KuppingerCole Report

MARKET COMPASS

By Mike Small

September 23, 2020

Cloud Access Security Brokers

The KuppingerCole Market Compass provides an overview of the product or service offerings in a certain market segment. This Market Compass covers CASB (Cloud Access Security Broker) solutions that help to secure the organizational use of cloud services.

By **Mike Small**
sm@kuppingercole.com

Content

1 Management Summary 4

2 Market Segment 6

2.1 Market Description 6

2.2 Market Direction 8

2.3 Capabilities 11

2.3.1 Basic Functionality 11

2.3.2 Discovery of Cloud Use 13

2.3.3 Cloud Service Access Control 14

2.3.4 Cloud Data Protection 15

2.3.5 Compliance 17

2.3.6 Posture Management 18

3 Vendors & Products 20

3.1 Vendors Covered 20

3.2 Vendors to Watch 21

4 Ratings at a Glance 23

4.1 Featured Vendors 25

4.1.1 Featured for Innovation: Bitglass 25

4.1.2 Featured for Access Governance: Forcepoint 26

4.1.3 Featured for Integration: Censornet 27

4.1.4 Featured for Integrated Data Security – CipherCloud 28

4.1.5 Featured for Custom Apps – McAfee 29

5 Product/Service Details 31

5.1 Bitglass 32

5.2 Censornet 35

5.3 CipherCloud 38

5.4 Cisco 41

5.5 Forcepoint 44

5.6 Fortinet 47

5.7 McAfee 50
5.8 Microsoft 53
5.9 Netskope 56
5.10 Oracle 59
5.11 Palo Alto Networks 62
5.12 Proofpoint 65
5.13 Symantec 68
6 Related Research 71
Endnotes 72
Methodology 73
Content of Figures 76
Copyright 77

1 Management Summary

The KuppingerCole Market Compass provides an overview of a market segment and the vendors in that segment. It covers the trends that are influencing that market segment, how it is further divided, and the essential capabilities required of solutions. It also provides ratings of how well these solutions meet our expectations.

This Market Compass covers CASBs (Cloud Access Security Brokers) that address the challenges of security and compliance around the use of cloud services.

Most organizations are now using business applications delivered through cloud services as well as on-premises and hosted IT services. This hybrid IT delivery environment has given rise to many challenges in the areas of management, security, and compliance. These challenges often arise because the use of cloud services is not well integrated into the normal IT security and access governance processes and technologies found within organizations. In addition, the use of cloud services creates other risks.

Employees and associates can use 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 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.

CASBs provide security controls that are not available through other security devices to provide a point of control over access to cloud services by any user and from any device. CASB solutions have evolved from the early products that focussed on the discovery of cloud usage, through network access control points to become integrated cloud security solutions.

The major IT and network security vendors all now offer CASBs that are deeply integrated with other end user security controls such as anti-malware, DLP (Data Leak Prevention). They also increasingly offer risk / compliance status reporting under the heading of CSPM (Cloud Security Posture Management). CASBs have traditionally focussed on controlling user access to SaaS services and the protection of unstructured data. However, the increasing use of IaaS to deliver custom business applications exposes new vulnerabilities that bring new risks, and CSPM is intended to help to manage these.

In our opinion, the market for a standalone CASB is shrinking and organizations are now looking for CASB as part of a complete cloud security solution. These are expected to include CASB, CSPM, Data and User Protection as well as Zero Trust Network Controls. In our opinion, this market will expand to embrace the hybrid IT delivery model that is now common as well as the security challenges from the growth in edge computing and 5G.

2 Market Segment

This Market Compass covers 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 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.

2.1 Market Description

There are many challenges around the secure and compliant use of cloud services and there are several types of solutions on the market that address different aspects of these. This report focusses on CASB (Cloud Access Security Brokers).

The fundamental functionalities that these solutions provide are:

- Discovery of the cloud services being used, by whom and for what data.
- Control over who can use which services and what data can be transferred or accessed.
- Protection of data in the cloud against unauthorized access and leakage.
- The capabilities to enforce and demonstrate compliance with regulations.

This latter functionality has evolved into what is being termed CSPM (Cloud Security Posture Management).

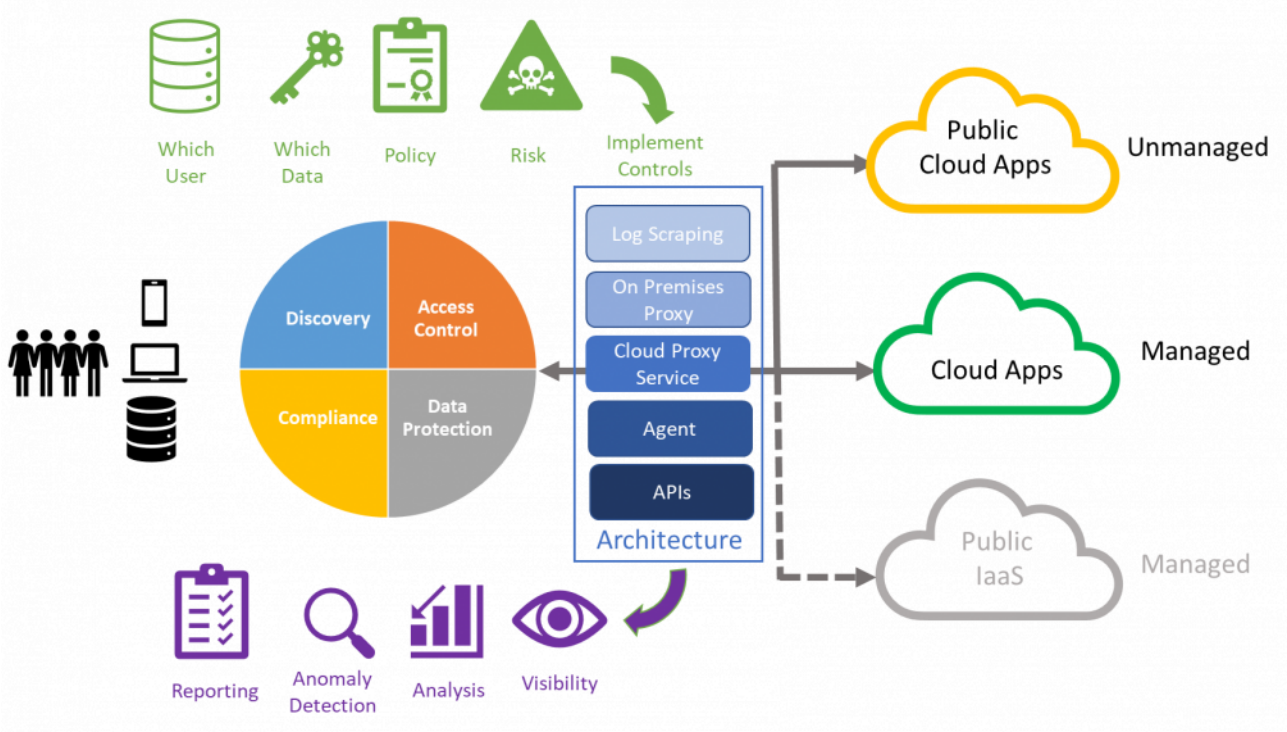


Figure 1: CASB Overview

Figure 1 provides an overview of CASB functionality and architecture. It is important to understand the architecture of a CASB solution because this impacts on its deployment and effectiveness.

The architecture of CASBs has evolved over time. The early CASB products focussed on discovering cloud use often by analysing the logs from enterprise network gateways. To enable control over access to cloud services one approach is to introduce a proxy server between the enterprise and the cloud. This makes it possible to block access in near real time and can perform other functions such as data encryption while retaining the encryption keys on premises. However, this approach duplicates some controls provided by cloud services and may not provide the same granularity. It may also impact on the use of the service. For example, Microsoft warns that the use of 3rd party inline network devices may affect Office 365[1] availability, performance, interoperability, and supportability.

Another approach is to exploit the native controls service controls using the APIs provided via an agent or intermediate cloud service. This enables granular control through the common administrative interface provided by the CASB to multiple cloud services. However, it does not provide real time response because of the delay between detection and the implementation of the cloud-based control, even though near-real time controls are available these can take seconds to trigger. Today, most CASBs use a combination of these approaches to enable coarse control over access to unmanaged services as well as real time blocking of threats at the same time as enabling granular controls.

Commonly CASB solutions are now packaged together with other functionality from the same vendor as a more generic cloud security solution. They may also integrate with functionality from other vendors using published interfaces such as ICAP (Internet Content Adaptation Protocol). These include:

- Rights Management – that provide granular 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 Gateway Solutions - protect end user device access the Web from infection and enforce company policies.
- Access Governance – provides control over how users, roles and entitlements are managed, enforced, and audited.
- Malware Protection – detect and protect against malware.
- Security Posture Management – provide insight into how well a service is configured to protect against threats. For CASB this mainly relates to the SaaS services.

The distinction between these types of products and the functionalities provided by Cloud Security Access brokers are shown in the table below.

	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 access and / or 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 end user devices from being infected by malicious Web traffic, websites, and virus/malware.
Access Governance	Of user, roles, devices, location and entitlements	Over entitlements in accordance with policies and separation of duties.	Auditing and enforcement of the allocation of entitlements that are against policies and separation of duties
Malware Protection	The presence of malware	Report, quarantine, and prevent upload, download, and execution of malicious content.	Protect against the upload, download, installation, and execution of malware.
Security Posture Management	Configuration and vulnerabilities in the SaaS cloud services	Report on vulnerabilities.	Advise on or automatically implement best practice configurations

2.2 Market Direction

The advent of cloud delivered services that were easily available to individuals as well as organizations combined with the prevalence of connected personal mobile computing devices led to a surge in the personal use of these services. This created challenges for organizational governance, risk and compliance

because, while organizations were becoming subject to an increasing level of regulation, there was little visibility on what cloud services were being used and no effective controls over how they were used. This led to the growth of products intended to plug these gaps which were named, by Gartner in 2011, as Cloud Access Security Brokers.

The early CASB products focussed on providing visibility into which cloud services were being used. The data for this was already available in organizational network appliance logs and these early products used knowledge of cloud service IP addresses to transform the data into a list of services being used. The realization that a high number of cloud services were being used from within organizations led to a high level of hype around these products and prompted demands for better controls. Early vendors in this market included CipherCloud, Netskope and Skyhigh Networks.

In response to these demands, the existing CASB products began to introduce or improve controls and more vendors entered the market. The new and improved products provided controls to identify who was making access and block access to specific cloud services. They also began to integrate with DLP products to control and encrypt data exported to cloud according to policies. While the hype around CASB was reached in around 2015 the CASB products at that point were not yet fully mature.

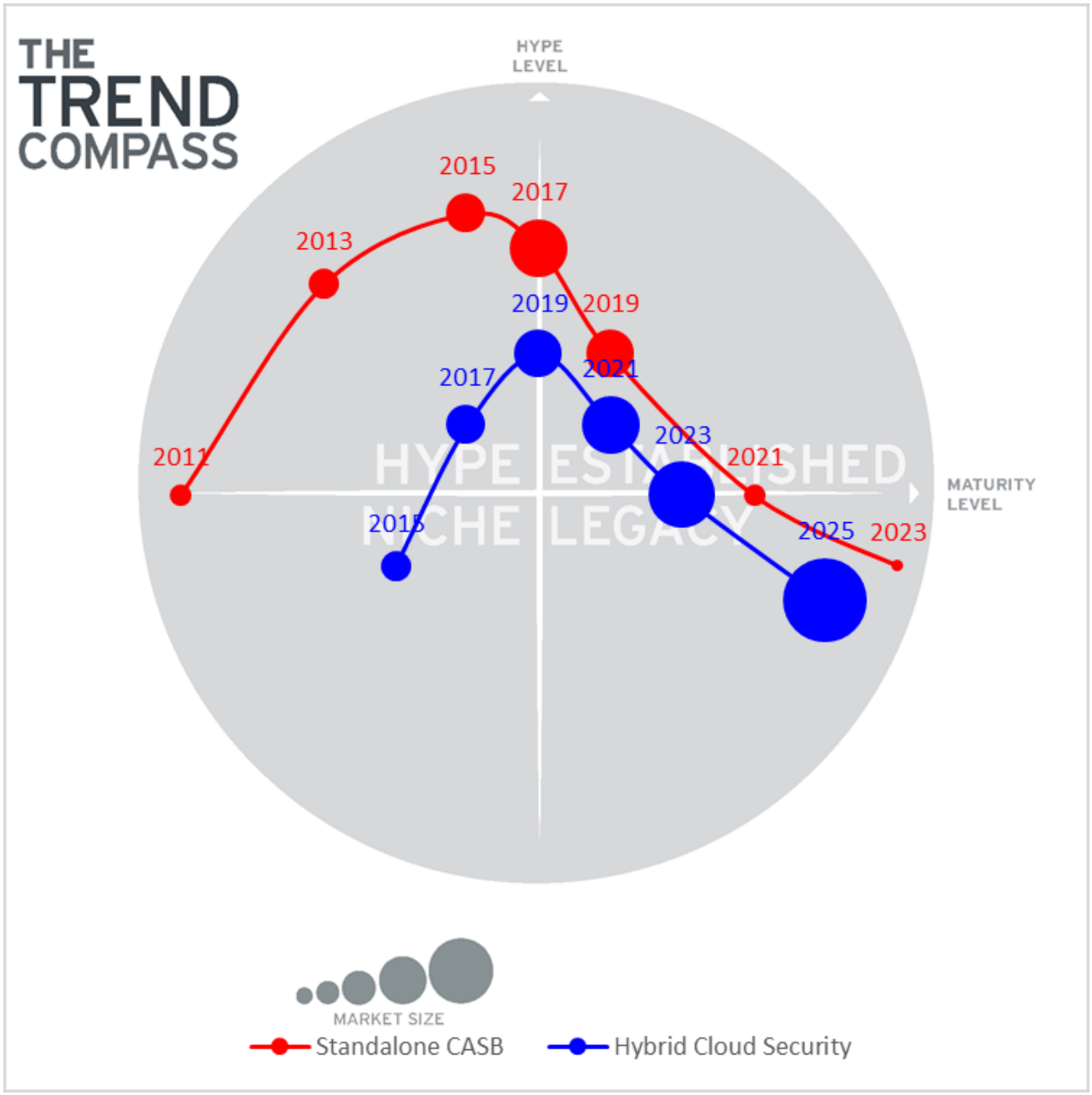


Figure 2: CASB Market Trend Compass

The products continued to improve through the use of a hybrid architecture that used inline network controls together with the exploitation of cloud service APIs to provide more granular controls. However, in order to deliver the improved functionality, the CASB had to duplicate or integrate with functionality from other security vendors. For example, network appliances, DLP, encryption and anti-malware, and this led to a flurry of acquisitions.

