



Securing Azure, Azure Secured



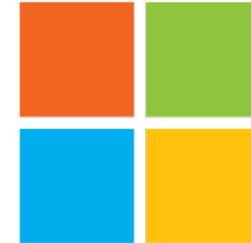
ISSA, Sept 19th 2018



@sdanelson

- Well traveled homebody
- Technology enthusiast
- Security journeyman
- Football (Soccer)

What this talk will not be about



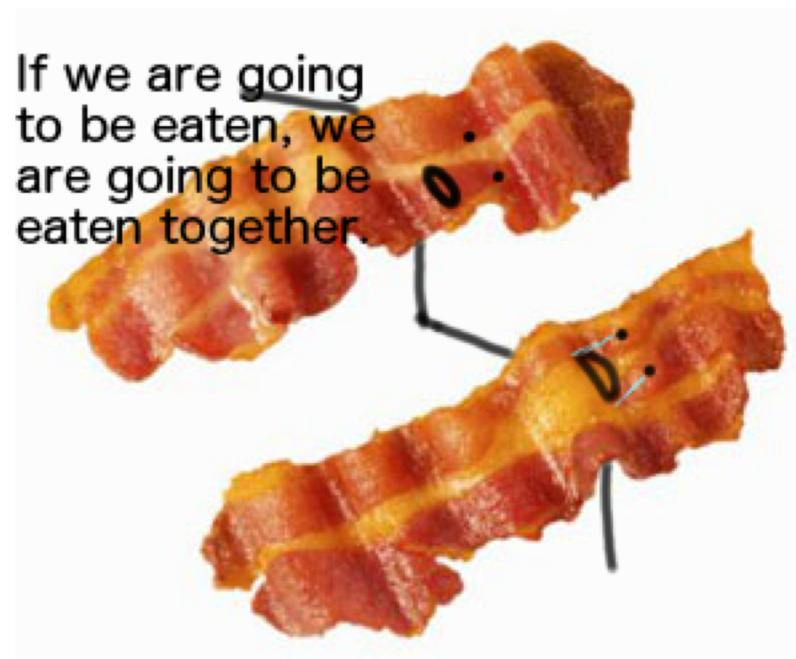
- Bashing Cloud
- Bashing Microsoft
- Comparing Clouds (Microsoft/Amazon/Google)
- Office 365 Security



What this talk IS



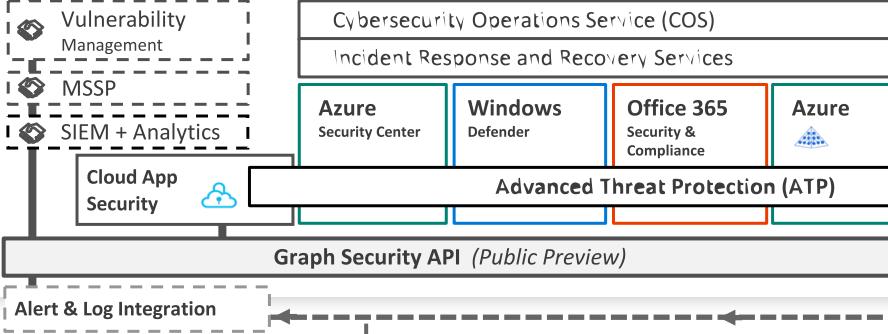
- Sharing Azure Security Tips
- Empowering you
- Building up the community



#0 RTM/RTFM/WheresTM/WhatM

- Where's the manual for my cloud?
 - Microsoft's Reference Security Architecture
 - <http://aka.ms/mcra>
 - <https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns>
 - <https://docs.microsoft.com/en-us/azure/>
 - Google?

Security Operations Center (SOC)



