Magic Quadrant for Cloud Access Security Brokers

Published: 29 October 2018 **ID:** G00348564

Analyst(s): Craig Lawson, Steve Riley

Cloud access security brokers have become an essential element of any cloud security strategy, helping organizations govern the use of cloud and protect sensitive data in the cloud. Security and risk management leaders concerned about their organizations' cloud use should investigate CASBs.

Strategic Planning Assumptions

By 2022, 60% of large enterprises will use a CASB to govern some cloud services, up from less than 20% today.

Through 2023, at least 99% of cloud security failures will be the customer's fault.

Market Definition/Description

Gartner defines the cloud access security broker (CASB) market as products and services that address security gaps in an organization's use of cloud services. This technology is the result of the need to secure cloud services — which are being adopted at a significantly increased rate — and access to them from users both within and outside the traditional enterprise perimeter, plus growing direct cloud-to-cloud access. They deliver differentiated, cloud-specific capabilities generally not available as features in other security controls such as web application firewalls (WAFs), secure web gateways (SWGs) and enterprise firewalls. CASB vendors understand that for cloud services the protection target is different: it's still your data but processed and stored in systems that belong to someone else. CASBs provide a central location for policy and governance concurrently across multiple cloud services — for users and devices — and granular visibility into and control over user activities and sensitive data.

CASB coverage scope applies broadly across the SaaS, PaaS, and IaaS cloud service delivery models. For SaaS coverage, CASBs commonly work with the most popular content collaboration platform (CCP), CRM, HR, ERP, service desk, office productivity suites, and enterprise social networking sites. Some CASBs extend support to less common SaaS applications through custom plug-ins or automated learning of application behavior. For IaaS and PaaS coverage, several CASBs govern the consoles of popular cloud service providers (CSPs) and extend visibility and governance to applications running in these clouds. Several CASBs now also offer cloud security posture

management (CSPM) capabilities to assess and reduce configuration risk in IaaS, PaaS, and SaaS cloud services, sometimes by reconfiguring native security controls directly in cloud services. However, IaaS and PaaS governance are new for almost every CASB, and therefore not yet as developed as SaaS governance. A few CASBs can be deployed in front of enterprise web-enabled applications to bring these under a consistent cloud service management framework, although this is an uncommon scenario.

CASBs deliver functionality through four pillars:

- **Visibility.** CASBs provide shadow IT discovery, a consolidated view of an organization's cloud service landscape, and details about the users who access data in cloud services from any device or location. Leading CASBs take this further with a cloud service security rating database to provide visibility into the trustworthiness of the CSP and associated risks it might introduce.
- **Data security.** CASBs provide the ability to enforce data-centric security policies to prevent unwanted activity based on data classification, on data discovery, and on user activity monitoring of access to sensitive data or privilege escalation. Policies are applied through controls, such as audit, alert, block, quarantine, delete and view only. Data loss prevention (DLP) features are prevalent and are one of the most commonly deployed controls after visibility. CASB DLP operates natively and in conjunction with enterprise DLP products via ICAP or RESTful API integration. Some CASBs provide the ability to encrypt, tokenize, or redact content at the field and file level in cloud services. But because encryption and tokenization outside a SaaS application can affect functionality, CASB-facilitated encryption and tokenization are not commonly used.
- **Threat protection.** CASBs prevent unwanted devices, users and versions of applications from accessing cloud services by providing adaptive access controls (AACs). Cloud application functionality can be changed based on signals observed during and after login. Other examples of CASB capabilities in this category are embedded user and entity behavior analytics (UEBA) for identifying anomalous behavior, and the use of threat intelligence, network sandboxing, and malware identification and remediation. All CASBs are primarily using OEMs of existing enterprise-grade anti-malware and sandbox tools rather than building their own. In some cases, CASB vendors have their own analyst teams researching cloud-specific and cloud-native attacks.
- **Compliance.** CASBs help organizations demonstrate that they are governing the use of cloud services. They provide information to determine cloud risk appetite and establish cloud risk tolerance. Through their various visibility, control, and reporting capabilities, CASBs assist efforts to conform to data residency and regulatory compliance requirements. Many CASB vendors have added CSPM capabilities to their products. CSPM assesses and manages the security posture of the cloud control plane, mostly for IaaS and occasionally for SaaS. The better offerings provide this across multiple public cloud providers for consistent policy enforcement.

CASB capabilities are delivered primarily as a SaaS application, occasionally accompanied by an on-premises virtual or physical appliance. SaaS delivery is significantly more popular for most use

cases. However, an on-premises appliance might be required for conformance with certain regulatory or data sovereignty rules, especially if in-line encryption or tokenization is performed.

Magic Quadrant

Figure 1. Magic Quadrant for Cloud Access Security Brokers

Source: Gartner (October 2018)

Vendor Strengths and Cautions

Bitglass

Bitglass was founded in January 2013 and began shipping a CASB in January 2014. With a focus on sensitive data discovery, classification and protection, it also includes several document management and protection capabilities, such as watermarking and encryption methods that support searching and sorting functions in SaaS applications. It uses an agentless "AJAX Virtual Machine (VM)" abstraction layer that is transparently embedded within the user's browser to support real-time data protection in specific scenarios including unmanaged devices. The AJAX VM detects and reacts to changes in underlying SaaS applications that might otherwise bypass traditional reverse proxies. Bitglass offers well-developed capabilities across all four CASB pillars. It is primarily deployed as a reverse proxy; forward proxy is also available along with API inspection support for an increased number of SaaS applications. Bitglass also offers basic mobile device management (MDM) and identity and access management as a service (IDaaS) capabilities. Bitglass runs natively from the cloud and can also be deployed as a Docker container for customers to host on-premises.

