A SANS Spotlight

The SANS Guide to Evaluating Attack Surface Management

Written by **Pierre Lidome**

October 2020

Sponsored by:

Randori

Many organizations spend vast amounts of time and money trying to identify, catalogue and track every asset they have exposed to the internet. With the rise of cloud computing and the rapid transition to work from home, maintaining a perfect inventory of every internet-exposed asset has become an impossible challenge. As a result, organizations are searching for new ways to better manage the risk introduced by these rapid changes.

Attack surface management (ASM) is an emerging category of solutions that aims to help organizations address this challenge by providing an external perspective of an organization's attack surface.

A few statistics that highlight the challenges ASM addresses:

- 83% of new enterprise workloads are hosted in the cloud.[1]
- The number of connected devices has doubled during the past five years to more than 25 billion (see Figure 1).[2]
- 82% of organizations plan to continue supporting work-from-home arrangements post COVID-19.[3]

[1] LogicMonitor, "Cloud Vision 2020: The Future of the Cloud," www.scribd.com/document/403188911/LogicMonitor-Cloud-2020-The-Future-of-the-Cloud-pdf, p. 3. [Subscription required.]

[2] Strategy Analytics, "Global Connected and IoT Device Forecast Update," www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update [Subscription required.]

[3] Gartner, "Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time," www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

An organization's attack surface is made up of all internet-accessible hardware, software, SaaS and cloud assets that are discoverable by an attacker. In short, your attack surface is any external asset that an adversary could discover, attack and use to gain a foothold into your environment.

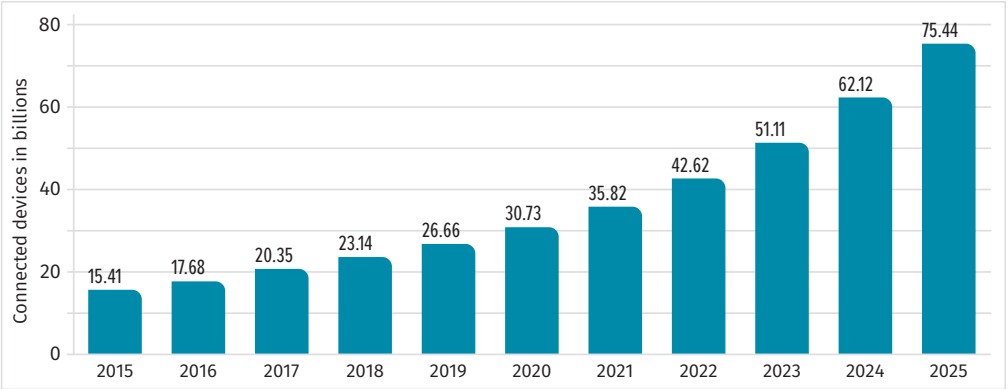

Figure 1. Global Connected Device Forecast[4]

This guide will provide an overview of the benefits and limitations of attack surface management and actionable guidance for organizations looking to evaluate an ASM solution.

Evaluating Attack Surface Management Solutions

ASM solutions help security teams manage risk by providing an ongoing assessment of an organization's external-facing assets and risk profile. Cloud-based and turnkey, ASM solutions provide an adversary's assessment of an organization's discoverable attack surface, enabling teams to better assess the likelihood and impact of weaknesses. Further, they continually monitor the attack surface to help organizations track and identify changes over time. Setup is typically minimal and should begin to provide value to organizations within days.

Common use-cases for adoption of an ASM solution include:

- Identification of external gaps in visibility
- Discovery of unknown assets and shadow IT
- Attack surface risk management
- Risk-based vulnerability prioritization
- Assessment of M&A and subsidiary risk

Leveraged by vulnerability management, threat intelligence and security operations teams, ASM solutions provide an ongoing external view and personalized risk assessment of an organization's attack surface, complementing existing asset management and vulnerability management solutions. ASM solutions are often integrated into larger security workflows through SIEM, SOAR platforms, ticketing systems, and asset management and vulnerability management solutions. Good ASM solutions should provide robust APIs or integrations to enable these workflows.

[4] Strategy Analytics, "Global Connected and IoT Device Forecast Update," www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update [Subscription required.]

As you evaluate vendor offerings, SANS recommends dividing your requirements into two distinct but related categories:

- **Product requirements—**How well do the product features and capabilities meet the functional technical requirements defined by the organization? For example, what techniques does the ASM solution use to discover external assets, including cloud and IPv6 assets?
- **Operational requirements—**How well will the product align with the operational needs and requirements of the organization, including ease of deployment, breadth of coverage, and interoperability with existing security and asset management infrastructure?

Product Requirements

Your ASM solution must have three key features: automated discovery, continuous monitoring and risk-based management.

Automated Discovery

The purpose of the ASM solution is to automate the discovery of your assets. There should be no need to provide IP address ranges or other asset information to get started. The ASM solution must have an advanced algorithm capable of building a map of your assets with minimal input and limited false positives. Ideally, just your domain name should be sufficient.

