GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Implementing and Auditing CIS Controls (Security 566)"
at http://www.giac.org/registration/gccc

A Technical Approach at Securing SaaS using Cloud Access Security Brokers

GIAC (GCCC) Gold Certification

Author: Luciana Obregon, lucianaobregon@hotmail.com
Advisor: Dave Hoelzer
Accepted: August 14th 2017

Abstract

The adoption of cloud services allows organizations to become more agile in the way they conduct business, providing scalable, reliable, and highly available services or solutions for their employees and customers. Cloud adoption significantly reduces total cost of ownership (TCO) and minimizes hardware footprint in data centers. This paradigm shift has left security professionals securing abstract environments for which conventional security products are no longer effective. The goal of this paper is to analyze a set of cloud security controls and security deployment models for SaaS applications that are purely technical in nature while developing practical applications of such controls to solve real-world problems facing most organizations. The paper will also provide an overview of the threats targeting SaaS, present use cases for SaaS security controls, test cases to assess effectiveness, and reference architectures to visually represent the implementation of cloud security controls.

1. Introduction

As organizations strategize for ways to reduce cost, increase revenue, enhance the user experience, and achieve greater business agility, migrating services to the cloud seems like an appealing proposition that aligns to this strategy. The biggest selling point of cloud-based solutions is the significant reduction in total cost of ownership (TCO) for IT assets. Gartner defines TCO as a comprehensive assessment of IT or other costs across enterprise boundaries over time (Gartner, 2005). One way organizations can reduce TCO is by identifying IT services that deplete IT budgets and look for opportunities to reduce cost by migrating those services to the cloud.

In a traditional on-premises model, organizations pay for a perpetual license upfront for hardware that has a life expectancy of three to five years (Software TCO Calculator, n.d.). If the on-premises solution needs to scale up to support a larger user population or to accommodate new business requirements, the organization is forced to make additional investments to acquire more hardware and software. Conversely, almost all cloud-based solutions are offered using a pay-as-you-go model, ranging from monthly to annual or multi-annual terms, eliminating the need for organizations to make large capital expenditures (Amazon, n.d.).

Although cloud services offer many benefits to organizations, it's implementation not without risk. Most of the risks facing cloud consumers center around the privacy and security of their corporate data. CSPs follow a shared responsibility model where the CSP is responsible for the "security of the cloud" while the cloud consumer is responsible for the "security in the cloud" (Amazon, n.d.). In other words, for SaaS offerings, the CSP is responsible for securing the underlying application and the infrastructure (i.e., network, storage, database, etc.) while the consumer is responsible for securing the application's content and its usage (Skyhigh, n.d.). For example, to reduce the risk of unauthorized access to their tenants' data, Microsoft supports multi-factor authentication for global administrators and users of Office 365 services. But, it is the responsibility of the tenant to enable and enforce this feature and to ensure the effectiveness of the security control. Organizations that understand the shared responsibility model will be better equipped to protect corporate data by developing a cloud security strategy that provides

clear direction for designing adequate cloud security controls while ensuring that security professionals gain sufficient cloud security knowledge to execute the strategy.

The first step in implementing an effective cloud security strategy for SaaS is to understand the types of threats targeting cloud services. Secondly, organizations should gain full visibility into employee-led cloud usage and, lastly, organizations should design appropriate security controls, both technical and administrative, to safeguard their data in the cloud. This paper will introduce the technical controls that can be implemented in cloud-based applications, with a focus on their practical application in real-world scenarios. Securing PaaS and IaaS cloud models is not within the scope for this research.

2. Threat Targeting Cloud Environments

Cloud services are targeted by both internal and external threats. Skyhigh's 2016 Cloud Adoption Risk Report revealed that the average organization faces 23.2 cloud-related security incidents each month (Skyhigh, 2016). Unfortunately, if an organization does not have visibility into their cloud usage, most of those incidents will go unnoticed.

There are four (4) major categories of cloud-based threats (Skyhigh, 2016), described in more detail in the upcoming sections:

- Insider threats
- Compromised accounts
- Privileged user
- Data exfiltration by malware

2.1. Insider Threats

Insider threats are the most prevalent type of threat. An insider threat is an employee, contractor, or business partner that intentionally or unintentionally inflicts harm on the organization by stealing intellectual property, causing system outages, or deleting or modifying sensitive documents. The most dangerous type of insider threat are those individuals within an

organization that deliberately expose the organization to risk. For example, a disgruntled employee who downloads the organization's mergers and acquisitions strategy document from SharePoint Online and subsequently uploads it to his personal Dropbox account before going to work for a competitor. Insider threat also includes honest employees who accidentally expose company data to unauthorized external parties. For example, an administrative assistant who mistakenly shares a spreadsheet through OneDrive with an unknown recipient by mistyping the recipient's e-mail address could be considered an insider threat if the spreadsheet contains her CEO's Personal Identifiable Information (PII).

Data loss prevention and user behavior analytics can be used collectively to reduce the likelihood that an insider threat will cause significant damage to the organization.

2.2. Compromised Accounts

Compromised account threats consist of threat actors that obtain an employee's corporate credentials by either launching a credential harvesting phishing campaign against an organization, buying a password database in the Darknet, or simply guessing passwords frequently used by users. The threat actor could then use the stolen credentials to attempt to gain access to the cloud services that the employee is authorized to use.

Two methods by which users can be authenticated to cloud-based applications are:

- Local account
- Federated identity

Local accounts are created by the cloud administrator and are stored in a local database by the CSP. Each cloud application is a separate security realm with independent user databases. As a result, the attacker's window of opportunity to harvest credentials is significantly reduced as long as the cloud users do not use the same password across multiple cloud services. For example, if an attacker is after a company's sales forecast stored in Salesforce, he would first have to identify all the employees that have access to Salesforce and launch a phishing attack against those employees to harvest their credentials. If the stolen credentials do not provide access to Salesforce, he would have to go a step further and gain remote access to the employees'

machines, install a keylogger, and wait until one of the employees accesses Salesforce to capture the Salesforce username and password.

Federated identity enables employees to use their corporate credentials to authenticate to external resources (Microsoft, n.d.). In this case, the attacker's opportunity is much broader. Going back to the Salesforce example, if the attacker targets the right group of employees, a single phishing attack could be enough to harvest the credentials he is looking for.

Many enterprise SaaS applications support multi-factor authentication natively (i.e., Office 365) or can be integrated with an identity and access management solution that supports multi-factor authentication to thwart this type of attack.

2.3. Privileged User

Privileged user threats include cloud administrators that knowingly or unknowingly weaken the security posture of cloud applications by either accessing other users' accounts, changing cloud security settings in an effort to increase usability or enhance user experience (Skyhigh, n.d.), or create backdoors for stealth and persistent access to the application. For example, an Office 365 administrator could enable the feature that allows Skype users to communicate with other Skype users in external domains in an attempt to communicate with friends and family during business hours. This may seem benign, but presents an avenue through which malware can be infiltrated into the company's network.

Heightened monitoring to identify misuse of privileged accounts can help thwart this type of threat.

2.4. Data Exfiltration by Malware

Some malware variants leverage unmonitored public clouds to exfiltrate large volumes of data stolen from an organization's on-premises systems. For example, after an attacker has compromised an organization's Enterprise Resource Planning (ERP) system, the attacker can begin the exfiltration phase by uploading the stolen data to a Google Drive account of his choice. If the organization does not have a policy in place to block unauthorized personal cloud storage sites or to monitor cloud usage, the incident will be successful and go unnoticed.

Figure 1 shows the percentage of organizations experiencing the cloud-based threats defined in the previous section. Insider threats are the most prevalent, with 93.5% of organizations experiencing this kind of attack each month.

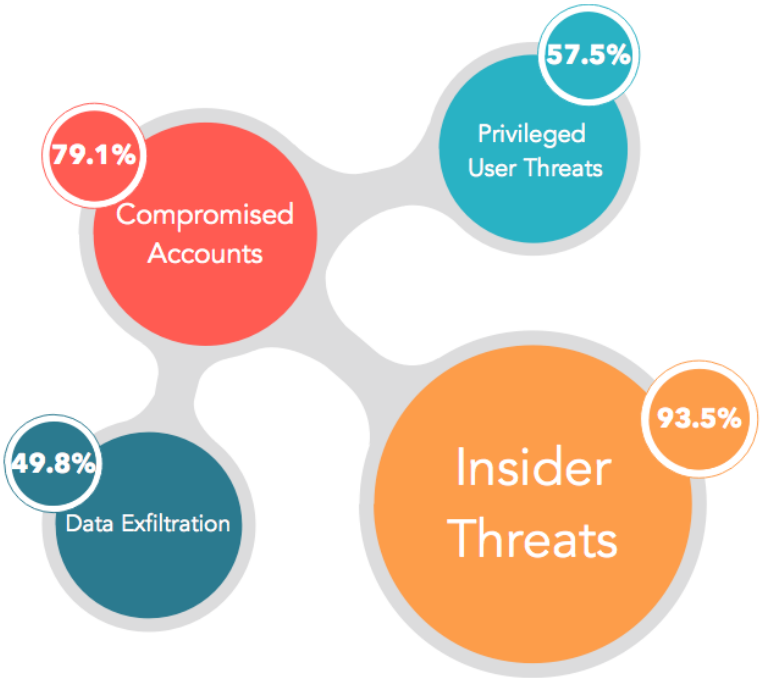


Figure 1 - Percentage of organization experiencing at least one threat each month - Cloud Adoption and Risk Report Q4 2016 - Skyhigh

3. Shadow IT vs. Sanctioned Cloud Services

The approach towards securing sanctioned cloud services is significantly different from that of shadow IT. It is, therefore, appropriate to define the terminology, highlight the main differences between shadow IT and sanctioned cloud services, and understand the limitations for security.

