AN INTEGRATED CASB IMPLEMENTATION MODEL TO ENHANCE ENTERPRISE CLOUD SECURITY

Co-authored by

Rajat Wason, Shaun Aghili, Pavol Zavarsky

Information Systems Security Management

Concordia University of Edmonton

Project Report

Submitted to the Faculty of Graduate Studies,

Concordia University of Edmonton

In Partial Fulfillment of the

Requirements for the Final

Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

Faculty of Graduate Studies

Edmonton, Alberta

April, 2020

AN INTEGRATED CASB IMPLEMENTATION MODEL TO ENHANCE ENTERPRISE CLOUD SECURITY

Rajat Wason

Approved:

Shaun Aghili [Original Approval on File]
Shaun Aghili   Date: April 20, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci   Date: April 20, 2020

Dean, Faculty of Graduate Studies

Abstract

Enterprises are migrating towards cloud solutions for every possible business function. The obvious reason for this paradigm shift is that cloud technology allows enterprises to have more agile, scalable and reliable cloud services available to their employees and customers at all times. Due to the adoption of cloud services, enterprises are facing an upsurge in cloud related threats. Use of cloud technologies takes away the much needed control and visibility into the cloud network. This leaves enterprises at risk with regard to data security and compliance. In order to deal with the security concerns raised from cloud usage, enterprises are looking for highly effective security controls such as Cloud Access Security Broker (CASB). The research done in this paper aims to provide a CASB implementation model that helps enterprises in the deployment of CASB in their existing security mechanism, integrated with other security controls that deliver enhanced visibility into the cloud usage, dynamic control over cloud services use and uses machine learning based user and entity behavior analysis to provide protection against threats. In this paper, CASB solutions from the top vendors are compared to identify the strengths and weaknesses of each solution and a list of features/functions is provided that every CASB solution should possess to fit the security needs of all enterprises. The paper also rationalizes the efficacy of the CASB solution by providing protection against the top threats to cloud computing.

Keywords: Cloud Access Security Broker, User and Entity Behavior Analysis

Introduction

In March 2019, one of the biggest data breaches occurred when a hacker gained access to Capital One’s server to expose the personal information of more than 100 million of its customers. The data breach disclosed sensitive information like social security numbers, social insurance numbers, bank account numbers, credit scores, credit limits, balances, etc. Capital One stored the data on the server which was hosted on amazon web services (AWS), to which the hacker gained access by targeting a misconfigured firewall (Mclean, 2019). In 2017, another attack on the financial sector was witnessed when attackers managed to exploit a vulnerability in the Apache Struts server hosting Equifax’s online dispute portal. According to a report from the United States Government Accountability Office, the attackers managed to gain access to 51 databases over a time period of 76 days and extracted personally identifiable information (PII) of at least 145.5 million individuals. These incidents have raised doubts about the security of loads of information that different organizations store.

Recent trends show that organizations are now more open to cloud solutions than before. According to the 2018 IDG Cloud Computing Study, 77% of the enterprises have at least one application or a portion of their enterprise computing infrastructure in the cloud. Cloud technology has IT solutions for all, from small to large enterprises and from the public to personal computing. But the security of the cloud environment is a major concern. The shift in the technology landscape has made conventional security controls inefficient. There is a strict need to look beyond the usual security measures to modern security solutions that provide more visibility and better control into the usage of cloud services. Cloud hosts a wide variety of services (may or may not be known to Enterprise

IT) which are accessed from a large number of devices (may or may not be managed by Enterprise IT). This makes securing cloud services and the data very challenging. To deal with this problem, enterprises are required to have better control over cloud usage; continuous monitoring and policy enforcement are required to safeguard users, data and cloud applications from being compromised.

Cloud access security brokers, identity federation platforms, etc. are the security tools that the organizations are adopting to help centralize control in the cloud environment (Shackleford, 2019). According to the SANS Cloud Security Survey 2019, about 35% of organizations are using CASBs to centralize user access and identity, enforce policy at the granular level, monitor user-activity and protect data. By 2020, 85% of large enterprises will use a cloud access security broker platform to secure their cloud services (Gartner, 2015). CASB is a multi-functional cloud security solution that can be used with other security components for enhanced security.

In this research paper, a detailed study of CASB is done to explore the various security features that CASB offers. The study done in this paper shows how CASB can integrate with the existing security controls of an enterprise and complement the functionality of the security controls. The purpose of this research is to propose a fully integrated, artificial intelligence (AI) driven cloud access security broker implementation model that enhances enterprise cloud security.

The organization of this paper is as follows: the introduction section briefs about the recent data breaches due to shaky cloud environment and briefly describes the challenged faced by the use of cloud services in enterprises and how the use of CASB can be an effective solution. The literature review includes the top threats related to cloud computing, introduction to cloud access security brokers (CASB), features provided by CASB, various CASB deployment modes, a detailed comparison of CASB solutions from the leaders of the industry, key CASB integrations with the other security controls in the enterprise, and the use of machine learning heuristics for user behavior analysis. In the methodology section, the scope, research questions, procedures, and limitations are discussed. The presentation of the results section introduces and discusses the final research deliverable. The research paper concludes with a discussion of final conclusions and considerations, including recommendations for further studies of the exploratory and theoretical framework presented in this paper.

Literature Review on Broker based Cloud Security

Cloud solutions are cost-effective, easily accessible and scalable still, there are persistent security issues in the cloud. Cloud technology is very dynamic in nature and traditional security approaches and tools are not enough to provide security to it. There is a need to think beyond just firewalls and IDPS systems and bring in advanced and intelligent security mechanisms to keep up with the current security threats (Garbis & Koilpillai, 2019). Cloud broker is one such mechanism that plays a vital role in protecting the cloud data and its consumers. Cloud security is based on the shared-responsibility model in which both consumers and CSPs have their own set of responsibilities. In the SaaS platform, the CSPs are responsible for securing the application and the underlying infrastructure while the consumer is responsible for securing the contents and usage of the application by configuring its security settings (Obregon, 2017). For large enterprises, using cloud applications to serve their business requirements, secure access to cloud services is a big challenge. The simple reason behind this is that the number of users is very large and the number of cloud applications (known and unknown to the enterprise IT) used is on the high side as well. It becomes very important to track and monitor user activity, discover the use of unknown cloud services (shadow IT), enforce granular level access control policies, etc. CASB is a cloud security solution capable of meeting enterprise requirements to secure the use of cloud services by its users.

Challenges Faced by Enterprises to Secure Cloud Applications

Despite the benefits that the cloud offers to its consumers, the security of data is still a major concern for enterprises. McAfee’s 2019 Cloud Adoption and Risk Report says that the compromised accounts and insider threats are the major threats to the security of data in the cloud (McAfee, 2019). Stolen credentials of the cloud services is another major threat, as per the report. In this section of the paper, major security concerns related to the enterprise’s cloud environment are discussed.

According to Shackleford (2017), enterprises are using cloud technologies to store sensitive data like personally identifiable information (PII), health records, and financial records. Security professionals believe the sensitive data stored in the cloud environment is exposed to many security threats. In 2016, the Cloud Security Alliance (CSA) identified the top threats to cloud security in the report “The Treacherous 12 - Cloud Computing Top Threats in 2016”. Some of the major security issues to enterprise cloud security as per the report are as follows (Cloud Security Alliance, 2016):

- Data Breaches: Data breach is unauthorized access to an organization’s sensitive, protected or confidential data. A data breach may occur as a result of a targeted attack on the cloud environment, human error, misconfiguration or poor security practices being followed in the organization. A data breach may reveal loads of sensitive information that is not intended for public release.

- Weak Identity, Credential, and Access Management: A weak Identity and Access Management (IAM) system could lead to data breaches and other attacks launched on the cloud infrastructure. Strong password policies, multi-factor authentication, enterprise-wide security awareness and robust public key infrastructure (PKI) are required to prevent against this type of threat.
- Insecure APIs: Cloud consumers make use of application programming interfaces (APIs) to communicate with cloud applications. Provisioning, management, orchestration, and monitoring are all performed with these interfaces. If the APIs are insecure, they can be exploited by the attackers to compromise the application.
- System Vulnerabilities: The bugs in the program that can be exploited by the attackers with the intent to steal data, gain unauthorized access to the system, or bringing the services down. Vulnerable operating systems, system libraries and applications put the security of the services and data at risk.
- Account Hijacking: Account hijacking starts with stolen credentials. Attackers use techniques like phishing, social engineering, exploitation of system vulnerabilities, etc. to steal the login details and gain unauthorized access to the cloud service. Eavesdropping, manipulation, and deletion of data are some activities that can be performed by the attacker after gaining access through account hijacking. Account hijacking is used by the attacker to use an authorized

account to access cloud services, in order to steal data or disrupt cloud services running.

