Magic Quadrant pour les tests de sécurité des applications

Lecture minimale publiée 17 mai 2023 - ID G00 770949 - 49

Par **et 3 de plus** Mark Horvath , Dale Gardner ,

La conception d'applications modernes, le passage au cloud et l'adoption accélérée de DevSecOps élargissent la portée du marché AST. Les responsables de la sécurité et de la gestion des risques peuvent respecter des délais plus serrés et tester des applications plus complexes en intégrant et en automatisant AST dans le cycle de vie du logiciel.

Définition/Description du marché

Ce document a été révisé le 19 mai 2023. Pour plus d'informations, consultez la page Corrections sur gartner.com.

La vision du marché de Gartner se concentre sur les technologies ou les approches transformationnelles répondant aux besoins futurs des utilisateurs finaux. Il n'est pas axé sur le marché comme il l'est aujourd'hui.

Gartner définit le marché des tests de sécurité des applications (AST) comme les acheteurs et les vendeurs de produits et services conçus pour analyser et tester les applications pour les vulnérabilités de sécurité. Ce marché est très dynamique et continue de connaître une évolution rapide en réponse à l'évolution des architectures d'applications et des technologies habilitantes.

Dans cette analyse et dans les évaluations des fournisseurs, nous continuons à nous concentrer davantage sur les technologies et approches émergentes, ainsi que sur les outils AST qui répondent aux nouvelles exigences qu'ils apportent . Dans l'ensemble, le marché comprend des outils offrant des capacités de test de base - par exemple, des tests statiques, dynamiques et interactifs ; logiciel d'analyse de composition (SCA); et diverses capacités facultatives et spécialisées.

Les outils AST sont proposés soit sous forme d'offres d'abonnement basées sur un logiciel en tant que service (SaaS), soit moins souvent sous forme de logiciel sur site. De nombreux fournisseurs offrent les deux options . Les fonctionnalités de base offrent des fonctionnalités de test fondamentales, la plupart des organisations utilisant un ou plusieurs types, notamment :

- **AST statique (SAST) :** analyse la source, le bytecode ou le code binaire d'une application pour détecter les vulnérabilités de sécurité, généralement pendant les phases de programmation et/ou de test du cycle de vie du développement logiciel (SDLC).
- **Analyse de la composition logicielle (SCA) :** utilisée pour identifier les composants open source et, beaucoup moins fréquemment, commerciaux utilisés dans une application. À partir de là, les vulnérabilités de sécurité connues, les problèmes de licence potentiels et les risques opérationnels peuvent être identifiés.

Les capacités facultatives fournissent des formes de tests plus spécialisées et complètent généralement les capacités de base en fonction du portefeuille d'applications d'une organisation ou de la maturité du programme de sécurité des applications. Ils comprennent:

- **Tests d'API :** les API sont devenues une partie importante des applications modernes (par exemple, les applications monopage ou mobiles), mais les ensembles d'outils AST traditionnels peuvent ne pas les tester complètement, ce qui nécessite des outils et des capacités spécialisés. Les fonctions typiques incluent la possibilité de découvrir les API dans les environnements de développement et de production et de tester le code source de l'API, ainsi que la capacité d'ingérer le trafic enregistré ou les définitions d'API pour prendre en charge le test d'une API en cours d'exécution.
- **Gestion de la posture de sécurité des applications (ASPM) :** ASPM gère en permanence les risques applicatifs grâce à la détection, la corrélation et la hiérarchisation des problèmes de sécurité à travers le SDLC, du développement au déploiement. Ils ingèrent des données provenant de plusieurs sources, puis corrèlent et analysent leurs résultats pour faciliter l'interprétation, le tri et la correction. Ils agissent comme une couche de gestion et d'orchestration pour les outils de sécurité, permettant des contrôles et l'application des politiques de sécurité. En fournissant une perspective consolidée des résultats de sécurité des applications, les outils ASPM facilitent la gestion et la

correction des résultats individuels tout en offrant une vue complète de l'état de la sécurité et des risques sur l'ensemble d'une application ou d'un système.

- **Sécurité du conteneur :** l'analyse de sécurité du conteneur examine les images de conteneur, ou un conteneur entièrement instancié avant le déploiement, pour détecter les problèmes de sécurité. Les outils de sécurité des conteneurs se concentrent sur une variété de tâches, y compris les tâches de renforcement de la configuration et d'évaluation des vulnérabilités. Les outils analysent également la présence de secrets, tels que des informations d'identification codées en dur ou des clés d'authentification. Les outils d'analyse de la sécurité des conteneurs peuvent fonctionner dans le cadre du processus de déploiement de l'application ou être intégrés aux référentiels de conteneurs, de sorte que les évaluations de sécurité peuvent être effectuées lorsque les images sont stockées pour une utilisation future.

- **Activation du développeur :** les outils et fonctionnalités d'activation du développeur aident les développeurs et les membres de l'équipe d'ingénierie dans leurs efforts pour créer un code sécurisé. Ces outils se concentrent principalement sur la formation à la sécurité et les conseils de correction des vulnérabilités, soit sur une base autonome, soit intégrés dans l'environnement de développement.

- **AST dynamique (DAST) :** DAST analyse les applications dans leur état d'exécution (c'est-à-dire dynamique) pendant les phases de test et d'exploitation. DAST simule des attaques contre une application (généralement des applications Web, mais aussi de plus en plus d'interfaces de programmation d'applications [API]), analyse les réactions de l'application et détermine si elle est vulnérable.

- **Fuzzing :** les tests fuzz reposent sur la fourniture d'entrées aléatoires, malformées ou inattendues à un programme pour identifier les vulnérabilités de sécurité potentielles - par exemple, les pannes d'application ou le comportement anormal, les fuites de mémoire ou les débordements de tampon, ou d'autres résultats qui laissent le programme dans un état indéterminé. Le fuzzing, parfois appelé test non déterministe, peut être utilisé avec la plupart des types de programmes, bien qu'il soit particulièrement utile pour les systèmes qui reposent sur une quantité importante de traitement d'entrée (par exemple, applications et services Web, API) .

- **Tests d'infrastructure en tant que code (IaC) :** Gartner définit l'IaC comme la création, le provisionnement et la configuration d'une infrastructure de calcul défini par logiciel (SDC), de réseau et de stockage en tant que code source. Les outils de test de sécurité IaC aident à garantir la conformité aux normes courantes de renforcement de la configuration, à identifier les problèmes de sécurité associés à des environnements opérationnels spécifiques, à localiser les secrets intégrés et à effectuer d'autres tests prenant en charge les normes et les exigences de conformité spécifiques à l'organisation.

- **AST interactif (IAST) :** les outils IAST lancent et équipent une application en cours d'exécution (par exemple, via la machine virtuelle Java [JVM] ou le .NET Common Language Runtime [CLR]) et examinent son fonctionnement pour identifier les vulnérabilités. La plupart des

implémentations IAST sont considérées comme passives, en ce sens qu'elles s'appuient sur d'autres tests d'application pour créer une activité que les outils IAST évaluent ensuite.

- **Mobile AST (MAST) :** cela répond aux exigences spécialisées associées au test d'applications mobiles, telles que celles qui s'exécutent sur des appareils utilisant iOS, Android ou un autre système d'exploitation. Ces outils utilisent généralement des approches de test traditionnelles (par exemple, SAST et DAST) qui ont été optimisées pour prendre en charge les langages et les cadres couramment utilisés pour développer des applications mobiles et/ou Internet des objets (IoT). Ils testent également les vulnérabilités et les problèmes de sécurité propres à ces environnements.

- **Sécurité de la chaîne d'approvisionnement logicielle (SSCS) :** Fonctions destinées à identifier et gérer les risques associés aux chaînes d'approvisionnement logicielles. Ils peuvent inclure :

  - Analyse proactive des logiciels provenant de sources externes (open source ou commerciales) pour identifier les composants pouvant présenter un risque inacceptable (par exemple, projets mal entretenus, contrôles de sécurité inadéquats, présence de logiciels malveillants ou de code malveillant, etc.).

  - Création et gestion d'artefacts pour permettre aux utilisateurs de logiciels d'évaluer la sécurité des logiciels produits par une organisation (comme les nomenclatures logicielles [SBOM] ou les attestations de sécurité des applications).

  - Garantir l'intégrité du code source et d'autres artefacts de développement ou de déploiement, ainsi que les systèmes sous-jacents utilisés pour les produire, afin d'empêcher les attaques directes sur le processus de développement.

