

Top 7 Office 365 Security Use Cases for a CASB



TABLE OF CONTENTS

Introduction	2		
CASB deployment architectures	7		
Office 365 use cases for a CASB	13		
Prevent unauthorized data from being shared externally	16	Capture an audit trail of activity for forensic investigations	39
Prevent regulated, high-value data from being stored in the cloud	22	Prevent loss of corporate O365 data from use of personal O365 instances	44
Block download of O365 data to personal devices	29	Prevent proliferation of malware	48
Detect compromised accounts and insider/privileged user threats	33	What to look for in a CASB	52
		Customer maturity model	61

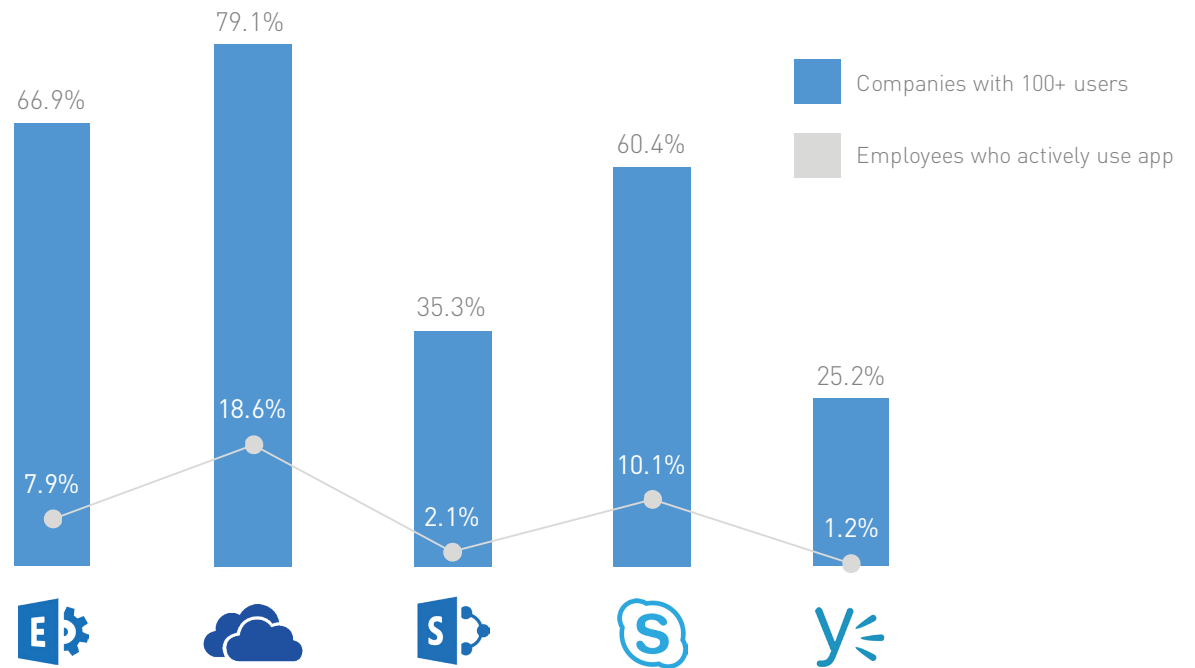
A man in a blue shirt is sitting at a white desk in a bright office, working on a laptop. The office has large windows with a view of a building with arched windows. The scene is overlaid with a blue tint. The text 'Chapter 1: Introduction' is displayed on the left side of the image.

Chapter 1:

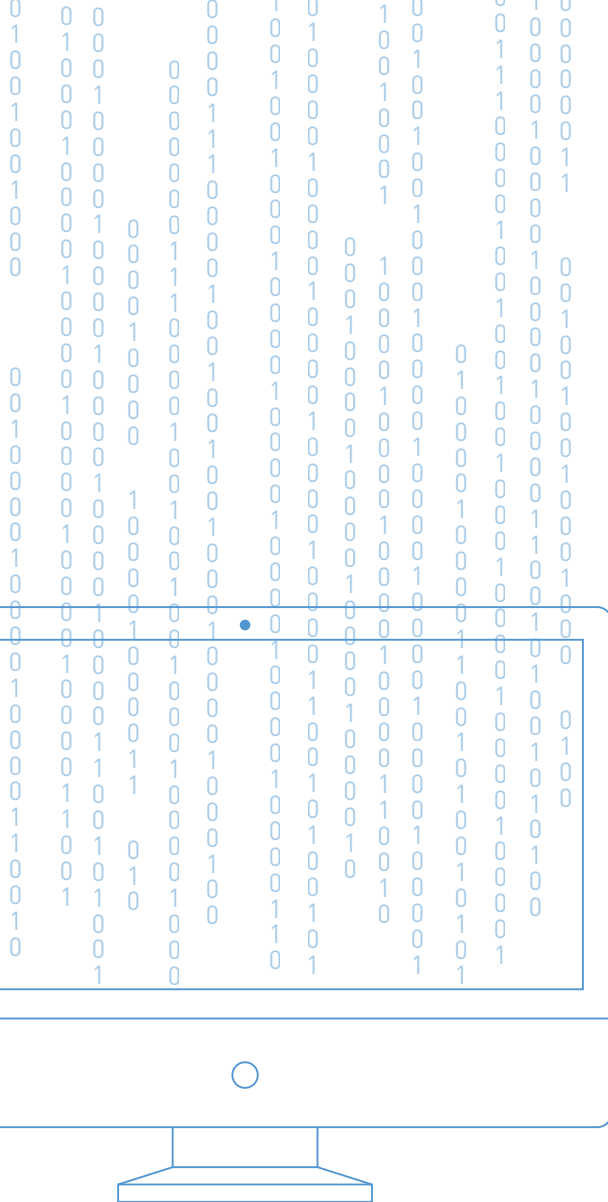
Introduction

As more enterprises adopt Office 365, new questions are arising about the security and compliance of corporate data. In moving to the cloud, enterprises outsource server management, upgrades, and datacenter operations to Microsoft. However, they only partially outsource their security responsibilities. Operating under a shared responsibility model, Microsoft takes responsibility for intrusions to the Office 365 platform. However, Office 365 customers are still responsible for actions users take that can expose corporate data to loss or create compliance violations.

Previously, when most corporate data lived in Windows file servers and on-premises applications, such as SharePoint, and collaboration was primarily done via Exchange Server, enterprises invested in a generation of security technology to enforce corporate policies and protect against threats.

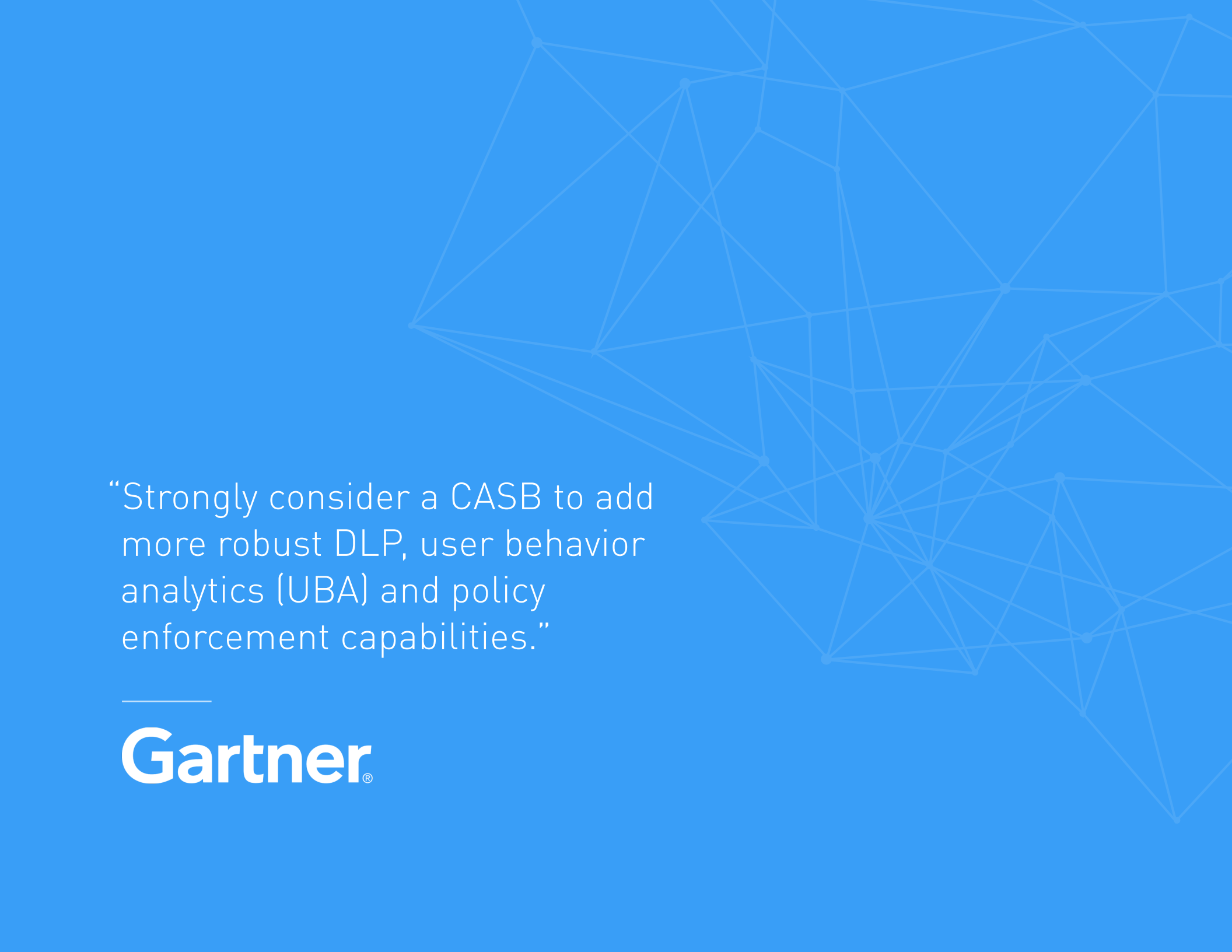


Office 365 Adoption by Application



Some of the security technologies enterprises deployed to protect on-premises applications and data stores include:

- Data loss prevention (DLP) to enforce external sharing policies and prevent the unintended disclosure of sensitive corporate data, primarily via email
- Intrusion prevention systems (IPS) to detect third-party compromise of corporate data, in some cases using compromised credentials
- Security incident and event management (SIEM) to record events and provide a tool for security analysts to perform forensic investigations
- User and entity behavior analytics (UEBA) to identify malicious or careless users via machine learning and big data analytics

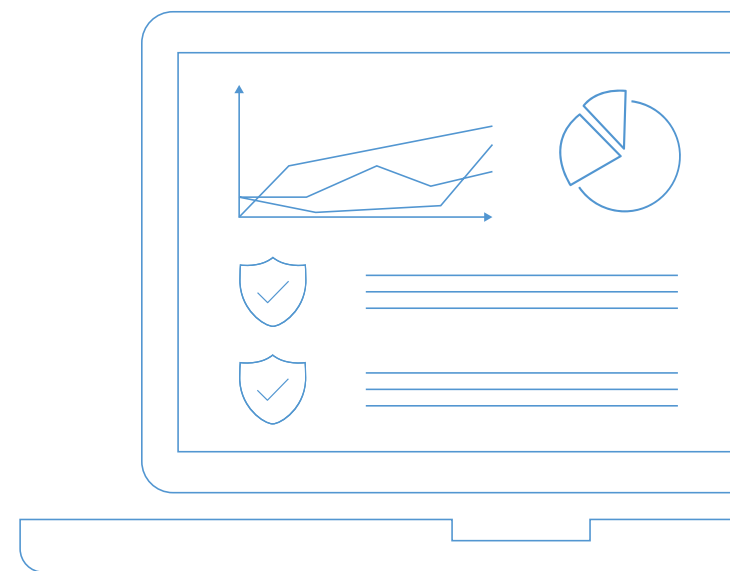


“Strongly consider a CASB to add more robust DLP, user behavior analytics (UBA) and policy enforcement capabilities.”

Gartner[®]

The ease of sharing and moving data to and from cloud applications has magnified the potential for judgement errors and exposed greater volumes of data to malicious users. Individually, some cloud providers have introduced limited controls that allow customers to enforce policies within a specific cloud application. However, the maturity of these tools varies widely (most are at an early stage of development). Additionally, all cloud provider security policy enforcement suffers from one major flaw—it requires the enterprise to maintain policies and perform remediation separately across multiple different platforms with different interfaces and workflows, creating siloes of security, inconsistent policy enforcement, and costly administrative overhead.

Enter the cloud access security broker (CASB). CASBs, such as Skyhigh, provide enterprises with a single, cross-cloud control point that consolidates many different security and compliance capabilities into a single platform. Skyhigh has helped hundreds of enterprises address their cloud security requirements, including 40% of the Fortune 500, and has broad experience helping enterprises ensure their Office 365 environments are secure and compliant. This extensive experience has revealed patterns in what use cases enterprises look to a CASB to solve. This e-book describes the seven most common Office 365 security and compliance use cases for a CASB and shows in detail how Skyhigh customers address them.





Chapter 2:

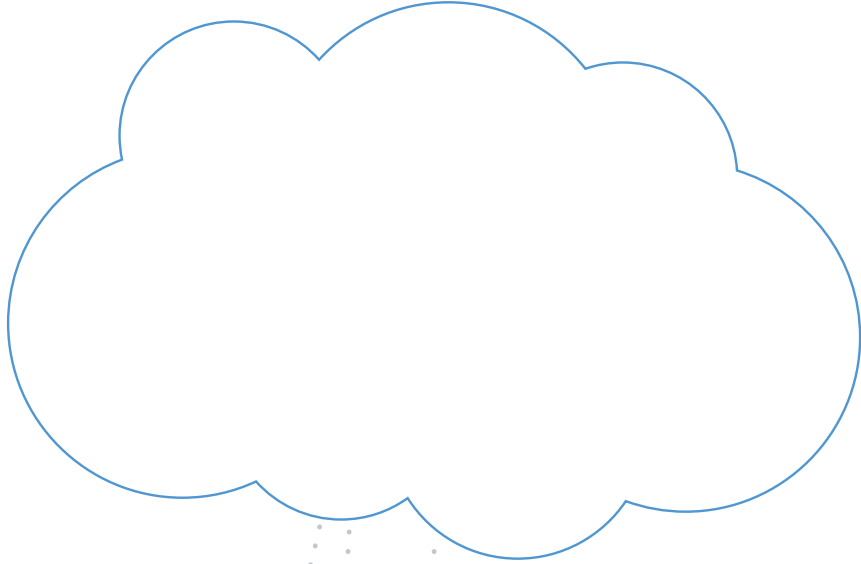
CASB Deployment Architectures



A cloud access security broker leverages several architectural modes to gain complete visibility and control over cloud services. In the case of Office 365, CASBs use the API, forward proxy, and reverse proxy modes. In API mode, a CASB connects directly to Office 365 via Microsoft’s APIs to gain visibility into usage and data and to enforce policies. In the two proxy modes, the CASB intermediates user-to-cloud sessions inline. The difference between a forward proxy and reverse proxy is the traffic steering mechanism. In forward proxy mode, a CASB uses network configuration or an endpoint agent to steer traffic through the proxy. In reverse proxy mode, the CASB uses routing

