Cloud Access Security Brokers (CASBs)

Characterization of the CASB market and its alignment with corporate expectations
Commissioned by KPMG Netherlands

Marius Brouwer
University of Amsterdam
mbrouwer@os3.nl

Anand Groenewegen
University of Amsterdam
agroenewegen@os3.nl

ABSTRACT

This research is aimed at the current Cloud Access Security Broker (CASB) market and its alignment with the expectations of corporations. The main goals are to come to a common definition of CASB, finding the relationship between CASB and Shadow IT, how addressing Shadow IT impacts a CASB as well as how administrative overhead can be kept to a minimum. These topics have been approached by interviewing nine CASB (prospective) users within the Dutch marketplace. The CASB vendors included in this research are defined as leaders by Gartner's 2020 Magic Quadrant. The outcome of this research indicate that "Leading CASBs are ahead of corporate expectations in regards of feature set, while vendors are extending their capabilities, organizations are hesitant to implement a CASB while acknowledging the need of one."

Index Terms: *Cloud Computing, Visibility & Control, Shadow IT, Proxy & Secure Web Gateway, Security Platform*

July 2, 2021

1 INTRODUCTION

Employees are less reliant on a companies' centralized infrastructure to perform their daily operations, combined with the 2020 pandemic, an increase can be seen towards employees working offsite [1]. A Forbes Insight research in 2019 highlights that more than one in five organizations have experienced a cyber event due to Shadow IT [2]. Shadow IT is a collective name for all resources not sanctioned by an organization's IT department. Employees using Shadow IT decrease an organization's visibility and control over the use of intellectual property and increase potential threats to sanctioned cloud and on-premise solutions [3]. These uncertainties led to the rise of CASB platforms to gain insight into the behavior of employees while accessing organization data [4].

The focus of a CASB is to increase the ability to protect and control access to data that is being stored outside the organizational boundaries. A theoretical example of this could be: a DevOps engineer has to connect "Application A" with "Application B", but internally there is no connectivity set up while "Application A" has access to the internet. The schedule does not allow a connectivity change to be applied before the deadline, therefore the DevOps Engineer sets up "Application B" on a private-owned cloud environment and lets it communicate with the internally hosted "Application A". The organization is now sharing intellectual property over the internet and risking a potential data leak. The core functionality of a CASB platform includes increasing visibility, data security, threat protection and compliance. As such that users and their third-party applications are made visible, sensitive data will be identified, control over user behavior will be extended and compliance reports with dashboards are capable of being generated.

In April 2021 a practical example of a Shadow IT breach has been brought to light where a vendor, paid to conduct COVID-19 contact tracing, had their data leaked [5]. Confidential data such as exposure status and sexual orientation was compromised due to employees using Google accounts to collaborate. Although the company states that Google's platform is an unauthorized collaboration channel within their organization because of the lack of control employees disregarded this. A news article on the matter concludes that the organization had to upscale under high pressure due to the pandemic [6]. This is an example of Shadow IT being used without considering the consequences, as the employees of this breached company merely wanted to fulfill their work as adequate as possible though in hindsight losing sight of a potential security violation.

2 BACKGROUND

This section is a precursor towards topics that relate to CASB to gain a better understanding of the fundamental building blocks.

A **forward proxy** is an internet-facing proxy that offers protection from the perspective of the on-premise client devices. There are three main methods used to deploy a forward proxy, using either endpoint agents, Proxy Auto-Config (PAC) or a Secure Web Gateway (SWG) [7].

Endpoint agents specifically are an integral part of CASBs. This component is installed on all endpoint devices and forwards its traffic to the CASB to be able to access cloud applications [7]. Forward proxies can be deployed in two modes. The first mode is **transparent proxy**, where all traffic is intercepted without modification. The second mode is **explicit proxy**, where only specific traffic is proxied based on e.g. DNS, IP, and/or port. Most often, port 80 and 443, to only capture web traffic [8].

A **reverse proxy** is situated between the internet and a cloud application. This solution is only effective in protecting server applications that are known to the IT landscape of an organization. Both forward and reverse proxies are considered to be **inline** protections methods because they capture data in transit [7].

On the contrary, data can also be processed while at rest through the use of an **API**. The advantage of this method is that data does not need to be routed through an extra hop and eliminates the possibility of having the proxy being a bottleneck. This is also referred to as **out-of-band protection** [7].

CASBs differentiates between two types of cloud applications. The first being **sanctioned** applications, these are known services within the cloud landscape of an organization and approved to work with or contain corporate data. **Unsanctioned** applications are synonymous for **Shadow IT**, all unknown resources within the

cloud-landscape of an organization that employees work with or contain corporate data [9].

Combining all previously discussed, figure 1 depicts the various architectures.

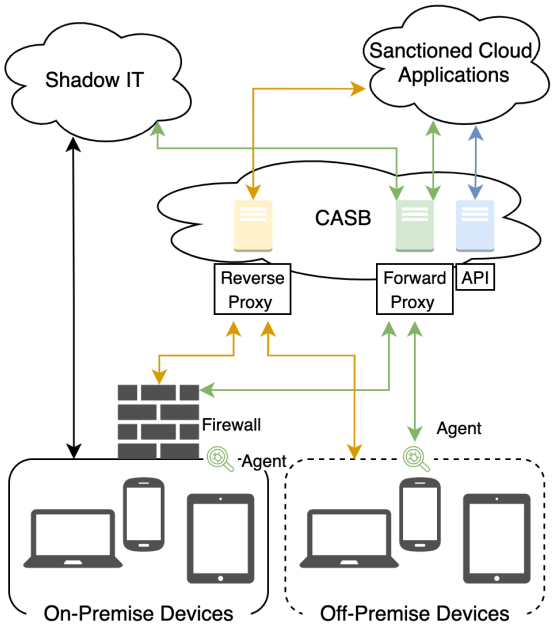

Figure 1: CASB Architectures

The **four pillars**, or core functionality, of a CASB are visibility (detecting cloud services), data security (controlling information), threat protection (mitigating anomalies), and compliance (cloud governance) [4].

3 PROBLEM STATEMENT

This research focused on providing an analysis of the current capabilities of the Cloud Access Security Broker market; vendor leaders versus the capabilities expected by corporate. The scope was based upon the relationship between CASBs and Shadow IT, since this is the original concept a CASB attempts to solve. Up until now, there is limited academic research on the topic of CASB and a gap exists between theory and practice. With this research, the authors set out to close this gap.

3.1 Research Questions

The main research question of this paper is:

"How do market-leading CASBs align with corporate expectations?"

This paper will be answering the main question by addressing the following set of sub-questions.

- How do market guides and corporations define a CASB?
- How does Shadow IT, including risk and mitigation, relate to CASB?
- How do the Leaders of the Gartner Magic Quadrant (2020) address Shadow IT?
- How can a CASB be implemented in such a way that the responsible party is capable of managing the administrative overhead generated by CASBs?

4 RELATED WORK

CASB is a term coined by Gartner in their article on the matter in 2012 [10]. Their first market guide was published in 2015 while their first magic quadrant was published in 2017 [11] [12]. They analyze the technical definition and market landscape in these articles. A CASB acts as a gatekeeper, or checkpoint, for an organizations cloud environment [13]. In 2020, Gartner defines the CASB market as products and services that address security gaps in an organizations use of cloud services [4]. According to research done by Wadhwa et al. practice-informed research could help develop, improve, and standardize the CASB solutions [14].