- Malicious Insiders: Malicious insiders are the employees of the organization who try to misuse their authority for personal gain or as vengeance against the company. They have direct access to the organization’s resources like network, system, data, etc. But they misuse the access provided, against the organization to compromise the security of the information systems.
- Advanced Persistent Threats: APTs are the threat actors that function over a course of time and steadily take hold of the enterprise's IT infrastructure to infiltrate data and intellectual property.
- Data Loss: Data stored in the cloud can be lost accidentally by human error, system crashing, or environmental hazards. If there is no data recovery mechanism in place, data will be lost permanently which can lead to a huge financial and reputational impact on enterprises.
- Abuse and Nefarious Use of Cloud Services: The features of cloud technology like easy accessibility can sometimes go against it as well. For example, SaaS applications can be accessed by users from anywhere or from their own devices if proper controls are not in place. This way users can infiltrate the sensitive enterprise data without being getting noticed.
- Denial of Service (DoS): With Denial of Service attack, attackers prevent authentic users from using cloud services. Cloud computing is based on resource pooling, where each resource serves one user request. Attackers may exhaust the resources available for legitimate users, resulting in Denial of Service.

- Shared Technology Threats: Cloud services are offered by sharing infrastructure, platform, and applications to multiple end-users. By compromising a single user in the cloud network, the entire cloud network can be affected at once. A single vulnerability of any component may lead to the exploitation of the entire cloud infrastructure.

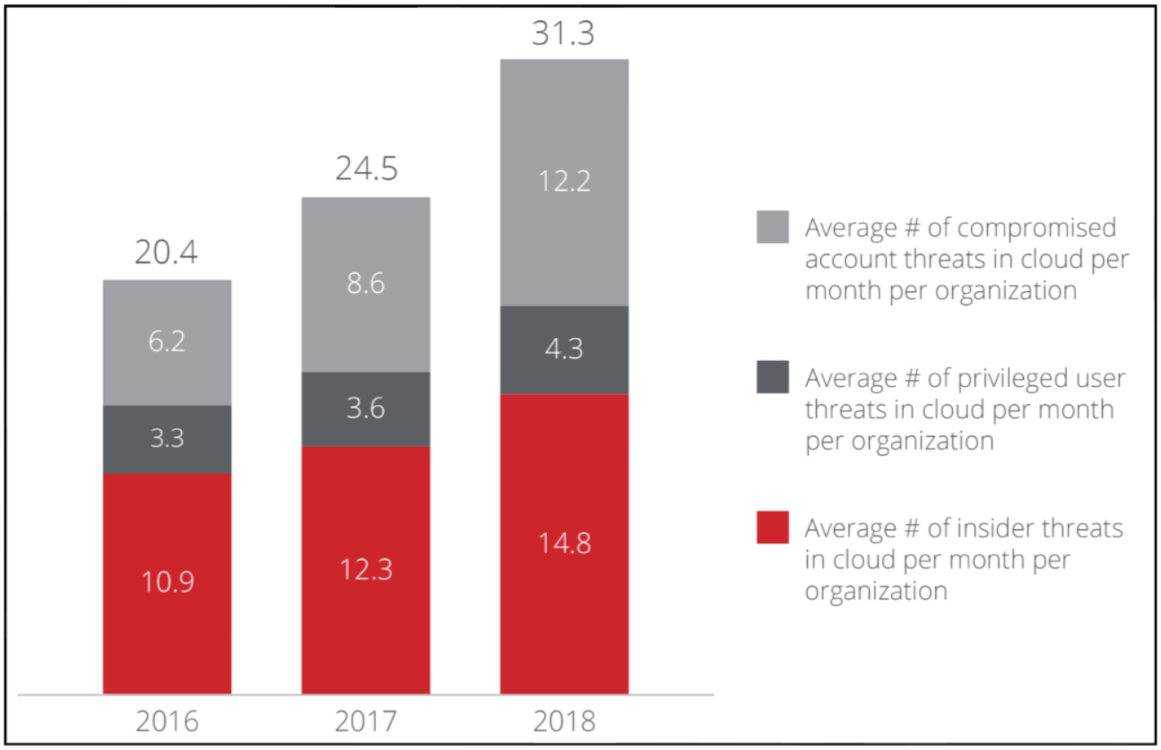


Figure 1. Cloud threats by category. Adapted from McAfee's "Cloud Adoption and Risk Report 2019"

The amount of sensitive data an enterprise stores on the cloud remains on the higher side, despite concerns about the security of this data in the cloud. It becomes very important for security teams to control user access and manage cloud service usage. But with the number of users in the enterprise and many different cloud applications in use, the monitoring and control of user access to these services becomes very complex (Shackleford, 2017). A Cloud Access Security Broker (CASB) is one such security solution that enterprises are looking up to protect themselves from threats related to cloud services usage. In the next section of this paper, CASB is defined in detail, along with its deployment modes and the functionalities it provides in each mode.

What is Cloud Access Security Broker (CASB)?

Gartner defines cloud access security broker (CASB) as an on-premises, cloud-based security enforcement point that sits between the cloud consumer and cloud service providers to implement the enterprise security policies on cloud services being accessed by the cloud consumer. The security policies that a CASB can implement include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention, etc. (Gartner, 2016).

Cloud service broker serves as an intermediary between cloud consumers and cloud providers. It assists enterprises in choosing services and offerings that best suit their needs (Surianarayanan & Chelliah, 2019, p.268). Enterprises use CASB to enhance visibility into the authorized and unauthorized use of cloud services, disclose noncompliance regulations, ensure secure data storage in the cloud and provide protection against the threats. Earlier CASB solutions or first-generation CASBs tend to provide security only to the data at rest, while the second-generation CASBs possess extended capabilities that provide a better insight into application traffic as well (Symantec, n.d.). CASB is an effective strategy in mitigating threats in the cloud, and its effectiveness can be increased by integrating it with other security controls, like Security Information and Event Management (SIEM), firewalls, Data Loss Prevention (DLP), endpoint management, encryption and authentication (ISACA, 2018). CASBs are highly customizable, and its implementation and integration with other security controls in the cloud network depend on the enterprise cloud security requirements.

CASB deployment modes.

The common deployment modes which can be used to deploy a CASB are as follows (Obregon, 2019):

- Log Collection: CASB's deployment in log collection mode is the easiest to set up. In this mode, user activity is logged to track the use of cloud services. Using firewalls and secure web gateways event logs are generated which are collected using a connector server. The collected logs are normalized, which are then forwarded to the CASB. Normalization helps in better analysis of the logs collected by CASB. CASB deployed in log collection mode supplement the functioning of Security Information and Event Management (SIEM).

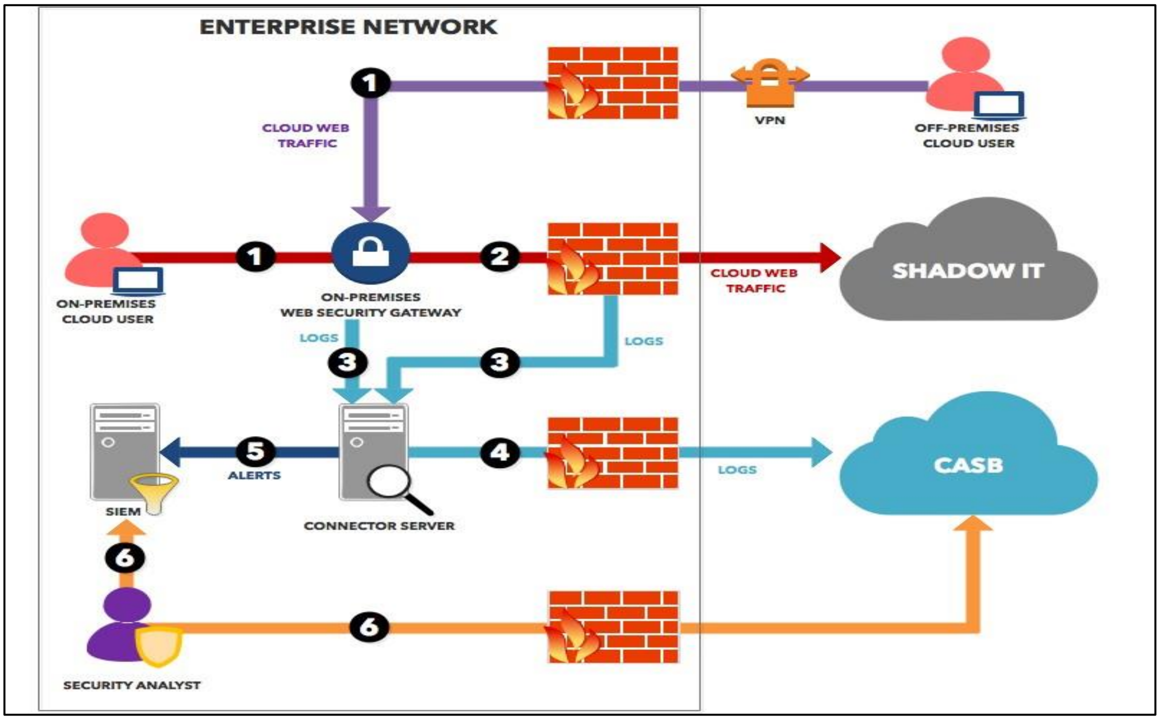
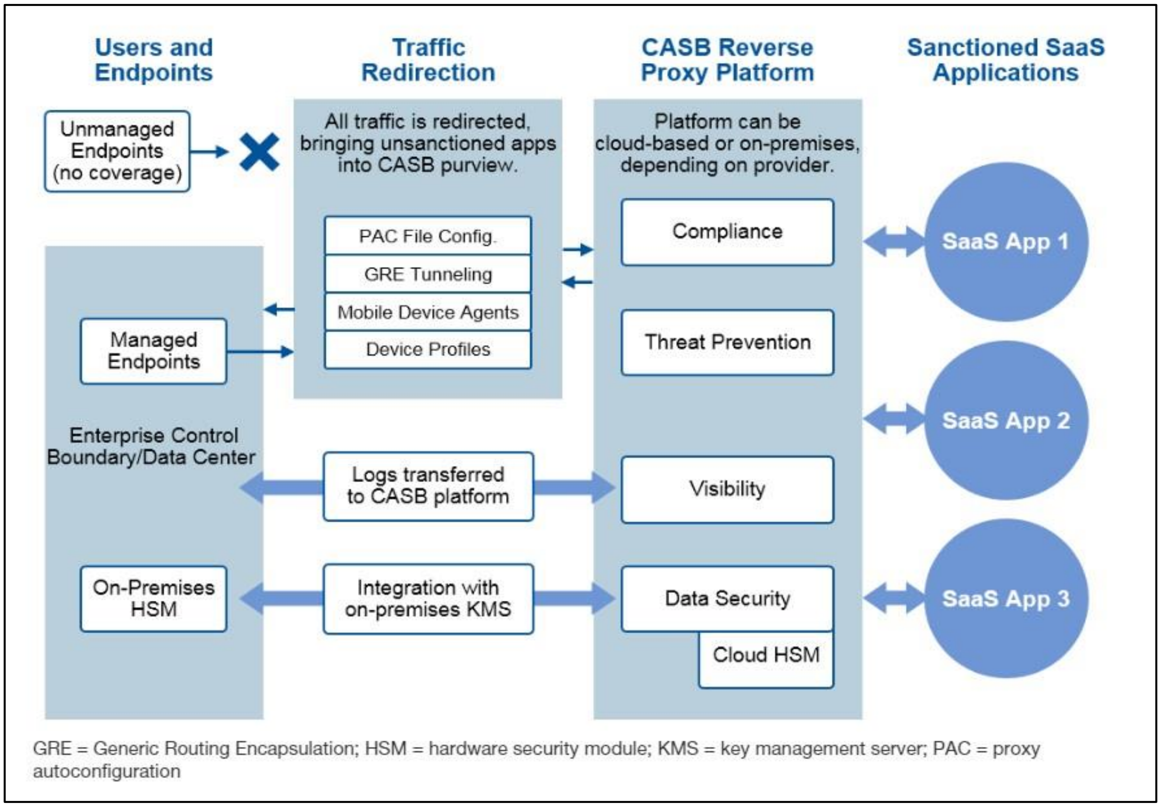


