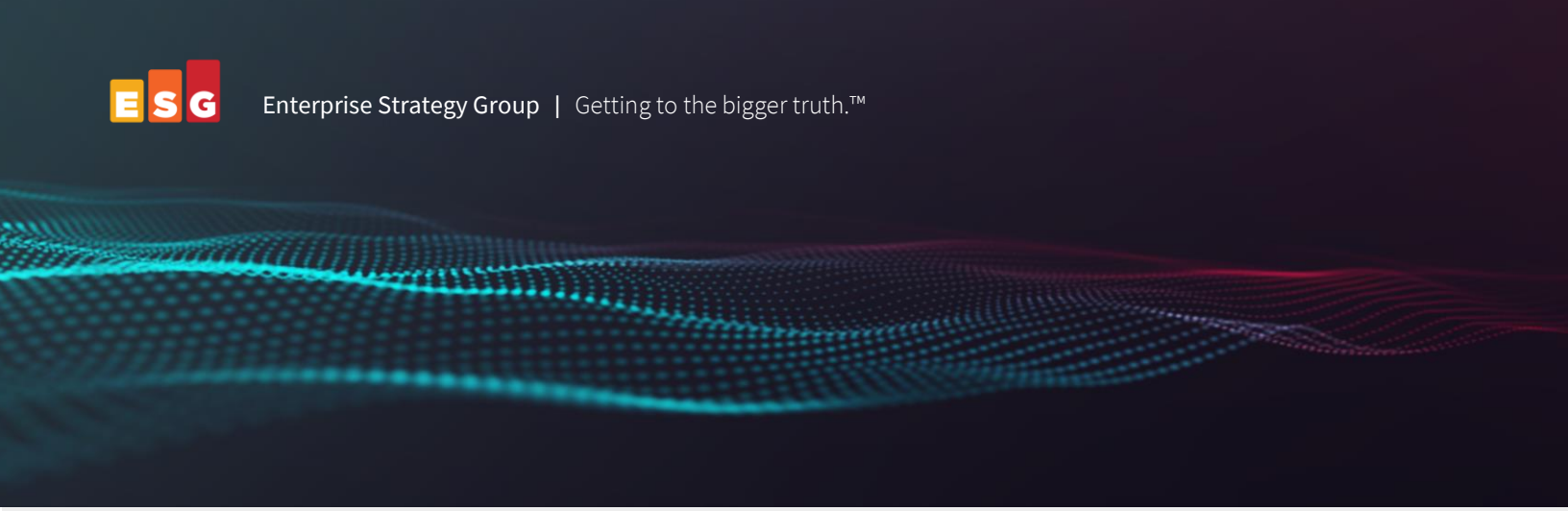


ESG WHITE PAPER

Attack Surface Management (ASM) Buyer's Guide

Things to Consider

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

October 2021

This ESG White Paper was commissioned by Palo Alto Networks and is distributed under license from ESG.

Contents

What Is ASM and Why Is It Needed?

For the purposes of this paper, the term "attack surface" is defined as follows:

