KuppingerCole Report

LEADERSHIP COMPASS

by Mike Small | November 2018

Cloud Access Security Brokers

How do you ensure secure and compliant access to cloud services without losing the agility and cost benefits that these services provide? This report gives you an overview of the market for Cloud Access Security Brokers and a compass to help you to find the product that you need.

by **Mike Small**
mike.small@kuppingercole.com
November 2018

Leadership Compass
Cloud Access Security Brokers
By KuppingerCole

Content

Content of Tables

Content of Figures

Related Research

Leadership Compass: Infrastructure as a Service – Global Providers - 70303
Buyer's Guide: Hybrid Cloud Services - 72562
Advisory Note: Cloud Services and Security - 72561
Advisory Note: How to Assure Cloud Services - 72563
Advisory Note: Security Organization Governance and the Cloud - 72564
Advisory Note: Security Organization, Governance, and the Cloud – 71151
Executive View: NextLabs Data Centric Security in the Hybrid Cloud - 72531
Executive View: CensorNet Cloud Security Platform - 72529
Executive View: CipherCloud Trust Platform - 72530
Executive View: Skyhigh Cloud Security Platform - 72532
Advisory Note: Rising to the Security Challenge of Heavy Cloud Adoption - 72542
Executive View: Microsoft Security Suite - 72541

1 Introduction

The KuppingerCole Leadership Compass provides an overview of vendors and their product or service offerings in a certain market segment. This Leadership compass focuses on the market segment of CASBs (Cloud Access Security Brokers). CASBs address the challenges of security and compliance around the use of cloud services. They provide security controls that are not available through existing security devices and provide a point of control over access to cloud services by any user and from any device. The market for CASBs has evolved from the first products that focussed on the discovery of cloud usage, through network access control points to become integrated cloud security solutions. These are sometimes called CASB+ or CASB 2.0.

1.1 Market Segment

Most organizations are now using several cloud services as well as on-premises and hosted IT services. This hybrid environment has given rise to many challenges in the areas of management, security, and compliance. This is because the use of these services is not well integrated into the normal IT and access governance processes and technologies found within organizations. Furthermore, the use of these services create other risks.

Employees and associates can use their personal cloud services to perform their jobs without reference to their employer. Line of business managers can acquire cloud services without performing risk assessment or considering the impact of these on compliance. The requirements for control over the processing and storage of personal data from the recent EU GDPR is one example of these challenges. The uncontrolled use of cloud services also increases cyber-risks; cyber adversaries may obtain unauthorized access to steal or corrupt data held in the services, as well as to plant malware that could then infect the organization using them.

In an ideal world, the functionality to manage access to cloud services and to control the data that they hold would be integrated with the normal access governance and cyber security tools used by organizations. However, these tools were slow to develop the required capabilities, and this has led to a market in CASBs (Cloud Access Security brokers) to plug the gap. It is notable that some of the CASBs on the market have already been acquired by major security software vendors and are being integrated into their toolsets.

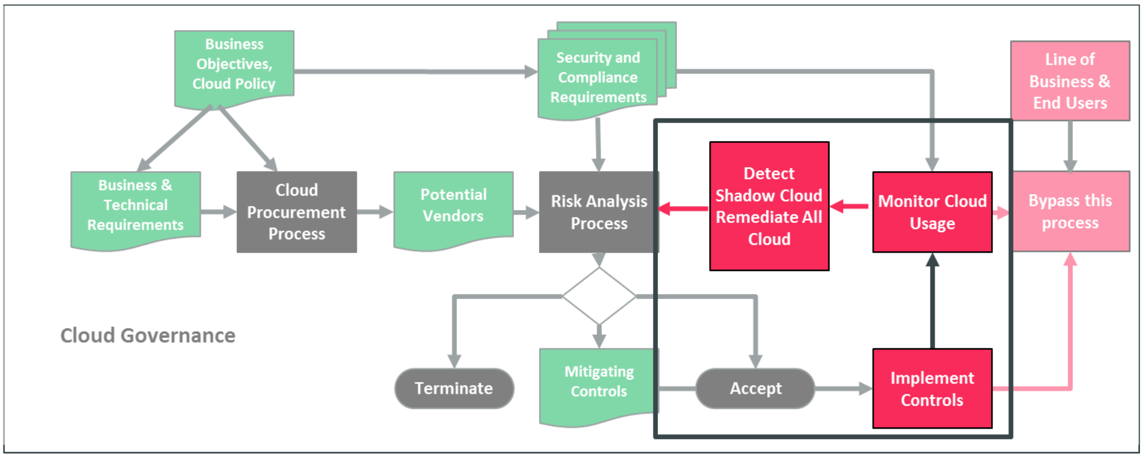

Business Objectives, Cloud Policy
Security and Compliance Requirements
Line of Business & End Users
Business & Technical Requirements
Cloud Procurement Process
Potential Vendors
Risk Analysis Process
Detect Shadow Cloud Remediate All Cloud
Monitor Cloud Usage
Bypass this process
Cloud Governance
Terminate
Mitigating Controls
Accept
Implement Controls

Figure 1: How CASB fits into Cloud Governance

Figure 1 illustrates how CASBs fit into the overall cloud governance process. The basic functionalities that CASBs provide are:

- Discovery of what cloud services are being used, by whom and for what data.
- Control over who can use which services and what data can be transferred.
- Protection of data in the cloud against unauthorized access and leakage as well as cyber threats.

The products which address various aspects of this provide overlapping functionality and these solutions include:

- Rights Management – that provide granular access control over access to unstructured files.
- Data Leakage Prevention – that provide discovery and control over the sharing, transmission, and storage in the cloud of specific classes of data.
- Secure Web Gateways – that protect web-surfing devices from infection and enforce company policies.
- Cloud Access Security Brokers – that provide granular access over who can access cloud services and the functions that they can perform.

	Discovery	Control	Protection
Rights Management	Sometimes include rules to detect specific kinds of data.	Over individual access to unstructured files.	Against unauthorized access to files including if forwarded or leaked.
Data Leakage Prevention	Of specific kinds of data stored or being transmitted	Warn, report, quarantine, remove data, prevent transmission	Against unauthorized storage and transmission of specific types of data.
Secure Web Gateway	Access to URLs	Over which services (URLs) can be accessed and malware filtering	Protect web-surfing devices from infection and enforce company policies.
Cloud Access Security Broker	Who is accessing which cloud services	Granular control over who can access which transactions from where using which device	Against unauthorized access to specific services, transactions, and data
Access Governance	Of user, roles and entitlements.	Over entitlements against policies and separation of duties.	Enforcement of allocation of entitlements that are against policies and separation of duties

The distinction between these types of product and the functionalities provided by Cloud Access Security Brokers are shown in the table. The next generation CASB 2 or CASB+ solutions now on the market providing several of these functions, sometimes through inbuilt capabilities and sometimes through integration with other products.

There are two basic discovery and control models used by CASB+ solutions: network-based control (using a proxy for example) and cloud-service-based control (using cloud service APIs). Each of these approaches has advantages and disadvantages. The better solutions use a combination of the two.

However, the integration of CASBs with the traditional security products is not enough. CASBs should become more integrated with identity and access technologies over time. There is already a level of integration between most CASBs and user directories and IDaaS to identify users and feedback to enable or disable access via these. Access to cloud services and the ability to upload/download content should ultimately be governed through the same processes as access to other kinds of services.

1.2 Required capabilities

The core features and functionalities that we are looking for include but are not limited to:

- Discovery - of cloud services being used from within the organization;
- Access Control - of access to cloud services from within the organization in a granular manner;
- Securing Data - The functionality provided by the product to implement security controls over organizational data that is held in or being moved to cloud services;

These features should also be supplemented in ways that support:

- Compliance - functionality provided by the product to support the use of cloud services by the organization in compliance with laws and regulations;
- Cyber Security - how the products help the organization to protect against cyber security risks from the use of cloud services.

Specific functionality that we are looking for include:

1.2.1 Discovery of Cloud Usage

How the product helps an organization to discover and control the use of cloud services from within and from outside of the organization. This includes:

- The approach used to discover the use of cloud services;
- Whether or not the individual identities of people using the services are recorded;
- The kinds of enterprise data that the product can detect are being held in cloud services;
- Risk profiles of different cloud services;
- Cloud traffic (to/from, sharing, collaboration etc.);
- The functionality provided to control access to cloud services;
- Cloud service configuration assessment and controls

1.2.2 Access Control

How the product helps to control access to cloud services. This may be at a service by service level – giving the ability to prohibit or allow the use of specific cloud services. It may also enable more finely grained access control based on individual user identities, devices, transactions, and data. We specifically look at:

- Access policies supported;
- The granularity of access controls;
- Support for standards like SAML, OAuth and XACML;
- Integration with organizational identity and policy stores;
- Integration with the access controls provided by the cloud services themselves;
- Adaptive authentication;
- Identifying user activity, such as privileged user traffic patterns.
- Integration with on-premises access governance.

1.2.3 Securing Data in the Cloud

This includes the functionality provided by the product to implement data security controls. These may include controls based on the classification or types of data as well as functionality to discover sensitive data that is held in or being moved to a cloud service. Controls may be implemented through detection, warning, quarantining, blocking, encrypting or tokenizing data. The granularity of the controls is also important, and include:

- Cloud service models supported;
- Specific cloud services supported "out of the box";
- Types of data protected;
- The mechanisms used to protect the data - (UEBA, collaboration control, device control etc.)
- DLP and RMS capabilities and integration with other vendors' DLP and RMS solutions
- Kinds of encryption used and how keys are managed.

1.2.4 Compliance

How the product helps to support the use of cloud services by the organization in a way that is compliance with laws and regulations, specifically:

- The kinds of functionality provided by the product to support compliance;
- The compliance areas and regulations for which the product provides "out of the box" functionality;
- The standards to which the product has been certified;
- The product's monitoring and reporting capabilities.

1.2.5 Cyber Security

This area covers how the products help the organization to protect against cyber risks. Using cloud services increased the attack surface for cyber criminals. The products often provide features to mitigate this. For example, through control over which devices have access to specific cloud services and hence prevent access from unregulated devices. They may also provide mechanisms to monitor access behaviors to help to identify hijacked accounts and malware. Specifically, we consider:

- The kinds of cyber risks that the product can detect and protect against;
- The way in which the product protects data held in cloud services against unauthorized access and leakage;
- The extent to which the product monitors access to data held in the cloud;
- Integrated malware detection and antimalware capabilities or integration with solutions from other vendors;
- Reporting and integration with security intelligence systems.

1.2.6 Other Unique Features

We also consider any other unique features or functionality provided by the product.

2 Leadership

Selecting a vendor of a product or service must not be only based on the comparison provided by a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help to identify vendors that should be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept pilot phase, based on the specific criteria of the customer.

