Understanding Identity with Azure AD

John Savill

Agenda

• Why does identity matter? A review
• The four pillars of identity
• Q&A

Identity – A brief history

In the beginning you only had a single identity on your companies network
All systems were internal to your organization tied into that identity
Where systems used their own identity a solution was used to replicate usernames/passwords where possible
With the Internet and unlimited connectivity organizations use services from Internet based providers
This has led to users having multiple identities which leads to other challenges or the use of federation

Azure AD Fundamentals

Azure AD SKUs

There are four (and a half) Azure AD SKUs
• Free
• Basic
• Premium P1
• Premium P2
• With Office 365 benefits

Premium commonly part of EMS/M365

Azure AD B2B and B2C

You may want to collaborate with partners via their own Azure AD or Microsoft identities
• Azure AD B2B

If you want to provide a web/mobile application to your customers using their own identity (social, local or Azure AD)
• Azure AD B2C
Azure AD B2B

Collaborate on internal solutions, for example Office 365

Azure AD B2C

Designed for customer facing web and mobile applications

Four Pillars of Secure Identity with Azure AD

- MFA
- Conditional Access
- Identity Protection
- Privileged Identity Management

Multi-Factor Authentication

As identities in Azure AD become the single identity across all services it's critical that single identity is well protected.

A single network secret is unacceptable in today's world.

Multi-factor all the way:

- Something I know
- Something I have
- Something I am

Azure AD has a native MFA solution that utilizes your mobile phone.

Can also integrate with other MFA solutions if federation is used.

End User Experiences

myapps.microsoft.com
Azure AD SKUs and MFA

There are four primary SKUs for Azure AD (plus an Office 365 variant)
Key point is MFA is included with the Azure AD Premium P1 and P2 (and for Office apps only with the Office 365)
Also available for Free and Basic when a separate Multi-Factor Authentication Provider is used which is licensed on a per-user or per-authentication basis
Also available with a subset of capabilities for Azure Global Administrators when the Azure AD instance has not been MFA enabled

Conditional Access

Focused around attributes, conditions and controls

Identity Protection

75% of intrusions are based on user credentials
Identity Protection provides insights about identity based on a consolidated view of machine learning
- Brute force attacks/leaked credentials/suspicious sign-ins
- Infected devices
- Configuration vulnerabilities
Provides a risk calculation along with remediation recommendations
Can integrate with conditional access

Privileged Identity Management

No standing privileges, the cornerstone of good security
Enables users to be granted access to roles that are activated via elevation
Can include approval as part of elevation
15 roles require MFA, others are optional
If MFA is used for initial logon an additional MFA at elevation is not required
No custom roles

Clark Kent or Superman

Which do you need to be?
There is a large population that believes in powered individuals having two separate identities
The normal user
The privileged user
Ordinarily login with the normal user and use the privileged user only when required
This approach has the benefit of enabling additional conditions to be placed on the privileged users via technologies like Conditional Access

Constant New Features!

Follow me on twitter
@NTFAQGuy
I’ll try to keep you updated ☺
Take the Survey!
Your feedback is important! Please rate the session for a chance to win!
Survey is below session description at http://elus18.expertslive.us

Related Sessions - Azure

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Room</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/8: 10:30</td>
<td>Wren</td>
<td>Waterway 6</td>
<td>Advanced Analytics in Azure</td>
</tr>
<tr>
<td>2/8: 10:30</td>
<td>Joyner</td>
<td>College Park</td>
<td>Azure Site Recovery - Tips from the Trenches</td>
</tr>
<tr>
<td>2/8: 11:45</td>
<td>Savill</td>
<td>Waterway 6</td>
<td>Azure IaaS: State of the Union</td>
</tr>
<tr>
<td>2/8: 2:15</td>
<td>Nikolic</td>
<td>Alden Bridge</td>
<td>Cloud Shell: Your Admin Machine for Azure</td>
</tr>
<tr>
<td>2/8: 3:30</td>
<td>Savill</td>
<td>Alden Bridge</td>
<td>Understanding Identity with Azure AD</td>
</tr>
<tr>
<td>2/8: 3:30</td>
<td>Rangama</td>
<td>Sterling Ridge</td>
<td>Infrastructure-as-Code with ARM</td>
</tr>
<tr>
<td>2/9: 9:00</td>
<td>Rangama</td>
<td>College Park</td>
<td>Building Process Automation w/ Azure Logic Apps</td>
</tr>
<tr>
<td>2/9: 3:30</td>
<td>Joyner</td>
<td>Sterling Ridge</td>
<td>Business Continuity in the Microsoft Cloud</td>
</tr>
</tbody>
</table>