Securing Azure, Azure Secured

BSidesOK, April 13th 2018

@sdanelson

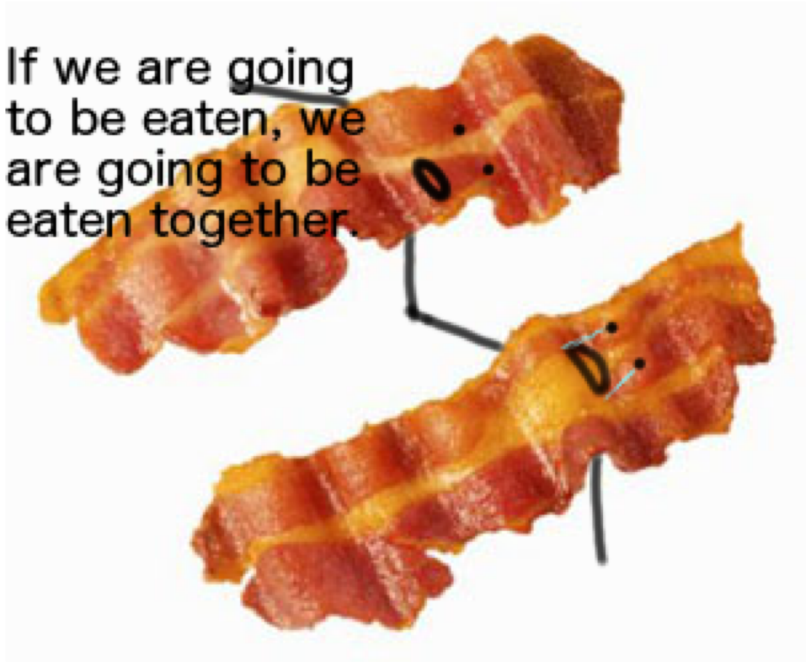
- Well traveled homebody
- Technology enthusiast
- Security journeyman
- Football (Soccer)

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

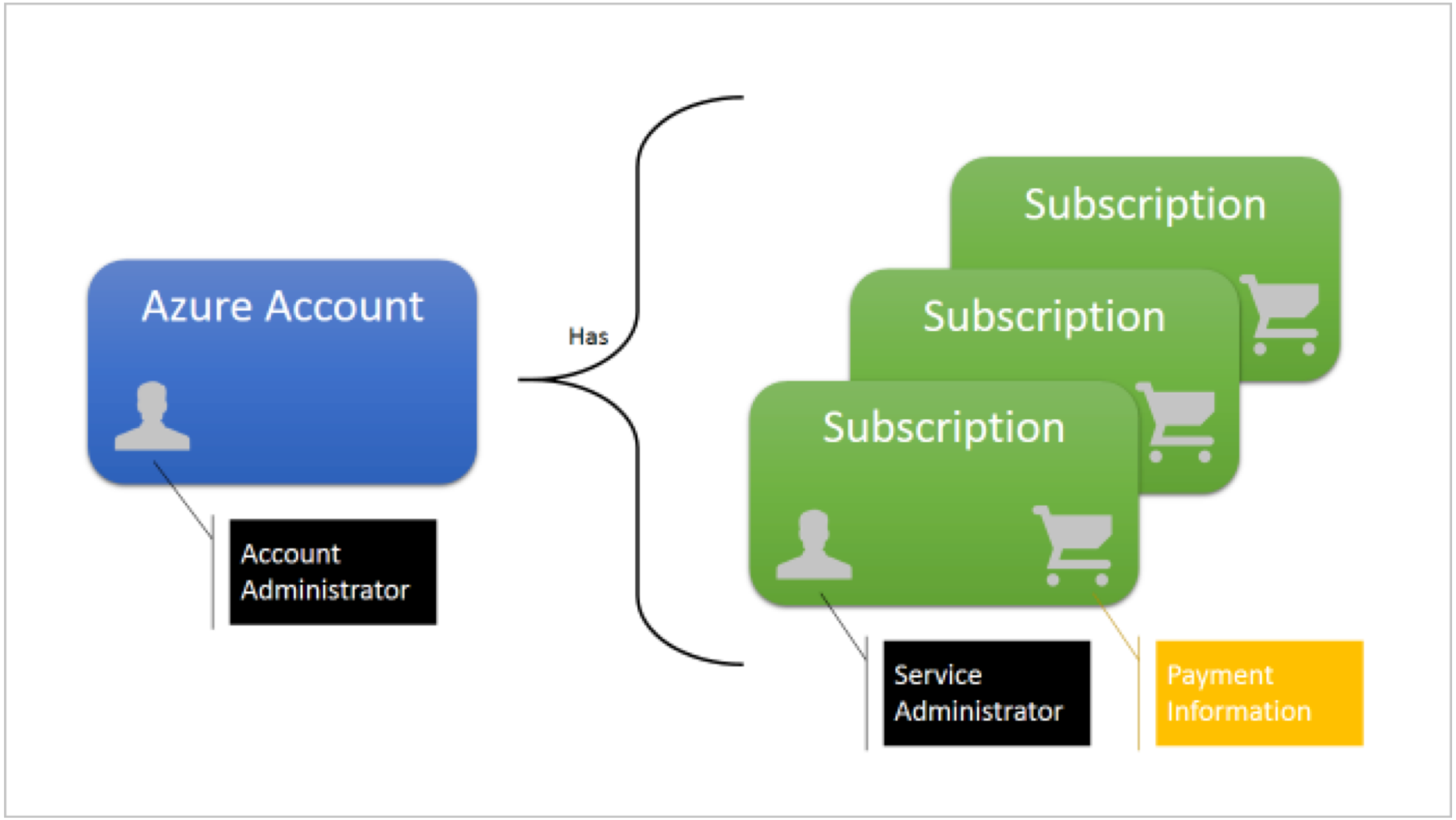


How about you?

#1 Who owns your cloud?

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

#1 Who owns your cloud? Cont.



#1 Who owns your cloud? Cont.

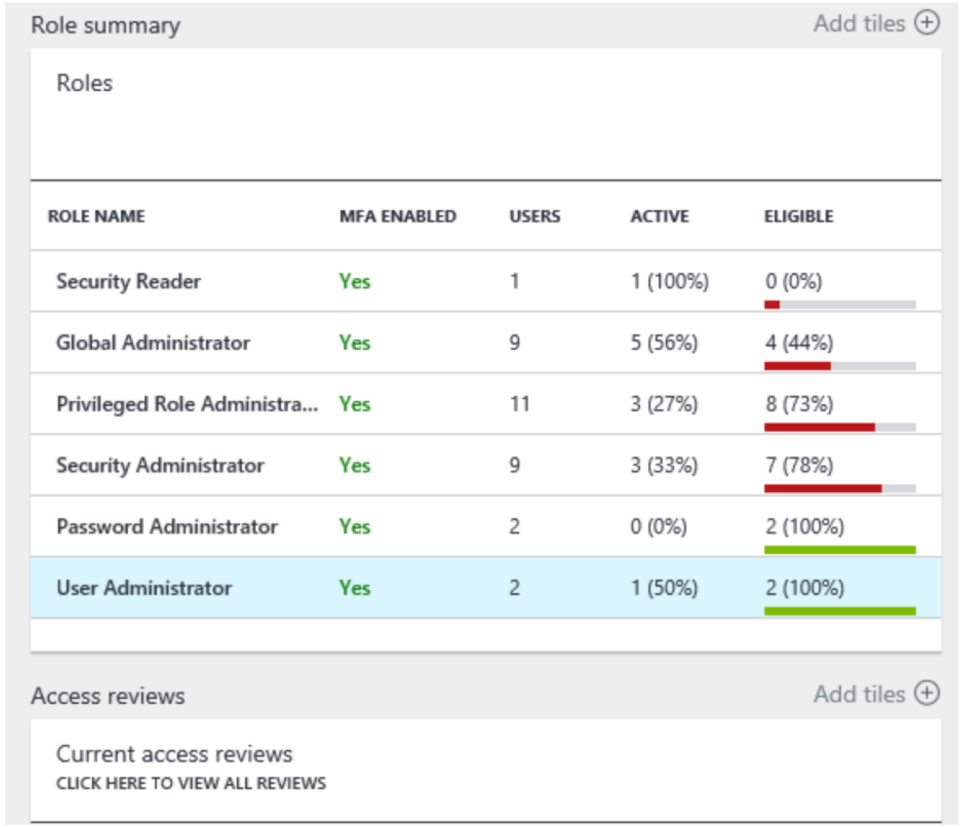
- Azure Cloud Shell
  - az role assignment list –include-classic-administrators

#1 Who owns your cloud? Cont.

```
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@[redacted],
    "roleDefinitionId": "NA(classic admin role)",
    "roleDefinitionName": "ServiceAdministrator;AccountAdministrator",
    "scope": "/subscriptions/[redacted]"
  }
]
stephen@Azure:~$
```

