Discover and Control Shadow IT with Defender for Cloud Apps

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Introduction to Shadow IT

Microsoft Defender for Cloud Apps

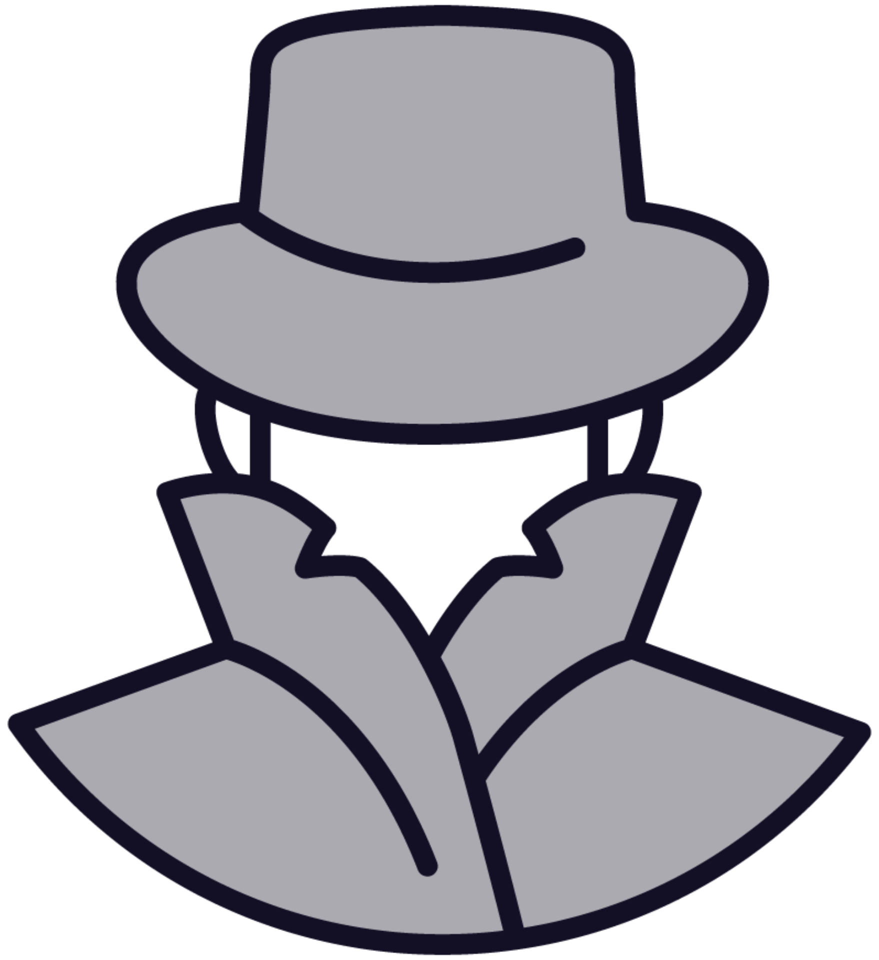
Introduction to Shadow IT

Shadow IT

Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization. It can encompass cloud services, software, and hardware.

https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html

Why Is Shadow IT a Thing?



User needs evolved over time

IT was often too slow to deploy new software

- Or lock it down too much

Users find a way to fill the business need by using consumer tools

Common Example

Users need to share large files with external partners

- Too large for e-mail

IT blocks all external sharing in SharePoint Online

- For “security reasons”

Department gets a Dropbox consumer subscription to share files with the external partners

- IT has no idea

Downsides of Shadow IT

Lack of security

- Often don’t use the most secure identity/ access methods

Lack of compliance

- Tools don’t necessarily follow the right compliance requirements for the business

Lack of integration

- Don’t integrate with other systems which can cause a lack of productivity

At the end of the day, it’s better if users have more permissions/ features inside your IT system rather than them having content somewhere you have no idea about!

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that operates on multiple clouds. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.

