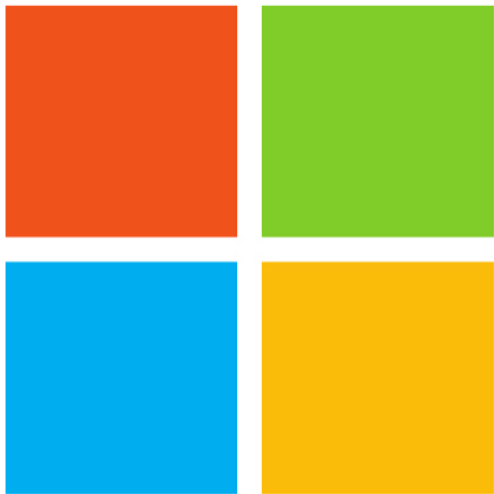
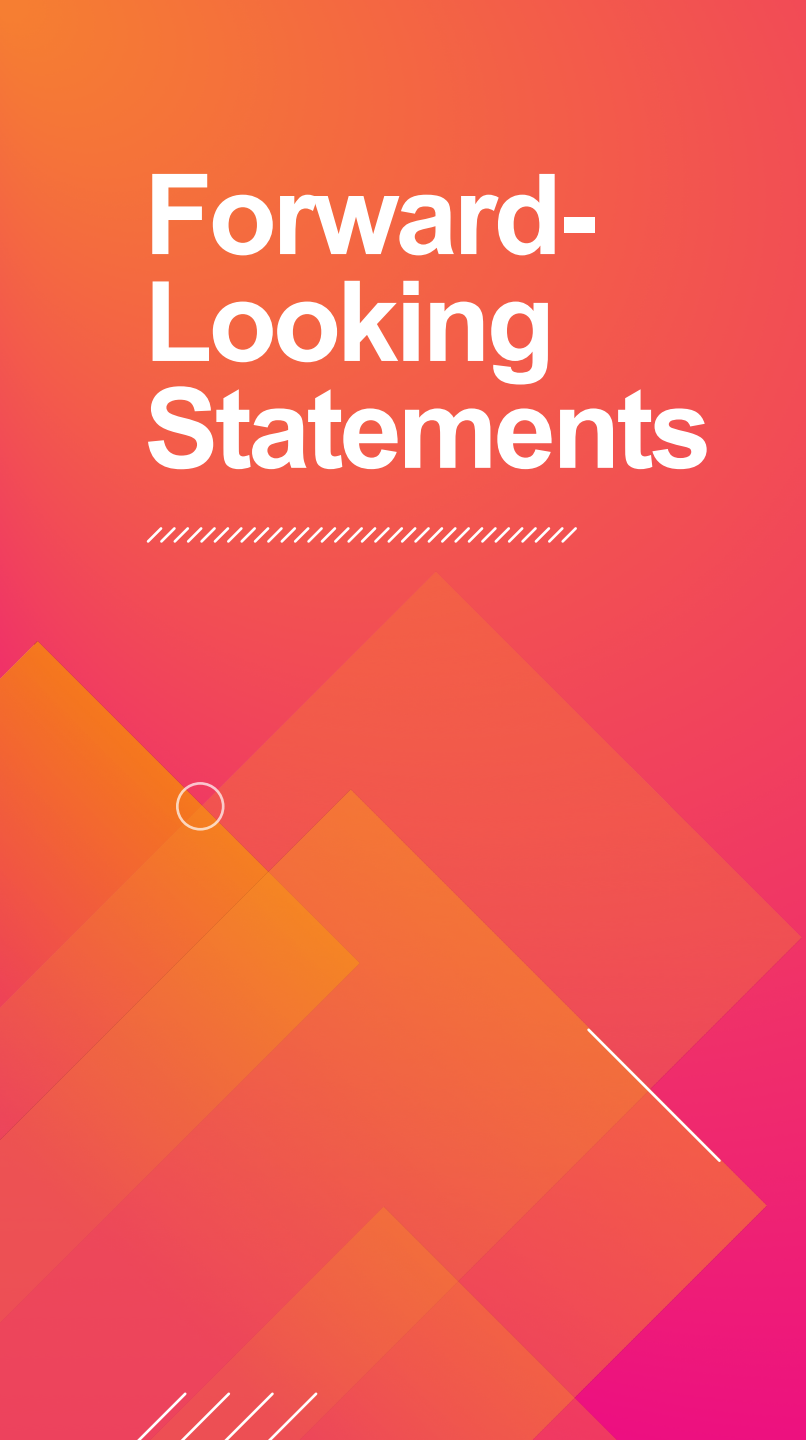




Show and Tell: Prescriptive Use Cases for Azure and Office 365

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>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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. © 2019 Splunk Inc. All rights reserved.

