

Security Assessment Case Study – Azure

• Problem

- The Customer knew there were gaps in security configuration cross their various workloads but were unsure where to start and what things were the most critical to focus on first.
- Currently there were no common patterns were defined for analysis and assessment of workloads for security standards that they were having trouble defining.
- They wanted to ensure new workloads and critical data was secure and easily managed by moving to an Infrastructure as Code deployment model.

• Solution

- Spyglass provided a review of their Azure environment for security best practice configuration and patterns for their cloud architecture as well as configuration of workloads that are deployed.
- Reviewed and discussed moving to Infrastructure as Code deployment module to improve security and standardization and how to evolve practices over time.

• Benefits

- The Customer received a breakdown of most important recommendations rated on risk based analysis.
- Detailed recommendations which contained actionable items to jumpstart remediation and given a roadmap for planning purposes.

Roadmap of Prioritized Findings - Immediate

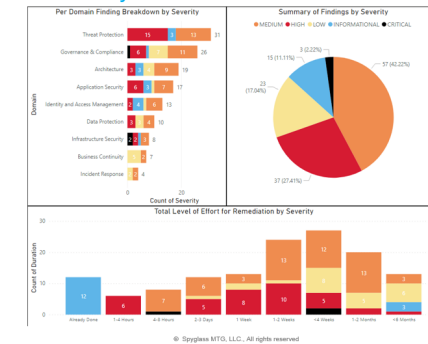
Severity	Capability/Solution	Sub-Topic	Recommended Setting(s)	Risk Owner	Domain
CRITICAL	Public IP	How are public IPs managed?	Public IPs should never be assigned to VMs and more commonly used on load balancers. Having a public IP assigned to a VM means that VM is accessible from anywhere on the internet. This can be secured by NSGs but as a best practice, public IP usage should be limited to application access only and should also route through some type of firewall appliance first. It is very important to limit access to the SA plane so that only a small set of people have the rights to create/delete subscriptions.	Azure Admin	Infrastructure Security
CRITICAL	Subscriptions	Who has access to manage subscriptions?	VM management needs to be strictly controlled and made available via internal network. Azure Bastion or Defender for Cloud. Remote management through public IP should be limited to only when necessary.	Azure Admin	Governance & Compliance
CRITICAL	VM Remote Management	How are VMs managed remotely?	VM management needs to be strictly controlled and made available via internal network. Azure Bastion or Defender for Cloud. Remote management through public IP should be limited to only when necessary.	Azure Admin	Infrastructure Security
HIGH	DevOps Infrastructure	What accounts are used in your DevOps Infrastructure?	Access to DevOps tools should require SSO migration, centralized access control management, usage of PIM to elevate to privileged roles and/or look to more access to privileged accounts.	DevOps Admin	Application Security
HIGH	DevOps Infrastructure	Do teams use consistent tools?	Consolidate the number tools that are used to as few as are needed so that environments are easier to manage, track and secure.	DevOps Admin	Application Security
HIGH	Management Groups	How are you using management groups?	Management groups are important configurations that allow for access controls and policies to be applied through inheritance to subscriptions within your environment.	Azure Admin	Governance & Compliance
HIGH	Network Architecture	How will cloud stands be managed?	All networks should be managed to ensure as deployed VMs are secured and audited correctly. Cloud stands can be more secure than hybrid connected networks if they are secured correctly.	Network Admin	Architecture
HIGH	Network Architecture	How is internet inbound traffic handled?	Inbound traffic should be sent through a Firewall Appliance, whether a third party appliance or Azure Firewall. Public IPs directly assigned to virtual machines should be limited and rarely used given the security issues that can arise from that configuration.	Network Admin	Architecture
HIGH	Peer Review	What is in place for peer reviews?	Peer reviews should be standard on all pull requests.	DevOps Admin	Application Security
HIGH	Resource Tagging	What is in place for tagging standards?	It is important to have resources tagged so that the meta data can be used in reporting, governance, performing actions, leading to issues, etc.	Azure Admin	Governance & Compliance

14

© Spyglass MTG, LLC. All rights reserved



Security Domain Summary



4

© Spyglass MTG, LLC. All rights reserved

