Microsoft Cloud App Security

Microsoft

Top 20 use cases for CASBs

Contents

Introduction

Moving to the cloud requires a new approach to security. As you enable employees to work from virtually anywhere and from any device of their choice, your organizational access perimeters and boundaries change. Your new security controls need to adapt to this dynamic environment and be able to quickly respond to the constantly evolving threat landscape.

Cloud Access Security Brokers (CASBs) are cloud-based security solutions that provide a new layer of security to enable oversight and control of activities and information across public and custom cloud SaaS apps and IaaS services. CASBs are broken down into four key capability areas including Shadow IT Discovery, Information Protection, Threat Protection and Compliance, and provide a central control plane for governance and policy enforcement across all of your cloud apps and services.

In this guide we share the top 20 use cases for CASBs that we recommend as a baseline for a successful implementation to improve your cloud security.

The use cases can be leveraged as a starting point during a proof of concept, or as you're getting ready to deploy your CASB solution and want to prioritize your deployment.

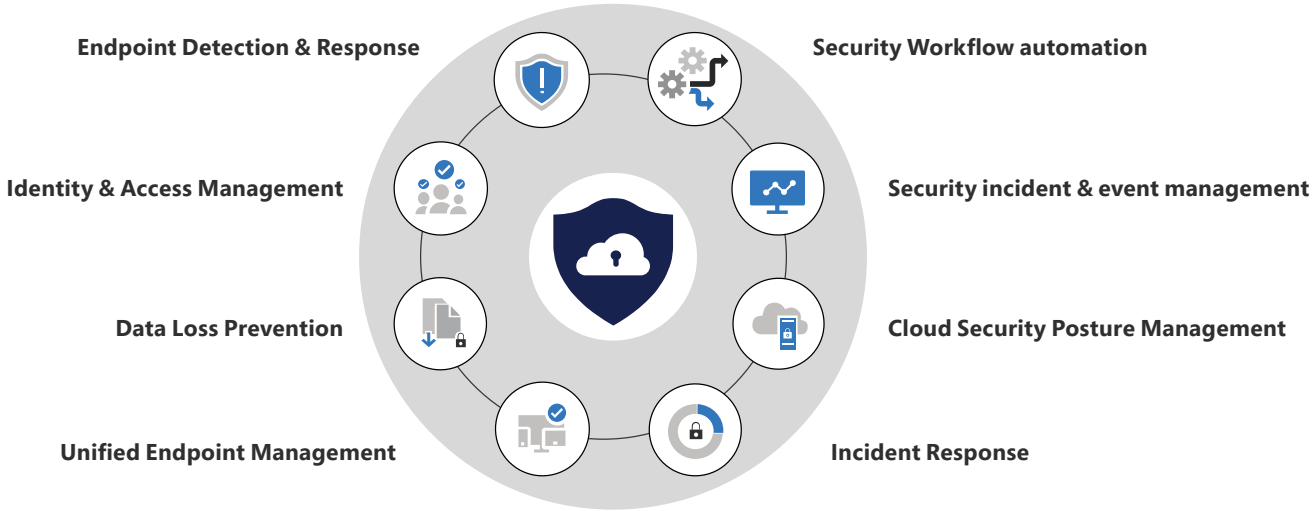
A uniquely integrated Cloud Access Security Broker

Microsoft Cloud App Security (MCAS) is a multimode Cloud Access Security Broker. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.

MCAS is designed with security professionals in mind. It is built as a state-of-the-art concept of native integrations to provide a simple deployment experience, centralized management, and innovative automation capabilities—while still allowing you to integrate non-Microsoft solutions from your existing environment such as a SIEM or Secure Web Gateway.

Our unique approach ensures that we deliver a powerful security solution that enables a higher level of security and compliance for heterogeneous cloud environments— across all your cloud apps and services.

One example is how Microsoft Cloud App Security delivers the only native Identity and Access Management (IAM) + CASB solution in the market, by integrating with Azure Active Directory (AAD) conditional access. This enables selective routing via our reverse proxy infrastructure, and thereby minimizes end user impact, while ensuring the highest level of control under risky conditions. AAD conditional access allows you to specify when traffic is routed via the reverse proxy using conditions such as device state, user, cloud app, location, and network, allowing for an unprecedented balance of cloud security and end user productivity.



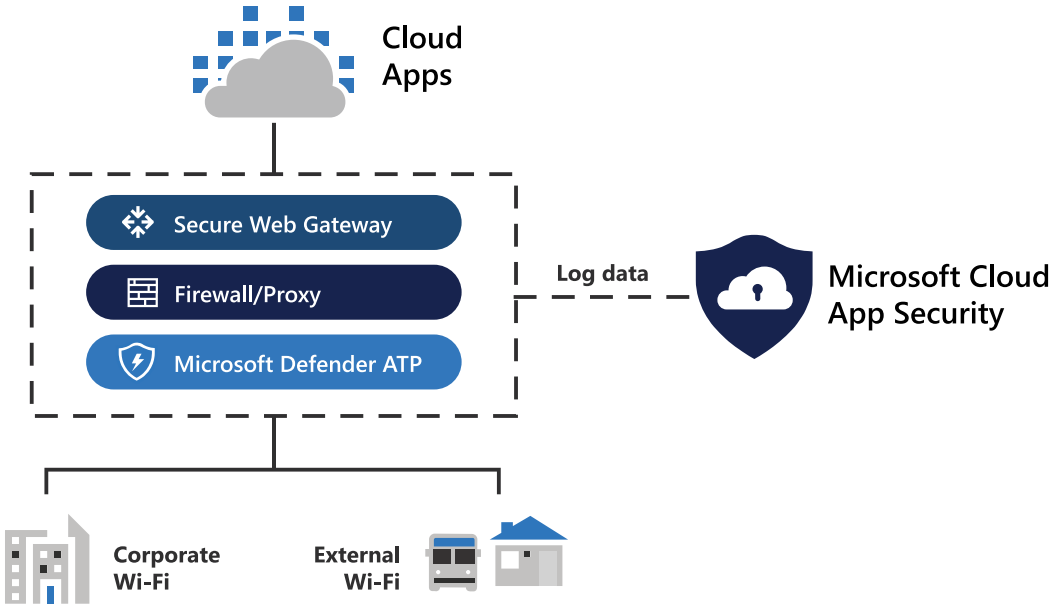
Architectural considerations

When implementing the various CASB use cases that are outlined in this document, organizations need to ensure a seamless integration with their existing architecture and software solutions.

A Cloud Access Security Broker should support multiple deployment modes to ensure full coverage of the key use cases within a single management experience, including:

- Log ingestion from Firewalls, Secure Web Gateways and SIEMs
- Cloud-to-cloud APIs-based connectors
- Reverse Proxy integration with the primary (IAM) provider

Integrations with other enterprise solutions are important for an effective and sustainable management of the CASB solution and the organization's processes and workflows. Microsoft Cloud App Security supports all of the implementation scenarios listed above and integrates with Microsoft native solutions, as well other market leading solutions in the previously listed categories.



Deployment options for cloud app discovery and blocking

A user's Wi-Fi connection will dictate point of access to the cloud, but the log data will be sent to Microsoft Cloud App Security.

Addressing Shadow IT in your organization

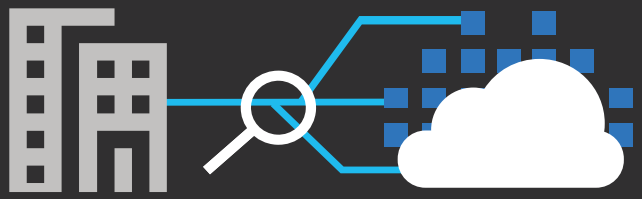
1. Discover all cloud apps and services used in your organization

Our numbers show that Shadow IT makes up more than 60% of cloud services in large organizations, introducing unknown and unmanaged risks into the environment.

A CASB enables you to identify which cloud apps and services are being used across your organization. Whether these cloud services are being accessed on or beyond the corporate network, managed or unmanaged by IT—all data is captured. The discovery report includes all relevant information based on users, IP addresses and machines.

Deployment mode: Log collection
Native integrations: Microsoft Defender Advanced Threat Protection, Azure Sentinel
Other integrations: SIEM, Firewall, Secure Web Gateway

Technical implementation



2. Assess the risk and compliance of your cloud apps

It's important for your IT teams to confirm whether all apps that are currently being used across the organization meet internal security policies and relevant industry or compliance requirements.

Microsoft's CASB can help you assess the risk and compliance of any discovered cloud app or service against more than 70 risk factors, including general security—for example whether the app captures an admin audit trail—regulatory compliance such as ISO 27018 and legal factors including GDPR. These allow your IT team to make informed decisions about which apps should be supported in the organization, and which require additional governance or need to be blocked entirely.

Deployment mode: Log collection
Native integrations: Microsoft Defender Advanced Threat Protection, Azure Sentinel
Other integrations: SIEM, Firewall, Secure Web Gateway

Technical implementation

Addressing Shadow IT in your organization

3. Govern discovered cloud apps and explore enterprise-ready alternatives

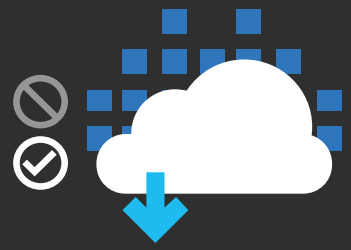
Making informed decisions is key when putting governance actions for cloud apps in place.

Once you have analyzed the risk and compliance of your cloud apps, you can use the CASB to start managing them by classifying them into relevant app groups, which commonly include *Sanctioned, Unsanctioned* or *Restricted* app tags. Once categorized, further governance actions can include onboarding an app to Azure Active Directory, dedicated monitoring of an app over time, or blocking its use by end users.

In case you discover risky or duplicate apps, the cloud app catalog—which includes more than 16,000 cloud apps—can be leveraged to find enterprise-ready alternatives.

Deployment mode: Log collection
Native integrations: Microsoft Defender Advanced Threat Protection, Azure Sentinel
Other integrations: SIEM, Firewall, Secure Web Gateway

Technical implementation



4. Enable continuous monitoring to automatically detect new and risky cloud apps

With end users always on the lookout for apps to improve their productivity, it's key to stay on top of new services in your organization.

With a CASB, you can setup a policy to detect changes in the usage pattern of cloud apps, and be alerted when new, risky or high-volume apps are discovered in your environment.

When the usage of a specific app spikes, you may want to re-evaluate its risk score to ensure corporate data is being handled safely. At the same time, this continuous monitoring enables you to be alerted when new, risky apps are detected and immediately take action to limit the impact on your organization.

Deployment mode: Log collection
Native integrations: Microsoft Defender Advanced Threat Protection, Azure Sentinel
Other integrations: SIEM, Firewall, Secure Web Gateway

Technical implementation

Addressing Shadow IT in your organization

5. Detect when data is being exfiltrated from your corporate apps

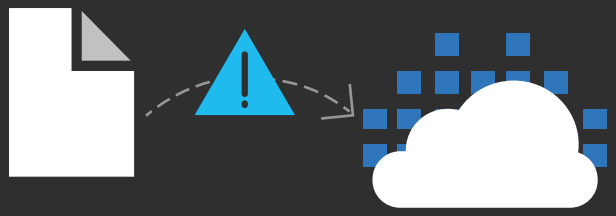
Sensitive, corporate data is the most valuable asset in many organizations. Therefore, it's key to ensure that your data is protected and cannot be exfiltrated from your organization for improper use.

Microsoft's CASB has out-of-the-box policies that will alert you on suspicious usage within unsanctioned apps when activities are performed that indicate a potential attempt to exfiltrate information from your organization.

In addition you can configure custom policies to get alerted on events that are important to your organization.

Deployment mode: Log collection
Native integrations: Microsoft Defender Advanced Threat Protection, Azure Sentinel
Other integrations: SIEM, Firewall, Secure Web Gateway

Technical implementation



6. Discover OAuth apps that have access to your environment

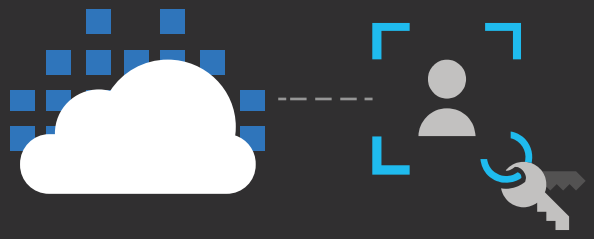
With OAuth apps users grant cloud apps access to their corporate user accounts without sharing credentials. While originally created for consumer-facing services such as Facebook, enterprise adoption of OAuth apps is increasing, giving them programmatic access to a user's corporate data and permission levels.

With Microsoft's CASB you can analyze 3rd party OAuth apps that have been authorized to use the credentials of your corporate logins to Office 365, G-Suite or Salesforce, to access other cloud services that may not be sanctioned by IT.

Analyze their access levels and related activities to ensure they are compliant with your internal guidelines.

Deployment mode: API-Connector

Technical implementation



Protect your information in the cloud

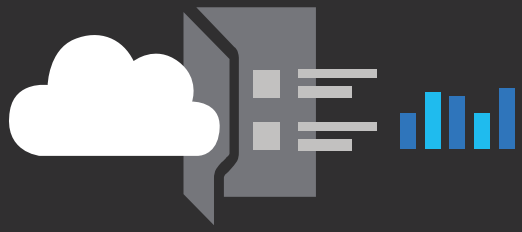
7. Gain visibility into corporate data stored in the cloud

No matter where in your cloud journey you are, many of your end users likely started leveraging cloud services a long time ago and have stored corporate data in various cloud applications.

A CASB provides you with full visibility over all data stored in sanctioned and connected cloud apps. It gives you deep insights about each file, allowing you to identify whether it contains any sensitive information, the owner and storage location, as well as the access level of the file. Access levels distinguish between private, internal, externally shared and publicly shared files, allowing you to quickly identify potentially overexposed files putting sensitive information at risk.

Deployment mode: API-Connector
Native integrations: Azure Information Protection

Technical implementation



8. Enforce DLP and compliance policies for sensitive data stored in your cloud apps

Cloud services such as Office 365 or Slack are key productivity solutions in many organizations today. Consequently, sensitive corporate data is uploaded and shared across them.

For existing data, a CASB solution can help you identify files that contain sensitive information and it provides several remediation options including removing external sharing permissions, encrypting the file, placing it in admin quarantine or deleting it if necessary.

Additionally, you can enforce DLP policies that scan every file as soon as it's uploaded to a cloud app, to alert on policy violations and automatically apply data labels and relevant restrictions to protect your information. These policies can be created using advanced techniques such as data identities, regular expressions, OCR and exact data matching.

Deployment mode: API-Connector, Reverse Proxy
Native integrations: Azure Information Protection, Azure Active Directory, Microsoft Intune, Microsoft Defender Advanced Threat Protection
Other integrations: Non-Microsoft DLP solution

Technical implementation

Protect your information in the cloud

9. Ensure safe collaboration and data sharing practices in the cloud

Increasing collaboration needs and the simplicity of external sharing require companies to enforce controls that protect the sharing of sensitive information, as users collaborate internally, as well as externally, using various cloud services.

With Microsoft Cloud App Security, you can enforce a wide set of collaboration policies relevant to the sensitivity of a file. Automatic actions include setting an expiration date on a shared link or removing external collaborators, while informing the file owner.

In addition, you can configure controls that are applied to user actions in real-time. For example, if a user is trying to send sensitive information like a password via instant message (IM) in apps such as Microsoft Teams or Workplace by Facebook, you can enforce policies that will instantly block the message from being sent.

Deployment mode: API-Connector, Reverse Proxy
Native integrations: Azure Information Protection, Azure Active Directory, Microsoft Intune, Microsoft Defender Advanced Threat Protection
Other integrations: Non-Microsoft DLP solution

Technical implementation

10. Protect your data when it's downloaded to unmanaged devices

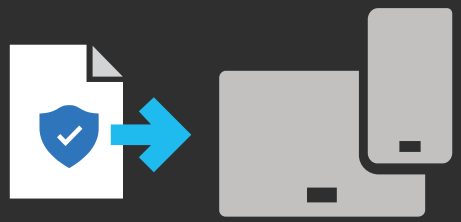
Today employees can work from anywhere. Whether it's an internal user accessing corporate apps from a hotel PC, or their personal device at home, many devices are no longer managed by your IT. In addition, external users such as agencies or partners you're collaborating with, are also allowed to access corporate resources, using unmanaged devices.

Microsoft Cloud App Security identifies the relevant device state upon user login and can be configured with granular controls to either prevent the download of sensitive files altogether, or always apply a protection label when a file is downloaded from an unmanaged device.

This ensures the continued productivity of all users, while ensuring your data is safe wherever it travels.

Deployment mode: Reverse Proxy
Native integrations: Azure Information Protection, Azure Active Directory, Microsoft Intune, Microsoft Defender Advanced Threat Protection
Other integrations: Non-Microsoft DLP solution
Non-Microsoft Mobile Device Management

Technical implementation



Protect your information in the cloud

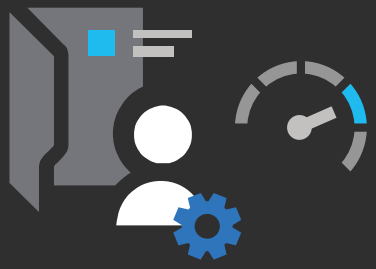
11. Enforce adaptive session controls to manage user actions in real-time

In a cloud-first world, identity has become the new perimeter—protecting access to all your corporate resources at the front door.

Microsoft Cloud App Security leverages Azure Active Directory conditional access policies to determine a user's session risk upon login. Based on the risk level associated with a user session, you can enforce adaptive in-session controls, that determine which actions a user can carry out, and which may be limited or blocked entirely. This seamless identity-based experience ensures the upkeep of productivity, while preventing potentially risky user actions in real-time. The adaptive controls include the prevention of data exfiltration by blocking actions such as download, copy, cut or print, as well as the prevention of malicious data infiltration to your cloud apps by preventing malicious uploads or pasting text.

Deployment mode: Reverse Proxy
Native integrations: Azure Information Protection, Azure Active Directory, Microsoft Intune, Microsoft Defender Advanced Threat Protection
Other integrations: Non-Microsoft DLP solution, Non-Microsoft Mobile Device Management

Technical implementation



Detect and protect against cyberthreats

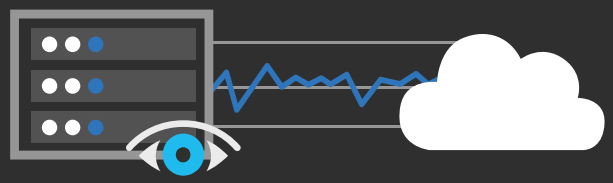
12. Record an audit trail for all user activities across hybrid environments

Whether a user identity is compromised, or an employee is deliberately carrying out risky actions across your environment of cloud apps, it's key to understand that adversaries act regardless of whether an app or information is located on-premises or in the cloud. Therefore, it's key for your IT to be able to trace and investigate the actions of any end user or privileged account laterally and across hybrid environments.

A CASB enables you to capture a detailed audit trail of all user and admin activities across your managed cloud and on-prem services for forensic investigations. This allows your IT to retrace all actions in case a breach or risky event is identified. Tracked events include activities such as sign-ins, downloads or uploads, and lateral movements, to provide full coverage for hybrid environments.

Deployment mode: API-Connector, Reverse Proxy
Native integrations: Azure Active Directory, Azure Advanced Threat Protection

Technical implementation



13. Identify compromised user accounts

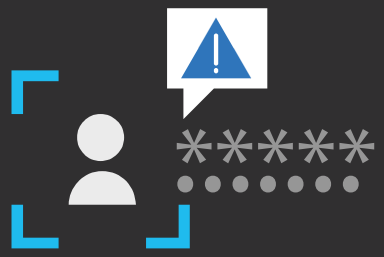
Identity attacks have increased by more than 300% over the past year, making them a key source of compromise and the number one threat vector for organizations.

A CASB learns the behavior of users and other entities in an organization and builds a behavioral profile around them. If an account is compromised and executes activities that differ from the baseline user profile, abnormal behavior detections are raised.

Using built-in and custom anomaly detections, your IT will be alerted on activities such as impossible travel, as well as activities from infrequent countries or the implementation of inbox forwarding rules, where emails are automatically forwarded to external email addresses. These alerts allow you to act quickly and quarantine a user account to prevent damage to your organization.

Deployment mode: API, Reverse Proxy
Native integrations: Azure Active Directory, Azure Advanced Threat Protection,

Technical implementation



Detect and protect against cyberthreats

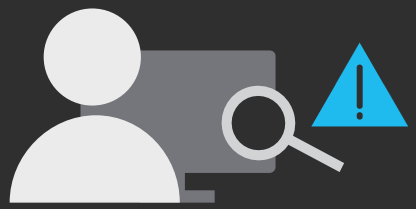
14. Detect threats from users inside your organization

Whether an employee is looking to leave your organization with valuable information, or external partners with access to your environment are trying to exfiltrate relevant, sensitive data for competitive gain—there are many scenarios in which users with legitimate access to your cloud resources become a threat to your organization.

A CASB can help you detect anomalous behavior from individual users. It will alert you to events such as mass downloads by an internal user, or unusual, repeated activities from your external user group, indicating insider threats and allowing you to act quickly and suspend the relevant user accounts to prevent data exfiltration.

Deployment mode: API-Connector, Reverse Proxy
Native integrations: Azure Advanced Threat Protection, Azure Active Directory

Technical implementation



15. Detect threats from privileged accounts

Attackers use mechanisms such as phishing, password spray, and breach replay to compromise user accounts, and their ultimate goal is often to gain control over a privileged account, making these the most at-risk accounts and most important to monitor.

A CASB will alert you to various activities indicating that a privileged account may have been compromised. Relevant alerts include mass impersonation by a single user, login from a new country with an admin account, or unusual activity from an MSSP admin.

The unified, identity-based Security Operations experience provides a true hybrid identity threat protection. And to ensure alerts are investigated in a timely manner, Microsoft Cloud App Security provides an investigation priority—a list of accounts recommended for immediate review, that considers factors like the access level of a user.

Deployment mode: API-Connector, Reverse Proxy
Native integrations: Azure Advanced Threat Protection, Azure Active Directory

Technical implementation

Detect and protect against cyberthreats

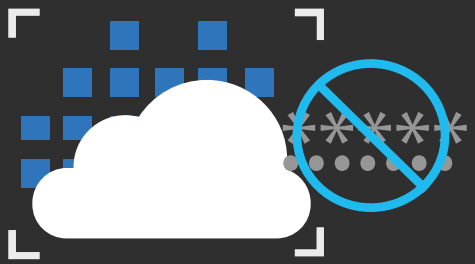
16. Identify and revoke access to risky OAuth apps

In recent years OAuth apps have become a popular attack vector for adversaries. Hacker groups such as Fancy Bear have leveraged OAuth apps to trick end users into authorizing the use of their corporate credentials, for example by duplicating the UI of a seemingly trustworthy platform.

A CASB enables you to closely monitor which OAuth apps are being authorized against your corporate environments and either manually review them or create policies that automatically revoke access if certain, risky criteria are met. Key threat indicators are the combination of an app that has requested a high level of permissions, while having a low community use status, indicating that it's not commonly found in other organizations and therefore more unlikely to be trustworthy.

Deployment mode: API Connector

Technical implementation



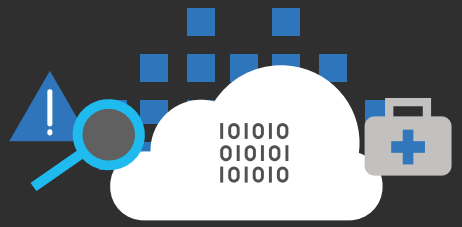
17. Detect and remediate malware in your cloud apps

As the sophistication of cyber threats continues to evolve, malware is becoming one of the fastest growing security concerns for organizations, with the majority of reported breaches now involving some type of malware.

A CASB allows you to closely monitor your cloud storage applications and identify potentially malicious files in your environment. Pre-existing files are scanned using multiple layers of detection engines to assess whether a file is malicious and associated with known malware. Microsoft Cloud App Security runs suspicious files through a sandboxing engine to detect malicious behavior and enables you to react quickly to zero-day malware in cloud storage solutions. You can also leverage session controls to prevent the upload and infiltration of known malware in real-time across all of your apps.

Deployment mode: API-Connector
Native integrations: Office 365 Advanced Threat Protection

Technical implementation



Assess and protect your IaaS environment

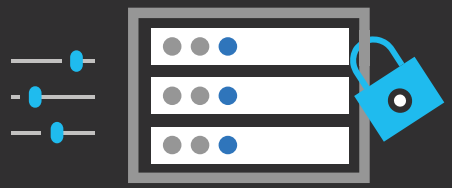
18. Audit the configuration of your IaaS environments

The increase of automation and user self-service across IaaS services requires continuous auditing to ensure that these cloud instances have been configured correctly. Due to the large amount of data, a single mistake can expose thousands of data records and go undetected for extended periods of time.

A CASB's Cloud Security Posture Management capabilities enable you to conduct a security configuration assessment across your IaaS environments. It enables you identify key data leak sources such as publicly exposed AWS S3 buckets and provides specific recommendations to improve your overall security configuration. Common suggestions include enabling multi-factor authentication (MFA) to accounts with owner permissions on your IaaS subscription, applying disk encryption, or alerting you to a lack of endpoint protection on your virtual machines.

Deployment mode: API Connector
Native integrations: Azure Security Center

Technical implementation



19. Monitor user activities to protect against threats in your IaaS environments

The impact of a user able to alter your IaaS environment can be significant and directly impact your ability to run your business, as key corporate resources like the servers running your public website, or a service you're providing to customers can be compromised.

Microsoft Cloud App Security captures and analyzes activity within the IaaS platform, including custom applications. These activities are analyzed with a highly sophisticated UEBA engine to detect anomalous usage associated with compromised accounts, insiders, and privileged users. It will alert you to events such as an unusual deletion of virtual machines, indicating an attempt to manipulate your environment in near real-time to ensure that you quickly remediate any impacts.

Deployment mode: API Connector, Reverse Proxy
Native integrations: Azure Security Center, Azure Advanced Threat Protection

Technical implementation

Assess and protect your IaaS environment

20. Capture user activities within custom cloud and on-premise apps

Organizations often have a magnitude of custom applications serving business-critical functions. IaaS platforms have brought an even greater level of accessibility and flexibility to the adoption and development of custom applications, sometimes at the expense of security and compliance standards.