Figure 2. Log Collection Deployment Mode (Obregon, 2017)

- Forward Proxy: A CASB in the forward proxy deployment mode helps in proxying the user traffic to the cloud services providing more visibility into the cloud network and supporting the implementation of cloud access policies for the cloud consumers. There are two ways in which the forward proxy can be implemented. First, the enterprise's web security gateways could be configured to route all the outbound traffic to the end-user through the CASB. Another way of implementing forward proxy is to configure end-user devices with the endpoint security agent that routes all web traffic towards the CASB.


Users and Endpoints
Traffic Redirection
CASB Reverse Proxy Platform
Sanctioned SaaS Applications
Unmanaged Endpoints (no coverage)
All traffic is redirected, bringing unsanctioned apps into CASB purview.
Platform can be cloud-based or on-premises, depending on provider.
PAC File Config.
GRE Tunneling
Mobile Device Agents
Device Profiles
Compliance
Threat Prevention
SaaS App 1
SaaS App 2
SaaS App 3
Managed Endpoints
Enterprise Control Boundary/Data Center
Logs transferred to CASB platform
Visibility
On-Premises HSM
Integration with on-premises KMS
Data Security
Cloud HSM

GRE = Generic Routing Encapsulation; HSM = hardware security module; KMS = key management server; PAC = proxy autoconfiguration

Figure 3. Forward Proxy Model (Gartner, 2015)

- Reverse Proxy: CASBs are deployed in reverse proxy mode to implement access policies for specific sanctioned cloud services. Traffic to and from the specified cloud services is passed through the CASB in order to enhance the visibility in the network and monitor traffic for the sanctioned cloud services. Reverse proxy deployment mode for CASB is easier to implement as compared to the forward proxy as there is no need to configure special devices to direct the traffic towards CASB. However, Identity and Access Management platform is required since the traffic generated from an authenticated user only is forwarded to the sanctioned cloud service.

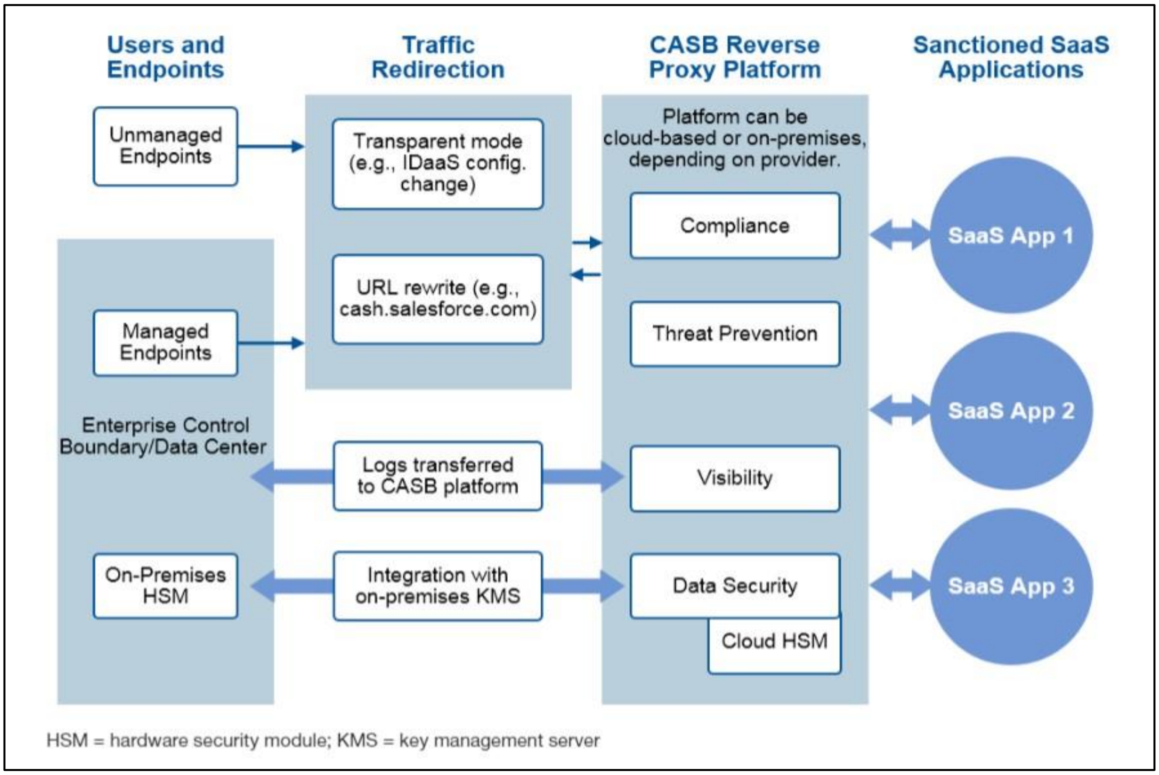

Users and Endpoints
Traffic Redirection
CASB Reverse Proxy Platform
Sanctioned SaaS Applications
Unmanaged Endpoints
Transparent mode (e.g., IDaaS config. change)
Platform can be cloud-based or on-premises, depending on provider.
Compliance
SaaS App 1
URL rewrite (e.g., cash.salesforce.com)
Threat Prevention
Managed Endpoints
SaaS App 2
Enterprise Control Boundary/Data Center
Logs transferred to CASB platform
Visibility
On-Premises HSM
Integration with on-premises KMS
Data Security
SaaS App 3
Cloud HSM
HSM = hardware security module; KMS = key management server

Figure 4. Reverse Proxy Mode (Gartner, 2015)

- API: The CASB deployment modes mentioned above are all inline deployments. API is another possible CASB deployment mode that is better than the inline deployment modes (log collection, forward proxy, reverse proxy) in a way that does not obstruct the network passage by sitting in the network between end-user and the cloud service provider. API collects the traffic by establishing an

API connection between the CASB and the CSP. One limitation of the API based CASB deployment model is that not every cloud application supports API integration.