Another important aspect of this paper is Shadow IT. Extensive work can be found on the matter, such as the Forbes Insight research in 2019 as is the subject extensively covered by Silic et al [2]. This project on "Understanding Shadow IT risks, benefits and opportunities" researches Shadow IT in-depth via a psychological manner [15]. A thesis written by Hulsebosch on the differences between traditional Shadow IT and Cloud-Based Shadow IT including a managed framework based on the risks and opportunities is also leveraged [9]. This research explores the relationship between CASBs and Shadow IT.

5 METHODOLOGY

The following steps have been taken to research the given subject:

- Interviewing: Reaching out to corporate executives, or those who decide on implementations within a company, to interview them on the given subject (RQ1).
- Literature Study: Reviewing documentation written by service providers, market guides, published articles and other (security) experts writing blog posts on the given subject (RQ1 and RQ2).
- Hands-on Review: Practical review on how service providers deploy a CASB (RQ3 and RQ4).

This research involved interviewing various vendors, service providers, customers or parties interested in CASBs. All participants, except for vendors, are based within the Netherlands. As such the corporate expectations of a CASB is from a Dutch market perspective. The interviews were semi-structured. The interview questions can be found in appendix A. The candidate list can be found below.

Corporate

- Security Officer of a cloud service provider
- Chief Technology Officer of a professional services firm (A)
- Senior Manager of a professional services firm (A)
- Product Manager of a telecommunications company
- Security Engineer of a telecommunications company
- Security Consultant of telecommunications company
- Cloud Engineer of a managed security service provider
- Senior Consultant of a professional services firm (B)
- Chief Information Security Officer of a University

Vendors

- Bitglass: interview, demonstration of platform
- Netskope: interview, demonstration of platform, trial environment
- McAfee: interview, demonstration of platform, trial environment
- Microsoft: interview, trial environment

Remaining vendors either indicated not to be available or did not reply to inquiries to participate.

The interviews and literature study were complemented by a hands-on platform which reviewed trial environments. Not all vendors were capable of doing so, see the above list. A total of three environments were available. Based on the outcome of the corporate interviews this research defined four use cases. They were written so that the experiments could be performed in each environment to validate how a vendor addresses Shadow IT and how potential administrative overhead can be mitigated. The uses cases are as follows:

(1) Assessing risk and compliance of cloud applications: Validate if the cloud applications being used align with the risk appetite/policy of an organization and for what reasons the application is either suitable or unsuitable e.g. data located outside of the EU (RQ3).
(2) Enforcing fine-grained Shadow IT policies on cloud applications: The ability to implement policies on a fine-grained level that risk and compliance are factored into defining specific applications as Shadow IT (RQ3).
(3) Ease of onboarding and implementation: A CASB provides built-in ease of onboarding within the organizational perimeter through the assistance of documentation and frameworks while the CASB can connect with external platforms to handle alerts or provide automation and machine learning built-in (RQ4).
(4) Aligning CASB policies with organizational structure: The possibility to facilitate multi-tenancy per department. E.g. the ability to differentiate between policies set for business operations and researchers of an institution (RQ4).

6 RESULTS

The results are divided into four sections, based on the sub-questions. The first section focuses on giving a common definition of the term CASB, including vendor and corporate thoughts. In the second section, the relationship between CASBs and Shadow IT is identified. The third section discusses how major vendors address Shadow IT with their CASB solution while the last section reviews how potential administrative overhead can be mitigated within a CASB.

6.1 The definition of CASB

To characterize the market of CASBs, a common understanding of the solution is required. Therefore market guides were exhausted and interviews were held with corporations that either deploy CASBs (Service Providers), have or have had one within their organization (User Base) or are orientating on purchasing a CASB (Prospectives). In total eighteen vendors, research/advisory firms, and other related companies (e.g. Microsoft, Gartner, CloudFlare) were consulted on their CASB definition. After compiling these and performing a text analysis the following can be concluded: multiple occurrences were found centered around “extend the reach of security”, “as a service”, “between users and organization”, “users and cloud”, “on premises or cloud”, and “security policies”. Outside the words of CASB, “data’, “service”, “software”, “applications”, “organizations”, “between” and “policies” occurred frequently. Although each market guide has their own take on the definition of CASBs and differs on some ground, e.g. if it is solely software or also hardware, a common understanding is found that a CASB is to extend the reach of an organization’s security. A CASB is often found within ‘X as a Service’ models and is placed between the employees (users) and the perimeter of an organization. Whereas it will try to extend between users and cloud, being deployed on-premise or in a cloud-hosted environment to extend the security reach, such as security policies, into the cloud-hosted environment instead of only being able to determine policies on-premise.

Gartner’s 2020 security spend forecast predicts a significant, but slowing growth rate for CASB’s [4]. Though they also indicate that this growth in the CASB market remains higher than all other security solutions. Gartner concludes that this growth is based on enterprises moving away from traditional devices, the increase of cloud services and the abnormal spike in remote working due to the pandemic in 2020. Though a new solution might overtake CASBs entirely in the future. Palo Alto states that “While in the past, CASB was the only choice, SASE platforms are now challenging that historical dominance.” [16]. Gartner defines Secure Access Service Edge (SASE) as “a package of technologies including Software-defined Wide Area Network (SD-WAN), Secure Web Gateway (SWG), CASB, Zero Trust Network Access (ZTNA) and FireWall as a Service (FWaaS) as core abilities, with the ability to identify sensitive data or malware and the ability to decrypt content at line speed, with continuous monitoring of sessions for risk and trust levels." [17]. A practical example can be observed through McAfee’s rebranding of their platform to MVISION Unified Cloud Edge, where they see CASB as a part of their solution instead of the primary solution. Netskope is taking the same actions by redefining CASB as part of their SASE platform. These vendors, and others, seem to be responding to this trend.

Vendors indicate that the main reason to implement CASBs is to maintain control and visibility when using cloud services. Vendors are now offering a more software-based approach when implementing CASB. Initially, CASB vendors relied on hardware on-premise, in the form of a connector service. Currently, these solutions are moving towards being virtualized.

The interviews have indicated that organizations come to know about CASBs after having a secure web gateway solution that needs an upgrade. Naturally, most will reach out to their existing vendor to fulfill their informational needs on what solutions they have to offer. At this point, vendors use this opportunity to inform the organization about their newest solutions, such as CASB. The organizations indicate that they are often unaware of security solutions such as CASB. Although they do indicate the need for increased visibility, data security and threat protection. Especially taking into consideration that employees are working remotely due to the pandemic in 2020. On other occasions, organizations will learn about CASB when speaking to their managed service provider advising

them on the matter of Shadow IT and compliance or when already in possession of an extensive security suite that incorporates a CASB.

CASBs have come into existence due to organizations embracing cloud computing, increasing use of unmanaged devices and the lack of traditional tooling to manage this. These changes introduced new security risks such as lack of visibility and control of corporate data through the use of unsanctioned applications. CASBs have been developed to identify and assess these security threats. In addition to this, vendors are developing more advanced Data Loss Prevention (DLP) tooling and developing their API's to the point where real-time processing of data is possible.

Interviews with corporate executives revealed that the main reason to implement a CASB is to gain more insight and control of how employees are performing their daily work. More often than not employees use unsanctioned applications to perform their daily duties. This is not done with malicious intent, but rather a pragmatic approach to be more effective. The consensus was that CASBs should function more as a tool to gain insight into behavior and with this information accommodate the users' needs. Rather than implement it as a control measure to block all unsanctioned apps. Corporates define a CASB as a middleman layer between their on-premise and cloud landscape to ensure visibility of their organizational perimeter.

Gartner defines a CASB as "on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed" [18]. While Frost and Sullivan define a CASB as "A security platform which resides between cloud service users and cloud apps. It allows an organization to consolidate multiple security policy enforcement's across multiple cloud apps and extend the reach of these security policies beyond its infrastructure" [19]. After reviewing the market guides and the interviews while comparing these to the above research definitions we can conclude that a CASB is: Software that addresses security gaps in an organization's cloud usage by extending security policies leveraged from on-premise to the cloud. With this, the first sub-question, "How does Shadow IT, including risk and mitigation, relate to CASB?", has been addressed.

6.2 Relationship between Shadow IT and CASBs

The previous chapter explored the market definition of CASBs through market guides and interviews with corporate executives. A common understanding has been defined on what a CASB should solve: Shadow IT. While such a platform is capable of solving more than just this, the original idea always centered on IT's visibility and control of enterprise data and to extend the discovery of Shadow IT [10] [20]. This ideology originates from the seminal article of Gartner on CASBs in 2012 and their first Technology Overview on CASBs in 2015. Gartner's definition of Shadow IT is "IT devices, software and services outside the ownership or control of IT organizations" [21]. While McAfee, a vendor of CASBs, defines Shadow IT as "IT projects (like cloud services) that are managed outside of, and without the knowledge of, the IT department" [22]. To reach an extensive understanding of Shadow IT, including the risk and mitigation, this chapter will analyze two academic projects.

First discussed is a project conducted by Mario Silic Ph.D who has written four papers on the matter, which specifically looks into the psychological side of Shadow IT [15]. The second discussion is centered on an MSc graduation thesis, Cloud Strife, written by Marc Hulsebosch [9]. This paper discusses the differences between traditional Shadow IT and Cloud-Based Shadow IT including a managed framework based on the risks and opportunities.

Silic et al.'s project has identified greynet, an elusive networked computer application, to be the most prevalent type of Shadow IT software in an organization. The threats that pose the most risk are data integrity and (account) information leakage. The project also indicates that the employees are aware of these risks and despite this, continue using Shadow IT. The more technically inclined users are using Shadow IT in the form of cloud solutions to increase productivity. Whereas less technically inclined users resort to unsanctioned locally installed applications. These applications produce the largest threats for information security and privacy as they are less controllable than managed software and possibly lead to data leakage issues.

Silic et al. stipulate that risks can be mitigated by heightening employee awareness and simplifying IT policies combined with monitoring/restriction. Simply restricting users is not sufficient since it is only a matter of time before users will find a method to bypass such limitations.

Shadow IT is shifting from software run locally on an end client to cloud applications. This change requires a new approach to identify Shadow IT within an organization. Whereas previously scanning for installed applications on managed devices was adequate to identify Shadow IT. Now, more comprehensive measures are needed, such as inspecting network traffic, e.g. scanning for user activity on unsanctioned cloud apps. The consensus of the first published paper in the project is that implementing stricter IT together with better and simpler IT policies that would help mitigate the risk of Shadow IT. Although Silic does touch on using software to identify Shadow IT, such as network traffic monitoring and firewalls, the term CASB is not used specifically.

The Cloud Strife paper argues that there is a difference between Shadow IT and Cloud-Based Shadow IT. The definition of Shadow IT aligns with that of Gartner, however, a distinction is made towards cloud computing. Cloud Strife defines Cloud-Based Shadow IT to solely cloud computing-based services within an organizational context without any explicit approval. The paper identifies nine causes and effects of Cloud-Based Shadow IT. The takeaways of the causes are Business and IT misalignment, organizational considerations and employee perspectives. The takeaways of the effects are divided into negative risks: data loss, continuity, legal, performance and financial; opposite are the positive effects: innovation, productivity, cost and security.

Cloud Strife seeks to solve the negative effects by implementing a managed framework based on the following phases: prevention, detection, analysis, response and evaluation. The primary focus is upon defining organizational policies, creating security awareness, monitoring organizational aspects and (automatic) filtering/action-taking.

The author does not explicitly define the relationship between CASBs and Shadow IT, though the technology is mentioned frequently within the strategies for managing Cloud-Based Shadow IT. A naive conclusion can be made that the relationship is to be found within the ability to secure an organization's use of cloud computing, thus covering Cloud-Based Shadow IT. Cloud strife defines the following strategies for managing the risks of Cloud-Based Shadow IT: ignoring, monitoring, blacklisting, whitelisting and prohibiting. Ranging from tolerant to restrictive. On a practical level, Cloud Strife proposes to use a CASB for monitoring (detection, response), blacklisting (response) and whitelisting (analysis and response) of Shadow IT.

Based on the previous work by Silic, it can be concluded that employee awareness in conjunction with technology is needed to lower the risk of Shadow IT. Hulsebosch integrates this further by creating a framework in which both of these aspects are integrated. The main difference between both researchers is that Silic focuses on locally installed Shadow IT and Hulsebosch pivots towards Cloud-Based Shadow IT. On top of this Hulsebosch's framework allows for organizations to follow a strategy depending on how risk-averse an organization is.

Netskope indicates that the first feature of a CASB before the term was coined by Gartner to be discovery [23]. They state that discovery is the first step into obtaining visibility in unsanctioned cloud applications. Organizations are often inclined to invest in the idea of a CASB after needing to replace their Secure Web Gateway (SWG) due to lifecycle management [24]. Having previously used an SWG to be able to identify on-premise Shadow IT, they now can detect cloud-based Shadow IT with a CASB. Though vendors, such as McAfee, receive the question from their client base as to why they should implement a CASB over an SWG reporting to a Security Information and Event Management (SIEM) solution. Their answer is additional context [25]. A CASB is capable of informing an organization of in-depth information on a (non)sanctioned application. While an SWG informs the organization on a more traditional perspective such as the spam level, a CASB will assess business risks such as where the application is hosted, if the data is encrypted when at rest and data leakage history. While a SWG will report the application to be okay of use, a CASB would inform the organization to be more security-conscious. For this example, the relationship between Shadow IT and CASB is to be found within the extra contextual information that can be leveraged.

Shadow IT relates to CASB by approaching it, Shadow IT, in phases. Simply blocking Shadow IT will not solve the risks involved in the matter. Before Shadow IT can be controlled it needs to be gauged to gain visibility. This is done in the so-called discovery phase, where all the cloud usage of employees is logged. At this point, the current risk level of the organization can be determined and adjusted to fit the risk strategy. The next step is to define policies to match the risk appetite of an organization. This can be achieved in collaboration with employees to not minimize hindering their work activities. After policies are fine-tuned the third phase comes into play, where a CASB can mitigate risks against threats. A baseline has been defined on what is sanctioned and unsanctioned and behavior that deviates from this can be mitigated. By following these phases a relationship is found between Shadow IT and CASBs. With this, the second sub-question, "How does Shadow IT, including risk and mitigation, relate to CASB?", has been addressed.

6.3 Addressing Shadow IT with CASBs

CASB is often approached by categorizing its functions according to the four pillars as defined by Gartner. Based on the interviews, this research has identified visibility and control to be the main factors contributing to implementing a CASB. Organizations want to be able to assess and control the risk of cloud applications being used within an organization. The starting point of implementing a CASB entails gaining visibility through the discovery phase. The next phase is determining if the risk appetite of the cloud solutions being used, align with the organization's risk profile. After defining a policy the control element of a CASB can be enforced.

The discovery phase of CASB is very similar between all CASB vendors and not a differentiating feature, all CASBs more or less introduce the same level of visibility. What sets CASB vendors apart is the ability to provide context about the vast amount of cloud applications. It is not feasible for each organization to explore the risks that each cloud application brings with it. For this reason, all CASB providers introduce a framework to classify the risk level of a cloud application. This paper will refer to this framework using the term Cloud Index. A use case is defined to validate the Cloud Index framework of each CASB vendor. A second feature CASBs have that sets them apart is the enforcement of policy control. To see how extensive these policy control features are a second use case is defined to determine how these policies hold up in practice.

The **first use case** will evaluate the correctness of the Cloud Index data generated for each vendor. Each CASB solution has many different attributes that all sum up to a total risk score. To create a fair comparison between the CASB Cloud Index reports this research looks at the discrepancies between each CASB report based on a publicly verifiable attribute. The researchers have opted to choose an attribute that is technical of nature and objectively verifiable. A well-suited attribute is the HTTP security headers an application has implemented on its login page.

This use case has verified the validity of the security headers as listed in each CASB solution. The research's validation was verified by using Scott Helme's tool, securityheaders.com [26]. This research has revealed that all of the login pages have the five HTTP security headers enabled as can be seen in column two, Findings, in table 1. If the CASBs were to be accurate then this would require them to score 100% based on this research's findings. The results from McAfee show a total rate of 68%. Microsoft and Netskope both achieve a 48% rate. Users are offered the option to flag attributes for review if they need updating. However, it is unclear on what basis the vendors update the attributes, either it being event-based (e.g. published news), periodically, or solely triggered by users requesting a review. The URLs used for the HTTP Security Header findings can be found in Appendix B, as well as the normalization of the indexing scores and outcomes per cloud application.

Besides validating one specific attribute this research has also reviewed the overall rating a CASB attributed to a set of cloud applications. An overview of this can be found in Appendix C. Of particular interest is the finding of ProtonMail. ProtonMail advocates secure communication with its services by offering end-to-end

Header	Findings	McAfee	Microsoft	Netskope
Strict-Transport-Security	5/5	4/5	2/5	2/5
X-Content-Type-Options	5/5	3/5	3/5	2/5
X-XSS-Protection	5/5	3/5	3/5	3/5
Content-Security-Policy	5/5	3/5	2/5	1/5
X-FRAME-OPTIONS	5/5	4/5	2/5	4/5
Total rate	100% (25/25)	68% (17/25)	48% (12/25)	48% (12/25)

Table 1: Cloud Index Validation

encryption, protection of user data by strict Swiss privacy laws, secure datacenters protected with biometrics and located in a bunker 1000 meters under the Swiss alps. A blog post published in April 2018 discussed how each of their datacenters is ISO 27001 certified [27]. When reviewing (dated 06-21) this attribute in each of the vendors' Cloud Index: McAfee stated 'No', while NetSkope states 'N/A' and Microsoft states 'Yes'. The authors reached out to ProtonMail for an explanation. They stated, "...although ProtonMail as a service is not ISO27001-certified, our data center providers and servers are...". As can be observed, there is a discrepancy across the three platforms indicating that although a vendor tries to assist their clients, however self-effort is yet required to obtain an accurate understanding.

The **second use case** is aimed at exploring the enforcement of Shadow IT policy and to which degree this is possible. Not all Shadow IT is treated equal, for instance, a healthcare provider has more interest in safekeeping patient/customer information, personally identifiable information (PII), than a manufacturer. In this use case it would be beneficial for a Dutch healthcare provider to query for specific Shadow IT that relates to organizations that do not comply with GDPR and have their data center located in The Netherlands, or at the very least in the European Union (EU). Additionally, it is important to be able to employ more filters to minimize false positives. If the false positives can be kept to a minimum it opens the door for governance actions. Which makes it possible to tag the application as unsanctioned immediately. Depending on the risk appetite of the organization traffic to these services could automatically be flagged or blocked. The use case will use the following criteria: Identify personal identifiable information, GDPR compliant level, Data center housing in EU or Netherlands, Set alerts if the risk level is a medium risk or riskier, and If more than X amount of data is transferred in X time.

McAfee requires Cloud Access Policies to be configured to enforce Shadow IT discovery. With these options, it is possible to define specific User Groups to match certain criteria and have specific actions take place such as blocking. With it is possible to enforce DLP policies to identify PII. The predefined filters are very extensive. ID categorized per world region and market-space such as financial, healthcare and cryptocurrency. Hosting locations are also available and grouped in regions. The Cloud Access Policies are limited in their ability to define filters as defined in our criteria. It is not possible to select criteria based on the Cloud Index or based on traffic volume. McAfee has a Web Policy that offers more granular control of web traffic. However, this policy is applied across the entire organization making it unusable to implement on an OU basis. There are options available to generically block traffic of a certain risk level but not due to a specific attribute.

Microsoft can use DLP to detect PII information. However, this feature is mainly targeted towards the US for information such as home address, social security number, and driver license number etc. Relating this to our defined use case it is not the case that this DLP engine can find Dutch PII based on the preset expressions. One can opt to use custom expressions to achieve this. Microsoft can discover applications that are not compliant with very specific GDPR attributes such as 'right to erasure' and an overall broad GDPR readiness state. Microsoft also has the option to filter on the data center location on a per-country basis. This can also be combined with a policy to match if users have uploaded x MB of data to this service per day. All of the previously mentioned features only allow for alerting. It is only possible to block traffic when using a so-called Conditional Access App Control Policy (Reverse proxy). There is a list of featured apps that can easily be configured to enable blocking actions. However, to be able to block additional applications single sign-on such as SAML 2.0 is required.

Netskope allows for identification of PII with the use of DLP. They have defined a comprehensive list of profiles to assist in detecting various kinds of PII e.g. EU Identification to Singapore Identification as well as medical reports. Netskope has well balanced DLP profiles serving most western countries. Additionally, it is also possible to define custom DLP profiles for specific use cases. Netskope defines the GDPR level a cloud application offers in its Cloud Confidence Index but does not offer a filter to define an action based on users visiting an app that does not meet a set GDPR compliance level. Netskope does not keep a record of the data center an application uses and can therefore not meet this use case requirement. The ability to define a filter based on the overall Cloud Index score is possible. Lastly, it is not possible to generate an alert or block action if a user uploads an X amount of data within a certain period of time to an unsanctioned application.

Based on the first use case Shadow IT is addressed by the leader vendors by implementing a Cloud Index to measure the risk an organization is taking with the use of unsanctioned cloud applications. They all share an overall rating scale and multiple overlapping attributes within that scale. When comparing the validity of the attribute HTTP Security Headers they are far from accurate, with McAfee being the most accurate. These Cloud Index scores are more of a general guideline than actually being very accurate. With the second use case, it seems that all vendors apply DLP to identify personal information, to varying degrees of readily available templates. All offer options to see if an organization is GDPR compliant. Microsoft is the most extensive offering the ability to use all attributes defined in their Cloud Index and filter traffic accordingly. Both McAfee and Netskope lack in this space. Microsoft is the vendor that has the most feature-rich filtering capabilities to address Shadow IT with. With this, the third sub-question, "How do the Leaders of the Gartner Magic Quadrant (2020) address Shadow IT?" has been addressed.

6.4 Mitigating overhead from CASBs

Seven out of the nine interviewed corporate candidates indicated that administrative overhead remains to be an issue with any CASB implementation. Only service providers did not recognize the administrative overhead. All vendors acknowledged the phenomenon while stating to be able to mitigate any of the administrative overhead through multiple features. This research defines administrative overhead as unforeseen costs and manpower during or after implementation of software. Administrative overhead leads to alert fatigue within an organization, i.e. the Security Operations Center (SOC). Due to the fatigue, a CASB might possibly never reach a successful implementation within the organization and may be deemed unnecessary or merely used to comply during audits. During the literature study and interviews, this research highlights the need for a CASB though the reason why the platform is not a defacto standard within organizations, is because of either the fear of overhead or experiencing the overhead.

Microsoft published an article in which they acknowledge cybersecurity alert fatigue within a SOC and provide six mitigation strategies [28]. Besides this, they refer to an Enterprise Strategy Group study indicating "forty four percent of these alerts go uninvestigated due to a combination of talent scarcity and the multiplicity of security solutions generating a huge volume of alerts.". Microsoft states the following six mitigation strategies: threat intelligence, native integration, machine learning, watchlists, User and Entity Behavior Analytics (UEBA), and automation. This research proposes two use cases based on these strategies and have been explored as experiments within the trial environments.

The **third use case** is centered around exploring the way a CASB eases the onboarding and implementation processes. Therefore this use case has analyzed the simplicity of the CASB solution in terms of native integrations, assisting frameworks, documentation, and automation to inhibit any administrative overhead.

McAfee does this by advocating the use of their Cloud Security Advisor (CSA), which is a built-in framework assisting an organization in terms of increasing visibility and control. Its purpose is to showcase the amount of visibility that is established, taking the outcome and comparing security metrics to selected McAfee peers while providing recommendations on areas to improve. The CSA provides implementation improvements in terms of Software-as-a-Service, Shadow IT and Infrastructure-as-a-Service. For example, it will guide an organization on enabling a log collector to start the discovery of Shadow IT. The CSA also integrates with the MITRE ATT&CK framework. McAfee also offers bidirectional native integration with SIEM platforms supporting Common Event Format (CEF).

Microsoft in comparison has no built-in assisting framework, though a quick-start can be found and the MITRE ATT&CK framework is implemented for correlation. They highlight their publicly available library of documentation in which they offer quick-starts, tutorials, concepts and how-to's in a textual form. Besides this, they offer two pre-made SIEM integrations for Microsoft's Azure Sentinel and MicroFocus's ArcSight while enabling any SIEM supporting Common Event Format (CEF). Though based on the documentation it is only possible to have one way-traffic, sourcing from the CASB to the SIEM. Which might cause the CASB to flood with alerts without handling the alerts in the solution itself, defeating the purpose of having one centralized platform.

Netskope is lacking both an intuitive assisting framework and built-in documentation. Though Netskope emphasized being able to provide an organizational specific onboarding and implementation project during an interview. No information was found within Netskope's CASB solution in terms of integrating with a SIEM platform. Though Netskope did indicate afterwards through contact being able to do so, backed up by publicly available whitepapers. For example, one paper indicates that Netskope is capable of integrating with SIEM solutions such as QRadar while also being the first CASB to mention SOARs such as Splunk Phantom. Like the other CASBs, Netskope also mentioned their ability to integrate with any solution supporting Common Event Format (CEF). The highlight of Netskope was to be found within their capability of integrating with Security Orchestration Automation and Response (SOAR) platforms. Such platforms are capable of implementing machine learning and automation from a centralized manner.

The **fourth use case** is centered around exploring the possibilities to align CASB policies with an organizational structure. For example, an institution should be able to set specific policies for business operations while maintaining a different set of policies for researchers. This is done by validating if the CASB solution is capable of enforcing a so-called multi-tenancy technique. An analysis will be performed during the familiarization of the provided trial environments while consulting vendors and their documentation.

The reviewed CASBs reached similarity in terms of ingesting data, though having each of their terms for it, allowing in-line solutions (forward/reverse proxy or endpoint agents) and out-of-band protection (API's or endpoint agents). Though the differentiation is found within applying the policies and accompanying structure. Another similarity found across all platforms is the handling of user groups, which require to be imported through an external source such as an Active Directory or LDAP server.

McAfee appears to be limited in terms of reaching a multi-tenancy environment. Matters that have been reviewed, are the way McAfee implements web traffic, data loss prevention, and access policies. For example, when applying a web policy, scoping rules can be set based on location, IP's, users or user groups. Though this ruleset is then only defined for the given scope and the ruleset can not be applied again on a different scope. McAfee's data loss prevention and access policies do allow more in-depth refining in terms of applying different policies per user attributes, such as groups, IP addresses or agents though the documentation around these are lacking and require a steep learning curve.

Microsoft is capable of filtering before setting a scope within a policy. It does this by creating reports on data sources that can be scoped on user groups, IP tags, or IP ranges. When having such a report in place set on a specific user group, policies can be applied to merely this report. For example, a Shadow IT application discovery policy can be set to trigger alerts only for a report set on the Sales & Marketing Organizational Unit (OU) while a different policy is defined for the Security Team OU.

Netskope does this similar to Microsoft where they do filtering on ingested data. For example, it is possible to have a group of users only send their web traffic (HTTP and HTTPS) to Netskope for analysis while traffic for a set of applications (DNS) can be

disregarded for analysis. A policy can then be set on a specific user group source while the destination can be a category of websites (e.g. gambling). Thus a practical example would be to set all traffic, i.e. transparent proxy, for the marketing department to be sent while the IT department only sends out specific applications for analysis.

Besides these experiments, potential mitigations strategies were also highlighted via the corporate interviews. An example would be to run a pilot immediately after a CASB implementation with a Managed Security Service Provider (MSSP). This provider would do the initial trajectory of fine-tuning according to the needs of an organization. They will mitigate the overhead so that it is possible to transfer control back to the organization to continue a successful implementation.

The explored CASBs mitigate administrative overhead each in their own way. McAfee excels with their assisting framework, Microsoft does this with their documentation while Netskope takes a more personal approach. McAfee lacks in-depth policing for organizational structures while Microsoft and Netskope exhaust this extensively. Via the help of native integration with a SIEM platform alerts can be ingested so that correlation can be made within one centralized platform instead of having security analysts monitor the CASB separately. Besides this, a SIEM is often already successfully implemented and fine-tuned to the way of working of the security analysts. Having implemented the CASB according to the approaches of the vendors, an organization should not have to worry about the CASB solution itself. Administrative overhead can be mitigated, or prevented, by selecting a vendor that suits the initial needs of organization the most including the onboarding trajectory. The second way is with the built-in possibility to integrate with SIEM solutions, or even further as more vendors will integrate with automation platforms such as SOARs. A third way of mitigating overhead is being able to enforce policies according to the needs of an organizational structure, e.g. business operations versus independent institution researchers. The fourth and last way this research found was to pilot with an MSSP and let them fine-tune the onboarding. With this, the fourth and final sub-question, "How can a CASB be implemented in such a way that the responsible party is capable of managing the administrative overhead generated by CASBs?", has been addressed.

7 DISCUSSION

This section will discuss the limitations and impact these have on the paper.

This research interviewed companies within the Dutch marketplace and consisted mainly within the field of professional services, managed security service providers, telecommunications, and an academic institution. Besides this the interviews were semi-structured by design, making the outcome of the interviews colored to a certain degree. If other sectors would have been interviewed, different expectations than described the current demographic could have been made. The CASB market alignment with corporate expectation was made between the paper's demographic and vendors listed by Gartner as leaders in 2020. Differing between these two foundations may result in other conclusions.

The first use case verified the validity of data provided by the CASBs in regards to the HTTP security header attribute. Each CASB solution does inspect HTTP security headers, however, they do not specify which URL the score is based on. This lack of transparency makes it difficult to interpret the actual results of the HTTP hardening score. This case study has opted to scan the login pages for each specific service and compare this with the results published by the CASB. Our preliminary research identified that the HTTP security headers used on the main URL pages of a vendors varies greatly from the login pages. This research opted to use login pages since this can be seen as the gateway to an application.

It is difficult to obtain a fair comparison of attributes between each CASB report since many reporting attributes are specified differently. E.g. on the surface, comparing if an organization has been ISO 27001 certified may seem to be a fair comparison. However, the degree to which an organization is certified can vary greatly. The certification could be limited to the data center where the application itself is hosted rather than the application itself. Depending on how the CASB vendors interpret this results can vary in their Cloud Index. Besides this, the ISO certification of a company is not always publicly available. It would be beneficial to include more CASB attributes in future research.

The second use case, evaluating the ability to enforce a fine-grained Shadow IT policy as defined earlier was very specific. This research was influenced by the Cloud Index score and attempted to introduce filters based on this information. Introducing additional use cases, from another perspective than the Cloud Index, could very much influence the results of the capabilities of the CASB platforms. Therefore, to gain a more balanced approach additional use cases should be investigated in future research.

The third and fourth use case relied on the given trial environments. The authors of this paper reached out to a total of eight vendors (listed by Gartner, focus on leaders), which resulted in three environments. The use cases were explored within these three and other outcomes could have been made when different environments were made available. Our use cases are based on the functionality as seen within the CASBs. The research use cases could therefore be tainted by the knowledge we have acquired during the exploration of the CASB platforms. A different approach could have been taken by inquiring the interviewees explicitly on which use cases they would deem relevant within a CASB.

8 CONCLUSIONS

The main research question is set out to address if the functionality that CASB vendors deliver matches the corporate expectations. The importance of CASBs has grown due to the COVID pandemic and has led to a rise of employees becoming caretakers of their own infrastructure. In practice, there is a shift towards cloud applications, which hampers the visibility of applications being used within an organization (Shadow IT). To support the main research question the following sub-question has been defined: "How do market guides and corporations define a CASB?". Based on the text analysis findings of market guides this research has determined that vendors tend to define a CASB to be a service that extends the reach of security in the cloud, with a focus on the topic of security. Interviews with vendors indicate the main reason why

organizations implement a CASB is to gain more visibility and control. Interviews with the user base confirm that the immediate goal is to gain visibility in the use of Shadow IT. The security aspect is of lesser immediate importance but seen as a beneficial addition when a CASB reaches a successful implementation. Providers indicated that a CASB is recommended, or introduced, when an organization is trying to increase compliance, discover Shadow IT or replace software and hardware (e.g. gateways). Based on input from the service providers, the user base and perspectives this research proposed the following CASB definition: Software that addresses security gaps in an organization's cloud usage by extending security policies leveraged from on-premise to the cloud.

To further this research the following sub-question was posed: "How does Shadow IT, including risk and mitigation, relate to CASB?". One of the key roles of a CASB is to identify and aid in controlling Shadow IT. Within the context of a CASB this research identified Shadow IT specifically to be cloud applications. The feature used to identify and gain visibility over Shadow IT with a CASB is referred to as the discovery phase. Completing this phase enables identifying the risk exposure of cloud applications being used within an organization. The second phase can commence with raising awareness for Shadow IT being used and engaging with employees to identify which Shadow IT applications fit within the risk appetite of an organization. What follows in phase three is the mitigation of unsanctioned apps that do not fit the organizations' risk profile. This research advocates that the relationship between Shadow IT and CASB is found within the extra contextual information that can be leveraged for an organizational perimeter.

To extend this research between theory and practice, exploration has been conducted in trial environments. This was done via the following sub-question, "How do the Leaders of the Gartner Magic Quadrant (2020) address Shadow IT?". One of the features that all CASBs offer is a Cloud Index rating to assess the level of risk an organization faces when using those cloud applications. This research identified the accuracy of Cloud Index provided within the CASBs based on the HTTP security header attribute to be weak in its accuracy. McAfee obtained a success rate of 68% versus 48% for Microsoft and Netskope. CASBs were also explored in their effectiveness in being able to filter Shadow IT based Cloud Index attributes, and user behavior. Microsoft offers the most comprehensive filtering policy with the ability to cross-reference the filter policy with data in the Cloud Index combined with user behavior. McAfee and Netskope both lack in this respect. Each vendor, although having similarities, is trying to address Shadow IT in its own way. It is impossible to agree on one winning method, as it will always boil down to the needs of an organization.

A much-heard phenomenon during this research was administrative overhead generated by CASBs. Therefore the practical approach of this research explored mitigation considerations by posing the following sub-question, "How can a CASB be implemented in such a way that the responsible party is capable of managing the administrative overhead generated by CASBs?". This research has proposed two use cases to answer this question and the outcome of these use cases has led to four approaches to implementing a CASB. The first approach is scoping based on matching your needs with the onboarding procedures trajectory offered by the CASBs. The second approach, is verifying if the CASB integrates with an already implemented SIEM and or SOAR solution. The third approach, determine if your organizational structure requires varying enforcement of policies and verify if the CASB supports this feature. The fourth and last approach is to have an MSSP aid in implementing the CASB and take the lead in fine-tuning the solution to suit the organizations' needs during a pilot phase. By employing these approaches administrative overhead can be kept to a minimum.

