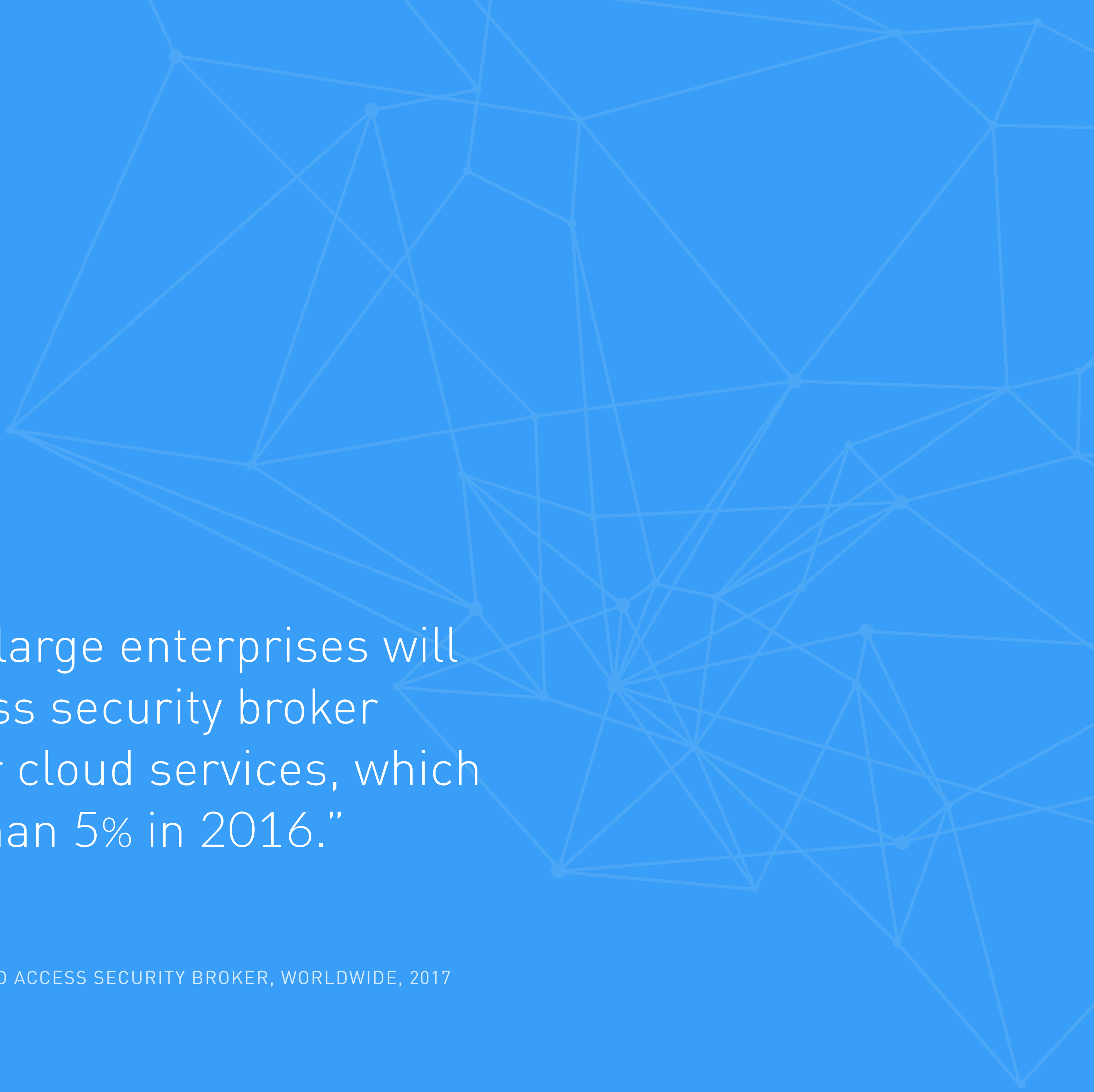
Skyhigh

Deployment Architectures for the Top 20 CASB Use Cases

When enterprises embark on a cloud security project, they usually discover that there are multiple ways to deploy a cloud access security broker (CASB). Deciding on the right architecture for your project is one of the most important decisions you'll make since it impacts what CASB features you'll be able to apply to which users, devices, and services and under what conditions. The enforcement point in the on-premises era was clear – it was at the network edge. In the cloud era, the perimeter is undefined. When deploying a CASB, how do you ensure you have visibility and control over all users, all devices, and all cloud services?

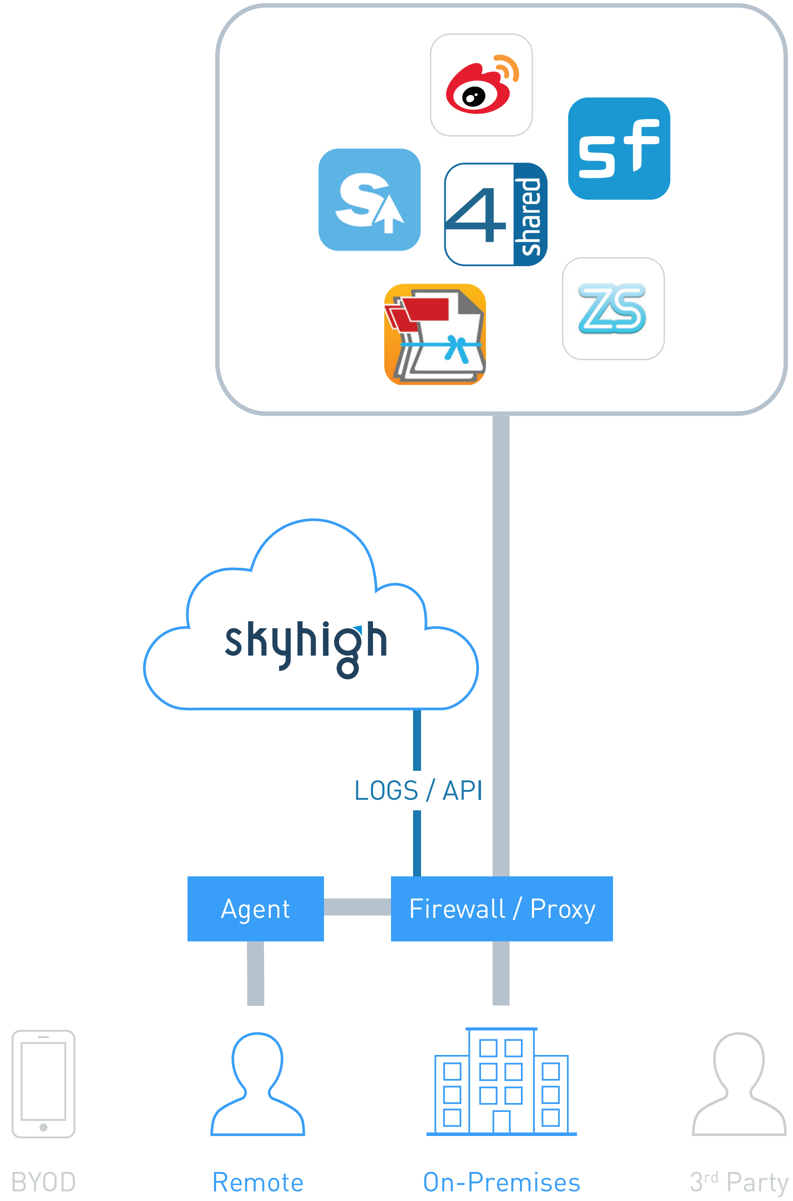
This document reviews the primary CASB deployment modes and then describes the 20 most common CASB use cases, revealing which deployment mode best supports each of the use cases.

TABLE OF CONTENTS



“By 2020, 85% of large enterprises will use a cloud access security broker platform for their cloud services, which is up from less than 5% in 2016.”

