IMPROVING AZURE SECURITY POSTURE USING RESOURCE SECURITY HYGIENE

5/21/2020
Summary of experience

• AWS, Azure, and Microsoft 365
• Data Loss Prevention
• Azure Information Protection
• Endpoint Security

Professional affiliations and credentials

• Microsoft 365 Security Administrator

Education

• BS, Business Administration, Lewis University
Summary of experience

• Defense Focused
• Network Architecture
• Logging and SIEM
• Various Controls and Framework Assessments
• Incident Response

Professional affiliations and credentials

• GIAC Security Expert (GSE) #82

Education

• MS, Information Security Engineering, SANS Technology Institute
• BS, Information Systems, Baldwin-Wallace University
Today’s Agenda

• Cloud Security Stats
• Azure Security Hygiene
• Azure Secure Score
• Azure Security Policies
• Demo
• Q & A
Cloud Security Stats

• According to a survey of Cybersecurity Insiders’ 400,000 information security community members:
  - 64% are concerned with Data Loss and Leakage via the cloud
  - 42% are concerned with insecure APIs and access interfaces
  - 33% are concerned that their SOC does not offer full visibility into the cloud

WHAT IS SECURITY HYGIENE

How organizations are managing security posture in Azure Today
Security Hygiene

- Simple grouping of Azure services to focus on security
- Identifies affected resources
- Provides recommendations
- Directs the admin to remediation steps
WHAT IS SECURE SCORE

Microsoft’s measurement of security posture
Example Secure Score

Overall Secure Score

340 OF 625

Secure Score by category

- 65 / 180 Compute & apps resources
- 50 / 90 Data & storage resources
- 90 / 140 Networking resources
- 135 / 215 Identity & access resources
# Example Recommendations

## Compute

### Add Servers

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Secure Score Impact</th>
<th>Failed Resources</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediate vulnerabilities found on your virtual machines (powered by Qualys) (Preview)</td>
<td>&lt;30</td>
<td>1 of 1 virtual machines</td>
<td></td>
</tr>
</tbody>
</table>
Secure Score Calculations

- Nightly process collects telemetry from workloads
- Ignore and third party information is stored in another location
- Reviewing report data is anonymized and stored separately

Data sources:
- SharePoint
- Exchange
- OneDrive
- Azure Active Directory
- Azure Information Protection
- Microsoft Cloud App Security
- Windows Defender Advanced Threat Protection
- Azure Advanced Threat Protection
AZURE SECURITY POLICIES
Azure Security Policies Types

- Built-in Default from Security Center
- Custom Policies
- Regulatory Compliance Policies
Azure Custom Security Policy

Initiative definition
New initiative definition

BASICS
Definition location *
Azure subscription 1

Name *
NGFW Required

Description
All Internet traffic should be protected by Azure NGFW

Category
Create new

Security Center

[Preview]: All Internet traffic should be routed via your deployed Azure Firewall

[Add]

Details
Definition

Description
Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall

Effect
[parameters[effect]]

Type
Built-in

Mode
All

Category
Network

Definition location --

Definition ID
/providers/Microsoft.Authorization/policyDefinitions/f5e4035e-d5d4-4532-b035-c0448d374b3c

Parameters
Name
[Preview]: Effect

Type
String

Default Value
Audit/NotExists

Allowed Values
Audit/NotExists, Disabled
Azure Compliance – PCI CIS ISO

- Built in functions to help your organization become compliant
### Additional Compliance Standards

**Add regulatory compliance standards**

Click **Add** on the standards that you want to add to the regulatory compliance dashboard and then assign it to the subscription. After completing the assignment, the custom policies will be available in the **Regulatory compliance** dashboard.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Add</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST SP 800-53 R4</td>
<td>Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a recommended set of policies and ...</td>
<td>Add</td>
</tr>
<tr>
<td>UK OFFICIAL and UK NHS</td>
<td>Track UK OFFICIAL and UK NHS controls in the Compliance Dashboard, based on a recommended set of polici...</td>
<td>Add</td>
</tr>
<tr>
<td>Canada Federal PBMM</td>
<td>Track Canada Federal PBMM controls in the Compliance Dashboard, based on a recommended set of policies a...</td>
<td>Add</td>
</tr>
<tr>
<td>Azure CIS 1.1.0 (New)</td>
<td>Track Azure CIS 1.1.0 (New) controls in the Compliance Dashboard, based on a recommended set of policies an...</td>
<td>Add</td>
</tr>
<tr>
<td>Azure Security Benchmark</td>
<td>Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies ...</td>
<td>Add</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Track HIPAA controls in the Compliance Dashboard, based on a recommended set of policies and assessments.</td>
<td>Add</td>
</tr>
<tr>
<td>SWIFT CSP CSCF v2020</td>
<td>Track SWIFT CSP CSCF v2020 controls in the Compliance Dashboard, based on a recommended set of policies ...</td>
<td>Add</td>
</tr>
</tbody>
</table>
Azure Cloud Compliance

- Bit more complex
- Available standards can be enabled
- Custom initiatives
- If your cloud provider is compliant, that does not mean that you are compliant
- Microsoft does provide a blueprint and steps to deploy
  - [https://aka.ms/healthblueprint](https://aka.ms/healthblueprint)
AZURE SECURITY CENTER RECOMMENDATIONS
Free vs. Standard Azure Security Center