Gartner observe que l'évolution du marché AST est largement motivée par la nécessité de prendre en charge les DevSecOps d'entreprise et les initiatives d'applications cloud natives. Les clients ont besoin d'offres qui fournissent des résultats de haute assurance et de grande valeur, tout en ne ralentissant pas inutilement les efforts de développement. Les clients s'attendent à ce que les offres s'intègrent dans le processus de développement à un stade plus précoce, les tests étant souvent pilotés par des développeurs plutôt que par des spécialistes de la sécurité. Par conséquent, cette évaluation du marché se concentre fortement sur les besoins de l'acheteur, y compris la prise en charge de tests rapides et précis de divers types d'applications et la capacité à s'intégrer dans les workflows de livraison de logiciels avec un niveau d'automatisation croissant.

Quadrant magique

Figure 1 : Magic Quadrant pour les tests de sécurité des applications

Points forts et mises en garde du fournisseur

Checkmarx

Checkmarx est un leader dans ce Magic Quadrant. Checkmarx fournit une suite complète de fonctionnalités, notamment SAST, DAST, SCA, les vérifications de conteneurs, les tests d'API, la sécurité IaC et d'autres fonctions, à la fois sur une base autonome et via sa plate-forme Checkmarx One. La plupart sont disponibles en mode SaaS ou en tant que services gérés. Checkmarx IAST est un produit séparé et IaC est également disponible en tant qu'outil open source (KICS de Checkmarx). Checkmarx a son siège social aux États-Unis, mais opère dans le monde entier.

Son objectif est en grande partie d'améliorer l'expérience des développeurs et de fournir aux clients des résultats hiérarchisés et basés sur les risques. Outre les principales capacités AST, Checkmarx propose également une formation aux développeurs et des recherches sur la sécurité, ce qui ajoute des capacités d'autoremédiation à son portefeuille. Checkmarx jouit d'une bonne réputation parmi les développeurs et convient parfaitement aux organisations qui commencent à travailler avec DevSecOps.

Forces

- **Intégration du référentiel** : Checkmarx Fusion, son moteur de corrélation et de priorisation, peut désormais corréler tous ses résultats au niveau du référentiel et les intégrer dans la console, donnant aux développeurs un aperçu de leurs applications.
- **Intégration des développeurs :** Checkmarx se concentre sur l'intégration des développeurs tout au long du cycle de vie. Son lancement récent de DevHub répond aux besoins des développeurs en leur fournissant des informations complètes sur les vulnérabilités open source, ainsi que des suggestions de correction.
- **Outils DAST :** Checkmarx a introduit une nouvelle fonctionnalité DAST. C'était auparavant une lacune importante dans son produit, bien qu'il fournisse toujours DAST via Invicti en tant qu'OEM.

Précautions

- **Tarification complexe** : les clients ont cité la tarification de Checkmarx comme un défi, ce qui est une préoccupation commune à de nombreux fournisseurs d'AST. Cependant, Checkmarx s'est efforcé de fournir des produits à moindre coût, tels que la « Developer Edition » récemment introduite de sa plate-forme, qui vise à répondre à la fois aux besoins des développeurs et aux exigences de sécurité des applications.

- **Installation et configuration** : les clients ont indiqué que, malgré la flexibilité de Checkmarx, sa mise en œuvre peut être compliquée en raison de son haut niveau de configurabilité.
- **Support client le week-end** : les clients ont remarqué que le manque de disponibilité du support client le week-end était un problème relativement courant. Cependant, l'assistance le week-end est disponible dans le package d'assistance Premium.

Sécurité du contraste

Contrast Security est un visionnaire dans ce Magic Quadrant. Son produit IAST, Contrast Assess, peut soit tirer parti de l'analyse active d'un autre outil (par exemple, Burp Suite de Portswigger pour DAST) pour générer des attaques et identifier les vulnérabilités, soit s'appuyer sur des tests existants, tels que l'assurance qualité (QA).

En 2021, Contrast a ajouté la fonctionnalité SAST (Contrast Scan) et la prise en charge AST pour les applications cloud natives (telles que les fonctions sans serveur sur Amazon Web Services [AWS] Lambda). Il a également amélioré son SCA, Contrast Scan, en ajoutant le support SBOM.

Contrast Security est basé aux États-Unis, mais vend également dans les régions EMEA et Asie/Pacifique. Il convient parfaitement aux organisations qui recherchent des tests de sécurité automatisés et continus avec une faible surcharge sur le cycle de vie du développement.

Forces

- **Autoprotection des applications d'exécution** : Gartner constate un regain d'intérêt pour RASP (voir la section Contexte de cette recherche) alors que les organisations de développement se concentrent de plus en plus sur le cloud. L'expérience de Contrast dans l'espace IAST/RASP le place en bonne position pour profiter de cette tendance.
- **Tests interactifs de sécurité des applications** : Contrast Assess est l'une des solutions IAST les plus largement adoptées et continue de rivaliser sur presque toutes les listes restreintes IAST examinées par Gartner. Alors que les solutions IAST gagnent en popularité auprès des clients natifs du cloud, l'expérience de développeur de Contrast se démarque et obtient de bonnes critiques pour sa facilité d'utilisation et sa précision.
- **Assistance aux développeurs** : Contrast propose une version gratuite de CodeSec (activation des développeurs), ainsi que GitHub Actions for Scan et SCA pour rationaliser l'adoption par les développeurs.

Précautions

- **Partenaires pour certaines fonctions :** Contrast Security ne fournit pas de tests DAST, ASOC ou mobiles. Bien qu'il ait des accords de partenariat pour offrir ces fonctionnalités, il convient de noter que les accords de partenariat peuvent changer de manière inattendue et que le fardeau de l'ajout de ces outils incombe fermement au client.

- **Prise en charge des langues SAST :** SAST de Contrast Security prend en charge relativement peu de langues par rapport aux concurrents. Cependant, il a commencé à s'associer à d'autres sociétés (par exemple, Kiuwan) pour tirer parti de la vaste bibliothèque de support linguistique de ses partenaires , ce qui devrait considérablement étendre sa couverture. Cela ne s'applique pas à la prise en charge de la langue IAST, qui est assez large.

- **Support client :** Contrast Security propose des options de support client mondial 24h/24 et 7j/7. Cependant, la prise en charge linguistique est relativement limitée par rapport aux autres fournisseurs. Il couvre l'Amérique du Nord, le Royaume-Uni, l'UE et le Japon, et prend en charge les langues anglaise , allemande, française et japonaise .

GitHub

GitHub est un Challenger dans ce Magic Quadrant. GitHub offre des fonctionnalités AST via la référence SKU complémentaire GitHub Advanced Security (GHAS) pour GitHub Enterprise. Cela inclut des capacités propriétaires pour SAST, SCA, l'analyse des secrets et la sécurité de la chaîne d'approvisionnement logicielle , en plus des intégrations open source, commerciales et tierces pour DAST, la sécurité des API, MAST, l'analyse IaC et la sécurité des conteneurs.

Au cours de l'année écoulée, GitHub a ajouté une fonctionnalité pour empêcher de manière proactive que les secrets soient poussés vers les référentiels de code source, une fonctionnalité qu'il appelle «protection push».

GitHub convient parfaitement aux organisations utilisant GitHub Enterprise qui cherchent soit à rationaliser leurs investissements dans la sécurité des applications, soit à mieux intégrer les pratiques de sécurité dans leurs workflows de développement.

Forces

- **Habilitation des développeurs :** la propriété par GitHub de la gestion du code source et des outils CI/CD le positionne bien pour intégrer étroitement la sécurité dans les workflows de développement (par exemple, l'examen des dépendances), ce qui peut améliorer l'expérience du

développeur et déplacer les pratiques de sécurité des applications vers la gauche.

- **Communauté open source** : la popularité de GitHub en tant que plus grand référentiel de code open source aide les développeurs open source à accéder aux fonctionnalités de GHAS et à fournir des commentaires. La boucle de rétroaction de la communauté aide GitHub à améliorer continuellement ses capacités AST.

- **Analyse des packages npm** : GitHub possède le registre public npm, qui est la plus grande collection de packages JavaScript open source. Il dispose d'équipes dédiées à la chasse aux menaces et à la détection des logiciels malveillants pour analyser en continu les packages npm. La base de données consultative GitHub comprend plus de 10 000 CVE et avis de sécurité révisés par GitHub, dont plus de 2 800 sont spécifiques à npm. Cette intelligence alimente les alertes Dependabot, les révisions de dépendance et un graphique de dépendance.

Précautions

- **Prise en charge mobile** : GitHub n'offre pas de fonctionnalités MAST propriétaires et s'appuie sur les intégrations de partenaires avec NowSecure et l'outil/framework open source Mobile Security Framework (MobSF). Au moment de la rédaction, le support de CodeQL pour Swift (iOS) est en version bêta privée, tandis que son support pour Kotlin (Android) est en version bêta publique sur GHEC.

- **Boucle de développement externe** : l'innovation produit de GitHub est en retard par rapport à d'autres fournisseurs de premier plan dans la sécurisation de la boucle de développement externe, où elle s'appuie sur des intégrations tierces. Les exemples de domaines concernés incluent DAST, IAST, les tests fuzz, l'analyse IaC, la sécurité des API et la sécurité des conteneurs.