Show and Tell: Prescriptive Use Cases for Azure and Office 365



Jason Conger
Staff Solutions Architect | Splunk



Ryan Lait
Senior Sales Engineer | Splunk

Am I In The Right Place?

Target Audience: Splunk Power User and Azure/O365 Exposure

You should be familiar with:

- Basic Splunk Searching
- Splunk Add-ons
- Azure
- Office 365

You will learn:

- Azure and Office 365 Data Types
- Azure and Office 365 Plumbing
- Targeted Splunk Searches
- How to be an Azure/O365 + Splunk hero

Presentation Synopsis

Mostly Demo, with a Sprinkle of Slideware

Use Case



Security

- Abnormal File Access
- Login for former employee
- PST Export

Presentation Synopsis

Mostly Demo, with a Sprinkle of Slideware

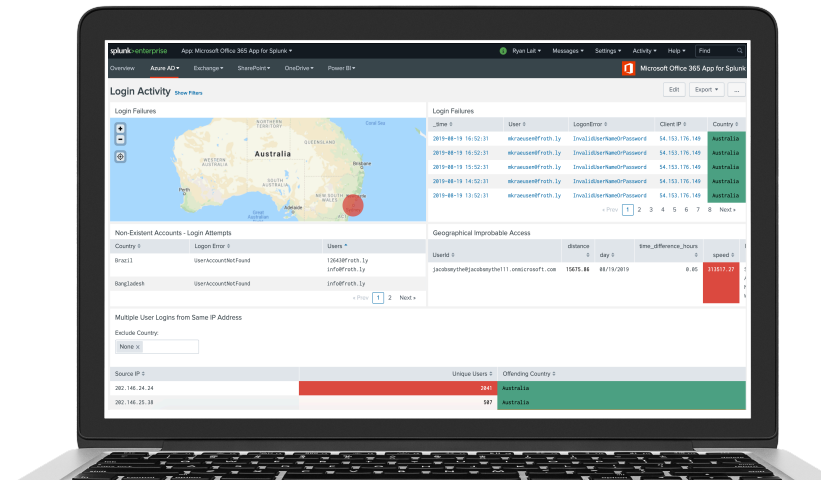
Use Case



Security

- Abnormal File Access
- Login for former employee
- PST Export

Fulfill the Use Case in Splunk



- Searches
- Visualizations
- Integration

Presentation Synopsis

Mostly Demo, with a Sprinkle of Slideware

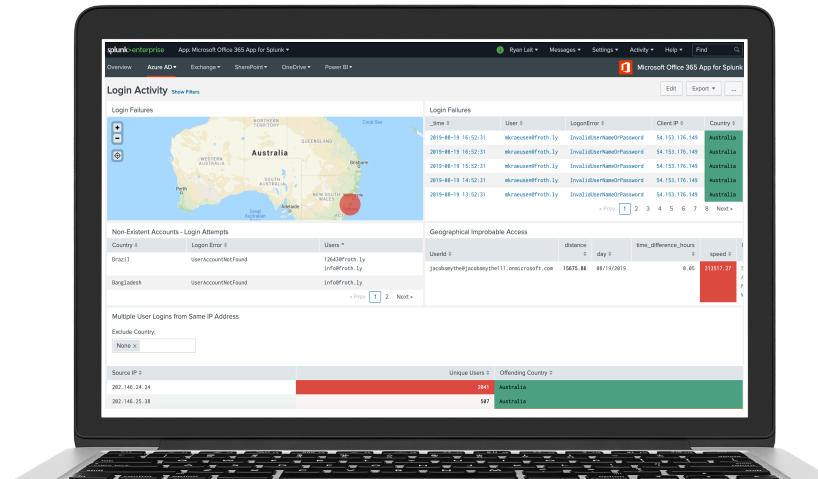
Use Case



Security

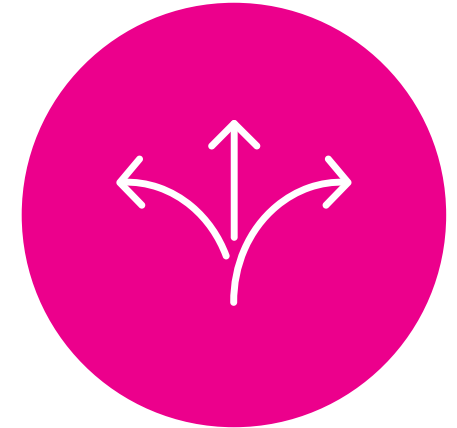
- Abnormal File Access
- Login for former employee
- PST Export

Fulfill the Use Case in Splunk



- Searches
- Visualizations
- Integration

Data Collection



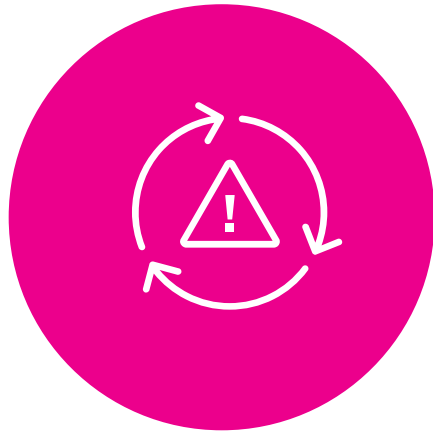
- Add-ons
- Configuration
- Pro tips

Synopsis

Rinse and Repeat



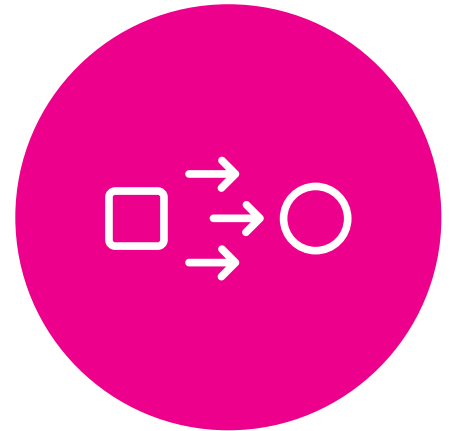
Security



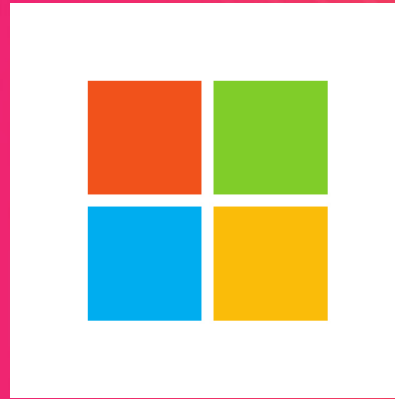
IT Ops



Billing



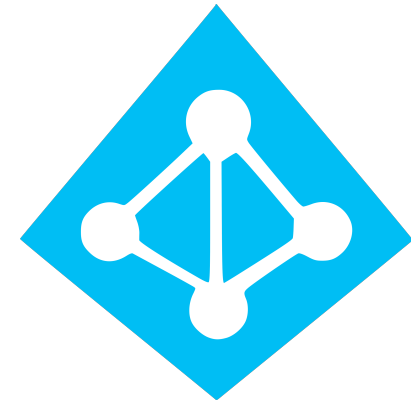
Migration

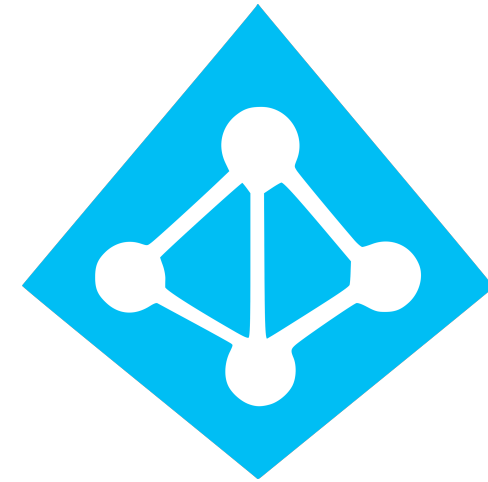


Microsoft Cloud Services

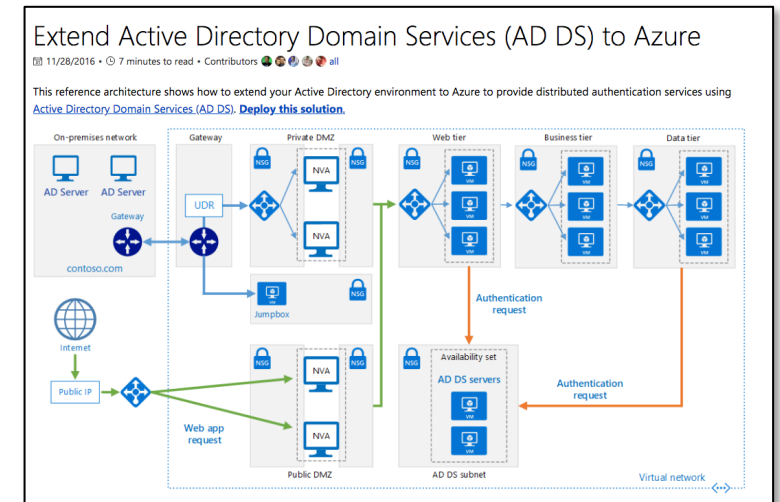
Distinct, yet related







Azure AD





**Before we get started...let's talk
about data types and plumbing.**





3 Log Types in Azure

1) Control/Management, 2) Data Plane, 3) Processed Events

Control: System Configuration and Management

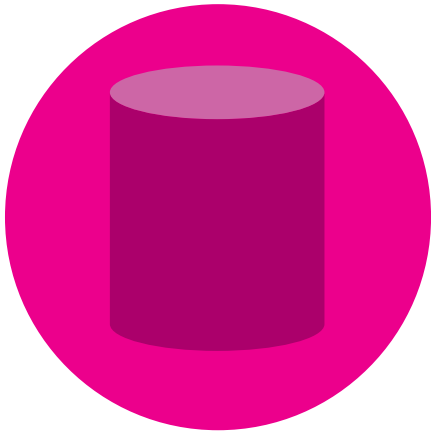
Data Plane: Provisioned Service and Diagnostic Data



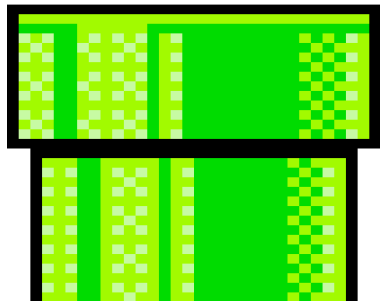
Processed Events: Alerts & Recommendations

3 Main Azure Data Access Methods

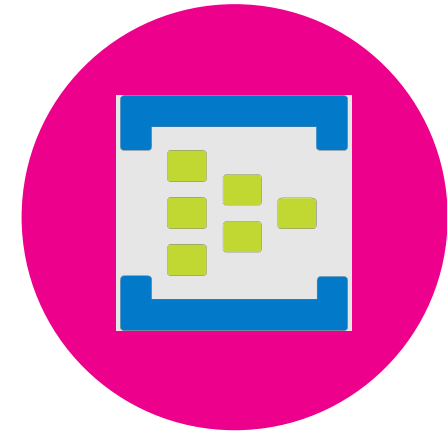
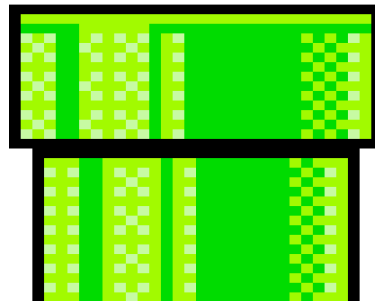
Storage Accounts



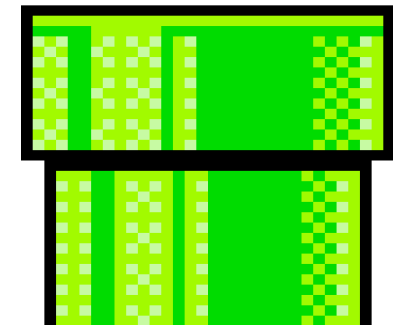
Storage Accounts



REST APIs



Event Hubs





2 Log Types in Office 365

1) Activity Data, 2) State Data

Activity: Who Did What and When

State Data: Mailboxes, Files, Collaboration, etc.

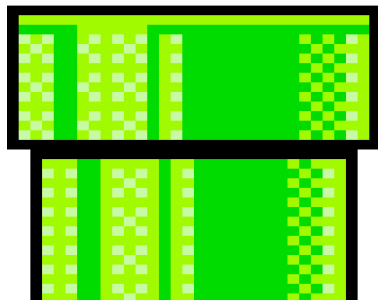


1 Main Office 365 Data Access Method

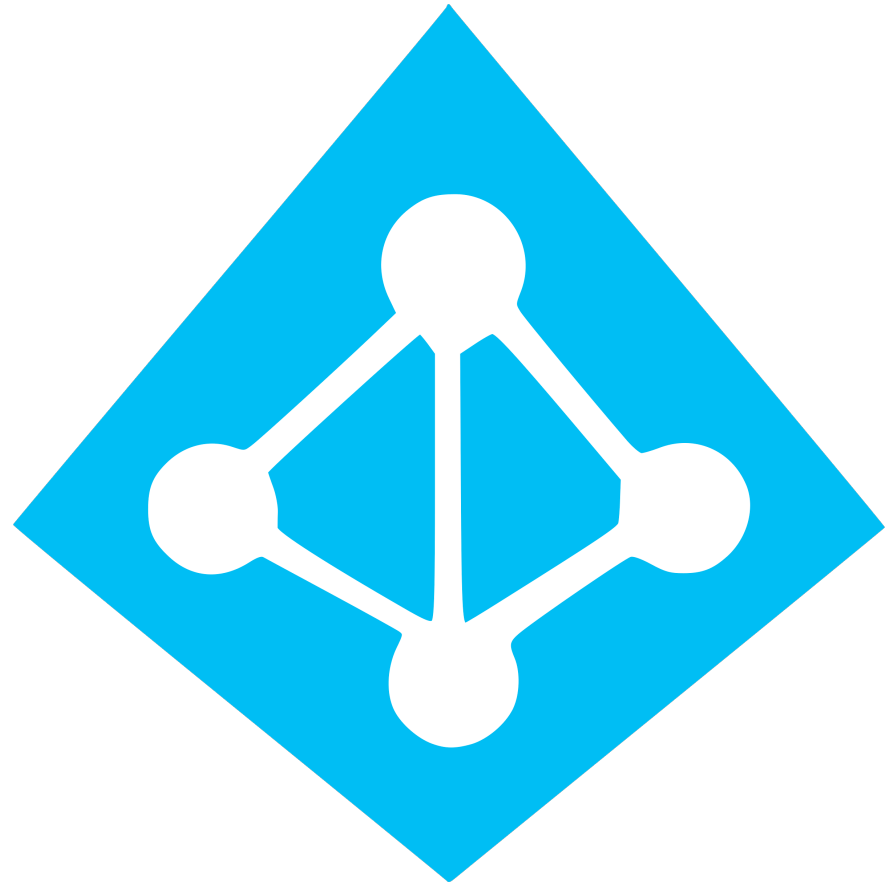
But 3 Main Sources



REST APIs



1. Office 365 Management Activity API
2. Graph API
3. Office 365 Reporting Web Services



3 Log Types in Azure Active Directory

1) Users, 2) Sign-ins, 3) Directory Audits



Users



Sign-ins



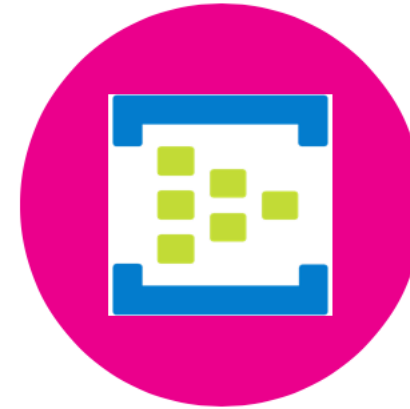
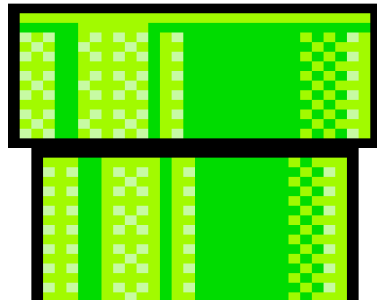
Directory Audits

