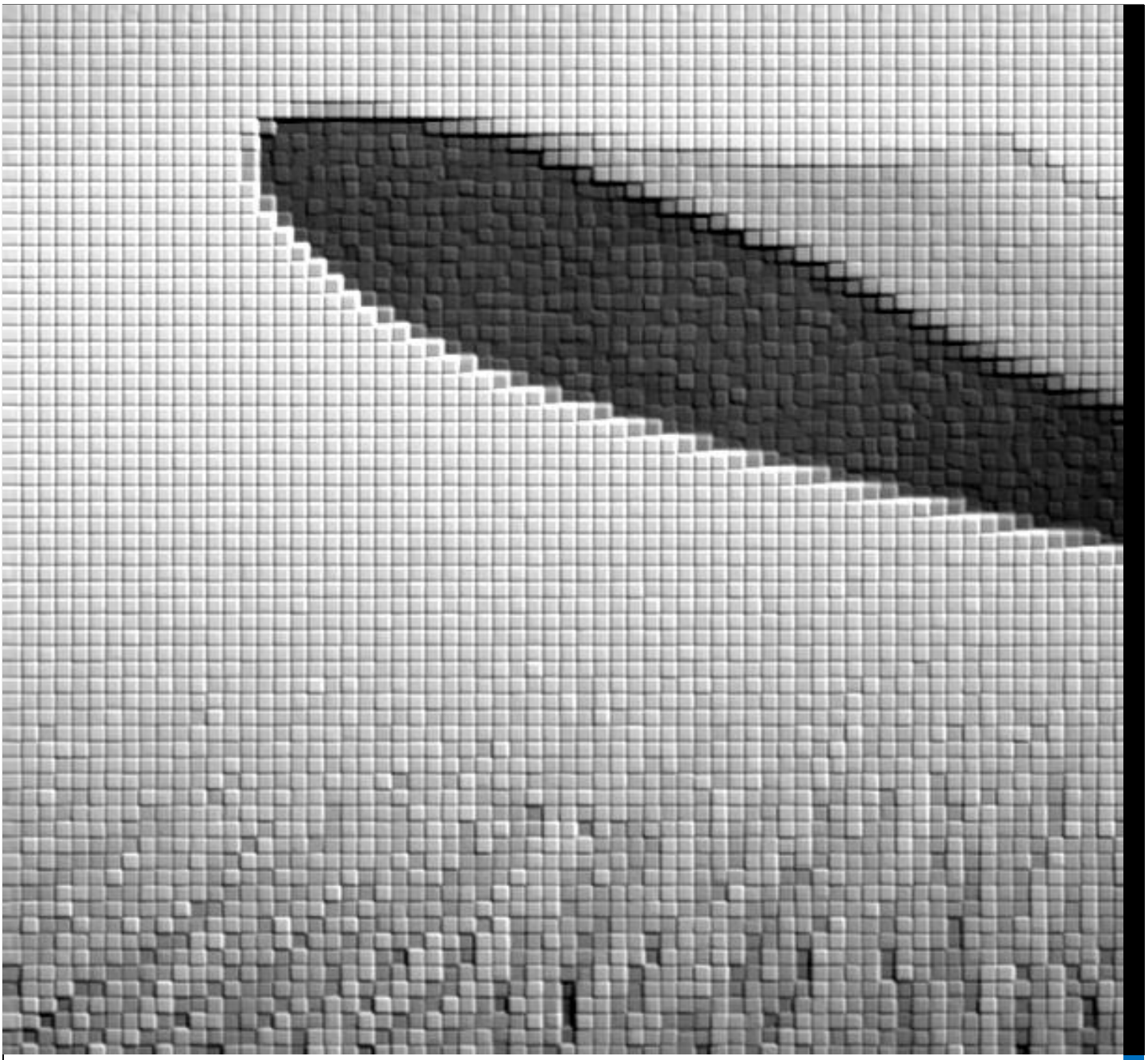

MICROSOFT AZURE SECURITY

A FOCUS ON CLOUD SECURITY SOLUTIONS

This whitepaper focuses on the Microsoft Azure security options to secure cloud deployments with a view for a defense-in-depth cloud strategy. Organizations should consider the technical solutions, which Azure provides, in order to ensure that compliance needs of the business are met appropriately in any Microsoft Azure cloud deployment.

Written by **Tejinder Rai**, Aspire Cloud Solutions Limited, 1st February 2017 rev 1.0

MICROSOFT AZURE SECURITY

A FOCUS ON CLOUD SECURITY SOLUTIONS

Azure Active Directory

Azure Active Directory (AAD) is a key component that is associated to an Azure subscription. AAD can be associated with many Azure subscriptions and provides the authentication mechanism for users to access, manage and deploy resources in an Azure subscription. Essentially AAD has a trust to the Azure subscription and manages the authentication to the subscription through this trust.

