Cloud Security – First topics

James Beatty

avanade

Who I am

Two decades worth of technology, beginning in route/switch infrastructure, up through infrastructure and security architecture, and culminating in security program building.

Security program build at Allina, Target post-breach, and now consulting.

"There are no security problems."

Alphabet soup: CISSP, ITILv3, GIAC Security Leadership certifications, CISM, BS Software Engineering

I am married, and have five daughters, with number six due October 23rd.

jamesm.beatty@gmail.com

Topics Today

- Shared responsibility
  - Why talk about it?
  - Cloud models
- Office 365 and Azure authentication
  - Active Directory
  - Multifactor
  - Other enterprise authentication
- AWS authentication
  - Active Directory
  - Multifactor
  - Other enterprise authentication

avanade

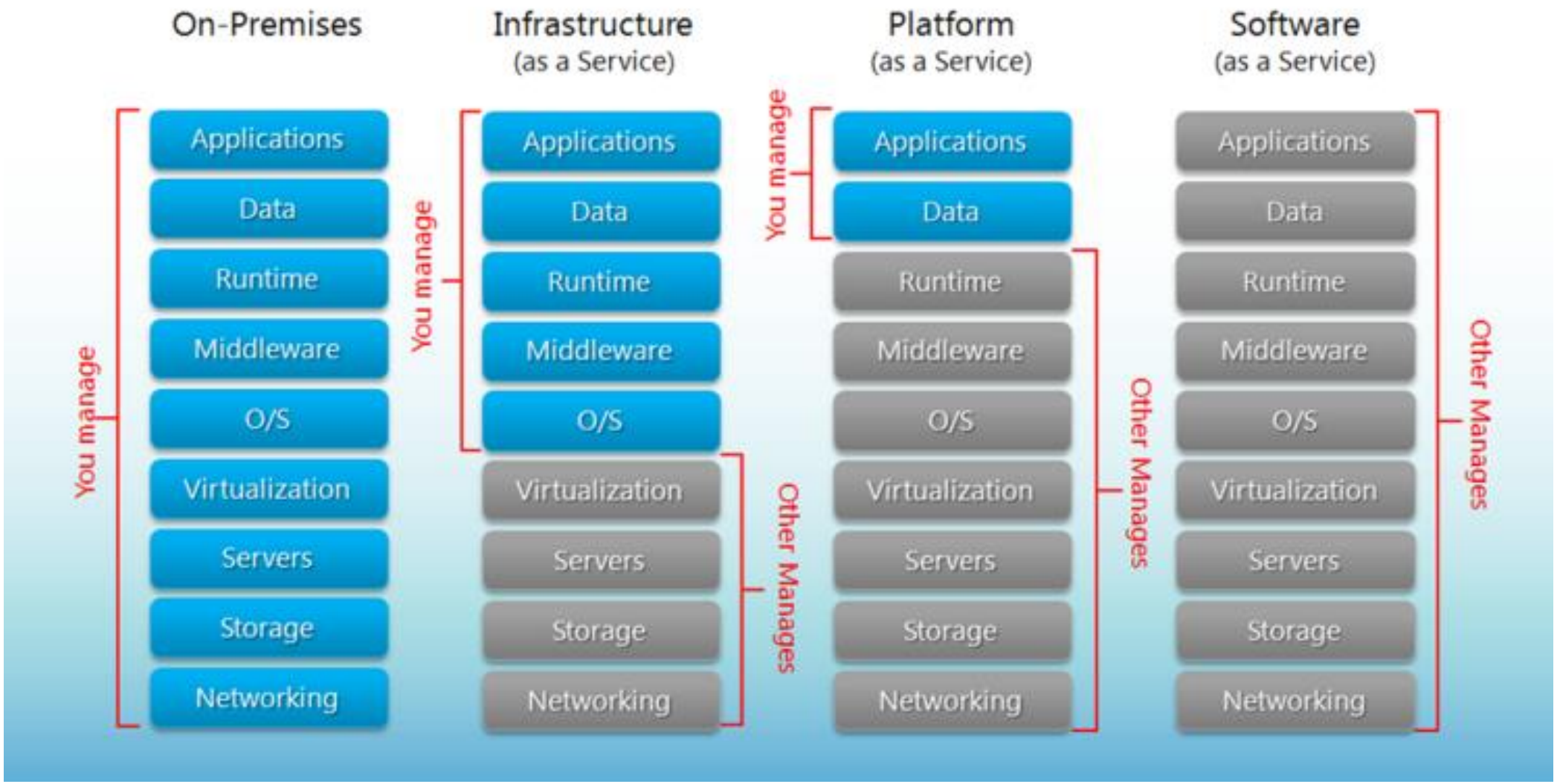
Shared responsibility

- Generally what we would expect

- Why do we talk about it?
  - It enables the cloud security discussion
  - Understand cloud provider expectations
  - Clarify conversations and understanding
  - Know what our work is

- Cloud models
  - On premises (and hybrid)
  - Infrastructure as a Service (IaaS); Ex. Rackspace, Azure VMs
  - Platform as a Service (PaaS); Ex. Azure App Service
  - Software as a Service (SaaS); Ex. Service-Now, SalesForce, Office 365

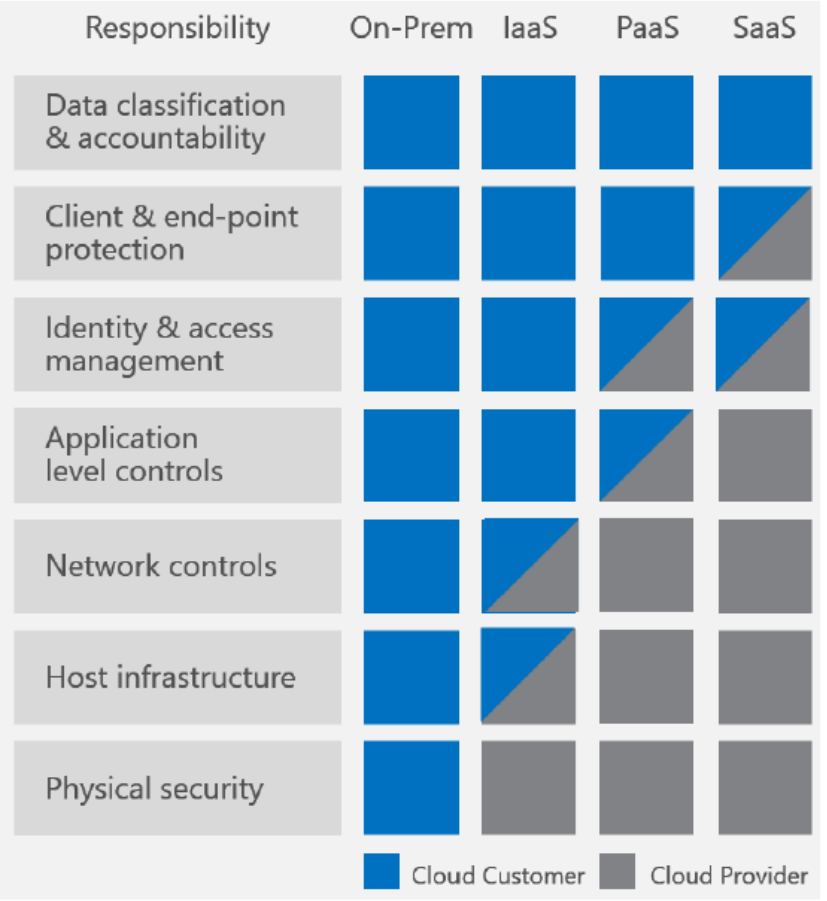
Shared responsibility – general view



Shared responsibility – Microsoft view

- Security centric – focused on security concerns
- Note the breakdown for IAM
- Encryption is in nearly all categories