- **Inadéquation de la cadence de publication entre SaaS et sur site** : les clients GitHub peuvent constater une disparité des fonctionnalités entre GitHub Enterprise Cloud et GitHub Enterprise Server. Être sur GHEC permet aux clients de recevoir des correctifs et des fonctionnalités plus tôt .

GitLab

GitLab est un Challenger dans ce Magic Quadrant. GitLab fournit des fonctionnalités AST dans le cadre de sa plate-forme DevSecOps plus large. Certaines fonctionnalités, telles que SAST, l'analyse IaC, l'analyse de conteneurs et la détection de secrets, sont disponibles à tous les niveaux, tandis que DAST, l'analyse des dépendances, les tests fuzz et ASOC sont limités au niveau Ultimate de la plate-forme.

Au cours de l'année écoulée, GitLab est passé d'un grand nombre de ses analyseurs SAST spécifiques à un langage à un analyseur commun basé sur Semgrep , ce qui apporte une cohérence entre plusieurs langages de programmation et frameworks.

GitLab convient parfaitement aux organisations qui souhaitent faire progresser leur maturité DevSecOps en adoptant une plate-forme avec des fonctionnalités intégrées qui intègrent la sécurité dans les workflows de développement d'applications.

Forces

- **Plate-forme DevSecOps unique sur le SDLC :** GitLab adopte une approche d'application unique pour intégrer la sécurité dans plusieurs phases du cycle de vie DevOps. Cela permet une visibilité partagée et réduit la charge cognitive, ce qui facilite l'adoption des pratiques AST par les équipes.

- **Sécurité de la chaîne d'approvisionnement logicielle :** GitLab a une visibilité et une traçabilité complètes sur le pipeline de livraison de logiciels, de la validation du code aux applications exécutées en production. Reconnaissant l'avantage que cela offre dans la sécurisation de la chaîne d'approvisionnement logicielle, GitLab a introduit la prise en charge de la génération SBOM (CycloneDX), l'attestation d'artefact de construction et les validations de code vérifiées avec des clés SSH pour mieux s'aligner sur le cadre SLSA.

- **DAST et fuzzing intégrés :** le DAST basé sur un navigateur de GitLab est un changement fondamental par rapport aux capacités DAST précédentes basées sur OWASP ZAP. La technique utilise un navigateur, plutôt qu'un proxy, pour analyser les applications Web à la recherche de vulnérabilités, ce qui est plus fiable pour les applications Web modernes. GitLab est la seule plate-forme DevOps avec une capacité de test fuzz nativement intégrée.

Précautions

- **Intégrations IDE :** les capacités SAST et SCA de GitLab manquent actuellement d'intégrations IDE pour aider à détecter les vulnérabilités ou fournir aux développeurs des suggestions de code exactes dans le code propriétaire et tiers au sein de l'IDE en dehors du pipeline CI.

- **Cas d'utilisation avancés de SCA :** GitLab ne prend actuellement pas en charge l'analyse binaire des dépendances, la visualisation des dépendances ou la vérification de la provenance des dépendances en amont.

- **Capacités AST réparties sur les éditions de la plate-forme :** bien que les éditions Free, Premium et Ultimate de GitLab partagent des aspects des capacités de sécurité, la plupart des entreprises devront investir dans l'édition Ultimate pour répondre à leurs exigences de sécurité et de conformité. Par exemple, certains aspects de l'analyse des conteneurs sont disponibles à tous les niveaux, tandis que l'analyse des conteneurs déployés dans les clusters est limitée à Ultimate. De même, les analyseurs SAST sont inclus dans l'édition GitLab Free, mais vous auriez besoin de l'édition Ultimate pour personnaliser les ensembles de règles SAST.

Logiciel HCL

HCLSoftware est un Challenger dans ce Magic Quadrant. Le portefeuille HCL AppScan offre une combinaison de fonctionnalités AST disponibles via une variété de canaux de distribution. Les produits sont disponibles dans le monde entier, avec une forte pénétration en Amérique du Nord, en Asie/Pacifique, au Royaume-Uni et dans l'UE, et les ventes et l'assistance sont assurées via une combinaison de canaux directs et indirects.

Au cours des 12 derniers mois, HCLSoftware a lancé une solution SCA propriétaire, qui comprend à la fois la numérisation de projets et la numérisation de conteneurs. HCLSofware a également ajouté une technique d'analyse hybride pour SAST, qui se situe entre SAST traditionnel et CodeSweep. Cela permet un flux de données contextuel et une mise à l'échelle horizontale pour la vitesse, et comble les écarts entre les analystes de sécurité et les développeurs. AppScan Standard a fourni une interface utilisateur nouvellement conçue qui répond mieux aux besoins des utilisateurs.

Forces

- **Expérience utilisateur unifiée** : HCL AppScan fournit une couverture complète de diverses techniques de test de sécurité des applications sur une plate-forme consolidée, avec des expériences utilisateur unifiées (UX) et une visibilité sur plusieurs étapes du SDLC.
- **Apprentissage automatique** : HCL AppScan utilise des techniques éprouvées d'apprentissage automatique (ML) et de traitement du langage naturel pour améliorer la précision et réduire les faux positifs dans ses résultats. Les fonctionnalités Intelligent Findings Analytics (IFA) et Intelligent Code Analytics (ICA) améliorent le processus d'analyse de la sécurité en regroupant les résultats et en étudiant les API nouvelles et inconnues.
- **Vues basées sur les rôles** : HCL AppScan fournit des vues et des expériences personnalisées pour différents rôles. Le profilage d'analyse est flexible à mettre en œuvre et permet à l'utilisateur d'appliquer différentes technologies AST à différents points du pipeline de développement logiciel. Les flux de travail peuvent être personnalisés pour correspondre aux politiques et priorités de sécurité spécifiques d'une organisation.

Précautions

- **Outils sur site** : tous les produits sont disponibles en tant que services sur site, SaaS, IaaS et gérés, à l'exception de SCA, qui est uniquement disponible en tant que SaaS et services gérés. Le SAST sur site n'a pas la même étendue de plug-ins et d'intégrations prêts à l'emploi.

- **Temps d'analyse plus longs :** certains clients ont rencontré des temps d'analyse longs, en particulier pour les applications Web volumineuses. Bien qu'AppScan dispose d'une variété impressionnante de contrôles qui permettent à l'utilisateur de régler la vitesse d'exécution, cela semble quelque peu déroutant et il faudra du temps aux utilisateurs pour comprendre les options et les compromis. Cela peut conduire à la perception de temps de balayage plus longs.

- **Tarification et assistance :** la tarification de la plate-forme AST de HCLSoftware est citée par certains clients comme une préoccupation, en particulier pour les organisations disposant de budgets limités ou d'équipes de développement plus petites. Les services d'assistance à la clientèle dans certaines régions peuvent ne pas être aussi complets que prévu.

Mend.io

Mend.io est un visionnaire dans ce Magic Quadrant. Ses produits se concentrent sur la SCA et la sécurité de la chaîne d'approvisionnement, ainsi que sur l'analyse statique, la numérisation des conteneurs et les tests IaC. Bien que de taille plus petite, Mend.io est en concurrence avec les leaders pour les ventes mondiales et les capacités de support. Ses clients représentent les logiciels, les services, la finance, les télécommunications et d'autres industries, et comprennent de petites et de très grandes organisations.

Mend.io était auparavant limité à la SCA et à la sécurité des conteneurs. Récemment, il a investi dans la sécurité de la chaîne d'approvisionnement, y compris les capacités de détection de code malveillant dans les projets open source, ainsi que la correction automatisée pour le code open source et le code propriétaire.

Forces

- **SCA et sécurité de la chaîne d'approvisionnement :** le produit SCA de la société est une solution complète pour l'évaluation des images open source et des conteneurs et fonctionne avec les gestionnaires de packages pour bloquer et détecter le code malveillant. Mend.io Supply Chain Defender travaille avec les gestionnaires de packages pour détecter le code malveillant. Mend.io SCA importe et exporte des SBOM aux formats CycloneDX ou SPDX. Les SBOM importés peuvent être analysés pour les problèmes de sécurité ou les violations des politiques organisationnelles.

- **Correction automatisée :** Mend.io propose une variété d'approches pour aider à la correction automatisée. Renovate, disponible en tant que projet open source, génère automatiquement des demandes d'extraction avec des informations de mise à niveau lorsqu'une nouvelle version d'une dépendance devient disponible. Les outils prennent en charge une fonction Merge Confidence pour les mises à niveau open source, fournissant des indications sur la probabilité que la mise à niveau introduise une modification radicale. Mend.io SAST génère

automatiquement une proposition de correctif pour les programmes Java que les développeurs peuvent appliquer en tant que demande d'extraction.