GARTNER, FORECAST SNAPSHOT: CLOUD ACCESS SECURITY BROKER, WORLDWIDE, 2017

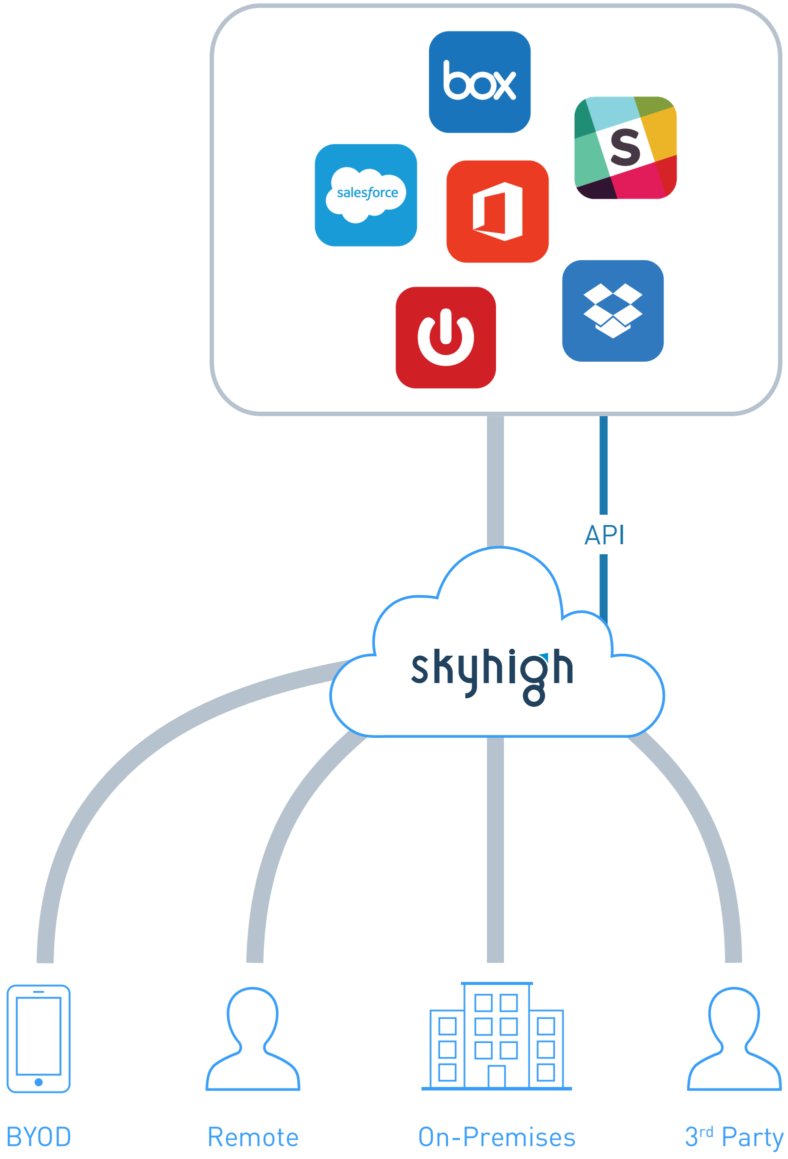


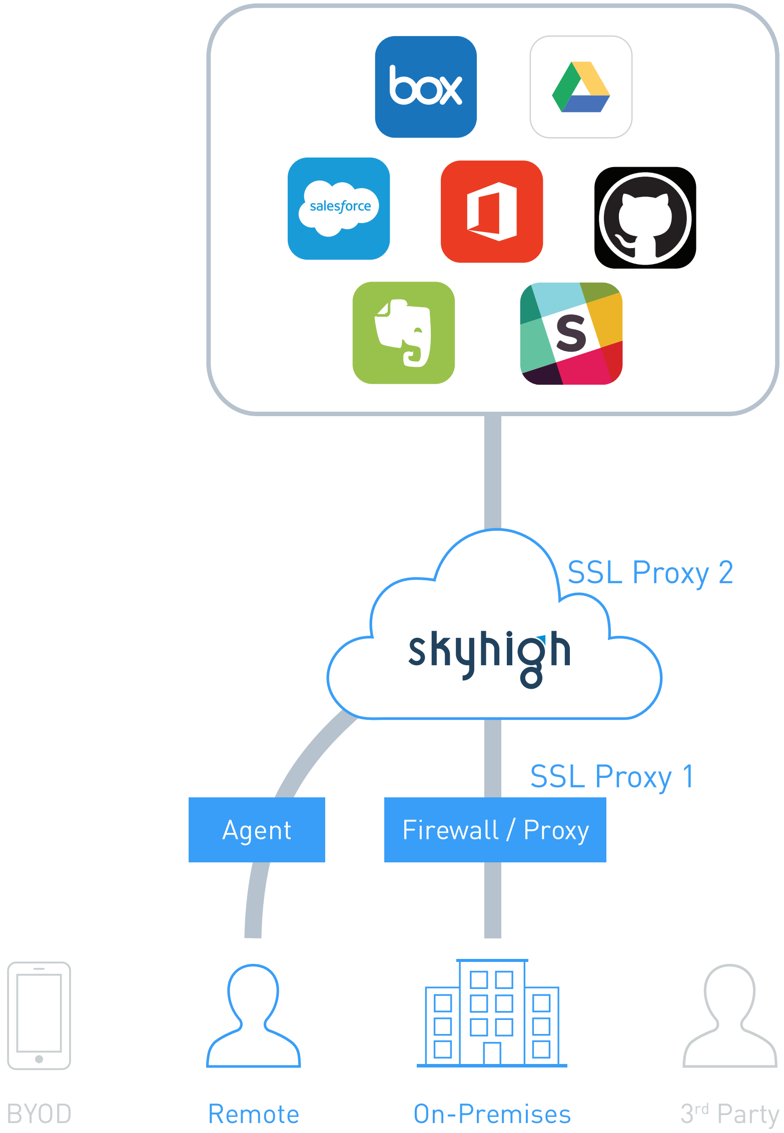
CLOUD DEPLOYMENT MODES: LOG COLLECTION

In this mode, a CASB collects event logs generated by existing infrastructure such as firewalls and secure web gateways. Generally, logs capture user activity but not content. A CASB uses a on-premises connector which runs on a virtual machine to collect log files from firewalls and web proxies, or from SIEMs where these logs have already been collected and aggregated from multiple devices.

CLOUD DEPLOYMENT MODES: API

Enterprise-grade cloud services offer APIs that support visibility and policy enforcement by a CASB. Generally, these APIs support audit trails of user activity, content inspection, and scanning user privileges, sharing permissions on files and folders, and application security settings. Of course, API-based capabilities vary for each cloud service provider.



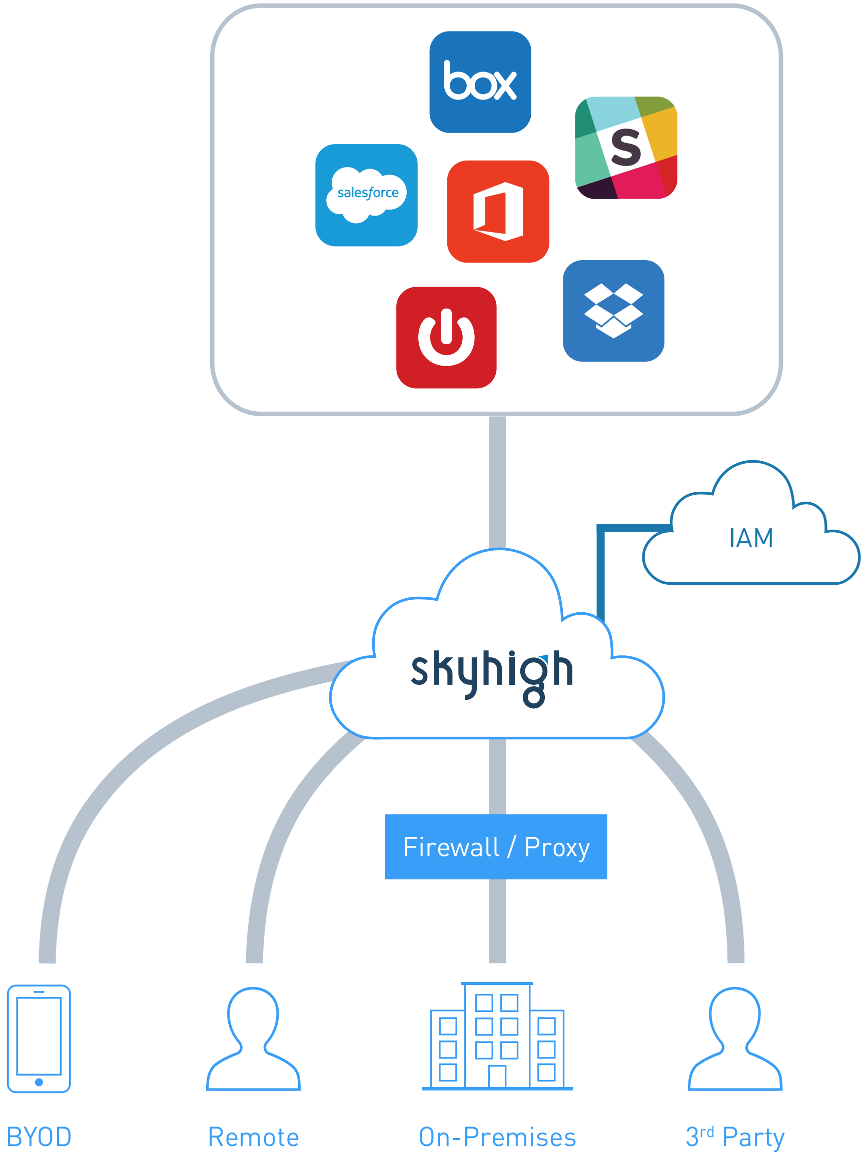


CLOUD DEPLOYMENT MODES: FORWARD PROXY

A CASB in forward proxy mode routes all cloud traffic via the user's endpoint device. There are two ways to deploy forward proxy. First, if you have an existing secure web gateway, you can configure proxy chaining to the upstream CASB forward proxy. If no secure web gateway exists, you can also deploy an endpoint agent to route cloud traffic through the forward proxy.