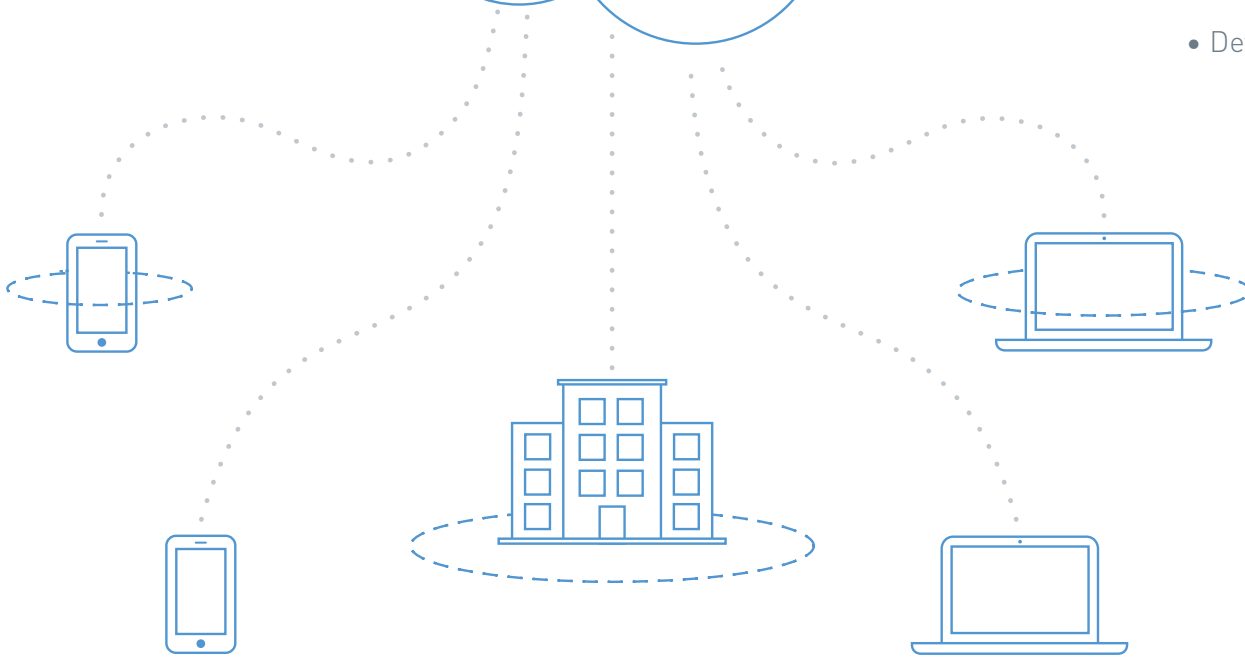
rules with the identify provider or a DNS redirect to steer traffic after authentication.

Each deployment mode offers sometimes substantially differing coverage for user access scenarios and support for cloud security controls. These limitations are inherent to the mechanism of enforcing controls and are independent of the CASB provider’s implementation. CASB customers generally deploy multiple architectural modes to achieve complete coverage, starting with the highest ROI deployment modes first (i.e. least user friction and broadest controls).

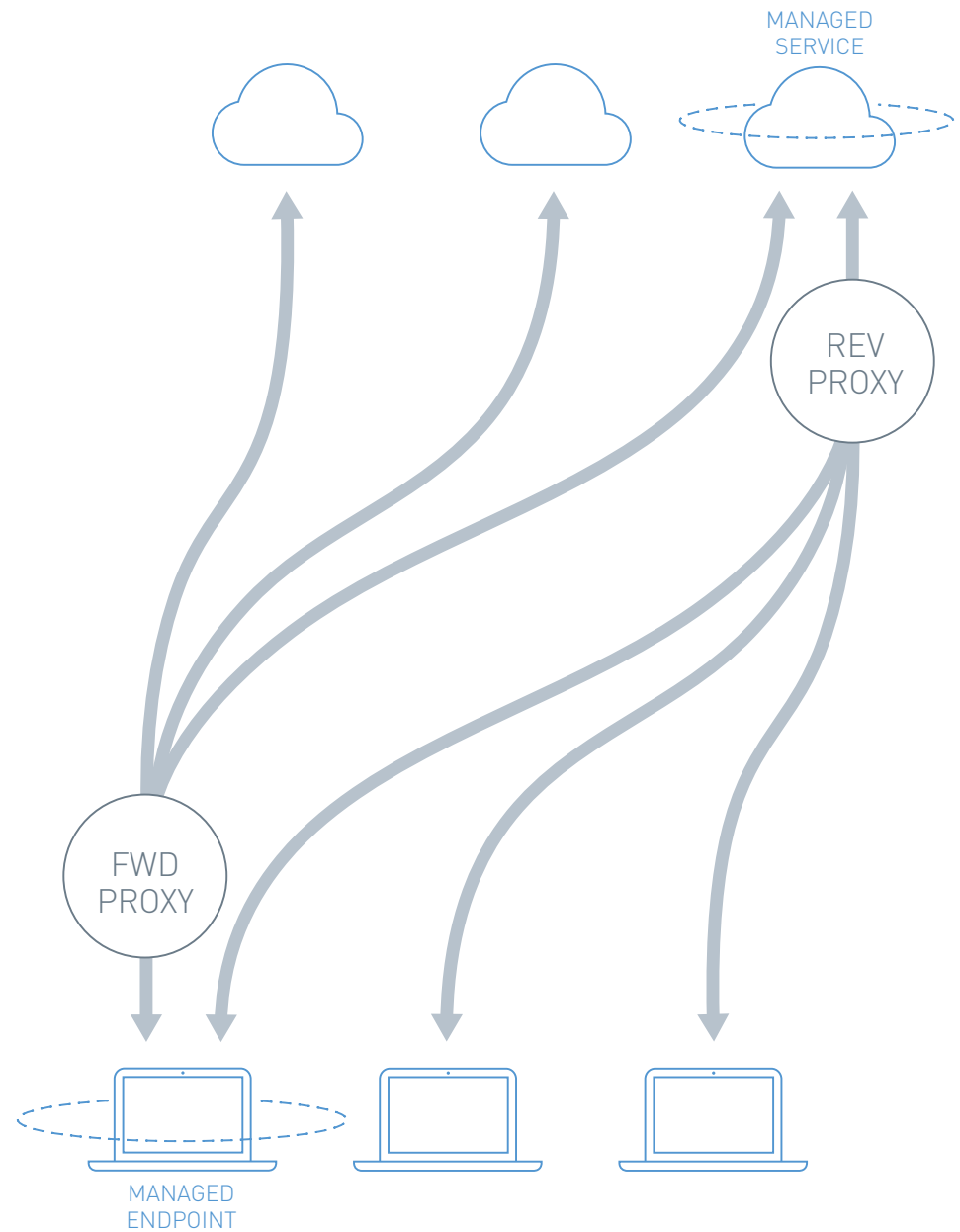


Skyhigh delivers complete Office 365 coverage by leveraging multiple deployment modes to cover all access scenarios including:

-
- Users (employees, third parties)
 - Network types (on-network, off-network)
 - Application experiences (web app, native app)
 - Device types (unmanaged and managed)



The proxy modes have several coverage limitations. Since steering traffic in forward proxy mode relies on network configuration or an endpoint agent, this mode does not offer coverage for third parties such as customers and partners. These users generally log in from off the corporate network using a device unmanaged by the enterprise. Similarly, employees that access Office 365 from unmanaged devices when travelling are also not covered, since an unmanaged device, by definition, does not have the enterprise's endpoint software deployed. Finally, proxying the usage of native applications presents a number of challenges in both forward proxy mode and reverse proxy mode.



	 MOST COMPLETE COVERAGE	API	Forward Proxy	Reverse Proxy
Users				
Employees		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Third parties (customers, partners)		<input type="radio"/>		<input type="radio"/>
Network types				
On network		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Off network		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Application experiences				
Web application		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Native application		<input type="radio"/>	<input type="radio"/>	
Device types				
Managed		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unmanaged		<input type="radio"/>		<input type="radio"/>

First, the reverse proxy mode only supports native applications that allow URL rewriting (e.g. Salesforce1) and therefore does not currently support Office 365 native applications. Proxies also have limitations that don't apply to Office 365 today, but could apply in the future. Neither proxy mode supports the ability to intermediate traffic from native apps that utilize certificate pinning, since the application only trusts certificates that are encoded into the application. Also, neither mode supports file sync and share apps that sync file changes progressively, rather than syncing the entire file each time an update is made. Neither of these limitations apply to Office 365 applications today, but application

developers are increasingly using both approaches in native apps, so they are important considerations as you think about how to future-proof your cloud security strategy.

Despite significant limitations of the proxy approach for most use cases, there are several key use cases, covered in this eBook, that absolutely require proxy mode deployments. In addition to user, network, application, and device coverage, in the following sections we'll provide an objective overview of how security capabilities vary between these deployment modes.

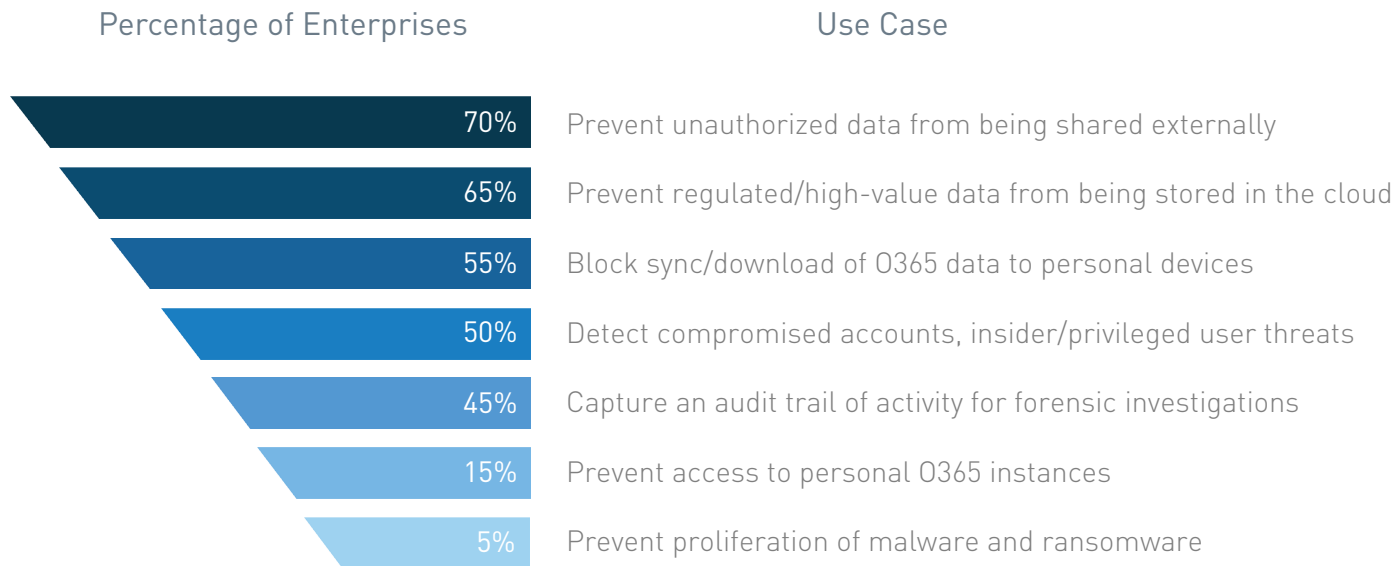
A person wearing a blue and white checkered shirt is sitting at a desk, holding a smartphone with both hands. The person is also wearing a watch with a blue face and a gold and black strap. On the desk, there is a laptop keyboard, some papers, and a pair of glasses. The background shows a chair with vertical stripes. The entire image has a blue tint.


Chapter 3:

Office 365 Use Cases for a CASB

Office 365 delivers a powerful set of collaboration tools and frees employees to access data from anywhere, using any device. However, these capabilities also introduce potential issues that enterprise security, risk, compliance, and audit teams have not faced before. After working with hundreds of enterprises to help address security and compliance requirements as corporate data migrates to Office 365, Skyhigh has surfaced the seven primary use cases enterprises look to fulfill with a CASB. Some use cases are more common than others, as summarized in this list in descending order of frequency.

In the following sections, we will describe each use case in detail, explain Skyhigh's approach to addressing the use case, and offer helpful evaluation criteria to use as you consider a CASB.





“We’re thrilled that Skyhigh is extending its cross-cloud security and governance solution to serve our Office 365 customers.”