Cybersecurity Reference Architecture

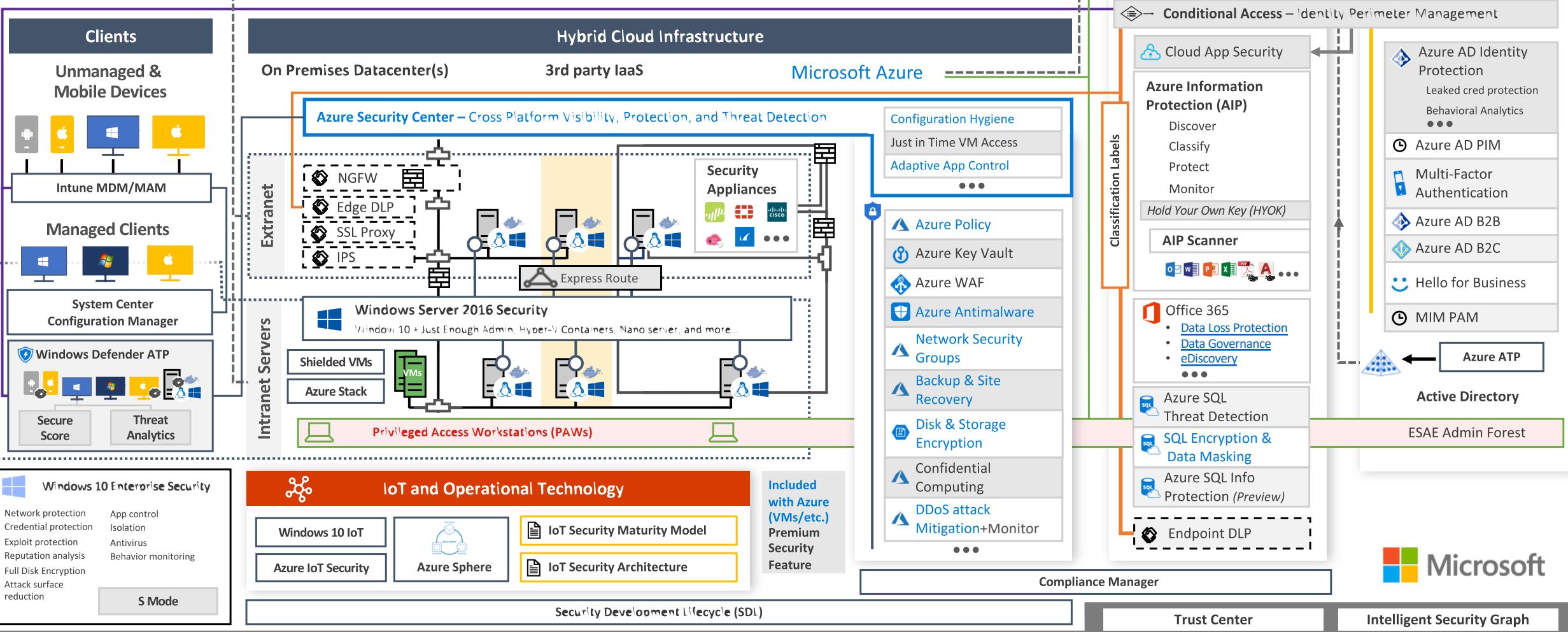
May 2018 – <https://aka.ms/MCRA> | [Video Recording](#) | [Strategies](#)

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. [Securing Privileged Access](#)
2. [Office 365 Security](#)
3. [Rapid Cyberattacks \(Wannacrypt/Petya\)](#)



Software as a Service

Office 365

- Secure Score
- Customer Lockbox



Dynamics 365

Information Protection

Identity & Access

- Azure Active Directory

- Azure AD Identity Protection (Leaked cred protection, Behavioral Analytics)
- Azure AD PIM (Multi-Factor Authentication)
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM

Conditional Access – Identity Perimeter Management

- Azure AD Identity Protection (Leaked cred protection, Behavioral Analytics)
- Azure AD PIM (Multi-Factor Authentication)
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM

Active Directory

ESAE Admin Forest



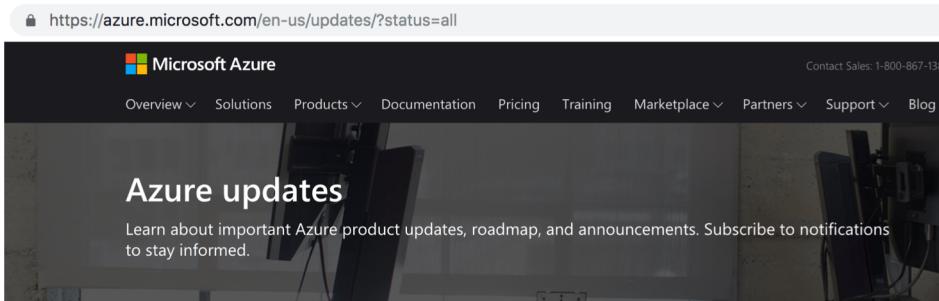
Intelligent Security Graph

#1 Clouuud Training, Sir!!