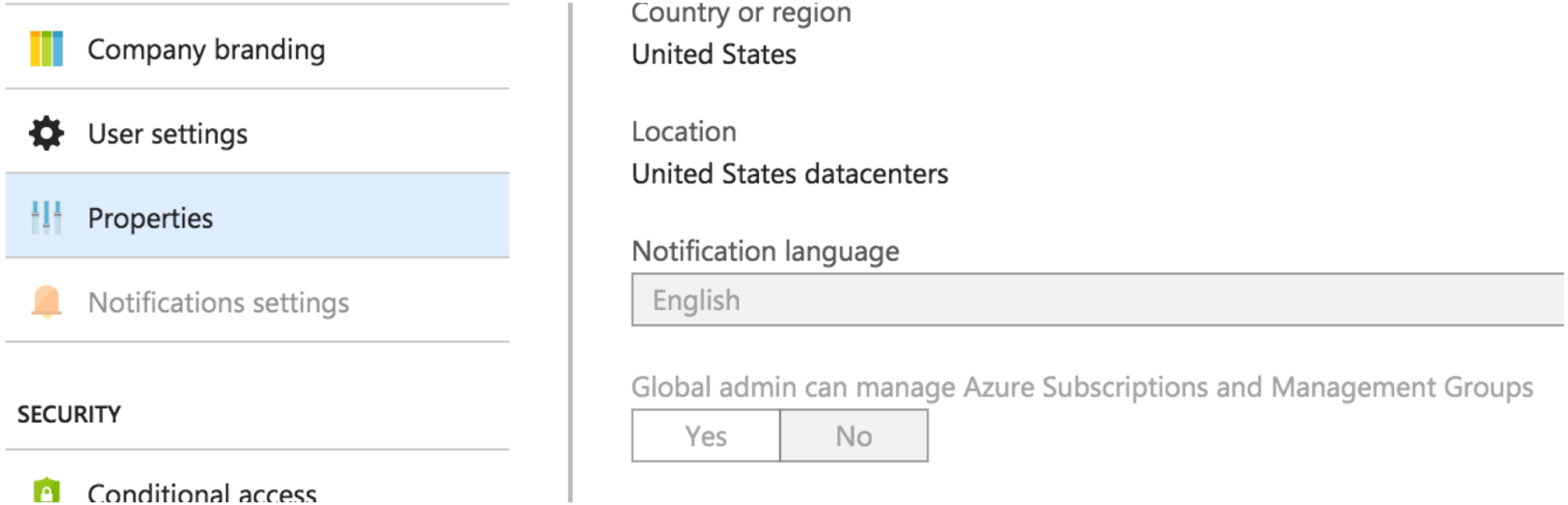
#1 Who owns your cloud? Cont.

- Privileged Identity Management (PIM)



#1 Who owns your cloud? Cont.

