WHITE PAPER

Benefits of ASM in Cybersecurity Strategy

Gain visibility, prioritization, and offensive perspective on dynamic environments.

praetorian

Stay a step ahead of attackers using Attack Surface Management.

Enterprise security programs face an uphill battle that requires constant vigilance over an **ever shifting environment with essentially no margin for error**. In contrast, attackers can bide their time and try endless permutations of attack vectors with the certain knowledge that they only need to find one golden opportunity. Attack Surface Management (ASM) is an essential component of mature security strategies because it provides the visibility, prioritization, and offensive perspective necessary to minimize business risk across digital environments.

Visibility

Network infrastructure has come a long way since the early days of static, monolithic applications that only received updates once or twice a year. Now, standing up a brand new asset takes seconds and code pushes occur multiple times a day. **The environments security teams must protect do not look the same from one day to the next.**

Further complicating matters is the phenomenon of Shadow IT. These cloud-based assets exist without the knowledge of an organization's IT and security teams. Vulnerability scanners never scan them because they are not listed as assets. How can security teams manage what they do not measure?

Visibility of the full attack surface, therefore, is crucial to understanding the true risk to an enterprise. An effective ASM service can help identify your shifting assets–including the Shadow IT–and monitor them continuously. Yet, internet exposures are only part of the ASM picture.

In 2022 JupiterOne conducted a study of over 1,270 organizations with 210 million cyber assets between them. They found that on average only "0.2% of the attack surface has a first-degree relationship to the public internet." Their corollary finding was that 99% of high-risk assets are only two to six degrees removed from the public internet. Efforts to increase attack surface visibility must account for both of these phenomena, in addition to unknown assets.

And, as we already mentioned, that attack surface is constantly changing. Human monitoring by internal teams at an enterprise scale simply becomes cost prohibitive, but ASM offers a solution.

! The entirety of an enterprise environment constitutes the organization’s attack surface, from the places touching the internet inward along all the connections that branch from each exposure.

Prioritization

Attaining true visibility of organizational assets and monitoring them all continuously exacerbates an existing challenge for security teams–that of prioritization. Simply put, lots of constantly changing assets means lots of vulnerabilities. The organizations that participated in the JupiterOne study had an average backlog of 130,000 vulnerabilities each. No organization has the financial or human resources to address every single finding equally, so they must prioritize.

Historically, the cybersecurity industry has relied on Intel and CVSS for guidance in prioritizing vulnerabilities. Yet attackers have demonstrated exploits that circumvent the key indicators those frameworks emphasize. If we take a step back and think about the ideas we have already laid out, this makes a lot of sense. The most effective way (and possibly most efficient) for an attacker to find their golden opportunity is to avoid the highly defended vectors on which organizations typically focus.

Attackers also move alarmingly fast to identify and exploit weak spots in an organization’s perimeter. Palo Alto Networks’ Unit 42 conducted a project that involved setting up 320 honeypots across four types of applications, and among the data they collected was the time from honeypot launch to initial compromise (see Figure 1).

