Innovation Insight for Attack Surface Management

Published 24 March 2022 - ID G00748467 - 11 min read

By Analyst(s): Mitchell Schneider, John Watts, Pete Shoard

Initiatives: Security Operations

Information security teams are responsible for identifying and managing an attack surface across internal and external digital assets. Security and risk management leaders aware of their attack surface can improve their risk posture by prioritizing security hygiene and increasing its visibility.

Additional Perspectives

- Invest Implications: Innovation Insight for Attack Surface Management (24 May 2022)
- Summary Translation: Innovation Insight for Attack Surface Management (10 May 2022)

Overview

Key Findings

- Organizations have to manage a growing attack surface as their technological environments become increasingly complex and dispersed, both on-premises and in the cloud, and involve containers, the Internet of Things and cyber-physical systems. SaaS applications and supply chain touchpoints also present new attack surfaces.
- For every organization, it is essential that any deficiencies of security hygiene are internally visible, so that a strong security posture can be established and maintained. Most organizations lack the capabilities required to validate control coverage and quantify digital and cyber risks effectively.
- New ways of visualizing and prioritizing management of an organization's attack surface are required as enterprise IT becomes more dispersed, owing to the expansion of public-facing digital assets and increased use of cloud infrastructure and applications. Security and risk management leaders can start by aggregating asset and risk context into a platform for visualization of their attack surface.

Recommendations

Security and risk management leaders responsible for managing their organization's attack surface as part of the security operations function should:

- Align their security program to address the threats posed by new technologies and business initiatives by investing in a better understanding of the continuous expansion of their organization's attack surface.
- Create attack surface management (ASM) processes to implement technologies and prioritize risks. Initial efforts should focus on the need for, and deficiencies in, attack surface visibility.
- Match tools and services that provide attack surface assessment (ASA) capabilities to the most important attack surface use cases. ASA capabilities support overlapping, but not identical, types of assets and ASM capabilities.

Strategic Planning Assumptions

By 2026, 20% of companies will have more than 95% visibility of all their assets, which will be prioritized by risk and control coverage by implementing cyber asset attack surface management functionality, up from less than 1% in 2022.

By 2026, 70% of all functionality relating to cyber asset attack surface management, external attack surface management and digital risk protection services will be part of broader, preexisting security platforms, rather than provided by stand-alone vendors, up from less than 5% in 2022.

Introduction

ASM involves a combination of people, processes, technologies and services deployed to continuously discover, inventory and manage an organization's assets. These assets can be both internal and external, and they pose digital risks. This visibility can help reduce exposure that could be exploited by malicious threat actors.

ASA involves the set of tools and services that may be used to achieve ASM.

This research focuses on only the first pillar of exposure management: ASM. The elements of ASM are supported by three main capabilities: cyber asset attack surface management (CAASM), external attack surface management (EASM) and digital risk protection services (DRPS), which are represented by "internal," "external" and "digital risks," respectively, in the first pillar in Figure 1.

Gartner has adopted the National Institute of Standards and Technology's (NIST's) definition of attack surface: "The set of points on the boundary of a system, a system element, or an environment [the assets] where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment." [1]

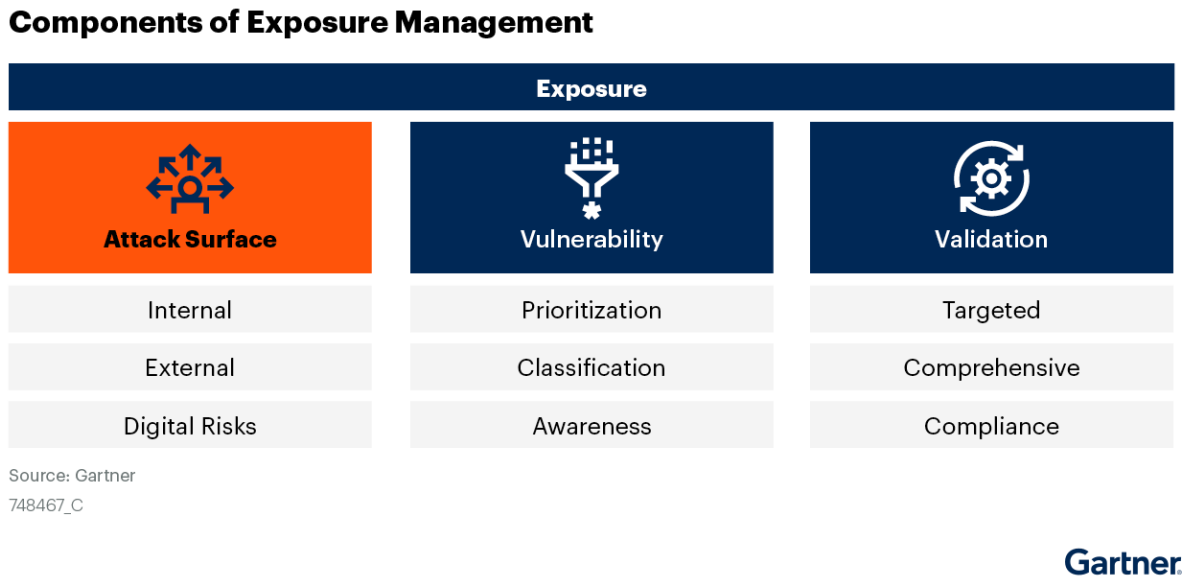
Each pillar of exposure management has its own objectives and answers specific questions that Gartner clients ask, for example:

