

splunk> .conf2017

# Monitor And Manage Your Cloud Environment With Azure Monitor And Splunk

John Kemnetz | Program Manager, Microsoft Azure

Date | Washington, DC

# 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.

Splunk, Splunk>, Listen to Your Data, 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. © 2017 Splunk Inc. All rights reserved.

# Session Objectives

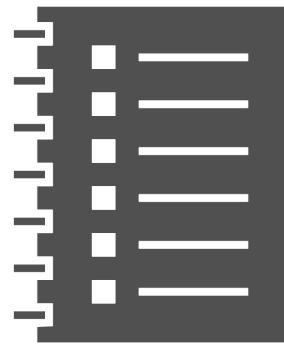
- ▶ Understand Azure's monitoring strategy, and how it embraces 3<sup>rd</sup> party tools like Splunk
- ▶ Learn how, as an existing Splunk customer, you can effectively manage your Azure environment with Splunk
- ▶ Learn how you can seamlessly move from on-premises or another cloud to Azure without needing to retrain your monitoring experts

# Key Monitoring Concepts In Azure

---

# Monitoring Data On Azure

## Three key types to know about



Logs



Metrics

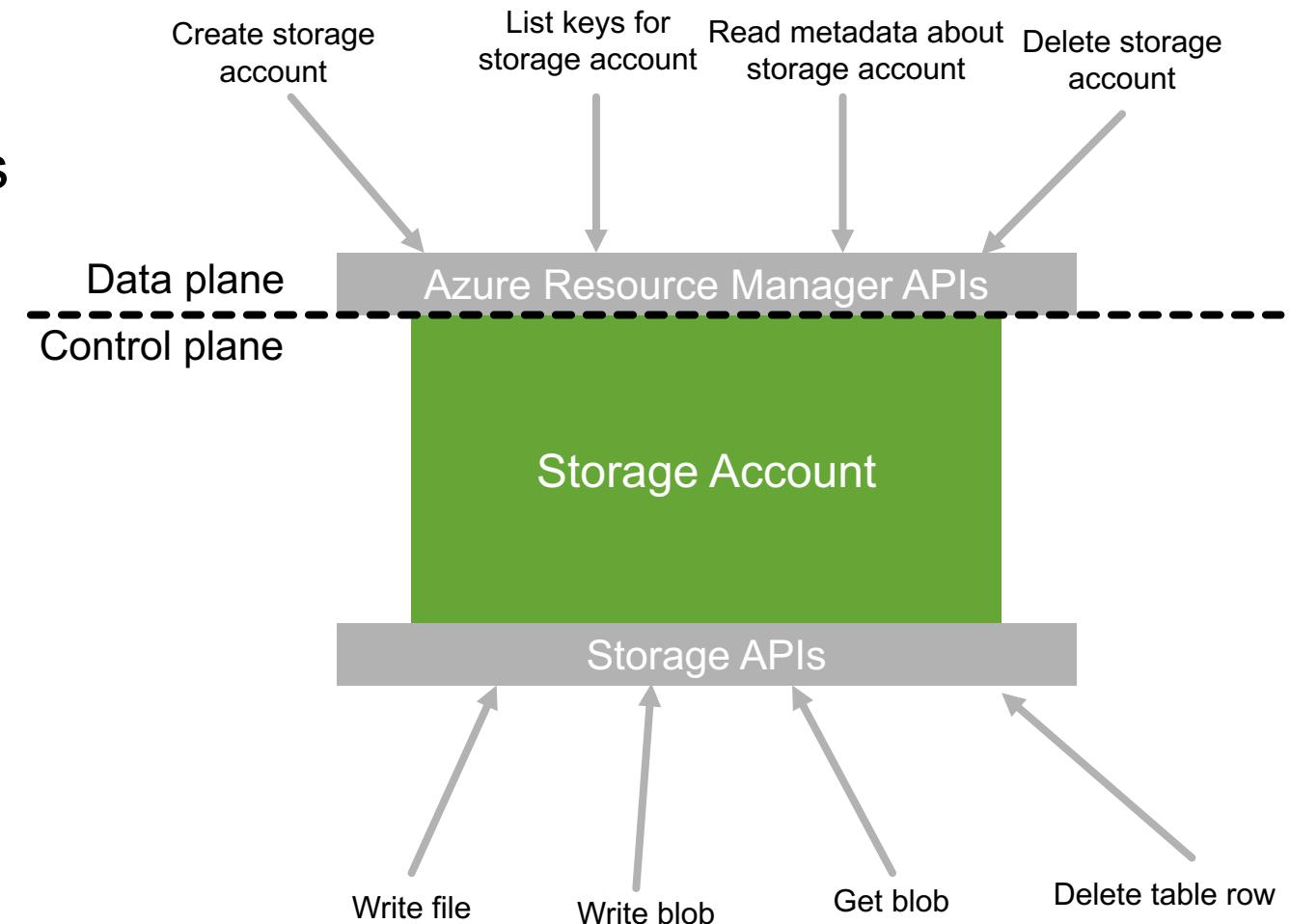


Health

```
130,60,4, - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=F1-SW-01", "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)", "/buttercup-shopping.com/cart.do?action=view&itemId=EST-26&product_id=F2-ZL11a/4", "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)", "[07/Jan 18:10:56:156]" "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&productId=AUTOCUP-SHOPPING.COM-01", "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36", "[07/Jan 18:10:57:123]" "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD59L4FF1ADFF7 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&JSESSIONID=SD10SLBFF2ADFF6 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&JSESSIONID=SD08SLAFFF1ADFF8 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&JSESSIONID=SD09SLAFFF1ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-23&JSESSIONID=SD13SLAFFF1ADFF0 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-22&JSESSIONID=SD12SLAFFF1ADFF1 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-19&JSESSIONID=SD11SLAFFF1ADFF2 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-17&JSESSIONID=SD10SLAFFF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-15&JSESSIONID=SD09SLAFFF1ADFF4 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-13&JSESSIONID=SD08SLAFFF1ADFF5 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-12&JSESSIONID=SD07SLAFFF1ADFF6 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14&JSESSIONID=SD06SLAFFF1ADFF7 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-16&JSESSIONID=SD05SLAFFF1ADFF8 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&JSESSIONID=SD04SLAFFF1ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-20&JSESSIONID=SD03SLAFFF1ADFF0 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-21&JSESSIONID=SD02SLAFFF1ADFF1 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-22&JSESSIONID=SD01SLAFFF1ADFF2 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-23&JSESSIONID=SD00SLAFFF1ADFF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-24&JSESSIONID=SD01SLAFFF1ADFF4 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-25&JSESSIONID=SD02SLAFFF1ADFF5 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&JSESSIONID=SD03SLAFFF1ADFF6 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-27&JSESSIONID=SD04SLAFFF1ADFF7 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-28&JSESSIONID=SD05SLAFFF1ADFF8 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-29&JSESSIONID=SD06SLAFFF1ADFF9 HTTP/1.1" 200 3865 
```