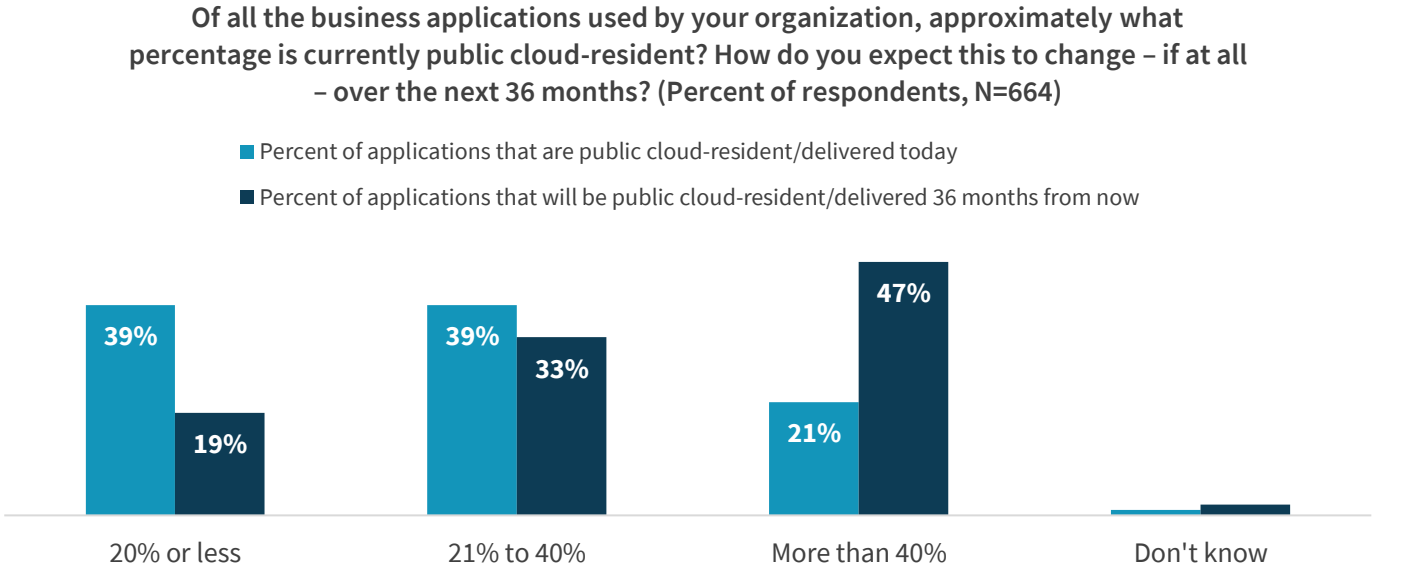
An "attack surface" is defined as the sum of the different internet-facing points (i.e., hardware, software, and cloud assets with fully qualified domain names and/or IP addresses) where an unauthorized user (the "attacker") can try to penetrate a network or compromise a system to conduct some type of cyber-attack.

Based on this definition, attack surface management (ASM) solutions are used by organizations to discover, analyze, categorize, and manage externally facing assets. By doing so, security teams gain an "outside-in" view of their assets, emulating an attacker's perspective of the organization's attack surface. This can help them identify any vulnerable exposed assets that attackers might use as part of a cyber-attack and then take appropriate remediation actions to address these vulnerabilities and thus mitigate cyber-risks.

Why do organizations need ASM solutions and why now? Several important reasons, include:

- Precipitous attack surface growth. Over the past few years, attack surfaces have greatly expanded, driven by things like cloud computing adoption, remote network access, and third-party connections. It is not unusual for an enterprise organization to have hundreds of thousands of internet-facing assets, including servers, subdomains, APIs, digital certificates, code repositories, S3 buckets, etc. Any one of these assets can provide a straightforward path back to corporate networks, data centers, and sensitive data. It is worth noting that attack surface growth is closely correlated with increasing use of cloud computing in all its variations (i.e., IaaS, PaaS, and SaaS). According to ESG research, 21% of organizations claim that more than 40% of their business applications reside in the public cloud today. However, 47% of organizations believe that more than 40% of their business applications will be cloud-resident in 36 months (see Figure 1).[1] This trend toward cloud computing adoption and growth will only make attack surface management more onerous and crucial over time.

Figure 1. Business Applications are Migrating to the Cloud, Increasing Attack Surface



Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

- Incomplete attack surface visibility. At most organizations, security teams use a combination of red teaming/penetration testing and vulnerability management tools to discover and manage their attack surface, but this strategy is deficient in several ways. Vulnerability management systems depend on specific inputs to accurately scan and discover assets, typically across known IP ranges. Unfortunately, this is a small percentage of the externally exposed attack surface and won't help at all when the attack surface also contains thousands of unknown assets across alternative domains and IP address ranges. Penetration testers and red teams provide a better alternative as they tend to use attack surface discovery as part of the reconnaissance phase of their projects. Unfortunately, many organizations only perform penetration testing/red teaming sporadically, so insights about the organizations' attack surface are at single points in time—hardly adequate when a dynamic attack surface is constantly evolving and changing.