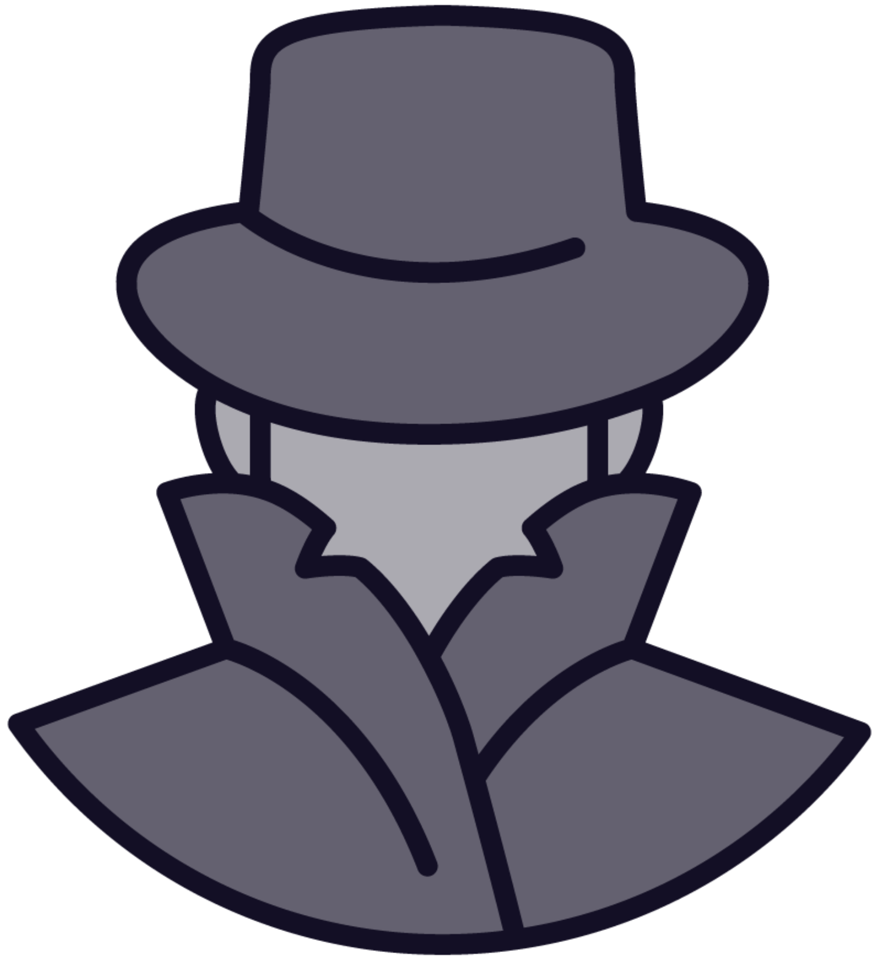
https://learn.microsoft.com/en-us/defender-cloud-apps/

Cloud Access Security Broker (CASB)

Cloud Access Security Brokers 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.