A CASB can help you monitor and act on various activities across these apps in your organization in real-time, to ensure that you have awareness and control of the location, and actions taken on sensitive resources. Furthermore, by leveraging integrations with Azure Active Directory, Microsoft Cloud App Security enables you to achieve this deep visibility and parity across your cloud apps, custom apps, and on-premise apps.

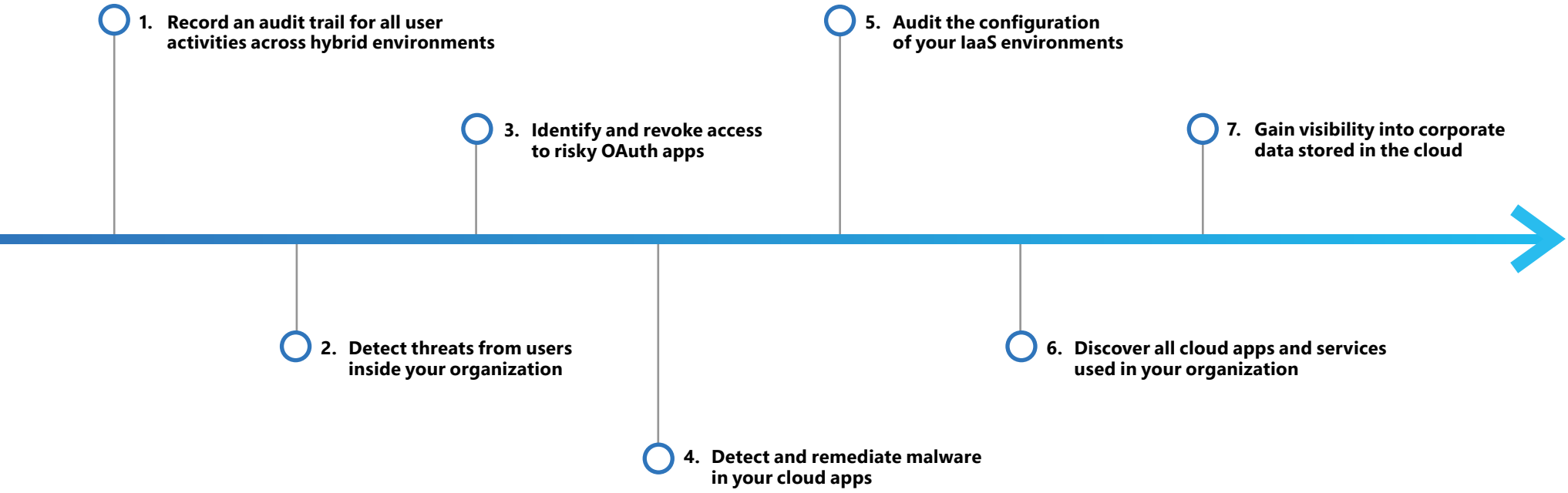
Deployment mode: API-Connector, Reverse Proxy
Optional integrations: Azure Active Directory conditional access, Azure Active Directory App Proxy

Technical implementation

Getting started with your proof of concept and prioritizing your deployment

We understand that many organizations need to prioritize their deployment when implementing a Cloud Access Security Broker.

We've created a prioritized list of the use cases in the document that will allow you to improve your overall cloud security posture within a few hours and with very little configuration, due to a seamless UI-based deployment experience and many out-of-the-box capabilities of Microsoft Cloud App Security.



Resources

Visit our website
aka.ms/mcas

Learn more about Microsoft Cloud App Security
aka.ms/mcasguide

Stay up to date and subscribe to our blog!
aka.ms/mcasblog

Join the conversation on Tech Community!
aka.ms/mcascommunity

Get started with a free trial
aka.ms/mcastrial

Use our PoC guide to kick off your CASB project
aka.ms/mcaspoc

Technical documentation
aka.ms/mcastech

Learn more about Microsoft Security solutions
microsoft.com/en-us/enterprise-mobility-security