- **Rapports basés sur les risques :** le produit permet aux utilisateurs d'intégrer les impacts commerciaux et les indicateurs de risque à utiliser comme facteurs dans la hiérarchisation et le tri des vulnérabilités. Les exemples incluent la nature de la surface d'attaque de l'application, la présence de données sensibles, etc. Pour les problèmes open source, l'outil rapporte des données comprenant (mais sans s'y limiter) la gravité de la vulnérabilité, l'accessibilité et la présence d'exploits connus.

Précautions

- **Étendue du produit :** Mend.io n'offre pas de fonctionnalité DAST ou IAST. Cela limitera l'attrait du produit auprès des organisations utilisant un nombre important d'applications bénéficiant de tels tests. Mend.io n'offre pas non plus de capacité de sécurité API dédiée ou de test d'applications mobiles, bien que le moteur SAST puisse analyser les langages de programmation mobiles courants, tels que Swift et Kotlin.

- **Maturité :** Mend.io a élargi son portefeuille de produits de sécurité des applications et n'a introduit que récemment sa solution SAST en 2022.

- **Fonctionnalité IaC limitée :** la recherche d'erreurs de configuration susceptibles d'avoir un impact négatif sur la sécurité est prise en charge pour plusieurs formats IaC. Cependant, l'outil ne prend pas en charge la détection des secrets et est incapable de détecter la dérive de configuration dans les environnements de production.

Onapsis

Onapsis est un joueur de niche dans ce Magic Quadrant. Onapsis se concentre fortement sur les applications critiques pour l'entreprise, en particulier celles construites sur SAP, Oracle et Salesforce Apex . La Plateforme Onapsis offre SAST/DAST/IAST/SCA, ainsi que la supply chain mobile et logicielle. L'exécution d'IAST par Onapsis diffère des autres fournisseurs, car son outil IAST est conçu sur mesure pour s'adapter aux environnements préférés de ses clients.

Onapsis Research Labs est la seule équipe de renseignement sur les menaces du secteur entièrement dédiée à la protection des applications critiques pour l'entreprise. Cette orientation permet à Onapsis de développer des informations sur les nouvelles vulnérabilités du code, les exploits des acteurs de la menace et les solutions ou solutions de contournement du jour zéro pour ses clients. En 2022, Onapsis a franchi un cap en découvrant et atténuant sa 1 000e vulnérabilité.

Onapsis convient parfaitement aux organisations qui ont réalisé d'importants investissements dans des applications métier (LOB) et critiques pour l'entreprise.

Forces

- **Prise en charge des frameworks critiques :** Onapsis est l'un des rares fournisseurs à prendre en charge la gamme complète de langages utilisés dans les systèmes SAP, y compris les référentiels de style Git, les référentiels ABAP/HANA et les environnements SAP BTP Neo/CloudFoundry.
- **Analyse des risques :** Au-delà de la gravité d'une vulnérabilité, Onapsis cadre ses conclusions en termes de risque pour l'entreprise, en fournissant une explication accessible du risque commercial, des exemples et, si possible, des solutions rapides automatisées.
- **Prise en charge de Microsoft Azure :** les entreprises qui exploitent Azure Pipelines pour rationaliser le processus de déploiement de l'écosystème SAP peuvent désormais ajouter des analyses Onapsis Control à leur processus de développement existant, ajoutant ainsi de la sécurité au cycle de vie DevOps.

Précautions

- **Assistance 18h/24 et 5j/7 :** Onapsis n'offre pas d'assistance mondiale 24h/24 et 7j/7. Cependant, il offre une assistance 18/5 (de 2 h à 20 h, heure de l'Est des États-Unis, du lundi au vendredi). Onapsis revendique un temps de réponse de 90 minutes pour les problèmes S1 critiques, mais cela pourrait être une préoccupation pour les grandes organisations multinationales opérant sur plusieurs fuseaux horaires.
- **IAST non traditionnel :** par rapport à d'autres fournisseurs, l'offre IAST d'Onapsis semble différente, mais son offre conceptuellement similaire est conçue pour et fonctionne dans le contexte des cadres spécifiques qu'elle prend en charge. Ses tests sont intégrés au runtime et les vérifications sont exécutées pendant l'exécution du code à l'aide d'un runtime JavaScript spécialisé.
- **Peu de partenariats AST :** Onapsis n'a pas beaucoup de partenariats avec les fournisseurs traditionnels d'AST (ou corrélations entre fournisseurs de résultats et de suggestions). Cependant, dans des clouds comme Azure, ces services peuvent être disponibles auprès d'autres fournisseurs sur une base ad hoc.

OpenText

OpenText est un leader dans ce Magic Quadrant. Ses produits Fortify couvrent la gamme des capacités évaluées dans ce Magic Quadrant, et la société est bien connue pour ses outils d'analyse statique et dynamique. Il fournit des fonctionnalités SCA et d'activation des développeurs en partie via ses partenariats avec les équipementiers.

Basée au Canada, OpenText est une société mondiale, avec des ventes et un support dédiés pour Fortify dans le monde entier. Les grands services bancaires et financiers, les fournisseurs de services informatiques et les gouvernements figurent en bonne place parmi ses clients.

OpenText a acquis Micro Focus en janvier 2023. Au cours des 12 derniers mois, la société a apporté des améliorations significatives à l'ensemble de son portefeuille. Plus particulièrement, OpenText a investi dans SCA, la sécurité de la chaîne d'approvisionnement et l'utilisation de ML.

Forces

- **Investissements SCA et SSCS :** Fortify a fait des progrès significatifs dans les segments SCA et de la sécurité de la chaîne d'approvisionnement grâce à son acquisition de Debricked et à l'expansion et à l'extension d'une relation OEM de longue date avec Sonatype. Un exemple notable est l'introduction d'Open Source Select, qui fournit des conseils facilement assimilables sur les risques associés aux logiciels open source avant leur sélection et leur utilisation.

- **Apprentissage automatique :** OpenText a utilisé les technologies ML pour offrir de nouvelles fonctionnalités et améliorer celles existantes. L'offre Open Source Select est alimentée en partie par ML. Fortify a également tiré parti des capacités d'analyse d'OpenText pour améliorer considérablement la détection des faux positifs parmi les résultats des tests, répondant ainsi à une plainte de longue date concernant le produit.

- **Déploiement flexible :** La portée du portefeuille de produits de l'entreprise se classe parmi les plus vastes du secteur et est prise en charge par de multiples options de déploiement. Ceux-ci incluent des packages traditionnels sur site, des offres SaaS et des options pour les installations de cloud privé et de services gérés.

Précautions

- **Acquisition :** L'acquisition de Micro Focus par OpenText introduit un certain nombre de problèmes de routine concernant la stabilité des feuilles de route des produits, le support et d'autres opérations. Les clients sont encouragés à prendre des précautions pour minimiser l'impact de toute perturbation.

- **Expérience utilisateur** : le portefeuille de produits de Fortify s'est considérablement élargi au cours de plusieurs années. Bien que bénéfiques, les ajouts n'ont pas toujours suivi un thème UX cohérent. Les chefs de produit ont étendu les intégrations pour aider à fournir aux développeurs une interface cohérente avec leurs outils existants. La société est en train de lancer un assistant d'audit mis à jour et des rapports étendus, promettant une expérience améliorée pour les utilisateurs axés sur la sécurité et la gestion.

- **Tarification** : sa longévité sur le marché, combinée à un large éventail d'options de déploiement, a conduit OpenText à disposer de l'un des modèles de tarification les plus complexes du marché. Bien que cela offre une flexibilité accrue, cela peut compliquer les négociations car les acheteurs recherchent l'approche de licence optimale pour leurs besoins spécifiques.

Snyk

Snyk est un leader dans ce Magic Quadrant. Snyk est un nouveau venu dans ce corpus de recherche, mais est un fournisseur AST établi et populaire. Basée aux États-Unis, Snyk a une présence mondiale, avec une forte pénétration en Amérique du Nord. Son offre AST comprend Snyk Code (une plate-forme SAST basée sur le cloud), Snyk Open Source (une solution SCA), Snyk Container, Snyk Infrastructure as Code et Snyk Cloud (CSPM).

Au cours de l'année écoulée, Snyk a lancé une nouvelle interface utilisateur en intégrant son acquisition TopCoat et en proposant de nouveaux rapports intégrés. Snyk a également étendu son approche centrée sur les applications à IaC et au cloud (via l'acquisition de Fugue), a permis l'application cohérente des normes de sécurité de l'IDE au cloud et a fourni un contexte de code en ligne pour les correctifs aux équipes DevOps et cloud.

Forces

- **Prise en charge native du cloud** : Snyk dispose de solides capacités de sécurité des applications natives du cloud , notamment la capacité de fournir un contexte d'application complet, d'analyser l'infrastructure cloud et les images de conteneurs dans différents environnements cloud et de guider les développeurs pour résoudre les problèmes.