Based on our analysis, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

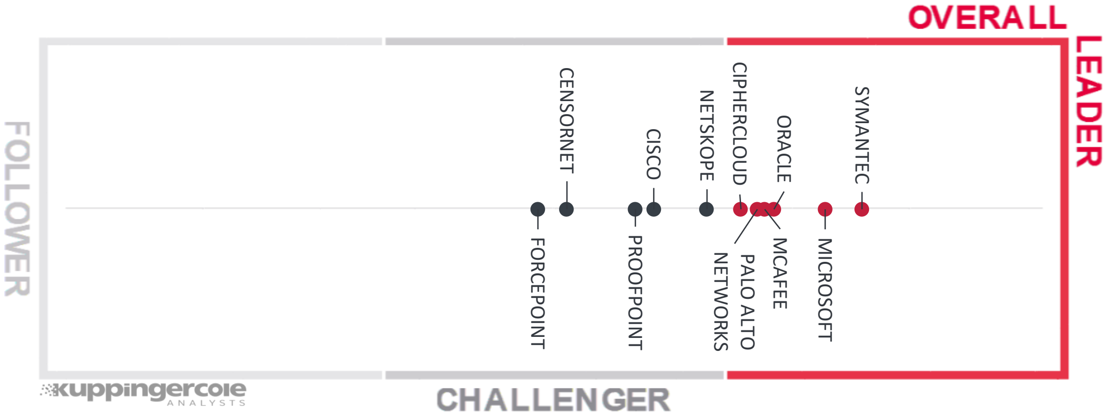


Figure 2: The Overall Leadership rating for the Cloud Access Security Brokers market segment

In the Overall Leadership rating, we find several vendors in the Leaders segment.

Microsoft and Symantec now take the leadership positions following their integration of the products that they acquired into fully functional CASB 2.0 solutions. Microsoft, through its acquisition of Adallom, has a strong product which has been well integrated with Microsoft Enterprise Mobility + Security Suite. Symantec has integrated the cloud data protection products that were acquired and developed by Blue Coat and released them as Symantec CloudSOC. Also included are Oracle that acquired Palerra LORIC and CipherCloud that was an early entrant into this market and has a mature product with a strong and still growing user base. McAfee acquired Skyhigh Networks, an early entrant in this market, with a strong customer base. Palo Alto Networks acquired CirroSecure in 2015, which was later launched as Aperture after integration into the Palo Alto Networks Security Operating Platform which added to the Palo Alto Networks Next-Generation Security Platform. Their platform’s CASB capabilities were extended in 2017 to include forward and reverse proxy CASB capabilities through its GlobalProtect cloud service.

In the Challenger segment, we see some of the large security vendors who have now developed or acquired CASB products to fill a gap in their product line. These include Cisco that acquired Cloudlock Inc. and has integrated their CASB product as Cisco Cloudlock. Forcepoint CASB came through the acquisition of Skyfence from Imperva in early 2017 and Proofpoint through FireLayers in 2016.

There are no vendors in the Follower’s segment.

Overall Leaders are (in alphabetical order):

- CipherCloud
- McAfee
- Microsoft
- Oracle
- Palo Alto Networks
- Symantec

2.2 Product Leadership

The first of the three specific Leadership ratings is about Product Leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

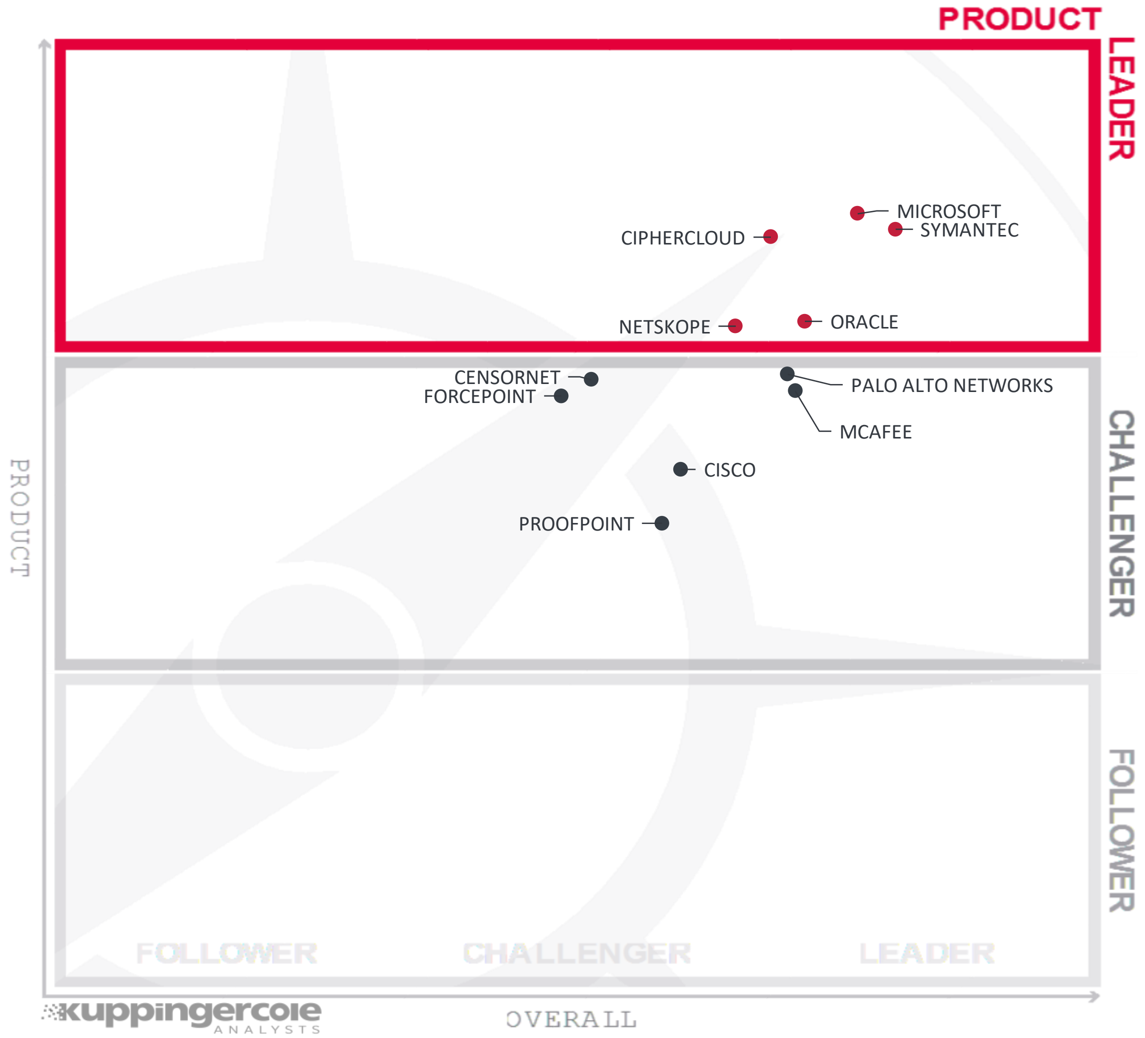


Figure 3: Product Leaders in the Cloud Access Security Brokers market segment

Product Leadership is the view where we look specifically at the functional strength and completeness of products. Here, we find some more vendors that made it into the Leader's segment.

Support for full CASB 2.0 functionality now sets the benchmark for inclusion in the product leaders. There are now many good products in this market but only a few that provide complete CASB 2.0 functionality. These include the products from CipherCloud, Microsoft, Netskope, Oracle and Symantec.

In the Challenger's section, we find a range of good products which didn't quite make it into the Leaders sections because of maturity or missing some of the features found amongst the leaders.

Product Leaders (in alphabetical order):

- CipherCloud
- Microsoft
- Netskope
- Oracle
- Symantec

2.3 Innovation Leaders

Another angle we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require for keeping up with the constant evolution and emerging requirements they are facing. Innovation is not limited to delivering a constant flow of new releases, but focuses on a customer-oriented upgrade approach, ensuring compatibility with earlier versions especially at the API level and on delivering leading-edge new features which meet emerging customer requirements.

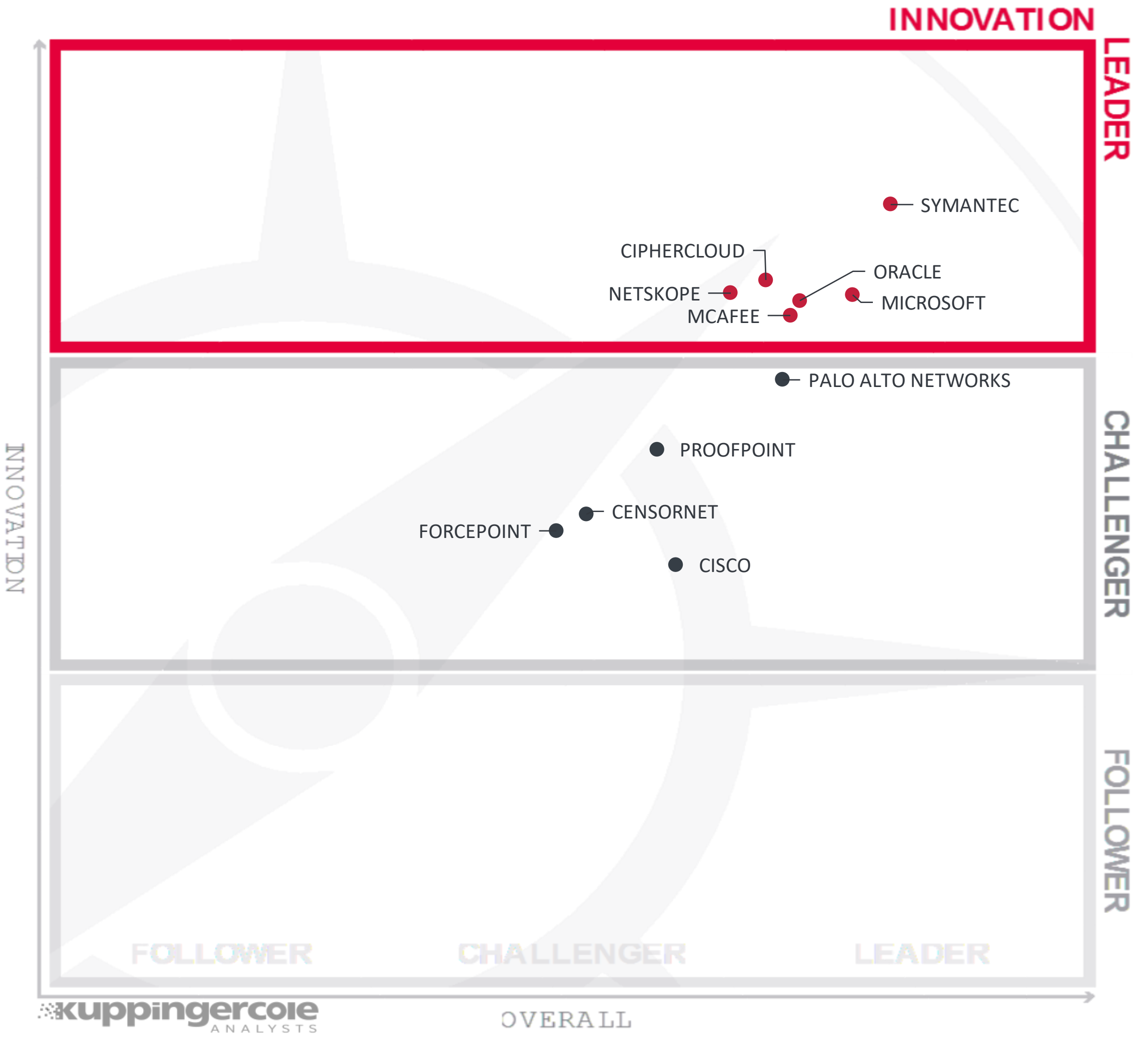


Figure 4: Innovation Leaders in the Cloud Access Security Brokers market segment

When looking at Innovation Leadership, we see a different picture. The Innovation Leadership rating shows the vendors as the leaders in this segment that have shown the consistent innovation and where they have acquired products these have been innovatively integrated. Many of the major vendors in the security marketplace have moved into the Cloud Access Security Broker market segment through acquisition. This has promise for customers when the acquired products have been fully integrated with the relevant vendor’s other products.

