

Productivity App Discovery in Office 365 Cloud App Security

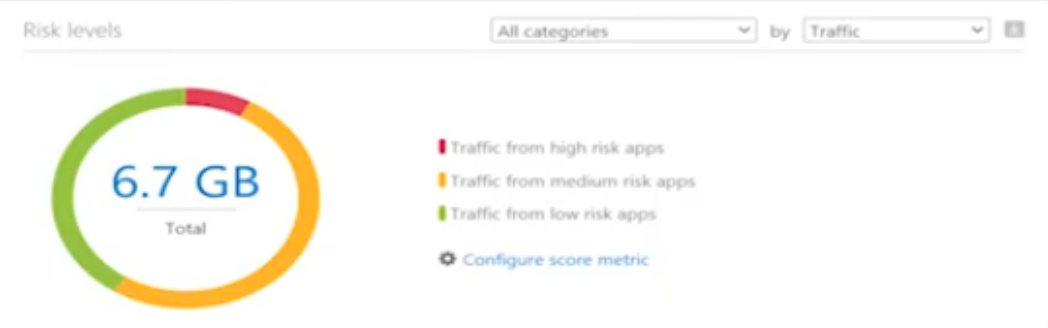
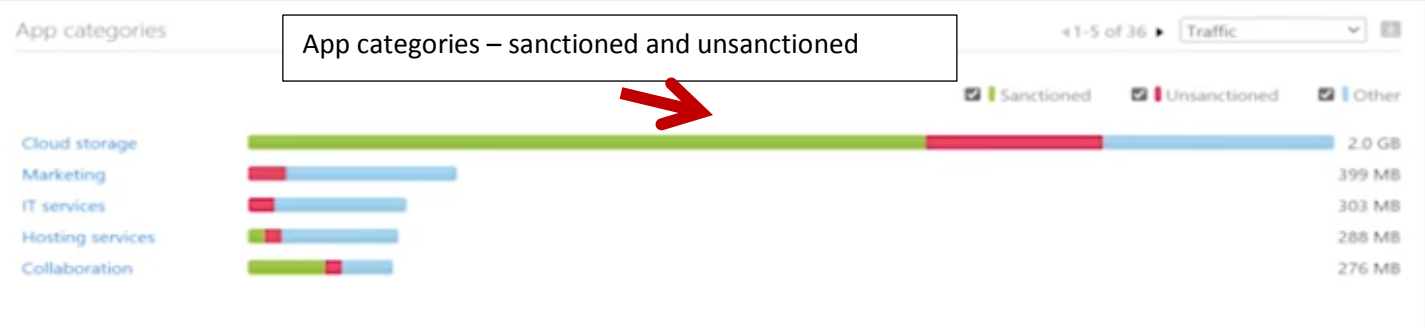
Productivity App Discovery in Office 365 Cloud App Security gives you the ability to understand what cloud services are being used in your organization. Cloud App discovery will get you information about which cloud applications are in use in your environment and whether these are perfectly sanctioned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

Dashboard Discovered apps IP addresses Users

Global View of the data capture by MCAS. Apps, IP addresses, users, traffic

Apps 301 IP addresses 2527 Users 1020 Traffic 6.7 GB 2.4 GB 4.3 GB

Cloud Discovery open alerts 56 Cloud Discovery alerts 6 Suspicious use alerts



Discovered apps

Top apps being used by the users

App	Sanctioned	Unsanctioned	Other	Total
Microsoft OneDrive	~900 MB	~86 MB	~0 MB	986 MB
Box	~200 MB	~42 MB	~0 MB	242 MB
Microsoft Skype for Business	~70 MB	~9 MB	~0 MB	79 MB
Microsoft Exchange Online	~60 MB	~10 MB	~0 MB	70 MB
Office 365	~50 MB	~10 MB	~0 MB	60 MB
Microsoft Dynamics 365	~40 MB	~19 MB	~0 MB	59 MB
Microsoft Azure	~30 MB	~11 MB	~0 MB	41 MB
Amazon Web Services	~20 MB	~16 MB	~0 MB	36 MB
Google Cloud Platform	~10 MB	~24 MB	~0 MB	34 MB
Amaxus	~10 MB	~12 MB	~0 MB	22 MB
SurePayroll	~10 MB	~12 MB	~0 MB	22 MB
OnlineNIC	~10 MB	~12 MB	~0 MB	22 MB

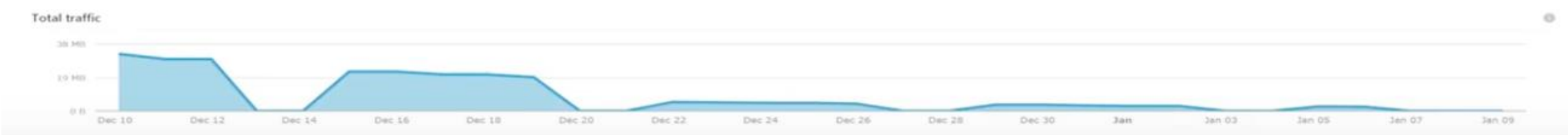
Top entites

User	Total
Wallace@contoso.com	28 MB
Alana@contoso.com	25 MB
Alberto@contoso.com	24 MB
Alani@contoso.com	23 MB
Taryn@contoso.com	23 MB



Investigating Box

Overview



Active source IP addresses

Use Info IP addresses Users Alerts Sub-domains

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

1 connected instance, 1 proxied instance
Box centralises your files online so that you can securely share, manage and collaborate anytime.

Suggest an improvement 9
Disclaimer

GENERAL

Category: Cloud storage	Headquarters: United States	Data center: Germany	Hosting company: Box.com (UK) Ltd
Founded: 2005	Holding: Public	Domain: *.box.com, *.boxcloud.com, *.boxlocalhost.com, *.b...	Terms of service: box.com/en-gb/legal/terms-of-service
Domain registration: Feb 16, 1999	Consumer popularity: 10	Privacy policy: box.com/en-gb/legal/privacy-policy	Login URL: account.box.com/login
Vendor: Box	Data types: Documents, Media files, Database files, Coding fi...	Disaster Recovery Plan	

SECURITY

Latest breach: —	Data-at-rest encryption method: AES	Multi-factor authentication	IP address restriction
User audit trail	Admin audit trail	Data audit trail	User can upload data
Data classification	Remember password	User-roles support	File sharing
Valid certificate name	Trusted certificate	Encryption protocol: TLS 1.2	Heartbleed patched
HTTP security headers: Partial	Supports SAML	Protected against DROWN	Penetration Testing
Requires user authentication	Password policy		

COMPLIANCE

ISO 27001	ISO 27018	ISO 27017	ISO 27002
FINRA	FISMA	GAAP	HIPAA
ISAE 3402	ITAR	SOC 1	SOC 2
SOC 3	SOX	SP 800-53	SSAE 16
Safe Harbor	PCI DSS version: 3.1	GLBA	FedRAMP level: Moderate
CSA STAR level: Self-assessment	Privacy Shield	FFIEC	GAPP
COBIT	COPPA	FERPA	HITRUST CSF
Jericho Forum Commandments			

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.

Go to user page
Select username...