Between 2015 and 2019 many of the major vendors including CISCO, Microsoft, McAfee, Oracle, and Symantec acquired CASB technology which is now integrated into their product lines and adds to their cloud security solutions. These major vendors continue to invest in the CASB technology but as one component of

an overall cloud security solution. The major functionality missing from CASB is hybrid access governance enabling the access rights and entitlements of users to be governed consistently across services and applications however they are delivered.

Therefore, in our opinion, the market for a standalone CASB is shrinking and organizations are now looking for complete cloud security solutions. These are expected to include CSPM, Data and User Protection, as well as Zero Trust Network Controls. In our opinion this market will expand to embrace the hybrid IT delivery model that is now common as well as the security challenges from the growth in edge computing and 5G.

2.3 Capabilities

This report describes the basic capabilities that all solutions should support. It then looks in more detail at each of the capabilities. The precise functionality required from a solution depends upon the organizational use case. Not all use cases might require all capabilities in depth. For a solution to be categorised as a CASB it should provide all of the essential basic functionality.

2.3.1 Basic Functionality

The basic functionality that should be provided by all solutions solution includes:

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Cloud Use Discovery	The solution should be capable of discovering the use of cloud services by members of the organization.	Essential	X			X
Access Controls	The solution should enable to organization to control which cloud services can be accessed in what way by members of the organization.	Essential		X	X	X

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Data Security	The solution should enable the organization to discover and control which data is uploaded into cloud services and the protection afforded to that data.	Essential	X	X	X	X
Compliance	The solution should help the organization to use cloud services in a way that complies with laws and regulations.	Essential	X	X	X	X
Security Posture Management	The solution should assist the organization to manage the risk posture associated with their use of cloud services.	Recommended	X	X	X	X
Auditability	The solution should support secure logging of administrative activity.	Recommended	X	X	X	X
Deployability	The solution architecture should support the functionality in a manner that is easy to deploy	Recommended	X	X	X	X
Scalability	The solution should be scalable to support the large number of concurrent users found within organizations	Recommended	X	X	X	X

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Integration	The solution should integrate with commonly used identity sources such as: Microsoft ADS Microsoft Azure Directory Services IDaaS providers LDAP	Recommended	X	X	X	X

2.3.2 Discovery of Cloud Use

Individuals within the organization can use cloud services for organizational purposes without the knowledge of the organization or consideration of the risks involved. The solution should provide the organization with the means to discover this usage. The focus is on SaaS service use but increasingly this needs to cover IaaS and PaaS.

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Access to unsanctioned cloud services	The solution should be capable of discovering the use of unsanctioned cloud services by members of the organization.	Essential	X			X
Access to sanctioned cloud services	The solution should be capable of discovering the use of sanctioned cloud services by members of the organization.	Essential	X			X
Access by partners, suppliers, and contractors	The solution should be capable of discovering the use of sanctioned cloud services by contractors, partners, and suppliers.	Essential	X			X

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Identity of users	The solution should enable to organization identify the individuals accessing cloud services by their corporate user ID.	Essential	X			X
Access from outside the organizational network	The solution should be able to discover the use of sanctioned cloud services from outside the organizational network.	Essential	X			X

2.3.3 Cloud Service Access Control

The solutions should enable the organization to control which users can access which cloud services and in what way.

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Limit access to unsanctioned cloud services.	The solution should be capable of limiting which unsanctioned cloud services can be accessed by members of the organization. Allow access to only specific services. Allow access based on risk ratings. Configurable risk.	Essential		X		X

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Control Point	The solution should provide mechanisms to enforce controls such as: On premises network proxy / gateway Cloud based network controls Exploit native cloud service controls	Essential		X		X
Control access to sanctioned cloud services	The solution should be capable of controlling the access to sanctioned cloud services according to policies. Provide granular control based on: Users identities. Data accessed. Functionality accessed.	Essential		X		X
Control access to a wide range of common clouds	The solution should be capable enforcing granular controls over access to a wide range of common cloud services including: Microsoft Office 365 G Suite Salesforce.com ServiceNow #Slack Drop Box for Business SuccessFactors Oracle Business Suite Apps SAP Others	Recommended		X		X

2.3.4 Cloud Data Protection

The solutions should enable the organization to implement security controls over organizational data and that are hosted in the cloud services. This includes protection of data against unauthorized access as well as protection from cyber risks.

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Detect sensitive data	The solution should be capable of detecting sensitive data that is. Uploaded to cloud services. Stored in cloud services. Downloaded from cloud services.	Essential			X	X
Protect data against unauthorized access	The solution should provide mechanisms to protect identified data for example: By encryption By tokenization By anonymization	Essential			X	X
Types of data protected	The solution should be capable of protecting various types of data held in cloud services: Unstructured files. Database contents.	Essential			X	X

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Protection against cyber threats	The solution should be capable of protecting data held in cloud services against cyber threats including: Data exfiltration Unauthorised administrative access Unauthorised changes Ransomware Malware	Essential			X	X

2.3.5 Compliance

The solution should provide the capability to enforce and demonstrate that the use of cloud services complies with laws and regulations.

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Out of the box support for common regulations	The solution should provide out-of-the box support for demonstrating compliance with a variety of common laws, regulations, and standards including: ISO/IEC 27001. PCI-DSS Privacy Laws (GDPR) HIPAA/HITRUST GLBA Others	Recommended				X

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
Reporting and alerting capabilities	The solution should provide reporting capabilities out-of-the-box: Standard usage reports Configurable reports Alerting capabilities Integration with SIEM	Recommended				X

2.3.6 Posture Management

The solution should provide the capability to identify and remediate vulnerabilities in the configuration of cloud services. In this report the primary focus is on SaaS clouds however, we do consider how the product approaches IaaS.

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
User Entitlements	The solution should provide the capabilities to manage users' entitlements in cloud services.	Recommended				X
Privilege Management	The solution should provide the capabilities to control and limit privileged access to cloud services (i.e. cloud admin rights)	Recommended		X	X	X
Cloud Object Permissions	The solution should provide the capabilities to identify and remediate objects with excessive / public access permissions.	Recommended			X	X

Capability	Description	Relevance	Discovery	Access Control	Data Security	Compliance
IaaS Cloud coverage	The solution should provide the capabilities to manage a range of commonly used IaaS cloud services including: AWS Azure GCP IBM Cloud SAP	Recommended			X	X
IaaS Resource Vulnerability Management	The solution should provide the capabilities to identify and remediate the configuration of IaaS services resources according to security policies VM Configuration / Patch Network configuration Database configuration Web server configuration API Gateway configuration	Recommended			X	X

3 Vendors & Products

The vendors in this market covered by this report are those with CASB products that match the criteria set out earlier in the report.

3.1 Vendors Covered

The vendors covered in this report are:

- **Bitglass** was founded in 2013 with its HQ in Campbell CA in the USA and with offices worldwide. It offers CASB as part of a platform that combines CASB, an on-device Secure Web Gateway, Zero Trust Network Access, IAM, UEBA, CSPM and Advanced Threat Protection.
- **Censornet** Limited was founded in 2007 and has its HQ in Basingstoke in the UK. It offers a CASB as part of the Censornet platform which covers Web, CASB, and Email security as well as MFA.
- **CipherCloud** was founded in 2010 and has its HQ in San Jose CA in the USA. It offers CipherCloud CASB+ Platform.
- **CISCO** was founded in 1984 and has its HQ in San Jose CA in the USA. It offers Cisco Cloudlock an API-based CASB as part of CISCO Umbrella.
- **Forcepoint** was founded in 1994 and has its HQ in Austin TX in the USA. In 2017 Forcepoint acquired the Skyfence CASB product and business from Imperva.
- **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.
- **McAfee** was founded in 1987 with its HQ in Santa Clara CA in the USA. In 2018 McAfee acquired Skyhigh Networks and the Skyhigh CASB is now sold as McAfee® MVISION Cloud.
- **Microsoft** - Microsoft Cloud App Security is based on the Adallom Cloud Access Security Broker which was acquired in 2015.
- **Netskope** was founded in 2012, has its headquarters in Santa Clara CA, in the USA. The Netskope Security Cloud uses patented technology called Netskope Cloud XD™.
- **Oracle** was founded in 1977 and has its HQ in Redwood City CA in the USA. It offers the Oracle

CASB Cloud Service.

- **Palo Alto Networks Inc.** founded in 2005 with its HQ in Santa Clara CA USA. Prisma™ SaaS is a multi-mode cloud access security broker (CASB) service.
- **Proofpoint, Inc.** was founded in 2002 and has its HQ in Sunnyvale CA in the USA. It offers Proofpoint Cloud App Security Broker (Proofpoint CASB).
- **Symantec** was founded in 1982 and is owned by Broadcom. This report covers Symantec CloudSOC CASB.

3.2 Vendors to Watch

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.

Why worth watching: It provides is a central gateway security solution that runs on premise under full control of the customer. It encrypts data on premises so that the data is not held in clear in the cloud.

CloudCodes which was founded in 2011 with its HQ in Pune India. Its focus is on providing cloud security solutions to enterprise customers through a single sign-on solution. The objective is to provide a simple, effective, and efficient platform for securing cloud applications for an enterprise.

Why worth watching – its solutions have been adopted by the government of India and provide access control, DLP, and integrate with Microsoft AD. The solutions cover AWS as well as G Suite and Office 365.

CyberArk a vendor that is well known for its PAM (Privileged Access Management) solutions, acquired certain assets of Vaultive, Inc., including a stateless network-layer software encryption proxy.

Why worth watching: 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.

NextLabs® has its USA headquarters in San Mateo, CA with offices worldwide.

Why worth watching: 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 Centre, NextLabs Rights Management, and NextLabs Entitlement Management.

Oracle Cloud Infrastructure has recently announced wide ranging enhancements to their cloud services and cloud security. Full details of these are not yet fully available but will be published in the fall of 2020.

Why worth watching: Oracle Cloud Infrastructure has announced plans to replace CASB with a more integrated Cloud Guard service which was not GA at the time of this report writing, but will be available in August.

4 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	Interoperability	Usability	Deployment	Discovery	Access Control	Data Protection	Compliance	Posture Management
Bitglass Cloud Security Platform	●	●	●	●	●	●	●	●	●
Censornet Cloud Access Security Broker	●	●	●	●	●	●	●	●	●
CipherCloud CASB+ Zero Trust Platform	●	●	●	●	●	●	●	●	●
Cisco Cloudlock	●	●	●	●	●	●	●	●	●
Forcepoint CASB	●	●	●	●	●	●	●	●	●
Fortinet FortiCASB™	●	●	●	●	●	●	●	●	●
McAfee MVISION Cloud	●	●	●	●	●	●	●	●	●
Microsoft Cloud App Security	●	●	●	●	●	●	●	●	●
Netskope Security Cloud	●	●	●	●	●	●	●	●	●
Oracle CASB Cloud Service	●	●	●	●	●	●	●	●	●
Palo Alto Networks Prisma™ SaaS	●	●	●	●	●	●	●	●	●
Proofpoint Cloud App Security Broker	●	●	●	●	●	●	●	●	●
Symantec CloudSOC	●	●	●	●	●	●	●	●	●
Legend						● critical	● weak	● neutral	● positive ● strong positive

4.1 Featured Vendors

All the vendors that we reviewed in this market segment offer strong basic functionality and protection for employee access to SaaS. The differences can be seen in the other aspects notably the lack of coverage in the products from some vendors of deep posture management for IaaS.

Some vendors are better positioned to meet narrow use cases, while others have stronger offerings across the whole range of use cases. We have identified a few vendors that are notable for their unique strengths that may not be apparent in the table above. Vendors are featured for innovation, access governance, and for integration.

4.1.1 Featured for Innovation: Bitglass

One major problem with the deployment of CASB is the need to install agents on devices or as part of a forward proxy. The Bitglass solution leverages patent pending AJAX-VM agentless reverse proxy capabilities. This enables the Bitglass solution to provides support any application with real-time data and threat protection, identity, and visibility.

Different CASB architectures address different use cases. API-based architectures integrate with application programming interfaces to provide visibility and control over data at rest within managed cloud applications. Forward proxy architectures require that agents be installed on all user devices in order to provide inline visibility and control over managed and unmanaged app traffic and data. Reverse proxy architectures provide inline visibility and control over managed app traffic and data and are deployed in the cloud without the need for agents.

