black hat®
USA 2019

AUGUST 3-8, 2019

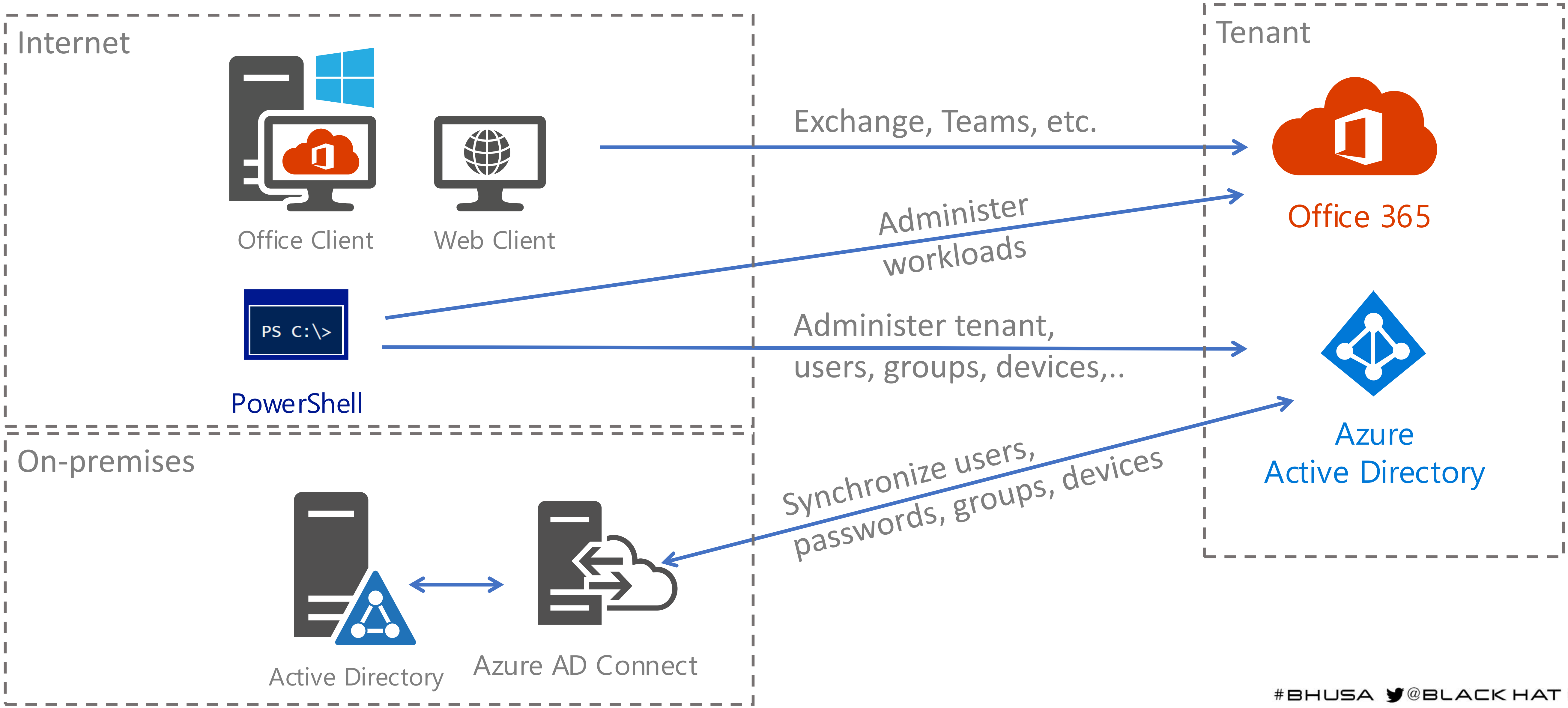
MANDALAY BAY / LAS VEGAS

#BHUSA @BLACK HAT EVENTS

AADInternals

- PowerShell module for administering Office 365/Azure AD
  - Utilizes (mostly) administrative REST APIs
  - Reveal “hidden” information
  - Create backdoors
  - Bypass security features (e.g. MFA)
- Available at:
  - http://o365blog.com/aadinternals
  - https://github.com/Gerenios/AADInternals
  - `PS:\>Install-Module AADInternals`