When reviewing the main question of the paper, "How do market-leading CASBs align with corporate expectations?", this research can conclude that there is a misalignment between the level of requirements of the Dutch marketplace relative to the feature set the CASB vendors offer. Most organizations are not mature enough to effectively weigh the feature set each CASB vendor has to offer. Making it difficult for them to assess if the features offered meet their present and also future requirements. CASB vendors have put considerable effort into developing a Cloud Index framework to determine the risk of cloud applications. Though when validating a specific portion of this framework, discrepancies can be found across vendors and an organization is required to exhaust resources themselves. Overall, the possibility to define policies on a fine-grained level to address Shadow IT is lacking, with Microsoft being the exception. CASBs do align with corporate needs to integrate them in existing solutions such as SIEM and SOAR platforms. While this research advocates organizations and vendors to reach a middle ground in terms of onboarding. A successful implementation is dependent on this phase and this research indicates that alignment can be reached through adequate scoping of needs, native integrations, applying organizational structure and piloting with a managed security service provider or the use of assisting frameworks. The conclusive answer to the main question is "Leading CASBs are ahead of corporate expectations in regards to the feature set. While vendors are extending their capabilities, or even moving to SASE, organizations are hesitant to implement a CASB while acknowledging the need of one".

9 FUTURE WORK

The authors agree that future work should focus on analyzing the Cloud Indexing scores of CASBs more in-depth. As such, a specific use case was written for this research. This research explored the Cloud Indexes on a specific level whereas the authors think more comprehensive research into the differences between CASBs is beneficial. To obtain a more comprehensive analysis of the Cloud Index of each provider, as done in use case one, more attributes would need to be compared.

Furthermore, the authors agree that a case study implementation would be beneficial to close the gap between theory and practice further. If time had allowed, the authors would have selected a vendor based on the outcomes of this research and conduct a proof-of-value for a client. Another practical research that the authors propose is to review the integrations with external tooling such as SIEM and SOAR platforms.

The industry trend is now shifting towards a Secure Access Service Edge (SASE) platforms to secure cloud native services. CASB is a vital element within a SASE and vendors are migrating from a standalone CASB solution to SASE platforms. The authors agree that research into this trend would explore if CASBs were a steppingstone to SASE platforms.

ACKNOWLEDGMENTS

This work was supported by KPMG, in specific by Ruud Couwenberg MSc (Senior Cyber Security Consultant). We greatly thank Ruud for his supervision and guidance. We also thank all the participants, corporate and vendors, for their willingness to be interviewed. Besides this, we acknowledge all of the contributions provided by the external reviewers.

REFERENCES

[1] Aakash Jain. *COVID-19 Security Impact: Rise of Shadow IT*. 2020. URL: https://awakesecurity.com/blog/covid-19-security-impact-rise-of-shadow-it/.

[2] *perception gaps in cyber resilience: where are your blind spots? the hidden risks of shadow it, cloud and cyber insurance*. URL: https://www.ncsc.govt.nz/assets/NCSC-Documents/Perception-Gaps-in-Cyber-Resilience.pdf.

[3] Melanie Steinhueser et al. "Knowledge Management without Management-Shadow IT in Knowledge-Intensive Manufacturing Practices". In: (2017).

[4] Craig Lawson Steve Riley. "Magic Quadrant for Cloud Access Security Brokers". In: *Gartner* (2020).

[5] *Notice of data event related to Pennsylvania contract tracing*. URL: https://insightglobal.com/notice-of-data-event.

[6] *Contract tracing breach impacts private info of 72K people*. URL: https://apnews.com/article/coronavirus-data-privacy-technology-business-health-4b9a172a90bc1a82f83e6a44ff06a445.

[7] Luciana Obregon. "Technical Approach at Securing SaaS using Cloud Access Security Brokers". In: *Information Security Reading Room* (2017).

[8] Broadcom. *The differences between Explicit proxy and Transparent proxy*. 2017. URL: https://knowledge.broadcom.com/external/article/166958/the-differences-between-explicit-proxy-a.html.

[9] M.A.C Hulsebosch. "Cloud Strife : an analysis of cloud-based shadow IT and a framework for managing its risks and opportunities". University of Twente, 2016.

[10] Peter Firstbrook Neil MacDonald. "The Growing Importance of Cloud Access Security Brokers". In: *Gartner* (2012).

[11] Craig Lawson Brian Lowans Neil MacDonald. "Market Guide for Cloud Access Security Brokers". In: *Gartner* (2015).

[12] Steve Riley Craig Lawson. "Magic Quadrant for Cloud Access Security Brokers". In: *Gartner* (2017).

[13] Shabnam Kaur and Rajandra Gupta. "Enhancing Features of Cloud Computing Using Cloud Access Security Brokers to Avoid Data Breaches". In: *European Journal of Engineering and Technology Research* 4.10 (2019), pp. 185–189.

[14] Bimlesh Wadhwa, Aditi Jaitly, and Bharti Suri. "Making sense of academia-industry gap in the evolving cloud service brokerage". In: *Proceedings of the 1st International Workshop on Software Engineering Research and Industrial Practices*. 2014, pp. 6–9.

[15] *Understanding Shadow IT risks, benefits and opportunities*. URL: https://www.researchgate.net/project/Understanding-Shadow-IT-risks-benefits-and-opportunities.

[16] *Is CASB Alone Enough? Long Live SASE*. URL: https://www.paloaltonetworks.com/blog/2019/11/cloud-casb-sase/.

[17] *Is CASB Alone Enough? Long Live SASE*. URL: https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/.

[18] *Cloud Access Security Brokers (CASBs), Gartner Glossary*. URL: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs.

[19] "Analysis of the Global Cloud Access Security Broker Market (CASB), Forecast 2021". In: *Frost & Sullivan* (2017).

[20] Jay Heiser Craig Lawson Neil MacDonald. "Technology Overview for Cloud Access Security Broker". In: *Gartner* (2015).

[21] *Shadow It, Gartner Glossary*. URL: https://www.gartner.com/en/information-technology/glossary/shadow.

[22] *What Is Shadow IT?* URL: https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-shadow-it.html.

[23] *Is there a Gartner CASB Magic Quadrant?* URL: https://www.netskope.com/blog/gartner-casb-magic-quadrant.

[24] *Interviews with Corporate*.

[25] *Why do I need a CASB for Shadow IT when I already have a SIEM?* URL: https://www.mcafee.com/blogs/enterprise/cloud-security/why-do-i-need-a-casb-for-shadow-it-when-i-already-have-a-siem/.

[26] Scott Helme. *Security Headers*. 2021. URL: https://securityheaders.com/.

[27] *ProtonMail's world-class reliability is now backed by a 99.95% service level agreement (SLA)*. URL: https://protonmail.com/blog/protonmail-reliability-sla/.

[28] *6 strategies to reduce cybersecurity alert fatigue in your SOC*. URL: https://www.microsoft.com/security/blog/2021/02/17/6-strategies-to-reduce-cybersecurity-alert-fatigue-in-your-soc/.

Below is a complete overview of appendixes used to complete the research.

A APPENDIX: INTERVIEW TOPICS

Below are generic questions which were used to interview vendors and corporations. Interviews were held in a dialogue manner and questions were not handled as ticking boxes but intervened into the interview.