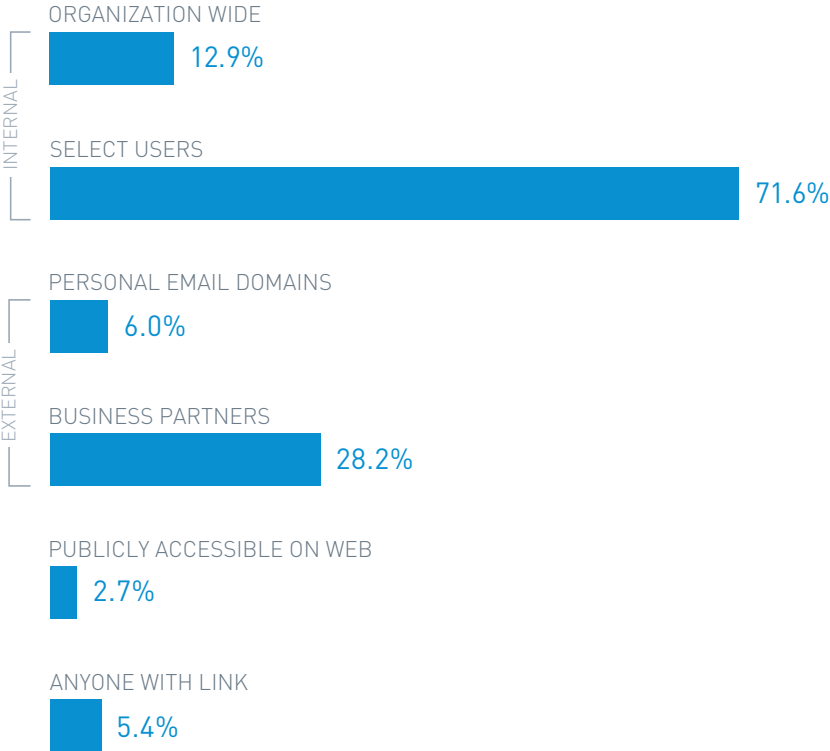
Microsoft

NAGESH PABBISSETTY, PARTNER GROUP PROGRAM MANAGER

PREVENT UNAUTHORIZED DATA FROM BEING SHARED EXTERNALLY

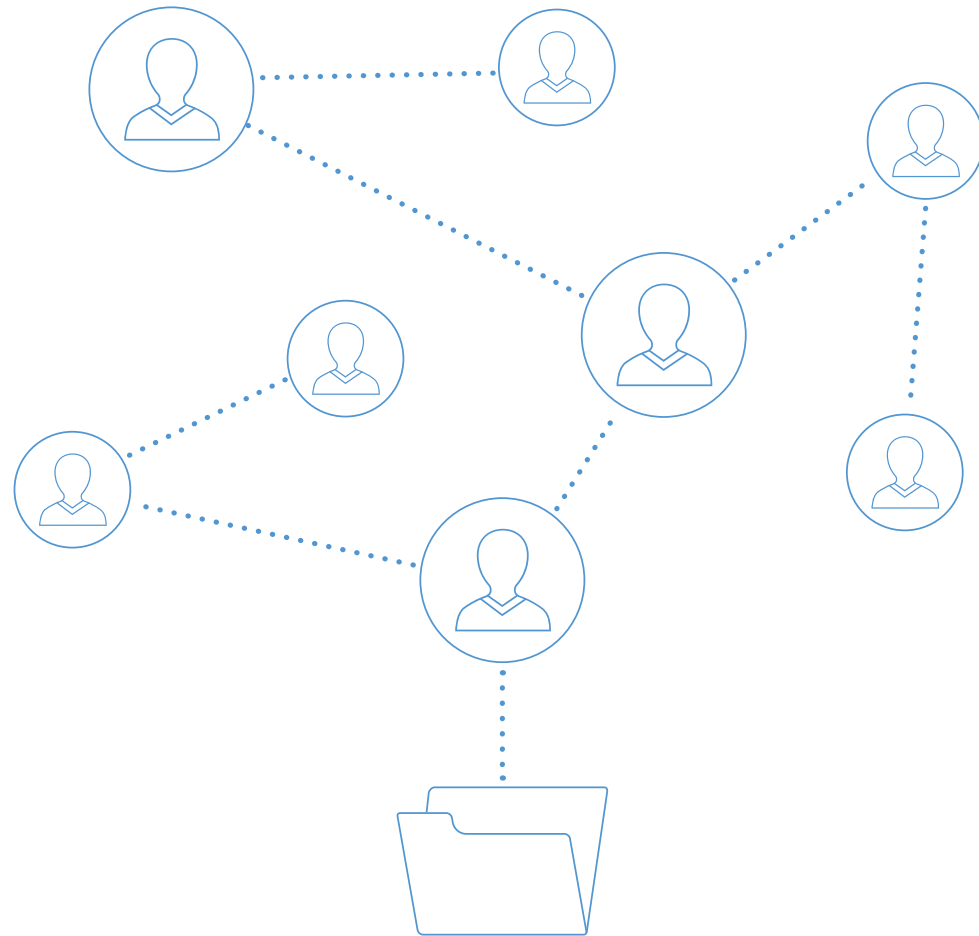
Formerly, email was the primary method of collaboration within and between enterprises. Today, using cloud-native tools such as OneDrive, employees share a significant amount of data with collaborators internally and with external suppliers, distributors, vendors, and customers. Cloud collaboration is replacing email as the primary way sensitive data leaves the enterprise. A small percentage of oversharing incidents are due to malicious users. Most incidents are due to well-intentioned employees who inadvertently expose corporate data.

Users can share files in three ways: 1) by inviting a user by the recipient's email, 2) by sending a link, or 3) by configuring the sharing policy to make a document publicly available and searchable. Analyzing the sharing permissions of files in the cloud, Skyhigh has found 28.3% of files are shared with email domains associated with business partners. However, another 6.2% are shared with personal email domains (e.g. gmail.com, yahoo.com), introducing questions about who has access to corporate data. And troublingly, 5.5% of files are shared using links that can be forwarded to anyone and the recipient's accessing the files cannot be traced, and 2.7% of documents are publicly accessible to anyone on the Internet.



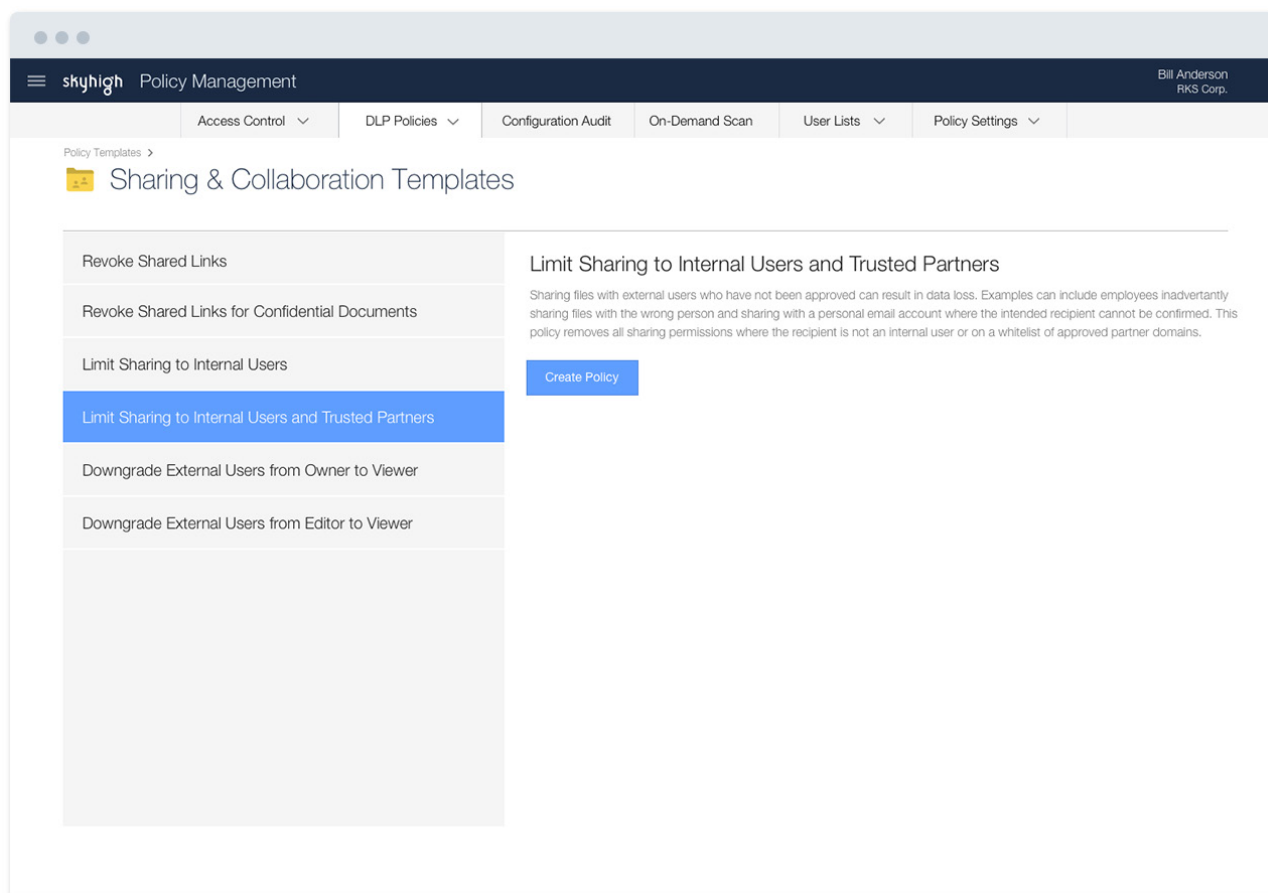
Sharing Permissions in OneDrive and SharePoint

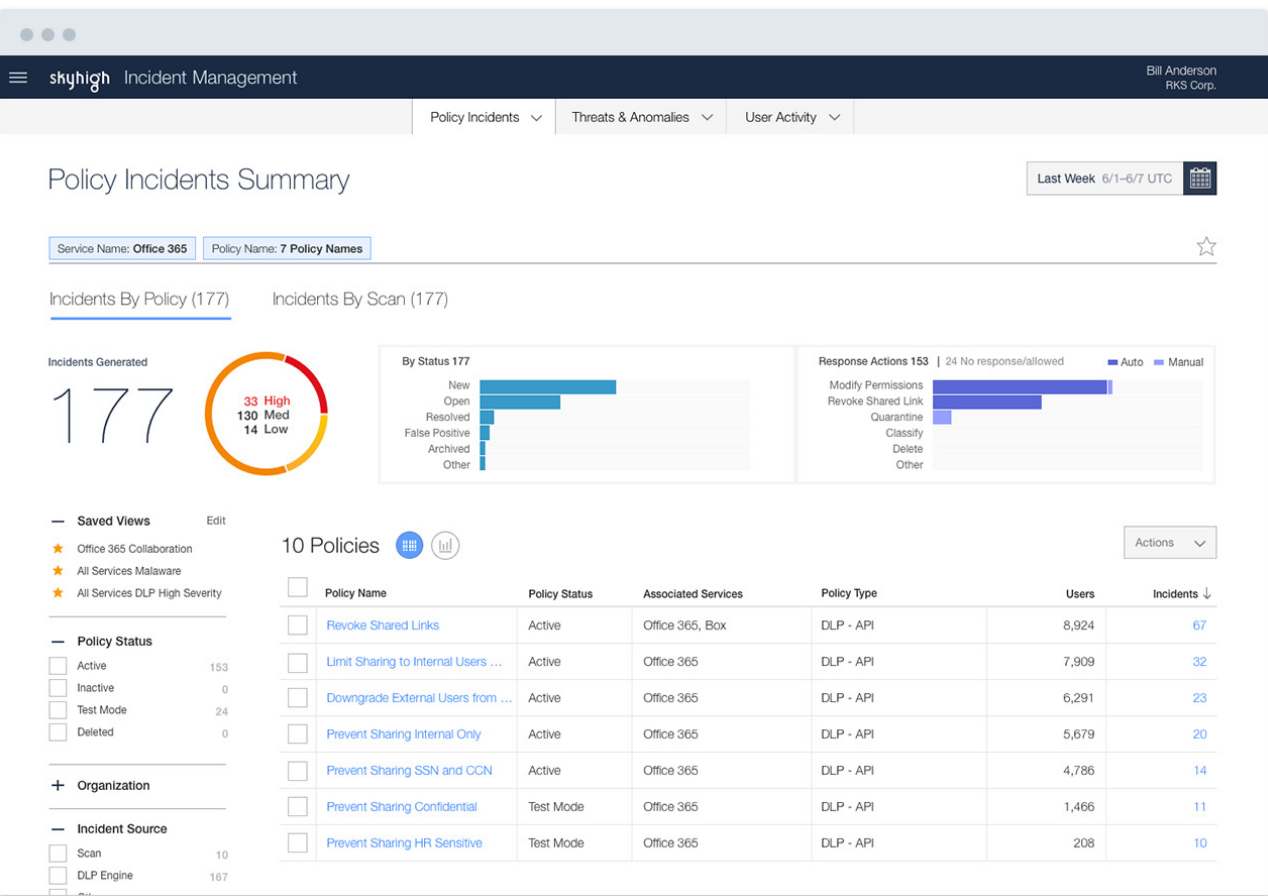
When sharing large volumes of sensitive data is just a few clicks away, it's easy for employees to mistakenly share files or folders too broadly with external users. It's also commonplace to type in a recipient's name and mistakenly select the incorrect individual or a personal email address from the autocomplete suggestions. Employees may also be sharing sensitive data externally, unknowingly violating policies. Depending on your corporate policies, you may have blanket rules about which business partners your organization's employees can share data with via Office 365. You may also have detailed policies on the type of content that can be shared with business partners.



How Skyhigh helps

Skyhigh provides guardrails to ensure appropriate sharing via content-aware data sharing policies in OneDrive and SharePoint Online that leverage a policy-based framework. Policies can include multiple rules, including whether a file is shared via a link or has external collaborators. Collaboration rules can trigger off the specific permissions assigned for the file or folder including viewer, editor, or owner. Some enterprises have a whitelist of acceptable external collaborators. For example, you may prohibit external sharing by default except with pre-approved business partners known to the organization, or prevent sharing with personal email domains such as those from Gmail or Yahoo! Mail.





In response to a policy violation, Skyhigh can take remedial action to correct the violation. Remediation actions include revoking a shared link and limiting the scope of sharing permissions (e.g. changing editors to viewers) or removing sharing permissions entirely. When content is shared externally, enforcement timing matters. An external user can download a file within seconds of receiving an invite to collaborate. Skyhigh's approach ensures that collaboration policies are enforced in real-time before the sharing action is fully executed within the Office 365 platform, preventing the unintended disclosure of corporate data outside of policy.

Skyhigh policies can be targeted to specific user groups within the organization based on Active Directory attributes. Skyhigh's DLP policy framework also supports combining collaboration rules with content-aware rules within a single policy. For example, you may want to allow collaboration with business partners but prevent sensitive intellectual property from being shared. These policies may be configured in Skyhigh's DLP engine or an on-premises DLP solution such as those from Symantec, EMC RSA, Intel McAfee, and Websense. For more details on content-aware policies, see the next use case on uploading regulated and high-value data.


Required CASB capabilities:

- ✓ Collaboration-aware engine for files and folders
- ✓ Ability to integrate DLP policies with collaboration policies
- ✓ Ability to detect and revoke shared links
- ✓ Whitelist/blacklist of approved/unapproved collaborators
- ✓ Ability to detect specific permission level and modify
- ✓ Real-time sharing remediation
- ✓ Integration with AD, on-premises DLP systems, and SIEMs

How it works: Deployment Architecture

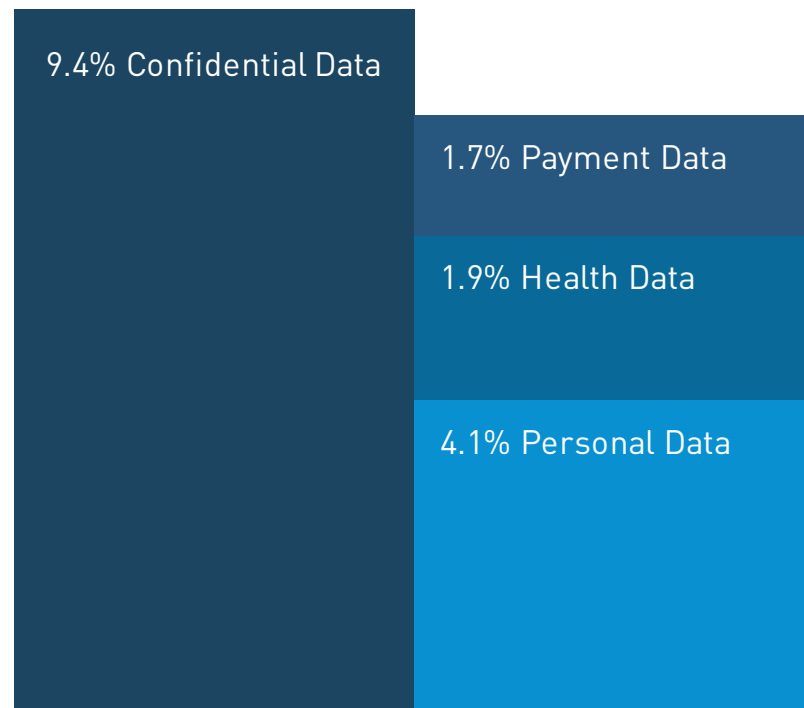
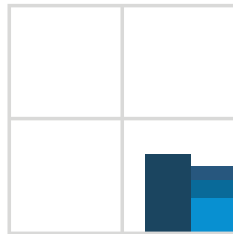
Collaboration actions users take on files and folders in Office 365 are cloud-centric in nature. Therefore, the only way to gain visibility into these actions and enforce policy controls is via API. Forward and reverse proxy do not support deep collaboration controls for Office 365 because they do not have visibility into the full context of sharing in the cloud and may not have visibility into the content of the file.