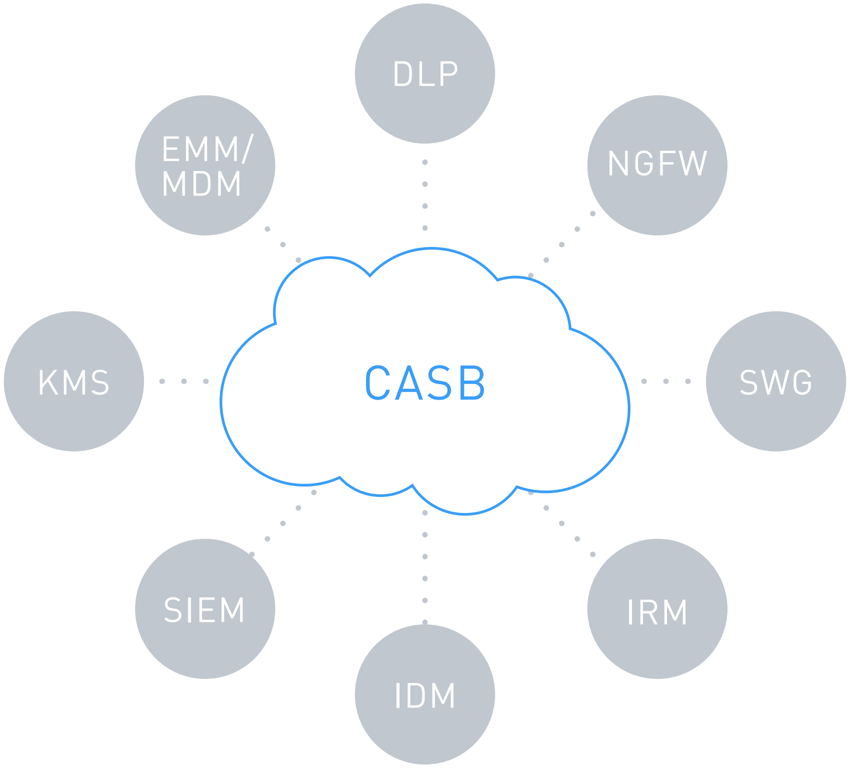
CLOUD DEPLOYMENT MODES: REVERSE PROXY

A CASB in reverse proxy mode proxies all traffic to and from a specific cloud provider. Unlike a forward proxy, the endpoint or network does not need to be managed. Instead, the identity solution (IDM) routes traffic through the reverse proxy following authentication. In this way, all traffic bound for a cloud service is seamlessly and pervasively steered to the proxy.



> “Choose multimode CASB solutions that offer a variety of in-line and API-based visibility options.”

GARTNER, HOW TO EVALUATE AND OPERATE A CLOUD ACCESS SECURITY BROKER



INTEGRATIONS TO EXISTING SECURITY INFRASTRUCTURE

Enterprises already have an ecosystem of security tools used to enforce policies and perform reporting. A CASB can integrate with these technologies to extend existing policies and workflows to the cloud. In these cases, the CASB acts as the enforcement point, optionally leveraging existing solutions where available to ensure a holistic approach to security.

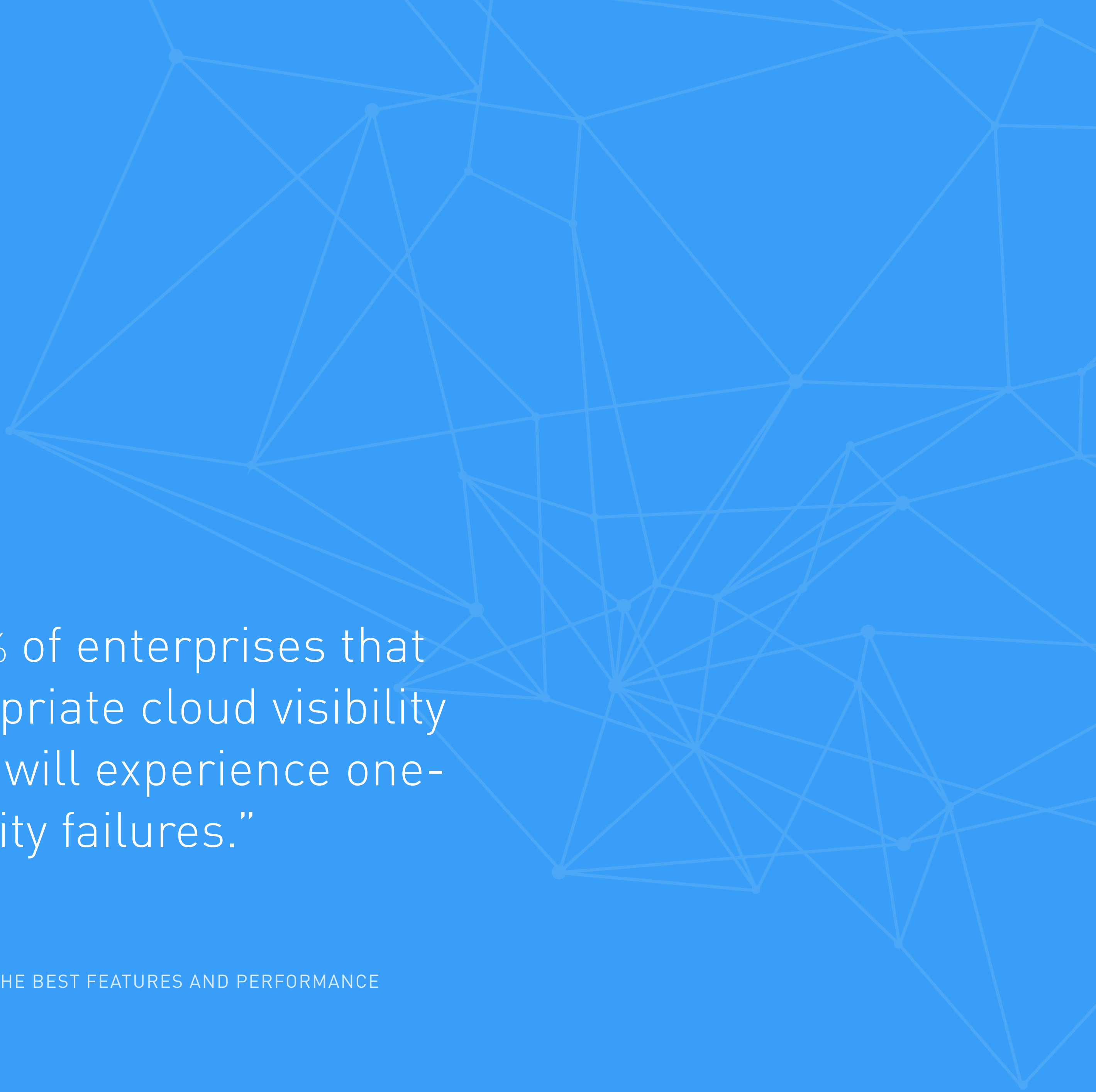
- Data loss prevention (DLP)
- Next generation firewall (NGFW)
- Secure web gateway (SWG)
- Enterprise digital rights management (EDRM) or IRM
- Enterprise mobility management (EMM) / mobile device management (MDM)
- Identify management (IDM)
- Security information and event management (SIEM)
- Key management service (KMS)

Now, we'll look at the top 20 CASB use cases in the context of the deployment architectures and integrations that support them. The use cases are categorized by controls applied on cloud service types – shadow SaaS, sanctioned SaaS, and IaaS services. While each use case has corresponding deployment modes and integrations listed, they represent multiple options and are not all required to support the use case.

Chapter 1:

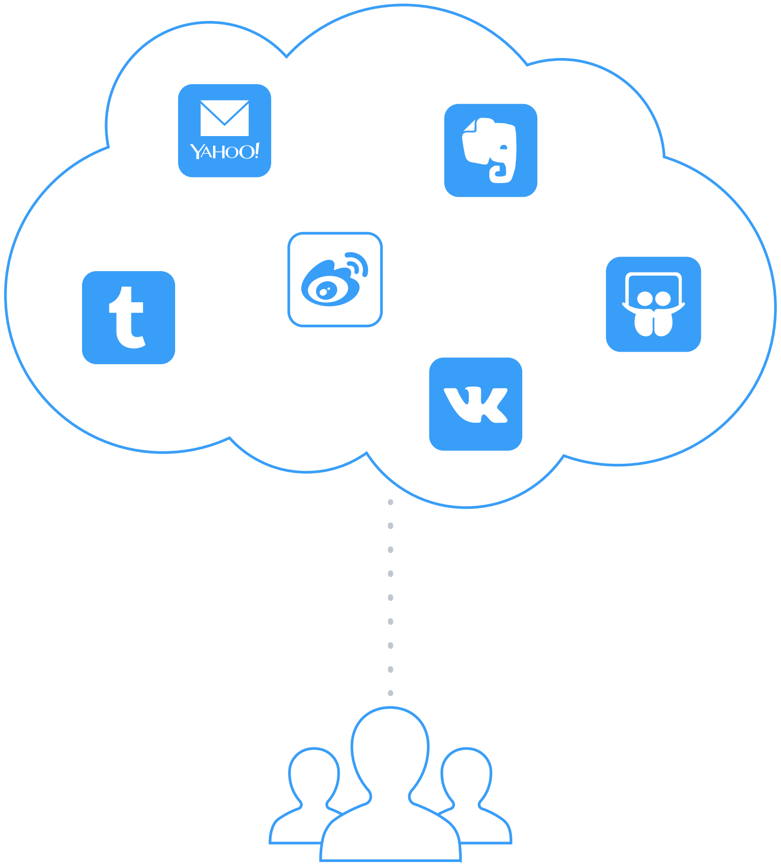
Securing Shadow Cloud Services

The average organization uses 1,427 cloud services and most of these are not sanctioned by IT. The growth of shadow cloud usage represents a security vulnerability because many apps used by employees may not conform to the company's security requirements. In fact, out of the 20,000+ cloud services in use today, less than 8.1% meet enterprise-grade data security and privacy requirements as defined by Skyhigh's CloudTrust program. So, enterprises are using CASB solutions to gain visibility and control over shadow SaaS usage while enabling employees to remain productive.



