploitable vulnerabilities. If there's no known exploit (yet!), BAS won't find it.

04 BAS delivers a technical outcome, not a business outcome

BAS can tell you which exploitable vulnerabilities can be successfully exploited, but cannot deliver a meaningful assessment of overall organizational risk because of limited scope, visibility and context.

All in all, BAS will let you test the security controls you believe are already in place, in a way that's automated and continuous – and fairly inexpensive. BAS works quite well for this use case, though it does require you to spend time and effort configuring it. But BAS will not help you identify where breaches are likely to occur across your entire external attack surface so that you can prevent them, so if you're looking for that kind of solution, EASM is a better option.

External Attack Surface Management (EASM)

What is EASM?

By definition, the external attack surface includes all of an organization's IT assets – or those that are closely related to the organization – that can be seen by would-be attackers looking in from the outside. Attackers continuously survey and test the attack surface to find the path of least resistance into an environment. External Attack Surface Management (EASM) enables your organization to do the same thing, performing comprehensive ongoing reconnaissance across the entire IT ecosystem from an attacker's point of view.

EASM is also able to contextualize assets – meaning it can automatically attribute them to the business entity that owns them – and can prioritize the risks that assets pose.

External Attack Surface Management was first identified as a market category by Gartner in March 2021 and then included in the 2021 Hype Cycle for Security Operations. As Gartner defines it, EASM describes a set of products that help organizations in identifying risks coming from internet-exposed assets that may be unknown to the organization and may contain unknown vulnerabilities. EASM is seen to be expanding into aspects of BAS, digital risk protection services (DRPS), and Security Rating Services (SRS) as Gartner noted in their subsequent "Quick Answer: What is the Difference Between EASM, DRPS, and SRS?" on February 21, 2022.

How Does EASM Measure Risk?

EASM focuses on identifying critical risks on Internet-exposed assets that can lead to breaches.

EASM solutions begin with the automatic, external discovery of assets – from the same perspective an attacker would have – rather than scanning a catalog of known assets for missing patches or misconfigurations. EASM is also able to contextualize assets – meaning it can ***automatically attribute them to the business entity that owns them***.

EASM products also continuously perform automated and active security testing on all externally exposed assets in the organization's IT ecosystem to identify changing risk posture and prioritize risks that need to be remediated immediately.

How Does EASM Reduce Cost?

While any cybersecurity solution helps organizations reduce business risk, industry- leading EASM solutions are implicitly designed to help organizations reduce the total cost of risk management by assisting with measurement, communication and decision-making around risks. EASM enables security teams to measure risk accurately, communicate risk effectively and optimize risk management. While all EASM solutions enable organizations to efficiently discover "unknown unknowns," the leading EASM products also understand asset business context, assess assets' security continuously and consistently and decide which high-priority risks need to be addressed immediately and which risks are to be transferred or accepted.

The Reality: EASM and BAS

Let's take a closer look at the similarities and differences between their capabilities:

> **EASM automatically identifies risk in subsidiaries or other entities related to the organization, whereas BAS won't unless (a) those environments are known and (b) BAS is deployed in those locations.**

- **EASM doesn't need to be configured where to look,** whereas BAS only tests known security products within predefined IP ranges. EASM starts with business entity identification and also performs externally-exposed asset discovery, asset contextualization and testing, and risk prioritization on a ***global*** scale.

- **EASM evaluates risks broadly, whereas BAS conducts focused tests,** simulating specific threats and known attack sequences. This means that EASM can uncover risks that lie outside of BAS's purview while also including the risks that'd be tested by a BAS.

- **EASM both identifies and prioritizes risks,** whereas BAS lacks the broader context that would make comprehensive prioritization possible. For this reason, BAS can become one more data source in a world where many tools and telemetries are competing for security teams' attention.

- **EASM is non-intrusive,** whereas BAS products require that agents and/or virtual machines be deployed in various places across your environment. These "attacking agents" conduct active testing sequences to probe security assets for gaps and exploitable vulnerabilities. BAS is noisy by design; these products are intended to trigger alarms and create evidence.

- **EASM automatically identifies risk in subsidiaries or other entities related to the organization,** whereas BAS won't unless (a) those environments are known and (b) BAS is deployed in those locations. If operators don't know about a part of the company, BAS won't be able to investigate it. EASM solutions can assess the acquisition target, along with its acquisitions, connected partners and subsidiaries.

In Summary

Breach and Attack Simulation (BAS) is a component of security validation. The question BAS attempts to address seems simple: How do you ***validate your security controls*** in a way that's automated and continuous without breaking the bank? For that use case, BAS works quite well – assuming you understand where you need to train its sights and can afford to spend time and effort configuring it.

If the concept of "attack simulation" is why BAS captured your attention and you're actually looking to prevent attacks altogether, it's likely you want a solution that can ***effectively measure risks across all assets in your environment***, communicate risks to practitioners, and achieve all of this automatically and continuously. If that's the case, it's clear that EASM is what you're looking for, and need to invest in first.

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