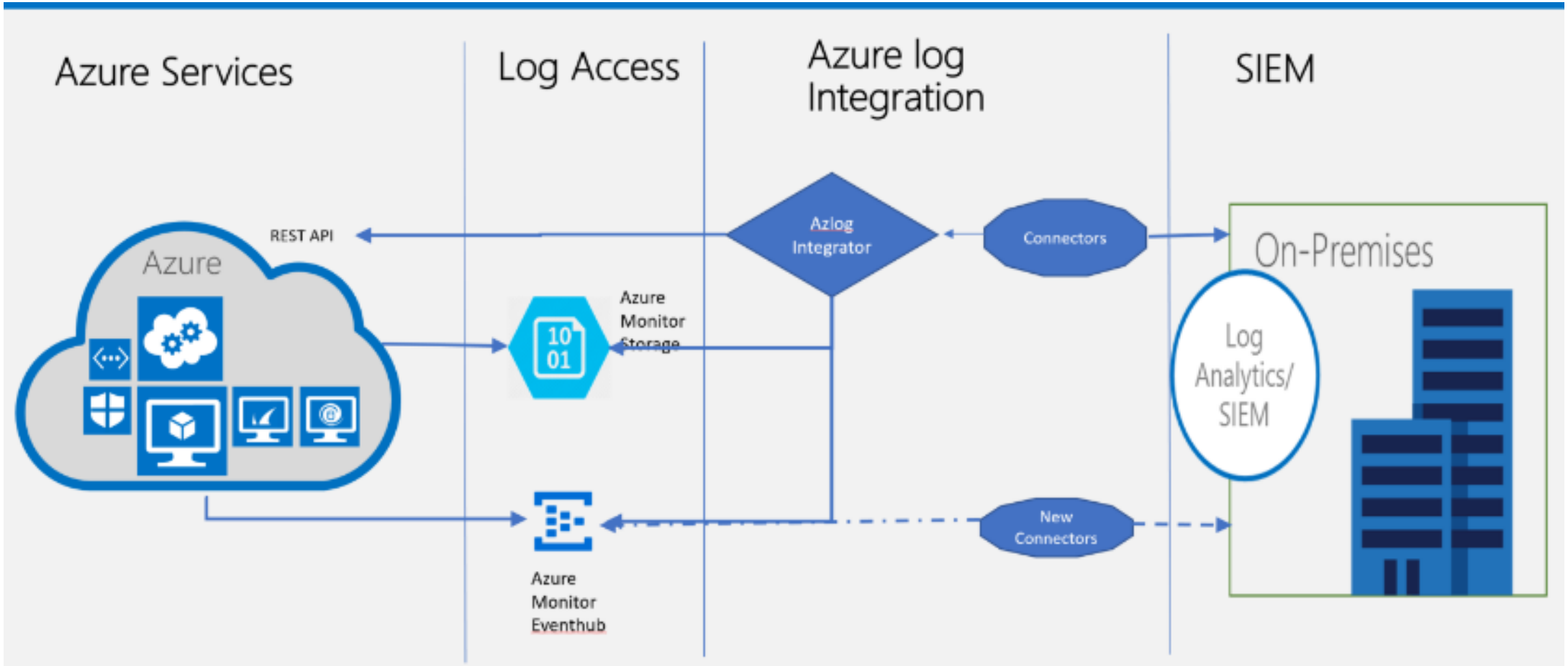
- Directory Global Admins – Azure AD - Properties



#2 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

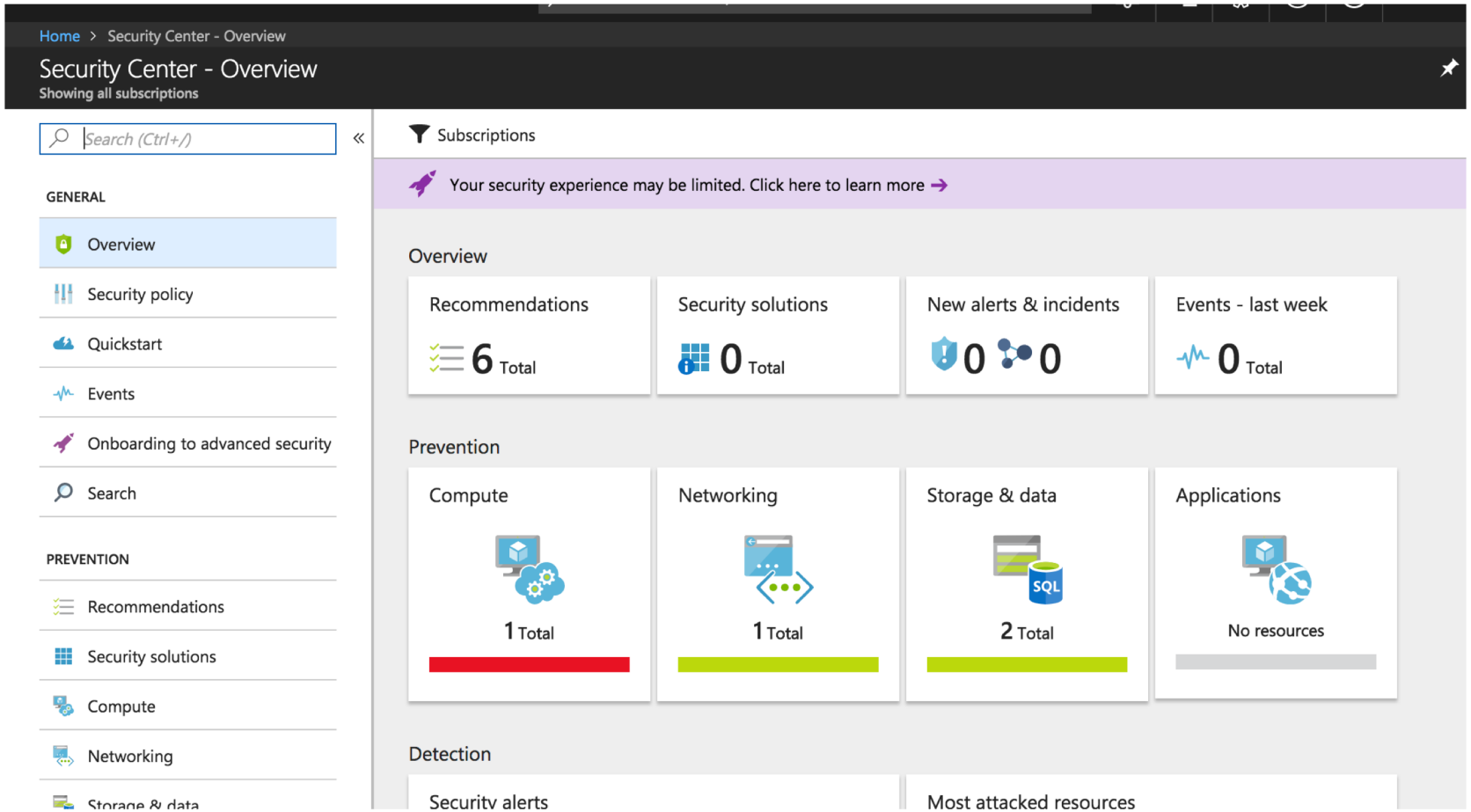
#2 Who, what, where, and how? Cont.



