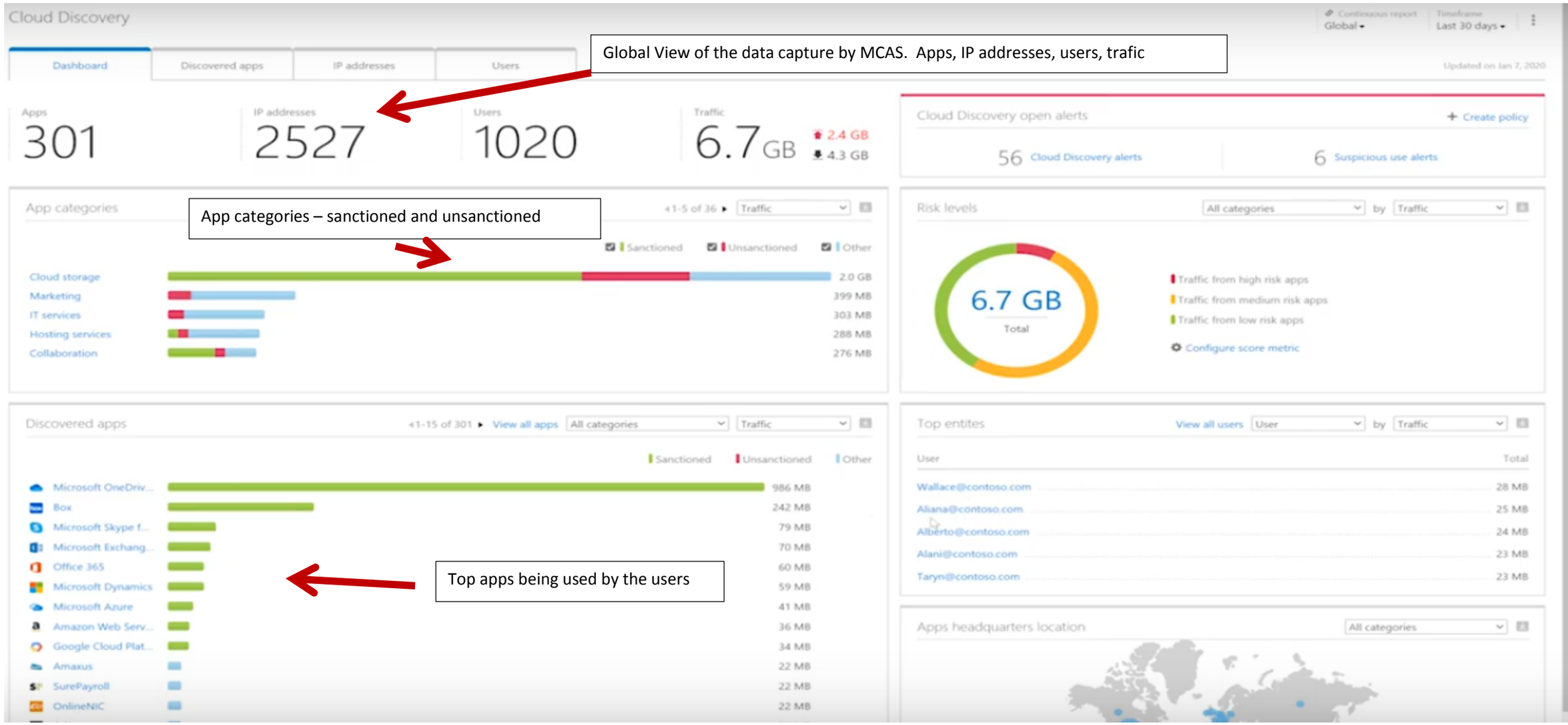
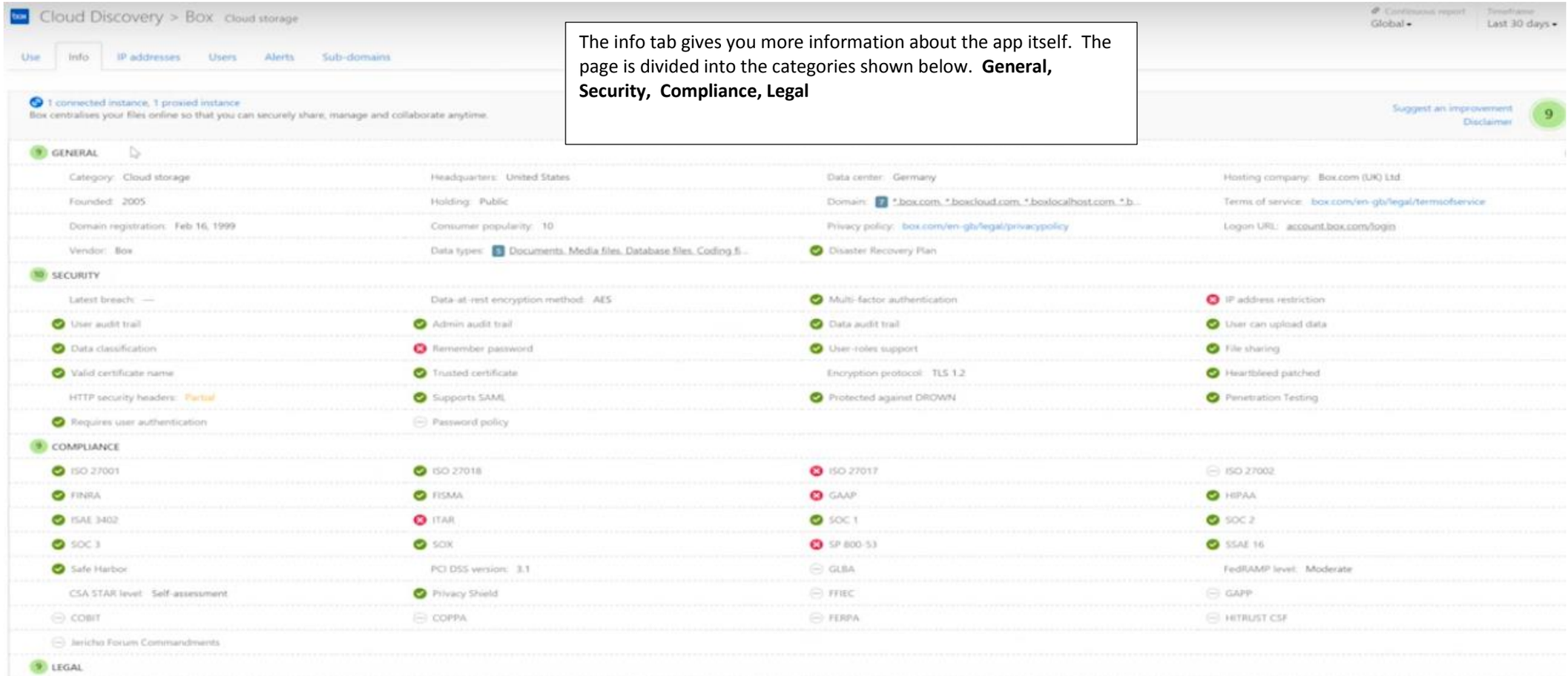
Productivity App Discovery in Office 365 Cloud App Security