Typically, reverse proxies are hardcoded to specific versions of applications. This means that when apps are updated and their underlying code is changed, the reverse proxy will not know what to do or how to pass the new code down to the user. Bitglass has developed AJAX-VM, technology for reverse proxy functionality. It employs machine learning so that it can automatically handle code rewrites when applications evolve and change. This means that there are is no need for engineers to manually fix the reverse proxy.

In addition, Bitglass claims to provide the world's only on-device secure web gateway. Traffic is decrypted and inspected directly on users' devices and only security events are uploaded to the cloud. This enables the solution to preserve user privacy, eliminate latency-inducing network hops, and deliver thorough web security. Threat URLs and unmanaged applications are blocked before they can be visited, and employee access to content is controlled by variables like category, destination trustworthiness, user group, device type, and location.

Figure 3: Featured for Innovation

4.1.2 Featured for Access Governance: Forcepoint

The key risks around the use of cloud services relate to the unauthorised use of the services and access to the data they contain. While there are many potential technical threats behind these risks the most common ones relate to the people. Some people have roles that are more commonly targeted, for example accounts receivable administrators and personal assistants expect to receive invoices from external email addresses. Some roles have a higher potential for fraud or potential impact through misuse or mistake, for example systems administrators. Other people engage in behaviour that is riskier from a cyber security perspective. So, it makes sense to focus on security controls on those users with the highest risk. Forcepoint takes a human centric approach to security.

While most CASB products include UEBA to identify anomalous behaviours none include what KuppingerCole would classify as full identity and access governance. However, the Forcepoint CASB does include their version of Access and Security Governance. For applications that have been defined as managed assets and for which governance has been configured, the product displays account governance and compliance information including account ownership, configuration policy violations, and user accounts that should be removed, according to configured policy. This functionality covers: Amazon AWS, Box, Dropbox, Google G Suite, Office 365, and Salesforce.

Figure 4: Featured for Access Governance

4.1.3 Featured for Integration: Censornet

Censornet's Autonomous Security Engine (ASE) is a core component of Censornet's single cloud security platform that delivers email security, web security, CASB and MFA. In this approach individual security engines automatically react to attacks and stop them before they can enter the kill chain. ASE enables previously siloed services to share security context, state data and events whilst leveraging threat intelligence. ASE leverages the intelligence gathered by the platform about user activity, devices, content, and other entities to deliver security outcomes rather than events and alerts that need manual analysis to be useful. For example, if a user attempts to exfiltrate a file via email then ASE will share the file hash with CASB to prevent subsequent attempts to transfer the file out via cloud applications (WeTransfer, Dropbox, OneDrive etc).

Figure 5: Featured for Integration

4.1.4 Featured for Integrated Data Security – CipherCloud

There are several CASBs with comprehensive capabilities from different vendors. However, many of these are the result of integrating multiple products acquired through mergers and acquisitions. CipherCloud was the first vendor in the CASB market to introduce a full reverse proxy based data centric cloud solution in 2011 and this functionality remains a key part of its solution. CipherCloud CASB+ provides differentiated capabilities such as native Rights Management, Zero Trust Network Access (ZTNA), Email protection, and end-to-end data protection with common enterprise SaaS, PaaS, and IaaS applications. It provides turnkey integration with a wide range of SaaS applications supporting field level data protection for these applications. This support includes encryption, tokenization, data masking, data loss prevention to protect a wide range of types of data including recognized keywords and sensitive numerical formats.

In addition, CipherCloud CASB+ AnyApp allows customers to exploit these data protection capabilities for their own custom cloud-based applications. This can help custom applications to protect data regardless of their chosen cloud platform. AnyApp allows custom applications to benefit from encryption, tokenization, dynamic access control, DRM, UEBA, as well as threat prevention.

Figure 6: Featured for Integrated Data Security

4.1.5 Featured for Custom Apps – McAfee

While CASBs provide IT security and compliance teams with visibility and control over SaaS they do not directly cover custom apps. This is becoming an increasing problem as organizations create more custom apps as part of their digital transformation and deploy them in the public cloud. Monitoring and controlling these custom apps is an essential component of secure and resilient digital transformation.

McAfee MVISION Cloud for Custom Applications enables organizations to extend the same CASB capabilities used to secure SaaS, such as DLP, activity monitoring, threat protection, access control, and encryption, to their custom-built applications running on IaaS and PaaS environments. It achieves this without any the need for any coding or development by the customer. It provides a self-service model that uses machine learning to automatically understand activity in the custom applications.

It monitors activity in custom apps and provides an audit trail of all user and administrator activities taking place in each application. It ensures that the same DLP policies used to protect data in sanctioned cloud services can be applied to custom applications. It identifies anomalous activities within a custom application and also correlates activities across all custom and SaaS applications to identify true threats. It supports enforcement of access policies for custom applications based on whether the device is managed or unmanaged, if the IP is blacklisted or safe, or whether the traffic originates from a trusted or untrusted location and can enforce additional authentication.

Figure 7: Featured for Custom Apps

5 Product/Service Details

Spider graphs

In addition to the ratings for our standard categories we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the Market Compass. For this Market Compass, we look at the following areas:

- **Discovery**
  How well the product or service provides discovery of cloud service usage based on the capabilities described in section 2.3.2.
- **Access Control**
  How well the product or service provides control over which users can access which cloud services and in what way based on the capabilities described in section 2.3.3.
- **Data Protection**
  How well the product or service provides protection for organizational data against unauthorized access as well as from cyber risks based on the capabilities described in section 2.3.4.
- **Compliance**
  How well the product or service provides the capability to enforce and demonstrate that the use of cloud services complies with laws and regulations based on the capabilities described in section 2.3.5.
- **Posture Management**
  How well the product or service provides the capability to identify and remediate vulnerabilities in the configuration of cloud services based on the capabilities described in sections 2.3.6.

These spider graphs provide comparative information by showing the areas where the products are stronger or weaker. Some products may have gaps in some areas, while being strong in others. These might be a good fit if only the specific features are required. Other services deliver strong capabilities across all areas, thus being a better fit for strategic choice of product.

5.1 Bitglass

Bitglass was founded in 2013 with its HQ in Campbell CA in the USA and with offices worldwide. The Bitglass CASB is part of a Cloud Security Platform that combines CASB, an on-device Secure Web Gateway, Zero Trust Network Access, IAM, UEBA, CSPM and Advanced Threat Protection. Built on its Polyscale Architecture, Bitglass' platform claims an independently verified uptime of 99.99% since 2014; while optimizing the performance of applications to any location in the world. The Bitglass CASB is based on a multi-mode deployment architecture and can operate in agent-based or agentless mode. Agentless mode enables rapid deployment and it is interoperable with existing infrastructure such as Secure Web Gateways. It can discover and manage shadow IT risks with over 600K cloud apps catalogued for risk —machine learning automatically identifies new applications and analyses them for their trustworthiness. It provides granular access controls to a wide range of managed apps through API integrations, SAML and network proxy configurations, as well as unmanaged app control.

The DLP solution enables a customizable information protection based on content and the context in which it is being accessed. It includes prebuilt and configurable data patterns and integration with on-premises DLP systems via ICAP for more granular policies. Customization includes the use of keyword matching, advanced regex with Boolean logic, exact data match, and file fingerprinting. Bitglass' agentless proxies enable data security for any app on any mobile device including device-level security policies. Contextual access control can be used to control where and how employees can access corporate data. Bitglass Cloud Encryption enables encryption of data-at-rest based on full-strength FIPS-compliant 256-bit AES encryption, while maintaining normal app functionality.

Bitglass has a native IAM system, with adaptive step-up multi-factor authentication. Bitglass also integrates with Active Directory and all major IDaaS solutions like Okta and Ping Identity. Bitglass dual-SAML termination ensures that the strength of SAML SSO is preserved. Bitglass' Advanced Threat Protection, powered by CrowdStrike, Cylance and Bitdefender, uses machine learning to identify both known and unknown malware in real-time. The system analyses hundreds of file characteristics, to detect and stop zero-day threats at upload and on download as well as at rest. With its agentless deployment mode, Bitglass can defend against malware even on personal devices. Bitglass CSPM can search IaaS instances for inconsistencies against custom organizational benchmarks, as well as established security standards like the PCI-DSS (Payment Card Industry Data Security Standard)

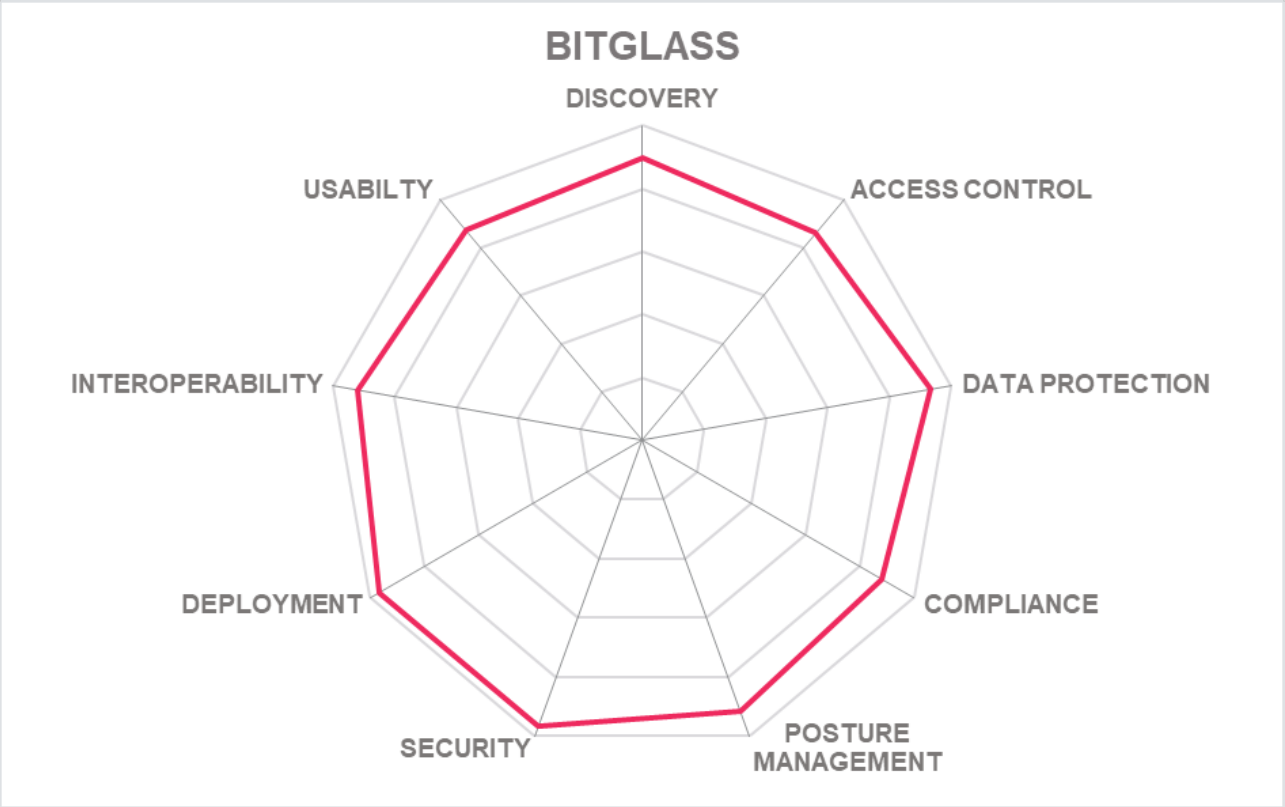
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Discovery	● ● ● ● ●
Access Control	● ● ● ● ●
Data Protection	● ● ● ● ●
Compliance	● ● ● ● ●
Posture Management	● ● ● ● ●

Strengths

- Comprehensive functionality.
- Multimodal architecture provides flexible deployment options.
- Independently verified performance and uptime,
- Strong shadow IT discovery capabilities.
- API integration with major public SaaS services.
- Strong inbuilt data protection.
- Flexibility of its DLP.
- Integrated functionality across CASB, SWG, IAM, UEBA, Advanced Threat Protection, CSPM and DLP.
- Agentless Advanced Threat Protection.
- Open integration through standards.
- Support for compliance with standards.
- Posture management covers major IaaS providers as well as SaaS.

Challenges

- Less well known in Europe than some other vendors
- Marketing clarity over how the solution range should be categorized.
- Improving presence in markets outside of North America.


BITGLASS
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.2 Censornet

Censornet has its headquarters in Basingstoke. Censornet provides a range of solutions to help with the challenges of managing cloud applications in an increasingly mobile work environment. Censornet CASB is fully integrated with Censornet's Cloud Security Platform that also includes Email Security, Web Security and Multi-Factor Authentication. The Censornet Platform provides a single web interface for central policy configuration and management, as well as data visualization and reporting.

Censornet's CASB has a flexible architecture that allows it to be deployed using agents or gateways, or both, to meet the needs of organisations. This provides users with the freedom to work however, whenever and wherever they want. CASB inline mode is deployed using agents or proxies, or a combination of both. Using purely agents on endpoints, CASB offers a proxy-less approach which significantly reduces latency, preserves the user's real IP address, and maintains privacy by allowing the browser to maintain direct communication with the cloud application server.

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. Censornet say that CSPM functionality is on the roadmap. Censornet products provide a good range of control over access to cloud services with a growing number of customers in Europe.