ASM solutions should generate a risk score for each asset, combining the ASM provider's external threat assessment with user-provided information on relative business value, impact and remediation status.

From there, the ASM solution must:

- Discover internet-exposed assets (both IPv4 and IPv6)
- Support cloud asset discovery
- Enumerate services running on these assets
- Enable organizations to import known assets not automatically discovered

Each ASM solution is likely to have different techniques to achieve the discovery phase. In general, however, you should expect them to leverage whois, passive DNS and network registration data to identify associated network ranges and domains. They should then scan discovered assets for open ports, analyze service banners, and analyze SSL certificates to identify assets and the services they are running.

ASM solutions should include some ability to discover cloud assets and include functionality to limit the noise created by dynamic infrastructure (rotating IPs, dynamic DNS). Be sure to thoroughly test your ASM solution for this functionality. Further, ASM solutions should enable organizations to import cloud ranges or asset lists to ensure monitoring of cloud assets not automatically discovered by the system.

Continuous Monitoring

Assets will be added and removed at various times. The ASM solution must be able to detect these changes by frequently scanning the estate. When an asset is removed, the ASM solution should maintain the information in the database for historical purposes. Again, with the dynamic nature of the cloud, it's important to keep track of what assets may have belonged to your organization in the past.

As your assets are analyzed against potential threats, the ASM solution needs to be able to alert you if a certain threshold is met. An integration with your security operation center or vulnerability management team is essential. We will address this concept in the "Operational Requirements" section later in this paper.

The most difficult requirement for any ASM solution is dealing with false positives. It's inevitable that some assets will be misclassified or perhaps not even belong to your company. The ASM solution must have the means to exclude these assets and manage them at an acceptable level. This problem is particularly difficult for ASM solutions leveraging keyword matching and other rigid methods of assigning ownership.

Risk-Based Management

Not all assets have the same value to your organization. A great ASM solution will enable users to prioritize resources based on additional information, such as business impact and remediation status. With your input, the ASM solution should create and maintain a risk score for each asset that combines the ASM provider's external threat assessment with user-provided information on relative business value, impact and remediation status.

An ASM solution's external threat assessment should take into account the following criteria:

- Applicability to your environment
- Asset criticality
- Known vulnerabilities
- Any known exploitation code
- Required level of sophistication

The value derived from an ASM solution will significantly increase if the assessment is performed from the perspective of the attacker. Remember that many attackers operate as a business and won't build an exploit simply because a new CVE is announced. With that in mind, the score should take into account both the likelihood of compromise and the business impact of the asset.

Table 1 summarizes the features and capabilities you would expect of your ASM solution. Evaluation criteria are also provided to assist you with your decision-making process.

Table 1. Product Requirements

Functionality	Feature	Capability	Evaluation Criteria
Automated discovery	External discovery	The solution requires minimal input to begin the discovery process.	Can the solution automatically discover external assets with little to no configuration?
	Comprehensive discovery	Automatically discover and monitor assets across IPv4 and IPv6 as well as data center and cloud infrastructure.	Does the solution provide broad asset support? Does the solution provide consistent discovery across asset types? Verify the results by taking a sample of known IPv4, IPv6 and external cloud IPs and making sure they were correctly discovered by the platform. *Note: ASM solutions commonly do not identify all known assets during initial discovery. The platform should give you the capability to input IP address ranges to force discovery for more unusual situations.*
	Detailed service discovery	Enumerate detailed service information for discovered assets, including service name and version running on a system. For select services, configuration information also may be available.	Does the solution provide detailed enumeration of discovered services, including name and version, with the capability to check configuration status either directly or through integration?
	Detailed artifact discovery	Collect detailed artifacts from monitored assets for each scan.	Does the solution collect detailed artifacts on each discovered asset, such as SSL certificates, screenshots and banners?
	Path discovery	Show a user how the solution discovered an asset and the artifacts used to assign it to an organization.	Does the solution provide details into how an asset was discovered? This feature is especially important for cloud assets.
Continuous monitoring	Ongoing discovery	Discover new assets in an ongoing manner, outside of initial discovery.	Does the solution provide ongoing asset discovery? Review the vendor's methodology for updating the asset database for frequency of updates and data sources used. Prioritize those with weekly updates and those that rely on external data sources (passive DNS, certificates, network registrations) beyond user-provided data (IP ranges, domains).
	Change monitoring	User can monitor and track changes, such as newfound assets and new or impactful changes in risk, to their attack surface over time.	Does the solution provide dashboards and alerts to enable change monitoring?
	Alerting	Automatically alert users to discoveries or changes on their perimeter.	Does the solution provide email, API and in-app mechanisms to alert on critical changes?
	False positives and noise reduction	Automatically reduce the number of false positives and filter out noise generated by routine changes in dynamic infrastructure.	Does the solution limit noise and present highly confident results? Take a sample of 50 assets and verify that: • The discovered asset does, in fact, belong to your organization • The discovered asset is active and not simply IP space or an unresolvable domain assigned to your organization • The risk assessment of that asset appears valid
Risk-based management	External assessment	Automatically provide an external assessment of risk beyond those provided by vulnerability scanners.	Does the solution leverage a multifactor methodology for external risk assessment, including vulnerabilities, asset prevalence, configuration and local indicators of weakness (expired certs, default pages, test/dev)?
	Impact scoring	User may input information about business value as well as remediation and workflow status into the system to develop a prioritized assessment of risk.	Does the solution include built-in functionality for users to adjust and manage risk based on business value and workflow status?