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

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

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



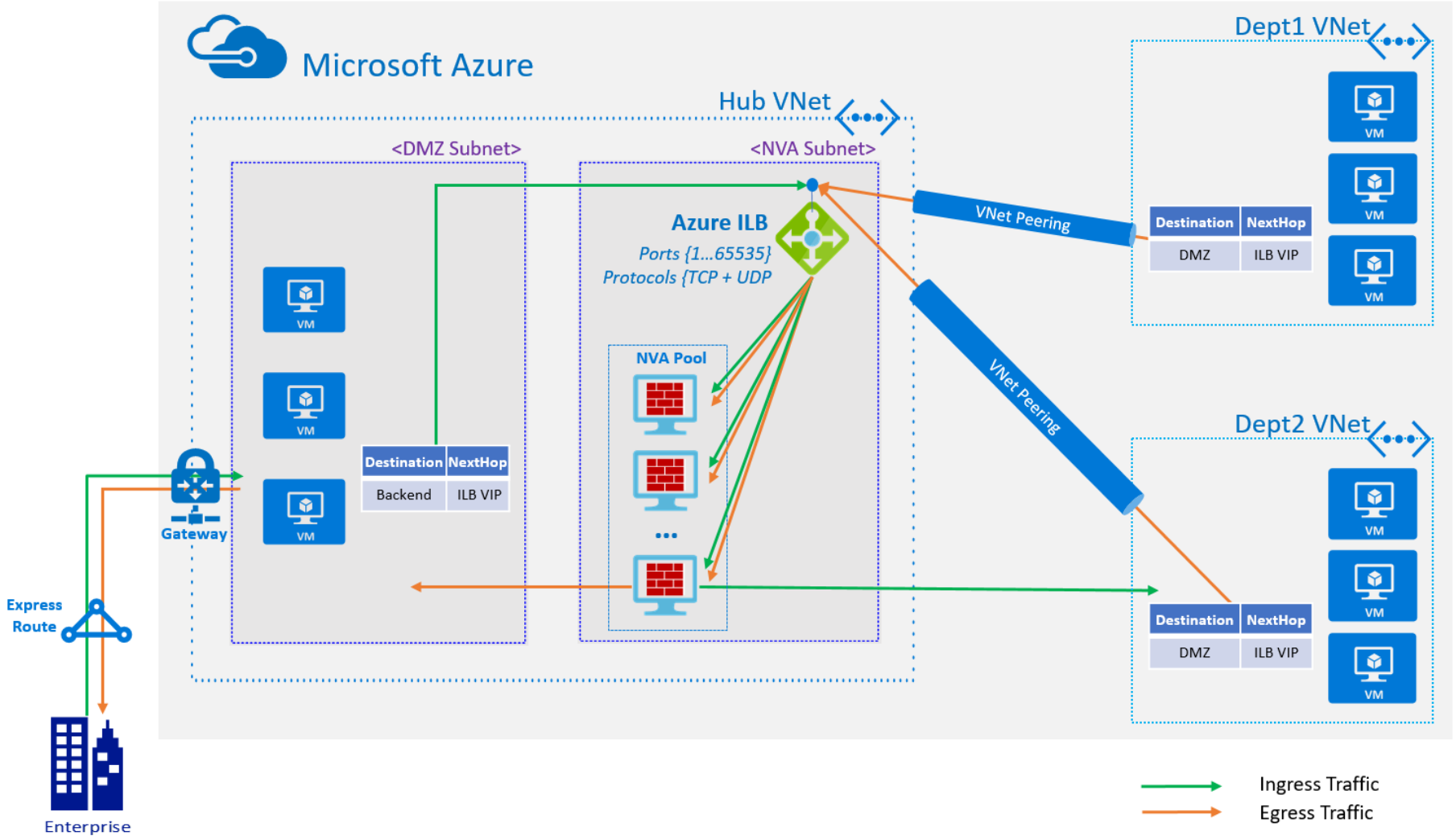
#3 Would the real NVA please stand up.

