KuppingerCole Report

LEADERSHIP COMPASS

by Mike Small |August 2016

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
August 2016

Leadership Compass
Cloud Security Access Brokers
By KuppingerCole

Content

Content Tables

Table of Figures

Related Research Documents

- **Advisory Note: Security Organization, Governance, and the Cloud – 71151**
- **Scenario Report: Understanding Cloud Security – 70321**
- **Advisory Note: Cloud Provider Assurance – 70586**
- **Advisory Note: Selecting your cloud provider – 70742**
- **Leadership Compass: Infrastructure as a Service - 70959**

1 Management Summary

The easy availability of IT services delivered as cloud services together with the revolution in the range of devices that are used to access these services has created challenges for organizations in the areas of security and compliance. 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. To compound the problem, mobile devices can be used to access these services from outside of the organizational perimeter. In order to meet these challenges, a market for products known as Cloud Access Security Brokers (CASBs) has developed.

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 such as Enterprise Network Firewalls, Web Application Firewalls and other forms of web access gateways. They provide a point of control over access to cloud services by any user and from any device.

CASBs are really a workaround that covers the unanticipated threats posed by the rich variety of cloud services available and the way in which organizational users have accepted their use without fully understand the risks that this poses to the enterprise. In an ideal world the controls provided by CASBs would be incorporated into the regular security infrastructure.

CASBs were primarily focused on controlling access to Software as a Service (SaaS) cloud services such as: CRM, ERP, Office Productivity tools and Service Desks. They are evolving into tools to control access to a wider range of cloud services including Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). They typically provide functionality in the following areas:

- **Detect Shadow Cloud** – they help to detect and identify the use of cloud services within an organization as well as who is using these services. This provides the organization with an overall view of the cloud services being used and performs a risk assessment of this use.
- **Access Control** – they provide a way 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.
- **Data Security** – the products provide functionality 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. These controls may be more or less granular.
- **Cyber Security** – the products may control which devices have access to specific cloud services and hence prevent access from unregulated devices. They may also provide mechanisms to monitor access behaviours to help identify hijacked accounts and malware.
- **Compliance** – all of the above functionality together with specific templates and reports can assist organizations to ensure that cloud services are being used in a compliant manner.

1.1 Overall Leadership

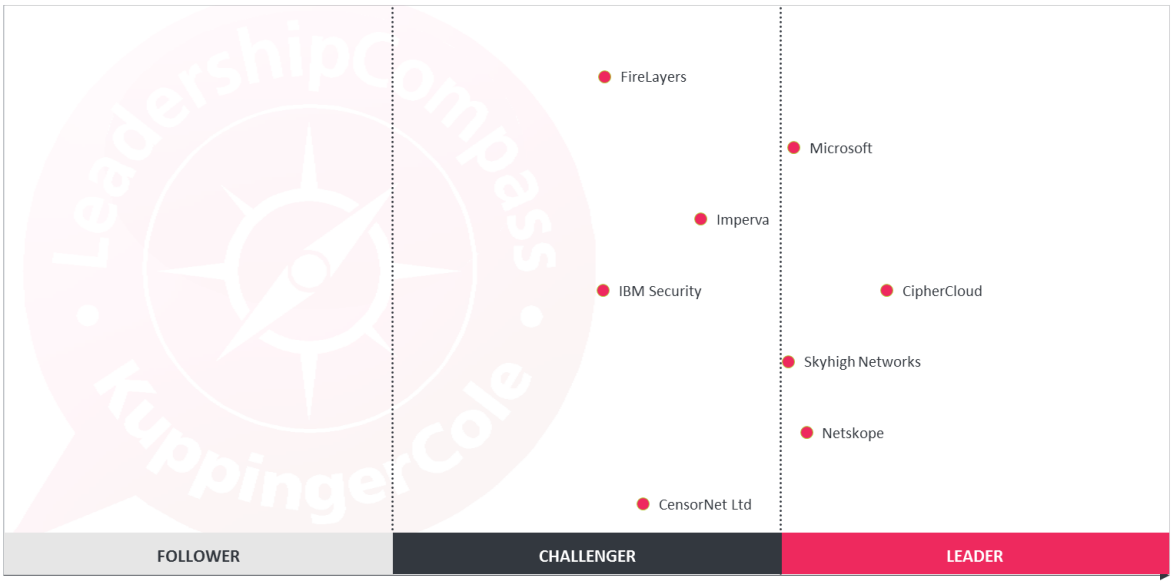


Figure 1: Overall Leaders in the Cloud Access Security Broker segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

In the Overall Leadership rating, we find a number of vendors in the Leaders segment. Of these CipherCloud maintains a clear lead. Close followers are Netskope, Microsoft (following their acquisition of Adallom) and Skyhigh Networks. There are a number of challengers to watch in this expanding market segment.

1.2 Product Leadership

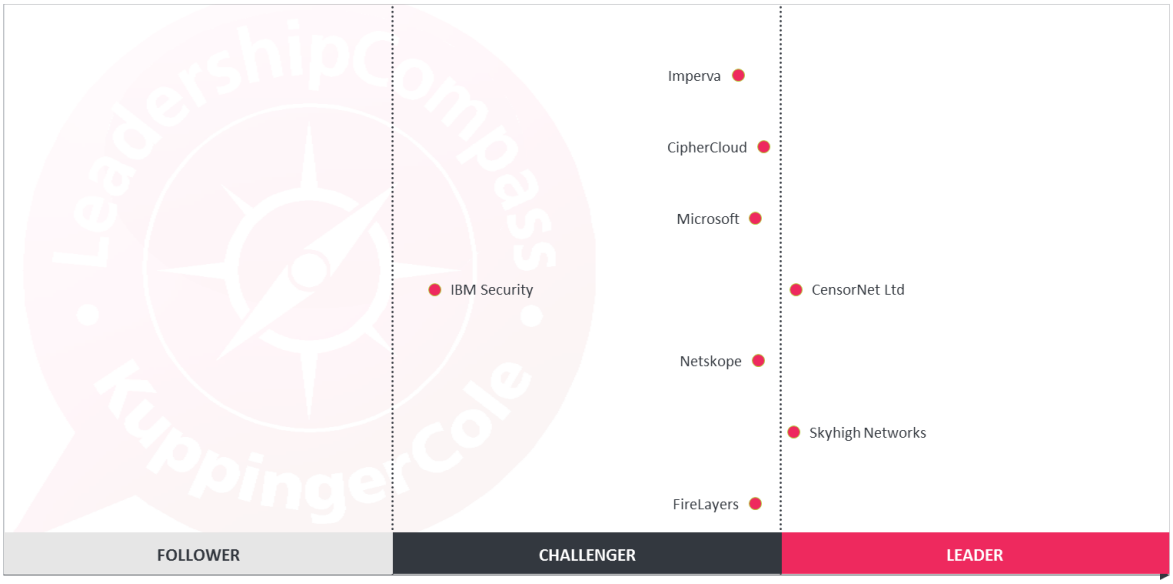


Figure 2: Product Leaders in the Cloud Access Security Broker segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

The Product Leadership rating focuses on the functional strength and overall completeness of vendors' products. This shows a very closely run competition between 3 companies that are in the leader rating and 4 that are challengers. The leaders in this are CensorNet and Skyhigh Networks. Both of these have a CASB product that is complete in that it provides control as well as discovery for a wide range of cloud service and data types. The closeness of the competition shows that the challengers also have very good products.