Strengths

- Trust ratings are prevalent throughout the UI. Access policies can be influenced by trust levels of users, of cloud services, and of third-party apps granted access to services.
- For browser-based access to cloud applications, the AJAX VM now includes an automated learning mode. Through this, it's possible to use Bitglass for in-line visibility and control of most existing SaaS applications without the use of custom plug-ins.
- Policies can apply watermarks to documents while being processed in line. Watermarks enable granular tracking of content for all devices, for content traversing to and from all managed cloud services, and can refine decisions made by other policies.
- DLP policies can include enterprise digital rights management (EDRM) actions that extend protection to data stored outside SaaS applications as links to read-only HTML files that require authentication or as local encrypted objects.
- Bitglass offers an extensive set of CSPM capabilities, many with guided or automatic remediation based on Center for Internet Security (CIS) Benchmarks that can be further customized as necessary.

Cautions

- The only customer-adjustable attribute in Bitglass' cloud risk database is the relative importance of a third-party attestation.
- The Bitglass CSPM capabilities do not extend to directly modifying SaaS application native security controls. IaaS CSPM for Microsoft Azure is less mature than for Amazon Web Services (AWS).

- Bitglass cannot assign or consume Azure Information Protection templates; its EDRM capability is entirely self-contained.
- While its presence has improved from last year, Bitglass is not as frequently mentioned during client inquiries as the some of the others in the CASB market.

CensorNet

CensorNet was founded in February 2007 and began shipping a CASB in April 2015. Its CASB complements existing email, web, and multifactor authentication (MFA) security products. Derived from its existing SWG, the CASB consists of on-premises appliances and on-device agents, which send only the metadata about requests to SaaS applications to CensorNet for analysis. If requests are allowed, direct user-to-cloud connections are permitted and optionally logged. Return traffic passes through CensorNet for analysis, including checking for malware (CensorNet is not a full forward or reverse proxy). CensorNet has a generalized policy engine through which a CASB administrator can define sensitive data based on content types, locations, users and other markers. CensorNet now includes some CSPM features to reveal and control actions taken inside AWS, Microsoft Azure and (to a lesser extent) Google Compute Engine. Unlike for SaaS applications, the entire request/response conversation passes through CensorNet's proxy. Entrust Datacard has acquired a minority stake in CensorNet and has taken over ownership and development of its SMS PASSCODE product.

Strengths

- The visual policy builder engine simplifies the task of creating policies that span multiple cloud services at once. Predefined templates offer good starting points for common scenarios and the drag-and-drop capabilities will be welcomed by end users for their simplicity.
- CensorNet's cloud risk assessment evaluates user behavior in SaaS apps to derive point-in-time risk scores.
- In addition to engineering staff responsible for updating the product as SaaS applications change, CensorNet runs an automated tool that continuously probes the most popular (top 50) SaaS destinations to learn about and react to changes in application architecture.
- CensorNet's combination of CASB, web, email and MFA along with its pricing structure make the product well-suited for small to midsize organizations.

Cautions

- DLP support is available (via the API only) for some cloud services, but it is primarily based on keyword matching and the use of default templates built around well-known industry compliance standards.
- Unlike the majority of CASBs with proxy mode, CensorNet lacks a reverse proxy and cannot support bring-your-own-device use cases that would require the ability to force traffic from any user on any device to traverse through the product.

- Cloud discovery and usage reporting are more rudimentary than that of the competition and lack the depth of attributes and the breadth of cloud services of other leading CASBs. Cloud telemetry is limited to that obtained via CensorNet's SWG.
- CensorNet's CSPM lacks API integration with IaaS/PaaS clouds and cannot perform the same in-depth posture evaluation as some of its competitors.

CipherCloud

CipherCloud was founded in October 2010 and has been shipping a CASB product since March 2011. CipherCloud initially emphasized field-level encryption and tokenization of structured data in popular enterprise cloud services via an on-premises gateway. Since then, it has added more cloud-based visibility and control of a broader set of SaaS applications that process and store both structured and unstructured data. Encryption and tokenization remain a strategic use case for CipherCloud, which can integrate with on-premises key management, DLP and data-centric audit and protection (DCAP) products. Its primary implementation is a reverse proxy for popular SaaS applications; it also supports forward-proxy implementations and API inspection of some cloud applications allowing for more complete multimode coverage. For CSPM capabilities, CipherCloud uses OEM technology from a CSPM vendor and exposes this through the CipherCloud console.

Strengths

- CipherCloud DLP is much improved this year and now includes selectors for exact data matching, document fingerprinting by uploading a corpus of content, and optical character recognition (OCR) in images.
- In addition to encrypting data before delivery to SaaS applications while preserving partial application functionality, CipherCloud can also manage keys for SaaS-native encryption mechanisms; these can be stored in CipherCloud or on a KMIP-compliant key management server.
- CipherCloud's default any-app connector detects common behaviors in SaaS applications, simplifying the process required for onboarding some new custom applications into the CASB.
- The interface has been improved and the workflow for creating new policies is easy to understand and manage.

Cautions

- Compared to the competition, CipherCloud's adaptive access controls are not as sophisticated and apply only at the start of a connection; continuous risk assessment during a session is less developed.
- Modifying the default any-app connector may require vendor or professional services for complex custom applications. No self-learning mode is available.
- CipherCloud does not have the level of market awareness as other CASB vendors and rarely appears on competitive shortlists or in Gartner client inquiry.

