Evaluation of Cloud Access Security Brokers (CASB) for enterprise risk mitigation and development of recommendations for the integration with existing organisational and operational structures

by

Moritz Roos

MSc Cloud Computing

Supervisor: Dr John Creagh

19.03.2017

This report is submitted in partial fulfilment of the requirements for the Degree of Master of Science in Software Development at Cork Institute of Technology. It represents substantially the result of my own work except where explicitly indicated in the text. The report may not be copied or distributed without the permission of the author.

Abstract

The broad adoption of cloud computing in the consumer domain passes over to the corporate domain. While many organisations recognise the benefits of cloud services and utilise them in a controlled manner, some employees act on their own and use additional cloud services outside the control of the organisation, at the expense of security and compliance. Software vendors emerged that promise remedy against the so-called Cloud Shadow IT and to regain control over the use of cloud services – the Cloud Access Security Broker (CASB).

This research provides guidance, methodologies, and tools for the awareness of Cloud Shadow IT, associated risks, as well as the evaluation and implementation of CASBs to close the gap in secure cloud usage.

Table of Contents

Chapter 1 Introduction

1.1 Problem Description

No comprehensive guidance is available on how to implement and integrate CASB on top of existing systems without creating yet another silo.

1.2 Research Goals

The primary goal of this research is to raise awareness for the risks companies are potentially exposed to by not controlling the usage of cloud services within their organisation. Once this is given and a company feels the need to assess these risks internally, the research then provides support to identify and rate specific risks in their context, gain knowledge about CASBs vendors and solutions, evaluate current CASB vendors and solutions for their needs, and finally to implement and integrate a CASB solution into existing structures.

1.3 Research Questions

The research questions below paraphrase the goal of this research into multiple questions.

1. What are the risks derived from the uncontrolled usage of cloud services (Cloud Shadow IT) within companies today?
2. Does the utilisation of Cloud Access Security Brokers sufficiently address the risks derived from Cloud Shadow IT?
3. How should a company integrate a CASB solution into the existing organisational and operational structures to best satisfy the company's needs?

1.4 Research Approach

The research questions are answered by performing Content (or Textual) Analysis Research, Experience Research, and Case Study Research.

Content or textual analysis research is required to gain valuable information about legal and compliance requirements that are at risk to be violated by the unapproved usage of cloud services. It is also applied to analyse the current market of CASB vendors and solutions. Illustrative case study research provides an approach to create use cases for prospective users of a CASB solution to define implementation recommendations for specific types of scenarios. Finally, experience research was essential to enhance the deliverables of this research with professional experiences from using a variety of CASB solutions and being involved in a high number of corporate IT audits throughout the last years.

Chapter 2 Definitions

2.1 Shadow IT

For the definition of the Shadow IT phenomenon, it is necessary to differentiate it from the private use of official IT resources. While the private use does not involve business related activities, Shadow IT usage serves the purpose to support the business processes, or rather the process activities. For IT departments, Shadow IT represents a loss of transparency and control that reaches from known but uncontrolled standalone solutions, over to unknown but detectable solutions, to unknown and undetectable solutions (Brenner, et al., 2011). As opposed to Shadow IT, official IT services are registered within the asset management and configuration management of the organisation's IT environment.

For the term Shadow IT this results in the following definition (Zimmermann & Rentrop, 2012): Shadow IT describes business process supporting IT systems, IT service processes and IT employees that are independently deployed by departments and IT users. Also, Shadow IT is not integrated into the IT service management of an organisation and therefore not registered within the asset and configuration management and the service portfolio.

Similar characteristics and purposes to Shadow IT can be found in End User Computing (EUC). This concept allows end users to individually modify or develop IT systems by using EUC (Barker & Fiedler, 2011). EUC was formally introduced by organisations to relieve the resources of their IT departments. However, EUC tools such as spreadsheets and user-friendly database applications contributed to the emergence of Shadow IT by enabling autonomous design and development of information processing systems (Hagemeister, et al., 2008).

In practice, Shadow IT can be categorised into two groups: Hard- & Software and personnel activities. On the hardware side, end devices such as personal computers, servers, routers or printers can be found that were procured and integrated into the corporate network directly by the departments. Mobile devices such as smartphones and tablets including apps that can be installed by the users also fall into this category. The "bring your own device (BYOD)" concept attempts to gain control over these devices. On the software side, applications can be found that were procured or developed by the departments or individual employees. Users often develop spreadsheet or database applications with Microsoft Excel or Microsoft Access to support the completion of their tasks. These shadow applications often emerge in connection with the launch of big IT solutions such as ERP systems. Individually developed systems are referred to as "feral systems" and are created due to insufficient features of the official systems, problems with their implementation or political tensions within the organisation (Jones, et al.,

2004). The shadow systems can be operated in parallel with official systems with similar features or as legacy systems that are listed in the service portfolio as discontinued but are continued to be used regardless. The other category of Shadow IT are employees that provide support to other departments and employees with IT related issues, which leads to the creation of informal structures.

The sourcing of cloud services over the internet introduces a whole new category of Shadow IT that is the underlying topic of this research and further discussed in Chapter 2.3.

2.2 Cloud Computing and Cloud Services

The perception of cloud computing continues to be shaped by marketing terms of various IT organisations that keep on taking advantage of the now subsiding hype around cloud computing. Figure 1 shows the Gartner Hype Cycle from 2014, where the term "Cloud Computing" already reached the "Trough of Disillusionment".

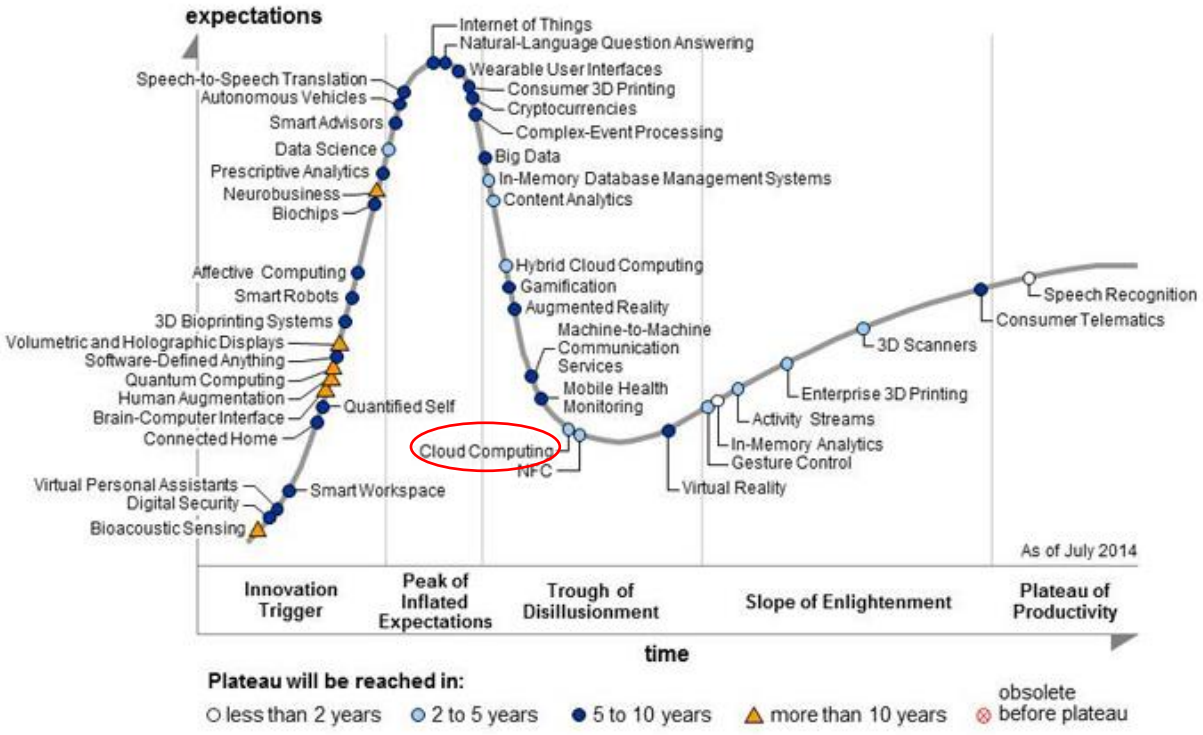


Figure 1: Gartner Hype Cycle 2014 (Gartner Inc., 2014)

In comparison, the term "Cloud Computing" is not present anymore in the Gartner Hype Cycle from 2016, as shown in Figure 2. However, a couple of other "emerging technology" terms are shown that can be associated with cloud computing: "Internet of Things" (IoT) and "Connected Home", for instance, rely heavily on cloud computing technology and many other technologies are "enabled" by cloud computing. It turns out that the general term of cloud computing arrived in today's technology portfolios as an established constant to support digital business

innovation. Further terms that are related to cloud computing can be expected to appear in the future (Hagenau, 2016).

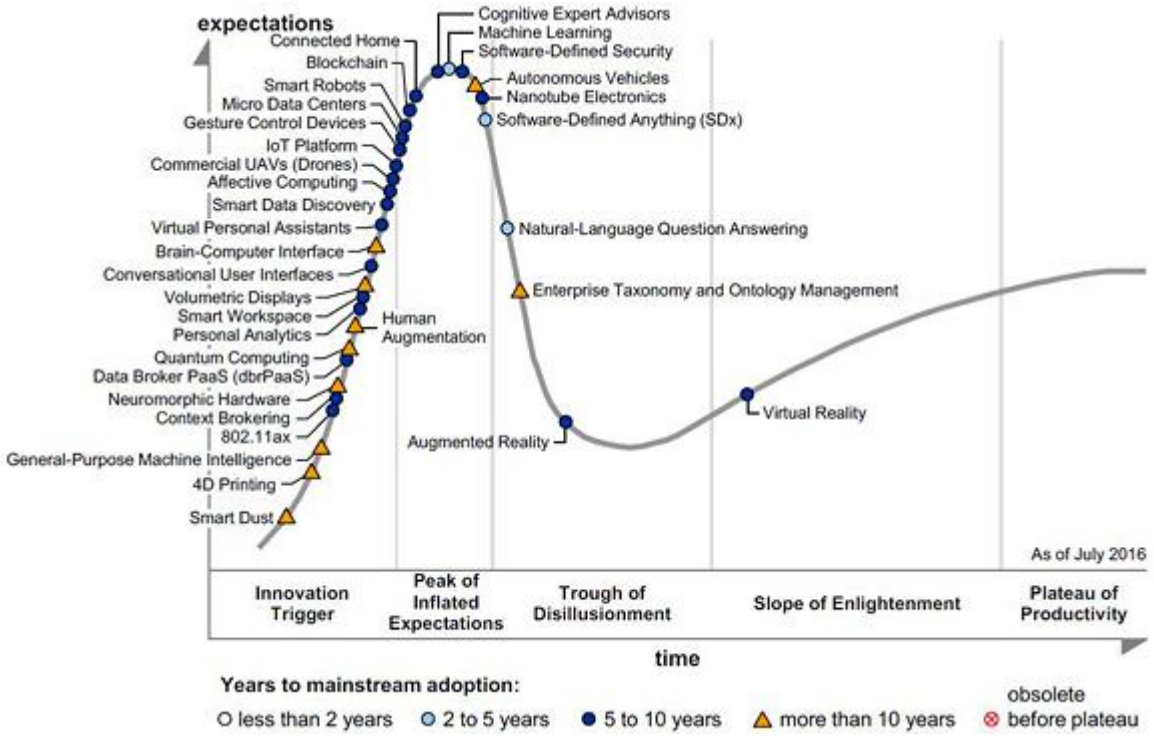


Figure 2: Gartner Hype Cycle 2016 (Gartner Inc., 2016)

Even though cloud computing exists for some time now and is commonly recognised, there still is no clear definition of what cloud computing actually represents. One definition that is often referred to was published by the National Institute of Standards and Technology (NIST). Combined with the definition from the Cloud Security Alliance (CSA), cloud services require the following characteristics.

Essential characteristics of cloud computing according to NIST (NIST, 2011)

- **On-Demand Self Service:** Users can provision resources such as server time and network storage at any given time, on-demand, and without requiring human interaction on the provider side.
- **Broad Network Access:** Access to the cloud service is provided through standard mechanisms that allow use by various clients (e.g. mobile phones, tablets, laptops, and workstations).
- **Resource Pooling:** The computing resources (storage, processing, memory, network bandwidth) are pooled to serve multiple customers using multi-tenant models that allow to dynamically assign and reassign physical and virtual resources to meet customer demands.

The exact location of the provided resources is usually not controlled or known by the customer but may be possible to be specified at the level of the country, state, or data centre.

- **Rapid Elasticity:** The resources are elastically provisioned and in some cases automatically scaled up or down. To the customer, the resources often appear to be unlimited and can be provided in any quantity and at any time.
- **Measured Service:** The resource usage of cloud services can be monitored, controlled, and reported to allow automatic optimisation and to provide transparency for both the provider and consumer. Metering the service on e.g. storage, processing, bandwidth, and active user accounts level also allows for consumption-dependent billing (pay per use) of the customer.

Additional characteristics according to the CSA

- **Service orienteered Architecture (SOA):** SOA is a key enabler of cloud computing. Cloud services are usually provided through an REST-API.
- **Multitenancy:** The concept of securely using a shared pool of resources is mandatory for cloud services.

The German Federal Office for Information Security (BSI) provided the following definition of cloud computing based on the NIST and CSA characteristics (BSI, 2011):

> *„Cloud computing describes the dynamic, demand-oriented provisioning, using, and billing of IT services through a network. Supply and usage of these services exclusively take place through defined technical interfaces and protocols. The range of services provided in regards to cloud computing comprises, among others, infrastructure (e.g. processing, storage), platforms and software."*

The IT services that fall under this definition can be categorised into the following deployment models.

Private Cloud: The cloud services are provided exclusively to one organisation with multiple users. The infrastructure the cloud service runs on is owned and managed by the organisation, the provider, or a combination of both. The location of the private cloud can be on-premise at the user site or off-premise at a provider.

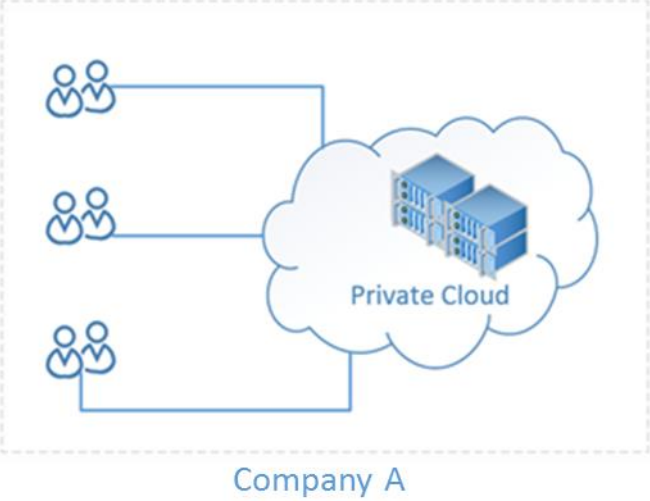


Figure 3: Private Cloud (own presentation)

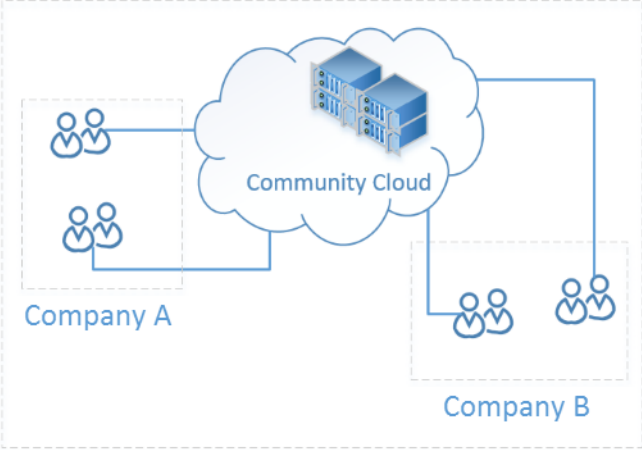


Figure 4: Community Cloud (own presentation)

Community Cloud: The infrastructure of a community cloud is based on a private cloud, but is used by multiple organisations that have common interests such as the same policies for sub-providers or the same compliance requirements that need to be adhered to.

Public Cloud: The provisioned infrastructure is publicly "accessible" by the users to the extent of their segregated tenant. A public cloud is operated and managed by an organisation, a scientific institution or a governmental organisation and it is located at the provider's datacentres.

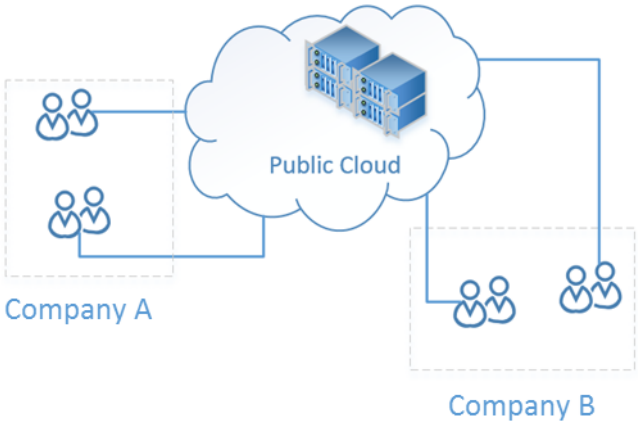


Figure 5: Public Cloud (own presentation)

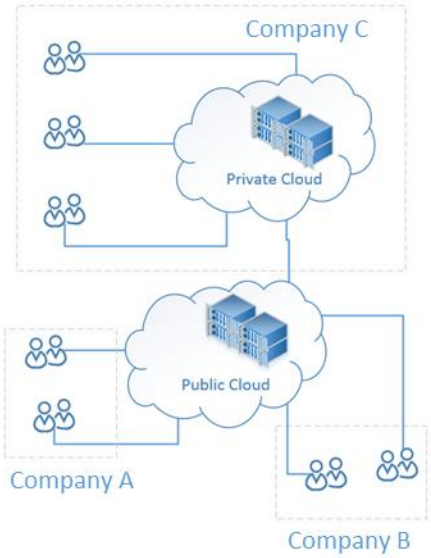


Figure 6: Hybrid Cloud (own presentation)

Hybrid Cloud: The cloud infrastructure is a combination of one or more deployment models. However, the models themselves are autonomous and interconnected through standardised interfaces.

The deployment models defined above are the most common models today. Alterations of these models exist and are developed for special use cases regularly, such as the "virtual private cloud". Also, terms exist that emphasise on who manages the infrastructure, e.g. "managed private cloud", where the infrastructure is exclusively used by one organisation but managed by another.

Additionally, every deployment model can be categorised into one of the three following service models:

- **Software as a Service (SaaS):** This is likely to be to best-known cloud computing service model, as users come across several SaaS solutions on a daily basis. Cloud services that fall under this service model provide software solutions such as web-based accounting email software.
- **Platform as a Service (PaaS):** On PaaS solutions, users can run or develop their own software. The user is provided with pre-installed language packages and additional tools and services. The management of the underlying infrastructure such as the network and the servers as well as the operating systems and Integrated Development Environments (IDE) is the responsibility of the cloud provider. Only the user has control over the software and the occupied storage.
- **Infrastructure as a Service (IaaS):** In the case of IaaS models, the user has control over the complete set of software including operating systems. Users can install and run their own operating systems with the applications he requires. The cloud provider manages only the underlying infrastructure.

Similar to the deployment models, alterations to the service models exist that have been developed and defined for special use cases and also marketing purposes. Some examples are Business Process as a Service (BPaaS), Security as a Service (SECaaS), Desktop as a Service (DaaS) and Big Data as a Service (BDaaS). However, most of these services rely on the three

models defined above but are used to emphasise on the plug-and-play and subscription based model availability.

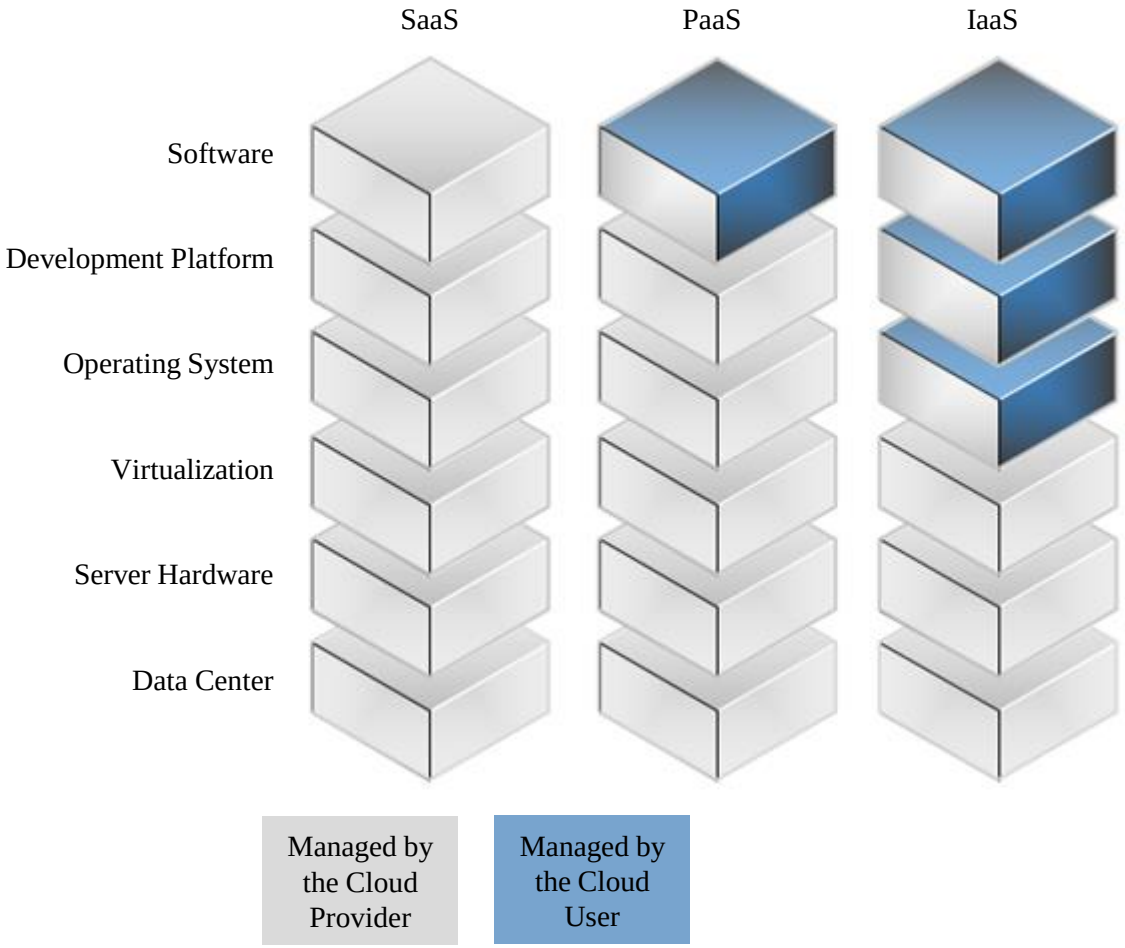


Figure 7: Service model overview (own presentation)

2.3 Cloud Shadow IT

The following sections define the phenomenon of Cloud Shadow IT (also referred to as "shadow cloud services", "unapproved services", "unauthorized services", or "unsanctioned services") and include basic research on the causes of its emergence as well as its presumed advantages over traditional cloud services (also referred to as "approved services", "authorized services", or "sanctioned services"). This, in turn, requires basic research on the general challenges of cloud computing in organisations regarding data protection and data security. Extensive research on the risks derived from Cloud Shadow IT is conducted in chapter Chapter 3 to address the first research question.

Furthermore, the term "cloud services" includes all deployment- and service models above in the remainder of this report.

2.3.1 Cloud Computing Challenges

Many adverse effects respectively risks that derive from Cloud Shadow IT can be traced back to global challenges of the cloud computing model and are not unique to Cloud Shadow IT. This section discusses these challenges regarding data protection and data security to draw a distinction between global and Cloud Shadow IT unique risks defined within this research. Nevertheless, the global risks of cloud computing apply to this research and must be considered in the risk register.

The rapid advance of cloud technology is increasingly transforming the corporate IT landscape to support the business more efficiently. However, these advances have created new security vulnerabilities and amplified existing vulnerabilities that can be exploited to cause damage to the cloud user and therefore pose threats to the organisation. The "Top Threats" working group of the Cloud Security Alliance (CSA) regularly analyses the latest cloud technologies and deployments to identify the biggest threats derived from cloud services to provide organisations with the necessary information to make educated risk management decisions. The following chapters provide a brief explanation of the top 12 risks of cloud computing, as identified by the CSA (Cloud Security Alliance (CSA), 2016).

Data Breaches

Data breaches were ranked as the top threat to cloud services. A data breach occurs when the customer data that are being processed by the service are released or disclosed to unintended parties. The severity of a data breach is usually determined by the classification of the data, e.g. strictly confidential or confidential data or by the sensitivity of its nature, e.g. health data, financial information, personally identifiable information (PII) or intellectual property (IP).

The possibility of a data breach is not unique to cloud services, but the shared resources of multitenant cloud infrastructures and the high accessibility highly amplify this threat.

Insufficient Identity, Credential and Access Management

Identity and Access Management (IAM) is used to authenticate users and to govern access to resources. A well-defined and well-implemented IAM solution is the key to secure the IT environment. Therefore, a weak IAM provides many attack vectors for all threat categories, as defined by the STRIDE Threat Model by Microsoft (Microsoft Corp., 2005): Identity spoofing, data tampering, repudiation, information disclosure, denial of service (DoS) and privilege elevation.

Again, this is not unique to cloud environments. With the use of cloud services, however, the perimeter around an organisations resources that needs to be controlled is becoming increasingly blurred. Multiple IAM solutions of the cloud user and CSP need to interact (using identity federation) efficiently to provide a seamless integration of the cloud service, but this interaction and the reliance on security measures of the other party offer plenty of room for new vulnerabilities.

Insecure Interfaces and APIs

Cloud services rely on outside-facing application programming interfaces (API) to enable cloud users to interact with the service for provisioning, management, orchestration and monitoring as well as third party providers to build upon then for additional services.

As these interfaces are accessible from anywhere on the internet, they are a popular target for attackers to e.g. compromise the confidentiality and integrity of cloud user's credentials or the availability of the cloud service.

System Vulnerabilities

Vulnerabilities of systems and applications that are introduced by bugs within the code can be exploited by attackers to commit any malicious activity. Bugs exist in on-premise and cloud environments alike, but again the multitenant cloud infrastructures offer additional attack vectors through shared memory and resources.

Account Hijacking

Hijacking user credentials through phishing, exploits or even social engineering to gain access to or to manipulate data are common practices among malicious attackers. Attackers gaining access to cloud services through user accounts with extensive privileges to e.g. the infrastructure layer can not only compromise the data but include malicious code to compromise entire applications and services or even making them unavailable.

Malicious Insiders

Malicious Insiders are current or former employees, contractors, or business partners who have or had access to an organisation's network, systems or data and misuse that access to compromise the security of the organisation's resources. While the risk of this to occur is difficult to assess, it can be considerably higher when using cloud services as the employees working at the CSP add to the group that could have access to the network, systems, or data while not being in the scope of the organisation's own security controls.

Advanced Persistent Threats (APTs)

Malicious attacks are considered APTs when infiltrating systems and networks through entry points mostly with user intervention or action (e.g. spearphishing, USB devices, use of unsecured networks) with the goal to steal information over extended periods. The attacks adapt to the security measures intended to detect them and move through the networks to achieve their goal.

APTs targeting a CSP have the potential to infiltrate a wide array of networks and steal information from many different organisations that use their cloud services as it moves through the data centres.

Data Loss

The risks of losing data not only through attacks but accidental deletion, hardware failure or natural disasters are higher with cloud services insofar as the data are stored at the CSP and not necessarily backed-up additionally by the organisation. The backup procedures vary between the CSP and subscriptions and are usually settled within the SLA.

In case the data are encrypted before uploading to the cloud service, and the encryption keys are managed by the organisation or a third-party, losing the key essentially means losing the data (crypto-shredding).

Insufficient Due Diligence

Adopting cloud technologies or using cloud services has become a matter of business strategy. Often, the decision is made prematurely to catch up to or stay ahead of the competition without assessing the "cloud maturity" of the processes and systems or without thoroughly evaluating the CSPs.

Attempting to move workloads to the cloud that are not mature enough (e.g. regarding automation, virtualization, or criticality) or choosing a CSP that can't fulfil all the requirements of an organisation exposes the organisation to a variety of commercial, financial, technical, legal and compliance risks.

Abuse and Nefarious Use of Cloud Services

The ease of provisioning and using cloud services is one of the major benefits of cloud computing. However, this can also be leveraged by attackers to use cloud resources for

malicious attacks, e.g. spamming, phishing, malware distribution, botnet servers, DDoS, or password cracking.

Denial of Service (DoS)

As cloud services are accessible from anywhere on the internet and available to a large customer base, they can easily become the target of DoS or DDoS attacks. Attackers force the cloud service to consume enough of the available system resources (CPU, RAM, disk space or network bandwidth) to cause severe system slowdowns or even inaccessibility of the entire cloud service.

Shared Technology Vulnerabilities

Sharing resources allows CSPs to reach high utilisation of their hardware and to scale individual cloud services rapidly. As this multitenancy can be implemented on multiple layers (application, storage, compute, network, VM, hypervisor), attackers are provided with various entry points with vulnerabilities that can be exploited to gain unauthorised access to data.

Evolving Threat Landscape

The threats described above are only a snapshot of the possibilities with the current state of technology. As the technology advances at increasing speed, the possibilities to attack and compromise cloud services evolve with it and are likely to increase as the gap between attacks vectors and the standardisation of security measures only widens.

A quick comparison of the latest list of "Top Threats" as defined by the CSA to the previous one from 2013 already shows that most of the threats still exist today but greatly vary in severity (Cloud Security Alliance (CSA), 2013). The current list also introduced three additional threats: Insufficient Identity and Access Management, System Vulnerabilities, and Advanced Persistent Threats.

2.3.2 Causes of Cloud Shadow IT

There are various reasons to bypass the internal IT department by using Shadow IT. In many cases, employees simply want to increase their productivity and feel constrained by missing or limited functionality of their corporate IT. They find "better" solutions on the internet, often at no charge. These solutions usually are deployed without any effort for installation and configuration and are ready to use within a short amount of time, while broadly covering the demands – therefore surpassing the official solutions.

Shadow IT is particularly established when internal IT departments, from the employee's point of view, don't provide suitable solutions promptly. To fill this gap, employees autonomously and without the knowledge of the IT department make use of easily and directly accessible cloud services: Shadow cloud services arise.

The emergence of shadow cloud services gives reason to further research on the causes that drive this trend. The following list of practical problems and desires regarding the corporate IT environment can be considered as common causes of shadow cloud services. It does not claim to be exhaustive and is not ordered by frequency of occurrence or any specific value.

2.3.2.1 Cost savings

A large number of public cloud services can be used at no cost - at least for private use or a small number of users. In times of tight budgets and ambitious goals, organisations are anxious to keep the IT cost low. "Free" services are therefore very welcomed, and some organisations quietly accept the usage of shadow cloud services.

2.3.2.2 Generation Y

Employees born in the 1980s and 1990s know and appreciate the intuitive user interfaces of public cloud services from their personal life. In many cases, they are not willing to step back regarding usability and performance at work. They also might handle data and information less restrictively since being used to social media when it comes to sharing information.

2.3.2.3 Bring your own device

The increasing merger of professional and personal life encourages the use of shadow cloud services: employees use their private infrastructure (such as internet access, personal computer, smartphone) for work and also expect, in return, that the provided infrastructure at work can also be used for private purposes.

2.3.2.4 Insufficient functionality of corporate IT

Another factor that drives the adoption of shadow cloud services are obsolete, missing, or for the purpose inappropriate applications provided by the corporate IT. If employees encounter this, the chances are that they find their way to complete their tasks more efficiently, effectively, and much faster. Such gaps can also originate from restrictive security requirements that prevent the provision of better alternatives in a cost-effective and user-friendly manner.

2.3.2.5 Unawareness

Before using shadow cloud services, employees in most cases do not consider technical, organisational, and legal requirements that need to be met before productively using an

application – especially in the case of public cloud services. This does not only affect the geographical storage location of the data but also e.g. if the data is encrypted in transit and at rest, who manages the encryption keys, how is the backup process designed, what sub-providers can access the data and which laws and regulations apply. Details about these topics are often not known or ignored.

2.3.2.6 Simplicity

For many public cloud services, users can register simply with their E-Mail addresses. The provider does not differentiate between private or business addresses or between private and business payment methods. While using software yet required an installation and therefore was under the control of the internal IT department, public cloud services can be directly accessed by end users.

2.3.2.7 Lack of or simple approval processes

Using lightweight cloud services is much more attractive compared to introducing new complex extensions or applications within the organisation: no integration into the IT processes is required. Therefore, complicated requests, business case analyses, approval rounds, budgeting (among others) is skipped, and a quickly available, cost effective, and simple solution to a problem can be used.

2.3.2.8 Missing policies

Vague and incomplete policies make it more difficult for employees to make the right decisions and act appropriately. Not all organisations have defined conditions for the use of public cloud services and added them to their policies. Therefore, employees do not necessarily know whether the organisation considers unauthorised use of cloud services as negative (risky, incautious, incorrect) or positive (enthusiastic, creative, pragmatic).

2.3.2.9 Lack of governance

Not every organisation has a strict governance and all tools to detect and prevent shadow cloud structures early on. Especially small and medium-sized organisations lack the expertise and resources to implement such management processes. Even though large organisations often have a strict governance established, they rarely can detect shadow cloud structures.

2.3.3 Measures against Cloud Shadow IT

When there are risks, there are also measures to manage the risks. Obvious measures to manage the risks derived from Cloud Shadow IT can be roughly categorised into prevention, detection, and response.

Preventive measures may include the creation of policies for cloud usage with specifications on shadow cloud services or risk awareness training and campaigns. On a technological level, any filtering or blocking mechanisms would also fall under this category. To address the causes of Cloud Shadow IT from the "simplicity" and "no or simple approval process", preventive measures could also employ a time reduction to contract, provision, and implement approved services.

Detection measures may be as simple as seeking the dialogue with employees as potential users to get to know what applications they are using for process execution. Also, financial statements could be regularly inspected for billing transactions with unapproved cloud service providers. Advanced technical measures for detection monitor the connections and traffic from the corporate network to the Internet and vice versa for unapproved cloud services.

Response measures are applied when shadow cloud services are found to be used within an organisation. If a policy regarding Cloud Shadow IT is in place, disciplinary sanctions or corrective actions according to the policy are applied. Technical measures could include updating the blocking mechanisms (e.g. blacklist or whitelist) or redirecting the user, but additional awareness training could also be conducted in response to the detection of unapproved services.

2.4 Cloud Access Security Broker (CASB)

Cloud Shadow IT, along with its risks, exists for some time now. Vendors in the IT security business developed solutions that provide a range of capabilities (including the measures mentioned above) to support the secure usage of cloud services and to manage Cloud Shadow IT. These products are known as Cloud Access Security Brokers (CASB) (also referred to as "Cloud Security Gateways") and are discussed in detail within this research. Other important products are Identity & Access Management-as-a-Service (IAMaaS, also referred to as IDaaS) that can play a major role in managing cloud services. CASB vendors often partner with IDaaS solutions to steer traffic to the CASB solution (Forrester Inc., 2016), because direct access from public networks to the cloud without going through the company infrastructure is usually not covered by the CASB.

CASBs help to prevent, detect, and respond to Cloud Shadow IT. Some also offer advanced analysis of internet traffic or log files combined with an up-to-date database of Cloud Service Providers (CSPs) to determine a risk rating that considers the usage behaviour and security-related information about the CSP, such as the nature of the service, known security breaches, certifications, or the terms and conditions. As some of the obvious measures, such as blocking

or redirecting, are provided by most CASB solutions as core functions, they vary in their exact functionality, architecture and also possibilities to integrate with existing organisational and operational structures. Therefore, Chapter Chapter 4 evaluates the current market of CASBs to address the second research question.

Most CASB solution can be implemented or deployed in different operating modes, e.g. for simple log collection, as a forward proxy, reverse proxy, or utilising CSP specific APIs for advanced security controls. This allows supporting different use cases that are discussed in more detail in Chapters Chapter 4 and Chapter 5 .

Chapter 3 Enterprise Risks of Cloud Shadow IT

3.1 Enterprise Risk Management for Cloud

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a study in 1992 titled “Internal Control – Integrated Framework” (COSO-Model). Their definitions of Corporate Governance and illustrations of structural interrelationships became a central standard for the development of an Internal Control System (ICS). In 2004, the COSO-Model for Enterprise Risk Management Framework (COSO II) was further developed to an enterprise-wide risk management (ERM) to consider the increasingly important integration of risk management with ICS (Bungartz, 2012).

In 2012, COCO published a “Thought Paper” for enterprise-wide risk management of cloud computing on the basis of COSO II. This paper recommends the development of a “Cloud Computing Governance”[1] before the first cloud service is implemented. As this only applies to properly authorised cloud services, companies will likely find shadow cloud services already in place at this point. In this case, a subsequent risk evaluation should be conducted, and a cloud computing governance should be implemented.

For risk evaluation, companies should first identify the legal and regulatory requirements that apply to their organisation. This strongly depends on the jurisdiction and industry of the organisation. Chapter 3.2 provides a comprehensive list of standards, best practices, frameworks, and regulatory and industrial requirements that are widely accepted and have an impact on the security and privacy of cloud services within an organisation. Once identified, these requirements should be matched against potential or identified shadow cloud services (COSO, 2012).

[1] „Cloud Governance“ indicates the adaption of an ICS to the characteristics of cloud computing.

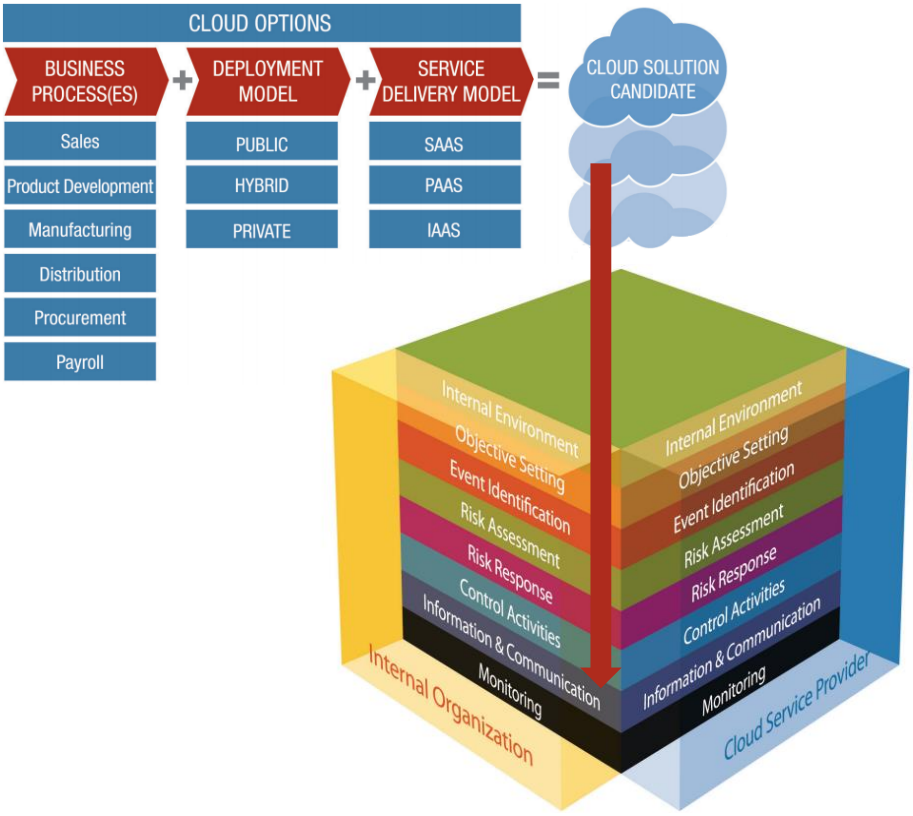


Figure 8: Implementation of Cloud Services into an ERM according to COSO II (Source: (COSO, 2012))

COSO recommends to run every potential cloud service through the COSO II model (see Figure 8) and provides guidance particularly for the risk management.

The risk types (e.g. security, integrity, availability, and performance) had not changed with cloud computing compared to non-cloud technology solutions, but the likelihood and impact had changed and with it the risk profile of the enterprise (COSO, 2012). COSO underlines this with examples that can be seen as complementary to the security and privacy threats in Chapter 2.3.1. Please refer to Appendix A for a detailed extract from the COSO document.

As a result of the risk evaluation, COSO recommends the adjustment of controls in the ICS. Due to the outsourcing nature of cloud computing, some of these controls stay under the responsibility of the cloud user, while others are under the responsibility of the CSP (COSO, 2012).

COSO also provides the following guidelines to address these risks:

- The creation of a policy for cloud computing is recommended to prevent the unauthorised usage of cloud services.
- To fulfil the compliance requirements and to prevent data leakages, data should be classified according to their confidentiality, and only data should be transferred to cloud

services that can comply with their requirements for confidentiality, integrity, and availability.

- An exit strategy should be developed to prevent a “vendor lock-in”.

These guidelines are not very detailed, but COSO emphasised that existing control models (in this case COSO II), in consideration of cloud-specific risks, can be suitable to satisfy the cloud computing challenges (COSO, 2012).

3.2 Collection of Relevant Documents

As mentioned above, every organisation needs to define their individual policies and directives that set the internal requirements on topics like cloud security and privacy. To what extent these requirements are aligned with best practices is left to the organisation, but it is recommended to start with widely accepted practices and alter them to the specific needs and objectives. When it comes to external requirements from regulations and industry standards, organisations do not have much opportunity to choose. Before using cloud services, organisations need to assess which requirements they may and must adhere to. Depending on the country they are registered in and operate in, this may differ greatly. In the best case, the external requirements have been assessed and are reflected or referenced in the internal policies and directives.

The following table provides a selection of standards, best practices, frameworks and regulatory and industrial requirements that are widely accepted and have an impact on the security and privacy of cloud services within an organisation.

Name	Publisher
Audit Standards and Certifications	
ISO/IEC 27001:2013	ISO/IEC
ISO/IEC 27017	ISO/IEC
SOC1/SSAE16	AICPA
SOC2/TSP (SysTrust & WebTrust)	AICPA
SOC3/TSP (SysTrust & WebTrust)	AICPA
ISAE 3402	IAASB
CSA STAR Attestation	CSA
Best Practices	
Cloud Computing Security Risk Assessment	ENISA
Enterprise Risk Management for Cloud Computing	COSO

Name	Publisher
Guiding Principles for Cloud Computing Adoption and Use	ISACA
IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud	ISACA
Security Considerations for Cloud Computing	ISACA
Frameworks	
SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing	NIST
Cloud Controls Matrix (CCM)	CSA
USAGE MODEL: Data Security Framework Rev 1.0	ODCA
COBIT 5	ISACA
Risk Management Framework (RMF)	NIST
SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations	NIST
Regulatory and Industry Requirements	
German Federal Data Protection Act (Bundesdatenschutzgesetz)	German Government
German IT Security Act	German Government
EU-General Data Protection Regulation (GDPR)	European Commission
Guidelines for the proper bookkeeping and storage of accounts and records in electronic form (GoBD)	German Government
Health Insurance Portability and Accountability Act (HIPAA)	US Government
Health Information Technology for Economic and Clinical Health (HITECH) Act	US Government
GxP	Intl. Bodies
Solvency II Directive	European Commission
Basel II	Basel Committee on Banking Supervision
Minimum Requirements for Risk Management for financial institutions in Germany (MaRisk)	BaFin
Sarbanes-Oxley Act (SoX)	US Government

Name	Publisher
Payment Card Industry Data Security Standard (PCI DSS)	PCI SSC
Gramm-Leach-Bliley Act (GLBA)	US Government

Table 1: Relevant standards, best practices, frameworks, regulatory requirements

These sources may be used by organisations to identify applicable requirements as well as to develop an individual risk register to enable proper management of the risks derived from the uncontrolled usage of cloud services within the organisation.

3.3 Risk Register Development

The following table provides a comprehensive list of risks that organisations may use as a template and guideline for the development of an individual risk register. Each risk is categorised into one or more of the following categories:

- Financial: The risk has a potential financial impact on the organisation, resulting in direct or indirect financial losses e.g. due to penalty payments, licensing fees, or loss of customers.
- IT Governance: The risk has a potential impact on the effective and efficient use of IT to support the organisation in achieving its goals.
- Information Security: The risk has a potential impact on the security of the IT systems and information. The security goal is met through the security objectives confidentiality, integrity, and availability (CIA).
- Legal: The risk has a potential impact on legal requirements of the organisation. The use of shadow cloud services may violate applicable laws.
- Compliance: The risk has a potential impact on internal compliance requirements of the organisation. Best practises are considered as these vary for each organisation.
- Data Protection: The risk has a potential impact on requirements for the processing and storing of personally identifiable information (PII). The requirements strongly depend on the jurisdiction of the organisation and location of the data.

To provide further guidance, the risks in the register are mapped to specific documents from Chapter 3.2 shown in the column “Relevant Document”. This helps organisations to look for risks that concern documents of interest. Please note that this mapping has no claim to completeness as many of the documents have overlapping requirements or cross-references and therefore is merely an indicator to important documents connected to the individual risk.

ID	Risk Category ("x" = direct impact, "(x)" = indirect impact, "-" = no impact)						Risk	Relevant Document
	Financial	IT Governance	Information Security [CIA]	Legal	Compliance	Data Protection		
1	-	x	x	x	x	-	Employees share corporate data with unauthorised third parties	Enterprise Risk Management for Cloud Computing
2	-	x	x	x	x	x	Employees share highly sensitive data with unauthorised third parties	German Federal Data Protection Act (Bundesdatenschutzgesetz)
3	-	x	x	x	x	x	Employees share personal identifiable data with unauthorised third parties located in other jurisdiction	German Federal Data Protection Act (Bundesdatenschutzgesetz)
4	-	-	x	x	x	(x)	Incidents related to misuse of data or highly sensitive data may remain undetected	German Federal Data Protection Act (Bundesdatenschutzgesetz)
5	-	-	x	x	-	-	Data loss due to insufficient procedures and technical (security) precautions at the cloud provider	SOC2/TSP (SysTrust & WebTrust)
6	-	-	x	x	x	(x)	Data or highly sensitive data may be stolen by employees of cloud provider	Payment Card Industry Data Security Standard (PCI DSS)
7	-	-	x	-	-	(x)	Data or highly sensitive data may be manipulated by employees of cloud provider	Payment Card Industry Data Security Standard (PCI DSS)
8	x	-	-	x	-	-	Blackmailing based on threat to publish stolen / captured data	German IT Security Act
9	x	-	-	x	x	-	Risk of lawsuits due to stolen data	n/a
10	x	-	x	x	-	x	Insufficient legal options / actions due to detrimental contract / terms and conditions	Enterprise Risk Management for Cloud Computing
11	-	-	x	x	x	(x)	Exposure of data or highly sensitive data to third parties due to insufficient tenant separation	SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
12	-	-	x	x	x	(x)	Exposure of data or highly sensitive data to third parties due to subservice organisations of cloud provider (e.g. cloud chaining)	SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
13	-	-	x	(x)	x	(x)	Insufficient data deletion due to lack of control over deletion mechanisms in productive environment, backups and offline data at cloud provider	Cloud Controls Matrix (CCM)
14	-	-	x	x	x	(x)	Theft of data or highly confidential data due to no or weak protection of network connections (e.g. during transfer to cloud service provider)	Cloud Controls Matrix (CCM)
15	(x)	-	-	x	x	-	Consistency and reliability of BCM and DR plans for mission critical business processes or systems at risk as shadow cloud services are out of scope	SOC2/TSP (SysTrust & WebTrust)
16	x	-	-	x	(x)	-	Loss of brand reputation / image due to security breaches becoming public	Enterprise Risk Management for Cloud Computing
17	x	-	-	x	-	-	Penalties due to violation of contracts, laws and regulations	n/a
18	x	x	-	x	-	-	Multiple service fees and inefficiencies due to multiple contracts with the same cloud provider	n/a
19	x	x	-	(x)	(x)	-	Loss of revenue due to business interruption caused by difficulties in operations in case of cloud service outages / downtimes	Enterprise Risk Management for Cloud Computing
20	x	-	-	x	-	-	Loss of current and / or potential customers	n/a
21	x	x	-	-	(x)	-	Incomplete overview of actual IT spending	n/a
22	-	x	-	-	-	-	Shadow cloud services support business and IT processes to an unknown extent	COBIT 5
23	-	x	-	-	-	-	Potentially lower availability and reliability of shadow cloud services (productivity risk)	n/a
24	x	x	-	-	-	-	Inappropriate IT governance due to incomplete information as monitoring, reporting and control systems do not include shadow cloud services	COBIT 5

ID	Risk Category ("x" = direct impact, "(x)" = indirect impact, "-" = no impact)						Risk	Relevant Document
	Financial	IT Governance	Information Security [CIA]	Legal	Compliance	Data Protection		
25	-	x	-	x	x	-	Processing client data or highly sensitive client data in the cloud violates agreements with customer and / or supplier	Health Insurance Portability and Accountability Act (HIPAA)
26	x	-	-	x	x	-	Penalties due to non-Compliance with internal and external (industry) regulations	Health Insurance Portability and Accountability Act (HIPAA)
27	x	-	-	x	x	-	Achievement of certifications /attestations (TPA) issued by third parties at risk	n/a
28	-	x	x	x	x	(x)	Data resides within different jurisdictions and protection levels	EU-General Data Protection Regulation (GDPR)
29	-	-	x	x	x	-	'Loss' of copyrights / data ownership / IP due to detrimental contract / terms and conditions	Cloud Controls Matrix (CCM)
30	-	-	-	x	x	-	Cloud provider violates NDA that has been agreed between enterprise and third party	SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
31	-	x	x	-	-	-	Introduction of malicious code into IT environment (by e.g. installing local agents)	ISO/IEC 27001:2013
32	-	-	-	x	x	(x)	Problem of assigning ownership of account info and transferred data in case a non-corporate email address has been registered at cloud provider	n/a
33	x	x	-	x	x	-	Licensing disputes if violation of Terms and Contracts evident, e.g. in case of licences granted for free for "non-commercial use only"	n/a
34	-	x	-	-	-	-	Challenges for future system and data consolidation and standardisation due to distributed and / or not even known system, services and data stored in unknown / incompatible format. This adds complexity to the IT landscape.	COBIT 5
35	x	-	x	x	x	-	If the company falls under the German IT-Security act: the obligation to notify the authorities in case of IT security incidents may be violated	German IT Security Act
36	-	x	-	x	x	x	If personal data of German citizens is affected a required 'Data Processing Agreement' (Auftragsdatenverarbeitung § 11 BDSG) has not been agreed	German Federal Data Protection Act (Bundesdatenschutzgesetz)
37	(x)	x	-	x	x	-	Violation of obligation to display the outsourcing to authorities and / or auditors	German IT Security Act
38	(x)	x	-	x	x	-	Violation of 'examination and control rights' of the authorities if auditing the cloud provider is not possible	German IT Security Act
39	(x)	x	-	x	x	-	Violation of the duty to store data relevant for taxation within the territory of application of the Fiscal Code	Sarbanes-Oxley Act (SoX)
40	(x)	-	-	x	x	-	Data and electronic documents are not stored for the retention time required by law or regulation	Sarbanes-Oxley Act (SoX)
41	(x)	-	-	x	x	-	Authorised Authorities and other authorised third parties are not able to access the data	Sarbanes-Oxley Act (SoX)
42	(x)	x	-	-	-	-	Impaired flexibility and agility of IT environment	COBIT 5
43	(x)	x	(x)	x	x	(x)	Acquisition of cloud provider by a third party, e.g. competitor, supplier or customer	Enterprise Risk Management for Cloud Computing
44	-	-	x	-	x	(x)	Compromised user access or management access to frontend or API of cloud service	Cloud Controls Matrix (CCM)
45	(x)	-	-	x	x	-	Failure of providing data in the required format to internal and / or external stakeholders	Sarbanes-Oxley Act (SoX)
46	(x)	(x)	-	x	-	-	Violation of exclusive agreements / contracts with cloud vendors when also using services of competitors	n/a
47	x	x	-	-	-	-	Low utilisation and poor TCO / ROI of existing on-premises solutions	COBIT 5

ID	Risk Category ("x" = direct impact, "(x)" = indirect impact, "-" = no impact)						Risk	Relevant Document
	Financial	IT Governance	Information Security [CIA]	Legal	Compliance	Data Protection		
48	x	x	-	-	-	-	Interference with company-wide IT Strategy (and Cloud Strategy if applicable), which are supposed to support the Business Strategy	COBIT 5
49	x	x	x	x	x	x	End-to-End monitoring not possible as e.g. no SLA has been agreed (monitoring refers to various perspectives such as financial, IT security etc.)	Enterprise Risk Management for Cloud Computing
50	-	x	x	-	-	-	Available bandwidth of internet connection impaired by increased utilisation of shadow cloud services	COBIT 5
51	-	x	x	-	-	-	Changes of network parameters block shadow cloud services (e.g. changes in port mapping, NAT, blacklisting, proxy or firewall configuration, IP addresses etc.) that may be required for certain business processes	n/a
52	-	x	x	-	-	-	Changes in configuration of client systems may prevent shadow cloud services from being used, unexpectedly	n/a
53	-	x	x	-	x	x	Shadow cloud services become essential for operations (dependency) and can't be easily migrated to internal or supported/approved cloud solutions (vendor lock-in)	Enterprise Risk Management for Cloud Computing
54	(x)	x	x	-	x	x	Solutions provided internally are not used as intended and shadow cloud services are used instead (e.g. file sharing, collaboration etc.)	COBIT 5
55	x	-	-	-	-	-	Exposure to competitive DISadvantages / Internal Weaknesses (regarding SWOT) compared to competitors	n/a
56	x	-	-	-	-	-	Untapped potential: The major benefits of cloud (cost reduction, flexibility, etc.) don't apply to shadow cloud because of improper implementation and usage.	Guiding Principles for Cloud Computing Adoption and Use
57	-	x	-	-	x	-	Heterogeneous collaboration environment: Multiple not integrated solutions for collaboration instead of few integrated solutions (Most shadow cloud services can be categorized as collaboration solutions)	COBIT 5
58	-	x	x	-	-	-	Data leaks due to insufficient control over employee devices (e.g. smartphones, tablets, storage media), the applications on these devices, and the mobile data network. Caused by lack of BYOD-Policy and/or MDM.	Cloud Controls Matrix (CCM)
59	-	-	x	-	-	-	Employees purchase or develop applications or systems (e.g. client-server, virtualized environments) with insufficient security mechanisms (e.g. encryption of data at rest and in transit, password protection).	Cloud Controls Matrix (CCM)
60	-	-	x	-	-	-	Insecure credential storage and authentication. Shadow Cloud Service may independently store credentials that may be compromised and be used for unauthorized access to the enterprise system and resources (in case the same password is used).	Cloud Controls Matrix (CCM)
61	-	-	x	-	x	-	Employee accounts are not under the control of the enterprise and, upon termination of the employee, the employee's access to the data remains.	SOC2/TSP (SysTrust & WebTrust)
62	-	-	x	-	-	-	Loss of knowledge and control in case an employee who set up a shadow cloud service (with a personal account) leaves the organization and certain business processes or functions that rely on this service (e.g. as a data storage) are impaired.	n/a
63	-	x	-	-	-	-	Hampering of the IT department to support business processes by supplying and operating technology. Cloud Shadow IT may thus hurt the execution of these business processes themselves.	COBIT 5

Chapter 4 CASB Market Evaluation

Many vendors provide a wide range of capabilities and options to support organisations secure their cloud usage. This chapter aims to paint a clear picture of the current CASB market as an orientation tool for potential users of a CASB solution. While doing this, the overall question if the utilisation of CASBs sufficiently addresses the risks identified in chapter 3.3 is covered. This is achieved by defining a universal set of evaluation criteria that is applied to the current state of a representative selection of solutions and making a statement about the maturity of the CASB product.

4.1 CASB Market

According to analysts, the market for CASB is rapidly evolving since its emergence in 2012 (Gartner Inc., 2016). It will quickly reach maturity, even though most the providers are still startups financed by venture capital. The market experiences a movement of consolidation driven by acquisitions and partnerships between CASB vendors and established companies. The following selection of events confirm this movement:

- February 2017: Forcepoint acquires Skyfence (ZDNet, 2017)
- October 2016: Proofpoint acquires Firelayers (geektime, 2016)
- September 2016: Oracle acquired Palerra (TechCrunch, 2016)
- June 2016: Symantec acquired Blue Coat, which includes Elastica and Perspecsys (Symantec, 2016)
- June 2016: Cisco acquired CloudLock (Cisco, 2016)
- March 2016: Imperva announces CounterBreach — an integrated DCAP behaviour analytics product integrating its Skyfence CASB and on-premises SecureSphere products (Imperva, 2016)
- October 2015: Check Point partnership with FireLayers (betanews, 2015)
- September 2015: IBM's entry into the CASB market (eSecurityPlanet, 2015)
- September 2015: Microsoft acquisition of Adallom and the launch of Microsoft Cloud App Security (WSJ.com, 2015)
- November 2015: Blue Coat acquired Elastica (VentureBeat, 2015)
- October 2015: Akamai's investment in FireLayers (Business Wire, 2015)
- September 2015: Deloitte's partnership with Bitglass
- July 2015: Imperva's partnership with Forcepoint (then Websense) (Imperva, 2016)
- July 2015: Blue Coat acquired Perspecsys (Blue Coat Systems, 2015)

- April 2015: Palo Alto Networks' acquisition of CirroSecure (Palo Alto Networks, 2015)
- May 2015: Cisco's reseller arrangement with Elastica (businesscloudnews, 2015)
- April 2015: HP's partnership with Adallom (Businesscloudnews, 2015)
- April 2014: Imperva's acquisition of Skyfence (Imperva, 2014)
- February 2014: Centrify's partnership with Elastica (elastica, 2014)

Considering these characteristics, this research focuses on the following list of representative vendors and products for the CASB vendor evaluation. It is not intended to be an exhaustive list of all vendors and products on the market today.

Vendor	Product
Bitglass	Bitglass
CensorNet	Cloud Application Control
CipherCloud	CipherCloud Trust Platform: Cloud Discovery Cloud Security Broker Cloud Security Gateway
CloudLock/Cisco	CloudLock Security Fabric
Forcepoint/Imperva	Forcepoint CASB
Microsoft/Adallom	Cloud App Security
Netskope	Netskope Active Platform: Active Cloud DLP Active Introspection Active Encryption Active Threat Protection Netskope Discovery
Oracle/Palerra	Loric
Palo Alto Networks	Aperture
Proofpoint/FireLayers	FireLayers
Skyhigh Networks	Skyhigh Cloud Access Security Broker
Symantec/Blue Coat	CASB Gateway (Part of Symantec CloudSOC platform)

Table 2: Representative CASB Vendors

Apart from this, the following vendors also offer products with partial CASB functionality, but are not considered complete CASB products and not further evaluated within this research:

Vendor	Product
IBM	Cloud Security Enforcer
StratoKey	StratoKey
Protegrity	Cloud Security Gateway
Vaultive	Vaultive

Table 3: Additional Vendors

4.2 Criteria Definition

An evaluation of the numerous CASB vendors and products with different capabilities and functionalities can become very complex. Therefore, each product is evaluated in four functionality categories and their deployment architecture possibilities, as illustrated in Figure 9. Please note: Some of the features for e.g. file-level access control or DLP are only available for cloud services "supported" by the CASB solution, as it requires specific API utilisation to the cloud services. The list of supported cloud services is different for each CASB product, but the most supported ones across all CASBs include Dropbox, Office 365, Box, Salesforce, Google Apps, and ServiceNow. As the products are constantly extended, more cloud services will be supported in the future. Features for cloud services that are not controlled via API are limited by the information that can be intercepted on e.g. web proxy devices.

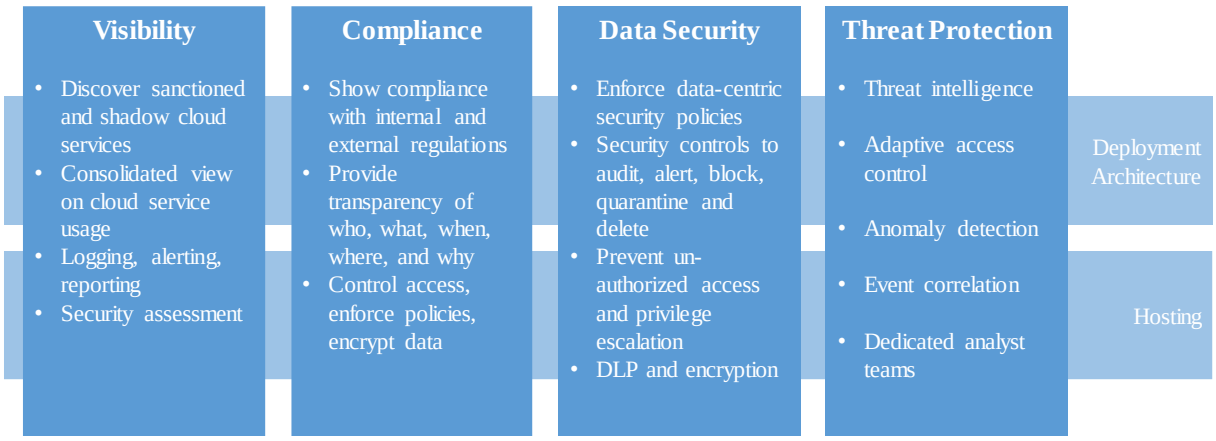


Figure 9: Evaluation Criteria (own presentation)

4.2.1 Visibility

The CASB solution provides functionality to discover the usage of shadow cloud service as well as sanctioned services to create a consolidated view of the organisation's cloud service usage and activities. It provides audit-level logging, alerts and reports to discover unauthorised access or suspicious behaviour such as simultaneous logins into multiple cloud services from

different geographical locations using the same user account. Some solutions also provide security posture assessment databases for visibility into the trustworthiness of cloud service providers. Please refer to Appendix B for screenshots of an exemplary CASB solution with some of these features.

4.2.2 Compliance

The CASB solution helps to comply with internal and external regulations and standards regarding data residency and access to data, as well as cloud usage and the risk associated with specific cloud services. This is achieved by providing transparency over access and activity logs that shows “who, what, when, where, and why” to prove compliance towards auditors. They fill the gap of many SaaS vendors that don’t offer tools for visibility and data protection needed to maintain internal and external compliance.

Some solutions actively help to comply with regulations by controlling access to the cloud, enforcing policies, or encrypting data transferred to the cloud service or at rest. Please refer to Appendix C for screenshots of an exemplary CASB solution with some of these features.

4.2.3 Data Security

The CASB solution provides functionality to protect data by enforcing data-centric security policies that are based on data classification and user access monitoring. These policies are applied through controls such as audit, alert, block, quarantine and delete.

Contextual access control helps to detect and prevent unauthorised access to sensitive data or privilege escalation by governing the level of access a user has based on their role, devices used, and location. Data Loss Prevention (DLP) features help to prevent sensitive data to be shared outside of the organisation by quarantining the data. They are included natively in the CASB product or can be integrated through on-premises DLP products via Internet Content Adaptation Protocol (ICAP).

Some CASB solutions also provide encryption or tokenization features on a file-level and encryption key management can be integrated with on-premises products. Please refer to Appendix D for screenshots of an exemplary CASB solution with some of these features.

4.2.4 Threat Protection

The CASB solution has the capability to protect the organization from the threats posed by cloud services, such as data breaches, account hijacking, malicious insiders, data loss, or APTs (see Chapter 2.3.1). It may utilise threat intelligence to provide adaptive access control, or prevent unwanted devices, users and applications from accessing cloud services and data stored

in the cloud. Anomalous activities are detected by correlating data from different sources, e.g. threat intelligence feed, user data, and malware identification.

Some CASB vendors have dedicated analyst teams to research cloud-specific and cloud-native attacks. Please refer to Appendix D for screenshots of an exemplary CASB solution with some of these features.

4.2.5 Hosting

Most CASB products are available as SaaS applications, on-premises via virtual or physical appliances, or both using a hybrid combination of Cloud-based and on-premises policy enforcement points. While the full-SaaS solution is the most popular and preferred option for most use cases, on-premises components are indispensable for specific use cases regarding regulatory compliance and data sovereignty.

4.2.6 Deployment Architecture

As mentioned in Chapter 2.4, CASB solutions can be deployed in different ways, namely as a forward proxy, reverse proxy, or in API mode that utilises CSP specific APIs.

When CASB products emerged in 2012, the market was segregated between providers that offer proxy modes (forward or reverse) and others that exclusively support API modes (Gartner Inc., 2016). This segregation faded as vendors increasingly offered “multimode CASBs” that can be deployed in the two proxy modes and also support APIs. This leaves the decision to the customer how to deploy the CASB to support the desired use cases. However, not all of the products in this evaluation are considered multimode, and the available options are therefore part of the evaluation criteria.

The deployment architecture of a CASB solution is an integral part of their implementation into existing organisational and operational structures. Further definition and evaluation of the available architectures are therefore discussed in Chapter 5.2 for the development of implementation recommendations.

4.3 Vendor Evaluation

In this section, the representative list of vendors is evaluated according to the criteria defined above and a maturity level is defined (low-medium-high). This evaluation intends to provide a better understanding of the CASB market and is aimed towards organisations as potential users of a CASB solution. It is not, nor is it intended to be, a competitive analysis of the vendors discussed. The functionalities within the categories do not represent a full list of supported features but highlight focus areas of each vendor and major differentiations from other CASB

products. Considering the rapid development of the market and the products, a definite statement about the maturity and functionality of certain CASB solutions would be obsolete very quickly.

4.3.1 Bitglass

General	
Founded	January 2013
CASB Offering	Since January 2014
Functionality	
Visibility	• Cloud application and breach discovery • SaaS security posture assessment DB
Compliance	Patented searchable encryption
Data Security	• Integrated DLP and contextual access control • Data security policy integration • Document management protection (watermarking, encryption with search and sort)
Threat Protection	Universal cloud security analytics
Deployment Architecture	• Multimode (API Support on top of forward- and reverse-proxy modes) • Agentless Ajax-VM technology within the user's browser for real-time data protection and including unmanaged devices
Hosting	SaaS or on-premises
Integration	• MDM and IAM integration (remote wiping, SSO, SAML, IDaaS) • DLP Vendor support • Key Management Interoperability Protocol (KMIP) interface supported
Maturity	
Level	High
Rationalization	• CASB only provider, therefore full concentration on CASB without the need for additional components • Multimode architecture with high feature coverage

4.3.2 CensorNet

General	
Founded	February 2007
CASB Offering	Since April 2015
Functionality	
Visibility	• Cloud service discovery • Risk assessment DB
Compliance	• User and policy control • Real-time reporting of e.g. domains accessed and user actions, productivity and compliance by user, top used cloud applications, trends and bandwidth consumption as well as custom reports
Data Security	Enforce data security policies
Threat Protection	• Online threat detection • Reputation and heuristics across multiple platforms • Detection of threats in SSL-encrypted traffic
Deployment Architecture	• Makes use of existing SWG platform to capture traffic to and from cloud services, therefore based on forward-proxy architecture
Hosting	On-premises physical or virtual appliances, or SaaS
Integration	CASB is a module of CensorNet's Unified Security Service, including Web Security, Email Security, and a 2-Facter authentication solution
Maturity	
Level	Medium
Rationalization	• Full feature coverage only in combination with other products in CensorNet's Unified Security Service • Limited API support

4.3.3 CipherCloud

General	
Founded	October 2010
CASB Offering	Since March 2011
Functionality	
Visibility	• Cloud service discovery • Security posture assessment
Compliance	• Content and user activity monitoring • Industry-specific compliance requirements through tokenization and encryption of sensitive data
Data Security	• Data protection through encryption/tokenization of data flowing to specific cloud services (e.g. Salesforce) to maintain data sovereignty • Integrated cleaning and quarantining on all inbound and outbound cloud content
Threat Protection	Integrated malware detection
Deployment Architecture	Reverse-proxy for Salesforce and a few other services, forward-proxy, API mode for specific cloud services,
Hosting	On-premises virtual or physical appliance or SaaS (only API mode), different functionality of SaaS vs. on-premises
Integration	On-premises key management, and Data-centric audit and protection (DCAP) solutions, DLP
Maturity	
Level	High
Rationalization	• Experienced in the area of CASB • Large customer based in different highly regulated industries • Multimode deployment architecture and high feature coverage

4.3.4 CloudLock/Cisco

General	
Founded	January 2011 (acquired by Cisco in June 2016)
CASB Offering	Since October 2013
Functionality	
Visibility	Crowdsourcing risk ratings for cloud services through the community
Compliance	• Log analysis and reporting for forensics • User and Entity Behaviour Analytics (UEBA) for SaaS, IaaS, PaaS, and IDaaS environments
Data Security	• DLP, data protection • Protection of data (structured and unstructured) • Possibility to leverage native encryption provided by SaaS services that support it through API control
Threat Protection	• Analyses logs from firewalls and proxies • Threat and malware detection • Crowd-sourced cloud cyber security platform with machine learning to provide intelligent cybersecurity analytics
Deployment Architecture	API mode only, supporting a large number of SaaS, PaaS, and IaaS, as well as providing its own API framework that CSPs can integrate
Hosting	SaaS
Integration	• Leverages other APIs of existing firewalls, SIEM, etc. • Support custom applications built on public IaaS or PaaS (e.g. AWS, Force.com) by embedding SDKs via API • Integration with Cisco security products
Maturity	
Level	High
Rationalization	• Experienced in the area of CASB as a focused start-up, now backed by large network and security company • API mode only, but provides innovative API framework and can be integrated with other security products • High feature coverage

4.3.5 Forcepoint/Imperva

General	
Founded	November 2002 (acquired by Forcepoint in February 2017)
CASB Offering	Since January 2014
Functionality	
Visibility	• Cloud service discovery • Security posture assessment
Compliance	Access control
Data Security	• Detailed user activity monitoring • Cloud DLP
Threat Protection	Leverages Imperva's threat intelligence service ThreatRadar
Deployment Architecture	API and reverse-proxy
Hosting	SaaS, within existing DDoS and Incapsula cloud WAF and content delivery network (CDN), or as on-premises physical or virtual appliance
Integration	• Covers custom internally developed SaaS applications built on public SaaS as part of Imperva's DCAP offering • Breach detection product (CounterBreach) integration
Maturity	
Level	-
Rationalization	Highly mature CASB solution as part of Imperva's security portfolio, but the solution was recently acquired by Forcepoint, and it is currently uncertain how Forcepoint will integrate it in its portfolio.

4.3.6 Microsoft/Adallom

General	
Founded	2012 (acquired by Microsoft in September 2015)
CASB Offering	Since February 2013
Functionality	
Visibility	• Cloud service discovery • Risk assessment
Compliance	Reporting over cloud service usage
Data Security	• Data control over supported/sanctioned SaaS via predefined or custom policy enforcement • DLP capabilities, but not in real time, as no proxy mode is currently supported • User activity monitoring
Threat Protection	Detect risky or abnormal behaviour that indicates possible attack
Deployment Architecture	API only
Hosting	SaaS on Azure
Integration	Part of Microsoft's Enterprise Mobility and Security (EMS) suite
Maturity	
Level	Medium-High
Rationalization	• Experienced in the area of CASB as a focused start-up, now backed by large company • High feature coverage, but only API mode and predestined for protecting Microsoft products • Part of a security product suite

4.3.7 Netskope

General	
Founded	October 2012
CASB Offering	Since October 2013
Functionality	
Visibility	Emphasis on cloud service discovery and security posture assessment
Compliance	Deep user behaviour analytics for managed/sanctioned and unmanaged/unsanctioned SaaS
Data Security	• User activity monitoring • DLP/DCAP capabilities • File-level encryption via agents
Threat Protection	Inspection of content for malware (in-line or API based)
Deployment Architecture	• Primarily as forward-proxy (with agents or via proxy chaining) • Reverse-proxy added in 2014 • API support
Hosting	• SaaS on own distributed proxy fabric • Agents available for end-user device control and encryption
Integration	With on-premises DLP systems via ICAP
Maturity	
Level	High
Rationalization	• Experienced and focused on the area of CASB • Multimode deployment architecture • Large customer base • High feature coverage

4.3.8 Oracle/Palerra

General	
Founded	July 2013 (acquired by Oracle in September 2016)
CASB Offering	Since January 2015
Functionality	
Visibility	Dedicated product for cloud shadow IT discovery
Compliance	• User behaviour analytics • Access and in-application activity analytic • Central control of the configuration of SaaS and other cloud service policies
Data Security	• Identification of risky applications installed from Salesforce AppExchange platform
Threat Protection	• Security monitoring, threat protection and incident response via dedicated product for sanctioned cloud services • Incident response with case management, alerting, notification • Support for threat intelligence feeds • Custom enterprise threat modelling
Deployment Architecture	API mode covering SaaS, PaaS, and IaaS
Hosting	SaaS on shared infrastructure or dedicated appliance
Integration	External ticketing system support for incident management
Maturity	
Level	High
Rationalization	• Experienced in the area of CASB as a focused start-up, now backed by large company • API mode only, but covering certain PaaS and IaaS as well • High feature coverage, with an emphasis on threat protection

4.3.9 Palo Alto Networks

General	
Founded	2005
CASB Offering	Since September 2015
Functionality	
Visibility	• Cloud service discovery • Risk identification
Compliance	• Policy management • Reporting • Granular policy enforcement across users • Contextual Risk Control
Data Security	• Security management • File-level monitoring and protection • Content scanning • Quarantine of users and data
Threat Protection	• Malware detection • Threat prevention • Remediation • Analytics
Deployment Architecture	API mode
Hosting	SaaS
Integration	• Palo Alto Networks Next-Generation Security Platform • Palo Alto firewalls required for traffic interception
Maturity	
Level	High
Rationalization	• Experienced security company with successful complementary security products • High feature coverage • API mode only, but large and growing number of supported cloud services

4.3.10 Proofpoint/FireLayers

General	
Founded	November 2013 (acquired by Proofpoint in October 2016)
CASB Offering	Since April 2014
Functionality	
Visibility	Cloud Application discovery (without security posture assessment)
Compliance	• User behaviour analytics • Access control
Data Security	• Activity monitoring (focus on privileged account monitoring) for supported SaaS and IaaS • Email inspection for Office 365
Threat Protection	Contextual access control
Deployment Architecture	• Multimode (API, forward- and reverse-proxy) • SAML Gateway
Hosting	On AWS or on-premises with a virtual appliance
Integration	2-factor authentication for cloud services that don't natively support it
Maturity	
Level	-
Rationalization	Highly mature CASB solution, but recently acquired by Proofpoint and it is currently unclear how it will be integrated into Proofpoints strong security portfolio and if it will be available as a standalone CASB.

4.3.11 Skyhigh Networks

General	
Founded	December 2011
CASB Offering	Since January 2013
Functionality	
Visibility	• Visibility into Cloud usage and risk • Dedicated intelligence team to maintain risk rating DB • Understand data leaving the organisation • Identify gaps in policy enforcement
Compliance	• User behaviour analytics • Audit internal and external sharing • Enforce governance policies • Enforce DLP policies for data at rest and in motion
Data Security	• User activity monitoring • DLP/DCAP features • Encryption and tokenization or structured and unstructured data for supported cloud services
Threat Protection	• Identify, mitigate, and remediate insider threats, compromised accounts, and privileged user threats • Contextual access control • Cross-app threat intelligence • Incident remediation
Deployment Architecture	Multimode (forward- and reverse- proxy, API)
Hosting	SaaS or on-premises virtual appliance
Integration	Integrates with leading DLP solutions via ICAP
Maturity	
Level	High
Rationalization	• Experienced and focused on the area of CASB • Multimode deployment architecture • Large customer base • High feature coverage • High quality of risk rating DB

4.3.12 Symantec/Blue Coat

General	
Founded	1996 (acquired by Symantec in June 2016)
CASB Offering	Since July 2015
Functionality	
Visibility	• Cloud service discovery • Cloud service assessment rating • Cloud usage analytics
Compliance	• Granular policy enforcement • User behaviour analytics • Reporting • Enforce consistent policies for sensitive data discovery and protection across on-premises and cloud services
Data Security	• Tokenization and encryption of data in SaaS (proprietary tokenization method) • Deep content inspection with DLP features
Threat Protection	• Cloud service intrusion detection • Malware analysis • Incident and response activities • Data science and machine learning methods
Deployment Architecture	Multimode (forward- and reverse-proxy, API)
Hosting	SaaS and on-premises
Integration	• Part of Symantec CloudSOC platform • Blue Coat SWG • Symantec DLP • On-premises encryption suites • Encryption products from Symantec, HPE, Gemalto, etc.
Maturity	
Level	High
Rationalization	• Experienced in the area of CASB, recently acquired by large security company with synergistic portfolio, but part of a security suite

	• Multimode deployment architecture • High feature coverage

4.3.13 Evaluation Result

Today, CASBs primarily address SaaS applications that support back-office processes (e.g. file sharing, CRM, ERP, HR, service desk, collaboration and productivity). However, the functionalities of some vendors evaluated above (e.g. CloudLock/Cisco, Oracle/Palerra, Proofpoint/Firelayers) indicate a trend also to cover popular IaaS offerings. PaaS support is not increasing in a similar way. Industry-specific applications, such as healthcare or pharma, as well as applications for business intelligence or data analytics, are not well-covered.

The evaluation shows that API mode is widely adopted and continues to cover more cloud services. In the long term, API support should be able to obviate the need to intercept traffic on a proxy level if they mature not just in breadth (supporting more cloud services) and depth (more granular features and deeper integration), but also in availability and performance. The maturity of APIs today is widely divergent across the vendors evaluated. However, smaller SaaS providers are unlikely to develop mature APIs for their service, and therefore the need for proxy capabilities will not disappear completely.

As almost all of the evaluated vendors are big players in the CASB market, the maturity is generally high. However, recent acquisitions and the resulting consequences for the CASB solution itself add uncertainty to the maturity of some solutions. When looking only at the list of features of the products, a majority of the risks introduced by Cloud Shadow IT can be addressed be either one of them. However, this strongly depends on how the solutions are implemented within an organisation and on the use cases they cover. With a clearer picture of the CASB market and some vendors, the implementation and use case coverage are discussed in more detail in Chapter Chapter 5 .

4.4 Trends and Future Developments

The rapid development of the CASB market shows no signs to decline in the near future. While today less than 5% of large enterprises use a CASB, Gartner predicts that by 2020, this number is expected to rise to 85% (Gartner Inc., 2016). This increase is closely tied to the growing significance of SaaS: The persistent concerns about the security, privacy, and compliance of these services increase the urgency for control and visibility of cloud services. Another beneficial factor is the wide adoption of IDaaS solutions that deliver cloud single-sign on and provide synergistic integration with CASBs.

The market growth gives reason to anticipate battles for control over this market and the already strong movements caused by acquisitions will increase. Large vendors will likely acquire rather than build their own CASB solution to satisfy the demand of their customers.

As briefly mentioned in chapter 2.4, products such as IDaaS or Secure Web Gateways (SWG) as well as other cloud services such as DDoS protection, DLP, DCAP, or Web Application Firewalls (WAF) have high potential to work synergistically with CASB products. As their functionality constantly extends, it can even be speculated that some of these products and their markets eventually merge, but the CASB market development has shown that this becomes increasingly less likely (Gartner Inc., 2016).

Another significant development will be the increasing maturity and coverage of APIs for cloud services. Improved APIs will deliver more utility and support new security use cases.

These trends show that the maturity of CASB solutions will only rise, either through in-house developments or acquisitions and therefore will address more and also upcoming new risks introduced by Cloud Shadow IT and cloud services in general.

Chapter 5 CASB Implementation

This chapter focuses on the third research question, of "How should a company integrate a CASB solution into the existing organisational and operational structures to best satisfy the company's needs?". However, every organisation has individual requirements.

The right fit - regarding CASBs - strongly depends on the IT environment, compliance requirements with related controls, and motivation regarding taking control of the cloud usage. The recommendations for implementing CASB solutions are therefore based on company profiles that reflect these characteristics. The key differentiators between these company profiles are the following:

- ***Existing security infrastructure***: Organisations may already utilise security solutions that provide critical points of integration with CASB solutions. Examples include, but are not limited to, Secure Web Gateways (SWG), Security Information and Event Management (SIEM), and Identity Management (IDM). Integrations with these solutions do not only enable additional use cases and improve the overall security but also prevent CASB from becoming another enterprise security silo.
- ***Client device location***: The cloud services may be accessed from end-user devices (e.g. PC, Laptop, and Smartphone) within the corporate network through managed infrastructure, or remotely from outside of the network with a direct connection to the cloud service through the public internet and unmanaged infrastructure.
- ***Device management***: The end-user devices themselves may be corporate- or employee-owned equipment and managed via e.g. Mobile Device Management (MDM) or local agents that control the connections to cloud services. More and more organisations embrace the adoption of BYOD, which poses additional challenges for the device management and introduces security risks, as private devices are not controlled in the same way as corporate devices.
- ***Sanctioned cloud services or IDaaS***: The organisation may have approved specific cloud services for corporate usage with subscriptions that provide control functionality and integration with internal authentication services. Alternatively, IDaaS solutions may also provide a mechanism for authentication to approved cloud services.
- ***Motivation and desired use cases***: Regardless of how the IT landscape of an organisation is constructed, the motivation of supporting the business with specific use cases and addressing specific risks or compliance requirements also determines the course of IT and the implementation of a CASB solution in particular.

The resulting recommendations are categorised as follows:

- ***Deployment Architecture***: Forward- or reverse-proxy with or without API mode.
- ***Hosting***: CASB on-premises or as SaaS.
- ***Integration Leverages***: Making use of specific existing security solutions.
- ***Pre-Integration Actions***: Actions that should be conducted before the implementation.
- ***Post-Integration Actions***: Actions that should be conducted after the implementation.

5.1 Company Profiles

5.1.1 Company A

This hypothetical organisation has advanced security infrastructure in place and is interested in a way to provide visibility of the cloud services by its employees to gain an overview and to define measures according to the results such as adjusting the configuration of the existing infrastructure.

Profile	
Existing security infrastructure	• Identity Management (IDM) • Firewall (FW) • Secure Web Gateway (SWG) • Security Information and Event Management (SIEM)
Corporate network or remote devices?	Corporate
BYOD or corporate devices?	Corporate
Sanctioned Cloud Services/IDaaS	No
Motivation/Use Cases	• Discover shadow cloud services • Assess risk of identified cloud services • Monitor of cloud usage and logging of activities • Identify policy enforcement gaps of existing security infrastructure • Identify connections to bad domains and IP addresses • Enforce controls on identified cloud services

5.1.2 Company B

This organisation has some security infrastructure in place and already encourages its employees to use approved cloud services. It is looking for a way to identify unapproved cloud services used by its employees as well as to detect malicious behaviour on approved services that should ideally be communicated to the existing SIEM solution as an interface to event monitoring and incident management.

Profile	
Existing security infrastructure	• SWG • FW • SIEM • IDM
Corporate network or remote devices?	Both
BYOD or corporate devices?	Corporate
Sanctioned Cloud Services/IDaaS	Yes
Motivation/Use Cases	• Identify sensitive data upload to unsanctioned cloud services and block upload in the event of policy violations • Detect data leakage by users or exfiltration by malicious on-premises software to unsanctioned cloud services • Detect malicious user and privileged user behaviour within sanctioned cloud services • Detect compromised user accounts across sanctioned cloud services • Feed all event information to a SIEM solution for correlation and alerting

5.1.3 Company C

This organisation has limited security infrastructure in place and uses a variety of approved cloud services. It is primarily looking for a way to increase the security of these services by enforcing existing policies on the users of these services and the data transferred to and stored within. Any encryption should be done with keys managed by the organisation.

Profile	
Existing security infrastructure	• IDM • Data Loss Prevention (DLP) • SWG
Corporate network or remote devices?	Both
BYOD or corporate devices?	Corporate
Sanctioned Cloud Services/IDaaS	Yes
Motivation/Use Cases	• Detect malicious data stored in sanctioned cloud services that could be distributed to user devices • Identify users with excessive privileges that could be compromised or pose an insider threat • Prevent sensitive data uploads to sanctioned cloud services • Discover sensitive data stored in sanctioned cloud services and enforce DLP policies • Monitor permissions for sharing files and folders within sanctioned cloud services • Encrypt data stored in sanctioned cloud services with keys owned and managed by the organisation • Check and verify security configuration of sanctioned cloud services

5.1.4 Company D

This organisation has advanced security infrastructure in place and has approved a variety of cloud services for usage by its employees. It also approved the usage of employee-owned devices (BYOD) that are not closely managed by the mobile device management (MDM) software to allow unrestricted access to the approved cloud services from these devices. Therefore, the organisation is looking for a way to increase the security of the approved cloud services and the data stored within, particularly from unmanaged devices.

Profile	
Existing security infrastructure	• Enterprise Mobility Management (EMM) / Mobile Device Management (MDM) • IDM • Information Rights Management (IRM) • Key Management Service (KMS) • SWG
Corporate network or remote devices?	Both
BYOD or corporate devices?	BYOD
Sanctioned Cloud Services/IDaaS	Yes
Motivation/Use Cases	• Restrict access to sanctioned cloud services (e.g. read-only) from unmanaged devices • Require 2-factor authentication for access to sanctioned cloud services from unmanaged devices outside of the corporate network • Encrypt data before the transfer to the cloud and support access to encrypted data from any device • Apply sensitive data protection mechanisms on data downloaded to unmanaged devices

5.2 Deployment Architecture

This section describes the three major deployment modes of CASB solutions, as mentioned in Chapter 4.2.6, in more detail and discusses advantages and disadvantages that come with each mode for controlling devices, networks, and services. Additionally, a fourth deployment mode is discussed for simple log collection purposes that is suitable for most visibility-only use cases.

5.2.1 Forward-Proxy

When deployed as a forward proxy, the CASB routes all cloud traffic from end-user devices to the cloud services and back, as shown in Figure 10. This is the most intrusive deployment method from the end-user point of view, as all traffic is forced to be routed to the CASB. If an organisation already uses gateways such as web proxies, the CASB can be “chained” as an

upstream proxy. Some organisations also use web proxies that are hosted in the cloud for devices outside of the corporate network.

If an organisation has no existing web proxies or Secure Web Gateways (SWG) for chaining, some CASB vendors may deploy agents on the on-premises or remote devices that route the traffic directly to the forward proxy. Another method to control end-user devices is to enforce proxy auto-configuration files (PAC) via mobile device management (MDM) solutions.

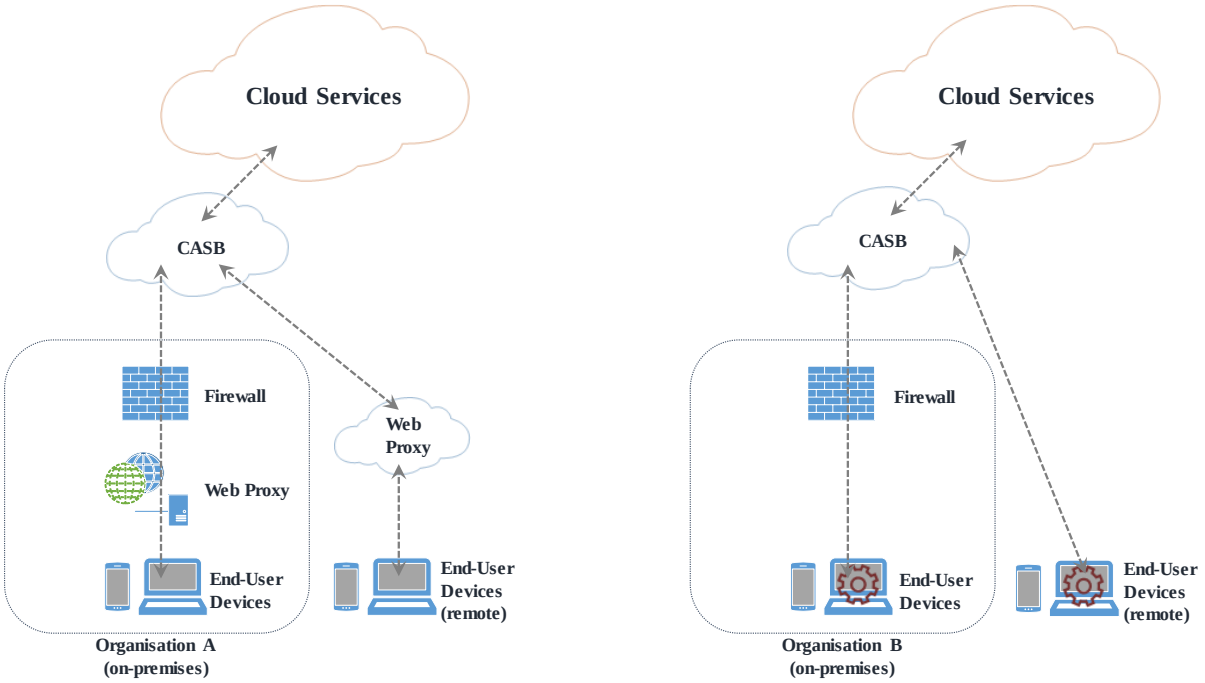


Figure 10: CASB as Forward-Proxy via chaining and with managed devices (own presentation based on Skyhigh)

CASB in forward-proxy-mode typically provide encryption methods with end-user devices and may use digital certificates or support key management solutions managed by the organisation.

Advantages

- Gaining visibility of shadow cloud services, since all traffic goes through the CASB (only managed devices)
- SSL/TLS encryption is handled well due to forwarding
- Ability to interpret web service API-based access (e.g. REST, JSON, SOAP)
- Existing web proxies/SWGs can be utilised (proxy chaining)

Disadvantages

- Privacy concerns due to full traffic analysis of managed devices, especially with SSL decryption enabled
- Unmanaged devices and BYOD difficult to cover
- Single point of failure and exposure to DDoS attacks and bottlenecks

5.2.2 Reverse-Proxy

CASBs deployed as reverse-proxies follow a different approach to controlling access to cloud services. When a user attempts to access specific cloud services, the cloud service redirects the traffic of this user to the reverse proxy. The CASB then passes the authentication to an identity provider/IDM solution (that may also be hosted in the cloud [IDaaS]) but modifies the URL as belonging to the CASB instead of the cloud service. This way, access to the cloud service is routed through the reverse proxy without the need to control the end-user devices. The initial redirection is controlled by the cloud service and is based on the user's credentials and rulesets in the cloud service to determine which users to redirect where. Figure 11 illustrates this deployment mode.

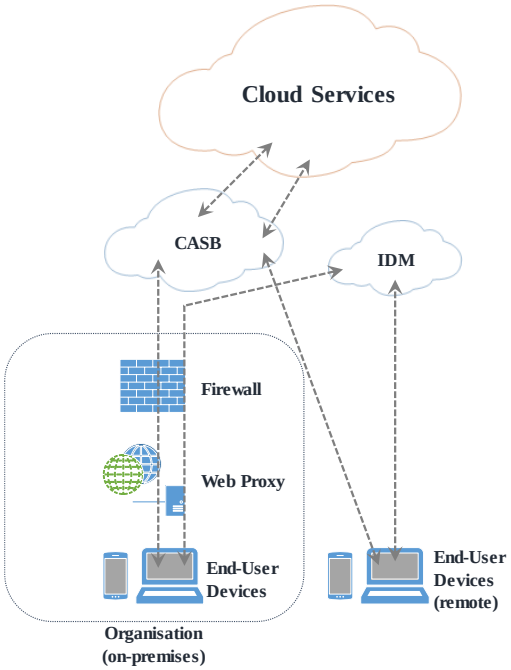


Figure 11: CASB as Reverse Proxy (own presentation based on Skyhigh)

Advantages

- No privacy concerns as only traffic with specific cloud services goes through the CASB
- BYOD is addressed without the need to control the end-user devices

Disadvantages

- Traffic with unsanctioned cloud services is not covered
- URL modification is difficult to enforce for mobile SaaS applications with hard-coded URLs
- SSL/TLS encryption is difficult to handle due to redirect
- Single point of failure and exposure to DDoS attacks and bottlenecks

5.2.3 API-Mode

CASBs with API mode rely on native features of the cloud services by giving CASBs permission to access its API directly. This exposes mechanisms by which the CASB can provide extra security controls, such policy enforcement, as audit trails of user activity, content inspection, scanning of user privileges, sharing permissions on files and folders, or application security settings - without requiring measures at the organisation's side. However, the cloud service must be configured to allow API access from the CASB, and the user must be associated with an organisation, e.g. by corporate credentials. This utilisation of cloud service APIs can be configured in a complementary manner with forward- or reverse-proxy architectures. For encryption, the CASB may offer on-premises or cloud hosted key management options. Figure 12 illustrates this mode.

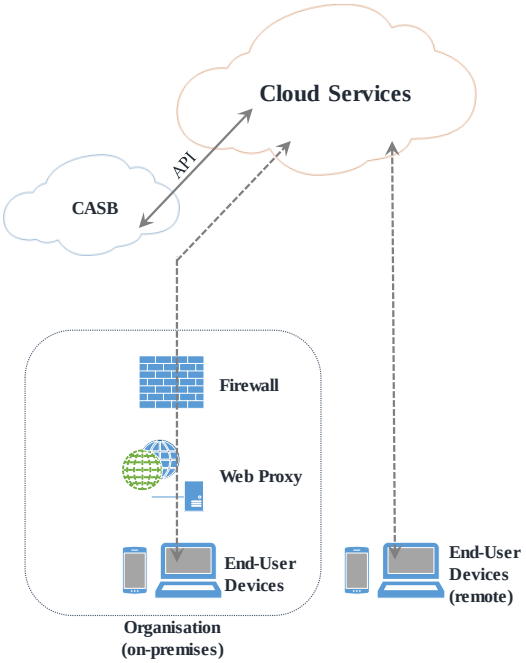


Figure 12: CASB with API mode (own presentation based on Skyhigh)

Advantages

- Deep and granular visibility into SaaS usage and user behaviour

- Visibility over data already uploaded to the cloud service and control over activities with that data, e.g. access control, policy enforcement, and activity logs
- Can be used on top of forward- or reverse-proxy architectures
- No single point of failure or DDoS exposure, since it does not route the traffic
- BYOD is addressed without the need to control the end-user devices

Disadvantages

- Only a small number of major cloud services provide API support and the functionality differs between the providers and may not fully support all CASB use cases
- Hybrid deployment (proxy and API) may be required for encryption and tokenization use cases with some cloud services

5.2.4 Log collection

In some cases, organisations may only be interested in a low profile CASB implementation that provides functionality to gain visibility into the cloud service usage and activities. Some CASB solutions can be deployed with basic functionality for log collection and processing to create a consolidated view of cloud usage as well as audit-level logging, alerting, and reporting. This mode is non-intrusive to the IT environment but relies on existing infrastructure such as proxies, firewalls, or security monitoring to collect log files from and offers limited to none functionality in the areas of compliance, data security, and threat protection.

5.3 Hosting

Another implementation consideration of CASB solutions, besides the deployment architecture, is the hosting location of the service. The solution components can be located at the supplier and provided to the organisation as a cloud service, or they can be located at the organisation in the form of physical or virtual appliances which are then integrated with the existing infrastructure. The decision whether to host a CASB on-premises or via SaaS should be based upon to its security and compliance requirements. While a SaaS brings a variety of advantages, it could be hosted outside of the organisations' jurisdictions and contradict local regulatory requirements on personal data processing. An on-premises model is required in this case.

5.4 Requirements and Recommendations

This section defines requirements and recommendations for the implementation of a CASB solution for each defined company profile based on their characteristics.

5.4.1 General Implementation Requirements

The two most important architectural choices – deployment architecture and hosting – are not solely determined by the organisations' preferences and desired use cases: Direct dependencies exist between certain characteristics of the IT environment and possible CASB architectures.

Forward-proxy mode is always possible, as long as the client device is on the corporate network and accesses the cloud service through it. If a forward-proxy CASB must cover remote devices, these devices must be managed to force all traffic through the CASB. Unmanaged remote devices are not reliably covered by a forward-proxy, but it can still be used if these devices are prevented from using the cloud service. This is achieved by configuring the cloud service to accept access from CASB connections only.

Reverse-proxy and API mode are only possible with sanctioned cloud services that support this integration with the specific CASB or with a supported IDaaS solution that is integrated with the CASB.

5.4.2 Company A

Based on the characteristics of this organisation, the following implementation with additional actions is recommended.

Recommendations	
Deployment Mode	Log collection
Hosting	SaaS
Integration Leverages	**IDM**: Authentication log and metadata source, enhanced user intelligence (e.g. for user geographies or departments) **FW, SWG**: Traffic log sources and control enforcement points after discovery, SSL/TLS decryption is required for deeper cloud usage monitoring and activity logging **SIEM**: Central log source
Pre-Integration Actions	• Verify log quality and completeness of relevant log providers • Create list of approved cloud services and ensure compliance of approved services with e.g. EU GDPR • Populate list of approved services to the CASB • Conduct organisation-wide employee training regarding cloud service use

Post-Integration Actions	• Block high-risk services (or splash pages) • Weekly or monthly audit reports to verify policy • Closely monitor low-medium risk services • Whitelist low-risk services for allowed use cases • Weekly or monthly review list of allowed services • Conduct targeted training for employees involved in unwanted cloud activities

5.4.3 Company B

Based on the characteristics of this organisation, the following implementation with additional actions is recommended.

Recommendations	
Deployment Mode	Forward-Proxy and API (hybrid mode)
Hosting	SaaS
Integration Leverages	**SWG**: Use for proxy-chaining, traffic log source and control enforcement point **SIEM**: Source of traffic log data, destination for events detected by the CASB **IDM**: Authentication information across cloud services, enhanced user intelligence (e.g. for user geographies or departments)
Pre-Integration Actions	• If the CASB must be deployed on-premises, deploy agents on the endpoint devices that route the traffic directly to the forward-proxy to cover remote clients • If not already defined, consider the definition of policies for data classification to identify sensitive data
Post-Integration Actions	• Corrective measures against detected incidents • Security improvements to prevent incidents

5.4.4 Company C

Based on the characteristics of this organisation, the following implementation with additional actions is recommended.

Recommendations	
Deployment Mode	API
Hosting	SaaS
Integration Leverages	**IDM:** Enhanced user intelligence for account compromise and insider threat detection (e.g. for user geographies or departments) **DLP:** Policy enforcement on sensitive data in the cloud **KMS:** Key management for file encryption
Pre-Integration Actions	• If not already defined, consider the definition of policies for data classification, role-based access control, segregation of duties (SoD), secure cloud service configuration, collaboration, and encryption • Populate policies to on-premises DLP solution • Conduct organisation-wide employee training regarding cloud service use
Post-Integration Actions	• Put users with detected behavioural anomalies on watch lists • Conduct targeted training for employees involved in unwanted cloud activities

5.4.5 Company D

Based on the characteristics of this organisation, the following implementation with additional actions is recommended.

Recommendations	
Deployment Mode	Reverse Proxy
Hosting	SaaS
Integration Leverages	**EMM/MDM**: Provide security features for both corporate and BYOD devices **IDM**: Leverage where possible to enable familiar and improved user experience (e.g. for user geographies or departments) **IRM**: Provide protection mechanisms for sensitive data **KMS**: Manage encryption keys
Pre-Integration Actions	• If not already defined, consider the definition of policies for data classification, BYOD

	• Conduct organisation-wide employee training regarding cloud service and device usage • Consider the implementation of a 2-factor authentication solution to use across all cloud services • Configure KMS according to best practices
Post-Integration Actions	• Conduct periodic security training for employees with own devices • Consider the prohibition of employee-owned devices and move to corporate devices with increased management

5.5 Challenges

The implementation of a CASB solution, even with the recommendations above, is not free from additional risks introduced by the solution. When deployed in forward- or reverse-proxy mode, a CASB represents a single point of failure that could potentially compromise access to cloud services if it becomes unavailable. A CASB is exposed to the public internet and therefore exposed to vulnerabilities through e.g. DDoS attacks to compromise the service. Availability and performance issues can also occur if the CASB does not have sufficient resources to handle all requests from regular users. The organisation is responsible for providing sufficient resources if the solution is hosted on-premises on physical or virtual appliances. For SaaS solutions, organisations must rely on the provider.

Further complications for the use of CASBs are privacy concerns. Forward-proxies intercept and analyse the entire internet traffic of connected devices, not only limited to cloud services. With SSL/TLS encryption enabled without restriction, this also includes sensitive data such as online banking and other PII that are subject to data protection laws and regulations.

Organisations must consider these challenges early in the process of implementing a CASB solution and take appropriate measures to avoid the exposure to additional risks while attempting to address the risks derived from Cloud Shadow IT. It is also recommended to work on these challenges together with the CASB vendor in close collaboration, even after the implementation, to create a sustainable solution against Cloud Shadow IT.

Chapter 6 Conclusion

This chapter contains the conclusion of this research. The fundamental problem stated that no comprehensive guidance exists on how to implement and integrate CASB on top of existing systems without creating yet another silo. This led to several research goals that were paraphrased into three main research questions:

1 What are the risks derived from the uncontrolled usage of cloud services (Cloud Shadow IT) within companies today?
2 Does the utilisation of Cloud Access Security Brokers sufficiently address the risks derived from Cloud Shadow IT?
3 How should a company integrate a CASB solution into the existing organisational and operational structures to best satisfy the company's needs?

The following sections briefly summarise and discuss the answers to these questions.

6.1 Risks Derived from Cloud Shadow IT

Enterprise risk management is an integral part of every organisation. In 2012, COSO defined a way to integrate cloud computing into the risk management by developing a Cloud Computing Governance. This can be used to evaluate the risks of potential cloud services before implementing them. The message is that risks are individual to every organisation and that an evaluation is inevitable to determine the likelihood and impact of harmful events. Therefore, the goal of this research was to create awareness for potential risks derived from the uncontrolled usage of cloud services and to enable organisations to evaluate their risk exposure. This is achieved firstly by providing information about the phenomenon of Cloud Shadow IT, its causes, and measures against it. The research then provides a comprehensive list of documents that support organisations to define internal and external requirements they commit to comply with. Lastly, the risk register presents a pool of Cloud Shadow IT risks already defined for organisations to use in their risk identification, definition, and evaluation activities.

6.2 Utilisation of CASB to address risks

The second research question compliments the research to clarify if CASBs are capable of addressing the risks derived from Cloud Shadow IT. Again, this depends on the needs of the individual organisation. Therefore, the goal of this research was to assist organisations to gain knowledge about the CASB market and current vendors of CASB products. The market was found be rapidly evolving but mature enough to have spawned a large number of competitive vendors with products sufficient to manage Cloud Shadow IT risks. The functionality break-

down of 12 representative vendors supports organisations to evaluate each one against their specific needs.

6.3 CASB Implementation

The third research question completes the goal of this research by providing recommendations on the implementation of a CASB to gain control of the cloud usage. Practical recommendations require knowledge about the organisation, its IT landscape and needs. Therefore, assumptions are made about important characteristics and several company profiles are defined to reflect the diversity of organisations that may use this research. Thus, the profile that best matches can be identified to provide valuable recommendations on the CASB architecture, leveraging existing infrastructure, and actions to be taken before and after the implementation.

Combined, this research represents a holistic approach on Cloud Shadow IT with end-to-end guidance from the risk awareness to mitigation.

Chapter 7 Bibliography

Barker, S. & Fiedler, B., 2011. Decision Makers, Strategists or Just End-users? Redefining End-User Computing for the 21st Century: A Case Study. *Journal of Organizational and End User Computing,* Issue 23, pp. 1-14.

betanews, 2015. *FireLayers and Check Point bring security to enterprise cloud apps.* [Online]
Available at: https://betanews.com/2015/10/05/firelayers-and-check-point-bring-security-to-enterprise-cloud-apps/
[Accessed 15 01 2017].

Blue Coat Systems, 2015. *Blue Coat acquires Perspecsys to make the public cloud private.* [Online]
Available at: https://www.bluecoat.com/company/news/blue-coat-acquires-perspecsys-make-public-cloud-private
[Accessed 15 01 2017].

Brenner, W., György, A., Pirouz, M. & Uebernickel, F., 2011. *Bewusster Einsatz von Schatten-IT: Sicherheit & Innovationsförderung,* St. Gallen: s.n.

BSI, 2011. *Cloud Computing Grundlagen.* [Online]
Available at:
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html
[Accessed 22 October 2016].

Bungartz, O., 2012. *Handbuch interne Kontrollsysteme (IKS). Steuerung und Überwachung von Unternehmen.* 3rd ed. Berlin: Erich Schmidt Verlag.

Business Wire, 2015. *Akamai Joins YL Ventures in FireLayers Funding Round.* [Online]
Available at: http://www.businesswire.com/news/home/20151020005048/en/Akamai-Joins-YL-Ventures-FireLayers-Funding
[Accessed 15 01 2017].

businesscloudnews, 2015. *Cisco, Elastica join forces on cloud security monitoring.* [Online]
Available at: http://www.businesscloudnews.com/2015/04/22/cisco-elastica-join-forces-on-cloud-security-monitoring/
[Accessed 15 01 2017].

Businesscloudnews, 2015. *Cloud security vendor Adallom secures $30m from HP, Rembrandt Venture Partners.* [Online]
Available at: http://www.businesscloudnews.com/2015/04/15/adallom-secures-30m-in-series-c-led-by-hp/
[Accessed 15 01 2017].

Cisco, 2016. *Cisco completes its acquisition of CloudLock.* [Online]
Available at: http://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/cloudlock.html
[Accessed 15 01 2017].

Cloud Security Alliance (CSA), 2013. *The Notorious Nine - Cloud Computing Top Threats in 2013.* [Online]
Available at: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf
[Accessed 5 January 2016].

Cloud Security Alliance (CSA), 2016. *The Treacherous 12 - Cloud Computing Top Threats in 2016.* [Online]
Available at: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[Accessed 5 January 2017].

COSO, 2012. *Enterprise Risk Management for Cloud Computing - Thought Paper.* [Online]
Available at: https://www.coso.org/Documents/Cloud-Computing-Thought-Paper.pdf
[Accessed 5 January 2017].

elastica, 2014. *Centrify and Elastica Partner to Provide Comprehensive Cloud Security Solution for SaaS Applications.* [Online]
Available at: https://www.elastica.net/2014/02/centrify-and-elastica-partner-to-provide-comprehensive-cloud-security-solution-for-saas-applications/
[Accessed 15 01 2017].

eSecurityPlanet, 2015. *IBM Cloud Security Enforcer Emerges from the Shadows.* [Online]
Available at: http://www.esecurityplanet.com/network-security/ibm-cloud-security-enforcer-emerges-from-the-shadows.html
[Accessed 15 01 2017].

Forrester Inc., 2016. *The Forrester Wave™: Cloud Security Gateways, Q4 2016.* [Online]
Available at: The Forrester Wave™: Cloud Security Gateways, Q4 2016
[Accessed 10 01 2017].

Gartner Inc., 2014. *Gartner's 2014 Hype Cycle for Emerging Technologies.* [Online]
Available at: http://www.gartner.com/newsroom/id/2819918
[Accessed 22 October 2016].

Gartner Inc., 2016. *Gartner's 2016 Hype Cycle for Emerging Technologies.* [Online]
Available at: http://www.gartner.com/newsroom/id/3412017
[Accessed 22 October 2016].

Gartner Inc., 2016. *Market Guide for Cloud Access Security Brokers.* [Online]
Available at: https://www.gartner.com/doc/3488119/market-guide-cloud-access-security
[Accessed 16 12 2016].

geektime, 2016. *Proofpoint acquires Firelayers for $55 million and announces new anti-malware tool.* [Online]
Available at: http://www.geektime.com/2016/10/21/proofpoint-acquires-firelayers-and-announces-new-anti-malware-tool-for-2017/
[Accessed 15 01 2017].

Hagemeister, G., Lui, B. & Kons, M., 2008. Individuelle Datenverarbeitung in den Unternehmen. Anforderungen aus Sicht der Ordnungsmäßigkeit. *Zeitschrift Interne Revision,* Issue 42, pp. 76-80.

Hagenau, T., 2016. *Cloud Computing - der Hype ist vorbei.* [Online]
Available at: http://www.computerwoche.de/a/cloud-computing-der-hype-ist-vorbei,3069749
[Accessed 22 October 2016].

Imperva, 2014. *Imperva to Acquire Incapsula and Skyfence.* [Online]
Available at: http://investors.imperva.com/phoenix.zhtml?c=247116&p=irol-newsArticle&ID=1897860
[Accessed 15 01 2017].

Imperva, 2016. *Imperva Announces General Availability of Imperva CounterBreach.* [Online]
Available at: http://investors.imperva.com/phoenix.zhtml?c=247116&p=irol-newsArticle&ID=2152035
[Accessed 15 01 2017].

Imperva, 2016. *Imperva Skyfence and Raytheon|Websense Team to Help Organizations Secure Cloud Applications.* [Online]
Available at: http://investors.imperva.com/phoenix.zhtml?c=247116&p=irol-newsArticle&ID=2071122
[Accessed 15 01 2017].

Jones, D., Behrens, S., Jamieson, K. & Tansley, E., 2004. The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation. *ACIS 2004 Proceedings*, Issue Paper 96.

Microsoft Corp., 2005. *The STRIDE Threat Model.* [Online]
Available at: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
[Accessed 5 January 2016].

NIST, 2011. *Special Publication 800-145: The NIST Definition of Cloud Computing.* s.l.:s.n.

Palo Alto Networks, 2015. *Palo Alto Networks® Acquires CirroSecure.* [Online]
Available at: https://www.paloaltonetworks.com/company/press/2015/palo-alto-networks-acquires-cirrosecure.html
[Accessed 15 01 2017].

Symantec, 2016. *Symantec Acquires Blue Coat.* [Online]
Available at: https://www.symantec.com/theme/blue-coat-acquisition?inid=ghp_banner_bcaquisittion
[Accessed 15 1 2017].

TechCrunch, 2016. *Oracle Buys Palerra to Boost Its Security Stack.* [Online]
Available at: https://techcrunch.com/2016/09/18/oracle-buys-palerra-to-boost-its-security-stack/
[Accessed 15 01 2017].

VentureBeat, 2015. *Blue Coat acquires cloud security startup Elastica for $280M.* [Online]
Available at: http://venturebeat.com/2015/11/07/source-blue-coat-is-buying-cloud-security-startup-elastica-for-more-than-300m/
[Accessed 15 01 2017].

WSJ.com, 2015. *Microsoft Plans to Buy Israeli Cloud-Security Firm Adallom for $320 Million.* [Online]
Available at: https://www.wsj.com/articles/microsoft-plans-to-buy-israeli-cloud-security-

firm-adallom-for-320-million-1437390286
[Accessed 15 01 2017].

ZDNet, 2017. *Forcepoint acquires Skyfence in cloud security push.* [Online]
Available at: http://www.zdnet.com/article/forcepoint-acquires-skyfence-in-cloud-security-push/
[Accessed 16 02 2017].

Zimmermann, S. & Rentrop, C., 2012. *Schatten-IT*, Konstanz: s.n.

Appendix A

Typical Risks of Cloud Computing (Source: (COSO, 2012))

Disruptive force

Facilitating innovation (with increased speed) and the cost-savings aspects of cloud computing can themselves be viewed as risk events for some organizations. By lowering the barriers of entry for new competitors, cloud computing could threaten or disrupt some business models, even rendering them obsolete in the future. For example, streaming media over the Internet was a technology solution that significantly reduced the sales of CDs and DVDs and the need for physical retail stores. Existing competitors that fully embrace the cloud might be able to bring new ideas and innovation into their markets faster. Since cloud computing solutions yield considerable short-term cost savings due to reduced capital expenditures, an organization adopting the cloud might be able to extract better margins than its non-cloud competitors. Thus, when an industry member adopts cloud solutions, other organizations in the industry could be forced to follow suit and adopt cloud computing.

Residing in the same risk ecosystem as the CSP and other tenants of the cloud

When an organization adopts third-party-managed cloud solutions, new dependency relationships with the CSP are created with respect to legal liability, the risk universe, incident escalation, incident response, and other areas. The actions of the CSP and fellow cloud tenants can impact the organization in various ways. Consider the following:

- Legally, third-party cloud service providers and their customer organizations are distinct enterprises. However, if the CSP neglects or fails in its responsibilities, it could have legal liability implications for the CSP’s customer organizations. But if a cloud customer organization fails in its responsibilities, it is less likely there would be any legal implications to the CSP.
- Cloud service providers and their customer organizations are likely to have separate enterprise risk management (ERM) programs to address their respective universe of perceived risks. Only in a minority of cases (involving very high-dollar contracts) will CSPs attempt to integrate portions of their ERM programs with those of their customers. The universe of risks confronting an organization using third-party cloud computing is a combination of risks the individual organization faces along with a subset of the risks that its CSP is facing.

Lack of transparency

A CSP is unlikely to divulge detailed information about its processes, operations, controls, and methodologies. For instance, cloud customers have little insight into the storage location(s) of data, algorithms used by the CSP to provision or allocate computing resources, the specific controls used to secure components of the cloud computing architecture, or how customer data is segregated within the cloud.

Reliability and performance issues

System failure is a risk event that can occur in any computing environment but poses unique challenges with cloud computing. Although service-level agreements can be structured to meet particular requirements, CSP solutions might sometimes be unable to meet these performance metrics if a cloud tenant or incident puts an unexpected resource demand on the cloud infrastructure.

Vendor lock-in and lack of application portability or interoperability

Many CSPs offer application software development tools with their cloud solutions. When these tools are proprietary, they may create applications that work only within the CSP's specific solution architecture. Consequently, these new applications (created by these proprietary tools) might not work well with systems residing outside of the cloud solution. In addition, the more applications developed with these proprietary tools and the more organizational data stored in a specific CSP's cloud solution, the more difficult it becomes to change providers.

Security and compliance concerns

Depending on the processes cloud computing is supporting, security and retention issues can arise with respect to complying with regulations and laws such as the Sarbanes-Oxley Act of 2002 (SOX), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the various data privacy and protection regulations enacted in different countries. Examples of these data privacy and protection laws would include the USA PATRIOT Act, the EU Data Protection Directive, Malaysia's Personal Data Protection Act 2010, and India's IT Amendments Act. In the cloud, data is located on hardware outside of the organization's direct control. Depending on the cloud solution used (SaaS, PaaS, or IaaS), a cloud customer organization may be unable to obtain and review network operations or security incident logs because they are in the possession of the CSP. The CSP may be under no obligation to reveal

this information or might be unable to do so without violating the confidentiality of the other tenants sharing the cloud infrastructure.

High-value cyber-attack targets

The consolidation of multiple organizations operating on a CSP's infrastructure presents a more attractive target than a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a CSP solution in most cases are higher with respect to confidentiality and data integrity.

Risk of data leakage

A multi-tenant cloud environment in which user organizations and applications share resources presents a risk of data leakage that does not exist when dedicated servers and resources are used exclusively by one organization. This risk of data leakage presents an additional point of consideration with respect to meeting data privacy and confidentiality requirements.

IT organisational changes

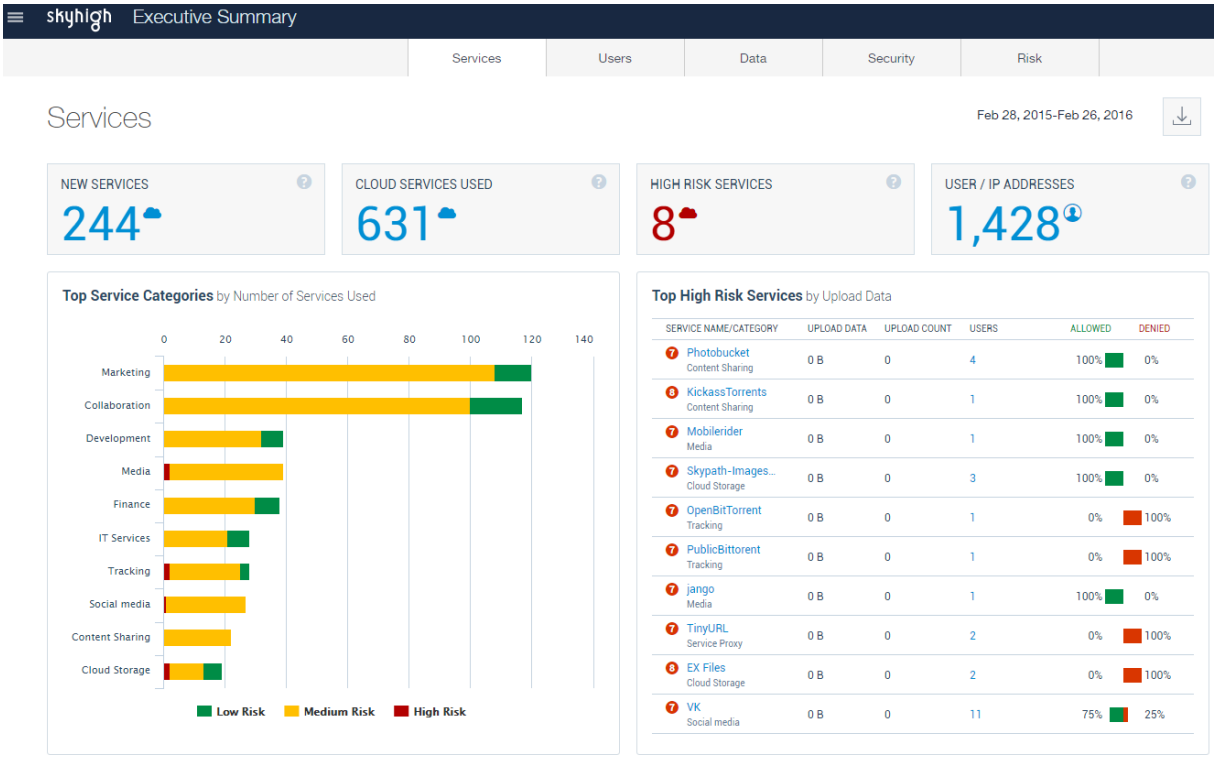
If cloud computing is adopted to a significant degree, an organization needs fewer internal IT personnel in the areas of infrastructure management, technology deployment, application development, and maintenance. The morale and dedication of remaining IT staff members could be at risk as a result.

Cloud service provider viability

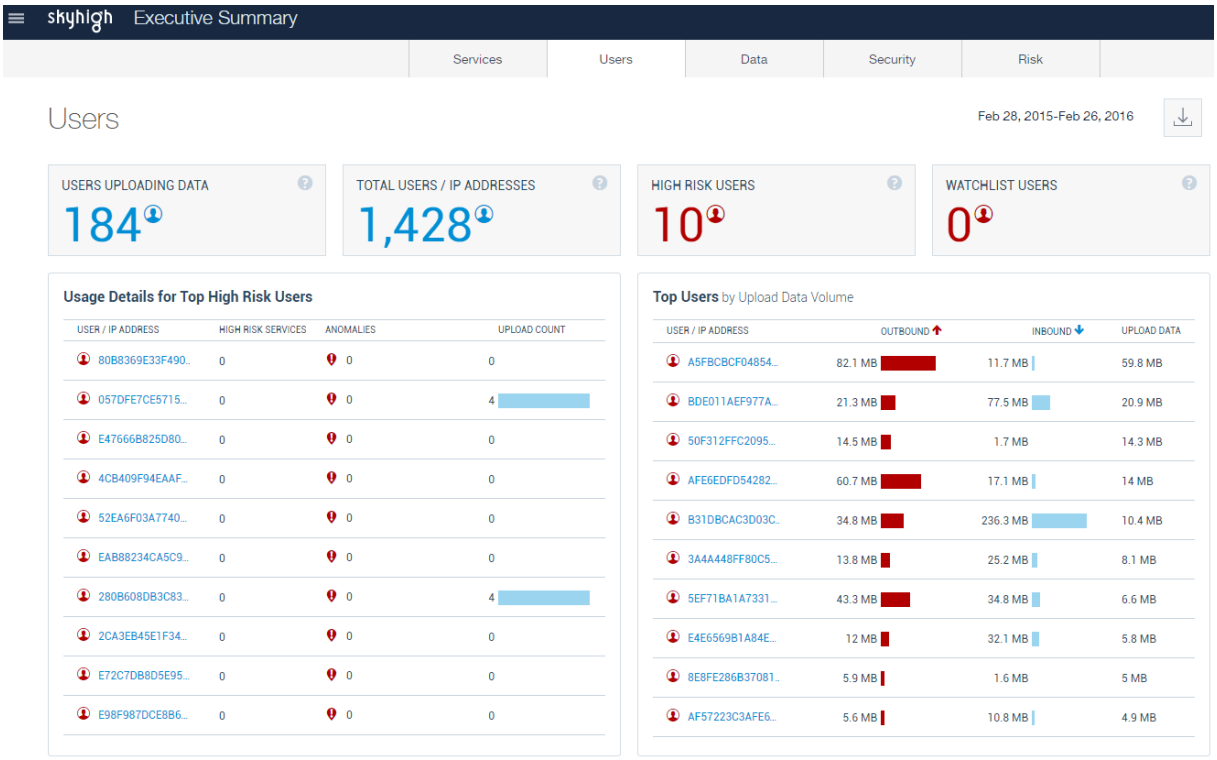
Many cloud service providers are relatively young companies, or the cloud computing business line is a new one for a well-established company. Hence the projected longevity and profitability of cloud services are unknown. At the time of publication, some CSPs are curtailing their cloud service offerings because they are not profitable. Cloud computing service providers might eventually go through a consolidation period. As a result, CSP customers might face operational disruptions or incur the time and expense of researching and adopting an alternative solution, such as converting back to in-house hosted solutions.

Appendix B

Visibility Functionality (selection)

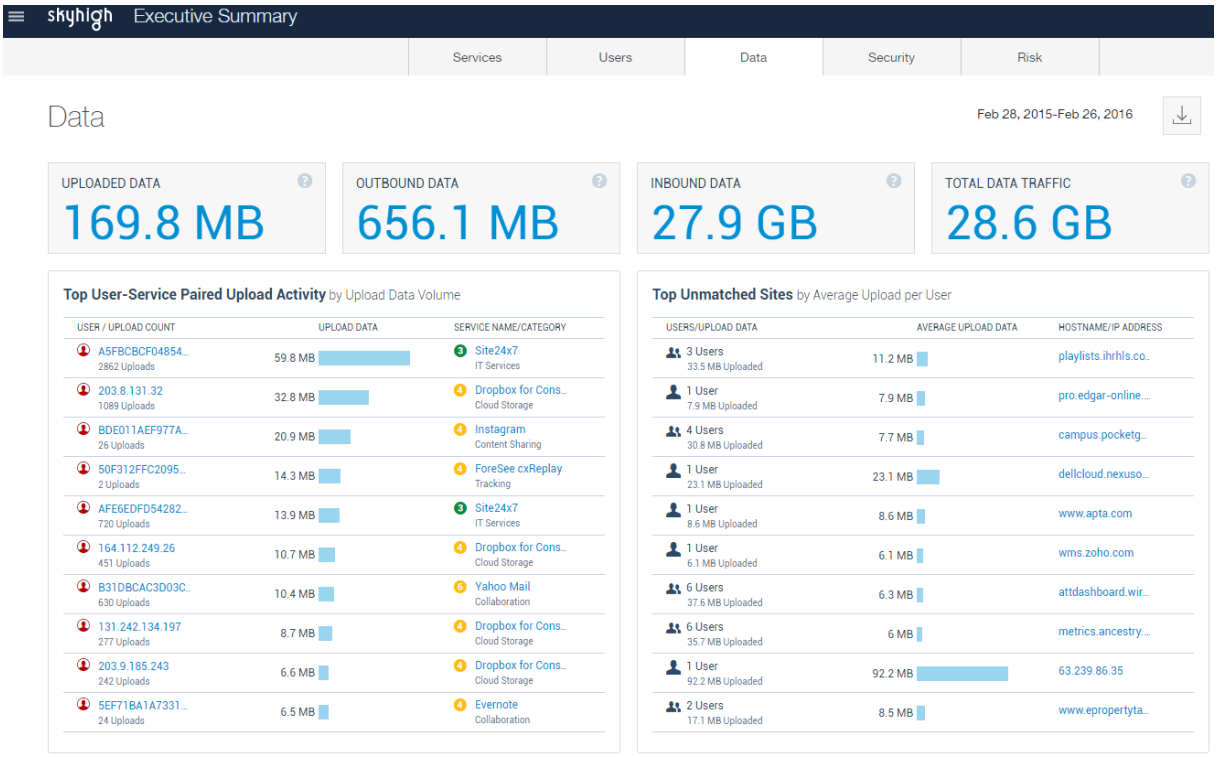


Screenshot 1: Dashboard with overview of discovered cloud services

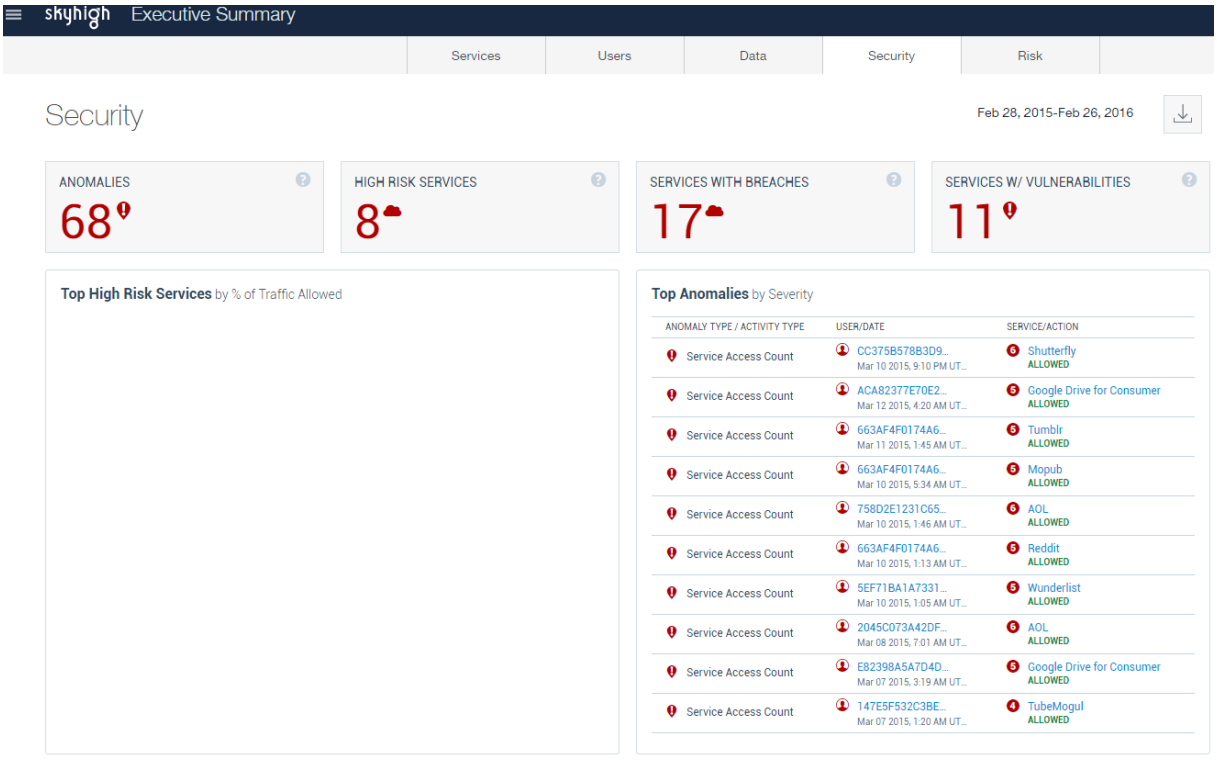


Screenshot 2: Dashboard with overview of cloud service users (usernames/IP-Addresses are tokenized)

Appendix B: Product Screenshots of Visibility Functionality - Source: Skyhigh

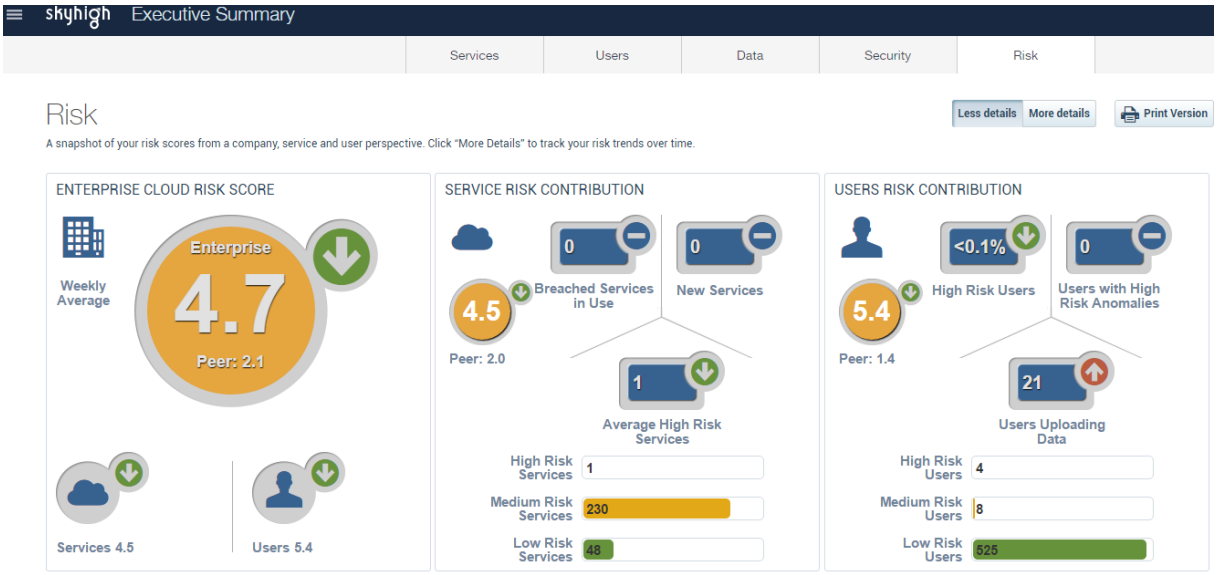


Screenshot 3: Dashboard with overview of data transferred between the organization and cloud services

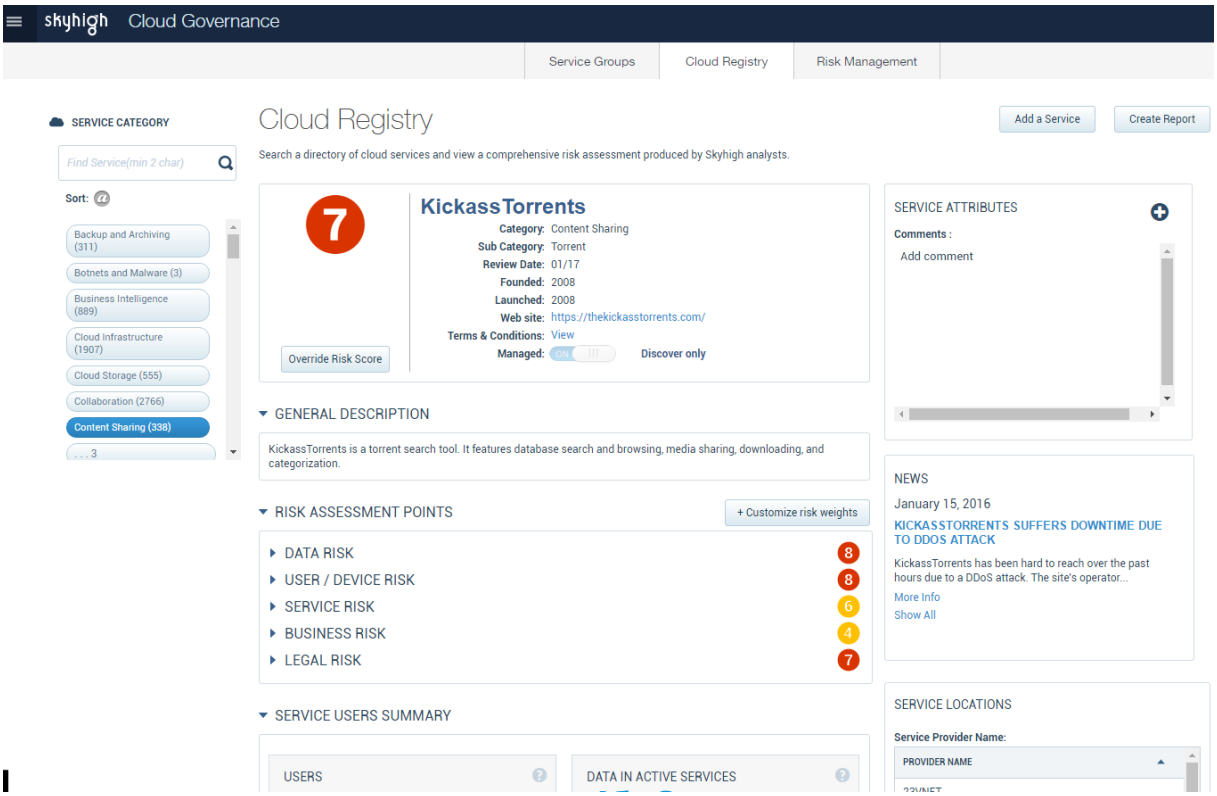


Screenshot 4: Dashboard with overview of security incidents

Appendix B: Product Screenshots of Visibility Functionality - Source: Skyhigh

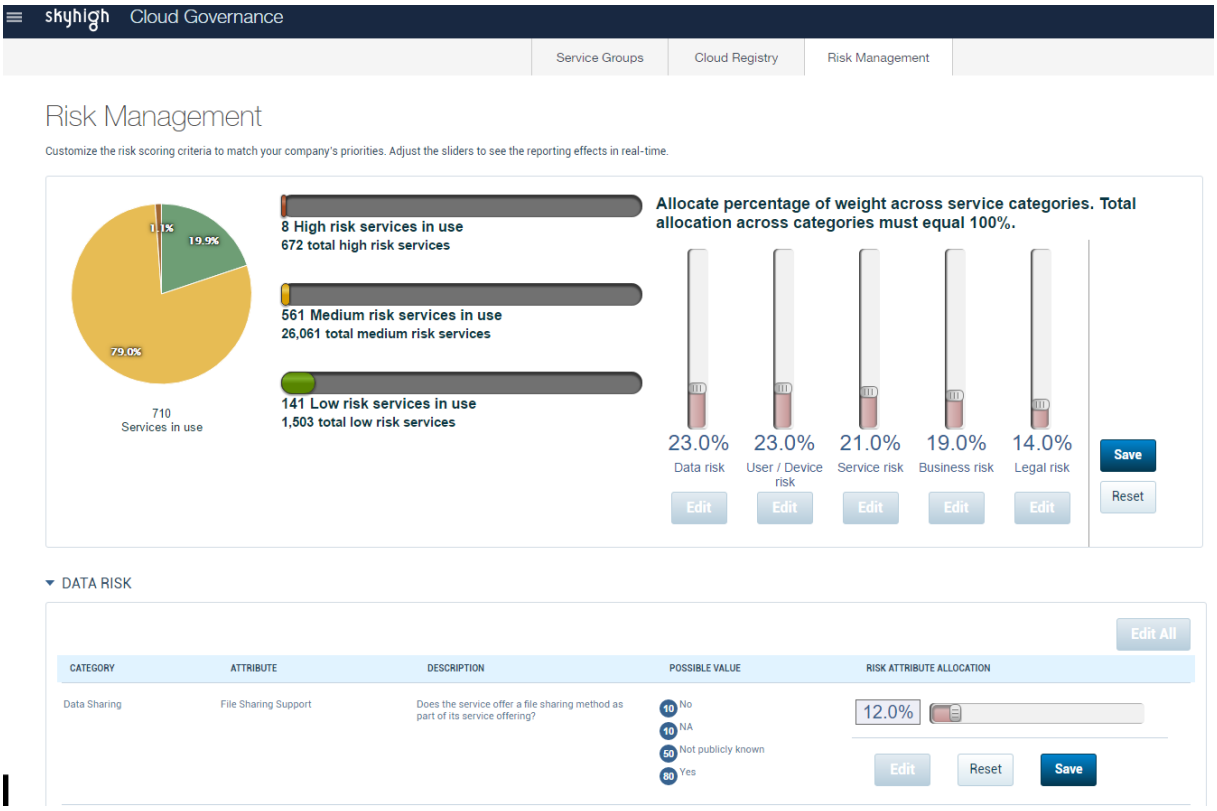


Screenshot 5: Dashboard with overview of overall and detailed risk scores of discovered cloud services



Screenshot 6: Risk score breakdown of exemplary cloud service, comprised of 45 individual risk attributes

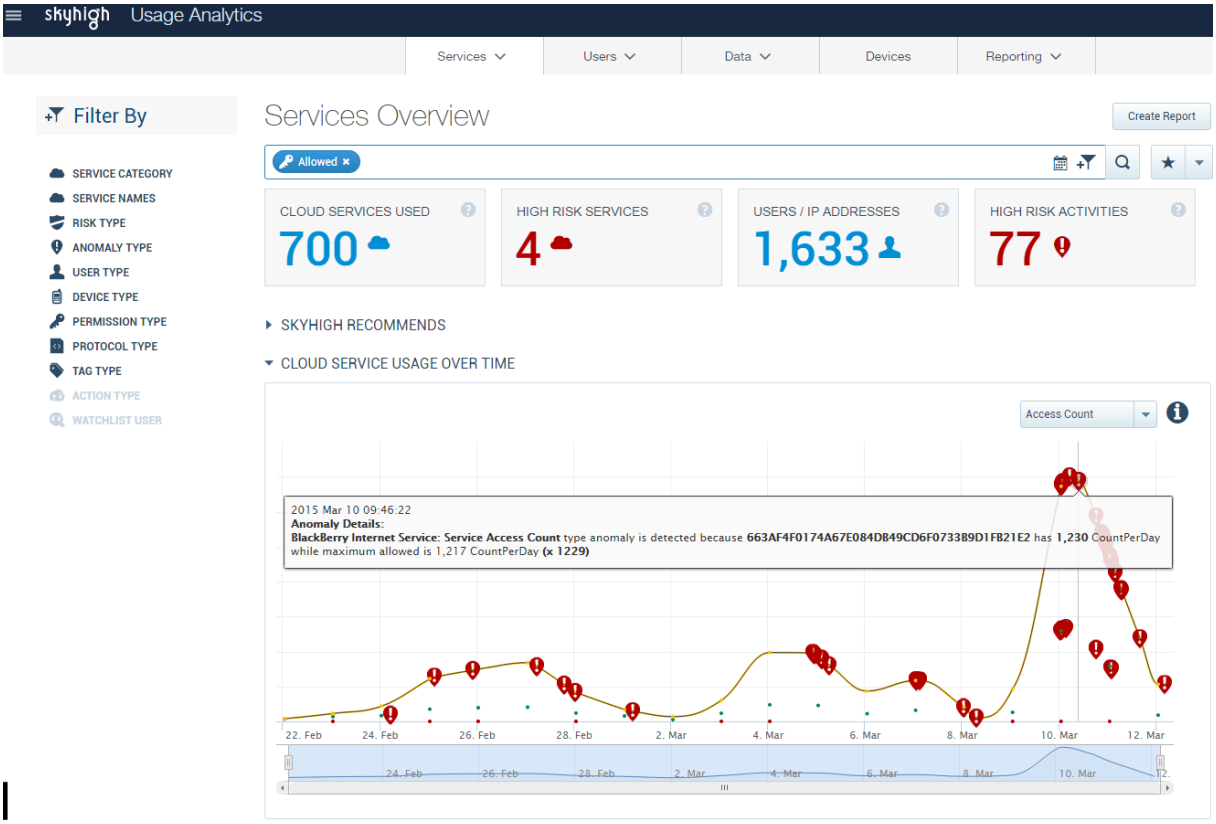
Appendix B: Product Screenshots of Visibility Functionality - Source: Skyhigh



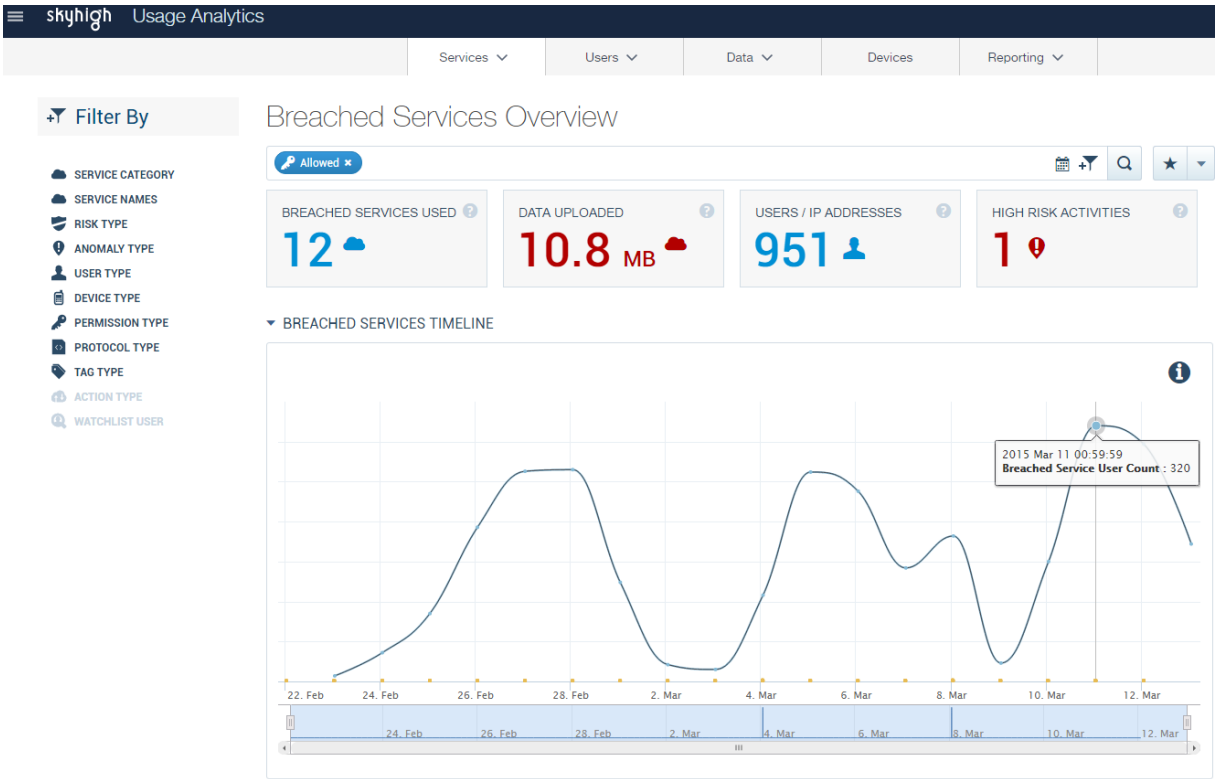
Screenshot 7: Customization of risk weights per category of for each individual risk attribute

Appendix C

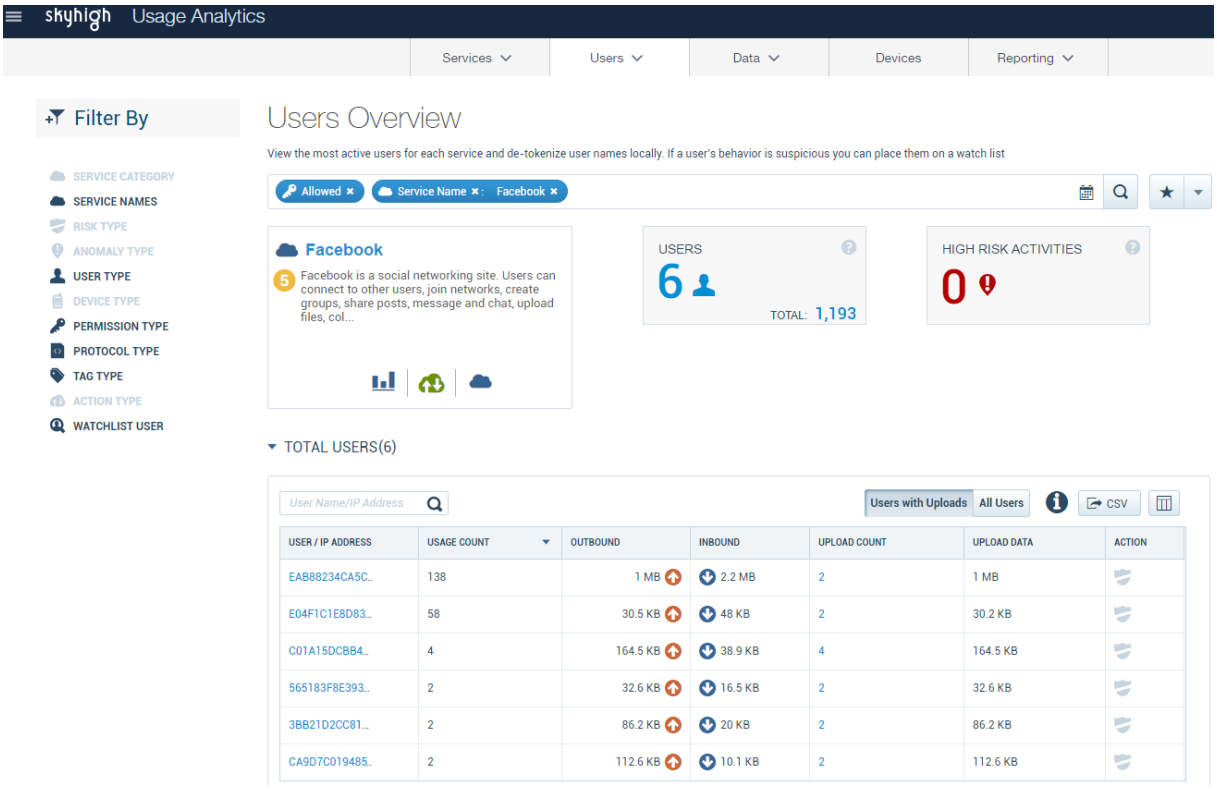
Compliance Functionality (selection)



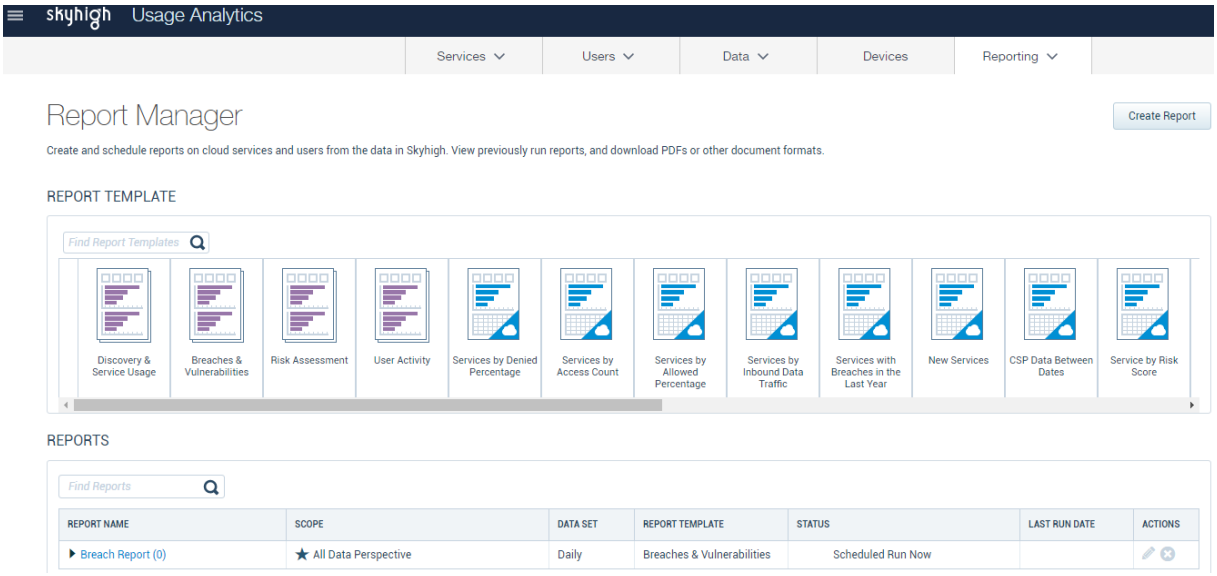
Screenshot 8: Cloud service usage over time



Screenshot 9: Overview of breached service usage over time



Screenshot 10: Usage overview of specific cloud services and users

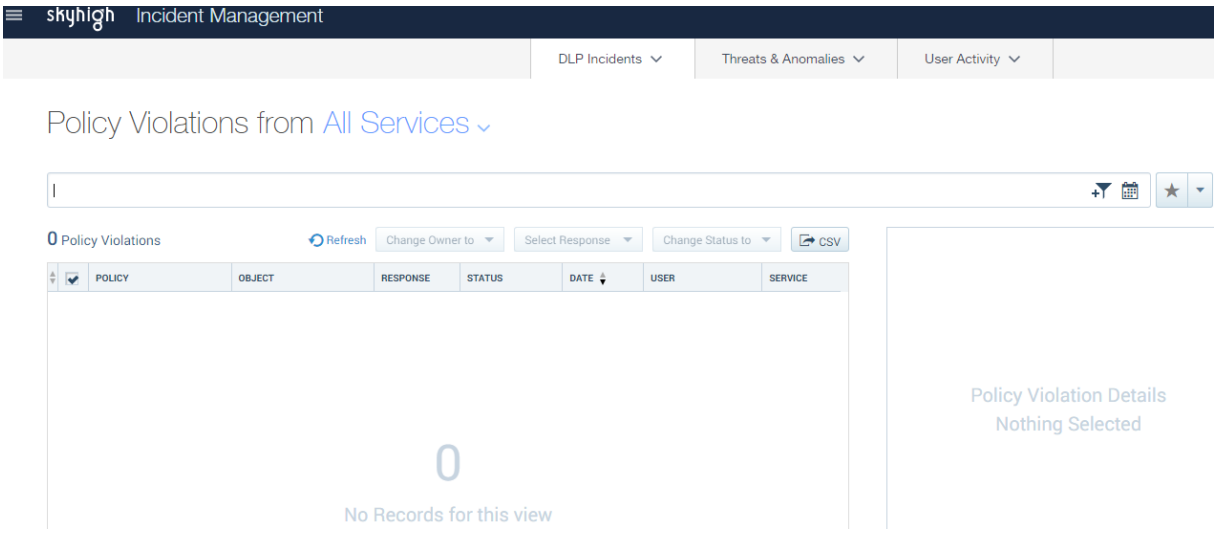


Screenshot 11: Report manager for custom report creation

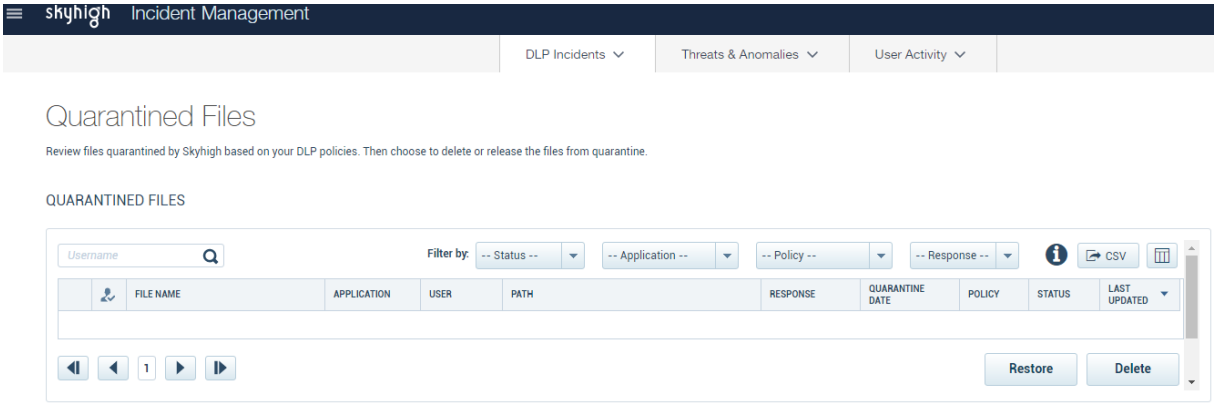
Appendix D: Product Screenshots of Data Security and Threat Protection Functionality - Source: Skyhigh

Appendix D

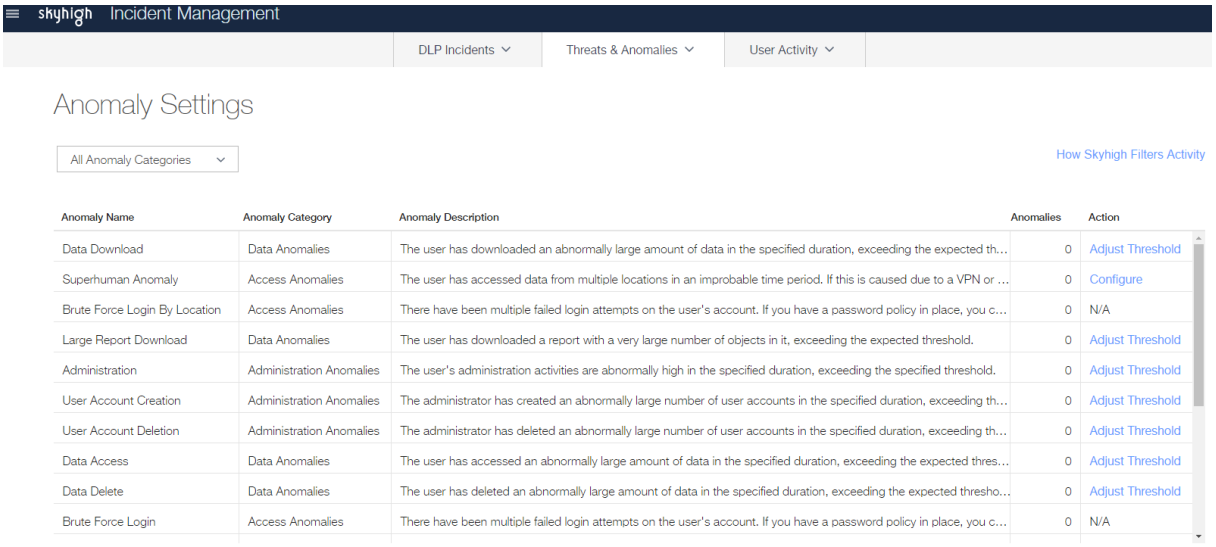
Data Security and Threat Protection Functionality (selection)



Screenshot 12: Policy Violations (no data)

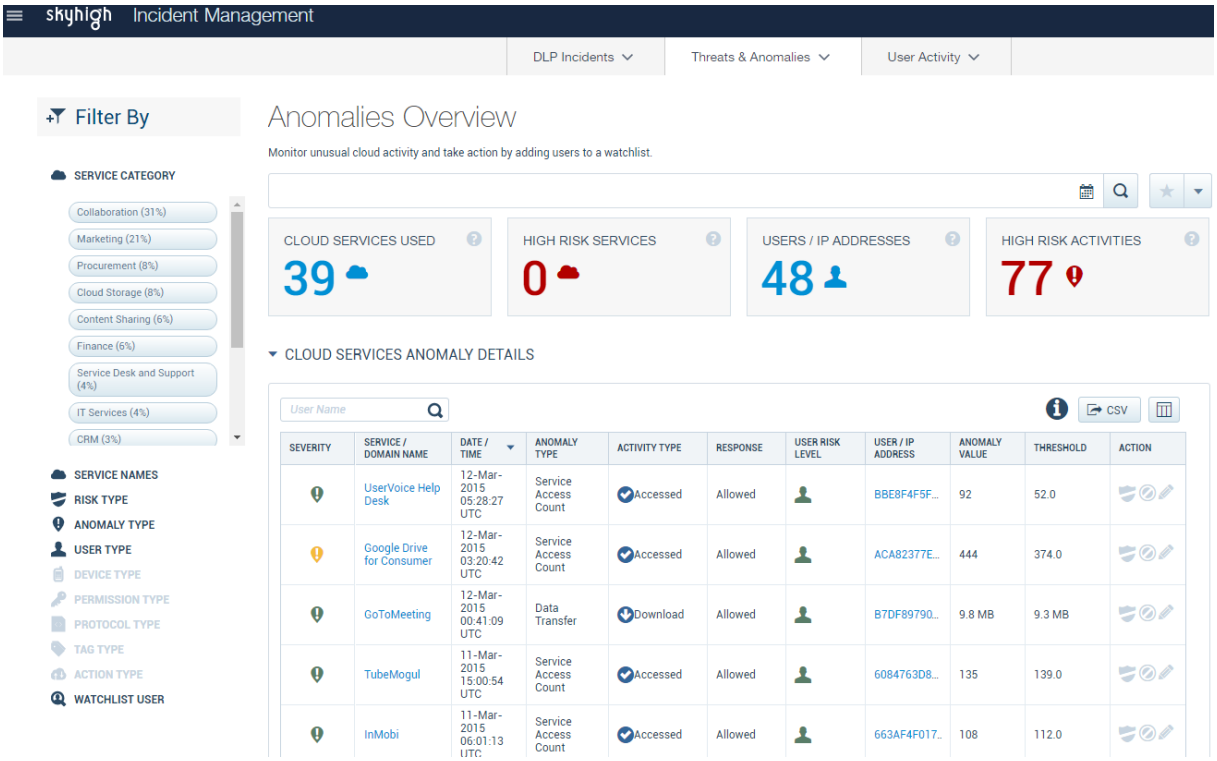


Screenshot 13: Quarantined Files (no data)

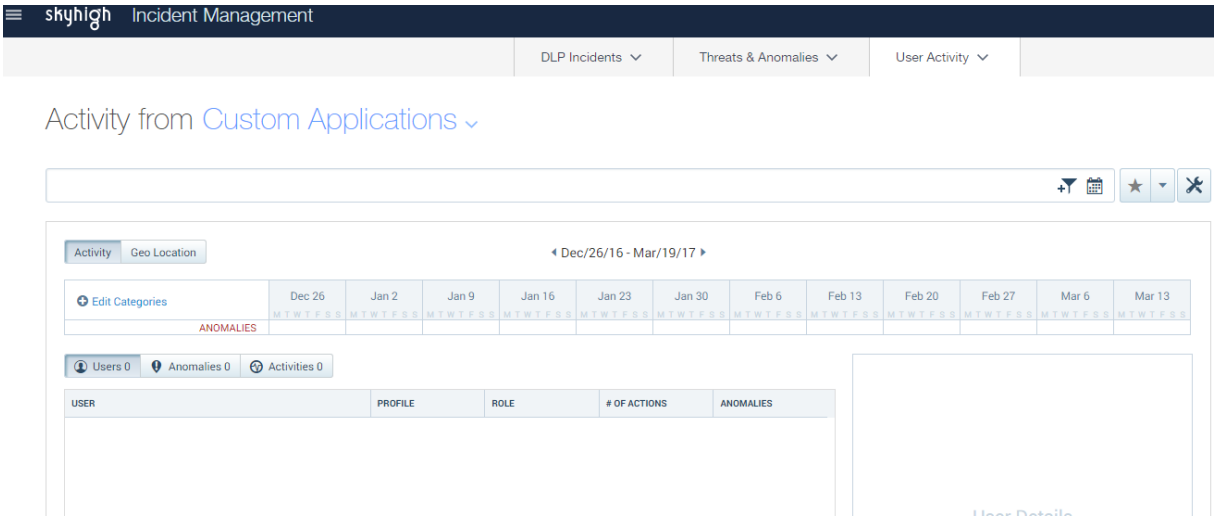


Screenshot 14: Anomaly settings

Appendix D: Product Screenshots of Data Security and Threat Protection Functionality - Source: Skyhigh

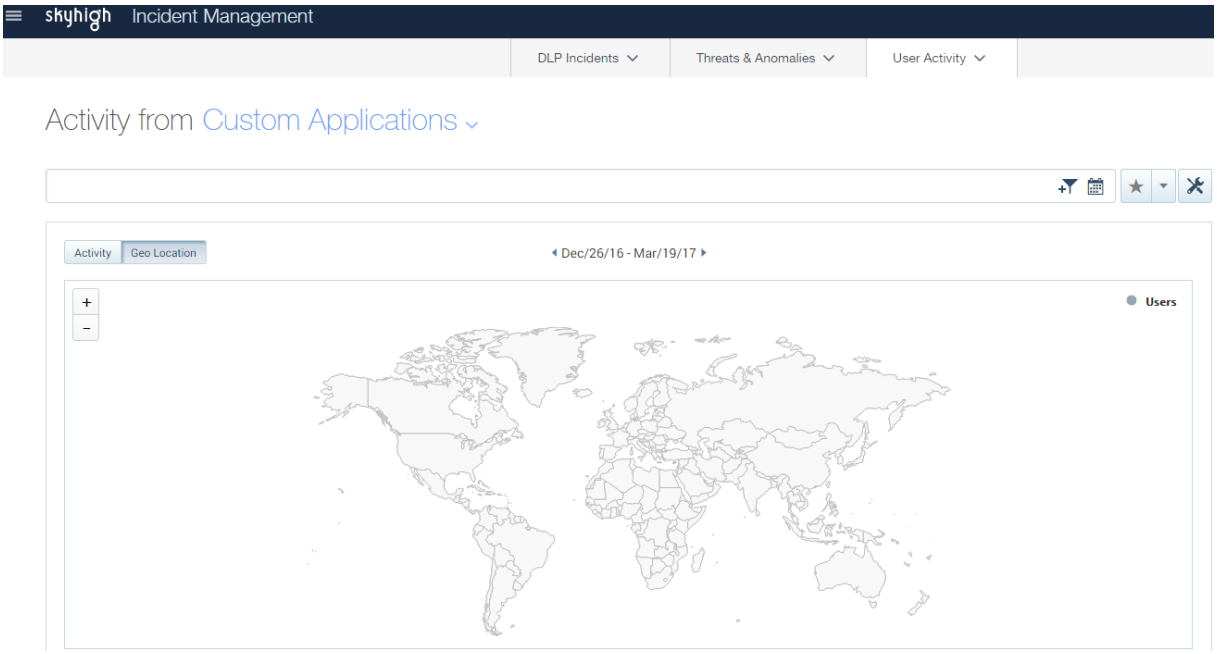


Screenshot 15: Overview of detected anomalies across unsanctioned cloud services

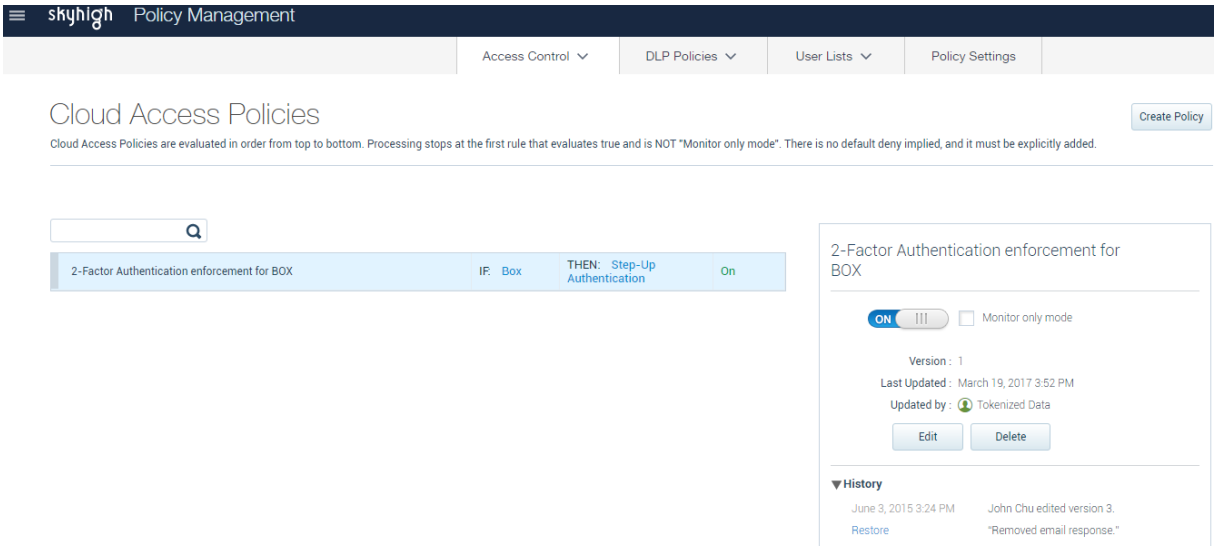


Screenshot 16: User activity on sanctioned cloud services over time (no data)

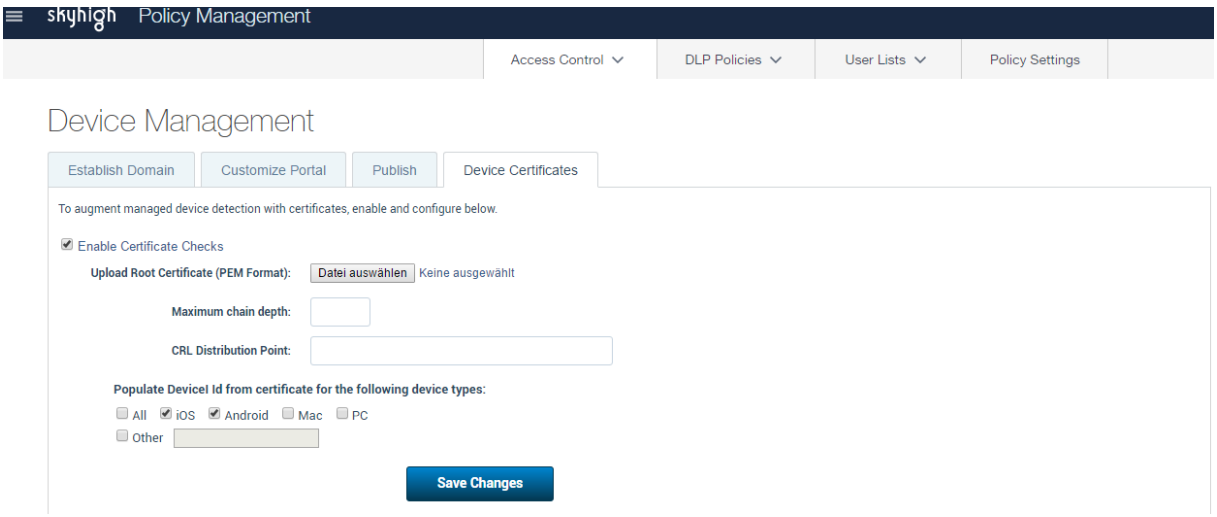
Appendix D: Product Screenshots of Data Security and Threat Protection Functionality - Source: Skyhigh



Screenshot 17: User activity on sanctioned cloud services with geographic location (no data)

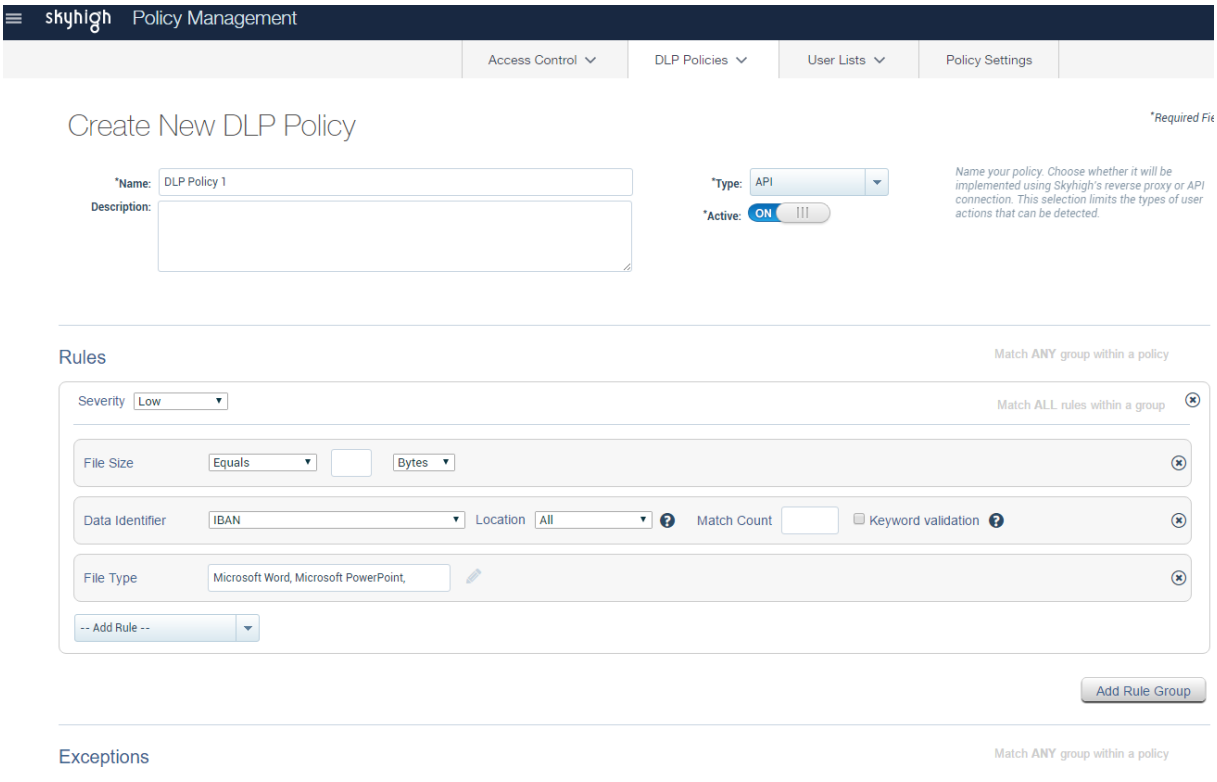


Screenshot 18: Exemplary custom access policy to step-up authentication for the sanctioned cloud service BOX

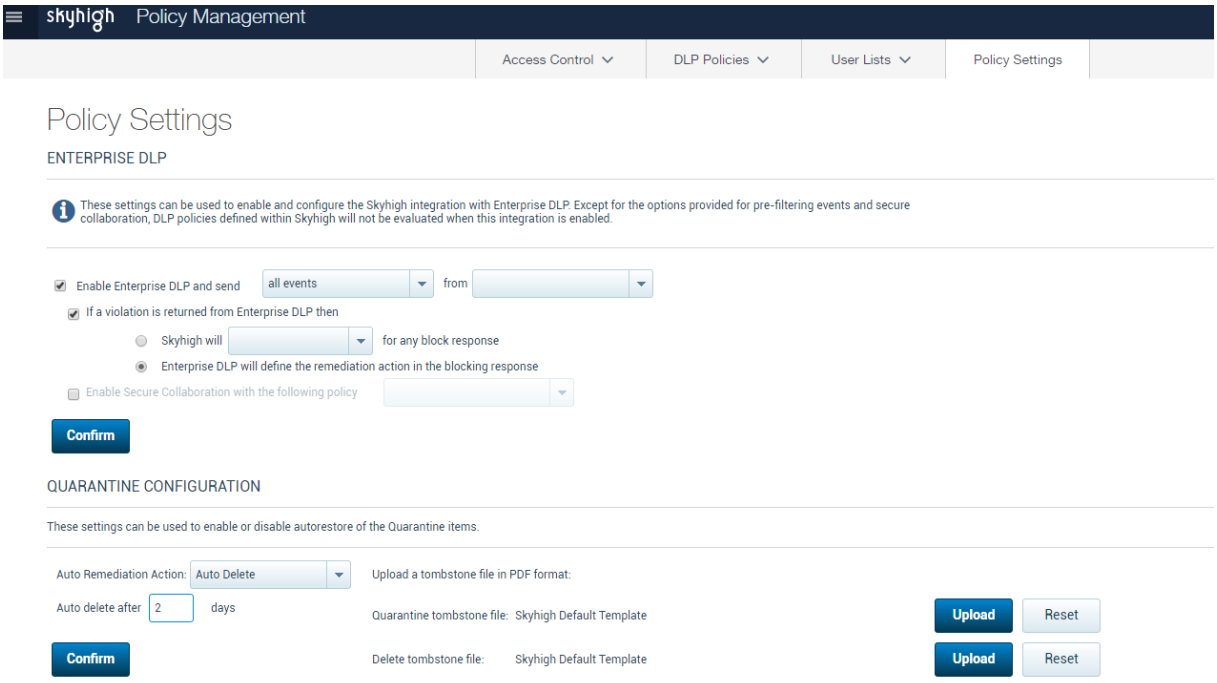


Screenshot 19: Device management configuration

Appendix D: Product Screenshots of Data Security and Threat Protection Functionality - Source: Skyhigh



Screenshot 20: Creation of custom DLP policy



Screenshot 21: Enterprise DLP policy settings