# Magic Quadrant for Cloud Access Security Brokers

Published 22 October 2019 - ID G00377508 - 46 min read

By Analysts Steve Riley, Craig Lawson

CASBs have become essential elements of cloud security strategies, helping organizations use the cloud and protect their sensitive data in the cloud. Security and risk management leaders concerned with their organizations' cloud use should evaluate CASBs and use this research to assess the market.

## Market Definition/Description

This document was revised on 5 November 2019. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

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 provide access to them from users inside and outside the traditional enterprise perimeter, plus growing direct cloud-to-cloud access. They deliver differentiated, cloud-specific capabilities that are generally not available as features in other security controls, such as web application firewalls (WAFs), secure web gateways (SWGs) and enterprise firewalls. Unlike those premises-focused security products, CASBs are designed to identify and protect data that's stored in someone else's systems. 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 software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) cloud service delivery models. For SaaS coverage, CASBs commonly work with the most popular content collaboration platforms (CCPs), CRM systems, HR systems, ERPs, service desks, 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 API-based usage (including console access) of popular cloud service providers (CSPs) and extend visibility and governance to applications running in these clouds.

Several CASBs now offer cloud security posture management (CSPM; see "Market Guide for Cloud Workload Protection Platforms") capabilities to assess and reduce configuration risk in

capability for many CASBs, the maturity level varies, and it is typically not as well developed as their capabilities for SaaS governance nor as well developed as CSPM products. 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 the 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 Internet Content Adaptation Protocol (ICAP) or RESTful API integration. A few vendors now offer a common DLP engine for their cloud and on-premises products, which eliminates policy duplication and overlap. Some CASBs provide the ability to encrypt, tokenize or redact content at the field and file level in cloud services. However, 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. Most CASB vendors rely primarily on OEM versions of existing enterprise-grade anti-malware and sandbox tools, rather than build 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 to establish cloud risk tolerance. Through their various visibility, control and reporting capabilities, CASBs assist efforts to

of the cloud control plane, mostly for IaaS and increasingly 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 or on-premises log aggregation is required.

## Magic Quadrant

Figure 1. Magic Quadrant for Cloud Access Security Brokers

### Bitglass

Bitglass was founded in January 2013 and began shipping a CASB in January 2014. With a focus on discovery of sensitive data, classification and protection, the CASB product 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 pushed to the user's browser to support real-time data protection in specific scenarios including unmanaged devices. This capability is unique to Bitglass and one that continues to add value for customers relying on less-common SaaS applications. The AJAX VM detects and reacts to changes in underlying SaaS applications that might otherwise bypass traditional, network-based reverse proxies. Bitglass offers well-developed capabilities across all four CASB pillars. It supports reverse proxy on browsers and mobiles; forward proxy with agents for Windows and Macs, and forward proxy with PAC files for any OS, along with API inspection support for an increased number of SaaS applications.

Bitglass also offers agentless mobile device management (MDM) capabilities and basic 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

- Policies can apply watermarks to documents, while being processed in line. Watermarks enable granular tracking of content for all devices and 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.
- Data uploaded into structured applications can be tagged 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.
- Bitglass offers an API gateway for any API-enabled cloud application, allowing organizations to control who can call which APIs and under which circumstances.

#### Cautions

- Other than revoking OAuth tokens granting third-party access to SaaS applications, Bitglass' CSPM capabilities do not extend to directly modifying SaaS application native security controls. Its CSPM for IaaS evaluates Amazon Web Services (AWS) and Azure against multiple frameworks, but the available autoremediation choices are inconsistent between the two CSPs, and are not as thorough as some other vendors.

- Although its visibility in the market has improved from last year, Bitglass is not as frequently mentioned during client inquiries as the some of the others in the CASB market.

- The emergence of the secure access service edge (SASE) market and the ability of a few vendors to offer such capabilities already may place Bitglass at a disadvantage with respect to its competitors in a few years. Customers should discuss Bitglass' roadmap with their Bitglass representatives to determine whether the vendor's plans align with the organization's objectives.

### 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 appliance.

Since then, it has developed the product into a fully featured CASB, delivered principally as a cloud-based service, with useful and effective capabilities for all four CASB functionality pillars of discovery, data security, threat protection and compliance. It is a well-developed product for governing a broad range of SaaS applications and IaaS services, and offers native CSPM, AAC and UEBA capabilities. CipherCloud can scan data stored in structured and unstructured applications to automatically apply classification labels. Furthermore, it can integrate with third-party key management, DLP and data classification products.