1.3 Market Leadership

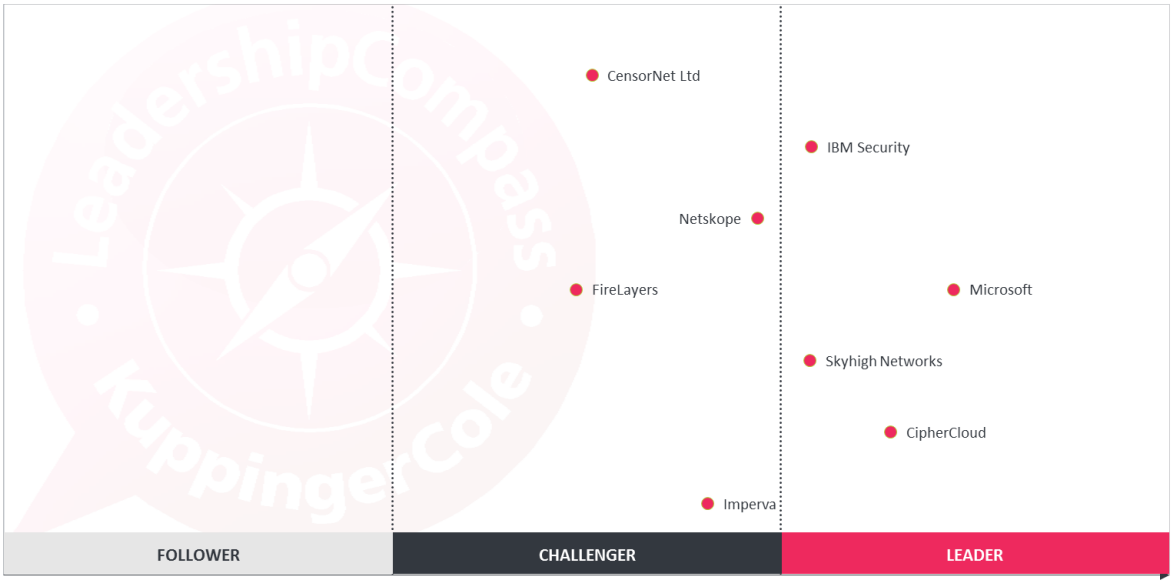


Figure 3: Market Leaders in the Cloud Access Security Broker segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

The Market Leadership rating focuses on the vendors with the go to market capability and existing market presence. In this segment Microsoft, CipherCloud, Skyhigh Network and IBM are the leaders. These vendors have a global presence with large customer bases and extensive partner ecosystems. The positioning of vendors as Leaders, Challengers and Followers simply demonstrates the breadth of the market.

1.4 Innovation

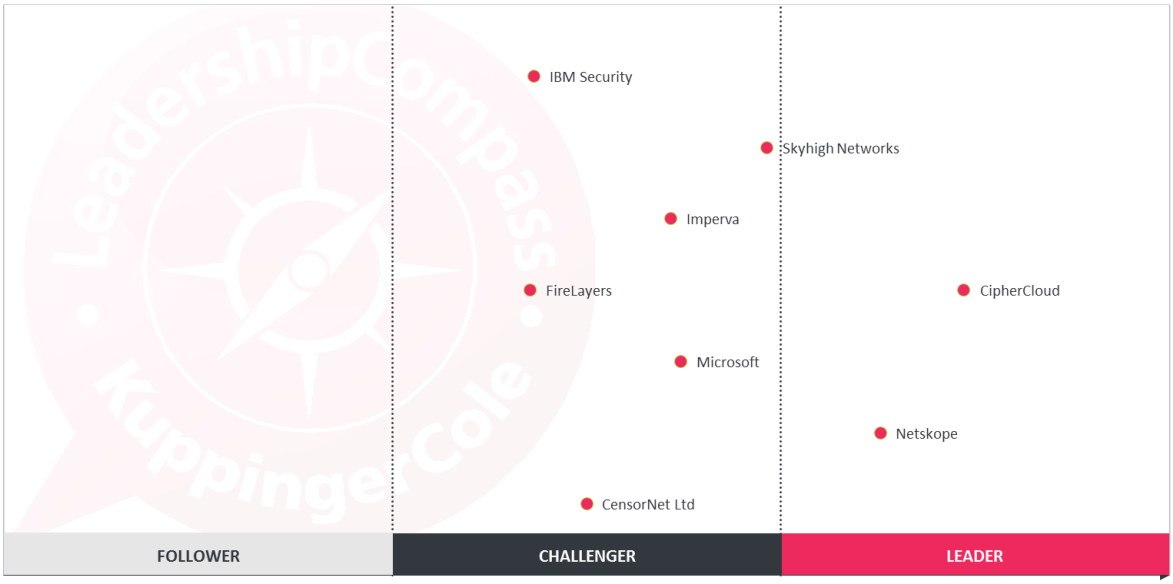


Figure 4: Innovation Leaders in the Cloud Access Security Broker segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

Finally, the Innovation Leadership rating shows CipherCloud and Netskope as the leaders showing the most innovation. However, most vendors are driving innovation forward by adding new features to their products and delivering to a number of the areas we see as relevant to achieving Innovation Leadership.

2 Methodology

KuppingerCole Leadership Compass is a tool that provides a synopsis of a particular IT market segment and identifies the vendors that are Market Leaders in the segment. It is the compass that assists you in identifying the vendors and products in a particular market segment that you should consider when making the best solution decisions for your company.

It is recommended that the information provided in this Leadership Compass be augmented with local analysis. Customers should always define their specific requirements and analyse in greater detail solutions to those needs. Picking a vendor for a specific customer scenario is beyond the scope of this report. This requires a more thorough and comprehensive analysis of customer requirements and will typically require a more detailed mapping of these requirements to product features. KuppingerCole Advisory Services provides customer-specific assessments.

We look at four types of Leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market segment. These products to a large extent deliver 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 new ideas, devices, or methods in the particular market segment. They provide several of the most innovative and upcoming features we hope to see in the particular 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 best choice for specific use cases and customer requirements but are of limited value in other situations.

In addition, we have defined a series of tables which

- **Compare,** for instance, the rating for innovation with the one for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path from established vendors, but also established vendors which no longer lead in innovation. These tables provide additional viewpoints on the vendors and should be considered when picking vendors for RFIs (Request for Information), long lists, etc. in the vendor/product selection process.
- **Add additional views** by comparing the product rating to other feature areas. This is important because not all customers need the same product, depending on their current situation and specific requirements. Based on these additional matrices, customers can evaluate which vendor fits best to their current needs but also is promising regarding its overall capabilities. The latter is important given that a product not only should address a pressing challenge but become a sustainable solution. It is a question of helping now, but also of being good enough for the next steps and future requirements. Here these additional matrices come into play.