Cisco

In 2016, Cisco acquired the API-only CASB Cloudlock and bundled it into a larger offering called Umbrella. Umbrella includes several related cloud and cloud-based security offerings, which represent Cisco's strategy of growth through acquisition rather than organic development. The strategy results in a range of products that deliver traditional security capabilities from the cloud, and products that deliver cloud-native security services but that still are not yet fully integrated into the single unified offering Cisco has been promising. Cisco's plans to evolve Umbrella into a secure internet gateway (SIG) remain largely in development for now. Other Cisco products that could increase visibility to Cloudlock, like the AnyConnect VPN agent and the recently acquired Duo MFA application, are not integrated yet. Customers of all Cisco security products, including Cloudlock, receive threat intelligence from Talos, Cisco's well-regarded threat research organization. Cloudlock obtained Federal Risk and Authorization Management Program (FedRAMP) authorization at the Moderate Impact level in December 2017.

Strengths

- Policies can be configured to dynamically move users into specific groups depending on real-time assessment of behavior; these groups, in turn, can constrain certain user or application behavior, supplying an effective form of adaptive access control.
- Cisco was an early identifier of potential OAuth abuse and provides a mechanism for overriding permissions granted to OAuth tokens, thus blocking an increasingly common form of cloud attack.
- Cisco's addition of developer APIs allows organizations to extend Cloudlock to SaaS applications not natively supported and to custom applications running in IaaS clouds and on-premises.

Cautions

- As an API-only CASB, DLP support is constrained to sanctioned applications that provide APIs. It can take some time for DLP actions to occur, because SaaS APIs vary with respect to how quickly they report the movement of data. Basic DLP centers on keywords, regular expressions, and some exact data matching; it includes no support for OCR or corpus training.
- The workflow for investigating a particular user's activity is unintuitive and more cumbersome than it should be. For instance, obtaining an answer to the simple request "Show all of Alice's open shares" is not immediately obvious.
- Cisco offers no CSPM capabilities in Cloudlock.
- Cloudlock's cloud service risk scores contain fewer attributes than the competition and customers can't adjust weightings to reflect their own risk appetites and tolerances.

Forcepoint

In February 2017, Imperva sold its Skyfence CASB to Forcepoint. It has joined a series of other acquisitions to form a broad portfolio of security products and services including secure web gateway, email security, user and entity behavior analytics, DLP and data security, and network firewall. Forcepoint CASB runs primarily as a cloud service, but requires on-premises components for cloud discovery via log ingestion and for advanced DLP. Also in 2017, Forcepoint agreed to license sandboxing technology from Lastline, which is bundled with Forcepoint CASB and operates transparently to the end user, increasing threat protection capabilities. The CASB is multimode, supporting forward and reverse proxy along with API inspection.

Strengths

- The policy engine exposes a very clear who, what, how, where, when workflow. Policies contain "typical" and "unusual" predicates that are derived by using analytics. Typical predicates are behavior from the CASB learned over time and don't require further refinement; while unusual predicates can be explicitly defined.
- Forcepoint CASB analyzes both behavior (what they do) and impact (what they have access to) to calculate risk scores for individual users. These scores are risk-prioritized for security enforcement.
- Its cloud service discovery capabilities pragmatically focus on business applications and exclude extraneous services such as travel booking sites, wikis, etc.
- Existing Forcepoint secure web gateway customers can combine SWG and CASB policies to block access to cloud services determined to be too risky. Similarly, existing Forcepoint DLP customers can extend policies for Forcepoint CASB.

Cautions

- Forcepoint relies on its separate on-premises DLP product to configure policies that include fingerprinting, matching against a corpus, and OCR, while enforcement can occur at the CASB in the cloud. The CASB's native DLP is rudimentary in comparison and includes only simple policy elements such as keywords and regular expressions.
- Support for custom applications requires writing XML files that map application behavior to CASB policy elements. The lack of automated learning makes this less useful than some competitors' offerings, especially as applications change over time.
- CSPM capabilities rely entirely on routing IaaS console activity and workload automation tools through the proxy; Forcepoint itself doesn't interact with IaaS provider APIs and thus can't alter native cloud service security settings.
- Access control policies cannot be configured to coach users toward preferred SaaS applications, a feature that's common in other CASBs and often requested by Gartner clients.

McAfee

In January 2018, McAfee closed its acquisition of Skyhigh Networks, thus augmenting its existing security portfolio of DLP, SWG, network sandboxing, and more. Skyhigh was founded in December 2011 and began shipping a CASB in January 2013. McAfee Skyhigh Security Cloud was one of the first CASB products to raise awareness of shadow IT. Over time, the product expanded to provide thorough coverage of all four CASB pillars across a broad range of cloud services and now includes significant CSPM capabilities. Several well-developed controls are available including encryption and tokenization of structured and unstructured data, UEBA, and a comprehensive DLP engine with a broad array of selectors. The CASB is primarily deployed for API inspection with some reverse-proxy mode; forward proxy is also possible but less common. An on-premises virtual appliance is available for customers requiring it. McAfee has adjusted its pricing and simplified its licensing. Skyhigh (preacquisition) obtained FedRAMP authorization at the Moderate Impact level in November 2017.

Strengths

- McAfee supplies a comprehensive dashboard with several views of cloud security analysis and remediation recommendations, some of which can be automated. Remediations can configure actions in network firewalls, SWGs and endpoint security products.
- McAfee has made considerable improvements in mechanisms for investigating open shares, including a visualization graph that maps connections between objects. The Lightning Link feature hooks into sharing events and applies actions to triggers before the trigger completes, which makes API-based control over sharing behave in near real time.
- Mechanisms for achieving effective visibility and control over sensitive content has been one of the key improvements since the previous iteration of this CASB Magic Quadrant. The product offers several options for detecting, labeling, and reacting to sensitive information on managed and unmanaged devices, in sanctioned and unsanctioned cloud services.
- Creating DLP policies for custom applications requires no coding; a recording extension observes behavior as the app is exercised and finds elements of the application (fields, variables, files) that can be used in DLP selectors.
- McAfee offers extensive CSPM capabilities that exceed those of even some pure CSPM vendors. It includes strong auditing and compliance scanning plus multiple options for automatic and guided manual remediation.