- Azure – <https://azure.microsoft.com/en-us/free/>
- AWS - <https://aws.amazon.com/free/>
- GCP - <https://console.cloud.google.com/freetrial>

#2 Microsoft just made me a liar

- Change is coming - how do you keep up with all the changes?



All Now available In preview In development

Product Search: All Update type: All

September 2018

Sep 18 [General availability: Azure Availability Zones in West US 2 and North Europe](#)
Azure Availability Zones, a high-availability solution for mission-critical applications, is now generally available in West US 2 and North Europe.
[Regions & Datacenters](#)

Sep 17 [General availability: Python 2 runbook support in Azure Automation](#)
Azure Automation now supports Python 2 for general availability. You can import, author, and run Python 2 runbooks in Azure or on a Hybrid Runbook Worker.
[Automation](#) [Features](#) [Open Source](#)

#2 Microsoft just made me a liar. Cont.

- <https://azure.microsoft.com/en-us/updates/>
- <https://azure.microsoft.com/en-us/roadmap/>



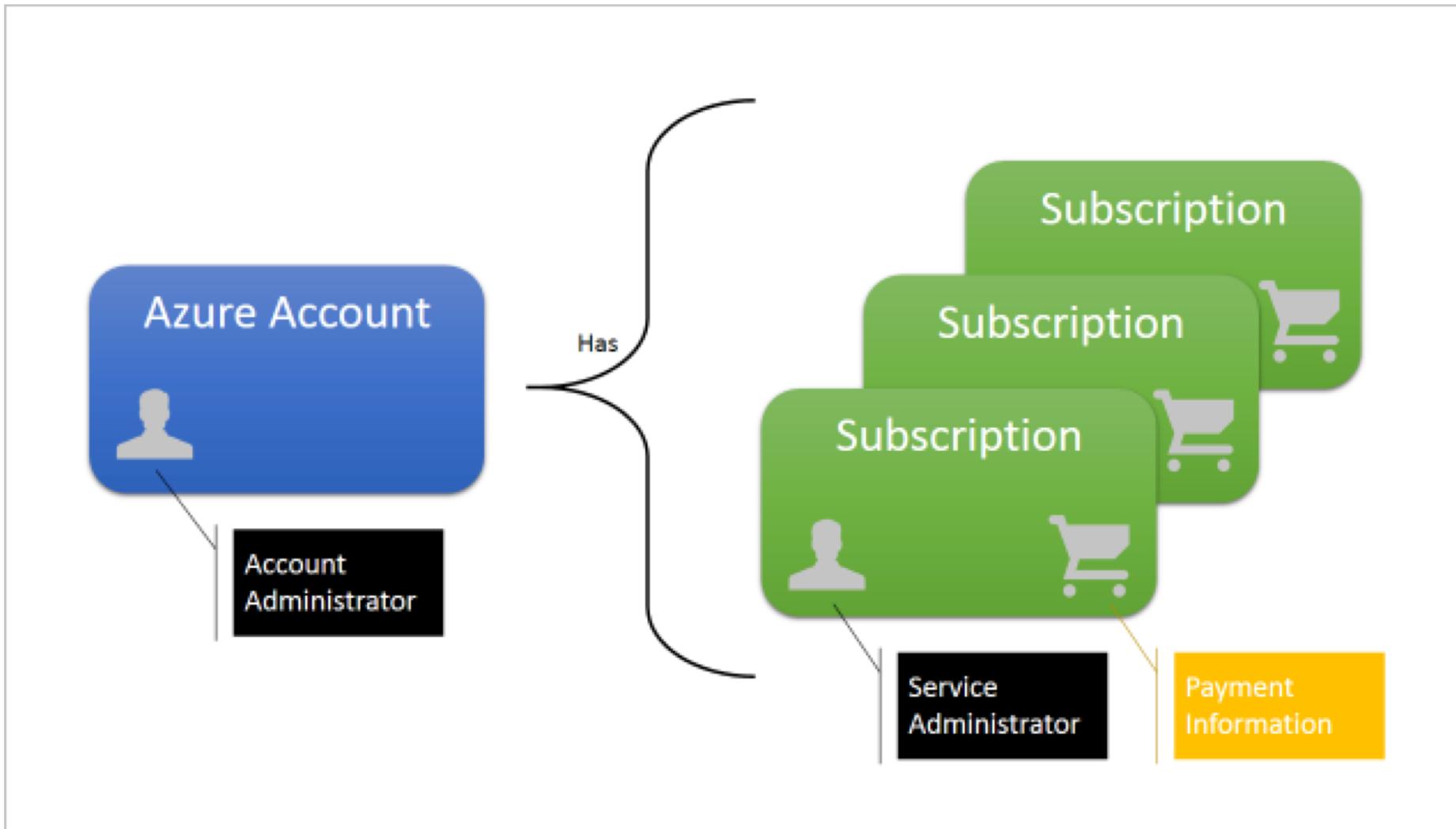