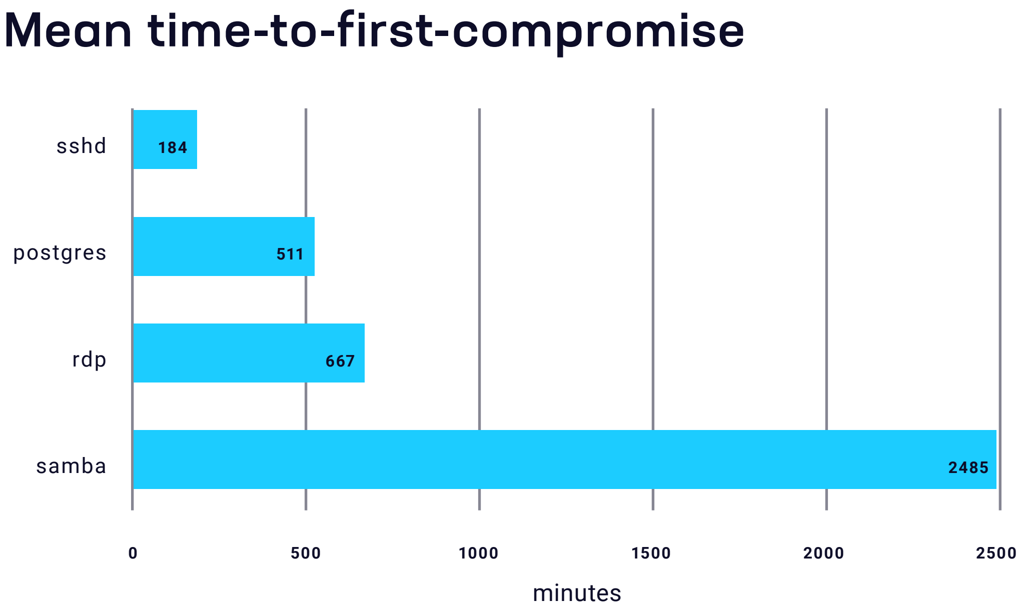

Figure 1: Mean time-to-first-compromise of Unit 42’s 320 honeypots. Note that the unit of time is minutes

Given the rapidity with which attackers can find and exploit new vulnerabilities, we see a clear need to prioritize based on external accessibility. If an attack surface is composed of relatively few exposure points, but those lead directly to high-value assets as JupiterOne found, **the key is to mitigate any internet-facing vulnerabilities first and foremost. If the perimeter looks robust, then the branches and connections that comprise the majority of the attack surface can take priority based on their degree of removal from the internet.**

The task of prioritizing vulnerabilities in an attack surface therefore requires an ongoing heavy load of analysis that even most enterprise organizations cannot sustain internally. Incorporating an ASM service can resolve this challenge.

Offensive Perspective

We have spent a fair portion of this piece discussing the attacker point of view, and that was intentional. Attack surfaces are complex and changeable, which plays to an attacker’s advantage. **For truly effective security, organizations must have some way**

of evaluating their environments from an offensive perspective. This is the best way to recognize where their security teams' defensive mindset has led them to overlook a novel attack vector.

In traditional security penetration testing, the scope of the project limits the testers to a specific application or silo of the network. This is efficient from a compliance perspective, of course, but attackers have no such limitations. Attackers' golden opportunities might occur via a "low-risk" internet-exposed vulnerability. Exploiting that weakness then could provide the attacker a foothold for lateral movement across the network. As Unit 42 observed, "most of these internet-facing services are connected to some other cloud workloads, [so] any breached service can potentially lead to the compromise of the entire cloud environment."

Organizations that incorporate ASM, on the other hand, can perform open-scope analysis spanning their entire environment. They can notice how assets connect to one another, and which of those connections form the links in a chain between a high-value asset and an internet exposed asset. JupiterOne noted in their report that, "If there is an asset in the graph [or network diagram] with many relationships, it's best to zoom in, analyze those relationships, and understand the context and quality."

In fact, the preponderance of attacks via lateral movement is a key reason why we think a managed service approach to ASM is critically important. The offensive perspective provides necessary context for the visibility and prioritization security programs also get from incorporating an ASM service. At this time, the majority of ASM solutions in the marketplace do not include manual analysis, and so omit a key value proposition that ASM can offer.

ASM for Enterprise Security

The combination of visibility, prioritization, and offensive perspective that ASM brings to enterprise security programs is a game changer. Internal security teams can maximize their impact by focusing on the highest priority remediations, confident that they are monitoring the entirety of their organization's attack surface. Furthermore, when enterprise security programs incorporate ASM to their cybersecurity strategy, they have the assurance that their plans and approach account for the way an attacker perceives their environment.

RESOURCES

"A tacky graph and listless defenders: Looking beneath the attack surface." Henry, Jasmine.JupiterOne. 2022. https://info.jupiterone.com/hubfs/077_Tacky%20Graph%20and%20Listless%20Defenders%20Report_r3.1.pdf

"Observing attacks against hundreds of exposed services in public clouds." Chen, Jay. Palo Alto Networks. 2022. https://unit42.paloaltonetworks.com/exposed-services-public-clouds/