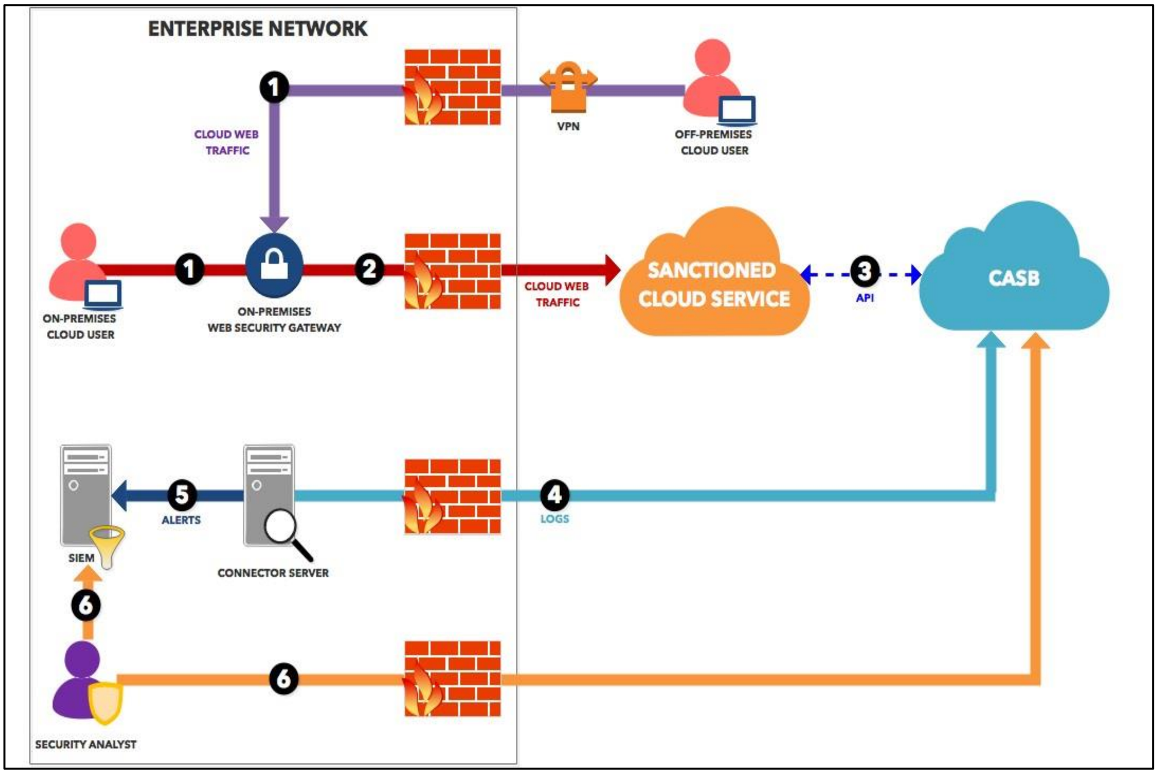


Figure 5. API Mode (Obregon, 2017)

- Hybrid: In Hybrid mode, CASB is deployed in a combination of proxy mode and API mode to analyze application data and network traffic at the same time. CASB deployed in hybrid mode support much more use cases in terms of increasing visibility, policy enforcement and integration with other security components (Friedman & Bouchard, n.d.).

In the cloud architecture, CASBs play an important role to bridge the gaps in enterprise cloud security. CASB makes use of APIs to provide secure means to access different cloud applications without any overhead on the network. Garbis et al. (2019) state that CASB operates at the Application Layer (Layer 7) of the TCP/IP model, to examine the application traffic. Therefore, CASBs can protect against threats like exfiltration of data, privilege escalation, etc. The features that any CASB can provide depends not only on its vendor but also on its deployment. Not every security feature is feasible in every CASB deployment (McAfee, n.d.). The functions of a CASB in the different deployment modes are provided in the Appendix.

There are four pillars through which CASB provides their functionality, which is as follows (McAfee, n.d.):

- Visibility provides continuous monitoring of user activity on sanctioned cloud services and identifies the Shadow IT services being used within an enterprise.
- Compliance and regulatory requirements like HIPAA, PCI-DSS, etc. are met by enforcing data loss prevention (DLP) policies and integration policies in a multi-cloud environment.
- Data Security protects sensitive data from leakage by providing data-centric security which includes access control policies, encryption key management, tokenization, and authorization.
- Threat Protection detects and analyzes suspicious traffic to provide protection against insider threats, privileged user threats and compromised user accounts. Using behavioral analysis, anomalies in the user activity and network traffic are found which provides protection against the user threats.

Study of Top CASB Solutions

According to the 2019 Gartner's Magic Quadrant for Cloud Access Security Broker, organizations are looking at CASB as a cloud security solution at an increasing pace. CASB is effective in identifying security gaps in the usage of cloud services. CASB has capabilities which traditional security controls like web application firewalls (WAFs), secure web gateways (SWGs) and enterprise firewall could not offer individually. CASB provides a centralized mechanism for policy control, governance, and visibility into cloud usage across multi-cloud platforms.

The leaders of the CASB industry are Microsoft, McAfee, Netskope, Symantec and Bitglass according to the 2019 Gartner's Magic Quadrant for Cloud Access Security Broker. In this report, the leaders are considered to possess all CASB capabilities and deployment options that cover a wide variety of cloud services. In the next section, the top three CASB solutions according to Gartner's report: Microsoft Cloud App Security (MCAS), McAfee MVISION, Symantec CloudSOC, and Netskope are discussed and their strengths and weaknesses are compared.

Microsoft Cloud App Security.

According to the Gartner's Magic Quadrant for CASB 2019, Microsoft entered into the CASB market in 2015, with the acquisition of Adallom, which has been providing CASB solutions since early 2013. Microsoft avails MCAS as a standalone CASB and as a part of the Enterprise Mobility + Security (EMS) E5 suite. Microsoft has also included MCAS in its Microsoft 365 E5 bundle. MCAS on its own provides features to each of the four pillars of CASB, but when it is used in any probable combination with the EMS suites, its functionalities multiply. This makes MCAS a preferred CASB solution to the enterprises of all sizes and even to the individual users. MCAS supports multiple deployment modes like API, forward proxy, reverse proxy, and log collection. MCAS is now capable of providing real-time inspection by reverse proxying Office 365 traffic.

Microsoft Cloud App Security provides a security solution which is based on integrations with existing security solutions to enhance the security and control over the cloud network. MCAS is capable of collecting logs from different sources such as firewalls, SIEM, secure web gateways, etc. MCAS integrates seamlessly with the Microsoft native solutions to provide better control and visibility. The other components with which MCAS can be easily integrated are Identity & Access Management (IAM), Incident Response, Data Loss Prevention, Cloud Security Posture Management, Unified Endpoint Management, etc.

McAfee MVISION cloud.

McAfee entered the CASB industry with the acquisition of Skyhigh Networks in 2018 (Gartner, 2019). The CASB is now known as McAfee MVISION Cloud. McAfee's CASB discovers the usage of Shadow IT in enterprises with enhanced visibility into the cloud environment. It provides protection against threats to cloud security and prevents data loss from cloud usage. The product has developed to provide coverage to all four CASB pillars in addition to security controls like encryption, tokenization, DLP engine, etc. (Gartner, 2019). This CASB is very popular in sectors which have a high internal policy and compliance requirements. For example, finance, health industry, and government organizations rely on MVISION Cloud for their enterprise's client security requirements (Rubens, 2019).

Netskope for SaaS.

Netskope is one of the earliest vendors that came up with the commercial CASB in 2013. It has well-developed behavior analytics and alerting system to monitor the usage of managed and unmanaged SaaS applications (Gartner, 2019). Netskope supports the implementation modes such as API, forward and reverse proxy, but forward proxy and API inspection mode are commonly used. Cloud traffic is passed to the Netskope's cloud using a proxy chaining mechanism. Inline proxy and API's are used to deeply analyze content for malware detection. Netskope's services are API enabled that helps easy and strong integration with other security measures (Gartner, 2019).

Symantec CloudSOC.

In 2016, Symantec acquired two CASB solutions from Blue Coat Systems, these are Perspecsys and Elastica. The merger of these two CASBs is known as CloudSOC which is now Symantec's CASB product (Rubens, 2019). Symantec CloudSOC is a multimode CASB whose high-level functions include:

- Cloud app visibility to discover and control the use of Shadow IT
- Data security by identifying and classifying sensitive data at risk of exposure in cloud
- Threat protection by identifying suspicious user activity on cloud services
- Incident Response by investigating areas of concern in cloud accounts with rich log based intelligence.

CloudSOC collects logs and inspects traffic for the cloud usage analysis, user's behavior analysis and malware analysis. It provides easy integration with user authentication, data loss prevention, advanced threat protection, endpoint protection, email security and other security components (Gartner, 2019). CloudSOC also offers encryption and tokenization gateway to make it the most complete CASB solution. Table 1 provides a comparison of the CASB solutions from the industry leaders according to Gartner's report, which can be found at the google drive address:

https://drive.google.com/file/d/1B08bpzy-KeMPLk_yUEw_PI1yz1O8Ny88/view?usp=sharing (Sheet 2)

How CASB delivers functionalities critical to its success?

Cloud application discovery (Discover Shadow IT).