Subscribe

- <https://channel9.msdn.com/Shows/Azure-Friday> - @azurefriday
- @buildazure – not MS
- @azure - MS

#3 Who owns your cloud?

- What is the Azure equivalent of Root?
 - Account Administrator
 - Service Administrator
 - Directory (Azure AD)
 - Service Administrator
 - Co-Administrator

#3 Who owns your cloud? Cont.



#3 Who owns your cloud? Cont.

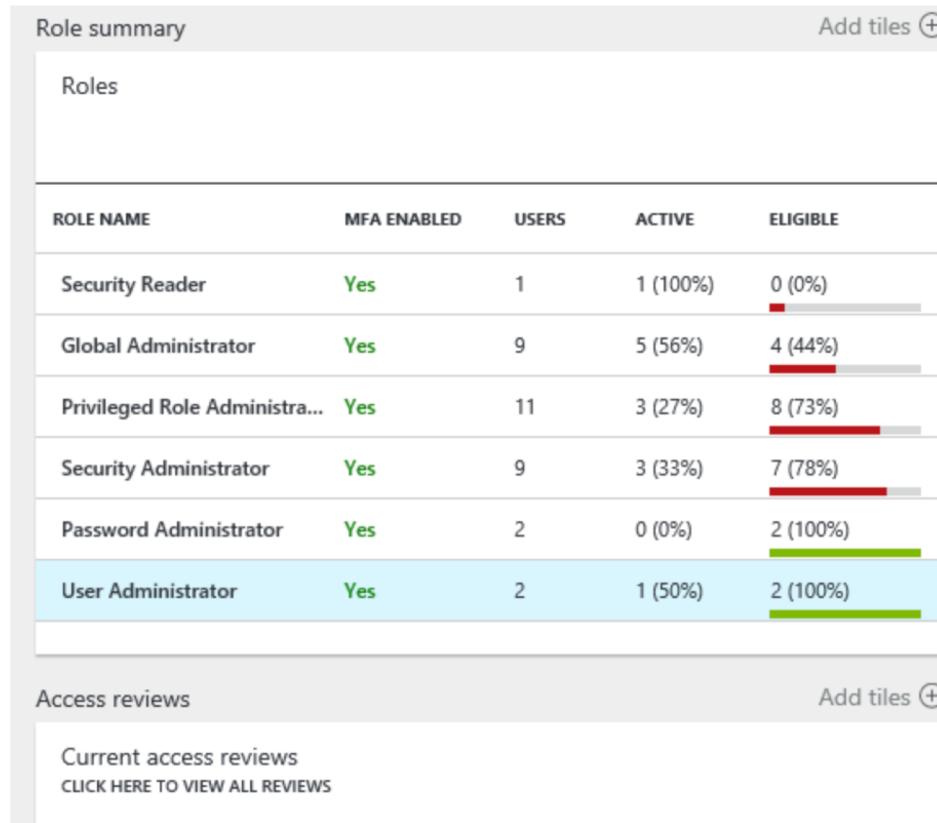
- Azure Cloud Shell
 - az role assignment list –include-classic-administrators

#3 Who owns your cloud? Cont.

```
stephen@Azure:~$  
stephen@Azure:~$ az role assignment list --include-classic-administrators  
[  
  {  
    "id": "NA(classic admins)",  
    "name": "NA(classic admins)",  
    "principalId": "3a429454-ceb9-4d82-9acc-8658c4bb7ecc",  
    "principalName": "stephen@██████████",  
    "roleDefinitionId": "NA(classic admin role)",  
    "roleDefinitionName": "ServiceAdministrator;AccountAdministrator",  
    "scope": "/subscriptions/██████████"  
  }  
]  
stephen@Azure:~$ █
```

#3 Who owns your cloud? Cont.

- Privileged Identity Management (PIM)



#3 Who owns your cloud? Cont.

- Directory Global Admins – Azure AD - Properties

 Company branding	Country or region United States
 User settings	Location United States datacenters
 Properties	Notification language English
 Notifications settings	Global admin can manage Azure Subscriptions and Management Groups <input type="button" value="Yes"/> <input type="button" value="No"/>
SECURITY	
 Conditional access	

#4 Know your assets

- Asset management in Azure
- <https://docs.microsoft.com/en-us/rest/api/resources/resources/list>

Resources - List

Service: Resource Management

API Version: 2018-02-01

Get all the resources in a subscription.

HTTP	 Copy	 Try It
GET https://management.azure.com/subscriptions/{subscriptionId}/resources?api-version=2		
<div style="height: 10px; background-color: #ccc;"></div>		

With optional parameters:

HTTP	 Copy
GET https://management.azure.com/subscriptions/{subscriptionId}/resources?\$filter={\$fil	
<div style="height: 10px; background-color: #ccc;"></div>	

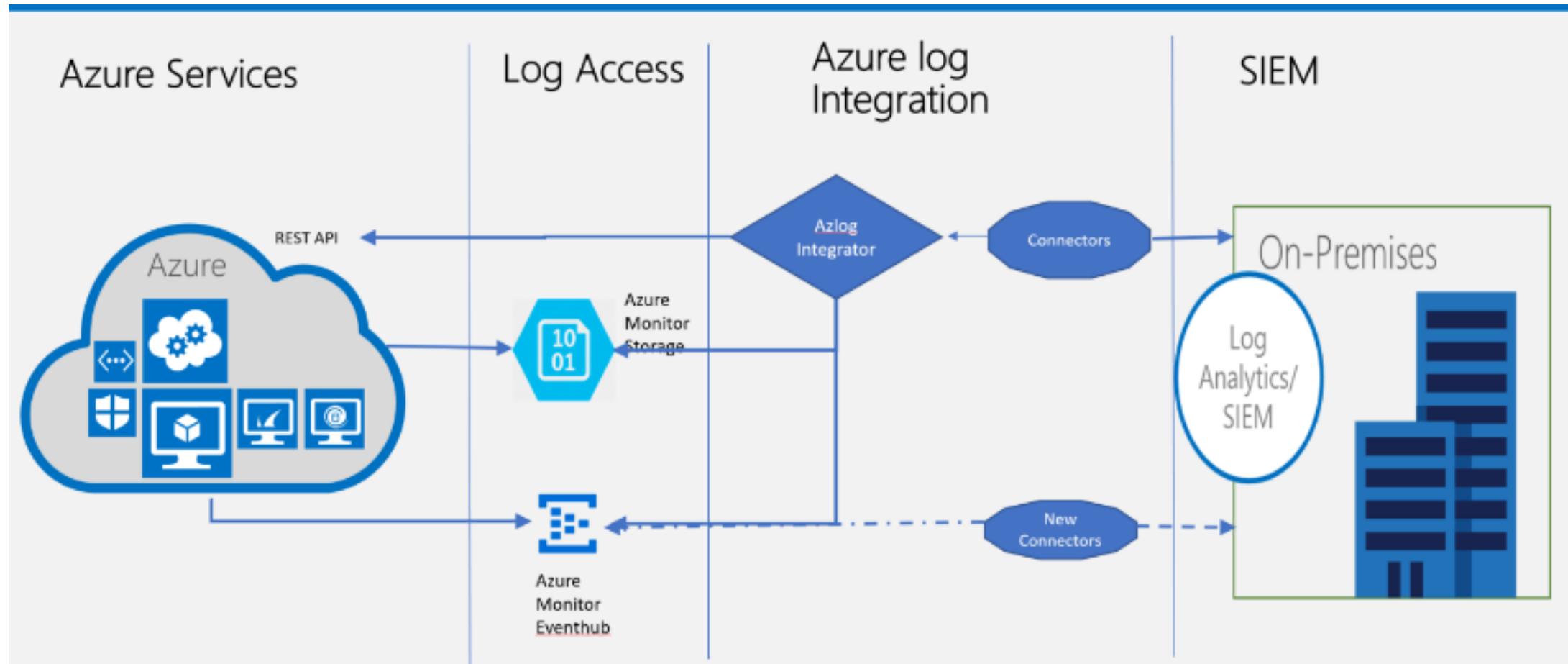
#4 Know your assets, cont.

- To scan or not scan – Do I need a vulnerability scanner for Azure?
- Tenable
- Qualys
- Rapid7
- Azure Configuration Scanners
 - Microsoft Azure Policy

#5 Who, what, where, and how? (Logs, Logs..)

- Logs, logs, and more logs – how do you get your logs out?
 - Three main types of logs:
 - Control/Management Logs
 - Data Plane Logs
 - Processed events

#5 Who, what, where, and how? Cont.



#5 Who, what, where, and how? (Logs, Logs..)

- Azure Security Center
- OMS (not really a SIEM, yet)
- SaaS – Security as a Differentiator (\$\$)

#5 Who, what, where, and how? (Logs, Logs..)

Home > Security Center - Overview

Security Center - Overview

Showing all subscriptions

Search (Ctrl+ /)

Subscriptions

Your security experience may be limited. Click here to learn more →

GENERAL

- Overview
- Security policy
- Quickstart
- Events
- Onboarding to advanced security
- Search

PREVENTION

- Recommendations
- Security solutions
- Compute
- Networking
- Storage & data

Subscriptions

Overview

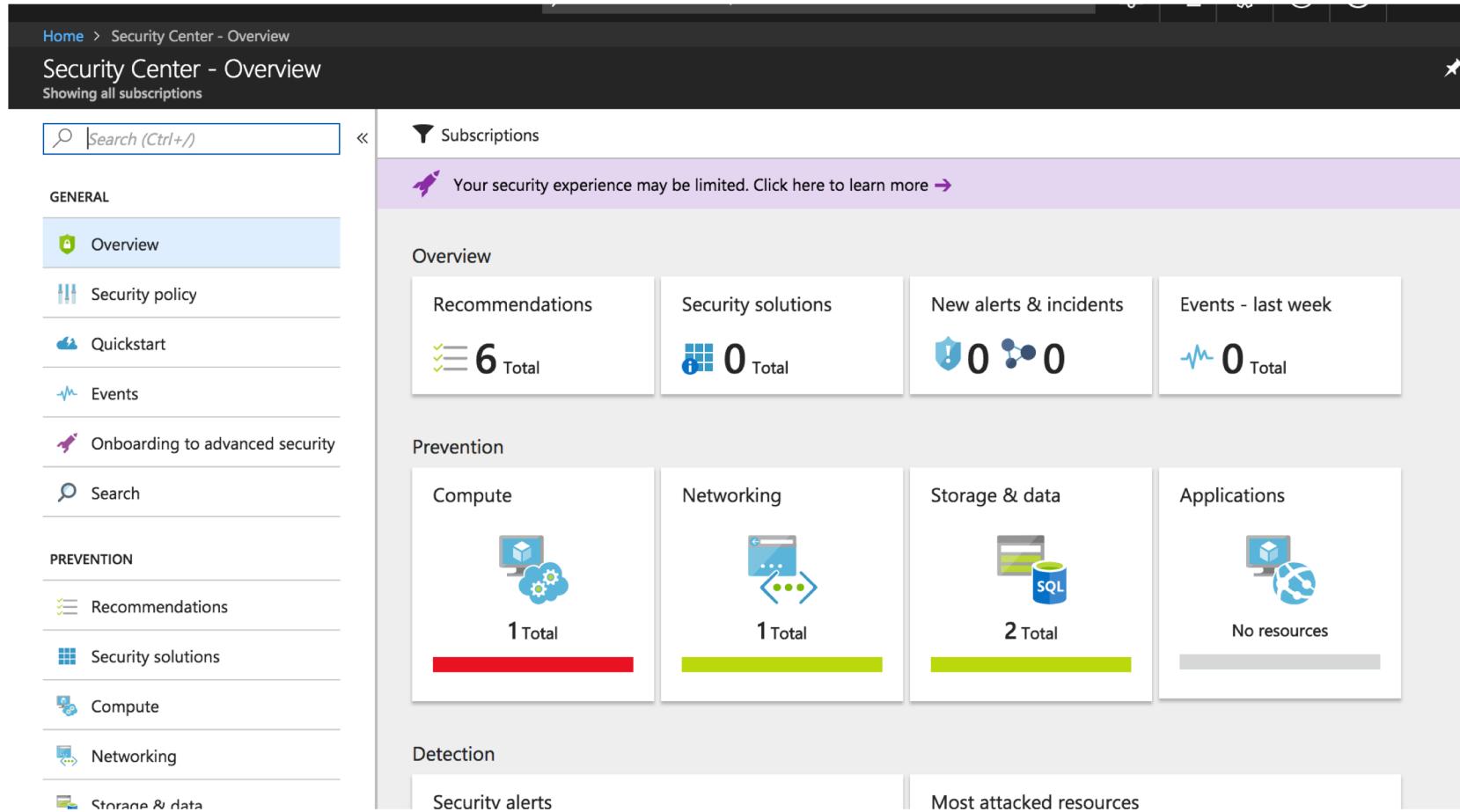
Recommendations	Security solutions	New alerts & incidents	Events - last week
 6 Total	 0 Total	 0 	 0 Total

Prevention

Compute	Networking	Storage & data	Applications
 1 Total	 1 Total	 2 Total	 No resources

Detection

- Security alerts
- Most attacked resources



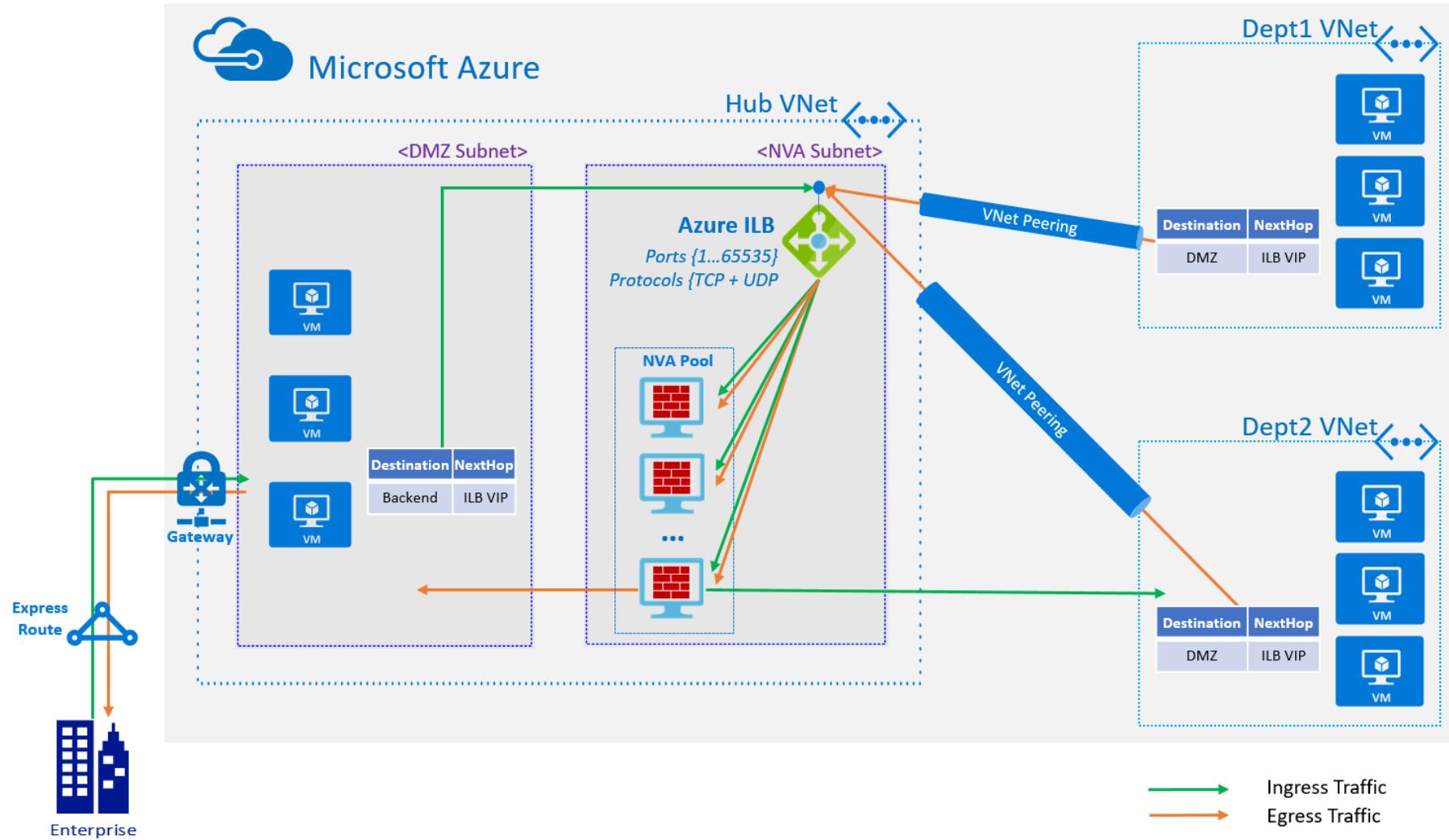
#6 Would the real NVA please stand up.