Thus, the KuppingerCole Leadership Compass provides a multi-dimensional view of vendors and their products.

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

3 Product Rating

KuppingerCole as an analyst company regularly performs evaluations of products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products/services 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/services:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – the security measure indicates the degree of security features incorporated within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (**Scenario: Understanding Identity and Access Management - 70129**). It provides a mature approach to security assessment and a model for product security; a key requirement for evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization are identified as weaknesses in security. Security vulnerabilities to known hacks are also rated as weaknesses. The security rating is based on the severity of such weaknesses and the way in which the product vendor accommodates them.

Functionality – this is measured in relation to three factors:

- vendor promises
- status of the industry
- expected functionality.

In mature market segments, the status of the industry and KuppingerCole expectations 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 the market segment. When vendors fail to meet customer's expectations in a market segment, lower ratings will result, unless a product provides additional features, or uses another approach, that provides additional customer benefits.

Integration — integration is measured by the degree to which a vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent in which products interoperate. The level of integration a product exhibits is uncovered by analysing the configuration effort required to deploy, operate and manage the product. The degree of integration is then directly related to this effort. For example: if each product maintains its own identity record for each user, it is not well integrated; if products use multiple databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single account allows the administrator to manage all aspects of the product suite, then a better level of integration has been achieved.

Interoperability — interoperability refers 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 equipped their products or technologies to work with other products or standards that are important in the market segment. Extensibility is a component of this and measured by the degree to which a vendor allows its technologies and products to be extended for wider use by its customers. Extensibility is given equal status to interoperability 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; the future is one in which programmatic access through a well-documented and secure set of APIs is expected (refer to the Open API Economy Document **(#70352 Advisory Note: The Open API Economy**) for more information).

Usability — accessibility refers to the degree to which the vendor enables accessibility to its technologies and products by various user groups. Typically, at least two aspects of usability must be addressed – the end user view and the administrator view. While good documentation is the basis for adequate accessibility, we have strong expectations regarding well integrated user interfaces and a high degree of consistency across user interfaces, particularly across different products from a single vendor. We also expect vendors to follow common, established approaches to user interface design rather than creating their own UI conventions.

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

- **People Participation**—Human participation in systems at any level is the highest area of cost and causal factor of failure for any IT endeavour.
- **Level 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.
- **Level of Identity and Security Exposure to Failure**—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increase costs, but inevitably lead to increased manual intervention with its attendant mistakes and decreased customer satisfaction with breakdowns in their business processes. It also creates openings for malicious attacks and system failure.

When KuppingerCole evaluates a set of technologies or products from a vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided is of utmost importance because the lack of excellence in any or all of these areas will inevitably lead to identity and security shortcomings and poor infrastructure.

4 Vendor Rating

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

- Level of Innovation
- Market position
- Financial strength
- Ecosystem

Level of Innovation – this is measured as the capability to drive innovation in a direction which aligns with the direction of the particular market segment in question. Innovation has no value in 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 where applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus active participation in standardization initiatives adds to the positive rating of innovativeness. Innovativeness, despite being part of the vendor rating, looks at the innovativeness in the particular market segment analysed in this KuppingerCole Leadership Compass.

Market position – measures the position of the vendor in the market or in 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 takes into account the vendor's presence in major markets. Again, while being part of the vendor rating, market position evaluates the vendor's position in the particular market segment analysed in this KuppingerCole Leadership Compass. Note: a very large vendor might not be a Market Leader in the particular market segment in question, but may enjoy a higher overall market position.

Financial strength – KuppingerCole doesn't consider size to be of value by itself but financial strength is an important factor for customers when selecting a solution. In general, publicly available financial information is an important factor for this rating. Companies which are venture-financed are rated lower because they are more likely to become an acquisition target, with potential risk for customers adopting their product as a solution.

Ecosystem – this dimension looks at the ecosystem of the vendor for the market segment covered in this Leadership Compass document. It focuses on the partner base of a vendor and the approach they have taken in acting as a "good citizen" in heterogeneous IT environments.

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.

5 Vendor Coverage

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

However, there might be vendors which don't appear in this document for various reasons:

- **Limited market visibility**: There might be vendors and products/services 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 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 report will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only a small overlap with the market segment we are analysing. In these cases, we might decide not to include the product in that KuppingerCole report.

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

For this KuppingerCole Leadership Compass, we observed broad participation. However, some vendors with niche offerings refrained from appearing in the Leadership graphics and opted for being only mentioned in chapter 14, which also covers a number of vendors we do not yet see as full contenders in this market segment. Notably, chapter 14 lists a number of vendors that can be ideal choices for certain requirements, even while they may not provide the full functionality of a CASB.

6 Market Segment

There are a number of challenges around the security and compliant use of cloud services and there are a variety of types of solutions on the market that address different aspects of these. The fundamental functionalities that these solutions provide are:

1. Discovery of what cloud services are being used, by whom and for what data.
2. Control over who can use which services and what data can be transferred.
3. Protection of data in the cloud against unauthorized access and leakage.

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

- Storage encryption – that provide whole disk, volume or file level encryption of data.
- 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.
- Access gateways – that discover what cloud services are being accessed and provide protection of data at a transaction level.
- Access Brokers – that provide granular access over who can access cloud services and the functions that they can perform.

	Discovery	Control	Protection
Storage Encryption	None	Over access by application to volume or file	Against leakage of data if volume, media, file or backup is compromised
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
Cloud Access Gateway	Of cloud services being accessed	Over which services can be accessed	Some provide encryption / tokenization of transaction data
Cloud Access 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

This document focusses on Cloud Access Brokers – however many of these products also contain other functions. This additional functionality is illustrated in the spider chart for each product covered.

7 Specific Features Analysed

When evaluating the products, there are a number of specific elements we look at besides looking at the more general aspects of:

- Overall functionality
- Size of the company
- Number of customers
- Number of developers
- Partner ecosystem
- Licensing models
- Platform support

7.1 Shadow Cloud

Here we consider how the product helps an organization to discover and control the use of cloud services from within 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;
- The functionality provided to control access to cloud services.

7.2 Data Security

Specifically, we look at 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. These controls may be more or less granular, 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;
- Kinds of encryption used and how keys are managed.

7.3 Access Control

This is 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. 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.

7.4 Compliance

In this area we consider the functionality provided by the product to support the use of cloud services by the organization in 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.

7.5 Cyber Security

This area covers how the products helps the organization to protect against cyber security risks. The products may control which devices have access to specific cloud services and hence prevent access from unregulated devices. They may also provide mechanisms to monitor access behaviours to help to identify hijacked accounts and malware. In particular, 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;
- Reporting and integration with security intelligence systems.