- "What does my organization look like from an attacker's point of view, and how should it find and prioritize the issues attackers will see first?" The ASM pillar addresses this question.

- "What software is present and what configuration has my organization set that will make it vulnerable to attack?" The vulnerability management pillar addresses this question.

- "What would happen if an attacker carried out a campaign against my organization's infrastructure, how would its defenses cope and how would processes perform?" The validation pillar addresses this question.

Figure 1: Components of Exposure Management



The aforementioned technological capabilities help organizations understand their attack surface by, for example, providing an attacker's view, prioritizing issues that attackers will see first and aggregating asset data for security use cases. But they are by no means the only ones that can help manage an organization's exposure or make this visible. That said, traditional security technologies have capability gaps that may render them inadequate, given recent changes to organizations' environments and the threat landscape. For example, vulnerability assessment (VA) only provides visibility into what an organization designates that the scanning tool should scan (IP addresses, for instance). ASA provides a more comprehensive view of an organization's asset inventory, including unknowns. Some ASA technologies can close capability gaps and can even show where VA is missing scans.

There are ASA technologies in both emerging, innovative markets and established markets. These technologies help organizations assess more of their attack surface and prioritize risks affecting both controlled and uncontrolled digital assets.

Most ASA tools fall into two major categories of capability:

- **Visibility:** Provides a way of widening the definition of what assets are "in scope" and of the risks that security and risk management leaders must help create awareness of and mitigate.

- **Prioritization:** Provides the ability to score risk in a way that can pragmatically assist with identification of the issues that would have the largest impact on an organization.

ASA capabilities complement or overlap with those of other security technologies, such as VA, vulnerability prioritization technology, and breach and attach simulation (BAS) (see Market Guide for Vulnerability Assessment and Quick Answer: What Are the Top Use Cases for Breach and Attack Simulation Technology?).