Microsoft

Discover the Use of Shadow IT



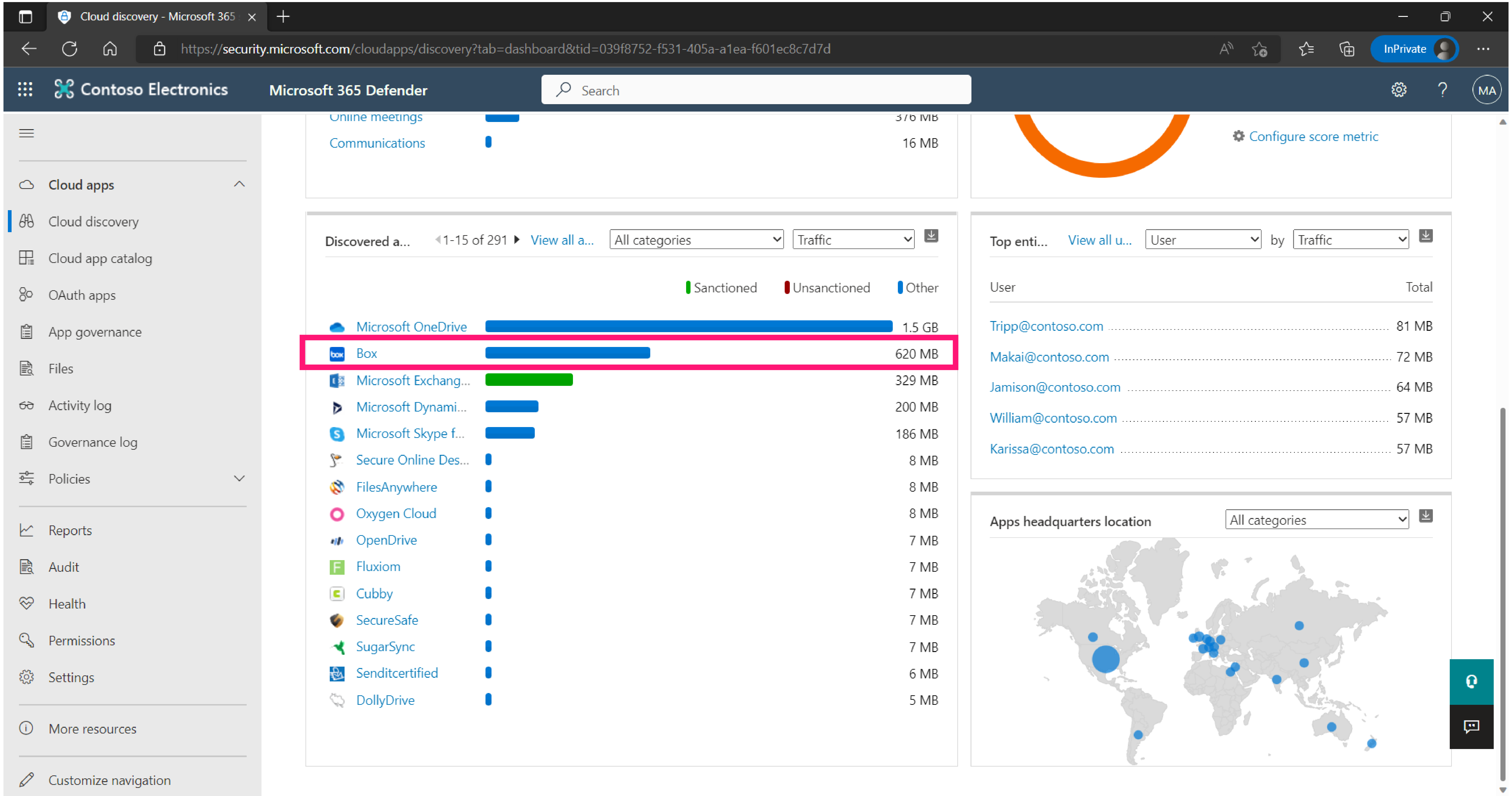
Identify the cloud apps and services used by your organization

Defender for Cloud Apps can import traffic logs directly from your firewall/proxies

- Compare it to an app catalog of over 31,000 cloud apps curated by Microsoft
- Microsoft ranked and scored the apps based on 90+ risk factors

This knowledge can also serve as innovation fuel for new enterprise apps

Defender for Cloud Apps: Discovered Apps



Cloud discovery - Microsoft 365

https://security.microsoft.com/cloudapps/discovery?tab=dashboard&tid=039f8752-f531-405a-a1ea-f601ec8c7d7d

Online meetings	376 MB
Communications	16 MB

Discovered a... 1-15 of 291 View all a... All categories Traffic

🟩 Sanctioned 🟥 Unsanctioned 🟦 Other

Microsoft OneDrive	1.5 GB
Box	620 MB
Microsoft Exchang...	329 MB
Microsoft Dynami...	200 MB
Microsoft Skype f...	186 MB
Secure Online Des...	8 MB
FilesAnywhere	8 MB
Oxygen Cloud	8 MB
OpenDrive	7 MB
Fluxiom	7 MB
Cubby	7 MB
SecureSafe	7 MB
SugarSync	7 MB
Senditcertified	6 MB
DollyDrive	5 MB

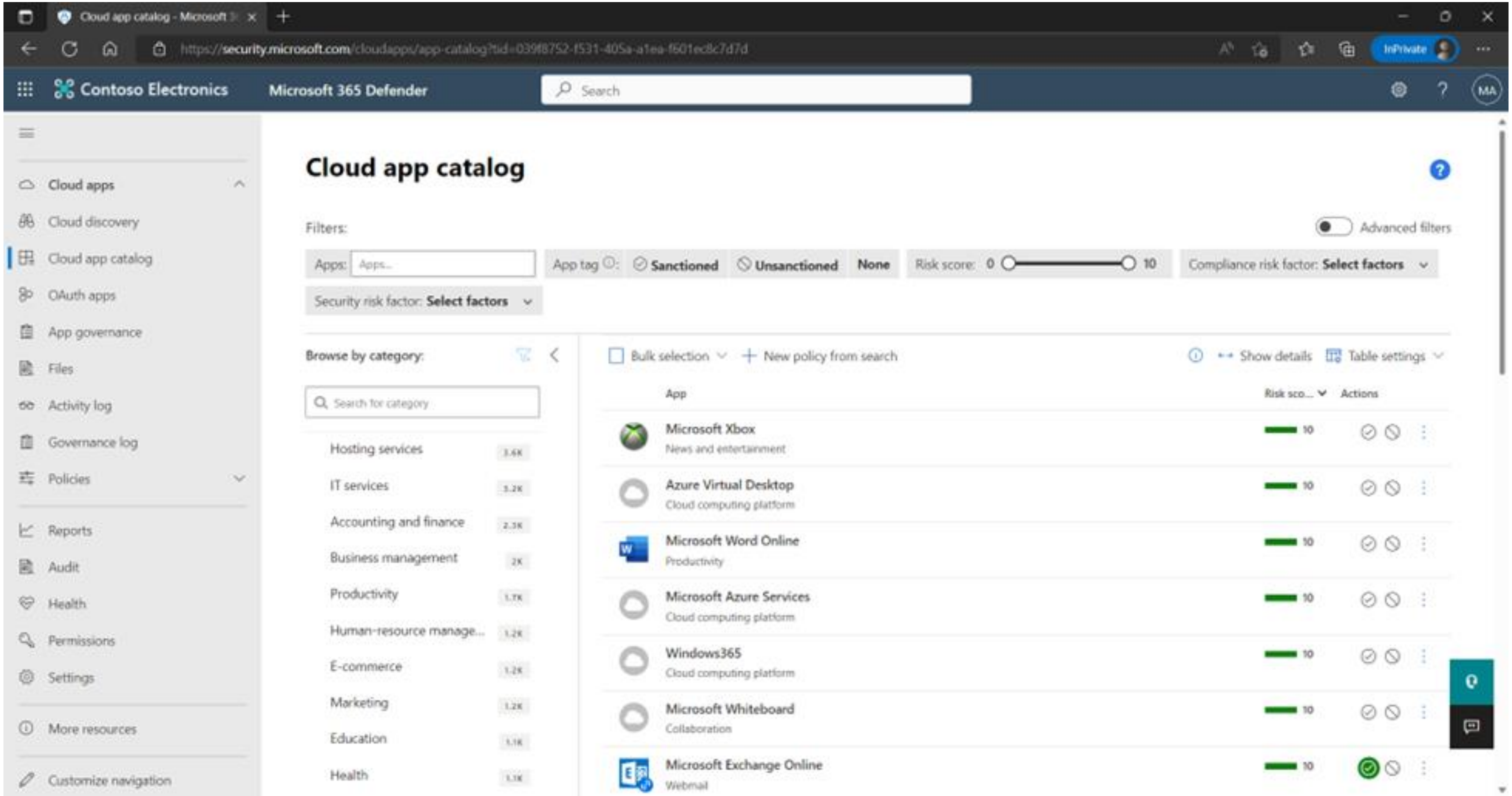
Top enti... View all u... User by Traffic

User	Total
Tripp@contoso.com	81 MB
Makai@contoso.com	72 MB
Jamison@contoso.com	64 MB
William@contoso.com	57 MB
Karissa@contoso.com	57 MB

Apps headquarters location All categories

Source: Microsoft

Defender for Cloud Apps Cloud: App Catalog



Cloud app catalog - Microsoft

https://security.microsoft.com/cloudapps/app-catalog?tid=039f8752-f531-405a-a1ea-f601ec8c7d7d

Contoso Electronics Microsoft 365 Defender

Cloud app catalog

Filters:

Advanced filters

Apps: Apps... | App tag: Sanctioned | Unsanctioned | None | Risk score: 0 – 10 | Compliance risk factor: Select factors

Security risk factor: Select factors

Browse by category:

Hosting services	3.6K
IT services	3.2K
Accounting and finance	2.3K
Business management	2K
Productivity	1.7K
Human-resource manage...	1.2K
E-commerce	1.2K
Marketing	1.2K
Education	1.1K
Health	1.1K

App	Risk sco...	Actions
Microsoft Xbox News and entertainment	10	
Azure Virtual Desktop Cloud computing platform	10	
Microsoft Word Online Productivity	10	
Microsoft Azure Services Cloud computing platform	10	
Windows365 Cloud computing platform	10	
Microsoft Whiteboard Collaboration	10	
Microsoft Exchange Online Webmail	10	

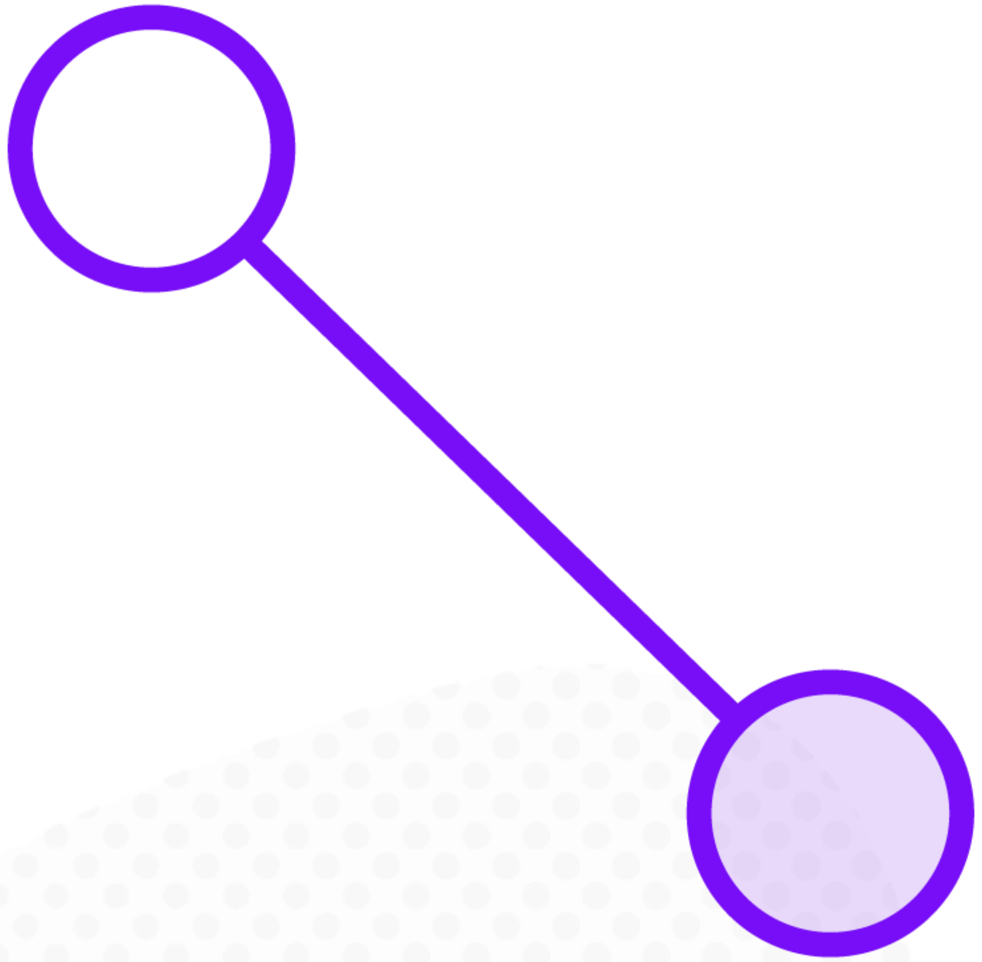
Source: Microsoft

Built-in App Connectors

Defender for Cloud Apps has multiple app connectors allowing you to access information from other apps

- Account Information
- Audit Trail
- Data Scan
- Account Governance
- Data Governance