	API	Forward Proxy	Reverse Proxy
Policy rule triggers			
Invite users to files/folders	●		
Generate shared links	●		
Remediation actions			
Modify sharing permissions	●		
Revoke shared links	●		

 MOST COMPLETE COVERAGE

17.1%

of files in OneDrive and SharePoint Online contain sensitive data



PREVENT REGULATED, HIGH-VALUE DATA FROM BEING STORED IN THE CLOUD

In a growing sign that enterprises trust Microsoft to protect their sensitive data (or perhaps that users are operating unaware of their organizations' cloud policies) Skyhigh has found that employees upload a significant amount of sensitive data to Office 365. Analyzing the data loss prevention policies customers implement using Skyhigh, we found that, on average, 17.1% of files an enterprise stores in OneDrive and SharePoint Online are sensitive.

Depending on your organization's compliance and security posture, your policies may dictate this information can be stored in Office 365 provided it is not shared inappropriately. But, many companies have high-value or regulated data they wish to prevent from living in the cloud. And, regardless of compliance requirements, some types of data are simply unfit to be stored in the cloud. For example, Skyhigh has found the average enterprise stores 204 files containing user passwords in OneDrive. These files often take the form of a Word or Excel document with usernames and passwords for all the applications and devices an employee uses.

Preventing regulated or high-value data from being stored in the cloud is a two-part problem: 1) detecting sensitive data and 2) enforcing controls to prevent this data from living within Office 365. Identifying sensitive data is not a trivial undertaking because it often requires going beyond simple keyword matching.

Consider the following real-world examples of sensitive content that enterprises rely on a CASB to detect and prevent from being stored in Office 365 or shared inappropriately:

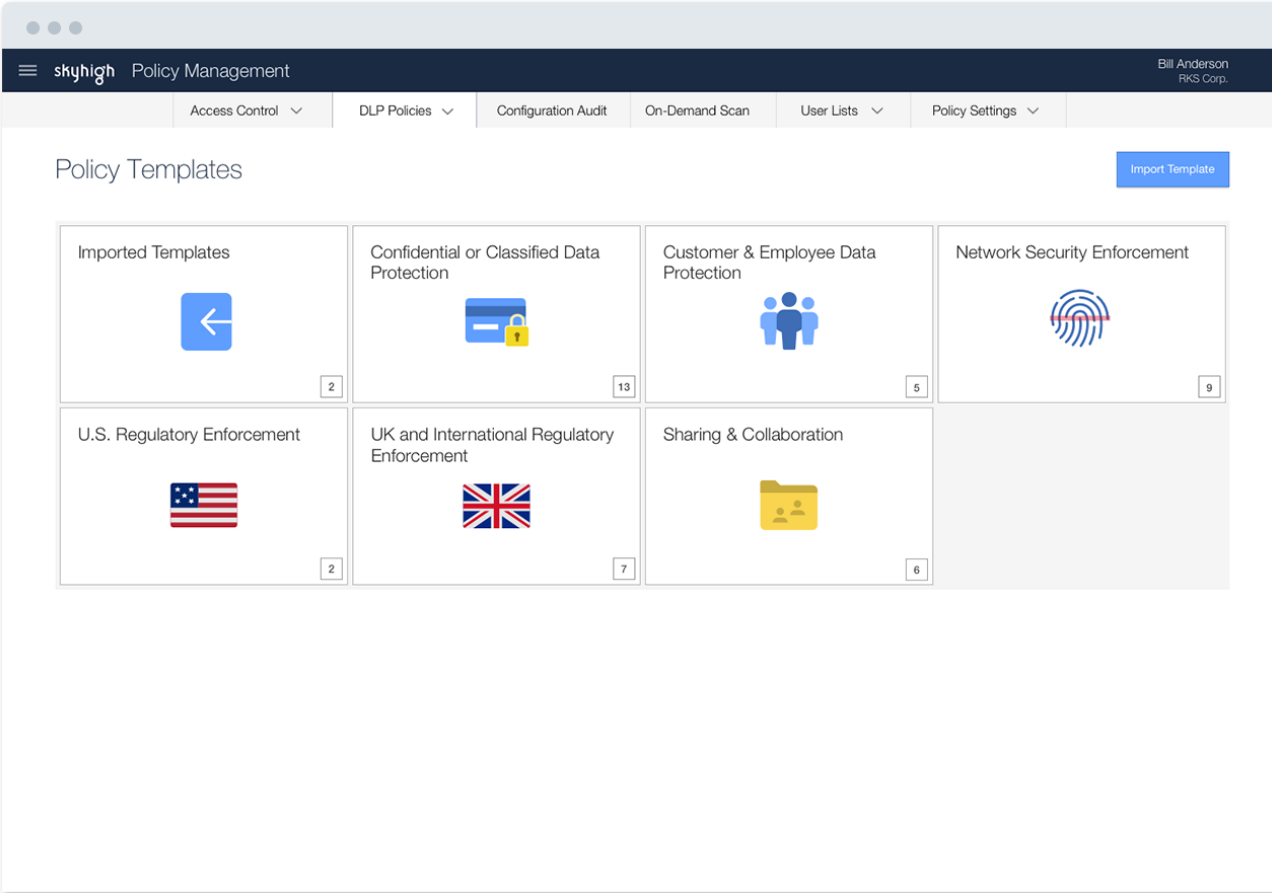
-
- A lexicon containing hundreds or thousands of keywords that are common across several different corporate policies (e.g. prescription drug names, stock symbols)
 - Data classification tags applied by classification technologies that appear in the metadata of files (e.g. confidential, internal only)
 - Standard alphanumeric patterns that follow a set of defined rules such as length, prefix or suffix, or checksum (e.g. Social Security numbers, credit card numbers)
 - Custom alphanumeric patterns that are unique to the organization and follow a set of defined rules (e.g. parts numbers, product SKUs)
 - All versions of a specific, sensitive document including the exact file or any derivative of the file (e.g. design document for production process, legal contract)
 - Any piece of content that refers to current or former customers (e.g. any field from a structured database with personal data on 300 million customers)

When deploying data loss prevention technology, enterprises want to simultaneously minimize the number of sensitive files missed by the system (false negatives) and minimize the number of non-sensitive files flagged by the system (false positives). A CASB uses a variety of technologies to match the above sensitive content types and enforce policies.

How Skyhigh helps

Skyhigh delivers a robust content-aware DLP engine with comprehensive remediation and reporting. Many organizations have standard data loss and compliance scenarios and Skyhigh includes dozens of off-the-shelf DLP templates for common use cases such as HIPAA compliance and M&A documents. These policies are customizable, or you can create your own unique DLP policies using a flexible policy framework that leverages Boolean logic to combine two or more rules and associated remediation actions.

DLP policies can contain rules leveraging document metadata and content including file attributes, keywords, keyword dictionaries, document classification tags, data identifiers, regular expressions, and fingerprinting of structured databases and unstructured files.



The screenshot displays the Skyhigh Policy Management interface. At the top, there is a navigation bar with the Skyhigh logo and 'Policy Management' text. On the right side of the navigation bar, the user's name 'Cameron Coles' and 'shdemo' are visible. Below the navigation bar, there are several menu items: 'Access Control', 'DLP Policies', 'Configuration Audit', 'On-Demand Scan', 'User Lists', and 'Policy Settings'. The main content area is divided into three sections: 'Rules', 'Exceptions', and 'Response'.

Rules Section: This section is titled 'Rules' and includes a sub-header 'Match ANY group within a policy'. It features a 'Severity' dropdown menu set to 'Medium'. Below this, there is a 'Data Identifier' dropdown set to 'Credit Card Number', a 'Location' dropdown set to 'All', and a 'Match Count' input field with the value '1'. There are also checkboxes for 'Keyword validation' (checked) and 'Exclude'. An 'Add Rule Group' button is located at the bottom right of this section.

Exceptions Section: This section is titled 'Exceptions' and includes a sub-header 'Match ANY group within a policy'. It contains an 'Add Exception' dropdown menu and an 'Add Exception Group' button at the bottom right.

Response Section: This section is titled 'Response' and includes a sub-header 'Match ALL rules within a group'. It features a conditional rule: 'If Any severity then Incident'. Below this, there is another conditional rule: 'If Medium severity then Quarantine using Select Email Template'. An 'Add action' button is located at the bottom left of this section.

These rules can be combined in nested groups connected with AND and OR logic. Also, rule sets support an associated severity. For example, if a document contains one credit card number, the violation severity can be set to “medium” and if it contains 100 or more violations the severity can be set to “high”, and since remediation actions within a policy can be tiered based on severity, you can define a policy, such as “quarantine files with high severity violations but only alert users for files with low severity violations”. Skyhigh also supports integration to on-premises DLP solutions from Symantec, EMC RSA, Intel McAfee, and Websense to leverage existing policies.

Skyhigh can target DLP policies to specific user groups, business units, roles, or departments by pulling user information from directory services that support LDAP, such as Microsoft Active Directory. For example, you can target a DLP policy to a specific department, or to all users with a specific role. Policies can also exclude specific groups.

Skyhigh supports numerous automated remediation actions in response to DLP policy violations. Depending on the deployment architecture, Skyhigh can enforce policies via blocking, quarantining, deleting, coaching, and notification.

The screenshot displays the Skyhigh Incident Management interface. At the top, there are navigation tabs for 'DLP Incidents', 'Threats & Anomalies', and 'User Activity'. The main heading is 'Policy Violations from Office 365'. Below this is a table with 17 rows of violations. The table columns are: POLICY, OBJECT, RESPONSE, STATUS, DATE, USER, and SERVICE. A detailed view on the right side shows the details for a specific violation: 'Credit Card Number/s - API' on Oct 26, 2016. It indicates that 10 matches were found on a file named '10 Unique CCNs in the Wild 2_mark.docx' uploaded to OneDrive. The status is 'Allowed' and the original file was 'Allowed'. There are dropdown menus for Status (set to 'New'), Owner (set to 'None'), and Response (set to 'Select Response'). The content section shows the type as 'File' and the location as '/personal/demo_shnpocdemo_com/Doc...'. It also displays a snippet of the content with 10 matches found, including a credit card number and a Visa account number.

POLICY	OBJECT	RESPONSE	STATUS	DATE	USER	SERVICE
Credit Card Number/s - API	10 Unique CCNs in the Wild 2_mark.docx	Allowed	New	Oct 26, 2016 3:17 PM PDT	demo@shnpocdemo.com	OneDrive
Credit Card Number/s - API	10 Unique CCNs in the Wild.docx	Allowed	New	Oct 26, 2016 2:44 PM PDT	demo@shnpocdemo.com	OneDrive
Credit Card Number/s - API	50 Unique CCNs in the Wild.docx	Quarantined	New	Jul 15, 2016 1:40 AM PDT	michael@skyhighdemo19.onmicrosoft.com	OneDrive
Credit Card Number/s - API	10 Unique CCNs in the Wild.docx	Allowed	New	Jul 15, 2016 1:40 AM PDT	michael@skyhighdemo19.onmicrosoft.com	OneDrive
Resume upload detected and removed	Resume - Bill Matson.docx	Quarantined	New	May 18, 2016 1:37 PM PDT	Bill Matson	OneDrive
DLP Policy for Confidential data(DLP for data in motion, via API)	Confidential.doc	Quarantined	New	May 5, 2016 1:24 PM PDT	Allision Reed	Sharepoint
DLP Policy for Confidential data(DLP for data in motion, via API)	M&A.doc	Quarantined	New	May 5, 2016 1:23 PM PDT	Allision Reed	Sharepoint
US Social Security Numbers (DLP for data in motion, via API)	Social Security List	Quarantined	Resolved	May 5, 2016 1:18 PM PDT	Bill Matson	OneDrive
(On Demand Scan) File names containing Password	mwg_72_pg_product_700-3883a00_en-us.pdf	Allowed	Resolved	May 4, 2016 1:27 PM PDT	dheeraj@skyhighdemo28.onmicrosoft.com	OneDrive

Skyhigh's review interface provides full context of the violation including the user, file name, and a highlighted excerpt showing the content that triggered the violation. Depending on the deployment mode, a compliance reviewer can also take manual action. For example, some enterprises choose to run DLP policies in a monitor-only mode. If during review the compliance user decides action is required, she can quarantine or delete the file from the review interface. Both automated and manual remediation can be rolled back if required to restore a file. For all deployment modes, incidents can be marked with status and owners for follow up.


Skyhigh also integrates with SIEMs via syslog to provide a real-time feed of DLP violations so that enterprises can leverage pre-existing DLP incident workflows.

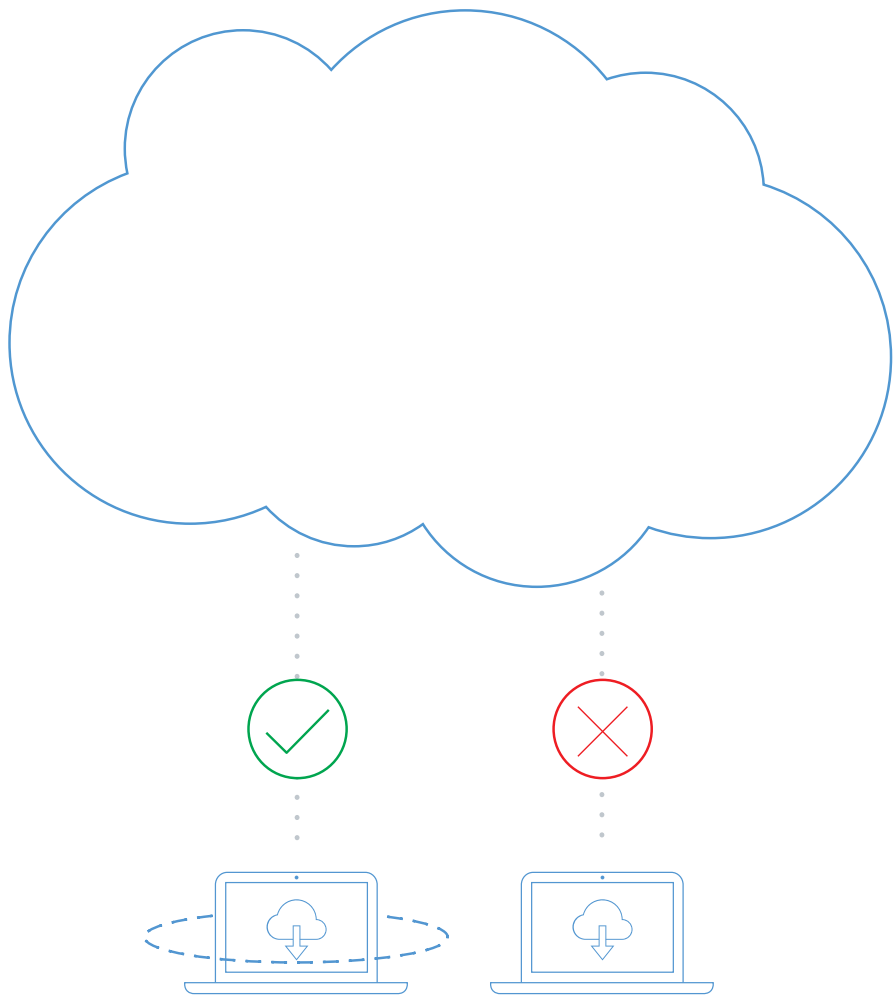
Required CASB capabilities:

- ✓ Content-aware DLP engine
- ✓ Fingerprinting of structured and unstructured data
- ✓ Pre-built policy templates for PCI, HIPAA, GDPR, etc.
- ✓ Policy tuning with monitor mode and preview
- ✓ Remediation workflow including match highlighting
- ✓ Stores no sensitive customer data
- ✓ Sub-minute response times
- ✓ Scale for cloud data volumes
- ✓ Severity-based remediation, including rollback
- ✓ Integration with AD, on-premises DLP systems, and SIEMs

How it works: Deployment Architecture

While either the API or inline proxy modes can support scanning new files, inline proxy modes do not support scanning data that is already stored at rest because they sit inline and only have visibility into data as it is uploaded to Office 365. To scan pre-existing data, a CASB must integrate to Office 365 via API with permissions to scan existing content. All CASB modes support scanning files uploaded to the cloud, but only the API mode supports scanning content created natively within the cloud applications such as Word Online and Excel Online because a proxy cannot enforce policies as content is typed character-by-character into the browser.