7.6 Other Unique Selling Propositions

The support for these functions is added to our evaluation of the products. We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products that distinguish them from other offerings available in the market.

8 Market Leaders

Based on our evaluation we have identified several Leaders in the Cloud Access Security Broker market segment. The Market Leaders are shown in the figure below.

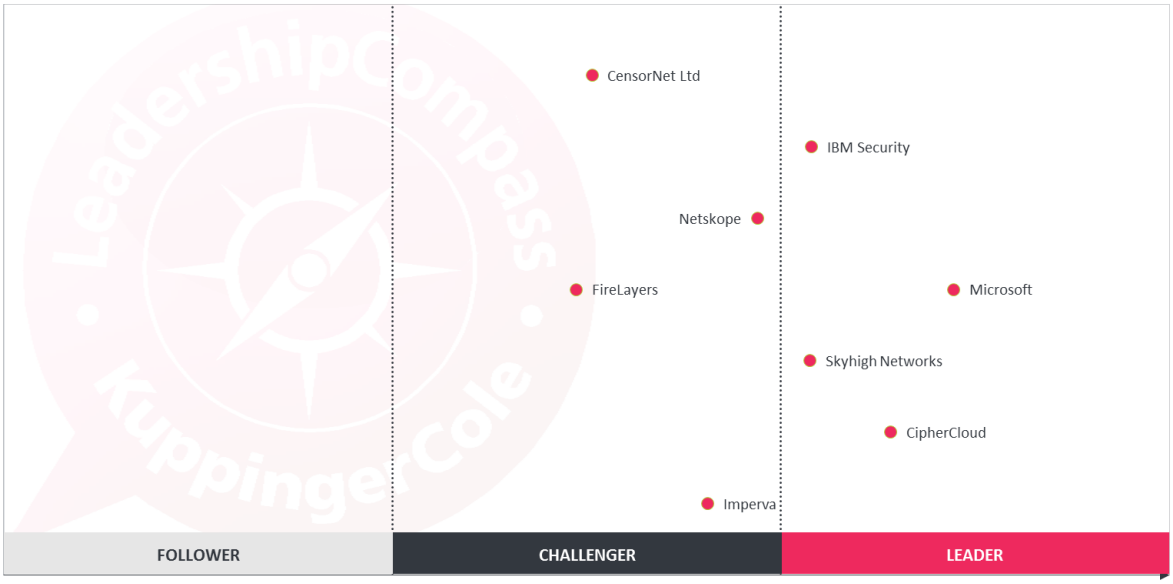


Figure 5: Market Leaders in the Cloud Access Security Broker segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.]

We expect Market Leaders to be Leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other major regions are not considered market Leaders. The same holds true for the vendor's partner ecosystem – without a global scale in the partner ecosystem, we don't rate a vendor as a Market Leader.

Market Leaders (in alphabetical order):

- CipherCloud
- IBM Security
- Microsoft
- Skyhigh Networks

9 Product Leaders

The second view we provide is about Product Leadership. This view is mainly based on the analysis of product features and the overall capabilities of the various products.

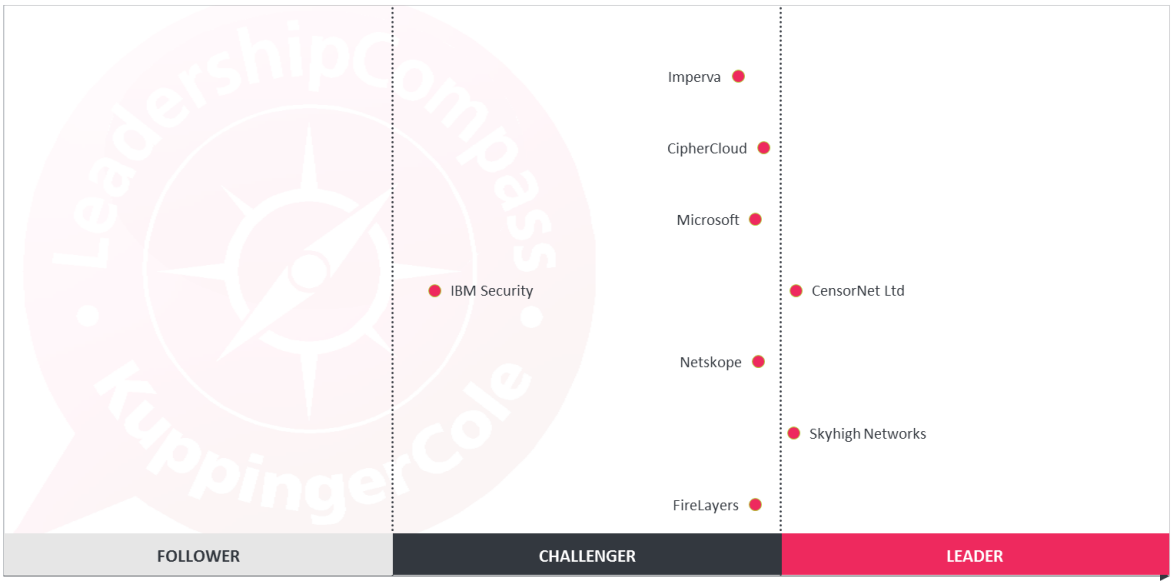


Figure 6: Product Leaders in the Cloud Access Security Broker segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.]

The Product Leadership rating focuses on the functional strength and overall completeness of vendors' products. This rating shows a number of vendors with very similar ratings which indicates very strong competition in an evolving market.

Again, when selecting a product, it is important to look at the specific features and map them to the customer requirements. There are examples where products which are not "feature Leaders" are nevertheless a better fit for specific customer scenarios.

Product Leaders (in alphabetical order):

- CensorNet Ltd
- Skyhigh Networks

10 Innovation Leaders

The third view we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what is required from vendors to continue to provide new functionality to meet their customers' needs. Hence an analysis of a vendor's record of innovation is often as important as the current features of their product/service.