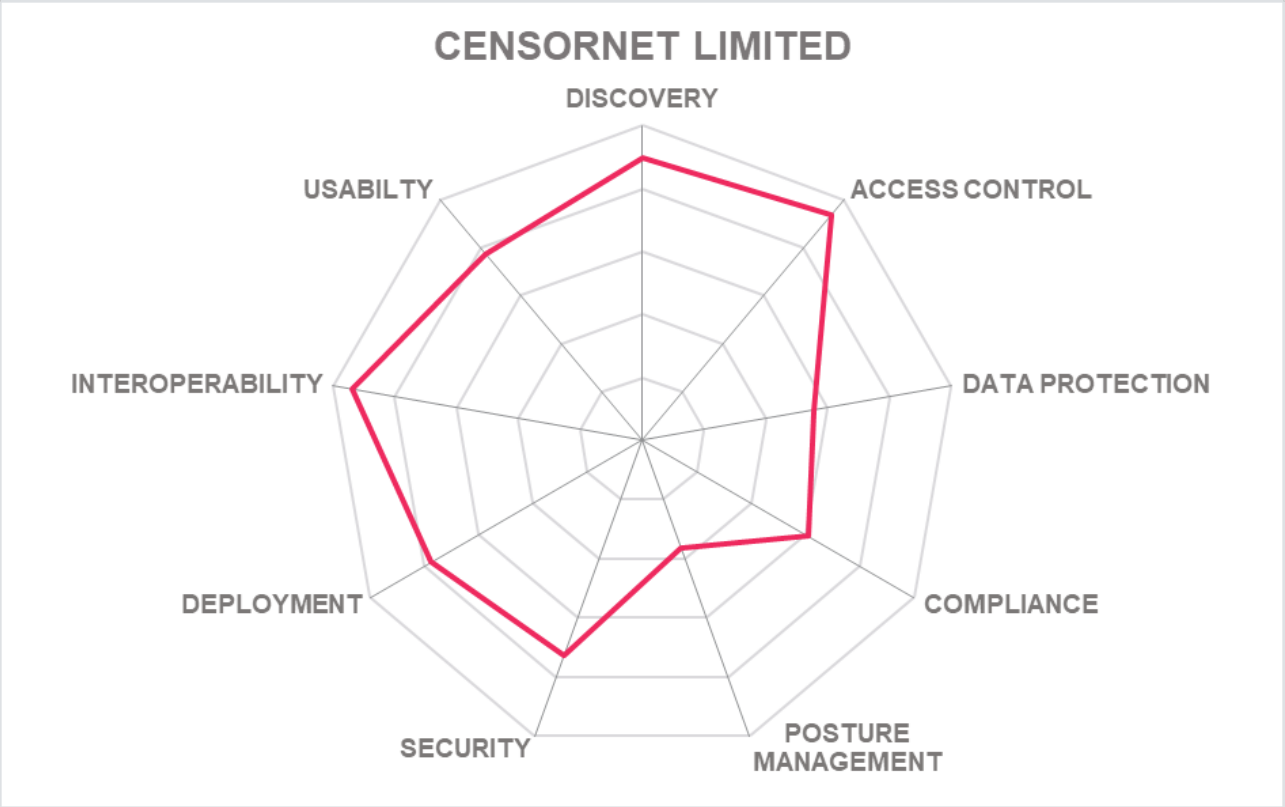
Security	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○
Discovery	●●●●●
Access Control	●●●●●
Data Protection	●●●○○
Compliance	●●●●○
Posture Management	●●○○○

Strengths

- Multi modal architecture with 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.

Challenges

- Lack of CSPM functionality (although this is said to be on the roadmap).
- Small partner ecosystem, but some large partners on global scale.
- Low penetration in the North American markets.
- Lack of inbuilt encryption functionality to protect data at rest in the cloud service.


CENSORNET LIMITED
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.3 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.

The CipherCloud CASB+ platform provides visibility, end-to-end data protection, advanced threat protection, ZTNA, and compliance capabilities for enterprise embracing cloud-based applications. CipherCloud CASB+ features turnkey integration with a wide range of SaaS applications, ensuring field level data protection including encryption, tokenization, data masking as well as data loss prevention. Applications include Office365® (including Email), Slack, G-Suite, Box®, Atlassian Cloud, AWS S3, SAP SuccessFactors, ServiceNow, Salesforce, Adobe®, Dropbox®, SAP S/4HANA, SAP Hybrid Cloud and others. PaaS ecosystem applications offered in each provider's marketplace are also protected. CipherCloud CASB+ AnyApp allows customers to integrate the data protection capabilities for their own custom cloud-based applications.

CipherCloud CASB+ provides 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 behaviour analytics (UEBA), and virus/malware protection. It helps organizations to be compliant with a broad mix of global privacy and compliance regulations. It includes the controls necessary to support cloud-based applications under PCI, PII, HIPAA, GDPR, and others. CipherCloud provides a strong solution for securing data held in cloud services and for controlling access to that data.

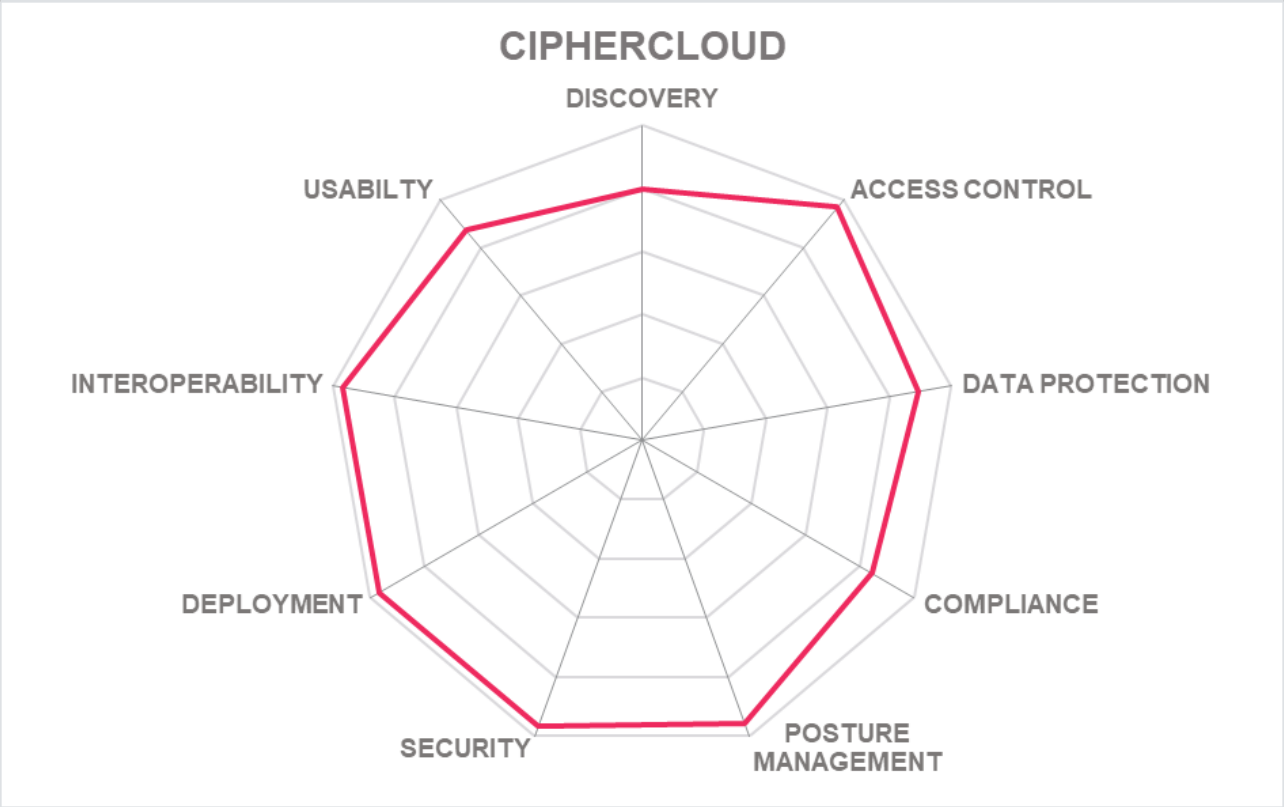
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Discovery	● ● ● ● ●
Access Control	● ● ● ● ●
Data Protection	● ● ● ● ●
Compliance	● ● ● ● ●
Posture Management	● ● ● ● ●

Strengths

- A mature and well proven solution with a wide customer base.
- Wide range of SaaS apps covered out-of-the box.
- Agentless solution using mature reverse proxy, battle tested since year 2011
- Secure Email Gateway for inline DLP, data protection and collaboration control
- Data Protection as a Service APIs for any system, device or technology stack
- ZTNA security to private apps
- OCR capability in any mode including Email
- AnyApp connector enables customers to protect their own applications using Cipher Cloud CASB+.
- Encryption for 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.
- Used by customers to achieve compliance with a wide range of data security standards.
- Integration with Microsoft ADS and other common user stores as well as IDaaS.

Challenges

- 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.
- Competition from vendors with a full range of security solutions.


CIPHERCLOUD
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.4 Cisco

Cisco is a worldwide security and networking company founded in 1984. Cisco's cloud security portfolio includes Cisco Umbrella, Cisco Cloudlock CASB (which was acquired in 2016) and Cisco Stealthwatch Cloud. Cloudlock can be purchased separately or as an integrated part of Cisco Umbrella. Umbrella is a multi-function, cloud-native internet security solution. It includes a Secure Web Gateway, CASB, Firewall as-a-service, DNS security, threat intelligence and the SecureX platform. Cisco Stealthwatch Cloud protects public cloud infrastructure by inspecting configurations and detecting abnormal behaviour indicative of threats. Cisco Cloudlock and Email Security provide visibility and protection for SaaS apps, including cloud email. This report covers the Cisco Cloudlock which is delivered as a cloud service hosted in AWS.

Cisco's CASB functionality provides a tool to discover and assess how cloud services are being used from within the organization. It provides visibility into and control over the Shadow IT in the form of user-enabled cloud apps connected to corporate systems, including Google G Suite and Microsoft Azure Active Directory (AD) using OAuth. In addition, the CASB functionality utilizes proxy/secure web gateway data, and augments this with cybersecurity insight, including app risk level ratings, traffic volumes, and visibility into the most active users.

Cisco Cloudlock monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments. Cisco Cloudlock can enforce policies focused on common sensitive information sets, such as PCI-DSS and HIPAA compliance, as well as custom policies to identify proprietary data, such as intellectual property. Cloudlock implements controls using the SaaS native APIs which eases deployment. However, it depends upon IDaaS to implement more granular access controls. It does not cover posture management of IaaS. Cisco Cloudlock CASB platform integrates with other Cisco products to provide a full multi-mode approach to cloud security that is easy to deploy and simple to manage.

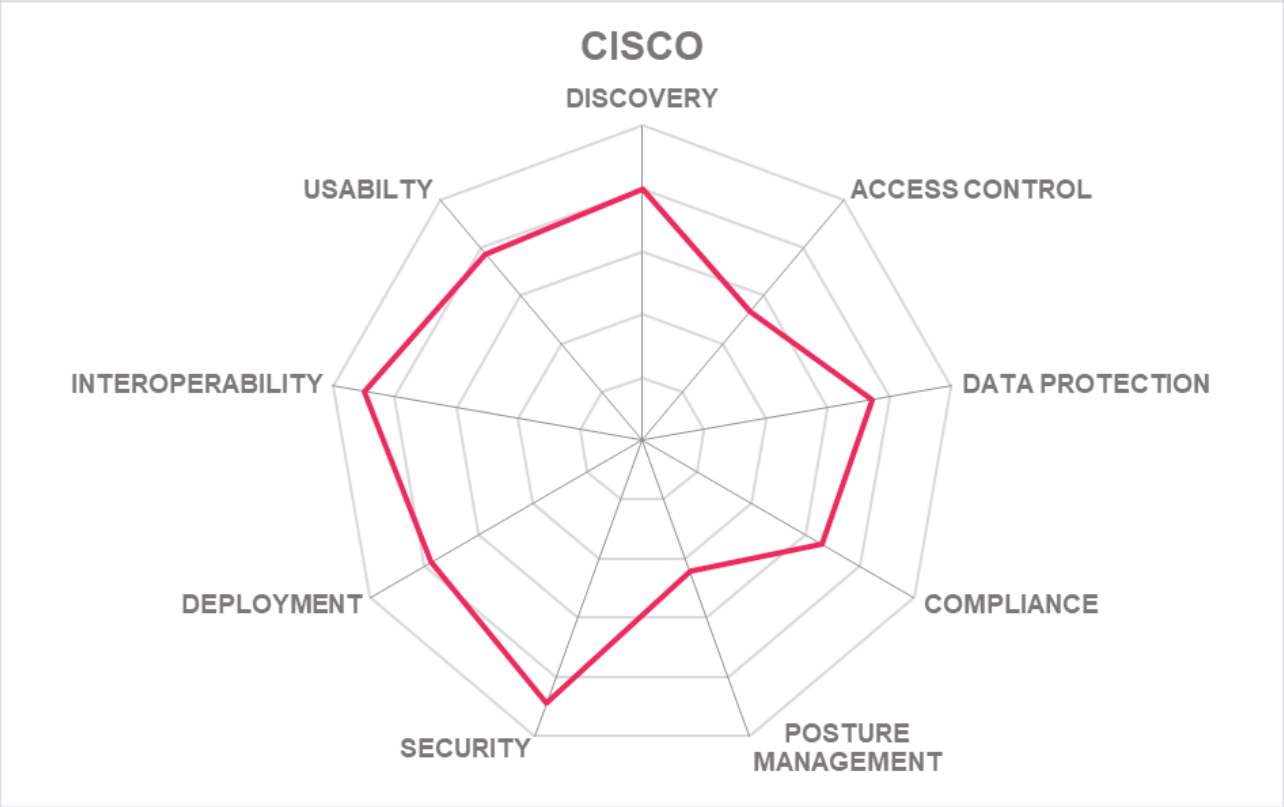
Security	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○
Discovery	●●●●●
Access Control	●●●○○
Data Protection	●●●●○
Compliance	●●●●○
Posture Management	●●●○○

Strengths

- Ease of deployment.
- App risk rating based on large amount of community-sourced data.
- Protection against OAuth based threats.
- Integrated DLP engine with range of standard policies out of the box.
- Detection of abnormal user behaviour enhances threat detection.
- Wide range of SaaS apps covered out of the box.
- Integration with other Cisco products.
- Cisco's strength in the market.