"By 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures."

GARTNER, CASB PLATFORMS DELIVER THE BEST FEATURES AND PERFORMANCE



1. DISCOVER CLOUD SERVICES IN USE

A CASB solution enables IT to discover cloud services in use by all employees and business units and identify which cloud services do not meet security requirements.

For example, a CASB solution, after analyzing web traffic logs, shows that a company's employees are using a total of 2,000 cloud services which include 80 services that do not meet the company's security requirements as they do not encrypt data at rest, do not commit to not sharing data with third parties, are hosted in an ITAR restricted country, or claim ownership of corporate data uploaded to them.

Deployment mode(s)

- Log collection

Integration(s) leveraged

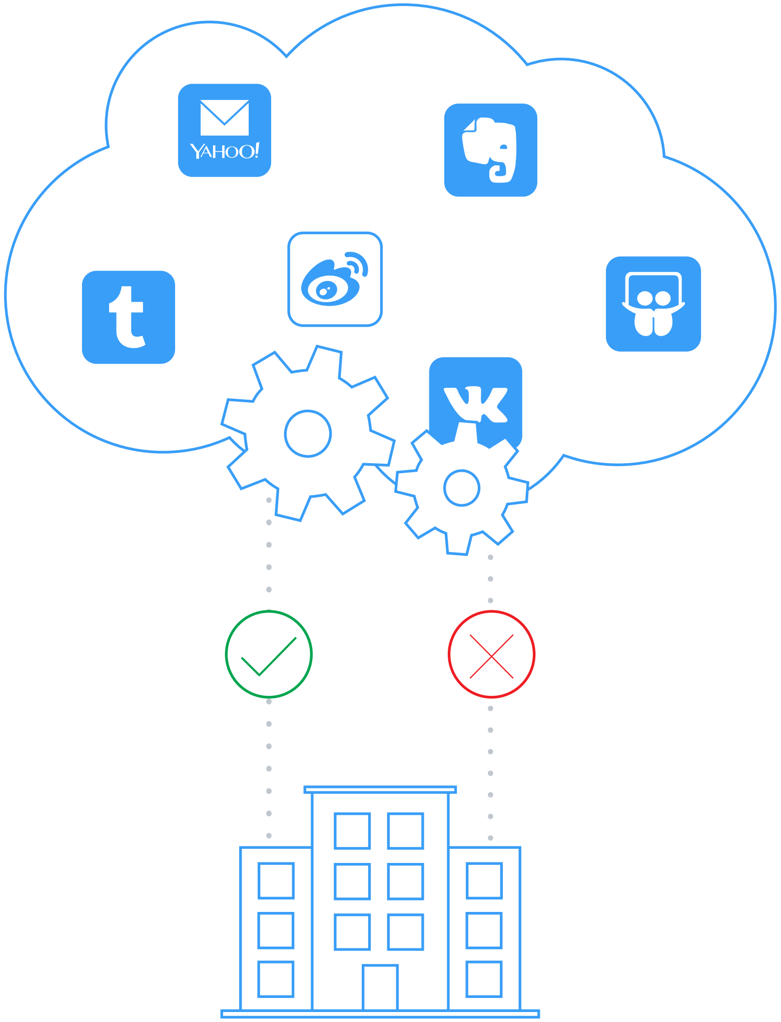
- Security information and event management (SIEM)
- Secure web gateway (SWG)
- Next generation firewall (NGFW)

2. ASSESS CLOUD SERVICE RISK

A CASB solution allows companies to assess the risk of any cloud service by providing a risk score calculated using 50+ attributes and 100+ sub-attributes. Having up-to-date security information for cloud services at hand saves several hours spent in evaluation before onboarding them and to expedite the approval of cloud service requests by employees.

Deployment mode(s)

- Log collection



3. APPLY CLOUD GOVERNANCE POLICIES

IT teams use the risk rating provided by the CASB solution to define acceptable use governance controls by integrating with existing infrastructure. For example, cloud PDF converter services that claim ownership of data uploaded to them are classified into the "not allowed" or "prohibited" service group and all uploads to these services are automatically blocked.

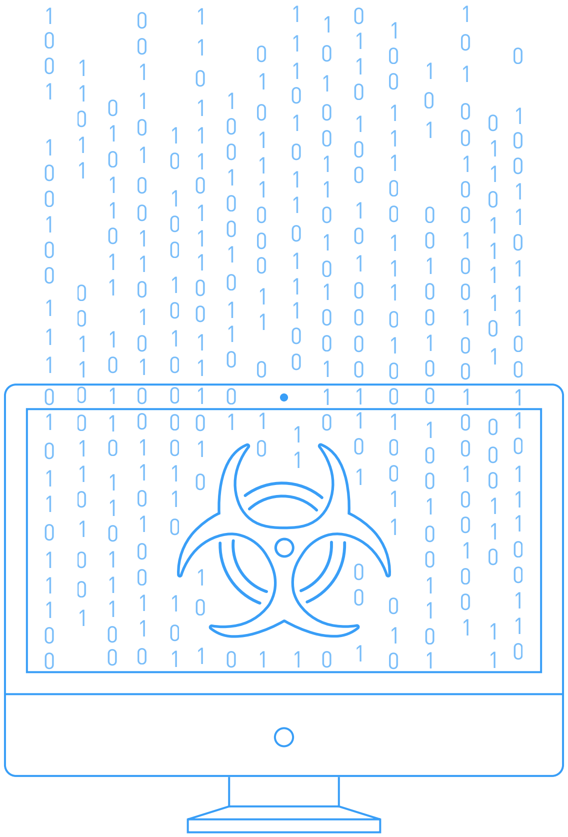
Typically CASB users create at least 3 categories: 1) IT-sanctioned services, 2) permitted services, and 3) prohibited services. By defining governance policies and leveraging integrations between the CASB and SWG/NGFW, companies enforce governance policies in real-time.

Deployment mode(s)

- Log collection

Integration(s) leveraged

- Secure web gateway (SWG)
- Next generation firewall (NGFW)



4. DETECT DATA EXFILTRATION AND PROXY LEAKAGE

Using a CASB, companies can detect malware operating on the enterprise network that leverages the cloud as a vector for data exfiltration, such as sensitive data exfiltrated via a private Twitter account. Companies also use CASBs to ensure acceptable use governance policies are fully enforced by existing SWG/NGFWs and there is no proxy leakage.

For example, a policy to block a risky cloud services URL may be enforced in the North America offices, but not in the EMEA ones before the CASB identifies and remediates the proxy leakage.

Deployment mode(s)

- Log collection

Integration(s) leveraged

- Secure web gateway (SWG)
- Next generation firewall (NGFW)

5. GAIN GRANULAR VISIBILITY AND ENFORCE ACTIVITY-LEVEL CONTROLS

Using a CASB, companies can gain deep visibility into selected shadow cloud services and enforce granular controls at the user, activity, and data levels.

For example, IT admins can define a policy where an engineering team is blocked from accessing selected repositories in GitHub, but has access to others.

Deployment mode(s)

- Forward proxy

Integration(s) leveraged

- Secure web gateway (SWG)
- Next generation firewall (NGFW)

Chapter 2:

Securing Sanctioned Cloud Services

Sanctioned cloud services such as Office 365, Salesforce, Box, and Slack are used in business critical processes and as a result, house sensitive corporate data. 18.1% of all documents uploaded into cloud-based file sharing services contain sensitive data such as confidential IP, personally identifiable information (PII), personal health information (PHI), or financial data. While leading cloud service providers have built state-of-the-art controls into their infrastructure, enterprises are responsible for securing their employees' usage and data.

"By 2018, 40% of Office 365 deployments will rely on third-party tools to fill in gaps in security and compliance, which is a major increase from fewer than 10% in 2015."

GARTNER, CASB PLATFORMS DELIVER THE BEST FEATURES AND PERFORMANCE

6. ENFORCE DLP POLICIES FOR DATA STORED IN THE CLOUD

Companies can enforce data loss prevention (DLP) policies to detect sensitive data that has been uploaded or is existing in the cloud. For example, if the corporate policy is to not permit credit card numbers to be stored in the company's cloud-based file sharing service, then a CASB can be used to scan pre-existing data at rest as well as inspect uploads on an ongoing basis to detect policy violations and provide multiple remediation options such as alert, block quarantine, encrypt, and delete.