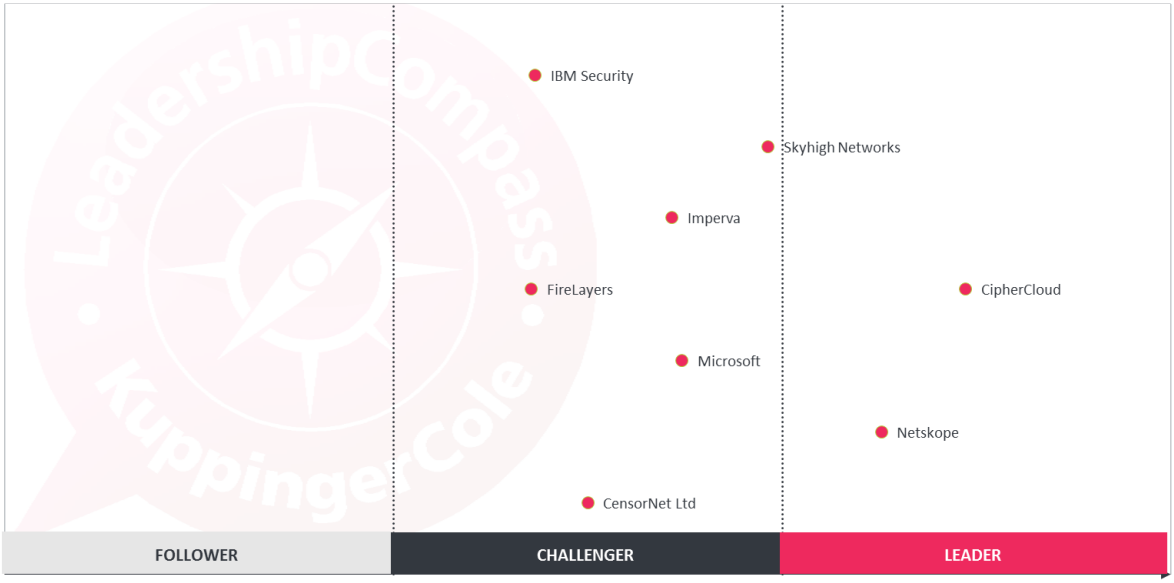


Figure 7: Innovation Leaders in the Cloud Access Security Broker segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.]

Finally, the Innovation Leadership rating shows that most vendors are driving forward innovation by adding new features to their products and delivering to a number of the areas we see as relevant to achieving Innovation Leadership.

Picking solutions always requires a thorough analysis of customer requirements and a comparison with product features. Leadership in a particular rating may not always mean that a product is the best fit for a particular customer and his/her requirements. However, what this Leadership Compass does is help identify those vendors that customers should look at more closely.

Innovation Leaders (in alphabetical order):

- CipherCloud
- Netskope

11 Product Evaluation

This section contains a quick rating for every product we've included in this report. For some of the products there are additional KuppingerCole Reports available, providing more detailed information.

In the following analysis we have provided our ratings for the products and vendors in a series of tables. These ratings represent the aspects described previously in this document. Here is an explanation of the ratings that we have used:

- **Strong Positive:** this rating indicates that, according to our analysis, the product or vendor significantly exceeds the average for the market and our expectations for that aspect.
- **Positive:** this rating indicates that, according to our analysis, the product or vendor exceeds the average for the market and our expectations for that aspect.
- **Neutral:** this rating indicates that, according to our analysis, the product or vendor is average for the market and our expectations for that aspect.
- **Weak:** this rating indicates that, according to our analysis, the product or vendor is less than the average for the market and our expectations in that aspect.
- **Critical:** this is a special rating with a meaning that is explained where it is used. For example, it may mean that there is a lack of information. Where this rating is given it is important that a customer considering this product look for more information about the aspect.

It is important to note that these ratings are not absolute. They are relative to the market and our expectations. Therefore, a product with a strong positive rating could still be lacking in functionality that a customer may need if the market in general is weak in that area. Equally, in a strong market a product with a weak rating may provide all the functionality a particular customer would need.

Each vendor evaluation also includes a spider chart showing our assessment of the performance of the product evaluated against the 5 aspects described in chapter 7.

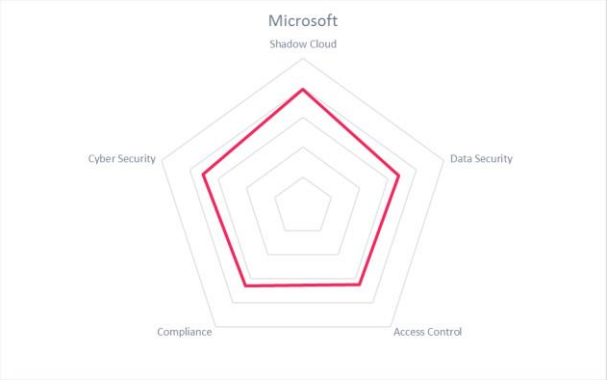
These are:

- Shadow Cloud
- Data Security
- Access Control
- Compliance
- Cyber Security

11.1 Microsoft

In September 2015 Microsoft completed its acquisition of Adallom and their Cloud Access Security Broker. This has now been fully integrated with Microsoft Azure and is offered as Microsoft Cloud App Security.

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



The key features provided by this solution are:

- Discover – It enables the organization to uncover Shadow IT by discovering apps, activities, users, data and files in their cloud environment as well as third-party apps that are connected to their cloud.
- Investigate - using cloud forensics tools to identify risky apps, specific users and files in the organizational network as well as finding patterns in the data collected from the organizational cloud and generating reports to monitor cloud usage.
- Control - Mitigate risk by setting policies and alerts in order to achieve maximum control over network cloud traffic. Cloud App Security can help to migrate the organizational users too safe, sanctioned cloud app alternatives.
- Protect – it exploits behavioural analytics and anomaly detection for threat protection. It enables the organization to sanction/prohibit applications, enforce data loss prevention (DLP), control permissions and sharing, and generate custom reports and alerts.

Microsoft Cloud App Security is based on a mature product from Adallom with proven capabilities and customers. It exploits the skills of the Microsoft team and the vast amount of threat intelligence collected by Microsoft to catalogue and rank the risks of the large number of cloud apps available. It enables the user organization to customize usage based on these scores. It provides control over users' access to cloud apps and the movement of data to the cloud. It integrates with other Microsoft tools to enable encryption of sensitive data and information rights management.

Strengths/Opportunities	Weaknesses/Threats
• Mature product with proven capabilities and customer usage. • Enables a risk based approach based on multiple factors including anomaly detection. • Deep integration with Microsoft Office 365 products. • Exploits cloud services API to extend range of monitoring and control. • Wide range of cloud services covered out of the box.	• Does not provide encryption/tokenization of structured data held in cloud applications such as CRM applications.

12 Products at a Glance

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

12.1 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 the table below:

Service	Security	Functionality	Integration	Interoperability	Usability
CensorNet Ltd	Positive	Positive	Strong Positive	Positive	Strong Positive
CipherCloud	Strong Positive	Positive	Strong Positive	Positive	Positive
FireLayers	Strong Positive	Neutral	Strong Positive	Positive	Strong Positive
IBM Security	Positive	Neutral	Strong Positive	Neutral	Neutral
Imperva	Positive	Positive	Strong Positive	Neutral	Strong Positive
Microsoft	Positive	Positive	Strong Positive	Positive	Strong Positive
Netskope	Strong Positive	Positive	Positive	Positive	Strong Positive
Skyhigh Networks	Strong Positive	Positive	Strong Positive	Positive	Positive

Table 1 Comparative overview of the ratings for the product capabilities

In addition, we also provide four additional ratings for the vendor. These go 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.

