

# Down In the Weeds, Up In the Cloud: Security

Azure, Microsoft 365 and all things Security, with Splunk!

*socially-distant edition!*

**Ryan Lait**

Senior Sales Engineer | Splunk



# Forward-Looking Statements



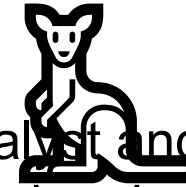
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

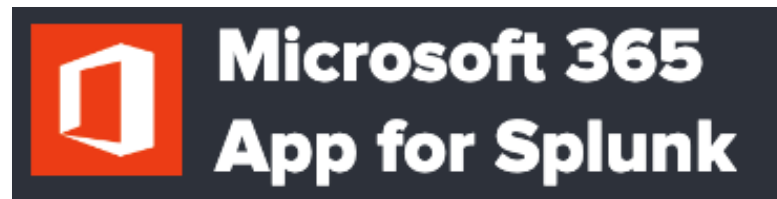
Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2020 Splunk Inc. All rights reserved

# Ryan Lait AU

Senior Sales Engineer | Splunk

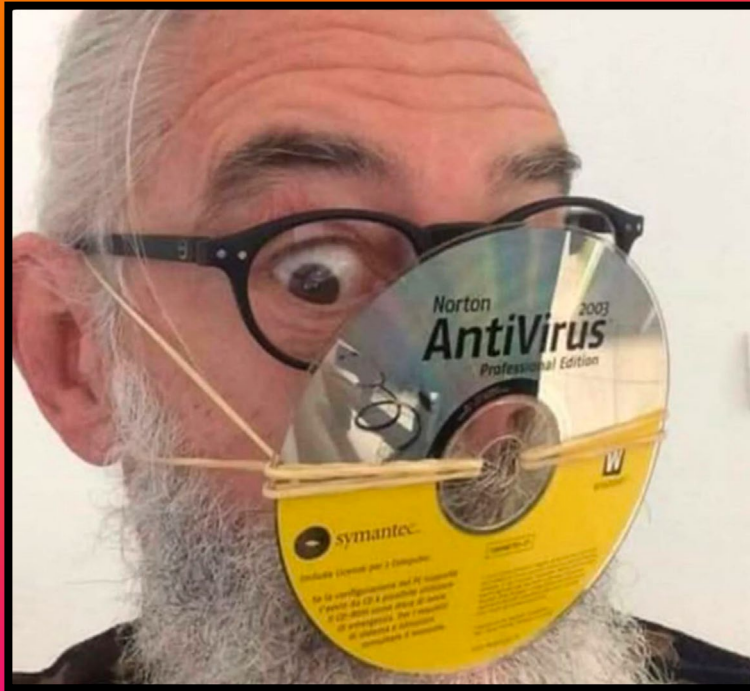


- Former cyber security analyst and Splunk customer
- Likes: Obstacle course racing, home automation
- Dislikes: Pie Charts



# Agenda

Stay safe and wash your hands



## 1. Microsoft 365

What's new and interesting?

## 2. Microsoft Teams

Call Record data and other juicy security data

## 3. Microsoft Azure

What's the latest?

## 4. Microsoft Azure

No more hating NSG flow logs!

## 5. Appendix

Download the slides for this!

# Firstly..

conf.splunk.com

Security All Skill Levels

## SEC1059C - Down in the Weeds, Up in the Cloud: Security

[Ryan Lait](#), Senior Sales Engineer, Splunk

.conf19 IT Operations All Skill Levels

## IT1433 - Down in the Weeds, Up in the Cloud: IT Ops

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud, Splunk IT Service Intelligence

Session Video

Session Slides

[Ry Lait](#), Senior Sales Engineer, Splunk

.conf18 Security, Compliance and Fraud Intermediate

## SEC1355 - Hunting the Known Unknown: Microsoft Cloud

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Enterprise Security

Session Video

Session Slides

[Ryan Kovar](#), Principal Security Strategist, Splunk

[Steve Brant](#), Senior Security Strategist, Splunk

.conf18 Security, Compliance and Fraud All Skill Levels

## SEC1297 - Down in the Weeds, Up in the Cloud: Splunking Your Azure and Office 365

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security

Session Video

Session Slides

[Ryan Lait](#), Senior Sales Engineer, Splunk

.conf19 Foundations/Platform Intermediate

## FN1328 - Show and Tell: Prescriptive Use Cases for Azure and Office 365

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Enterprise Security, Splunk Machine Learning Toolkit

Session Video

Session Slides

[Jason Conger](#), Solution Architect, Splunk

[Ry Lait](#), Senior Sales Engineer, Splunk

.conf19 Security, Compliance and Fraud All Skill Levels

## SEC1432 - Down in the Weeds, Up in the Cloud: Security

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security

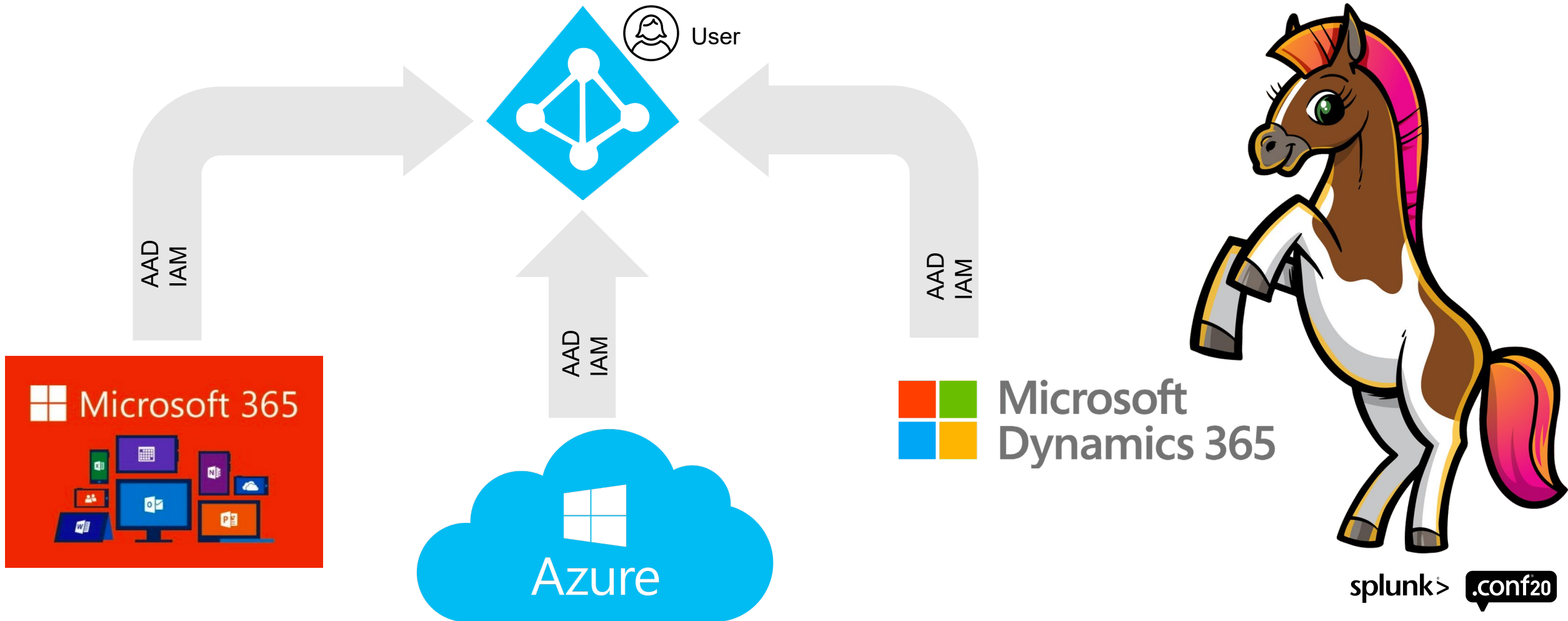
Session Video

Session Slides

[Ry Lait](#), Senior Sales Engineer, Splunk

# Secondly... A Word About Azure Active Directory

Identity and Access Management (IAM)



**.conf20**  
splunk>



# Office Microsoft 365

---

# An Admin Center for All Occasions!

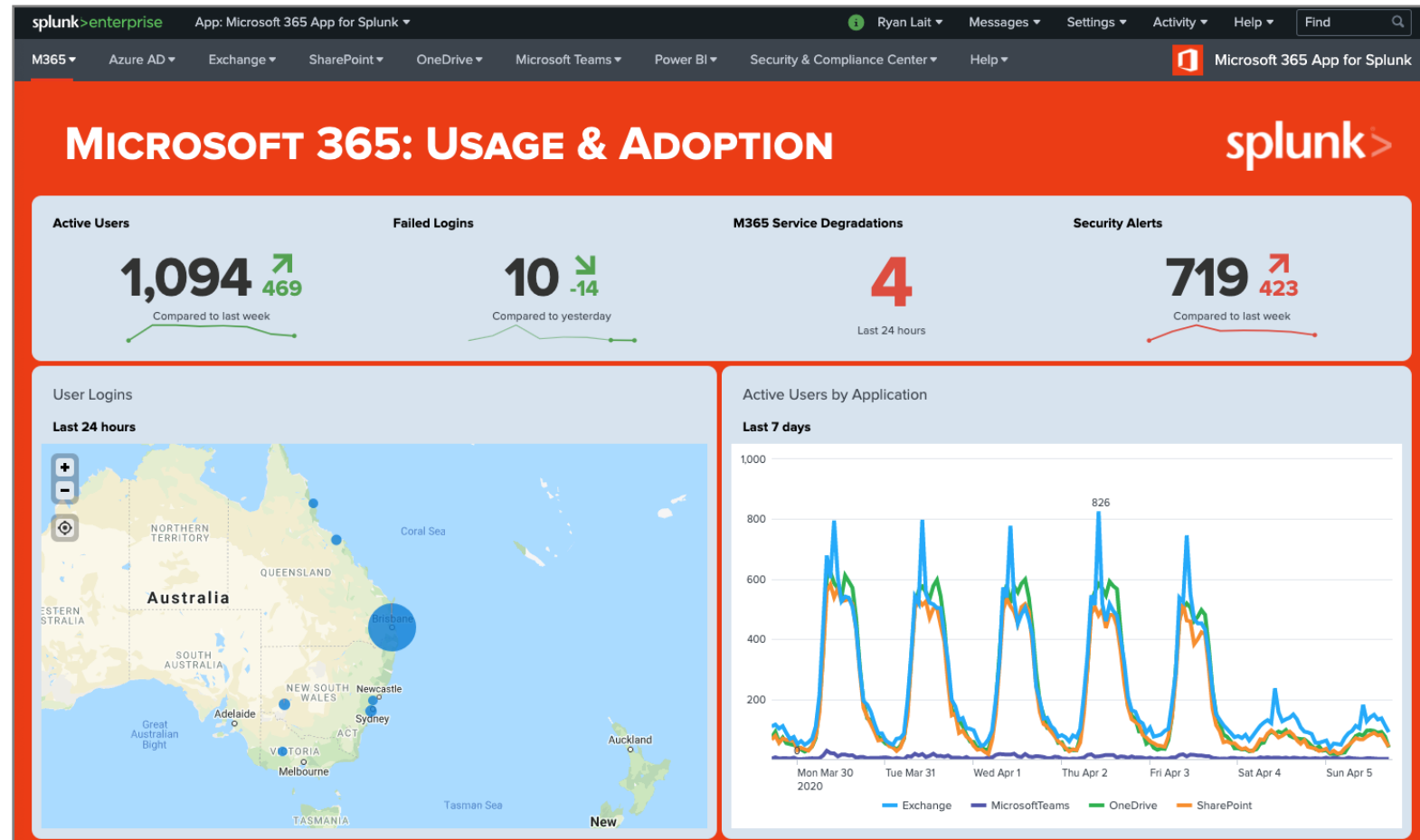




# Microsoft 365 App for Splunk

[splunkbase.splunk.com/app/3786](https://splunkbase.splunk.com/app/3786)

- M365 Service Status
- Azure Active Directory
- Exchange Online
- OneDrive
- SharePoint
- Microsoft Teams
- PowerBI
- Security & Compliance Center

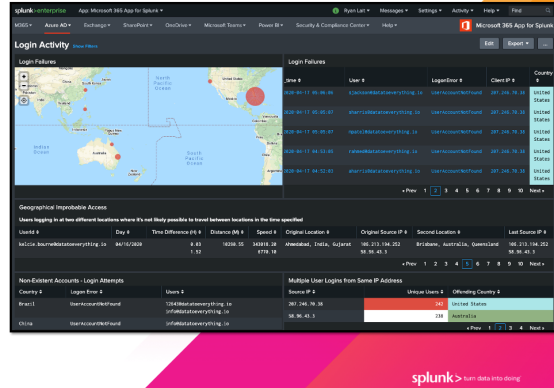


# Microsoft 365 App for Splunk

[splunkbase.splunk.com/app/3786](https://splunkbase.splunk.com/app/3786)

## Azure Active Directory

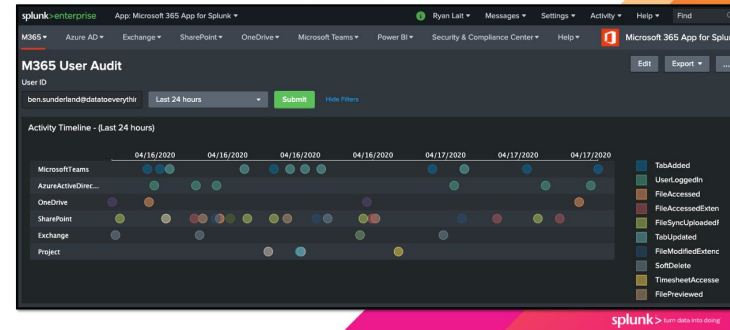
- Geo-based login tracking
- Login failure details
- Suspicious login activity
- Non-existent account login attempts



splunk> turn data into doing

## User Audit

Track user activity across multiple workloads in an instant

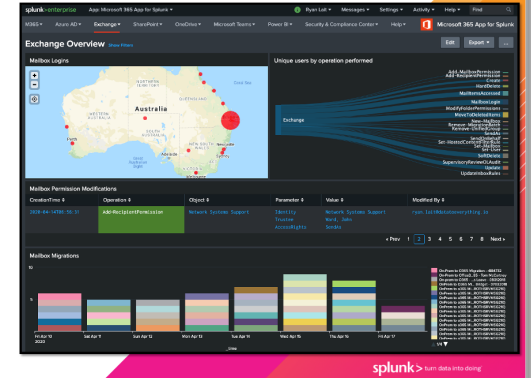


splunk> turn data into doing

## Exchange Online

- Mailbox Logins
- Exchange operation activity
- Mailbox permission changes
- On-Prem to M365 mailbox migrations
- Bot and Connector details

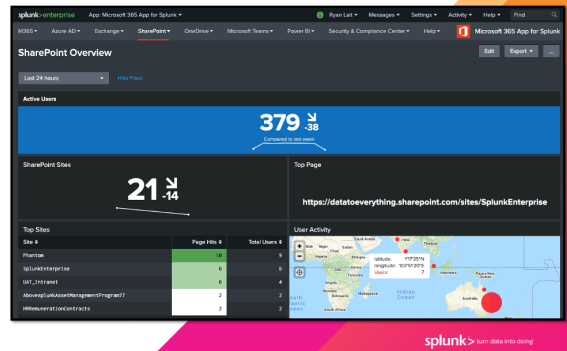
- Note**
- M365 Add-on does not ingest message tracking logs
  - These are ingested separately using [Microsoft Office 365 Reporting Add-on for Splunk](#)



splunk> turn data into doing

## SharePoint Online

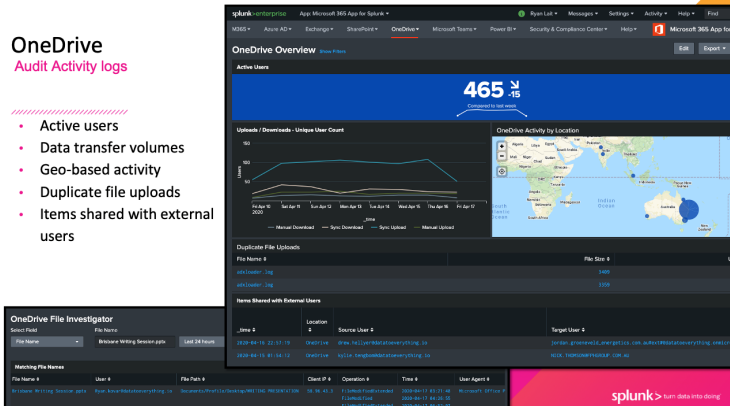
- Active users
- Site creations
- Top sites / pages
- Access activity
- Item audit
- Geographical access



splunk> turn data into doing

## OneDrive

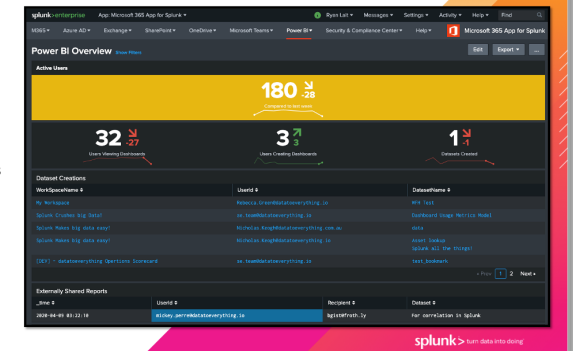
- Active users
- Data transfer volumes
- Geo-based activity
- Duplicate file uploads
- Items shared with external users



splunk> turn data into doing

## PowerBI

- Active users
- Dashboard activity
- Dataset activity
- Dataset creations
- Externally shared reports



splunk> turn data into doing

**.conf20**  
splunk>

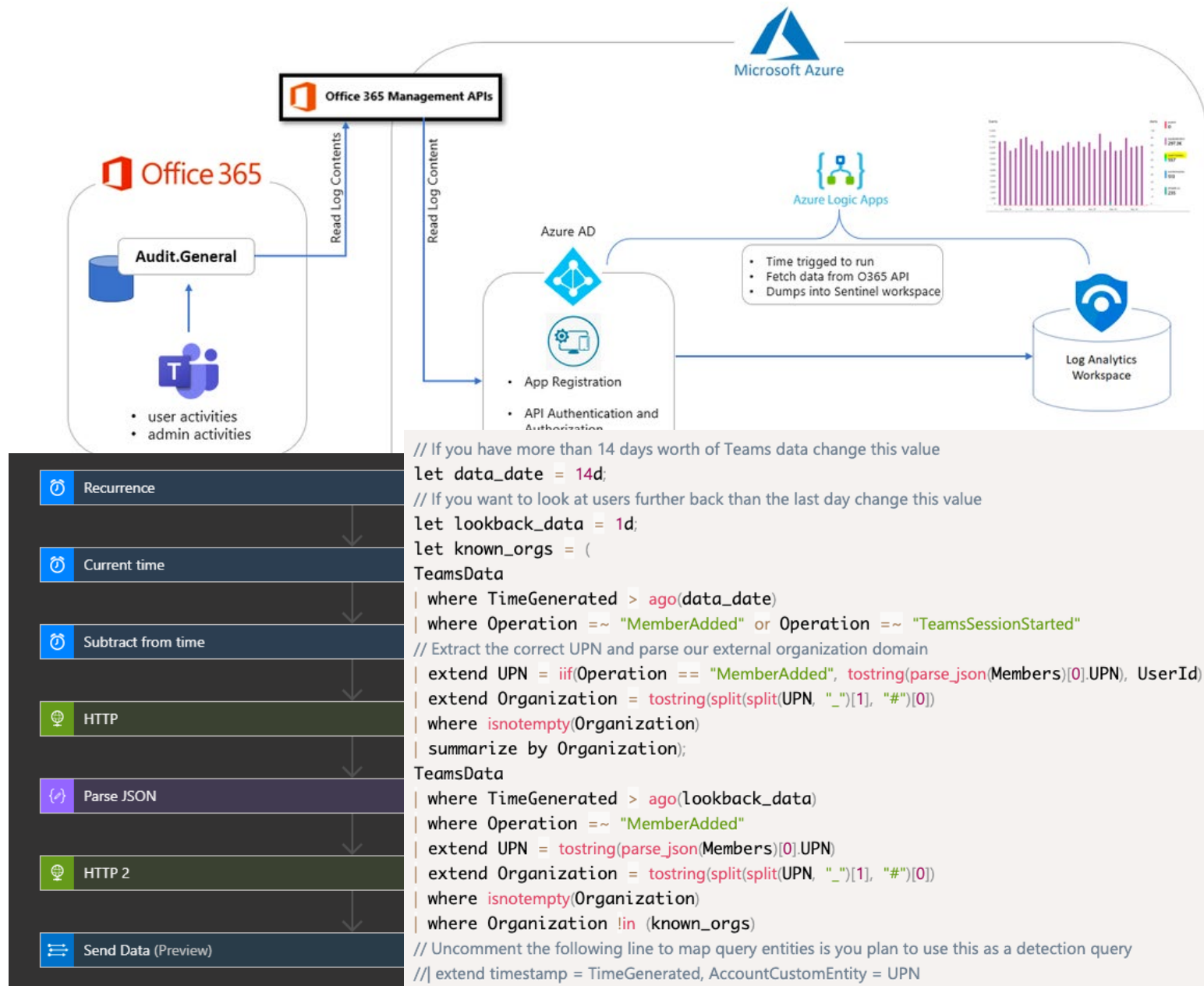


# Microsoft Teams

---

# Microsoft Teams The Sentinel Way...

1. Create app registration
2. Register API subscription
3. Deploy logic app
4. Parse data
5. Write query
  - 5.1 Understand query
  - 5.2 Write another query...



# Microsoft Teams

## The Splunk way

- External users added
- Short-lived external accounts
- Bot & Connector activity
- Team ownership activity
- Team deletions and modifications
- Aligned to Mitre ATT&CK!

splunk > enterprise App: Microsoft 365 App for Splunk

M365 > Azure AD > Exchange > SharePoint > OneDrive > **Microsoft Teams** > Power BI > Security & Compliance Center > Help

Microsoft 365 App for Splunk

### Teams Security Monitoring [Show Filters](#)

Edit Export ...