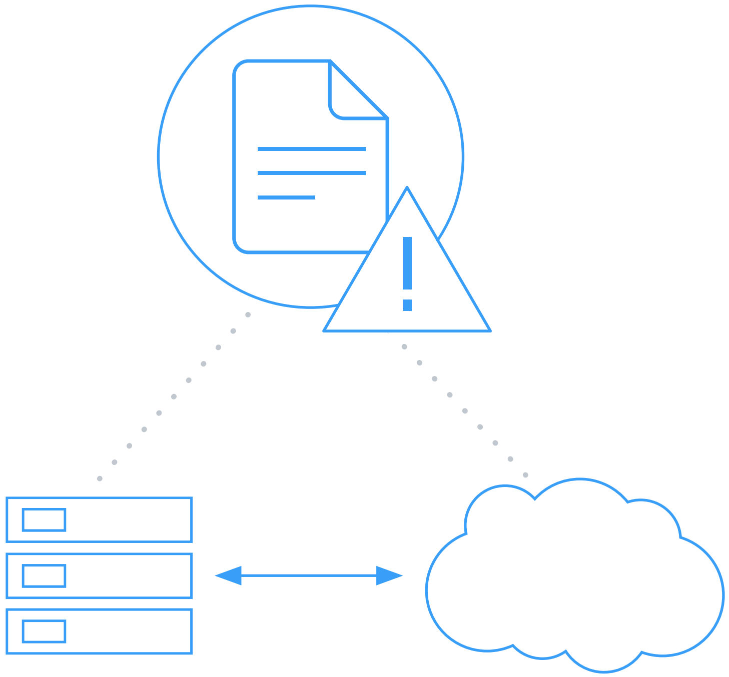
DLP policies can be created natively within the CASB using advanced techniques such as data identifies, indexed data matching, and exact data matching. API is typically the preferred option for collaboration services because it also enables policy enforcement for content created natively within the cloud service, but CASBs offer varying response times for API enforcement, which range from under 30 seconds to over 30 minutes.

Deployment mode(s)

- API (near real-time)
- Reverse proxy (real-time)

Integration(s) leveraged

- On-premises DLP solution



7. ENFORCE POLICIES FROM AN ON-PREMISES DLP SOLUTION

Most companies have made investments in acquiring on-premises DLP solutions and building workflows to cover a number of their existing processes. A CASB can integrate with these on-premises DLP solutions to extend workflows and controls to the cloud.

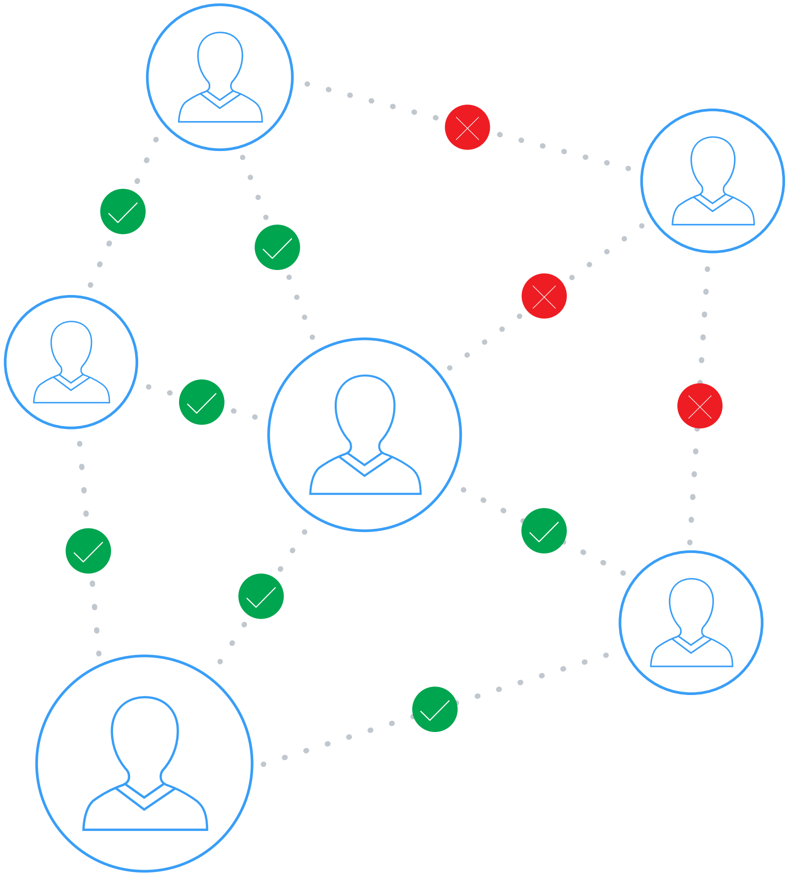
For example, a CASB can be used to evaluate all files stored in Box against policies in Intel McAfee DLP and enforce the appropriate remediation action based on those policies (e.g. quarantine, delete, encrypt, etc).

Deployment mode(s)

- API

Integration(s) leveraged

- On-premises DLP solution



Skyhigh

8. ENFORCE COLLABORATION POLICIES ON DATA SHARED FROM CLOUD SERVICES

Increase in cloud-to-cloud traffic requires companies to enforce controls that protect sharing and collaboration within cloud services between employees and external users.

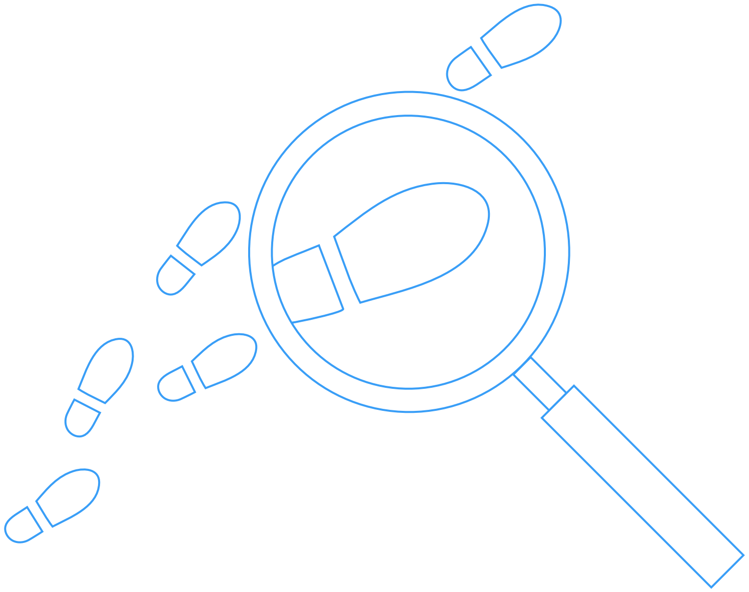
For example, a company can define a CASB policy to find all files in Box that are shared with non-approved domains such as personal email IDs and revoke sharing permissions. Policies can also be applied to revoke all untraceable shared links that can be forwarded to anyone. Companies will also leverage DLP policies and data classification to prevent the sharing of internal only documents with any external party.

Deployment mode(s)

- API

Integration(s) leveraged

- On-premises DLP solution



9. CAPTURE AN AUDIT TRAIL OF ALL USER ACTIVITY FOR FORENSIC INVESTIGATIONS

A CASB solution captures user activity data within a cloud service for audit trails or forensic investigations.

For example, an administrator looking to investigate user activity on SharePoint Online can filter audit logs by multiple parameters including user, date, activity category (upload/download/delete/access etc.), role, and location to get to the required information.

Deployment mode(s)

- API
- Reverse Proxy

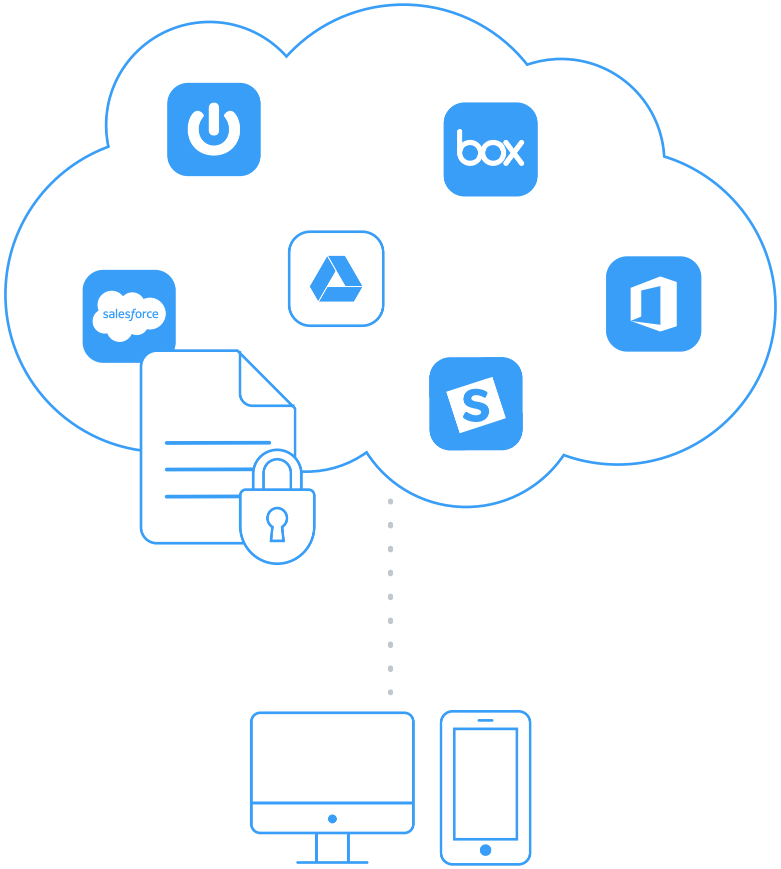
10. DETECT THREATS FROM COMPROMISED ACCOUNTS, INSIDERS, AND PRIVILEGED USERS

CASBs analyze cloud activity across multiple heuristics and uses machine learning to detect anomalous usage pertaining to compromised accounts, insider threats, and privileged user misuse.

For instance, if a user logs in to OneDrive from New York and then logs into Slack from Moscow 5 minutes later, the CASB will see this activity as anomalous and potentially indicative of a compromised account. Other examples of anomalies include excessive downloads by insiders and deletion of user accounts by a privileged users. CASBs are able to correlate multiple anomalies to surface true threats and reduce false positive alerts.

Deployment mode(s)

- API
- Reverse Proxy



11. ENCRYPT DATA STORED IN THE CLOUD

CASBs allow companies to encrypt structured and unstructured data residing in cloud services using customer-owned encryption keys.

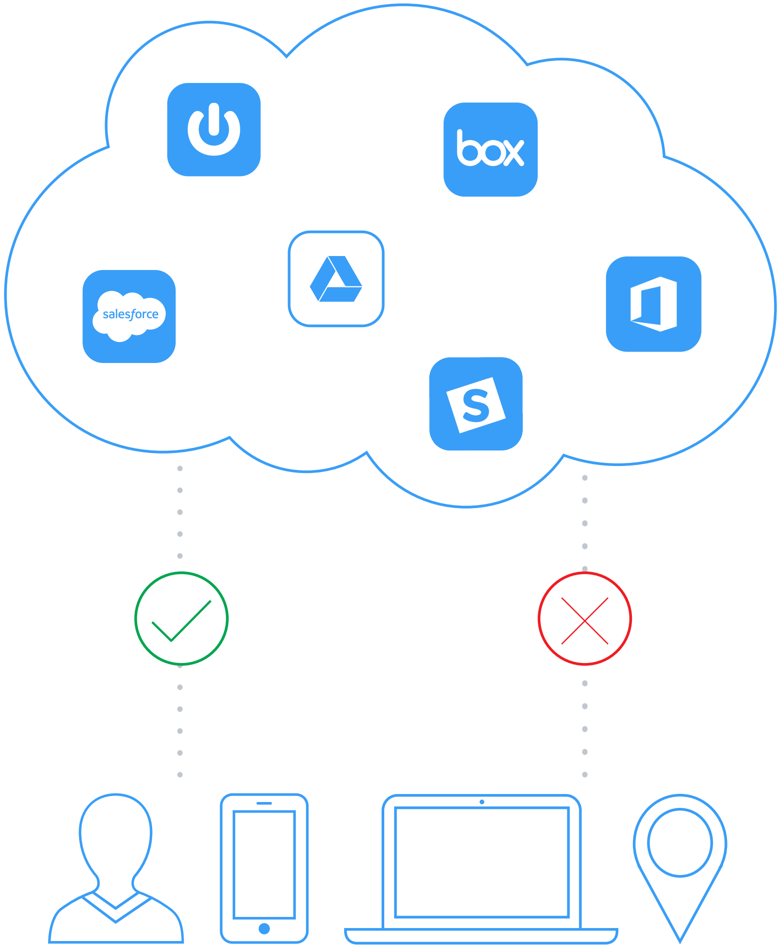
For example, when a user attempts to upload a document containing patient health information to OneDrive, the CASB detects and encrypts this document. IT teams can also define policies to encrypt structured data, such as name, address, and company fields within Salesforce. CASBs should be able to preserve important application functionality such as search and sort when encrypting structured data.

Deployment mode(s)

- Reverse Proxy

Integration(s) leveraged

- Key management service (KMS)



12. ENFORCE ACCESS CONTROL POLICIES

CASB solutions can be used to apply access controls based on contextual factors such as user, role, location, and department.

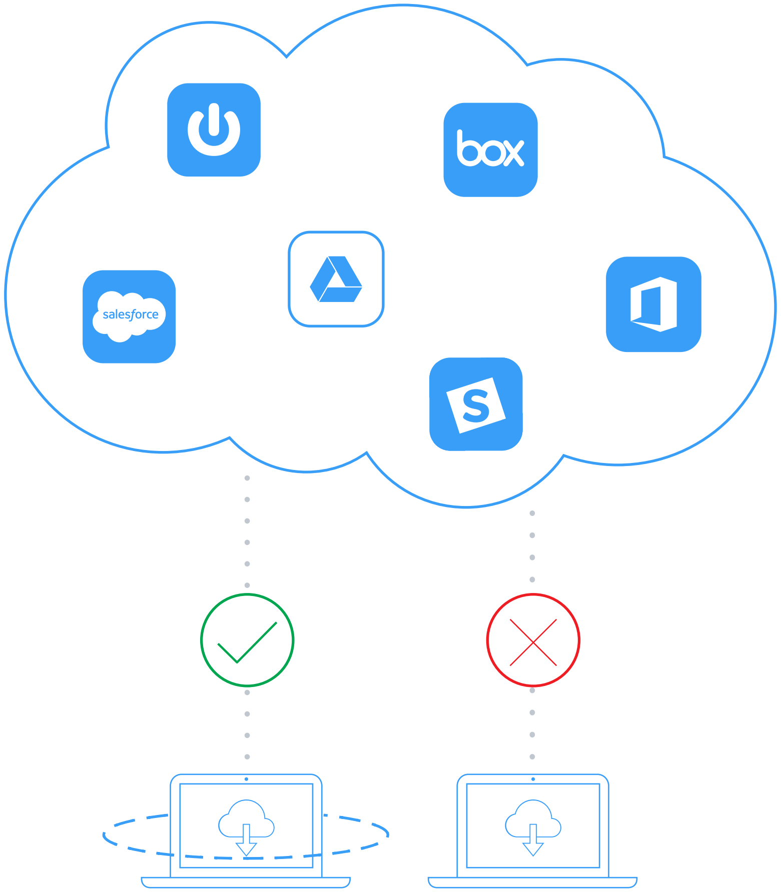
For example, a user attempting to download a customer report from Salesforce when on a public network is blocked, but a user on a corporate network (or VPN) is able to download the report.

Deployment mode(s)

- Reverse Proxy

Integration(s) leveraged

- Identity management (IDM)



13. PROTECT DATA DOWNLOADED TO UNMANAGED DEVICES

CASBs allow granular controls to be enforced based on whether the user is accessing data using a personal or a corporate device.

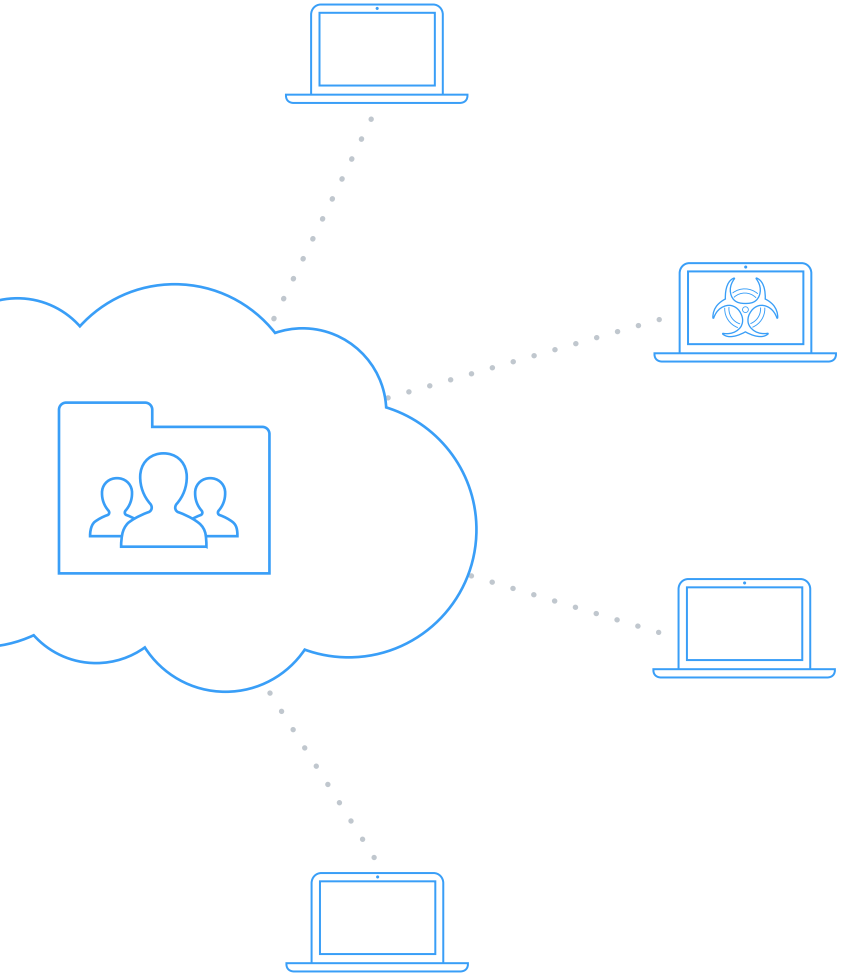
For example, a user accessing a product roadmap document in OneDrive is allowed to preview data, but not download the document to a device without appropriate endpoint security (e.g. remote wipe, strong device PIN) in place.

Deployment mode(s)

- Reverse Proxy

Integration(s) leveraged

- Enterprise mobility management (EMM) / mobile device management (MDM)
- Identity management (IDM)



14. DETECT AND REMEDIATE MALWARE

Malware residing in files uploaded to cloud services can be detected by the CASB solution so IT administrators can remediate before it infects systems within the company.