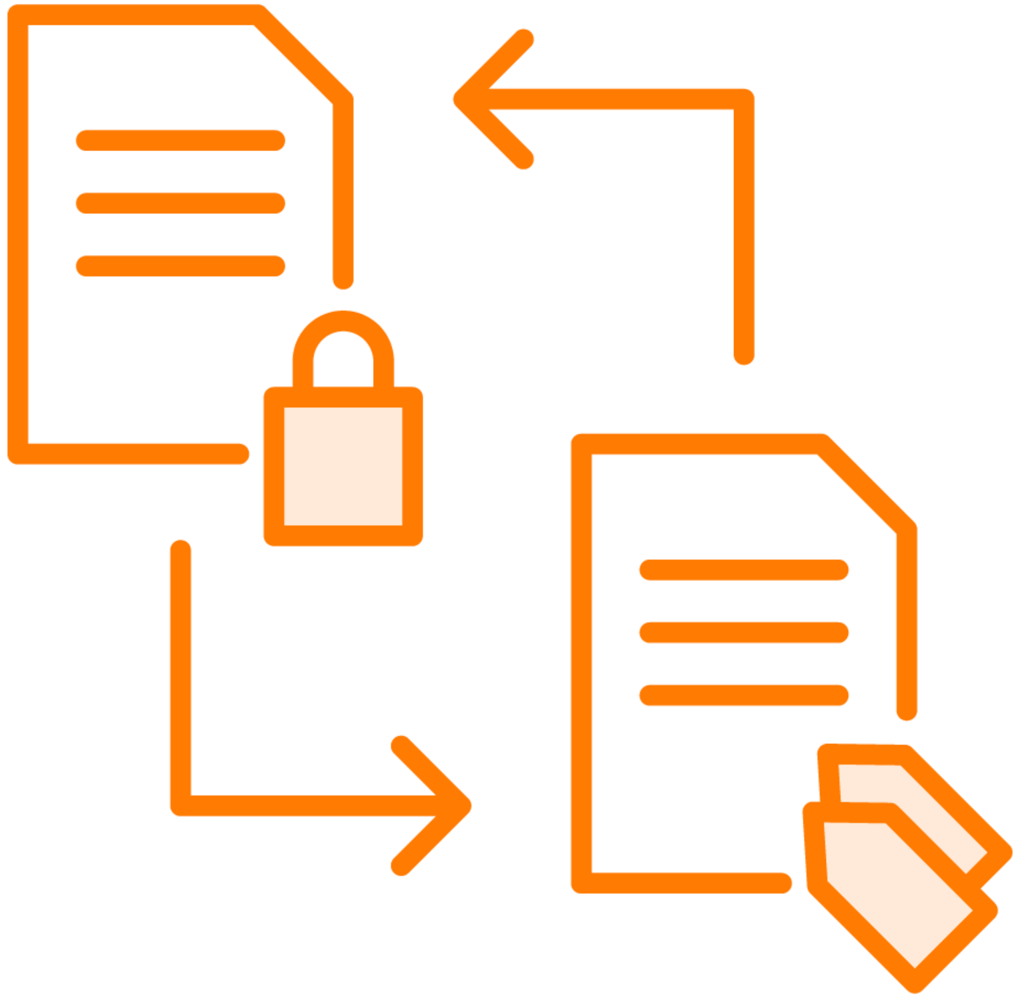
Capabilities depend on third-party app API



Sample Apps with App Connectors

- Box
- Dropbox
- AWS
- ServiceNow
- Google Workspace
- Salesforce

Integrates with Other MS Security & Compliance Tools



Microsoft Defender XDR

Microsoft Purview

- Apply sensitivity labels in other apps
- Data classification to discover sensitive information

Microsoft Sentinel

- Centralized monitoring of alerts and discovery data

Top 20 use cases for CASBs

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3nibJ

Module Conclusion

Introduction to Shadow IT

- Use of IT hardware/software without the knowledge of the IT or security groups

Microsoft Defender for Cloud Apps

- Cloud Access Security Broker
- Discover and control the use of Shadow IT
- Built-in App Connectors
- Integration with other Microsoft security and compliance apps

Up Next:

Course Conclusion