The leaders, Cipher Cloud, McAfee, Microsoft, Netskope, Oracle and Symantec have driven this market forward through innovation and integration of their products. These include in alphabetic order:

- CipherCloud
- McAfee
- Microsoft
- Netskope
- Oracle
- Symantec

2.4 Market Leadership

Finally, we looked at Market Leadership, i.e. the number of customers, the partner ecosystem, the global reach, and related factors affecting the leadership in a market. Market Leadership, from our point of view, requires global reach.

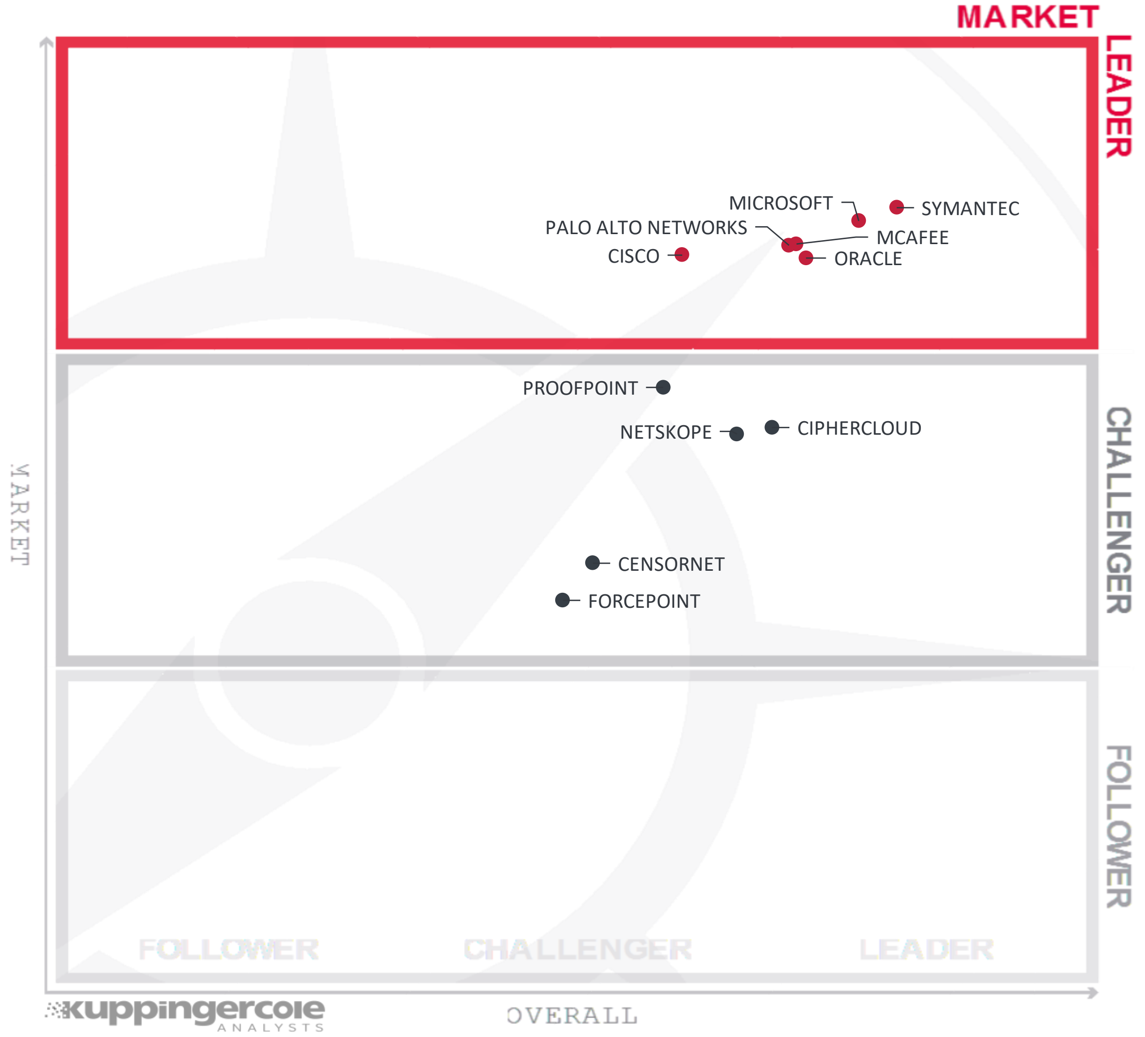


Figure 5: Market Leaders in the Cloud Access Security Brokers market segment

In this segment, the leading vendors are those that have a global presence with large customer bases and extensive partner ecosystems. These include the large multi-product vendors such as Microsoft and Symantec.

The other vendors in the challenger section have good products but do not have the same global presence.

Market Leaders (in alphabetical order):

- Cisco
- McAfee
- Microsoft
- Oracle
- Palo Alto Networks
- Symantec

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for, say, a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we deliver additional analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views looks at Product Leadership and Market Leadership.

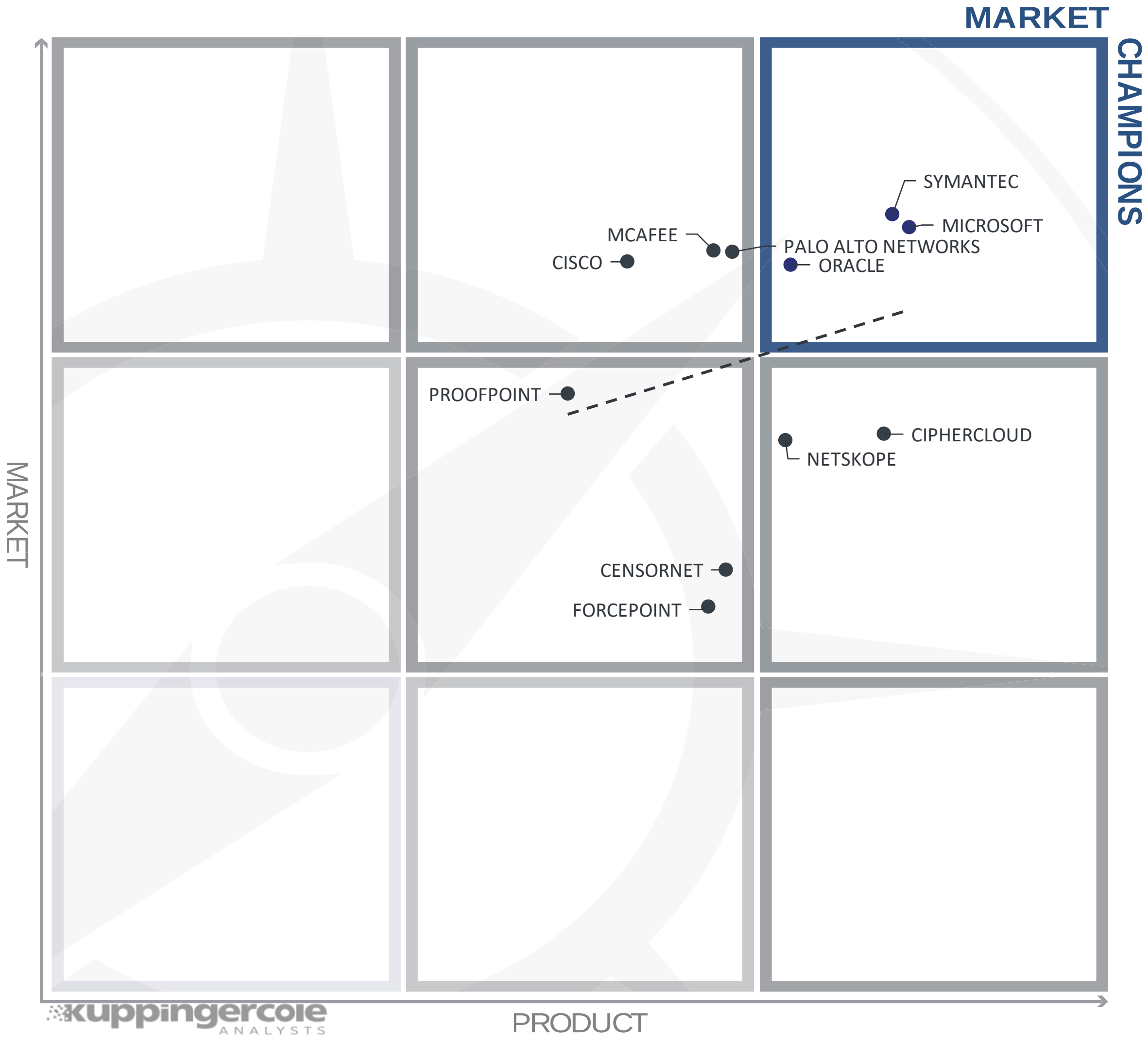


Figure 6: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line frequently are innovative but focused on specific regions.

The matrix shows a picture that is typical for evolving market segments, with a rather broad distribution of the various players across the quadrants and a weak correlation between Market Leadership and Product Leadership.

In the upper right box, we find Microsoft, Oracle, and Symantec. These vendors are leading in both the product and market ratings.

Below these, we find CipherCloud and Netskope which are product leaders but not in the Market Leader's segment.

On the other hand, in the center top box, we see Cisco, McAfee and Palo Alto networks having a significant market share while not being counted amongst the Product Leaders.

In the center of the graphic, we find (in alphabetical order): CensorNet, Forcepoint, and Proofpoint. These all have respectable positions in both the Product Leadership and Market Leadership ratings and thus are interesting alternatives to the leading vendors.

3.2 The Product/Innovation Matrix

The second view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with few exceptions. This distribution and correlation are typical for most markets with a significant number of established vendors plus some smaller players.