- Attacker automation. While security teams struggle with incomplete or infrequent attack surface visibility, attackers aren't burdened by these challenges. Attackers tend to conduct continuous red teaming, use automated tools to discover and assess the attack surface as part of their reconnaissance, or simply outsource attack surface scanning to third-party scanning specialists in the cyber-crime underworld. This puts defenders at a serious disadvantage. For example, recent research from the Palo Alto Networks Cortex Xpanse team reveals that as soon as new vulnerabilities are announced, adversaries rush to take advantage. The report further details that cyber-adversaries typically begin scanning the internet within 15 minutes after Common Vulnerabilities and Exposures (CVE) announcements. Attackers worked faster still upon the Microsoft Exchange Server zero-day vulnerabilities (March 2, 2021), launching scans within 5 minutes of Microsoft's announcement.

CISOs must understand that attack surface management gaps like these can lead to devastating consequences. According to the Palo Alto Networks Cortex Xpanse research, sample scans of enterprise customer attack surfaces revealed an average of two high priority internet exposures per day, including insecure remote access (for example, RDP, Telnet, etc.), database servers, and exposures to vulnerabilities in products like Microsoft Exchange. Any one of these could act as a doorway, ultimately leading to a costly ransomware attack (note: RDP is often used in ransomware attacks) or data breach. For example, a recent article in DarkReading described that stolen RDP credentials can be purchased on the dark web for as little as $10, demonstrating the low entry-level cost for cyber-attacks. Clearly, this is just one of many reasons why organizations need an attacker's view of their attack surface (and organization).

What Are the Most Important ASM Solution Characteristics?

The factors described above combine to set up a monumental mismatch: While attackers use automated tools to scan the attack surface for reconnaissance, many organizations rely on incomplete visibility or periodic testing for attack surface discovery and management. To close this gap, progressive CISOs are turning to ASM.

So, what's the problem? ASM is an emerging technology category with a multitude of vendors and a cacophony of hyperbolic noise. Thus, it can be confusing for security decision makers to understand which ASM product features and functionalities are most important. Therefore, it's important for prospective ASM buyers to determine whether potential products have the right feature set and whether they can gracefully fit into existing security/IT processes and workflows.

In terms of product requirements, ASM solutions should include (see Table 1):

- Automated discovery of all assets. A typical enterprise attack surface is broad and diverse, composed of applications, artifacts, devices, digital certificates, user credentials, sensitive data, services, etc. Leading ASM solutions should be able to discover an exhaustive ASM inventory of internet-facing assets across IPv4 and cloud service providers (CSPs). Unlike vulnerability management systems, ASM solutions should not require a lot of setup or configuration overhead.

Rather, they should use outside-in scanning techniques to perform automated attack surface discovery with minimal input. Aside from discovery alone, ASM solutions must be able to use publicly available sources (i.e., WHOIS, passive DNS, etc.) as well as scanning techniques to discover asset characteristics, applications installed, open ports, and a myriad of other details.

- Continuous monitoring for changes and new assets. Once a baseline of known and unknown assets is established, ASM solutions should continuously scan the internet and public clouds for any moves, adds, or changes. ASM solutions should also scale to be able to capture new and historical data in massive data repositories so security staff can compare new additions and changes to historical usage patterns, looking for anomalies that need attention. The best ASM solutions will present all this data for easy access, query, analysis, and sharing of data within the tool and with other security and IT systems. Finally, ASM solutions should be able to track outside-in communications, monitoring for suspicious communications. SOC teams can then pivot to firewall, network flow, and SIEM logs, cross referencing the ASM data as part of a broader security investigation.