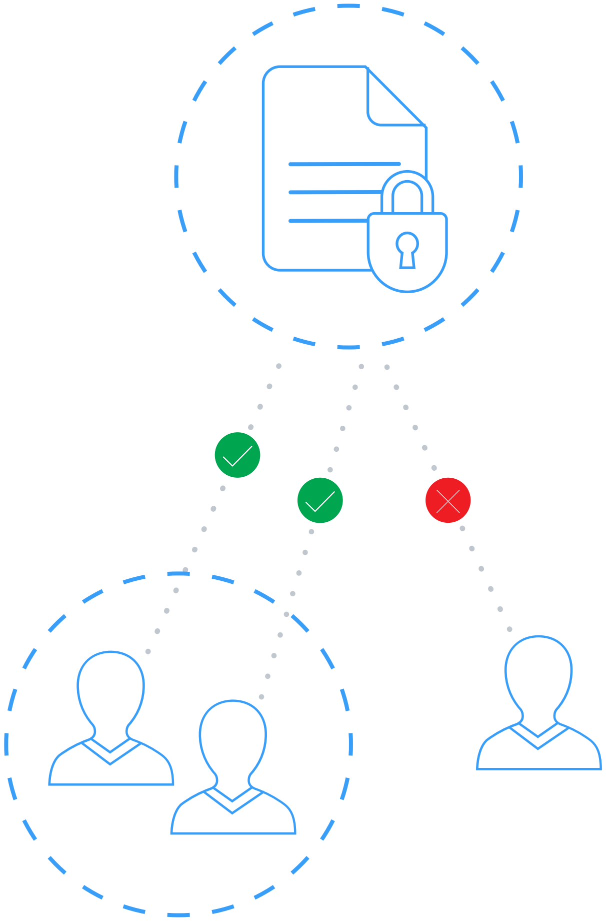
For example, a word document containing malicious macros is uploaded to the corporate Box folder from an infected system and is detected during a scan performed by the CASB solution before it syncs down to other employees' devices. CASBs may have built-in malware capabilities and also integrate with existing malware detection solutions.

Deployment mode(s)

- API

Integration(s) leveraged

- Malware detection solution



15. APPLY RIGHTS MANAGEMENT TO CLOUD DATA

IT teams can apply information rights management protection on files uploaded or downloaded from the cloud.

For example, customers can apply EDRM (or IRM) protection to a budget spreadsheet downloaded to OneDrive, so it cannot be accessed by anyone other than the authorized set of users.

Deployment mode(s)

- Reverse proxy
- API

Integration(s) leveraged

- Enterprise Digital Rights Management (EDRM)

Chapter 3:

Securing IaaS Services and Custom Apps

Adoption of IaaS platforms such as Amazon Web Services (AWS), Azure, and Google Cloud Platform is growing quickly as enterprises move data and applications out of their data centers. But to maintain compliance with their internal standards and industry regulations, they use CASB solutions to monitor and secure the IaaS environments as well as the custom applications that run on them. CASB solutions deliver advanced capabilities that allow IT teams to gain visibility and extend their existing controls on IaaS environments as well as home-built custom applications.

> “The average enterprise has 464 custom applications deployed and IT security professionals are only aware of 38.4% of these applications.”

CLOUD SECURITY ALLIANCE (CSA), CSA SURVEY – CUSTOM APPS AND IAAS TRENDS 2017

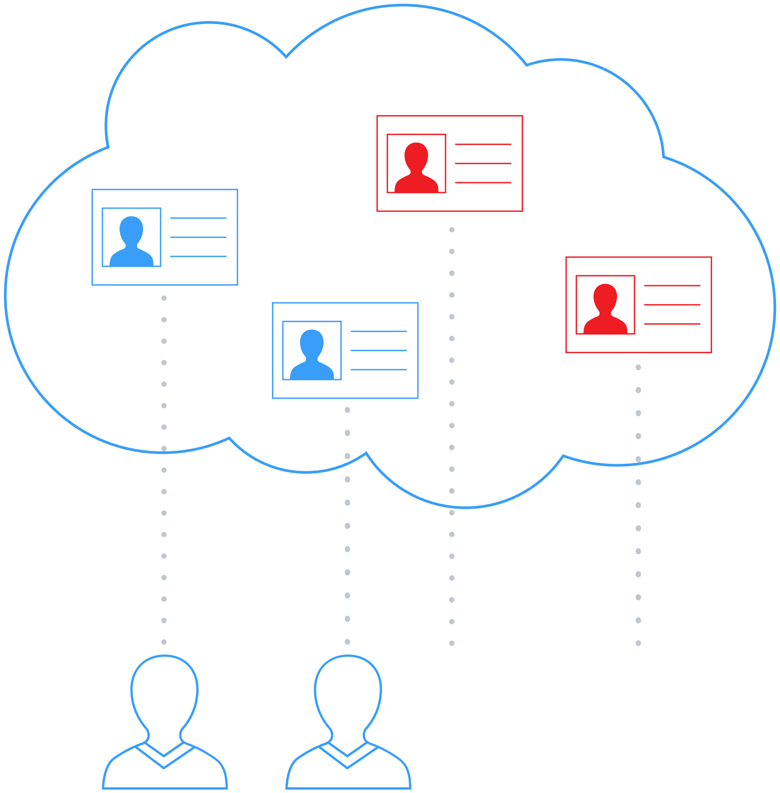
16. IAAS CONFIGURATION AUDIT

IaaS environments have extensive security settings, which if misconfigured can put the company at risk of compliance violations.

For example, an audit of the customer's AWS environment by a CASB solution can highlight that the administrator has not turned on CloudTrail, which logs activities within AWS. This can lead to a malicious user modifying or deleting key AWS resources and also destroying the logs, thereby eliminating detection.   A configuration audit can also identify security loopholes, like an S3 bucket with sensitive data that is publicly accessible.

Deployment mode(s)

- API



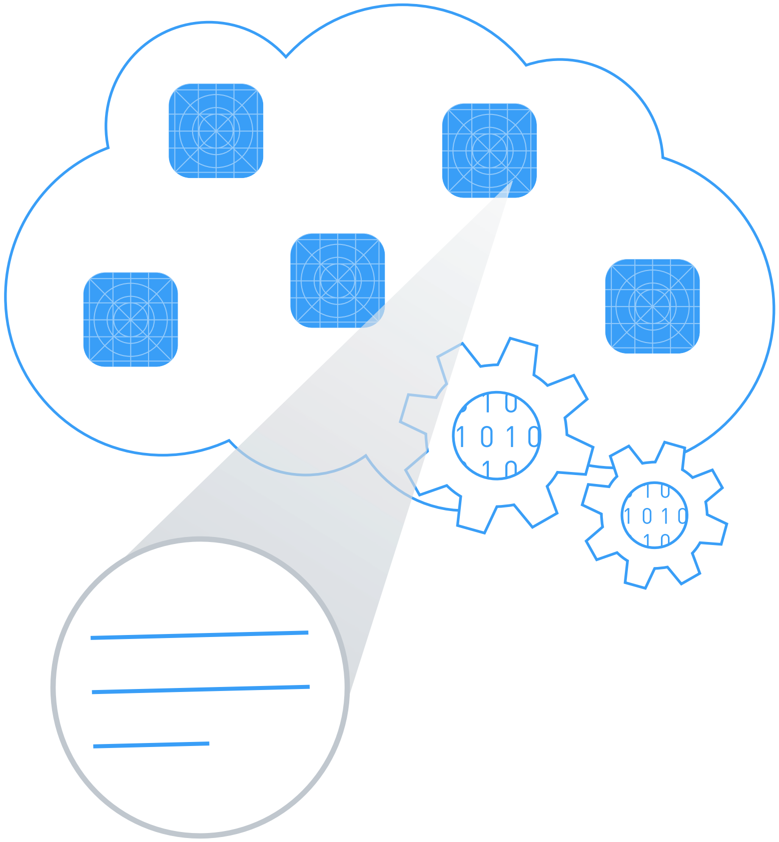
17. UNDERSTAND PROVISIONED USER RISK (OVER-PROVISIONED, INACTIVE)

Administrators provision access to a number of users, but a number of accounts may be inactive or have excessive permissions. A CASB can help identify dormant accounts and provide a unified view of IDM permissions assigned across user accounts.

For example, a CASB configuration audit can highlight that 15 engineers who have left the company in the last year still have active AWS accounts or that all engineers have been mistakenly provided admin access and can modify configurations.

Deployment mode(s)

- API



18. CAPTURE USER ACTIVITY LOG WITHIN CUSTOM APPS

Security teams usually don't have visibility into employee activities within custom applications deployed on IaaS platforms, and these apps often bypass the standard security reviews and processes. CASB solutions use an AI-driven application learning module to rapidly and accurately map activities within any custom application, allowing for visibility and enforcement of security controls.

For example, security incidents occurring on a custom loan origination application within a financial services company can be investigated by the security team using the audit log generated by the CASB solution.