- **Assistance aux développeurs** : les produits de Snyk sont conçus pour s'intégrer aux flux de travail de développement, permettant aux développeurs d'adopter facilement la plate-forme et de concevoir de meilleures pratiques de sécurité. La plate-forme orchestre l'exécution de plusieurs produits sur des calendriers automatisés et des événements push.

- **Base de données de vulnérabilités SCA :** Snyk dispose d'une base de données complète de vulnérabilités, qui est régulièrement mise à jour pour fournir les informations les plus précises et les plus récentes sur les menaces de sécurité. Il offre également une analyse et une correction automatisées des vulnérabilités de sécurité pour les applications, l'IaC et les conteneurs.

Précautions

- **Partenariats de mise sur le marché :** l'offre AST de Snyk n'inclut pas le DAST intégré (que Snyk fournit en partenariat avec Rapid7 et StackHawk), l'IAST ou le fuzzing . Il est important que les clients soient conscients du statut de partenariat de Snyk pour éviter toute interruption potentielle du service.

- **Personnalisation limitée des rapports :** certains utilisateurs ont noté que les options de personnalisation de la plateforme sont limitées. Malgré la nouvelle interface utilisateur et les fonctions de création de rapports, la création de rapports est toujours citée comme un point faible par certains clients, en particulier lorsque les clients ont de nombreux projets ou des besoins spécifiques en matière de métriques personnalisées.

- **Fréquence des alertes** : les clients ont signalé que la plate-forme de Snyk peut générer un grand nombre d'alertes, ce qui peut être accablant pour certains utilisateurs, en particulier dans des environnements vastes ou complexes. Cela obligerait les utilisateurs à consacrer plus de temps et de ressources à l'examen et au traitement des alertes.

Sonatype

Sonatype est un acteur de niche dans ce Magic Quadrant. Il s'est forgé une solide réputation dans les espaces de gestion SCA et open source au cours des 10 dernières années, et a récemment ajouté Lift, un outil SAST, à son offre. Sonatype est une société basée aux États-Unis avec des clients basés principalement aux États-Unis, au Royaume-Uni et dans l'UE.

Sonatype est depuis longtemps connu pour son serveur Nexus IQ (maintenant Sonatype IQ), un moteur de politique de gestion des composants open source. Sonatype a cultivé une bonne réputation dans la communauté des logiciels open source (OSS) pour ses recherches approfondies sur la sécurité et ses contributions à la communauté.

Lift, un scanner SAST qui complète l'ensemble d'outils existant de Sonatype, est un nouveau produit construit grâce à l'acquisition de MuseDev par le fournisseur fin 2021. Lift, avec les capacités SCA de Sonatype, constitue le cœur de son offre de chaîne d'approvisionnement logicielle.

Sonatype convient parfaitement aux clients qui souhaitent se concentrer sur les problèmes de chaîne d'approvisionnement de logiciels et d'OSS, où ils peuvent tirer parti de l'expérience de Sonatype.

Forces

- **Forte histoire SCA :** Sonatype travaille depuis longtemps avec la sécurité OSS et SCA. Il dispose d'une équipe de chercheurs expérimentés qui a identifié et renvoyé le code OSS vulnérable pendant plus d'une décennie.
- **Blocage par défaut :** Sonatype Firewall Release Integrity utilise des systèmes ML pour identifier les composants suspects et malveillants et les bloquer par défaut. Cela peut être une fonctionnalité pratique, en particulier pour les organisations qui découvrent (ou viennent de développer) un SDLC sécurisé.
- **Assistance juridique :** Le pack juridique avancé de Sonatype est conçu pour réduire les complications entre les services de développement et juridiques. Il peut se conformer automatiquement aux obligations de licence open source (par exemple, attributions, attestations), fournit des données juridiques complètes aux réviseurs juridiques et ses flux de travail créent un pont entre le juridique et le développement.

Précautions

- **Nouveau produit :** Sonatype est nouveau dans l'espace SAST et, bien que son offre semble compétitive, Lift n'a pas eu le niveau d'exposition réelle aux clients typique des fournisseurs de ce Magic Quadrant.
- **Outils limités :** Sonatype ne prend pas en charge DAST ou IAST, et n'a pas non plus de partenariats ou d'accords de mise sur le marché conjoints avec d'autres fournisseurs pour fournir ces fonctionnalités.
- **Prix :** Dans un marché déjà saturé d'outils SAST et SCA, il peut être difficile pour une nouvelle entreprise d'être compétitive parmi les acteurs de plateforme établis.

Synopsis

Synopsys est un leader dans ce Magic Quadrant. Il offre une large gamme de fonctionnalités AST, y compris des produits tels que Coverity (SAST), WhiteHat Dynamic (DAST), Black Duck (SCA), Seeker (IAST), Polaris (AST basé sur le cloud) et Code Sight (plug-in IDE) . Synopsys a son siège social aux États-Unis, mais ses offres sont géographiquement diversifiées, avec une présence en Amérique du Nord, en Asie/Pacifique et en Europe.

En juin 2022, Synopsys a finalisé l'acquisition de WhiteHat Security auprès de NTT Security. Cela ajoute une nouvelle capacité DAST améliorée à la suite de produits de Synopsys. Elle a également lancé la nouvelle version de Polaris (fAST Static et fAST SCA), qui est désormais disponible en tant que solution SaaS.

Synopsys a indiqué qu'il prévoyait d'intégrer des éléments de la plate-forme Vantage récemment lancée par WhiteHat et des acquisitions précédentes, y compris Tinfoil Security, dans les prochaines offres Polaris fAST. La société a également élargi son offre Rapid Scan Static, en ajoutant de nouveaux contrôles et en intégrant l'outil dans d'autres composants du portefeuille.

Forces

- **Mise à niveau de Polaris :** Synopsys a introduit une nouvelle version de Polaris, qui peut désormais fournir des fonctionnalités SAST et SCA en tant que solution SaaS intégrée, complétant son produit sur site et son plug-in IDE pour couvrir de larges besoins de déploiement.
- **Intégration des partenaires :** afin de renforcer son intégration dans les chaînes d'outils DevOps, Synopsys a étendu sa prise en charge des outils de développement tels que GitHub, GitLab et Artifactory. Les analyses de sécurité peuvent désormais être déclenchées par des demandes d'extraction ou des flux de travail GitHub Action, les résultats étant publiés directement au développeur dans GitHub.
- **ASOC :** L'achat par Synopsys en 2021 de CodeDx, un outil ASOC, a été intégré à la suite de produits. CodeDx gère une grande partie de l'analyse et de l'orchestration des données entre les outils de la plate-forme.

Précautions

- **Tarification :** la tarification de Synopsys est considérée comme extrêmement compliquée par les clients, en particulier les petites et moyennes entreprises, et est apparue comme un problème dans les révisions de tarification.
- **Interface utilisateur complexe :** L'interface utilisateur est toujours citée comme un point faible dans Gartner Peer Insights. Le retour le plus courant est qu'il est complexe à utiliser, et parfois déroutant pour certains types de numérisation . Cependant, certaines organisations l'utilisent plus efficacement en mode "headless".
- **Livraison SaaS :** la livraison SaaS et hybride (un mélange de SaaS et sur site) fait toujours défaut pour Coverity, la génération SBOM et l'ASPM. Tous les autres outils sont disponibles en tant que SaaS et/ou services gérés.

Véracode

Veracode est un leader dans ce Magic Quadrant. Il offre des fonctionnalités AST complètes, notamment SAST, DAST, IAST, SCA, l'analyse de conteneurs et l'analyse IaC, des tests de pénétration manuels, des conseils en matière de sécurité et de correction des applications, ainsi qu'une formation à la sécurité basée sur l'expérience et basée sur des cours pour les développeurs.

Au cours de l'année écoulée, Veracode a acquis Crashtest Security, améliorant ainsi ses capacités de test DAST et de pénétration pour les applications Web et les API. Il a également acquis Jaroona (un Gartner Cool Vendor en 2021) pour détecter et corriger les vulnérabilités logicielles via ML.

Veracode convient parfaitement aux organisations qui cherchent à améliorer la maturité de leurs initiatives de sécurité des applications en utilisant une combinaison d'outils de sécurité basés sur SaaS, de formation des développeurs, d'assistance à la gestion des programmes et de consultation d'experts.