- What is an NVA and do you need one?
- Network Virtual Appliance (NVA)
- 3rd party WAFs, Firewalls, gateways/routers, application delivery controllers and WAN optimizers
 - Note (not layer 2)

#6 Would the real NVA please stand up. Cont.

- Layer 7 Firewall or Network Security Groups (NSGs) or Azure FW
- 3rd Party
 - Cisco
 - Palo Alto
 - CheckPoint
 - Etc
- HA
 - Doesn't really exist because a lot of HA implementations depend on layer 2
 - Depends on Microsoft tooling

#6 Would the real NVA please stand up. Cont.



#6 Would the real NVA please stand up. Cont.

- 168.63.129.16/32 -
<https://blogs.msdn.microsoft.com/mast/2015/05/18/what-is-the-ip-address-168-63-129-16/>
- Scale out
- Availability Set
- Pre-provision

#7 Web Apps Feel special (WAFs)

- What the WAF – why you need a WAF and what our your options?
 - Web Application Firewall (WAF)
 - 3rd Party IaaS
 - Barracuda
 - Imperva
 - Etc
 - 3rd Party SaaS
 - Imperva Incapsula
 - CloudFlare
 - Etc
 - Microsoft

#7 Web Apps Feel special (WAFs), cont.

Home > New > Marketplace > Everything > Application Gateway > Create application gateway > Basics

Create application gateway

Basics

1 Basics Configure basic settings >

2 Settings Configure application gateway... >

3 Summary Review and create >

* Name

* Tier Standard WAF

* SKU size Medium

Instance count 2

* Subscription Pay-As-You-Go

* Resource group Create new Use existing

* Location South Central US

Your virtual network and public IP address must be in the same location as your gateway. If you

OK

The diagram illustrates the Application Gateway architecture and its role as a Web Application Firewall (WAF). At the center is a blue box labeled "Application Gateway" containing icons for "WAF" and "L7 LB". To the left, two user icons send requests to the Application Gateway. One request is labeled "XSS attack" and is blocked by a red "X". Another request is labeled "Valid Request" and is processed by a green checkmark. A third request is labeled "SQL Injection" and is blocked by a red "X". From the Application Gateway, two green arrows labeled "Valid Request" point to two separate boxes representing "Site1" and "Site2", each containing a monitor icon with a blue cube.

#8 Flip those bits, yes, no or default for SQL?

- Flip those bits - configuring encryption and security for Sql PaaS
- Is my data safe in transit?
 - Make sure TrustServerCertificate=False
- Firewall
- Turn on Auditing \$
- Threat Detection \$\$
- TDE on by default, but maybe bring your own key?

#9 A PIP here, a PIP there, a PIP everywhere

- PIP me – Why do I care?
 - PIP's are the new DMZ
 - Any VM NIC could be assigned a PIP
- stephen@Azure:~\$ az network public-ip list
- Policy Restricting (Azure or 3rd Party)
- RBAC

#10 All the factors belong to us

- All the factors – How can I use MFA to protect Azure?
 - <https://docs.microsoft.com/en-us/azure/multi-factor-authentication/>
- Global Admins (O365) for Free
- License MFA from Microsoft
- 3rd Party Federation
- Don't forget local (onmicrosoft.com) accounts

Q&A

- <https://github.com/sdanelson/ISSA20180919/>
- stephen[@]pinpointsecurity[.]io