"Shadow IT" (or unsanctioned) is a broad term that refers to IT projects that are managed outside of and without the knowledge of the IT department (Skyhigh, n.d.). As it relates to cloud computing, shadow IT are cloud services that are introduced by employees but have not been approved by an organization's IT department (Gartner, 2016). Employees introduce cloud

services for several different reasons, such as to enable them to be more efficient at their job, or simply because they are not aware that the company uses a similar product that has already been approved by the IT department. For example, an employee may use Box to store documents for easy access after work hours without knowing that the company's approved standard is OneDrive for Business.

Shadow IT cloud services introduce significant risk to the organization as they can be misused to exfiltrate high-value corporate data, or to introduce malware that can infect the organization's digital assets. It is, therefore, critical that organizations gain granular visibility into all employee-led cloud usage to identify and block high-risk services.

Contrary to Shadow IT, sanctioned cloud services are those that have been approved and are managed by an organization's IT department. For example, an organization may use ServiceNow as their cloud-based enterprise ticketing system, or Office 365 as their enterprise collaboration and productivity platform. Most opportunities for security are found in sanctioned cloud applications.

4. Technical Security Controls for Cloud Environments

There are several security controls—beyond those offered by the CSP—that organizations can implement to protect their resources in the cloud. Security professionals are better equipped to secure sanctioned cloud services because these are typically managed by the organization. Conversely, protecting company data that lives in unsanctioned cloud services becomes a challenging proposition; the organization may not be fully aware of the various cloud services being used by their employees, much less can security professionals affect the security posture of unsanctioned cloud services given the lack of administrative control. The following sections describe the security controls that can be applied to sanctioned and unsanctioned cloud services using a **Cloud Access Security Broker (CASB).**

4.1. Cloud Security Access Broker

Gartner defines a Cloud Access Security Broker as an on-premises or cloud-based security policy enforcement point placed between the cloud service consumer and the cloud service provider to enforce security policies as the cloud services are being accessed (Gartner, 2016). This paper focuses on cloud-based CASB solutions.

Generally speaking, there are four (4) main use cases for any CASB solution, each of which with its own set of security capabilities (Netskope, n.d.):

- **Continuous visibility** into employee-led cloud usage to understand data leakage patterns, identify highest risk cloud services, and highlight gaps in cloud policy enforcement (i.e., percentage of a cloud service blocked vs. percentage allowed).
- **Compliance** with regulatory and government mandates and internal corporate policies by enforcing data leakage prevention and secure collaboration policies with external parties.
- **Data security** to ensure the protection of critical data against inappropriate use by identifying gaps in security settings for sanctioned cloud services, enforcing context-based and role-based access control, encryption, and tokenization.
- **Threat Protection** to reduce the risk of cloud malware outbreaks, unauthorized access, privileged user threats, and insider threats by monitoring all activities in the cloud and by performing user behavior analytics to reduce the rate of false positives.

A CASB offers four distinct deployment models to meet almost every security requirement, each providing a different set of features (Skyhigh, n.d.):

- Log collection
- Forward proxy
- Reverse proxy
- API

The main purpose of the **log collection** model is to provide enhanced visibility into unsanctioned cloud usage. The deployment works by collecting web usage data from web policy enforcement points, such as a web security gateway, web proxy server, or firewall, to provide continuous visibility into cloud usage. The collection task is typically done by an on-premises connector server that, using a pull or push method, captures and normalizes web access logs and forwards them to the CASB at regular intervals. The connector server can also act as a bridge between the CASB and a Security Information and Event Management (SIEM) system by receiving security alerts from the CASB (i.e., anomaly detection) and forwarding them to the SIEM for correlation and analysis.

Log collection is the easiest to setup as it only requires a connector server running the log collection service and a web security gateway configured to forward logs to the connector server. Log collection is also least intrusive deployment model because it passively collects and analysts data, eliminating the impact on network performance or user experience.

Figure 2 provides a visual representation of this deployment model. On and off-premise cloud users (step 1 and 2) access unsanctioned cloud services through the organization's web security gateway. To increase the effectiveness of this deployment model, organizations must ensure that web security policies are equally enforced for both on and off-premise users. This means that, before being allowed access to the Internet from managed endpoints, off-premise users should be required to connect to the company's network through VPN. Alternatively, organizations can choose to install an endpoint agent on company-owned devices to enforce web security policies when employees are not connected to the company's network.

The web security gateway (or firewall if performing this function) forwards web access logs to the connector server (step 3) which normalizes the data before forwarding it to the CASB (step 4). The connector server also receives security alerts from the CASB (step 4) which are subsequently forwarded to a SIEM (step 5) for consumption by security analysts (step 6). The security analysts also access the CASB management interface (step 6) to learn about unsanctioned cloud usage, identify highest risk cloud services, and take appropriate actions. This process can be seen below.

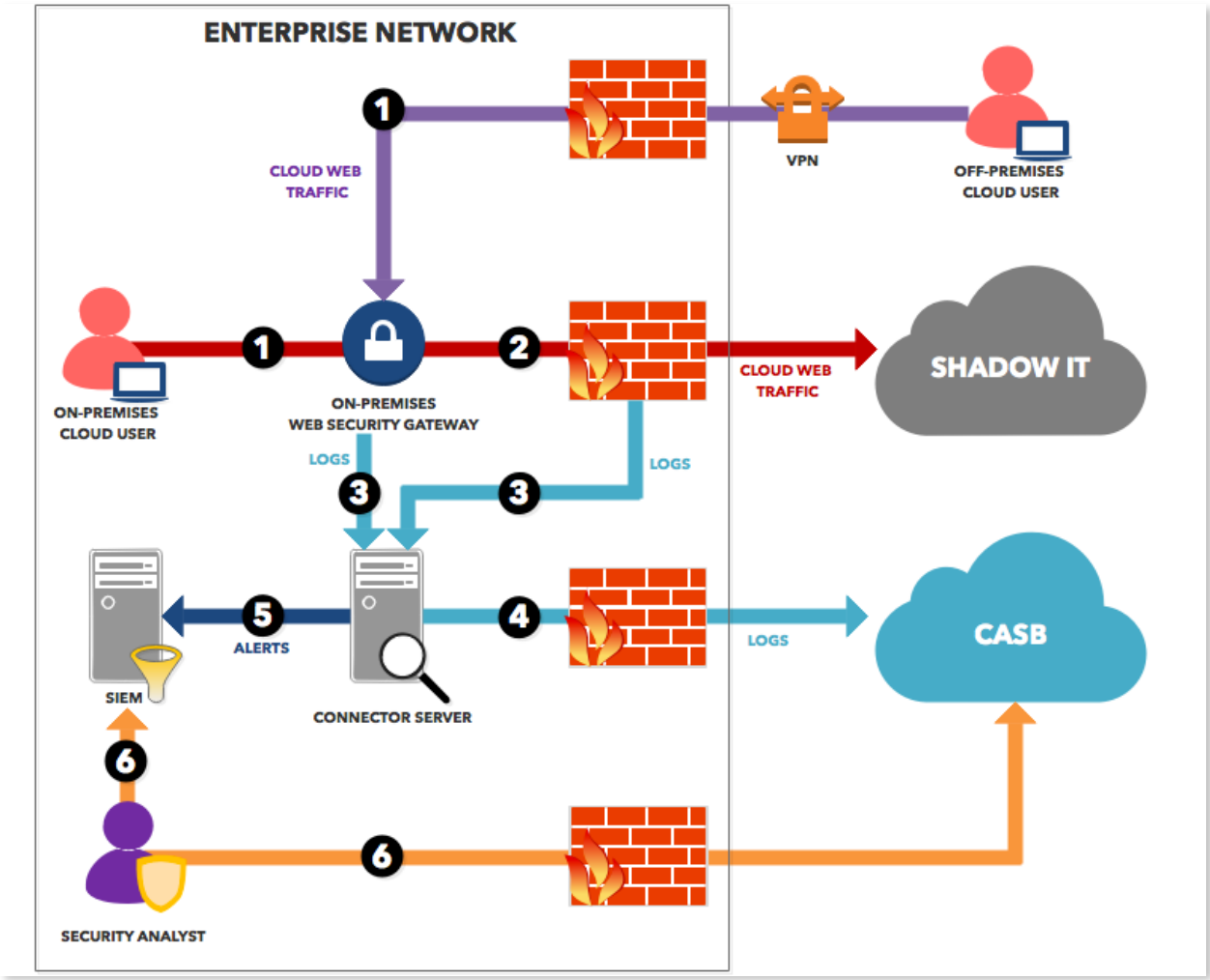


Figure 2 - CASB Log Collection Model (Skyhigh, n.d.)

The main purpose of the **forward proxy** deployment model is to provide enhanced visibility into cloud usage as well as to enforce cloud access policies for sanctioned cloud services. The forward proxy deployment model routes all end-user traffic through the CASB for policy enforcement. This model is more intrusive than log collection and could potentially disrupt end-user traffic as a result of misconfigured policies. To implement a forward proxy, organizations can configure their web security gateways or web proxies to route all outbound web traffic to the CASB (also known as proxy-chaining). Alternatively, end-user devices can be configured with an endpoint agent that routes all web traffic to the CASB.

Figure 3 provides a visual representation of the forward proxy deployment model. On-network users access the Internet through the organization's web security gateway (step 1).