CipherCloud is one of the few vendors that also extends its CASB functionality to email in Office 365 and G Suite, potentially making CipherCloud attractive to customers interested in a single vendor for SaaS governance and email security. In its primary implementation, it offers reverse proxy support and API inspection for popular SaaS applications; it also supports forward-proxy implementations, allowing for more-complete multimode coverage.

#### Strengths

- CipherCloud DLP includes selectors for exact data matching, document fingerprinting by uploading a corpus of content and optical character recognition (OCR) in images. Sensitive information can be masked from violation logs. Responses to DLP violations can include multiple steps.

- 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 Key Management Interoperability Protocol (KMIP)-compliant key management server.

- 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.

- CSPM has improved significantly from last year and is now CipherCloud's own (versus an

Multiple frameworks (such as CIS) are available for assessing workloads in AWS, Azure and GCP.

- The graphical visualization of user behavior is well designed. Investigators can add new attributes to UEBA telemetry to gain new insights from historical data. Additionally, a user's assignment into a UEBA group can then be used in other policies in the CASB, such as those defining AAC.

### Cautions

- 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 or in Gartner client inquiries.
- CipherCloud remains focused on the CASB market, which is likely to be disrupted by SASE in the coming years. Although CipherCloud offers limited SASE functionality, its recently released Secure Workplace is moving in that direction, with its roadmap pointing to future execution against SASE criteria.
- CipherCloud's ability to apply CSPM to SaaS applications is limited to Salesforce and Office365; no CSPM for other SaaS is currently available.

## Forcepoint

In February 2017, Imperva sold its Skyfence CASB to Forcepoint, which is now integrating it more deeply into its portfolio. This has joined a series of other acquisitions to form a broad portfolio of security products and services, including SWG, email security, UEBA, DLP and data security, and network firewall.

Forcepoint CASB runs primarily as a cloud service, but requires additional components (either on-premises or running from an IaaS cloud provider) for cloud discovery via log ingestion and for advanced DLP. The cloud-based DLP is functional enough for most entry-level DLP use cases. 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 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 they don't require further refinement. Unusual predicates can be explicitly defined.
- Forcepoint CASB analyzes behavior (what users do) and impact (what users have access to)

- For user-centric 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.
- Its cloud service discovery capabilities pragmatically focus on business applications and exclude extraneous services, such as travel booking sites and wikis.
- Forcepoint SWG customers can combine SWG and CASB policies to block access to cloud services determined to be too risky. Similarly, Forcepoint DLP customers can extend policies for Forcepoint CASB.

### Cautions

- Although integration between Forcepoint's on-premises DLP and its CASB DLP has improved, Forcepoint still relies on its separate DLP product (on-premises or in an IaaS cloud) to configure more-sophisticated policies. These include fingerprinting, matching against a corpus and OCR. Enforcement can occur at the CASB in the cloud.
- Adding AAC for custom SaaS applications requires asking Forcepoint to create a schema file that maps actions in the application to user behaviors that can be controlled through the CASB.
- For ERDM policy enforcement against Microsoft RMS, Forcepoint relies on its endpoint agent installed on devices. The CASB itself can't do this.
- CSPM is primarily for reporting and compliance, rather than policy enforcement and modifying configurations.

## McAfee

In January 2018, McAfee closed its acquisition of Skyhigh Networks, thus augmenting its security portfolio of DLP, SWG, network sandboxing, etc. McAfee MVISION Cloud (as it is now called) was one of the first CASB products to raise awareness of shadow IT. The product expanded to provide thorough coverage of all four CASB pillars across a broad range of cloud services, and it 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 capabilities; forward proxy is also possible, but less common. An on-premises virtual appliance is available for customers that require it. McAfee has adjusted its pricing and simplified its licensing. MVISION Cloud obtained FedRAMP authorization at the Moderate Impact Level in November 2017 and is about to undergo authorization at the High Impact Level.

### Strengths

- Remediations can configure actions in network firewalls, SWGs and endpoint security products.
- McAfee offers useful CSPM capabilities for auditing, control and remediation of cloud configuration issues — not just for IaaS, but also for popular SaaS applications.
- 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.
- The product offers several options for detecting, labeling, and reacting to sensitive information on managed and unmanaged devices, in sanctioned and unsanctioned cloud services, using native and third-party classification mechanisms.
- A wide array of policies that take full advantage of API inspection, forward-proxy redirection and reverse-proxy insertion, facilitated by a single agent that directs traffic to McAfee's CASB or SWG, are configurable.
- 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 (e.g., fields, variables and files) that can be used in DLP selectors.
- 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 customers must contend with two DLP engines across the MVISION fabric. When working with DLP, it's unclear which engine will perform the scanning and enforcement. Nevertheless, synchronization between the two is functional and, in most cases, will be acceptable for most customers.
- UEBA support for dynamic grouping is limited to system-defined groups only; customer-defined group memberships are static.
- McAfee's position is that managed devices interacting in predictable ways should be given direct access to SaaS 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.
- Although McAfee continues to adapt its product line to meet the needs of cloud security buyers, its large heritage endpoint, server protection and security information and event management (SIEM) products still dominate mind share among Gartner clients.

In September 2015, Microsoft completed its acquisition of Adallom, a CASB that had been shipping since early 2013. Microsoft Cloud App Security (MCAS) is a reverse-proxy-plus-API CASB available stand-alone and as part of Microsoft's Enterprise Mobility + Security (EMS) E5 suite. However, most customers purchase it as an add-on to the EMS E3 suite or receive it as part of Microsoft 365 E5, which is a bundle of Office 365 E5, EMS E5 and Windows 10 Enterprise E5. MCAS offers features for each of the four pillars of CASB and, when combined with either of the EMS suites, offers even more complete functionality. Microsoft customers looking for complete functionality should evaluate the combination of EMS E3 and MCAS. MCAS can now reverse-proxy Office 365 traffic, offering real-time, in-line inspection.

Although Gartner clients routinely question whether they need the larger Microsoft suites, the bundling has been successful for Microsoft overall. MCAS has experienced large increases in the number of customers and seats deployed, and has the largest installed base of any vendor in this research. Furthermore, Microsoft now demonstrates sufficient evidence that it is committed to equivalent governance of Microsoft and non-Microsoft cloud services.

Certain Office 365 subscriptions include Office 365 Cloud App Security (OCAS), which is a subset of MCAS, with fewer features, designed to protect only an Office 365 tenant (and no other SaaS applications).

Strengths

- The MCAS user interface is intuitive, and it 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 (AIP) 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 AIP 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.
- Microsoft Flow offers customers a basic SOAR-like capability across Microsoft's cloud services and others, including competing IaaS vendors.
- Microsoft has consolidated disparate classification mechanisms into one shared across MCAS, Office 365, AIP and Windows Information Protection (WIP). DLP actions are comprehensive and can even send real-time notifications of violations (with requests for

- The UEBA interface displays a useful consolidated view of a single account's activities across multiple governed cloud services.

### Cautions

- A typical Microsoft cloud security strategy will require multiple Microsoft products, not just its CASB. For example, AAC (Azure Active Directory Conditional Access) and EDRM (Azure Information Protection) require one of the EMS suites. Microsoft's cloud security products work best when customers deploy the entire suite; stand-alone or a la carte deployments offer reduced functionality.
- Onboarding SaaS applications to use the reverse proxy occurs through Azure AD Conditional Access. Customers requiring real-time proxy inspection must also use Azure AD to take advantage of the conditional access feature.
- Third-party threat intelligence integration evaluates only the IP addresses of incoming connections. Third-party UEM integration is limited to checking whether a device possesses a digital certificate; Intune is required for further device or application control.

## 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 cloud application discovery and SaaS security posture assessments. It includes well-developed behavior analytics and alerting in managed and unmanaged SaaS applications. Netskope has received FedRAMP authorization at the Medium Impact Level and is the only other CASB vendor in this Magic Quadrant suitable for agencies requiring such authorization.

Netskope's most common implementation models are API inspection and forward proxy. Traffic can be steered to the forward proxy via a variety of mechanisms, including endpoint clients, network configurations (e.g., GRE or IPSEC), on-premises appliances (secure forwarder or proxy chaining), and third-party SD-WAN integrations. Reverse proxy is also available. The agent permits monitoring and control of native mobile applications and sync clients and is used to steer traffic into Netskope's cloud (its primary function). 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 offers an SWG and a zero trust network access (ZTNA) service to complement a previous acquisition (Sift Security) for CSPM and incident response. Netskope has API-enabled its service to allow for deeper integrations, beyond SIEM, with more advanced tools such as those in the SOAR market.

### Strengths

- Netskope's vision clearly demonstrates a recognition of the importance of the emerging SASE market, and it is further along in that direction than any other CASB vendor.

- Netskope's Cloud Confidence Index (CCI) cloud risk database is comprehensive, measuring a large number of services across many criteria that include details about pricing, business risk and regulatory readiness.
- Netskope's DLP engine rivals that of many 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 (e.g., Carbon Black, which is being acquired by VMware) 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.
- Netskope offers a wide range of AACs for managed devices accessing governed and ungoverned cloud applications. The agent also supports the inspection of actions on mobile-native applications.
- Encryption and tokenization of structured data support searching and partial preservation of common application functions.
- Expanded CSPM capabilities this year now cover both SaaS and IaaS.

#### Cautions

- UEBA capabilities are rudimentary. The lack of an analytics graph limits the degree of sophistication available for modeling user behavior. Dynamic grouping is unavailable and instead relies on SIEM recipes.
- Netskope's ability to revoke third-party access to SaaS applications is limited to G Suite (as of the publication of this Magic Quadrant).
- Some Gartner clients express concern over the need to install agents to achieve maximum value from the product.
- Although less prevalent this year than in the past, inquiry trends continue to show minor complaints related to installation challenges, technical support quality and service performance.

### Palo Alto Networks

In May 2015, Palo Alto Networks acquired CirroSecure, a vendor founded in July 2013. Palo Alto Networks has combined previously disparate products into a single brand called Prisma. Prisma SaaS (formerly Aperture) is an API-based tool for governing SaaS applications. Prisma

offering, originally derived from a 2018 acquisition of RedLock. Before that, Palo Alto Networks purchased a substantially similar CSPM tool, Evident.io, which was discontinued and migrated to RedLock. The intended market for Prisma SaaS is Palo Alto Networks customers looking for cloud visibility and governance not available through Palo Alto Networks' firewall alone. Additional features in Prisma SaaS include content scanning, sensitive-data monitoring, malware detection (via WildFire) and remediation, analytics, risk identification, and reporting. It partners with Ionic for file encryption.

### 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.
- CSPM capabilities now extend to SaaS applications. Prisma can assess and improve the security configurations of common SaaS applications.
- Prisma SaaS extends beyond keywords and common content types using classifications Palo Alto Networks has developed via machine learning from a corpus of content; it can identify relevant document types by scanning for frequent combinations of words.

### Cautions

- Two separate consoles are necessary for configuring DLP policies. Policies requiring in-line inspection are configured in Prisma Access and are basic, offering only a few predefined patterns, strings and regular expressions. More-advanced policies are available only through Prisma SaaS and, thus, operate only via API inspection of cloud services.
- Prisma Cloud CSPM inspection and remediation rules require yet another console.
- Despite the Prisma rebranding, Palo Alto Networks needs to continue transitioning its multiple cloud security products into a single coherent offering.

## Proofpoint

FireLayers, initially launched in 2014, was acquired by Proofpoint in 2017 and became Proofpoint CASB, extending CASB to Proofpoint's existing threat response, mobile threat defense, remote browser isolation (another acquisition), ZTNA (another acquisition) 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

cloud and third-party OAuth apps governance, 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, including its own market-leading offering.
- 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, email security and remote browser isolation products offer useful synergies, which may be an attractive integration and bundle for some customers.
- Proofpoint favors a remote browser isolation mechanism rather than a reverse proxy for allowing unmanaged devices to access approved SaaS applications. Remote browsing is easier to configure, but requires additional bandwidth and computing resources from the vendor.
- 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 has no meaningful CSPM capabilities in its CASB. Other than detecting and removing excess permissions from and detecting files with DLP violations in IaaS storage objects, it cannot help IaaS customers reduce risk or provide governance for IaaS applications.
- Support for custom applications requires vendor involvement. Customers can request that Proofpoint write a plug-in for SaaS applications that require API integration; this can take as long as six weeks.
- Encryption and tokenization of data are not available in the product.

## 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. Founded in 2009, Perspecsys emphasized satisfying data residency requirements by tokenizing or encrypting data stored in SaaS applications. Elastica, founded in 2012, was best known for

remote browsing vendor. The technology was reintroduced into the CASB an alternative to the reverse proxy for forwarding traffic.

