Cloud Access Security Monitoring: To Broker or Not To Broker?

Understanding CASBs

Olga Kulikova MSc CCSK

When moving to the cloud, enterprises need to manage multiple cloud services that can vary significantly from one to another. This, together with the modern culture of working anywhere, anytime, from any device, introduces multiple security challenges for a company to resolve. The article explores the possibility of deploying Cloud Access Security Brokers (CASBs) to help enterprises stay in control of their information security when using various cloud services.

O. Kulikova MSc CCSK
is a senior consultant at KPMG.
kulikova.olga@kpmg.nl

Introduction

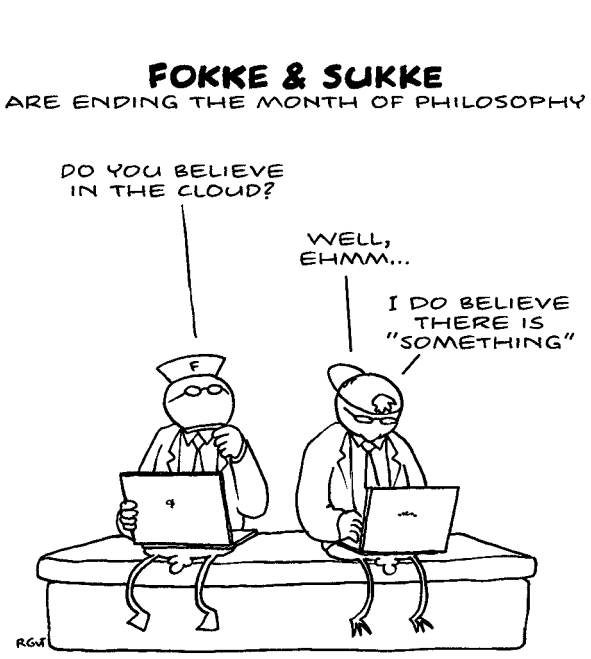
This year many Dutch companies were busy with cloud transformation programs, moving towards the "Cloud First" goal of their future enterprise IT. One of the key challenges enterprises are starting to face when moving to cloud is that it is extremely hard to ensure security for a variety of cloud services, each with their own unique settings and security controls, compared to the management of on-premises systems and applications. In addition, the mobility of the modern workforce is higher than ever before, when employees can easily access cloud systems and applications when off-premises and using personal devices or personal identities, not managed by the enterprise IT. This new context for enterprise IT – multiple clouds and extreme mobility, makes it hard for companies to keep up with all security risks that this new context introduces. This article examines the case of Cloud Access Security Brokers (CASBs) – a possible solution for the security of multiple cloud services in the operation of a mobile enterprise.

A State of Cloud Security in 2016

A famous Fokke & Sukke cartoon asks "Do you believe in the cloud?" ([RGvT12]). 2016 is finally the year where many of our clients are not only saying "Yes, we believe there is something", but they are already in the middle of execution of their cloud related programs. Moving to AWS, or Azure infrastructure, shifting to Office 365 for e-mail and collaboration are no longer unique use cases for the Netherlands. Cloud is transforming from being just one out of many projects within IT to serving as an actual context for the enterprise IT existence. A typical company of 2016 is already using IaaS with their VMs running somewhere in the cloud, PaaS utilized for apps development and management, and quite possibly its CRM, ERP, e-mail or collaboration software has already been procured as SaaS. The fact that becoming a cloud user only requires a few clicks on the web and completing credit card details increases cloud adoption even more, making enterprises going off-premises just a matter of time, money, and Internet existence.

It is great to be in the middle of this enterprise transformation – when cloud technologies are becoming an essential part of IT programs. Enterprise IT was revolutionized by the Internet, and Cloud (and mobile) technologies continue this move by further liberating the workforce from the office space, and bringing offices to employees homes. Still, without proper awareness and good risk programs, situations endangering the security of organizational information can easily happen.

Consider the following example. Many corporations use cloud storage solutions for their work, for example – Microsoft OneDrive or Google Drive. When they want to share documents outside the organization, they invite external users to join their cloud folder for example in Microsoft OneDrive. An invitation is usually sent to a work e-mail address of the external user with a link to join the cloud folder. Often, due to certain settings in Microsoft, if a user



already has a private Microsoft account, he can access the shared business folder with this account. All he needs is just the link; there are no other enforced authentication mechanisms. And here comes a risk for the business. Links can be easily shared; and what about finding and proactively removing all those private accounts joining a corporate cloud environment?

To address these questions and concerns, you would typically see organizations start using the combination of the words "cloud", "security", and "risk management". The problem here lies in the amount of different cloud services a company needs to manage to ensure security of their critical assets. The ideal situation would be that the shift to these multiple cloud services is performed in a risk neutral way, meaning staying risk-comparable with the previous IT set up. However, it is hard to ensure security for a variety of cloud services, with their own unique settings and security controls, compared to the management of on-premises systems. Most of the cloud security risk workshops we facilitated for our clients were aimed in addressing security issues for particular cloud solutions like Office 365, Salesforce, Google for Work, Evernote, etc. While a good exercise in general, such workshops only address a particular cloud service. The strategic question would be – what should be a sustainable approach to the security of multiple, if not *all*, cloud solutions in the operation of an enterprise.

CASB – A Silver Bullet for Enterprise Cloud Security?

International organizations like ENISA, CSA, NIST, ISO have produced multiple articles and best practices in attempt to standardize the approach for security of cloud solutions. Yet, key cloud speakers at the 2016 RSA Conference, admitted that finding a unified way to ensure the security of cloud services is still under investigation and construction ([Fult16]). One of the key initiatives since 2015 is the Cloud Security Open API – an initiative driven by the Cloud Security Alliance to ensure that in future all cloud services and enterprise security monitoring tools can "talk" using the same APIs ([CSA15]). This will allow standardization of the security of the cloud stack and eliminate the headache of designing unique security controls for different cloud services.

While Cloud Security Open API remains work in progress another, and more importantly already existing, approach for cloud security, was mentioned multiple times during the RSA. Many presentations were talking about Cloud Access Security Brokers, or CASBs, in such a way that made them sound almost as a silver bullet for cloud security. The term "CASB" was introduced by Gartner several years ago as one of the key ways to control the business risks when moving to cloud ([Gart16]). The CASB market has grown significantly since then and is now blooming with multiple providers offering cloud security services, such as SkyHigh Networks, CloudLock, Elastica, Netskope, Adallom. Some of them have been acquired by the IT giants such as Microsoft (Adallom), BlueCoat (Elastica) or Cisco (CloudLock) to name but a few.

If you look at the market acceptance of CASB solutions ([TMR16], [MM15]), then North America and Asia-Pacific are the main regions embracing the CASBs, compared to the lower adoption rates within Europe. With the forecasted growth of the CASB market from USD 3.34 billion in 2015 to USD 7.51 billion by 2020 ([MM15]), the question is why Europe, and the Netherlands in particular, seem to have less interest in acquiring CASBs as a means to control their cloud services? In the remaining part I will explore the key benefits, drivers and pre-requisites for adopting a CASB solution, to highlight the potential of CASBs in the enterprise cloud security.

Key Security Features of CASBs

I have created Figure 1 in an attempt to illustrate the full scope of the CASB offering – why, what and how they deliver their services. CASB business case starts with the technological context in which modern corporations operate. Think about the ways in which employees can access cloud resources nowadays. They can do it by being on the enterprise network (on-premises), or on any other network (off-premises). They can login from the enterprise managed devices, such as corporate laptops and mobile devices with installed MDM, or using their private laptops and smartphones. Finally, an employee can use his work

or private identity to login to the cloud service (as in my example in the beginning of this article).

CASBs can help companies enhance security for all these scenarios. CASB software provides multiple security features, ranging from discovering cloud services used by employees, highlighting key risks of such usage, protecting data stored and processed in cloud, providing end user behavior analytics and performing some form of malware and threat prevention. In short, CASBs are monitoring in real time what is going on with the enterprise cloud – its ins and outs. CASBs can deliver on their promises due to their ability to integrate with already existing security tools, by analyzing traffic as a reverse or forward proxy, and by connecting directly to cloud services via their APIs (for more architecture details, refer to Gartner publications [Gart15a] and [Gart15b]).

To summarize the key security features that CASBs can deliver:

- *Cloud visibility.* CASBs help enterprises to discover all cloud applications used by the enterprise employees and associated business risks. This addresses the issue of "Shadow IT" or unsanctioned apps within a company. The cloud discovery analysis will show, for example, how many different storage solutions, such as Google Drive, OneDrive, Box, Dropbox, Evernote, etc. are in use by an enterprise employees, and what the risk rating of each of those services is. To note, many enterprise on-premises tools, such as Secure Web Gateways (SWGs), can already show where their traffic goes. The advantage of CASBs is that they can also monitor traffic from users that are off-premises, and that CASBs have a large database of cloud services assessed regarding their potential security maturity that a company can rely on.
- *User behavior analytics.* CASBs can provide real-time monitoring of user activities, including high-privileged actions, and alerting or blocking strange behaviors (for example, an employee downloading a large volume of data, the same user account used from different locations within a short period of time, or a user using his work-identity to connect to cloud services for private use). While many big SaaS providers also offer DLP-like functionalities, the advantage of CASBs is that rules for user behavior analytics can be set up one time and across multiple cloud platforms.
- *Data security.* CASBs can act as Data Loss Prevention tools with the help of data-centric security policies such as alerting, blocking, encrypting or tokenizing data that leaves to go to the cloud. With respect to encrypting/ tokenizing data, a client can choose whether to encrypt all data (less recommended) or only specific files and fields.
- *Malware detection.* CASBs can help companies identify and cure malware across cloud solutions that offer API integration, such as Amazon S3, Office 365, Google for Work, and by integrating with on-premises or online anti-malware solutions and anti-virus engines. CASBs can also prevent certain devices and users from accessing cloud solutions, if required to stop malware spread.

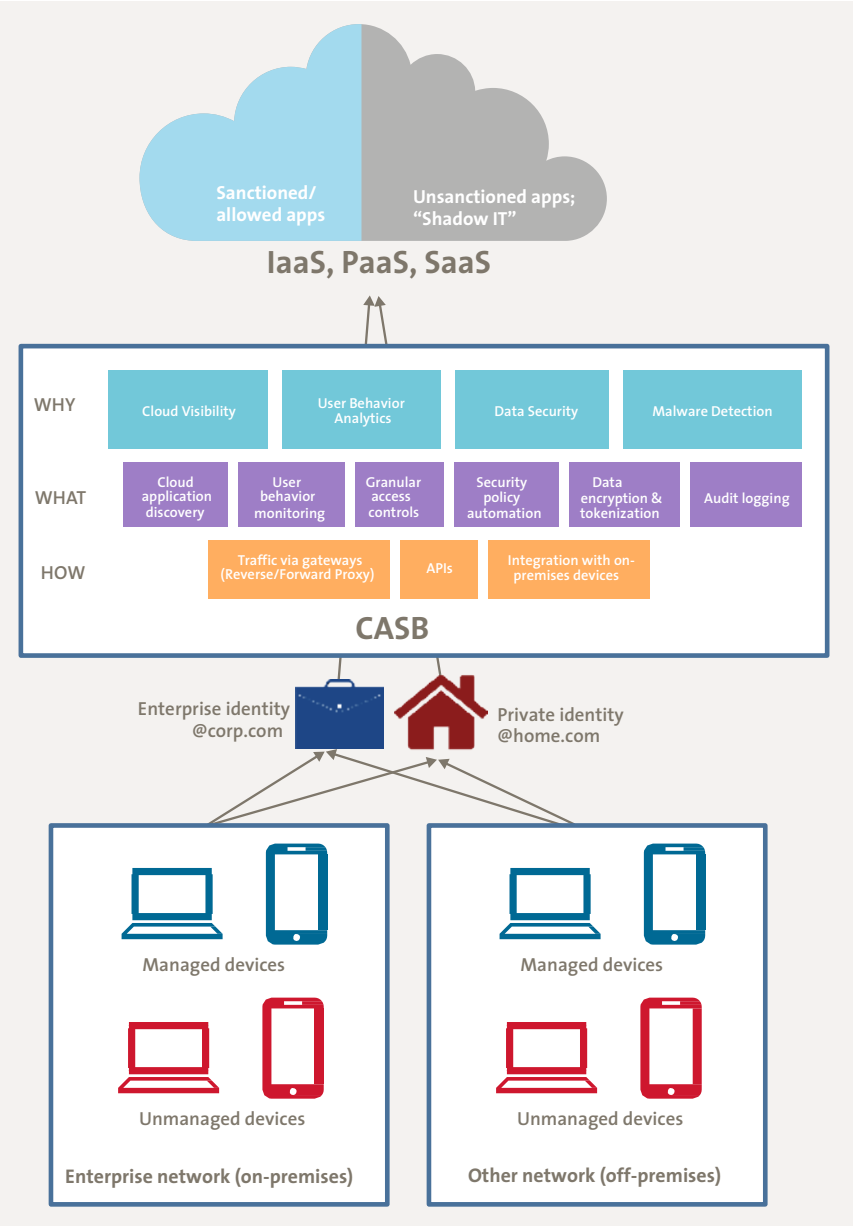


Figure 1. **Organizational assets versus CASBs capabilities.**

Practical Take-Aways

KPMG has been working with CASBs in recent years, for example, as part of Cloud Security Readiness Assessment projects. Below are some of my key observations from using CASB tools at our clients about what a company wanting to adopt a CASB should consider:

CASBs are monitoring in real time what is going on with the enterprise cloud – its ins and outs