- Attack surface analysis and prioritization. Finding external assets is an important but preliminary ASM task. Once ASM systems become aware of all internet-facing and cloud-based assets, they must be able to classify and analyze them to determine the business context of individual assets and which are most at risk. To be clear, this goes beyond simply categorizing assets based on CVE listing and CVSS scores. Instead, ASM solutions take an adversary perspective on assets, looking at them as targets and determining if each one could be used as part of a broader attack. Armed with this viewpoint, ASM solutions should then present their findings in terms of confirmed/potential problems, report on the depth of any problem, and advise on which remediation actions should be prioritized toward specific high-risk assets. ASM systems should also present the data in the context of the MITRE ATT&CK Framework, aligning issues discovered with adversary tactics, techniques, and procedures (TTPs). This can also help organizations better understand their vulnerabilities and implement the right controls as countermeasures.

Table 1. ASM Technical Requirements

Requirement	Description	Metrics and Capabilities
Automated asset discovery	Ability to create a baseline of all known and unknown assets across the entire internet and public cloud infrastructure	• No setup required • Scale and performance to deliver on time to interview • Low false positive rates • Discovery independent of other security product logs
Continuous monitoring	Ability to monitor for moves, adds, and changes associated with internet and cloud-based assets	• Detect changes continuously • Maintain historical records for future investigations • Present data in an intuitive UI/UX to support user productivity • Monitor and track progress of security posture over time
Attack surface analysis and prioritization	Ability to take an adversary perspective on any asset issues discovered; Ability to prioritize these issues based on their attractiveness for use in cyber-attacks	• Clear descriptions on issues discovered and why they are deemed to be remediation priorities. • Details regarding departments, owners, and stakeholders associated with each asset • Presentation of issues using the MITRE ATT&CK Framework taxonomy

Source: Enterprise Strategy Group

Breadth, depth, details, and performance are all important ASM metrics. This means that security teams should start with a new metric ("time to inventory") for the entire attack surface. The requirement here should be minutes, not hours or days, after a new critical CVE is posted. Depth equates to scanning and monitoring all externally facing assets across the internet and public clouds. Details refer to what ASM reports about asset characteristics, risk, and whether remediation should be considered a priority.

ASM and Operations

While ASM solutions should offer comprehensive technical coverage in the areas outlined above, they must also be designed with IT and security operations in mind. Operations affinity requires (see Table 2):

1. Enterprise functionality. Enterprise security teams can include dozens of individuals while IT departments may have five times as many employees. To accommodate these organizations, ASM tools must be built for individual roles and team collaboration by including functionality for alerting (i.e., using email, collaboration software, etc.), ticketing, data sharing, read-only access, rules-based/policy management, and commenting. In other words, ASM solutions must be built for enterprise needs and support organizational dynamics.

2. Multi-dimensional reporting and use cases for technologists and executives. With all the different roles and organizations using ASM, users will need dashboards, features, and reporting to meet their individual needs. For example, a penetration tester may use ASM as part of her reconnaissance phase, IT operations may want a clear list of high priorities, a threat hunter might need historical records for retrospective investigations, and network security teams may require reporting on internet assets engaged in anomalous/suspicious network behavior. Vulnerability managers and security analysts may also use ASM reporting to build complete asset inventories to bolster the effectiveness of their tools and technologies. In addition to these technical needs, ASM should also provide cyber-risk reports that align with business processes and initiatives. These reports can then be great communications tools as CISOs review cyber-risks with executives and board members.

3. Technology integration and interoperability. ASM is closely aligned with other processes like asset management, vulnerability management, risk management and mitigation, etc. This means that ASM can add tremendous value if it integrates with a variety of technologies like asset management systems, CMDBs, and vulnerability management systems. ASM data can also be helpful in threat investigation technologies like EDR, NDR, XDR, and SIEM, as well as case management, SOAR, and ticketing systems. Aside from strong development support (i.e., open/documented APIs, open source libraries, code repositories, etc.), leading ASM solutions will have established integrations with common security and IT operations tools, delivering a strong out-of-the-box ROI.

4. Remediation guidelines. While identifying high-risk vulnerabilities is an ASM requirement, strong solutions will take an additional step by providing clear and concise remediation guidelines. Based on their priority, remediation guidelines can then be operationalized through workflows, runbooks, and tools for process automation. To support other security initiatives, remediation steps may also be aligned with the MITRE ATT&CK Framework and various regulatory compliance mandates.

