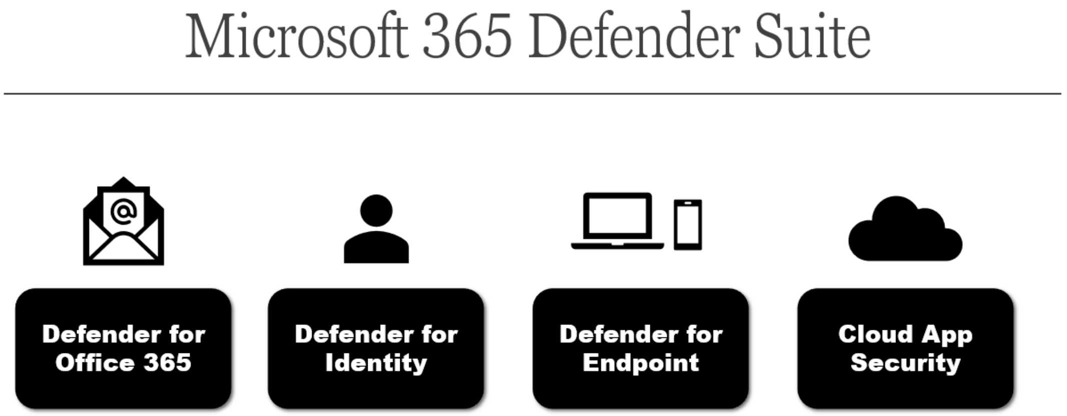
Microsoft Defender for Cloud Apps

Microsoft Documentation	https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security
Microsoft Roadmap	https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=



What is MDCA?

MDCA stands for Microsoft Defender for Cloud apps Like on our mobile phone we have applications like WhatsApp, Skype , Facebook etc similarly now a days enterprises also have apps which mostly are safe and sometime are malicious. If not managed by organisation properly this can lead to data exfiltration type of events without the need of compromised credentials.

It is good to have it because each enterprise has numerous apps (sometime thousands of applications) using which various integration and engineering tasks are completed. It becomes crucial to manage anything with high privileges especially to organisation data.

It can operate on multiple clouds

It is a user-based subscription service which means it can be taken standalone by a user.

This section should be understandable for Sales, CS, and anyone who is interested to get an overview about the MSFT Product. It should give a brief and clear overview of the whole product, what is it for, why it's good to have it, what licence is required and what features will customer get based on different licenses.

MDCA Explained	Watch the video!

Product Description

Microsoft Cloud apps Security is a comprehensive service that provides visibility, controls and enhanced protection for your cloud application. Cloud apps Security helps you extend the auditing and control you have on-premise to your cloud applications.

- **Uncover shadow IT.** Gain visibility by discovering apps , activities, users, data and files in your cloud environment as well as third-party apps that are connected to your cloud.
- **Investigate your cloud apps .** Use cloud forensics tools to deep-dive into risky apps , specific users and files in your network. Find patterns in the data collected from your cloud and generate reports to monitor your cloud.
- **Get control in the cloud.** Mitigate risk by setting policies and alerts in order to achieve maximum control over network cloud traffic and migrate your users to safe, sanctioned cloud apps alternatives.
- **Protect your data.** Use Cloud apps Security to sanction/unsanction applications, enforce data loss prevention (DLP), control permissions and sharing, and generate custom reports and alerts.

Licensing Requirements

MDCA is available with below licenses-:

1. Microsoft 365 E5
2. Microsoft 365 E5 Security
3. Microsoft 365 Compliance (via SKU)
4. Enterprise Mobility & Security E5 (EMS E5)
5. Microsoft Cloud apps Security + Enterprise Mobility & Security E3 (EMS E3)
6. Microsoft Cloud apps Security (standalone license)
7. Microsoft 365 Education A3
8. Microsoft 365 Education A5
9. Office 365 E5
10. Azure Active Directory Premium 1 / Azure AD Premium 2

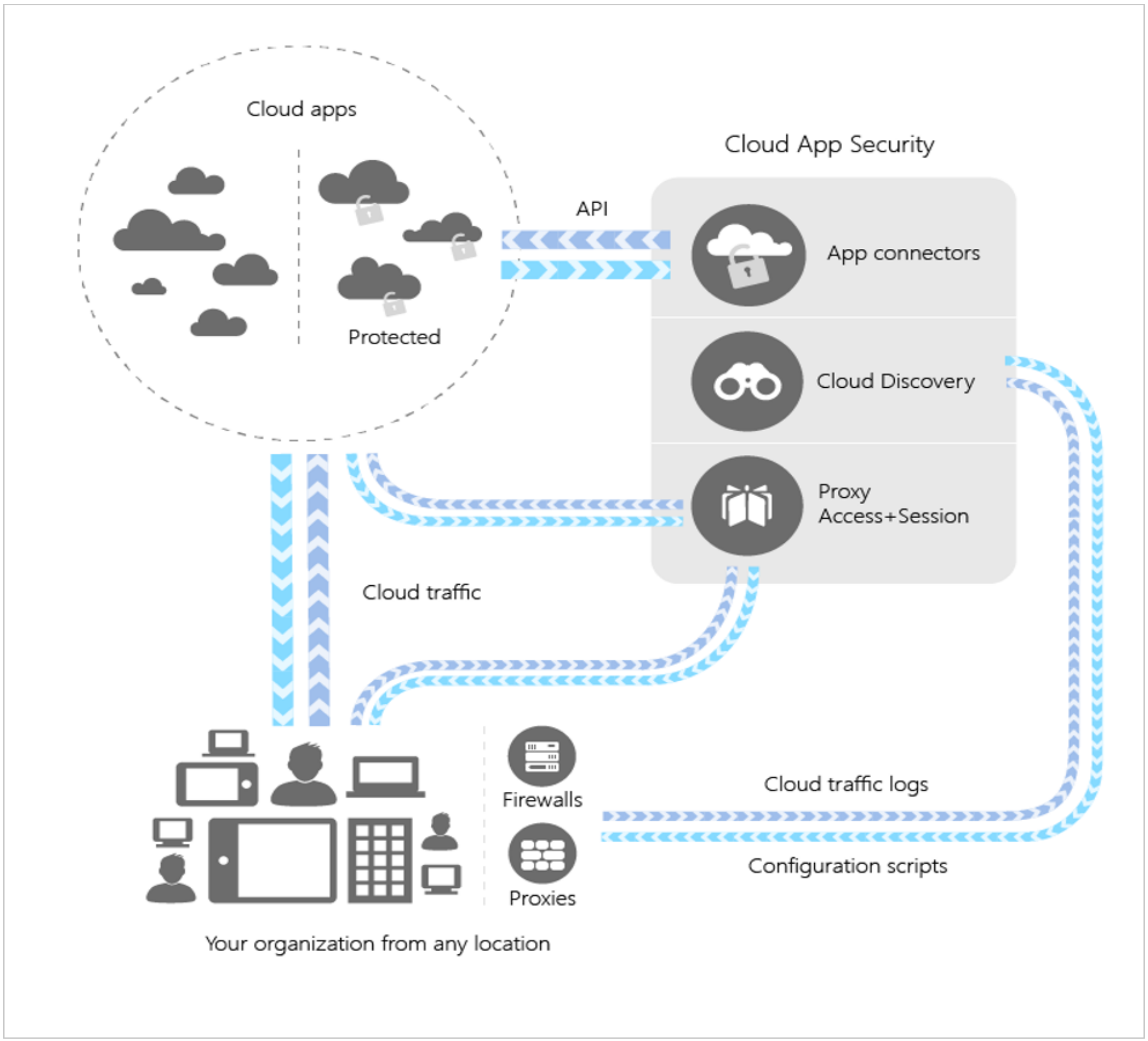
There are few more types but they are relevant to specific countries.

Licensing Datasheet	https://aka.ms/mcaslicensing

Architecture

Cloud apps Security integrates visibility with your cloud by:

- Using Cloud Discovery to map and identify your cloud environment and the cloud apps your organisation is using.
- Sanctioning and unsanctioning apps in your cloud.
- Using easy-to-deploy apps connectors that take advantage of provider APIs, for visibility and governance of apps that you connect to.
- Using Conditional Access apps Control protection to get real-time visibility and control over access and activities within your cloud apps .
- Helping you have continuous control by setting, and then continually fine-tuning, policies.



Features Overview

Setup Guide

This section is a detailed guide for CS and SOC T2 for setting up Product from scratch. What licence to buy, how to deploy it, how to configure it based on the best practices, how to integrate with other products and with MDR service. Everything that is needed for CS/SOC to know during customer onboarding should be clearly explained here. Link any installation guides available internally or from MSFT.

General Setup guide	https://docs.microsoft.com/en-us/cloud-app-security/general-setup

Installation Guide

Prerequisites / Requirements

Quickstart: Get started with Microsoft Defender for Cloud apps	https://docs.microsoft.com/en-us/defender-cloud-apps /get-started

Permissions Overview

Manage admin access	https://docs.microsoft.com/en-us/defender-cloud-apps /manage-admins

Admin User Settings	https://docs.microsoft.com/en-us/defender-cloud-apps /admin-settings
Activity privacy	https://docs.microsoft.com/en-us/defender-cloud-apps /activity-privacy

Installation Steps

Setup Portal, cloud Discovery, Policies, Tags	https://docs.microsoft.com/en-us/defender-cloud-apps /get-started

Configuration Guide

Recommended Configurations, "Best Practice"

Defender for Cloud apps best practices	https://docs.microsoft.com/en-us/defender-cloud-apps /best-practices

Integration Guide

Integration with other MS Products

Microsoft Defender for Cloud apps integrates with Microsoft Defender for Endpoint natively. The integration simplifies roll out of Cloud Discovery, extends Cloud Discovery capabilities beyond your corporate network, and enables device-based investigation.

The native integration enables you to run Cloud Discovery on any device in the corporate network, using public Wi-Fi, while roaming, and over remote access. It also enables device-based investigation.

Integration with MDFE	https://docs.microsoft.com/en-us/defender-cloud-apps /mde-integration
Benefits of using MDCA with MDFE	Watch our videos

It takes up to two hours after you enable the integration for the data to show up in Defender for Cloud apps .

Integration with Azure Sentinel (SIEM / SOAR)

You can integrate Microsoft Defender for Cloud apps with Microsoft Sentinel (a scalable, cloud-native SIEM and SOAR) to enable centralized monitoring of alerts and discovery data.

Benefits of using Microsoft Sentinel include:

- Longer data retention provided by Log Analytics.
- Out-of-the-box visualizations.
- Use tools such as Microsoft Power BI or Microsoft Sentinel workbooks to create your own discovery data visualizations that fit your organizational needs.

Integration with Sentinel	https://docs.microsoft.com/en-us/defender-cloud-apps /siem-sentinel

Microsoft Defender for Cloud apps integration with SWG

To integrate MDCA (Microsoft Defender for Cloud apps) with SWG (Secure Web Gateway),

1. Login to MDCA and configure the API access
2. Configure discovery via Log upload setting in MDCA
3. Verify the logs through governance
4. You can configure blocking of unsanctioned apps
    a. If you want to block an apps before user use it, then goto cloud apps catalog and block

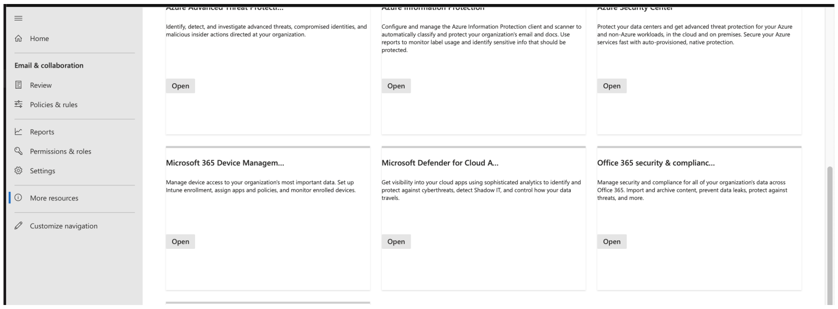
Integration with Open Systems SWG	Microsoft Cloud apps Integration with Secure Web Gateway SWG
Microsoft document for OS SWG integration	https://docs.microsoft.com/en-us/defender-cloud-apps /open-systems-integration

Operations Guide

This section is mostly for SOC T2, providing in depth detail about the product, features, detection, prevention and response capabilities of the product. Here we can link any extra guides on how to work with the product, how to investigate, how to maintain configuration after goLive and any additional supporting documentation which is tied to operations.

How to access MDCA portal from Defender portal

Login to defender portal>> Goto More Resources >> Click on open on the box for Microsoft Defender for cloud apps



Azure Advanced Threat Protecti...

Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Azure Information Protection

Configure and manage the Azure Information Protection client and scanner to automatically classify and protect your organization's email and docs. Use reports to monitor label usage and identify sensitive info that should be protected.

Azure Security Center

Protect your data centers and get advanced threat protection for your Azure and non-Azure workloads, in the cloud and on premises. Secure your Azure services fast with auto-provisioned, native protection.

Microsoft 365 Device Managem...

Manage device access to your organization's most important data. Set up Intune enrollment, assign apps and policies, and monitor enrolled devices.

Microsoft Defender for Cloud A...

Get visibility into your cloud apps using sophisticated analytics to identify and protect against cyberthreats, detect Shadow IT, and control how your data travels.

Office 365 security & complianc...

Manage security and compliance for all of your organization's data across Office 365. Import and archive content, prevent data leaks, protect against threats, and more.