	API	Forward Proxy	Reverse Proxy
 MOST COMPLETE COVERAGE			
Data			
Pre-existing	●		
New data	●	●	●
Creation method			
Uploaded	●	●	●
Cloud-native (e.g. Word Online)	●		
Remediation actions			
Block		●	●
Quarantine	●		
Delete	●		
Coach user	●		
Notify administrator	●	●	●



BLOCK DOWNLOAD OF O365 DATA TO PERSONAL DEVICES

One of the key advantages of Office 365 is the ability to extend productivity tools to employees no matter where they are or what device they use. In an earlier era, VPN was required to access enterprise applications running in the corporate datacenter. This requirement necessitated users to log in from managed devices that had the corporate VPN installed. Now that employees can access corporate data in Office 365 from personal devices, new risks are emerging to corporate data. One issue is that when data is downloaded or synced to a personal device, information leaves the company when the employee leaves.

An even greater concern is information falling into the wrong hands due to a lack of endpoint security controls. Personal devices that are unmanaged lack enterprise endpoint security that enforces device policies such as drive encryption and device PIN. If that device is stolen—for instance, when an employee is working from a coffee shop or if a laptop is left in the backseat of a car—corporate data is also stolen. Without endpoint security, the enterprise is unable to remotely wipe the data, which may not be protected at all on the endpoint. For these reasons, many enterprises want to allow employee access to the collaboration tools in Office 365 from any device, but limit the ability to download corporate data to only managed devices.

How Skyhigh helps

When users access Office 365, Skyhigh performs a certificate check to validate the device has appropriate endpoint security in the form of an EMM/MDM solution. Skyhigh also goes one step further by integrating with EMM/MDM providers to pull a mapping of users and their trusted devices and validates that not only does the endpoint have a certificate, but that the user is accessing from a known device and not another device. This second-level check ensures that a malicious user or third party has not spoofed a certificate on an untrusted endpoint in order to circumvent device policies.

The screenshot displays the 'Edit Cloud Access Policy' interface in the Skyhigh Policy Management console. The page is titled 'Edit Cloud Access Policy' and includes a 'Required Fields' indicator. The configuration is as follows:

- Name:** Personal devices blocked from download (read only access)
- Description:** (Empty text area)
- Implementation:** ON (toggle) and Monitor only mode (checkbox)
- Conditions:**
 - Device is Unmanaged
 - Service is Microsoft Office 365 and OneDrive
 - Activity is Download
- Action:** Block Access

Helpful text on the right side of the interface:

- Name your policy:** Choose whether it will be implemented using Skyhigh's reverse proxy or API connection. This selection limits the types of Activities that can be specified as conditions.
- Specify the conditions that will trigger this policy:** For example, you can specify which services (or categories), the types of users (referencing your custom attributes), managed or managed devices, and various activities and content types.
- Specify what you would like to occur when the above conditions are met.**

Buttons for 'Save' and 'Cancel' are located at the bottom right of the form.

Blocking download necessitates intermediating the user's session with a proxy, not just the login event. As discussed in the architecture section, personal, unmanaged devices can only be intermediated by a reverse proxy and not a forward proxy. However, while reverse proxies can intermediate logins to the web app and native app, they can only intermediate the usage (and therefore enforce download controls) for the web app.

Skyhigh solves this by enforcing a "no access" policy for unmanaged devices across native O365 applications, and a "view but no download" policy for unmanaged devices across web applications. Customers use Skyhigh to block access to corporate Office 365 instances via the native application on personal devices, while permitting web application access. By proxying the session to the web application, Skyhigh can allow employees to preview data and edit files in Word Online, Excel Online, and PowerPoint Online while preventing files from being downloaded to the endpoint.

Skyhigh can also perform detect device management status with a SAML assertion passed by the identity provider users log in to Office 365 with.


Required CASB capabilities:

- ✓ EMM/MDM certificate check
- ✓ Second-level user/device mapping check
- ✓ SAML traffic routing to reverse proxy

How it works: Deployment Architecture

When a file is downloaded or synced, there is no pause for an API call so enforcing a download policy requires the CASB to sit inline between the user and the cloud application. Since a personal device is unmanaged, and therefore traffic is not being routed via an endpoint agent, this control requires the reverse proxy mode. When a user accesses Office 365, Skyhigh checks the certificate and if it is a personal device it blocks access to the native application and proxies traffic to the web application. Sitting inline in reverse proxy mode, Skyhigh blocks download whenever a user attempts a download a file. If the device is managed, Skyhigh's reverse proxy gets out of line to allow direct access from the user to Office 365.

	API	Forward Proxy	Reverse Proxy
Certificate check on unmanaged devices			<input type="radio"/>
Block access to native application			<input type="radio"/>
Block download from web application			<input type="radio"/>

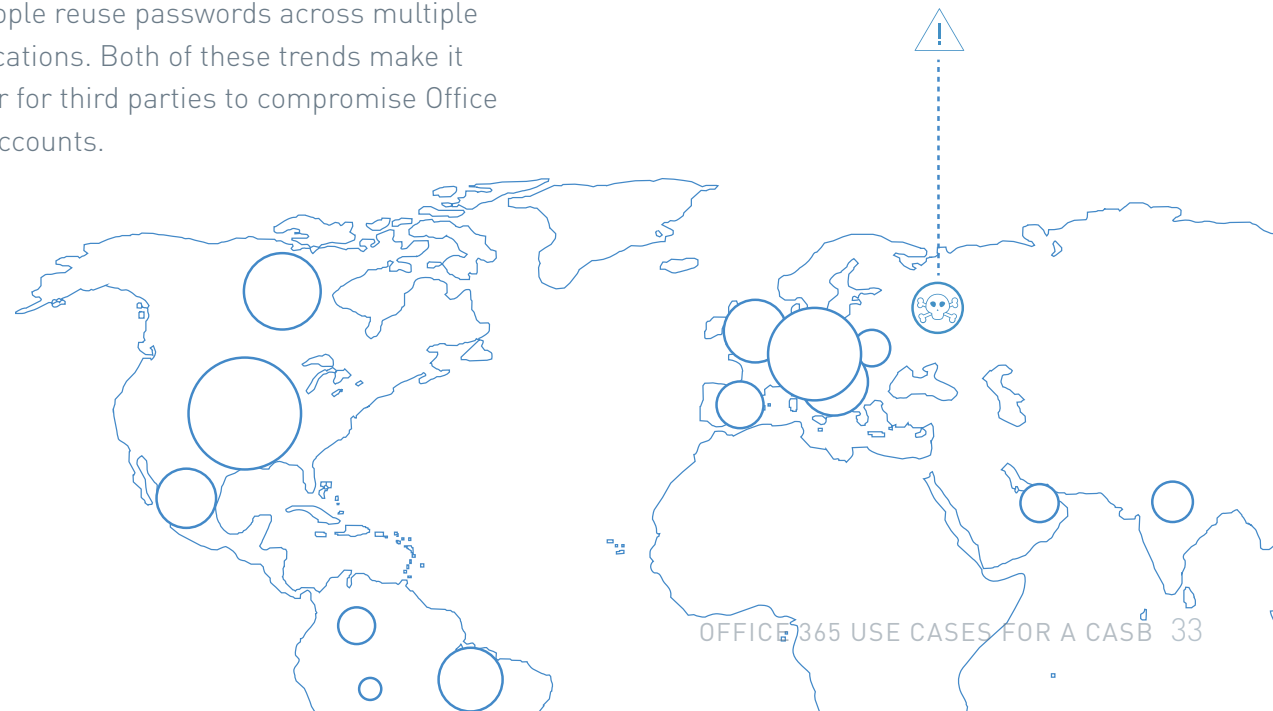
 MOST COMPLETE COVERAGE

DETECT COMPROMISED ACCOUNTS AND INSIDER/PRIVILEGED USER THREATS

Office 365 customers are responsible for actions users take within the platform that compromise data, and Skyhigh has found the average enterprise experiences 2.7 such threats in the platform each month. This number includes compromised accounts, insider threats, and privileged user threats. Insider threats can generate headlines. In a lawsuit Google subsidiary Waymo filed against Uber in February 2017, the company alleges a former Google employee downloaded 14,000 sensitive documents related to self-driving car technology before leaving the company. The former employee subsequently led the self-driving car project for Uber and Uber's technology bears a striking resemblance to components developed by Waymo.

Compromised accounts are also a significant threat. Cyber criminals gain access to corporate Office 365 accounts by

exploiting stolen user credentials gathered via phishing attacks, passwords leaked from other cloud services that an employee reuses for Office 365, and guessing common passwords. Analyzing stolen passwords for sale on the Darknet, Skyhigh found the top 20 most common passwords, which include "123456" and "password", account for 10.3% of all passwords. Furthermore, research by Joseph Bonneau at the University of Cambridge has found that 31% of people reuse passwords across multiple applications. Both of these trends make it easier for third parties to compromise Office 365 accounts.



5,451,908

Total events
per month

256

Anomalous
events per
month

2.7

Threats
per month

Detecting threats is challenging because, while they are often signaled by behavior patterns that are anomalous, there's no single threshold that can be applied to all users for all time frames that will accurately detect these threats while not also generating many false positives. For instance, it may be unusual for a one user to download a series of documents with company financial performance at home on the weekend, while it may be normal for another user to periodically download the most recent of these documents on the last Friday of each month.

Alert fatigue is a serious issue. In a survey of IT security professionals, 31.9% report that they ignore alerts because so many are false positives.¹ User and entity behavior analytics (UEBA) technology leverages machine learning to overcome many of these challenges, and CASBs can make use of this technology to accurately detect threats. UEBA technology builds models of user behavior that can accurately detect deviations from behavioral norms that signal insider threats, privileged user threats, and compromised accounts.

¹ Cloud Security Alliance "IT Security in the Age of Cloud"

skyhigh Incident Management Cameron Coles
shdemo

DLP Incidents ▾ Threats & Anomalies ▾ User Activity ▾

Threats from Office365 ▾ ⓘ Threat Protection Paused

Compromised Accounts: 17 Insider Threats: 8 Privileged Access: 2 All Anomalies: 914

Threats 25 | All Anomalies 914 CSV

THREAT	USER	SERVICE	DATE
Insider Threats 15 Insider Data Exfiltration	sallyburton@rks.com	Office365	Jul 19, 2016 9:05 AM
Data Download	sallyburton@rks.com	OneDrive	Jul 19, 2016 9:05 AM
Data Download	sallyburton@rks.com	SharePoint	Jul 21, 2016 9:05 AM
Data Download	sallyburton@rks.com	OneDrive	Jul 22, 2016 6:13 AM
Data Sharing	sallyburton@rks.com	OneDrive	Jul 22, 2016 6:13 AM
Data Access	sallyburton@rks.com	OneDrive	Jul 22, 2016 6:13 AM
Data Sharing	sallyburton@rks.com	OneDrive	Jul 22, 2016 6:05 AM

LOW SEVERITY

Data Download
Jul 21, 2016 9:05 AM

Description

Details
User activity (12 weeks UTC)

● User Activity ● Anomaly Threshold ● Anomaly

Anomaly Category: Data Anomalies
Activity Name: File downloaded
No. of Activities: 114 [Download CSV](#)
Anomaly Threshold: 50
Threshold Duration: weekly
Anomaly Generated: Jul 21, 2016 (9:05 AM)

How Skyhigh helps

Skyhigh accurately detects insider threats, privileged user threats, and compromised accounts leveraging machine learning. Unlike threshold-based solutions that require enterprises to define policies that detect activity outside an arbitrary static threshold, Skyhigh connects to Office 365 and immediately begins building behavior models based on actual user activity. In doing so, the solution can begin detecting threats automatically without any input from an administrator using an approach known as “unsupervised learning”.

Cloud threats can involve the use of multiple cloud services. Skyhigh cross-references activity in Office 365 with other cloud services in order to detect threats. For example, a user who logs in to Salesforce from New York City and then five minutes later logs in to OneDrive from London may indicate a compromised account since it would be impossible to travel this distance in such a short time frame. Downloading a significant amount of corporate data from SharePoint and then uploading the content to an anonymous file sharing service may also indicate an insider threat.

Recognizing that security incidents often involve more than one signal, Skyhigh leverages a threat funnel that combines

multiple anomalous events together into a higher-order threat object before generating an alert. For example, a user who successfully logs in after several failed attempts may not require attention, unless the user is also logging in from a new location and exhibits behavior that deviates from their usual pattern, more strongly indicating account compromise. By focusing IT security analysts on the highest probability incidents, the solution reduces the potential for alert fatigue. Investigators can also view all single-event anomalies.

While unsupervised learning makes it easy to get started, over time enterprises often want to provide input to fine tune alerts. Skyhigh delivers three ways for security analysts to provide feedback to models of behavior, known as “supervised learning.” When reviewing incidents, marking an alert as a false positive is incorporated into behavior models. Analysts can also whitelist specific users or types of events to suppress them. For example, if an IT administrator is tasked with cleaning up dormant accounts and deleting large numbers of them, this activity can be suppressed for the user. Finally, Skyhigh supports adjusting sensitivity with a real-time preview of how the adjustment would change the anomalies detected by the system, so security can optimize the balance between true positives and false negatives.

Skyhigh offers a comprehensive incident review and remediation interface for all cloud threats and also supports sending threat incidents to a SIEM via syslog.


Required CASB capabilities:

- ✓ Multi-event threats not single-event anomalies
- ✓ Machine learning to obviate arbitrarily defined thresholds
- ✓ Whitelisting of low-risk users or known events
- ✓ Incorporating “false positive” feedback
- ✓ Sensitivity adjustment with real-time preview
- ✓ SIEM integration via syslog feed

How it works: Deployment Architecture

The API deployment mode offers the most complete coverage for threat protection use cases. Privileged user threats and administration anomalies are not fully supported by an inline proxy because the context of the user's permissions are not available. Furthermore, when an unauthorized third party attempts to connect to Office 365 using compromised login credentials, a forward proxy does not have the ability to see this traffic since it generally originates off the corporate network from an unmanaged device.