Office 365 / Azure AD concepts



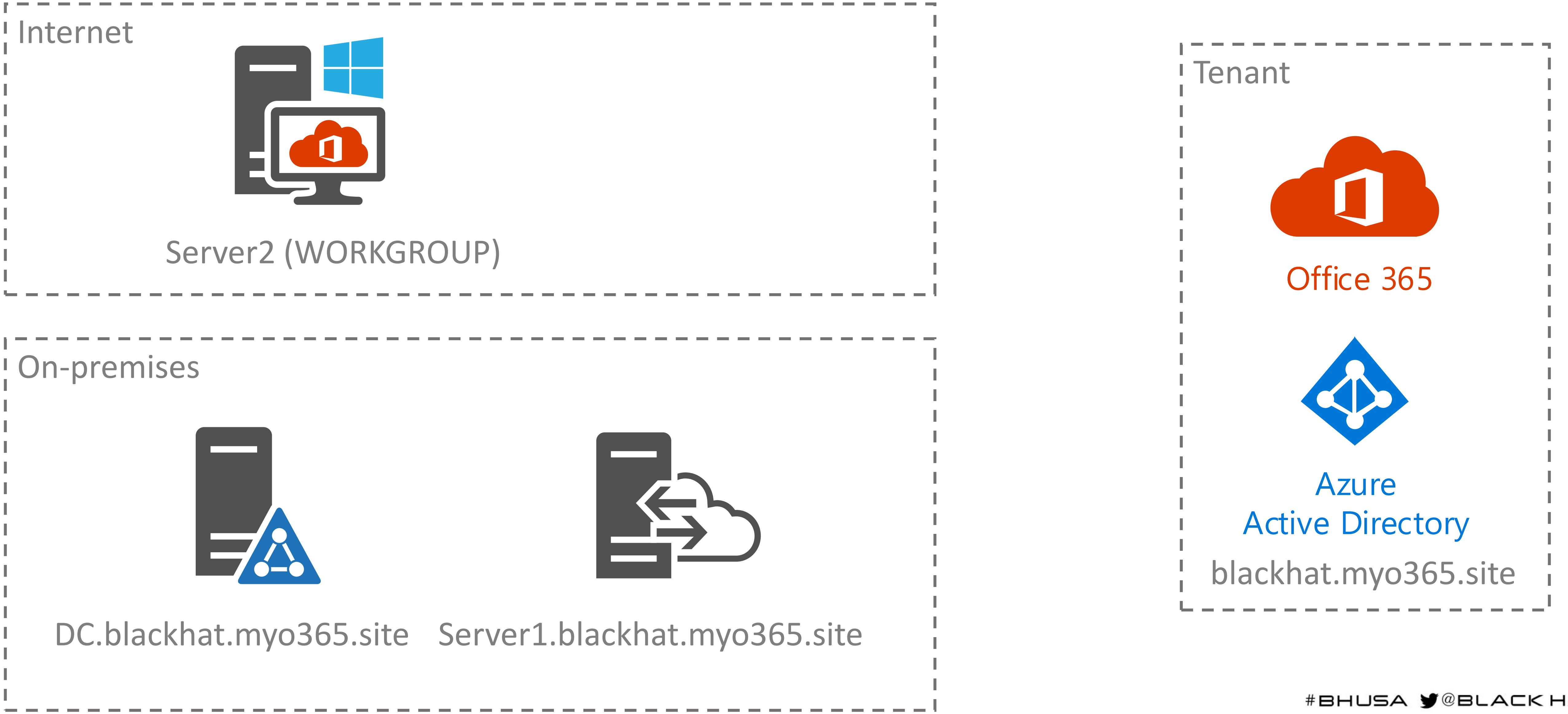
Azure AD Identity options

- Managed
  - Authentication performed by Azure AD
    - Against Azure AD
      - Cloud-only
      - Password-Hash Synchronization (PHS)
    - Against on-prem AD
      - Pass-Through Authentication (PTA)
- Federated
  - Authentication performed by external Identity Provider (i.e. on-prem AD)

Demo

- Getting information
- Azure AD connect
- Pass-through Authentication (PTA)
- Federated Identity
- Bypassing MFA

Demo setup



Internet

Server2 (WORKGROUP)

On-premises

DC.blackhat.myo365.site

Server1.blackhat.myo365.site

Tenant

Office 365

Azure
Active Directory

blackhat.myo365.site