Forces

- **Prise en charge UE/Royaume-Uni : Veracode** offre désormais une prise en charge dédiée pour la région européenne, qui fournit actuellement des capacités d'analyse statique et de SCA. Cela pourrait être utile aux organisations européennes préoccupées par les données résidant en dehors des juridictions européennes.
- **Analyse comparative par les pairs :** S'appuyant sur un ensemble de données anonymisées qui alimente également son rapport annuel sur l'état de la sécurité, Veracode a ajouté de nouvelles fonctionnalités en 2022 qui aident les organisations à évaluer les progrès et la maturité de leurs programmes de sécurité des applications par rapport à leurs pairs du même secteur. Cela permet aux responsables de la sécurité de présenter une analyse de rentabilisation solide pour leurs investissements dans la sécurité des applications.
- **Conformité FedRAMP :** En 2022, Veracode a obtenu l'autorisation modérée du Federal Risk and Authorization Management Program (FedRAMP) des États-Unis, qui certifie qu'il répond à des exigences de sécurité spécifiques, y compris les contrôles spécifiés par le Federal Information Security Management Act (FISMA) et le NIST 800-53 éditions.

Précautions

- **Offre SaaS uniquement :** Veracode propose un produit uniquement SaaS, ce qui limite ses possibilités d'entrée sur certains marchés qui ne sont pas encore à l'aise d'exposer leur code au cloud. L'interface utilisateur peut sembler lente lors de l'empaquetage et du téléchargement de fichiers volumineux pour la numérisation.

- **Prise en charge limitée de la sécurité IaC :** bien que Veracode ait réalisé des progrès significatifs dans l'ajout de fonctionnalités de sécurité des conteneurs et d'analyse IaC en 2022, il ne prend actuellement pas en charge la détection de la dérive de configuration de l'infrastructure ni ne permet aux organisations de définir leurs propres politiques IaC personnalisées.

- **Absence d'ingestion de SBOM :** Veracode n'a actuellement pas la capacité d'ingérer et d'attester des SBOM dans le cadre de décisions de politique automatisées dans les pipelines CI/CD.

Fournisseurs ajoutés et supprimés

Nous révisons et ajustons nos critères d'inclusion pour les Magic Quadrants à mesure que les marchés évoluent. À la suite de ces ajustements, la composition des fournisseurs dans n'importe quel Magic Quadrant peut changer au fil du temps. L'apparition d'un fournisseur dans un Magic Quadrant une année et non la suivante n'indique pas nécessairement que nous avons changé d'avis sur ce fournisseur. Cela peut être le reflet d'un changement sur le marché et, par conséquent, d'un changement des critères d'évaluation, ou d'un changement d'orientation de la part de ce fournisseur.

Ajoutée

- Mend.io

- Sonatype

Abandonné

Les fournisseurs suivants sont apparus dans l'itération précédente du Magic Quadrant AST, mais ont été abandonnés en raison des nouveaux critères d'inclusion.

- Invicti

- Rapide7
- Théorème des données

NTT Security a été abandonné en raison de son acquisition par Synopsys.

Critères d'inclusion et d'exclusion

Pour les clients de Gartner, la recherche Magic Quadrant et Critical Capabilities identifie puis analyse les fournisseurs les plus pertinents et leurs produits sur un marché. Gartner utilise, par défaut, une limite supérieure de 20 fournisseurs pour prendre en charge l'identification des fournisseurs les plus pertinents sur un marché. À certaines occasions spécifiques, la limite supérieure peut être étendue lorsque la valeur de recherche prévue pour nos clients pourrait autrement être diminuée. Les critères d'inclusion représentent les attributs spécifiques que les analystes jugent nécessaires pour être inclus dans cette recherche.

Pour être éligibles à l'inclusion, les fournisseurs devaient répondre aux critères suivants au 1er novembre 2022.

Participation au marché :

Les vendeurs doivent :

- Fournir une solution AST dédiée qui devrait être généralement disponible (GA) à partir du 31 décembre 2022 et qui prend en charge, au minimum, les deux capacités AST suivantes, telles que décrites dans la section Définition/Description du marché et les capacités techniques pertinentes pour les clients de Gartner :
  - Test de sécurité des applications statiques
  - Analyse de la composition logicielle
- Se conformer à un modèle d'engagement reproductible et cohérent en utilisant principalement leurs propres outils de test pour activer les capacités de test.

- Fournissez des outils sous forme de logiciel ou d'appliance sur site, d'appliance ou de conteneur basé sur le cloud, de SaaS ou d'une combinaison de ces trois facteurs de forme.

"Disponibilité générale" signifie que le produit ou le service est disponible sur une grille tarifaire/carte pour l'achat par les clients.

Traction du marché :

Les fournisseurs doivent également satisfaire à l'une des normes suivantes pour la traction commerciale :

Au cours des quatre derniers trimestres (4T21 et les trois premiers trimestres de 2022), le vendeur doit :

- Avoir généré au moins 100 millions de dollars de revenus annuels (GAAP) pour les produits AST.

Ou

- Avoir généré au moins 35 millions de dollars de revenus AST, dont au moins 20 % provenant de plus d'une région géographique.

Et

- Classez-vous parmi les 20 premières organisations dans l'indice Market Momentum défini par Gartner pour ce Magic Quadrant. Les entrées de données utilisées pour calculer la dynamique du marché AST MQ comprennent un ensemble équilibré de mesures :
  - Recherche de clients Gartner, volume de demandes ou demandes de tarification.
  - Fréquence des mentions en tant que concurrent d'autres fournisseurs AST MQ dans les avis sur le forum Peer Insights de Gartner au 1er novembre 2022.
  - Scores et fréquence des mentions mesurés dans Gartner Peer Insights.

- Innovations significatives sur le marché, telles que notées par des publications majeures, des améliorations ou des introductions de produits, ou des récompenses de l'industrie.
- Autres développements significatifs dans la posture de l'entreprise, par exemple, l'activité de fusions et acquisitions.

Ou

- Avoir généré au moins 20 millions de dollars de revenus AST et se classer parmi les 10 meilleurs fournisseurs de l'indice Market Momentum tel que défini ci-dessus.

Capacités techniques pertinentes pour les clients de Gartner :

Plus précisément, les fournisseurs doivent offrir les capacités techniques suivantes :

- Une offre principalement axée sur les tests de sécurité pour identifier les vulnérabilités de sécurité logicielle, avec des modèles de rapport par rapport au Top Ten de l'OWASP et d'autres définitions et normes de vulnérabilité courantes.
- Assistance ou conseils aux développeurs dans la correction des vulnérabilités.
- Pour les produits et/ou services SAST :
  - Prise en charge des langages de développement courants (par exemple, Python, Java, C#, PHP, JavaScript)
- Pour les produits et/ou services SCA :
  - Capacité à rechercher les vulnérabilités communément connues
  - Possibilité de rechercher des bibliothèques vulnérables obsolètes
  - Possibilité de rechercher des licences indésirables ou inappropriées

Capacités commerciales pertinentes pour les clients de Gartner

Les vendeurs doivent :

- Offrez un support client par téléphone, par e-mail et/ou sur le Web.
- Offrir un contrat, une console/un portail, une documentation technique et un support client en anglais (soit comme langue par défaut du produit ou service, soit comme localisation facultative).

Critère d'évaluation

Ce sont les attributs sur lesquels les fournisseurs et leurs produits sont évalués. Les critères d'évaluation et la pondération indiquent les caractéristiques spécifiques et leur importance relative qui soutiennent la vision Gartner du marché et qui sont utilisées pour évaluer de manière comparative les fournisseurs dans cette recherche.

Capacité d'exécution

Produit ou service : ce critère évalue les principaux biens et services qui sont en concurrence et/ou desservent le marché défini. Cela inclut les capacités actuelles des produits et services, la qualité, les ensembles de fonctionnalités, les compétences, etc. Ces biens et services peuvent être proposés en mode natif ou via des accords/partenariats OEM, tels que définis dans la section Définition/Description du marché et détaillés dans les sous-critères. Ce critère évalue spécifiquement les capacités, la qualité et la précision actuelles des produits/services AST de base, ainsi que les ensembles de fonctionnalités. Il évalue également l'efficacité et la qualité des capacités auxiliaires et de l'intégration dans le SDLC.

Viabilité globale : la viabilité comprend une évaluation de la santé financière globale de l'organisation, ainsi que du succès financier et pratique de l'unité commerciale. Il évalue la probabilité que l'organisation continue à offrir et à investir dans le produit, ainsi que la position du produit dans le portefeuille actuel. Plus précisément, nous examinons l'accent mis par le fournisseur sur l'AST, sa croissance et sa part de marché estimée de l'AST, ainsi que sa clientèle.

Exécution des ventes/tarification : ce critère examine les capacités de l'organisation dans toutes les activités d'avant-vente et la structure qui les soutient. Cela inclut la gestion des transactions, la tarification et la négociation, le support avant-vente et l'efficacité globale du canal de vente.

Nous examinons des fonctionnalités telles que la prise en charge des preuves de concept et des options de tarification pour les cas d'utilisation simples et complexes. L'évaluation tient également compte des commentaires reçus des clients sur leurs expériences avec le soutien aux ventes des fournisseurs, la tarification et les négociations.