Challenges

- Enforcement of user access controls depends upon integration with external IDaaS.
- Detection using cloud service APIs may lead to delay in enforcement. However, Umbrella provides full proxy-based detection and granular app controls.
- Posture management not supported for IaaS.


CISCO
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.5 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, Cloud Audit and Protection and Cloud Security Suite. These provide functions that discover cloud service usage, cloud access governance, data loss prevention, user activity monitoring and cyber threat prevention.

Forcepoint CASB Gateway virtual appliance that acts as a proxy between organizational users and cloud applications; it monitors cloud account activities and enforces organizational policy. This is controlled by and communicates with the Forcepoint CASB management server. Both components can be deployed on premises or can be hosted in the Forcepoint cloud. The Forcepoint Cloud Discovery Tool is a local application that scans network logs to discover cloud service usage.

Forcepoint CASB provides details on risk factors that 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. It monitors and controls uploading, downloading, and sharing of sensitive data through inbuilt DLP capabilities and integrates using ICAP with existing enterprise DLP. It monitors user activity including privileged users against normal usage patterns to provide user behaviour analytics. 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). Forcepoint CASB provides visibility and control over access to both sanctioned and unsanctioned apps from both managed and unmanaged devices.

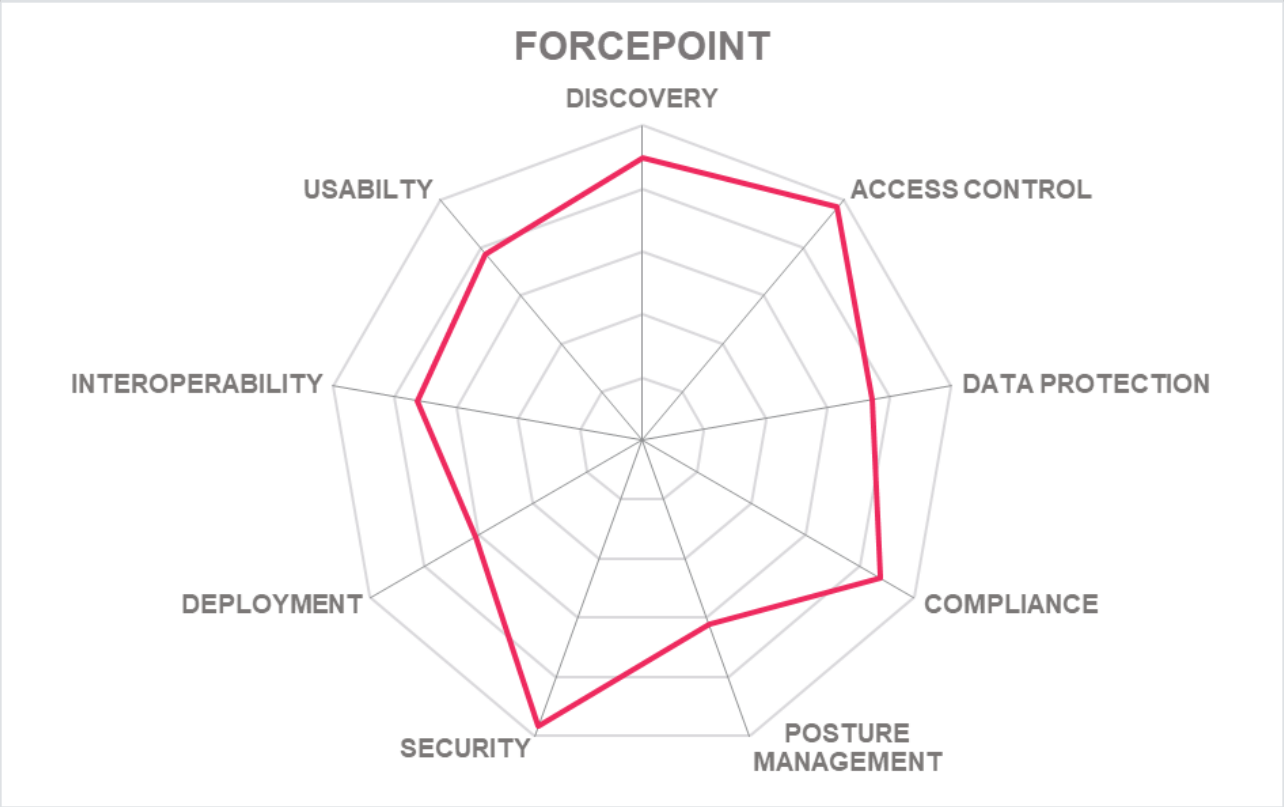
Security	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○
Discovery	●●●●●
Access Control	●●●●●
Data Protection	●●●●○
Compliance	●●●●●
Posture Management	●●●●○

Strengths

- Part of a comprehensive suite of products.
- Provides both in-line and offline deployment options.
- Provides some cloud identity and access governance capabilities.
- Audits cloud privileged user activity as part of UEBA.
- Integrated data classification and DLP integration as well as ICAP integration.
- Compliance templates provided out of the box.
- Support for major SaaS cloud services as well as AWS.
- Support for SAML.

Challenges

- Late entry into the market for CASBs.
- Very small partner ecosystem.
- Posture management of IaaS resource vulnerabilities not supported.


FORCEPOINT
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.6 Fortinet

Fortinet is a publicly traded cybersecurity company founded in 2000 with headquarters in Sunnyvale CA in the USA. It provides a wide range of network security and SD-WAN, switching and wireless access, network access control, authentication, public and private cloud security, endpoint security, and AI-driven advanced threat protection solutions for carriers, data centres, enterprises, and distributed offices. Its solutions are integrated into the Fortinet Security Fabric.

FortiCASB is a cloud-native CASB subscription with a set of Cloud Security Posture Management (CSPM) capabilities that provides visibility, compliance, data security, and threat protection for the cloud-based services used by an organization. FortiCASB uses an API-based approach, to connect directly to SaaS providers to access usage and data stored in the cloud. This provides the capabilities to scan provisioned cloud resource configurations for potential threats as well as SaaS application data for threats, proprietary information, or sensitive customer records. It also includes tools that provide insights into user behaviours and their activities on cloud-based applications. Administrators can monitor usage and have the ability to view user entitlements, dormant users, and conduct detailed configuration assessments.

FortiCASB includes a customizable suite of data loss prevention tools that defend against data breaches and provides a set of predefined compliance reports. Using regular expressions, FortiCASB can be configured for nearly any policy to meet data protection needs and provide tailored reports on DLP activities. FortiCASB offers predefined compliance reports for regulations and standards including SOX, GDPR, PCI, HIPAA, NIST, and ISO27001. FortiCASB is designed for deep integration into the Fortinet Security Fabric to provide consolidated cloud usage management and reporting with FortiGate and FortiAnalyzer. In addition, FortiCWP can extend the CSPM capabilities to cover the major IaaS platforms Azure, AWS and GCP.

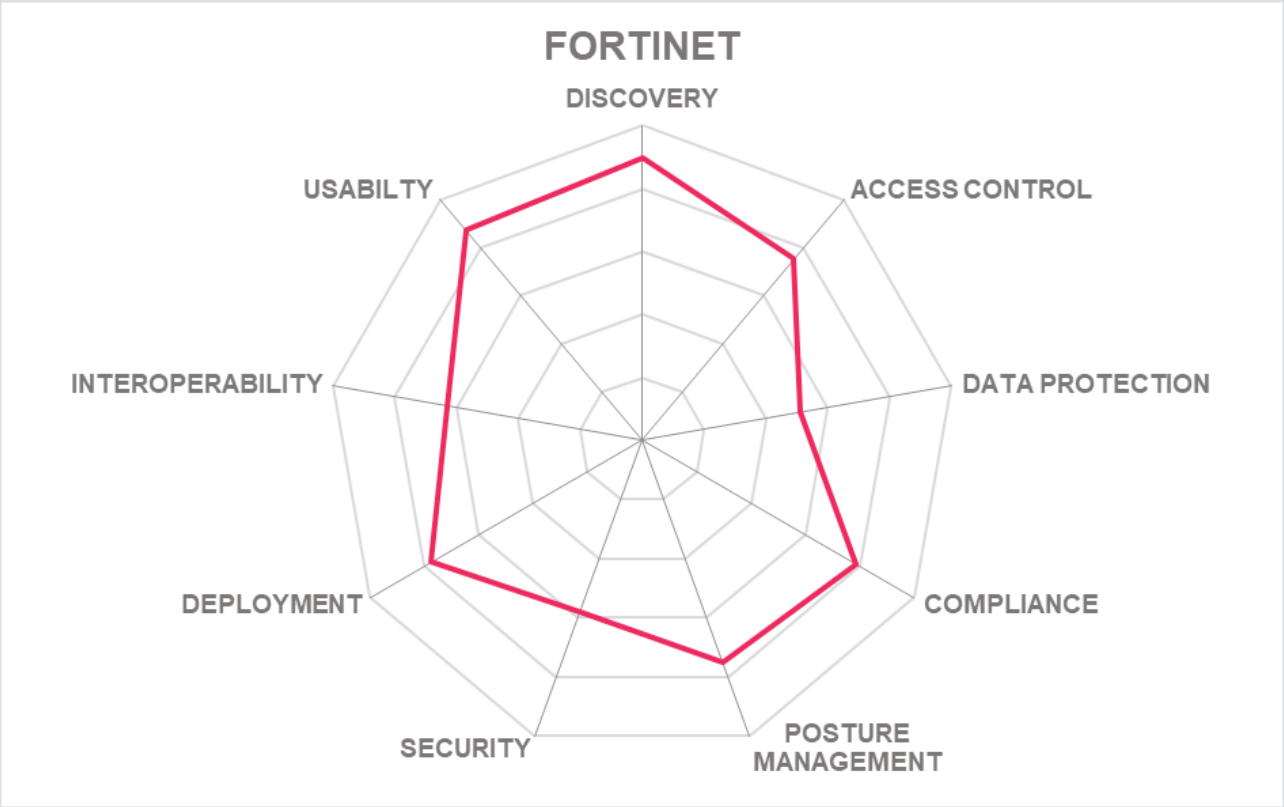
Security	●●●○○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●○
Discovery	●●●●●
Access Control	●●●●○
Data Protection	●●●○○
Compliance	●●●●○
Posture Management	●●●●○

Strengths

- Cloud native solution with API integration provides deep insight for managed SaaS.
- Integration with other Fortinet products provides insight and control over unmanaged SaaS.
- Covers the major SaaS apps in common use.
- Integrated configurable DLP with inbuilt data type templates.
- Provides insight into AWS S3 data permissions.
- Provides visibility into and controls over user entitlements, dormant users.
- Out-of-the box templates for common compliance needs out-of-the box.

Challenges

- FortiCASB is not well known in EMEA.
- DLP / data protection actions do not include encryption
- Does not provide fine grained access controls within managed SaaS.
- Limited range of managed SaaS apps in comparison with competitive products.
- Cyber security controls depend upon integration with other Fortinet solutions.


FORTINET
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.7 McAfee

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. What was the Skyhigh CASB has now been enhanced and integrated with other McAfee products to create the McAfee® MVISION Cloud Platform.

McAfee® MVISION Cloud helps to protect data and stop threats in the cloud across SaaS, PaaS, and IaaS from a single, cloud-native enforcement point. It provides visibility into data, context, and user behaviour and enables action in real-time to enforce policies. A registry of cloud services includes a Cloud Trust Rating for each service based on a 261-point risk assessment. It enables encryption of cloud data (in motion or at rest) using multiple encryption schemas and supports customer keys (BYOK). Privacy guard leverages an irreversible, one-way process to tokenize data holding key data on premises. It exploits machine learning to understand apps and to identify patterns indicative of malicious activity and data exfiltration. Through integration with IAM solutions it can enforce adaptive authentication based on policies.

As well as covering a wide range of SaaS applications McAfee MVISION Cloud includes options that provide posture management for the major IaaS clouds AWS, Azure and GCP. These provide monitoring, auditing, and remediation solution for the IaaS environments. They can audit the configuration a wide range of the IaaS service resources to identify those that are insecure or non-compliant and recommend corrective measures. They capture an audit trail of user activity related to these environments to detect threats from compromised accounts, insider threats, privileged access misuse, and malware infection. They can also enforce DLP policies for sensitive data stored in those clouds, for example in AWS S3 buckets, and take action to remediate. 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.