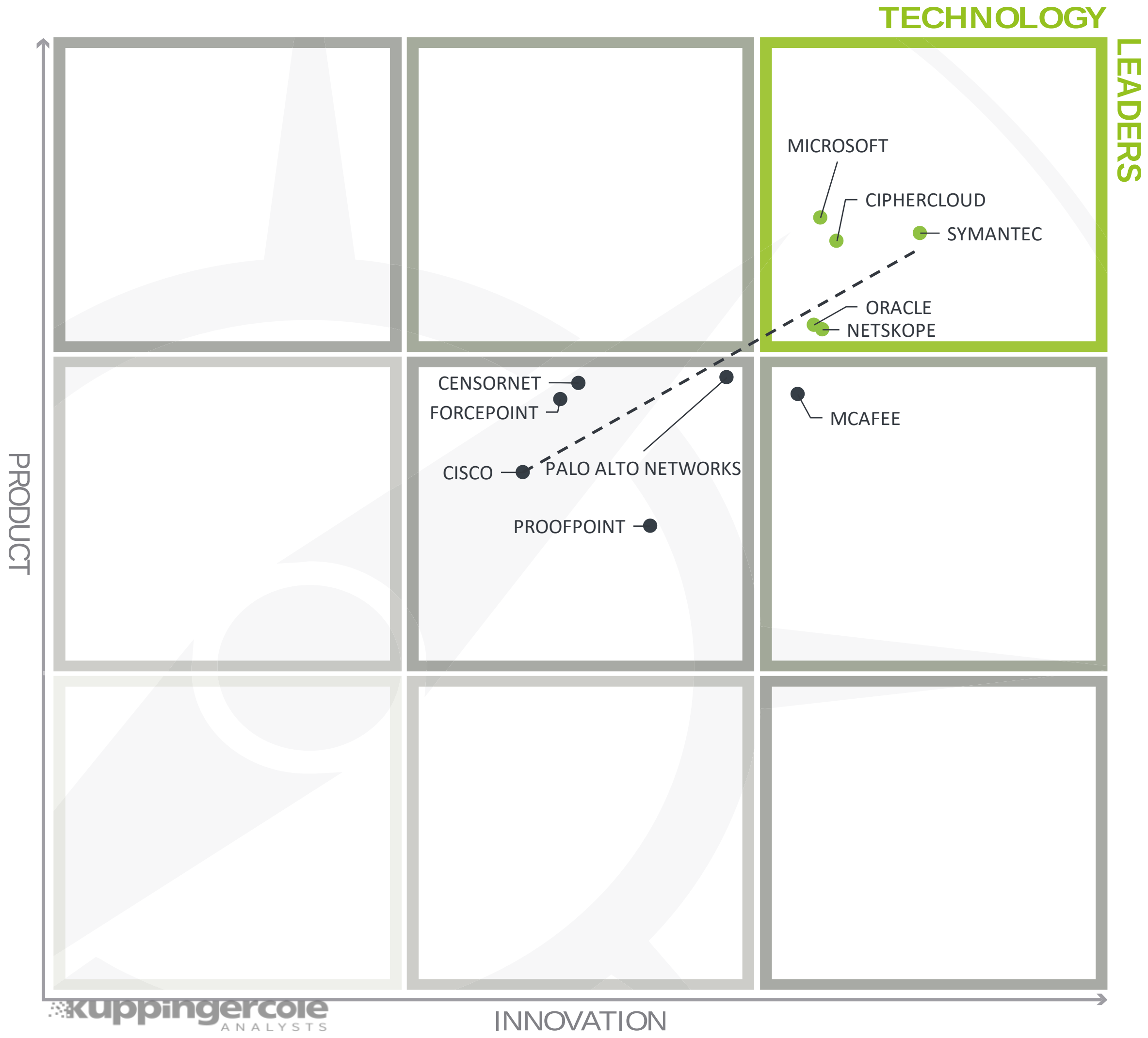


Figure 7: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

This chart shows a quite interesting picture with a spread of innovation and product capabilities.

CipherCloud, Microsoft, Netskope, Oracle and Symantec are both technology and innovation leaders and so are in the top right-hand quadrant.

McAfee has shown significant innovation but is not a product leader and so is in the right-hand center quadrant.

The remaining vendors’ products reside in the center of the chart including: CensorNet, Cisco, Forcepoint, Palo Alto Networks, and Proofpoint.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk to their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position but might also fail, especially in the case of smaller vendors.

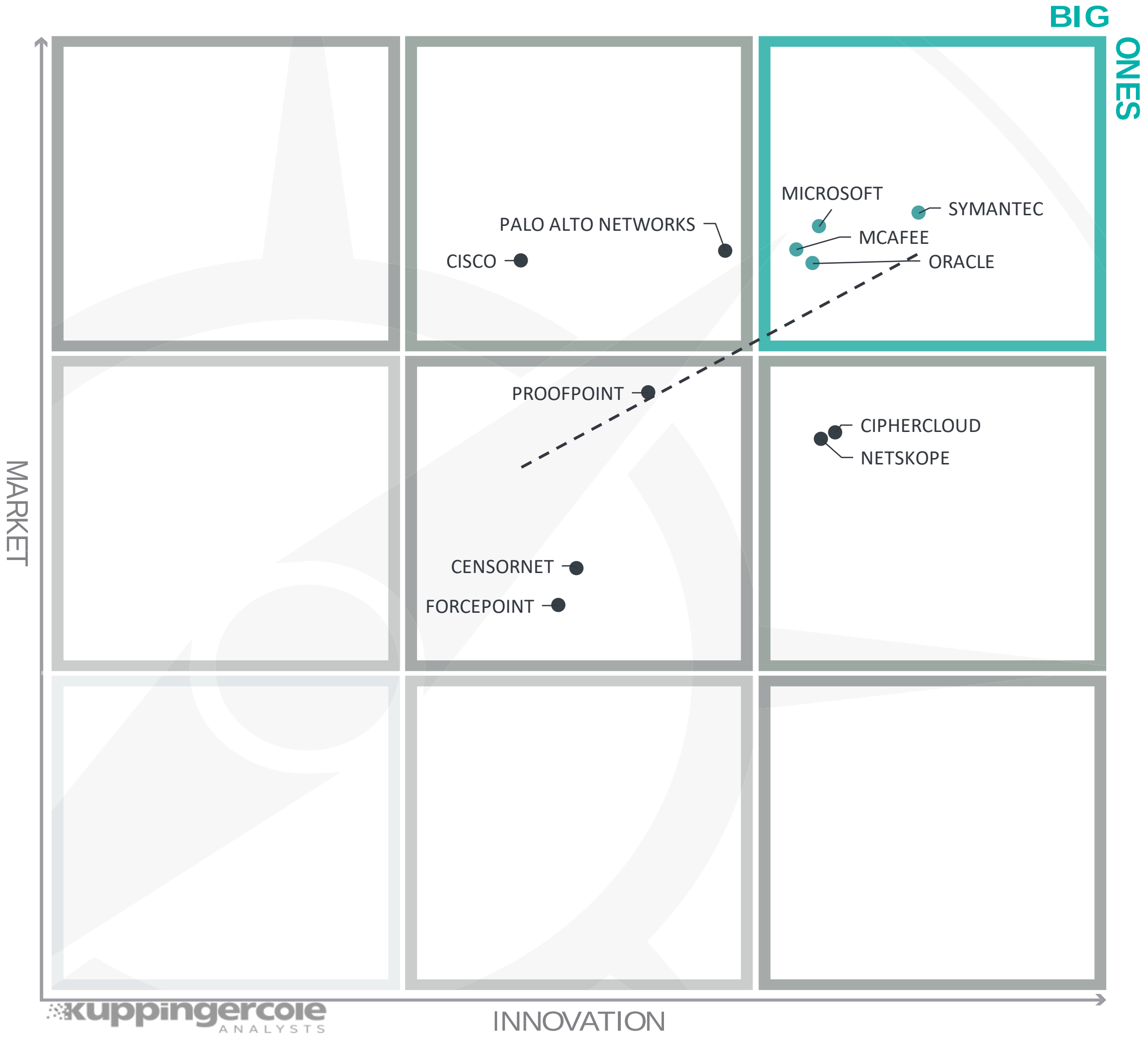


Figure 8: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relative position in the Innovation Leadership rating, while vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.

Again, as in the Product/Market Matrix, the vendors are widely distributed, showing only weak correlation between the market presence and the level of innovation they provide.

McAfee, Microsoft, Oracle, and Symantec are found in the top right-hand quadrant, having both an excellent position in the market and presenting innovative capabilities to their customers. Cisco and Palo Alto Networks are in the center top showing a strong market position but a lower level of innovation.

CipherCloud and Netskope are both innovative but do not have the same market share as the large vendors.

The remaining vendors surveyed fall into the center of the chart: CensorNet, Forcepoint, and Proofpoint.

4 Products and Vendors at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Cloud Access Security Brokers. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

4.1 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Product	Security	Functionality	Integration	Interoperability	Usability
CensorNet	Positive	Positive	Strong positive	Strong positive	Strong positive
CipherCloud	Strong positive	Strong positive	Strong positive	Strong positive	Positive
Cisco	Positive	Positive	Strong positive	Positive	Strong positive
Forcepoint	Positive	Strong positive	Strong positive	Positive	Strong positive
McAfee	Strong positive	Strong positive	Positive	Strong positive	Strong positive
Microsoft	Strong positive	Strong positive	Strong positive	Strong positive	Strong positive
Netskope	Strong Positive	Strong positive	Strong positive	Positive	Positive
Oracle	Strong positive	Strong positive	Strong positive	Positive	Strong positive
Palo Alto Networks	Positive	Strong Positive	Strong positive	Strong positive	Strong positive
Proofpoint	Positive	Positive	Positive	Positive	Positive
Symantec	Strong positive	Strong positive	Strong positive	Strong positive	Strong positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
CensorNet	Positive	Neutral	Positive	Neutral
CipherCloud	Positive	Strong positive	Neutral	Positive
Cisco	Positive	Strong positive	Strong positive	Strong positive
Forcepoint	Neutral	Positive	Neutral	Weak
McAfee	Strong Positive	Strong Positive	Positive	Strong Positive
Microsoft	Positive	Strong positive	Strong positive	Strong positive
Netskope	Positive	Strong positive	Neutral	Positive
Oracle	Positive	Positive	Strong positive	Strong positive
Palo Alto Networks	Positive	Positive	Strong positive	Strong positive
Proofpoint	Positive	Strong positive	Strong positive	Positive
Symantec	Strong positive	Strong positive	Strong positive	Strong positive

Table 2: Comparative overview of the ratings for vendors

Table 2 requires some additional explanation regarding the “critical” rating.

In Innovativeness, this rating is applied if vendors provide none, or very few, of the more advanced features we have been looking for in that analysis, like support for multi-tenancy, shopping cart approaches for requesting access, and others.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets like France or Germany or even within these markets. Usually, the number of existing customers is also limited in these cases.

In Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base but is also based on some other criteria. This doesn’t imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it’s also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no, or a very limited, ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

5 Product/service evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products, there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

5.1 CensorNet

CensorNet has its headquarters in Basingstoke, UK with offices in Austin, US; Copenhagen, Denmark, and Munich, Germany. CensorNet provides a range of solutions to help with the challenges of managing cloud applications in an increasingly mobile work environment. Cloud Application Security (CAS) from CensorNet provides a single point from which to discover, analyze and manage cloud services across multiple networks and devices.