Réactivité/enregistrement du marché : capacité à réagir, à changer de direction, à être flexible et à réussir dans la concurrence au fur et à mesure que les opportunités se présentent, que les concurrents agissent, que les besoins des clients évoluent et que la dynamique du marché change. Ce critère tient également compte de l'historique de réactivité du fournisseur aux demandes changeantes du marché.

Exécution du marketing : ce critère évalue la clarté, la qualité, la créativité et l'efficacité des programmes conçus pour transmettre le message de l'organisation afin d'influencer le marché, de promouvoir la marque, d'accroître la notoriété des produits et d'établir une identification positive dans l'esprit des clients. Ce « partage d'esprit » peut être motivé par une combinaison de publicité, d'activités promotionnelles, de leadership éclairé, de médias sociaux, de références et d'activités de vente. Nous évaluons des éléments tels que la réputation et la crédibilité du fournisseur auprès des spécialistes de la sécurité.

Expérience client : Nous examinons les produits et services et/ou programmes qui permettent aux clients d'obtenir les résultats escomptés. Plus précisément, cela inclut des interactions fournisseur/acheteur de qualité, un support technique et un support de compte. Il peut également inclure des outils auxiliaires, des programmes de support client, la disponibilité de groupes d'utilisateurs et des accords de niveau de service (SLA).

Opérations : Ce critère évalue la capacité de l'organisation à atteindre ses objectifs et ses engagements. Les facteurs comprennent la qualité de la structure organisationnelle, les compétences, les expériences, les programmes, les systèmes et les autres véhicules qui permettent à l'organisation de fonctionner de manière efficace et efficiente.

Tableau 1 : Capacité à exécuter les critères d'évaluation

Critère d'évaluation ↓	*Pondération* ↓
Produit ou service	Haut

Critère d'évaluation	*Pondération*
Viabilité globale	Haut
Exécution des ventes/Tarification	Haut
Réactivité du marché/Record	Haut
Exécution marketing	Haut
Expérience client	Haut
Opérations	Non classé
Depuis avril 2023	

Source : Gartner (mai 2023)

Intégralité de la vision

Compréhension du marché : il s'agit de la capacité du fournisseur à comprendre les besoins des clients et à les traduire en produits et services. Les fournisseurs qui montrent une vision claire de leurs marchés écoutent et comprennent les demandes des clients, et ils peuvent façonner ou

améliorer les changements du marché avec leur vision supplémentaire.

Stratégie marketing : Nous recherchons des messages clairs et différenciés qui sont constamment communiqués en interne et externalisés via les médias sociaux, la publicité, les programmes clients et les déclarations de positionnement. La visibilité et la crédibilité de la capacité du fournisseur à répondre aux besoins d'un marché en évolution sont également à prendre en considération.

Stratégie de vente : Nous recherchons une stratégie de vente solide qui utilise les réseaux appropriés, y compris les ventes directes et indirectes, le marketing, le service et la communication. En outre, nous recherchons des partenaires qui étendent la portée et la profondeur de la portée du marché, de l'expertise, des technologies, des services et de la clientèle du fournisseur. Plus précisément, nous examinons comment un fournisseur atteint le marché avec sa solution et la vend - par exemple, en tirant parti des partenaires et des revendeurs, des rapports de sécurité ou des canaux Web.

Stratégie d'offre (de produit) : nous recherchons une approche du développement et de la livraison de produits qui met l'accent sur la différenciation du marché, la fonctionnalité, la méthodologie et les caractéristiques en fonction des exigences actuelles et futures. Plus précisément, nous examinons l'offre de produits et de services AST, et comment son étendue et sa modularité peuvent répondre aux différentes exigences des clients et aux niveaux de maturité des programmes de test. Nous évaluons la capacité du fournisseur à développer et à fournir une solution qui se différencie de la concurrence d'une manière qui répond de manière unique aux exigences critiques des clients. Nous examinons également comment les offres peuvent intégrer des fonctionnalités non AST pertinentes qui peuvent améliorer la sécurité des applications dans leur ensemble.

Modèle d'entreprise : Ce critère évalue la conception, la logique et l'exécution de la proposition d'entreprise de l'organisation pour atteindre un succès continu.

Stratégie verticale/industrielle : nous évaluons la stratégie pour diriger les ressources (par exemple, les ventes, les produits, le développement), les compétences et les produits pour répondre aux besoins spécifiques des segments de marché individuels, y compris les marchés verticaux.

Innovation : Nous recherchons des agencements directs, connexes, complémentaires et synergiques de ressources, d'expertise ou de capital à des fins d'investissement, de consolidation, défensives ou préventives. Plus précisément, nous évaluons la façon dont les fournisseurs innovent pour répondre aux exigences changeantes des clients afin de prendre en charge les tests pour les initiatives DevOps, les tests de sécurité des

API, l'architecture sans serveur et les microservices. Nous évaluons également dans quelle mesure le fournisseur développe des méthodes pour rendre les tests de sécurité plus précis. Nous évaluons les innovations, non seulement en AST, mais également dans des domaines tels que les conteneurs, la formation et l'intégration avec la méthodologie de développement logiciel des développeurs.

Stratégie géographique : ce critère évalue la stratégie du fournisseur pour orienter les ressources, les compétences et les offres afin de répondre aux besoins spécifiques des zones géographiques en dehors de sa « maison » ou de sa géographie d'origine, directement ou par l'intermédiaire de partenaires, de canaux et de filiales, en fonction de cette géographie et de ce marché. Nous évaluons la disponibilité et la prise en charge de l'offre dans le monde entier, y compris la prise en charge de la langue locale pour les outils, les consoles et le service client.

Tableau 2 : Complétude des critères d'évaluation de la vision

Critère d'évaluation ↓	*Pondération* ↓
Compréhension du marché	Haut
Stratégie de marketing	Haut
Stratégie de soldes	Moyen
Stratégie d'offre (de produit)	Haut
Modèle d'affaires	Non classé

Critère d'évaluation	*Pondération*
Stratégie verticale/industrielle	Non classé
Innovation	Haut
Stratégie géographique	Haut
Depuis avril 2023	

Source : Gartner (mai 2023)

Descriptions des quadrants

Dirigeants

Les leaders du marché AST démontrent l'étendue et la profondeur des produits et services AST. Ils fournissent généralement des SAST/DAST/IAST/SCA matures et réputés et démontrent une vision à travers un chemin clair et bien articulé pour répondre aux besoins croissants des développeurs modernes. Les leaders offrent une prise en charge d'outils tels que les tests d'API, l'IaC, le fuzzing, la prise en charge des conteneurs et la prise en charge du développement cloud natif dans leurs solutions. Ils offrent également généralement aux organisations des options pour les modèles de prestation sur site et AST en tant que service pour les tests,ainsi qu'un cadre de création de rapports de classe entreprise pour prendre en charge plusieurs utilisateurs, groupes et rôles, idéalement via une console de gestion unique. Les leaders doivent être en mesure de prendre en charge les tests d'applications mobiles et doivent faire preuve d'une solide exécution dans les technologies AST de base qu'ils proposent. Bien qu'ils puissent exceller dans des catégories AST spécifiques, les leaders doivent offrir une plate-forme complète avec une forte présence sur le marché, une croissance et une fidélisation de la clientèle.

Challengers

Les challengers de ce Magic Quadrant sont des fournisseurs qui ont exécuté de manière cohérente, souvent avec force dans une ou plusieurs technologies particulières (par exemple, SAST, SCA, DAST ou IAST) ou en se concentrant sur un seul modèle de livraison (par exemple, sur AST en tant que service uniquement) . En outre, ils ont démontré qu'ils peuvent rivaliser avec les leaders dans leur domaine d'intervention particulier et ont démontré leur élan à la fois en termes de taille globale et de croissance de leur clientèle.

Visionnaires

Les visionnaires de ce Magic Quadrant sont des fournisseurs d'AST avec une vision forte qui répond aux besoins en constante évolution du marché. Les fournisseurs visionnaires offrent des capacités innovantes pour s'adapter aux DevOps, aux conteneurs, au développement cloud natif et aux technologies émergentes similaires. Les visionnaires peuvent ne pas exécuter aussi régulièrement que les leaders ou les challengers.

Acteurs de niche

Les acteurs de niche proposent des solutions viables et fiables qui répondent aux besoins d'acheteurs spécifiques. Parfois appelés spécialistes, les acteurs de niche s'en sortent bien lorsqu'ils sont considérés par les acheteurs à la recherche du "meilleur de la race" ou du "meilleur ajustement" pour répondre à un cas d'utilisation commerciale ou technique particulier qui correspond à l'objectif du fournisseur. Les acteurs de niche peuvent s'adresser à des sous-ensembles du marché global. Les entreprises ont tendance à choisir des acteurs de niche lorsque l'accent est mis sur quelques fonctions importantes, ou sur l'expertise spécifique d'un fournisseur, ou lorsqu'elles ont une relation établie avec un fournisseur particulier. Les acteurs de niche se concentrent généralement sur un type spécifique de technologie ou de modèle de livraison AST, ou sur une région géographique spécifique .