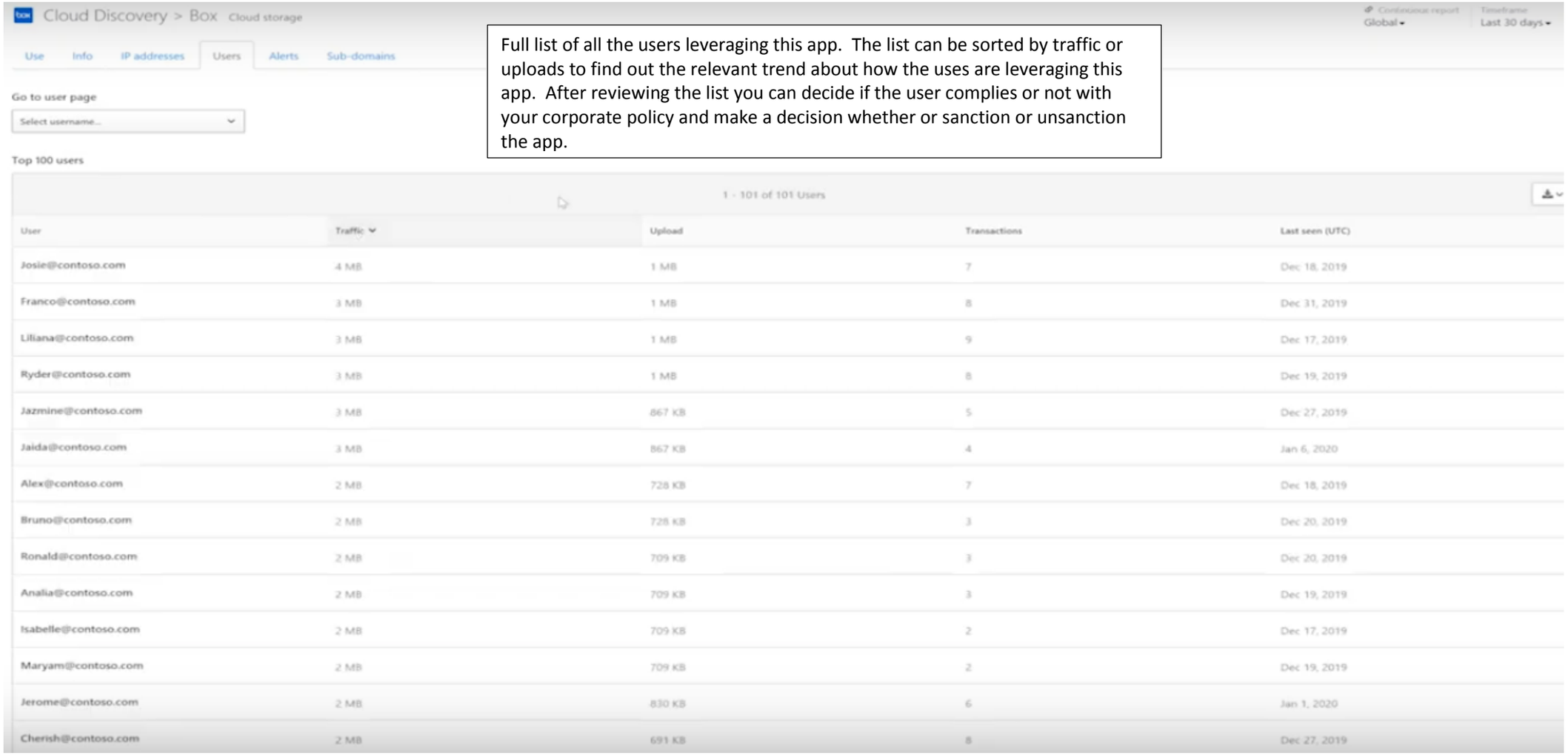
Productivity App Discovery in Office 365 Cloud App Security gives you the ability to understand what cloud services are being used in your organization. Cloud App discovery will get you information about which cloud applications are in use in your environment and whether these are perfectly sanctioned applications like offie 365 or applications that you do not want to see in your environemnt. You will be able to identify shadow IT, risky applications and applications that have potentially suspicious or risky tracffic such as too much upload, which could indicate some kind of data Exploitation.


Cloud Discovery
Dashboard
Discovered apps
IP addresses
Users
Global View of the data capture by MCAS. Apps, IP addresses, users, trafic
Apps
301
IP addresses
2527
Users
1020
Traffic
6.7 GB
2.4 GB
4.3 GB
Cloud Discovery open alerts
Create policy
56 Cloud Discovery alerts
6 Suspicious use alerts
App categories
App categories – sanctioned and unsanctioned
Sanctioned
Unsanctioned
Other
Cloud storage 2.0 GB
Marketing 399 MB
IT services 303 MB
Hosting services 288 MB
Collaboration 276 MB
Risk levels
6.7 GB
Total
Traffic from high risk apps
Traffic from medium risk apps
Traffic from low risk apps
Configure score metric
Discovered apps
Top apps being used by the users
Microsoft OneDriv... 986 MB
Box 242 MB
Microsoft Skype f... 79 MB
Microsoft Exchang... 70 MB
Office 365 60 MB
Microsoft Dynamics 59 MB
Microsoft Azure 41 MB
Amazon Web Serv... 36 MB
Google Cloud Plat... 34 MB
Amaxus 22 MB
SurePayroll 22 MB
OnlineNIC 22 MB
Top entites
User
Total
Wallace@contoso.com 28 MB
Aliana@contoso.com 25 MB
Alberto@contoso.com 24 MB
Alani@contoso.com 23 MB
Taryn@contoso.com 23 MB
Apps headquarters location

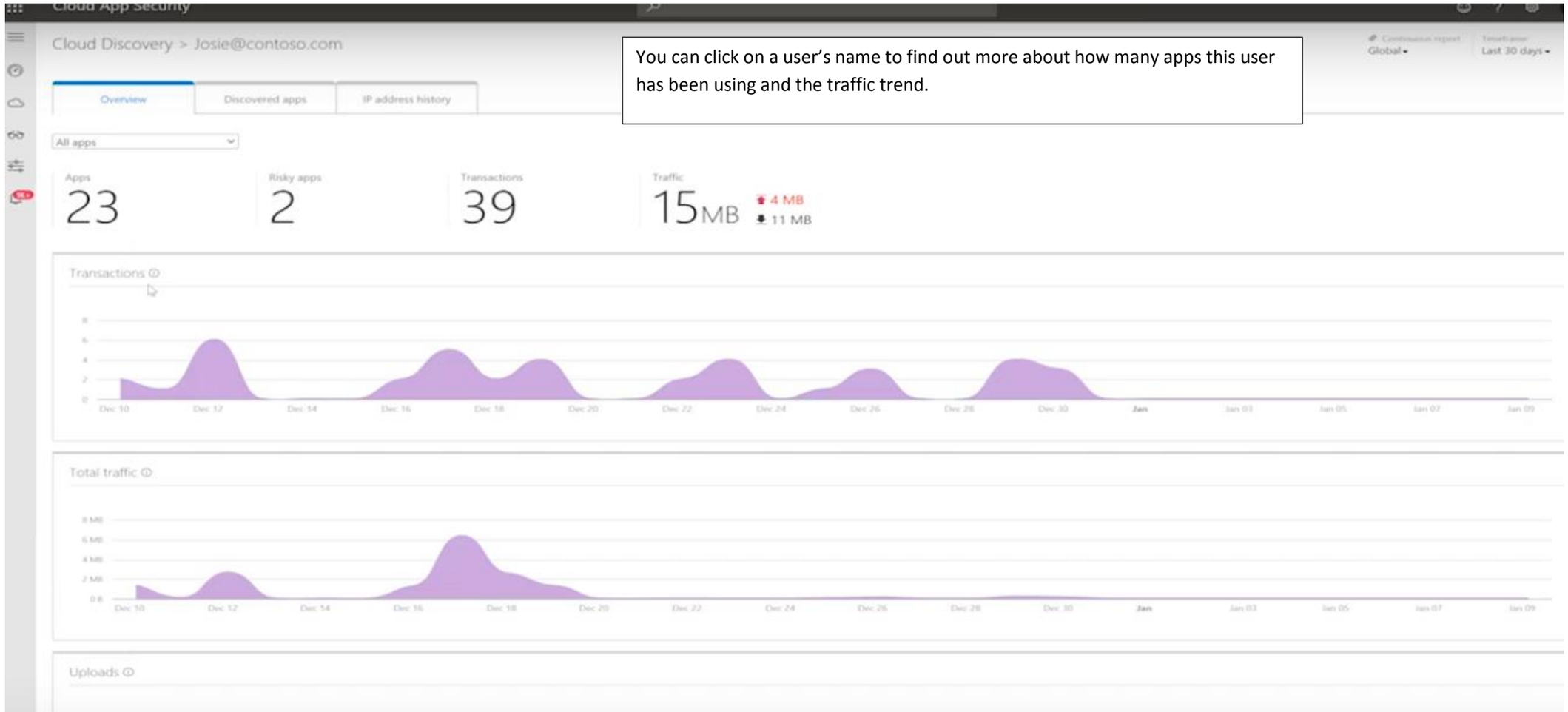

Cloud Discovery > Box Cloud storage
Use
Info
IP addresses
Users
Alerts
Sub-domains
Global
Last 30 days
Investigating Box
Overview
First seen (UTC): Dec 24, 2018
Total active users
Total ip address
Total upload traffic
Total download traffic
523
Total active users
514
Total IP addresses
103 MB
Upload traffic
139 MB
Download traffic
1757
Total transactions
75
Users blocked
25
Users accessed
32
Users warned on access
Trend of usage over the last two days
Users
Total traffic
Active source IP addresses