# Types Of Log Data

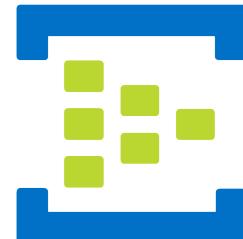
- ▶ **Control/management logs** – resource manager CRUD operations
- ▶ **Data plane logs** – events raised as part of using an Azure resource
- ▶ **Processed events** – analyzed events or alerts that have been processed on your behalf



# Accessing Monitoring Data

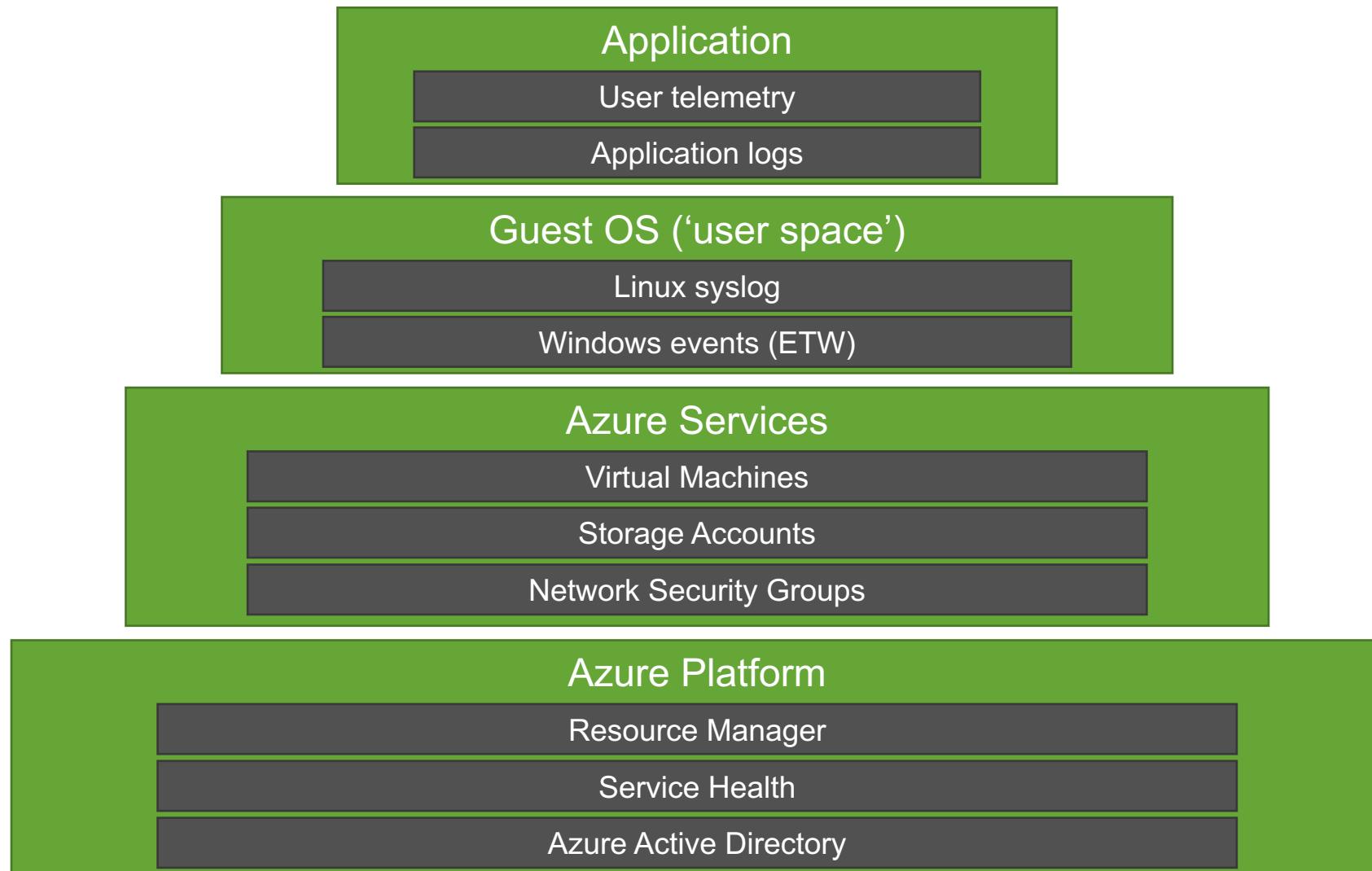
Depends on type of data, but methods include:

- ▶ Archive to storage accounts (blob, table)
  - ▶ Stream to event hubs (custom and 3<sup>rd</sup> party tools/SIEMs)
  - ▶ Route to Log Analytics (query, alerts, solutions)
  - ▶ Query via REST API