Depending on the policy enforcement method of choice, off-premise users access the Internet through a VPN connection to the organization's internal network (step 1) or through an endpoint agent installed on company-owned devices (step 3). In either case, all outbound Internet access is routed to the CASB (step 3) where cloud access policies are enforced before forwarding the traffic to the desired destination (step 4).

Similarly to the previous model, the connector server can receive security alerts from the CASB (step 5) which are subsequently forwarded to a SIEM (step 6) for consumption by the security analysts (step 7).

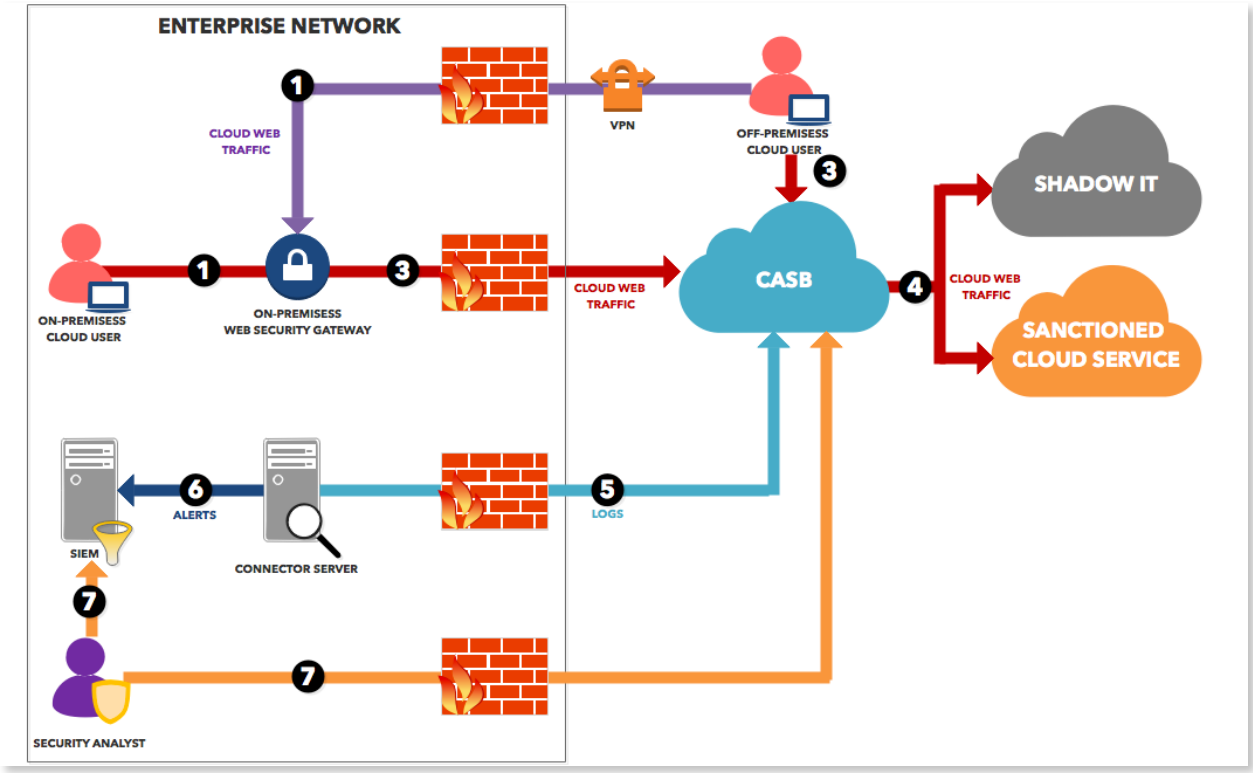


Figure 3 - CASB Forward Proxy Model (Skyhigh, n.d.)

The main purpose of the **reverse proxy** mode is to enforce cloud access policies for specific sanctioned cloud services. The reverse proxy deployment model routes all traffic to and from a particular cloud service provider through the CASB. This model requires an Identity

and Access Management (IAM) platform to forward authenticated user traffic to the CASB, which, in turn, seamlessly forwards the traffic to the cloud service provider.

In Figure 4, users (on and off-premise alike) authenticate to the organization's IAM platform before being granted access to the sanctioned cloud service (step 1). Once the users are successfully authenticated (steps 2 and 3), application traffic is routed through the CASB (step 4) where cloud policies are enforced. Traffic that meets the pre-configured cloud security policies is then forwarded to the cloud service provider (step 5).

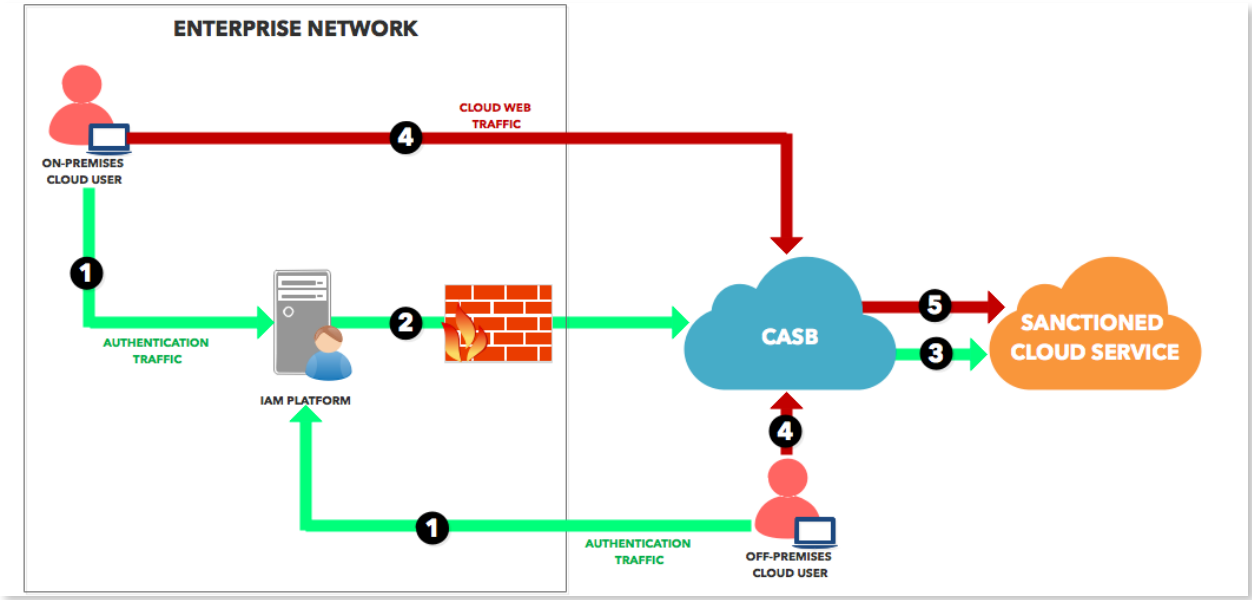


Figure 4 - CASB Reverse Proxy Mode (Skyhigh, n.d.)

The **API** deployment model provides granular visibility into and cloud policy enforcement for specific sanctioned cloud service. The API model requires an API connection established between the CASB and the cloud service provider. The capabilities offered by the API model vary for each cloud service provider and not all cloud service providers support API integration.

In Figure 5, users access sanctioned cloud services (step 1 and 2) through the organization's web security gateway. Any activity performed by the users in the specific cloud

application are captured by the CASB through the API connection (step 3). Additionally, pre-defined cloud security policies are enforced by the CASB through the API connection.

Similarly to log collection, this model is very easy to setup, however, misconfigured cloud security policies could potentially disrupt user activities in the cloud application. For example, a loosely configured data loss prevention policy that only looks for the keyword "confidential" in the body of a message could prevent a user from sharing a document through Salesforce Chatter, even if the document does not contain any confidential information.

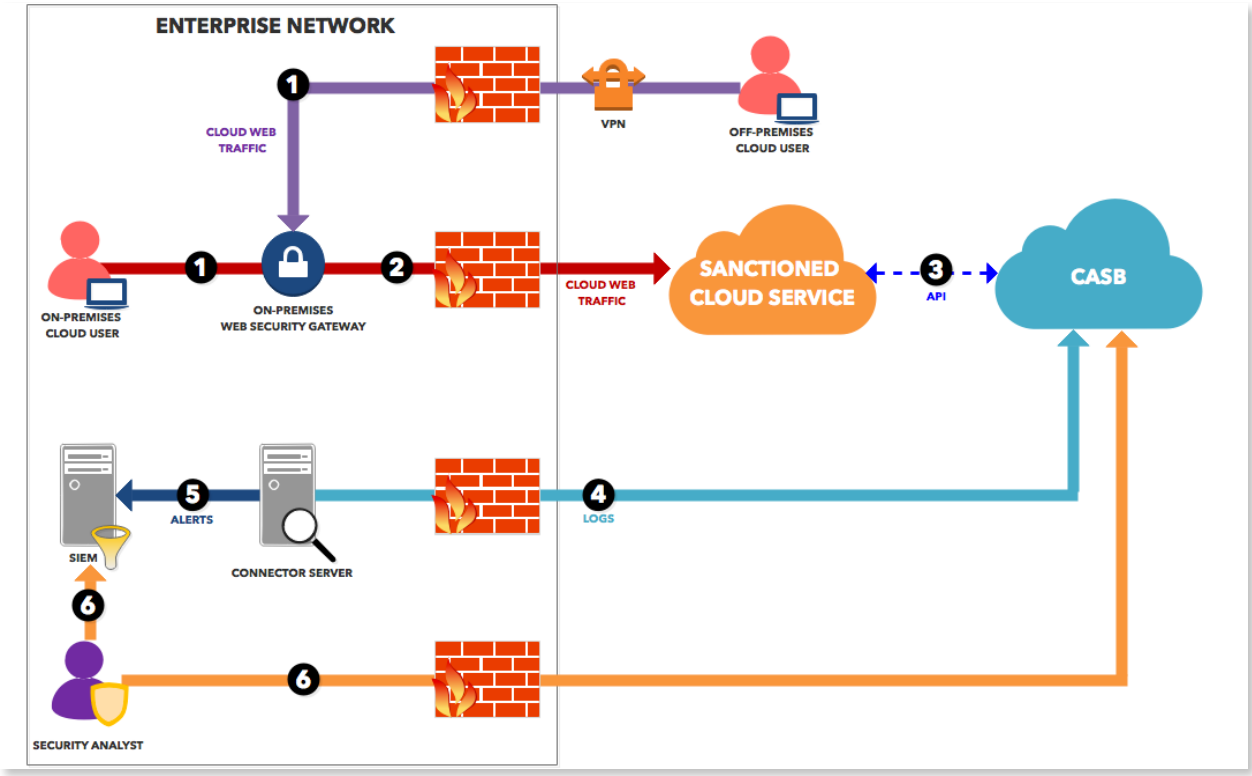


Figure 5 - CASB API Model (Skyhigh, n.d.)

4.2. Securing Unsanctioned Cloud Services

Before an organization can defend against threats that stem from the usage of unsanctioned cloud services, it must first gain granular visibility into user activity in the cloud. For effective cloud threat protection, a lifecycle approach—depicted in Figure 6—can be adopted which includes the following phases:

1. Gain visibility
2. Identify unsanctioned cloud services for which an approved equivalent is available
3. Block unauthorized and highest risk cloud services
4. Monitor for gaps, anomalies, and violations

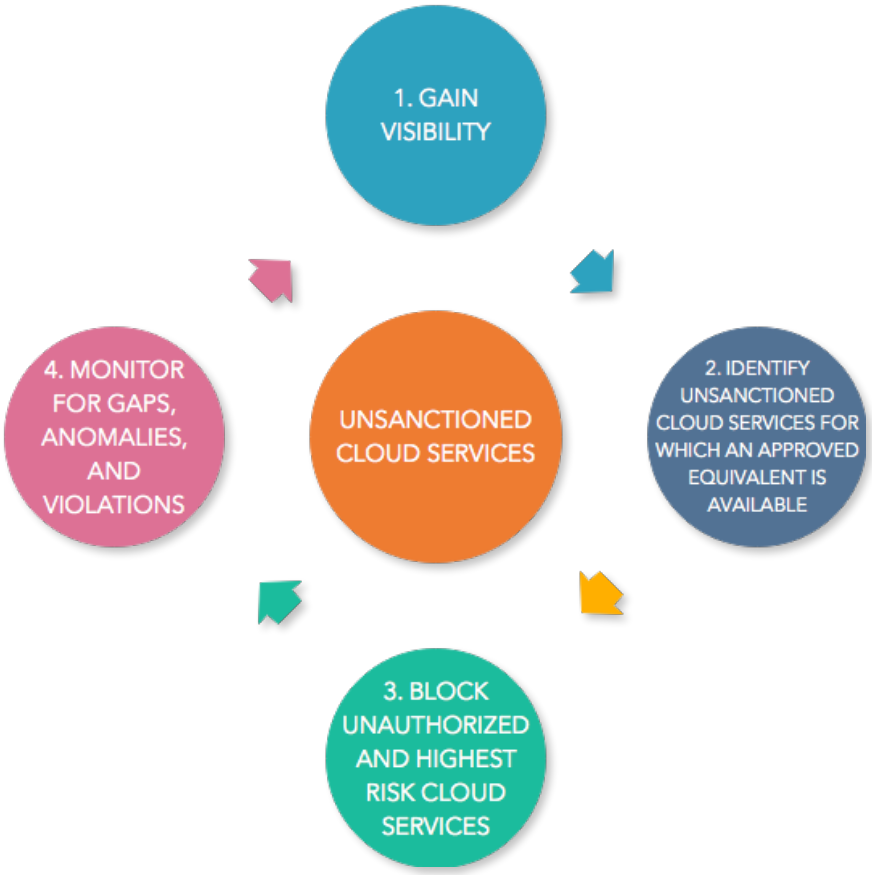


Figure 6 - Lifecycle Approach to Securing Unsanctioned Cloud Services

A CASB and a web security gateway can be used collectively to achieve continuous cloud visibility and policy enforcement (Skyhigh, n.d.). A web security gateway offers full inline content inspection for every Internet-bound web request and enforces web security policies as

defined by the organization. As such, it logs every web request initiated by internal employees, as well as by remote employees as long as the web requests are originated from a managed endpoints. The log data generated by the web security gateway is then fed into the CASB to provide granular visibility into cloud activities.

The web security gateway can be on-premises or cloud-based. In either scenario, a log collection service transmits the log data from the web security gateway to the CASB. The security analysts analyze and monitor cloud usage and its associated risks from the CASB's administrative portal and make continuous adjustments to the web security policies according to organizational acceptable use policies, security standards, and risk appetite.

Figures 7 and 8 provide a visual representation of the IT components required to reduce an organization's attack surface introduces by unsanctioned cloud services.

In Figure 7, on- and off-premises users access the shadow IT cloud service of their choice through an on-premises web security gateway (step 1). The web security gateway inspects the traffic and applies web security policies according to the organization's corporate policies and standards (step 2). Web access logs generated by the web security gateway are forwarded to a connector server (step 3), which normalizes the data before forwarding it to the CASB (step 4). Security analysts access the CASB to monitor for web filtering gaps, anomalies, and violations (step 5) and make adjustments to the web security policies to reduce the attack surface (step 6).

Figure 8 differs from Figure 7 in that the web security gateway is cloud-based, however, the same steps and concepts described in the previous paragraph apply.

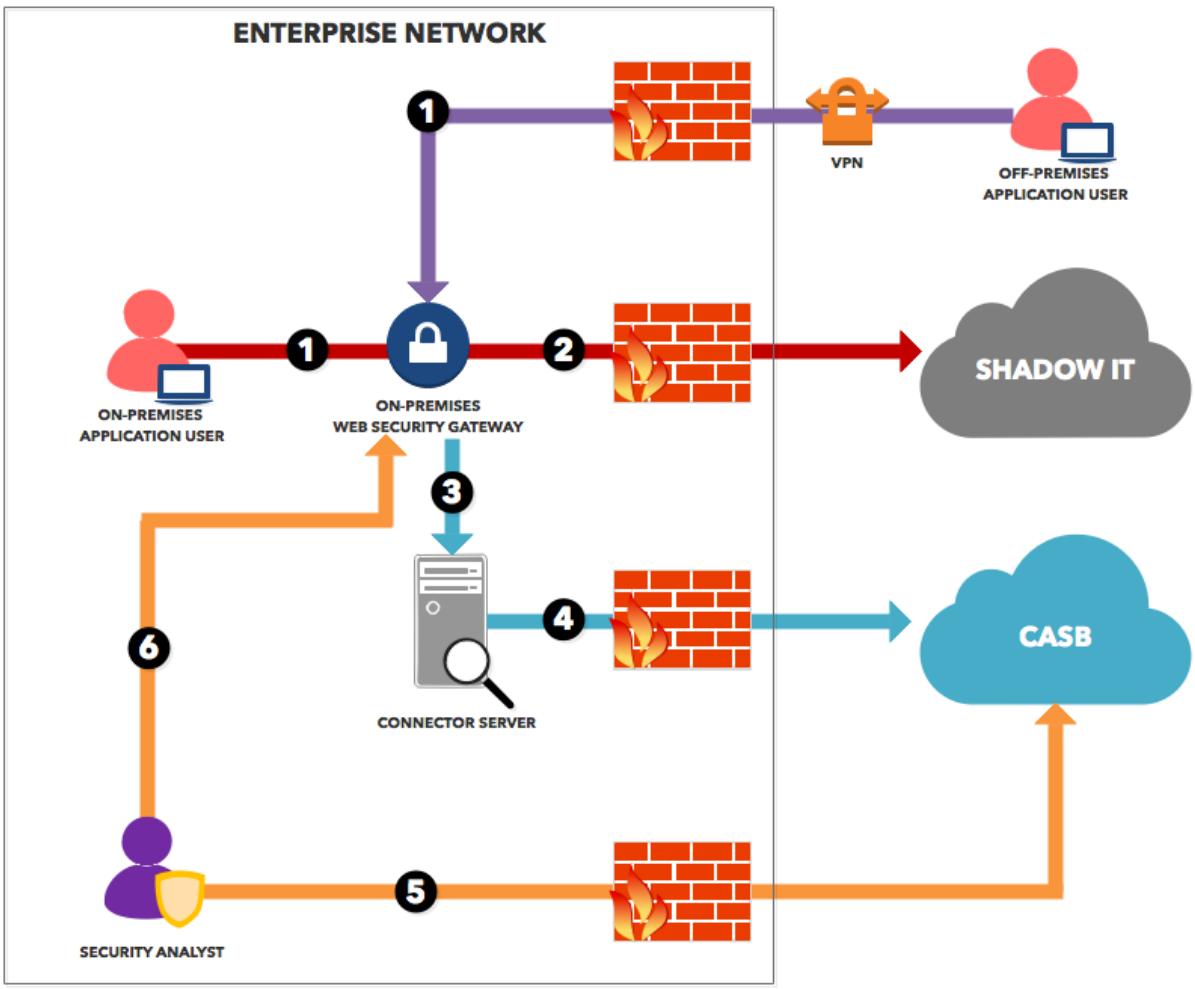


Figure 7 - Securing Unsanctioned Cloud Services using an On-premises Web Security Gateway

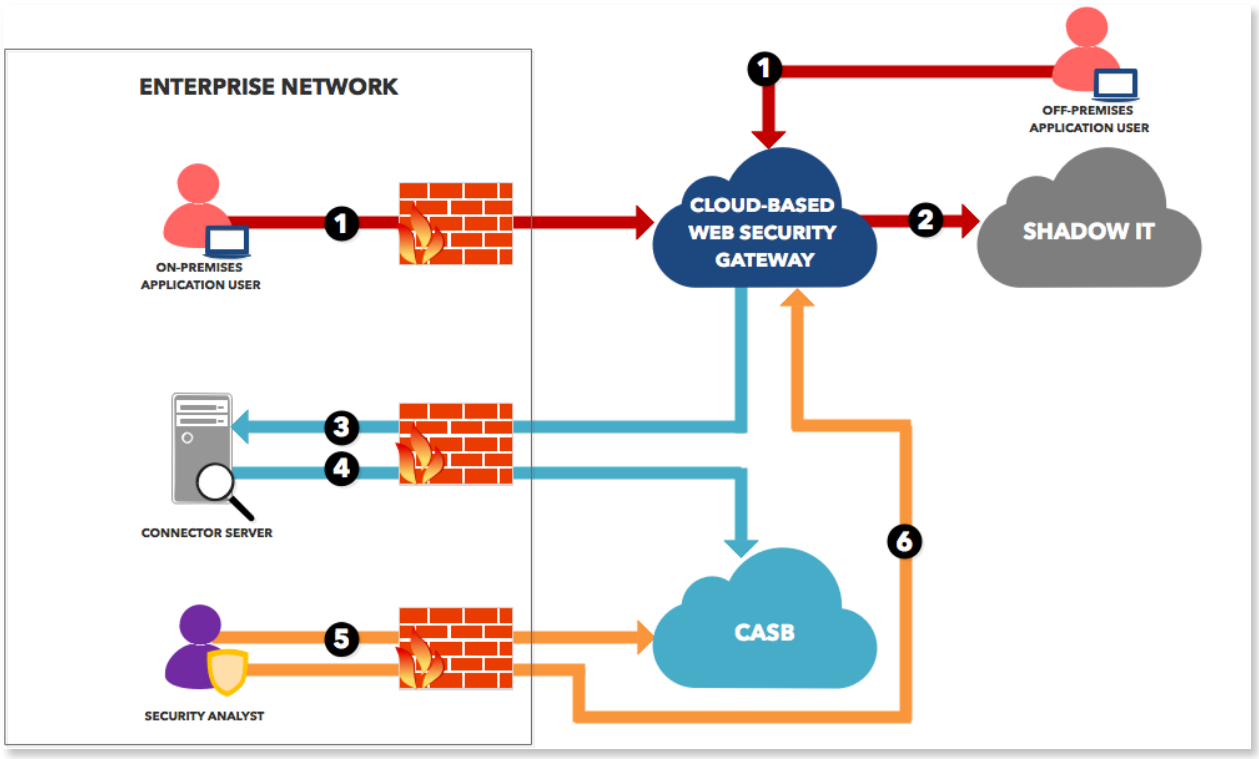


Figure 8 - Securing Unsanctioned Cloud Services using a Cloud-based Web Security Gateway

The deployment models presented in Figures 7 and 8 provide equal levels of protections, however, a 100% cloud solution may be more appropriate for organizations that are looking to reduce hardware footprint and enhance user experience (i.e., not requiring users to connect to VPN to access the Internet).

4.3. Securing Sanctioned Cloud Services

This section describes practical security controls that can be effectively implemented by cloud service consumers to their sanctioned cloud service. Chief among these are:

- Access control
- Encryption and key management
- Data loss prevention
- Anomaly detection and control

4.3.1. Access Control

Access control policies determine the allowed activities of legitimate users by mediating every attempt by the user to access a computing resource (NIST, 2006). Cloud access policies enable granular control over access to cloud applications. A CASB and an identity and access management (IAM) platform can be used in conjunction to control access to cloud-based resources based on pre-established conditions. The following access control capabilities are covered in this section:

- Single sign-on (SSO)
- Contextual cloud access control
- Unmanaged device control

To enforce access control policies, the CASB must be deployed in reverse or forward proxy mode.

Single Sign-On

SSO is an authentication process that enables users to access multiple applications using a single set of user credentials (OWASP, n.d.). The most significant security benefit derived from SSO is the central administration and management of user identities and password policies. SSO also enhances the user experience by eliminating the need to remember multiple passwords to access cloud applications.

In Figure 9, a user accesses a cloud service (step 1) which redirects unauthenticated requests to the organization's IAM platform (step 2). Upon successful authentication (step 3), the IAM platform communicates with the CSP to assert that the user is who he claims to be and that he is authorized to access the cloud application (step 4). Subsequent authenticated requests are intercepted by the CASB, which enforces security policies on the traffic based on pre-defined conditions (steps 5 and 6).

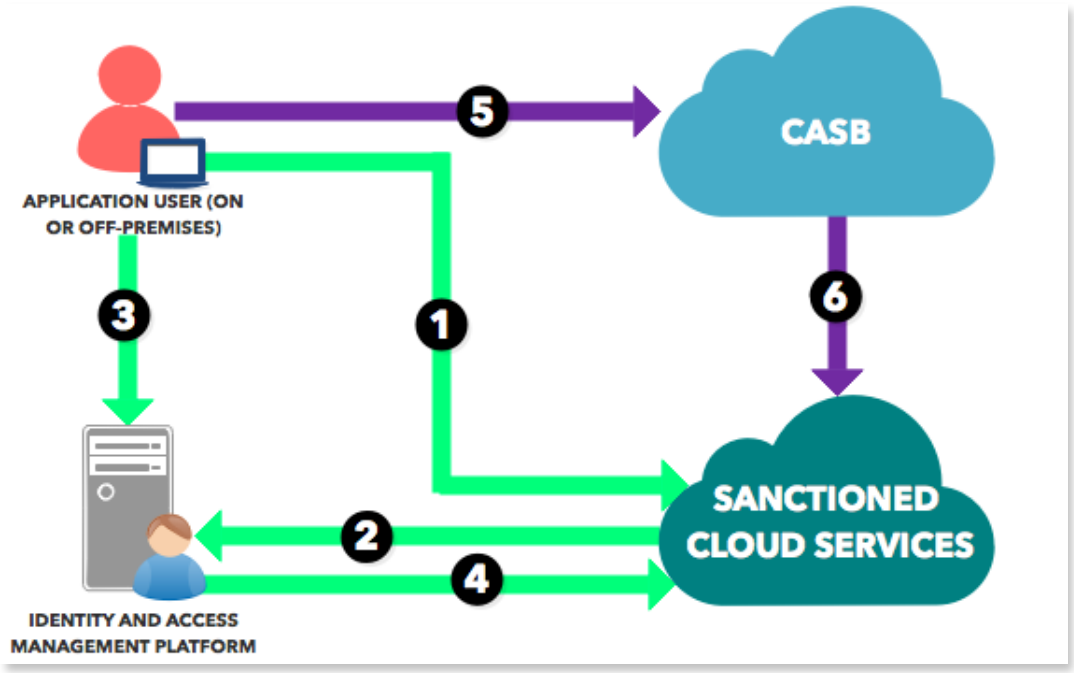


Figure 9 - SSO to access cloud services

Contextual Cloud Access Control

Contextual access control introduces additional conditions to the authentication and authorization process. With context-based access control, users are no longer authenticated only based on "something they have" and/or "something they know", such as a password and one-time token. Instead, additional conditions, such as the user's originating IP address, device type, or geographical location, are added to the authentication process to allow or deny access requests (Skyhigh, n.d.), allowing organizations to control access to their data with a higher degree of specificity.

A CASB can be used as an enforcement point for context-based access control for cloud-based resources. A CASB can also enforce granular authorization policies for user activities in cloud applications mapped to different types of user request. For example, a contextual access control policy can allow users to access ServiceNow from the IP address range registered to the cloud consumer's organization. This would require users to access the cloud service from within the organization's network at all times. Similarly, if an organization is concerned about the risk of storing sensitive corporate data in unmanaged devices, a CASB can

enforce an access policy to block users' requests to download data from Salesforce using personally-owned devices.

Any action that modifies user behavior requires the CASB to be placed inline between the cloud user and the cloud service. Therefore, context-based access control requires the CASB to be implemented in reverse or forward proxy mode.

In Figure 10, for example, the cloud user has already been authenticated by the organization's IAM platform. The user's attempts to access the desired cloud-based application are intercepted by the CASB solution (step 1) which applies the pre-configured context-based access control policies (step 2) to deny or allow traffic to the cloud-based application (step 3).

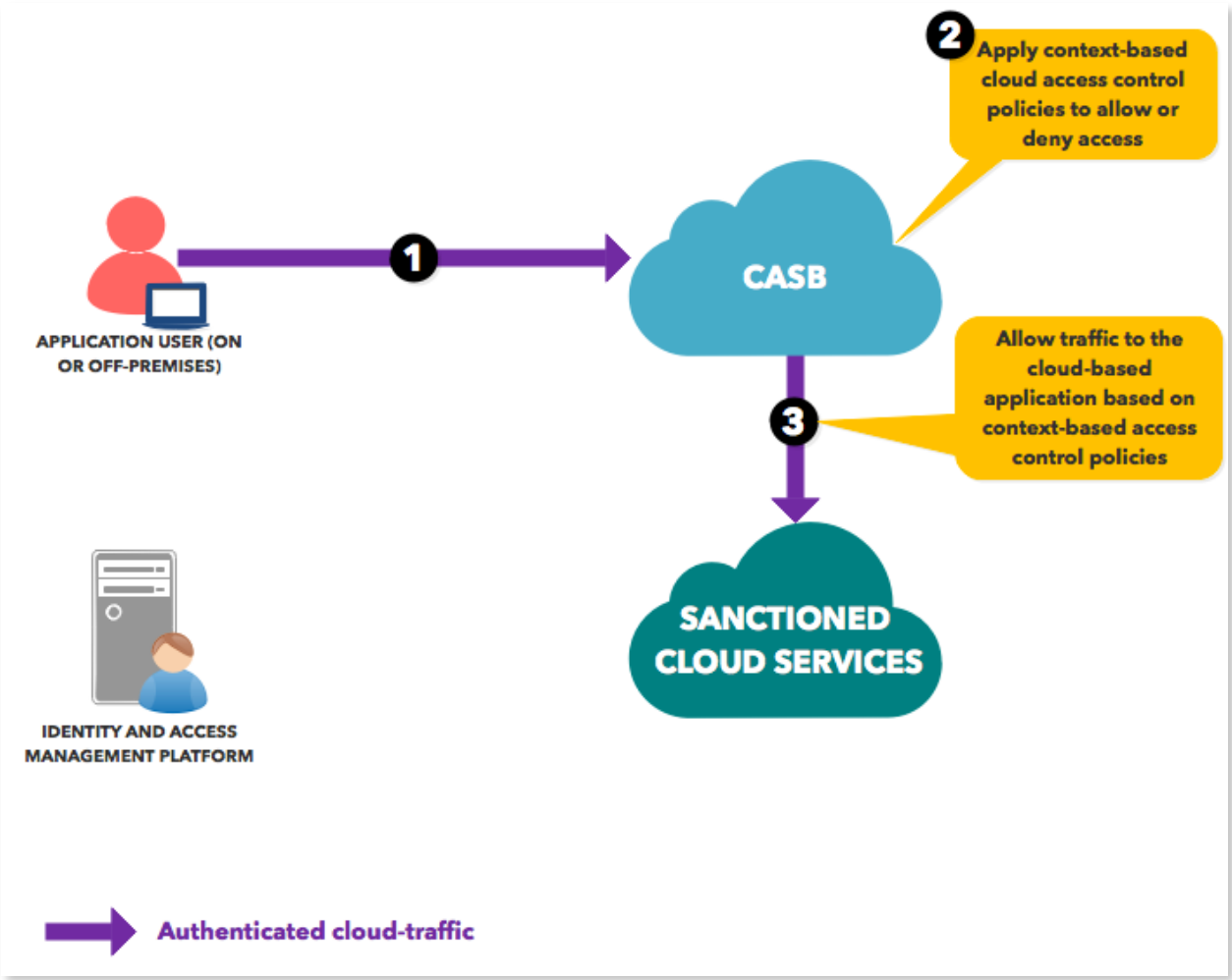


Figure 10 - Context-based Access Control using a CASB

Unmanaged Device Control

The use of unmanaged devices to access cloud services introduces several benefits to both the organization and its employees. First, it significantly reduces costs associated with managing corporate-owned endpoints. By allowing employees to use their personal devices for work purposes, organizations no longer have to provision a corporate-owned device for each of their employees. Secondly, it enhances user experience and productivity as employees can use the device of their choice. However, the risk of data leakage through this channel is a serious one, especially if the organization does not have adequate technical controls in place to prevent sensitive data from being stored in unmanaged devices.

A CASB can integrate with an organization's Enterprise Mobility Management (EMM) solution to enforce security policies based on device management status (managed vs. unmanaged), by checking if the connecting device is whitelisted or if it has a corporate certificate installed (Skyhigh, n.d.).

In Figure 11, a mobile device is first registered with the organizations EMM platform (step 1). Before the user is allowed to access the cloud application, the CASB intercepts the traffic and verifies the state of the connecting device (steps 2 and 3). The CASB then takes the appropriate response action (steps 4 and 5) as configured in the context-based access control policy (i.e., allow full access for managed devices, allow preview access only for unmanaged ones).

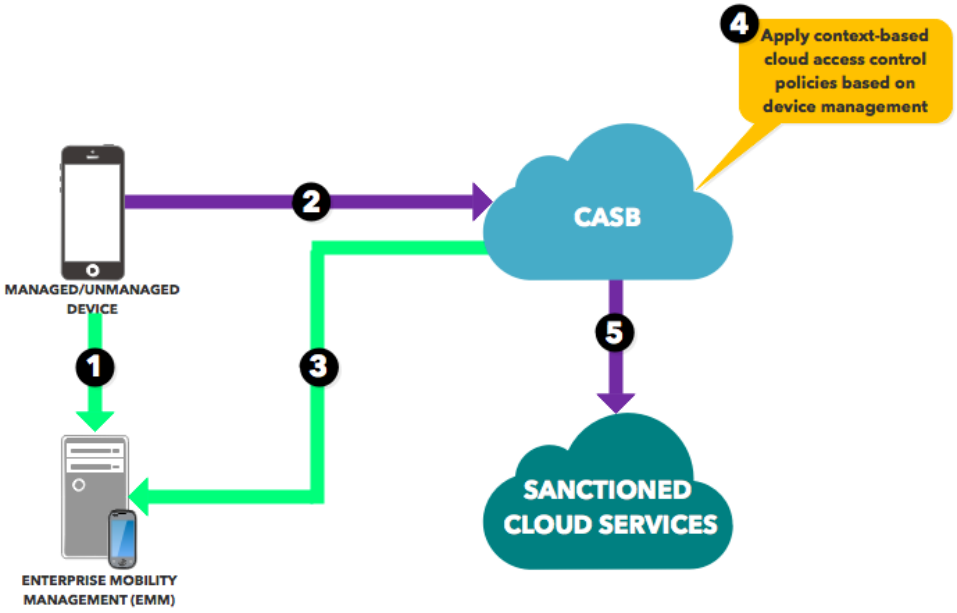


Figure 11 - Unmanaged Device Control using a CASB

4.3.2. Encryption and Key Management

The robustness and effectiveness of an encryption solution depends not only on the encryption algorithm in use, but also on the adequate protection of the encryption keys. Encrypting data in the cloud while maintaining full control of the encryption keys is now possible using a CASB solution that supports integration with an organization's key management platform. In such a scenario, the CASB solution transparently encrypts and decrypts data uploaded to a cloud service—based on pre-defined encryption policies—while the key management platform stores and manages the lifecycle (creation, rotation, revocation, destruction) of the encryption keys (Gemalto, 2015). For instance, ServiceNow is a cloud-based enterprise ticketing system. As such, organizations upload volumes of sensitive IT-related information that, if improperly disclosed, could allow an adversary to gain detailed knowledge of the organization's CMDB or the type of operational and/or security incidents facing the organization, to name a few. An organization can define an encryption policy in their CASB to encrypt specific fields in a ServiceNow ticket, such as the Configuration Item (CI) field which contains information about a physical, logical, or conceptual entity (ServiceNow, 2016).

In Figure 12, a user's attempt to upload sensitive data to a cloud service is intercepted by the CASB (step 1) which, based on pre-configured policies, encrypts specific fields (step 2) using the cloud consumer's encryption keys (step 3) stored in an on-premises or cloud-based key management platform. The CASB then uploads encrypted data to the cloud service (step 4) as seen below.