Enterprises are increasingly moving towards cloud applications to meet their day-to-day business requirements because of its feasibility and accessibility. Enterprises allow their users to use these cloud services after placing necessary security controls, these are known as sanctioned services. There are numerous applications available in the market which make user's task easy, so the enterprise users move towards those applications to ease their work and be more productive; enterprise IT is not aware of these applications in use, this is termed as Shadow IT. Enhanced visibility into the cloud network is the key pillar of CASB that helps in discovering cloud applications being used in the enterprise. CASB is deployed in log collection mode to discover the applications being used in the enterprise.

CASB collects network traffic from security devices using a firewall or a web security gateway. A web security gateway provides an in-depth inspection of web service requests from both on-premises and remote users (Obregon, 2017). The information logged by the gateway is passed on to the CASB for further analysis by the security analysts to discover the Shadow IT being used in the enterprise. An on-premises connector is used to pass on the logs collected by the gateway to the CASB (McAfee, n.d.). The logs collected are not only used for discovering Shadow IT but also by the integrated security systems like SIEM.

Now that CASB has collected the logs, security analysts discover the Shadow IT services and sanctioned services being used. CASB provides an interactive GUI or dashboard to view the statistics and analysis performed on user activity. After reviewing the logs, the Shadow IT applications which do not meet the company’s security requirements are identified and countermeasures are taken to stop its usage. For both sanctioned and unsanctioned services, user activity on these services is tracked, even the granular details about the usage of these services are analyzed that helps in implementing strong security policies on its usage.

The cloud services discovered that are being used in the enterprise are analyzed to ensure that they comply with the company’s security policies or other compliance policies. Each discovered application or service is rated on the basis of the risk factor involved with its usage. Enterprise IT can block the services with high risk value and suggest alternative secure applications to reduce the risk exposure of the enterprise (Andrews, Grealish & Jalil, 2019).

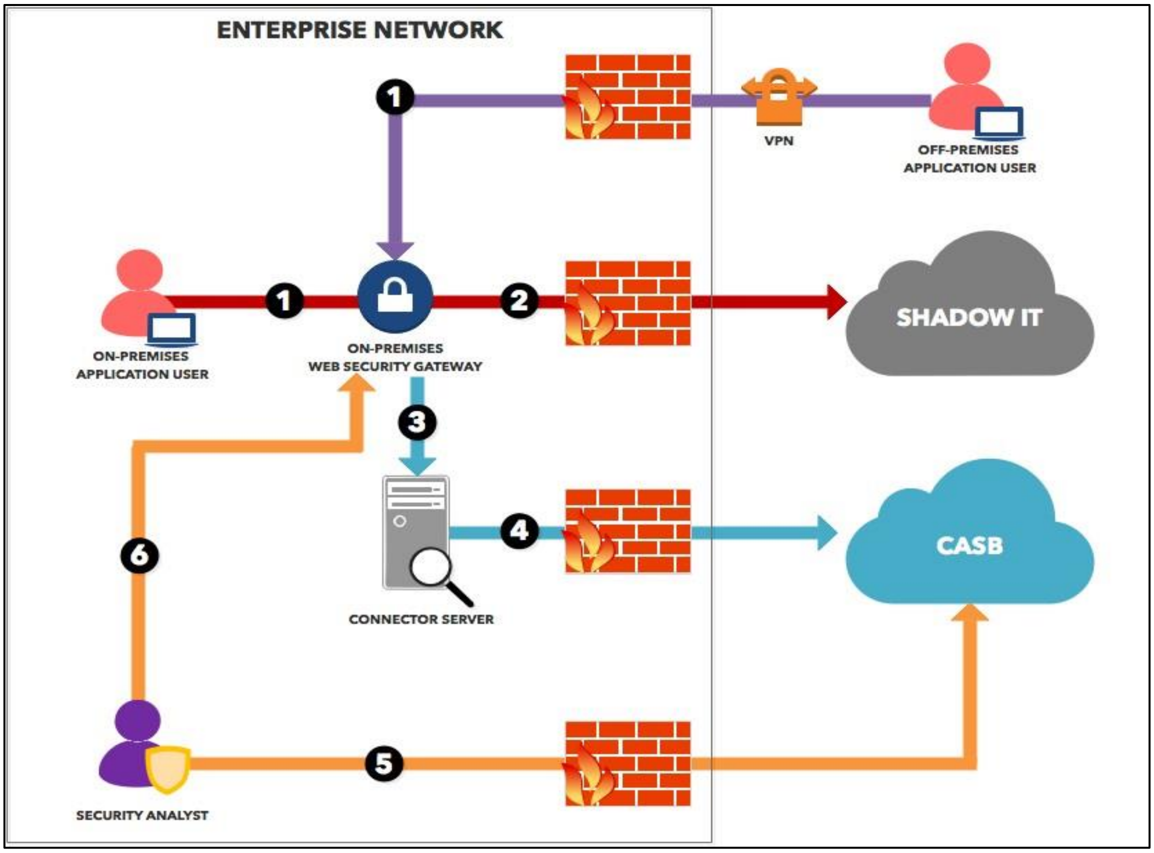

ENTERPRISE NETWORK
1
VPN
OFF-PREMISES APPLICATION USER
1
2
ON-PREMISES APPLICATION USER
ON-PREMISES WEB SECURITY GATEWAY
SHADOW IT
3
6
4
CASB
CONNECTOR SERVER
5
SECURITY ANALYST

Figure 6: Securing Unsanctioned Cloud Services using CASB (Obregon, 2017)

Governing usage of cloud services.

Cloud governance consists of assessing the risk in using cloud applications and mitigating the risk by enforcing the policies and placing required security controls. Cloud Governance is responsible to see if the cloud applications comply with government regulations and other industry standards or not. The deployment mode used to govern the usages of cloud services is log collection.

Forcepoint has given a CASB solution that governs the usage of cloud services in an enterprise. CASB is capable of assessing the risk associated with the different cloud services being used. With enhanced visibility into the user activity and cloud network, CASB identifies highrisk activities, finds security and compliance gaps by benchmarking current security configurations against regulations or best practice guidelines. Analysis and reports generated by CASB are used to govern the usage of cloud services by applying risk response techniques to the risks identified. Moreover, the analysis done by CASB helps in taking better policy making decisions to control user access to the cloud services and maintaining the privilege level to the applications.

McAfee's CASB solution MVISION integrates well with the secure web gateways (SWG) and next-generation firewalls (NGFW) to enforce the cloud governance policies in realtime.

Gain granular visibility and enforce activity-level controls.

Using CASB, enterprises can gain deep visibility into cloud usage and enforce granular controls at the user, activity and data levels (McAfee, n.d.). CASB uses forward proxy deployment mode to gain user activity level visibility and implementation of controls.

CASB's capability to enforce activity-level control helps enterprises to stop malicious activity itself, instead of blocking the application at all for usage. These activity level controls can be built using a wide range of criteria like specific users, applications, devices, locations, user actions, file properties, etc (Andrews et al., 2019). For example, a policy can be defined to block the action if any user tries to download files classified as sensitive data from Salesforce, to an unmanaged device (personal device). CASB serves as a single point of control to define and enforce rich and granular policies for all the cloud applications in an enterprise. Contextual analysis of traffic (detecting activities like 'upload' or 'download') and strong data classification mechanism is required to achieve this functionality of CASB (Andrews et al., 2019).

Cloud threat and anomaly detection.

CASB not only provides visibility and control in the cloud network but also protects against threats by alerting security operations center (SOC) & incident response (IR) teams. CASB monitors cloud services for unusual behavior such as data infiltration, unauthorized access, privilege escalation, noncompliance, etc. (Friedman & Bouchard, n.d.). As soon as CASB detects policy violation, malicious activity or anomalous behavior, it generates an alert on the CASB's GUI or SIEM (depending on the configuration) for immediate actions to be taken by the security team. CASB leverage a collection of API and reverse proxy deployment modes to detect threats and anomalies.

CASB uses machine learning based user and entity behavior analysis (UEBA) for advanced analysis and quick detection of abnormal behavior in the usage of cloud applications. McAfee MVISION CASB performs the below mentioned functions that provide protection against cloud threats and misconfigurations (McAfee, n.d.).

- Security Configuration Audit: Compares the security settings and configuration of the discovered cloud applications against industry standards such as CIS benchmarks and suggest changes to provide protection against misconfigured applications.
- Automated Configuration Remediation: Automatically changes the settings of misconfigured applications discovered in the audit using a policy-based response.
- User and Entity Behavior Analysis (UEBA): Perform heuristics and machine learning on user activity to develop a self-learning model to identify patterns of user activity that may pose a threat to enterprise security.

- Account Compromise Detection: Indicates possible compromised accounts based on the analysis of login attempts, brute-force attacks or untrusted location.
- Insider Threat Detection: Using machine learning analytics, it detects activity that indicates user negligence or malicious activity like stealing sensitive data.
- Malware Detection: Identifies malware by performing an intense scan on the cloud environment and removes malware by permanently neutralizing it.

Andrews et al. (2019) proposed establishing a baseline behavioral pattern for each user in the organization that defines the equivalent of fingerprint for that user. If the user's activity deviates significantly from the established baseline while using the cloud services, CASB's generate an indication or alert so that analysis can be done on this account to find if it has been compromised by attacker or malware. Symantec CloudSOC uses UEBA to calculate the risk level of a user's behavior and computes a numerical value called ThreatScore (Symantec, n.d.). The user accounts having high ThreatScore are cautiously monitored for malicious activity, thereby making CASB a proactive solution to cloud security.