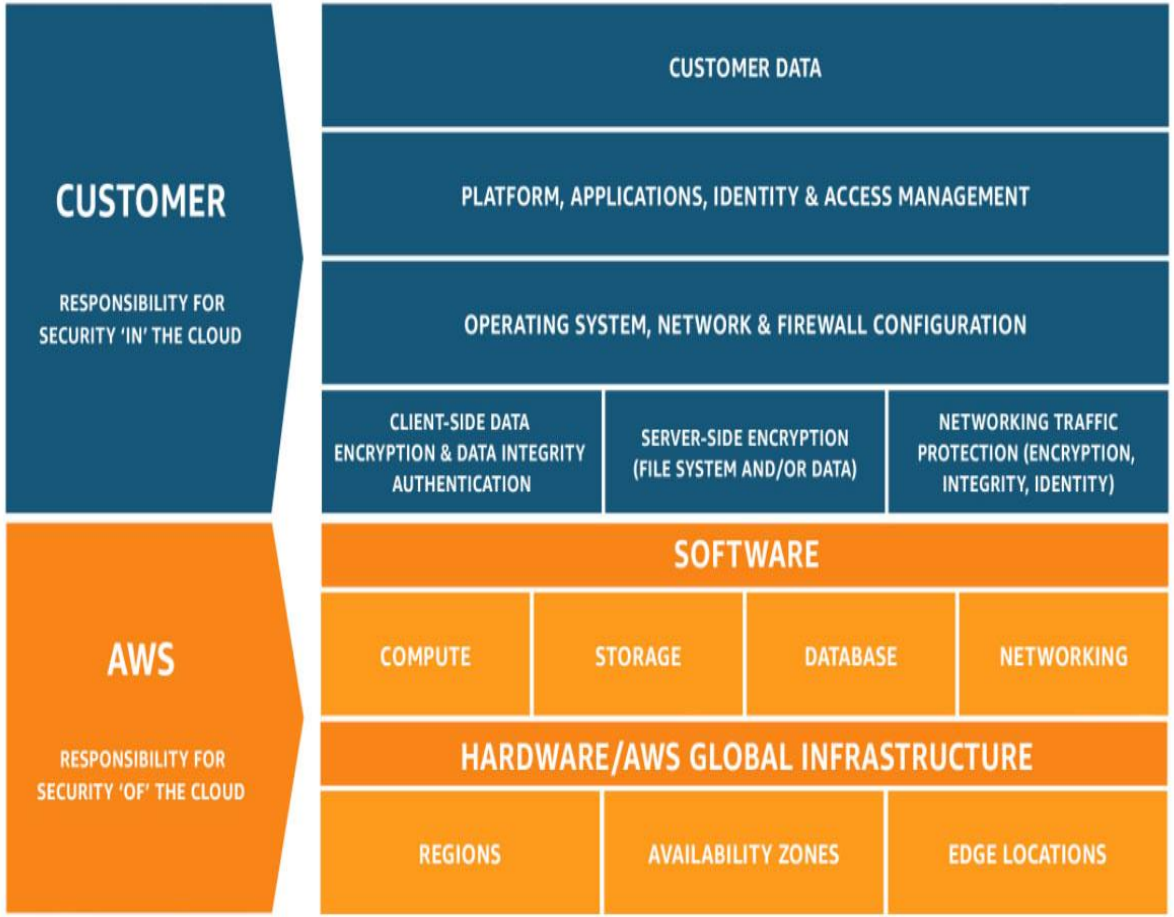
https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/



Shared responsibility – Amazon view

- Not as clean as presented here
  - Some network may be under AWS control
  - Customer can have say in regions
- Calls out encryption explicitly

https://aws.amazon.com/compliance/shared-responsibility-model/



Shared responsibility – significant concerns

- Authentication
  - Mostly your users, your responsibility
  - If SaaS, should be federating
- Encryption
  - In transit, probably your responsibility
  - Your data at rest, your responsibility
  - Separation of customers in the cloud, provider responsibility
  - Encrypting to prevent stealing data on hardware, provider responsibility
- End users
  - Entirely your responsibility
- How users connect and use it
  - Except for SaaS, your responsibility