	API	Forward Proxy	Reverse Proxy
Threat category			
Insider threat	●	●	●
Privileged user threat	●		
Compromised account	●		●
Anomaly detection			
Data Anomalies	●	●	●
Access Anomalies	●		●
Administration Anomalies	●		

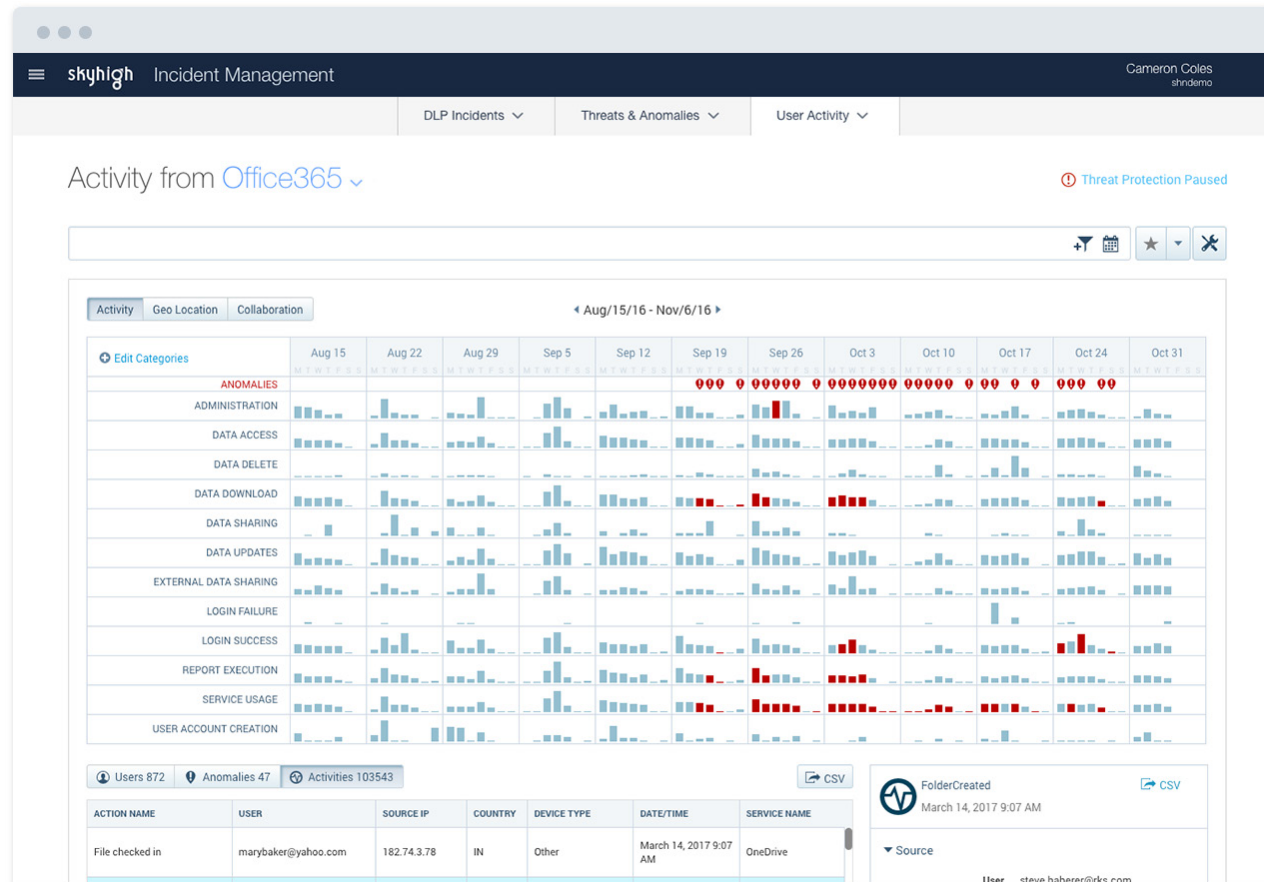

MOST COMPLETE COVERAGE

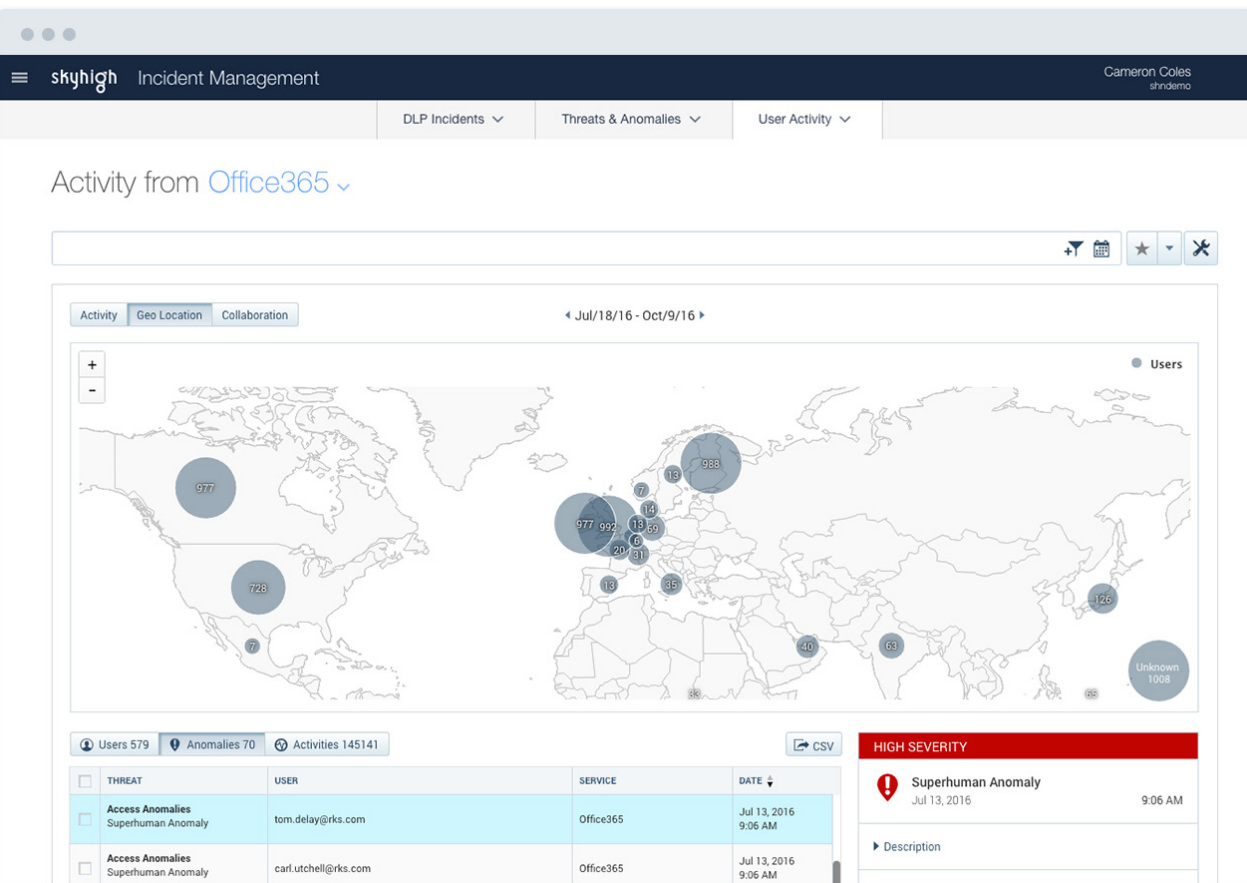
CAPTURE AN AUDIT TRAIL OF ACTIVITY FOR FORENSIC INVESTIGATIONS

Accurately detecting threats with UEBA in the previous section requires complete visibility into all user and administrator activity. Additionally, security analysts require this information in the format of an audit trail to effectively investigate a wide range of incidents, whether it be a data loss incident, insider threat, privileged user threat, or compromised account. For example, if an administrator is accessing data outside her job role, an audit trail of files accessed is essential. If a draft memo leaks to the press, it's important to know who accessed the file to narrow down who may be responsible. If an account compromise is found, the enterprise needs to know what data was accessed, particularly if the data accessed requires a breach notification.

How Skyhigh helps

Skyhigh captures a complete audit trail of all user activity in Office 365 for post-incident forensics. There are over 500 distinct activities that users and administrators can perform across Office 365 applications. Skyhigh categorizes each activity into one of 13 categories (e.g. data access, data sharing, data deletion, etc.) to normalize activities across cloud services and streamline the process of filtering. Security analysts can browse activity by category, for a specific user, or for a specific time frame using a graphical interface that visually summarizes activity over time. This default categorization schema can also be customized.





Geolocation analytics presents analysts with a clickable view of activities projected onto a map with the ability to visualize activity across geographic regions and drill down into a single region for deeper reporting. For example, if an account compromise originates in Pakistan, where the company has no offices or employees, security analysts can see all access from Pakistan to understand if the scope is limited to one account or a broader problem that may have impacted several users accounts. Then analysts can view activities for those accounts originating in Pakistan and understand the sequence of events that unfolded and data accessed.


Skyhigh provides a search omnibar that enables analysts to filter events based on any attribute associated with an action such as time frame, activity name, file name, user, device type, etc. and combine multiple criteria into one search that filters a list of activities. These criteria can be saved as a custom view and shared with other Skyhigh users, and events can be exported to a CSV file and imported into other solutions. Skyhigh also leverages third-party threat feeds to enrich the context surrounding each event, including the reputation of the user's IP address and whether they are using an anonymizing proxy or TOR connection.

Required CASB capabilities:

- ✓ Ability to capture over 500 distinct user activities
- ✓ Categorization and normalization of activities
- ✓ Visual interface for exploring activity
- ✓ Geographic view of user activity
- ✓ Search omnibar with saveable, shareable views
- ✓ Integration with Microsoft Active Directory
- ✓ Integration with SIEMs via syslog

How it works: Deployment Architecture

The full context of certain activities is cloud-centric in nature. That is to say that an inline proxy only sees part of the picture at the moment an activity occurs—only partial context is in the packets inspected by the proxy, or the proxy misses the activity altogether if it originates from a third-party user or an employee on an unmanaged device. Additional context is either in the cloud service or exchanged asynchronously, making it impossible for a proxy to fully understand. There are 532 activities in Office 365 that are available for monitoring using the Microsoft Graph API, but only 137 are supported by a proxy, regardless of the traffic steering mechanism.

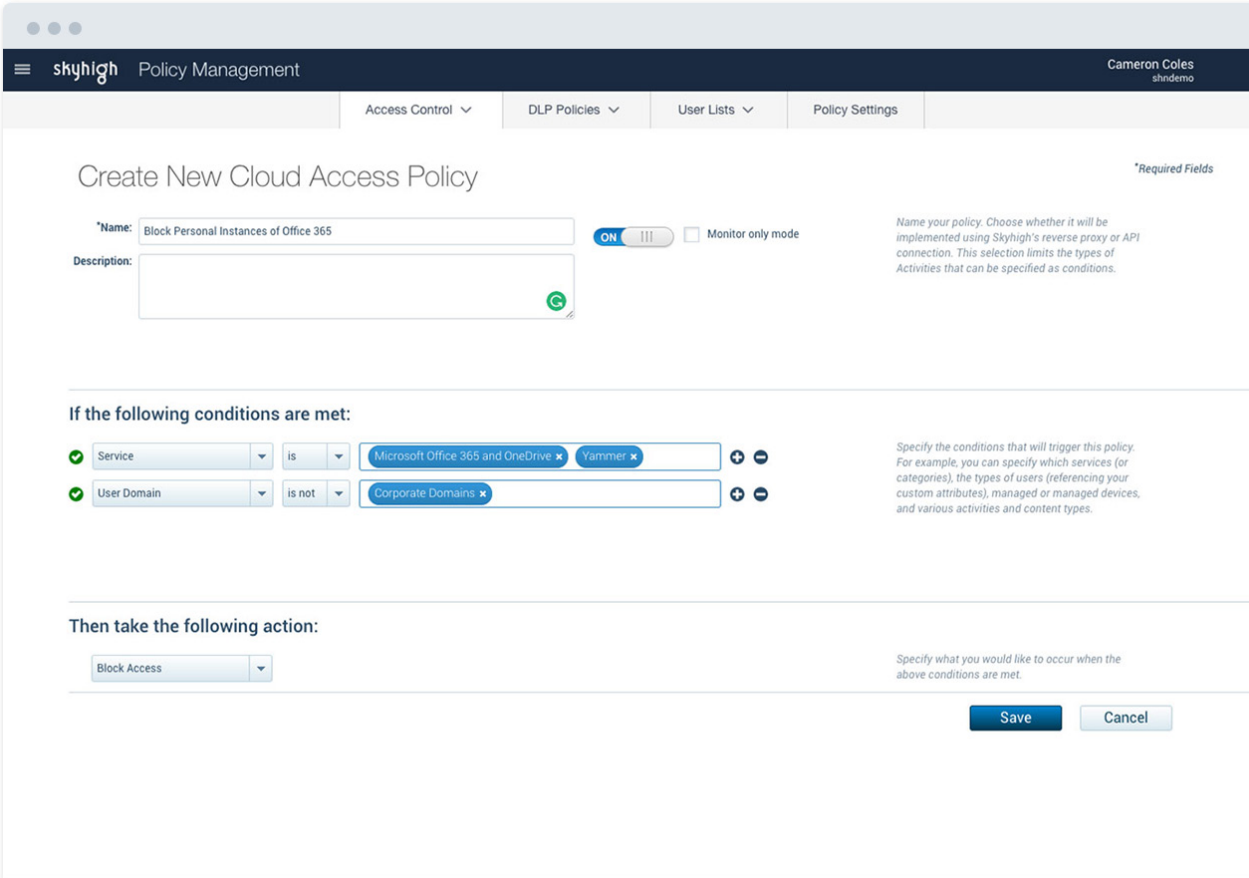
	 MOST COMPLETE COVERAGE	Forward Proxy	Reverse Proxy
Activity count	532	137	137

PREVENT LOSS OF CORPORATE O365 DATA FROM USE OF PERSONAL O365 INSTANCES

Some enterprises have acceptable use policies that dictate certain cloud services are allowed to store corporate data and others are not. For example, an organization may have a policy against uploading corporate data to all file sharing services not managed by the organization or just to those that claim ownership of data uploaded to them. These policies can also extend to personal instances of corporate-sanctioned services such as Office 365. In these cases, enterprises only want to permit upload of corporate to Office 365 accounts under management by the company. It would not be permitted to upload corporate data to a personal OneDrive account, for example.

How Skyhigh helps

Skyhigh enforces persona-based controls for Office 365 at the instance level. First, Skyhigh detects whether a user is logging in to a corporate instance of an Office 365 application or a personal instance. Based on policy, Skyhigh can block access to a personal instance while allowing access to the corporate instance. This capability requires the CASB to understand whether a user is accessing a corporate instance or not. It also requires inline controls to block access to personal instances while allowing access to the corporate instance.