Strengths	Challenges
● Discovery of use through inline inspection of network traffic, agents and API connectors; ● Strong cyber-security capabilities protect against malware and other cyber risks; ● Cloud Gateway can be installed on a virtual machine or physical server and is available as a cloud service; ● Control of access to cloud services based on enterprise identity and policies; ● Integration with ADS. ● Wide range of SaaS covered out of the box	● Limited but growing customer base; ● Small partner ecosystem, but some large partners on global scale; ● Low penetration in the North American markets.; ● Depends upon encryption functionality provided by cloud service to protect data at rest in the service.

Table 3: CensorNet's major strengths and challenges

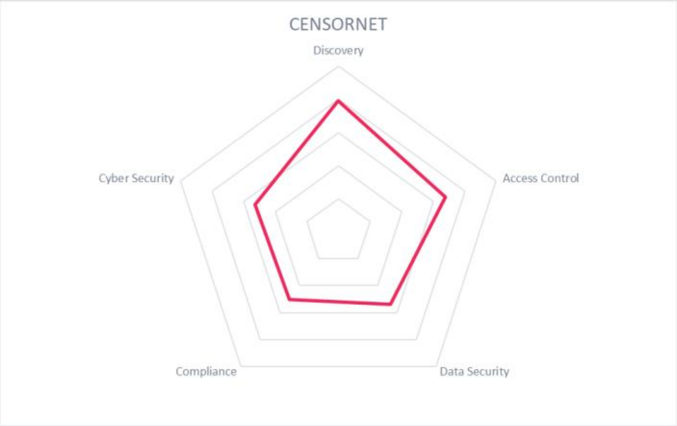
The key features provided by this solution are:

- Cloud Application Security is fully integrated with CensorNet's Unified Security Service (USS) that also includes Email Security, Web Security, and Multi-Factor Authentication. USS provides a single web interface for central policy configuration and management, as well as data visualization and reporting.
- Policies secure access to sanctioned cloud services such as Salesforce, Office365, and Box down to individual features and actions within applications. It is possible to block generic actions across all applications or groups of applications as well as based on content.
- Central keyword lists can be applied and used for DLP-style scanning of inbound and outbound email, web content, social media posts, and also in files uploaded to cloud storage apps (including Dropbox, Box, Google Drive, MS OneDrive and SharePoint).
- Protects against malware and other cloud threats using multiple security layers and a combination of technologies. Deep inspection allows SSL encrypted traffic to be scanned for malware.

Security	Positive
Functionality	Positive
Integration	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 4: CensorNet's Rating

CensorNet products provide a good range of control over access to cloud services with a growing number of customers in Europe. The challenge is for this success to be repeated in the USA.



5.2 CipherCloud

CipherCloud has its US headquarters in San Jose CA with offices worldwide. CipherCloud was founded in 2010 with a focus on enabling enterprises in a wide range of private and public sectors to secure their data and adopt the use of cloud services with confidence and compliance. The specific solutions covered by this report is CipherCloud CASB+ Platform which was launched in April 2018.

Strengths	Challenges
● AnyApp connector enables customers to protect their own applications with Cipher Cloud CASB+; ● Encryption provides full end to end data protection with a native key management solution in addition to with full support for HSM; ● Provides inline adaptive access control to data based on various contextual attributes like User, Groups, Device Profile, etc.; ● In use by customers to achieve compliance with a wide range of data security standards; ● Wide range of enterprise SaaS covered out of the box; ● Integration with leading IDaaS solutions.	● The integration with some SaaS services depends upon the undocumented and unsupported data structures in the network traffic. However, CipherCloud does use documented APIs where available. ● Potential customer base may be eroded by functionality built into SaaS services. CipherCloud claims the opposite is the case.

Table 5: CipherCloud's major strengths and challenges

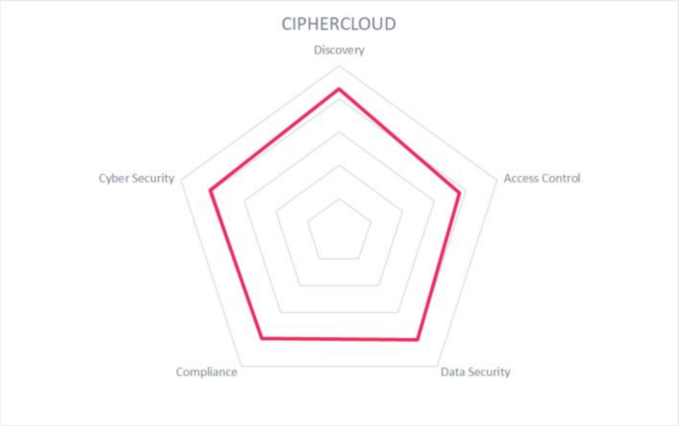
The key features provided by the CipherCloud CASB+ Platform are:

- AnyApp allows customers to integrate the data protection capabilities for their own custom cloud-based applications;
- Data tokenization, encryption, and key management with the flexibility to address a mix of security requirements. It includes data protection, data loss prevention, native device management, secure offline data access, automated PII anonymization, and HSM support;
- Visibility for the organization's cloud usage to reveal shadow IT activity, while providing an assessment on the risk of each cloud service being used;
- Protection to identify and stop threats that are being shared through cloud-based services.
- This includes capabilities such as adaptive access control, user and entity behavior analytics;
- Offers access controls during authentication based on attributes like user, groups, location, device, etc.
- Enables compliant use of cloud applications against a range of current and pending global privacy and compliance regulations including PCI, PII, HIPAA, GDPR, and others.
- Integration with enterprise tools like DLP, EMM, SIEM, IDP, etc. leverages existing investments.

Security	Strong Positive
Functionality	Strong Positive
Integration	Strong Positive
Interoperability	Strong Positive
Usability	Positive

Table 6: CipherCloud's Rating

CipherCloud provides a strong solution for securing data held in SaaS services and for controlling access to that data. It has numerous examples of customers that have used its products to achieve compliance with a range of laws and regulations.



5.3 Cisco Cloudlock®

Cisco is a is the worldwide technology company founded in 1984. Cisco's Cloud security portfolio is comprised of Cisco Cloudlock CASB which was acquired in 2016, together with Cisco Umbrella, which provides security for Internet access at the DNS layer, and Cisco Steathwatch that helps to identify threat activity in public cloud infrastructure. Cisco Cloudlock and Email Security provide visibility and protection for SaaS apps, including cloud email. This report covers the Cisco Cloudlock platform.

Strengths	Challenges
● App risk rating based on large amount of community-sourced data; ● Integrated DLP engine with range of standard policies out of the box; ● Detection of abnormal user behavior to enhance threat detection; ● Wide range of SaaS apps covered out of the box; ● Integration with other Cisco products; ● Cisco's strength in the market.	● Depends upon integration with external IDaaS to implement enforcement of user access controls; ● Detection depends upon Cloud service APIs which may lead to delay in enforcement; ● Dependency on other vendors for identity management tools (IDaaS); ● Integration with Access Governance systems.

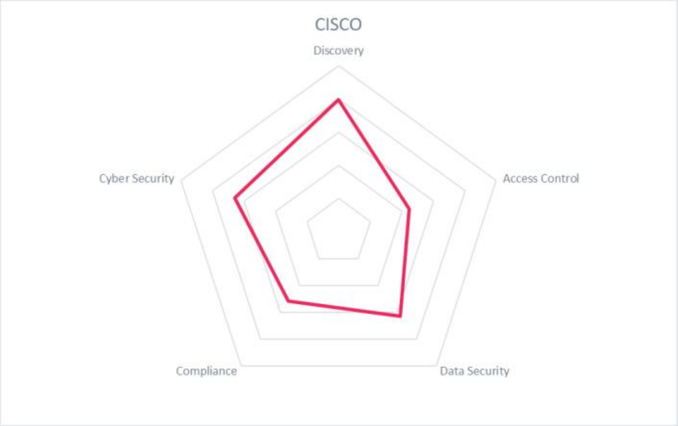
Table 7: Cisco Cloudlock's major strengths and challenges

The key features provided by the CloudLock Platform are:

- The Cisco Cloudlock Apps Firewall discovers cloud apps connected via OAuth to the corporate environment and provides a crowd-sourced Community Trust Rating for individual apps, as well as the ability to ban or whitelist them based on risk profile and access scope.
- Cloud Data Loss Prevention (DLP) continuously monitors cloud environments to detect and secure sensitive information using out-of-the-box policies as well as custom policies. Automated response actions can remediate risk in the event of a policy violation, including end-user notifications, encryption, transfer of ownership, quarantine, and more.
- Cross-platform User and Entity Behaviour Analytics (UEBA) for SaaS, PaaS, and IDaaS environments leverages machine learning algorithms to detect anomalies. Cloudlock can also detect activities outside of whitelisted countries and detect activities that cross distances at impossible speeds.

Security	Positive
Functionality	Positive
Integration	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 8: Cisco Cloudlock's Rating



Cisco Cloudlock CASB platform integrates with other Cisco products and Secure Web Gateway technologies to defend against cyber-threats and implement security control across on-premises and cloud environments. It provides an API-based approach to cloud security that is easy to deploy and simple to manage.

5.4 Forcepoint

Forcepoint was formed in 2016 as a result of the combination of the Raytheon Cyber Products, Websense and Stonesoft organizations. In 2017 Forcepoint acquired the Skyfence CASB product and business from Imperva.
Forcepoint CASB Application Security Suite includes Cloud Governance and Cloud Audit and Protection. These provide functions that discover cloud service usage, data loss prevention, user activity monitoring and cyber threat prevention.

Strengths	Challenges
● Part of a comprehensive suite of products; ● Both in-line and offline deployment options; ● Provides some cloud identity governance capabilities; ● Auditing of cloud privileged user activity; ● Integrated data classification and DLP integration.	● Late into the market for CASBs; ● Very small partner ecosystem; ● Integration with Access Governance systems.

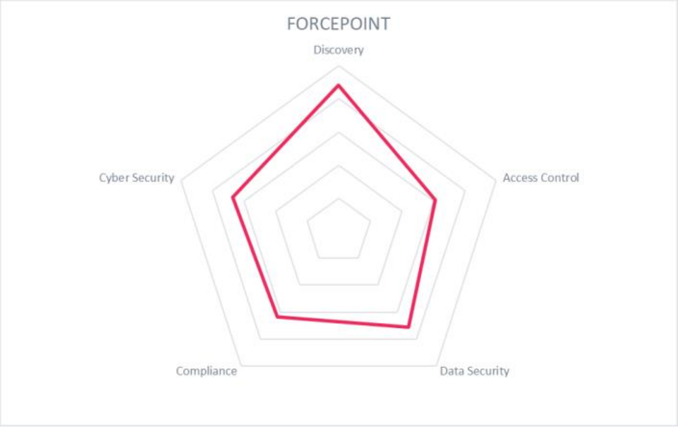
Table 9: Forcepoint's major strengths and challenges

The key features provided by these solutions are:

- Forcepoint CASB extends traditional cloud app discovery information by providing details on risk factors that are unique to the organization. These include visibility into dormant accounts, orphaned accounts and external accounts that present a variety of security risks.
- It also benchmarks the organization's cloud app security configurations against industry best practices and regulatory requirements, to identify security and compliance gaps.
- Monitors and controls uploading, downloading and sharing of sensitive data. It includes inbuilt DLP capabilities and integrates using ICAP with existing enterprise DLP.
- Real-time activity monitoring of users and analytics including privileged users
- Establishes detailed behavioral profiles based on the normal usage patterns for each user, department, and device. Anomalous access can be configured to alert, block or require two-factor authentication in real-time.
- It is also possible to block or restrict access from unmanaged endpoints (BYOD).