Vendor specific

- Can you tell us something about yourself?
- How does your company define a CASB?
- What is your perception regarding CASB and the landscape it operates in? In other words, how would you characterize the market?
- What is your perception regarding Shadow IT?
- What risks are accompanied to Shadow IT? Does your solution localize these risks and their potential mitigations?
- What is the advantage of a CASB over a SASE solution? Or do they intervene?
- What are the main features that your solution implements that differentiates it from its competitors?
- What is your experience with the "overhead" once a CASB has been implemented?
- Who do you consider to be your main competitors and why?
- Can we obtain a trial platform for our research? If not, could we have access to any of the platform's documentation so that we can analyze these?
- There are multiple degrees of forward proxy, completely transparent and explicit (certain ports, dns or ip based) How does your proxy implementation work?
- Would you like to add anything else? If not, thank you for your time.

Corporate Specific

- Can you tell us something about yourself?
- Can you tell us something about the organization you are working for?
- What is your perception regarding Shadow IT?
- What risks are accompanied to Shadow IT for your organization?
- Could you share what type of Shadow IT software is being used, what type of users do so and their reason behind it?
- How is your organization dealing with Shadow IT?
- If CASB deployed: Why did your organization choose to deploy a CASB solution?
- If no CASB deployed: Have you looked into a CASB solution to solve the risks of Shadow IT? If yes, why have you not deployed one? If not, is there any reason why not?
- What is your perception of CASB in the marketplace? Is this a growing trend or is the CASB solution mature or being replaced by alternative solutions?
- If CASB deployed: What changes did your organization go through after the deployment of a CASB solution?
- If no CASB deployed: Are there any plans on the road map to implement a solution to manage the risks of Shadow IT more?
- If CASB has been deployed: Which deployment method did you opt for and why?
- Would you like to add anything else? If not, thank you for your time.

B APPENDIX: CLOUD INDEX COMPARISON

Vendors each have a rating scale to judge the risk of an app. Table 2 shows the normalized risk score to be able to make a comparison between the Cloud Index score of each vendor.

Risk	McAfee	Microsoft	Netskope
Low	1-3	10-8	100-90
			89-75
Medium	4-6	7-4	74-60
			59-50
High	7-9	3-0	49-0

Table 2: Cloud Index Rating Normalization

HTTP Security Headers findings per cloud application: Results as per June 16, 2021. The domains that have been validated are the login page or subsequent redirect to a login portal. The primary domain often has less HTTP security headers enabled than the login pages.

Header	Findings	McAfee	Microsoft	Netskope
Strict-Transport-Security	Yes	Yes	No	No
X-Content-Type-Options	Yes	Yes	No	Yes
X-XSS-Protection	Yes	No	Yes	No
Content-Security-Policy	Yes	No	Yes	No
X-FRAME-OPTIONS	Yes	Yes	No	Yes
Total rate	5/5	3/5	2/5	2/5

Table 3: Cloud Index Validation login.salesforce.com

Header	Findings	McAfee	Microsoft	Netskope
Strict-Transport-Security	Yes	No	No	No
X-Content-Type-Options	Yes	No	No	No
X-XSS-Protection	Yes	No	No	Yes
Content-Security-Policy	Yes	No	No	No
X-FRAME-OPTIONS	Yes	No	No	Yes
Total rate	5/5	0/5	0/5	2/5

Table 4: Cloud Index Validation cloud.digitalocean.com

Header	Findings	McAfee	Microsoft	Netskope
Strict-Transport-Security	Yes	Yes	No	No
X-Content-Type-Options	Yes	Yes	No	No
X-XSS-Protection	Yes	Yes	No	No
Content-Security-Policy	Yes	Yes	No	No
X-FRAME-OPTIONS	Yes	Yes	No	No
Total rate	5/5	5/5	0/5	0/5

Table 5: Cloud Index Validation sso.redhat.com (OpenShift)

Header	Findings	McAfee	Microsoft	Netskope
Strict-Transport-Security	Yes	Yes	Yes	Yes
X-Content-Type-Options	Yes	Yes	Yes	Yes
X-XSS-Protection	Yes	Yes	Yes	Yes
Content-Security-Policy	Yes	Yes	Yes	Yes
X-FRAME-OPTIONS	Yes	Yes	Yes	Yes
Total rate	5/5	5/5	5/5	5/5

Table 6: Cloud Index Validation dropbox.com/login

Header	Findings	McAfee	Microsoft	Netskope
Strict-Transport-Security	Yes	Yes	Yes	Yes
X-Content-Type-Options	Yes	Yes	Yes	Yes
X-XSS-Protection	Yes	Yes	Yes	Yes
Content-Security-Policy	Yes	Yes	No	No
X-FRAME-OPTIONS	Yes	Yes	Yes	Yes
Total rate	5/5	5/5	4/5	4/5

Table 7: Cloud Index Validation account.protonmail.com

C APPENDIX: CLOUD INDEX CORRELATION AND DETRACTIONS BETWEEN CLOUD APPLICATIONS

Salesforce

Both Microsoft and Netskope deem Salesforce to be a low risk cloud application. McAfee has determined that Salesforce to be a medium risk. The reason McAfee rates Salesforce lower is due to the fact that they supposedly lack in the encryption front. Microsoft and Netskope both indicate that the data at rest is encrypted. McAfee indicates that this has last been reviewed in March 2021, whereas Microsoft updated this in October 2019 and Netskope in January 2021.

DigitalOcean

All three CASB solutions have indicated DigitalOcean to be a medium or medium/low risk. McAfee lists that a major impact on the risk score is due to DigitalOcean disclosing a breach in the past 1 to 3 months and not performing penetration tests on a regular basis. Microsoft also determined that they do not perform penetration testing and confirmed the latest breach to be in April 2021. Additionally, Microsoft reports a medium risk in the categories security and compliance. Netskope neglects to report that there has not been a breach in the past year. The Netskope categories auditability (no published audits) and privacy factors (sharing user information with third parties) are the factors that adversely affect the Cloud Index score.

OpenShift

OpenShift receives a medium risk score from McAfee, Microsoft rates them with a low risk score, and Netskope indicates them to be a high risk. McAfee attributes this risk due to a published CVE dating back to 2012, and not encrypting data at rest and backups. Microsoft also indicates that data at rest is not encrypted but does not mention backups. The main negative contributors according to Microsoft are medium risk in the category security and legal. These attributes are such as missing HTTP security headers and not preserving the user's ownership of data to name a few. Netskope's risk score is influenced by every category having a negative impact except for access control. Many attributes are negatively impacted by not being published by the vendor.

Dropbox

All three CASB vendors indicate Dropbox to be a low risk cloud application. McAfee indicates that the service does not publicize if the backups are encrypted and if so, with which encryption algorithm. Microsoft's only critique on Dropbox is in the category compliance, where dropbox is not in compliance with SOX, FINRA etc. Netskope indicates that the privacy level of their mobile and browser applications impact their risk score adversely.

ProtonMail

McAfee rates ProtonMail with a low risk score, whereas Microsoft and Netskope assess it as a medium risk. McAfee identifies the most risky drawbacks to be the lack of support for identity federation, lack of support for directory services integration, and not having datacenter security. Microsoft penalizes ProtonMail for not being conforming to many regulatory compliance requirements and lack of preserving the user's data ownership. Microsoft, also has many attributes that are missing a qualification.