Description

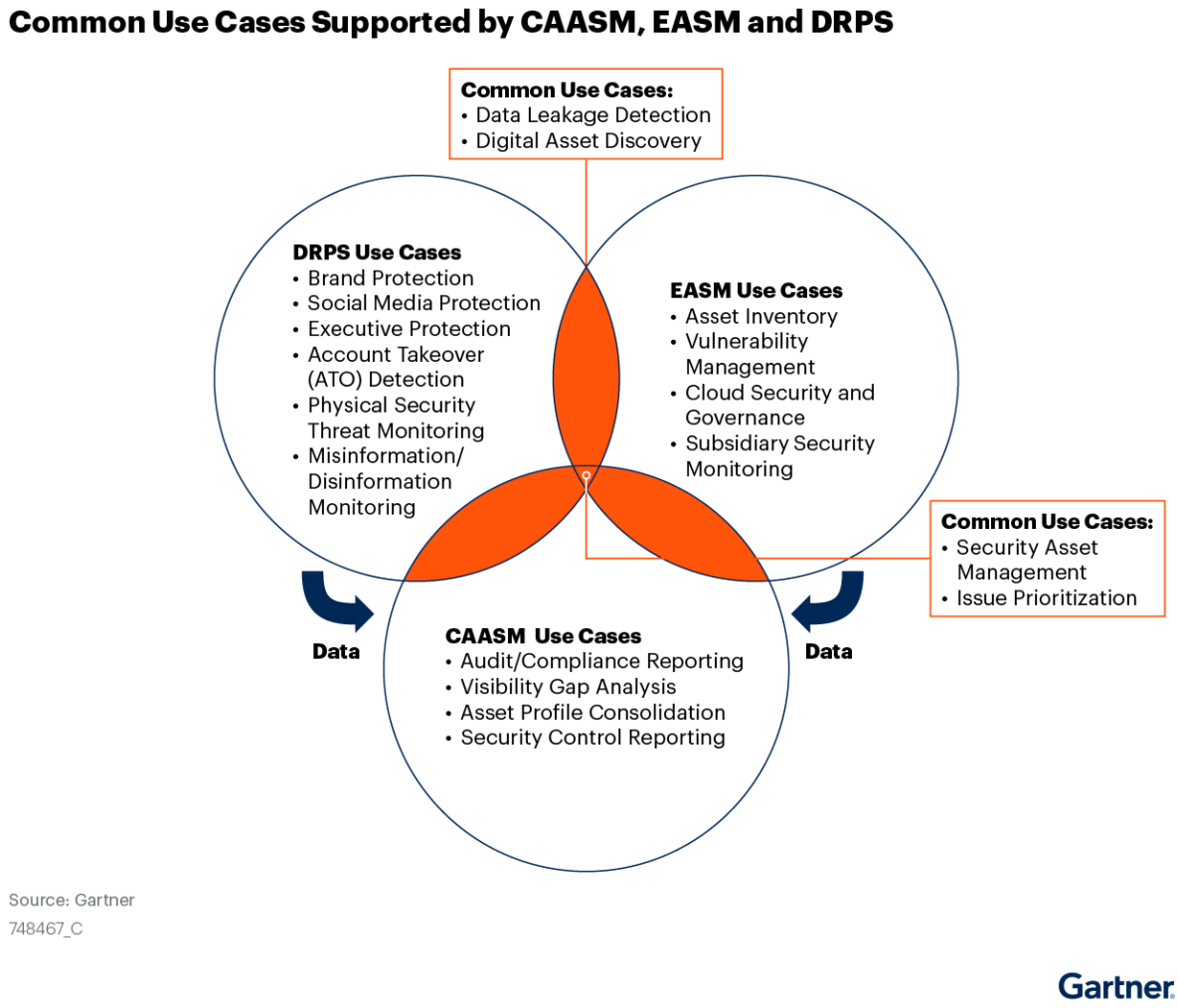
Managing an attack surface involves three emerging areas of technological innovation:

- **Cyber asset attack surface management (CAASM)** focuses on enabling security teams to solve persistent asset visibility and vulnerability challenges. It enables organizations to see all assets (internal and external) through API integrations with existing tools, query against the consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues.
- **External attack surface management (EASM)** uses processes, technologies and managed services deployed to discover internet-facing enterprise assets, systems and associated vulnerabilities, such as servers, credentials, public cloud service misconfigurations and third-party partner software code vulnerabilities that could be exploited by adversaries (see Emerging Technologies: Critical Insights for External Attack Surface Management).
- **Digital risk protection services (DRPS)** are delivered via a combination of technology and services in order to protect critical digital assets and data from external threats. These solutions provide visibility into the open (surface) web, social media, the dark web and deep web sources to identify potential threats to critical assets and provide contextual information on threat actors, their tactics and processes for conducting malicious activity (see Market Guide for Security Threat Intelligence Products and Services).

There is, however, some confusion about these three, owing to the overlap in some of the use cases they support (see Quick Answer: What Is the Difference Between EASM, DRPS and SRS?). EASM has a more technical and operational focus supporting security operations professionals engaged in activities such as VA, penetration testing and threat hunting. DRPS, by contrast, primarily supports more business-centric activities, such as enterprise digital risk assessment, compliance and brand protection. Another important distinction between EASM and DRPS is that the latter typically provides the service overlay, like takedowns. EASM focuses on external assets primarily (and scanning, actively), whereas CAASM focuses on internal assets. In addition, with CAASM, the discovery function works primarily through API integrations with existing tools (passively), whereas EASM uses a range of sources and methods to scan the internet. EASM also focuses on discovering externally facing assets — many of which may be unknown to the organization — whereas CAASM relies on other, already deployed technologies for context and enriches the data being pulled in from those technologies to provide a holistic view of an organization's asset inventory. Moreover, CAASM can reconcile duplicates or inconsistent data, and automate remediation steps to update data, such as data from a configuration management database (CMDB). CAASM is never a source of record, but rather an aggregator of data from other sources. EASM is a source of record and feeds into CAASM for added visibility (see Figure 2).

A good way to navigate the market is to understand that each technology was built to target certain core use cases primarily. Therefore, those core use cases are what each technology is best suited to support.

Figure 2: Common Use Cases Supported by CAASM, EASM and DRPS



Benefits and Uses

- Improving asset visibility enables organizations to avoid blind spots and unmanaged technology (such as “shadow IT”), thus improving their security posture and enabling more comprehensive risk management.
- Understanding potential attack paths toward assets helps organizations prioritize security control deployment and configuration. This, in turn, helps reduce unnecessary exposure to the internet and the public domain, which could be exploited.
- Quicker audit compliance reporting is enabled by more accurate, current, and comprehensive asset and security control reports.
- There is less resistance to data collection and better visibility into shadow IT organizations, installed third-party systems and line-of-business applications where IT lacks governance and control. Security teams need visibility into these things, whereas IT teams may not.
- Actionable intelligence and meaningful metrics are gained that can be tracked over time. These demonstrate the value of making ASM a part of a cybersecurity program.

Risks

- ASA tools are provided primarily by small vendors. In the short to medium term, these vendors may be subject to mergers and acquisitions, which could impact investments in them.
- ASA capabilities are largely a collection of open-source functions, and the barriers to entering this market are low. Large security platform vendors (such as extended detection and response [XDR]) providers may build or acquire functionality to provide a more robust ASA capability for organizations that buy into their larger ecosystem of cybersecurity tools.
- Each ASA technology can be siloed and may create extra overheads in terms of configuration, management and maintenance by trained personnel.
- ASA technologies' capabilities increasingly overlap with those of otherwise complementary markets, such as the threat intelligence, endpoint protection platform, BAS and VA markets. Organizations with adjacent products that provide perceivably similar visibility and risk assessments may struggle to justify the cost of adding ASA technologies.
- Integrations with other tools can suffer from technological limitations (such as a lack of APIs) or from incomplete visibility due to a product's technical limitations or inability to reconcile conflicts and overlaps in asset information.
- ASA technology improves asset visibility through aggregation and reconciliation processes from other systems of record, such as CMDBs, but does not inherently solve poor data quality and granularity issues at the source. Organizations will not succeed if no one bothers to actually manage their technology investments. Security teams must work with source system owners to fix systems of record.

Adoption Rate

Gartner estimates that less than 10% of organizations have adopted one or more ASA technologies to address their attack surface. Many rely on partial or manual ASM processes to assess their assets and any associated exposure.

Recommendations

- Perform an enterprise attack surface gap analysis to detect potential blind spots in IT and security practices and technology. This is a foundation for improving any security program, but especially when security and risk management leaders have to protect environments of growing complexity.
- ASA technologies and vendors are rapidly maturing, and consolidation into larger vendors is highly likely in the next three to five years. Evaluate the associated trade-offs, such as higher discounting and year-over-year price increases, to determine whether to procure point solutions on short-term contracts. Reevaluate the market on a yearly basis until the wave of innovation and changes in market dynamics have slowed, or sign a multiyear agreement.
- Since ASA technologies are generally passive and easy to deploy and configure, they are relatively easy to replace, compared with other security technologies early in their life cycle. Do not overinvest in proofs of concept or evaluations — which can cause "analysis paralysis" — but procure solutions quickly with an eye toward rapid retirement or replacement, if needed.
- Evaluate key risk drivers for your organization to understand which technology should be prioritized. In general, organizations should install and manage EASM and/or DRPS before CAASM, as CAASM technologies are extensible in managing EASM and DRPS outputs to complete its asset inventory.

Representative Providers

This is a representative (not exhaustive) list of 10 vendors that offer ASA capabilities:

- Axonius
- Brinqa
- Cyberpion
- CyCognito
- FireCompass
- JupiterOne
- LookingGlass Cyber (via its acquisition of AlphaWave)
- Noetic Cyber

- Palo Alto Networks (via its acquisition of Expanse)
- Randori

Evidence

[1] NIST's definition of "attack surface"

This document draws on analysis of conversations between Gartner analysts and end-user clients from June 2021 through March 2022.

This document's analysis of CAASM, EASM and DRPS capabilities is not tied to one particular vendor's offering. We researched multiple vendors and their capabilities using private and public resources, such as vendors' documentation, end-user inquiries, data sheets and vendors' briefings of Gartner analysts.

Acronym Key and Glossary Terms

ASA	attack surface assessment
ASM	attack surface management
BAS	breach and attach simulation
CAASM	cyberasset attack surface management
CMDB	configuration management database
DRPS	digital risk protection services
EASM	external attack surface management
VA	vulnerability assessment

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Quick Answer: What Is the Difference Between EASM, DRPS and SRS?

Emerging Technologies: Critical Insights for External Attack Surface Management

Market Guide for Security Threat Intelligence Products and Services