Security	Positive
Functionality	Strong Positive
Integration	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 10: Forcepoint's Rating



Forcepoint CASB Application Security Suite provides visibility and control over access to both sanctioned and unsanctioned apps from both managed and unmanaged devices. It includes integrated DLP technology and integrates with both on-premise user directories and a range of identity providers.

5.5 McAfee® MVISION Cloud

McAfee, from its foundation in 1987, has a long history in the world of cyber-security. Acquired by Intel in 2010, it was spun back out, becoming McAfee LLC, in April 2017 with headquarters in Santa Clara CA, USA. In January 2018 McAfee closed its acquisition of Skyhigh Networks. The Skyhigh CASB is now sold as the McAfee® MVISION Cloud integrated with other McAfee products.

Strengths	Challenges
● Comprehensive functionality ● Integration with existing deployed complementary solutions. ● Innovative encryption capabilities ● Proven Compliance capabilities	● Dependence upon external IAM systems. ● Full integration with other McAfee products. ● Administrator documentation is only available in a very limited set of languages.

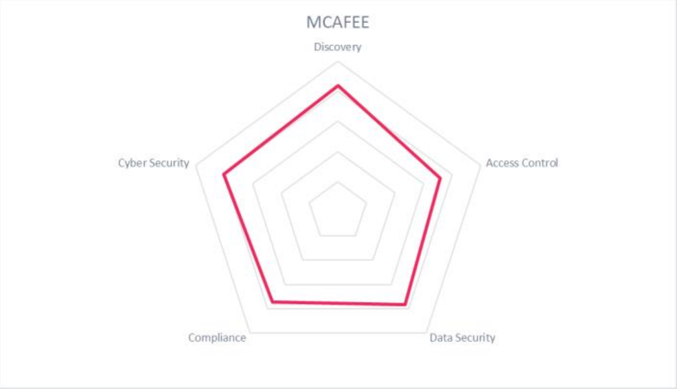
Table 11: McAfee's major strengths and challenges

The key features provided by McAfee® MVISION Cloud are:

- Provides visibility into data, context, and user behavior across all cloud services, users, and devices. Enables real-time actions to enforce policies (such as collaboration control, device control etc.) across all cloud services to apply consistent data protection. A registry of cloud services includes a Cloud Trust Rating for each service based on a 261-point risk assessment. Helps to remediate security threats by controlling risky user behavior and correcting misconfigurations.
- The platform provides a unified policy engine that covers data at rest and in transit which can leverage policy templates, import existing policies or create new ones. Out of the box policy templates cover a wide range of regulatory compliance needs.
- Encryption of cloud data (in motion or at rest) using multiple encryption schemas, supporting customer keys (BYOK).
- Cloud service configuration management.
- Privacy guard leverages an irreversible, one-way process to tokenized data holding key data on premises.
- Uses machine learning to identify patterns indicative of malicious activity and data exfiltration. Forces adaptive authentication based on policies through integration with IAM solutions.
- Detects malware through know signatures, sandboxes, and behavior indicative of data exfiltration or ransomware.
- Integration – integrates with existing deployed hardware and technology solutions including: firewalls, proxies, IAM, DLP, SIEM and key management.

Security	Strong Positive
Functionality	Strong Positive
Integration	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 12: McAfee's Rating



The McAfee® MVISION Cloud together with the other McAfee products provides a comprehensive set of functionalities to ensure the secure and compliant use of cloud services.

5.6 Microsoft

Microsoft Cloud App Security is based on the Adallom Cloud Access Security Broker which was acquired in 2015. This has now been fully integrated with other Microsoft products and forms part of Microsoft Enterprise Mobility + Security suite. Recently added new features include cloud conditional access app control through a reverse proxy and deep integration with Microsoft Information Protection.

Strengths	Challenges
● In use by many Microsoft customers; ● Native integration with Microsoft Enterprise Mobility + Security suite; ● Conditional access capabilities for any app both on-premises and in the cloud ● Automated information protection capabilities to apply labels and EDRMS across cloud and on-premises; ● Out of the box integration with a wide range of cloud applications; ● Simplified licensing – one license covers all.	● Does not provide encryption/tokenization of structured data held in cloud applications such as CRM applications. ● Gaining traction in organizations where use of Microsoft technology is limited. ● While well integrated with Microsoft Active Directory there is a lack of integration with other Access Governance systems.

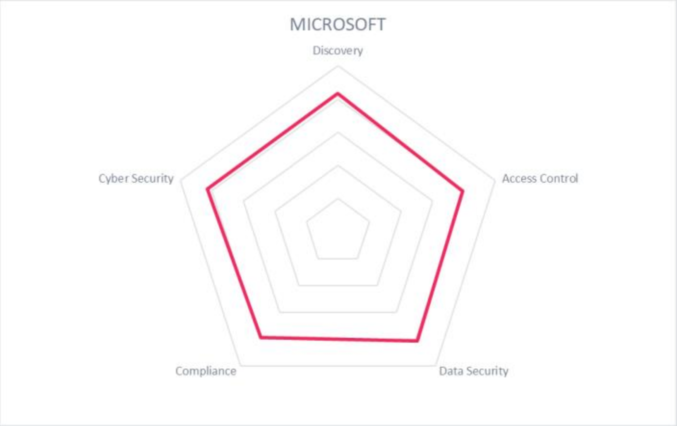
Table 13: Microsoft's major strengths and challenges

The key capabilities that Microsoft Cloud App Security provides are as follows:

- Discover – It enables the organization to discover the cloud apps being used from their cloud environment and evaluates the risk of these apps based on more than 70 parameters;
- Protect – it provides granular control over data and use through built-in or custom policies for data sharing and data loss prevention;
- Control access to cloud apps based on conditions and session context, including user identity, device, and location;
- Compliance – it factors compliance with regulations into the risk assessment score for each app, and helps to control and protect sensitive files through policies and governance;
- Threat detections - it exploits Microsoft threat intelligence and research to identify emerging threats and user behavioral analytics to detect anomalies. It includes templates to detect ransomware attacks and integrates with SIEM solutions

Security	Strong Positive
Functionality	Strong Positive
Integration	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 14: Microsoft's Rating



Microsoft Cloud App Security, as part of Microsoft Enterprise Mobility + Security suite, provides a well-rounded and complete CASB 2 solution. It enables the user organization to customize cloud usage and to control users' access to cloud apps and to protect data in the cloud.

5.7 Netskope

Netskope, which was founded in 2012, has its headquarters in Los Altos CA USA and offices in the UK, Australia, and India. This report covers Netskope Security Cloud which uses patented technology called Netskope Cloud XD™. It is intended to target and control activities across both SaaS and IaaS cloud services as well as websites.

Strengths	Challenges
● Enables granular control over unsanctioned but permitted cloud services; ● Inline and API based visibility and controls; ● Strong inbuilt data leak prevention capabilities; fine grained control over social media use; ● Detect and control IaaS misconfiguration; ● Visibility and control of cloud usage via managed and unmanaged devices.	● Netskope has achieved market penetration in the US but still needs to continue to grow in the rest of the world; ● Netskope is not yet profitable; ● Integration with Access Governance systems.

Table 15: Netskope's major strengths and challenges

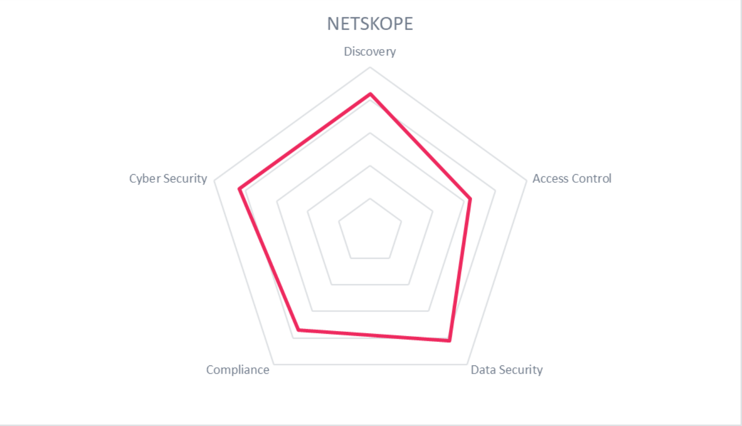
The key features provided by this solution are that it enables organizations to:

- Discover SaaS, IaaS, and web use details and assess risk. Netskope Cloud XD uses big data analytics to identify usage in "extreme definition" (XD) across all SaaS, IaaS, and web.
- Secure access to sanctioned cloud services such as Office 365, Box, and AWS and safely enable unsanctioned, business-led cloud services without the need to block them.
- Govern cloud and web use for users on-premises, mobile, and remote using security and access policies in context (e.g. based on service, activity, device).
- Encrypt both structured and unstructured data in sanctioned services using AES-256 encryption and the use of on-premises HSM.
- Prevent data leakage from SaaS, IaaS, and web with accuracy and precision. Supports more than 1,000 file types, more than 3,000 data identifiers, proximity analysis, fingerprinting, exact match, OCR, and others.
- Protect against malicious websites and block infected files. Identify anomalous user behavior that could indicate compromised credentials, privileged account abuse, and data exfiltration.
- Coverage of every deployment architecture offered in the market including log-based discovery, introspection, inline as a reverse proxy, inline as a forward proxy, in-line with or without agents or mobile profiles.

Security	Strong Positive
Functionality	Strong Positive
Integration	Strong Positive
Interoperability	Positive
Usability	Positive

Table 16: Netskope's Rating

Netskope Security Cloud provides a best of breed DLP solution that is applicable to protecting data in the context of cloud services.



5.8 Oracle

Oracle is a major IT software and hardware vendor. In September 2016 Oracle signed an agreement to acquire Palerra. Oracle has invested significantly in Oracle CASB Cloud Service, which was formerly called Palerra LORIC, by adding DLP and malware scanning, forward and reverse proxy deployment topologies, in conjunction with strong integration with Oracle's Identity SOC.