...more details to come

# Tiers Of Monitoring Data In Azure



# Tools Involved In Monitoring Azure

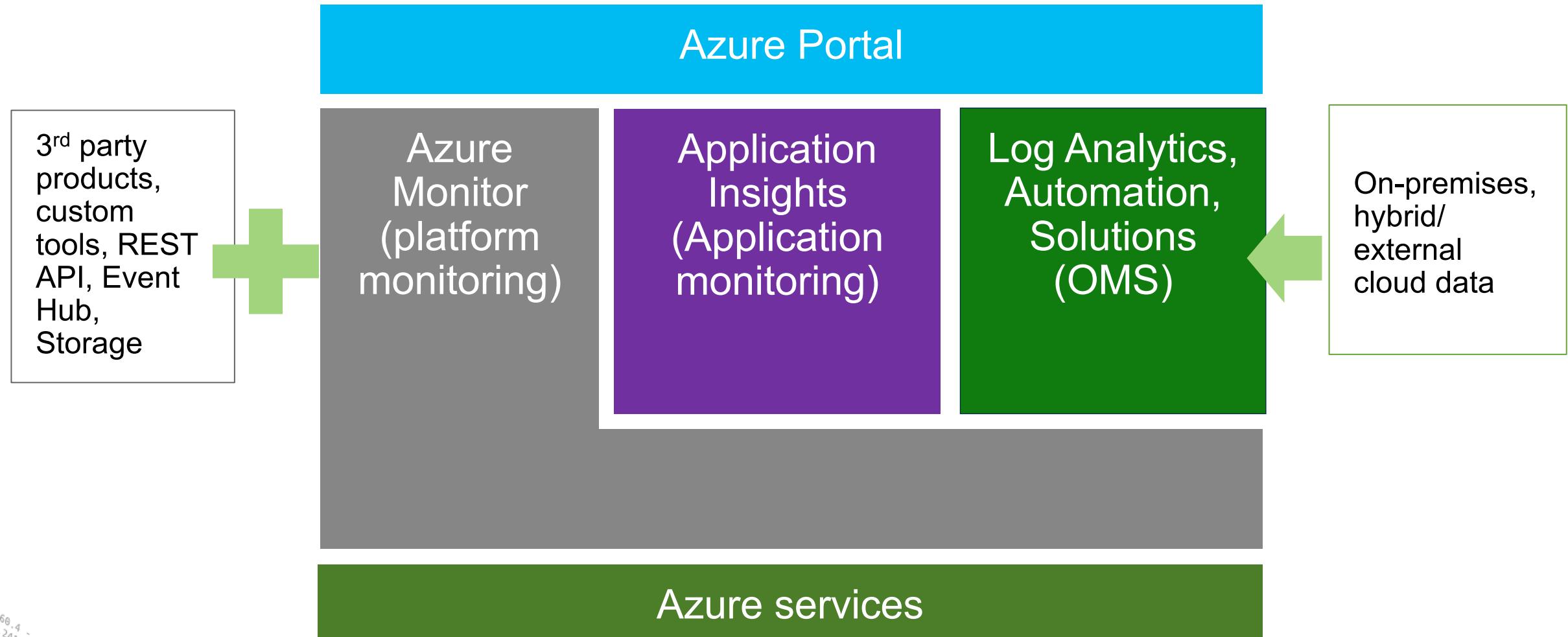
---

# Azure Services Involved In Consuming Log Data

- ▶ **Azure Monitor** – platform-level service for routing of logs
- ▶ **Log Analytics** – log search, alerting, and analysis (solutions) on top of data from Azure Monitor
- ▶ **Application Insights** – application-level logging and analysis
- ▶ **Network Watcher** – network performance monitoring
- ▶ **Storage Analytics** – collect logs and metrics for storage accounts

```
138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317 27.160.0.0 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=putInCart&itemId=EST-26&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317 27.160.0.0 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&productId=AU-CUP-SHOPPING SESSION.COM-01" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36" 317 27.160.0.0 - - [07/Jan 18:10:57:189] "GET /cart.do?action=changeQuantity&itemId=EST-18&productId=AU-CUP-SHOPPING SESSION.COM-01" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36" 317 27.160.0.0 - - [07/Jan 18:10:57:187] "GET /oldlink?item_id=EST-6&JSESSIONID=SD16SLBFF2ADFF7 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317 27.160.0.0 - - [07/Jan 18:10:57:108] "GET /category.screen?category_id=PR-01&JSESSIONID=SD08SLBFF1ADFFC HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317 27.160.0.0 - - [07/Jan 18:10:57:108] "GET /category.screen?category_id=PR-01&JSESSIONID=SD08SLBFF1ADFFC HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
```

# Interaction Of Monitoring Tools On Azure



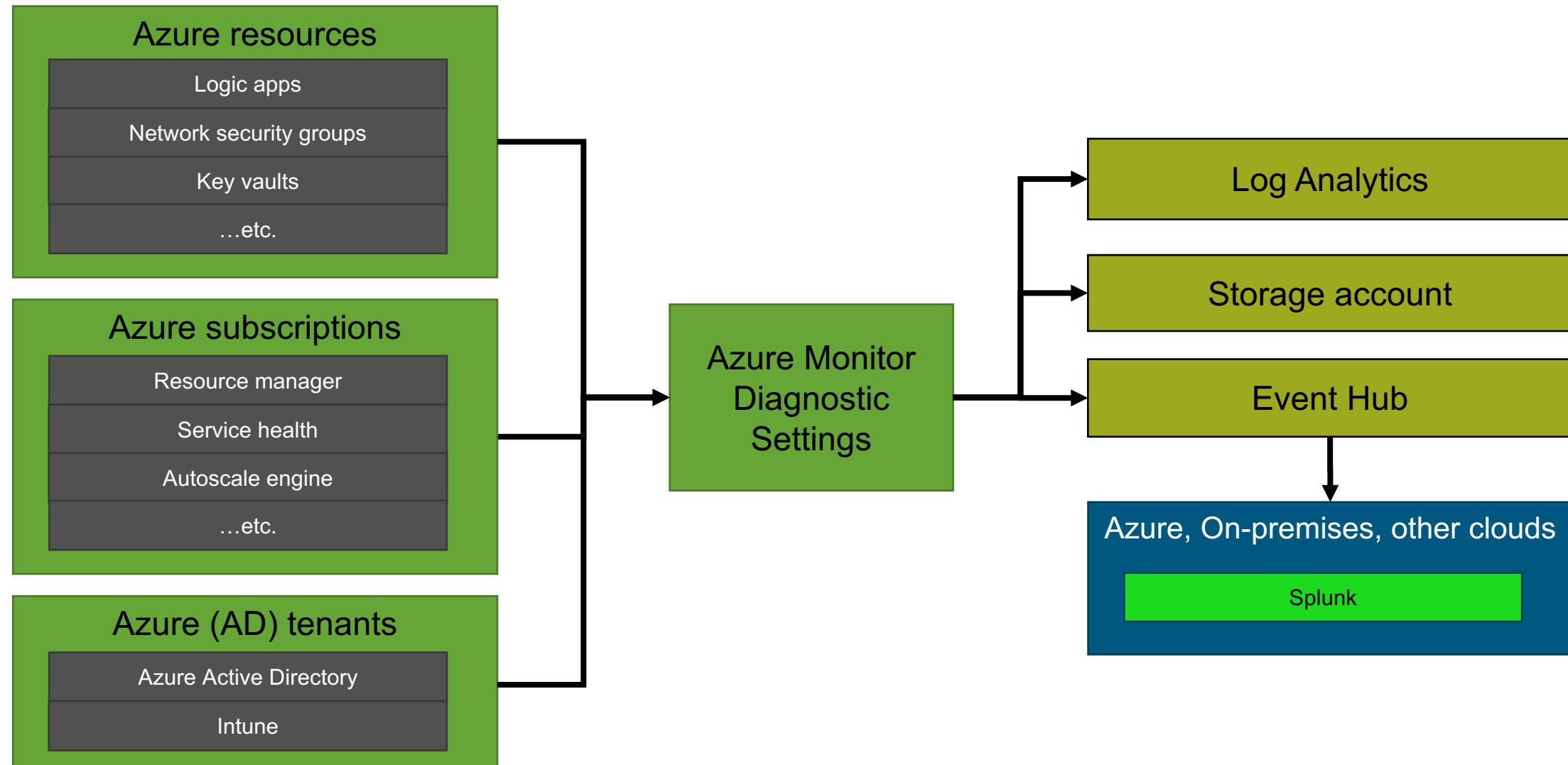
# Azure Monitor

Azure's platform monitoring service

- ▶ Built-in pipeline for all monitoring data coming out of Azure resources
- ▶ Out-of-the-box logs and metrics
- ▶ Alerts to get notified and take automated action
- ▶ Deep integration with Azure's advanced monitoring and analytics offerings
- ▶ **3<sup>rd</sup> Party integrations**

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFFF0 HTTP/1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFFF0 HTTP/1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-2&product_id=F2-ZL11&category_id=GIFTS&JSESSIONID=SD15LAFF10ADFFF0 HTTP/1.1" 200 423@ "http://buttercup-shopping.com/cart.do?action=updateSession&itemId=EST-18&product_id=AU-CUP-SESSION-CW-01" "Microsoft Internet Explorer/10.0 (Windows NT 5.1; Trident/6.0; .NET CLR 2.0.50727; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 4318@ "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&product_id=AU-CUP-SESSION-CW-01" "Microsoft Internet Explorer/10.0 (Windows NT 5.1; Trident/6.0; .NET CLR 2.0.50727; SV1; .NET CLR 1.1.4322)" 125.17.14.10 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLAFFF0 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=remove(itemId=EST-26)" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-LI-02&JSESSIONID=SD08SLAFFF0 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=remove(itemId=EST-26)" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLAFFF0 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=remove(itemId=EST-26)" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 125.17.14.10 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD08SLAFFF0 HTTP/1.1" 200 385@ "http://buttercup-shopping.com/cart.do?action=remove(itemId=EST-26)" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
```

# Azure Monitor And 3<sup>rd</sup> Party Tools

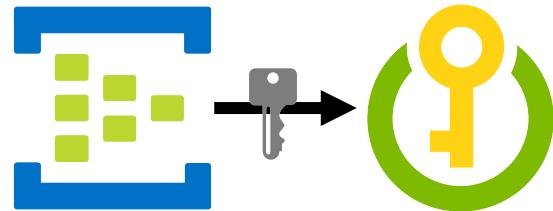


# Azure Monitor Add-On For Splunk

- ▶ Consumes metrics, activity log, and diagnostic logs
- ▶ Open source
- ▶ Easy to set up and configure
- ▶ Utilizes event hubs
- ▶ Extra security by storing keys in an Azure Key Vault

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_0&product\_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_26&product\_id=F1-ZL11&category\_id=GIFTS" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST\_26&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 4318@ "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST\_18&productId=AFC63818 SESSIONID=SD55L9FF1ADEF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST\_6&JSESSIONID=SD16SL8FF2ADEF9 HTTP/1.1" 200 2423@ "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST\_18&productId=AFC63818 SESSIONID=SD55L9FF1ADEF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:55:187] "GET /oldlink?item\_id=EST\_18&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 3865@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST\_26&productId=F1-ZL11&category\_id=GIFTS" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:55:188] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD55L9FF1ADEF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:55:188] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD55L9FF1ADEF3" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

# Configuring Splunk Add-On



**1. Create event hub & key vault to store event hub key**

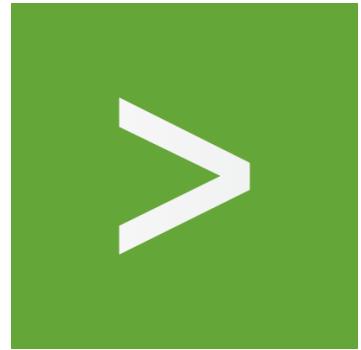


Activity log –  
log profile



Azure resource logs  
– diagnostic setting

**2. Set up routing**

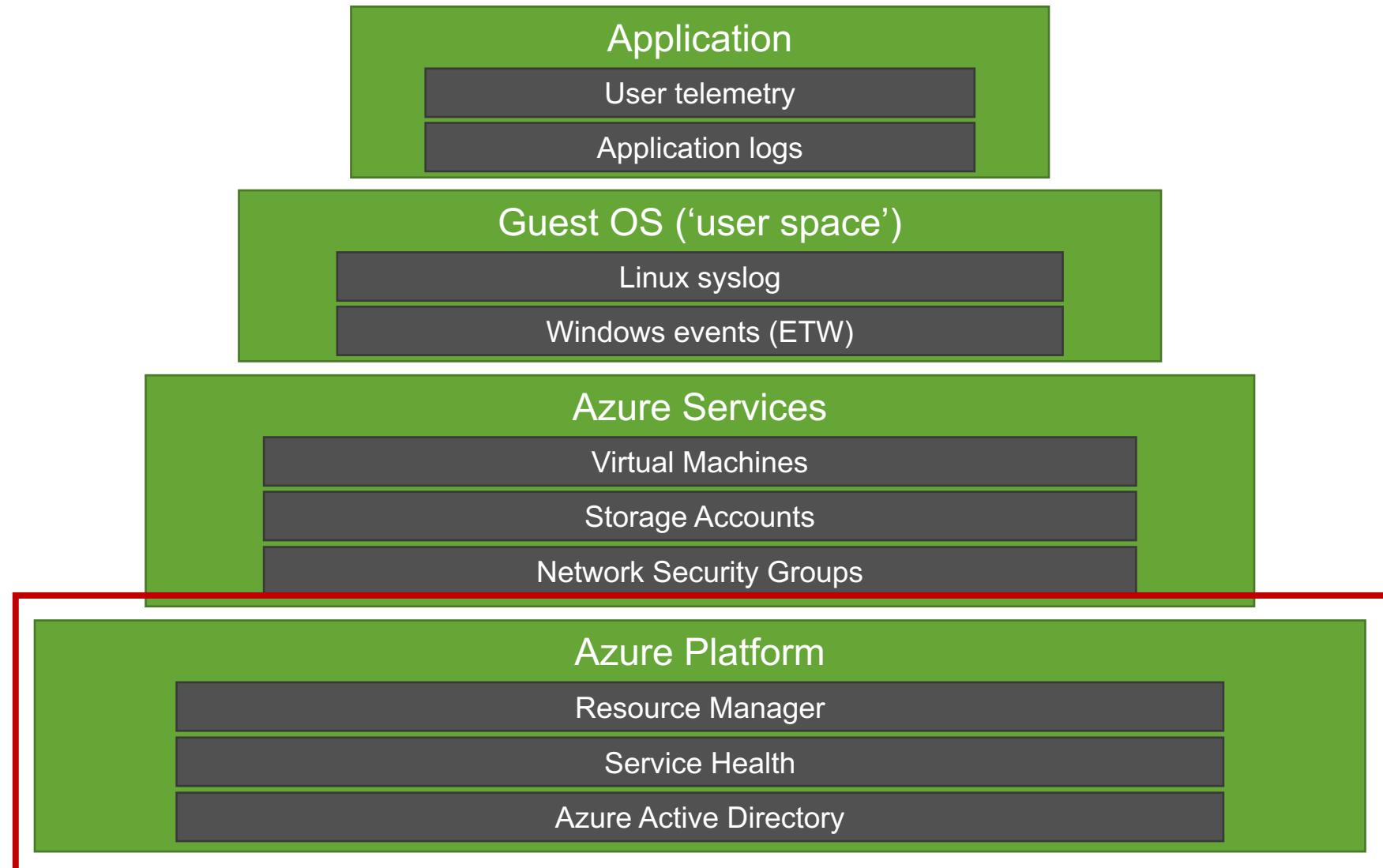


**3. Install Splunk Add-On & connect it to key vault**

# Working With Monitoring Data In Azure

---

# Tiers Of Monitoring Data In Azure



# Azure Platform-Level Logs

## ► Tenant level: Azure Active Directory

- Audit logs
- Sign in activities

## ► Subscription level: Azure Activity Log

- Categories: **Administrative**, **Service Health**, **Alerts**, **Autoscale**, Recommendation, (Security, and Policy)

## ► Subscription level: Azure Security Center

- Potential threats based on log correlation, including integrated threat intelligence, behavioral analytics, and anomaly detection

# Azure Activity Log – Key Categories

## ► Administrative

- “Audit” trail of all control plane operations in your subscription – who, what, where and when
- API calls to ARM: PUT, UPDATE, DELETE, Action
  - Time, caller (who), claims (JWT authentication token), operation details (action that was performed), resource impacted, [sometimes] HTTP request/response body, HTTP status code

## ► Service Health

- Azure platform outage and maintenance notifications including impacted services, impacted regions, RCA, incident information
- Five classes: Incident, Maintenance, Action required, assisted recovery, information, security

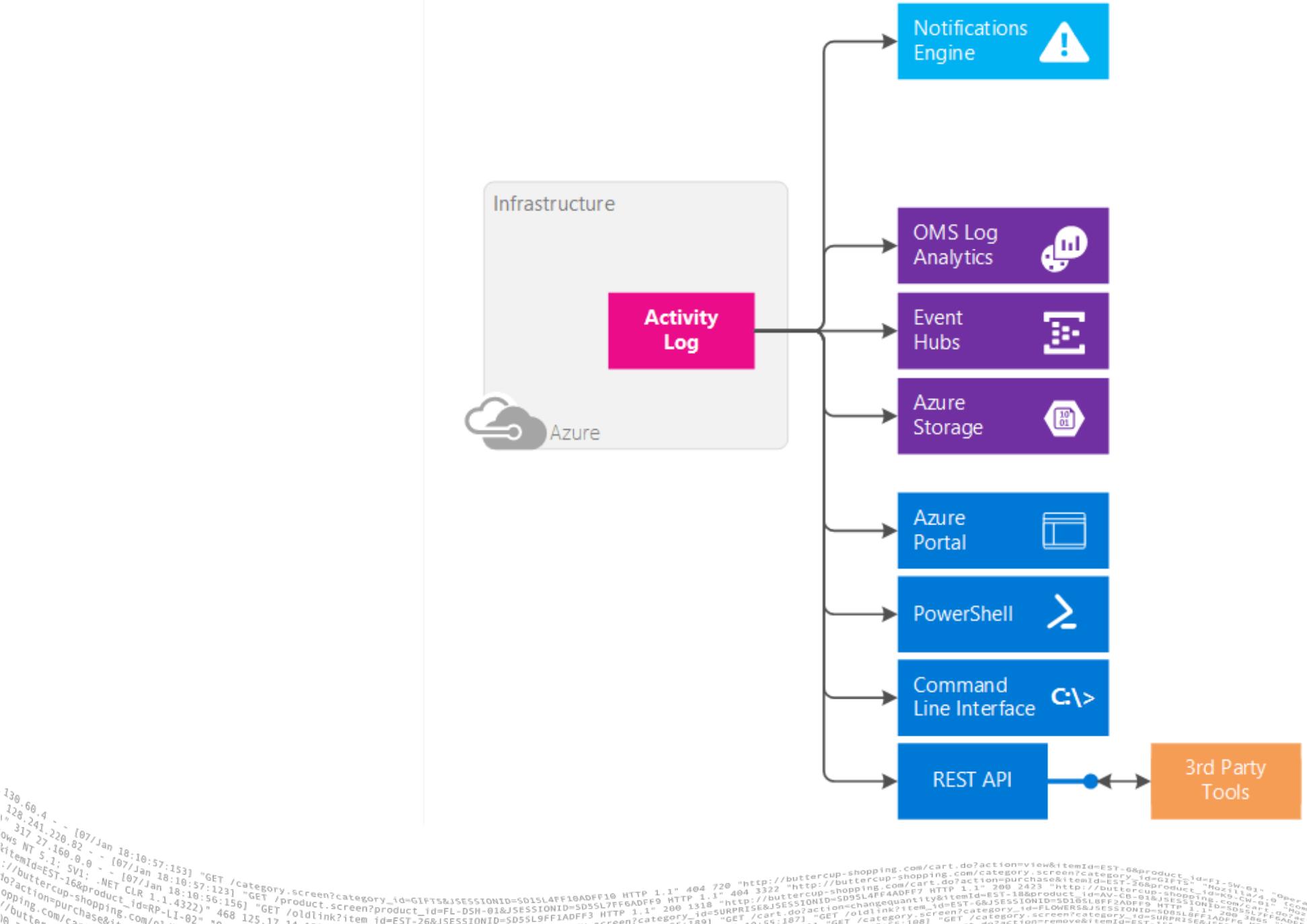
## ► Alert

- User-configured alert activations on metric alerts, Activity Log alerts, Application Insights alerts

# Demo

---

Accessing the Azure Activity Log



# Azure Activity Log

## Best Practices for Monitoring

### ► Security monitoring:

- Role assignments
- List keys

### ► Performance or health monitoring

- Deleting protected resources
- Identifying Service Health issues

### ► Change tracking

# Demo

---

Azure Activity Log in Splunk

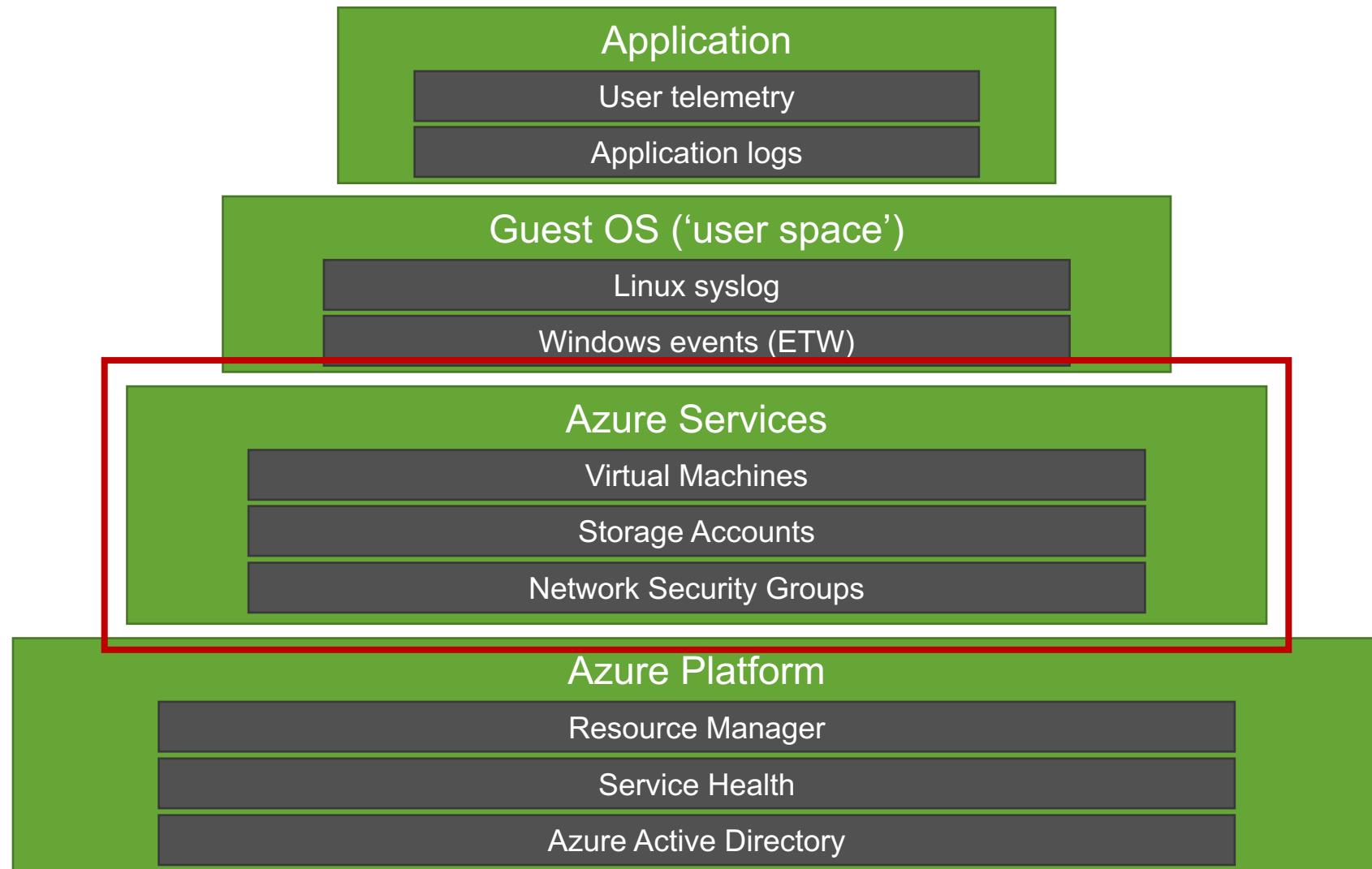


# Demo

---

Azure Active Directory Logs in Splunk

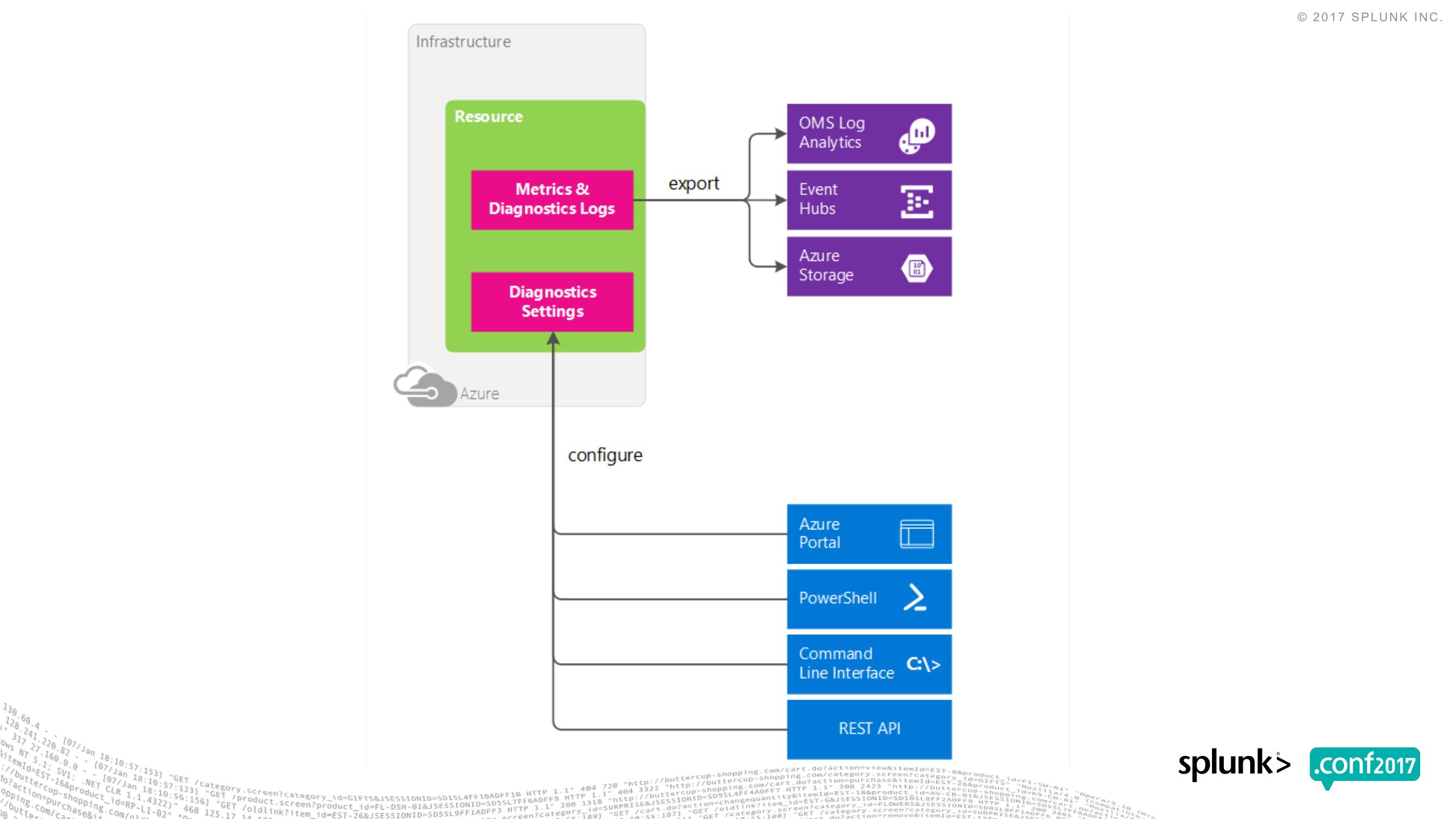
# Tiers Of Monitoring Data In Azure





# List Of Supported Resource Types

- ▶ API Management
- ▶ Application Gateways
- ▶ Azure Automation
- ▶ Azure Batch
- ▶ Customer Insights
- ▶ Content Delivery Network
- ▶ Data Lake Analytics
- ▶ Data Lake Store
- ▶ Event Hubs
- ▶ Key Vault
- ▶ Load Balancer
- ▶ Logic Apps
- ▶ Network Security Groups
- ▶ Recovery Services
- ▶ Search
- ▶ Server Management
- ▶ Service Bus
- ▶ Stream Analytics
- ▶ **Coming Soon:**
- ▶ SQL Databases – query store and diagnostics
- ▶ Cosmos DB
- ▶ IoT Hubs
- ▶ Traffic Manager
- ▶ Scheduler
- ▶ DB for PostgreSQL
- ▶ DB for MySQL



# Demo

---

Accessing the Azure Resource Diagnostic Logs

# Azure Resource Diagnostic Logs

## Best Practices for Monitoring

### ► Security monitoring:

- Audit data – Application Gateway, Automation, Batch, Data Lake Analytics, Data Lake Store, Event Hub, Key Vault, Service Bus, Stream Analytics

### ► Performance or health monitoring

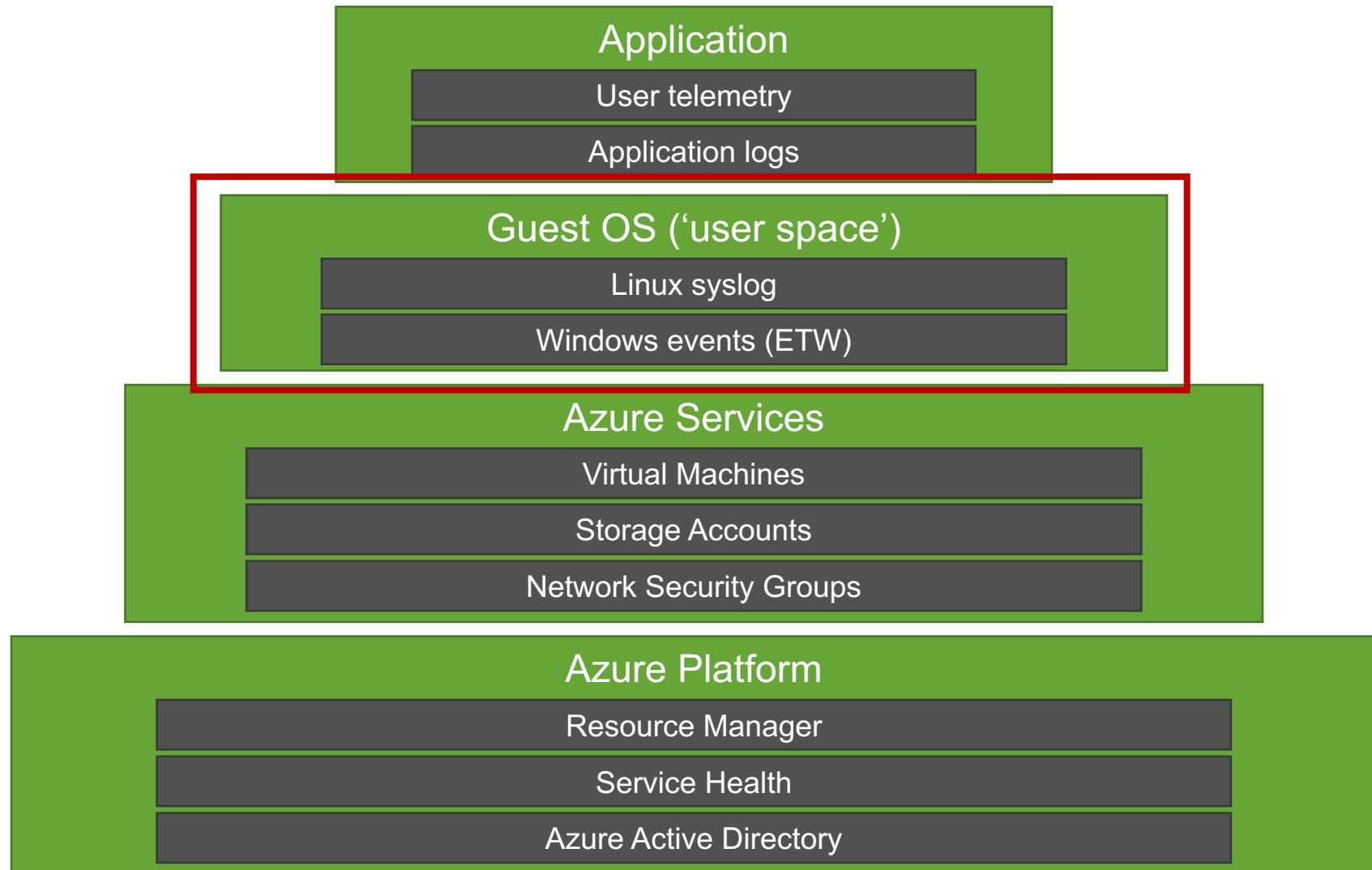
- Operational data – eg. Logic Apps
- Health alerts – eg. Load Balancer

# Demo

---

Azure Resource Diagnostic Logs in Splunk

# Tiers Of Monitoring Data In Azure

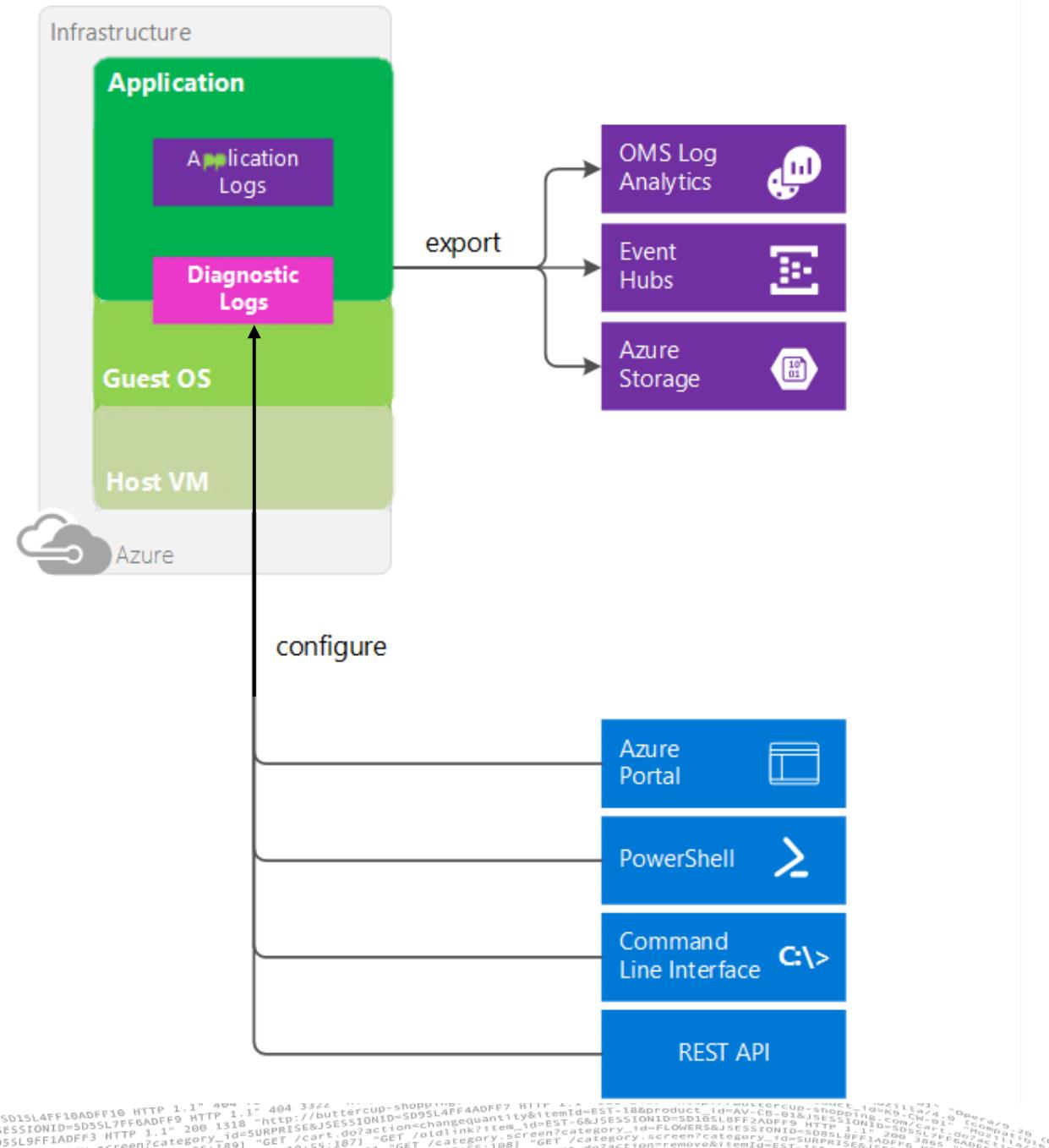


# Azure Guest OS Logging

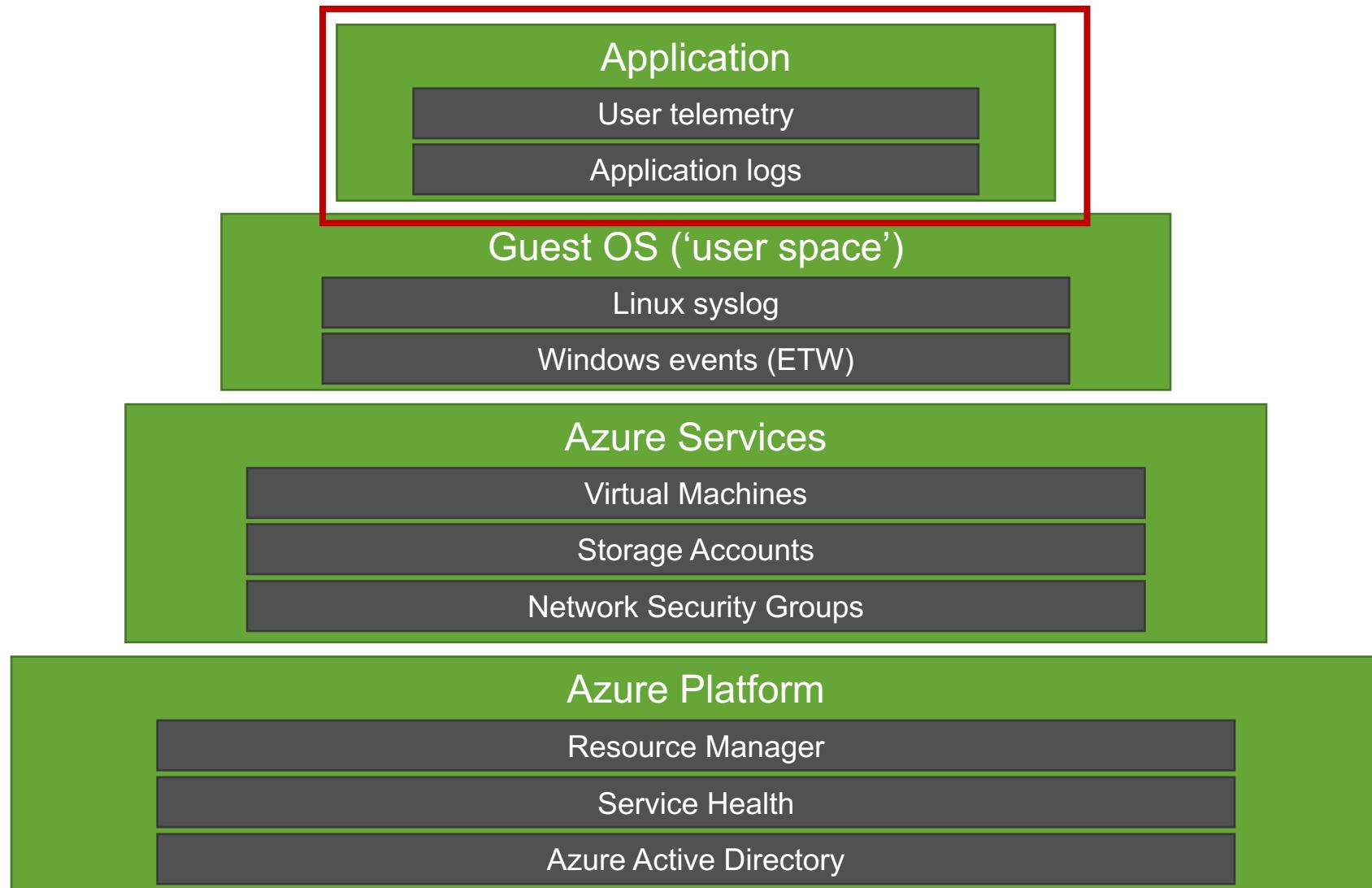
- ▶ Linux Azure Diagnostic extension (LAD) – Azure agent for collecting guest-level logs from Linux
  - Uses fluentd and other OSS monitoring tools
  - Open sourced on github
- ▶ Can collect Linux syslog (per facility and severity), arbitrary OMI queries, any file-based log, anything with a fluentd input plugin
- ▶ Windows Azure Diagnostic extension (WAD) – Azure agent for collecting guest-level logs from Windows
  - Can collect application logs, Windows event logs, .NET event source, IIS logs, manifest-based ETW, crash dumps, custom error logs, infrastructure logs

130.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD15LAFF10ADF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_0&product\_id=F1-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 128.241.220.82 ~ [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD15LAFF10ADF10 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_2&product\_id=F1-ZX11&category\_id=SURPRISE&JSESSIONID=SD59L4FFFADEFF" HTTPEquiv="refresh" value="200 2423" "http://buttercup-shopping.com/cart.do?action=view&itemId=EST\_2&product\_id=F1-ZX11&category\_id=SURPRISE&JSESSIONID=SD59L4FFFADEFF" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 317.27.160.0.0 ~ [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST\_18&product\_id=AFC-C018&SESSIONID=SD55L9FF1ADEF3" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 128.241.220.82 ~ [07/Jan 18:10:57:153] "GET /category.screen?category\_id=F1-SW-01&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST\_6&product\_id=AFC-C018&SESSIONID=SD55L9FF1ADEF3" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 128.241.220.82 ~ [07/Jan 18:10:57:153] "GET /category.screen?category\_id=F1-ZX11&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST\_2&product\_id=F1-ZX11&category\_id=SURPRISE&JSESSIONID=SD55L9FF1ADEF3" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) 128.241.220.82 ~ [07/Jan 18:10:57:153] "GET /category.screen?category\_id=F1-ZX11&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST\_2&product\_id=F1-ZX11&category\_id=SURPRISE&JSESSIONID=SD55L9FF1ADEF3" Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)

# Guest OS Logs And Metrics



# Tiers Of Monitoring Data In Azure





# Demo

---

Using Application Insights

# Recommended Reading

- ▶ Azure Active Directory reporting: <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-azure-portal>
- ▶ Activity log: <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs>
- ▶ Diagnostic logs: <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs> (see ‘Supported services and schema’)
- ▶ Network Watcher: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>
- ▶ Storage Analytics: <https://docs.microsoft.com/en-us/rest/api/storageservices/storage-analytics>

# Key Takeaways

1. Azure's monitoring strategy includes a range of built-in tools and embraces integration with 3rd party tools like Splunk too
2. The Azure Monitor Add-On for Splunk helps you to effectively manage your Azure environment with Splunk
3. Azure makes available all the monitoring data you need to seamlessly move from on-premises or another cloud to Azure without needing to reinvent the wheel

# Thank You

Don't forget to **rate this session** in the  
.conf2017 mobile app

splunk> .conf2017