Architecting secure cloud infrastructure on Azure

WHITE PAPER

MICROLAND®

WHITEPAPER

Architecting secure cloud infrastructure on Azure

Abstract

The global cloud IT market currently accounts for 42.8% [1] of the total IT spending (based on an estimate by IDC) and is set to hit $390 billion in revenues by 2020 (according to a study by Bain & Company)[2]. Cloud has revolutionized the world of IT and we are just beginning to scratch the surface. The proliferation of cloud infrastructure comes with its own share of challenges – and one of the most pressing concerns is that of security. A spending projection of $105 billion[3] on security technology by 2020 underscores the magnitude of the threat.

Bruce Schneier, well-known security guru has rightly said, "Security is a process and not a product" – because it is not a one-time effort but a continuous endeavor to keep threats at bay and secure the enterprise. This is especially true as attacks become more sophisticated and capable of wreaking unprecedented damage. In this whitepaper, we will outline steps that organizations must take while designing their security policies and sketch a secured reference architecture on Microsoft Azure to better understand how to protect and secure your cloud infrastructure.

[1] The global cloud IT market currently accounts for 42.8% of the total IT spending, https://www.idc.com/getdoc.jsp?containerId=prUS43508918

[2] According to a study by Bain & Company IT spending is set to hit $390 billion in revenues by 2020, http://www.bain.com/publications/articles/the-changing-faces-of-the-cloud.aspx

[3] A spending projection of $105 billion on security technology by 2020 underscores the magnitude of the threat, https://www.idc.com/getdoc.jsp?containerId=prUS42425417

Introduction

Cloud technology has been one of the key disruptors to shape the IT landscape in recent years. With the cloud, the C-suite has been able to slash huge expenditures on setting up private data centers. Cloud enables enterprises to scale up or down based on their need, implement advanced analytics, and pay only for what's been used. This has in turn enabled them to channel precious resources on development, minimize risks of managing mammoth data architecture, and boost the bottom line.

IDC's 'Worldwide Cloud 2016 Predictions' report estimates cloud spending to be over 50 percent of total IT spending in 2018 and growing at 4.5 times the rate of IT spending since 2009. This figure is expected to increase to more than six times by 2020. Bain & Company, in their 2017 'The Changing Faces of the Cloud'[4] report predict that cloud revenue will increase to $390B in 2020 with 17 percent compounded annual growth rate.

The importance of cloud security

The advent of the public cloud comes with its own challenges – increasing attacks from malicious sources and the unprecedented sophistication with which the attacks are executed. Along with the external attacks, corporations need to be wary of internal breaches, too. People inside the company have elevated privileges and thus have more potential to do greater damage. Providing superfluous access to malicious/ignorant insiders and trusting all the internal traffic can lead to devastating consequences. Most of the time, organizations don't even realize that someone is illegitimately accessing their data.

The ensuing cost of data breach can have serious ramifications on the company – the cost can be in the form of money spent to contain the breach, penalties paid to the government, ransom paid to the attacker, business impact, legal fee, technology upgrades, and so on. Finally, the time it takes to contain the breach after it has been identified has to be minimum so that the damage can be minimized, and enterprises can resume their regular processes and can re-establish their credibility in the market.

With cloud becoming the norm, more and more data is being transferred over public as well as private network which needs to be secured. This calls for a change in the approach to data security. Bruce Schneier, well-known security guru has rightly said, "Security is a process and not a product"[5] – because it is not a one-time effort but a continuous endeavor to keep threats at bay and secure the enterprise.

[4] The Changing Faces of the Cloud, http://www.bain.com/publications/articles/the-changing-faces-of-the-cloud.aspx
[5] Security is a process and not a product, https://www.schneier.com/essays/archives/2003/07/the_speed_of_securit.html

However, it is important to keep in mind that there should not be so many layers of security that it becomes difficult to operate and productivity is hampered. We've to find a sweet spot – the perfect balance between security and operability.

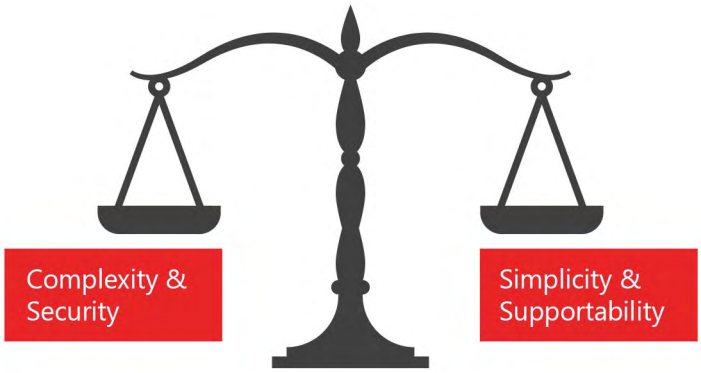
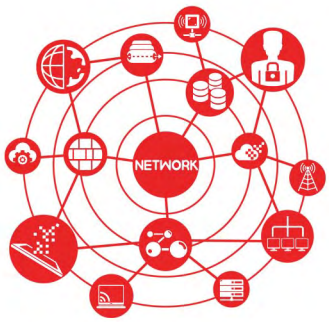


Figure 1: Maintaining a balance between security and operability is crucial

In this whitepaper, we will explore the various levels of security that organizations must set up for a secure cloud system. We will also look at the security functionality offered by Microsoft Azure, one of the leading cloud infrastructure service providers. Lastly, by combining these functionalities, we will create a reference architecture that can be used by organizations to secure and protect the cloud infrastructure.

Security planes

Before we understand how to create a secure infrastructure, we need to understand the several aspects of an infrastructure that needs to be secured in the first place. Security can be segregated primarily into three planes. They are 1) network plane, 2) data plane and 3) management plane. Let's see what these planes consist of and what Azure offers to secure each of them.



Network

Data

Management

Figure 2: The three security planes

MICROLAND®

1. Network plane

Networks are the lifelines through which data travels. And this lifeline can be vulnerable to attacks even without the presence of any physical intrusion. There is a plethora of Microsoft Azure offerings that can be utilized to make organization's cloud infra invincible. Figure 2 illustrates some of the offerings.

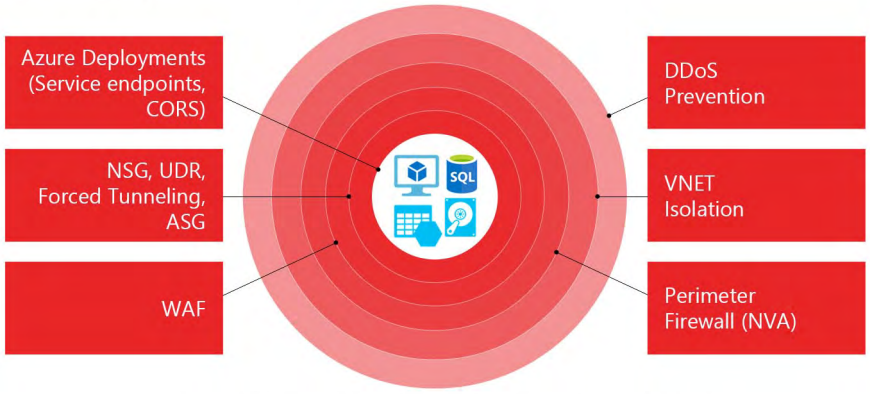


Figure 3: Azure offerings to secure the network plane

All these services provide different layers of network security that the traffic must clear to reach Azure deployments. While these layers of security protect the traffic inside the Azure network, what about the security of traffic between on-premises/employees outside office network and Azure network? These can be ensured through two options:

1. **Virtual Private Network Connection:** Securely sending data over internet using a VPN tunnel

2. **Express route:** A private connection between your on-premises network and Microsoft backbone network facilitated by a connectivity provider

2. Data plane

Security at this plane can be enhanced by keeping data at a safe place and enabling encryption when data is at rest as well as when it is travelling through the network.