# 72

External Users Added

# 24

Observed External Domains

# 19

Teams Deleted

#### External Users Added

Users added from external organizations

Timestamp	External User	Added To	Item Name	Added By	External Domain
2020-04-16T00:35:00	c.mowat@uqhealthcare.org.au	Team	PACE Diabetes	alison.cunnington@dataoeverthing.io	uqhealthcare.org.au
2020-04-16T00:27:58	adb52@hotmail.com	Team	Splunk Demo	ryan.lait@dataoeverthing.io	hotmail.com
2020-04-16T00:24:02	lee.baker@cisco.com	Team	Technology Services Transition Project	mickey.perre@dataoeverthing.io	cisco.com
2020-04-16T00:23:59	adb52@hotmail.com	Team	Splunk Demo	ryan.lait@dataoeverthing.io	hotmail.com
2020-04-16T00:18:57	peter.solomon@cisco.com	Team	Technology Services Transition Project	mickey.perre@dataoeverthing.io	cisco.com
2020-04-16T00:11:55	gabrielbarwell@gmail.com	Team	Family	wendy.barwell@dataoeverthing.io	gmail.com
2020-04-16T00:10:58	susannahoffmann@gmail.com	Team	Splunk Demo	ryan.lait@dataoeverthing.io	gmail.com
2020-04-16T00:10:54	declan.real@hotmail.com	Team	Integrated Live Run	peter.hoskins@dataoeverthing.io	hotmail.com
2020-04-16T00:08:56	oelkalla@microsoft.com	Team	SQL 2019 PoC	chris.nunn@dataoeverthing.io	microsoft.com
2020-04-16T00:00:57	craig.knight-dawson@brennanit.com.au	Team	Technology Services Transition Project	mickey.perre@dataoeverthing.io	brennanit.com.au

< Prev 1 2 3 4 5 6 7 8 9 10 Next >

#### Short Lived External Accounts

External accounts added and removed in within 24 hours


External Account	Team/Channel	Added & Removed From	Internal User	Added	Removed	Mins between Add/Remove
nish.wartski@gmail.com	Team	Splunk Demo	ryan.lait@dataoeverthing.io	04/15/2020 17:59:11	04/15/2020 18:00:13	1.0
cbtouch@anet.com	Team	Fun Committee	stephen.brand@dataoeverthing.io	04/15/2020 19:35:23	04/15/2020 19:59:24	24.0
steve.otto@felonsbrewingco.com.au	Team	Contractor's Meeting	tim.smot@dataoeverthing.io	04/16/2020 04:10:15	04/16/2020 04:56:22	46.1

# Microsoft Teams

## Call Record Forensics

- External user calls
- Device analysis
- Participant locations
- User-based analysis of activity

 **Microsoft Teams Add-on for Splunk**

★★★★★ 1 rating  Splunk AppInspect Passed

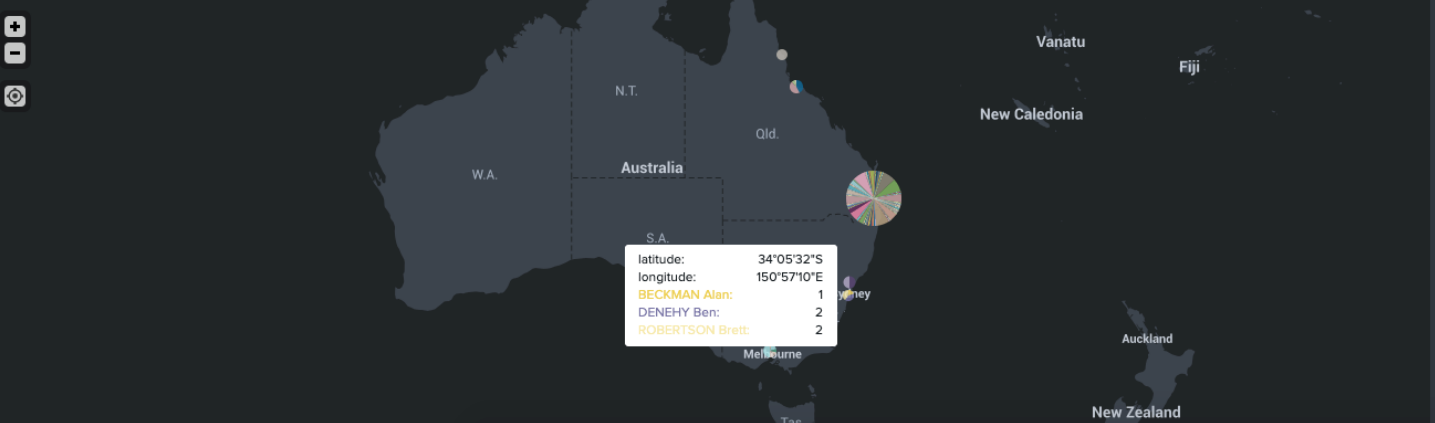
splunk>enterprise App: Microsoft 365 App for Splunk Ryan Lait Messages Settings Activity Help Find

M365 Azure AD Exchange SharePoint OneDrive Microsoft Teams Power BI Security & Compliance Center Help Microsoft 365 App for Splunk

### Call Record Forensics

_time	Participants	Organizer	Tenant ID	Source IP	Connection Type	Duration	Platform	Product Family
2020-08-13 13:34:17.929	External user SEPTEMBER Gavin	SEPTEMBER Gavin	7db2bee6-535c-4748-bf78-c30733511bcd	122.109.228.195	wifi	2 mins	windows	skypeForBusiness
2020-08-13 13:30:06.907	External user KAN Jessica	KAN Jessica	7448469d-8ba5-44d4-a43c-8d7ff6fb550d	203.8.131.212	wired	5 mins	unknown	skypeForBusiness
2020-08-13 13:30:06.907	External user KAN Jessica	KAN Jessica	7448469d-8ba5-44d4-a43c-8d7ff6fb550d	203.8.131.212	wired	5 mins	windows	skypeForBusiness
2020-08-13 13:23:44.109	BYRD Ben WAKE Chris	WAKE Chris	d16de530-94e7-4158-b7e2-6ee220af628d	203.8.131.216	wired	2 mins	windows	teams
2020-08-13 13:23:52.840	LARKIN Andrew SWAIN Randall	LARKIN Andrew	d16de530-94e7-4158-b7e2-6ee220af628d	138.217.37.196	wired	2 mins	windows	teams

< Prev 1 2 3 4 5 6 7 8 9 10 Next >



**.conf20**  
splunk>



# Microsoft Azure

---

# Don't Forget!

[conf.splunk.com](https://conf.splunk.com)

Security All Skill Levels

## SEC1059C - Down in the Weeds, Up in the Cloud: Security

[Ryan Lait](#), Senior Sales Engineer, Splunk

.conf19 IT Operations All Skill Levels

## IT1433 - Down in the Weeds, Up in the Cloud: IT Ops

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud, Splunk IT Service Intelligence

Session Video

Session Slides

[Ry Lait](#), Senior Sales Engineer, Splunk

.conf18 Security, Compliance and Fraud Intermediate

## SEC1355 - Hunting the Known Unknown: Microsoft Cloud

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Enterprise Security

Session Video

Session Slides

[Ryan Kovar](#), Principal Security Strategist, Splunk

[Steve Brant](#), Senior Security Strategist, Splunk

.conf18 Security, Compliance and Fraud All Skill Levels

## SEC1297 - Down in the Weeds, Up in the Cloud: Splunking Your Azure and Office 365

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security

Session Video

Session Slides

[Ryan Lait](#), Senior Sales Engineer, Splunk

.conf19 Foundations/Platform Intermediate

## FN1328 - Show and Tell: Prescriptive Use Cases for Azure and Office 365

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Enterprise Security, Splunk Machine Learning Toolkit

Session Video

Session Slides

[Jason Conger](#), Solution Architect, Splunk

[Ry Lait](#), Senior Sales Engineer, Splunk

.conf19 Security, Compliance and Fraud All Skill Levels

## SEC1432 - Down in the Weeds, Up in the Cloud: Security

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud, Splunk Enterprise Security

Session Video

























Session Slides

[Ry Lait](#), Senior Sales Engineer, Splunk









Google Cloud Platform

Available Regions	Azure Regions	AWS Regions and Zones	Google Compute Regions & Zones
<b>Compute Services</b>	 Virtual Machines	 Elastic Compute Cloud (EC2)	 Compute Engine
<b>App Hosting</b>	 Azure Cloud Services	 Amazon Elastic Beanstalk	 Google App Engine
<b>Serverless Computing</b>	 Azure Functions	 AWS Lambda	 Google Cloud Functions
<b>Container Support</b>	 Azure Container Service	 EC2 Container Service	 Container Engine
<b>Scaling Options</b>	 Azure Autoscale	 Auto Scaling	 Autoscaler
<b>Object Storage</b>	 Azure Blob Storage	 Amazon Simple Storage (S3)	 Cloud Storage
<b>Block Storage</b>	 Azure Managed Storage	 Amazon Elastic Block Storage	 Persistent Disk
<b>Content Delivery Network (CDN)</b>	 Azure CDN	 Amazon CloudFront	 Cloud CDN

# Pre-Built Add-ons for Microsoft Azure

## Splunk Add-on for Microsoft Cloud Services

Splunk Supported  
[splunkbase.splunk.com/app/3110/](https://splunkbase.splunk.com/app/3110/)

-  Azure Storage Table
-  Azure Storage Blob
-  Azure Audit
-  Azure Resources

## Microsoft Azure Add on for Splunk

Community Supported  
[splunkbase.splunk.com/app/3757/](https://splunkbase.splunk.com/app/3757/)

-  Azure AD Sign-Ins
-  Azure AD Users
-  Azure AD Audit
-  Azure Event Hub
-  Azure Metrics
-  Azure Security Center
-  Azure Subscriptions
-  Azure Resource Groups
-  Azure Resource Graph
-  Azure Topology
-  Azure Virtual Network
-  Azure Compute
-  Azure Billing & Consumption
-  Azure Reservation Recommendation

# Azure AD App Registration Permission Configuration

Granular permission requirements for each input

Add-on	Input	Splunk Sourcetype	API Name	Permission Type	Permissions
Microsoft Azure Add-on for Splunk	Microsoft Azure Active Directory Sign-ins	azure:aad:signin	Microsoft Graph	Delegated	AuditLog.Read.All Directory.Read.All
				Application	Directory.Read.All
	Microsoft Azure Active Directory Users	azure:aad:user	Microsoft Graph	Delegated	AuditLog.Read.All Directory.Read.All
				Application	Directory.Read.All
	Microsoft Azure Active Directory Audit	azure:aad:audit	Microsoft Graph	Delegated	AuditLog.Read.All Directory.Read.All
				Application	Directory.Read.All
	Azure Event Hub	azure:eventhub			Shared Access Policy Connection String
	Azure Metrics	azure:metrics	Azure Service Management	Delegated	user_impersonation
			Microsoft Graph	Delegated	User.Read

<https://docs.google.com/spreadsheets/d/1zI8gGIEJ1KOKdGYSrYahigYJzrShTssmKtylf6d9y9U>

# Azure NSG Flow Logs


How customers currently  
Splunk NSG flow logs

1. Configure NSG logging
2. Send flow logs to Azure Storage Blob
3. Configure MS Cloud Services Add-on to ingest storage blob data
4. Use complex props/transforms to pull apart flow tuples

```
18/08/2020 08:00:26.217 {"records":[{"time":"2020-08-17T22:00:26.2171308Z","systemId":"2cf332bc-4405-4663-80fc-2ea5b2b85188","macAddress":"000D3AE07B89","category":"NetworkSecurityGroupFlowEvent","resourceId":"/SUBSCRIPTIONS/1213B189-13FF-42FE-B370-DF6DA421BCE1/RESOURCEGROUPS/BOTS/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/RX-WIN10-NSG","operationName":"NetworkSecurityGroupFlowEvents","properties":{"Version":2,"flows":[{"rule":"DefaultRule_AllowInternetOutBound","flows":[{"mac":"000D3AE07B89","flowTuples":["1597701563,10.0.0.4,52.154.152.135,54013,443,T,O,A,B,,,,","1597701567,10.0.0.4,13.77.52.27,53998,443,T,O,A,E,2,108,1,54","1597701573,10.0.0.4,40.69.216.73,54001,443,T,O,A,E,0,0,1,60","1597701582,10.0.0.4,52.154.152.135,54013,443,T,O,A,E,8,2376,12,8858","1597701594,10.0.0.4,52.154.152.135,54014,443,T,O,A,B,,,,"}]},{"rule":"DefaultRule_DenyAllInBound","flows":[{"mac":"000D3AE07B89","flowTuples":["1597701573,91.229.112.7,10.0.0.4,53242,3032,T,I,D,B,,,,","1597701596,179.191.123.46,10.0.0.4,56572,7746,T,I,D,B,,,,","1597701609,45.129.33.8,10.0.0.4,50797,31559,T,I,D,B,,,,"}]},{"rule":"UserRule_RDP","flows":[{"mac":"000D3AE07B89","flowTuples":["1597701568,58.171.243.146,10.0.0.4,53029,3389,T,I,A,B,,,,","1597701581,193.124.57.60,10.0.0.4,57708,3389,T,I,A,B,,,,","1597701592,185.152.66.161,10.0.0.4,53462,3389,T,I,A,B,,,,","1597701593,185.141.170.163,10.0.0.4,60416,3389,T,I,A,B,,,,","1597701594,61.219.84.129,10.0.0.4,59718,3389,T,I,A,B,,,,","1597701598,40.123.39.82,10.0.0.4,64835,3389,T,I,A,B,,,,","1597701603,37.75.124.73,10.0.0.4,31458,3389,T,I,A,B,,,,","1597701603,185.202.0.109,10.0.0.4,61416,3389,T,I,A,B,,,,","1597701608,222.255.38.16,10.0.0.4,52797,3389,T,I,A,B,,,,","1597701616,54.171.167.220,10.0.0.4,57815,3389,T,I,A,B,,,,","1597701618,3.235.1.132,10.0.0.4,57192,3389,T,I,A,B,,,,"}]}}]},{"time":"2020-08-17T22:01:26.2194736Z","systemId":"2cf332bc-4405-4663-80fc-2ea5b2b85188","macAddress":"000D3AE07B89","category":"NetworkSecurityGroupFlowEvent","resourceId":"/SUBSCRIPTIONS/1213B189-13FF-42FE-B370-DF6DA421BCE1/RESOURCEGROUPS/BOTS/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/RX-WIN10-NSG","operationName":"NetworkSecurityGroupFlowEvents","properties":{"Version":2,"flows":[{"rule":"DefaultRule_AllowInternetOutBound","flows":[{"mac":"000D3AE07B89","flowTuples":["1597701627,10.0.0.4,52.154.152.135,54014,443,T,O,A,E,9,2636,12,8858","1597701639,10.0.0.4,52.154.152.135,54016,443,T,O,A,B,,,,","1597701657,10.0.0.4,52.154.152.135,54016,443,T,O,A,E,8,2376,11,8798","1597701661,10.0.0.4,52.114.128.73,54017,443,T,O,A,B,,,,","1597701670,10.0.0.4,52.154.152.135,54018,443,T,O,A,B,,,,","1597701678,10.0.0.4,52.114.128.73,54017,443,T,O,A,E,12,13314,12,5485"}]},{"rule":"DefaultRule_DenyAllInBound","flows":[{"mac":"000D3AE07B89","flowTuples":["1597701650,208.68.39.220,10.0.0.4,49703,28068,T,I,D,B,,,,","1597701654,223.71.167.163,10.0.0.4,24674,5986,T,I,D,B,,,,","1597701655,195.54.160.155,10.0.0.4,50036,8148,T,I,D,B,,,,","1597701671,117.206.95.97,10.0.0.4,1036,23,T,I,D,B,,,,","1597701671,91.229.112.8,10.0.0.4,53085,4596,T,I,D,B,,,,"}]},{"rule":"UserRule_RDP","flows":[{"mac":"000D3AE07B89","flowTuples":["1597701625,77.68.111.36,10.0.0.4,56609,3389,T,I,A,B,,,,","1597701631,46.250.220.75,10.0.0.4,62208,3389,T,I,A,B,,,,","1597701634,52.205.101.178,10.0.0.4,63855,3389,T,I,A,B,,,,","1597701640,144.76.113.220,10.0.0.4,50661,3389,T,I,A,B,,,,","1597701640,195.54.161.136,10.0.0.4,7391,3389,T,I,A,B,,,,","1597701645,217.198.124.44,10.0.0.4,63207,3389,T,I,A,B,,,,","1597701647,178.128.172.212,10.0.0.4,61332,3389,T,I,A,B,,,,","1597701661,177.94.223.213,10.0.0.4,65379,3389,T,I,A,B,,,,","1597701665,210.9.146.198,10.0.0.4,54183,3389,T,I,A,B,,,,","1597701672,40.122.165.7,10.0.0.4,55519,3389,T,I,A,B,,,,","1597701674,212.180.228.243,10.0.0.4,23088,3389,T,I,A,B,,,,","1597701678,185.141.170.163,10.0.0.4,60959,3389,T,I,A,B,,,,","1597701680,82.223.52.192,10.0.0.4,65335,3389,T,I,A,B,,,,","1597701681,58.171.243.146,10.0.0.4,55380,3389,T,I,A,B,,,,"}]}}]},{"time":"2020-08-17T22:02:26.2243491Z","systemId":"2cf332bc-4405-4663-80fc-2ea5b2b85188","macAddress":"000D3AE07B89","category":"NetworkSecurityGroupFlowEvent","resourceId":"/SUBSCRIPTIONS/1213B189-13FF-42FE-B370-DF6DA421BCE1/RESOURCEGROUPS/BOTS/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/RX-WIN10-NSG","operationName":"NetworkSecurityGroupFlowEvents","properties":{"Version":2,"flows":[{"rule":"DefaultRule_AllowInternetOutBound","flows":[{"mac":"000D3AE07B89","flowTuples":["1597701687,10.0.0.4,52.154.152.135,54018,443,T,O,A,E,7,2322,11,8798","1597701701,10.0.0.4,13.67.143.117,54019,443,T,O,A,B,,,,","1597701703,10.0.0.4,13.77.52.27,54020,443,T,O,A,B,,,,","1597701720,10.0.0.4,
```

# Azure NSG Flow Logs

How you **SHOULD** Splunk NSG flow logs!

1. Configure NSG logging
2. Send flow logs to Azure Storage Blob
3. Deploy Azure function app - 1 click via GitHub > 
4. Send to Azure Event Hub or directly to Splunk using HEC

rySplunk / AzureNetworkWatcherNSGFlowLogsConnector  
forked from microsoft/AzureNetworkWatcherNSGFlowLogsConnector

<> Code Pull requests Actions Projects Wiki Security Insights Settings

master 3 branches 0 tags Go to file Add file Code

This branch is 3 commits ahead of microsoft:master. Pull request Compare

rySplunk Update azureDeploy.json 6276dc3 21 days ago 28 commits

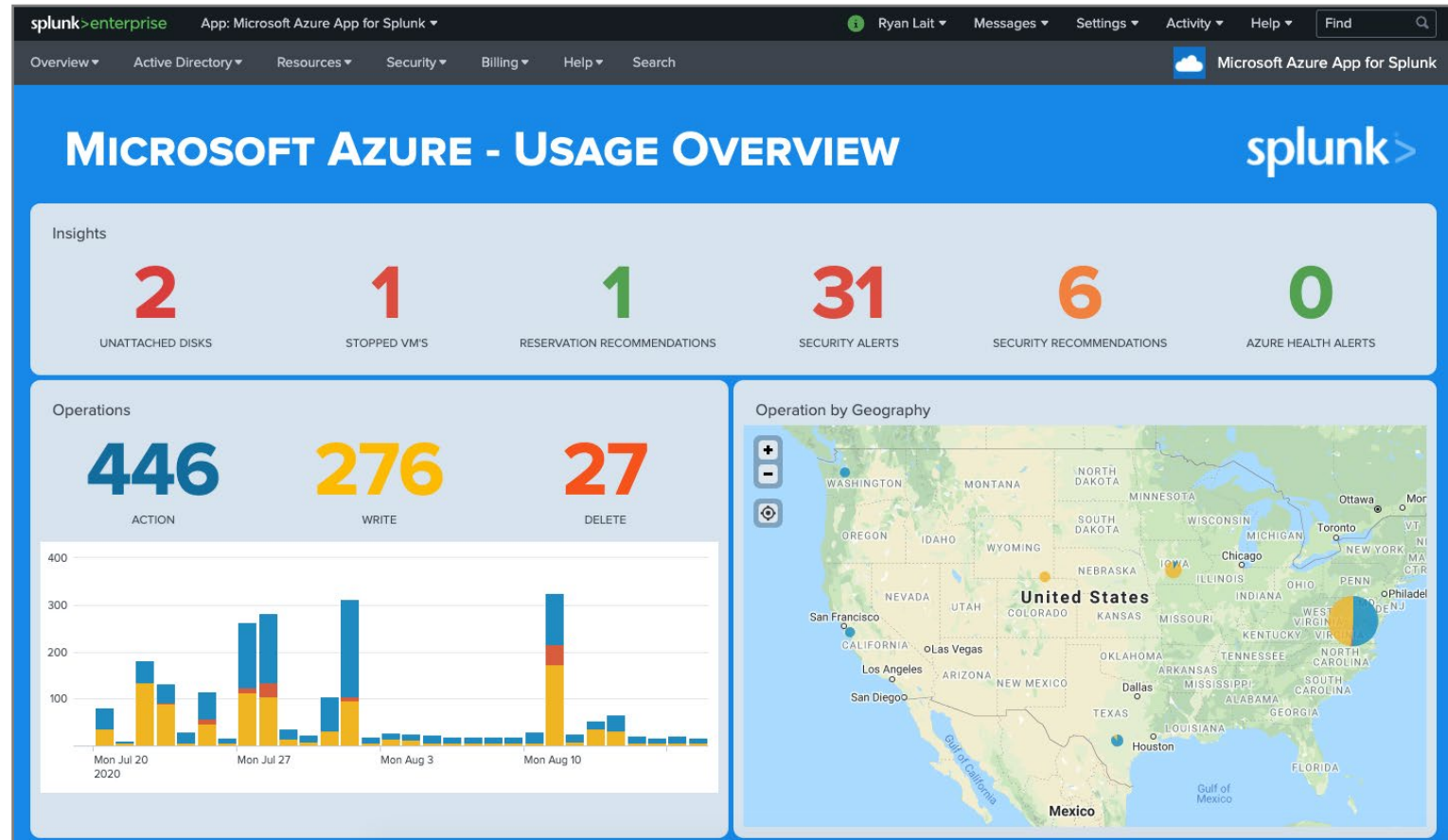
File	Commit Message	Time
NwNsgProject	Update azureDeploy.json	21 days ago
.gitignore	Refactor outputs (microsoft#4)	2 years ago
LICENSE	Initial commit	3 years ago
NwNsgProject.sln	Revert "perf testing adjustments."	2 years ago
README.md	Updates	21 days ago

i	Time	Event
>	31/07/2020 15:07:58.708	{ [-] category: NetworkSecurityGroupFlowEvent destinationAddress: 10.0.0.4 destinationPort: 3389 deviceAction: A deviceDirection: I flowState: B mac: 000D3AE07B89 nsgRuleName: UserRule_RDP operationName: NetworkSecurityGroupFlowEvents resourceId: /SUBSCRIPTIONS/1213B189-13FF-42FE-B370-DF6DA421BCE1/RESOURCEGROUPS/BOTS/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/Ry-WIN10-NSG sourceAddress: 193.93.62.44 sourcePort: 60191 startTime: 1596172073 time: 2020-07-31T05:07:58.7084019Z

# Microsoft Azure App for Splunk

[splunkbase.splunk.com/app/4882](https://splunkbase.splunk.com/app/4882)

- User auditing
- Subscription tracking
- Resource monitoring
- Performance metrics
- Security Center insights
- Billing & usage analytics
- Data onboarding guides





# Thank You

Please provide feedback via the

**SESSION SURVEY**



**.conf20**  
**splunk>**



# Appendix

---



**.conf20**  
splunk>



# Microsoft 365

---

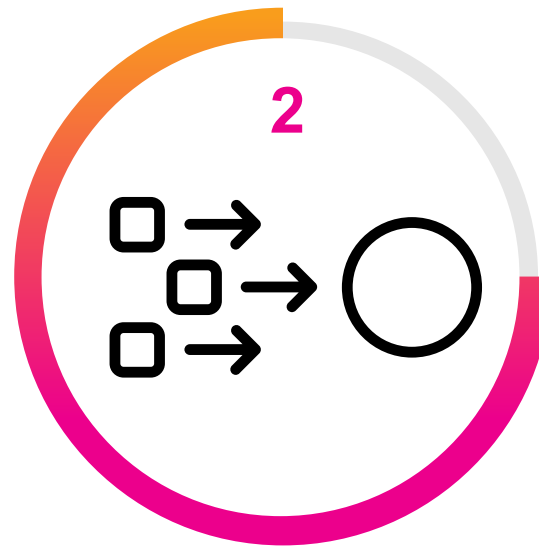
# Connecting the Dots

3 simple steps to be up and running in a matter of minutes



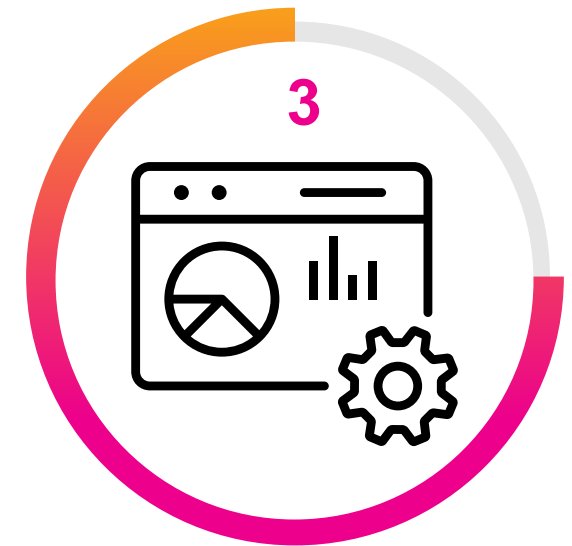
## Azure AD App Registration

Give Splunk permission to access M365 API



## Splunk Add-on for Microsoft 365

GUI wizard to collect data from M365



## Microsoft 365 App for Splunk

Dashboards & Pre-built Splunk content

# Azure Active Directory



- Geo-based login tracking
- Login failure details
- Suspicious login activity
- Non-existent account login attempts

splunk>enterprise App: Microsoft 365 App for Splunk

M365 Azure AD Exchange SharePoint OneDrive Microsoft Teams Power BI Security & Compliance Center Help

### Login Activity [Show Filters](#)

Edit Export ...

#### Login Failures

#### Login Failures

_time	User	LogonError	Client IP	Country
2020-04-17 05:06:06	sjackson@datatoeverything.io	UserAccountNotFound	207.246.70.38	United States
2020-04-17 05:05:07	sharris@datatoeverything.io	UserAccountNotFound	207.246.70.38	United States
2020-04-17 05:05:07	mpatel@datatoeverything.io	UserAccountNotFound	207.246.70.38	United States
2020-04-17 04:53:05	rahmed@datatoeverything.io	UserAccountNotFound	207.246.70.38	United States
2020-04-17 04:52:03	aharris@datatoeverything.io	UserAccountNotFound	207.246.70.38	United States

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

#### Geographical Improbable Access

Users logging in at two different locations where it's not likely possible to travel between locations in the time specified

Userid	Day	Time Difference (H)	Distance (M)	Speed	Original Location	Original Source IP	Second Location	Last Source IP
kelcie.bourne@datatoeverything.io	04/16/2020	0.03 1.52	10290.55	343018.20 6770.10	Ahmedabad, India, Gujarat	106.213.194.252 58.96.43.3	Brisbane, Australia, Queensland	106.213.194.252 58.96.43.3

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

#### Non-Existent Accounts - Login Attempts

Country	Logon Error	Users
Brazil	UserAccountNotFound	12643@datatoeverything.io info@datatoeverything.io
China	UserAccountNotFound	info@datatoeverything.io

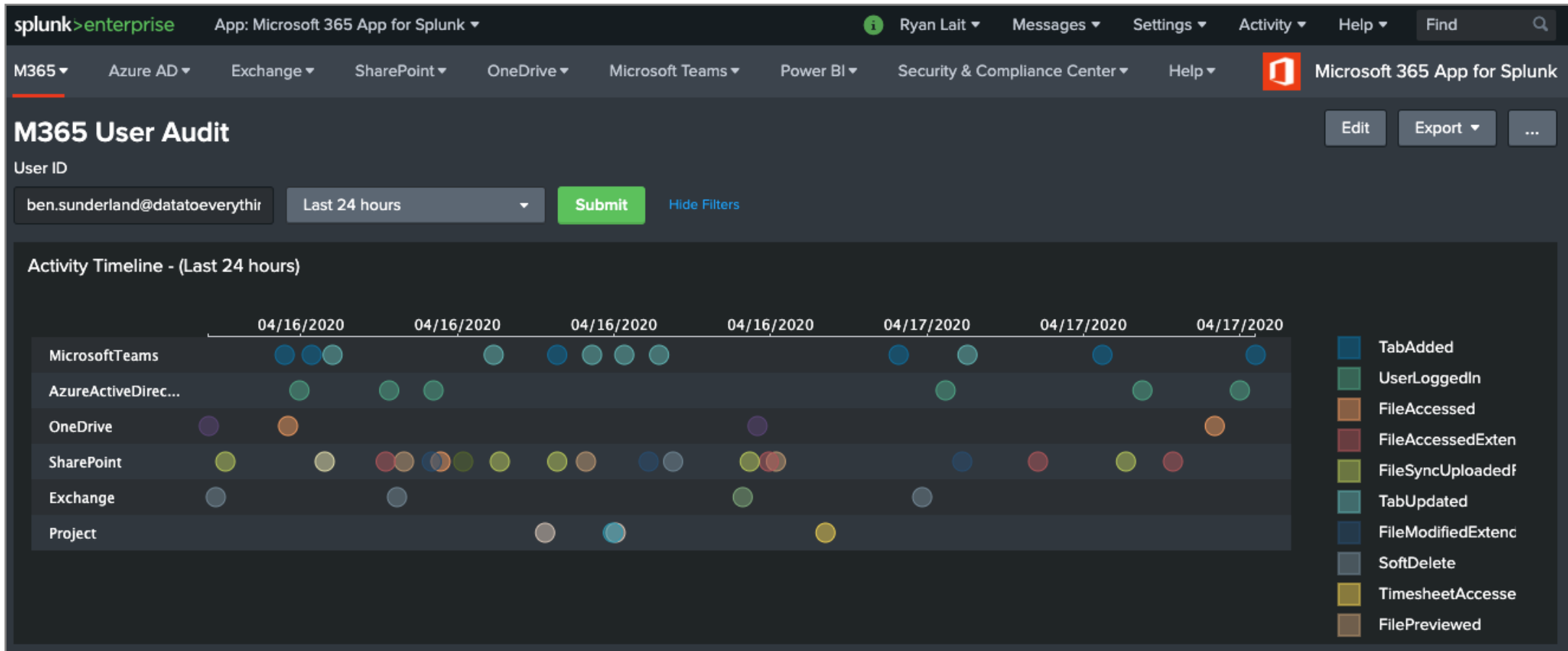
#### Multiple User Logins from Same IP Address

Source IP	Unique Users	Offending Country
207.246.70.38	242	United States
58.96.43.3	238	Australia

« Prev 1 2 3 4 Next »

# User Audit

Track user activity across multiple workloads in an instant



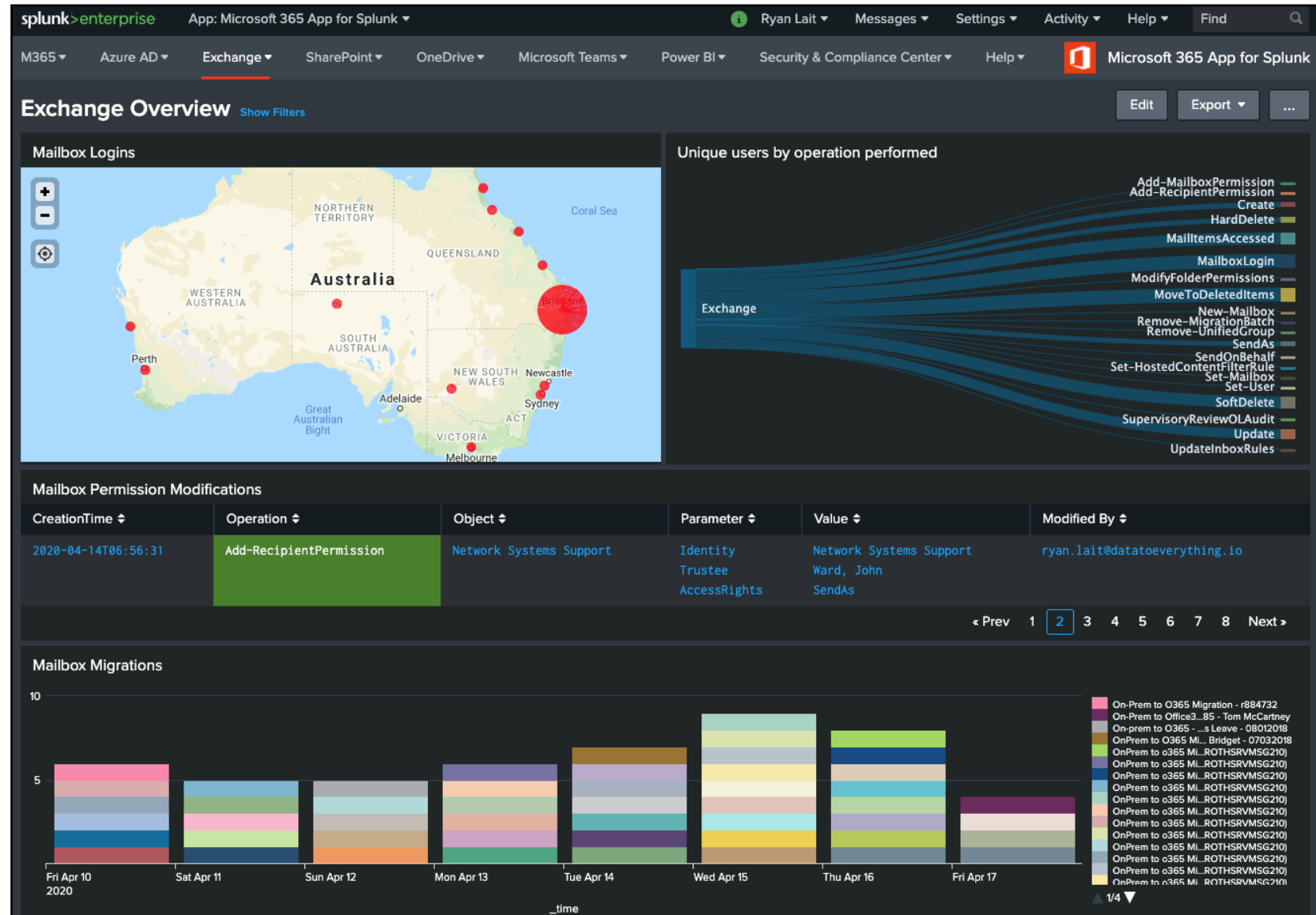
# Exchange Online

## Audit Activity logs

- Mailbox Logins
- Exchange operation activity
- Mailbox permission changes
- On-Prem to M365 mailbox migrations
- Bot and Connector details

### Note

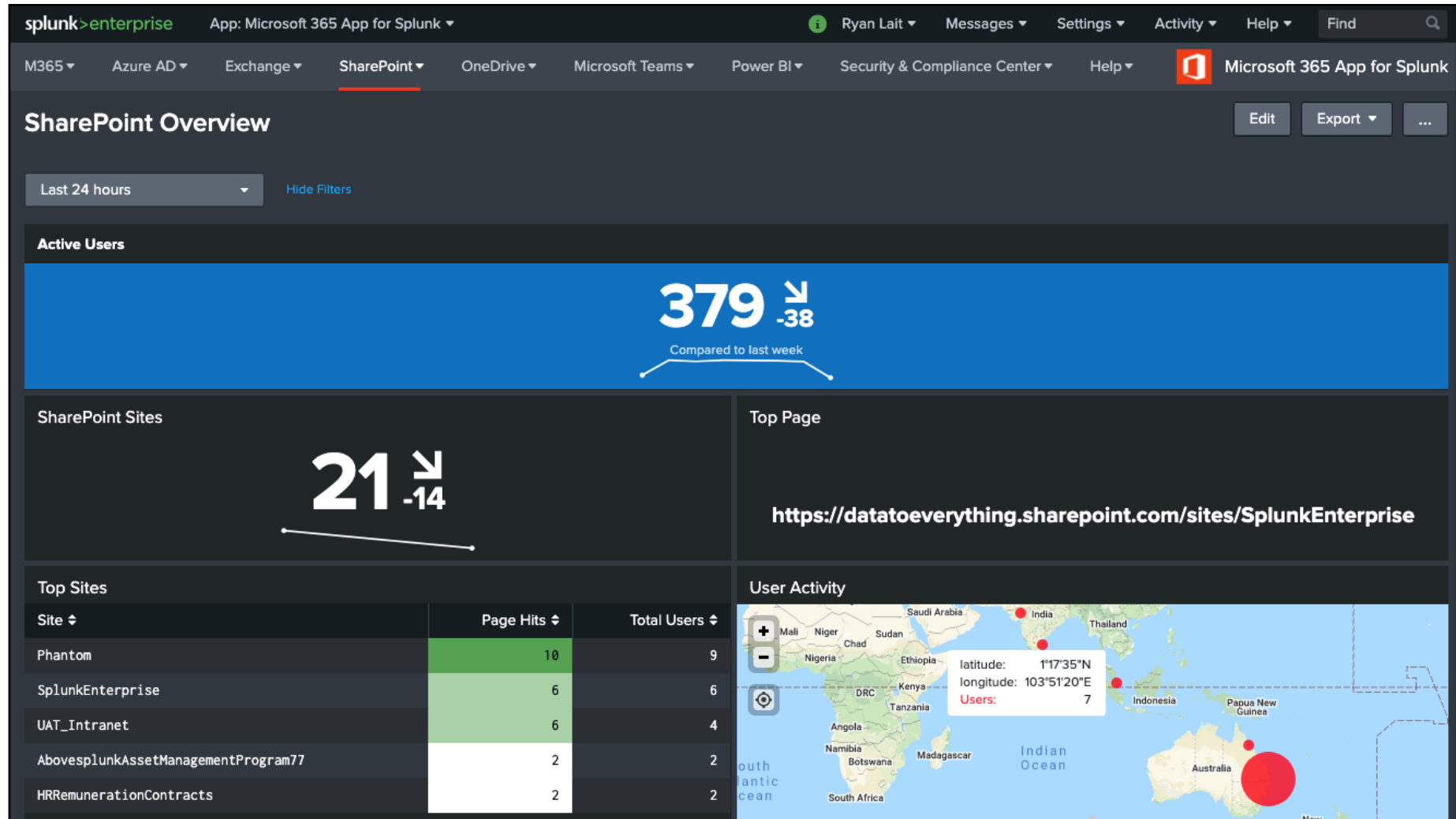
- M365 Add-on does not ingest message tracking logs
- These are ingested separately using [Microsoft Office 365 Reporting Add-on for Splunk](#)



# SharePoint Online

## Audit Activity logs

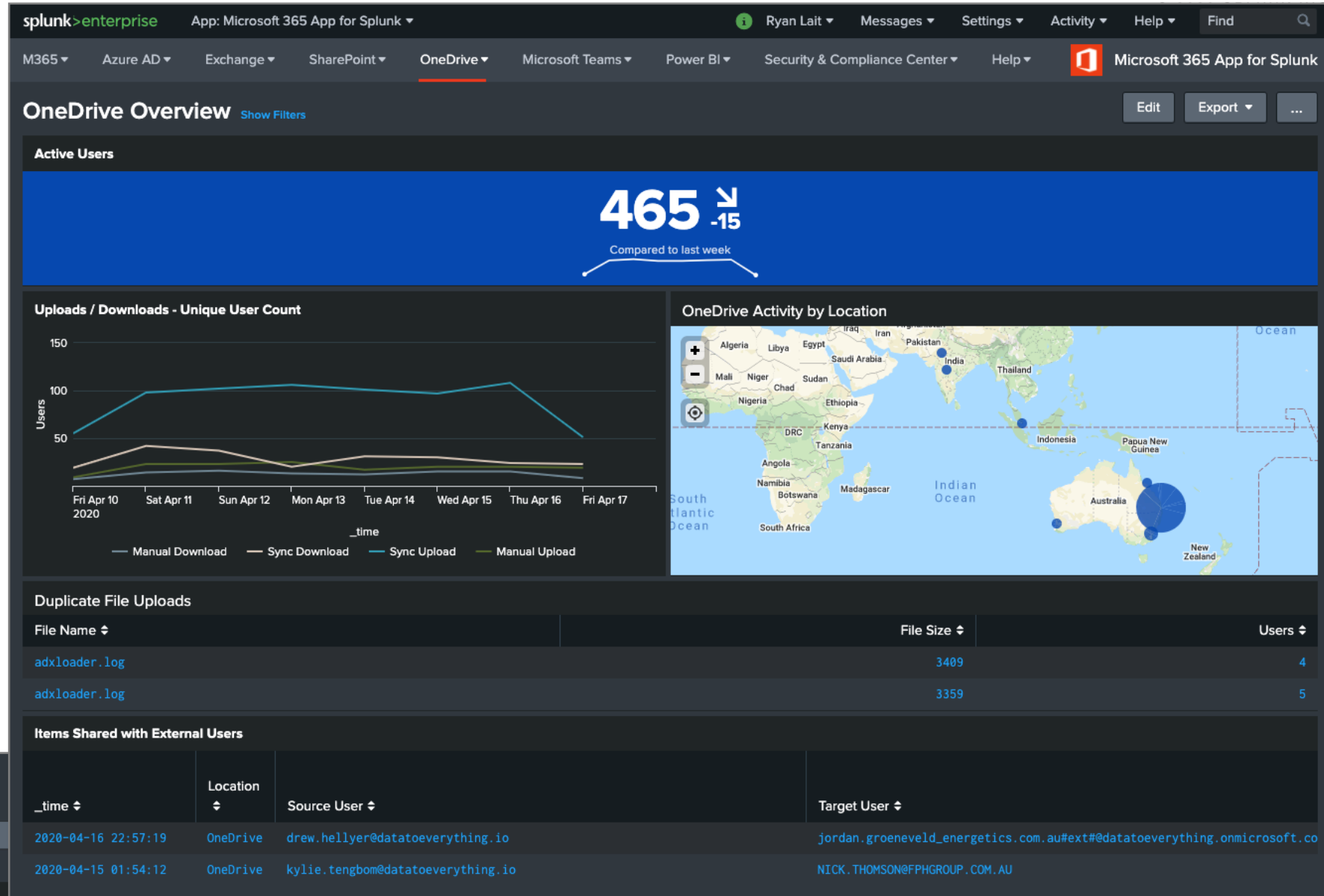
- Active users
- Site creations
- Top sites / pages
- Access activity
- Item audit
- Geographical access



# OneDrive

## Audit Activity logs

- Active users
- Data transfer volumes
- Geo-based activity
- Duplicate file uploads
- Items shared with external users



## OneDrive File Investigator

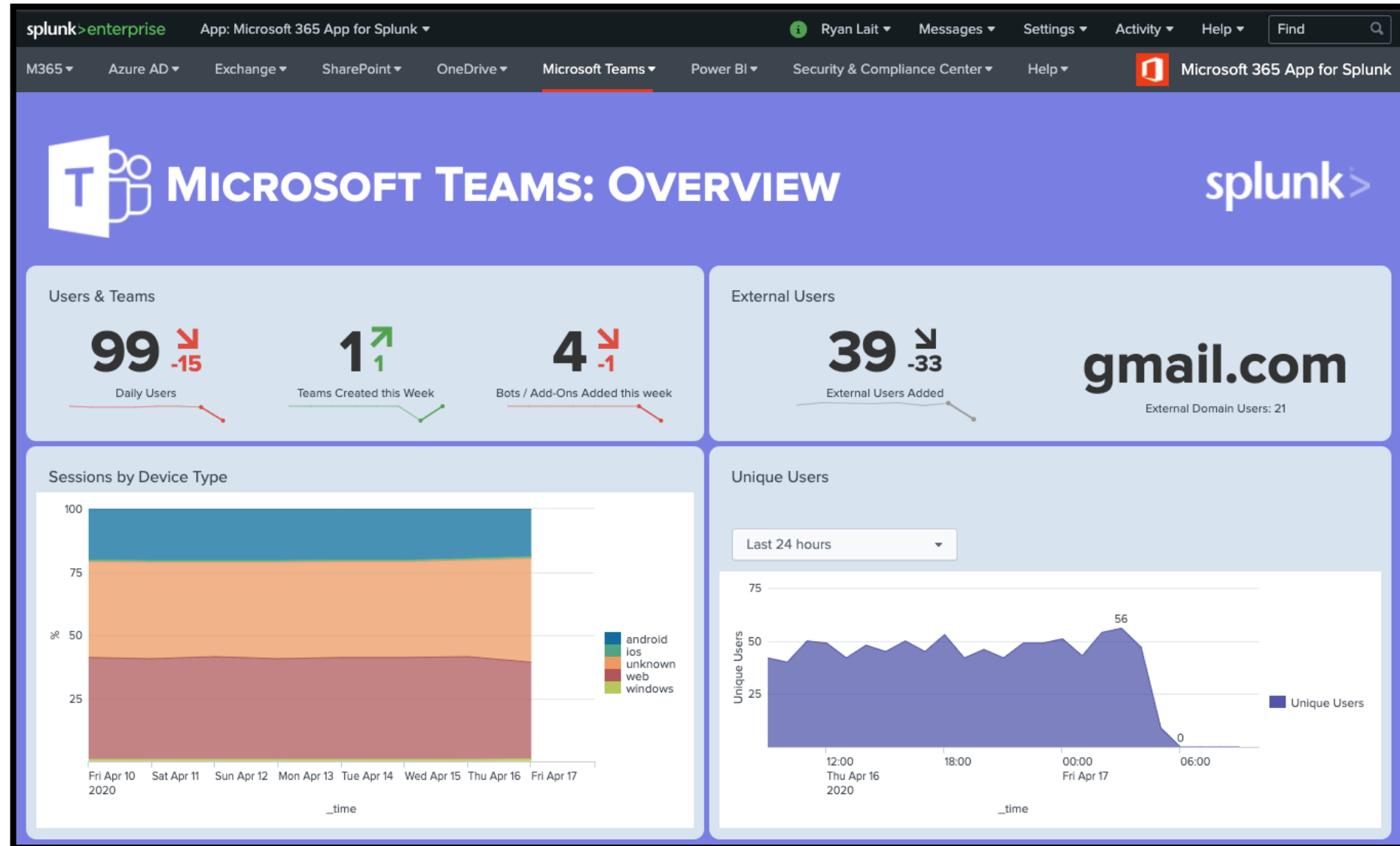
Select Field: File Name  
File Name: Brisbane Writing Session.pptx  
Last 24 hours

### Matching File Names

File Name	User	File Path	Client IP	Operation	Time	User Agent
Brisbane Writing Session.pptx	Ryan.kovar@datatoeverything.io	Documents/Profile/Desktop/WRITING PRESENTATION	58.96.43.3	FileModifiedExtended	2020-04-17 03:21:48	Microsoft Office P
				FileModified	2020-04-17 04:26:55	
				FileModifiedExtended	2020-04-17 06:52:07	

# Microsoft Teams Usage, Adoption, Auditing

- Active users
- Team creations / edits
- External user activity
- Device type info
- Bot and Connector details
- Meeting and call data
- Chat message details





# PowerBI

## Audit Activity logs



- Active users
- Dashboard activity
- Dataset activity
- Dataset creations
- Externally shared reports

splunk>enterprise App: Microsoft 365 App for Splunk

M365 Azure AD Exchange SharePoint OneDrive Microsoft Teams Power BI Security & Compliance Center Help Find

### Power BI Overview [Show Filters](#)

Active Users

**180** ↓ -28  
Compared to last week

**32** ↓ -27  
Users Viewing Dashboards

**3** ↑ 3  
Users Creating Dashboards

**1** ↓ -1  
Datasets Created

#### Dataset Creations

WorkspaceName	UserId	DatasetName
My Workspace	Rebecca.Green@datatoeverything.io	WFH Test
Splunk Crushes big Data!	se.team@datatoeverything.io	Dashboard Usage Metrics Model
Splunk Makes big data easy!	Nicholas.Keogh@datatoeverything.com.au	data
Splunk Makes big data easy!	Nicholas.Keogh@datatoeverything.io	Asset lookup Splunk all the things!
[DEV] - datatoeverything Operations Scorecard	se.team@datatoeverything.io	test_bookmark

< Prev 1 2 Next >

#### Externally Shared Reports

_time	UserId	Recipient	Dataset
2020-04-09 03:22:10	mickey.perre@datatoeverything.io	bgist@froth.ly	For correlation in Splunk

# Getting Started



- Full step-by-step documentation
- Creating an Azure App registration
- Configuring the Splunk Add-on for Microsoft 365

**1: Login to the Azure Portal**

**2: Select Azure Active Directory from the menu:**

**4: Enter Name of tenant**  
**5: Select O365 Endpoint** (usually "Worldwide")  
**6: Enter Tenant ID** of Azure tenant  
**7: Enter Client ID** of Azure app registration  
**8: Enter Client secret** of Azure app registration  
**9: Select Add**

**11: Select Add Input**  
**12: Select Management Activity**

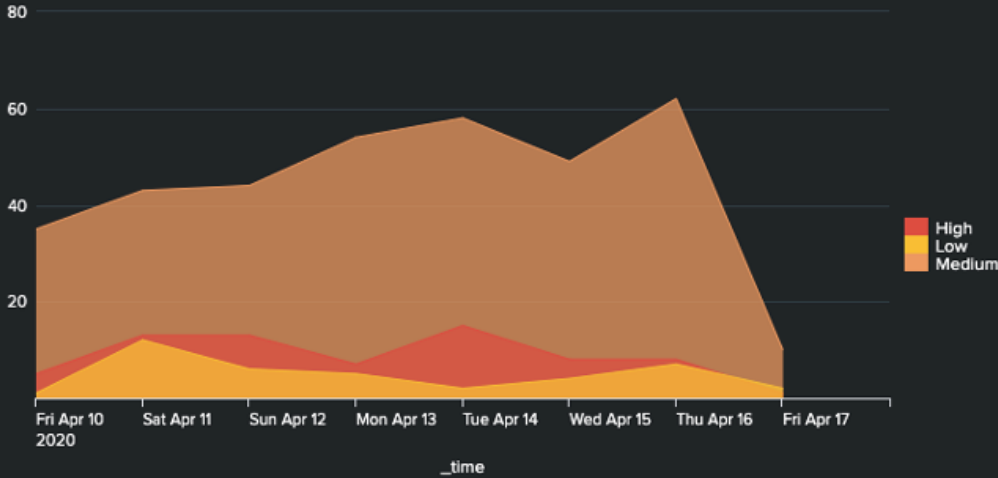
**28: Confirm data is being ingested by running the following search:**

Index	sourcetype	count
m365	o365:management:activity	158048
m365	o365:service:message	2375
m365	o365:service:status	703700

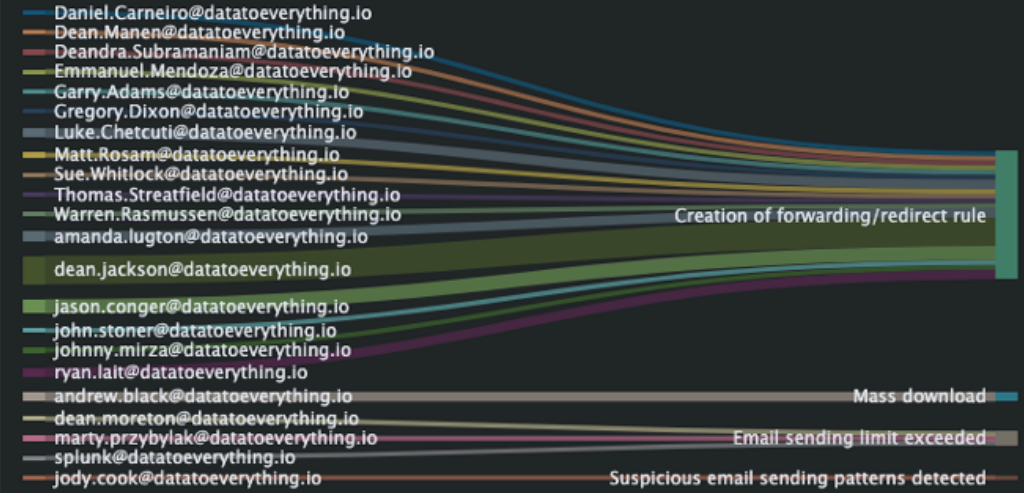
## Alerts Overview [Show Filters](#)

Edit Export ...

### Alerts over Time



### Alerts by User

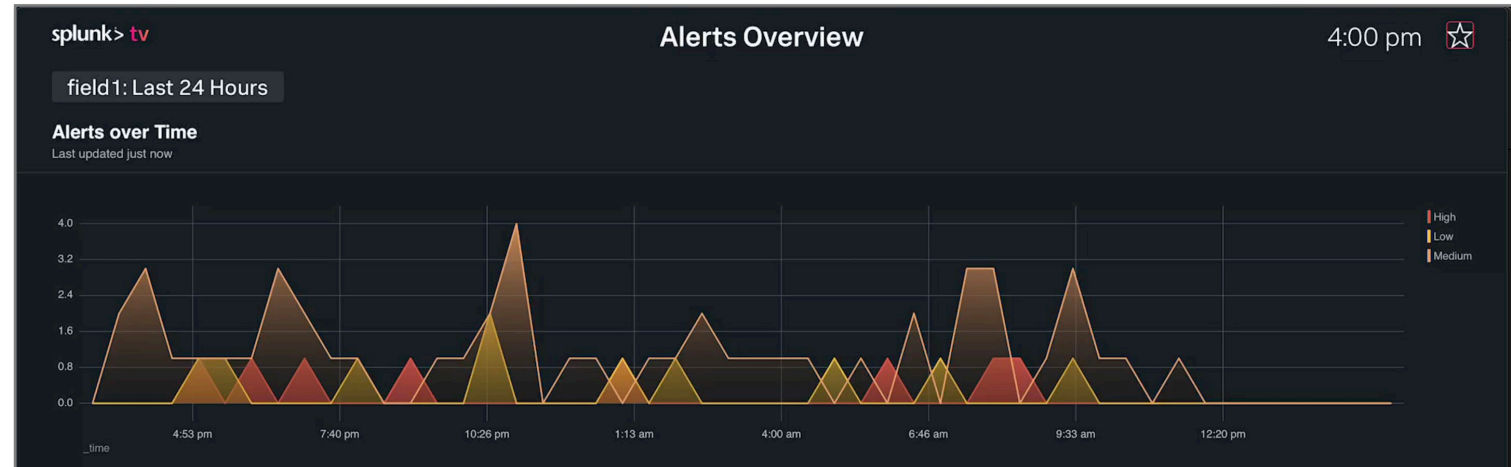
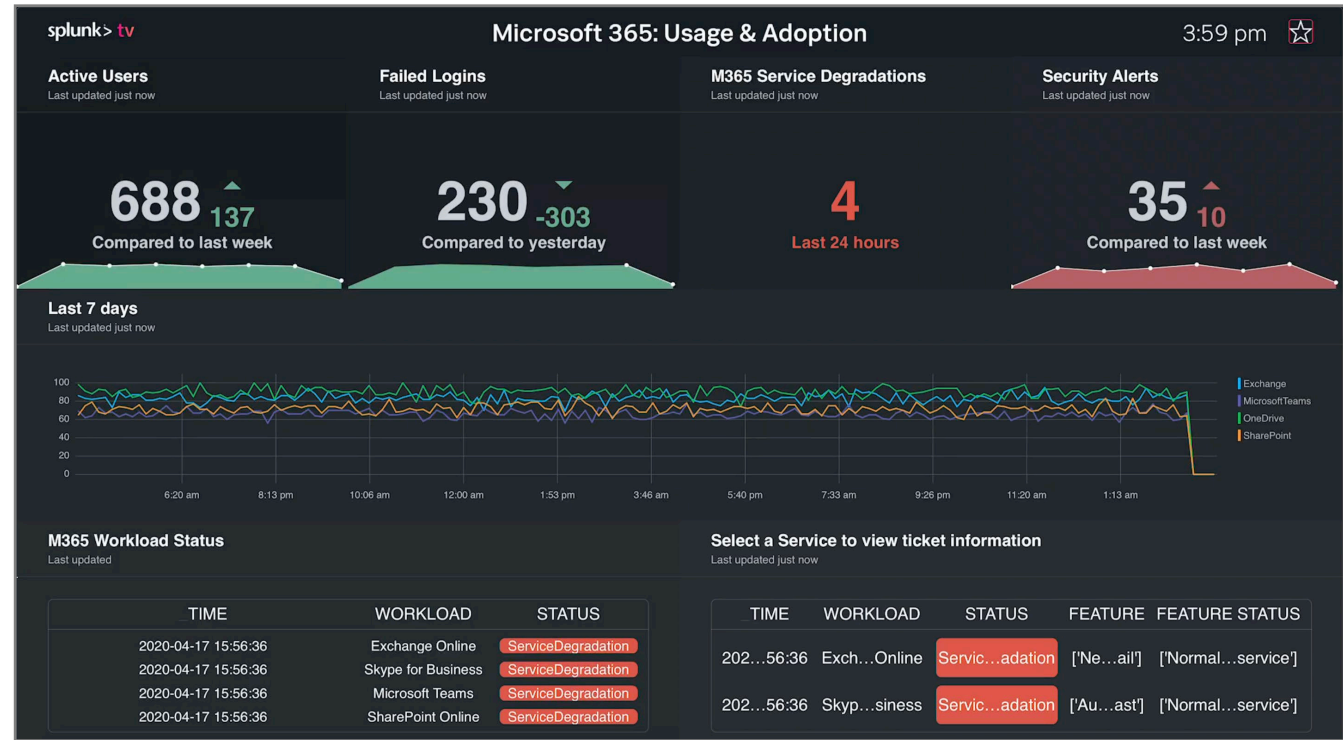
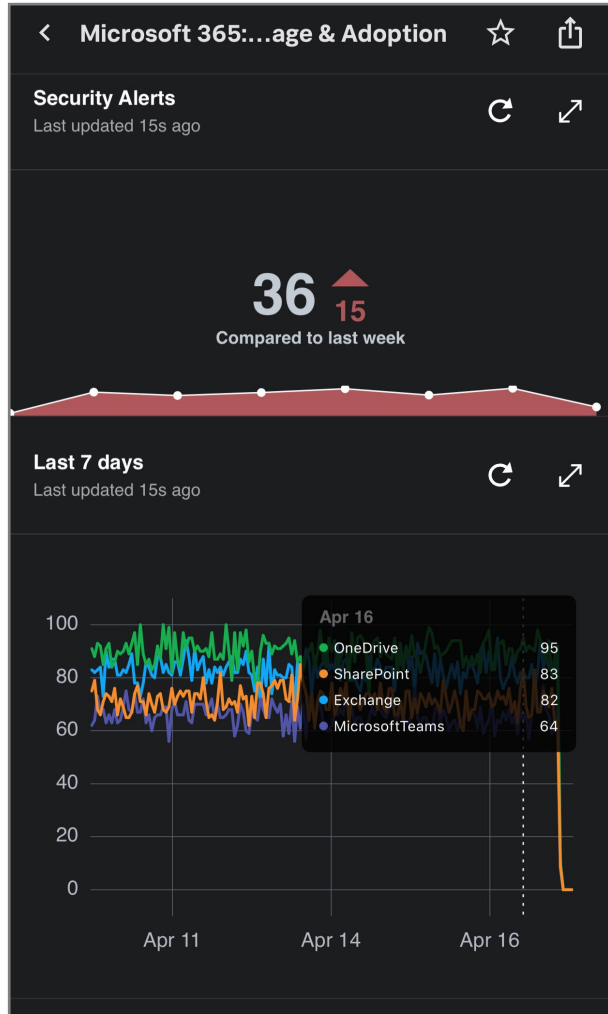