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>FREE TIER</th>
<th>STANDARD TIER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous assessment and security recommendations</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Azure secure score</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Just in time VM Access</td>
<td>- -</td>
<td>✔️</td>
</tr>
<tr>
<td>Adaptive application controls and network hardening</td>
<td>- -</td>
<td>✔️</td>
</tr>
<tr>
<td>Regulatory compliance dashboard and reports</td>
<td>- -</td>
<td>✔️</td>
</tr>
<tr>
<td>Threat protection for Azure VMs and non-Azure servers (including Server EDR)</td>
<td>- -</td>
<td>✔️</td>
</tr>
<tr>
<td>Threat protection for PaaS services</td>
<td>- -</td>
<td>✔️</td>
</tr>
<tr>
<td>Microsoft Defender ATP for Servers</td>
<td>- -</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Recommendations

- High severity
  - 8
- Medium severity
  - 5
- Low severity
  - 2

Resource health by severity:

- 2 Compute & apps resources
- 4 Data & storage resources
- 1 Identity & access resources

Networking:

- 2 Unhealthy resources
- 5 Monitored resources

Top recommendations by Secure Score impact:

- MFA should be enabled on accounts with owner permissions.
- Remediate vulnerabilities found on your virtual machines (powered by Qualys) (Preview).
- External accounts with owner permissions should be removed from your subscription.
- Vulnerability assessment solution should be installed on your virtual machines.
- MFA should be enabled on accounts with write permissions on your subscription.
- Vulnerabilities in security configuration on your machines should be remediated.
- System updates should be installed on your machines.
- All network ports should be restricted on NSS associated to your VM.
- Endpoint protection health issues should be resolved on your machines.
Remediation steps

Manual remediation:

We recommend that you edit the inbound rules of some of your virtual machines, to restrict access to specific source ranges.

To restrict access to your virtual machines:

1. Select a VM to restrict access to.
2. In the ‘Networking’ blade, click on each of the rules that allow management ports (e.g. RDP-3389, WINRM-5985, SSH-22).
3. Either change the ‘Action’ property to ‘Deny’, or, improve the rule by applying a less permissive range of source IP ranges.
4. Click ‘Save’.

Use Azure Security Center’s Just-in-time (JIT) virtual machine (VM) access to lock down inbound traffic to your Azure VMs by demand. Click here to learn more.
Networking

 Remediation steps

Quick fix remediation:
To remediate with a single click, in the Unhealthy resources tab (below), select the resources, and click “Remediate.”
Read the remediation details in the confirmation box, insert the relevant parameters if required and approve the remediation.

Note: It can take several minutes after remediation completes to see the resources in the ‘healthy resources’ tab.

Manual remediation:
To enable just-in-time VM access:

- Select one or more VMs from the list below and click “Remediate”, or click “Take action” if you’ve arrived from a recommendation for a specific VM.
- On the “JIT VM access configuration” page, define the ports for which the just-in-time VM access will be applicable.
  - To add additional ports, click the “Add” button on the top left, or click an existing port and edit it.
  - On the “Add port configuration” blade, enter the required parameters.
- Click “Save”.
Data & Storage

Remediation steps

Quick fix remediation:
To remediate with a single click, in the Unhealthy resources tab (below), select the resources, and click “Remediate.”
Read the remediation details in the confirmation box, insert the relevant parameters if required and approve the remediation.

Note: It can take several minutes after remediation completes to see the resources in the ‘healthy resources’ tab

View remediation logic

Manual remediation:
To enable SQL server auditing:
1. Select the SQL server.
2. Under Auditing, select On.
3. Select Storage details and configure a storage account for the audit log.
4. Click Save.
## Identity & Access

### Remediation steps

**Manual remediation:**

Before enabling MFA for the users, you may want to take this opportunity to delete any users listed that are no longer active users.

To enable MFA using conditional access you must have an Azure AD Premium license and have AD tenant admin permissions.

To enable MFA on user accounts:
1. Click a subscription from the list of subscriptions below or click 'Take action' if you are coming from a specific subscription. The list of user accounts that require enabling MFA opens.
2. Click 'Continue'. The Azure AD Conditional Access page opens.
3. In the Conditional Access page, add the list of users to an existing policy. If there are no existing policies, create a new policy following these instructions:
   a. Click + new policy.
   b. In the 'Name' text box, enter a policy name.
   c. Assign 'User and groups':
      i. Select 'Users and groups' in the 'Include' tab, select 'Select users and groups' and select the 'Users and groups' check box.
      ii. Select the users that are in the list of user accounts require enabling MFA. You can scroll back to the left to see the list.
   d. Click 'Done'.
   e. Assign 'Cloud apps':
      i. Select 'Cloud apps' in the 'Include' tab, select 'All cloud apps'. (Don't exclude any apps.)
   f. Click 'Done'.
   g. Assign 'Access Controls':
      i. Select 'Grant' and select 'Require multi-factor authentication'. (Don't select any other options)
   h. Click 'Select'.
   i. Enable Policy:
      i. Click 'On'.
   j. Click 'Create'.

**External accounts with write permissions should be removed from your subscription**

**Deprecated accounts should be removed from your subscription**
The Before

Overall Secure Score

340 OF 625

Secure Score by category

- 65 / 180 Compute & apps resources
- 50 / 90 Data & storage resources
- 90 / 140 Networking resources
- 135 / 215 Identity & access resources
The Demo

• Insert VIDEO Here
The After

Overall Secure Score
413 OF 720

Secure Score by category
- 113 / 295 Compute & apps resources
- 90 / 90 Data & storage resources
- 105 / 120 Networking resources
- 105 / 215 Identity & access resources
Leadership Questions

• Security Posture Questions
  - How do I feel about my current Azure security posture?
  - Do I have control over my resources?
  - Do I have visibility over my resources?
  - How would improving security posture impact current operations?
  - How does this improve my audit statements?
Summary

- Security Hygiene
- Secure Score
- Security Policies
QUESTIONS
AND ANSWERS
THANK YOU FOR YOUR TIME AND ATTENTION
Resources

• 2019 Cloud Security Report