Governing Your Azure Workloads

By: Jonathan Trull January 21, 2020

Disclaimer

Intro

Common attacks against cloud resources include accessing service endpoints exposed to the Internet, brute forcing weak passwords, re-using stolen credentials, and access to exposed data storage containers. The root cause leading to the success of these attacks is typically misconfigurations in the deployment and operation of cloud workloads. Although public clouds present unique challenges to security teams, Azure comes with several tools that can help prevent such attacks from occurring.

Built-in Policy Enforcement to Prevent Misconfigurations

Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources so that you can maintain compliance with corporate policies. All data stored by Azure Policy is encrypted at rest.

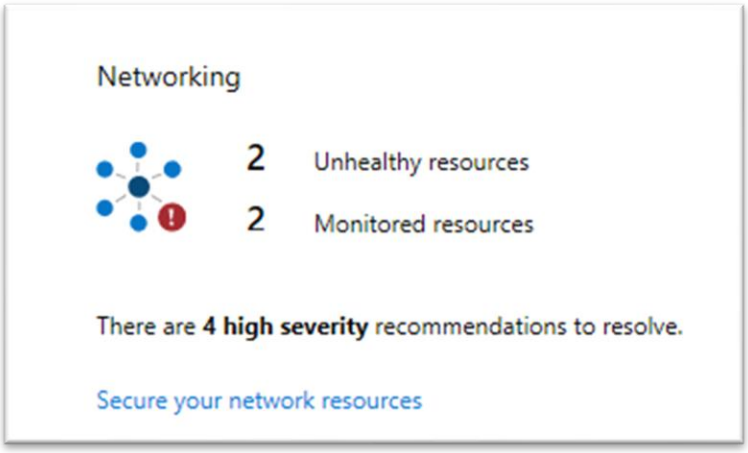
To leverage the power of Azure Policy, you need to create a policy definition and then assign that policy with a specific scope. This scope could range from a management group to a resource group and would be inherited by all child resources. This allows you to establish global policies across all Azure subscriptions and resource groups or to a smaller subset.

To prevent the misconfigurations mentioned earlier, a good approach would be to enforce the use of a Network Security Group that has been developed by your organization's security team. An example of such a policy can be found at https://docs.microsoft.com/en-us/azure/governance/policy/samples/nsg-on-subnet. Within the policy definition, you specify the

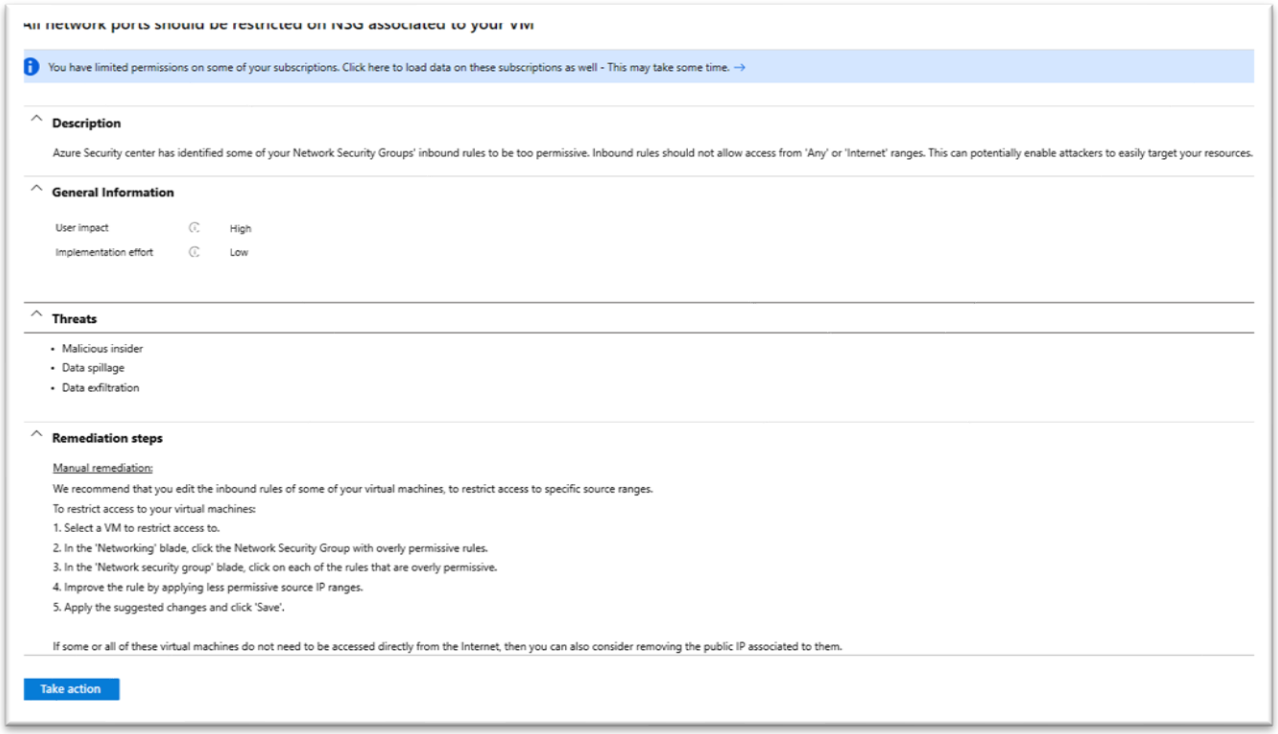
ID of the network security group to use. You can also create policies that required the use of approved Virtual Networks and Subnets that have been configured, tested, and approved by your security organization.

Global Monitoring and Alerting of Potential Security Misconfigurations

Azure also includes services that can provide security teams with real-time information about configurations and changes to configurations that either violate corporate policy or could indicate a potential vulnerability. Specifically, Azure Security Center includes the ability to strengthen your security posture. This includes managing and enforcing security policies over Azure resources and alerting and visibility over network security issues. For example, the following Azure Security Center dashboard shows the unhealthy networking issues related to Azure workloads:



By clicking on this network map, you are provided with the specific recommendations related to the 4 high severity issues that have been identified by Azure Security Center. One of the most urgent recommendations to address is listed below and relates to unrestricted service endpoints that are exposed to the Internet.



You can learn more about the capabilities of Azure Security Center at https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

In addition to Azure Security Center, you can leverage Azure Activity Logs to monitor changes that are made to the Azure management plane. For example, you can monitor changes made to Network Security Groups so that security team members can follow-up to determine if the change created a security weakness in the new configuration. Below is an example of the activity logs related to a Network Security Group protecting Azure resources.

Operation name	Status	Time	Time stamp
Create or Update Security Rule	Succeeded	21 h ago	Thu Jan 16 ...
Create or Update Security Rule	Started	21 h ago	Thu Jan 16 ...
Create or Update Security Rule	Succeeded	2 d ago	Wed Jan 15 ...
Create or Update Security Rule	Started	2 d ago	Wed Jan 15 ...
Create or Update Security Rule	Accepted	2 d ago	Wed Jan 15 ...
Create or Update Network Security Group	Succeeded	2 d ago	Tue Jan 14 ...
Create or Update Network Security Group	Started	2 d ago	Tue Jan 14 ...
Create or Update Network Security Group	Accepted	2 d ago	Tue Jan 14 ...
Create or Update Network Security Group	Succeeded	2 d ago	Tue Jan 14 ...

These logs can be streamed to Azure Log Analytics or another third-party log system for analysis and reporting.

You can find more details about configuring and using Azure Activity Logs at https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-monitor-azure-resource