Strengths	Challenges
● Support for Oracle Public Cloud including Oracle Cloud Infrastructure, Oracle HCM Cloud, ERP Cloud, CX cloud; ● Covers IaaS including AWS and Azure as well as OCI and Rackspace; ● Autonomous threat detection and remediation using ML & UEBA; ● Integrated IRM capabilities plus advanced DLP including OCR support.	● Integrates with cloud directories but not on premises user stores such as Microsoft Active Directory; ● Documentation only in English with no localized versions.

Table 17: Oracle's major strengths and challenges

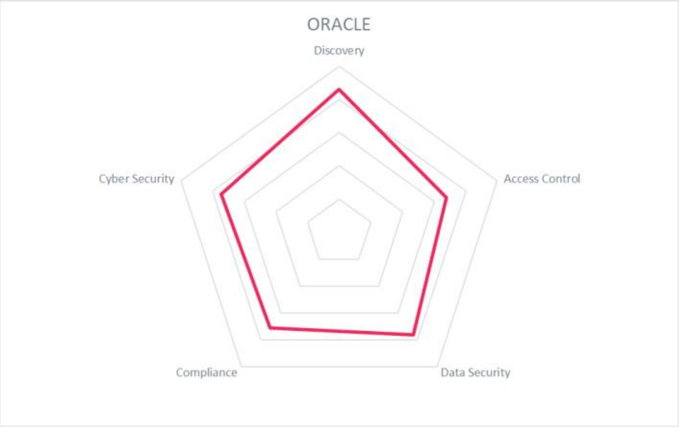
Oracle's Cloud Access Security Broker (CASB) Cloud Service is a cloud security solution that helps protect cloud-based infrastructure, platforms, and applications across vendors. Specifically, for customers adopting Oracle Cloud Infrastructure (OCI), Oracle CASB provides visibility, threat protection, data security and compliance for their OCI deployments. It provides capabilities covering visibility, compliance, data protection, and threat prevention, across the full landscape of enterprise Cloud Services. Oracle CASB is also available as an on-premises solution for customers of Oracle Cloud-at-Customer:

Oracle CASB has several important capabilities including:

- Broad support for IaaS/Custom Apps as well as SaaS with a java micro agent for code level monitoring of custom apps;
- Detects OCI components misconfiguration and includes Smart Policies based on security expertise are automatically turned on for each customer to ensure consistent security;
- User profiling and threat detection based on Machine Learning ensures accurate detection with low false positives;
- Inbuilt Information Rights Management and DLP capabilities for unstructured data;

Security	Strong Positive
Functionality	Strong Positive
Integration	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 18: Oracle's Rating



Oracle CASB Cloud Service is likely to be attractive to customers using Oracle's products. It provides a unique approach to the governance and security of cloud usage. It also forms part of a wider suite of security products from Oracle and these products provide a powerful combination when used together.

5.9 Palo Alto Networks Inc.

Palo Alto Networks Inc. is a security company with a mission to help organizations worldwide prevent cyber breaches. Palo Alto Networks acquired CirroSecure in 2015, which was later launched as Aperture after integration into the Palo Alto Networks Security Operating Platform which added to the Palo Alto Networks Next-Generation Security Platform. Their platform's CASB capabilities were extended in 2017 to include forward and reverse proxy CASB capabilities through its GlobalProtect cloud service. Palo Alto recently acquired Evident.io and RedLock for Cloud Security Posture Management.

Strengths	Challenges
● Provides visibility into data and end-user activity detects risky behaviors; ● Monitors and controls movement of data to external and cloud services; ● Integrates with other Palo Alto Networks products to provide extended security capabilities.	● Does not yet provide inbuilt encryption/tokenization of structured data held in cloud applications; ● Does not yet include UEBA analytics for threat detection. ● Full integration of the recently acquired products.

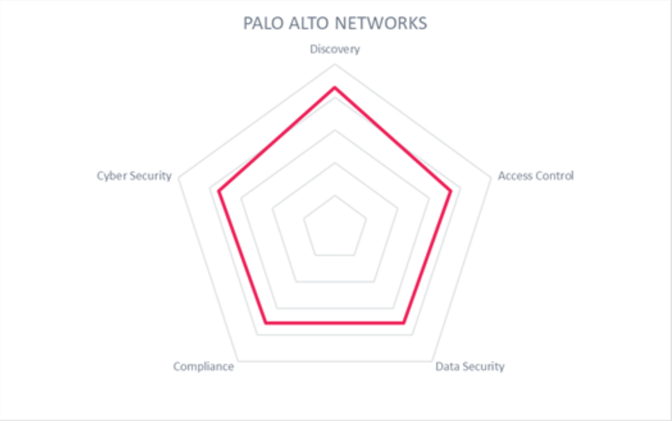
Table 19: Palo Alto Networks' major strengths and challenges

The key features provided by these products are:

- Visibility – for Shadow IT Palo Alto Networks GlobalProtect cloud service and Next-Generation Firewall provide inline capabilities to detect, monitor and report on access to and risk of a range of external cloud services and applications. Aperture extends these capabilities via SaaS provider APIs to provide visibility and enforcement across all user, folder and file activity for sanctioned cloud apps. Policy violations within existing data are proactively found no matter how old the data or share may be.
- Classification and control - Aperture inspects documents for hundreds of pre-defined and custom data patterns including credit card numbers, SSH keys, and Social Security numbers. Aperture provides the capability to define granular, context-aware policy and enforce control to quarantine users and data as soon as a risk occurs. The reverse proxy provides control over access to sanctioned SaaS apps from unmanaged devices without the need for access via a portal.
- Threat prevention - WildFire integrated with Aperture provides threat prevention to block known malware and identify and block unknown malware. This prevents threats from spreading through the sanctioned SaaS applications, controlling a potential insertion point for malware.

Security	Positive
Functionality	Strong Positive
Integration	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 20: Palo Alto Networks' Rating



Overall Palo Alto Networks' products in combination provide a powerful approach to control access to cloud applications. They have a strong roadmap to deliver enhancements and integration of recently acquired products.

5.10 Proofpoint.

Proofpoint is a security and compliance company that was founded by Eric Hahn, former CTO of Netscape, founded the company in 2002. The company went public in April 2012. In late 2016 Proofpoint acquired FireLayers an Israeli company with a CASB product. As well as acquiring a CASB this FireLayers product was intended to enrich and benefit from the Proofpoint Nexus platform. The report covers the Proofpoint Cloud App Security Broker (PCASB).

Strengths	Challenges
● People-centric protection for sanctioned cloud apps; ● Includes access governance capabilities; ● Risk-based access control and analytics; ● Threat aware data security; ● Third party application control; ● Policy-based response actions.	● Provides less functionality in Shadow IT governance than the market leaders; ● Does not provide inbuilt encryption/tokenization of structured data held in cloud applications such as CRM applications; ● Does not provide control over on-premise apps;

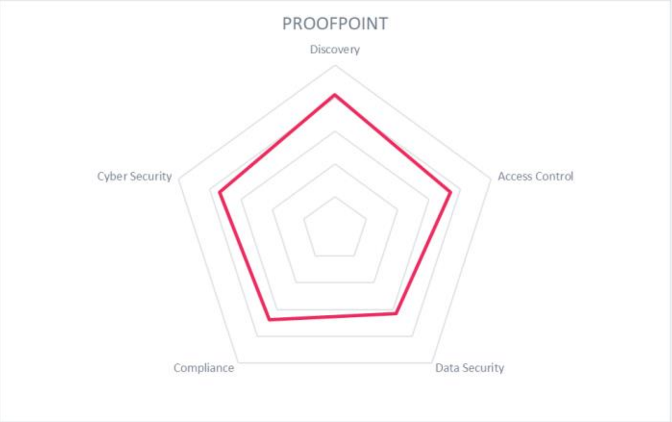
Table 21: Proofpoint's major strengths and challenges

The key features provided by this product are:

- Visibility – provides people-centred visibility into cloud access and data handling. This makes it possible to see privileged and very attacked accounts and their cloud activity. It also identifies files in SaaS that shared broadly may be violating DLP rules, their owners and who is accessing them. It provides risk assessments of unsanctioned apps in use with the capability to control access.
- Data security – it shares DLP classifications with other Proofpoint products to enable unified policies. These classifiers cover a wide range of compliance needs. Policies can be created to encrypt, mask or quarantine data. User-centric activity monitoring reveals activity on compromised or orphaned accounts. PCASB can also automate the control of third-party add-on apps that pose a significant risk to data security.
- Threat prevention – PCASB combines cross-channel threat intelligence that spans email, social media, mobile devices, cloud apps and network with user-specific risk indicators to analyze user behavior and detect anomalies in SaaS apps. It brings together contextual data about the user and behavior analytics to pinpoint suspicious activity. Policy templates make it possible to apply risk-based authentication or reduce privileges when needed. It also integrates with existing identity management solutions using SAML.

Security	Positive
Functionality	Positive
Integration	Positive
Interoperability	Positive
Usability	Positive

Table 22: Proofpoint's Rating



This product provides a unique people-centric approach to control over SaaS app use. However, the functionality provided is not as rich as the market leaders focussed on Shadow IT Governance. In combination with other Proofpoint products, it provides a useful approach to SaaS security and further integration with other Proofpoint products is on the roadmap.

5.11 Symantec

Symantec is an US software company headquartered in Mountain View, California that specializes in IT security software and services. This report covers Symantec CloudSOC which integrates with other Symantec products to provide a comprehensive CASB 2.0 solution.

Strengths	Challenges
● Broad and deep coverage of a wide range of cloud Apps including G Suite; ● Inbuilt ContentIQ DLP uses machine learning; ● Malware protection based on Symantec Threat Intelligence and technologies; ● User account protection through adaptive authentication and UBA; ● Powerful features enabled through integration with other Symantec products.	● Explaining the different kinds of integration provided by “Securelets” and “Gatelets”. ● While integrated with identity management systems there is little integration with Access Governance systems.

Table 23: Symantec’s major strengths and challenges

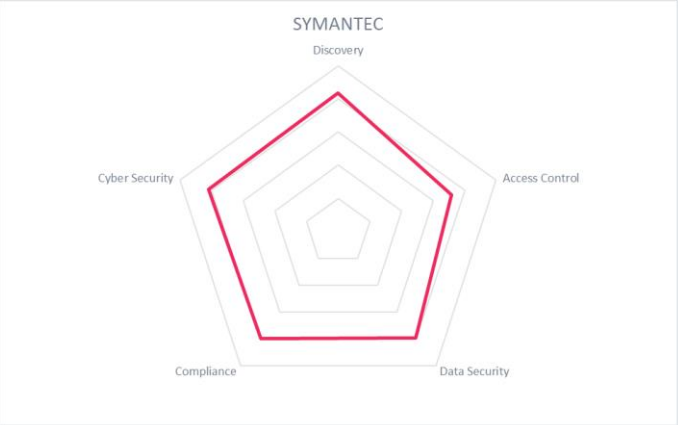
The key features provided by Symantec CloudSOC are:

- Visibility - Shadow IT analysis for both on-network and off-network users via intelligent integration with Symantec Secure Web Gateway.
- Risk analysis – User Behaviour Analytics (UBA) leverages machine learning to automatically maintain individualized Threat Score based on user activity.
- Adaptive authentication – risk analysis can also trigger the requirement for multifactor authentication before the user can proceed.
- Data Security – it provides data governance, DLP, malware scanning and encryption in real-time for cloud application traffic. This is based on machine learning-assisted ContentIQ for native CASB data governance and DLP capabilities, plus the option to fully integrate with Symantec DLP for Cloud.
- Information Centric Encryption: The ability to have security follow the data; intelligently encrypt data based on data classification rules and require end-devices to authenticate to view the data.
- Tokenization/Encryption – Field-level and file-level tokenization and encryption, without impacting functionality of the cloud app.
- Reporting and incident response - CloudSOC collects granular data on transactions with advanced visualization, filtering and search features to enable quick analysis of this data, along with extensive reporting options.

Security	Strong Positive
Functionality	Strong Positive
Integration	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 24: Symantec’s Rating

Symantec CloudSOC provides comprehensive CASB 2.0 functionality through intelligent integration with other Symantec products including Web Security, Malware Protection, DLP, Endpoint Protection and User Authentication.



6 Vendors and Market Segments to watch

Besides the vendors covered in this KuppingerCole Leadership Compass on the Cloud Access Security Brokers market segment, there are several other vendors which either declined participation in this KuppingerCole Leadership Compass, have only a slight overlap with the topic of this document or are not (yet) mature enough to be considered in this document.

6.1 Bitglass

Bitglass was founded in 2013 and has its headquarters in Campbell CA, with offices in the Netherlands, Australia, Singapore, and Brazil. Bitglass's CASB is delivered as a cloud service delivered through the AWS cloud. It provides a comprehensive solution that leverages both proxies and cloud service native APIs to control access to the cloud services and to protect the data held in these services. The solution includes inbuilt DLP and data encryption. It currently has a limited but growing customer base and has a relatively small partner ecosystem, but these include some large partners on a global scale.

6.2 Centraya

Centraya is the European Cloud Access Security Broker produced by e3 AG a Swiss company with offices in Zurich and Frankfurt in Germany.   Centraya protects organization data in cloud-based CRM, HR or any other application against unauthorized access or data theft. It provides data privacy for Salesforce, SAP Hybris, ServiceNow, Microsoft Dynamics CRM, and SugarCRM.

It is a central gateway security solution that runs on premise under full control of the customer. For example: when an employee creates a new account entry in a cloud CRM solution, Centraya identifies the content, encrypts it and stores it in encrypted form in the cloud. The organization defines what needs to be protected using a policy. When employee needs to access the data again: the central security gateway detects the request, decrypts the content and presents it in plain text to the user without the need for user interaction.

6.3 CyberArk and Vaultive

In March 2018, CyberArk announced the acquisition of certain assets of privately-held Vaultive, Inc., a cloud security provider. Vaultive had previously provided a stateless network-layer software encryption proxy that was mentioned in the previous version of this report.

Building upon the Vaultive technology, CyberArk plans to deliver greater visibility and control over privileged business users, and Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) administrators.

6.4 FireMon 40Cloud

In October 2016 – FireMon, a Network Security Policy Management company, acquired FortyCloud, a Cloud Infrastructure Security Broker (CISB) 40Cloud which is now offered by FireMon

CISBs are an emerging type of solution that takes the concept of CASB and applies it to IaaS (instead of SaaS). While CASBs are concerned with providing visibility and access control over the use of SaaS services CISBs are focussed on the network security issues that surround the use of IaaS (Infrastructure as a Service).   CISBs provide the following kinds of functionality:

- Network security – many public IaaS offerings provide a partial set of network security features. The CISB provides software components (e.g. gateways, agents) that can be installed on the cloud platform (and/or at the enterprise network) and complements the basic cloud network security elements.

- Abstraction – a CISB provides an abstraction layer that unifies multiple IaaS platforms under a single policy system. This enables the implementation of a single policy that can be enforced on all IaaS platforms (public, private and hybrid) that are used by the organization.
- Automation and Orchestration – The CISB's ensures that the network security policy (that encompasses firewall rules, identity-based access rules, encryption policies) are enforced on all IaaS platforms used by the organization.

6.5 Fortinet FortiCASB

Fortinet is a cybersecurity company founded in 2000 with headquarters in Sunnyvale CA in the USA. FortiCASB is a Cloud Access Security Broker (CASB) with Cloud Security Posture Management (CSPM) capabilities. The product exploits the APIs provided by cloud services to provide:

- Visibility into the resource usage of IaaS together with and control over the service configuration. It performs IaaS configuration assessments across an organization's global IaaS deployment on AWS, Azure, and GCP. It identifies risks associated with the insecure provisioning and configuration of cloud resources. Using the information gathered it generates compliance reports that list gaps from regulation requirements of supported reports.
- Visibility and control of over access to SaaS applications and stored data. It connects directly to the SaaS provider to access data and files stored in an organization's accounts. Changes are validated against data leakage policies and scanned for threats. Existing information or "data at rest" is also scanned to ensure it meets business policies.

6.6 NextLabs®

NextLabs® has its USA headquarters in San Mateo, CA with offices worldwide. Although it does not have a pure CASB product that fits into this analysis, its products provide functionality that is very relevant to protecting data in the cloud. These products include those in its Data Centric Security Suite: NextLabs Control Center, NextLabs Rights Management, and NextLabs Entitlement Management.

This suite of products provides strong policy-driven data-centric control that covers information wherever it is stored or processed; including data held and processed in the cloud. Given this focus, the suite does not provide specific functionality to detect "shadow" cloud services or provide any risk ratings for services. The NextLabs' products are based around the XACML standard and provide control through policy enforcement points which enable the movement of and access to data to be controlled wherever it resides. This is supplemented by digital rights management functionality that encrypts data so that, even if there is unauthorized access the information cannot be decrypted.

6.7 Nexus

The Identity and security company Nexus Group was founded in 1984. It has its headquarters in Hägersten, Sweden. Nexus's focus is on supporting organizations to connect people, services and things in a secure way with the Smart ID platform. The Nexus Hybrid Access Gateway is a software-based authentication and federation product used to enable secure access to digital services – no matter where those services or users are located. It can provide secure access to an organization's digital resources through its web portal or as an add-on 2FA service to a different online portal.

This can be used to give employees secure and remote access to central enterprise resources, partner-hosted systems as well as cloud services. The solution is also suitable for user authentication in online banking, e-commerce and e-government services. It is eIDAS compatible and can connect to the respective nodes. By implementing the identity federation functionality, users are enabled to log on once to securely reach all resources connected to the Nexus Hybrid Access Gateway.

Its main objectives are to enforce organizational access policies as cloud-based services are accessed. It supports open standards such as SAML and Oauth2 and the upcoming version Open ID Connect which ensures that users are provisioned as soon as they access a cloud application. It also supports a wide range of multi-factor authentication methods from OTP to PKI based form factors.

6.8 Salesforce Shield

The Salesforce Platform is extensively used by organizations to improve the service that they give to their customers. Therefore, the platform stores many kinds of data that are subject to privacy laws and other regulations, for example in the financial services industry. These requirements include the need for monitoring, control over access, auditing and encryption. The data within the Salesforce Platform is held in a structured database, and previously the users of tenant applications have had no control over the encryption of the data. CASBs have been the main tool that allowed tenants to exercise control over the encryption of their data held within the Salesforce platform.

In July 2015, Salesforce launched Salesforce Shield, a set of Salesforce1 Platform services that include Field Audit Trail, Platform Encryption and Event Monitoring with Transaction Security. This enables organizations with compliance or governance requirements, and businesses in regulated industries to build trusted and compliant cloud apps. The key functionality provided by Salesforce Shield includes:

- Platform Encryption –allows customers to natively encrypt data at rest while maintaining application functionality. In addition, customers can manage the lifecycle of their encryption keys while protecting the keys from unauthorized access. It also provides a Bring Your Own Key (BYOK) service with a variety of options for managing tenant secrets for sourcing, generating and managing key material.
- Event Monitoring gives customers visibility into Salesforce apps, so that they can see what data users are accessing, from what IP address, and what actions are being taken regarding that data. It also includes Transaction Security which allows real time enforcement of policies relating to access and consumption of Salesforce services.
- Field Audit Trail gives customers the ability to go back in time and see the state and value of their data on any date, at any time for up to 10 years.

As SaaS services extend the functionality provided by their platforms this could erode the potential customer base for CASB products.

6.9 SkyFormation

SkyFormation offers a solution that provides an “Operations Centric CASB” that delivers cloud visibility and threat detection by leveraging the organization’s existing SIEM/SOC. It claims to exploit existing SIEM/SOC and systems such as DLP, IAM, endpoint management, and threat intelligence to cover cloud services. This allows the detection of threats by delivering security information and detection rules on the organization’s cloud services and shadow IT in their SIEM. It provides connectors for a wide range of SaaS and IaaS cloud services.

7 Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders in that market segment. It is the compass which assists you in identifying the vendors and products/services in a particular market segment which you should consider for product decisions.

It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn’t provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

7.1 Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what we expect from products in that market segment. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains products which lag behind in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even the best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, as well as other sources.

7.2 Product rating

KuppingerCole as an analyst company regularly does evaluations of products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration—integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability—interoperability also can have many meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability —usability refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

[2] http://www.kuppingercole.com/report/cb_apieconomy16122011

7.3 Vendor rating

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position – measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength – even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to become an acquisition target, with massive risks for the execution of the vendor's roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

7.4 Rating scale for products and vendors

For vendors and product feature areas, we use – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

Strong positive Outstanding support for the feature area, e.g. product functionality, or outstanding position of the company, e.g. for financial stability.

Positive Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. for market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., a regional-only presence.

Weak Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

7.5 Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider graph for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the CASB Leadership Compass, we look at the following areas:

Shadow Cloud

Features and functionality provided to discover the use of cloud services from within the organization.

Data Security

The functionality provided by the product to implement data security controls. These include functionality to discover sensitive data that is held in or being moved to a cloud service. Controls may be implemented through detection, warning, quarantining, blocking, encrypting or tokenizing data

Access Control

The functionality provided by the product to control access to cloud services. This may be at a service by service level – giving the ability to prohibit or allow the use of specific cloud services. They may also enable more finely grained access control based on individual user identities, devices or transactions.

Compliance

The functionality provided by the product to support the use of cloud services in a way that is compliant with laws and regulations.

Cyber Security

Feature and functions to help to protect against cyber security risks. For example control over which devices have access to specific cloud services. It may also provide mechanisms to monitor access behaviors to help to identify hijacked accounts and malware.

The spider graphs add an extra level of information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas while being strong in other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on Cloud Access Security Brokers.

7.6 Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Denial of participation: Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.
- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview of vendors not covered and their Cloud Access Security Broker offerings in chapter 6, *Vendors and Market Segments to watch*. In that chapter, we also look at some other interesting offerings around the Cloud Access Security Broker market and in related market segments.

8 Copyright

All conclusions, recommendations, and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaims all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole does not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhemstrasse 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com