Required CASB capabilities:


- ✓ Detection of personal vs. corporate instances
- ✓ Forward proxy for inline controls
- ✓ Proxy chaining for on-network traffic steering
- ✓ Endpoint agent for off-network traffic steering

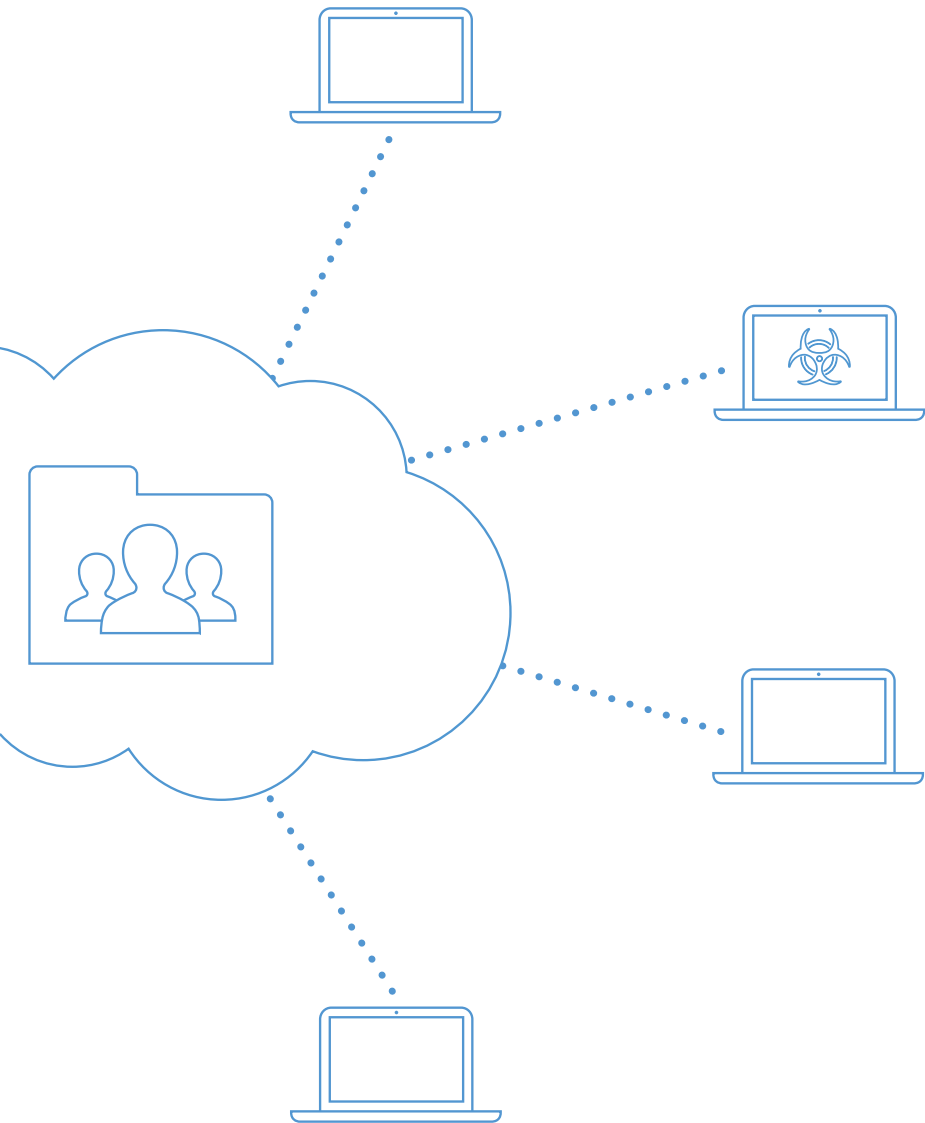
How it works:

Deployment Architecture

Enforcing controls on personal instances requires a CASB to be inline. Since personal instances are not under the control of the enterprise, it is not possible to control the post-authentication traffic which is used to route traffic through a reverse proxy. Therefore, this use case requires the CASB to operate in forward proxy mode. As such, Skyhigh enforces persona-based control for on-network users and off-network users accessing Office 365 from managed devices.

	API	Forward Proxy	Reverse Proxy
Visibility into personal instances		<input type="radio"/>	
Control over personal instances		<input type="radio"/>	

 MOST COMPLETE COVERAGE

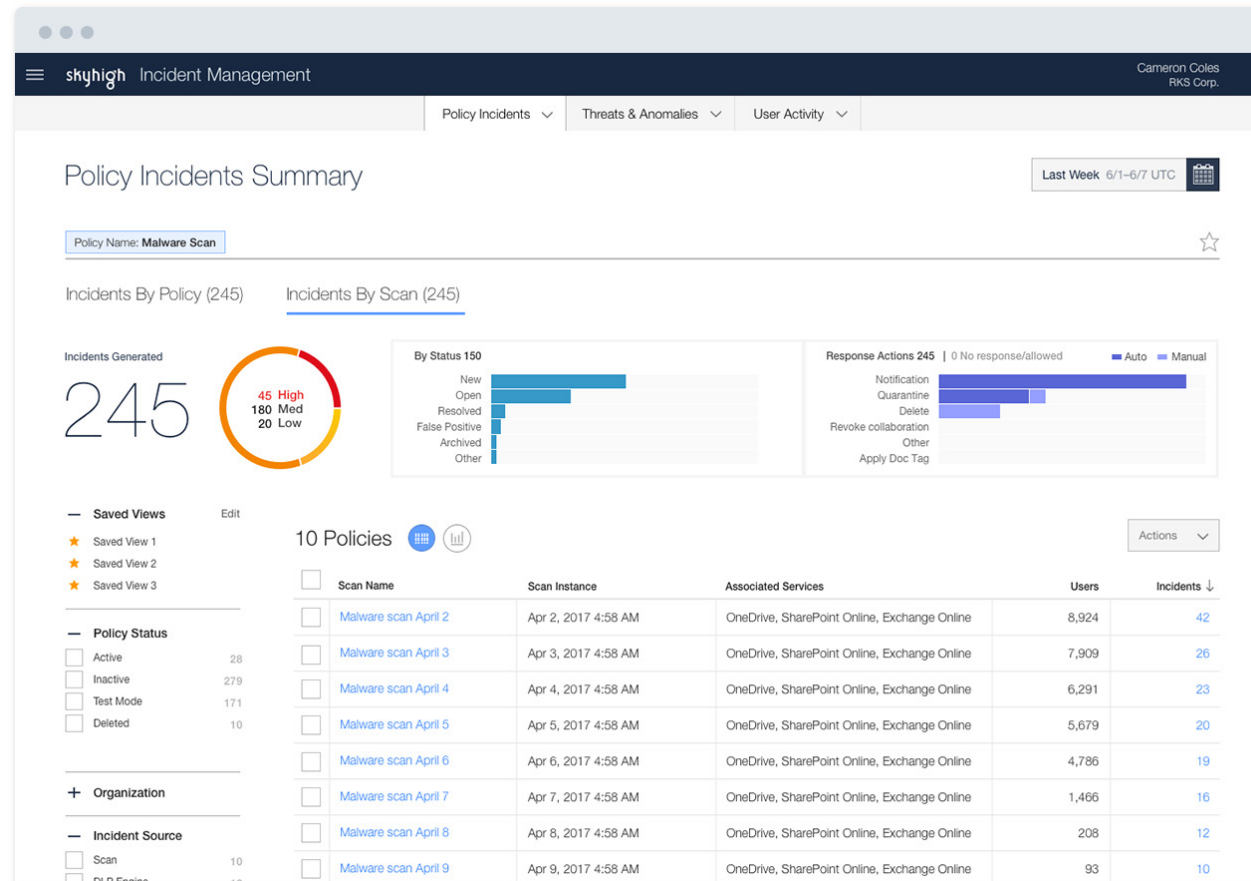


PREVENT PROLIFERATION OF MALWARE

Recognizing that malware can leverage file sync and share functions to proliferate, Microsoft offers built-in antivirus for Office 365 that identifies most malware with previously catalogued signatures. When malware is detected, Office 365 quarantines files to prevent download and syncing to user endpoints. Additionally, many enterprises utilize a secure web gateway (SWG) with malware protection for all on-network devices and off-network managed devices, and endpoint protection for managed devices. However, there is a gap in protection for zero-day threats without previously catalogued signatures for off-network unmanaged devices.

How Skyhigh helps

Skyhigh delivers a malware solution for Office 365 that extends protection against zero-day threats. First, Skyhigh pre-filters all known threats leveraging over 40 threat intelligence feeds. Next, Skyhigh executes suspicious files in a sandbox, leverages behavioral analysis to detect malware, and publishes indicators of compromise (IOCs). Skyhigh quarantines files to prevent syncing or sharing to other users who may not be covered by an enterprise's protection suite for malware. Once a zero-day threat is identified, Skyhigh quarantines the file wherever it exists in Office 365.



Required CASB capabilities:

- ✓ Static malware analysis for suspicious files
- ✓ Sandbox file execution with behavior analysis
- ✓ Quarantine malware infected files

How it works: Deployment Architecture

The API mode offers the most complete coverage for malware detection and remediation. Because zero-day threats in Office 365 are largely a problem for files synced with the native app from unmanaged devices off the corporate network, neither inline proxy approach provides complete coverage. The forward proxy mode does not offer this protection because it does not cover off-network unmanaged devices. The reverse proxy approach is also not appropriate because it does not cover native applications, such as the OneDrive sync client. For more details on access coverage, see the section “CASB deployment architectures” earlier in the e-book.

	API	Forward Proxy	Reverse Proxy
Identification of suspicious files	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Quarantine of malware files	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

MOST COMPLETE COVERAGE

A person is sitting at a desk in an office environment. They are wearing a light-colored sweater over a collared shirt and have white earbuds in their ears. They are holding a smartphone in their hands, looking at the screen. In front of them is a silver laptop. To the left of the laptop is a white coffee cup with a lid. To the right of the laptop is a yellow notepad with a silver pen resting on it. The background is slightly blurred, showing a window and some office equipment. The entire image has a blue overlay.

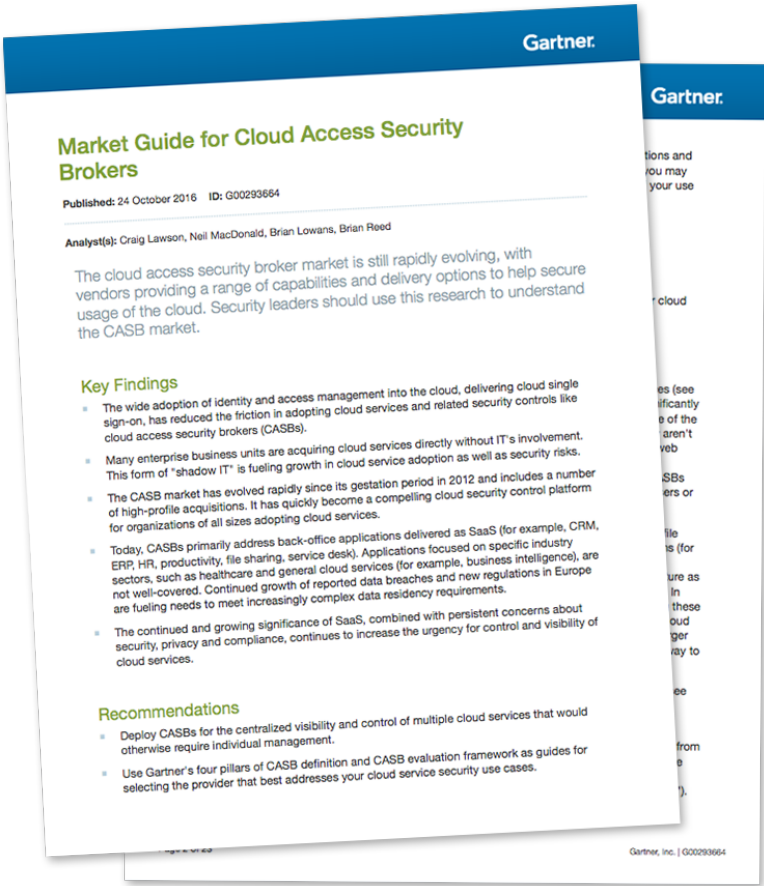
Chapter 4:

What to Look for in a CASB

Not all CASBs are the same. As Gartner points out, the capabilities of CASB vendors vary widely, so it's recommended that when evaluating a solution to secure Office 365 you view detailed product demos focused on core use cases, speak to 5-10 enterprise references of your size and scale, and in some cases perform a proof of concept to compare CASB products against the usage and data in your own Office 365 environment.

Organizations need to look past CASB providers' "list of supported applications and services," because there are (sometimes substantial) differences in the capabilities supported for each specific cloud service, based on its features, the CASB architecture used and the organization's end-user computing model.

For example, one CASB version's "support for Office 365" can be markedly different from another's, depending on bring your own device (BYOD) use cases, even though both "on paper" support these applications. Proxy or API architectures from a CASB have different abilities to perform different actions, which have various implications for how that provider delivers the four pillars (visibility, compliance, data security, and threat protection) for a specific cloud service.²



² Gartner Research: Market Guide for Cloud Access Security Brokers. Craig Lawson, Neil MacDonald, Brian Lowans, Brian Reed. October, 2016


Many vendors claim a wide range of capabilities for Office 365, but once you get into the details you'll find that the depth of these solutions varies widely. Here are some of the areas to explore with CASB vendors when evaluating a potential solution.

Active Directory integration

The ability to enforce policies for specific user groups or departments based on attributes pulled from Microsoft Active Directory is foundational to CASB. This capability involves pulling user attributes from Active Directory, including custom attributes from extended schema. Many vendors claim this functionality, but cannot deliver it in a production environment, so it's important to ask customer references whether they have been able to use this feature.

API time-to-enforcement

When a user uploads a file containing sensitive content to an Office 365 application or shares it externally, the time it takes to enforce a remediation matters. The longer the file is in Office 365, the greater its potential exposure. Skyhigh enforces sharing policies in Office 365 in real time using a synchronous API. Skyhigh enforces content-aware DLP policies with sub-minute response times, minimizing the potential window of exposure even at scale when deployed in production by large enterprises. During a technical evaluation of CASBs, measure the evaluation and enforcement time it takes for each solution after uploading or sharing a file.



“Skyhigh shows us what’s going on in Office 365 with DLP to remediate bad file permissions or people sharing data that they shouldn’t.”

Steelcase

RANDY MOON, SENIOR MANAGER OF IT SECURITY

DLP accuracy

When utilizing content-aware DLP, enterprises seek to minimize both false positives and false negatives because they do not want to miss violations, and at the same time they do not want to enforce remediation actions and generate alerts for files that do not have violations. Some CASB providers rely on OEM search technology to identify sensitive data patterns such as credit card numbers or Social Security numbers, which results in large numbers of false positives and negatives. In a product comparison, evaluate the effectiveness of CASB DLP engines across the same dataset.

Multi-tier remediation

Many enterprises have distinct remediation requirements depending on the scope and content of a policy violation. Depending on the severity, you may want to coach users and generate a violation alert, in other cases quarantine a file, and in other instances delete the file automatically. Skyhigh supports the ability to not only define severity level within a DLP policy, but also enforce distinct remediation actions based on that severity level. During evaluation, compare each CASB's ability to tier remediation based on severity and their variety of remediation options.



SIEM integration via syslog

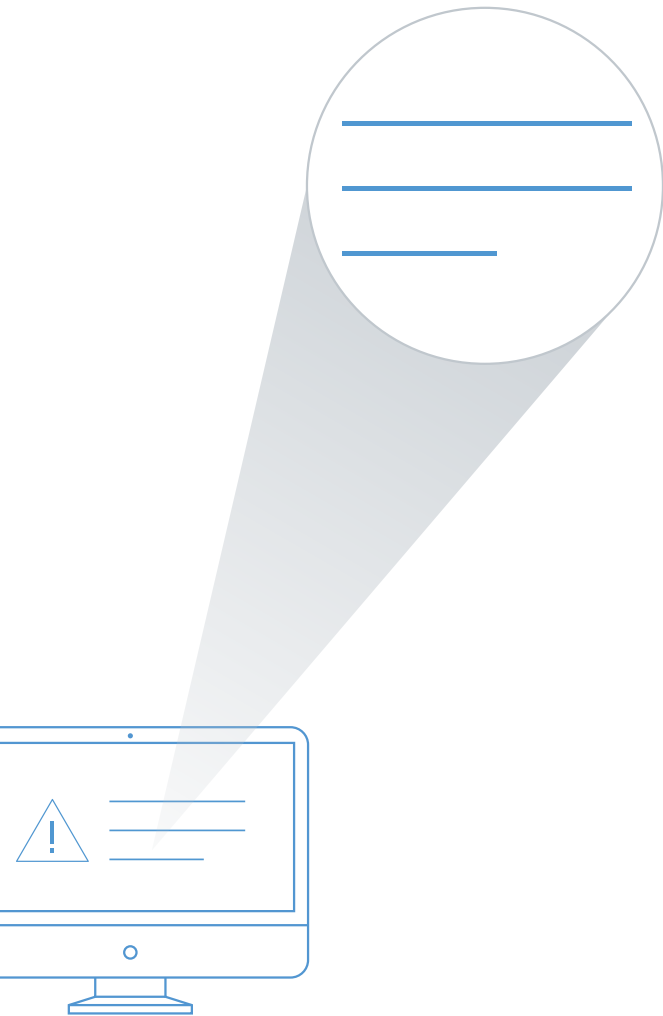
Some organizations review threats and policy violations within their SIEM. One approach is to generate a file that must be imported each time via a script. The disadvantage of this approach is that it requires manual work to periodically import violations. A better approach leverages a syslog feed to automatically populate a SIEM with policy violations. Skyhigh follows this approach and supports syslog formats utilized by the most popular SIEM solutions.