Cautions

- Configuring error messages to coach users toward sanctioned applications requires the use of a separate web proxy.
- Even though Lightning Link can capture and stop disallowed sharing in real time via APIs, users aren’t always notified within the application that the behavior was blocked.

- McAfee customers must now contend with two DLP engines across the Skyhigh fabric. It is not clear when working with DLP which engine will perform the scanning and enforcement or how the two can synchronize policies.
- McAfee's execution through acquisitions has been spotty. While the Skyhigh Security Cloud seems unaffected now, customers are advised to monitor the situation for potential service degradation and execution against roadmap commitments.

Microsoft

In September 2015, Microsoft completed its acquisition of Adallom, a CASB that had been shipping since early 2013. Microsoft Cloud App Security (MCAS) is now a reverse-proxy-plus-API CASB available stand-alone and as part of Microsoft's Enterprise Mobility + Security (EMS) suite. While MCAS alone offers features that touch each of the four pillars of CASB, more complete functionality requires the EMS suite (which can be purchased stand-alone or in a bundle called Microsoft 365 that combines EMS with Office 365 and Windows 10). The suite includes MCAS, Azure Active Directory (including Azure AD Conditional Access and Azure AD Identity Protection), Azure Information Protection, Advanced Threat Protection, Advanced Threat Analytics, and Intune. Although Gartner clients routinely question whether they need the larger Microsoft suites, the bundling has overall been successful for Microsoft: MCAS has experienced large increases in number of customers and seats deployed. Certain Office 365 subscriptions include Office 365 Cloud App Security (OCAS), a subset of MCAS with fewer features and designed to protect only an Office 365 tenant (and no other SaaS applications).

Strengths

- The MCAS user interface is intuitive and contains numerous hints and suggestions for creating effective policies. Complex policies can be built entirely within a visual editor that requires no programming or scripting.
- For supported CCP services, MCAS offers file history tracking and multiple-version control within the admin console.
- Azure Information Protection policies are the foundation of both document classification rules and DLP rules; actions include apply access control, limit printing and forwarding, apply a watermark, or encrypt. Organizations that have already invested in RMS for their data classification will appreciate this integration with MCAS.
- MCAS aggregates events and configuration details from Office 365, the Azure Security Center (free for all Azure customers; enablement required), many cloud services and on-premises products to present a consolidated view of risk.

Cautions

- A typical Microsoft cloud security strategy will require multiple Microsoft products, not just its CASB. For example, adaptive access control (Azure AD Conditional Access) and EDRM (Azure Information Protection) are separate products. Microsoft's cloud security products work best

when customers deploy the entire suite; stand-alone or a la carte deployments offer reduced functionality.

- While Microsoft now offers reverse-proxy mode for its CASB, onboarding SaaS applications to use the proxy occurs through Azure Active Directory. Customers requiring real-time proxy inspection must also purchase Azure AD. Similarly, basic adaptive access control is possible using CASB-only policies, but more complete AAC requires the addition of Azure AD Conditional Access.
- MCAS DLP is oriented toward tracking the movement of sensitive data into and out of sanctioned cloud services. It has little visibility into unsanctioned services. Some DLP rules, such as policies examining outgoing email, must be configured in Exchange DLP, not in the CASB. Furthermore, Office 365's native DLP presents yet another engine to configure, which does not share policies with MCAS.
- Microsoft's CSPM functionality is rudimentary compared to other competitors, lacking both breadth of supported IaaS cloud services and depth of posture measurement within those services. MCAS CSPM support does not extend to managing native controls of SaaS applications.
- Microsoft's dedication to supporting non-Microsoft operating systems (forward proxy for Mac) and non-Microsoft cloud services (G Suite, AWS) remains to be seen. Organizations using cloud services from multiple vendors should pay close attention to Microsoft's current capabilities, published roadmaps and execution against them.

Netskope

Netskope was founded in October 2012 and began shipping a CASB in October 2013. Netskope was one of the early CASB vendors that emphasized both cloud application discovery and SaaS security posture assessments. It includes well-developed behavior analytics and alerting within managed and unmanaged SaaS applications. Netskope's most common implementation models are API inspection and forward proxy, either via chaining or with a combination of an on-premises gateway and end-user agents. Reverse proxy is also available. The agents permit monitoring and control of native mobile applications and sync clients, and are used to steer traffic into Netskope's cloud (they have no other endpoint functionality). Netskope has further expanded its threat protection features by adding in-line proxy and API-based inspection of content for malware. To broaden its appeal to a wider set of buyers, Netskope has developed a secure web gateway and acquired other vendors for CSPM and for incident response. Netskope is in process for FedRAMP authorization at the High Impact level.

Strengths

- Netskope's Cloud Confidence Index cloud risk database is comprehensive, measuring 28,000 services across 50 criteria that include details about pricing, business risk and General Data Protection Regulation (GDPR) readiness.

- Netskope's DLP engine rivals that of some on-premises tools and is frequently cited by Gartner clients as a reason for choosing the product.
- 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 (like Carbon Black) to take various actions, including isolation from governed SaaS applications.
- Netskope offers multiple built-in and tenant-specific threat intelligence feeds and provides effective threat protection capabilities developed internally and sourced from multiple OEMs.
- Encryption and tokenization of structured data support searching and partial preservation of common application functions.