Company	Innovation	Market Position	Financial Strength	Ecosystem
CensorNet Ltd	Neutral	Neutral	Neutral	Positive
CipherCloud	Strong Positive	Strong Positive	Neutral	Positive
FireLayers	Neutral	Neutral	Neutral	Neutral
IBM Security	Neutral	Weak	Strong Positive	Strong Positive
Imperva	Positive	Neutral	Positive	Positive
Microsoft	Positive	Neutral	Strong Positive	Strong Positive
Netskope	Strong Positive	Positive	Neutral	Positive
Skyhigh Networks	Positive	Positive	Neutral	Positive

Table 2 Comparative overview of the ratings for the vendors

In the area of Innovation, we were looking for the service to provide a range of advanced features in our analysis. These advanced features include but are not limited to areas such as: performance guarantees, specific security features such as enhanced support for encryption, as well as a track record of introducing new functionality in response to market demand. Where we could find no such features we rate it as "Critical".

In the area of market position, we are looking at the visibility of the vendor in the market. This is indicated by factors including the presence of the vendor in more than one continent and the number of organizations using the services. Where the service is only being used by a small number of customers located in one geographical area we award a "Critical" rating.

In the area of Financial Strength, a "Weak" or "Critical" rating is given where there is a lack of information about financial strength. This doesn't imply that the vendor is in a weak or a critical financial situation. This is not intended to be an in depth financial analysis of the vendor; and it is also possible that vendors with better ratings might fail and disappear from the market. In the case of a cloud service provider financial failure or withdrawal from the market could create a major problem for a business that depended upon that provider for its business critical IT services.

Finally, a critical rating regarding Ecosystem applies to vendors which do not have, or have a very limited ecosystem with respect to numbers of partners and their regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that the success and growth of companies in a market segment relies on strong partnerships.

12.2 The Market/Product Matrix

Furthermore, we've compared the position of vendors regarding combinations of our three major areas of analysis, i.e. Market Leadership, Product Leadership, and Innovation Leadership. This analysis provides additional information.

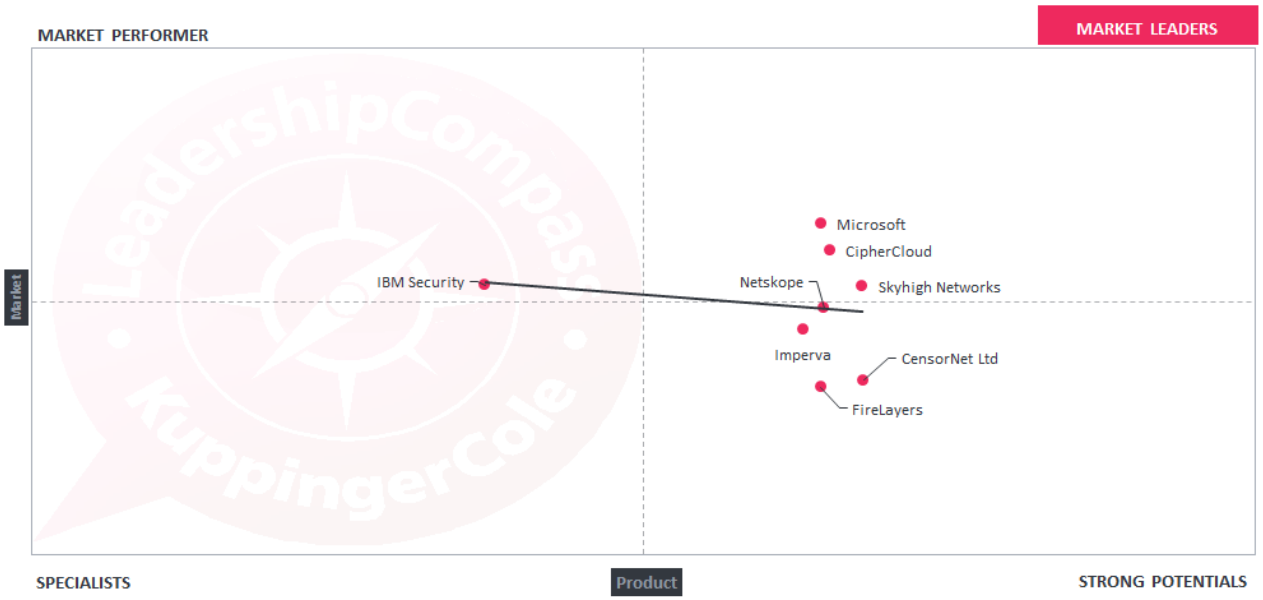


Figure 8: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "over-performers" when comparing Market Leadership and Product Leadership.

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 "over-performing" 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.

We've defined four segments of vendors to help in classifying them:

Market Leaders: This segment contains vendors which have a strong position in our categories of Product Leadership and Market Leadership. These vendors have an overall strong to excellent position in the market.

Strong Potentials: This segment includes vendors which have strong products, being ranked high in our Product Leadership evaluation. However, their market position is not as good. That might be because of various reasons, like a regional focus by the vendors or the fact that they are niche vendors in that particular market segment.

Market Performers: Here we find vendors which have a stronger position in Market Leadership than in Product Leadership. Typically, such vendors have a strong, established customer base due to other market segments they are active in.

Specialists: In this segment we typically find specialized vendors which have – in most cases – specific strengths but neither provide full coverage of all features which are common in the particular market segment nor count among the software vendors with overall very large portfolios.

In the Market Leaders segment, we see several companies lead by Cipher Cloud, Microsoft and Skyhigh Networks. These are the ones that have both strong product features and a significant market presence. CensorNet, FireLayers, Imperva and Netskope have strong potential. IBM has the ability to perform in this market but is a late entrant with a product that is still evolving.

12.3 The Product/Innovation Matrix

This 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 is typical an emerging market.