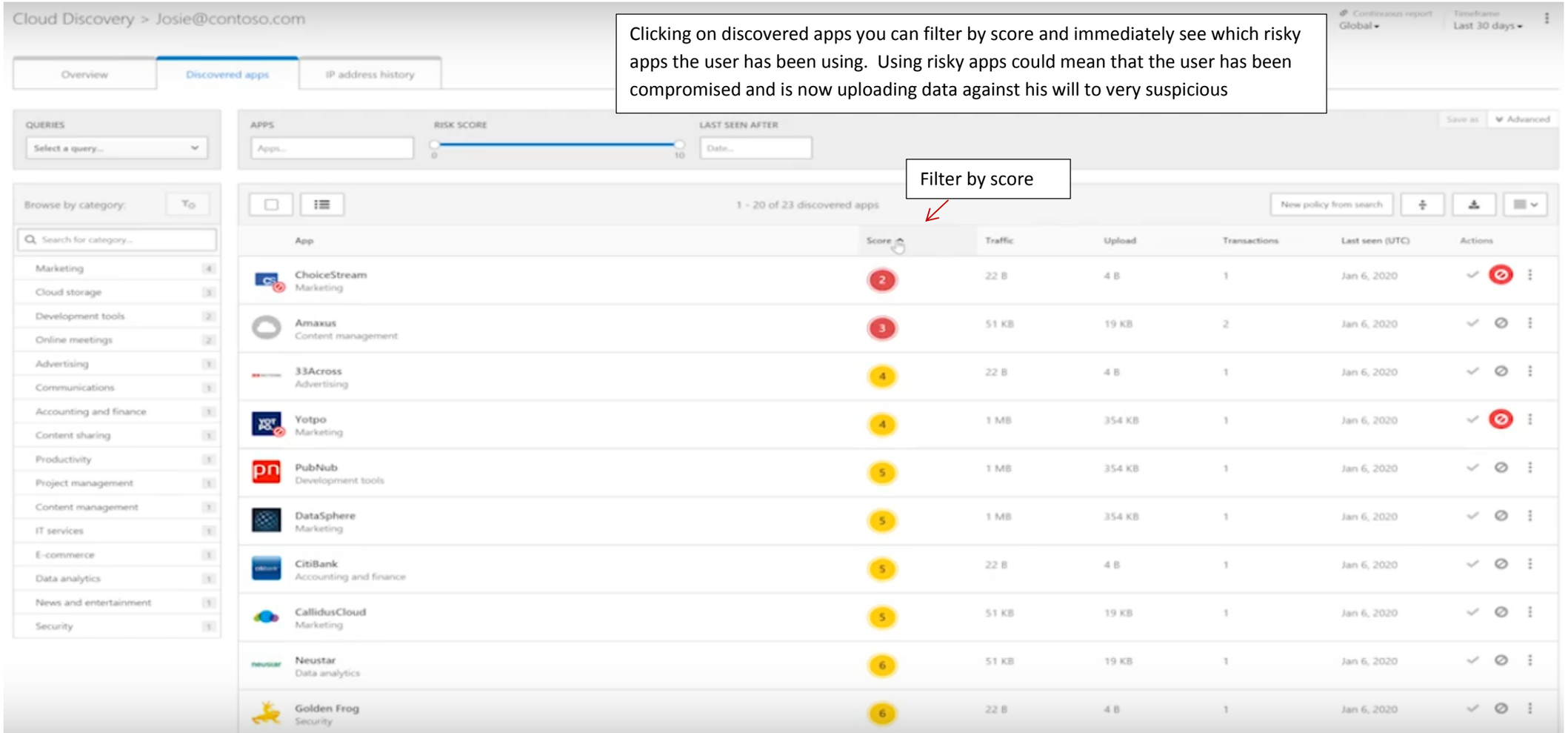
The info tab gives you more information about the app itself. The page is divided into the categories shown below. **General, Security, Compliance, Legal**



Full list of all the users leveraging this app. The list can be sorted by traffic or uploads to find out the relevant trend about how the uses are leveraging this app. After reviewing the list you can decide if the user complies or not with your corporate policy and make a decision whether or sanction or unsanction the app.



You can click on a user's name to find out more about how many apps this user has been using and the traffic trend.


Cloud Discovery > Josie@contoso.com
Clicking on discovered apps you can filter by score and immediately see which risky apps the user has been using. Using risky apps could mean that the user has been compromised and is now uploading data against his will to very suspicious
Filter by score
Overview
Discovered apps
IP address history
QUERIES
APPS
RISK SCORE
LAST SEEN AFTER
Browse by category:
1 - 20 of 23 discovered apps
App
Score
Traffic
Upload
Transactions
Last seen (UTC)
Actions
ChoiceStream
Marketing
Amaxus
Content management
33Across
Advertising
Yotpo
Marketing
PubNub
Development tools
DataSphere
Marketing
CitiBank
Accounting and finance
CallidusCloud
Marketing
Neustar
Data analytics
Golden Frog
Security

HOW DOES ALL THAT DATA GET INTO MICROSOFT CLOUD APP SECURITY

1. **Logs from your firewall are sent to microsoft cloup app security**
2. **Integration with MDATP Microsoft Defender ATP where logs will go from your laptop to MDATP in the cloud.**

How to integrate Microsoft Defender ATP with Cloud App Security

To enable Microsoft Defender ATP integration with Cloud App Security:

1. In the Microsoft Defender ATP portal, from the navigation pane, select **Preferences setup**.
2. In the **Settings** menu, under **General**, select **Advanced features**.
3. Toggle the **Microsoft Cloud App Security** to **On**.
4. Click **Save preferences**.

If you have Microsoft **Cloud App Security** up and running in the same tenant as **MDATP** it's down to a single click: Go to the Advanced Settings in the Windows Defender **Security** Center and **enable** the Microsoft **Cloud App Security** integration.