To maximize the operational benefits of ASM, CISOs should map prospective use cases to existing processes, workflows, and technologies and ask questions like: Could ASM make these processes more thorough? Could it bolster security? Are there opportunities to use ASM outputs as inputs into tools and processes? Can we use ASM data to automate processes for remediation and risk mitigation? Having an initial perspective on ASM capabilities will help organizations determine the best product fit for ongoing and future operations.

Table 2. ASM Operational Requirements

Requirement	Description	Metrics and Capabilities
Enterprise Operations Functionality	Ability to use ASM across different processes, roles, and organizations	• Role-based access control • Read-only access • Role-based dashboards and templates • Multiple alerting methods
Multi-dimensional reporting and use cases for technologists and executives	Technical reports/use cases for IT and security personnel; Executive-level reports for CISOs, executives, and corporate boards	• Templatized and custom reporting • Simple data query capabilities • Automated report generation • Executive-level summary reports
Technology integration and interoperability	Ability to integrate with a large variety of security and IT operations systems, like asset management, case management, CMDBs, SIEM, SOAR, vulnerability management, etc.	• Well-documented APIs • Developer support • Ecosystem of integration partners
Remediation guidelines	Clear and concise instructions for risk mitigation presented based on the priority of each known issue	• Intuitive risk prioritization model • Specific detailed remediation instructions • Ability to customize and share instructions • Ability to operationalize instructions through tools integration • Alignment with MITRE ATT&CK • Alignment with regulatory compliance requirements

Source: Enterprise Strategy Group

Other Evaluation Considerations

Like any enterprise solution, CISOs will want an understanding of any ASM vendor's team, financing, customer base, and roadmap. Aside from these general concerns, ASM product evaluations should also assess:

- Ease of implementation and use. ASM solutions should not require complex setup or data input. Rather, ASM solutions should be able to deliver fast time to value with minimal or no input at all. Upon deployment, leading ASM solutions should find misconfigured or unknown assets almost immediately. Furthermore, ASM solutions should offer an intuitive UI/UX that delivers value to the entire security and IT staff—from entry-level employees to "C-level" executives.

- Data accuracy. Organizations should spend ample time assessing the accuracy of each ASM solution they test. Some will find more external and cloud assets but be prone to high false positive rates, while others will deliver an incomplete inventory or minimal details about the assets discovered. Still other solutions will provide "black box" risk scoring with limited information about what inputs it analyzes to calculate risk scores. Unless these solution attributes

can be tuned for accuracy with minimal effort, they should be eliminated from consideration. Leading ASM solutions will be accurate, comprehensive, and easily customizable. CISOs should be diligent and cast a wide net to find the product that offers all three of these attributes.

- ROI. This is a bit tougher to calculate, but there are a few questions and answers worth considering. Can an ASM solution help an organization discover misconfigured or unknown assets? Can it accelerate this process and, if so, by how much? Can it continually discover new internet-facing and cloud-based assets faster and more accurately than current methodologies? Can it help prioritize or automate remediation tasks? Can it improve vulnerability management processes and/or support penetration testing/red teaming exercises? Can it help mitigate cyber-risk? While the answer to each question is likely "yes," CISOs should task analysts with calculating a dollar value for each one. These savings alone should not only justify an ASM purchase but also be used to measure its impact over time.

The Business Case

A robust ASM solution can be leveraged by multiple teams within an organization to address several use cases. ASM solutions under consideration should be able to address multiple use cases to justify an investment.

VM and SOC Team: Traditionally, most organizations can capture the most benefit by deploying an ASM solution within their VM and SOC teams first. Teams dealing with asset management, certificate lifecycle management, and incident response can become more efficient and reduce their MTTR & MTTD from having granular and comprehensive visibility into their attack surface.

Cloud Security Team: Traditional VM scanners fail in the cloud since they are IP-based, and cloud assets are constantly hopping IP addresses. This results in low scan coverage and an inefficient VM infrastructure. However, organizations can also leverage an ASM solution to improve their cloud scanning coverage and, as a consequence, improve the ROI on their existing cloud vulnerability management infrastructure investment.