Machine Learning in Cloud Access Security Broker

Salitin & Zolait (2018) stated that user and entity behavior analysis (UEBA) uses machine learning algorithms, mathematical models and statistics to determine deviation from standard behavior of different entities. UEBA is based on technologies such as artificial intelligence, deep learning, supervised and unsupervised machine learning, which are used to establish a behavioral baseline of all the users, files, devices, applications, etc. present in the network. UEBA generates an alert for the security professional if any malicious activity or significant deviation in the behavior of any user or entity is observed.

According to Gartner’s report “Market Guide for User and Entity Behavior Analytics”, UEBA could be used as a standalone security solution which is known as Pure-play UEBA. It can also be embedded in other security tools such as CASB, SIEM, identity management, etc. and these are known as embedded UEBA. UEBA requires a huge chunk of data from different data sources to perform precise behavior analysis of different users and entities. UEBA relies on different sources to collect data such as log management tools, network traffic, user logs, event logs, etc. Gartner recommends using a data-centric approach to provide contextual data to UEBA for analysis.

Shashanka, Shwab, and Wang in 2016 provided a User and Entity Behavior Analytics architecture, the Niara Security Analytics Platform, that implements machine learning based on Singular Values Decomposition (SVD). The Niara Platform collects all the information about an entity, may it be a user or a device, and uses it to generate a risk profile for the entity. The information or raw data is collected from a wide variety of sources (packets, logs, files, alerts, etc.) and then the data is correlated to make it understandable for analysis. Both supervised and unsupervised machine learning is used to identify the anomalies or threat events that are relevant to security analysts for in-depth analysis. The entire workflow of the UEBA module is broken into four phases described below:

1. Data Preparation: In the first step, relevant data is collected from all the sources.

2. Feature Extraction: In this step, information from the relevant fields of the data collected in the previous step is obtained, using which the entity's features are computed and stored.

3. Behavior Profiling: The features extracted for each entity in the previous step are grouped into configured baselines. SVD based machine learning model is applied to generate a behavior profile for that particular entity.
4. Anomaly Detection: In this step, the risk value of the entity is compared against the baseline for that entity. An alert is generated if a significant change is observed in the risk score.

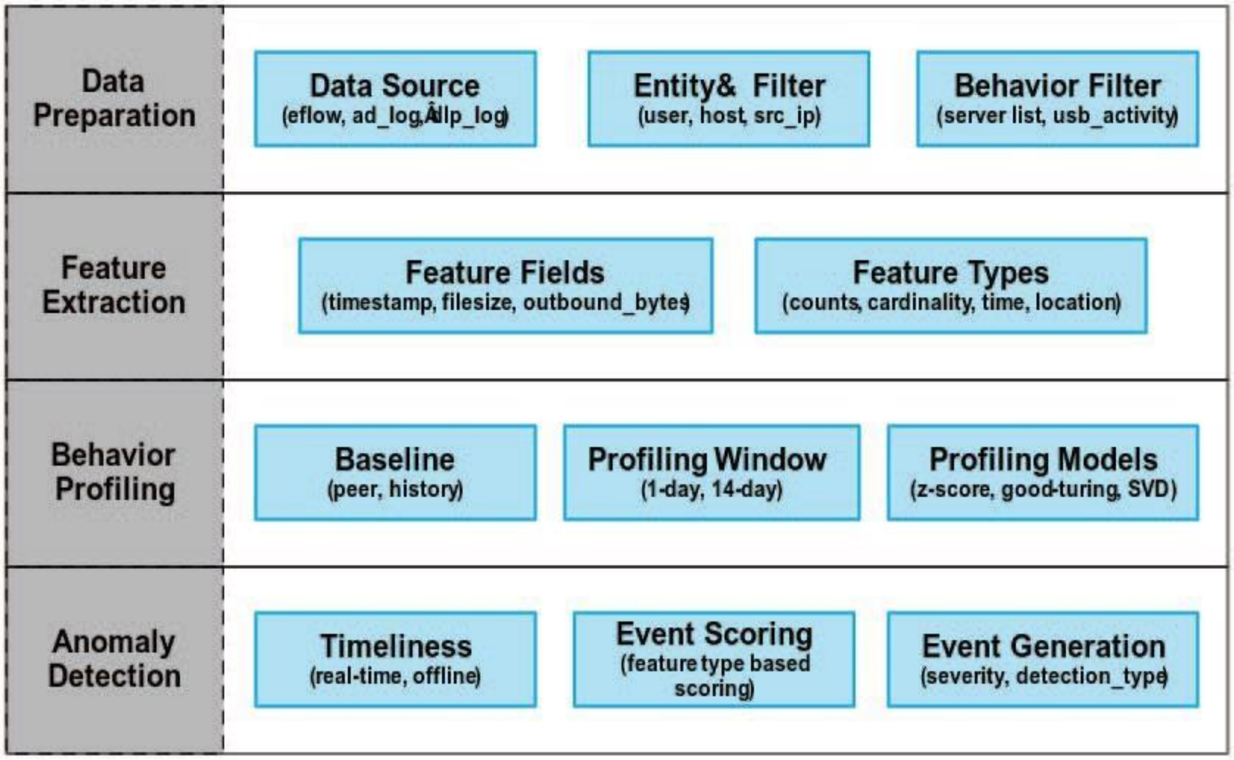


Figure 7. Generic Architecture for UEBA (Shashanka et al., 2016)

Malware protection (Sandboxing).

CASB extends to the cloud security yet another measure for threat protection i.e.

sandboxing which means to search for malware by dynamic analysis of files. A malware may enter a cloud network through direct cloud-to-cloud interaction, or it can be produced natively in cloud applications (Friedman & Bouchard, n.d.). In a cloud environment, malware spreads rapidly across the network, infecting other systems and user accounts in the organization. since the cloud is based on shared technology (Symantec, n.d.). CASB leverage a collection of API and reverse proxy deployment modes to provide protection against malware.

In Bitglass Top CASB Use Cases, CASB is integrated with Advanced Threat Protection (ATP) that leverages machine learning algorithms to detect known and even zero-day malware. CASB can detect malware from data at rest and in motion as well, where normal perimeter defense fails to offer. CASB is deployed in inline proxy mode to scan the cloud traffic for malware flowing in the network. To scan for malware in files and data stored in cloud applications (data at rest), CASB leverages API connections with the applications to prevent the flow of malware to other cloud applications or connected devices in the network.

Symantec in 'The Next Generation of Cloud App Security', has provided three key functions that a CASB should perform regarding malware protection, which are as follows:

- Global Threat Intelligence: CASB solution should tap on the best global threat intelligence to analyze cloud content from cloud applications being used around the globe.
- Block & Neutralize Malicious Files: CASB should have a leading antivirus scanning engine capable of inspecting content flowing in and out of the cloud

applications as well as the data stored in the applications. Moreover, CASB should be able to take actions like blocking and neutralizing malicious content, preventing malware to spread in the organizations.

- Detect Zero-Day Threats: CASB provides the enterprise with a solution to detect unknown threats by integrating with ATPs. All the files should be analyzed using the ATP to detect any malicious behavior.

Research Methodology

The purpose of this research is to protect enterprises against threats arising from the use of cloud technology. In this study, a conceptual model is defined that leverages the artificial intelligence of cloud access security brokers and highlights the important security features that CASB provides. The model defines an easy integration of CASB with major existing security controls to enhance their functionality as well. This research is limited to securing the cloud infrastructure of large enterprises that use a large number of cloud applications for its business. The provided model does not apply to individual users that use cloud applications for personal use outside of an organization. Another limitation of the research is that it is theoretical in nature and CASBs integration with other security components is not tested. Moreover, no tests are performed to test the efficiency of machine learning algorithms used for a better CASB solution. This research aims to address the following questions related to securing enterprises against threats arising from dependence on the use of cloud services:

- What would be an optimal architectural implementation of CASB that provides easy integration with conventional security components available in the enterprise to protect cloud applications against threats?

- Will Machine Learning based CASB's be able to provide strengthened protection against cloud-related threats?
- What features and benefits should be present in a "best in class" futuristic CASB?

In order to achieve the research deliverable, first, study the application of cloud access security broker in securing the cloud environment and review the different deployment modes and the capabilities of each deployment mode. Next, compare and list out the strengths and weaknesses of the top 3 CASB solutions according to Gartner's Magic Quadrant for CASB. The related work in the field of machine learning heuristics and behavior analysis to identify threats in advance and the use of machine learning algorithms in malware detection has been studied.

Use cases of CASBs integration with existing security components like identity and access management (IAM), the web security gateway (WSG), security incident and event management (SIEM), advanced persistent threats (APT), data loss prevention (DLP), etc. have been provided. The research deliverable is a "best in the class" conceptual blueprint of a CASB model encompassing the best security features, which uses machine learning capabilities to provide all-around security to enterprises against cloud-related threats.