Top 100 users

1 - 101 of 101 Users

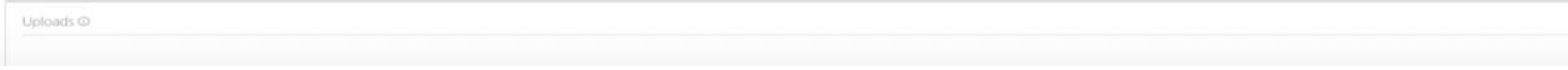
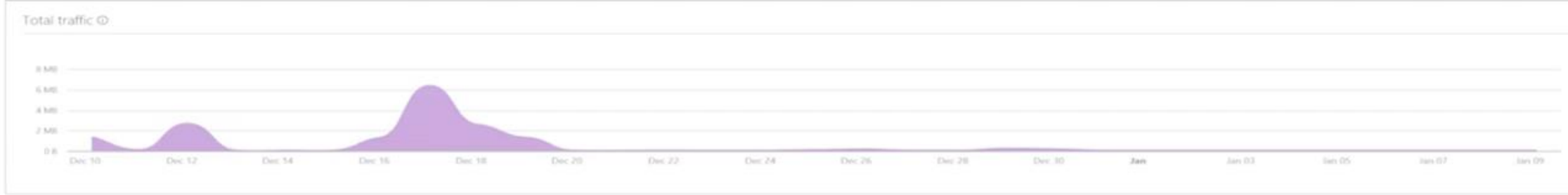
User	Traffic	Upload	Transactions	Last seen (UTC)
Josie@contoso.com	4 MB	1 MB	7	Dec 18, 2019
Franco@contoso.com	3 MB	1 MB	8	Dec 31, 2019
Liliana@contoso.com	3 MB	1 MB	9	Dec 17, 2019
Ryder@contoso.com	3 MB	1 MB	8	Dec 19, 2019
Jazmine@contoso.com	3 MB	867 KB	5	Dec 27, 2019
Jaida@contoso.com	3 MB	867 KB	4	Jan 6, 2020
Alex@contoso.com	2 MB	728 KB	7	Dec 18, 2019
Bruno@contoso.com	2 MB	728 KB	3	Dec 20, 2019
Ronald@contoso.com	2 MB	709 KB	3	Dec 20, 2019
Analia@contoso.com	2 MB	709 KB	3	Dec 19, 2019
Isabelle@contoso.com	2 MB	709 KB	2	Dec 17, 2019
Maryam@contoso.com	2 MB	709 KB	2	Dec 19, 2019
Jerome@contoso.com	2 MB	830 KB	6	Jan 1, 2020
Cherish@contoso.com	2 MB	691 KB	8	Dec 27, 2019

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.

- Overview
- Discovered apps
- IP address history

All apps

Apps: 23
Risky apps: 2
Transactions: 39
Traffic: 15MB (4 MB ↓, 11 MB ↓)



Overview **Discovered apps** IP address history

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

QUERIES
Select a query...

APPS RISK SCORE LAST SEEN AFTER
Apps... 0 10 Date...

- Browse by category:
- Marketing 4
 - Cloud storage 3
 - Development tools 2
 - Online meetings 2
 - Advertising 1
 - Communications 3
 - Accounting and finance 3
 - Content sharing 3
 - Productivity 3
 - Project management 3
 - Content management 3
 - IT services 3
 - E-commerce 3
 - Data analytics 3
 - News and entertainment 1
 - Security 1

Filter by score

1 - 20 of 23 discovered apps

App	Score	Traffic	Upload	Transactions	Last seen (UTC)	Actions
ChoiceStream Marketing	2	22 B	4 B	1	Jan 6, 2020	✓ ⚠ ⋮
Amaxus Content management	3	51 KB	19 KB	2	Jan 6, 2020	✓ ⚠ ⋮
33Across Advertising	4	22 B	4 B	1	Jan 6, 2020	✓ ⚠ ⋮
Yotpo Marketing	4	1 MB	354 KB	1	Jan 6, 2020	✓ ⚠ ⋮
PubNub Development tools	5	1 MB	354 KB	1	Jan 6, 2020	✓ ⚠ ⋮
DataSphere Marketing	5	1 MB	354 KB	1	Jan 6, 2020	✓ ⚠ ⋮
CitiBank Accounting and finance	5	22 B	4 B	1	Jan 6, 2020	✓ ⚠ ⋮
CallidusCloud Marketing	5	51 KB	19 KB	1	Jan 6, 2020	✓ ⚠ ⋮
Neustar Data analytics	6	51 KB	19 KB	1	Jan 6, 2020	✓ ⚠ ⋮
Golden Frog Security	6	22 B	4 B	1	Jan 6, 2020	✓ ⚠ ⋮

HOW DOES ALL THAT DATA GET INTO MICROSOFT CLOUD APP SECURITY

1. Logs from your firewall are sent to microsoft clou 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.