Compliance and Audit Team: Comprehensive and complete visibility is the bedrock of any robust cybersecurity practice. Organizations can leverage their complete asset lists from ASM tools to reduce audit duration and save costs on third-party audit and compliance processes.

M&A and Third-party Risk Teams: Most mature organizations involved in frequent mergers and acquisitions can use an ASM solution to gauge the cyber-attack surface of a target company and price it into their acquisition process. Post-acquisition, ASM solutions help an organization to rapidly integrate the new subsidiary into their network without creating any accidental exposures.

Organizations exploring an ASM solution should ensure that they have integrations that span beyond security into auxiliary compliance and merger and acquisitions use cases to ensure they can get the most out of a single solution and to justify the investment and make a business case to their board.

Consider the following checklist when buying an ASM solution:

Has the solution demonstrated the ability to scale the size of the organization's network	Y/N
Does the solution use multiple sources to comprehensively discover and automatically attribute assets that belong to an organization?	Y/N
Is the false-positive rate for the assets discovered and attributed by the ASM solution acceptable? (>99% accuracy is ideal)	Y/N
Can the solution help identify a wide range of issues like exposed RDP, Telnet, expiring/self-signed certs, etc.?	Y/N
Can the solution integrate with your cloud security solutions and identify advanced issues like co-located assets?	Y/N
Does the solution have strong out-of-the box policies and options for building custom policies?	Y/N
Does the solution help uncover both unknown assets in your network and unknown communications to your network?	Y/N
Can the solution seamlessly integrate with your existing SIEM/SOAR solution?	Y/N
Does the solution provide dashboards or executive-level reporting?	Y/N
Does the solutions provide a dedicated support team and not just documentation or email support?	Y/N

The Bigger Truth

This paper provides some analysis and recommendations around ASM that should help organizations find solutions that meet their individual needs. While this alone could satisfy some business and technical requirements, ASM programs should extend beyond data collection, processing, and analysis alone. To truly create a successful ASM program, organizations should:

- Approach ASM with a plan. Obviously, ASM solutions can provide visibility into the ever-changing world of internet-facing and cloud-based assets, and this alone should help security organizations reduce cyber-risk. Since ASM can do a lot more than improve visibility, however, CISOs should approach ASM with goals, KPIs, and metrics for assessing near- and long-term success. For example, organizations should baseline the current mean time to inventory their existing attack surface and then strive for continuous improvement using ASM. Once ASM practices are established, CISOs should plan for creative ways to use and benefit from the data.

- Get everyone involved. As described above, ASM data can be used in multiple areas like asset management, third-party risk management, application development, IT operations, etc. These use cases extend ASM to other departments for streamlining and automating processes, so it's important to get buy-in and cooperation from groups like risk management and IT operations at the onset of any ASM project. CISOs will also want to prep business executives and the corporate board by educating them on how ASM can be used to reduce cyber-risk and accurately measure future progress.

- Focus on areas of high risk and then make incremental progress. Once ASM is deployed, it will likely find lots of unknown, unmanaged, or misconfigured assets and deliver a priority list for remediation. Before proceeding, however, CISOs should make sure that ASM priorities align with their organization's business-critical systems and processes. Associating ASM and business priorities may take a bit of customization or integration with other systems like vulnerability management or CMDBs. Once this alignment occurs, organizations should establish asset categories and service levels for remediating high-priority vulnerabilities, measure progress, and strive for continuous improvement.

- Use ASM to establish standards. ASM tools will likely uncover some sloppy practices, insecure configurations, and human error. Smart organizations will look for patterns of misuse like inadequate password management, overly permissive administrator accounts, poor certificate management, etc. These patterns may open an opportunity to fine-tune corporate policies and establish best practices. For example, after uncovering multiple security vulnerabilities around S3 bucket configurations, organizations can create security policy requirements like establishing global S3 bucket access rules, ensuring that S3 buckets use a DNS-compliant naming convention, and confirming that S3 changes follow an established change management procedure.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188