- *Do not just purchase a well-known CASB, clarify the use-cases first.* Understanding the use cases for which a company plans to deploy CASBs is very important. Is the client considering monitoring the user behaviors in specific SaaS or controlling overall traffic? Is just a compliance check needed when reports are being generated showing where the corporate data goes? What about access to the cloud from (unmanaged) mobile devices, does the client also want to know about this? The answers can largely affect the choice of which potential CASB provider to opt for.
- *Do not rely on default CASB settings, set up the right security policies.* CASBs rely on rules or policies to generate security alerts, classify them and push that information to the built-in dashboards or to a client's SIEM. An example would be sending an alert whenever a file with credit card data is being uploaded to the cloud, or if a user from a certain country is trying to access a cloud service. Many security operation departments lack the staff to keep up with all the alerts, and adding alerts from CASBs only aggravates the situation. Ensuring the strict policies will guarantee that the additional alerts bring actionable information and not just more noise.
- *Integrate with the enterprise IAM for the maximum benefit.* To achieve the most from CASB functionality, such as the ability to alert on access to cloud services from unusual or prohibited locations, or prevent access to cloud services from unmanaged devices, it is essential that a company can connect to CASB with its enterprise Identity and Access management system (can be either on-premises IAM or IDaaS). Done correctly this will reduce the risk of unauthorized access to cloud services. For more information on using IAM for cloud solutions, please refer to [Stur11] and [Muru16].
- *Connect to cloud/on-premises SIEMs.* Having one source of alerts has proven to be a better and easier way for your employees to monitor and react on cloud anomalies. Many companies already use, for example Splunk, dashboards and other on-premises security and event monitoring systems (SEIMs). Many CASBs vendors allow integration with these tools.
- *Streamline users to specific cloud providers.* Finally, once a company understands where the traffic comes from and goes to and their user behavior patterns – they should build upon this knowledge by promoting specific cloud tools (for CRM, collaboration, storage, etc.) to minimize the amount of different cloud software being used for the same purpose. Banning cloud providers, for example Slack for project management, will not help much, as there will always be alternatives available (e.g. Teamwork or Trello) that users can easily switch too.

Conclusion

Even if CASBs are to be called a silver bullet for cloud security, any bullet still requires someone to shoot it. Organizations are responsible for ensuring a proper selection and integration of a potential CASB in their IT landscape. By taking into account the abovementioned considerations, enterprises that plan to deploy CASBs in order to increase their cloud security, can start their brokerage journey with a set of concrete decisions to make. This will ensure that the right CASB provider is chosen to fit the enterprise needs, and that CASB is "tuned" for the maximum security benefit of the enterprise.

References

[CSA15] CSA, *Cloud Security Open API: The Future of Cloud Security*, 2015, https://blog.cloudsecurityalliance.org/2015/06/29/cloud-security-open-api-the-future-of-cloud-security/

[Fult16] S.M. Fulton, *RSA 2016: There Is No Cloud Security Stack Yet*, The New Stack, March 2016, http://thenewstack.io/rsa-2016-no-cloud-security-stack-yet/

[Gart15a] Gartner, *Market Guide for Cloud Access Security Brokers*, 2015, https://www.gartner.com/doc/3155127/market-guide-cloud-access-security

[Gart15b] Gartner, *Select the Right CASB Deployment for Your SaaS Security Strategy*, 2015, https://www.gartner.com/doc/3004618/select-right-casb-deployment-saas

[Gart16] Gartner, *Cloud Access Security Brokers (CASBs)* (definition), http://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs/

[MM15] MarketsandMarkets, *Cloud Access Security Brokers Market by Solution & Service*, December 2015, http://www.marketsandmarkets.com/Market-Reports/cloud-access-security-brokers-market-66648604.html

[Muru16] S. Murugesan, I. Bojanova, E. Sturrus and O. Kulikova, *Identity and Access Management*, Encyclopedia of Cloud Computing (Chapter 33), Wiley, 2016, http://onlinelibrary.wiley.com/doi/10.1002/9781118821930.ch33/summary

[RGvT12] Reid, Geleijnse & Van Tol, Fokke & Sukke cartoon, 2012.

[Stur11] E. Sturrus, J. Steevens and W. Guensberg, *Toegang tot de wolken*, Compact 2011/2, https://www.compact.nl/articles/toegang-tot-de-wolken/

[TMR16] Transparency Market Research, *Global Cloud Access Security Brokers Market Revenue, by Geography*, TMR Analysis, March 2016, http://www.transparencymarketresearch.com/cloud-access-security-brokers-market.html

About the Author

O. Kulikova MSc is a senior consultant at KPMG Cyber. She has experience with advisory engagements related to Cloud Security, Identity and Access Management, Information Risk Management, and Cyber Defense. She is certified for Cloud Security Knowledge (CCSK) by the Cloud Security Alliance (CSA).