Rollback of an automated remediation action

Customers can minimize false positives by utilizing DLP engines purpose built for DLP and not search, however some DLP false positives are inevitable. When they occur, it is essential that compliance reviewers have the ability to rollback an automated remediation action taken by the system. For example, if a CASB detects a violation that turns out to be a false positive, a reviewer needs the ability to undo a quarantine action to restore a file. This capability is a requirement in order to deploy DLP with automated remediation.

No sensitive customer data stored in the CASB

In delivering DLP capabilities such as quarantine and match highlighting, some CASBs store this data within their cloud solution, which creates additional security and compliance issues. When Skyhigh quarantines files in response to a DLP violation, it stores the files in an administrator account in Office 365. Similarly, when Skyhigh provides match highlighting for DLP violations, the data is stored in a customer-controlled repository and not within Skyhigh. Finally, Skyhigh tokenizes personal information in violations such as username.



Review interface with match highlighting

When reviewing DLP violations, a compliance analyst needs to understand a violation in context. Without an excerpt that triggered the violation, they would need to review an entire document to find the violation. Skyhigh's review interface provides excerpts of each violation within a document, highlighting the specific content that triggered the violation. This capability is critical for the review and remediation of policy violations. Customers, not Skyhigh, store DLP violation excerpts, meeting stringent compliance requirements.

Scale for cloud data volumes

The volume of data in the cloud is growing exponentially. Enforcing DLP in a timely manner when data volumes and velocity are high is a challenge, which is why many solutions architected for on-premises DLP cannot scale to cloud data volumes. Ask references of your size about the performance of the CASB data loss prevention solution. How long does it take to enforce a DLP policy after a file is uploaded? Does the API connection to Office 365 crash?

Threat funnel focused on multi-event threats

Most security incidents have multiple signals that are anomalous—not only does a user have multiple failed login attempts, but she also accesses from a new location, and her behavior once gaining access to the application is outside her own behavioral norms. CASB solutions that generate alerts based on single-event anomalies will overwhelm security teams with false positives, leading to alert fatigue and alerts for actual threats being ignored. Skyhigh leverages a multi-event threat funnel that correlates several anomalies into a higher-order threat object before generating an alert in an approach that minimizes false positives.

Unsupervised machine learning for complexity-free setup

When deploying a CASB for the first time, it's difficult to anticipate what threshold for an activity will detect a threat. Moreover, what's atypical for one user and indicative of a threat may be a typical level of activity for another user, making it challenging to set manual thresholds and achieve accurate results with this approach. Skyhigh begins learning user behavior as soon as it's connected to Office 365 and builds a unique behavior model for each user. These baseline models can further be refined with input later by tuning sensitivity.

Supervised machine learning with real-time preview

Skyhigh provides multiple ways for security analysts to provide input on the threats detected by the system. First, Skyhigh supports whitelists for known user behavior and events. Second, each time a security analyst marks an alert as a false positive, this feedback is added to Skyhigh's models of user behavior. Finally, Skyhigh provides a sensitivity adjustment for each anomaly type with a real-time preview showing the impact of the change on anomalies detected by the system, enabling you to make the right choices based on your risk profile.

Support for more than Office 365

While your CASB project may today be focused on Office 365, nearly all organizations use multiple cloud services and expand their cloud security policies to cover additional cloud applications. The controls and policy enforcement tools from cloud providers vary and are unique to that provider. Leveraging a single cross-cloud platform that enforces security and compliance policies consistently across Office 365, other SaaS applications, and custom in-house developed applications deployed on IaaS improves both efficiency and security.

Third-party certifications

Many organizations have policies about required security certifications for using a cloud application, and a cloud security solution is no different. Skyhigh has attained ISO 27001 and 27018 certification and is the only CASB with FedRAMP compliance, which together provide strong evidence of the internal security practices of Skyhigh and our solution's security controls.

Single CASB platform with one interface

Some vendors claim CASB functionality, but in reality they deliver capabilities spread across multiple products, sometimes acquired from other companies. It can take a long time to integrate the interfaces of these products, to say nothing about integrating their code bases. Skyhigh delivers all CASB capabilities in a single unified platform accessible from a single user interface, without requiring policies to be managed and remediation to take place across multiple interfaces.



Chapter 5:

Customer Maturity Model

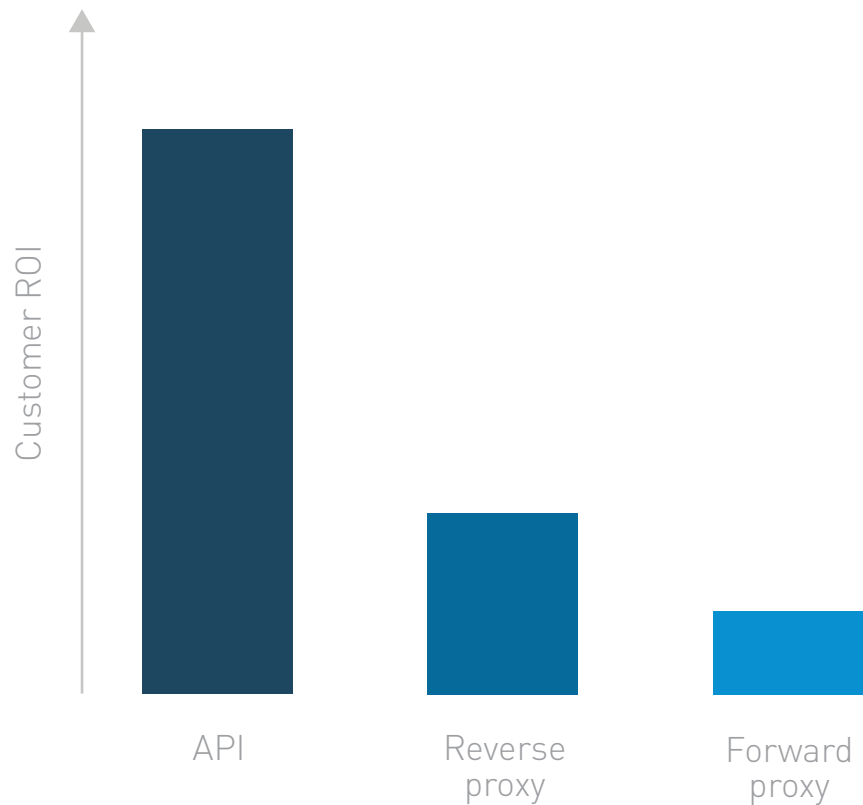
Skyhigh offers coverage for all access scenarios and Office 365 CASB use cases. As we've seen in the prior chapters, there is a deployment architecture that supports the most complete coverage for each use case.

	API	Forward Proxy	Reverse Proxy
Prevent unauthorized data from being shared externally	✓		
Prevent regulated/high-value data from being stored in the cloud	✓		
Block download of O365 data to personal devices			✓
Detect compromised accounts, insider/privileged user threats	✓		
Capture an audit trail of activity for forensic investigations	✓		
Prevent access to personal O365 instances		✓	
Prevent proliferation of malware and ransomware	✓		

When deploying Skyhigh, customers generally take a phased approach, starting with their highest priority use cases and coverage requirements and the least amount of deployment friction first. Deployment friction occurs with the inline CASB modes and includes changing settings in the identity management service, modifying traffic routing on the enterprise's secure web gateway (SWG), or deploying an endpoint agent for traffic steering.

Collectively, access coverage, use case functionality, and deployment friction constitute the ROI calculation many enterprises make when planning a CASB deployment. Seen in this light, the API mode delivers the highest level of coverage for users, devices, and network types among CASB deployment modes. Critically, the API mode supports the most common Office 365 use cases and delivers the most functionality. It also does so with minimal friction. A CASB deployment in API mode is measured in the minutes it takes to establish the API connection to the enterprise's Office 365 environment.

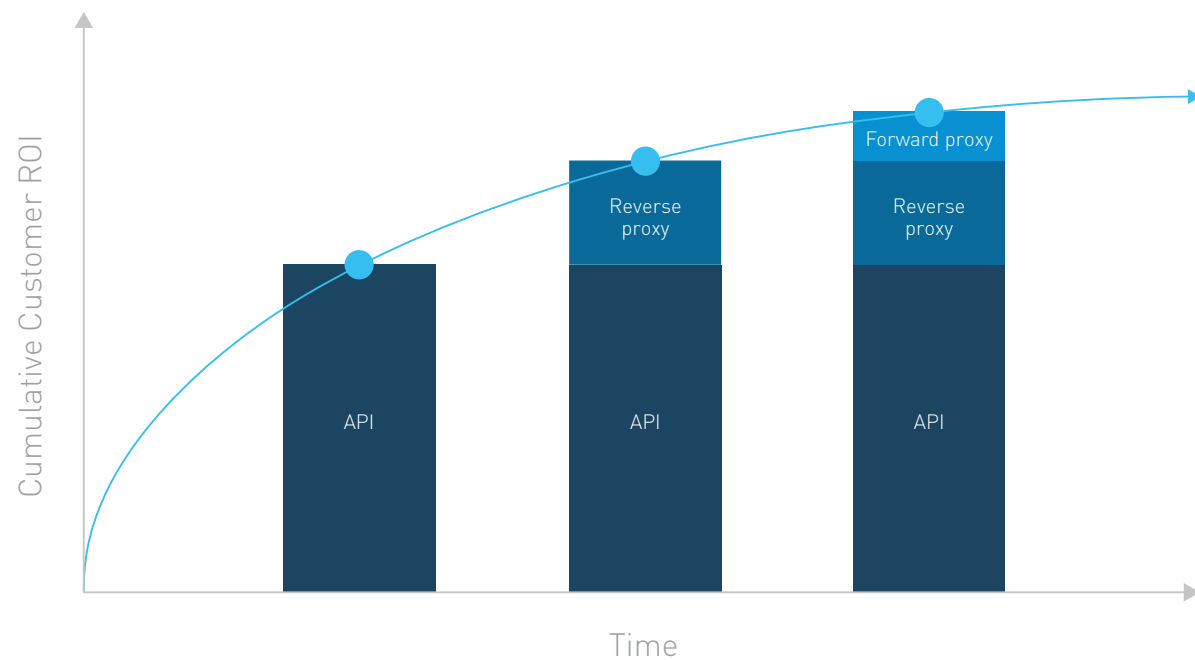
	Access coverage	Use case functionality	Deployment friction
API	High	High	Low
Reverse proxy	Med	Med	Med
Forward proxy	Med	Med	High



Next, the reverse proxy mode covers slightly less access scenarios and use cases. Specifically, the reverse proxy mode does not support native applications, collaboration policies, or persona-based control. Modifying the routing settings in the enterprise’s identity solution to route all Office 365 sessions through the reverse proxy requires some configuration work, but is not overly burdensome. However, once this change is made all sessions are seamlessly and pervasively routed through the CASB without any additional work, and without changes to end user behavior, so deployment friction is rated at moderate.

The forward proxy mode covers similar access scenarios and use cases as the reverse proxy mode. It does not support off-network devices that are unmanaged or collaboration policies. The friction for this mode is the highest, however. The enterprise’s secure web gateway (SWG) must be configured to route traffic through the CASB’s forward proxy for all network traffic. Not all SWG solutions support traffic forwarding, which can complicate forward proxy rollouts. Also, off-network users require the installation of an endpoint agent if their traffic is not already being routed to an SWG that supports traffic forwarding.

Most enterprises start with an architecture that maximizes coverage for access scenarios and security functionality while minimizing deployment friction. Doing so ensures the CASB project will be a “quick win” that delivers immediate and significant value. The API mode delivers the highest ROI and is generally deployed in an initial rollout of the CASB. Over time, as an enterprise develops greater maturity, it deploys inline proxy modes starting with the reverse proxy mode, which adds support for preventing data from being downloaded to personal devices. Finally, enterprises deploy the forward proxy mode to add support for instance control.



GET A FREE AUDIT OF YOUR OFFICE 365 USAGE

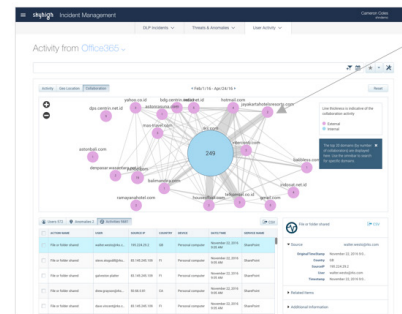
Get started with a free audit using Skyhigh Cloud Access Security Broker. We'll deliver a report summarizing:

- Documents containing sensitive data
- Collaboration and sharing with third parties
- Anomalous usage indicative of insider threats
- Events indicative of compromised accounts

REQUEST AN AUDIT

bit.ly/O365audit

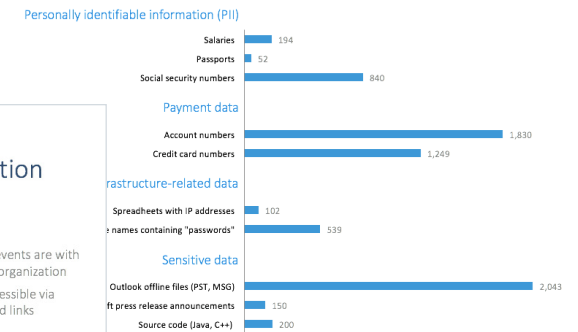
31.7% of sharing is with users outside the organization



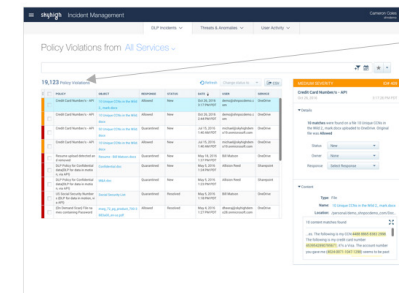
KEY FINDINGS

- 31.7% of sharing events are with users outside the organization
- 1,739 files are accessible via untraceable shared links

Breakdown of files containing sensitive data by policy



19,123 documents in Office 365 contain sensitive data



KEY FINDINGS

- 19,123 documents identified that contain sensitive data
- 539 files contain user passwords in OneDrive

RECOMMENDATIONS

Quarantine files containing sensitive data for review and implement real-time data loss prevention (DLP) policy enforcement for data uploaded to the cloud

DID YOU KNOW?

Skyhigh finds all files that contain PII, PHI, payment data, and other sensitive content