Magic Quadrant for Cloud Access Security Brokers

Published 28 October 2020 - ID G00464465 - 33 min read

CASBs, now essential elements of cloud security strategies, help security and risk management leaders to discover cloud services and assess cloud risk. They identify and protect sensitive information, detect and mitigate threats, and institute effective cloud governance and compliance.

Market Definition/Description

Gartner defines the cloud access security broker market as products and services that address security gaps in an organization's use of cloud services. Especially designed to protect and control access to data that's stored in someone else's systems, CASBs deliver differentiated, cloud-specific capabilities that generally aren't available as features in traditional security products. CASBs provide a central location for policy and governance concurrently across multiple cloud services and granular visibility into and control over user activities and sensitive data from both inside and outside the enterprise perimeter, including cloud-to-cloud access.

The core functionality areas (previously described as "pillars") of products in the CASB category include:

- Visibility. Detect all cloud services; assign each a risk ranking; identify all users and third-party apps able to log in
- Data security. Identify and control sensitive information (data loss prevention [DLP]); respond to classification labels on content
- Threat protection. Offer adaptive access control (AAC); provide user and entity behavior analysis (UEBA); mitigate malware

- Compliance. Supply reports and dashboards to demonstrate cloud governance; assist efforts to conform to data residency and regulatory compliance requirements

  Other functionality is present and includes, but isn't limited to:

- Provide threat intelligence and incident response workflows
- Assign classification labels to content
- Encrypt structured and unstructured data; tokenize structured data
- Integrate with enterprise DLP products
- Combine CASB capabilities with those typical for secure web gateways (SWGs) to provide a blended offering
- Perform cloud security posture management (CSPM) for IaaS and PaaS workloads and SaaS security posture management (SSPM) for SaaS applications.

  While they're important, Gartner doesn't deem these extensions to be core to its product definition.

  Note to the reader. This year's analysis style has changed from that of prior years and follows a specific format as defined in Gartner's Magic Quadrant methodology.

Magic Quadrant

Figure 1: Magic Quadrant for Cloud Access Security Brokers
Source: Gartner (October 2020)

Vendor Strengths and Cautions

Bitglass

Bitglass is a Leader in this Magic Quadrant. Its CASB is broadly applicable across the full range of requirements and use cases for effective SaaS security and governance, offering well-developed capabilities in all core and most optional functionality areas. Its operations are mostly in North America and Europe, plus a smaller presence in the Asia/Pacific region and South America. Its customers tend to be large enterprises in many industries. In 2020, Bitglass released a highly functional endpoint agent that adds

capabilities for zero trust network access (ZTNA) and SWGs. Beginning in October 2019, Bitglass CASB is in process for FedRAMP ATO at the Moderate impact level.

Strengths

- The AJAX-VM JavaScript enforcement code, delivered to the browser's document object model, continues to set Bitglass apart from the competition by providing a greater degree of visibility and control for activities on unmanaged devices interacting with managed SaaS applications.
- A new endpoint agent, along with in-browser JavaScript implementations of RDP and SSH, enables use cases beyond traditional CASBs to provide secure internet access and threat prevention (SWG), advanced threat protection (remote browser isolation [RBI]), access to private applications (ZTNA) and high levels of SaaS control from a single vendor managed with a single console.
- Data uploaded into structured applications can be recorded with attributes that can be used to define adaptive access rules. For example, a location tag can restrict access such that only those users in the specific location can access data to enforce data sovereignty requirements.

Cautions

- The policy builder user interface is dated. It displays an application-centric focus rather than a function-centric focus, which may result in inconsistencies across policies that are intended to enforce equivalent actions on multiple SaaS applications.
- Automatically remediating risky configurations through the CSPM for IaaS is limited compared to the competition. While well-integrated into the console, the CSPM hasn't been identified by Gartner clients as a suitable replacement for a stand-alone tool.
- Although its visibility in the market has improved from last year, Bitglass is not as frequently mentioned during Gartner client inquiries as some of the other vendors in the CASB market.

Broadcom (Symantec)

Broadcom (Symantec) is a Challenger in this Magic Quadrant. Its CASB, CloudSOC, is mainly focused on the core functionality areas and, via a separate console included in most product configurations, offers DLP harmonization across CASBs, SWGs, secure email gateways (SEGs), ZTNA and endpoints. Its operations are mostly in North

America, plus a smaller presence in Europe, South America and the Asia/Pacific region. Its customers tend to be large enterprises in many industries. In 2019, Broadcom, a hardware vendor with little history of software development or integration, acquired Symantec's enterprise security software products.

Strengths

- CloudSOC includes a wide range of predefined DLP selectors based on common data formats and types, dictionaries, file type detection, fingerprinting, and similarity matching that can be trained from a collection of positive and negative content.
- Adaptive access controls can be built from a sequence of selectable detectors, including thresholds, threats, behaviors, devices, user locations and sequences. Step-up authentication is possible for many types of policies.
- CloudSOC's CSPM is functional, satisfies typical requirements and can automatically remediate certain risky configurations.

Cautions

- The administrative interface appears dated and can be cumbersome at times, occasionally requiring moving between multiple areas to completely configure a single policy. This is particularly noticeable when working with DLP policies.
- CloudSOC provides fewer options for data visibility and interception than competitors. RBI (Web Isolation) is available as a separately priced add-on. Reverse proxy is slated to be discontinued and replaced by an SAML-integrated RBI (Mirror Gateway), which is delayed until the end of 2020.
- After the acquisition of Symantec's enterprise security software products, product development slowed compared to the competition. Execution also suffered; many Gartner clients expressed dissatisfaction with the vendor's apparent lack of interest in maintaining business and support relationships. Many clients are not renewing and instead are evaluating other vendors.

CipherCloud

CipherCloud is a Visionary in this Magic Quadrant. Its CASB is broadly applicable across all core and some optional functionality areas, and continues to serve as a good choice for organizations requiring high degrees of data confidentiality within SaaS applications. Its operations are mostly in North America and Europe. Its customers tend

to be midsize and large enterprises in many industries. Throughout 2020, CipherCloud expanded into several adjacent categories, including built-in ZTNA and SWG, along with SD-WAN and web application firewall integrations.

Strengths

- The interface is uncluttered, and the workflow for creating new policies is easy to understand and manage. Administrators can get up to speed and create effective policies quickly.
- CipherCloud's continued support for encryption and tokenization makes it suitable for organizations requiring a high degree of confidentiality of data stored in cloud applications.
- CSPM is well-developed, follows several common frameworks and can replace stand-alone tools. The SSPM offering is more advanced than most competitors and can automatically remediate risky configurations in some circumstances.

Cautions

- The ability to create fine-grained policies that distinguish between and alter the experience for managed versus unmanaged endpoints is minimal compared to other providers.
- Unlike most of its competitors, CipherCloud hasn't added RBI to its mechanisms for steering traffic, although it is a part of the vendor's roadmap and should be available by the end of 2020. RBI eliminates potential problems with URL rewriting required by reverse proxies.
- CipherCloud does not have the level of market share and client visibility that other leading CASB vendors enjoy, and it appears less frequently on competitive shortlists and in Gartner client inquiries.

Forcepoint

Forcepoint is a Visionary in this Magic Quadrant. Its CASB is mainly focused on adding a layer of SaaS visibility and control to its existing portfolio of products, aimed at its existing customers. Its operations are mostly in North America and Europe, plus a smaller presence in South America and the Asia/Pacific region. Its customers tend to be large enterprises in many industries. In 2020, Forcepoint integrated its CASB DLP with its cloud-based Data Protection Service. Beginning in April 2020, Forcepoint Dynamic

Cloud Solutions for CASB is in process for FedRAMP ATO at the Moderate impact level. In October 2020, Francisco Partners signed an agreement to acquire Forcepoint from Raytheon Technologies; this announcement has no bearing on Forcepoint's evaluation in the Magic Quadrant analysis..

Strengths

- Forcepoint SWG customers can combine SWG and CASB policies to block access to cloud services determined to be too risky. Forcepoint's cloud DLP presents a single policy engine across multiple products — a combination that reduces policy duplication.
- For user-centric dashboard and event processing, the interface is well laid out. It shows all cloud activities in the context of a user, which allows administrators to easily investigate a user's overall and detailed behavior.
- The product computes a business impact analysis score for each activity that users perform in SaaS applications. Scores reflect predefined, distinct per-application severity and simplify the creation of policies that manage risky behavior across a collection of applications.

Cautions

- Remote browser isolation is available through a partnership with Ericom Software, but needs to be better integrated into the CASB policy builder engine.
- CSPM operates only through proxying access to the IaaS console. Any nonconsole configuration settings and changes cannot be detected or evaluated.
- While Forcepoint offers a mechanism to apply risk scores to monitored events in governed SaaS applications, the CASB lacks SSPM, a capability that other vendors have begun showing this year.

McAfee

McAfee is a Leader in this Magic Quadrant. MVISION Cloud has expanded into several categories, including CASB, CSPM, cloud workload protection platform (CWPP), container security, SSPM and SWG. The CASB is broadly applicable across the full range of requirements and use cases for effective SaaS governance, offering well-developed capabilities in core and optional functionality areas. Its operations are mostly in North America and Europe, with a smaller presence in the Asia/Pacific region. Its

customers tend to be large enterprises in many industries. In 2020, McAfee introduced “micro POPs” — portions of MVISION Cloud that customers can install inside their IaaS environments to conduct scanning and assessment of resources not externally visible. In April 2020, McAfee MVISION Cloud achieved FedRAMP ATO at the High impact level.

Strengths

- A wide array of policies can take full advantage of API inspection, forward-proxy redirection, reverse-proxy insertion and RBI, facilitated by a single agent that directs traffic to McAfee’s CASB or SWG.
- The Mitre ATT&CK framework is well-supported in the interface for incident investigation and response.
- McAfee offers extensive CSPM capabilities that exceed those of even some pure CSPM vendors for IaaS/PaaS and SaaS. It includes strong auditing and compliance scanning, plus multiple options for automatic and guided manual remediation.

Cautions

- McAfee’s position is that managed devices interacting in predictable ways should be given direct access to SaaS collaboration applications and not passed through the forward or reverse proxy. Customers will need to assess whether this stance aligns with their supported enterprise security policies.
- UEBA is functional, but there is a not a “user risk score” perspective that is both dynamic and informed by its advanced analytics, when compared to some of its competitors.
- McAfee is still regarded as a large heritage security vendor by a number of Gartner clients and may struggle with perception issues, especially among organizations adopting a cloud-first strategy.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its CASB, Cloud App Security (MCAS), is mainly focused on the core functionality areas and works best when supplemented with other Microsoft security products. Its operations are geographically diversified. Its customers tend to be midsize and large enterprises in many industries. During 2020 and into 2021, Microsoft continues to emphasize endpoint-based and cloud-based controls,

directing attention away from the network. Beginning in May 2019, MCAS (as part of Office 365 GCC High) is in process for FedRAMP ATO at the High impact level.

Strengths

- Microsoft has consolidated disparate classification mechanisms into one shared across MCAS, Office 365, Azure Information Protection (AIP), Rights Management Services (RMS) on-premises and Windows Information Protection (WIP) on endpoints. DLP actions are comprehensive and can even send real-time notifications of violations (with requests for business justification overrides) through Teams. The list of common sensitive data types is frequently updated.
- Power Automate (previously Flow), an extra cost item, allows administrators to build playbooks to automate incident response workflows across all governed SaaS applications. MCAS's integration with Flow was distinctive compared to other CASB vendor integrations with third-party security orchestration, analytics and reporting (SOAR) tools.
- The UEBA interface displays a useful consolidated view of a single account's activities across multiple cloud services. MITRE ATT&CK labelling is displayed in some event analysis views to further assist investigation.

Cautions

- A typical Microsoft cloud security strategy will require multiple Microsoft products, not just its CASB. Examples include Azure Active Directory Conditional Access for AAC, Azure Information Protection for EDRM, Azure Security Center for CSPM, Endpoint Manager (previously Intune) for unified endpoint management (UEM) and Defender for Endpoint for endpoint protection platforms (EPPs). Microsoft's cloud security products work best when customers deploy the entire suite; stand-alone or a la carte deployments offer reduced functionality.
- The lack of support for webhooks and the lack of RBI and SWG capabilities reduce the number and types of sources of information for traffic and data visibility.
- Microsoft's licensing is overly complex. Multiple confusingly named bundles include MCAS or Office 365 Cloud App Security, a lightweight version of the full CASB that works only with Office 365. Clients occasionally discover that they have access to more

of Microsoft’s security products than expected when they review the details of enterprise licensing agreements.

Netskope

Netskope is a Leader in this Magic Quadrant. It has expanded into related categories, including ZTNA and SWG. Its CASB is broadly applicable across the full range of requirements and use cases for effective SaaS governance, offering well-developed capabilities in core and optional functionality areas. Its operations are mostly in North America, plus a smaller presence in South America, Europe and the Asia/Pacific region. Its customers tend to be large enterprises in many industries. Netskope’s roadmap exhibits meaningful progression toward a SASE framework. In September 2019, Netskope Security Cloud Government achieved FedRAMP ATO at the Moderate impact level.

Strengths

- Netskope has expanded into a portfolio vendor offering a wide range of cloud security and cloud-delivered security capabilities, including ZTNA, SWG, RBI (through a partnership with Ericom Software) and CSPM, consistently managed in a single console. Netskope’s progress in the SASE framework is farther along than any other vendor in this Magic Quadrant.
- Access control policies supply several opportunities to coach users in a variety of scenarios, including suggestions with links to appropriate applications. Device posture policies can signal an endpoint protection tool (for example, CrowdStrike and VMware Carbon Black) to take various actions, including isolation from governed SaaS applications.
- Netskope made numerous improvements to its CSPM capabilities this year and has also begun offering basic SSPM.

Cautions

- Netskope’s reverse proxy supports fewer SaaS applications than some of its competitors.
- Some Gartner clients continue to express concern over the need to install agents to achieve maximum value from the product, and have observed that Netskope’s utility in agentless scenarios is less mature than some competitors.

- A small number of clients have expressed concern about the complexity of Netskope's pricing and contracts.

Proofpoint

Proofpoint is a Challenger in this Magic Quadrant. Its CASB is mainly focused on core and some optional functionality areas, and is an effective complement to its SEG. Its operations are mostly in North America, with a smaller presence in Europe. Its customers tend to be large enterprises in many industries. Proofpoint's attention to SaaS threats, especially insider threats, is distinctive in the CASB market, and is spread across CASB, SEG and EPP.

Strengths

- Inbound actions to cloud services are risk-scored, based on behavior and privileges of users. Users who exhibit a propensity for being attacked the most (labeled "very attacked persons" in the administrative interface) can be placed into groups that minimize their exposure.
- Proofpoint's CASB, ZTNA, email security and RBI products offer useful synergies, which may be an attractive integration and bundle for some customers, particularly those with a large remote workforce.
- Once a new threat is detected, Proofpoint can reevaluate prior events to determine whether that threat was previously missed, and assess whether its actions were malicious or benign.

Cautions

- Proofpoint offers basic CSPM capabilities in its CASB through API-based analysis of IaaS configuration settings. It cannot proxy the IaaS console and it offers no DevOps-style guardrails for automated compliance and policy enforcement.
- Support for custom applications is minimal and limited to "well understood" HTML events. More sophisticated control of custom apps requires vendor involvement.
- The vendor lacks a native SWG, unlike several of its competitors. Also unlike several competitors, Proofpoint has removed reverse proxy from its CASB; however, the SAML-proxy-based RBI can accommodate common reverse-proxy use cases.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

No vendors were added to this Magic Quadrant.

Dropped

Palo Alto Networks was dropped from this Magic Quadrant. The vendor failed to meet certain product configuration and feature inclusion criteria.

Inclusion and Exclusion Criteria

To qualify for inclusion, vendors need to meet these criteria:

- Availability. CASB product must be generally available and fully supported.
- Revenue and deployment. CASB product revenue and CASB deployment must match one of the following minimums:
  - At least $60 million in revenue in the 12 months preceding 1 June 2020, and at least 500 distinct customers (logos) and at least 2,000,000 seats deployed, or
  - At least $24 million in revenue in the 12 months preceding 1 June 2020, and at least 30 new distinct customers (logos) during the same period, or
  - At least $8 million in revenue in the 12 months preceding 1 June 2020, and at least 20 new distinct customers (logos) during the same period
- Geography. Currently deployed in production by customers in at least two of the following regions:
  - Americas
  - Europe
  - Asia/Pacific

- Middle East/Africa

- Features. Product capabilities must include the following:
  - Inspect data and user behavior in cloud services via provider APIs.
  - Operate in-line between users and cloud services as a forward and/or reverse proxy, or optionally offer RBI as an alternative or supplement to reverse proxy (essentially be a multimode CASB and not API-only).
  - Support the ability to perform access control of any user, device and location.
  - If an endpoint agent is available for traffic steering, it must support Windows, macOS, iOS and Android; it must support deployment by software management tools.
  - Integrate with an enterprise's existing identity provider, security incident and event management tool, and UEM product.
  - Operate as a multitenant service delivered from the public cloud.
  - Optionally operate as a virtual or physical appliance in on-premises, colocation or public cloud environments.
  - Apply a variety of analytics when monitoring behavior of users, third-party apps and data.
  - Identify and respond to malicious and/or unwanted sessions with multiple methods (for example, terminate, allow, restrict, raise alert, step-up authentication and end-user coaching).
  - Distinguish between corporate and personal instances of cloud services and provide the ability to limit or block the exchange of data between them.
- Applicability. The product must support governing a minimum of 10 named SaaS applications, with the following distribution:
  - At least seven via API inspection
  - All 10 via forward proxy or all 10 via reverse proxy/remote browser isolation

  Products and vendors will be excluded if they:

- Rely principally on legacy products such as on-premises firewalls or on-premises SWGs to deliver CASB-like functionality.
- Fail to materially address all four core functionality areas (visibility, data security, threat protection and compliance).
- Fail to meet Gartner's installed base, deployment and revenue requirements.

Evaluation Criteria

Ability to Execute

Product or Service: This criterion refers to innovative and effective cloud visibility and control capabilities with rapid reaction to changes in SaaS application functionality and the speed/accuracy of SaaS application risk ranking. It includes strong and accurate DLP capabilities that rival enterprise DLP products, including mechanisms for identifying and classifying content at various sensitivity levels. Products that favor protection and control as much as or more than visibility are more highly rated, and the ability to provide (or work with other tools to orchestrate) AAC for users, devices and content to/from cloud services are weighted higher.

Overall Viability: This refers to sustained funding sources (venture capital or otherwise), including positive year-over-year growth in customers, seats and revenue. There should be evidence of continual investment in product development and sales.

Sales Execution and Pricing: This criterion includes pricing that places few restrictions on which SaaS applications and features can be used, with reasonably priced visibility use cases. Vendors should be able to successfully compete in deals that displace incumbents because of better value and customer use-case alignment with effective sales, presales and marketing teams, and win on highly competitive shortlists.

Market Responsiveness and Track Record: This refers to the vendor's ability to develop innovative security controls faster than competitors, addressing a wide range of use cases, and mitigating cloud security threats quickly.

Marketing Execution: This criterion assesses whether the vendor addresses well-defined use cases that highlight the value of a CASB over native cloud security controls. Also evaluated is whether the vendor provides well-articulated details about how traffic

is steered and processed, with a demonstrated track record of reducing customer risk posture.

Customer Experience: This refers to whether day-to-day operations can be performed by existing customer personnel. There is no significant change to the end-user experience with or behavior of cloud services after deployment. Also evaluated is whether there is a support escalation path that permits communicating, when the severity is appropriate, with vendor support resources (including engineers at the highest severity levels).

Operations: This criterion was not evaluated in this Magic Quadrant iteration.

Table 1: Ability to Execute Evaluation Criteria

Enlarge Table

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	NotRated

Source: Gartner (October 2020)

Completeness of Vision

Market Understanding: This refers to the correct blend of visibility, protection and control capabilities that meet or exceed the requirements for native cloud security features. Innovation, forecasting customer requirements and being ahead of competitors on new features are also regarded, as well as integration with other security products and services. Finally, vendors must solve challenging problems associated with the use of multiple cloud services by organizations of all sizes.

Marketing Strategy: An understanding of and commitment to the security market, the prevailing threat landscape and, more specifically, the cloud security market are evaluated. A focus on security as a business enabler over security for the sake of compliance is important, as is avoidance of unrealistic promises (like “unbreakable,” “impenetrable,” etc.). Marketing messages must align with actual product and service deliverables.

Sales Strategy: This criterion includes a recognition that SaaS (and SaaS security) and other cloud service buyers are not always from IT departments. Pricing and packaging that is familiar to cloud-using organizations, including immediate after-sales assistance with deployment, are weighted. Periodic follow-up contact with existing customers must be evident, along with a capable channel program that enables consistency and high-quality access to the product or service to organizations in all available geographic locations.

Offering (Product) Strategy: Well-regarded products must show the full breadth and depth of SaaS application support, the ability to react quickly to changes in cloud applications, and strong and action-oriented user behavior analytics. In addition, they must have successful completion of third-party assessments (such as ISO 27001 or SOC 2), a well-rounded roadmap with a sustained feature cadence and support for custom applications in IaaS.

Business Model: The process and success rate for developing new features and innovation through investments in research and development are evaluated. This includes a demonstrated understanding of the particular challenges associated with securing multiple cloud applications and a track record of translating that understanding into a competitive go-to-market strategy.

Vertical/Industry Strategy: This criterion evaluates evidence of product design and functionality to address the distinct nature of industry-specific, above-average requirements for controlling sensitive information and satisfying regulatory demands. It also evaluates evidence of deployment in multiple verticals, with multiple cloud services and multiple customer sizes. Pricing should be tailored for realistic availability of funds and budgets for multiple, varied industry segments.

Innovation: This criterion includes evidence of continued research and development with quality differentiators, such as performance, management interface and clarity of reporting. Features should be aligned with the realities of the distributed nature of cloud security responsibility (for example, consoles for various security/audit roles and consoles for business units' administration of their portions of policies). Included are a roadmap showing a platform focus, continued support for more cloud services and strategies for addressing evolving threats — including advanced threat detection and mitigation capabilities, with a strong in-house threat and risk research group.

Geographic Strategy: Third-party attestations relevant to regions in which the product is sold and an ability to help customers meet regional compliance requirements are weighted. The vendor should have an effective channel that delivers consistent messaging and support in every available geography.

Table 2: Completeness of Vision Evaluation Criteria

Enlarge Table

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Medium
Offering (Product) Strategy	High

Evaluation Criteria	Weighting
Business Model	Low
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Low

Source: Gartner (October 2020)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced progress and effort in all execution and vision categories. Their actions raise the competitive bar for all products in the market, and they can change the course of the industry. To remain Leaders, vendors must demonstrate a track record of delivering successfully in enterprise CASB deployments, and winning competitive assessments. Leaders produce products that embody all CASB capabilities and architectural choices, provide coverage of many cloud services, innovate with or ahead of customer challenges, and have a wide range of use cases. Leaders continually win selections and are consistently visible on enterprise shortlists. However, a leading vendor is not a default choice for every buyer, and clients should not assume that they should buy only from vendors in the Leaders quadrant.

Challengers

Challengers offer products that address the typical needs of the market, with strong sales, large market share, visibility and clout that add up to higher execution than Niche Players. Challengers often succeed in established customer bases; however, they do not often fare well in competitive selections, and they generally lag in new or improved feature introductions or architecture choices.

Visionaries

Visionaries invest in leading-edge/“bleeding-edge” features that will be significant in next-generation products, and that give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they lack the execution skills to outmaneuver Challengers and Leaders.

Niche Players

Niche Players offer viable products or services that meet the needs of some buyers with more narrowly defined use cases. Niche Players are less likely to appear on shortlists, but they fare well when given the right opportunities. Although they might lack the clout to change the course of the market, they should not be regarded as merely following the Leaders. Niche Players may address subsets of the overall market (for example, the small and midsize business [SMB] segment, a vertical market or a specific geographic region), and they often do so more efficiently than Leaders. Niche Players can be smaller vendors that don’t yet have the resources or features to meet all enterprise requirements, or larger vendors that operate in a different market and haven’t yet adopted the CASB mindset.

Context

Gartner continues to receive hundreds of inquiries each year from clients asking about how to select and implement a CASB. Common scenarios for CASBs enable security and risk management leaders to conduct useful comparisons of vendors across core sets of features in competitive environments. We advise starting with a reasonably detailed list of scenarios that are specific to your exact needs — the use cases in this research represent a starting point. From there, you should develop a proof of concept (POC) that will simplify the decision process and lead to a clear preference.

The CASB market has reached a point of relative stability. All vendors offer a variety of mechanisms that improve visibility and control of an ever-expanding list of cloud services. All vendors have sought, to varying degrees, ways to differentiate by adding capabilities beyond those necessary for addressing classic CASB use cases. For these reasons, the 2020 Magic Quadrant contains no Niche Players.

Full-featured CASBs provide more capabilities, for more cloud services, and for a wider array of enterprise use cases to protect data in and govern cloud services than do other security products. This agility still outpaces the security features delivered by cloud

service providers and by vendors that offer a subset of CASB features as an extension of their existing security technologies, such as firewalls and web gateways. Products from vendors with a cloud-first development strategy exhibit a deeper understanding of users, devices, applications, transactions and sensitive data than do products containing CASB functions delivered as add-ons to traditional network security tools.

Buyers need to look past a CASB provider's list of supported applications and services and closely examine how CASBs of interest specifically support the cloud applications they use now and plan to use in the future. To make a more informed purchase decision, buyers are advised to compile a comprehensive inventory of their end-user computing environments (including managed and unmanaged devices), the cloud services being accessed, the data stored in those services and the actions they want to monitor.

The CASBs in this research offer comprehensive protection and governance of many, but not all, popular and strategic SaaS applications when accessed from managed devices. However, substantial differences arise around edge cases, such as governing uncommon SaaS applications, governing applications that lack published APIs and controlling activity on unmanaged devices. Differences also arise when comparing integration with adjacent security tools, such as identity providers, log management and reporting systems, and incident response tools.

Of particular importance is a CASB vendor's choice to support only cloud APIs or to include in-line mechanisms, such as forward or reverse proxy or RBI. Providers that offer a combination of API plus at least one in-line mode are called "multimode CASBs." This architecture decision fundamentally defines how CASBs can perform different actions, with implications for how that provider delivers across the four pillars for a specific cloud service. Gartner clients overwhelmingly prefer CASBs that offer multimode operation because they provide the most flexibility. In this year's iteration of the CASB Magic Quadrant research, all vendors are multimode, but not all vendors offer the same set of in-line modes.

As cloud service APIs improve and expose greater amounts of visibility, improved degrees of control and, sometimes, near-real-time performance, the need for in-line traffic interception, especially via forward proxy, might slowly diminish eventually. While a small number of the most prominent cloud application and service providers publish public APIs, it remains the case that the majority of less popular or industry-specific

SaaS applications offer no APIs for external visibility or control, so the need for in-line visibility via proxying is unlikely to completely disappear.

Market Overview

- Vendors offer feature-rich products to increase cloud visibility and apply consistent policy across multiple providers. Execution across all vendors is variable: While some have incrementally improved and added new capabilities, the leading vendors continue to make significant investments that have contributed to the rapid maturation of the market. The acquisition phase of the market has ceased. Major incumbent security vendors now offer a CASB, either stand-alone or as part of a product portfolio; integration with other products in portfolios is inconsistent but improving. While the number of independent vendors has stabilized, the most relevant independent vendors demonstrate sustained innovation and broad market reach. Differentiation among vendors is becoming difficult, and several have branched beyond SaaS governance and protection to include custom application support in IaaS clouds, CSPM and SSPM capabilities, and UEBA features. Many also now offer capabilities that extend the utility of CASB, such as SWG, ZTNA and RBI.

- The most relevant independent vendors continue to receive venture capital funding, while funding for the less-well-known private vendors remains uncertain. The pace of client inquiry indicates that CASB is a popular choice for cloud-using organizations. Gartner’s 2020 security spend forecast predicts a significant, but slowing growth rate for CASB: 37.2% in 2021, 33.2% in 2022, 32.0% in 2023 and 30.5% in 2024. Although the forecast predicts slowing spend for all security markets, CASB’s growth remains higher than any other information security market (see Forecast: Information Security and Risk Management, Worldwide, 2018-2024). Five IT trends drive and sustain the CASB market:

- The enterprise moves away from traditional devices. The popularity with which organizations have offered non-PC devices for interacting with core business processes creates security risks that can be mitigated effectively with a CASB. CASBs enable safer interaction between SaaS applications and unmanaged devices, too, via policies that enable adaptive access for bring your own device (BYOD) users and business partners.

- The enterprise moves to cloud services. Cloud adoption shows no signs of slowing; Gartner expects SaaS spending to remain double that of IaaS (see Forecast: Public Cloud Services, Worldwide, 2018-2024, 2Q20 Update). The need to govern cloud use and demonstrate that governance is in place is clear. Significant amounts of spending and computing will aggregate around cloud service providers. This affects on-premises-based technology in the long term, including the security software and appliance markets.
- Intense cloud investments by vendors. Most large enterprise software providers continue to intensify their investments in the cloud, and are actively moving their large installed bases to their cloud services. The periodic enterprise software upgrade cycle has shifted to a subscription model characterized by continuous feature updates. Enterprise security teams will need CASB-like features to deal with the security implications of that evolution.
- A growing and uncertain regulatory environment. Regulations such as the General Data Protection Regulation (GDPR) and the Clarifying Lawful Overseas Use of Data (CLOUD) Act require organizations to understand where their data is, now that it is being shared with and among cloud services.
- A huge spike in remote working, as well as unmanaged device usage. This trend has compelled organizations to move even more rapidly to cloud services, particularly SaaS, as it enables critical business functions to work without the traditional friction associated with relying on VPNs to access internal applications in enterprise data centers. CASBs secure access to these applications and allow for workable guardrails to be in place for more risky scenarios.
- The forces of cloud and mobility fundamentally change how data and transactions move between users and applications. Consequently, cloud-using organizations will need to adjust the priorities of investment in security controls.
- To broaden their range of use cases, most CASB vendors have added CSPM, and a few have added SSPM, capabilities to their products. CSPM assesses and manages the security posture of the IaaS and PaaS cloud control plane, while SSPM evaluates the native security configurations of common SaaS applications. The better offerings provide this across multiple providers for consistent policy enforcement. For large, IaaS-based workload deployments, CSPM capabilities should be considered mandatory from your CASB; this research favors vendors that have moved in the combined CASB-plus-

CSPM direction. Although there are some CSPM-only vendors, they are finding it tougher to compete against vendors offering combined CASB and CSPM, as well as combined CWPP and CSPM products.

- SASE: Cloud-Delivered Security Convergence: Gartner draws a distinction between delivering security from the cloud and securing access to the cloud. Nevertheless, the common means for creating such distinctions are blurring; several formerly separate categories and markets are converging into the secure access service edge (SASE). This emerging framework combines comprehensive WAN capabilities with comprehensive network security functions — such as SWG, CASB, firewall as a service (FWaaS), RBI and ZTNA — to support the dynamic secure access needs of digital enterprises. The Future of Network Security Is in the Cloud describes this convergence. Important to this Magic Quadrant, CASB vendors that recognize and show movement toward SASE (either in their shipping products or in their roadmaps) demonstrate better vision than those that have not.

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.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.


Craig LawsonVP Analyst

Steve RileySr Director Analyst