- 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)

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

- Layer 7 Firewall or Network Security Groups (NSGs)
- 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

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



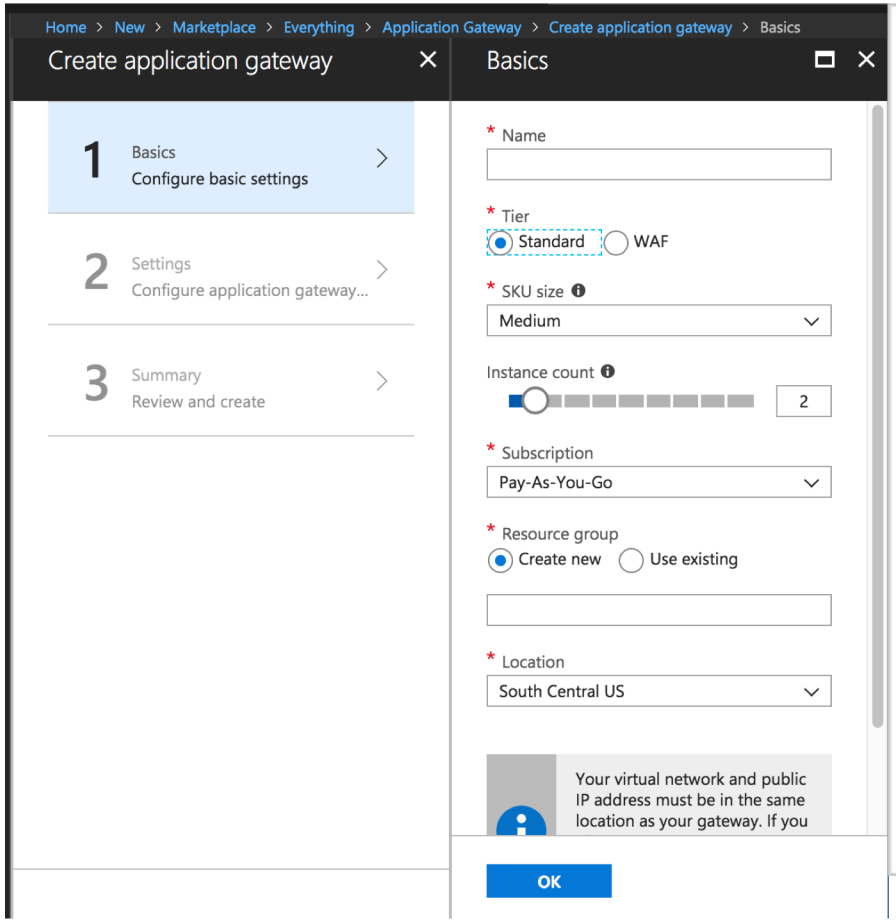
#3 Would the real NVA please stand up. Cont.