Operational Requirements

Critical requirements for operationalizing ASM solutions include alerting, enterprise management, and interoperability and integrations.

Alerting

Critical to the success of any ASM solution is its ability to monitor and alert on changes. It is not reasonable to expect users to routinely check the console of a solution to identify new or meaningful changes to an organization's attack surface. Successful operation of an ASM solution must support proactive email-based alerting, including:

- Immediate alerts for critical issues, such as newly discovered exploitable software
- Regular summary notifications of non-critical changes, such as newly discovered IPs or changes in configuration

Enterprise Management

ASM solutions should include basic enterprise management capabilities that enable large teams and organizations to operationalize the solution. Those capabilities should include:

- RBAC (role-based access control) enabling observer-only roles, such as asset owners, to view and comment on critical information in the solution
- Rule-based policy management for triage, status and workflow tracking
- SSO (single sign-on) to manage access to the ASM solution website

Interoperability and Integrations

To gain long-term value from an ASM solution, organizations should look to integrate ASM solutions into existing workflows via integrations and workflow automation. Essential for large enterprises, ASM solutions should provide robust APIs with supported integrations for leading use-cases such as SIEM and ticketing, as well as easy-to-read documentation for development of more custom integrations.

Table 2 summarizes the functionality and operational capabilities you would expect of your ASM solution. Evaluation criteria are also provided to assist you with your decision-making process.

Table 2. Operational Requirements

Functionality	Feature	Capability	Evaluation Criteria
Alerting	Change monitoring	Monitors and tracks changes, such as newfound assets and new or impactful changes in risk, to the attack surface over time.	Does the solution provide dashboards and alerts to enable change monitoring?
	Email alerting	Automatically alerts users to discoveries or changes on their perimeter via email.	Does the solution provide email, API and in-app mechanisms to receive alerts on critical changes?
Enterprise management	RBAC	Supports role-based access control.	Does the solution support RBAC control with permissions for write and read-only users?
	Rule-based management	Supports rule-based and policy-based configurations for ongoing management.	Does the solution provide an easy-to-use interface for policy-driven rule development? Can rules be shared internally across the organization?
	SSO	Supports single sign-on.	Does the solution integrate with your SSO policy?
Interoperability and integrations	API and integrations	Supports third-party integrations and custom development using a provided API.	Does the solution provide a robust API with documentation? Validate API by generating an API token and exporting a list of all IPs. Determine whether the product has demonstrated integrations with external third-party tools, such as API for interfacing with SIEMs.

Comparing ASM Solutions

Comparing datasheets will only go so far. ASM solutions are best compared by doing a proof of concept (POC), which will give you a full understanding of the breadth of their features. When creating a POC, use the tables provided to focus on the features that are most important to you.

After the vendor has completed the discovery phase, focus on the following:

- How did the results compare with your known infrastructure?
- How many assets were found that you didn't know about?
- What was the rate of false positives? Analyze a sample for best results.
- How accurate was the inventory regarding open services and applications?

Now that you have a better idea of your attack surface, focus your POC on your operational requirements:

- Establish a workflow for addressing the highest risk.
- Provide business impact input for critical assets (crown jewels).
- Evaluate the capabilities of the ASM's API to interface with your existing systems.

While ASM solutions focus on the discovery, assessment and prioritization of an organization's external attack surface, they don't test assets for known vulnerabilities. Automated and continuous testing of these assets is a natural progression for organizations as they mature. Leading ASM solutions should offer this additional feature.

Conclusion

Organizations struggling to maintain visibility of their internet-exposed assets or looking for help prioritizing and reporting on external risks will find great value in adopting an ASM solution. Use the selection criteria presented in this guide to help you evaluate and choose the ASM solution that's right for you.

Remember, though, that ASM solutions are not a replacement for a robust and effective asset and vulnerability management program and should be seen as an addition to those processes, rather than a replacement. No organization will be able to find every asset, but well-adopted ASM solutions can help security teams prioritize risks based on what is exposed and enumerable from an adversary's perspective and identify unknown assets missed by traditional vulnerability scanning solutions.

About the Author

Pierre Lidome is a SANS course author and a cyber threat hunter for a large oil and gas company. With more than 25 years' experience in network engineering, firewall management, security services delivery, data management, forensic analysis and e-discovery, he has worked on numerous digital forensics and incident response (DFIR) cases involving vectors such as insider threats and nation-state actors. Pierre's latest projects include migrating on-premises processes and tools to the cloud to efficiently conduct DFIR. He is a member of the GIAC advisory board and holds the GCTI, CCE and CISM certifications.

Sponsor

SANS would like to thank this paper's sponsor: