Down in the weeds, up in the Cloud: Security

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

Ryan Lait
Senior Sales Engineer | Splunk

splunk> .conf19

One Million Data Points

Ryan Lait 🇦🇺

- Senior Sales Engineer – Brisbane
- Chief Converse Officer*

splunk> 3 years

- **Customer for 4 years – Cyber Sec**
- **Likes: Obstacle course racing, home automation**
- **Dislikes: Pie Charts**

Microsoft Office 365 App for Splunk
★★★★★ 3 ratings Splunk AppInspect Passed

splunk> BOSS of the SOC 2017 .conf2017

.conf18 splunk> BOSS of the SOC

splunk> BOSS of the SOC Day 2019

* Self-appointed title

splunk> .conf19

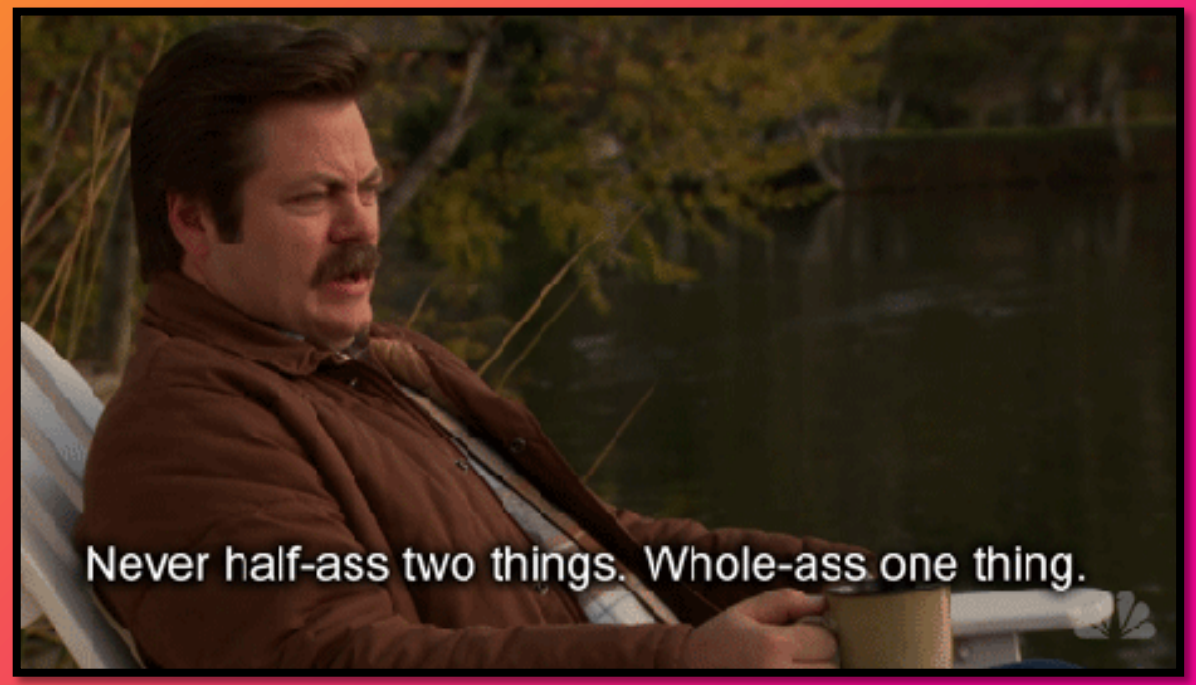
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

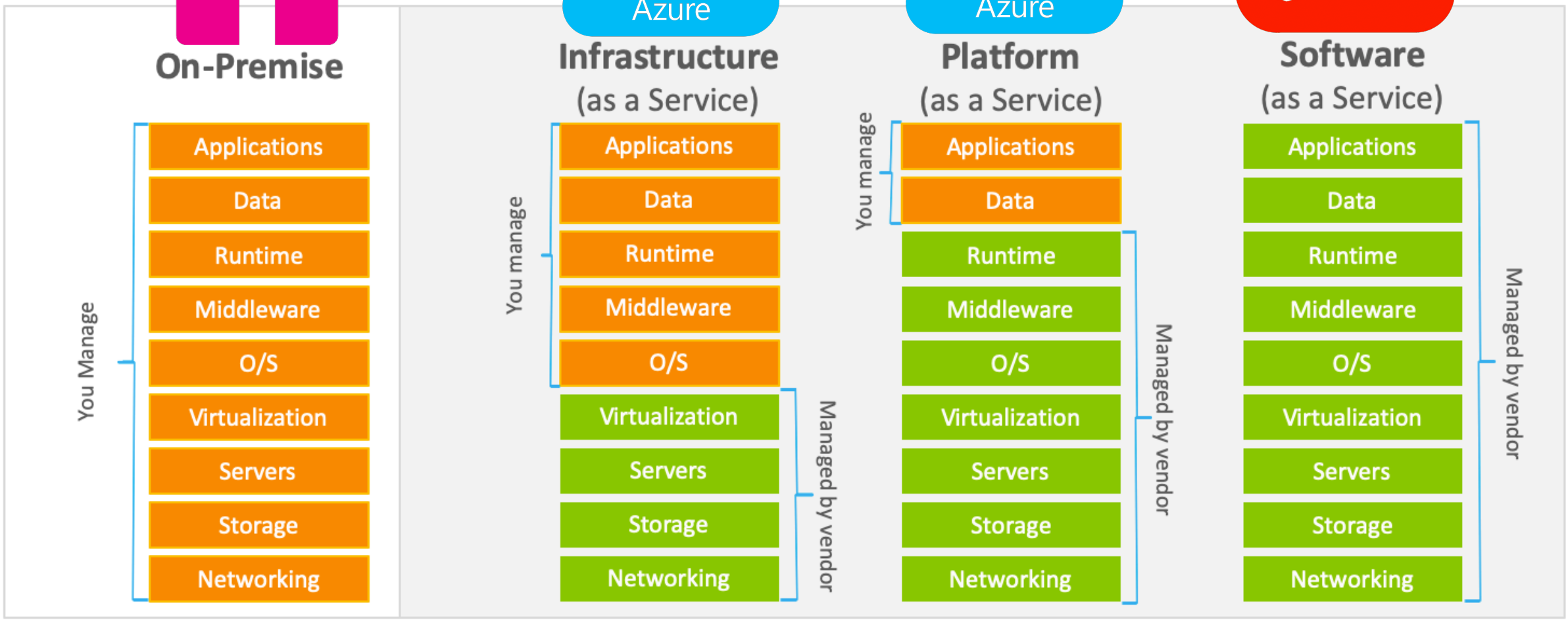
Agenda

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



- Microsoft Azure
- High Priority Security Data Sources
- Microsoft Office 365
- Getting Started
- Next Steps

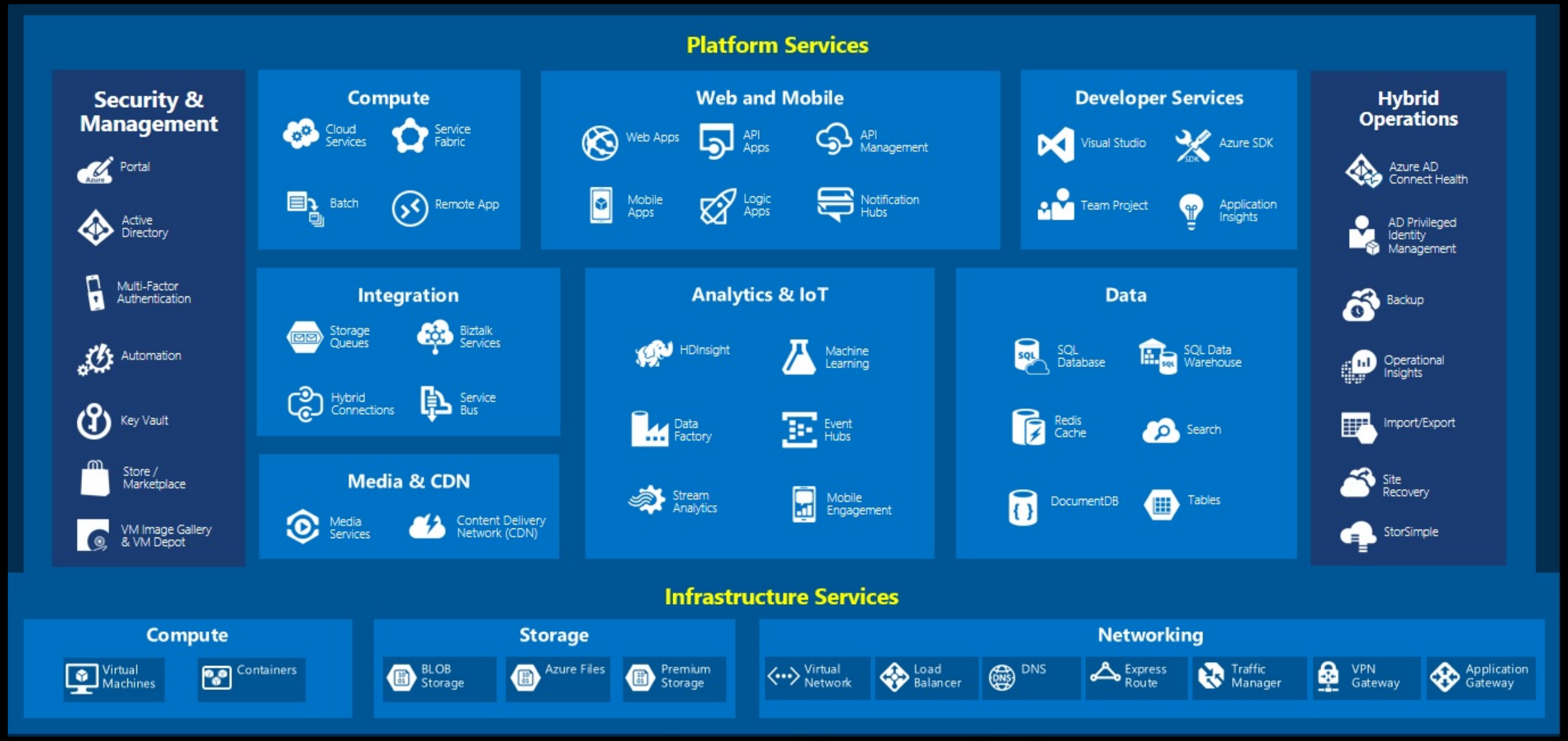
What's the difference?



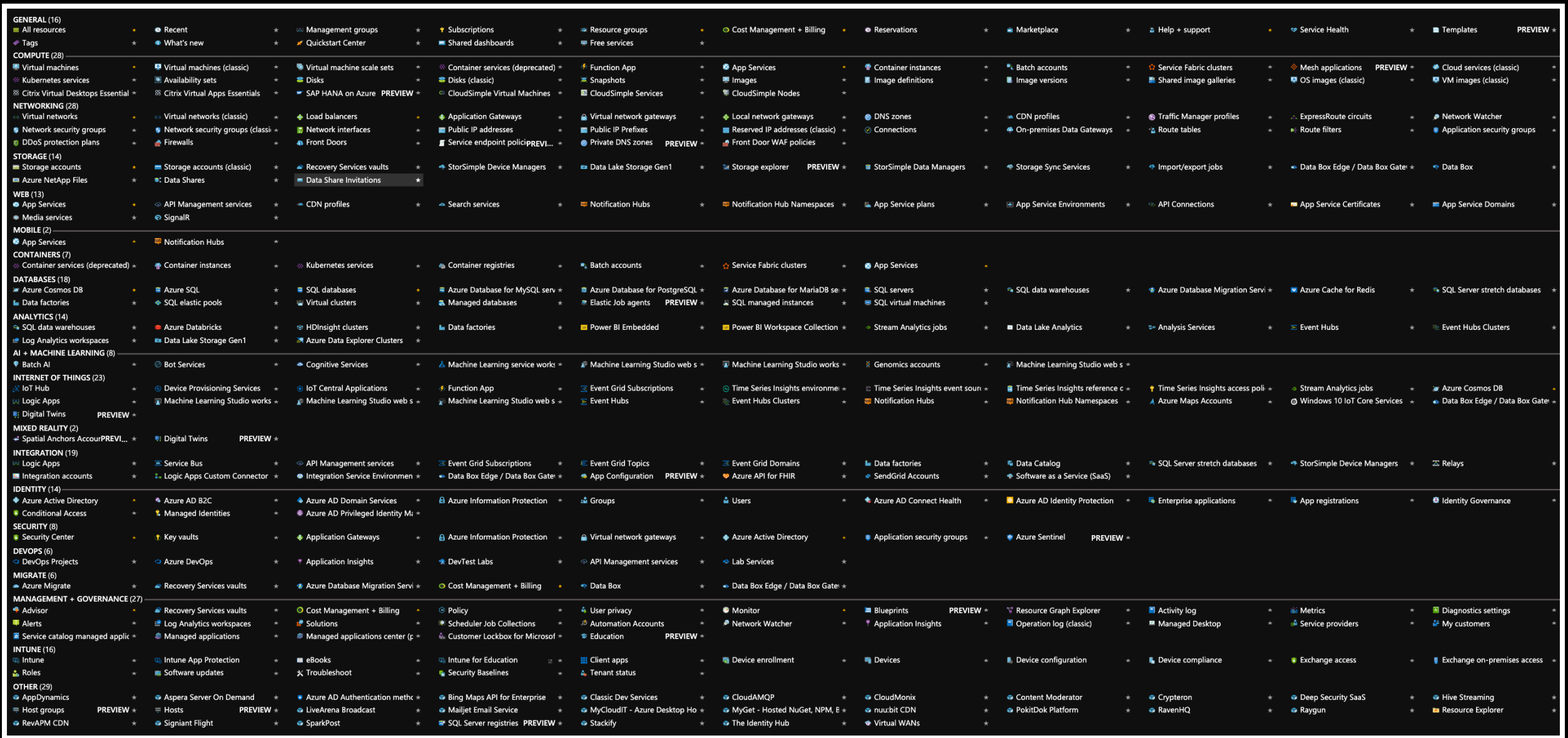
Microsoft Azure

.conf19
splunk>

Microsoft Azure Services



Microsoft Azure Services



But where do I start?

Simple: Forget the “cloud”

It’s just another data center

High Priority Data Sources for Security Visibility

Endpoint

Access & Identity

Network

Cloud

Threat Intelligence

6 Critical SIEM Use Cases

- Detection of Possible Brute Force Attacks
- Detection of Insider Threat
- Expected Host/Log Source Not Reporting
- Unusual Login Behavior
- Unexpected Events Per Second (EPS) from Log Sources
- Detection of Anomalous Ports, Services and Unpatched Devices

https://resources.infosecinstitute.com/top-6-seim-use-cases

High Priority Data Sources for Security Visibility

Endpoint

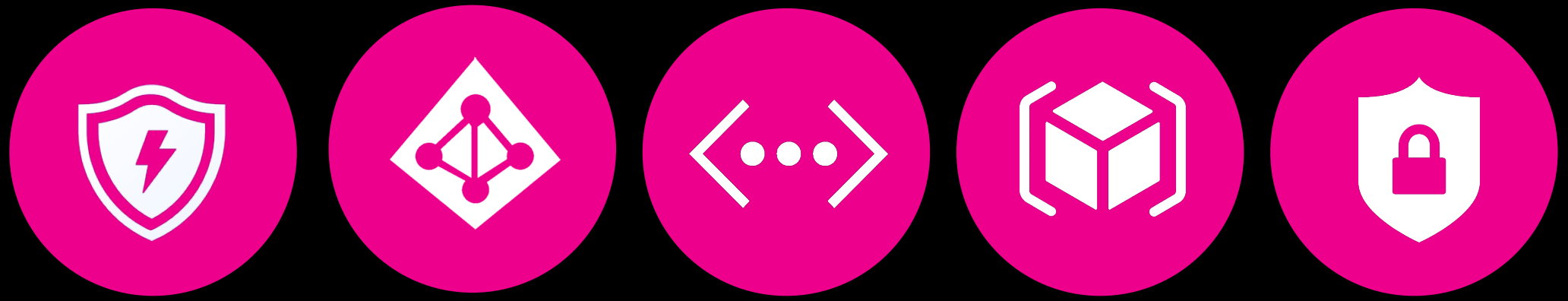
Access & Identity

Network

Cloud

Threat Intelligence

High Priority Data Sources for Security Visibility
Azure Edition



Windows Defender ATP

Azure Active Directory

Azure Virtual Network

Azure Resources

Azure Security Center

Windows Defender

TA for Microsoft Windows Defender

splunk>

{ [-]
  Actor:
  AlertId: da637000534964300640_1200806263
  AlertPart: 0
  AlertTime: 2019-07-30T03:16:18.2285466Z
  AlertTitle: [Test Alert] Suspicious Powershell commandline
  Category: Execution
  CloudCreatedMachineTags:
  CommandLine:
  ComputerDnsName: ghoppy-l.froth.ly
  CreatorIocName:
  CreatorIocValue:
  Description: *** This is a test alert ***
  A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without touching the disk and leaving any trace.
  The process powershell.exe was executing suspicious commandline
  powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-test\\invoice.exe'
  DeviceCreatedMachineTags:
  DeviceID: dd8bcd985f9a3661404552834822cd270cf4d840
  ExternalId: E9F1BD30E049D1FCB940DE1BF09F53D9C883B9FF
  FileHash: 3ce71813199abae99348f61f0caa34e2574f831c
  FileName: cmd.exe
  FilePath: C:\Windows\System32
  FullId: da637000534964300640_1200806263:VgaSWj+iwzADgEx5DecV_VbkB_5sVjyRYUyKwd0aeOQ=
  IncidentLinkToWDATP: https://securitycenter.windows.com/incidents/byalert?alertId=da637000534964300640_1200806263&source=SIEM

Microsoft Azure App for Splunk

InfoSec App for Splunk

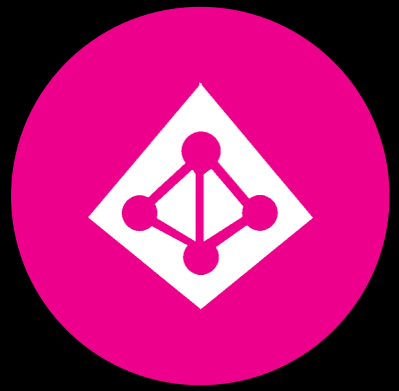
Splunk Enterprise Security™

Splunk User Behavior Analytics™

splunk> phantom

splunk> .conf19

Azure Active Directory



Microsoft Azure Active Directory Add-on for Splunk

Splunk Add-on for Microsoft Cloud Services

splunk>


```
{ [-]
   Actor:
   AlertId: da637000534964300640_1200806263
   AlertPart: 0
   AlertTime: 2019-07-30T03:16:18.2285466Z
   AlertTitle: [Test Alert] Suspicious Powershell commandline
   Category: Execution
   CloudCreatedMachineTags:
   CommandLine:
   ComputerDnsName: ghoppy-l.froth.ly
   CreatorIocName:
   CreatorIocValue:
   Description: *** This is a test alert ***
   A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some
   cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information
   about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without
   touching the disk and leaving any trace.
   The process powershell.exe was executing suspicious commandline
   powershell.exe  -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object
   System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-
   test\\invoice.exe'
   DeviceCreatedMachineTags:
   DeviceID: dd8bcd985f9a3661404552834822cd270cf4d840
   ExternalId: E9F1BD30E049D1FCB940DE1BF09F53D9C883B9FF
   FileHash: 3ce71813199abae99348f61f0caa34e2574f831c
   FileName: cmd.exe
   FilePath: C:\Windows\System32
   FullId: da637000534964300640_1200806263:VgaSWj+iwzADgEx5DecV_VbkB_5sVjyRYUyKwd0aeOQ=
   IncidentLinkToWDATP: https://securitycenter.windows.com/incidents/byalert?alertId=da637000534964300640_1200806263&source=SIEM
```


Microsoft Azure App for Splunk

InfoSec App for Splunk

Splunk Enterprise Security™

Splunk User Behavior Analytics™

splunk> phantom

splunk> .conf19

Azure Virtual Network

Microsoft Azure Metadata Inventory Add-on for Splunk

Splunk Add-on for Microsoft Cloud Services

splunk>

Microsoft Azure App for Splunk

InfoSec App for Splunk

Splunk Enterprise Security™

Splunk User Behavior Analytics™

splunk> phantom

splunk> .conf19

Azure Resources

Microsoft Azure Billing Add-on for Splunk

Microsoft Azure Metadata Inventory Add-on for Splunk

Splunk Add-on for Microsoft Cloud Services

splunk>


```
{ [-]
   Actor:
   AlertId: da637000534964300640_1200806263
   AlertPart: 0
   AlertTime: 2019-07-30T03:16:18.2285466Z
   AlertTitle: [Test Alert] Suspicious Powershell commandline
   Category: Execution
   CloudCreatedMachineTags:
   CommandLine:
   ComputerDnsName: ghoppy-l.froth.ly
   CreatorIocName:
   CreatorIocValue:
   Description: *** This is a test alert ***
   A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some
   cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information
   about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without
   touching the disk and leaving any trace.
   The process powershell.exe was executing suspicious commandline
   powershell.exe  -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object
   System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-
   test\\invoice.exe'
   DeviceCreatedMachineTags:
   DeviceID: dd8bcd985f9a3661404552834822cd270cf4d840
   ExternalId: E9F1BD30E049D1FCB940DE1BF09F53D9C883B9FF
   FileHash: 3ce71813199abae99348f61f0caa34e2574f831c
   FileName: cmd.exe
   FilePath: C:\Windows\System32
   FullId: da637000534964300640_1200806263:VgaSWj+iwzADgEx5DecV_VbkB_5sVjyRYUyKwd0aeOQ=
   IncidentLinkToWDATP: https://securitycenter.windows.com/incidents/byalert?alertId=da637000534964300640_1200806263&source=SIEM
```


Microsoft Azure App for Splunk

InfoSec App for Splunk

Splunk Enterprise Security™

Splunk User Behavior Analytics™

splunk> phantom

Azure Security Center

Microsoft Graph Security API Add-On for Splunk

splunk>


```
{ [-]
   Actor:
   AlertId: da637000534964300640_1200806263
   AlertPart: 0
   AlertTime: 2019-07-30T03:16:18.2285466Z
   AlertTitle: [Test Alert] Suspicious Powershell commandline
   Category: Execution
   CloudCreatedMachineTags:
   CommandLine:
   ComputerDnsName: ghoppy-l.froth.ly
   CreatorIocName:
   CreatorIocValue:
   Description: *** This is a test alert ***
   A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some
   cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information
   about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without
   touching the disk and leaving any trace.
   The process powershell.exe was executing suspicious commandline
   powershell.exe  -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference= 'silentlycontinue';(New-Object
   System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-test\\invoice.exe');Start-Process 'C:\\test-WDATP-
   test\\invoice.exe'
   DeviceCreatedMachineTags:
   DeviceID: dd8bcd985f9a3661404552834822cd270cf4d840
   ExternalId: E9F1BD30E049D1FCB940DE1BF09F53D9C883B9FF
   FileHash: 3ce71813199abae99348f61f0caa34e2574f831c
   FileName: cmd.exe
   FilePath: C:\Windows\System32
   FullId: da637000534964300640_1200806263:VgaSWj+iwzADgEx5DecV_VbkB_5sVjyRYUyKwd0aeOQ=
   IncidentLinkToWDATP: https://securitycenter.windows.com/incidents/byalert?alertId=da637000534964300640_1200806263&source=SIEM
```


Microsoft Azure App for Splunk

InfoSec App for Splunk

Splunk Enterprise Security™

Splunk User Behavior Analytics™

splunk> phantom

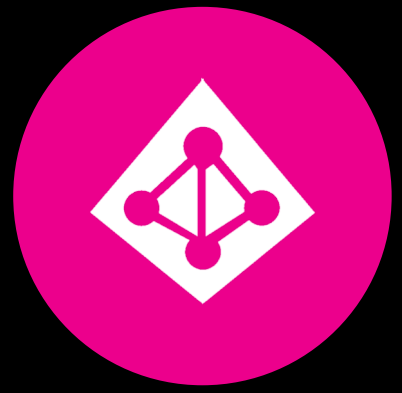
Source=Azure Destination=Splunk

TA for Microsoft Windows Defender

Windows Defender ATP

Microsoft Azure Active Directory Add-on for Splunk

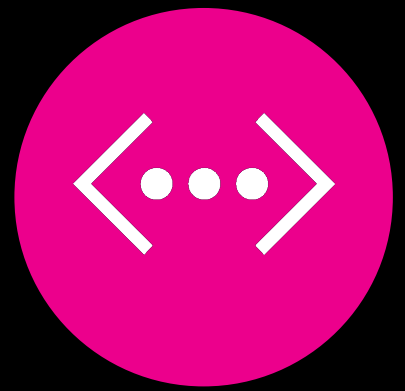
Splunk Add-on for Microsoft Cloud Services



Azure Active Directory

Microsoft Azure Metadata Inventory Add-on for Splunk

Splunk Add-on for Microsoft Cloud Services



Azure Virtual Network

Microsoft Azure Billing Add-on for Splunk

Microsoft Azure Metadata Inventory Add-on for Splunk

Splunk Add-on for Microsoft Cloud Services

Azure Resources

Microsoft Graph Security API Add-On for Splunk

Azure Security Center

splunk> .conf19

Demo

Office 365

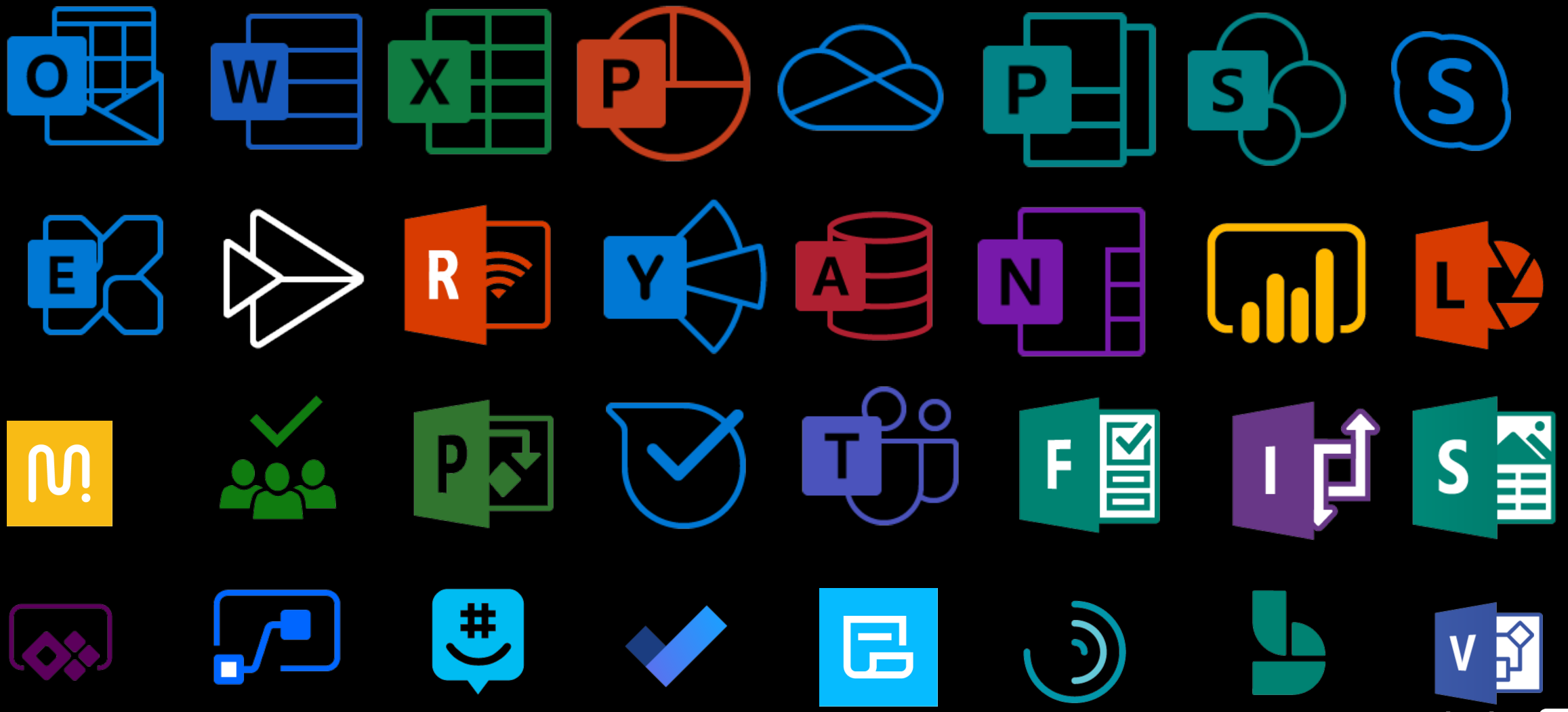
.conf19
splunk>

What is Office 365?

It's the apps you know and love

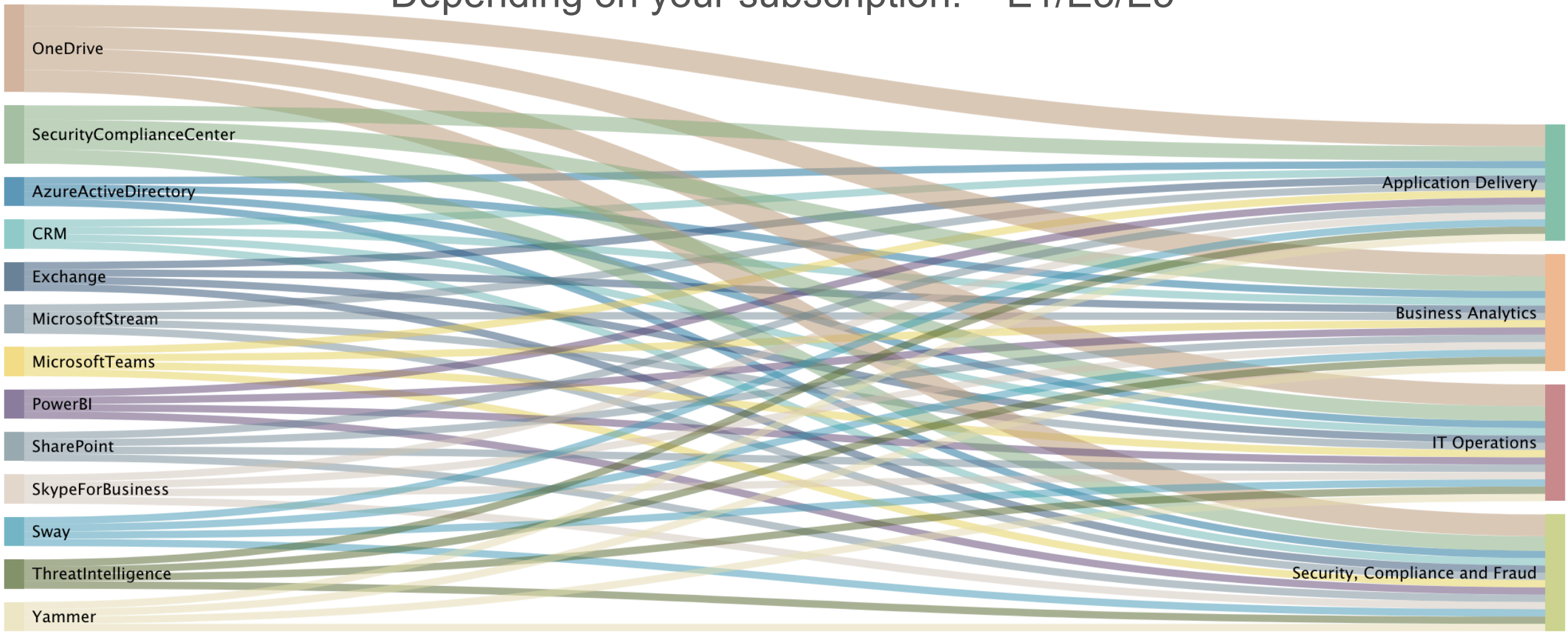
Word, Excel, PowerPoint, Outlook, OneNote, OneDrive—and on your PC, Publisher and Access. Everything you need for home, school, and work.

Microsoft Office 365



Workloads

Depending on your subscription! – E1/E3/E5



Demo

Next Steps

.conf19
splunk>

Check out these other awesome sessions!

This is where the subtitle goes

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

SCHEDULE Tuesday, October 22, 04:15 PM - 05:00 PM

Ry Lait, Senior Sales Engineer, Splunk

Analytics Workspaces, Application Insights, Azure Monitor, O365 Admin Centers, just a few of the many Microsoft tools required to monitor and interrogate information from Azure & Office 365. Getting the valuable intel and insights from your Azure...

Industries: Not industry specific
Products: Splunk Enterprise, Splunk Cloud, Splunk IT Service Intelligence

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

SCHEDULE Wednesday, October 23, 04:15 PM - 05:00 PM

Jason Conger, Solution Architect, Splunk
Ry Lait, Senior Sales Engineer, Splunk

Let's face it, sometimes you don't know what you don't know. With vast amounts of cloud data coming in at cloud-speed, it can be difficult to see through the noise and know what to look for. Are malicious adversaries attempting to comprise the...

Industries: Not industry specific
Products: Splunk Enterprise, Splunk Enterprise Security, Splunk Machine Learning Toolkit

IT2001 - Monitoring and troubleshooting workloads running on public cloud infrastructure made easy

SCHEDULE Wednesday, October 23, 11:15 AM - 12:00 PM

Subu Baskaran, Product Manager, Splunk
Om Thoppai, Principal Software Engineer, Splunk

Monitoring and troubleshooting infrastructure running on multiple public cloud environments can be a daunting task. In this session, we will demonstrate how Splunk App for Infrastructure can help you bring Metrics, Logs and Cloud Native Events to monitor the health of your environment in near real-time, troubleshoot failing entities and gain complete control over your public cloud infrastructure.

Industries: Not industry specific
Products: Splunk Enterprise, Splunk Cloud

splunk> .conf19

.conf19

splunk>

Thank You!

Appendix

Splunk Enterprise

Splunk App for Azure

- If you don't need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

splunk> .conf19

Splunk Infosec?

This is where the subtitle goes

- If you don’t need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

Splunk Enterprise Security

This is where the subtitle goes

- If you don’t need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

Splunk Phantom

This is where the subtitle goes

- If you don’t need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

Splunk Enterprise

Splunk App for Azure

- If you don't need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

splunk> .conf19

Splunk Infosec?

This is where the subtitle goes

- If you don’t need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

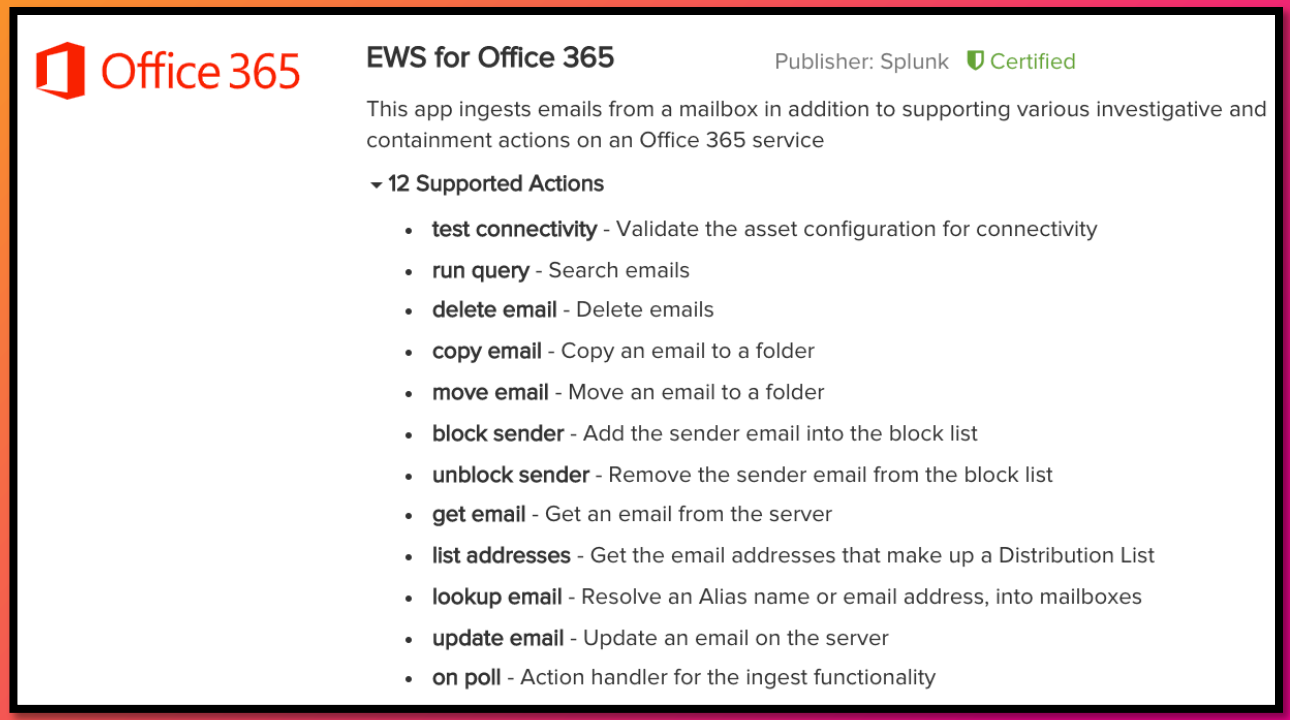
Splunk Enterprise Security

This is where the subtitle goes

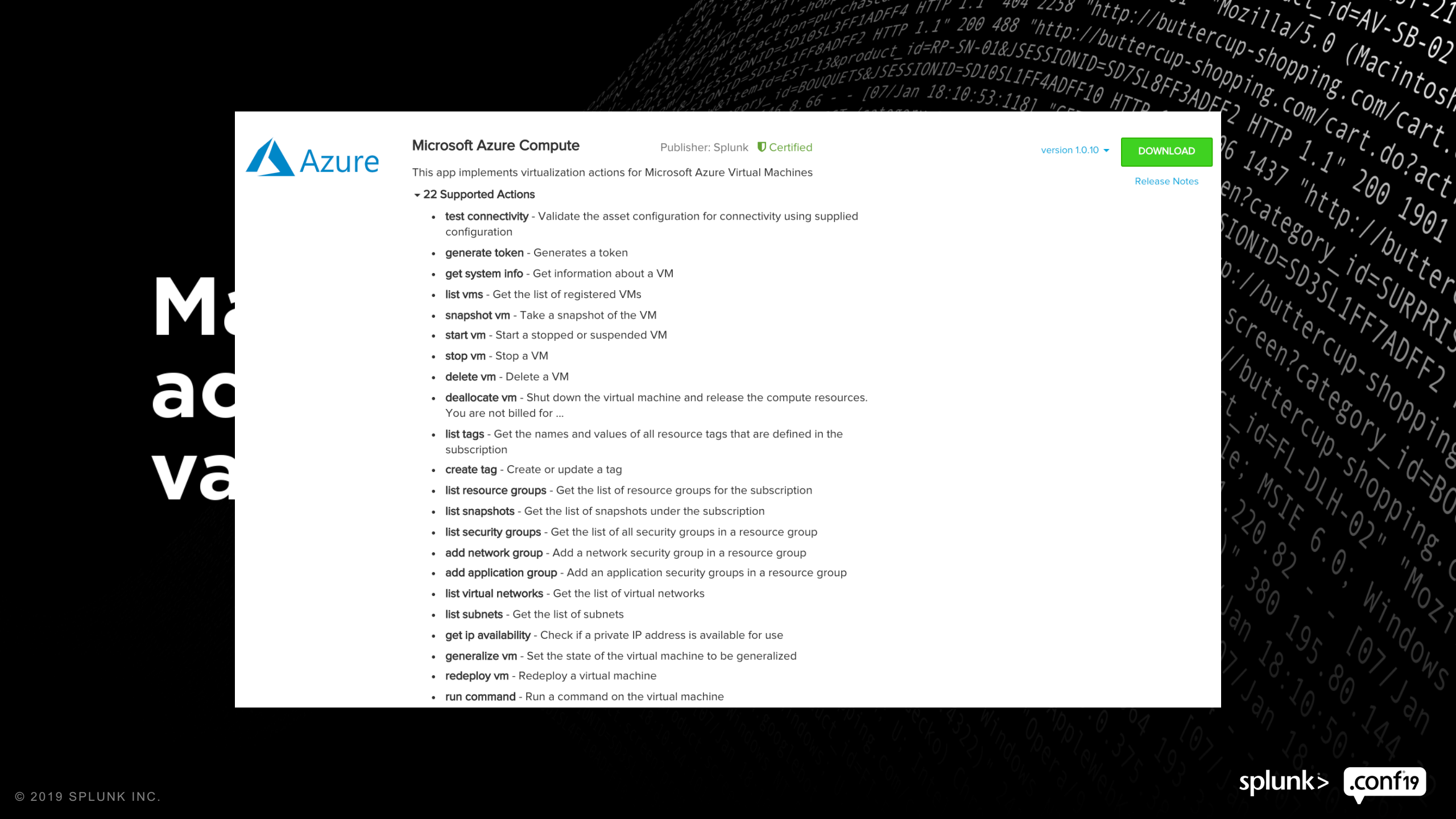
- If you don’t need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

Splunk Phantom

This is where the subtitle goes



- If you don't need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back



Azure AD Graph

Publisher: Splunk Certified

version 1.0.6

DOWNLOAD

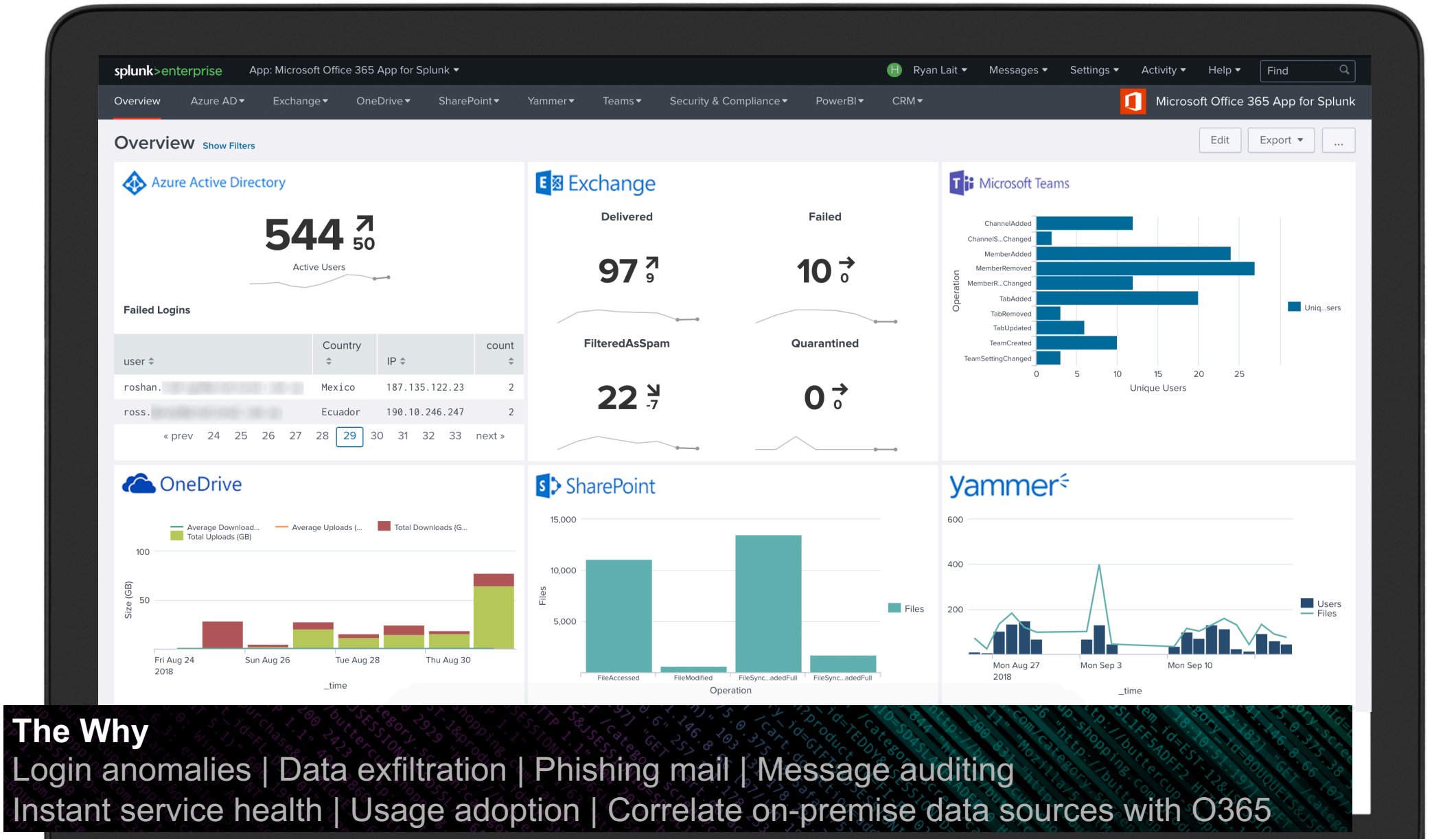
Release Notes

Connects to Azure AD Graph REST API services

15 Supported Actions

- **test connectivity** - Use supplied credentials to generate a token with MS Graph
- **list users** - List users in a tenant
- **reset password** - Reset or set a user's password in an Azure AD environment
- **disable tokens** - Invalidate all active refresh tokens for a user in an Azure AD environment
- **enable user** - Enable a user
- **disable user** - Disable a user
- **list user attributes** - List attributes for all or a specified user
- **set user attribute** - Set an attribute for a user
- **remove user** - Remove a user from a specified group
- **add user** - Add a user to the tenant by creating an organizational account
- **list groups** - List groups in organization
- **get group** - Get information about a group
- **list group members** - List the members in a group
- **validate group** - Returns true if a user is in a group; otherwise, false
- **list directory roles** - List the directory roles in a tenant

splunk> .conf19



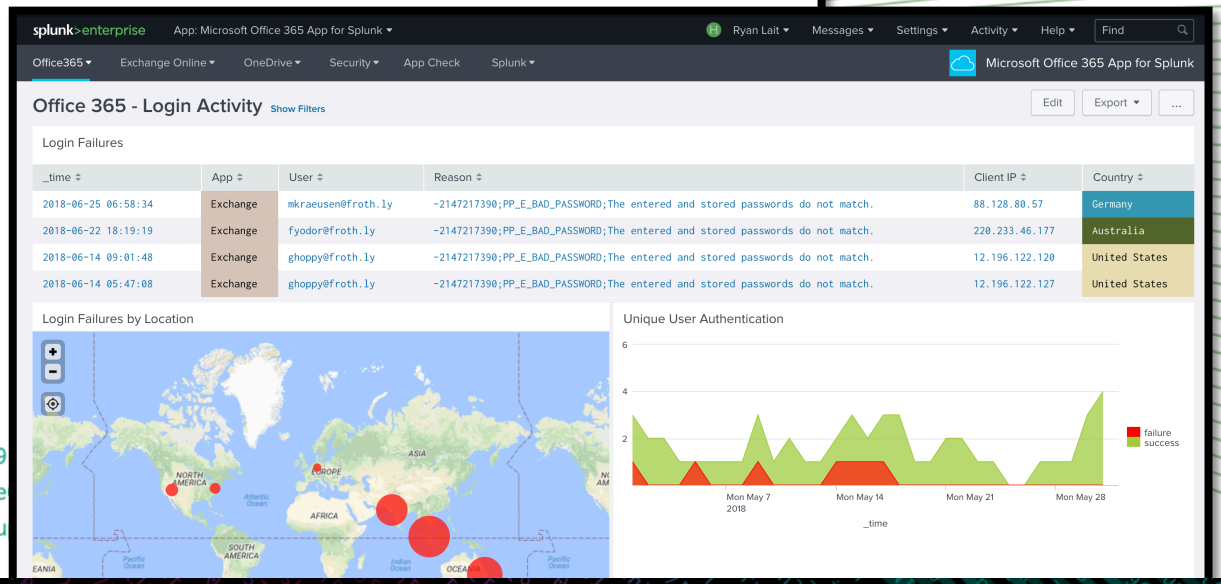
The Why

Login anomalies | Data exfiltration | Phishing mail | Message auditing

Instant service health | Usage adoption | Correlate on-premise data sources with O365

Azure Active Directory

{ [-]
  Actor: [[+]
  ]
  ActorContextId: d51ef8df-6617-4356-b8d4-89ad7efef31e
  AzureActiveDirectoryEventType: 1
  CreationTime: 2018-06-22T16:57:37
  Id: 274b971c-d57c-49e0-878b-58bceed7b654
  InterSystemsId: f103b4eb-1285-4bdb-8001-655bffb85059
  IntraSystemId: 76522644-af27-4f80-b51c-4b70c157b15b
  ObjectId: mkraeusen@froth.ly
  Operation: Reset user password.
  OrganizationId: 225e05a1-5914-4688-a404-7030e60f3143
  RecordType: 8
  ResultStatus: success
  Target: [[-]
    { [+]
    }
    { [-]
      ID: mkraeusen@froth.ly
      Type: 5
    }
    { [+]
    }
  ]
  TargetContextId: 225e05a1-59
  UserId: fim_password_service
  UserKey: 100300008060F582@su
  UserType: 0



Add OAuth2PermissionGrant.
Add app role assignment grant to user.
Add app role assignment to service principal.
Add application.
Add device configuration.
Add device.
Add group.
Add member to group.
Add member to role.
Add owner to group.
Add registered owner to device.
Add registered users to device.
Add service principal.
Add user.
Change user license.
Change user password.
Consent to application.
Create application password for user.
Delete device.
Delete group.
Delete user.
Disable account.
Enable Strong Authentication.
Finish applying group based license to users.
ForeignRealmIndexLogonInitialAuthUsingADFSFederatedToken
Hard Delete group.
PasswordLogonInitialAuthUsingADFSFederatedToken
PasswordLogonInitialAuthUsingPassword
Remove OAuth2PermissionGrant.
Remove member from group.
Remove member from role.
Remove owner from group.
Reset user password.
Set Company Information.
Set domain authentication.
Set federation settings on domain.
Set user manager.
Start applying group based license to users.
Trigger group license recalculation.
Update StsRefreshTokenValidFrom Timestamp.
Update application.
Update device configuration.
Update device.
Update domain.
Update group.
Update service principal.
Update user.
UserLoggedIn
UserLoginFailed

The Why

Login activity | Geographical activity | License usage | Device auditing | User auditing | ADFS auditing | etc

splunk> .conf19

Exchange Online

Message Tracking Logs

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

Overview | Azure AD ▾ | Exchange ▾ | OneDrive ▾ | SharePoint ▾ | Yammer ▾ | Teams ▾ | Security & Compliance ▾ | PowerBI ▾ | CRM ▾ | Microsoft Office 365 App for Splunk

Exchange Online - Message Trace

Edit | Export ▾ | ...

Option: Sender

Sender: fundreceiveoffice0003@yahoo.c

Last 30 days

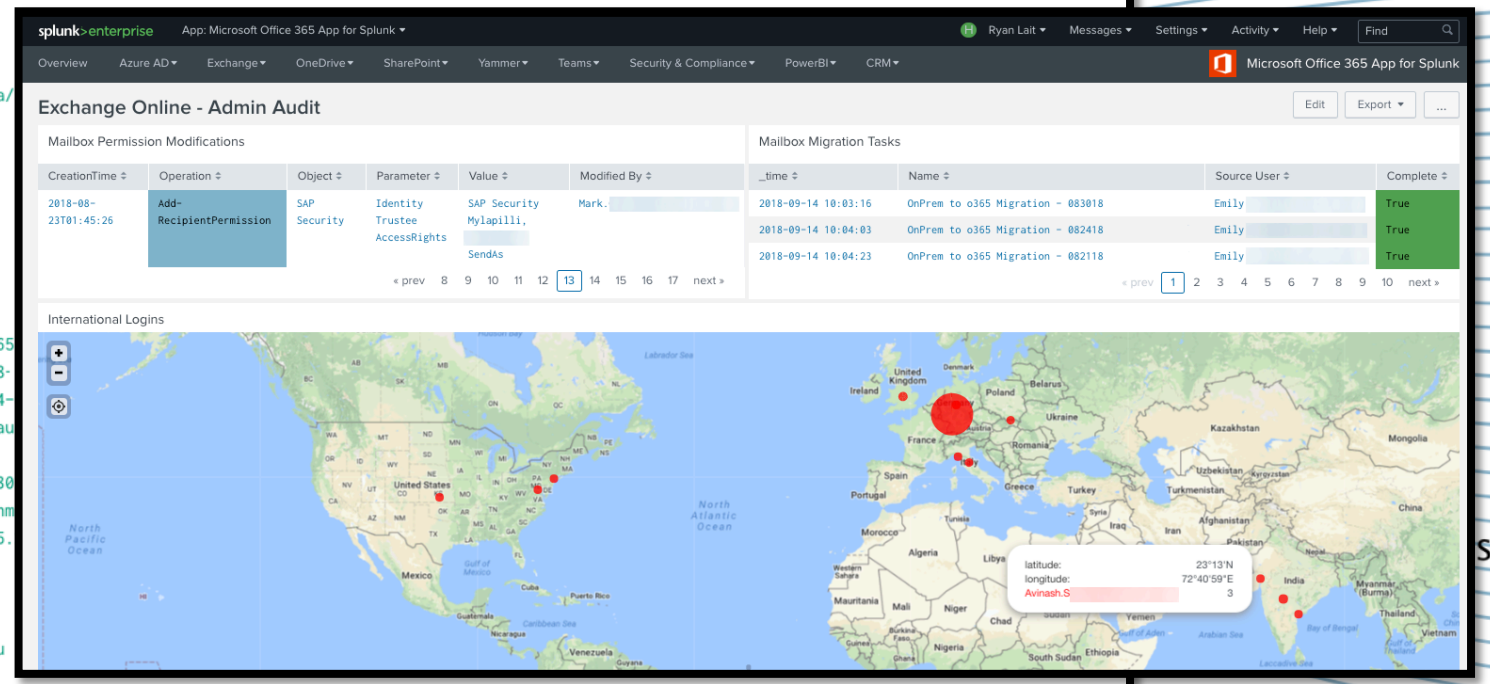
Hide Filters

_time	SenderAddress	RecipientAddress	Subject	Status
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	abungstein@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	GettingStatus
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	bstoll@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Delivered
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	mkraeusen@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Delivered
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	bgist@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Failed
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	fyodor@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Delivered
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	btun@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Delivered
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	pcerf@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Delivered
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	jwortoski@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Delivered
2018-09-04 19:34:06	fundreceiveoffice0003@yahoo.com	ghoppy@froth.ly	THIS IS YOUR ATM TRACKING NUMBER USE USPS Tracking number. EL350153872U	Delivered

Exchange Online

{ [-]
  AffectedItems: [[-]
    { [-]
      Attachments: [redacted].pdf
      Id: RgAAAADzDJswFhr6TYbUC0t7ad3aBwBKRAWKlNTlQ4SatmX5ZKHEAAAQMLCTAAA1Cz4/
      InternetMessageId: <1546522443.1095.1532310697837.JavaMail.gsadmin@pgsas204.asxprod.asx.com.au>
      ParentFolder: { [+]
      }
      Subject: [redacted]
    }
  ]
  ClientIPAddress: [redacted]
  ClientInfoString: Client=OWA;Mozilla/
  CreationTime: 2018-07-23T05:49:40
  CrossMailboxOperation: false
  ExternalAccess: false
  Folder: { [+]
  }
  Id: 07d9178c-138d-4fda-d42b-
  InternalLogonType: 0
  LogonType: 2
  LogonUserSid: S-1-5-21-3551695864-665
  MailboxGuid: 91810413-f0b3-47b5-a438-
  MailboxOwnerSid: S-1-5-21-3551695864-
  MailboxOwnerUPN: [redacted].com.au
  Operation: HardDelete
  OrganizationId: a74a1efc-372d-476c-80
  OrganizationName: [redacted].onm
  OriginatingServer: SYXPR01MB1408 (15.

  RecordType: 3
  ResultStatus: Succeeded
  UserId: [redacted].com.au
  UserKey: 1003000093F



Add-DistributionGroupMember
Add-MailboxFolderPermission
Add-MailboxPermission
Add-RecipientPermission
AddFolderPermissions
Create
Enable-AddressListPaging
FolderBind
HardDelete
Install-AdminAuditLogConfig
Install-DataClassificationConfig
Install-DefaultSharingPolicy
Install-ResourceConfig
MailboxLogin
ModifyFolderPermissions
Move
New-ExchangeAssistanceConfig
New-InboxRule
New-Mailbox
New-MailboxRelocationRequest
New-MailboxRestoreRequest
New-MigrationBatch
Remove-App
Remove-MailboxLocation
Remove-MoveRequest
Remove-UnifiedGroup
SendAs
Set-AdminAuditLogConfig
Set-DistributionGroup
Set-ExchangeAssistanceConfig
Set-MailUser
Set-Mailbox
Set-OwaMailboxPolicy
Set-RecipientEnforcementProvisioningPolicy
Set-SyncUser
Set-TenantObjectVersion
Set-TransportConfig
Set-UnifiedGroup
Set-User
SoftDelete
Update
Update-DistributionGroupMember

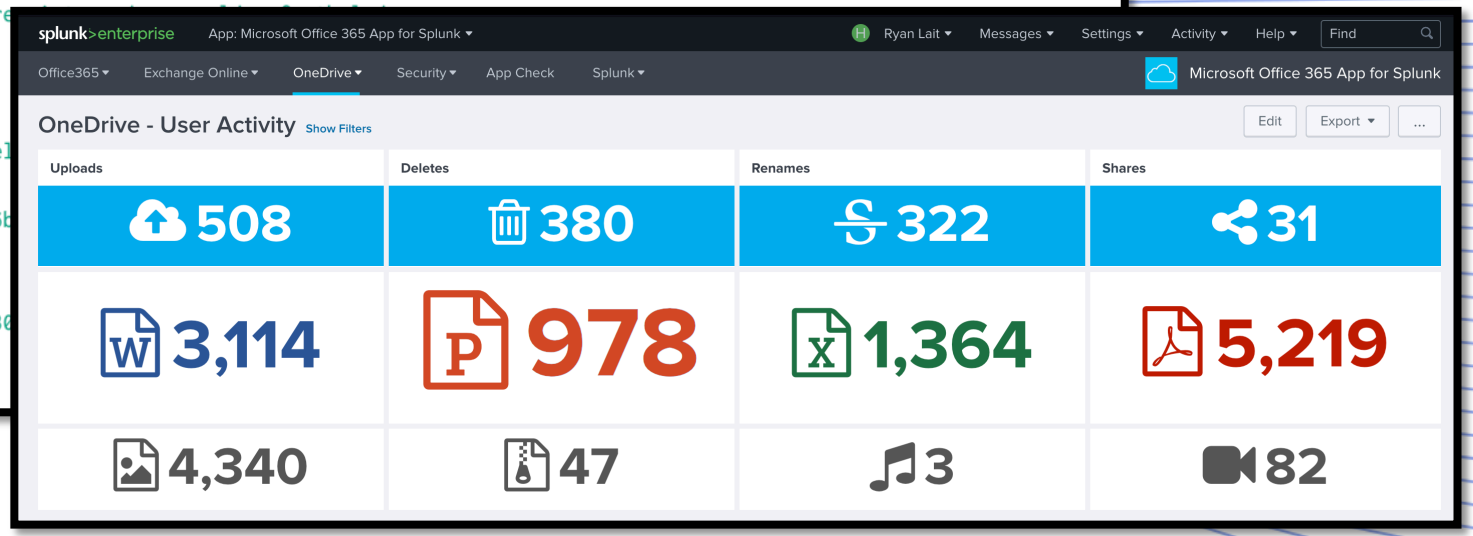
The Why

Mailbox investigations | Spam & phishing | Account compromise | Admin Audit | Misconfigurations | Device Management | Capacity planning |

splunk> .conf19

OneDrive

{ [-]
  ClientIP: [redacted]
  CorrelationId: ae207c9e-0054-6000-3667-3ef231038918
  CreationTime: 2018-07-19T00:08:42
  EventSource: SharePoint
  Id: 1c0c33fe-daa3-4d11-b586-08d5ed0bc9c3
  ItemType: File
  ListId: 67091393-e290-421e-ac6a-2734e2b12a94
  ListItemUniqueId: 933f7827-29c5-47a0-b41b-c977a7f70420
  ObjectId: https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg
  Operation: FileDeleted
  OrganizationId: 225e05a1-5914-4688-a404-7030e60f3143
  RecordType: 6
  Site: 66079e37-e489-49f1-b266-513657d785bb
  SiteUrl: https://jacobsmythe111-my.share
  SourceFileExtension: jpg
  SourceFileName: office365.jpg
  SourceRelativeUrl: Documents
  UserAgent: Mozilla/5.0 (Macintosh; Intel
  UserId: ry@froth.ly
  UserKey: i:0h.f|membership|10033fffac46b
  UserType: 0
  Version: 1
  WebId: 7acb35b6-e1ec-44ed-9099-38580e330
  Workload: OneDrive
}



AccessRequestApproved
AccessRequestCreated
AddedToGroup
AddedToSecureLink
AnonymousLinkCreated
CompanyLinkCreated
CompanyLinkUsed
FileAccessed
FileAccessedExtended
FileCheckedIn
FileCheckedOut
FileCopied
FileDeleted
FileDeletedFirstStageRecycleBin
FileDownloaded
FileMalwareDetected
FileModified
FileModifiedExtended
FileMoved
FilePreviewed
FileRenamed
FileRestored
FileSyncDownloadedFull
FileSyncDownloadedPartial
FileSyncUploadedFull
FileUploaded
FolderCreated
FolderDeleted
FolderModified
FolderMoved
FolderRenamed
FolderRestored
GroupAdded
ListCreated
ListUpdated
PageViewed
PageViewedExtended
PermissionLevelAdded
RemovedFromSecureLink
RemovedFromSharedWithMe
RemovedFromSiteCollection
SecureLinkCreated
SecureLinkDeleted
SecureLinkUsed
SharingInheritanceBroken
SharingRevoked
SharingSet
SiteCollectionAdminAdded
SiteCollectionAdminRemoved
SiteCollectionCreated
WACTokenShared

The Why

File auditing | External access | Data exfiltration | Policy enforcement | Adoption | Capacity planning |

splunk> .conf19

Photo with Title and Bullets

This is where the subtitle goes

- If you don’t need all four lines…
- Simply select a box and delete
- Delete the leftover placeholder box
- Reset the slide to bring boxes back

Bullet Slide

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

Seventh level is for paragraphs with no bullets, 24pt

Eighth level is for paragraphs with no bullets, 20pt

Ninth level is for paragraphs with no bullets, 16pt

Two Column Text Layouts

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

Comparison

This is where the subtitle goes

Title, 24pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

Title, 24pt, Bold

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Sixth level tab is for highlight content, 28pt, Bold

Three Column Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Fifth level tab is for highlighted text, 20pt

Three Column Quotes

This is where the subtitle goes

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

"First level quote should be sentence case, 24pt."

- ***Second level source, 14pt, Bold, Italic***

Title and Subtitle Only

This is where the subtitle goes

Title and Subtitle with No Footer Graphic

This is where the subtitle goes

“Quotes are more impactful when you selectively highlight key terms.”

Source information here

Screenshot and Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

splunk> .conf19

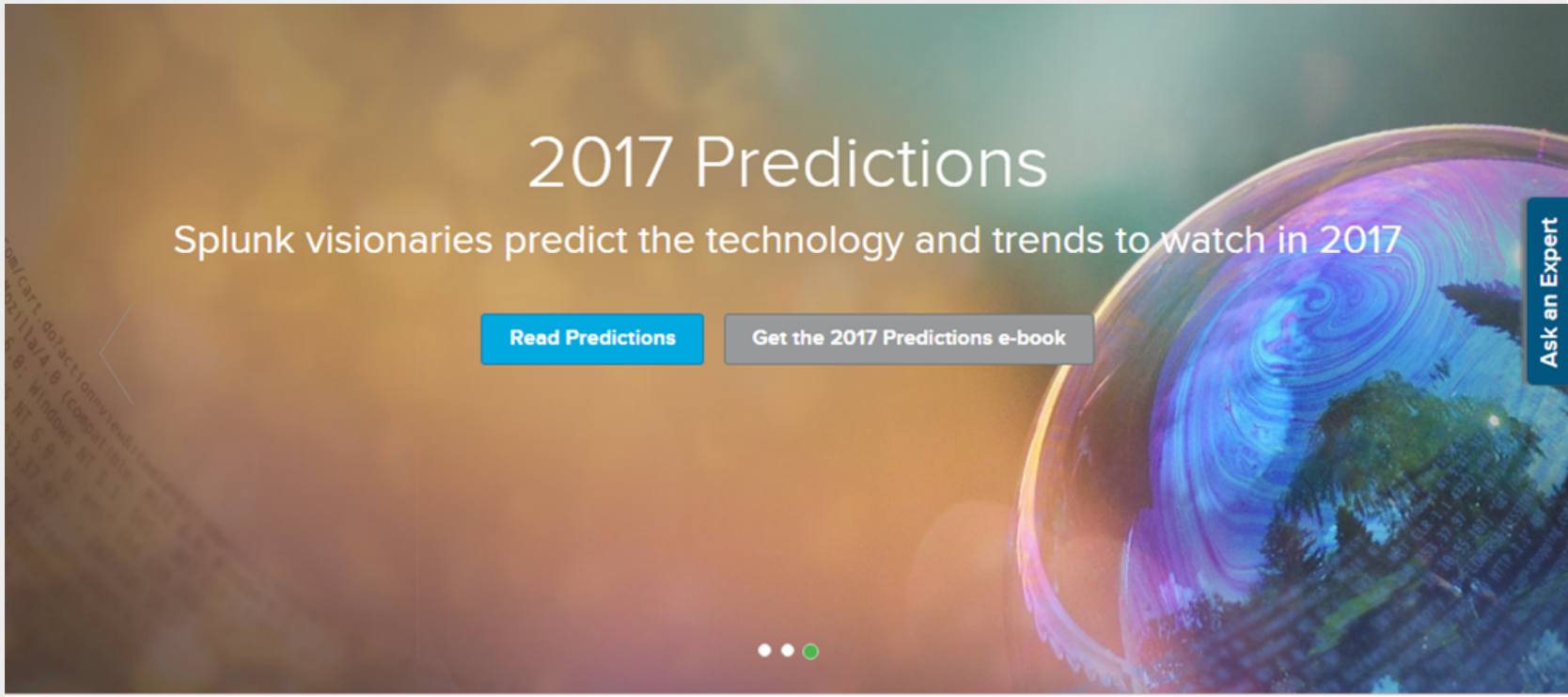
Screenshot and Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Screenshot and Title

This is where the subtitle goes



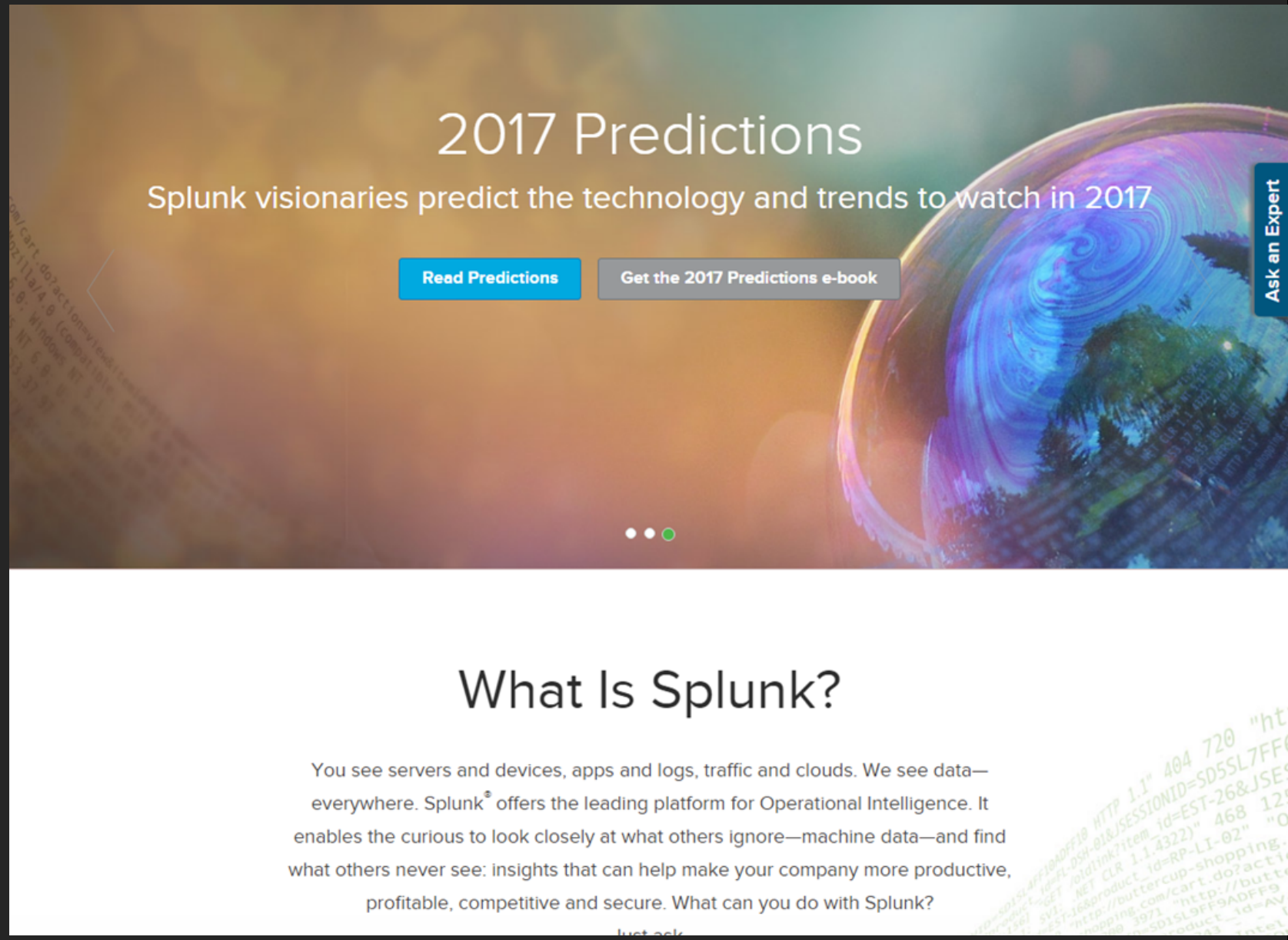
What Is Splunk?

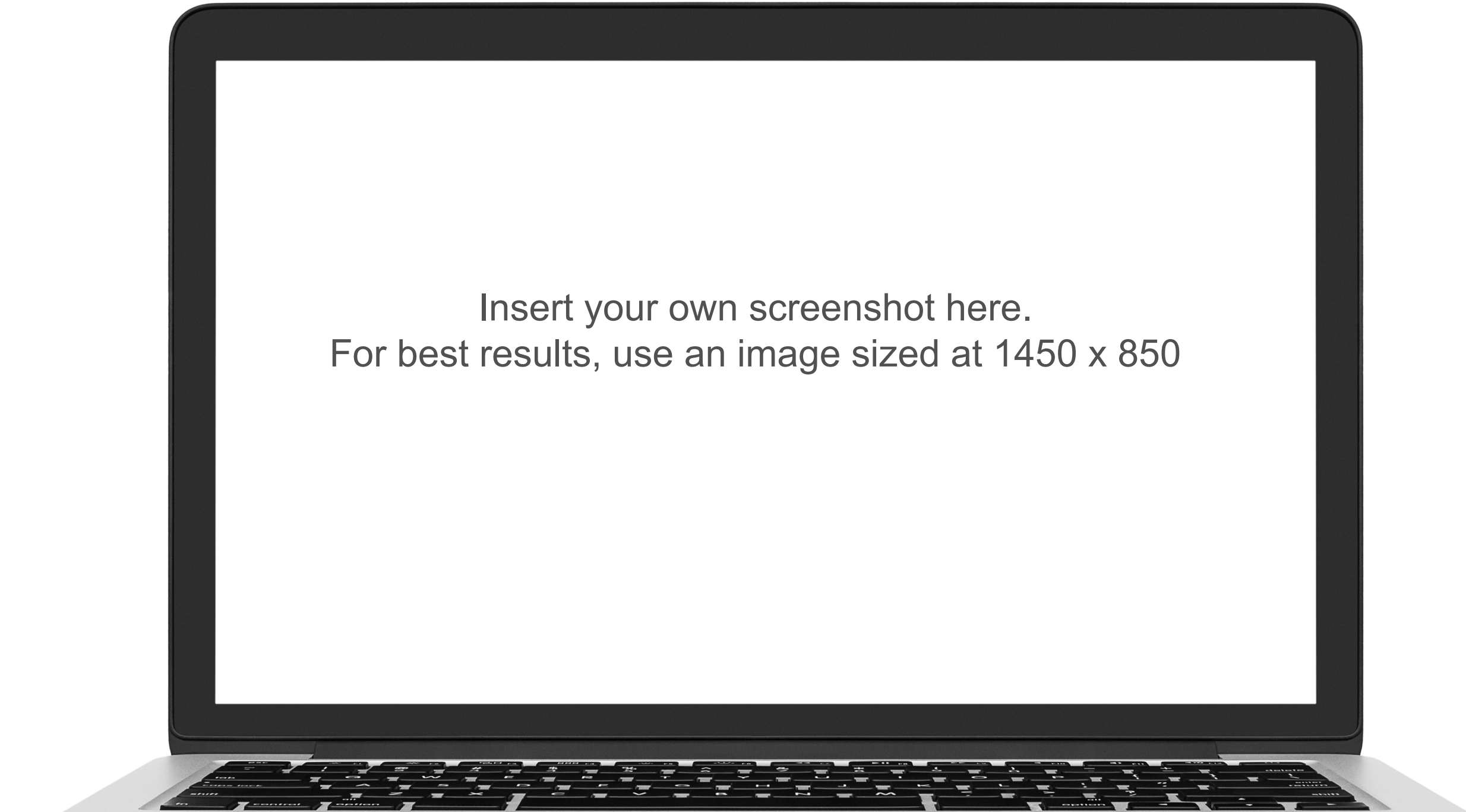
You see servers and devices, apps and logs, traffic and clouds. We see data—everywhere. Splunk® offers the leading platform for Operational Intelligence. It enables the curious to look closely at what others ignore—machine data—and find what others never see: insights that can help make your company more productive, profitable, competitive and secure. What can you do with Splunk?

Just ask.

Screenshot and Title

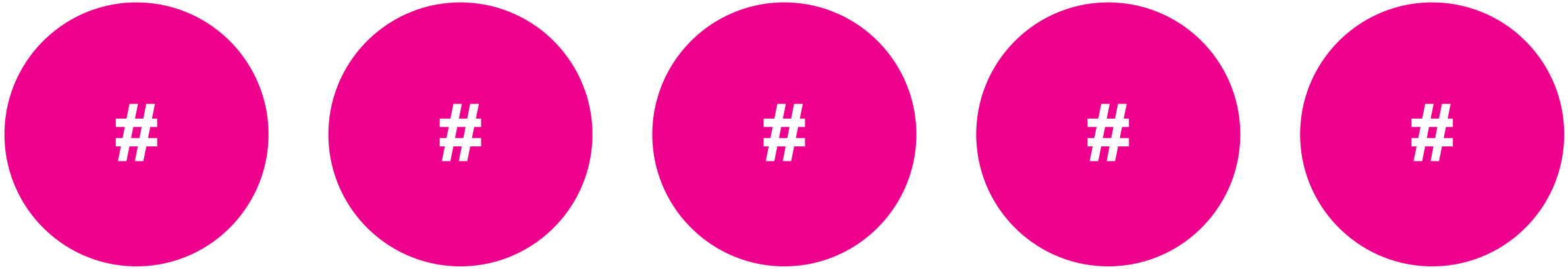
This is where the subtitle goes





Big Stats and Supporting Text

This is where the subtitle goes



This layout is used for large statistics

If you have fewer than five stats to display

Simply click on the extra circles and text boxes

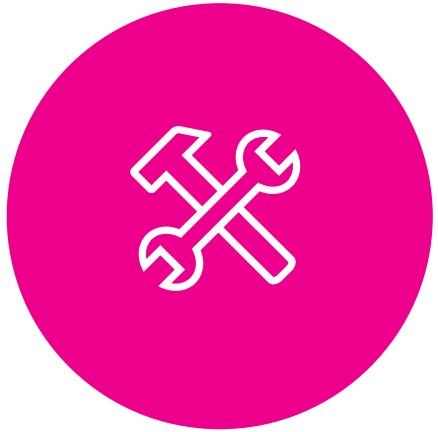
Choose delete

Delete one more time to remove the placeholders

Three Icons with Supporting Text

This is where the subtitle goes

Title, 24pt



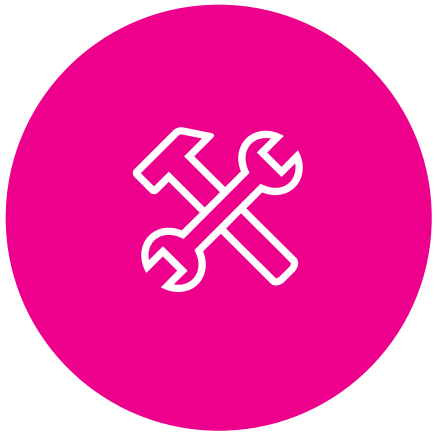
Title, 24pt

Title, 24pt

Four Icons with Supporting Text

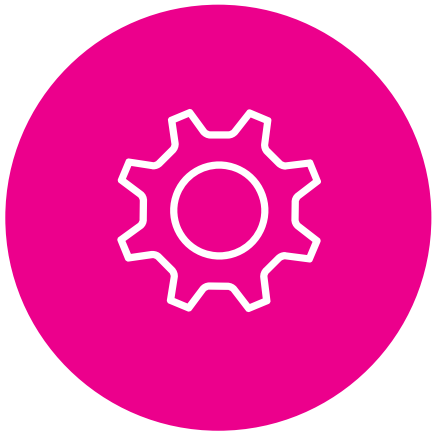
This is where the subtitle goes

Title, 24pt



Title, 24pt

Title, 24pt

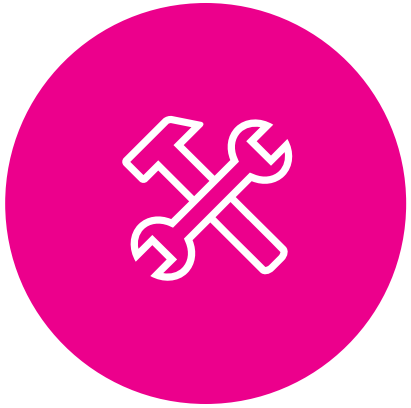


Title, 24pt

Five Icons with Supporting Text

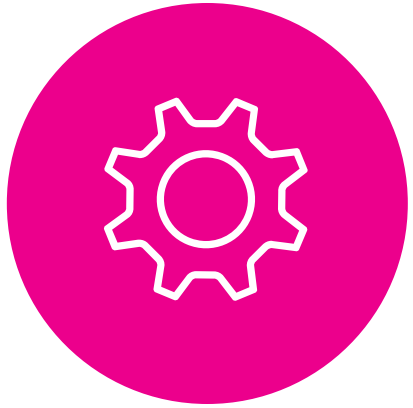
This is where the subtitle goes

Title, 24pt



Title, 24pt

Title, 24pt



Title, 24pt

Title, 24pt

Photo and Title in Circle

This is where the subtitle goes

Photo with Title and Bullets

This is where the subtitle goes

IT2001 - Monitoring and troubleshooting workloads running on public cloud infrastructure made easy

SCHEDULE Wednesday, October 23, 11:15 AM - 12:00 PM

Subu Baskaran, Product Manager, Splunk

Om Thoppai, Principal Software Engineer, Splunk

Monitoring and troubleshooting infrastructure running on multiple public cloud environments can be a daunting task. In this session, we will demonstrate how Splunk App for Infrastructure can help you bring Metrics, Logs and Cloud Native Events to monitor the health of your environment in near real-time, troubleshoot failing entities and gain complete control over your public cloud infrastructure.

Industries: Not industry specific

Products: Splunk Enterprise, Splunk Cloud

Photo with Content

This is where the subtitle goes

- First level bullets should be sentence case, 24pt
  - Second level bullets, 20pt
    - Third level bullets, 20pt
      - Fourth level bullets, 16pt

Making machine data accessible, usable and valuable to everyone.

splunk> .conf19

Key Takeaways

This is where the subtitle goes

1. First level bullets should be sentence case, 28pt
2. First level bullets should be sentence case, 28pt
3. First level bullets should be sentence case, 28pt

.conf19

splunk>

Thank You!

Demo

Q&A

Participant name | Role

Participant name | Role

.conf19

splunk>

Splunk Corporate Logo

Copy/paste these graphics to use in your own presentation

Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

splunk> .conf19

Splunk Corporate Logo

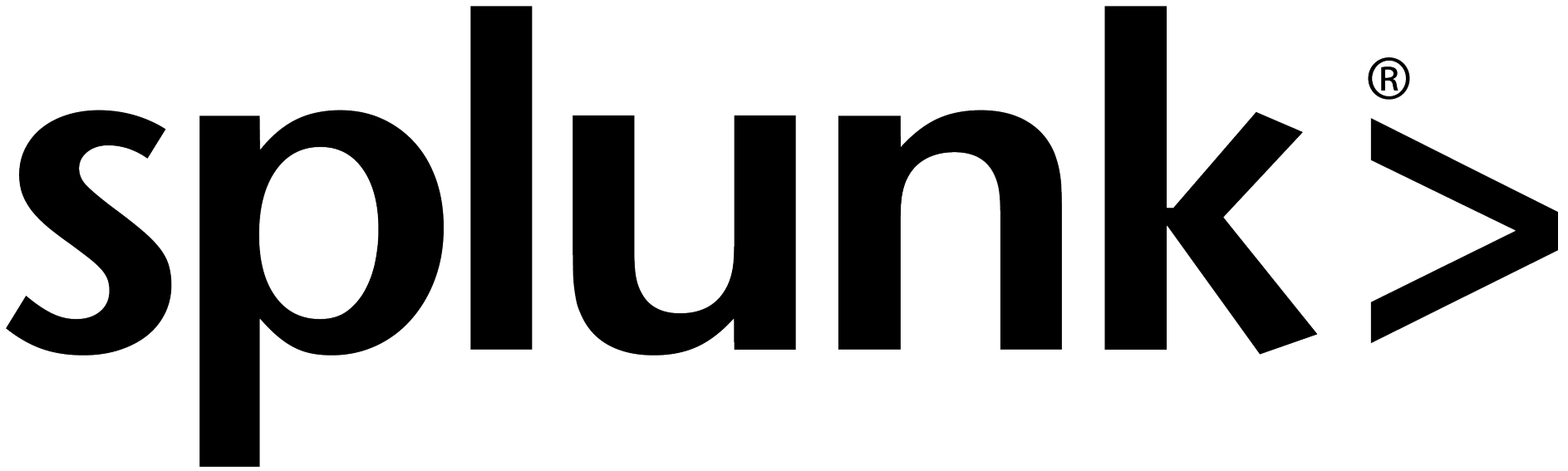
Copy/paste these graphics to use in your own presentation

Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

splunk> .conf19

Splunk Corporate Logo: One Color

Copy/paste these graphics to use in your own presentation



Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

splunk> .conf19

Splunk Corporate Logo: One Color

Copy/paste these graphics to use in your own presentation

Note: The Splunk corporate logo should be used whenever you are referencing Splunk as a company. When you're representing the product, use the product logo (with the green **>** symbol).

splunk> .conf19

Splunk Product Logo: Two Color

Copy/paste these graphics to use in your own presentation

Note: The Splunk product logo should be used whenever you are referencing the product or its capabilities.

Splunk Product Logo: Two Color

Copy/paste these graphics to use in your own presentation

Note: The Splunk product logo should be used whenever you are referencing the product or its capabilities.

splunk> .conf19

Premium Solutions Logos

Copy/paste these graphics to use in your own presentation

Splunk User Behavior Analytics™

Splunk User Behavior Analytics™

Splunk IT Service Intelligence™

Splunk IT Service Intelligence™

Splunk Enterprise Security™

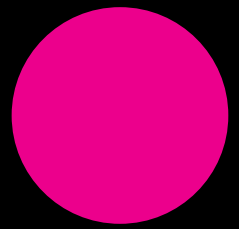
Splunk Enterprise Security™

Line and Shape Assets

Copy/paste these graphics to use in your own presentations

Dark background assets

Dark background overlay



Icon placeholder

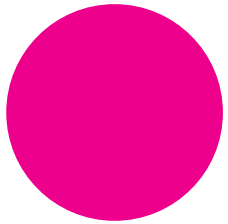
Green Line, 1pt, Cap type: Round

Gray 25% Line, 1pt, Cap type: Round

Gray 25% Line, 1pt, Cap type: Round

White background assets

White background overlay,
Gray 80%, Accent 3, Transparency 85%



Icon placeholder

Green Line, 1pt, Cap type: Round

Gray 25% Line, 1pt, Cap type: Round

Gray 25% Line, 1pt, Cap type: Round

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Custom Applications

OS

VM

APP OS


Applications


Energy Meters


Messaging


Databases


GPS Location


RFID


Call Detail Records


Web Services/Global


Security/ Lock


Telecoms


Web Clickstreams


Online Services


Desktop


Laptop


Online Shopping Cart


Cell Phones and Devices


Servers


Networks


Networks Alt


Storage


On-Premise


Public Cloud


Private Cloud


Internet of Things


Active Directory


Search


Advanced Search


Analyze


Document


Folder

Log Files


Envelope

Splunk Server Database

Splunk Server


Server


Virtual Server

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Servers

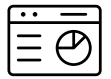

Hadoop Storage


Bar Chart


Pie Chart


Pie Chart Alt


Shipping Container


Enterprise Scale Platform

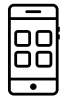

Gear


Gears / Setting

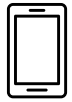

VoIP

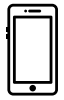

Script


Mobile App

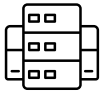

Mobile App Alt


Tag/Ticket


Galaxy Note


iPhone


Datacenter


Datacenters


iPad

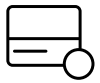

Blackberry


Check Mark


Indexer


Forwarder


Search Head


Blank Database


Forwarder Database


Forwarder AIX


Forwarder Free BSD


Forwarder Linux


Forwarder Windows


Forwarder Web


Forwarder OSX


Forwarder Solaris


Splunk Server AIX


Splunk Server Gearz


Splunk Server Linux


Splunk Server Network


Splunk Server Web


Splunk Server Free BSD


Splunk Server Windows

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Splunk Server Solaris


Splunk Server OSX


Splunk Server Search


Failed Splunk Server


Failed Server


Server License


Tools


Clock


RSS


Send Arrow


Android


Network Switch


Router


Cloud Services Monitoring


Telephone


Facebook


Facebook Color


Twitter


Twitter Color


LinkedIn


LinkedIn Color

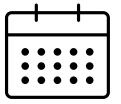

YouTube


YouTube Color


Healthcare


Info


Stop


Calendar

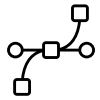

Alert

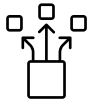

Hospital

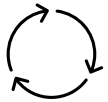

Office Building


Process Analytics


Universal Collection


Wire Data


Load Balancing


Cycle


Customer Support


Customer Support Alt


Male


Female


Stacked Document/ Documents

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


People


People Alt

Splunk People

Splunk Male

Splunk Female


Meter


Signature Capture


POS Card Reader


EMV Card Reader


Factory


Electric Car


Shield


Footsteps


Malware Document


Malware

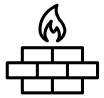

Malware Packaged


Security Server


Security Badge


Virus


Key


Firewall


Botnet

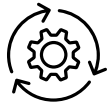

Attacker General


Attacker Insider

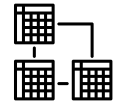

Attacker Nation/State


Real Time Monitoring


Detect Unknown Threats


Asset Lifecycle Management


Instant Pivot


Data Model


Fraud Detection


Product Analytics/ Custom Dashboard


Host/ Activity/Security


Operational Efficiency


Shield Revised


Waste Reduction


Monitoring


Environmental and Industrial


House


Innovate

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Mission Operations


Facilities and Assets


Warfighter


Vehicle Fleet


Vehicle Fleet Cloud


Share with Mission Partners


Collaboration


Data Management


Device Usage Analytics

DHCP/DNS

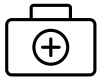

Disaster Relief


Campus Experience

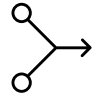

Learning Management System


Machine learning


Learning Management


Emergency Management

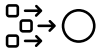

Shared Services

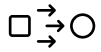

Consolidation

Grades


Admissions


Admissions and Registratio


Consolidation and Modernization


Consolidation and Modernization


Situational Awareness


Infrastructure


Public Services


IT Infrastructure

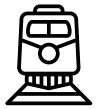

Campus Housing


Connected Campus + Smart Campus


Control Fraud Waste and Abuse


Dispatch Systems


Subway


Locomotive

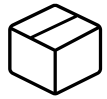

Energy


Water


Vulnerability Scans


Transportation


Threat Intelligence


Package


Business Analytics

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Badge/Pass


Tailored


Hourglass


Predictive Analytics


Satellite


Intrusion Prevention


Application Management


DevOps/ Application Deployment


IT Operations


Adaptive Response


Automation or Operational Efficiency


Preventative Maintenance


Splunk Enterprise License


Aviation

New Developer Resources


Data Prep & Analysis


Filter Results

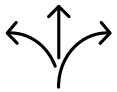

Parallel Processing


Scalable

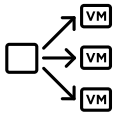

Kiosk


Value Assurance


Trading Systems


Flexible


Platform



Hypervisor


Heart


Patient Generated Data


Healthcare App


CMDB


Service Monitoring


Cost Savings


Education

Threat PDF Stealing

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations

Custom Applications

OS

VM

APP OS


Applications


Energy Meters


Messaging


Databases


GPS Location


RFID


Call Detail Records


Web Services/Global


Security/ Lock


Telecoms


Web Clickstreams


Online Services


Desktop


Laptop


Online Shopping Cart


Cell Phones and Devices


Servers


Networks


Networks Alt


Storage


On-Premise


Public Cloud


Private Cloud


Internet of Things


Active Directory


Search


Advanced Search


Analyze


Document


Folder

Log Files


Envelope

Splunk Server Database

Splunk Server


Server


Virtual Server

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Servers


Hadoop Storage


Bar Chart


Pie Chart


Pie Chart Alt


Shipping Container


Enterprise Scale Platform


Gear


Gears / Setting


VoIP


Script


Mobile App


Mobile App Alt


Tag/Ticket


Galaxy Note


iPhone


Datacenter


Datacenters


iPad


Blackberry


Check Mark


Indexer


Forwarder


Search Head


Blank Database


Forwarder Database


Forwarder AIX


Forwarder Free BSD


Forwarder Linux


Forwarder Windows


Forwarder Web


Forwarder OSX


Forwarder Solaris


Splunk Server AIX


Splunk Server Gearz


Splunk Server Linux


Splunk Server Network


Splunk Server Web


Splunk Server Free BSD


Splunk Server Windows

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Splunk Server Solaris


Splunk Server OSX


Splunk Server Search


Failed Splunk Server


Failed Server


Server License


Tools


Clock


RSS


Send Arrow


Android


Network Switch


Router


Cloud Services Monitoring


Telephone


Facebook


Facebook Color


Twitter


Twitter Color


LinkedIn


LinkedIn Color


YouTube


YouTube Color


Healthcare


Info

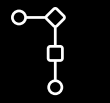

Stop


Calendar

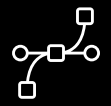

Alert

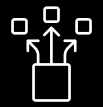

Hospital


Office Building


Process Analytics


Universal Collection


Wire Data


Load Balancing


Cycle


Customer Support


Customer Support Alt


Male


Female


Stacked Document/ Documents

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


People


People Alt

Splunk People

Splunk Male

Splunk Female


Meter


Signature Capture


POS Card Reader


EMV Card Reader


Factory


Electric Car


Shield


Footsteps


Malware Document


Malware


Malware Packaged


Security Server


Security Badge


Virus


Key


Firewall


Botnet


Attacker General


Attacker Insider

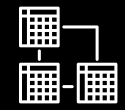

Attacker Nation/State


Real Time Monitoring


Detect Unknown Threats


Asset Lifecycle Management


Instant Pivot


Data Model


Fraud Detection


Product Analytics/ Custom Dashboard


Host/ Activity/Security


Operational Efficiency


Shield Revised


Waste Reduction


Monitoring


Environmental and Industrial


House


Innovate

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Mission Operations


Facilities and Assets


Warfighter


Vehicle Fleet


Vehicle Fleet Cloud


Share with Mission Partners


Collaboration


Data Management


Device Usage Analytics

DHCP/DNS


Disaster Relief


Campus Experience

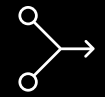

Learning Management System


Machine learning


Learning Management


Emergency Management

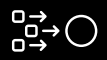

Shared Services

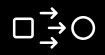

Consolidation

Grades


Admissions


Admissions and Registration


Consolidation and Modernization


Consolidation and Modernization


Situational Awareness


Infrastructure


Public Services


IT Infrastructure


Campus Housing


Connected Campus + Smart Campus


Control Fraud Waste and Abuse


Dispatch Systems


Subway


Locomotive


Energy


Water


Vulnerability Scans


Transportation


Threat Intelligence


Package


Business Analytics

splunk> .conf19

Splunk Marketing Icons

Copy/paste these graphics to use in your own presentations


Badge/Pass


Tailored


Hourglass


Predictive Analytics


Satellite


Intrusion Prevention


Application Management


DevOps/ Application Deployment


IT Operations


Adaptive Response


Automation or Operational Efficiency


Preventative Maintenance


Splunk Enterprise License


Aviation

New Developer Resources


Data Prep & Analysis


Filter Results


Parallel Processing


Scalable

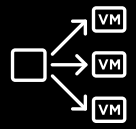

Kiosk


Value Assurance


Trading Systems


Flexible


Platform



Hypervisor


Heart


Patient Generated Data


Healthcare App


CMDB


Service Monitoring


Cost Savings


Education

Threat PDF Stealing

splunk> .conf19

1

How to Use This Presentation Template

.conf19

splunk>

Install PowerPoint 2016

Please upgrade now if you are using a previous version of PowerPoint.

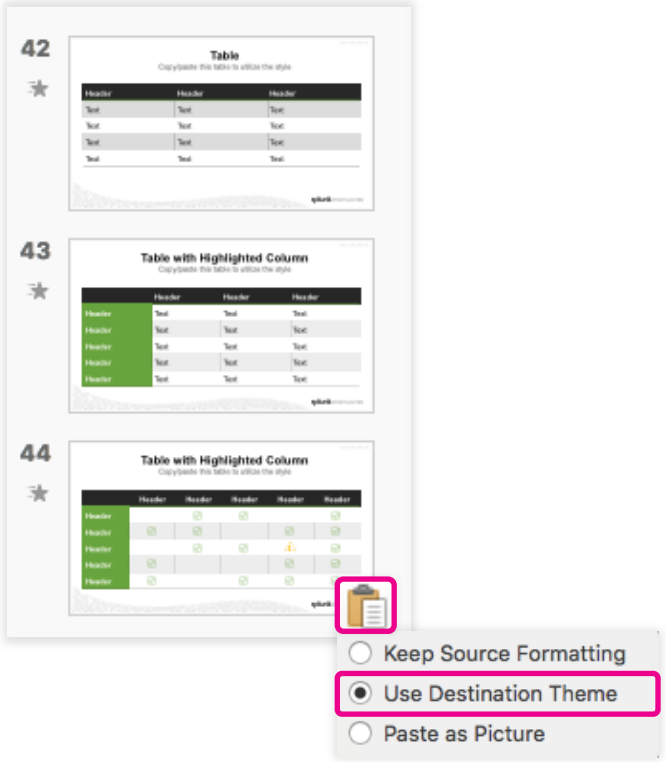
- Go to portal.office.com
- Log in with your Okta credentials
- Follow the instructions to install Office 2016

Note: This template is optimized for PowerPoint 2016, and the Splunk Brand Team does not support previous versions of PowerPoint.

Importing Slides into the New Template

From the normal view in PowerPoint, you will have a visual list of slides on the left of your slide space. You can use this space or the Slide Sorter view to copy and paste old slides into a presentation that uses the new template.

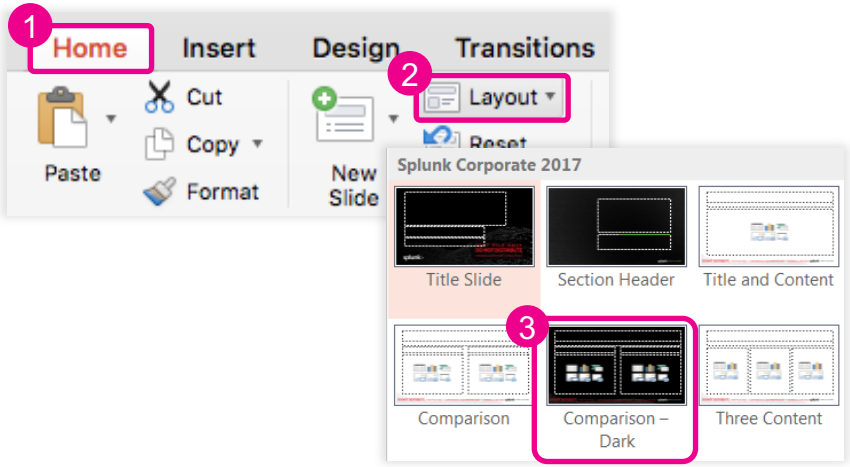
- The paste options clipboard icon will appear on the last slide you copied with three choices:
  - Keep Source Formatting
  - Use Destination Theme
  - Paste as Picture
- Choose Use Destination Theme
  - There may be color shift if the color palettes of the two files vary
  - Some slide objects may need adjusting of colors



Applying and Resetting Slide Layouts

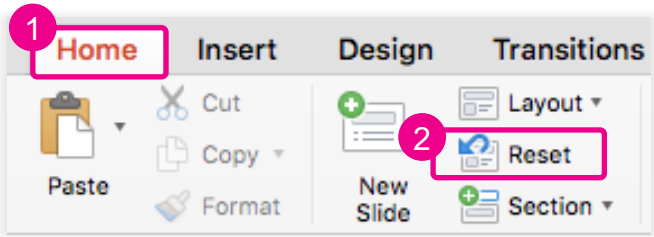
Applying a Slide Layout

- With a slide selected, click on the Home tab
- Select the dropdown Layout button
- Choose the layout that is most appropriate for the content



Resetting a Slide Layout

- With a slide selected, click on the Home tab
- Select the Reset button to update layout style details such as text size, spacing, and color



Note: Resetting your slide layout can help resolve Wonky Slide Syndrome.

2

Working with the Color Palette

.conf19

splunk>

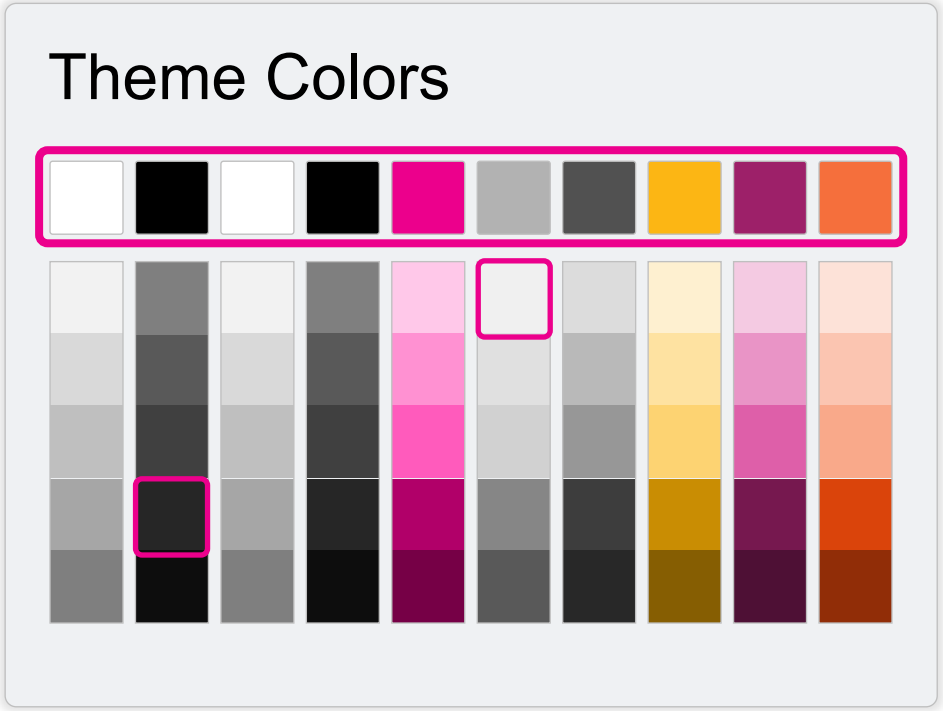
Using The PowerPoint Template Colors

Changing text color

- With text selected, choose the Home tab
- Under the Font section, click on the Font Color button
- Select the box with the color you wish to apply

Changing object color

- Object selected, choose the Shape Format Tab then click Shape Fill
- Select the box with the color you wish to apply



Note: When selecting colors from the color palette, only use the colors from the top row. The exception to that rule is when we use the gray chips for text and line use.

3
Working with Images

.conf19
splunk>

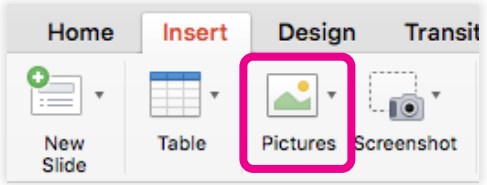
Inserting Images

Into an empty placeholder:

- Click the picture placeholder
- Navigate to the image and select it
  - PowerPoint will automatically fill the height (vertical image) or width (horizontal image) of the placeholder with the entire picture

Directly onto a slide:

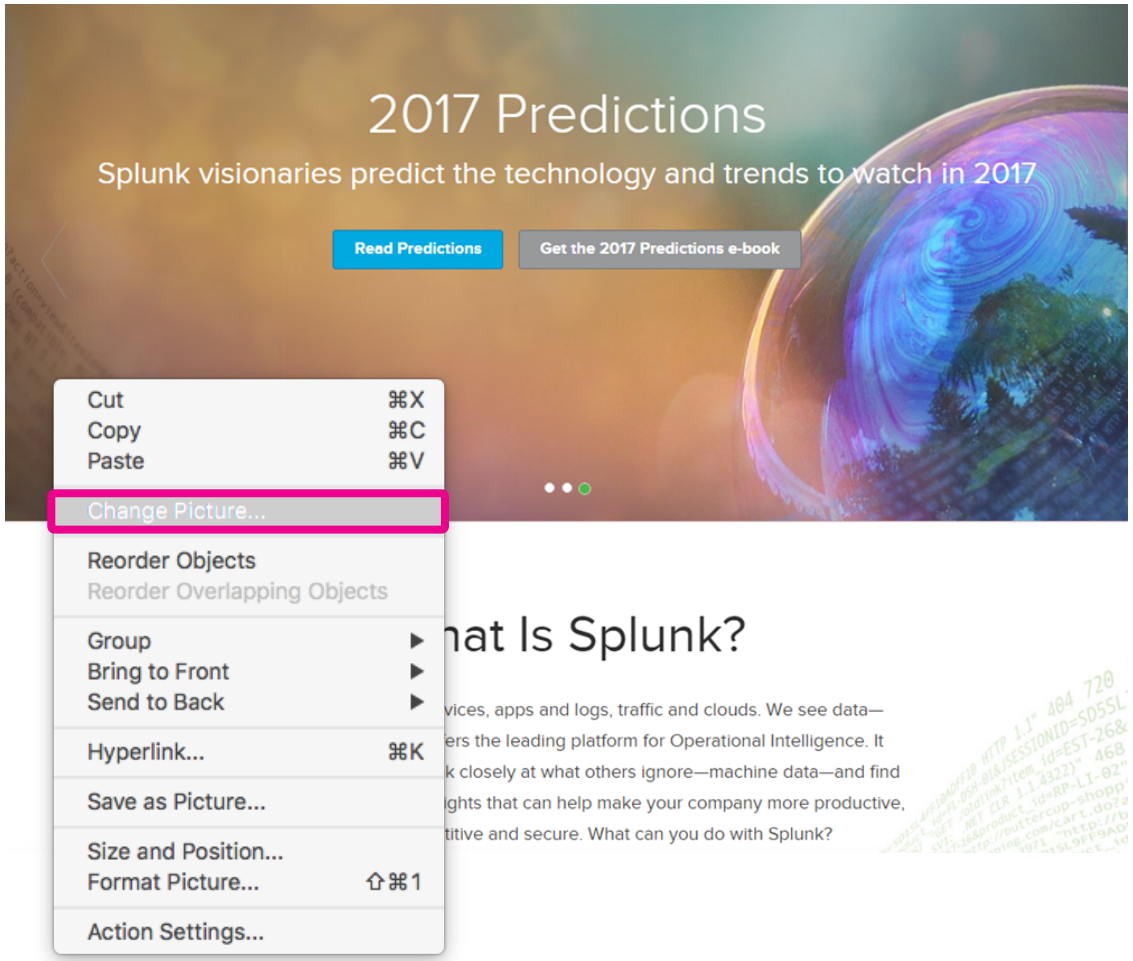
- On the Insert tab, click the Pictures button
- Navigate to the image you would like to use and select Insert



Note: If the image is larger than the slide, (1280x720px,) PowerPoint will resize it to the maximum width or height possible to get the entire image on the slide. To keep file size down, only insert images that are at maximum sized to the width or height of a slide.

Changing an Existing Image

- Right click on an image
- Choose, Change Picture
  - Note, new image will fit the height or width of the old photo
  - Some cropping adjustments may be needed



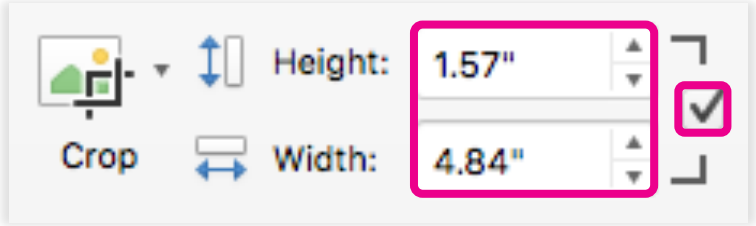
Resizing Images

Dragging to resize an image:

- Select the image you want to resize
- Hold the Shift key to keep the proportions of the image
- Click and drag a corner of the image

To precisely resize an image:

- Select the image you want to resize
- Go to the Picture Format tab
- At the far right, enter the new size, or use the arrow buttons to the right of the size
- The check mark ensures the proportions stay true to the original



Cropping Images

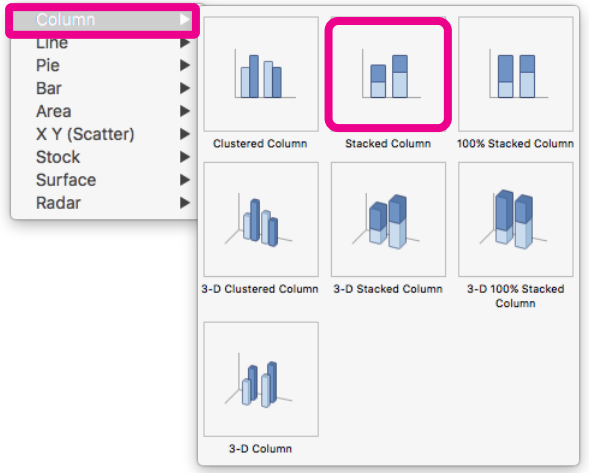
- Select the image you want to crop
- Select the Picture Format tab
- Click the Crop button on the far right
- The picture cursors change to black handles
  - Click and drag the handles to hide parts of the image

4
Working with Charts

.conf19
splunk>

Building Charts

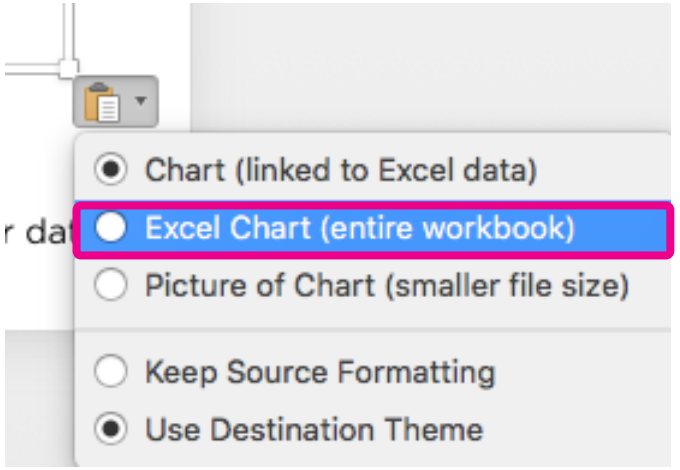
- From a blank slide with content placeholder, click the chart icon placeholder
- Select a chart type and choose a chart
- Add data into the Excel spreadsheet that opens, or copy and paste data from another spreadsheet
  - The small blue bracket indicates what data will be used for the chart
  - It will expand as you fill data into the cells
- Close the Excel file when done entering or copying data



	A	B	C
1		Sales	
2	1st Qtr	8.2	
3	2nd Qtr	3.2	
4	3rd Qtr	1.4	
5	4th Qtr	1.2	
6			
7			

Importing Charts from Other Sources

- Copy the chart from the originating document
- In the new presentation choose the Title and Content layout, then select the content placeholder on the slide
- Paste the chart into the placeholder
  - The paste options clipboard icon will appear on the bottom right of the chart, with various options*
  - If copying directly from Excel, choose Excel Chart (entire workbook) to embed the chart for best results



***Note:** Options will differ depending on the type of document used for the source (ppt, xlsx, etc.)

Updating a Chart to Match the Template Theme

If a chart's formatting doesn't appear to match the template style, try resetting it

- With the chart selected, click on the Format tab
- Choose the Reset to Match Style button

There are additional style options under the Chart Design tab

- Style 1 is the recommended formatting in most cases

5

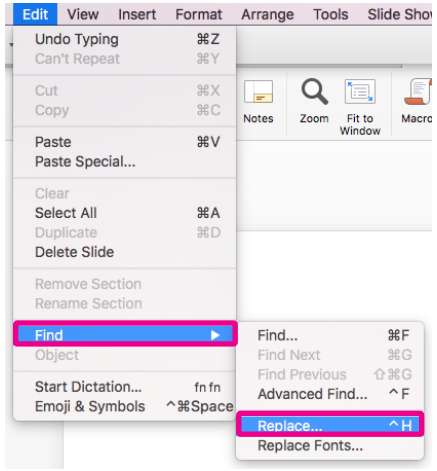
Tips and Tricks

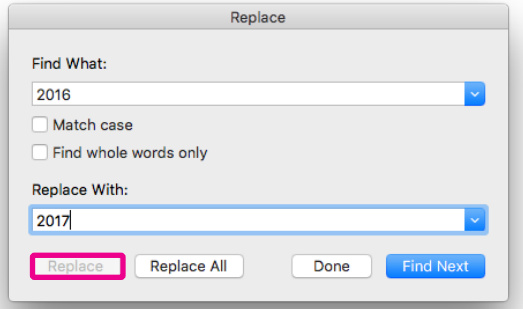
.conf19

splunk>

Using Find and Replace

- Choose Edit, Find, Replace or use the key command Ctrl + H
- Type text that should be changed in the Find what field
- Type the new text in the Replace with field
- Click the Replace button to make the replacements one at a time or click Replace All to replace everything at once





Note: Use caution when replacing content with the **Replace All** command. It will change content in your entire presentation (dates, numbers, words, etc.), not just the slide or master you happen to be on in that moment.

Checking for Quality

- Use spell check (Review/Spelling) to ensure that all words are spelled correctly
- Read your slides out of order (ex., start at the back) which causes reading to be more focused
- Check the flow of the presentation in the Slide Sorter view
- Run through the presentation in Slide Show view
- Check animations, alignments, and transition consistency
- Check that images are placed properly and that text is legible
- If possible run the presentation through the medium that you will be using (online, overhead, print, etc.)

PowerPoint Shortcuts

Function	OS X	Windows
Select all	Cmd + A	Ctrl + A
Cut	Cmd+ X	Ctrl + X
Copy	Cmd + C	Ctrl + C
Paste	Cmd + V	Ctrl + V
Duplicate	Cmd+ D	Ctrl + D
Insert new slide	Cmd + Shift + N	Ctrl + Shift + M
New presentation	Cmd + N	Ctrl + N
Save	Cmd + S	Ctrl + S
Save as	Cmd + Shift + S	Ctrl + Shift + S
Undo last change	Cmd + Z	Ctrl + Z

Tips for Reducing File Size

- Eliminate unnecessary graphics and slides
- Compress images and delete cropped areas of images
  - Use document resolution for optimum quality
  - Compress one image at a time, not the entire presentation, so that if compression is too low on any one image, you can adjust the level of compression on that image
- Create basic shapes in PowerPoint instead of importing images of shapes
- Import images at the exact size they will be displayed
- Build charts from the template, or paste charts in as single Excel worksheets (i.e., no extra data / worksheets in the document)
- Delete rogue masters and layouts
- Use Save As to delete information retained in the file from fast saves

6
Rules for Creating Great Presentations

.conf19
splunk>

Treat Your Audience As King

Takeaways for creating great presentations

1. Design with a clear, concise message to better capture your audience

2. Your audience should walk away with an understanding of your message and how it affects them

Spread Ideas and Move People

Takeaways for creating great presentations

1. Convey meaning and be inspirational with your message when possible
2. Use powerful imagery to support your point
3. Use animation to support your message, not just to entertain the audience

Help Them See What You Are Saying

Takeaways for creating great presentations

1. Minimize text quantity; use meaningful visuals that support your topic

2. Brainstorm effective graphics prior to placement to be assured your image communicates well

Practice Design, Not Decoration

Takeaways for creating great presentations

1. Minimize any elements that are only causing noise on your slide
2. Feature only necessary key images or text highlights for easier consumption by your audience

Cultivate Healthy Relationships

Takeaways for creating great presentations

1. Use key images and text as visual cues for your dialogue
2. Put the bulk of your text into the speaker notes
3. Your slides should be supporting you, not driving the presentation
4. You are the focal point

.conf19

splunk>

Thank You!