### Alert Details

_time	Severity	Status	email	Name	Comments	Category	AlertType	Data
2020-04-16 19:25:27	Medium	Active	andrew.black@datatoeverything.io	Mass download	New alert	ThreatManagement	System	{"ts":"2019-02-07 09:25:27Z","te":"2019-02-07 Additional risks in this user session: This us (pdf).","f3u":"andrew.black@datatoeverything.io id=eq(5a4cba6ac0bc12a35cb97be7,),"mat":"MCAS_
2020-04-13 09:18:20	Medium	Active	splunk@datatoeverything.io	Email sending limit exceeded	New alert	ThreatManagement	System	{"f3u":"splunk@datatoeverything.io","ev":"splu MessagetraceId=1cd6eef5-efc7-48d5-daac-08d7cee: 12T23:18:20.000000Z","op":"EmailSendingLimitE: 8ed8c94b2676","cid":"2cc44934-4d16-420b-b4e8-7- V1.0.0.0","lon":"EmailSendingLimitExceeded","ai

# Go mobile!

## Splunk Mobile + SplunkTV



**.conf20**  
splunk>



























# Microsoft Azure

---
























Google Cloud Platform

Available Regions	Azure Regions	AWS Regions and Zones	Google Compute Regions & Zones
<b>Compute Services</b>	 Virtual Machines	 Elastic Compute Cloud (EC2)	 Compute Engine
<b>App Hosting</b>	 Azure Cloud Services	 Amazon Elastic Beanstalk	 Google App Engine
<b>Serverless Computing</b>	 Azure Functions	 AWS Lambda	 Google Cloud Functions
<b>Container Support</b>	 Azure Container Service	 EC2 Container Service	 Container Engine
<b>Scaling Options</b>	 Azure Autoscale	 Auto Scaling	 Autoscaler
<b>Object Storage</b>	 Azure Blob Storage	 Amazon Simple Storage (S3)	 Cloud Storage
<b>Block Storage</b>	 Azure Managed Storage	 Amazon Elastic Block Storage	 Persistent Disk
<b>Content Delivery Network (CDN)</b>	 Azure CDN	 Amazon CloudFront	 Cloud CDN












Google Cloud Platform

<b>SQL Database Options</b>	 Azure SQL Database	 Amazon RDS	 Cloud SQL
<b>NoSQL Database Options</b>	 Azure DocumentDB	 AWS DynamoDB	 Cloud Datastore
<b>Virtual Network</b>	 Azure Virtual Network	 Amazon VPC	 Cloud Virtual Network
<b>Private Connectivity</b>	 Azure Express Route	 AWS Direct Connect	 Cloud Interconnect
<b>DNS Services</b>	 Azure Traffic Manager	 Amazon Route 53	 Cloud DNS
<b>Log Monitoring</b>	 Azure Operational Insights	 Amazon CloudTrail	 Cloud Logging
<b>Performance Monitoring</b>	 Azure Application Insights	 Amazon CloudWatch	 Stackdriver Monitoring



Google Cloud Platform





<b>Administration and Security</b>	 Azure Active Directory	 AWS Identity and Access Management (IAM)	 Cloud Identity and Access Management (IAM)
<b>Compliance</b>	 Azure Trust Center	 AWS CloudHSM	 Google Cloud Platform Security
<b>Analytics</b>	 Azure Stream Analytics	 Amazon Kinesis	 Cloud Dataflow
<b>Automation</b>	 Azure Automation	 AWS Opsworks	 Compute Engine Management
<b>Management Services &amp; Options</b>	 Azure Resource Manager	 Amazon Cloudformation	 Cloud Deployment Manager
<b>Notifications</b>	 Azure Notification Hub	 Amazon Simple Notification Service (SNS)	None
<b>Load Balancing</b>	 Load Balancing for Azure	 Elastic Load Balancing	 Cloud Load Balancing



# Pre-Built Add-ons for Microsoft Azure

## Splunk Add-on for Microsoft Cloud Services

Splunk Supported  
[splunkbase.splunk.com/app/3110/](https://splunkbase.splunk.com/app/3110/)

-  Azure Storage Table
-  Azure Storage Blob
-  Azure Audit
-  Azure Resources

## Microsoft Azure Add on for Splunk

Community Supported  
[splunkbase.splunk.com/app/3757/](https://splunkbase.splunk.com/app/3757/)

-  Azure AD Sign-Ins
-  Azure AD Users
-  Azure AD Audit
-  Azure Event Hub
-  Azure Metrics
-  Azure Security Center
-  Azure Subscriptions
-  Azure Resource Groups
-  Azure Resource Graph
-  Azure Topology
-  Azure Virtual Network
-  Azure Compute
-  Azure Billing & Consumption
-  Azure Reservation Recommendation

# Splunk Add-on for Microsoft Cloud Services

<https://splunkbase.splunk.com/app/3110/>



Splunk Supported

## Inputs (4)



### Azure Storage Table

Structured NoSQL data storage location

Native logging output for Azure resource monitoring

- Windows Event Logs
- Performance Counters
- Infrastructure Diag Logs



### Azure Storage Blob

Binary Large **OB**ject storage for large unstructured data sets.

Native logging destination for NSG Flow logs (firewall logs)

Not S3 compliant

- NSG Flow logs
- Custom app logging



### Azure Audit

Management / Control Plane Audit Events

Azure Portal Logins

Resource Modifications

Subscription Activity

CRUD activities

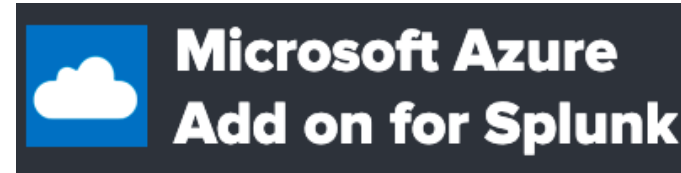


### Azure Resource

Stateful resource events

- **Virtual Machine**
- State: Powered On
- **Virtual Network**
- Provisioning State: Succeeded
- **Network Interface Card**
- enable IP Forwarding: False
- **Public IP Address**
- Allocation Method: Dynamic

# Microsoft Azure Add-on for Splunk



Community Supported

<https://splunkbase.splunk.com/app/3757/>

## Inputs (15)



### Azure AD Sign-Ins

Tenant-level authentication data.

Captures detailed auth events across all MS cloud environments. Azure, M365, etc.

MFA Details, interactive logins, locations, Use agents etc.



### Azure AD Users

Stateful list of Azure AD users and AD attributes.

AD Attributes including applied licences, status.

Useful for ES identity framework!



### Azure AD Audit

Azure AD specific audit activities.

CRUD-type events for users and groups.

Device enrolments, user creations, etc.



### Azure Event Hub

Subscribe to an event hub stream of information

Scalable method to collect data from multiple subscriptions, resources

Native configuration options in Azure to send data like << directly to an Event Hub and into Splunk!

# Microsoft Azure Add-on for Splunk



**Microsoft Azure  
Add on for Splunk**

Community Supported

<https://splunkbase.splunk.com/app/3757/>

## Inputs (15)



### Azure Metrics

Performance and availability metrics of almost everything in Azure

Hundreds of metrics available with a simple input configuration.

Performance metrics of Azure PaaS services



### Azure Security Center

Alerts, Tasks and recommendation events from Azure Security Center

Alerts for suspicious activity on a VM, storage account, etc.

Tasks to suggest proactive changes to increase security posture

Useful to correlate with other events already in Splunk.  
Don't reinvent the wheel!



### Azure Subscriptions

List of active subscriptions inside the specified tenant

A customer can have 1, dozens, even hundreds of subscriptions.

Useful to track activities across subscriptions, billing info, new, old, unused subscriptions etc.



### Azure Resource Groups

Stateful list of provisioned resource groups in the specified subscription

Provides overview of Resource Group Name, availability zone, etc.

# Microsoft Azure Add-on for Splunk



**Microsoft Azure  
Add on for Splunk**

Community Supported

<https://splunkbase.splunk.com/app/3757/>

## Inputs (15)



### Azure Virtual Network

Stateful list of provisioned virtual networks in the specified subscription

Provides overview of vnet name, availability zone, network details, IP configurations, vnet peering etc.

Details DDoS protection and VM protection details



### Azure Compute

Stateful compute object events

- **VM**
- OS, storage, No power state!
- **Disk**
- Size, IOPS, state (attached)
- **Image**
- OS image details
- **Snapshot**
- Disk snapshot details
- **VM Instance View**
- Power state, Agent status, OS details



### Azure Billing & Consumption

Details billing charges for individual resources and services

Meter details and costs incurred

Does not include any post-billing discounts. (MSP arrangements, MEA's etc.)

Billing periods to align billing cycles



### Azure Reservation Recommendation

Recommendation events to optimise and lower Azure running costs.

Cost of running a standard VM as compared to running it as a reserved instance.

Shows cost savings and benefits.

# Microsoft Azure Add-on for Splunk



Microsoft Azure  
Add on for Splunk

Community Supported

<https://splunkbase.splunk.com/app/3757/>

## Inputs (15)



### Azure Resource Graph

- Run queries from a Splunk input to access properties returned by resource without needing to make individual calls to each resource provider.
- Advisories
- Alerts
- Azure platform health
- Maintenance
- Resource
- Security



### Azure Topology (auto)

Correlated resource details to align resources in a hierarchical fashion. E.g., a VM inside a resource group, with details of its assigned vnet, storage account, NSG, OS Disk, etc.



### Azure Topology (manual)

The screenshot shows the Splunk interface for the Microsoft Azure App. The main view is 'Topology (beta)' for the 'splunk' resource group in 'Australia Southeast'. It displays a hierarchical tree of resources including Virtual Network (7), Instance (8), Subnet (6), Volume (1), Security Group (6), and Network Interface (8). A detailed view for 'SPLUNKHF01' is shown on the right, displaying metrics for CPU Utilization (5.74%), Disk IOPS (82.34), Network Traffic Size (12.73KB), and Cost - Last Month (84). The interface also shows the resource ID, Name (SPLUNKHF01), Type (Instance), and Account ID.

SPLUNKHF01	
Brief	CPU Utilization 5.74%
Relationship	Disk IOPS 82.34
Usage	Network Traffic Size 12.73KB
Billing	Cost - Last Month 84
ID:	/SUBSCRIPTIONS/1213b189-13ff-42fe-b370-df6da421bce1/RESOURCEREGROUPS/BO
Name:	SPLUNKHF01
Type:	Instance
Account ID:	1213b189-13ff-42fe-b370-df6da421bce1





# Permission Configuration

1 single App Registration for all permissions

## API Permissions

API / Permissions name	Type	Description
▼ Azure Service Management (1)		
user_impersonation	Delegated	Access Azure Service Management as organization users (preview)
▼ Microsoft Graph (6)		
AuditLog.Read.All	Delegated	Read audit log data
AuditLog.Read.All	Application	Read all audit log data
Directory.Read.All	Delegated	Read directory data
Directory.Read.All	Application	Read directory data
SecurityEvents.Read.All	Application	Read your organization's security events
User.Read	Delegated	Sign in and read user profile
▼ WindowsDefenderATP (1)		
Alert.Read.All	Application	Read all alerts

## IAM Roles

Billing Reader				
<input type="checkbox"/>		Ry_P5_Splunk_Azure	App	Billing Reader ⓘ
Network Contributor				
<input type="checkbox"/>		Ry_P5_Splunk_Azure	App	Network Contributor ⓘ
Reader				
<input type="checkbox"/>		Ry_P5_Splunk_Azure	App	Reader ⓘ
Security Reader				
<input type="checkbox"/>		Ry_P5_Splunk_Azure	App	Security Reader ⓘ