Analysis and Discussion of Results

Machine learning-based CASB implementation model

The study done on the different CASB solutions in this paper is used to come up with a CASB implementation model that takes into account the use of all cloud based applications that the users in an enterprise may use. The proposed integrated model tracks user request to all cloud services; monitors the traffic, send logs to other security components for in-depth analysis and also performs behavioral analysis on users and other entities present in the network. The deployment mode of the CASB implementation model is hybrid, which uses a combination of forward proxy, reverse proxy, and API mode. The key components in the model are web security gateway, CASB, data loss prevention (DLP), security incident and event management (SIEM), user and entity behavior analysis (UEBA), identity and access management (IAM), enterprise mobility management (EMM), etc.

The proposed model takes into account users on- and off-premises and covers all managed and unmanaged devices using enterprise mobility management (EMM). In the given model, CASB is deployed in hybrid mode in a combination of API and inline mode. API mode helps CASB to monitor cloud application data while proxy or inline mode helps in monitoring network traffic. As soon as a request for cloud service is generated from a user, the service request from the user is authenticated by using the IAM; EMM verifies the device from which the request generated. Different controls can be implemented on users and devices based on the access policies defined.

In this implementation, all cloud traffic to and from the cloud applications is required to pass through the secure web gateway. It adds an additional layer of security by preventing unsecured traffic from entering into the network or restricted data to go out of the network. Rules can be applied to filter the traffic to provide enhanced security using a web gateway. Secure web gateway logs all network traffic and forwards it to the connector server for normalization. Normalized data is then fed to CASB for further analysis. It is better to collect as many logs as possible, this makes implementing real-time policy enforcement easier and supplements the machine learning capabilities of the CASB.

One of the important pillars of CASB is visibility, the logs collected by the CASB are used for cloud application discovery which includes all cloud services including sanctioned and unsanctioned services. In the given model, CASB works incorporation with the endpoint encryption service to manage the encryption of data at rest and in transit across all the endpoints. Endpoint encryption service manages the encryption keys provided to the users in the enterprise (bring your own key), provides support to different types of encryption standards like Advances Encryption Standard (AES-256) and Rivest, Shamir, Adleman (RSA), etc. CASB provides centralized encryption policy enforcement, inspect encryption endpoints to make sure all network data and application data is encrypted at all times according to the defined encryption policies. All of these actions can be taken using CASB’s management console. The encryption mechanism provided using endpoint encryption service provides a real boost to cloud data security.

In this implementation model, CASB is also connected to the data loss prevention manager that allows easy extension of on-premises data loss policies to the cloud network as well. Enterprises enforce data loss prevention policies to protect sensitive data from unauthorized access or from loss. Existing DLP policies could be used and more DLP policies can be defined using the CASB to provide enhances protection against data loss. The DLP manager also has some predefined inbuilt policies which can be imported and applied to sensitive data over the network. Real-time actions can be performed based on the data loss policies such as alerting, deleting, blocking, encrypting, etc. when there is a violation in a DLP policy.

Another important integration in this implementation model is Security, Incident and Event Management (SIEM). It is important to understand that the function of CASB is limited to the cloud environment only while SIEM gives alerts related to the entire network. SIEM collects network logs from web gateways, firewalls, host machines, server logs, etc. These logs are filtered for the cloud network and are forwarded to the CASB for in-depth analysis and better decision making.

The given implementation model is powered by User Entity and Behavior Analysis (UEBA) that uses machine learning algorithms and statistical modeling to perform analysis on users, applications, files etc. It uses supervised, unsupervised and deep learning to develop a base behavioral pattern for each and every entity (user, files, devices) and applications present in the cloud network. UEBA prevents cloud services against a wide variety of threats by creating profiles for every entity and then detecting anomalies using machine learning. A separate section for UEBA on the CASB dashboard would provide a better insight into the user profiles, their risk score of all the applications and assessment of every application and file using UEBA. Different threats that can be generated to the cloud services can be viewed as alerts under the UEBA tab. These alerts are continuously monitored by the security analysts to take prompt actions. Machine learning CASBs are able to take real-time actions on alerts based on guided learning.

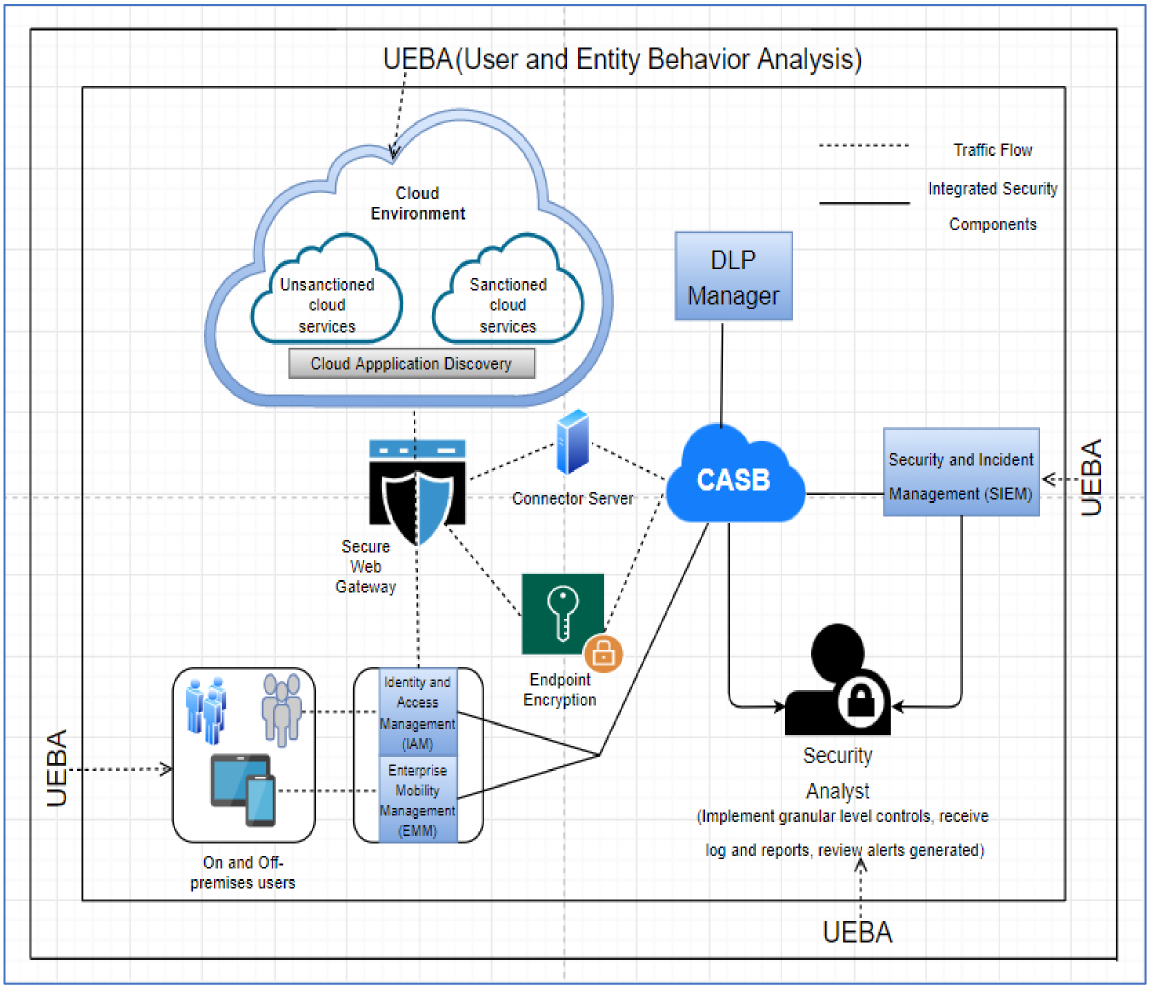

UEBA(User and Entity Behavior Analysis)
Cloud Environment
Unsanctioned cloud services
Sanctioned cloud services
Cloud Appplication Discovery
Traffic Flow
Integrated Security Components
DLP Manager
CASB
Connector Server
Secure Web Gateway
Endpoint Encryption
Security and Incident Management (SIEM)
UEBA
Identity and Access Management (IAM)
Enterprise Mobility Management (EMM)
On and Off-premises users
Security Analyst
(Implement granular level controls, receive log and reports, review alerts generated)
UEBA
UEBA

Figure 8. *CASB Implementation Model*

State-of-the-art features of CASB

In this section, the important features that a CASB should possess are listed. The features provided are expected to fit the requirements of most enterprises that provide access to lots of sensitive data through cloud services, but they can still be customized based on individual organization's needs. The complete list of features can be accessed at the google drive address https://drive.google.com/file/d/1B08bpzy-KeMPLk_yUEw_PI1yz1O8Ny88/view?usp=sharing (Sheet 3).

How does the given CASB implementation model protect against the top 12 threats to cloud computing?

In this section, the CASB solution is validated by explaining how this CASB solution provides protection against the top cloud threats according to the report " The Treacherous 12 – Cloud Computing Threats". Table 3. in the research deliverable provides the explanation in the defense of the provided CASB solution and it can be found at the google drive address https://drive.google.com/file/d/1B08bpzy-KeMPLk_yUEw_PI1yz1O8Ny88/view?usp=sharing (Sheet 4).