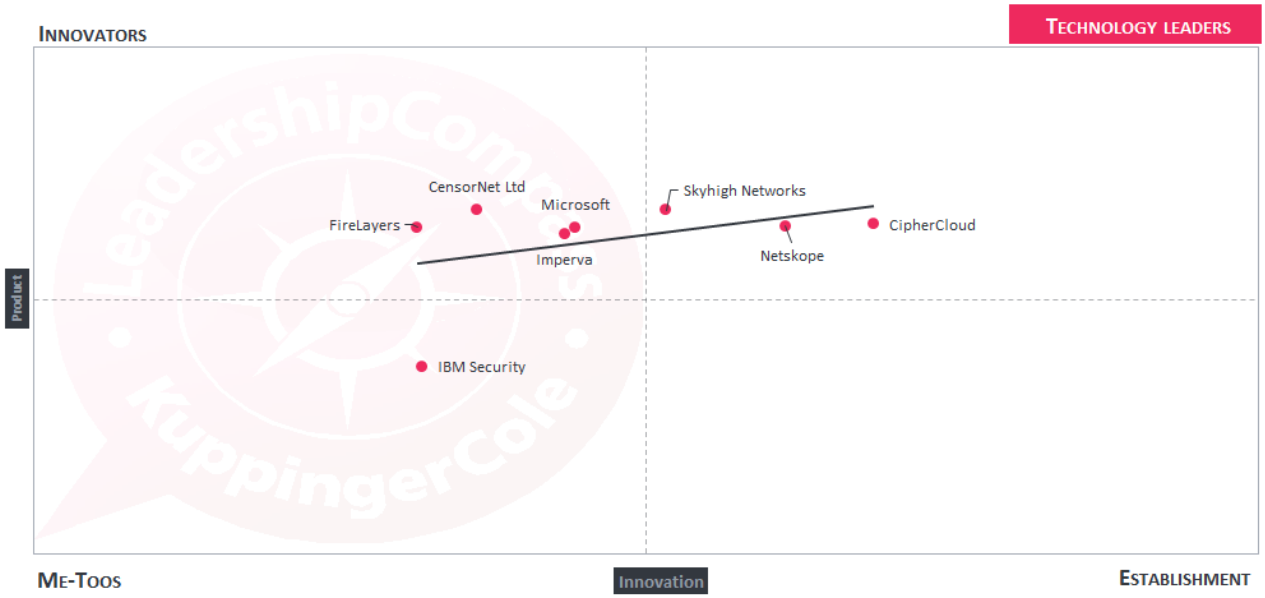


Figure 9: The Product/Innovation Matrix. Vendors below the line are less innovative, vendors above the line are, compared to the current Product Leadership positioning, more innovative.

Again we've defined four segments of vendors. These are

Technology Leaders: This group contains vendors which have technologies which are strong regarding their existing functionality and which show a good degree of innovation.

Establishment: In this segment we typically find vendors which have a relatively good position in the market but don't perform as strong when it comes to innovation. However, there are exceptions if vendors take a different path and focus on innovations which are not common in the market and thus do not count that strong for the Innovation Leadership rating.

Innovators: Here we find highly innovative vendors with a limited visibility in the market. It is always worth having a look at this segment because vendors therein might be a fit especially for specific customer requirements.

Me-toos: This segment mainly contains those vendors which are following the market. There are exceptions in the case of vendors which take a fundamentally different approach to provide specialized point solutions. However, in most cases this is more about delivering what others have already created.

Again we see a good percentage of vendors in the upper right segment of the matrix, which we define as the Technology Leaders segment. These vendors show good to excellent innovation and provide strong product capabilities.

This is a relatively new market segment and so there are no "Establishment" vendors. The Technology Leaders include CipherCloud, Netskope and Skyhigh Networks. The Innovators are CensorNet Ltd, FireLayers, Imperva and Microsoft. IBM is in the "Me-Too" section having only recently entered the market.

12.4 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 for 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.

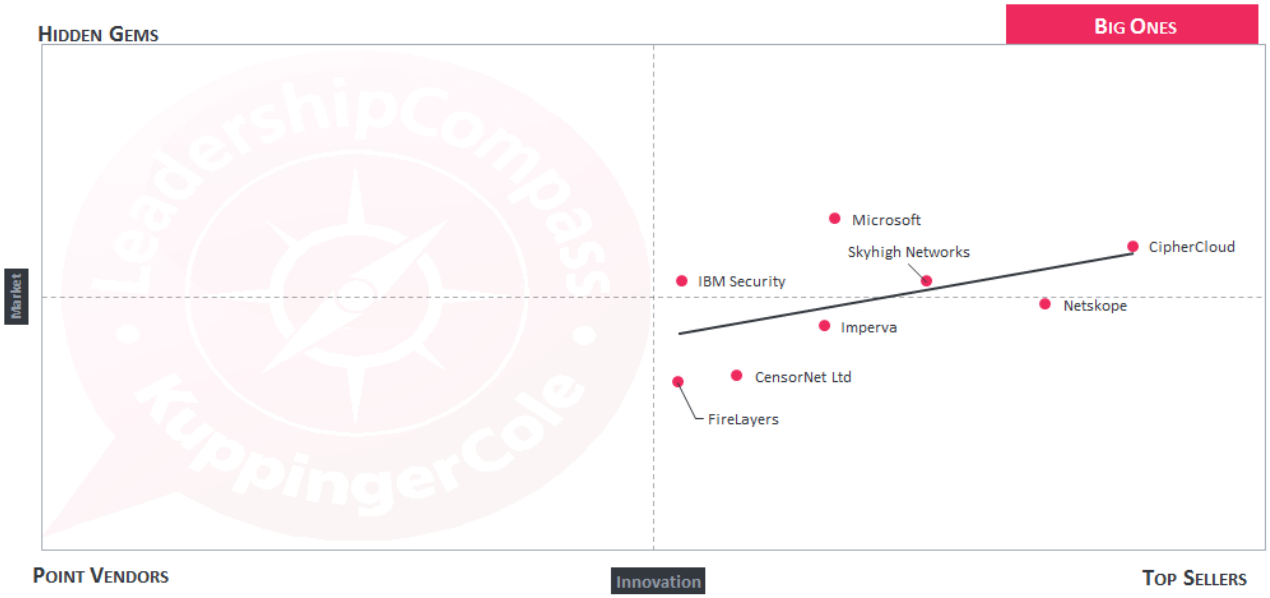


Figure 10: The Innovation/Market Matrix. Vendors below the line are performing well in the market compared to their relative weak position in the Innovation Leadership rating, while vendors above the line show based on their ability to innovate, the biggest potential to improve their market position

The four segments we have defined here are

Big Ones: These are market leading vendors with a good to strong position in Innovation Leadership. This segment mainly includes large software vendors.

Top Sellers: In this segment we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of "customer customers", i.e. a loyal and powerful group of contacts in the customer organizations.

Hidden Gems: Here we find vendors which are more innovative than would be expected given their Market Leadership rating. These vendors have a strong potential for growth, however they also might fail in delivering on that potential. Nevertheless, this group is always worth a look due to their specific position in the market.

Point Vendors: In this segment we find vendors which typically either have point solutions or which are targeting specific groups of customers like SMBs with solutions focused on these, but not necessarily covering all requirements of all types of customers and thus not being among the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

The vendors in the Big Ones section include CipherCloud, IBM, Microsoft, and Skyhigh Networks. Although IBM is a late entrant in the market expect strong performance in the future. The other vendors in this analysis are all place in the “Top Sellers” segment having an excellent market position for their products.

There are no “Hidden Gems” or “Point Vendors” amongst the vendors analysed.

13 Overall Leadership

Finally, we've put together the three different ratings for Leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in figure 11.