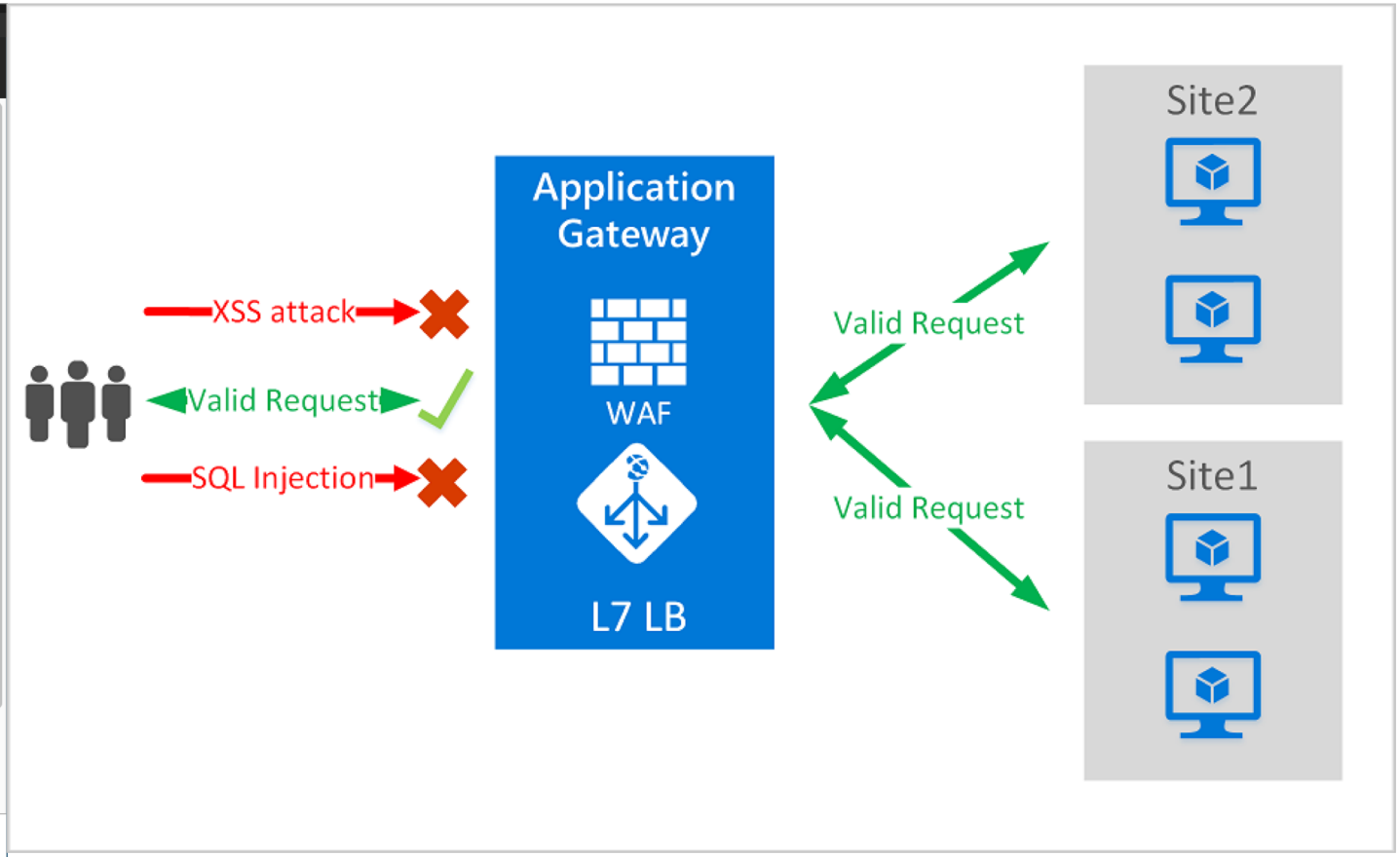
- 168.63.129.16/32
- Scale out
- Availability Set
- Pre-provision

#4 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

#4 Web Apps Feel special (WAFs)