Recommendations and Conclusions

In the research done in this paper, a CASB implementation model is derived that tends to provide a secure environment protecting users, data and applications against the threats related to cloud technology. The implementation model describes how to deploy a CASB in a cloud network to protect enterprises from the risks associated with the use of cloud technology. The CASB implementation explains the deployment mode of CASB, key integrations with other security components and the use of important technologies such as UEBA and machine learning to provide a robust security mechanism for cloud technologies. The research deliverable also provides a list of features that a CASB should have at the minimum. In the provided list of CASB features, the pillar of CASB is provided to which each feature/function of CASB is related. The features listed in this deliverable make the state-of-the-art features that every CASB solution is expected to have in order to be considered as a possible security solution to cloud-related threats. Additionally, a verification of the CASB implementation model comprising of the mentioned features and functions is provided by explaining how this solution protects the enterprise cloud environment against the treacherous top 12 threats to cloud computing.

The CASB implementation model provides seamless integration of CASB with core security components to complement the functionality of each component. In the provided model, for the components that could not be integrated with the CASB just as such, their functionality has been increased by providing controls in the CASB management plane. This helps CASB in implementing real-time, contextual access control policies to secure the cloud network. Machine learning empowered CASB upgrades the security of the cloud by providing real-time protection against threats. Not only does it provide protection against insider threats by using behavioral analysis, but it also provides protection against known and zero-day threats by using artificial intelligence driven global threat intelligence system.

The research done in this paper provides a clear insight into the essential features that any enterprise will require in a CASB solution regardless of its business domain. And, the implementation model provides guidance in deploying the CASB in the cloud network by integrating it with the enterprise's existing information security components.

A limitation of this research is that this research is theoretical in nature, the CASB implementation model and its machine learning capabilities are not tested. Both unsupervised and guided learning is required for an AI-based CASB which will require feeding very huge data sets to CASB. Future research in this area could include providing CASB solutions to protect individual users (personal use) against cloud related threats at affordable prices.

Preliminary Bibliography

Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. (2020). Retrieved 18 March 2020, from https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf

Obregon, L. (0AD). SANS Institute Information Security Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/cloud/technical-approach-securing-saas-cloudaccess-security-brokers-37960.

Top Threats Working Group The Treacherous 12. (2016, February). Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_CloudComputing_Top-Threats.pdf.

Security Guidance for Critical Areas of. (n.d.). Retrieved from https://cloudsecurityalliance.org/download/security-guidance-v4/.

Liu, C., Wang, G., Han, P., Pan, H., & Fang, B. (2017). A Cloud Access Security Broker based approach for encrypted data search and sharing. 2017 International Conference on Computing, Networking and Communications (ICNC). doi: 10.1109/iccnc.2017.7876165

CASB 101: How Cloud Access Security Brokers Can Make Your Data More Secure. (n.d.). Retrieved from https://www.esecurityplanet.com/mobile-security/casb.html.

Cloud Access Security Brokers. (2018). Retrieved 23 October 2019, from http://www.isaca.org/Knowledge-Center/Research/Documents/Tech-Brief-CASB_res_eng_0218.PDF

Deployment Architectures for the Top 20 CASB Use Cases. (n.d.). Retrieved from https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/wp-deployment-modestop-20-use-cases-102716.pdf.

Rubens, P. (2019, July 10). 8 Top CASB Vendors. Retrieved from https://www.esecurityplanet.com/products/top-casb-vendors.html.

Thomchick, D. (2018, March 8). 5 Key Integrations for a Successful CASB 2.0 Deployment. Retrieved from https://www.symantec.com/blogs/product-insights/5-key-integrations-successful-casb-20deployment.

Shackleford, D. (2019, May). SANS 2019 Cloud Security Survey. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/2019-cloud-security-survey-38940.

MacDonald, N., Lowans, B., & Lawson, C. (2015, October 22). Market Guide for Cloud Access Security Brokers. Retrieved from https://www.gartner.com/en/documents/3155127/market-guide-forcloud-access-security-brokers.

McLean, R. (2019, July 30). A hacker gained access to 100 million Capital One credit card applications and accounts. Retrieved from https://www.cnn.com/2019/07/29/business/capital-one-databreach/index.html.

2018 Cloud Computing Executive Summary. (n.d.). Retrieved from https://resources.idg.com/download/executive-summary/cloud-computing-2018.

IBM X-Force Threat Intelligence Index. (n.d.). Retrieved from https://www.ibm.com/security/data-breach/threat-intelligence

Cloud Adoption and Risk Report 2019. (2019). Retrieved 26 November 2019, from https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-riskreport-2019.pdf

Shackleford, D. (2017, November). Cloud Security: Defense in Detail if Not in Depth. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/cloud-security-defense-detail-in-depth38120.

Suryateja, P. (2018). Threats and Vulnerabilities of Cloud Computing A Review. *International Journal of Computer Sciences and Engineering*, *6*(3), 297–302. doi: 10.26438/ijcse/v6i3.297302 Surianarayanan, C., & Chelliah, P. R. (2019). *Essentials of cloud computing: a holistic perspective*. Cham: Springer.

Select the Right CASB Deployment for Your SaaS Security Strategy. (2015, March 12). Retrieved from https://www.gartner.com/en/documents/3004618/select-the-right-casb-deployment-for-yoursaas-security-

Salitin, M. A., & Zolait, A. H. (2018). The role of User Entity Behavior Analytics to detect network attacks in real time. 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). doi: 10.1109/3ict.2018.8855782

Friedman, J., & Bouchard, M. (n.d.). Definitive Guide to Cloud Access Security Brokers. Retrieved from https://4b0e0ccff07a2960f53e-707fda739cd414d8753e03d02c531a72.ssl.cf5.rackcdn.com/wpcontent/uploads/2015/12/Definitive-Guide-to-CASB_HPE-eBook.pdf.

Garbis, J., & Koilpillai, J. (2019). SDP Architecture Guide v2. Retrieved From https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/.

Coles, C. (2018, May 31). New eBook: Which CASB Deployment Architecture is Right for Me? - McAfee MVISION Cloud. Retrieved from https://www.skyhighnetworks.com/cloud-security-blog/newebook-which-casb-deployment-architecture-is-right-for-me/.

Magic Quadrant for Cloud Access Security Brokers. (2019, October 22). Retrieved from https://www.gartner.cohttps://www.gartner.com/doc/reprints?id=1-

1XOEZTG0&ct=191024&st=sb&aliId=eyJpIjoiUzNiNG5hQ1JQV2M2ZnAwRyIsInQiOiI4U2p QSURRSDhOV1VUSGRTbkFRZ3hnPT0ifQ%3D%3Dm/en/documents/3834266/magic-quadrant-for-cloud-access-security-brokers.

Andrews, E., Grealish, G., & Jalil, R. (2019). Securing Cloud Applications & Services. Retrieved 28 November 2019, from https://www.symantec.com/content/dam/symantec/docs/other-resources/securing-cloud-applications-and-services-executive-guide-en.pdf

Small, M. (2018). KuppingerCole Report LEADERSHIP COMPASS Cloud Access Security Brokers 2018. Retrieved 28 November 2019, from https://www.oracle.com/assets/kuppinger-cole-leadership-compass-5223769.pdf

What is a CASB? (Cloud Access Security Broker). (2019, October 30). Retrieved from https://www.forcepoint.com/cyber-edu/casb-cloud-access-security-broker.

Secure Use of Cloud Apps & Services. (2019). Retrieved 28 November 2019, from https://www.symantec.com/content/dam/symantec/docs/solution-briefs/secure-use-of-cloud-apps-andservices.pdf

McAfee MVISION Cloud. (2019). Retrieved 28 November 2019, from https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-mvision-cloud.pdf

CASB 2.0 The Next Generation of Cloud App Security. (2019). Retrieved 28 November 2019, from https://www.symantec.com/content/dam/symantec/docs/white-papers/casb-2.0-the-next-generation-ofcloud-app-security-en.pdf

Shashanka, M., Shen, M.-Y., & Wang, J. (2016). User and entity behavior analytics for enterprise security. *2016 IEEE International Conference on Big Data (Big Data)*. doi: 10.1109/bigdata.2016.7840805

Appendix A: CASB capabilities in different deployment modes (Source: Coles, 2018)

	Log Collection	Forward Proxy	Reverse Proxy	API
Top-level usage statistics (which employees use which services)	✓			
Risk assessment (risk profile of cloud services in use)	✓			
Detect enforcement gaps (access of apps not effectively blocked)	✓			
Collaboration analytics (sharing permissions on files/folders)				✓
Activity monitoring (audit trail of user and admin actions)	✓	✓	✓	✓
Detect insider threats	✓	✓	✓	✓
Detect compromised accounts			✓	✓
Detect malware (exfiltrating data via unsanctioned apps)	✓			
Detect malware (stored within sanctioned apps)				✓
DLP inspection (data at rest within sanctioned apps)				✓
DLP inspection (data in transit)		✓	✓	

DLP enforcement (quarantine, delete, modify collaboration)				✓
DLP enforcement (block, tombstone)		✓	✓	
Security configuration audit (security settings of apps)				✓