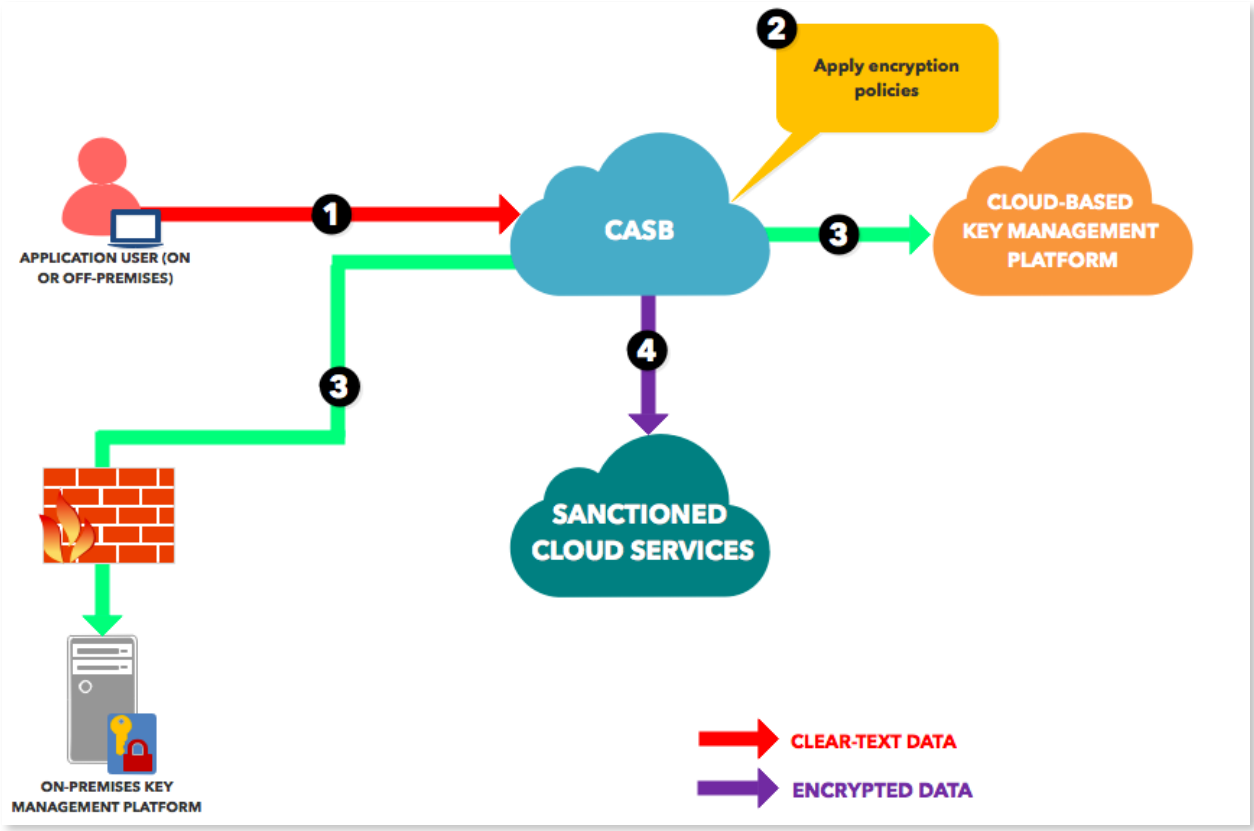


Figure 12 - Encrypting Data in the Cloud

4.3.3. Data Loss Prevention

Organizations use all sorts of data on a daily basis to make business decisions, however not all business data is equally important. There are specific data sets that an organization considers business-critical that, if improperly disclosed, could negatively impact the organization's bottom line. Organizations must, therefore, implement technical controls, like the

ones mentioned in the previous sections, that provide visibility into the usage of business-critical data and ensure that it never leaves their network perimeter.

In the cloud realm, most organizations are not so much concerned about critical data being stored in sanctioned cloud services. After all, organizations have procured these services to achieve greater business agility and, for some, this may mean storing sensitive documents in cloud applications for easy retrieval. The concern is more centered around how the cloud data is shared with external parties (Skyhigh, 2016). Most collaboration tools (e.g., Office 365) allow for easy sharing of documents with external users. This represents a data leakage channel that, if not controlled, could present an opportunity for threat actors to exfiltrate a company's most valued data.

The first step in developing an effective cloud DLP strategy is to identify the corporate data that is intended for the cloud and classify it according to corporate data classification policies and regulatory mandates. Once this is completed, a CASB can be used to enforce corporate DLP policies by inspecting every bit of every packet that traverses it.

A CASB can detect sensitive data as it is uploaded to the cloud as well as after it has been stored in the cloud. The former requires the CASB to be deployed in either reverse or forward proxy mode while in the latter the CASB must have an API connection to the sanctioned CSP (Skyhigh, n.d.). For example, a CASB in forward or reverse proxy mode can detect when password files are being attached to ServiceNow tickets. Similarly, a CASB that has an API connection to Office 365 can detect when an employee shares the mergers and acquisitions plan for the upcoming year with an external user through OneDrive for Business. An organization can choose to implement all or a group of the CASB deployment models previously discussed in order to cover all possible attack surfaces.

In Figure 13, security analysts use the CASB to define, deploy and enforce DLP controls based on pre-established corporate DLP policies (steps 1 and 2). A user's attempt to upload sensitive data to a cloud service is intercepted by the CASB (step 3), which inspects every bit of every packet for matching keywords, patterns, or regular expressions (step 4), and then applies the preconfigured response actions to either allow or block the request (step 5).

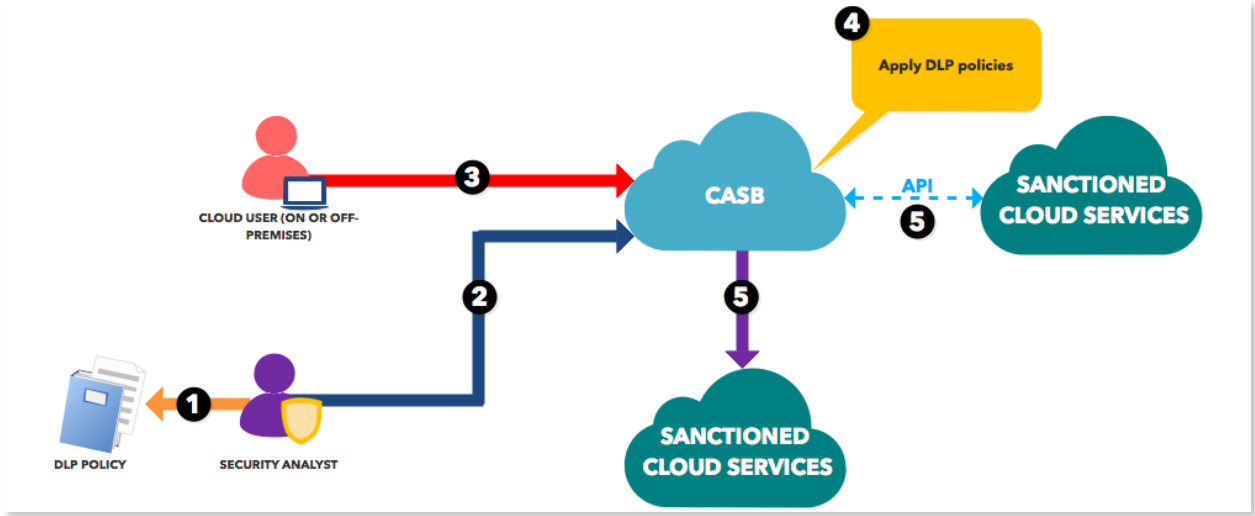


Figure 13 - Enforcing DLP Policies using a CASB

4.3.4. Anomaly Detection and Response

CASBs incorporate machine-learning-enabled user and entity behavior analysis (UEBA) to enable rapid detection of threats targeting cloud services. As discussed by Skyhigh in their "Definitive Guide to Cloud Threat Protection", UEBA builds accurate behavior models for users across cloud services, continuously integrating new data to refine the model and create a dynamic and unique profile for each user or group of users.

An effective UEBA cloud threat protection solution has five key attributes (Skyhigh, n.d.):

1. Transformation of cloud usage data into a unique mathematical model per user or user group
2. Continuously learning usage patterns that do not require human input
3. Grouping users based on specific behaviors (i.e., a group of Help Desk employees who constantly use ServiceNow to open, update, and close trouble tickets during business hours)
4. Understanding of cloud usage throughout different times in the hour, day, week, or month

5. Continuous visibility into cross-cloud threats

Some of the anomalies that a CASB can detect using UEBA include (this list is not exhaustive):

1. Superhuman anomaly when a user has accessed data from multiple geographical locations in an improbable period of time. This may be an indication that the user's account has been compromised.

2. Abnormal data downloads when a user has downloaded an abnormally large amount of data within a short period of time. This may be an indication of an insider threat.

3. Brute force login when a user's account makes multiple failed attempts to log on to a cloud service within a short amount of time. This may also be an indication that the account may be compromised.

Figure 14 represents the anomaly detection and response model for cloud services. The activities generated by the various threat agents (step 1) are captured by the CASB through forward proxy, reverse proxy, or API deployments. The CASB then runs the collected data through the UEBA engine to detect threats (step 2). Threat alerts are then forwarded to an on-premises SIEM (step 3) for consumption by the security analysts (step 4).

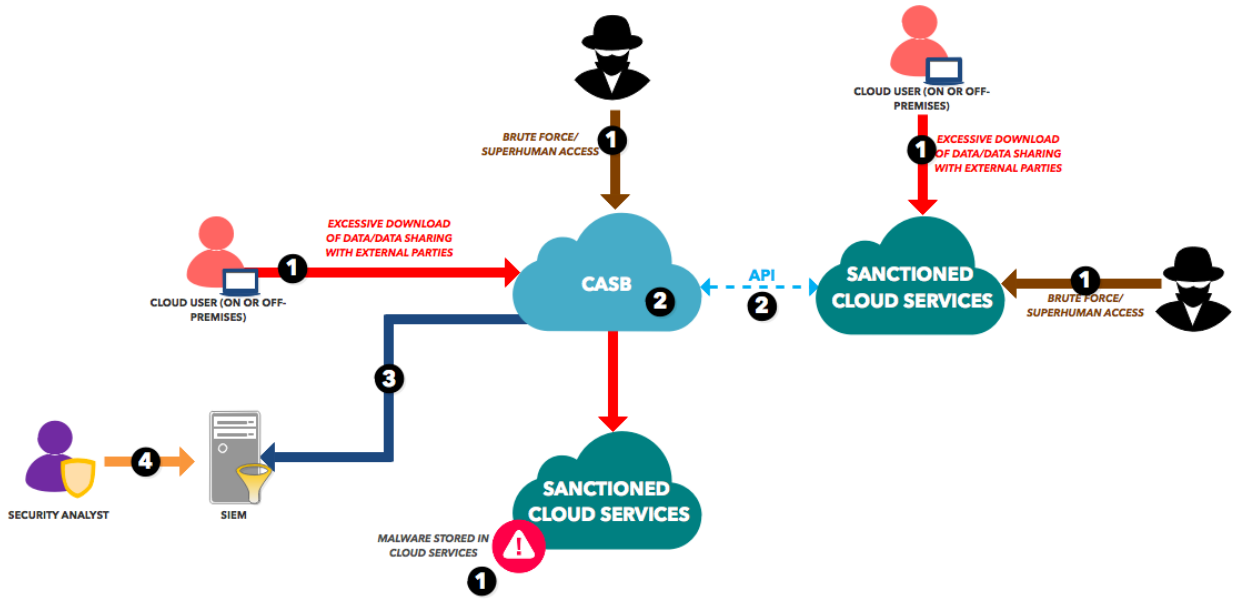


Figure 14 - Anomaly Detection and Response

5. CASB Use Cases

A use case is a written description of how users will perform tasks on a particular IT system (usability.gov, 2013). A security use case defines how security analysts will use a particular tool to enforce security standards and policies. This section will introduce three security use cases for CASB.

Use Case 1: Identify and monitor the usage of unsanctioned cloud services for inappropriate use and potential data leakage.

Threats: insider threat; data exfiltration by malware

CASB deployment model: log collection

Solution:

1. Force all Internet-bound traffic (for users on and off the network) through a web security gateway and feed the logs generated by the web security gateway to the CASB.

2. Analyze cloud usage data in near real-time by developing usage alerts and reviewing daily or weekly actionable reports

3. Take appropriate action to block highest risk cloud services

Effectiveness Test:

1. Upload a rather large (~1 Gb) benign file to an unsanctioned cloud service (i.e., Dropbox or iCloud) while on and off the network, and verify that the CASB has detected the increase in usage for that particular cloud service. The CASB should also capture an audit trail of the activity including offending username, IP address, action, the number of bytes uploaded, destination cloud service, etc.

Use Case 2: Detect when files stored in SharePoint Online and OneDrive for Business that match the keywords "2018 Mergers and Acquisitions" are shared with external domains.

Threats: insider threat

CASB deployment model: API

Solution:

1. Establish an API connection between a CASB and Office 365.

2. Define a DLP policy in CASB that looks for the keywords "2018 Mergers and Acquisitions" in the body and metadata of various file formats including .DOC, .PDF, .XLSX, .TXT, etc. Set the DLP policy action to alert when these types of files are shared (via links) with external domains.

3. Set the scope of the DLP policy to SharePoint Online and OneDrive for Business.

4. Configure the CASB to send alerts to the on-premises SIEM for consumption by the security analysts.

Effectiveness Test:

1. Create a benign file that contains the keywords "2018 Mergers and Acquisitions" in its body and then upload it to SharePoint Online and OneDrive for Business. Share the file

with a bogus external e-mail account, such as jane.doe@gmail.com, via both Office 365 services.

2. Verify that the CASB triggers a DLP policy violation for both Office 365 services.

3. Verify that the CASB sends an alert to the SIEM.

Use Case 3: Enforce step-up authentication and preview-only access when users access ServiceNow from unmanaged endpoints.

Threats: insider threat; compromised accounts

CASB deployment model: Reverse proxy

Solution:

1. Integrate a CASB with the Enterprise Mobile Management (EMM) solution for device management status awareness.

2. Create a cloud access policy that enforces step-up authentication and prevents downloading and uploading of data if the connecting endpoint is unmanaged.

3. Set the scope of the policy to ServiceNow.

4. Configure the CASB to send alerts to the on-premises SIEM for consumption by the security analysts.

Effectiveness Test:

1. Access ServiceNow from an unmanaged endpoint.

2. Attempt to create a ServiceNow incident ticket (data upload attempt).

3. Attempt to download a file attached to a ServiceNow incident or change ticket (data download attempt).

4. Verify that the CASB blocks access for both attempts.

5. Verify that the CASB triggers a cloud access policy violation

6. Verify that the CASB sends an alert to the SIEM

Use cases for CASB must be defined before an organization begins evaluating CASB vendors to ensure that the selected product meets their security and business requirements. Continuously testing the effectiveness of the CASB solution as well as developing relevant metrics are also crucial steps to validate that the organization is getting a return on their security investments.

6. Conclusion

The rapid adoption of cloud services has left information security professionals protecting abstract environments for which traditional security defenses are no longer effective. The majority of CSPs subscribe to a shared responsibility model, where the CSP is responsible for securing the cloud applications and underlying infrastructures while the cloud consumer is responsible for securing their corporate data stored in the cloud. As a result of the shared responsibility model, organizations must take cloud security serious and develop a cloud security strategy that closely aligns with their corporate strategic priorities. A cloud security issue-specific policy, as well as cloud technical security standards, must also be developed to support the cloud security strategy. The cloud security issue-specific policy must address the proper usage of cloud resources while the standards define the technical security controls required to reduce the attack surface of cloud services and to identify cloud-based anomalies and threats before they materialize. Only after these elements are put in place should organizations being to secure their cloud resources.

References

TCO | Total Cost of Ownership. (2014, June 09). Retrieved May 23, 2017, from http://www.gartner.com/it-glossary/total-cost-of-ownership-tc

Software TCO Calculator - SaaS vs. On-premises Pricing. (n.d.). Retrieved May 23, 2017, from http://www.softwareadvice.com/tco/

Shared Responsibility Model - Amazon Web Services (AWS). (n.d.). Retrieved May 23, 2017, from https://aws.amazon.com/compliance/shared-responsibility-model/

Definitive Guide to Cloud Threat Protection - Skyhigh. (n.d.). Retrieved May 23, 2017, from http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP-Definitive-Guide-to-Cloud-Threat-Protection-eBook.pdf

Skyhigh Cloud Adoption Risk Report | Q4 2016 - Skyhigh. (2016). Retrieved May 23, 2017, from http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP-Cloud-Adoption-and-Risk-Report-Q4-2016.pdf

Shadow IT Security Checklist Cheat Sheet - Skyhigh. (n.d.). Retrieved May 23, 2017, from http://info.skyhighnetworks.com/rs/274-AUP-214/images/Skyhigh_Shadow%20IT%20Security%20Checklist.pdf

Federated Identity for Web Applications - Microsoft. (n.d.). Retrieved May 23, 2017, from https://msdn.microsoft.com/en-us/library/ff359110.aspx

Cloud Customer Architecture for Securing Workloads on Cloud Services - Cloud Standards Customer Council. (April, 2017). Retrieved May 23, 2017, from http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-Securing-Workloads-on-Cloud-Services.pdf

Gartner (2016, June 07). Don't Let Shadow IT Put Your Business at Risk. Retrieved May 23, 2017, from http://www.gartner.com/smarterwithgartner/dont-let-shadow-it-put-your-business-at-risk/

Gartner (2005, December 08). Defining Gartner Total Cost of Ownership. Retrieved June 7, 2017, from https://barsand.files.wordpress.com/2015/03/gartner_tco.pdf

Instant Access to Gartner research on Securing Sensitive SaaS Using Cloud Access Security Brokers. (2016, October 04). Retrieved May 23, 2017, from https://research.gartner.com/define-casb?resId=3339317&srcId=1-7651971052

Top-ranked CASB: What is a Cloud Access Security Broker? (n.d.). Retrieved May 23, 2017, from https://www.netskope.com/company/about-casb/

Deployment Architectures for the Top 20 CASB Use Cases - Skyhigh. (n.d.). Retrieved May 23, 2017, from http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP%20Deployment%20Modes%20Top%2020%20Use%20Cases%20102716.pdf

Skyhigh for Shadow IT - Skyhigh (n.d.) - Retrieved May 23, 2017, from http://info.skyhighnetworks.com/rs/274-AUP-214/images/DS-Skyhigh-for-Shadow-IT.pdf

Assessment for Access Control, NISTIR 7316 - NIST (September, 2006) - Retrieved May 23, 2017, from http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

Single Sign-On - Vijay Kumar, OWASP (n.d.) - Retrieved May 23, 2017, from https://www.owasp.org/images/a/ac/OWASP-Single-Sign-On-Vijay.pdf

Skyhigh Data Security - Skyhigh (n.d.) - Retrieved May 23, 2017, from http://info.skyhighnetworks.com/rs/274-AUP-214/images/SB%20Skyhigh%20Data%20Security%200116.pdf

Encrypting Data in the Cloud - Gemalto (2015) - Retrieved May 23, 2017, from https://safenet.gemalto.com/resources/solution-brief/data-protection/Encrypting_Data_in_Cloud_Skyhigh_and_KeySecure_-_Solution_Brief/?langtype=1033&usg=AFQjCNEgaT9EY8cDLhWhiQhGJmRdiprRJQ&sig2=_4t1KP1129fMGfFh9o0gpA

ITIL Configuration Management - ServiceNow (2016, July 05). Retrieved May 24, 2017, from http://wiki.servicenow.com/index.php?title=ITIL_Configuration_Management#gsc.tab=0

Cloud Data Loss Prevention Cheat Sheet - Skyhigh (2016, September). Retrieved May 23, 2017, from http://info.skyhighnetworks.com/rs/274-AUP-214/images/CH%20Cloud%20Data%20Loss%20Prevention%20Cheat%20Sheet.pdf

Use Cases. Affairs, A. S. (2013, October 09). Retrieved May 24, 2017, from https://www.usability.gov/how-to-and-tools/methods/use-cases.html

AWS Total Cost of Ownership Calculator. (n.d.). Retrieved June 07, 2017, from https://aws.amazon.com/tco-calculator/