Contexte

Depuis 2021, Gartner parle du niveau de maturité des organisations en termes de early, middle et advanced (voir l'itération 2022 du Magic Quadrant for Application Security Testing). Bien que cette catégorisation soit encore largement valable, en 2022, nous avons vu le marché exprimer un mélange plus compliqué de technologies, de tendances et de maturité qu'auparavant. Quelques faits saillants :

Le "décalage à gauche" a déjà été réalisé

Alors que les équipes de sécurité ont joué, et joueront toujours, un rôle important dans le SDLC sécurisé, Gartner reçoit désormais plus de demandes à ce sujet de la part des équipes de développement que des responsables de la sécurité. Il existe certainement des organisations héritées , souvent de très grandes organisations multinationales qui ont une variété de styles de développement, et des petites et moyennes entreprises pour lesquelles les modèles existants de sécurité et de développement fonctionnent bien. Les responsables du développement cherchent de plus en plus à fusionner ce qui était historiquement considéré comme des tâches de sécurité dans les phases précédentes du SDLC. Ces tâches incluent la détection des vulnérabilités, la correction du code et les tests de sécurité. Une enquête Gartner de 2021 auprès des leaders du génie logiciel a révélé que plus de la moitié des répondants étaient principalement responsables de la sécurité des applications qu'ils construisent. Bien que cela puisse sembler ralentir le rythme de production ("vitesse"), surtout au début, la correction des vulnérabilités le plus tôt possible permet d'économiser de l'argent, du temps et de l'énergie à long terme.

Plus important encore, les chefs d'équipe de sécurité et de développement définissent ces tâches de sécurité comme des problèmes de développement et les mappent directement dans le workflow de développement existant. Ils associent également les résultats de sécurité réussis à des métriques et des KPI plus significatifs pour les développeurs. Par exemple, les problèmes de sécurité sont souvent des indicateurs d'autres problèmes de qualité du code ; c'est-à-dire que les problèmes de sécurité qui peuvent être résolus par les développeurs surviennent souvent lorsque les métriques de qualité du code sont médiocres. En recadrant la discussion autour des problèmes centrés sur les développeurs, les chefs d'équipe de sécurité constatent que les développeurs sont un public plus coopératif. La plupart des fournisseurs du Magic Quadrant de Gartner pour les tests de sécurité des applications classent désormais l'expérience des développeurs comme une métrique importante à suivre aux côtés des métriques d'outil habituelles telles que la précision, la vitesse et la reproductibilité. L'industrie AST a longtemps cherché à « décaler vers la gauche » pour faciliter et accélérer la correction des vulnérabilités, et à ce stade de 2023, cela semble être la position acceptée par défaut.

Accroître l'expérimentation avec l'IA et les chatbots

Les développeurs et les professionnels de la sécurité estiment que les conseils de remédiation juste à temps sont à peu près aussi importants que la formation formelle en classe. Bien que le travail en classe soit important, en particulier pour les équipes qui commencent tout juste à inclure la sécurité dans leur cycle de développement, ce type de formation formelle a tendance à s'estomper avec le temps. Bien que les coachs de sécurité soient une bonne ressource pour aider à améliorer les résultats en matière de sécurité, ils ne s'adaptent souvent pas au degré requis. Des avancées telles que les chatbots commencent à être incluses dans de nombreux outils SAST et SCA . Ils peuvent répondre à des questions simples avec des réponses préprogrammées et connecter l'utilisateur à un agent de support humain pour résoudre des problèmes plus

complexes. Cela s'est avéré être une fonctionnalité populaire de nombreux outils. Alors que l'utilisation d' assistants de code AI complets (e.g. GitHub Copilot, ChatGPT) is still at an early stage, Gartner has begun to receive inquiries on how they may be used to address security issues, and specifically code remediation. It remains to be seen how effective this will be, as security remediation often involves specific knowledge outside the actual code, such as defense-in-depth issues or exploitability.

Software Supply Chain Risks/SBOMs

Since May 2021, U.S. software vendors have been required to provide buyers with SBOMs for each product purchased, either directly or by publishing it on a public website. [1] This requirement has pushed some of the biggest issues in software security into the public eye, especially in relation to commercial off-the-shelf software. Tools for performing software assessments and composition analysis have existed for many years, especially focusing on the use of open-source code. However, the introduction of this requirement moved the issue forward in significant ways, enabling a lot of software to come into scope and giving customers a chance to understand the security posture of many of the applications they purchase.

In this year's iteration of the Magic Quadrant and Critical Capabilities report for AST, we note that most AST companies have staked out a position on SBOMs and have at least some capacity to address them. However, it should be noted that, at this early stage, although a lot of SBOMs are being produced, far fewer are being consumed and operationalized. Furthermore, vendors are inconsistent in terms of which standard formats they support, although there are signs that they are starting to coalesce.

Market Overview

Over the past year, the AST market has undergone explosive growth and expansion. Worldwide end-user spending on application security tools reached approximately $3.4 billion in 2022, a dramatic jump of 27% compared to 2021's total of $2.6 billion. Geographic spending trends remain largely unchanged year over year. North America remains the largest overall market, representing approximately 68% of total spending. The EU and U.K. ranked second, at 17%, with the Asia/Pacific region totaling 12% of spending. The Middle East and Africa, at 2%, and South America, at 1%, remain nascent but growing markets.

This increase in customer demand is driven by a combination of factors, which appear to be largely resilient to adverse global macroeconomic trends. First, we note greater urgency around application security, driven by various regulatory and industrial mandates, along with multiple high-profile security incidents traced back to unsecure code and development practices. Additionally, we observe signs of a retooling initiative, as

organizations reassess the ability of their existing tools to properly address changing application architectures and continually evolving development approaches. The emergence of new concerns — specifically, software supply chain security, along with an increased focus on cloud-native applications — is creating opportunities for both new features and vendors in the market.

The increased focus on application security, and the subsequent increase in demand for tooling, creates both benefits and disadvantages for buyers. On the positive side, buyers enjoy a greater choice, as new vendors enter the market to address emerging requirements, such as software supply chain security and application security posture management. Existing vendors have also acted aggressively to meet these needs. However, despite this increased competition, extremely strong demand has enabled vendors to maintain higher pricing than might normally be expected. Well-prepared buyers can expect to obtain discounts, especially if economic conditions eventually lead to the deceleration of market growth, although aggressive negotiation may be required.

The AST vendor landscape remains dynamic. Mend.io (formerly WhiteSource) acquired Xanitizer and DefenseCode in February 2022 to support its entry into the static analysis segment of the market. This follows the vendor's 2021 acquisition of Diffend, which supports software supply chain security. Software supply chain concerns also prompted Micro Focus to acquire Debricked in March 2022. Micro Focus itself was subsequently acquired in whole by OpenText, in a $6 billion transaction that closed in January 2023. Snyk acquired Fugue, a cloud security posture management vendor, in February 2022, aiding the vendor's expansion into the cloud-native application security market. Snyk also acquired TopCoat, a data analytics firm, in March as an avenue to enhance data reporting and visualizations within its broader portfolio. Synopsys acquired WhiteHat Security from NTT in June 2022, enhancing its dynamic scanning capabilities. WhiteHat was previously acquired by NTT Security Corporation in March 2019, but failed to achieve the initially expected growth. In April 2022, Veracode acquired Jaroona for its ML-powered autoremediation technology, which has since been integrated into the Veracode portfolio. Jaroona was a 2021 Gartner Cool Vendor for DevSecOps.

Evidence

The 2021 Gartner Enabling Cloud Native DevSecOps Survey was conducted online from 12 through 21 May 2021 to identify the emerging governing structures, security owners, technologies used and the current challenges in the DevSecOps pipeline to secure cloud-native applications. In total, 85 IT and business leaders with involvement in DevSecOps initiatives participated in the survey. Eighty-two were from Gartner's IT and Business Leaders Research Circle — a Gartner-managed panel — and three were from an external sample. Participants from North America (37), EMEA (29), Asia/Pacific (7) and Latin America (11) responded to the survey.The survey was developed collaboratively by a team of Gartner analysts and Gartner's Research Data, Analytics and Tools team.

Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[1] Executive Order on Improving the Nation's Cybersecurity, The White House.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer

support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Stratégie géographique : la stratégie du fournisseur pour orienter les ressources, les compétences et les offres afin de répondre aux besoins spécifiques des zones géographiques en dehors de la zone géographique "d'origine" ou d'origine, soit directement, soit par l'intermédiaire de partenaires, de canaux et de filiales, selon les besoins de cette zone géographique et de ce marché.