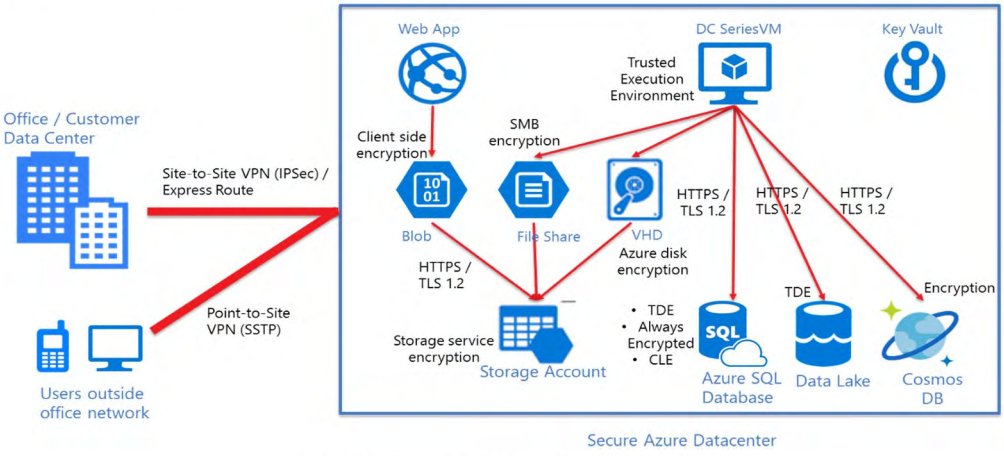


Figure 4: Various levels of data encryption

a) Encryption at-rest involves encrypting data on persistent storage. This can be through client-side or server-side encryption.

1. **Client-side encryption:** Encrypting data (blobs, tables, queues) using application (Azure service application or app running in customer data center) before sending it to the resource provider.

2. **Server-side encryption:** This can be done in two ways:
   - Service managed keys: Microsoft manages the keys. For some of the services, it's already available whereas for others, we've to opt for it.
   - Customer managed keys: Customer manages their keys either using Azure key vault or their own hardware.

b) Encryption in-transit involves protecting data as it moves through public or private networks. This can be done through the following mechanisms:

1. **Transport Layer Security (TLS):** Any requests made to Azure SQL database, data lake, Cosmos DB, data warehouse or any other cloud services are made using HTTPS protocol in which data is encrypted using TLS 1.2 protocol with 2048-bit RSA/SHA256 encryption keys thus securing data in motion. For Azure storage, we can enable only HTTPS traffic to interact with the storage account. Traffic between two peered virtual networks (VNets) also follow TLS protocol. Not just that, RDP sessions to VMs can also be secured using TLS.

2. **SMB Encryption:** To secure access to file shares by SMB 3 clients, SMB encryption can be enabled.

3. **SSH:** Secure log-in to Linux VMs using asymmetric keys.

4. **VPN:** Data encryption in a secure tunnel when interacting with on-premises network/ employees accessing cloud services outside office.

5. **Confidential Computing:** To secure the data while it is in processor cache by running code in Trusted Execution Environment (TEE).

6. **Azure Key Vaults** helps users to manage and store their own encryption keys, storage account keys. PFX files (e.g. TLS certificates) and passwords; access to which is given using Azure Active Directory. It also supports **Shared Access Signatures** (SAS), which are strings containing security token attached to Unique Resource Identifier (URI) and are used to give access to storage services for a limited period.

3. Management plane

Managing the cloud environment in terms of access control, threat detection, and prevention is crucial. An ideal cloud ecosystem is the one with least privilege access restriction i.e., minimal access given to relevant people for a fixed time. Also, if the environment is under attack, corrective actions should be taken automatically while notifying the user regarding the same along with recommendations to enhance security. Microsoft offers Azure AD and Azure Security Center.

a) **Azure AD:** It helps us in identity management and giving Role-Based Access Control (**RBAC**) to users, groups or applications on subscription, resource group (multiple resources grouped together) or individual resource level. Azure AD protects the cloud infrastructure using advanced mechanisms such as **privileged identity management, identity protection, and conditional access and reporting.**

b) **Azure Security Center:** This is a one-stop-solution for all security issues for public, private as well as hybrid cloud. With Azure Security Center, we can set **security policies, service based and geography-based restrictions** for all deployments, verifying compliance, raising alerts in case of anomalies, and pushing them back to compliance. Through Azure Security Center, we can also collect logs, raise alerts, and automate remedial actions by allowing users to set up security playbooks in case of specific trigger alerts.

Reference architecture for a secure cloud

Let us now look at a reference architecture keeping in mind things we have discussed so far. This reference architecture has also been made while considering security, scalability of design, governance and compliance and can be modified according to the needs of the enterprise.

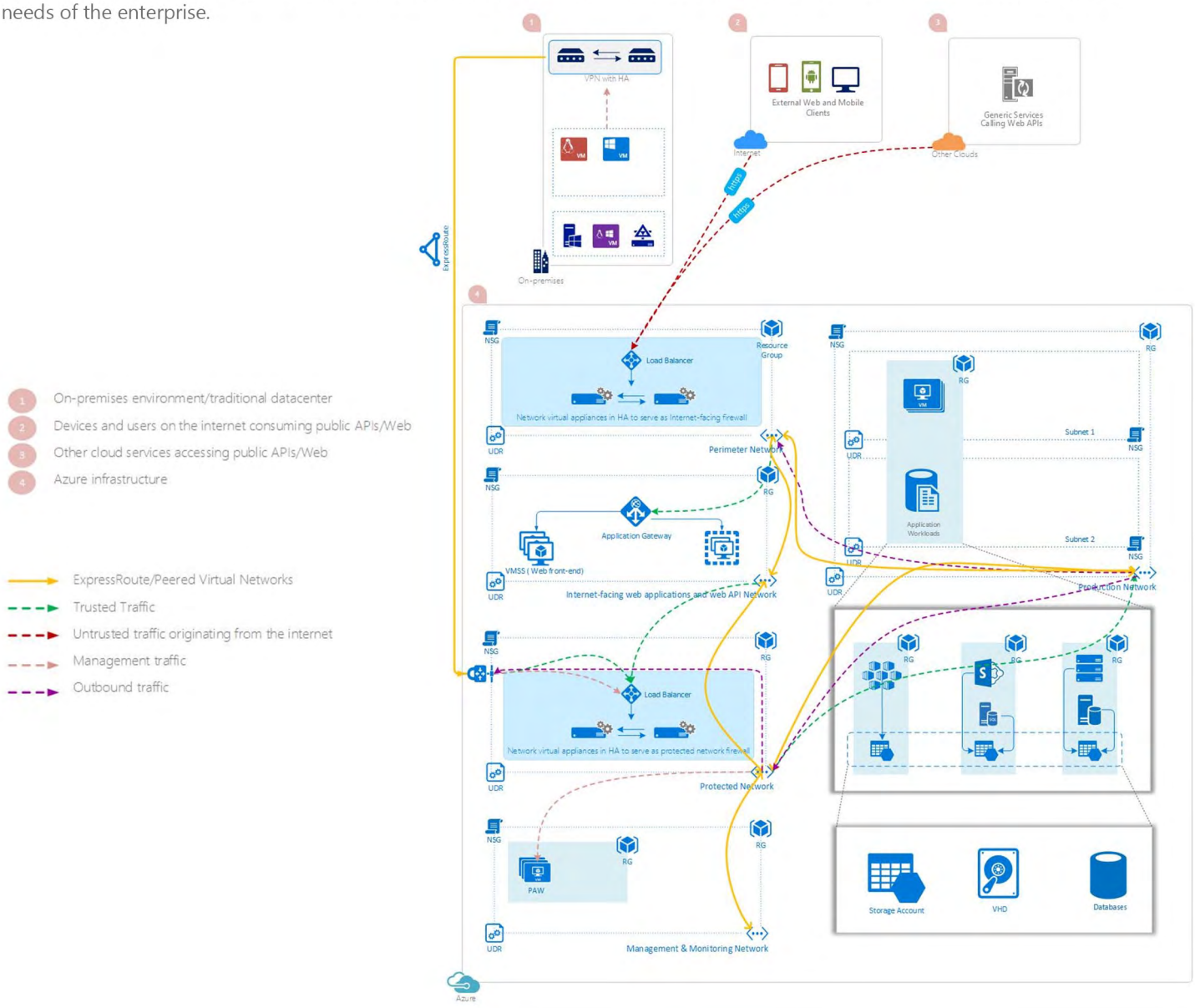


Figure 5: Reference Architecture for a Secure Cloud

MICROLAND®

Let's break down the reference architecture to understand its individual components:

Virtual networks: The Azure resources are grouped together according to their functionality, the kind of traffic they handle, and the administrative access given to them. Resources in every group have their own separate virtual networks (VNets).

Traffic flow: Defense in depth mechanism is applied to ensure that only secure and legitimate traffic is allowed inside the network. As discussed earlier, VNets are completely isolated. To connect two VNets and allow traffic flow via Azure backbone network, they need to be peered. In this scenario, perimeter network peered only with internet facing web app network which in turn is peered with protected network (to send requests) and production network (to receive response). The management network and the production network are also peered with protected network.

Data encryption: The encryption mechanisms at rest and in-transit discussed earlier apply here. Both client-side and server-side encryptions should be enabled with their keys stored in Azure key vault. To avoid any human error, it is suggested to use Microsoft managed keys in as many services as possible.

Administration: Segregation of access is very important to avoid any abuse of administrative powers. Any combination of these roles should never be assigned to any one person and the least privilege access restriction should be enforced in privileged access management. Securing high impact privileged accounts and tasks such as IT administrative roles and sensitive business functions from attacks such as phishing, pass-the-hash, pass-the-ticket, and keystroke logging is extremely critical.

Authentication: Along with the usual password, multi-factor authentication must be enforced for administrative accounts. It can be through a voice call, app push, SMS, and so on. Additionally, instead of giving the key to the storage account, SAS tokens should be given to access any storage service.

Threat detection and prevention: Services such as Azure Security Center, Azure AD Privileged Identity Management, and Azure Operations Management Suite can be used to keep a close eye on cloud infrastructure and manage the resources. These will help us in making the infrastructure more secure by continuously checking for security vulnerabilities, giving recommendations, detecting threats using advanced threat intelligence, raising alerts, and taking actions automatically.

Governance: All the resources can be tagged under the business units/projects for show back/ chargeback purposes. Subscription level spend can also be monitored and limited.

Conclusion

Cloud services are undeniably the future of computing. However, it comes with its share of risks and vulnerabilities. Security technology has risen to meet these challenges and mitigate the threat of attacks – both from external and internal sources. Through this whitepaper, we have answered critical aspects of securing and protecting data on the cloud infrastructure. We have also illustrated the various offerings of Microsoft Azure to enable enterprises to effectively secure their cloud. The framework of reference architecture can help organization identify how they can use Azure's offerings to secure their cloud as they surge into the next-generation of IT.

About the author

Akanksha Sharma
Architect, Microland

Akanksha is an Architect at Microland. She is a part of the automation team and is actively architecting and building NextGen solutions using cutting edge technologies. Akanksha works closely with multiple stakeholders to build solutions and products that drive business efficiency and productivity for enterprises. She has also presented technology solutions in multiple global events including Global Azure Bootcamp. She holds an engineering degree in Chemical Engineering from IIT Guwahati.

For further information
Contact us at: **+1 646-254-3598** or Email us at : **info@microland.com**

About Microland

Microland accelerates the digital transformation journey for global enterprises enabling them to deliver high-value business outcomes and superior customer experience. Headquartered in Bangalore, India, Microland has more than 4,100 professionals across its offices in Australia, Europe, India, Middle East and North America. Microland partners with global enterprises to help them become more agile and innovative by integrating emerging technologies and applying automation, analytics and predictive intelligence to business processes.

© 2019 Microland Limited

Learn more about us at:

www.microland.com