How to create cloud discovery reports?

Guide to create snapshot reports	https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports
Configure automatic log upload for continuous reports	https://docs.microsoft.com/en-us/defender-cloud-apps /discovery-docker

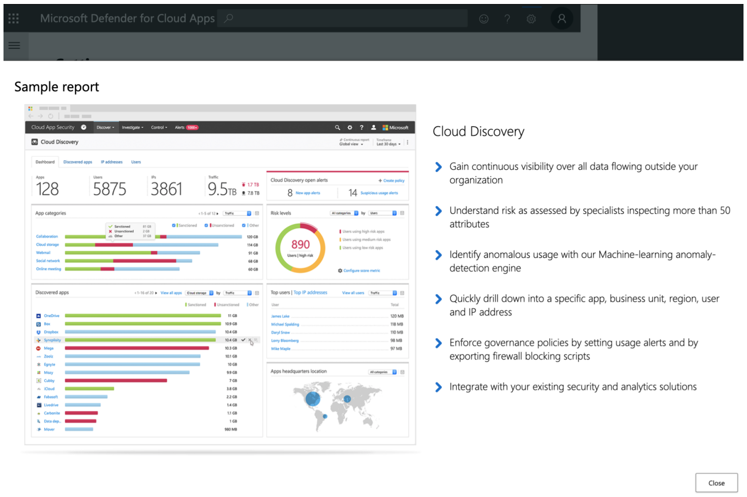
Brief: In cloud discovery snapshot you can select the vendor for which you want to generate e.g bluecoat, Cisco ASA etc. If customer needs to share this report out of the organisation there is an option to Anonymise private information like user name etc. You can also upload logs manually (Files with activities up to 90 days old and up to 1 GB in size per log file). Sample log can also be downloaded for the given log source.

Sample log file needs to be .log and you can upload multiple files in one go.

Once submitted, goto `settings>> cloud discovery>> snapshot reports` and check the status of the report. It will take a while meanwhile chill!

What happens backstage?

Upload → Parse → Data analysis → Generated report



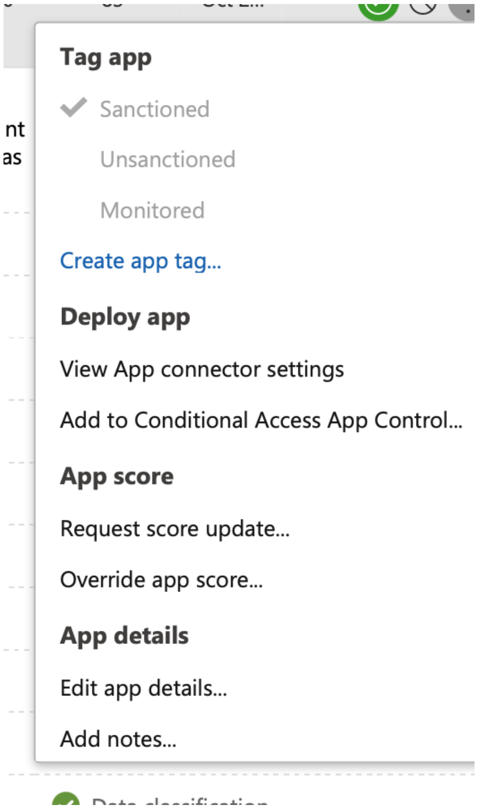
Sample report

Cloud Discovery

- Gain continuous visibility over all data flowing outside your organization
- Understand risk as assessed by specialists inspecting more than 50 attributes
- Identify anomalous usage with our Machine-learning anomaly-detection engine
- Quickly drill down into a specific app, business unit, region, user and IP address
- Enforce governance policies by setting usage alerts and by exporting firewall blocking scripts
- Integrate with your existing security and analytics solutions

Report is interactive and you can use the slider to sort apps by Risk score. Score from 1-3 is a risky application represented by Red colour, 4-7 is medium risk apps shown by Yellow colour and score of 8-10 is safe apps and represented by Green colour. An apps could be risky because it does not in sync with certain compliance standard or there are Security risks like "An apps which remembers password"

From the report opened in the portal, you can do following things with an app-:



Please note: Sometime based on amount of data and analysis required it can take upto 24 hours to generate the report.