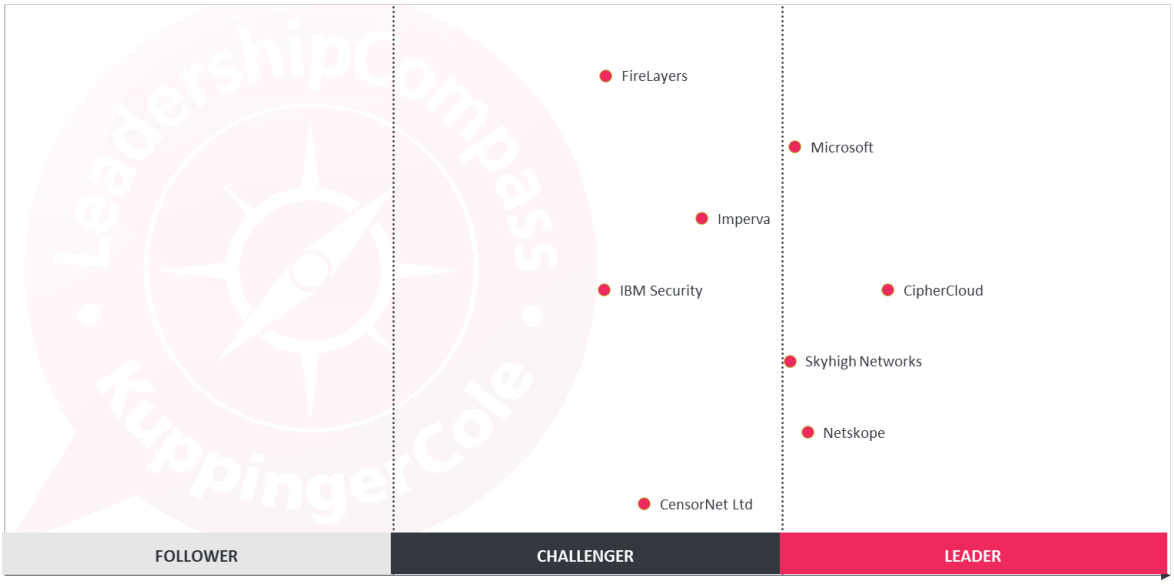


Figure 11: The Overall Leadership rating for the Cloud Access Security Broker segment

In the Overall Leadership rating, we find three vendors in the Leaders segment. Of these, CipherCloud maintains a clear lead challenged by Microsoft (particularly after their recent acquisition of Adallom) and Skyhigh Networks.

Overall Leaders are (in alphabetical order):

- CipherCloud
- Microsoft
- Netskope
- Skyhigh Networks

14 Vendors and Market Segments to Watch

This is an emerging market segment with a high growth and consolidation with smaller product vendors being acquired by the larger ones. This is likely to continue. As customers adopt cloud services and move to a hybrid cloud they will require the functionality needed to monitor and control access as well as to protect data in a common way across their increasingly heterogeneous environment. Some of the functionality provided by the current products will be absorbed into the cloud services themselves. Tools providing the required functionality in a common way irrespective of how the service is delivered will emerge. This will be important to reduce the cost to the end customer as well as to increase the effectiveness.

Besides the vendors covered in this KuppingerCole Leadership Compass on Cloud Access Security Brokers, 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. This includes the following vendors:

14.1 Bitglass

Bitglass is a US company that was founded in 2013. Its cloud access security broker (CASB) solution is designed to protect cloud data from the cloud down to the device. Its CASB solution is based on three technologies:

- Citadel DLP engine that functions bi-directionally and can sync policies with an existing DLP system as well as providing a library of prebuilt policies.
- Omni Multiprotocol Proxies and Access Control that enables access control and data protection across a wide range of devices.
- Harbor Cloud Encryption that provides 256-bit AES encryption for data stored in cloud apps.

14.2 Symantec, Blue Coat, Perspecsys and Elastica

Symantec is a global security company that provides products and services to help companies, governments and individuals secure their data wherever it lives. In June 2016 Symantec announced the intention to acquire Bleu Coat and this acquisition was completed on August 1st, 2106. Thorough this acquisition, Symantec now has the cloud data protection products that were acquired and developed by Blue Coat. This can be seen as part of the pattern mentioned above and makes Symantec an important player in this market segment.

Blue Coat is a provider of web security solutions for global enterprises and governments. Their mission is to protect enterprises and their users from cyber threats – whether they are on the network, on the web, in the cloud or mobile.

In July 2015 Blue Coat acquired[1] Perspecsys. The Perspecsys Cloud Data Protection platform solves the business risks associated with data compliance, privacy and security for enterprises as they move to adopt cloud-based applications. Through the use of its patented cloud data tokenization and encryption capabilities, Perspecsys puts enterprises in control of their data, regardless of where the data resides.

In November 2015 Blue Coat acquired[2] the US company Elastica. Elastica's CloudSOC™ provides capabilities such as threat scoring powered by machine learning, user and end-point behavior modeling, natural language-based cloud DLP, and analysis with remediation in a cloud application SOC. Elastica delivers these capabilities via its CASB gateway and API controls for cloud application security management and enforcement.

14.3 CloudLock and Cisco

CloudLock is a US company launched in 2011 with a focus on transforming cloud security into a business enabler. The CloudLock Cloud Access Security Broker harnesses crowd-sourced, cybersecurity intelligence to enable enterprises to securely leverage the cloud. It is able to secure SaaS, IaaS, PaaS, and IDaaS environments. On June 28th, 2016 Cisco announced[3] its intention to buy CloudLock.

14.4 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 NextLab's products are based around the XACML standard and provides 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.

14.5 Palerra

Palerra is a US company. Palerra LORIC™ is a CASB that combines threat detection, predictive analytics, security configuration management and automated incident response and remediation in a single solution. It covers branded applications such as Microsoft Office 365 as well as infrastructure like AWS. LORIC does not require hardware, software or agents and is not deployed in-line with cloud services. LORIC is delivered as a service.

[1] https://www.bluecoat.com/company/press-releases/blue-coat-acquires-perspecsys-effectively-make-public-cloud-applications
[2] https://www.bluecoat.com/company/press-releases/blue-coat-acquires-elastica
[3] https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1775941

14.6 Palo Alto Networks

In September 2015 Palo Alto Networks launched its own CASB offering called Aperture. Aperture builds upon the existing SaaS visibility and granular control capabilities of the Palo Alto Networks® Next-Generation Security Platform provided through App-ID™. Adding visibility and control within SaaS applications with Aperture provides a full end-to-end security solution without any additional software, hardware or network changes required.

14.7 SkyFormation

The SkyFormation solution allows the organizations Security Operation Center (SOC) to monitor security activities and threats across Cloud-based (e.g. Salesforce, Office365, Box) and non-Cloud-based (e.g. home-grown) applications, by acting as a broker between the applications and the existing SOC system tools (e.g. SIEM, Splunk). This provides a solution to leverage the existing investments in cyber-security SOC to monitor both Cloud-based and non-Cloud-based applications with the same consistent methodology and approach.

14.8 Vaultive

Vaultive provides a stateless network-layer software encryption proxy. Vaultive's Cloud Data Encryption Platform can support a wide range of cloud-based and on-premise applications. In particular, the Vaultive Cloud Data Protection Platform provides Office 365 security and is capable of encrypting Microsoft Exchange Online data in the cloud without changing the users' experience.

15 Copyright

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**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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