Cautions

- Netskope's ability to revoke third-party access to SaaS applications is limited to G Suite (as of the publication of this Magic Quadrant).
- Gartner clients continue to report that the use of agents is required to derive full value from the CASB. While reverse proxy is supported by Netskope, governing sanctioned applications accessed by unmanaged devices is not a common scenario for which Gartner clients choose Netskope.
- CSPM capabilities for controlling IaaS actions are primarily applied via in-line interception of traffic rather than via APIs. APIs are used only for posture assessment and not for remediation, unlike some competitors.
- Inquiry trends over the past 12 months show a minor increase, compared to the competition, in the number of complaints related to installation challenges, technical support quality and service performance.

Oracle

In September 2016, Oracle acquired Palerra, a vendor founded in July 2013 and that has been shipping a CASB product since January 2015. Oracle CASB Cloud Service is a multimode CASB available in several flavors. Oracle CASB for Discovery provides visibility into SaaS applications by analyzing logs for cloud service activity and identifying risky applications (including those installed from Salesforce's AppExchange). Oracle CASB for SaaS, Oracle CASB for IaaS, and for Oracle CASB for Custom Apps (each a separate product) are suitable for use cases such as security monitoring, threat protection and incident response. Inline DLP (for real-time detection) and API DLP (for retroactive scanning) require additional licensing. The user behavior analytics features in Oracle CASB incorporate data from access and in-application activity, support threat intelligence feeds, and provide threat modeling to assist with threat detection. Oracle CASB offers features that allow organizations to centrally control the native security configurations of SaaS applications and IaaS consoles. Oracle CASB is delivered as SaaS or sold through a managed security service provider.

Strengths

- New DLP rules and malware detection scans can easily be applied to new content or to new-plus-existing content with a single click. Near-real-time DLP via APIs is possible via webhooks for SaaS applications that publish them.
- Custom applications running in the Java Virtual Machine (JVM; the only kind of custom application supported currently) can be protected by Oracle CASB via a runtime application self-protection (RASP)-like insertion into the JVM with no further work required.
- Oracle CASB can assess SaaS applications for common misconfigurations that result in security incidents. It can assess IaaS applications against popular benchmarks and notify when configurations drift from initially measured baselines.

Cautions

- Oracle's primary sales target for its CASB is organizations already using Oracle SaaS applications, multicloud IaaS, and the most popular SaaS applications. While general SaaS governance is possible, it isn't a primary use case.
- No mechanism for midtransaction step-up authentication, a significant feature many Gartner clients require, is available natively. Either of two separate products, Oracle Adaptive Access Manager or Oracle Identity Cloud Service, is required.
- Other than removing excess permissions from IaaS storage objects, Oracle CASB's CSPM capabilities are limited to reporting only; no automatic remediation is possible — instead, it creates incidents in ticketing systems that must then be followed separately.

Palo Alto Networks

In May 2015, Palo Alto Networks acquired CirroSecure, a vendor founded in July 2013. It relaunched CirroSecure's product as an API-only CASB called Aperture, focused on discovery, SaaS policy and SaaS security management. Palo Alto Networks initially offered cloud application discovery and in-line control capabilities via its firewall, but now the GlobalProtect cloud service (a firewall as a service [FWaaS] offering) reduces the need to pass all cloud traffic through on-premises equipment. Aperture adds API-based visibility and governance for users who are either on- or off-premises, on managed and unmanaged devices. Evident, via a 2018 acquisition of Evident.io, brings IaaS CSPM capabilities into the portfolio; RedLock, a very recent second acquisition, adds additional threat-centric CSPM capabilities. (RedLock was not included in the evaluation for the 2018 CASB Magic Quadrant.) The intended market for Aperture is existing Palo Alto Networks customers seeking cloud visibility and governance not available through Palo Alto Networks' firewall alone. Additional features within Aperture include content scanning, sensitive data monitoring, malware detection and remediation (via WildFire), analytics, risk identification, and reporting.

Strengths

- Cloud risk reports include numerous SaaS and non-SaaS web applications that can be used to exfiltrate data; these display a useful overall view into organizational risk. Rules that block access to unsanctioned services can coach users toward sanctioned services and provide links for users to easily navigate there.
- CSPM capabilities include comparisons against multiple industry baselines and can suggest proper configurations to meet several compliance mandates. Remediation options include guided manual steps or (in some cases) automatic reconfiguration.
- Aperture DLP extends beyond keywords and common content types using classifications they have developed via machine learning from a corpus of content; it can identify relevant document types by scanning for frequent combinations of words.

Cautions

- Multiple separate, nonsimilar consoles remain necessary for configuring policies. Those requiring in-line inspection are configured in the GlobalProtect cloud service UI, while those requiring API inspection are configured in the Aperture UI. CSPM capabilities remain distinct from other CASB controls and require the Evident UI, which hasn't yet been integrated into the overall product. RedLock adds a fourth console.
- DLP rules do not span GlobalProtect cloud service and Aperture; in many situations, configuring the same DLP rule in both services will be required.
- Reverse-proxy inspection requires a firewall instance for SaaS and custom SaaS applications. As of this writing, GlobalProtect cloud service does not support this functionality.

Proofpoint

FireLayers was initially launched in 2014. It was acquired by Proofpoint in 2017 and became Proofpoint CASB, extending CASB to Proofpoint's existing threat response, mobile threat defense, remote browser isolation, and threat intelligence offerings. Proofpoint has a large installed base for its email security product; the target market for Proofpoint's CASB is as an add-on for this installed base plus new customers not currently using Proofpoint products. After the acquisition, Proofpoint continues to evolve the product, adding capabilities for improved DLP, advanced threat detection, threat intelligence, and built-in two-factor authentication. Proofpoint has also added multiple nonproxy mitigations for SaaS, including a mechanism that hooks sharing and posting event APIs in common SaaS applications and content-scanning bots, which can provide near-real-time DLP.