2 Main Azure Data Access Methods

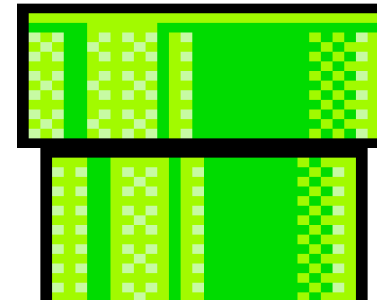
1) REST, 2) Event Hubs



REST APIs



Event Hubs





DEMO Time!

Let's see this in action

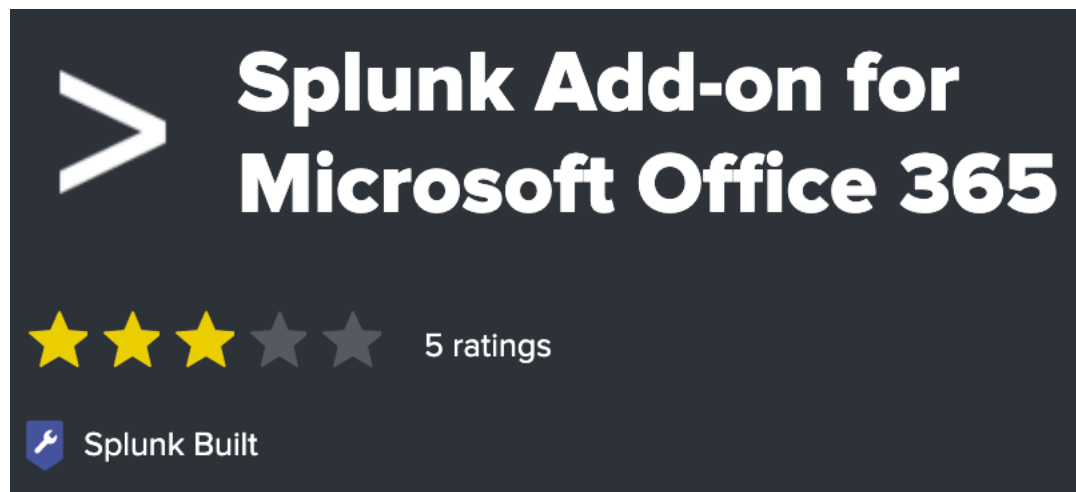


Getting Data In

Splunk Add-on for Microsoft Office 365

Management API Data

<https://splunkbase.splunk.com/app/4055/>



Service Status

Delete the leftover placeholder box

Reset the slide to bring boxes back

Splunk Add-on for Microsoft Cloud Services

Azure Audit Logs



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

Storage Blog & Table

Microsoft Office 365 Reporting Add-on for Splunk

Management API Data



<https://splunkbase.splunk.com/app/3720/>

Service Status

Delete the leftover placeholder box

Reset the slide to bring boxes back

Microsoft Azure Add-on for Splunk

Azure AD sign-ins, audits, users



**Microsoft Azure Add-on
for Splunk**

★★★★★ 0 rating

<https://splunkbase.splunk.com/app/4648/>

Consumption and cost

Inventory

Event Hubs & Metrics

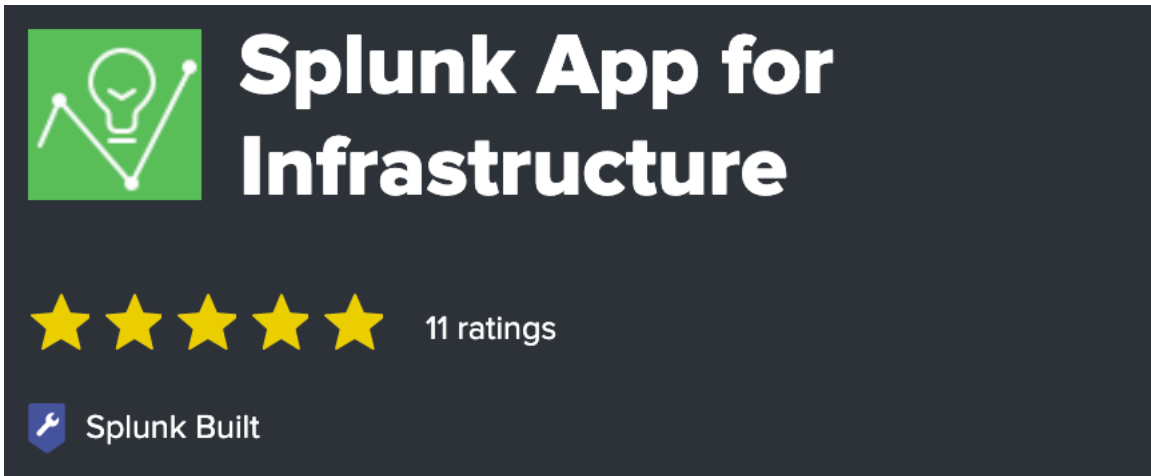
Security Center



Get the Most from Your Data

Splunk App for Infrastructure

Infrastructure Metrics