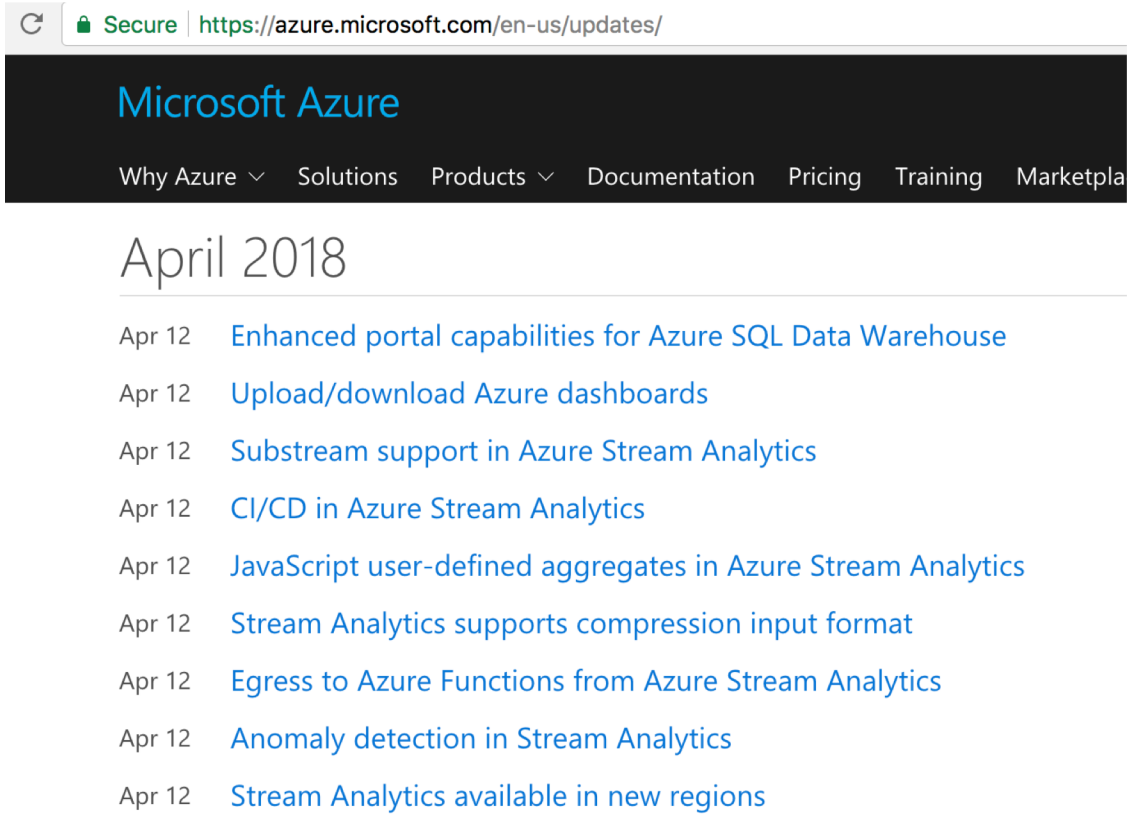


#5 Flip those bits, yes, no or default for SQL?

- 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?

#6 Microsoft just made me a liar

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



#6 Microsoft just made me a liar. Cont.

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

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

#7 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

#8 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

#9 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?

Cybersecurity Reference Architecture

Microsoft

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- Analytics / UEBA
- SIEM
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Windows Security Center
- Azure Security Center
- Office 365
  - Security & Compliance
  - Threat Intelligence

Security Development Lifecycle (SDL)

80% + of employees admit using non-approved SaaS apps for work (Stratecast, December 2013)

Internet of Things

Unmanaged & Mobile Clients

Software as a Service

Office 365
- ASM
- Lockbox

Identity & Access

Azure Active Directory
- Conditional Access
- Azure AD Identity Protection
- Azure AD PIM
- Multi-Factor Authentication
- Hello for Business
- MIM PAM
- ATA
- Active Directory
- ESAE Admin Forest
- Certification Authority (PKI)

Information Protection

- Cloud App Security
- Office 365 DLP
- Azure Information Protection (AIP)
  - Classify
  - Label
  - Protect
  - Report
- Hold Your Own Key (HYOK)
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Endpoint DLP
- Windows Info Protection

Classification Labels

Intune MDM/MAM

SIEM Integration

Microsoft Azure

Azure Security Center (ASC)
- Threat Protection
- Threat Detection

- Azure Key Vault
- Azure App Gateway
- Azure Antimalware
- Network Security Groups
- ...
- SQL Firewall
- Disk & Storage Encryption
- DDoS attack mitigation
- Backup & Site Recovery

On Premises Datacenter(s)

- NGFW
- Edge DLP
- SSL Proxy
- IPS
- Office 365 ATP
  - Email Gateway
  - Anti-malware
- Extranet
- Express Route
- Colocation
- Security Appliances
- VPN

Enterprise Servers

- Shielded VMs
- VMs
- Domain Controllers

Windows Server 2016 Security
Shielded VMs, Device Guard, Credential Guard, Just Enough Admin, Hyper-V Containers, Nano server, Defender AV, Defender ATP (Roadmap), and more...

Privileged Access Workstations (PAWs)

Managed Clients

- Sensitive Workloads
- Legacy Windows
- Windows 10
- Mac OS
- IoT
- EDR - Windows ATP
- EPP - Windows Defender AV
- System Center Configuration Manager + Intune

Windows 10 Security
- Secure Boot
- Device Guard
- Exploit Guard
- Application Guard
- Credential Guard
- Windows Hello
- Remote Credential Guard
- Device Health Attestation

WEF

Nearly all customer breaches that Microsoft's Incident Response team investigates involve credential theft
63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

Last updated July 2017 – latest at http://aka.ms/MCRA

#10 To scan or not to scan, that is the ?

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

Q&A

- https://github.com/sdanelson/BSidesOK2018/