Deployment mode(s)

- Reverse proxy

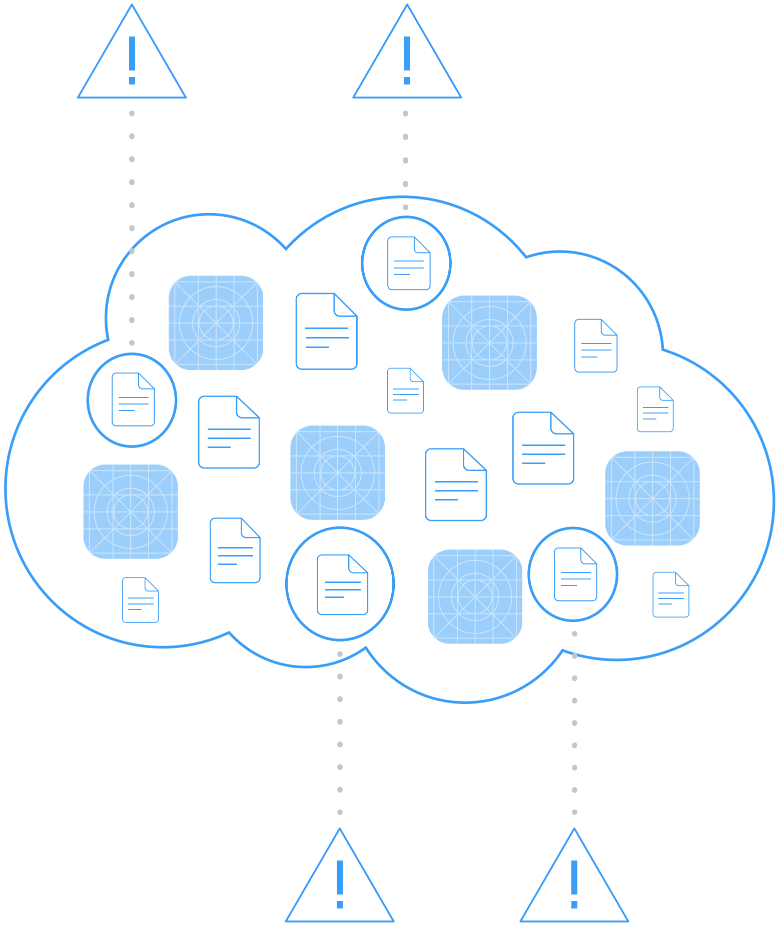
19. ACTIVITY MONITORING AND THREAT PROTECTION

A CASB solution is able to capture and analyze activity within the IaaS platform and custom applications and use machine learning to detect anomalous usage associated with compromised accounts, insiders, and privileged users.

For example, if an AWS account or a custom application user account is being accessed from multiple countries within a short time period (representing impossible travel), the CASB records a geolocation anomaly and may trigger a compromised account threat.

Deployment mode(s)

- API
- Reverse proxy



20. DATA LOSS PREVENTION ON DATA IN CUSTOM APPLICATIONS

Sensitive corporate data uploaded to custom apps can be accessed by unauthorized users or could result in a compliance violation. A CASB can apply granular DLP policies (or extend existing policies from on-premises systems) to protect sensitive data from being exfiltrated via custom apps.

For example, if an employee is entering customer credit card numbers into an unencrypted field of a custom registration application, a CASB can be used to restrict the upload of this information as it is a violation of PCI compliance.

Deployment mode(s)

- Reverse proxy

Integration(s) leveraged

- On-premises DLP solution

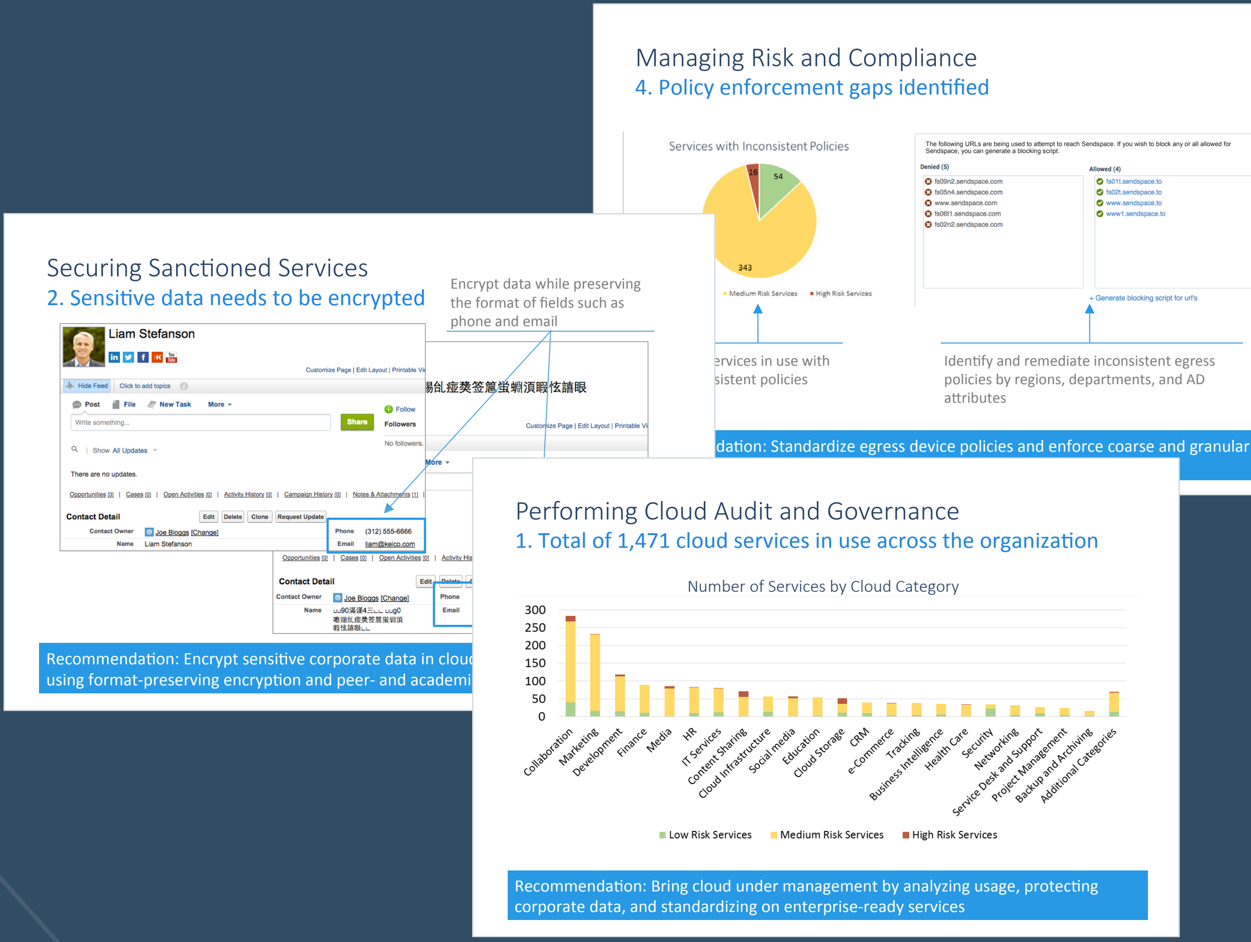
GET AN AUDIT OF YOUR CLOUD USAGE

Skyhigh can provide a personalized assessment of cloud usage in your organization. We'll deliver a report summarizing:

- All cloud applications in use
- High-risk apps accessed by your employees
- Gaps in your proxy/firewall policy enforcement
- Redundant services used in each category

REQUEST AN AUDIT

bit.ly/2i0Z9S4



Managing Risk and Compliance

4. Policy enforcement gaps identified

The following URLs are being used to attempt to reach Sendspace. If you wish to block any or all allowed for Sendspace, you can generate a blocking script.

Denied (5)	Allowed (4)
☒ fs09n2.sendspace.com	✓ fs01t.sendspace.to
☒ fs05n4.sendspace.com	✓ fs02t.sendspace.to
☒ www.sendspace.com	✓ www.sendspace.to
☒ fs06t1.sendspace.com	✓ www1.sendspace.to
☒ fs02n2.sendspace.com	

+ Generate blocking script for url's

ervices in use with sistent policies

Identify and remediate inconsistent egress policies by regions, departments, and AD attributes

dation: Standardize egress device policies and enforce coarse and granular

Securing Sanctioned Services

2. Sensitive data needs to be encrypted

Encrypt data while preserving the format of fields such as phone and email

Liam Stefanson

No followers.

There are no updates.

Opportunities [0] | Cases [0] | Open Activities [0] | Activity History [0] | Campaign History [0] | Notes & Attachments [1] |

Contact Detail

Contact Owner: Joe Bloggs [Change]

Name: Liam Stefanson

Phone: (312) 555-6666

Email: liam@kelco.com

睗乩瘂葵签篙蚩蝴湏暇怯請眼

Opportunities [0] | Cases [0] | Open Activities [0] | Activity His

Contact Detail

Contact Owner: Joe Bloggs [Change]

Name: ㄩㄩ90滿謹4三ㄩㄩ ㄩㄩg0 嚓睗乩瘂葵签篙蚩蝴湏 暇怯請眼ㄩㄩ

Phone

Email

Recommendation: Encrypt sensitive corporate data in clou using format-preserving encryption and peer- and academi

Performing Cloud Audit and Governance

1. Total of 1,471 cloud services in use across the organization

Recommendation: Bring cloud under management by analyzing usage, protecting corporate data, and standardizing on enterprise-ready services