A dark grey rectangular card representing the Splunk App for Infrastructure. At the top left is a green square icon with a white lightbulb and a line graph. To its right, the text "Splunk App for Infrastructure" is written in white. Below the icon, there are five yellow stars and the text "11 ratings". At the bottom left, there is a blue square icon with a white wrench and the text "Splunk Built".

Splunk App for Infrastructure

★★★★★ 11 ratings

 Splunk Built

<https://splunkbase.splunk.com/app/3975/>

Data onboarding Wizard

Multi-Cloud Correlation

Microsoft Office 365 App for Splunk

Pre-built Dashboards



<https://splunkbase.splunk.com/app/3786/>

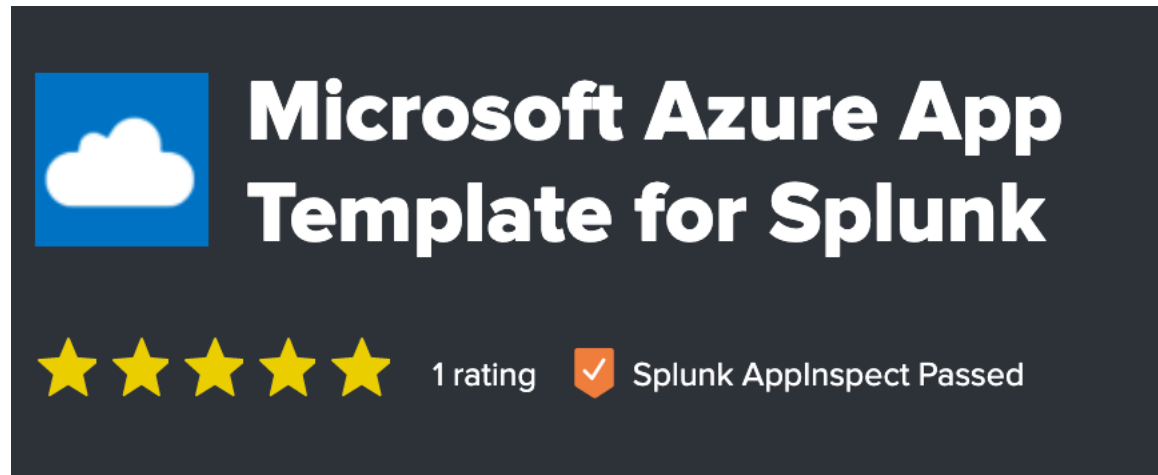
Office 365

Cloud Services

Message Tracking logs

Microsoft Azure App Template for Splunk

Pre-built Dashboards



<https://splunkbase.splunk.com/app/3564/>

Subscription Operations

VM Overview

Performance Monitoring

Key Takeaways

This is where the subtitle goes

1. Add-on Landscape ->
http://bit.ly/Splunk_Azure_Add-ons
2. Add-on Permissions ->
http://bit.ly/Splunk_Azure_Permissions
3. GitHub Link



Q&A

Jason Conger | Staff Solutions Architect
Ryan Lait | Senior Sales Engineer



Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION