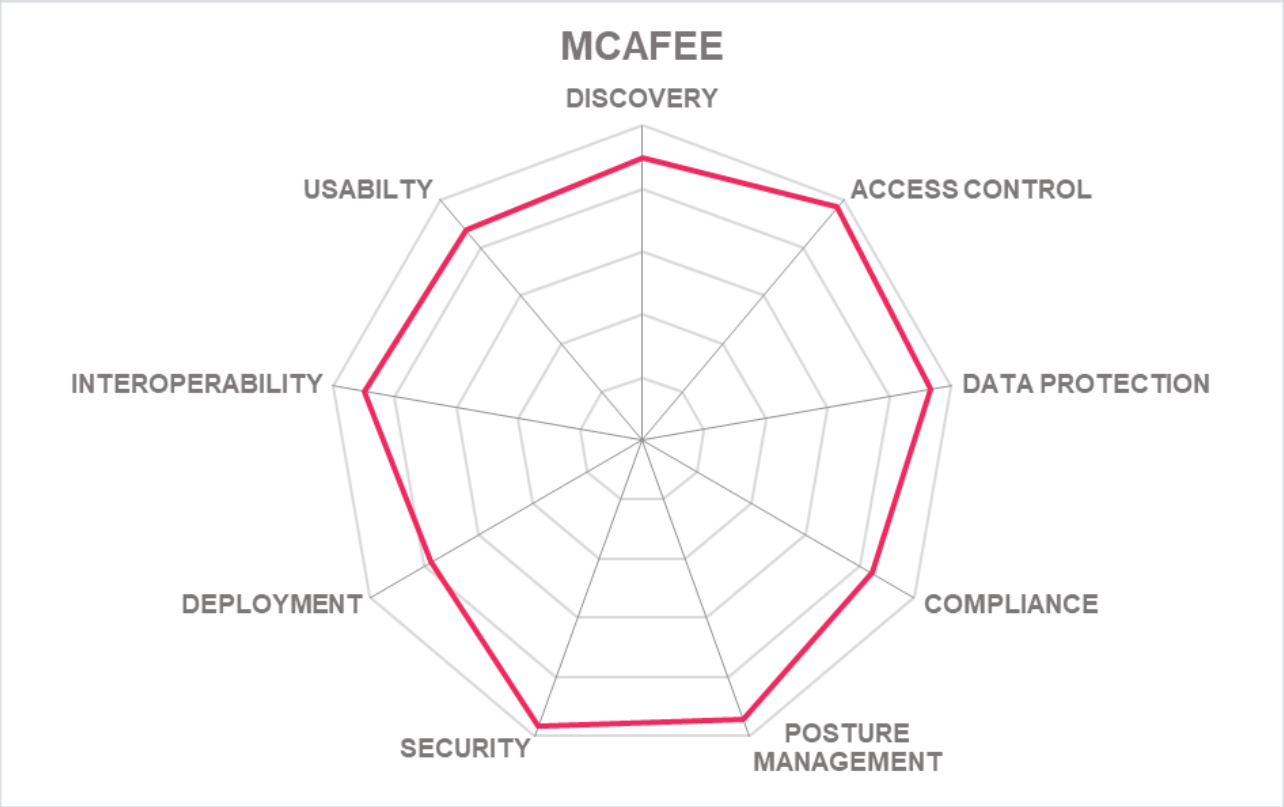
McAfee™
Together is power.

Strengths

- Mature product with large user base.
- Comprehensive functionality.
- Coverage for a wide range of SaaS apps out-of-the-box.
- API based control over managed apps.
- Enables risk and configuration management of SaaS.
- Supports posture management for AWS, Azure and GCP IaaS environments.
- Integrated with other McAfee products.
- Strong DLP capabilities that include AWS IaaS data.
- Innovative encryption capabilities.
- Integration with other vendors' products DLP, SIEM etc.

Challenges

- Full functionality depends upon the deployment of multiple options.
- Integration with on-premises apps
- Integration with traditional access governance tools for SoD, entitlement attestation, etc.


MCAFEE
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.8 Microsoft

Microsoft Cloud App Security is based on the Adallom Cloud Access Security Broker which was acquired in 2015. This is fully integrated with other Microsoft products and forms part of Microsoft Enterprise Mobility + Security suite. This product has undergone significant development since its acquisition and recent improvements include real time malware detection, enhanced SAML access and session controls with any Identity Provider, and enhanced privacy controls.

Microsoft Cloud App Security provides visibility of shadow IT and provides risk classification of discovered apps based on over 70 factors that include regulatory and industry standards. Discovered apps can be governed and sanctioned by onboarding the app to Azure AD or blocking them on the network. API level integration with a wide range of common SaaS apps provide granular controls and integration with Secure Web Gateways enable inline discovery as well as enforcement of controls that can be based on conditions and session context, including user identity, device, and location. It includes governance and compliance reporting against a range of common regulatory needs. The capabilities for governance and control extend beyond SaaS to include some aspects of AWS and Azure IaaS.

Information protection capabilities provides granular control over data and use through built-in or custom policies for data sharing and data loss prevention. They enable the classification and labelling of sensitive information when it is uploaded to the cloud. This identifies information at risk of and controls include quarantine, revoking privileges or notifying the user. It exploits Microsoft threat intelligence and research to identify emerging threats and user behavioural analytics to detect anomalies. It includes templates to detect ransomware attacks and integrates with SIEM solutions. Microsoft Cloud App Security, as part of Microsoft Enterprise Mobility + Security suite, provides a well-rounded and complete CASB solution.

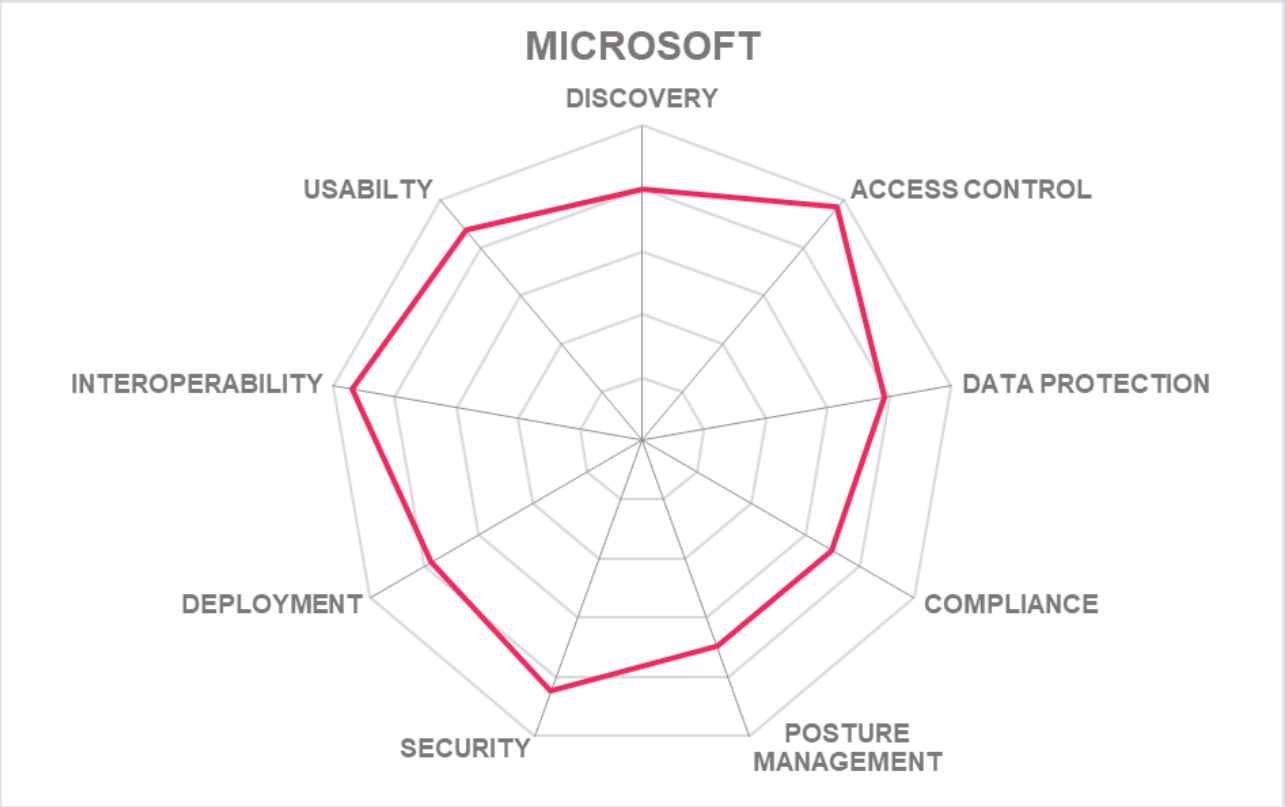
Microsoft

Strengths

- A comprehensive solution with the backing of Microsoft development expertise.
- Widely used by Microsoft customers.
- Exploits threat intelligence from Microsoft threat teams.
- 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.

Challenges

- Does not provide encryption / tokenization of structured data held in cloud applications such as CRM applications.
- Needs deployment of other Microsoft security tools to get the full benefits.
- Gaining traction in organizations where use of Microsoft technology is limited.
- Extending posture management to include a wider range of IaaS services and resources.


MICROSOFT
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.9 Netskope

Netskope, which was founded in 2012, has its headquarters in Santa Clara, CA and offices in San Francisco, Seattle, London, the UK, Australia, India, Singapore, and Japan. This report covers the Netskope Security Cloud which uses patented technology called Netskope Cloud XD™. It is intended to discover and control activities across both SaaS and IaaS cloud services as well as websites.

Netskope Security Cloud can discover usage of SaaS, IaaS, and web in detail and assess risk. Netskope Cloud XD uses big data analytics to identify this usage in “extreme definition” (XD). It is delivered through Netskope NewEdge which is a carrier-grade private cloud network that spans more than 40 regions around the world to provide performant and secure access with the goal of minimal latency between the customers and the Netskope Security Cloud.

It uses a multi modal approach and the customer can choose the deployment architecture including log-based discovery, API mode, inline as a reverse proxy, inline as a forward proxy, in-line with or without agents or mobile profiles. It enables to customer to secure access to a wide range of sanctioned cloud services such as Office 365, Box, and AWS and safely enable unsanctioned cloud services without the need to block them. It helps to 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).

It provides data protection capabilities to prevent data leakage from SaaS, IaaS, and web. It supports more than 1,000 file types, more than 3,000 data identifiers, proximity analysis, fingerprinting, exact match, OCR, and others. It can encrypt both structured and unstructured data in sanctioned services using AES-256 encryption and the use of on-premises HSM. It provides protection against malicious websites and block infected files. It included UEBA to identify anomalous user behaviour that could indicate compromised credentials, privileged account abuse, and data exfiltration. Netskope Security Cloud provides a best of breed DLP solution that is applicable to protecting data in the context of cloud services.

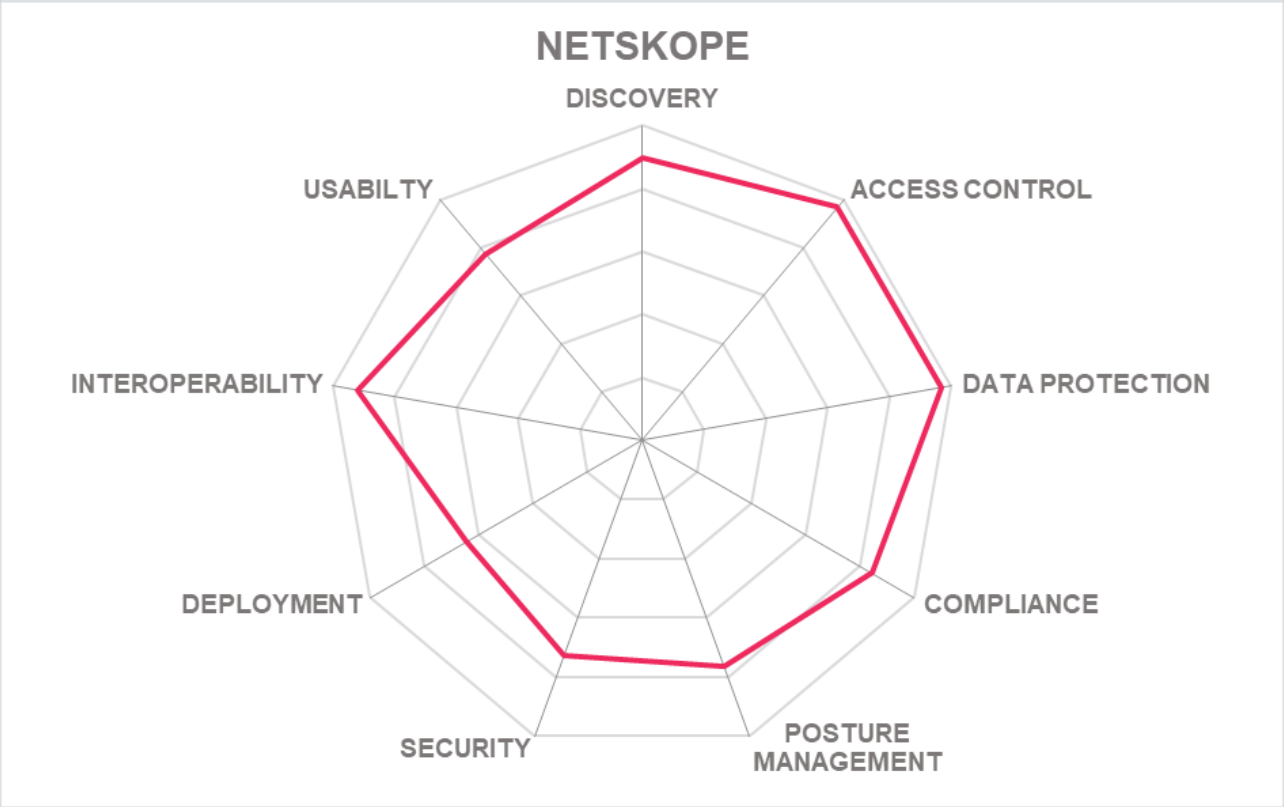
Security	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○
Discovery	●●●●●
Access Control	●●●●●
Data Protection	●●●●●
Compliance	●●●●●
Posture Management	●●●●○

Strengths

- Strong capabilities for discovery and control of cloud service usage.
- Flexible multi-modal deployment architecture.
- Enables granular control over unsanctioned as well as sanctioned cloud services.
- Visibility and control of cloud usage via managed and unmanaged devices
- Inline and API based visibility and controls.
- Strong inbuilt data leak prevention capabilities.
- Encryption of both structured and unstructured data.
- Provides fine grained control over social media use.
- Extensive compliance templates
- Covers a wide range of SaaS service.
- Enables the detection and control over IaaS administrators and data.

Challenges

- Less well known in Europe than in the US but is now deployed in many of the largest organizations in EMEA
- Complexity of different deployment options. However, Netskope offers several packages to provide our customers with the most common groupings of products.
- Needs deployment of the Advanced Threat Protection (vs. Standard) and Advanced DLP (vs. Standard)for best results.


NETSKOPE
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.10 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.

Oracle Cloud Infrastructure announced plans to replace CASB with a more integrated Cloud Guard service which was not GA at the time of this report writing but will be available in August.

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. It provides capabilities covering visibility, compliance, data protection, and threat prevention, across a range of enterprise Cloud Services including Oracle ERP Cloud, Oracle HCM Cloud and Oracle Sales Cloud. In addition, for customers adopting Oracle Cloud Infrastructure (OCI), Oracle CASB provides visibility, threat protection, data security and compliance for their OCI deployments.

Oracle's CASB solution integrates with existing solutions such as secure web gateways (SWG), next-generation firewalls (NGF), identity as a service (IDaaS), data loss prevention (DLP), and security information and event management (SIEM). Oracle current integrations include PAN, Fortinet, Check Point, Sophos, Okta, and Ping Identity. As well as providing posture management for OCI deployments it also covers IaaS services AWS and Azure. Oracle CASB leverages analytics and machine learning techniques to detect potential security issues. This includes User and Entity Behaviour Analytics (UEBA) to determine anomalies and risks. Oracle CASB provides built in incident management functionality. Additional integrations with incident management solutions such as ServiceNow are is also provided. Oracle CASB Cloud Service provides a unique approach to the governance and security of cloud usage that is likely to be attractive to customers using Oracle's products.

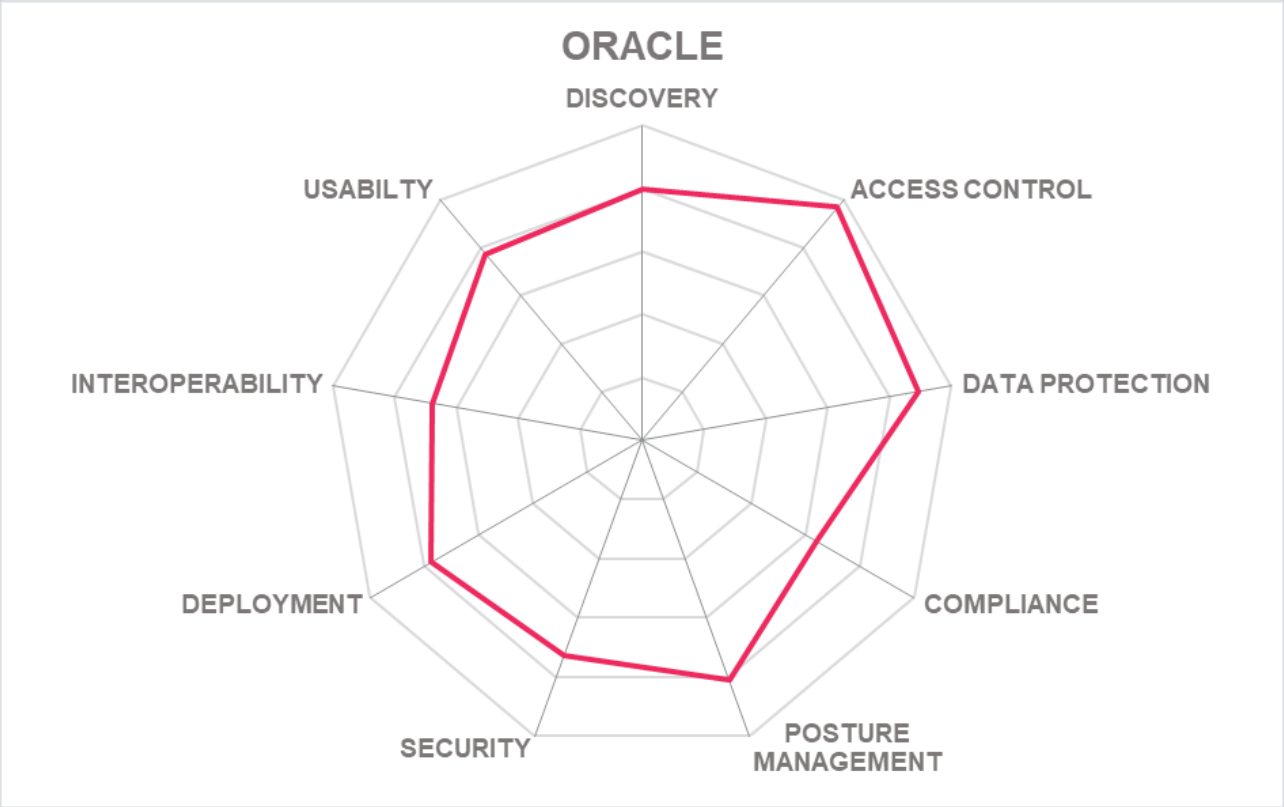
ORACLE®

Strengths

- Support for Oracle Public Cloud including Oracle Cloud Infrastructure, Oracle HCM Cloud, ERP Cloud, Oracle Sales Cloud.
- Integration with Oracle Identity Suite.
- Includes discovery of unmanaged SaaS apps.
- API level integration with manged apps provides fine grained controls.
- Covers IaaS including AWS and Azure as well as OCI.
- Autonomous threat detection and remediation using ML & UEBA.
- Integrated IRM capabilities plus advanced DLP including OCR support.
- Integration with Microsoft Azure Directory as well as other IDaaS.
- Integration with other vendors DLP and network gateways.
- Integration with SIEM.

Challenges

- No integration with on premises Active Directory.
- Lack of compliance policies / reports for common regulations out-of-the-box.
- No integrated malware / ransomware detection.


ORACLE
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.11 Palo Alto Networks

Palo Alto Networks Inc. is a cybersecurity company with a mission to protect our digital way of life through a comprehensive security approach in a world where everything, everywhere must establish trust. In 2015, Palo Alto Networks acquired CirroSecure which was then integrated into the Palo Alto Networks Security Operating. This has now been developed into the Prisma™ SaaS. Integrated with the in-line visibility and security capabilities of the Palo Alto Networks next-generation firewalls, the solution provides full multi-mode cloud access security broker (CASB) service that allows organizations to secure corporate SaaS applications and cloud data, and minimize the use of shadow IT. In 2018, Palo Alto Networks acquired Evident.io and RedLock and these have been developed into the Prisma™ Cloud security posture management offering. This report focusses on Prisma SaaS.

Prisma™ SaaS is a cloud service that allows organizations to govern sanctioned SaaS application usage across all their users. The service provides capabilities to discover and classify data stored across the supported SaaS applications, protect sensitive data from accidental exposure, identify and protect against known and unknown malware, and perform user activity monitoring to identify potential misuse or data exfiltration. It delivers visibility and granular enforcement across all user, folder, and file activity within sanctioned SaaS applications. Discovery and control of unsanctioned SaaS depends upon native integration with the in-line next-generation firewalls, available in any form factor (cloud, hardware or virtual).

Prisma SaaS connects to sanctioned SaaS application using the SaaS application's API. This allows the service to discover and scan all assets retroactively when first connected as well as to continuously monitor for threats. It scans and analyzes assets against policy to identify potential risks including exposures, external collaborators, risky user behavior, and sensitive documents. Embedded enterprise data loss prevention (DLP) service discovers, monitors, and protects sensitive data, such as Personally Identifiable Information (PII) and Intellectual Property (IP), from theft and loss. Both data in-motion and at-rest is discovered with a high degree of accuracy, and consistently protected across sanctioned and unsanctioned SaaS applications and public cloud, and everywhere else across all networks, branch offices and mobile users. The Prisma SaaS service also performs deep content inspection and protects assets from malware, data exposure, and data exfiltration. As the service identifies incidents, it is possible to define automated actions to eliminate or close the incident. It covers a wide range of SaaS out of the box and includes monitoring of AWS. In combination Palo Alto Networks' products provide a complete secure access service edge (SASE) solution and powerful approach to secure access to cloud services.

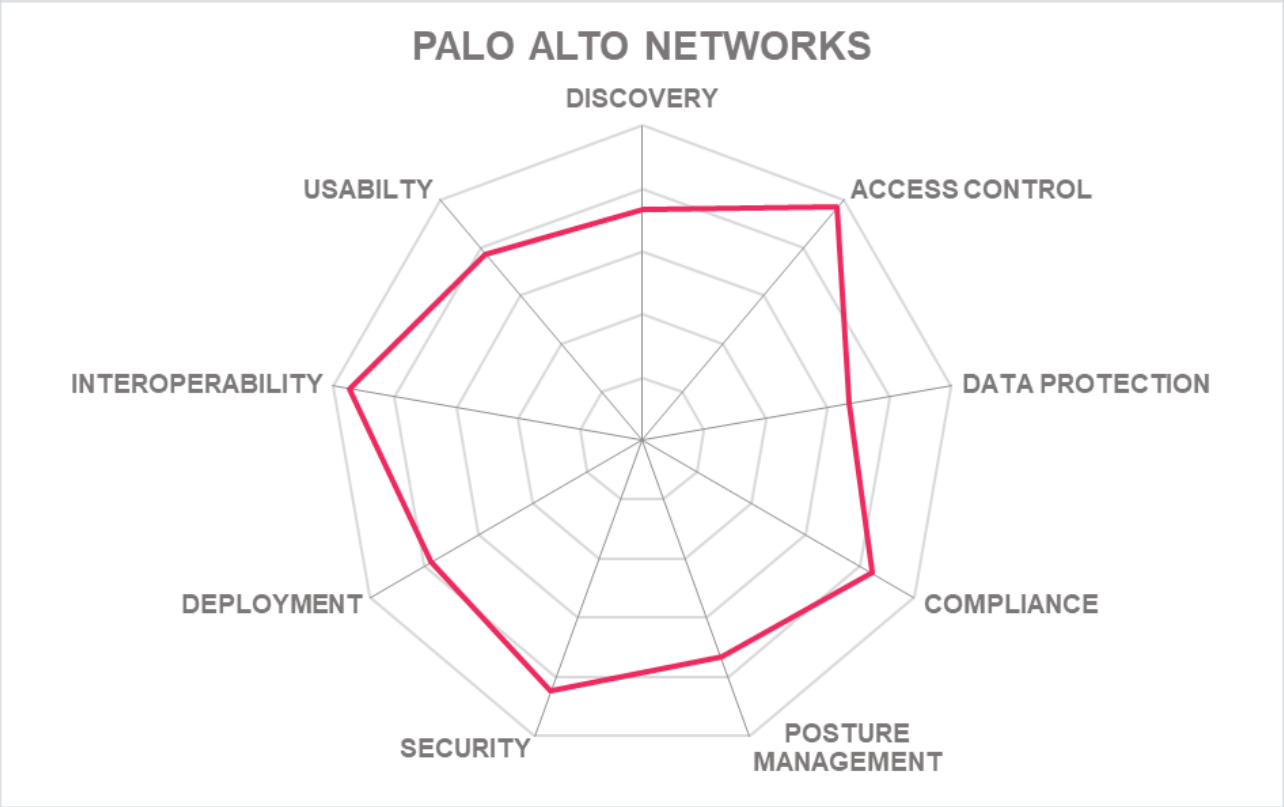
Security	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○
Discovery	●●●●○
Access Control	●●●●●
Data Protection	●●●●○
Compliance	●●●●●
Posture Management	●●●●○

Strengths

- Provides granular control over sanctioned apps through API level integration.
- Enterprise DLP service covers SaaS apps and consistently extends everywhere else.
- Deep discovery of assets held in SaaS apps.
- Assesses the shared or exposed data and identifies the potential risk and impact.
- Automates remediation of identified risks to data and assets.
- Assesses risks based on UEBA using machine learning.
- Provides policies to manage and restrict privileged user activity.
- Protects against risks arising from misconfigurations.
- Support for a wide range of SaaS apps.
- Integrates with other Palo Alto products.

Challenges

- Does not include inbuilt encryption capabilities for data protection.
- Depends upon integration with other Palo Alto Networks products for unmanaged app discovery.
- Separate consoles for in-line protection and at-rest SaaS security.


PALO ALTO NETWORKS
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.12 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. This report covers the Proofpoint Cloud App Security Broker (CASB).

Proofpoint CASB takes a unique “people centric” approach to protect users from cloud threats, safeguard sensitive data, and helps to discover shadow IT as well as govern cloud and third-party OAuth apps. The people centric approach is intended to provide visibility into email and cloud threats to help to identify what Proofpoint term as Very Attacked People™ (VAPs) and so to protect their cloud accounts and data. Proofpoint CASB uses analytics and provides adaptive controls to help to grant the right levels of access to users and third-party OAuth apps based on risk factors tailored to the organization’s needs. 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.

Proofpoint CASB shares DLP classifiers with other Proofpoint to accelerate the identification and protection of sensitive data. It enables consistent DLP policies across cloud apps (SaaS, IaaS, and mailboxes), email, web, and on-premises file repositories. More than 240 built-in classifiers cover regulations such as PCI, PII, PHI and GDPR. It helps to protect data at risk by identifying broad file permissions and unauthorized data sharing. It enables the correlation of suspicious logins or misconfigured AWS S3 buckets with DLP incidents. Policies can be created to quarantine data or stop unauthorized uploading/downloading of data through browser isolation. 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 such as malicious OAuth apps.

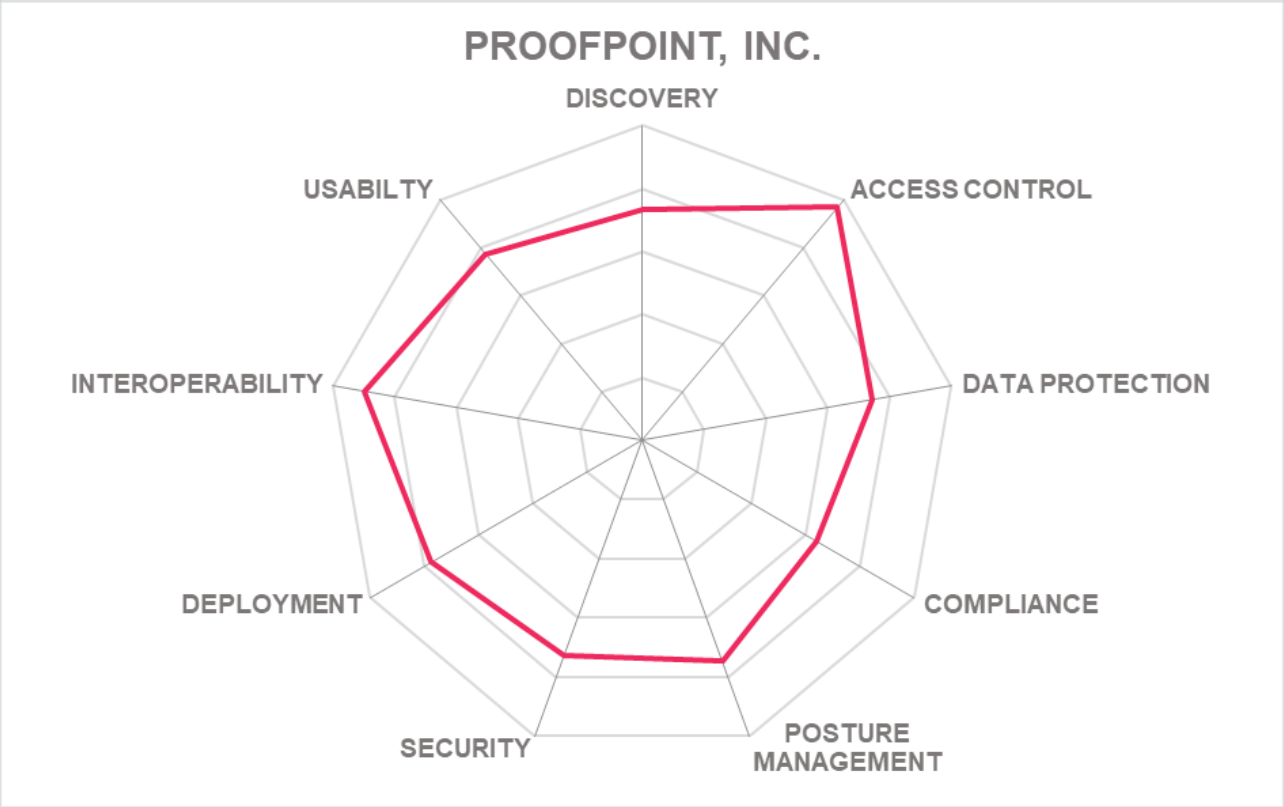
Security	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○
Discovery	●●●●○
Access Control	●●●●●
Data Protection	●●●●○
Compliance	●●●●○
Posture Management	●●●●○

Strengths

- People-centric protection for sanctioned cloud apps.
- Identifies people at risk of attack and provides the ability to provide these with extra protection.
- API based approach provides fine grained controls for sanctioned apps.
- SAML based approach with risk based adaptive authentication.
- Shadow IT discovery and risk assessment using a catalogue of 46,000 applications with more than 50 attributes per app.
- Integration with other Proofpoint products.
- Includes controls over OAuth based authentication risks, including malicious OAuth apps.
- Strong DLP capabilities and templates including real-time data controls and unified incident management and compliance reporting across cloud apps and email.
- Support for Azure and AWS account and resource discovery, controls over IaaS administrators and bucket permissions, and cloud security posture management.

Challenges

- Does not provide inbuilt encryption of sensitive data.
- Less capabilities for shadow IT discovery and risk assessment than other vendors.
- Less compliance-oriented reports out-of-the-box than other vendors.
- Limited coverage of IaaS services and resources.


PROOFPOINT, INC.
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

5.13 Symantec

In November 2019, Broadcom also acquired Symantec and it now continues to market products under the Symantec brand. This report covers Symantec CloudSOC which integrates with other Symantec products to provide a comprehensive CASB solution. Symantec CloudSOC provides comprehensive CASB functionality through intelligent integration with other Symantec products.

Symantec CloudSOC CASB monitors and controls use of sanctioned SaaS platforms such as Office 365, G-Suite, Box, Dropbox, Salesforce, and more through API integrations and in-line traffic analysis. It can identify risky SaaS, PaaS, and IaaS cloud apps and mobile apps being used based on hundreds of customisable security attributes. It identifies the employees using these services, as well as how much they are being used. It can block access to unapproved cloud services while allowing access ones that meet specific security guidelines. CloudSOC offers a range of deployment options that can leverage unified authentication, integrated endpoint options, agentless solutions, integrated web security, proxy chaining, shared intelligence, unified policy management, between CloudSOC and integrated Symantec DLP, authentication, encryption, threat protection, and secure web gateway solutions.

It identifies a wide range of sensitive data including PII, PCI, PHI, and source code that is at risk through user activity and enables policy controls to prevent data loss. It exploits machine-learning, predefined and customer dictionaries, and learned profiles for accurate data-matching. CloudSOC User Behaviour Analytics (UBA) leverages intelligence from APIs via StreamIQ and machine learning to maintain individualized user profiles, map user activity, and compile a live user ThreatScore. It enforces policies inline and using APIs based on the ThreatScore, and abnormal user behaviour to prevent data exposures and control access. It enables the enforcement of policies governing how sensitive and regulated data is stored, shared, and accessed in the cloud. It can protect regulated data with integrated encryption and multi-factor user authentication. Additionally, Symantec Cloud Workload Assurance provides a cloud security posture management solution for public cloud infrastructure-as-a-service (IaaS) platforms, including AWS and Microsoft Azure.

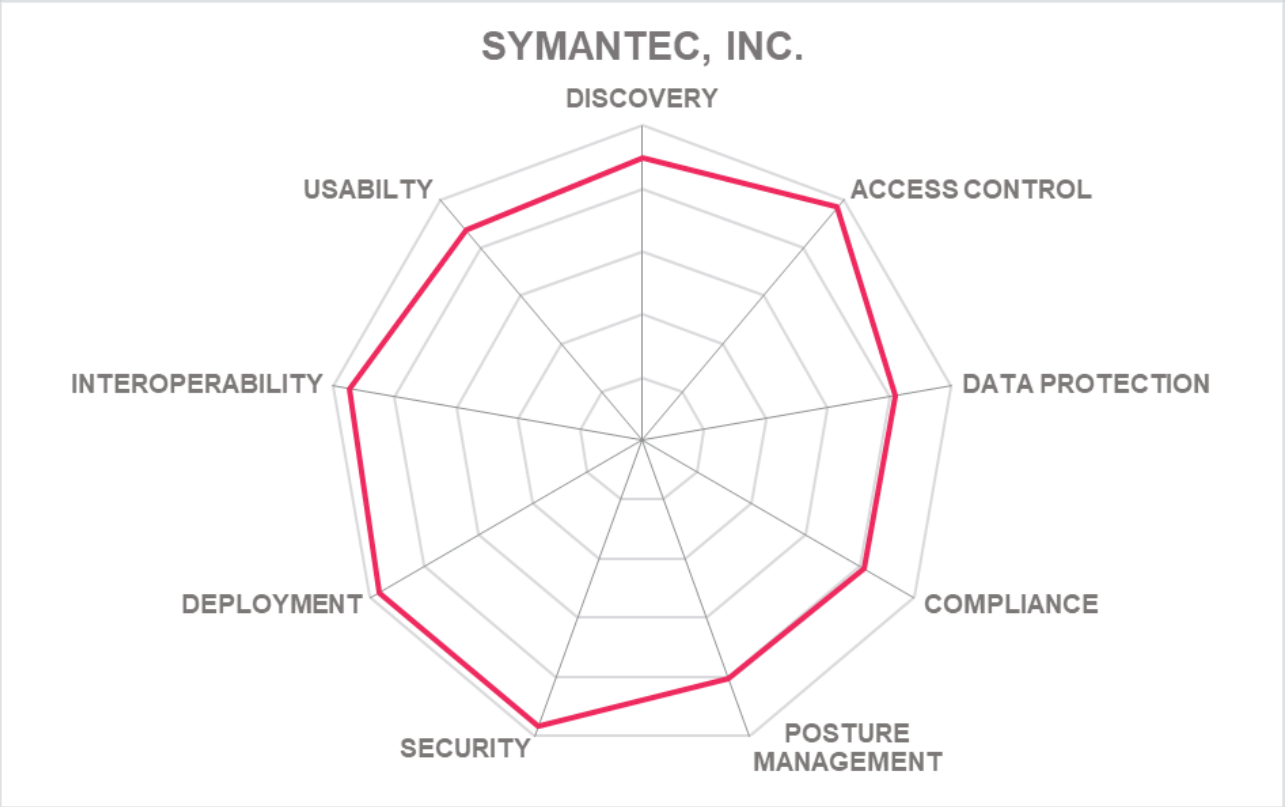
Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Discovery	● ● ● ● ●
Discovery	● ● ● ● ●
Access Control	● ● ● ● ●
Data Protection	● ● ● ● ●
Compliance	● ● ● ● ●
Posture Management	● ● ● ● ●

Strengths

- Broad and deep coverage of a wide range of cloud apps.
- Wide choice of deployment options.
- Shadow IT analysis for both on-network and off-network users via integration with Symantec Secure Web Gateway.
- Data governance, DLP, malware scanning and encryption in real-time for cloud application traffic.
- Field-level and file-level tokenization and encryption of data without impacting functionality of the cloud app.
- Exploits machine learning for UBA, DLP and risk analysis.
- User account protection through adaptive authentication and UBA.
- Malware protection based on Symantec Threat Intelligence and technologies.
- Powerful features enabled through integration with other Symantec products.

Challenges

- Full functionality depends upon the deployment of multiple options.
- Integration with on-premises apps.
- Integration with traditional access governance tools for SoD, entitlement attestation, etc.
- Uncertainties regarding future strategy following the acquisition by Broadcom.


SYMANTEC, INC.
DISCOVERY
ACCESS CONTROL
DATA PROTECTION
COMPLIANCE
POSTURE MANAGEMENT
SECURITY
DEPLOYMENT
INTEROPERABILITY
USABILTY

6 Related Research

Advisory Note: KRIs and KPI for Cyber Security - 80239
Architecture Blueprint: Identity and Access Management - 72550
Leadership Brief: Privileged Account Management Considerations - 72016
Leadership Brief: Identity Fabrics – Connecting Anyone to Every Services – 80204
Architecture Blueprint: Hybrid Cloud Security - 72552
Advisory Note: Maturity Level Matrix for Cyber Security - 72555
Advisory Note: GRC Reference Architecture - 72582
Advisory Note: Protect Your Cloud Against Hacks and Industrial Espionage - 72570
Advisory Note: Security Organization Governance and the Cloud - 72564
Advisory Note: Cloud Services and Security - 72561
Advisory Note: How to Assure Cloud Services - 72563
Advisory Note: Firewalls Are Dead - How to Build a Resilient, Defendable Network - 72163
Architecture Blueprint: Access Governance and Privilege Management - 79045
Architecture Blueprint: Identity and Access Management - 72550
Leadership Compass: Identity as a Service (IDaaS) IGA – 80051
Leadership Compass: Identity Governance & Administration – 80063
Leadership Compass: Identity Provisioning - 71139

Endnotes

1 https://docs.microsoft.com/en-us/office365/troubleshoot/miscellaneous/office-365-third-party-network-devices

Methodology

About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.

While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices 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.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates 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 on 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
- Ease of Delivery
- Interoperability
- Usability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and

the way the vendor deals with them.

Ease of Delivery is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, 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 the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are

- **Strong positive**
  Outstanding support for the subject area, e.g. product functionality, or security etc.)
- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an

example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

- **Neutral**
  Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren't met, while others are well served.

- **Weak**
  Below-average capabilities in the area considered.

- **Critical**
  Major weaknesses in various areas.

Content of Figures

Figure 1: CASB Overview

Figure 2: CASB Market Trend Compass

Figure 3: Featured for Innovation

Figure 4: Featured for Access Governance

Figure 5: Featured for Integration

Figure 6: Featured for Integrated Data Security

Figure 7: Featured for Custom Apps

Copyright

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 back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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