Here is the docs page to access various defender portals-:

EDR Defender Access packages and Portal link	https://docs.open.ch/docs/display/MC/EDR+-+Defender+Access+Links

Detection

apps threat detection and remediation	https://docs.microsoft.com/en-us/defender-cloud-apps /app-governance-detect-remediate-overview
Activity Policies (To monitor specific actions by users)	https://docs.microsoft.com/en-us/defender-cloud-apps /user-activity-policies
Behavioural Analytics and Anomaly detection	https://docs.microsoft.com/en-us/defender-cloud-apps /anomaly-detection-policy
OAuth apps policies	https://docs.microsoft.com/en-us/defender-cloud-apps /app-permission-policy

Prevention

Conditional Access apps control	https://docs.microsoft.com/en-us/defender-cloud-apps /proxy-deployment-aad
Onboard and deploy Conditional Access apps control	https://docs.microsoft.com/en-us/defender-cloud-apps /proxy-deployment-any-app
Control over files across your cloud environment	https://docs.microsoft.com/en-us/defender-cloud-apps /control
Control cloud apps with policies	https://docs.microsoft.com/en-us/defender-cloud-apps /control-cloud-apps -with-policies

Investigation & Response

Investigate Cloud apps	https://docs.microsoft.com/en-us/defender-cloud-apps /investigate

Configuration Maintenance

Troubleshooting	https://docs.microsoft.com/en-us/azure/defender-for-cloud/troubleshooting-guide
Troubleshooting cloud discovery	https://docs.microsoft.com/en-us/defender-cloud-apps /troubleshooting-cloud-discovery
Troubleshooting apps Connectors using error messages	https://docs.microsoft.com/en-us/defender-cloud-apps /troubleshooting-api-connectors-using-error-messages
Troubleshooting content inspection	https://docs.microsoft.com/en-us/defender-cloud-apps /troubleshooting-content-inspection
Troubleshooting the SIEM agent	https://docs.microsoft.com/en-us/defender-cloud-apps /troubleshooting-siem
Troubleshooting Microsoft Defender for Cloud apps policies	https://docs.microsoft.com/en-us/defender-cloud-apps /troubleshoot-policies
Troubleshooting access and session controls	https://docs.microsoft.com/en-us/defender-cloud-apps /troubleshooting-proxy
Troubleshooting - What is *.cas.ms, *.mcas.ms, or *. mcas-gov.us?	https://docs.microsoft.com/en-us/defender-cloud-apps /troubleshooting-proxy-url

Training Material

High Level

- Any videos about the service overview / products, configs. I find quite useful to check Microsoft Security Channel

Technical

- Any Ninja Training courses available , MDCA Ninja, MDI Ninja, and more...

Webinars	https://docs.microsoft.com/en-us/defender-cloud-apps /webinars

apps Discovery and Log collector configuration	https://www.microsoft.com/videoplayer/embed/RE4GtTy
Connecting third-party apps	https://www.microsoft.com/videoplayer/embed/RE4GriX
Conditional Access apps control	https://www.microsoft.com/videoplayer/embed/RE4GoIC

FAQ

Question	Answer
Any additional costs?	
Different deployment scenarios?	
Is there a monitoring if agent stops working?	
How do agent updates work?	It works by updating the MDFE agent because it uses to collect information
Current customers with Product?	
How long are logs stored?	Defender for Cloud apps retains data as follows: • Activity log: 180 days • Discovery data: 90 days • Alerts: 180 days • Governance log: 120 days https://docs.microsoft.com/en-us/defender-cloud-apps /cas-compliance-trust
Are there any known issues?	1. Defender for Cloud apps leverages Transport Layer Security (TLS) protocols 1.2+ to provide best-in class encryption. Native client applications and browsers that do not support TLS 1.2+, will not be accessible when configured with session control. However, SaaS apps that use TLS 1.1 or lower will appear in the browser as using TLS 1.2+ when configured with Defender for Cloud apps . 2. Updates which were made for existing issues can be found here https://docs.microsoft.com/en-us/defender-cloud-apps /release-note-archive

In short it is also called as "MDCA". It is a CASB solution which stands for Cloud Access Security Broker.

Applications are widely used now a days and we are surrounded with apps thus monitoring apps is need of the time. apps which appear fine to start with begins to change their behaviour later. With high permissions these apps can be dangerous

It is much productive when integrated with defender for endpoint, this enables you to block any apps which is suspicious.

Antivirus is for multiple OS , In same fashion MDCA is also for multiple clouds.

One strong use case of MDCA is having seperate controls for unmanaged devices for e.g you can prevent download, copy, cut and print of sensitive documents

- File labeling
- Discovering unmanaged cloud apps and blocking their access
- Because it is integrated with Endpoint Defender it can monitor devices when they are outside office network too

Best Practises

- IP addresses tagging or enrichment to reduce false positive. It is defining trusted and untrusted subnets