kriativ.tech

Edição Nº 11 – 14-12-2025
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2023-06-97

Attack surface management (ASM): Strategic pillar of modern cybersecurity operations

Ivo Ricardo Dias Rosa

Invited Assistant Professor
ISTEC - Instituto Superior de Tecnologias Avançadas
Lisbon, Portugal
ivorosa@gmail.com | ivo.rosa@my.istecpt
ORCID: 0000-0002-9612-4491

Abstract: *In an increasingly dynamic digital landscape, the expansion of the attack surface has become one of the foremost challenges for modern cybersecurity. Traditional perimeter-based defense models are no longer sufficient in the face of distributed digital assets, widespread cloud adoption, and the proliferation of connected devices. In this context, Attack Surface Management (ASM) emerges as a strategic pillar, enabling organizations to adopt a proactive stance in identifying, monitoring, and mitigating cyber risks. This article explores the core principles of ASM, outlining key categories of the attack surface and addressing both EASM (External Attack Surface Management) and CAASM (Cyber Asset Attack Surface Management) approaches. Strategic benefits—such as continuous visibility, integration with Security Operations Centers (SOCs), and risk-based prioritization—are discussed, along with technical and operational challenges tied to ASM implementation. Practical use cases and performance indicators are presented to support effective exposure management. Ultimately, ASM is positioned as a cybersecurity maturity accelerator, essential for building a resilient and adaptive security posture aligned with regulatory demands and business continuity imperatives in an ever-evolving digital ecosystem.*

Keywords: *Attack Surface Management (ASM), External Attack Surface Management (EASM), Shadow IT, Threat Intelligence, Risk-Based Prioritization, Cybersecurity Maturity, CI/CD Security, Security Operations Center (SOC), Exposure Management, Regulatory Compliance.*

I. Introduction

In an increasingly complex, distributed, and ever-evolving digital ecosystem—where traditional perimeters have disappeared—the growing technological complexity and the escalation of cyberattacks demand new defense approaches. Attack Surface Management (ASM) is emerging as a strategic pillar of modern cybersecurity operations. The widespread adoption of cloud computing, the proliferation of connected devices, and the agile development of applications have all contributed to expanding organizations' attack surfaces often beyond the full visibility of security teams. [1]

In this context, integrating ASM into security operations, particularly within Security Operations Centers (SOCs), becomes critical to ensuring a proactive and resilient security posture. The proliferation of digital assets, the adoption of hybrid and complex environments, and the acceleration of digital transformation call for a continuous, automated, and risk-oriented approach. It is within this framework that ASM solutions gain strategic relevance. [2]

II. State of the Art

What is ASM?

Attack Surface Management (ASM) is a continuous and proactive process of discovering, inventorying, classifying, and monitoring digital assets — both internal and external — with the goal of continuously reducing an organization's exposure points that may represent potential attack vectors exploitable by malicious actors [1, 2].

Unlike traditional approaches that focus on the organization's internal perimeter, ASM observes the ecosystem from an attacker's perspective, analyzing what is visible and exploitable from the outside [3]. This approach provides a more realistic view of vulnerabilities and weaknesses, promoting an adaptive and risk-based defensive posture [4].

Categories and Approaches

There are two main categories:

- **EASM (External Attack Surface Management):** focuses on identifying internet-exposed assets such as servers, web applications, domains, IPs, APIs, cloud services, IoT devices, digital certificates, and public data [5].
- **CAASM (Cyber Asset Attack Surface Management):** complements internal visibility by integrating data from tools such as EDR (Endpoint Detection and Response), CMDB (Configuration Management Database), and vulnerability scanners, providing a consolidated view of assets and associated risks [6].

These approaches should be integrated with solutions like CSPM (Cloud Security Posture Management), UEM (Unified Endpoint Management), and DevSecOps pipelines, leveraging automation and API-driven interoperability to enable a coordinated and effective response [7, 8].

ASM vs. Security Ratings: Complementary Approaches with Distinct Purposes

Although often mentioned in the same context, ASM solutions and Security Ratings have distinct natures and purposes. Both can coexist within a comprehensive cybersecurity strategy [9], but it is essential to understand their differences to ensure effective implementation aligned with organizational goals.

Characteristic	ASM	Security Ratings
Purpose	Discovery and operational mitigation of real-time exposures	Reputational assessment and external benchmarking
Frequency	Continuous and near real-time	Periodic, with updates on defined cycles
Action	Remediate exposures and reduce the attack surface	Identify risks associated with exposed services and third parties (suppliers, partners)
Target Users	Technical security teams (SOC, SecOps, DevSecOps)	Risk management, compliance, procurement, and audit teams

Table 1 – Comparison between ASM and Security Ratings approaches, highlighting their distinct purposes, operational characteristics, and target users.

While ASM focuses on active and operational visibility of an organization's own attack surface, enabling immediate corrective actions [10], Security Ratings provide an external and reputational perspective, useful for assessing third-party risk or for market benchmarking purposes [11].

Integrating both approaches can enhance a more holistic view of the security posture, combining tactical action with strategic insight.

Attack Surface Categories

To better understand the scope of ASM, it is helpful to segment the attack surface into five main categories:

- **Digital**: presence on social media, the dark web, and compromised assets that impact reputation [12].
- **External**: websites, domains, public IPs, certificates, and APIs accessible via the internet.
- **Cloud**: assets in IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service), and serverless components, often created quickly and without centralized visibility from IT or security teams [5].
- **Internal**: on-premises assets, including IT, IoT (Internet of Things) devices, and OT (Operational Technology) equipment [13].
- **End-user**: endpoints and mobile devices often beyond the direct control of the organization [14].

III. Discussion

Strategic Benefits and Challenges in Adopting ASM Solutions

The adoption of Attack Surface Management (ASM) solutions brings a range of strategic benefits but also involves important challenges that must be considered. Among the key strategic benefits is the continuous and comprehensive visibility over digital assets, including those that are not inventoried or are managed outside official channels (shadow IT) [15]. This visibility is essential for maintaining an up-to-date and controlled attack surface. Additionally, risk-based prioritization allows organizations to align mitigation efforts with potential business impact by integrating data on vulnerabilities, organizational context, and active threats [16].

Another strong point is the integration with threat intelligence sources, which enriches analysis with information from the dark web, ongoing malware campaigns, and other external sources [17]. This contextualization capability is fundamental for more effective and informed responses. At the same time, ASM helps reduce the attack surface by identifying exploitable vulnerabilities and malicious activities such as automated scans, phishing attempts, or the use of compromised credentials [18].

Operational integration with Security Operations Centers (SOCs) is also critical, feeding tools such as SIEM, SOAR, and EDR with actionable data, leading to a reduction in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) [6, 19]. From a regulatory perspective, these solutions facilitate compliance with frameworks such as NIS2, ISO 27001, NIST, GDPR, among others, by providing structured inventories and reports [20].

In agile development environments, ASM can be integrated into CI/CD pipelines, promoting a shift-left security approach that detects and mitigates risks before code is even published. Lastly, ASM serves as a foundational pillar in the Continuous Threat Exposure Management (CTEM) model, supporting dynamic and ongoing threat exposure management [21, 22].

However, the adoption of these solutions is not without challenges. The occurrence of false positives can generate operational noise and divert resources from critical incidents [23]. The technical complexity of integrating with multiple data sources and existing systems requires planning and specialized skills [24]. Moreover, the investment in tools, training, and human resources can be significant. It is also important to emphasize that no solution guarantees full visibility into the digital environment — human validation remains an indispensable element to ensure the reliability of the analysis [25].

Use Cases and Performance Indicators for ASM Solutions

ASM solutions are especially valuable in contexts where visibility and control over digital assets are critical. Common use cases include:

- **Discovery of forgotten domains and shadow IT**, allowing the identification of assets created outside formal management processes that pose significant risks by operating under the radar of security teams [26].
- **Monitoring of unauthorized cloud usage (shadow cloud)**, essential for detecting cloud service instances created without approval or oversight — often used by development teams or independent departments [27].
- **Identification of exposed APIs and outdated software**, which may represent vulnerable entry points for malicious actors, especially when undocumented or not properly maintained [28].
- **Asset assessment in mergers and acquisitions**, where it is crucial to gain a clear and rapid view of the inherited attack surface to mitigate risks before system integration [29].
- **Validation of incomplete system decommissioning**, ensuring that discontinued assets are not unintentionally still accessible and exposed to the internet [30].

To ensure effective attack surface management, it is essential to monitor metrics that reflect the progress and effectiveness of implemented actions. Some of the most relevant KPIs include:

- **Mean time to detect new assets**, measuring how quickly the solution identifies changes in the attack surface [31].
- **Percentage of assets with controls applied**, indicating the level of effective security coverage over identified assets [32].
- **Mean exposure time**, evaluating the interval between the detection of a vulnerability and its remediation [33].
- **Percentage of discoveries integrated into the CMDB**, reflecting the alignment between operational visibility and asset management systems [34].
- **Percentage of unknown assets identified**, a critical metric for assessing the solution's effectiveness in discovering shadow IT and undocumented assets [35].

Recommended Maturity Level for ASM Adoption

The adoption of ASM solutions should be seen as an advanced step in the cybersecurity maturity journey. Although the benefits of ASM are significant, their effectiveness depends on the existence of a solid foundation of processes, tools, and organizational integration.

Ideally, an organization should consider implementing ASM once it has achieved a maturity level that includes:

- A reasonably controlled asset inventory, with visibility over key systems, applications, and exposed services [36];
- Functional integration between IT and security teams, ensuring that the discovery of new assets or infrastructure changes are quickly communicated and addressed [37];
- Consistent operation of essential tools such as EDR, CMDB, and vulnerability scanners, which provide the data necessary to feed and contextualize ASM findings [6, 38].

Organizations in early stages of maturity should focus on consolidating these foundations before investing in ASM. Without a minimally structured base, ASM may generate a high volume of data with no adequate response capacity, compromising both return on investment and operational effectiveness [39].

Thus, ASM should be seen as a maturity accelerator — not a starting point. Its adoption should be strategic, aligned with the organization's capacity to interpret, integrate, and act upon the data these solutions provide [40].

IV. Conclusion

Attack Surface Management (ASM) represents a paradigm shift in modern cybersecurity. By adopting the attacker's perspective, it enables realistic and actionable visibility, strengthening the defensive posture through context, risk, and automation [41]. ASM is not just a technical map but an adaptive defense system with direct impact on operational resilience and business continuity.

For executive decision-makers, ASM is an essential tool to communicate risk in business language, justify investments, and position cybersecurity as a driver of competitiveness, trust, and strategic leverage [42].

In an ever-evolving digital landscape, investing in ASM means investing in the ability to anticipate, adapt, and withstand [43].

V. References

[1] M. C. Montoya, D. C. Yates, and P. N. Otto, "Managing Your Digital Attack Surface," *ISACA Journal*, vol. 4, pp. 1–5, 2021.

[2] Gartner, "Market Guide for Attack Surface Management," *Gartner Research*, 2021.

[3] S. Adair and C. Hessel, "Seeing Your Organization Through the Eyes of an Attacker," *Dragos White Paper*, 2020.

[4] ENISA, "Threat Landscape for Attack Surface Management," European Union Agency for Cybersecurity, 2023.

[5] Palo Alto Networks, "Understanding EASM: External Attack Surface Management," *Palo Alto Whitepaper*, 2022.

[6] Rapid7, "InsightVM and ASM Integration Guide," *Rapid7 Documentation*, 2021.

[7] M. Curphey, "DevSecOps and ASM Automation," *OWASP Global AppSec*, 2020.

[8] Trend Micro, "ASM with API-first Security Architecture," *Trend Micro Blog*, 2021

[9] BitSight, "Security Ratings vs. Attack Surface Management: Understanding the Differences," *BitSight Whitepaper*, 2022.

[10] Randori, "Real-Time Visibility with ASM," *Randori Attack Surface Report*, 2021.

[11] SecurityScorecard, "How Security Ratings Complement ASM," *SecurityScorecard Insights*, 2021.

[12] Recorded Future, "Dark Web Monitoring for ASM," *Recorded Future Intelligence Report*, 2020.

[13] Forescout Technologies, "Visibility and Control of OT and IoT Assets," *Forescout Whitepaper*, 2022.

[14] IBM, "Zero Trust and Endpoint ASM," *IBM Security Report*, 2021.

[15] McAfee, "Shadow IT: A Growing Risk," *McAfee Threats Report*, 2020.

[16] SANS Institute, "Prioritizing Risk in Attack Surface Management," *SANS White Paper*, 2022.

[17] FireEye, "Threat Intelligence for ASM," *FireEye Threat Research*, 2021.

[18] Proofpoint, "ASM and Credential Phishing Trends," *Proofpoint Quarterly Report*, 2022.

[19] Splunk, "ASM Data in SIEM/SOAR Workflows," *Splunk Security Essentials*, 2021.

[20] ISO/IEC, "ISO/IEC 27001:2022 - Information Security," *ISO Standard*, 2022.

[21] GitLab, "Shift Left with DevSecOps and ASM," *GitLab DevSecOps Handbook*, 2021.

[22] Gartner, "Continuous Threat Exposure Management: A New Framework," *Gartner Report*, 2022.

[23] Tenable, "Managing False Positives in ASM," *Tenable Blog*, 2021.

[24] Cisco, "ASM Integration Challenges," *Cisco Cybersecurity Series*, 2020.

[25] Forrester, "The Limits of Attack Surface Visibility," *Forrester Consulting*, 2021.

[26] Netskope, "Discovering Shadow IT Assets," *Netskope Cloud Report*, 2020.

[27] Check Point, "Identifying Shadow Cloud Instances," *Check Point Research*, 2021.

[28] OWASP, "API Security Top 10," *OWASP Foundation*, 2023.

[29] Deloitte, "Cyber Due Diligence in M&A," *Deloitte Insights*, 2021.

[30] Bugcrowd, "Zombie Servers and Forgotten Assets," *Bugcrowd ASM Report*, 2022.

[31] Axonius, "Asset Inventory Metrics for ASM," *Axonius Tech Brief*, 2021.

[32] Gartner, "KPIs for ASM Platforms," *Gartner*

Research Note, 2021.

[33] Mandiant, “Measuring Exposure Time in ASM,” *Mandiant Threat Report*, 2022.

[34] ServiceNow, “CMDB Integration with ASM,” *ServiceNow Whitepaper*, 2021.

[35] Qualys, “Unmanaged Asset Discovery in ASM,” *Qualys Whitepaper*, 2021.

[36] NIST, “Cybersecurity Framework Implementation Tiers,” *NIST CSF*, 2020.

[37] ISACA, “Bridging the Gap between IT and Security,” *ISACA Cyber Leadership Study*, 2022.

[38] CrowdStrike, “Feeding ASM with Endpoint Intelligence,” *CrowdStrike Tech Blog*, 2021.

[39] Gartner, “Maximizing ROI from ASM Investments,” *Gartner Strategic Planning Assumptions*, 2021.

[40] Accenture, “ASM Maturity Assessment Framework,” *Accenture Cyber Strategy*, 2022.

[41] Microsoft, “ASM and Adaptive Security Architecture,” *Microsoft Security Blog*, 2022.

[42] World Economic Forum, “Cybersecurity Leadership and Communication,” *WEF White Paper*, 2021.

[43] KPMG, “Cyber Resilience in a Digital World,” *KPMG Security Insights*, 2022.