Strengths

- With a focus on threats, Proofpoint's CASB identifies risks in a broad range of categories that can be weighted as desired in policy creation, enriched by multiple sources of threat intelligence.

- 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 can be placed into groups that minimize their exposure.
- Access to risky services can be forced through a remote browser isolation mechanism that protects users, devices and applications from remote attack. Proofpoint is the only CASB offering this capability, which is a nice feature for users remotely accessing from potentially dangerous locations and with unmanaged devices.

Cautions

- Proofpoint's CSPM is less developed than some of its competition and actions are limited primarily to in-line visibility. For more useful API CSPM features, Proofpoint recommends supplementing the CASB with service from Dome9.
- Support for custom applications requires vendor involvement. Customers can request Proofpoint to write a plug-in, which can take up to six weeks.
- Encryption is limited to unstructured data (files). For field-level structured data, encryption or tokenization of data in SaaS applications is not possible; instead, Proofpoint performs in-line temporary masking of sensitive information only when accessed through the proxy. Watermarking, labeling and EDRM are not available.

Saviynt

Saviynt was founded in January 2010 and began shipping a CASB in July 2014. Saviynt offers only API-based inspection for some common SaaS applications and for IaaS cloud infrastructure components. Saviynt emphasizes the role of identity in its cloud security products; indeed, its CASB is derived from its identity and access governance platform, and available SaaS controls exhibit a focus on identity. Visibility is available only for sanctioned applications and does not extend to unsanctioned applications or to unmanaged devices, which can limit the overall set of available use cases. Nevertheless, Saviynt may be appropriate for organizations concerned only with governing the most popular SaaS applications and governing developer interaction with IaaS consoles and components. Saviynt is available as SaaS and as on-premises physical and virtual appliances.

Strengths

- Saviynt's focus on identity simplifies managing identity and access policies for cloud services, including detecting and removing excess permissions, permitting time-based role creation, and reporting unused roles and permissions.
- Saviynt offers a thorough set of CSPM capabilities for supported IaaS consoles and SaaS applications, including informative visualizations of audit data. The ability to assess control configurations from multiple sources eases the creation of compliance reports.

- Saviynt supports DevSecOps methodologies by scanning code stored in source code repositories and recipes built with automation frameworks to look for poor configurations and incorrect security settings inside recipes and build scripts.

Cautions

- Saviynt has no native shadow IT discovery and no mechanism for blocking access to consumer versions of services but can audit transfer of files (if the SaaS service exposes an audit API and audit permission is granted).
- To implement adaptive access control policies with step-up authentication, a separately priced privileged access module is required. While Saviynt can manage service accounts for cross-cloud access, no generalized mechanism for detecting and revoking access of third-party apps to cloud services is available.
- Support for custom applications relies on a robotic process automation (RPA) tool that produces a complex workflow to map across application behaviors. This is not nearly as streamlined as the competition.

Symantec

In June 2016, Symantec acquired Blue Coat Systems, adding several security products to its portfolio. Included were two CASBs previously acquired by Blue Coat: Perspecsys and Elastica. Perspecsys, founded in 2009, emphasized satisfying data residency requirements by tokenizing or encrypting data stored in SaaS applications. Elastica, founded in 2012, was best-known for its DLP, UEBA and content inspection capabilities. Combined, the renamed Symantec CloudSOC offers a complete multimode CASB with an optional data encryption/tokenization gateway. Through a combination of log analysis and traffic inspection, CloudSOC provides cloud service assessment ratings, cloud usage analytics, user behavior analytics, malware analysis, remediation actions, and reporting. Symantec incorporated cloud application discovery and security posture assessment capabilities into its traditional management console for SWG customers, creating an upsell opportunity to its full CASB. Symantec is working to combine its existing on-premises DLP appliance with CloudSOC's DLP for consistent discovery of sensitive data. Currently, this is a separate console and requires additional licensing, although the same policies can now be enforced on-premises and in the cloud.

Strengths

- Cloud risk reports, informed by a large number of CSP attributes and behaviors, are formatted appropriately for board-level conversations about exposure and risk reduction.
- Cloud service discovery and usage is one of CloudSOC's strongest capabilities. Policy violation notices can not only include lists of approved cloud services but can also provide links for users to access them.
- Adaptive access controls can be built from a sequence of selectable "detectors" including thresholds, threats, behaviors, device, user location and sequences. Step-up authentication is possible for many types of policies.

- 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 corpus of positive and negative content.

Cautions

- Navigating the UI can be cumbersome, sometimes requiring moving between multiple areas to completely configure a single policy.
- Support for custom applications sometimes requires manually creating a mapping file that describes application behavior; the expectation is that customers or SaaS vendors will perform this work.
- While CloudSOC can apply rights protection to content, recipients must use a Symantec-provided agent installed on PCs and devices to open it.
- CloudSOC's CSPM features provide useful configuration auditing and guided manual remediation steps but lack automatic remediation in most 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

- Forcepoint
- Proofpoint

Dropped

No vendors dropped for 2018.

Inclusion and Exclusion Criteria

The assessments in this Magic Quadrant represent vendor capabilities and positions during the evaluation period, which was January 2017 through June 2018. Like all Magic Quadrants, this is a snapshot in time and vendors will have likely added additional capabilities not captured here. In a few cases, product names will have changed, too.