Combined, the renamed Symantec CloudSOC offers a multimode CASB with an optional data encryption/tokenization gateway. Through a combination of log analysis and traffic inspection, CloudSOC provides effective cloud service assessment ratings, cloud usage analytics, user behavior analytics, malware analysis, remediation actions, and reporting to both technical and nontechnical stake holders. When it comes to remediation capabilities, it has also improved its CSPM capabilities over previous research.

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 on-premises DLP appliance with CloudSOC's DLP for consistent discovery of sensitive data. This is a separate console that may require additional licensing, although the same policies can now be enforced on-premises and in the cloud with the same level of DLP functionality.

In 2019, Symantec announced its intention to sell its enterprise security software products to Broadcom, a chip manufacturer with no history of software product investment or integration. Thus, continuing investment in the roadmap and high levels of client support of CloudSOC are unclear.

### Strengths

- AACs 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.
- Mirror Gateway, the remote browsing technology, is an effective alternative to traditional reverse proxies for governing access to approved applications from unmanaged devices. It avoids the need to rewrite URLs and offers greater control over content delivered to users.
- The ability to add integrations with native and third-party party two-factor authentication (2FA) to policies is wide-ranging and convenient, especially for customers choosing Symantec's mobile push 2FA client.
- Recent contract reviews consistently show that CloudSOC's pricing is consistent and easy to consume in a per-user/per-year model, regardless of the number of governed cloud services.

### Cautions

- Reverse-proxy mode now applies only to Office 365. Other reverse-proxy use cases now require the Mirror Gateway, which is a separately licensed feature.
- Gartner believes Broadcom's acquisition of Symantec's enterprise security business to be problematic in some aspects. We expect to see some level of disruption to staff, partners, product roadmaps and end-user support in the coming year.

### 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 in 2019.

#### Dropped

The following vendors were dropped in 2019:

- **Censornet** — Censornet failed to meet the 2019 revenue inclusion criterion.
- **Cisco** — Cisco's strategy for cloud security has changed. The Umbrella branding emphasizes DNS-based security, CASB, firewall as a service (FWaaS) and SWG. Although Cisco continues to sell Cloudlock as a stand-alone CASB solution, it did not meet multiple inclusion criteria for this year's report.
- **Oracle** — Oracle failed to meet certain 2019 product configuration and product feature inclusion criteria.
- **Saviynt** — Saviynt failed to meet certain 2019 product configuration and product feature inclusion criteria.

## Inclusion and Exclusion Criteria

The assessments in this Magic Quadrant represent vendor capabilities and positions during the evaluation period, which was July 2018 through July 2019. Like all Magic Quadrants, this is a snapshot in time, and vendors are likely to have added capabilities not captured here. In a few cases, product names will have changed, too.

To qualify for inclusion, vendors need to meet the following criteria:

- **Revenue and deployment** — Must have achieved CASB product sales in 2018 of more than

deployed. (When calculating sales and customer numbers, adjacent or related products can't be included.)

- **Geography** — Must compete in at least two of the four major regional markets: the Americas, Europe, the Asia/Pacific (APAC) region 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 and have most of the features below:
  - 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 (a capability strongly favored by Gartner clients) or optionally offer remote browser capabilities
  - 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 and coach user

Products and vendors will be excluded if they:

- Rely principally on legacy products, such as a firewall or SWG to deliver CASB-like functionality
- Support policy and governance of fewer than 10 SaaS applications
- Do not materially address all four pillars of capabilities (visibility, data security, threat

- 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. However, they have capabilities for some CASB use cases (even if the vendors aren't actively selling them as such) or products with some CASB-like features:

- Avanan
- CensorNet
- Centraya
- Cisco
- CloudCodes
- Fortinet
- ManagedMethods
- Oracle (for Oracle SaaS applications only)
- Saviynt
- 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, including mechanisms for identifying and classifying content at various sensitivity levels. 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) AAC for users, devices and content to/from cloud services are weighted.

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

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:** 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:** Not evaluated in this Magic Quadrant iteration.

**Customer experience:** Day-to-day operations 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.

**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 | Not Rated |
| 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

solve challenging problems associated with the use of multiple cloud services by organizations of all sizes.

**Marketing strategy:** Not evaluated in this Magic Quadrant iteration.

**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 geographic locations.

**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 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 (e.g., 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.

| Evaluation Criteria ↓ | Weighting ↓ |
|---|---|
| Market Understanding | High |
| Marketing Strategy | Not Rated |
| Sales Strategy | Medium |
| Offering (Product) Strategy | High |
| Business Model | Medium |
| Vertical/Industry Strategy | Low |
| 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 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 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 [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

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?”

Gartner continues to receive hundreds of inquiries per year from clients asking about how to select and implement a CASB. Common use cases have formed, which enable IT security leaders to conduct useful comparisons of vendors on core sets of features in competitive environments. We strongly advise starting with a reasonably detailed list of use cases that are specific to your exact needs. From there, a proof of concept (POC) can be developed, which will make acquisition considerably easier. (See “10 Best Practices for Successful CASB Projects” for suggestions on use-case starting points and POC evaluation criteria.)

The CASB vendor market has reached a point of relative stability. All vendors offer various mechanisms for adding security value to an ever-expanding list of cloud services. Many vendors are now seeking ways to differentiate by adding capabilities beyond those necessary for addressing classic CASB use cases.

Full-featured CASB platforms provide more capabilities, for more cloud services, and for a wider array of enterprise use cases to protect your data in cloud services. This agility still outpaces the security features delivered by CSPs, as well as by other vendors that offer a subset of CASB features as an extension of their security technologies. 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 designed to be 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 in use and planned by their organizations. The most popular SaaS applications (e.g., Office 365, Salesforce and Box) enjoy good feature coverage; there is less differentiation across the CASB market for these services. However, substantial capability differences might exist, which show 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, such as forward or reverse proxy or remote browsing. This architecture decision fundamentally defines how CASBs can perform different actions. This has implications for how that provider delivers the four pillars for a specific cloud service. Gartner clients overwhelmingly prefer CASBs that offer both API and in-line inspection, which we refer to as a multimode architecture.

As cloud service APIs expose greater amounts of visibility, improved degrees of control and, sometimes, near-real-time performance, the need for in-line traffic interception will slowly diminish. Although this is not the case today or into the midterm, we expect the most prominent cloud application and service providers to continue developing their APIs significantly during the next two to three years (even if they aren't pursuing compliance with an industry or recommended standard, such as Cloud Security Alliance's Open API Charter). APIs will increasingly deliver more utility, supporting the potential for newer security use cases not yet envisioned. However, smaller SaaS providers might never develop useful APIs for visibility and control, so it's unlikely the need for in-line visibility via proxying will ever disappear completely.

## Market Overview

A large amount of venture capital funding, many hundreds of millions of dollars, has fueled the initial growth of the CASB market. Acquisitions by large vendors and the lack of new rapid-growth startups suggest the market is reaching a point of maturity. Other vendors in adjacent markets (e.g., IDaaS, SWG, and unified endpoint management [UEM]) regularly partner 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, UEM, SWG, firewall or other vendors delivering (or hoping to deliver) 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, to start a new or extend an existing cloud security portfolio. The consolidation and acquisition phase of the market has come to a halt; however, the two remaining pure-play CASB vendors evaluated in this Magic Quadrant (Bitglass and CipherCloud) might, at some point, become acquisition targets.

security, web filtering, firewalling and SIEM move away from on-premises appliances into cloud-delivered services. The second is securing access to cloud services, in which capabilities such as CASB, CSPM, cloud workload protection platform (CWPP) and IDaaS become evident as critically important tools. These two aspects are related, but are fundamentally different in their scope, design and deployment approaches, as well as 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. Although 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 shows no signs of slowing; Gartner expects SaaS spending to double that of IaaS (see "Forecast: Public Cloud Services, Worldwide, 2017-2023, 2Q19 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 CSPs. 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 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.

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 capabilities to their products. CSPM assesses and manages the security posture of the cloud control plane, mostly for IaaS and PaaS and, increasingly, for SaaS. The better offerings provide this across multiple

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.

Some SaaS vendors discourage the placement of products such as proxies, caches and WAN optimizers in front of their services. 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 in-line. 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 underpinned by a breadth and depth of features, as well as performance and availability. The need for proxies in front of their services could diminish, if APIs are improved enough by cloud providers. 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.

### The SASE: Cloud-Delivered Security Convergence

As described above, Gartner draws a distinction between delivering security from the cloud and securing access to cloud services. We are witnessing credible convergence in the former. Gartner has identified this phenomenon as a new market: the SASE. This emerging offering combines comprehensive WAN capabilities with comprehensive network security functions — such as SWG, CASB, firewall as a service (FWaaS), remote browser isolation 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 that those who haven't.

## 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.

**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.

**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.