The importance of AAD, just like on-premises provides Active Directory Domain Services (ADDS), is fundamental to unlocking the resources and access to your Azure subscription resources. Microsoft Accounts (MSAs), e.g. someone@outlook.com can be added, as can any AAD domain user with someone@aadtenant.onmmicrosoft.com accounts, including user accounts synchronized using AAD Connect from ADDS can be registered within AAD for authentication and authorization. Administrators and Co-Administrators have full control over the subscription and the resources which are deployed into the subscription. The subscription planning model, whether the company is in one country or several countries, needs to ensure subscriptions and the security around subscriptions is organized appropriately to meet security needs.

Organizations must consider who will be registered in AAD, how organizational accounts, from ADDS, will be synchronized with AAD and what roles are suitable for each person who requires access to the subscription to deploy and manage resources. Role Based Access Control (RBAC) should be designed for every Azure subscription deployed for an organization. Security policies should enforce complex passwords and Multi-Factor Authentication (MFA) for any administrative access to anyone who has access to manage Azure subscription resources. These few items help organizations manage how resources are deployed, managed, secured and decommissioned with an effective approach to baselining access to Azure subscriptions.

STARTING WITH AZURE ACTIVE DIRECTORY SECURITY

Azure Active Directory and the subscription model is key to securing access for deployment and management of Azure resources in the Microsoft Azure Cloud. Ensure the correct decisions are made to plan an effective subscription model and Role Based Access Control (RBAC) model.

SUBSCRIPTION ISOLATION

Depending on how the organizational subscriptions are organized, with consideration of Azure subscription scalability, there may be a need to isolate subscriptions based on the risk the business is willing to take on for projects. For example, if your company has a cloud-first strategy, which will likely involve a hybrid architecture, there may still be a need to isolate subscriptions for various reasons. These may include:

- MSDN Subscriptions for developers
- Supplier space for development of new solutions for the business
- Temporary team collaboration areas for testing adhoc solutions
- Testing new features from Microsoft in Public Preview
- Providing Services for public facing business systems

Subscription isolation still needs to be plumbed into the security model and whilst there may not be an immediate need for this, operational and business processes must be aligned to accept that subscription isolation is in fact not a myth but provides a viable opportunity for many circumstances that may arise with your cloud deployments. Ensure that you continue to manage and continually monitor activity for any isolated subscriptions, especially with leaving behind unwanted resources and data.

ISOLATION IS NOT A MYTH BUT A VALID PRACTICE

Subscription isolation provides many benefits and there are likely business needs that this may fulfill. Ensure that security polices and standards are not waived for temporary subscriptions.

AZURE NETWORKING AND SECURITY FUNDAMENTALS

Whilst this paper does not focus on network fundamentals, it is important to consider the network challenges and mitigations that need to be taken into consideration for the following purposes:

- Within the Azure subscription resources
- On-Premises to Azure resources
- From the Internet to Azure resources
- Inbound and outbound activity from resources in Azure (IaaS or PaaS services)

Depending on the connectivity model, to the azure resources, you must consider that you effectively follow an assume-breach approach. Microsoft follow this approach for securing the Azure data centers in all the regions across the world. Any data that flows from an external source into Azure, within Azure or from Azure to/from any on-premises or internet facing service must be secured using industry standard protocols and encryption.

Microsoft secure all API's to either access an Azure PaaS service e.g. using storage APIs or Azure Service Bus and any access to perform administrative functions with the Azure Service Management REST APIs. Customers have the power to design their own services, but it is inherently very simple to expose an endpoint or transfer data which is not achieved using a secure mechanism.

The key consideration here is to design services and endpoints, networks and resources with encryption in mind at all times. Any traffic that flows in and out of the Azure subscription must conform to security standards which adhere to industry best practices for the confidentiality, integrity and availability (CIA) of data flows and resources to ensure traffic on the wire is secured within and outside of the subscription.

UNPLUGGED = SECURE?

How you secure your network and managing the traffic that flows to and out of your Azure subscriptions is fundamental to your security design.

APPLYING BASIC NETWORK SECURITY FUNDAMENTALS

Half of the controls and security around Software Defined Networking (SDN) within Azure is managed by Microsoft. Customers do not need to be concerned about how Microsoft secures the cloud, it is more in the use of what is implemented that needs to be addressed. The customer crosses a boundary on responsibilities based upon the cloud services being provisioned in either IaaS, PaaS or SaaS. The Microsoft Incident Response and Shared Responsibilities for cloud computing whitepaper discusses the crossover in detail.

Virtual Networks (VNets) need to be planned accordingly as these provide a layer of isolation between the deployed resources across VNets. Two Azure VNets are completely provide isolation from each other, until the VNets are peered or connected using VPN gateways. VNets can be connected to on-premises networks using either Site-to-Site (S2S) VPN, Point-to-Site (P2S) VPN or an ExpressRoute circuit. When VNets are connected to each other or to an on-premises environment traffic will flow freely between the networks unless security controls are enforced. VNet planning is a core networking design challenge that companies face when designing their networks in the Azure cloud.

Network Virtual Appliances

Network Virtual Appliances (NVAs) can be used at each end of the VPN tunnel to manage the inbound and outbound traffic flows to ensure that only the required traffic is permitted. NVAs can also be used to control traffic between VNet to VNet connections with VPN Gateways or by using the VNet peering model. NVAs can be used in association with User Defined Routes (UDRs) to ensure that subnet to subnet to VNet traffic can be controlled via an NVA. Access to the internet from IaaS workloads also needs to be secured using this approach.

Network Security Groups

Network Security Groups (NSGs) can be used for filtering traffic and applied to either Virtual Machines or subnets within VNets. NSGs can be used in conjunction with NVAs to further filter traffic between subnets that may not be destined for a route using a UDR. These are very useful for traffic flows to and from virtual machines and load balancers or between virtual machines in the same subnet. The NSG rules can be managed in Azure Resource Manager (ARM) templates also.

NETWORK SECURITY

Anything in the clear has a potential to be compromised. Use strict controls and practices to create private conversations and limit the endpoint communication.

VIRTUAL MACHINE HARDENING

With strict ADDS group policies, flexible policies can be applied to virtual machines, including the new datacenter firewall feature available in Windows Server 2016. Ensure that the types of roles each server provides on the VNet has an appropriate security policy applied by group policy as this will be applied periodically by the domain controllers.

The Windows firewall should never be turned off. The relevant features which are enabled in Windows Server enable various firewall rules to ensure the appropriate ports and processes can communicate to and out of the host.

An appropriate monitoring solution should be in place to ensure the virtual machine stays in a compliant state, with future patching and policy updates throughout the lifecycle of the virtual machine.

Azure Security Center

The Azure Security Center is a key component to assist you with detection, prevention and visibility to assist you in developing and managing your security controls.

POLICIES AND STATE

The state and baseline of all virtual machines should be known and comply with the controls that are enforced.

Azure Security Center to the rescue!

DATA AT REST

Until now I have discussed data in transit and securing connectivity between hosts and networks. Data at rest should be compliant to the business policies for the data that is held within any system. Whilst the data evolves, through operating units within the business functions, there can be situations where it may be unknown where the data resides and if the data at rest should actually be present in the location where it is placed. Data and information leakage is a top concern for companies and even though companies do as much as they can to control where the data resides, it is still possible to have information leakage if it is not controlled or liability is not passed to the party who receives the information and discards of the information as per the guidelines policies state. This is a known fact.

Follow the steps below to ensure you have a robust security approach to securing data at rest.

Consider Azure Drive Encryption

Enable Transparent Data Encryption on SQL Server databases

Consider KeyVault to lock away your secrets

Consider Azure Storage Service Encryption

DATA ENCRYPTION

Data encryption is key to ensuring that you are safe guarding your data appropriately. Utilize all possible options Microsoft provide.

MALICIOUS SOFTWARE

Malicious software needs to be detected, quarantined, removed safely and logged and notified in any security solution. Microsoft provide a solution called Microsoft Antimalware for Azure Cloud Services and Virtual Machines. Unless you have an existing solution you wish to implemented, this should be considered as a standard practice in any cloud deployment scenario for ensuring that the integrity of your systems are held in place.

Should you find a breach, don't assume that the problem has gone away. Any breach requires a security response and investigation into the occurrence with a view to find the source of the underlying problem. The extent of information leakage also needs to be considered, or possibly the event of information removal.

COMPLIANCE: STAY INFORMED

Malicious software

- Detect
- Log
- Notify
- Quarantine
- Removal
- Investigation
- Security Review

MONITORING & COMPLIANCE

Monitoring the services in your Azure subscription is key to understanding your services are operating as expected. This will need to cover the following scenarios.

- Operating environment event logs
- Diagnostic logs
- Application logs
- Network threat logs
- Security monitoring

Microsoft provide the Operational Management Suite (OMS) to support the above needs and this should be considered for any cloud deployment. If you have an existing System Center Operations Manager (SCOM) implementation, it is well suited to integration with the OMS suite.

Security and compliance is built into the OMS suite and plays a key role in your cloud deployments.

UP / DOWN?

Establish a clear monitoring strategy.

CLOSING THOUGHTS

This whitepaper was written to introduce some of the security options available in Microsoft Azure, to introduce how customers could utilize complimentary Microsoft services and products for a successful secure cloud deployment.

The planning and implementation of a cloud deployment requires distinct focus on several aspects before any deployment of a single service leveraged in Microsoft Azure.

Tejinder Rai
Microsoft Certified Azure Solutions Architect
Aspire Cloud Solutions Limited

THANK YOU