To qualify for inclusion, vendors must meet the following criteria:

- **Revenue and deployment.** Must have achieved CASB product sales in 2017 globally of more than $6 million, have at least 50 paying customers and at least 50,000 seats deployed. (Adjacent or related products were not included when calculating sales and customer numbers).
- **Geography.** Must compete in at least two of the four major regional markets (Americas, Europe, Asia/Pacific and the Middle East/Africa).
- **Product configuration.** Must sell the product as primarily meeting stand-alone CASB use cases — that is, not relying on some adjacent product or service to fulfill the four pillars of capabilities (visibility, data security, threat protection and compliance).
- **Product features.** Must meet Gartner's definition of a CASB:
  - Inspect data and user behavior in cloud services via provider APIs
  - Optionally operate in-line between users and cloud services as a forward and/or reverse proxy (a capability strongly favored by Gartner clients)
  - Support a range of endpoint deployment and configuration options
  - Support the ability to perform access control of any user, device and location accessing cloud services
  - Support the integration of CASB into an existing enterprise's identity provider and event management system
  - Operate as a multitenant service delivered from the public cloud
  - Optionally operate as a virtual or physical appliance in on-premises or public cloud environments
  - Able to use various forms of advanced analytics to monitor behavior of users and data
  - Able to identify and respond to malicious and/or unwanted sessions with multiple methods, such as allow, restrict, raise multiple alert types, prompt for additional authentication, end session, coach user, etc.

Products and vendors will be excluded if:

- They rely principally on legacy products such as a firewall or secure web gateway to deliver CASB-like functionality
- They support policy and governance of fewer than four SaaS applications
- They do not materially address all four pillars of capabilities (visibility, data security, threat protection and compliance)
- They do not meet Gartner's installed base, client visibility, and sales requirements

Other Vendors

The CASB market contains more vendors than those evaluated in this Magic Quadrant. The following vendors weren't evaluated because they failed to meet one or more criteria:

- Avanan
- Centraya
- CloudCodes
- Fortinet
- ManagedMethods
- Skyguard
- StratoKey

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 speed/accuracy of SaaS application risk ranking. It includes strong and accurate DLP capabilities that rival enterprise DLP products. A focus that favors protection and control as much as or more than visibility, and the ability to provide (or work with other tools to orchestrate) adaptive access control for users, devices and content to/from cloud services are weighted.

Overall viability. Overall viability 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 in highly competitive shortlists.

Market responsiveness and track record. This includes developing innovative security controls faster than competitors, addressing a wide range of use cases, and mitigating cloud security threats quickly are well-regarded for this research.

Marketing execution. Well-defined use cases that highlight the value of a CASB over native cloud security controls, and well-articulated details about how traffic is steered and processed with a demonstrated track record of reducing customer risk posture are being evaluated for this research.

Customer experience. Day-to-day operation can be performed by existing customer personnel. There is no significant change to end-user experience with or behavior of cloud services after deployment. A support escalation path that permits communicating, when the severity is appropriate, with vendor support resources (including engineers at the highest severity levels) is

evaluated. There is evidence of deployment in multiple verticals, with multiple cloud services and multiple customer sizes.

Operations. Not evaluated in this Magic Quadrant iteration.

Table 1. Ability to Execute Evaluation Criteria

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	Not Rated

Source: Gartner (October 2018)

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 in 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 geographies.

Offering (product) strategy. Well-regarded products must show full breadth and depth of SaaS application support, the ability to react quickly to changes in cloud applications, and strong and

actionable 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 and on-premises (which was not weighted for the 2017 Magic Quadrant, but is a differentiator).

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. Not evaluated in this Magic Quadrant iteration.

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 (e.g., consoles for various security/audit roles, 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

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Low

Source: Gartner (October 2018)

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 in 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 must 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 or midsize business segment, or a vertical market, or a certain geography), 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

The rapid adoption of cloud services has caught many security teams unprepared. Visibility into users, devices and data application interactions in cloud environments is required to answer the question, "How do I secure my data in someone else's system?"

The CASB market has evolved rapidly, displaying credible examples of products being shipped from venture capital (VC)-funded startups and from incumbent vendors. In recent years, a considerable amount of volatility from several acquisitions has created confusion for buyers. Of 14 CASB startups formed since 2011, nine have been acquired.

The market has grown significantly but stabilized somewhat in terms of the vendor landscape. Common use cases (see "10 Best Practices for Successful CASB Projects") have formed, and vendors now focus on adding security value for an ever-expanding list of cloud services. These use cases suggest that the market for CASB will continue to be dominated by full-featured platform providers for the next three to five years, a common scenario when new IT product categories emerge. The growth in common use cases also enables IT security leaders to conduct useful comparisons of vendors on core sets of features in competitive environments.

In the past 24 months, Gartner has received almost 2,500 inquiries from clients asking about how to select a CASB. We strongly advise starting with a reasonably detailed list of use cases that are specific to your exact needs. See "CASB Platforms Deliver the Best Features and Performance" for some suggestions. Then a proof of concept (POC) can be developed, which will make acquisition considerably easier.

Pure-play, stand-alone CASB platforms provide more features, for more cloud services, and for a wider array of enterprise use cases to protect your data in cloud services. This agility is far outpacing the features being delivered by CSPs, as well as by other vendors that offer a subset of CASB features as an extension of their existing security technologies for their client bases. Furthermore, platforms from leading CASB vendors were born in the cloud and designed for the cloud. They have a deeper understanding of users, devices, applications, transactions, and sensitive data than CASB functions that are designed as extensions of traditional network security and SWG security technologies.

