MONDAY
GET OFF YOUR BUTS AND MOVE YOUR APPS!

CREATING AN APP MODERNIZATION STRATEGY

Ricky Pullan @rickypullan
Christina Morillo @divinetechygirl
Program Managers - Identity Engineering
GET OFF YOUR BUTS AND MOVE YOUR APPS!

CREATING AN APP MODERNIZATION STRATEGY

Ricky Pullan @rickypullan
Christina Morillo @divinetechygirl
Program Managers - Identity Engineering
LET’S TALK ABOUT

Why you should care

What ‘modernizing’ actually means

How you build your modernization strategy?

Your go do’s starting Monday
YOUR APP STORY TODAY...

Traffic may not traverse corp net

Data may exist off premises

Legacy identity stores

Insecure network traffic

Crazy dependencies

Manage outdated infrastructure

That one app that someone built 20 years ago that no one gets
HOW WE SEE APPLICATIONS...

SaaS Apps

- Cloud hosted apps
- Server hosted apps

Legacy

- Windows Integrated auth
- LDAP auth
- Header-based auth
- Basic/Forms based auth
- SAML 1.1/WS-Fed auth
- OIDC OAuth Modern
MODERN AUTHENTICATION (WEB FLOW)

• More tools to protect resources
• Ability to handle an MFA challenge/response
• Can include additional information about the device (Hybrid Domain Join)
• Applies to mobile devices as well (MAM Policies)
• More information an attacker has to guess correctly to spoof (this is good news for us!)
• User Agent, Application Target
New App Policy

• All new applications must support modern auth

STOP FEEDING THE FIRE
App modernization is a journey. You need as many facts as you can possibly gather.

“Insufficient facts always invite danger.” - Spock
COLLECT YOUR FACTS...

New App Policy

• All new applications must support modern auth

Discovery

• App inventory
• Cloud App Security Broker
• ADFS Readiness tool
• Start sniffing traffic
• Log analysis
New App Policy
- All new applications must support modern auth

Discovery
- App inventory
- Cloud App Security Broker
- ADFS Readiness tool
- Start sniffing traffic
- Log analysis

Classify
- Bucketize

COLLECT YOUR FACTS...
Can we turn it off?

Decommission
Can we turn it off?

Decommission

Does the app support modern authN?

Move it!

Ask your vendor if they support modern authentication. If they don’t, ask them why.
Can we turn it off?

Decommission

Does the app support modern auth?

Move it!

Is there a modern auth/SaaS equivalent?

Acquire and deploy

Check if it's in the Azure AD Enterprise Apps gallery. If it's not, email us and we'll get it added in a week*.

*ish
AZURE APP GALLERY

• Minimal configuration
• Step-by-step setup guides
• App provisioning
• SCIM support
Can we turn it off?

Decommission

Does the app support modern authN?

Move it!

Is there a modern auth/SaaS equivalent?

Acquire and deploy

Can the codebase be updated?

Refactor!

- Use modern authN stack
- Integrate app protection SDKs
- Use secure channels for transmission
RE-FACTOR YOUR AUTHENTICATION STACK

• DON’T BUILD YOUR OWN LIBRARY – We got you!
  • MSAL – js, .NET, Python, Java, iOS/macOS, Android, OmniAuth, PHP
  • Natively support all Microsoft identities and APIs
  • Leverage token logic
• DON’T OVERPERMISSION!
• Include app protection SDKs
  • Restrict movement of files, configure clipboard restrictions, prevent screenshots
Can we turn it off?

Decommission

Does the app support modern authN?

Move it!

Is there a modern auth/SaaS equivalent?

Acquire and deploy

Can the codebase be updated?

Refactor!

Does app functionality require legacy protocols and remain on prem?

Keep on prem; proxy/VDI

- Azure App Proxy
- Secure Hybrid Access integrations (F5, Zscaler, Akamai, Citrix, and Aryaka)
Can we turn it off? 

Does the app support modern authN? 

Is there a modern auth/SaaS equivalent? 

Acquire and deploy 

Can the codebase be updated? 

Refactor! 

Does app functionality require legacy protocols and remain on prem? 

Keep on prem; proxy/VDI 

Lift and shift + proxy 

Decommission 

Move it!
WHAT ABOUT LEGACY PROTOCOLS?

- Easily enable lift and shift scenarios
- LDAP, Kerberos, NTLM v1 and NTLM v2 support
- Securely managed service, removing legacy auth traffic on your network
- Use corporate credentials and existing groups
Decommission
Move it!
Acquire and deploy
Refactor!
Keep on prem; proxy/VDI
Lift and shift + proxy

TEMPORARY
New App Policy

- Decommission
- Refactor!

Discovery

- Move it!
- Keep on prem; proxy/VDI

Classify

- Acquire and deploy
- Lift and shift + proxy

New App Policy
Discovery
Classify

Decommission
Move it!
Acquire and deploy
Refactor!
Keep on prem; proxy/VDI
Lift and shift + proxy
New App Policy
• All new applications must support modern auth

Discovery
• Cloud App Security Broker
• ADFS Readiness tool

Classify
• Bucketize

Prioritize
• Ease of migration
• Security needs
• App lifecycle
GO DO’S

MONDAY

✓ Stop the bleeding – “New App Policy”
✓ Schedule your discovery exercise
✓ Explore SaaS apps already available in the Azure Portal/your IDP

BY DAY 30

✓ You should now have a good picture of all apps in your environment.
✓ Start classifying “bucketizing your apps”

BY DAY 60

✓ Your apps should now be classified
✓ Prioritize (present your findings to stakeholders and get buy-in)

BY DAY 90

✓ Have your execution plan in place based on your buckets—understand who's doing what/what’s going where
✓ Start and get it done!
RESOURCES

- App Migration Toolkit – https://aka.ms/MigrateApps
  - General migration guidance
  - AD FS to Azure AD readiness tool
  - Deployment plans
  - Solution guides
- Microsoft identity platform: https://aka.ms/identityplatform
- InTune App Protection SDKs: https://aka.ms/IntuneAppSDK
THANK YOU!