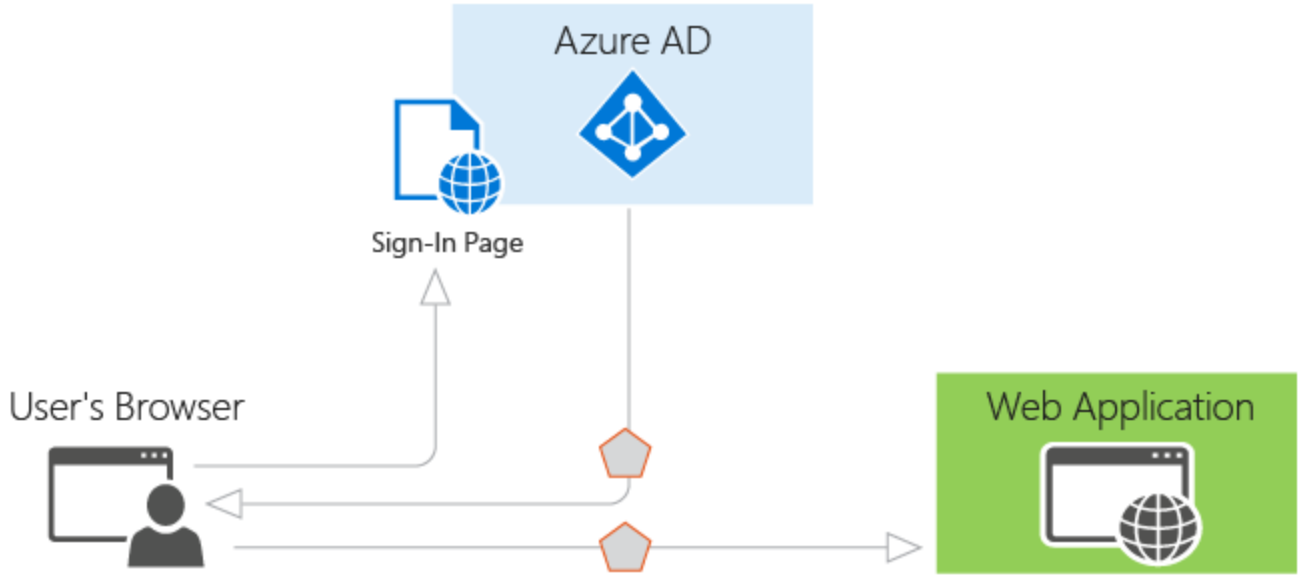
Office 365 authentication

- Every tenant has it's own Azure AD identity, behind the scenes
  - Can use these independently, but requires administration
- Using existing authentication systems
  - Synchronized
    - Two user accounts; internal, Azure AD
    - Can sync passwords, or have separate for internal and Azure AD
    - Two logins
  - Federated – users authenticate against your internal directory
    - One user account, one logon
- Multifactor
  - Physical device
    - By text or call
  - Mobile app
  - Office 365 multifactor is configured in Office 365 Admin Center
  - Can get granular by user or group

avanade

Azure authentication

Basic Scenario – web browser user need access to web app



https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-authentication-scenarios

Azure authentication – tech bits

- Communication between apps and AD are by claims issued and tracked with tokens
- Applications need to be registered in AD
- Single tenant, one directory. Multi tenant, multiple directories
- Uses OAuth 2.0 for authorizing web apps and APIs

avanade

Azure authentication – AD options

- All on-premise AD
  - No cloud authentication
- Integrated with on-premise AD
  - Azure AD Connect
    - Tool for synchronizing on-prem directory with Azure AD
    - DirSync and Azure AD Sync are deprecated
  - Synchronizing users to Azure AD is free
  - Common identity for cloud and on-premise apps
- All Azure AD

Azure authentication – Azure AD Connect

Tool for synchronizing on-prem and Azure

- Sync – makes IDs match
- AD FS – optional, for hybrid environments