Buyers need to look past a CASB provider's list of supported applications and services and closely examine how CASBs of interest specifically support cloud applications currently in use and planned by their organizations. The most popular SaaS applications, like Office 365, Salesforce, Box and so on, all enjoy good feature coverage; there is less differentiation now across the CASB market for these services. However, substantial capability differences might exist, which exhibit themselves depending on familiarity with SaaS application functionality, CASB architecture, user and device status, and integration with existing 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 also include an in-line mechanism like forward or reverse proxy. This architecture decision fundamentally defines how CASBs can perform different actions, which has various implications for how that provider delivers the four pillars for a specific cloud service. Gartner clients overwhelmingly prefer CASBs that offer both API inspection and reverse or forward proxy, which we refer to as a multimode architecture.

Over time, as cloud service APIs expose greater amounts of visibility, improved degrees of control, and near real-time performance, the need for in-line traffic interception will slowly diminish. This is not the case today or into the medium term, however. Gartner clients overwhelmingly prefer CASBs that offer both API connections to and in-line inspection of cloud services. We expect the most

prominent cloud application and service providers will continue to develop their APIs significantly during the next two to three years. This is even if they aren't pursuing compliance with an industry or recommended standard like the Cloud Security Alliance's Open API Charter. APIs will increasingly deliver more utility, supporting the potential for newer security use cases not yet envisioned. Recently, many CASB vendors have reported encountering performance slowdowns resulting from cloud service providers increasingly throttling responses to API requests. Smaller SaaS providers might never develop useful APIs for visibility and control, so it's unlikely that the need for in-line visibility via proxying will ever disappear completely.

Market Overview

A large amount of VC funding, many hundreds of millions of dollars now, fueled the initial growth of the CASB market. Recent acquisitions by large vendors suggest the market is maturing, as some startups have been acquired to take their place as part of bigger vendors' portfolios. Other vendors in adjacent markets (like IDaaS, SWG, and enterprise mobility management [EMM]) have begun partnering with CASB vendors to increase reach and find new buyers. CASB could also be the driver for vendors in adjacent markets to enter the fray with further acquisitions — for example, EMM, secure web gateway, firewall or other vendors who want to, or are already, delivering cloud security.

Interest in CASBs is intense and customer adoption is rapid — driven by enterprises of all sizes embracing the cloud as the default starting point for new projects and the next step for updates and enhancements to existing applications. To address the critical need for a security visibility and control point in the cloud, incumbent security vendors have, for the most part, bought their way into the CASB market. A minority of CASBs were sold to larger existing security vendors as those vendors adjusted their cloud security portfolios. The consolidation and acquisition phase of the market is slowing but will likely continue for some time, as there are at least three credible stand-alone CASBs that should be considered acquisition targets.

One thing that has become clear is that there are two aspects to cloud security. The first is the notion of delivering security from the cloud, in which existing technologies like email, web filtering and even firewalling move away from on-premises appliances into cloud services. The second is securing access to cloud services, in which capabilities like CASB and IDaaS become evident as the most important tools. These two aspects are related but fundamentally different in their scope, their design and deployment approaches, and where they fit in the life cycle of managing users, data, actions, transactions, and applications.

Gartner sees four IT trends driving the expansion and maturation of the CASB market:

- **The enterprise moves to adopt bring your own (BYO) traditional PC and non-PC form factors, and usage increases from unmanaged devices.** The massive enterprise adoption of tablets and smartphones for core business processes creates security risks that can be mitigated effectively with a CASB, as the average enterprise end user is spending significantly more screen time on non-PC devices. While employee BYOPC may be waning, business partner access to cloud services is certainly on the rise; here, too, CASBs have a role, with separate policies for business partner access to enterprise data.

- **The enterprise moves to cloud services.** Cloud adoption exhibits no signs of slowing; Gartner expects SaaS spend to more than double that of IaaS (see "Forecast Analysis: Public Cloud Services, Worldwide, 2018 Update"). The need for governing cloud usage and demonstrating that governance exists 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.
- **Heavy cloud investments by vendors.** Most large enterprise software providers, such as Oracle, IBM, Microsoft and SAP are now heavily invested in cloud, and are actively moving their large installed bases to their cloud services. The enterprise software upgrade cycles will shift to cloud over time. Enterprise security teams will need CASB-like features to deal with the security implications of that evolution.
- **A growing and uncertain regulatory environment.** Regulations like 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 between cloud services.

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, many CASB vendors have added CSPM capabilities to their products. CSPM assesses and manages the security posture of the cloud control plane mostly for IaaS and occasionally for SaaS. The better offerings provide this across multiple public cloud providers for consistent policy enforcement (for example, alerting or blocking when network groups in any IaaS are directly exposed to the public internet). For large IaaS-based workload deployments, CSPM capabilities should be considered mandatory.

Some SaaS vendors — Microsoft is a prime example — discourage the placement of certain products like proxies, caches and WAN optimizers in front of their applications. The worry is that performance or availability issues lying entirely within the other product will be perceived as issues with the cloud service itself. Don't let this dissuade you from evaluating and deploying a CASB. SaaS vendors can't place restrictions on how their customers consume their services. Meanwhile, SaaS vendors should be encouraged to continue to develop a range of APIs that support enterprise integration and security use cases. Over time, the need for proxies in front of their services will diminish. Also, realize that troubleshooting any issues will require you to include the CASB in your investigations. In several cases, CASBs can assist this troubleshooting process, rather than hinder it.

Gartner Recommended Reading

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

"10 Best Practices for Successful CASB Projects"

"CASBs Must Not Be Data Security Islands"

“Peer Lessons Learned: Implementing Cloud Access Security Brokers”

“Don’t Let Cloud Migration Flip Your Network and Put Users in Charge of Enterprise Security”

“How Markets and Vendors Are Evaluated in Gartner Magic Quadrants”

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.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp