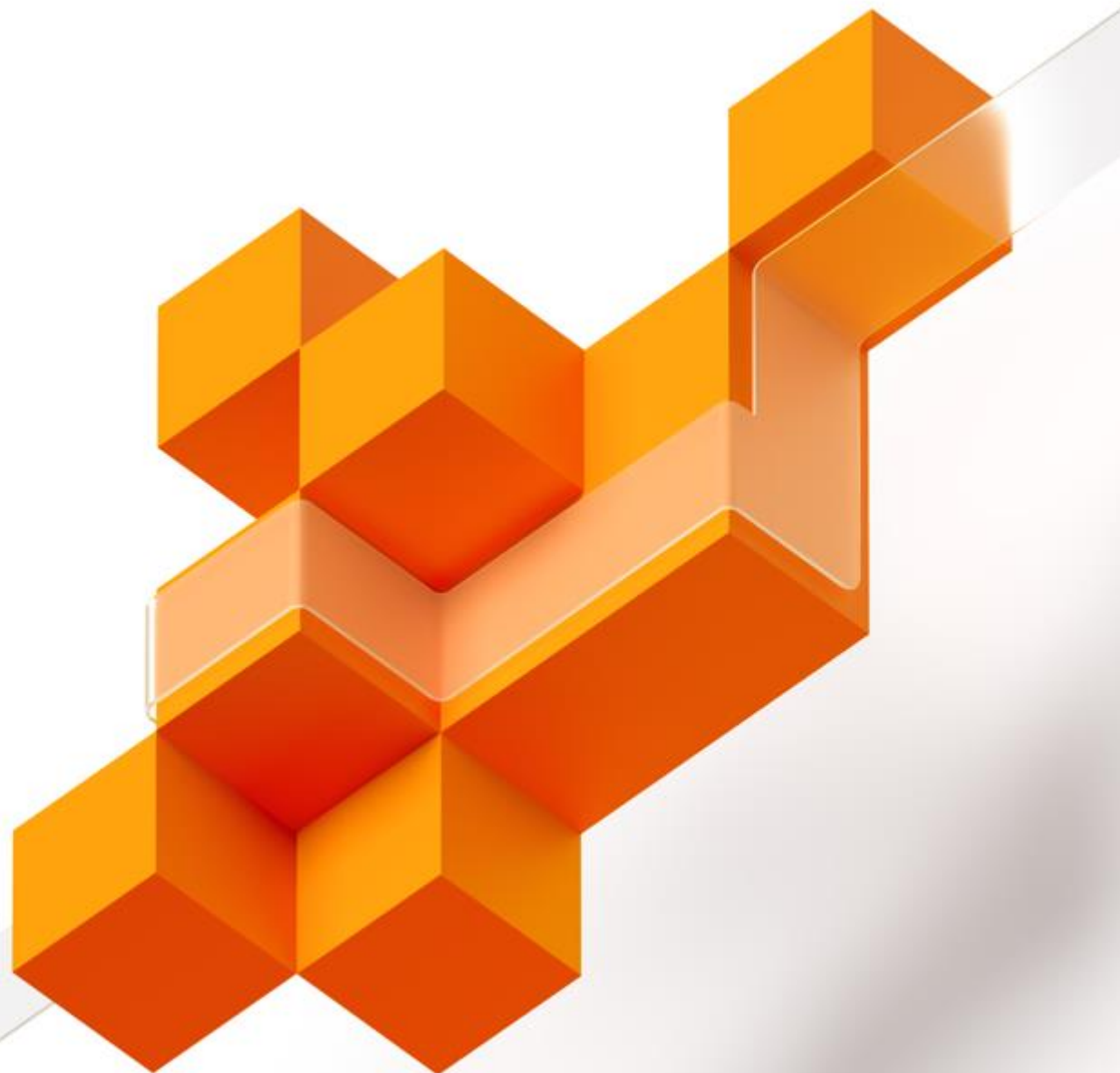




# Microsoft Ignite



# Shut the door on cybercrime with identity- driven security

Rohini Goyal (@rohinigo)

Mark Morowczynski (@markmorow)

Program Managers Identity Division



# Agenda

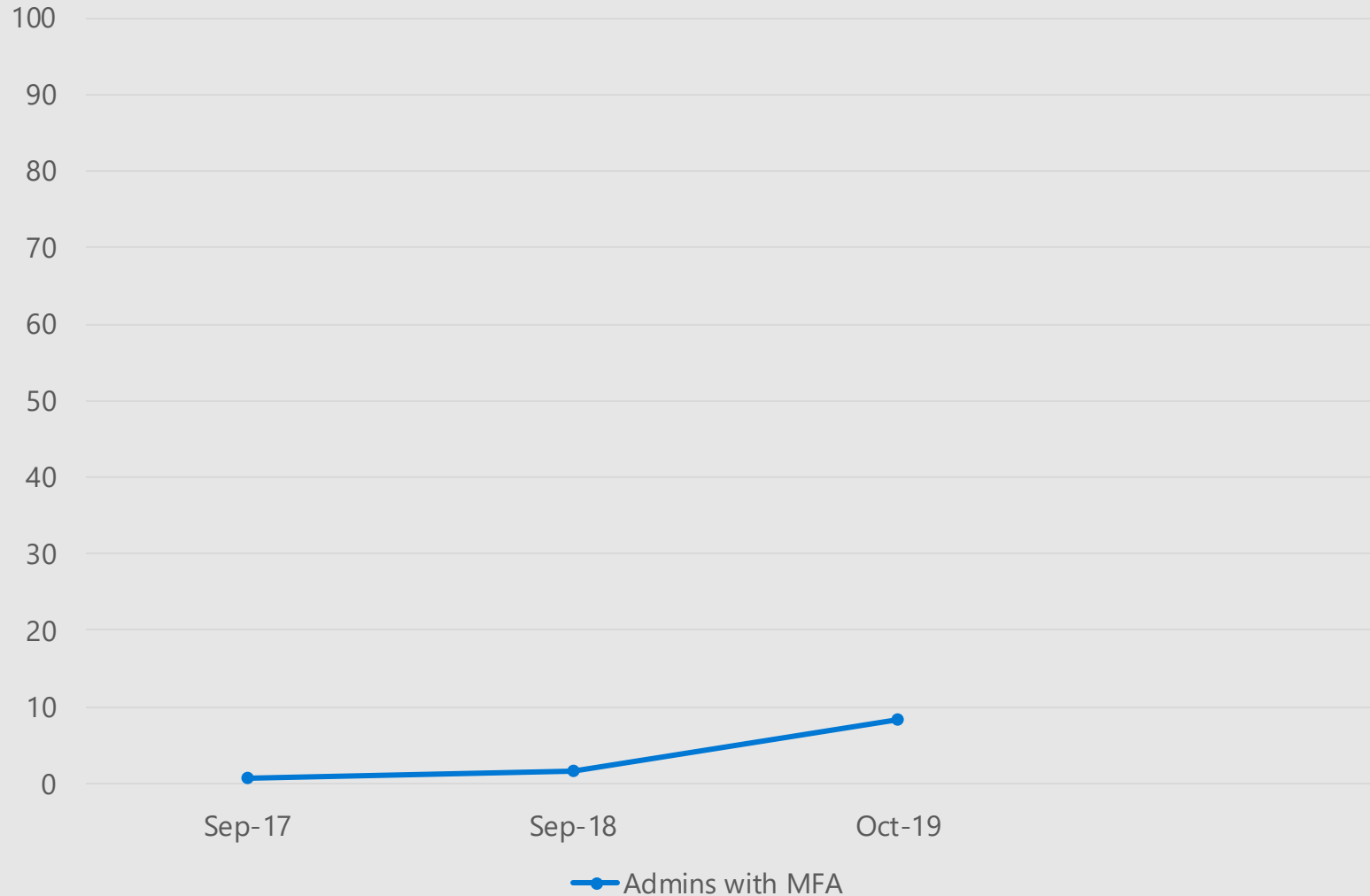
- Protect Your Admins
- Enable Password Hash Sync
- Identity Protection
- Azure AD Password Protection
- Blocking Legacy Auth
- Security Defaults and Go Dos

Admin Accounts with MFA Sept 2017: 0.7%

Admin Accounts with MFA Sept 2018: 1.7%

Admin Accounts with MFA Oct 2019: 8.2%

### Admins with MFA



**91.8% of  
admins with  
NO MFA**

# How To Enable MFA For Your Admins

- Good: Turn MFA on!
- Better: Conditional Access
- Best: Azure AD Privilege Identity Management
  - No standing admin access
  - Admin access requires elevation + MFA
  - Approval workflows and elevation scheduling
  - Alerts on admin activity taking place outside of PIM
  - Applies/Protect Azure Resources as well!
  - Can buy Azure AD P2 license for just your admins
  - <https://aka.ms/deploymentplans>

# Resilient Access Control Strategy

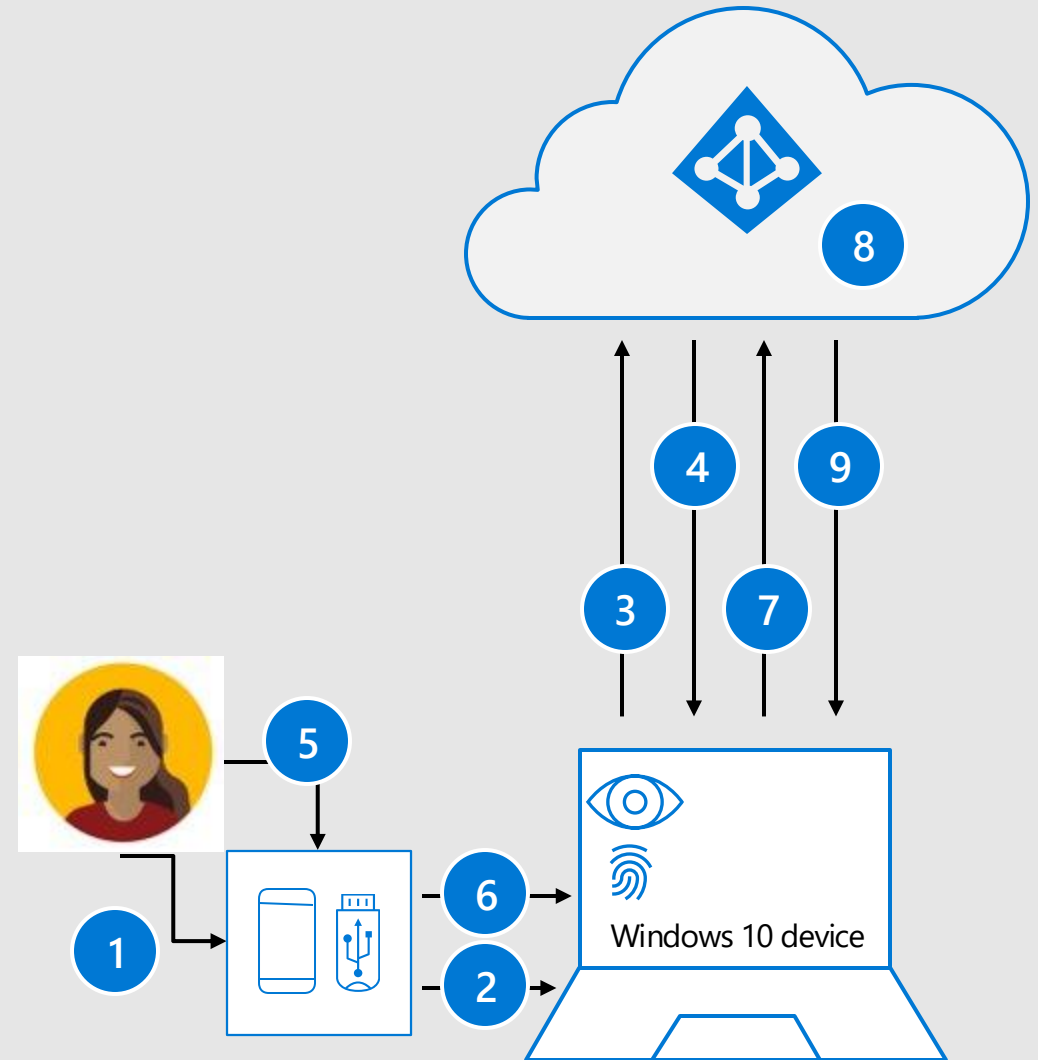
- Have a resilient access control management strategy
  - Even small service interruptions can have impact
  - Example: 10/18/2019 Azure MFA service network packet loss
    - 0.51% of active users in North America blocked on MFA for 3 hours
    - Full RCA at <https://status.azure.com/en-us/status/history/>
  - Regardless of the number, we will continually push ourselves to improve.
- <http://aka.ms/resilentaad>
  - Have policy pre-configured in disabled state, business decision when to switch
  - Look to leverage trusted devices: Hybrid Azure AD Join or InTune compliance
- Windows Hello for Business and FIDO2 both fulfill MFA requirement

# FIDO2

- Standards-based Passwordless authentication
- WebAuthN and CTAP(Client To Authenticator Protocol) standards are final
- Public/Private Key infrastructure
  - Private keys are securely stored on the device
- Local gesture (e.g., biometric, PIN) required
- Data bound to a single device

# Strong Authentication with FIDO2 security key

- 1 User plugs FIDO2 security key into computer
- 2 Windows detects FIDO2 security key
- 3 Windows device sends auth request
- 4 Azure AD sends back nonce
- 5 User completes gesture to unlock private key stored in security key's secure enclave
- 6 FIDO2 security key signs nonce with private key
- 7 PRT token request with signed nonce is sent to Azure AD
- 8 Azure AD verifies FIDO key
- 9 Azure AD returns PRT to enable access to cloud resources







## FIDO2 public preview expanding to Hybrid environments (Early 2020)



# What will be included?



**Passwordless sign-in using FIDO2 security keys**

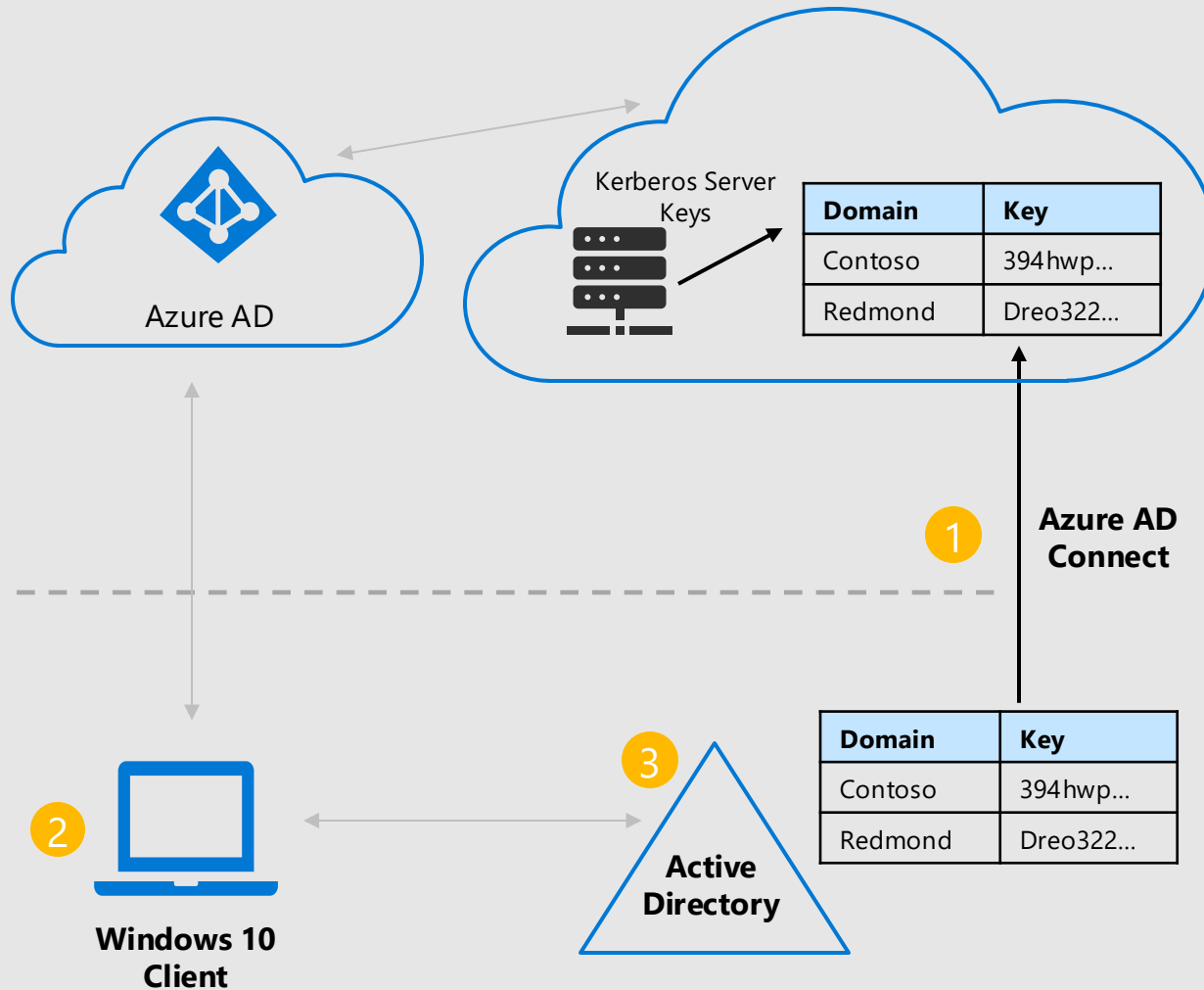


**- Azure Active Directory Joined (AADJ)  
- Hybrid AADJ Windows 10 devices**



**Seamless SSO to Cloud and on-premises resources**

# Deployment Components



- 1 Latest version of AAD Connect
- 2 Latest Windows Insider Build
- 3 Patch for Domain Controller (Server 2016/2019)

**BRK3257** Friday 10:30am  
Leverage the cloud to strengthen  
your on-premises Active  
Directory security

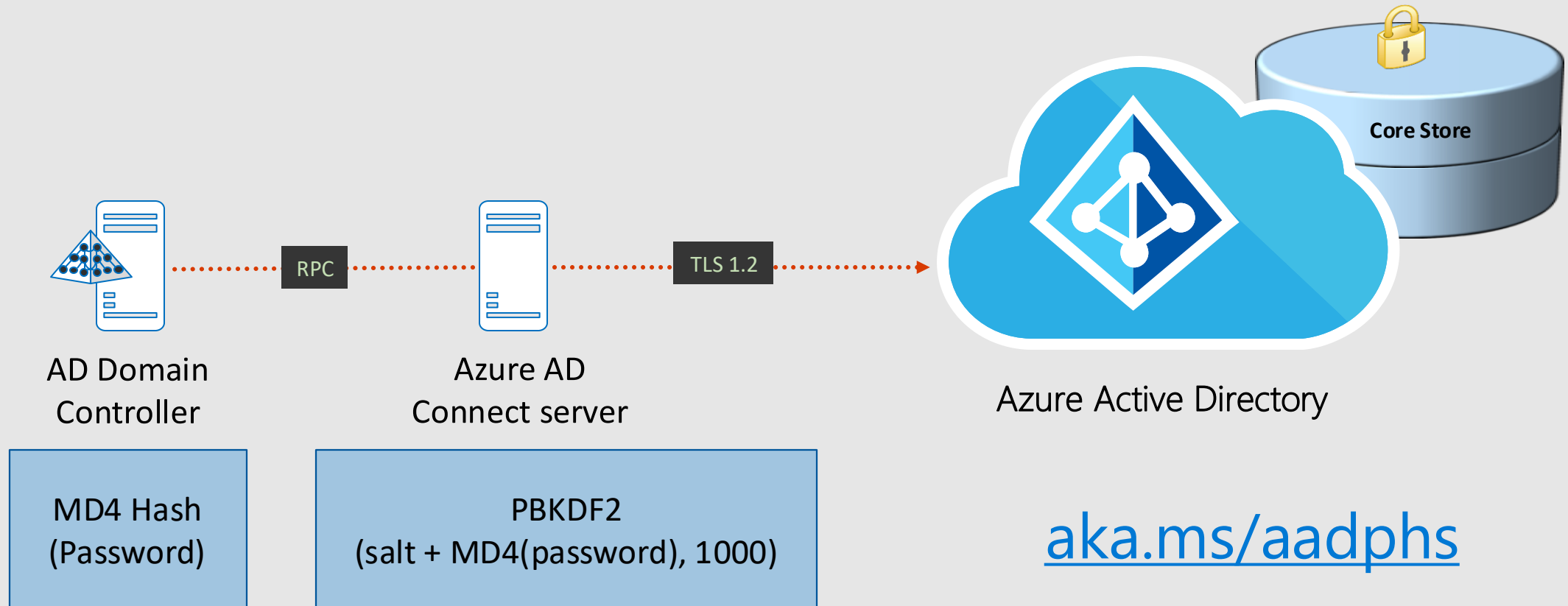
# Agenda

- Protect Your Admins
- Enable Password Hash Sync
- Identity Protection
- Azure AD Password Protection
- Blocking Legacy Auth
- Security Defaults and Go Dos

# Turn on Azure AD Connect Password Hash Sync

- Leaked Credential Reporting
  - Dark Web, Law Enforcement, and Security Researchers
- When something catastrophic happens
  - WannaCry, NotPetya
  - Wired-The Untold Story Of Notpeya, The Most Devasting Cyberattack In History
    - <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

# How Password Hash Sync Works





# Updated Stats

**5.5+ billion**

Leaked credentials Processed

**14.2+ million**

Leaked credentials matched

**82%**

Azure AD active tenants with  
PHS – Sept 2018

**91%**

Azure AD active tenants with  
PHS – Oct 2019



# Agenda

- Protect Your Admins
- Enable Password Hash Sync
- Identity Protection
- Azure AD Password Protection
- Blocking Legacy Auth
- Security Defaults and Go Dos



# Azure AD Identity Protection

User risk - Probability an identity is compromised

Sign-in risk - Probability a sign-in is compromised

Real-time - Based on only real-time detections

Aggregate - Based on all detections (real-time and non real-time)

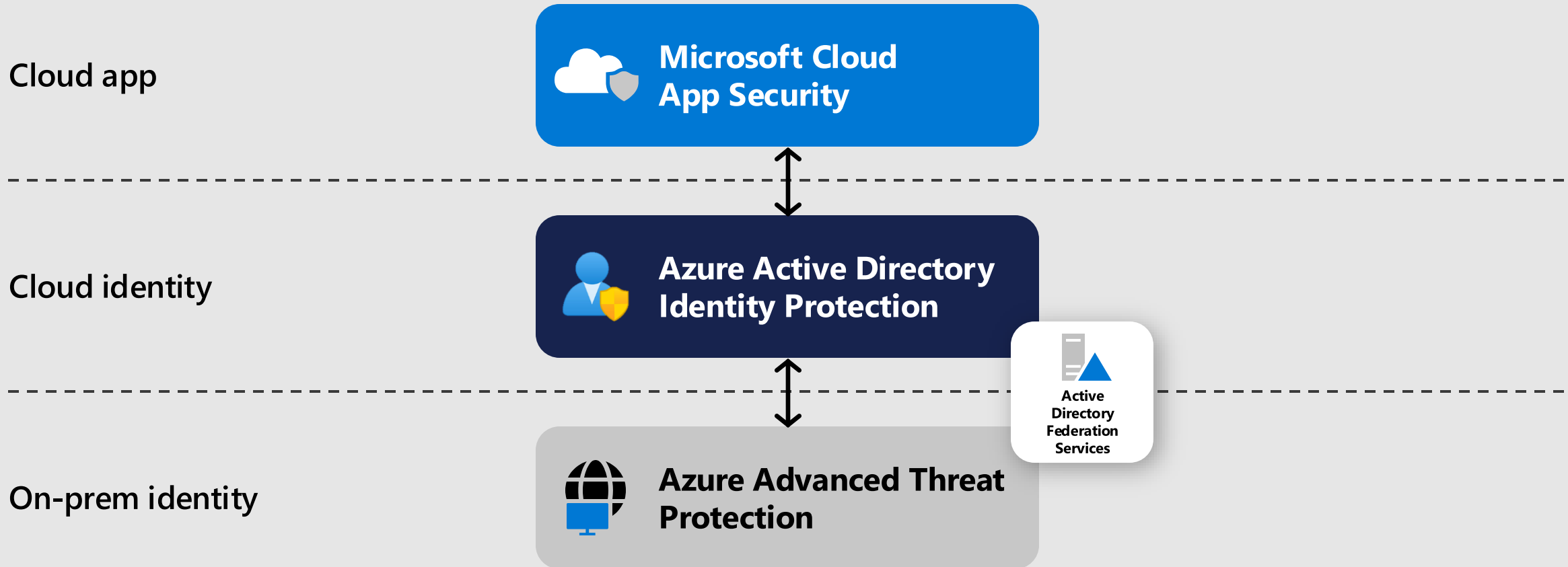
# Why Azure AD Identity Protection

- More Prompts != More Security
  - Only prompt for MFA when needed
- Automate User Risk response
  - Block or Secure Password change
- Confirm user(s) compromised via RiskyUsersAPI
  - Feed from your other threat intel sources
- Automatically getting new signals and updates
  - **BRK4017-The science behind how Azure Active Directory defends your organization and protect identities (Thursday AM)**

# Azure AD Identity Protection Risk Signals

Name	Description	Timing	Linked to	Detection source	Status
<b>Anonymous IP address</b>	Tor or anonymizer VPNs	<b>Real-time</b>	Azure AD login	Identity Protection	GA
<b>Atypical travel</b>	Travel distance > Travel time	Offline	Azure AD login	Identity Protection	GA
<b>Leaked credentials</b>	Valid credentials compromised	Offline	User	Identity Protection	GA
<b>Malware linked IP address</b>	Botnet linked IP address	Offline	Azure AD login	Identity Protection	GA
<b>Unfamiliar sign-in properties</b>	Periodicity based unfamiliar properties.	<b>Real-time</b>	Azure AD login	Identity Protection	<b>GA (New)</b>
<b>Unfamiliar sign-in properties</b>	Multiple failed sign-ins in a short time period	<b>Real-time</b>	Azure AD login	Identity Protection	GA
<b>Azure AD threat intelligence</b>	ISP investigations intel	Offline	User	ISP investigations	GA
<b>Admin confirmed user compromised</b>	Admin feedback	Offline	User	Admin	GA
<b>Malicious IP address</b>	Valid creds, blocked IP (Sharkfin, etc.)	Offline	Azure AD login	Identity Protection	<b>GA (New)</b>
<b>Impossible travel</b>	Inter / intra session travel (MCAS)	Offline	Azure AD login	<b>MS Cloud App Security</b>	Preview
<b>Suspicious inbox manipulation rules</b>	Mailbox manipulation (MCAS)	Offline	Azure AD login	<b>MS Cloud App Security</b>	Preview

# End-to-end Identity Protection



Protection at all levels of the hybrid cloud via the E5 product suite

# Agenda

- Protect Your Admins
- Enable Password Hash Sync
- Identity Protection
- [Azure AD Password Protection](#)
- Blocking Legacy Auth
- Security Defaults and Go Dos

# Password Spray

Josi@contoso.com	Winter2019!
Chance@wingtiptoy.com	Winter2019!
Rami@fabrikam.com	Winter2019!
TomH@cohowinery.com	Winter2019!
AnitaM@cohovineyard.com	Winter2019!
EitokuK@cpandl.com	Winter2019!
Ramanujan@Adatum.com	Winter2019!
Maria@Treyresearch.net	Winter2019!
LC@adventure-works.com	Winter2019!
EW@alpineskihouse.com	Winter2019!
info@blueyonderairlines.com	Winter2019!
AiliS@fourthcoffee.com	Winter2019!
MM39@litwareinc.com	Winter2019!
Margie@margiestravel.com	Winter2019!
Ling-Pi997@proseware.com	Winter2019!
PabloP@fineartschool.net	Winter2019!
GiseleD@tailspintoys.com	Winter2019!
Luly@worldwideimporters.com	Winter2019!

# 730,000+

Compromised accounts due to password spray  
in the last 4 months

# Azure AD Password Protection

Cloud intelligence to ensure strong passwords

## Global banned password list

Microsoft defines a global list with almost 2,000 common words, phrases, patterns

## Custom banned password list

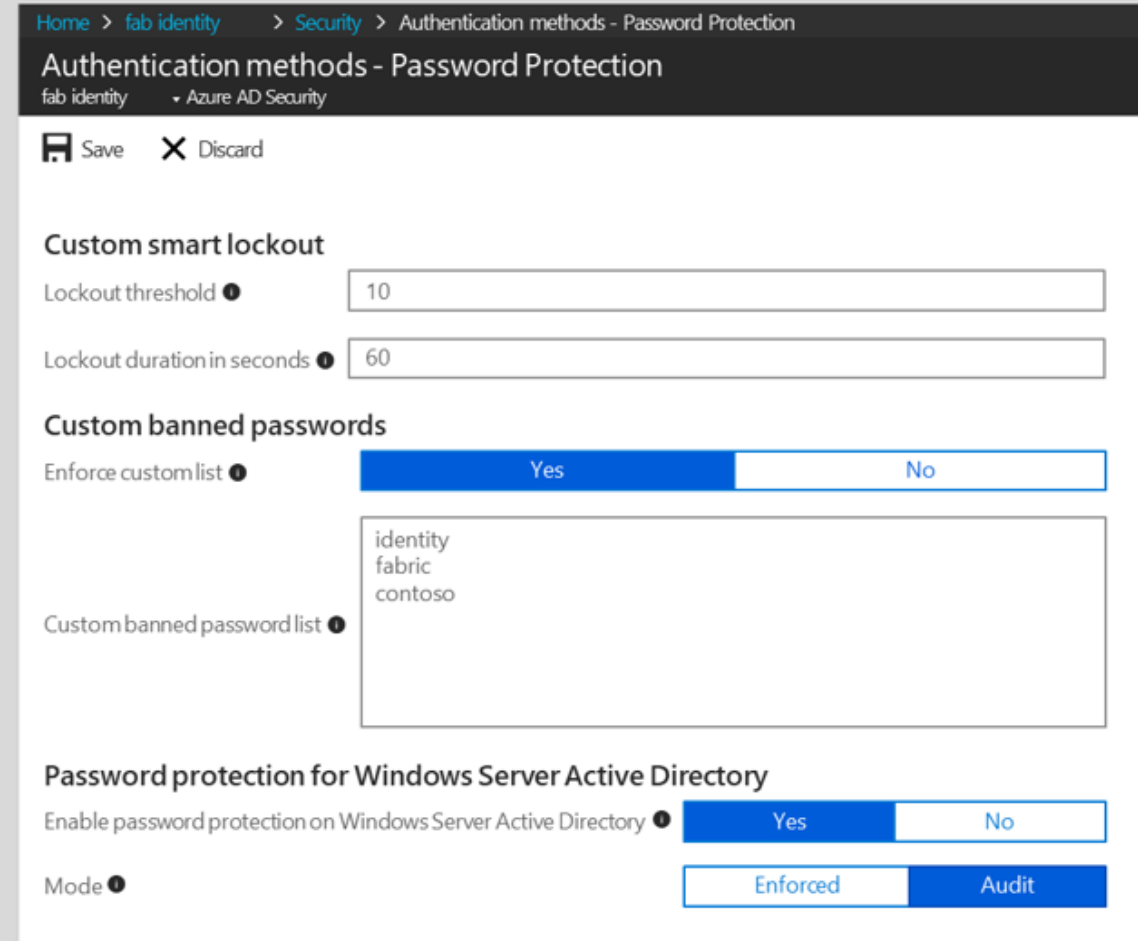
1,000 words and phrases unique to your organization.  
Do NOT put variations!

## Banned password algorithm

Not your traditional strength policy - finds all weak password variations using global and custom lists

## The best part!

Available for your on-prem Active Directory environment.



The screenshot shows the 'Authentication methods - Password Protection' page in the Azure portal. The breadcrumb trail is 'Home > fab identity > Security > Authentication methods - Password Protection'. The page title is 'Authentication methods - Password Protection' with a sub-header 'fab identity > Azure AD Security'. At the top, there are 'Save' and 'Discard' buttons. The 'Custom smart logout' section has two input fields: 'Lockout threshold' set to 10 and 'Lockout duration in seconds' set to 60. The 'Custom banned passwords' section has a toggle for 'Enforce custom list' set to 'Yes' and a text area for 'Custom banned password list' containing the text 'identity', 'fabric', and 'contoso'. The 'Password protection for Windows Server Active Directory' section has two toggle controls: 'Enable password protection on Windows Server Active Directory' set to 'Yes' and 'Mode' set to 'Enforced' (with 'Audit' as an alternative).

Home > fab identity > Security > Authentication methods - Password Protection

Authentication methods - Password Protection

fab identity > Azure AD Security

Save Discard

**Custom smart logout**

Lockout threshold 10

Lockout duration in seconds 60

**Custom banned passwords**

Enforce custom list Yes No

Custom banned password list identity  
fabric  
contoso

**Password protection for Windows Server Active Directory**

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit



Banned  
Password Lists



Banning that word  
entirely

# Password strength evaluation



**Global and custom lists are combined**



**All inputs normalized**

All characters lower-cased

Common character substitutions

'\$' -> 's'

'@' -> 'a'

'!' -> 'l'



**Identify banned passwords**

A user's first name, last name, username, and domain name automatically disqualify a password



**Final scoring**

Each banned password = 1 point

Each unique character = 1 point



**Min score of 5 required to pass**



**Global and custom  
lists are combined**



**All inputs  
normalized**



**Identify banned  
passwords**



**Final scoring**



**Min score of 5  
required to pass**

**Global list:** password 2019 1234

**Custom list:** secure ignite



**Global and custom  
lists are combined**



**All inputs  
normalized**



**Identify banned  
passwords**



**Final scoring**



**Min score of 5  
required to pass**

**Global list:** password 2019 1234

**Custom list:** secure ignite

\$3cureP@\$w0rd8



**Global and custom  
lists are combined**



**All inputs  
normalized**



**Identify banned  
passwords**



**Final scoring**



**Min score of 5  
required to pass**

**Original list:** password 2019 1234

**Custom list:** secure ignite

\$3cureP@\$w0rd8

1



Global and custom  
lists are combined



All inputs  
normalized



Identify banned  
passwords



Final scoring



Min score of 5  
required to pass

Combined list: password 2019 1234 secure ignite

↓ ↓ ↓ ↓ ↓

\$3cureP@\$w0rd8



1  
Global and custom  
lists are combined



2  
All inputs  
normalized



Identify banned  
passwords



Final scoring



Min score of 5  
required to pass

Combined list: password 2019 1234 secure ignite

↓ ↓ ↓ ↓ ↓

securepassword8



1  
Global and custom  
lists are combined



2  
All inputs  
normalized



Identify banned  
passwords



Final scoring

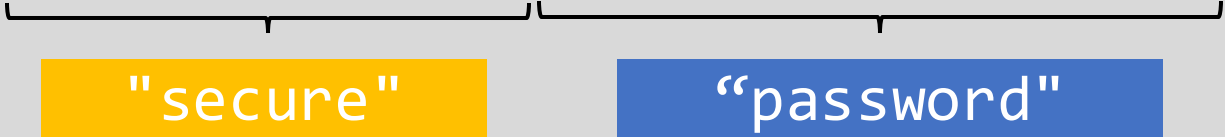


Min score of 5  
required to pass



Combined list: password 2019 1234 secure ignite

securepassword8



Global and custom lists are combined



All inputs normalized



Identify banned passwords



Final scoring



Min score of 5 required to pass

Combined list: password 2019 1234 secure ignite

securepassword8

"secure"

"password"

1

+

1

+

1



1  
Global and custom  
lists are combined



2  
All inputs  
normalized



3  
Identify banned  
passwords



4  
Final scoring



Min score of 5  
required to pass

Combined list: password 2019 1234 secure ignite

securepassword8



1 + 1 + 1

3 points = Weak Password!!



1  
Global and custom  
lists are combined



2  
All inputs  
normalized



3  
Identify banned  
passwords



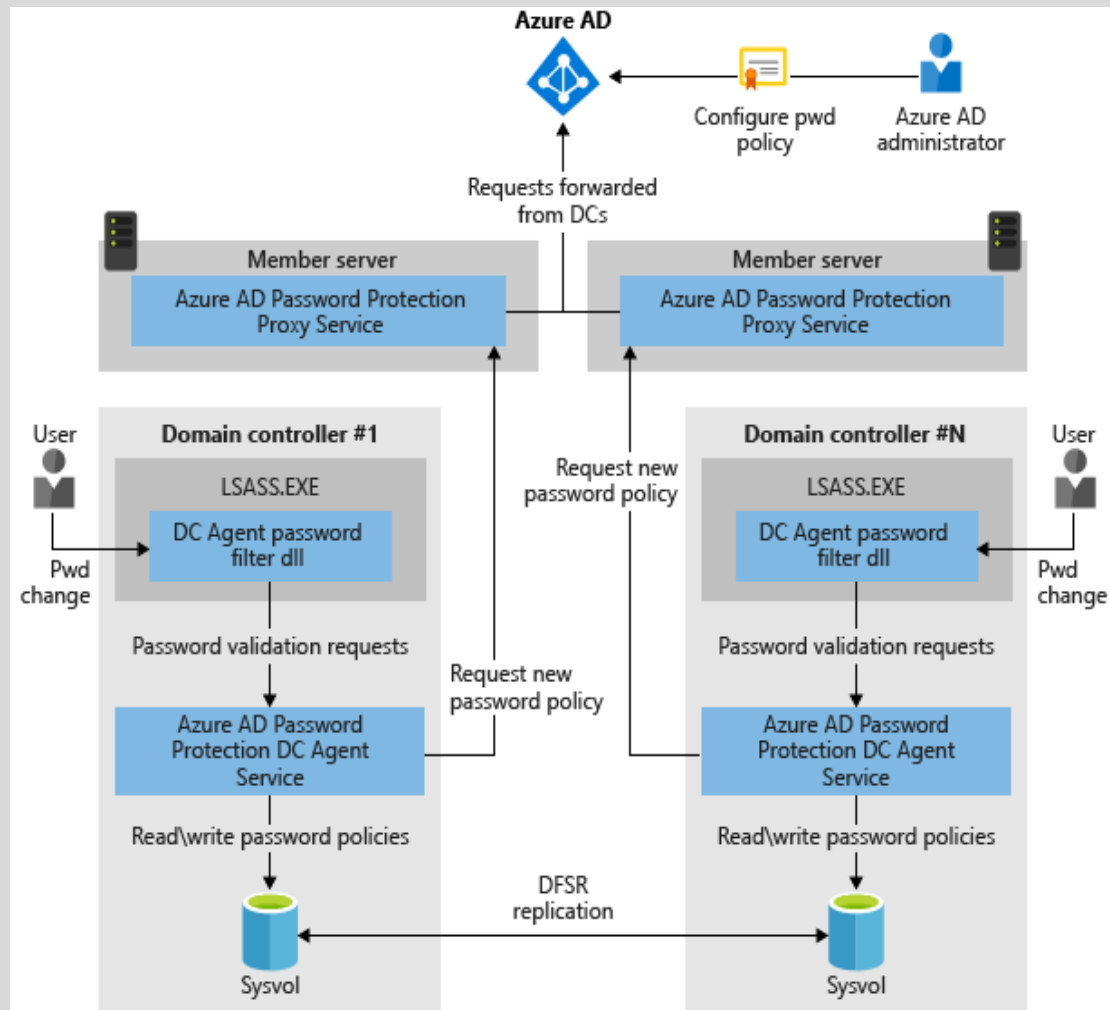
4  
Final scoring



5  
Min score of 5  
required to pass

# The best part!

## Azure AD Password Protection – on premises



### No internet required on DCs

Built for secure no-internet zone domain controllers. Supports multi-forest environment

### Works with your other on-prem password filters

### Audit Mode

“what if” mode – logs when password would have been rejected

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-monitor#powershell-cmdlet-logging>

# Agenda

- Protect Your Admins
- Enable Password Hash Sync
- Identity Protection
- Azure AD Password Protection
- [Blocking Legacy Auth](#)
- Security Defaults and Go Dos

# What is Legacy Authentication?

- Authentication requests made by legacy protocols

POP3

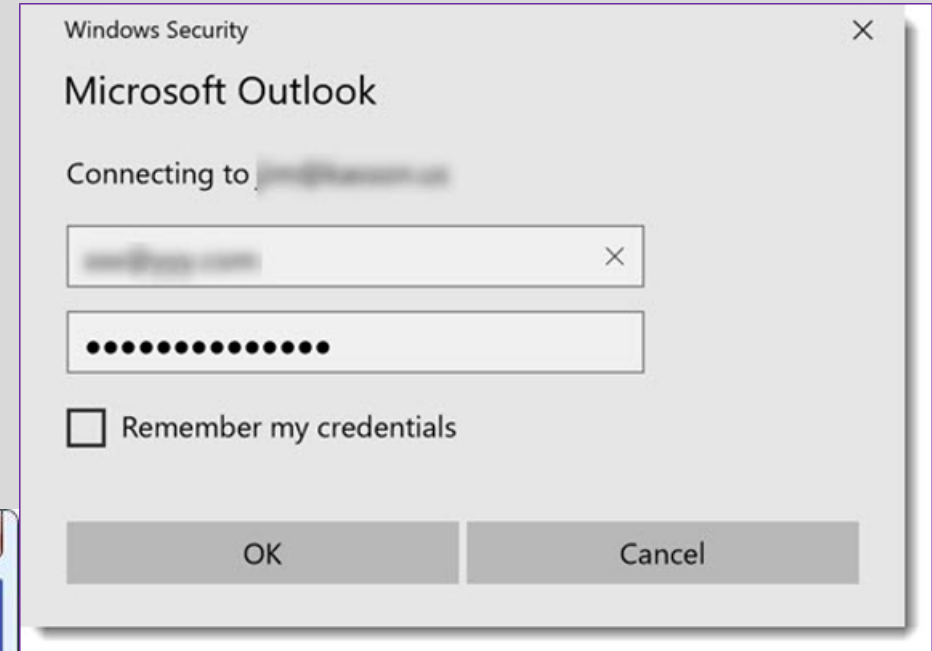
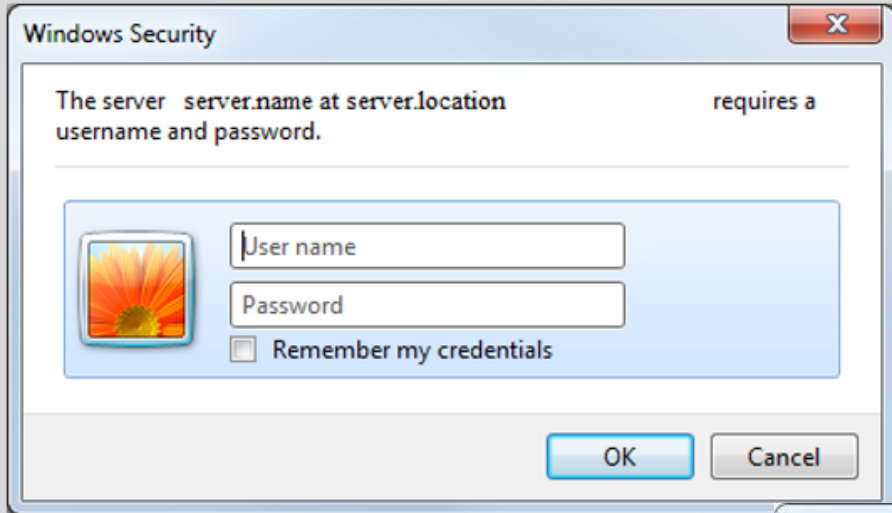
IMAP

SMTP

EAS BasicAuth

- Typically a single factor (username/password). These protocols do not support multi-factor authentication
- Federated with Azure AD/O365: IDP is responsible for authentication, including basic auth!

# Legacy Authentication Examples



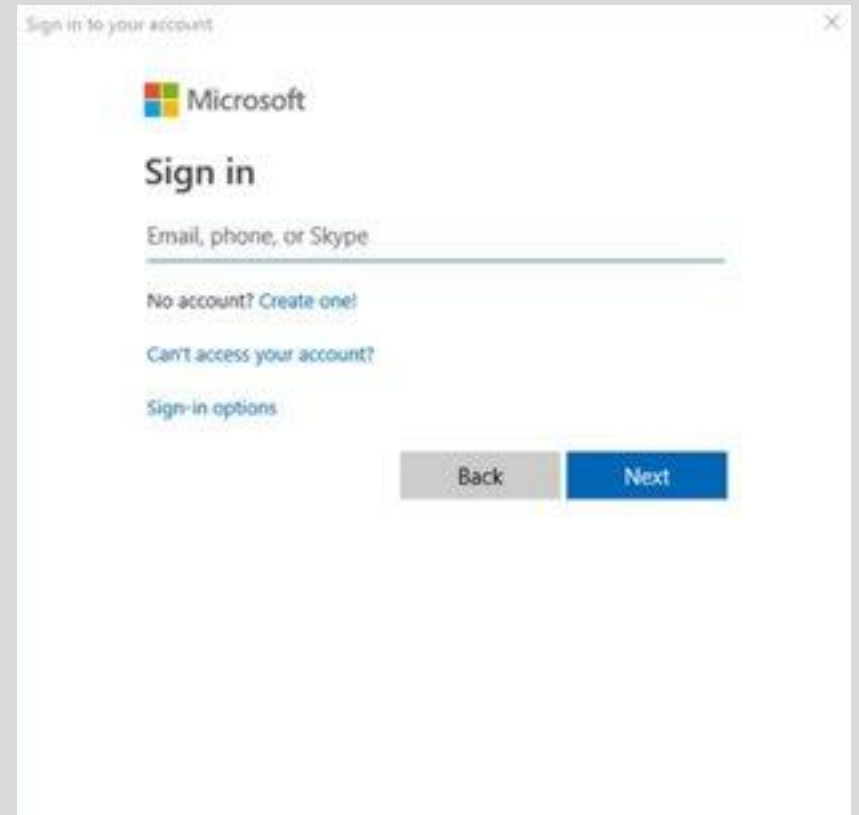
# ~100%

Percentage of password spray attacks  
coming from legacy protocols



# Modern Authentication (Web Flow)

- 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



# Legacy Authentication Examples

## Office 2010

- Does not support modern authentication

## Office 2013

- Does not support modern authentication by default.
- Requires registry keys

## Office 2016 and later

- Uses modern authentication by default

## iOS Native Mail Client

- iOS version 11.0 or later required

## Gmail Client

- Requires most recent version of Gmail

## Outlook Mobile App

- Uses Modern Authentication on all platforms
- Supports MAM policies

[aka.ms/legacyauthguide](https://aka.ms/legacyauthguide)

# Identifying Legacy Auth Usage in Azure AD

## Sign-In Logs to examine usage

Exchange Protocols:

- POP
- IMAP
- MAPI
- SMTP
- ActiveSync

“Other Clients”

- SharePoint
- EWS

If you are federated this will only show the SUCCEFUL

Sign-In Events

Columns

Refresh

Download

Script

Power BI

Troubleshoot

Search is case sensitive and supports 'starts with' operator

User

Filter by name or object id

Username

Filter by UPN

Application

Filter by app name or application...

Sign-in status

All

Client App

Any

Conditional Access

All

Show dates as:

Local

UTC

	USERNAME	APPLICATION	SIGN-IN STATUS	CLIENT APP	CONDITIONAL ACC...	
	audrey.oliver@wingt...	Azure Portal	Success	Browser	Success	
	audrey.oliver@wingt...	Azure Portal	Failure	Browser	Success	
	audrey.oliver@wingt...	Azure Portal	Failure	Browser	Failure	
	audrey.oliver@wingt...	Azure Portal	Failure	Unknown	Not Applied	
7/17/2018, 1:15:08 AM	Hannah Han	hannahhanhaha@wi...	Microsoft App Acce...	Success	Browser	Success
7/16/2018, 11:11:35 PM	Barbara Kess	barbarak@wingtipt...	Azure Portal	Success	Browser	Not Applied
7/16/2018, 11:11:24 PM	Barbara Kess	barbarak@wingtipt...	Azure Portal	Failure	Unknown	Not Applied
7/16/2018, 11:10:58 PM	Barbara Kess	barbarak@wingtipt...	Azure Portal	Failure	Unknown	Not Applied

Timestamp	Trigger Type	IP Address	Bad Password Error Count	Extranet Lockout Error Count	Unique Users Attempted
2/28/2018 6:00 PM	hour	104.208.238.9	0	284	14
2/28/2018 6:00 PM	hour	104.44.252.135	0	27	1
2/28/2018 6:00 PM	hour	168.61.144.85	0	164	2

# Blocking Legacy Authentication Directly at Exchange

## Disable services at the mailbox level

<https://docs.microsoft.com/en-us/powershell/module/exchange/client-access/set-casmailbox?view=exchange-ps>

## Authentication Policies

<https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online>

## Client IP Block

<https://docs.microsoft.com/en-us/powershell/module/exchange/organization/set-organizationconfig?view=exchange-ps>



Ramiro Calderon

ramical@rcdemos.net

Choose the apps the user can use to access their Office 365 email.

```
PS O:\> New-AuthenticationPolicy -Name "Block Basic Authentication"

RunspaceId          : 
AllowBasicAuthActiveSync : False
AllowBasicAuthAutodiscover : False
AllowBasicAuthImap    : False
AllowBasicAuthMapi     : False
AllowBasicAuthOfflineAddressBook : False
AllowBasicAuthOutlookService : False
AllowBasicAuthPop      : False
AllowBasicAuthReportingWebServices : False
AllowBasicAuthSmtpt    : False
AllowBasicAuthWebServices : False
AllowBasicAuthPowerShell : False
```

```
PS O:\> Set-OrganizationConfig -IPListBlocked 41.204.224.0/24,41.203.78.0/24
PS O:\>
```

Save

Cancel



# Blocking Legacy Auth Usage in ADFS/Federation Provider

## Authorization Rules

- Very rich expressions using ADFS claims language
- Happens after authentication
- Applies to ALL applications behind Azure AD

Edit Rule - Block Legacy Auth for Extranet for migrated users

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

Block Legacy Auth for Extranet for migrated users

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value  
== "false"]  
  && c1:[Type ==  
"http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-  
endpoint-absolute-path", Value =~ "/adfs/services/trust/.*"]  
  && c2:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",  
Value =~ "^(?i){[a-z0-9-]{1,64}}$"]  
=> issue(Type =  
"http://schemas.microsoft.com/authorization/claims/deny", Value =  
"DenyUsersWithClaim");
```

# Blocking Legacy Authentication in Azure AD

## Block those that are NOT using FIRST

- Block Today with Conditional Access
- Requires Azure AD P1

## Update Clients

## Only Service Accounts / Apps should remain

### FYI:

Legacy auth support for Exchange Online being deprecated on October 13th, 2020.

Impacts:

- Exchange ActiveSync (EAS)
- IMAP
- POP
- Remote PowerShell

The screenshot displays the Azure AD Conditional Access policy configuration interface. It is divided into two main panes: 'Conditions' on the left and 'Client apps (preview)' on the right.

**Conditions Pane:**

- Info:** Information icon.
- Sign-in risk:** Not configured.
- Device platforms:** Not configured.
- Locations:** Not configured.
- Client apps (preview):** 1 included (highlighted in blue).
- Time (preview):** Not configured.
- Device state (preview):** Not configured.

**Client apps (preview) Pane:**

- Configure:** Yes (selected) / No.
- Select the client apps this policy will apply to:**
- ☐ Browser
- ☒ Mobile apps and desktop clients (highlighted with a red box)
- ☐ Modern authentication clients
- ☐ Exchange ActiveSync clients
- ☒ Other clients (highlighted with a red box)

# Agenda

- Protect Your Admins
- Enable Password Hash Sync
- Identity Protection
- Azure AD Password Protection
- Blocking Legacy Auth
- Security Defaults and Go Dos



# Security Defaults

## One-click method

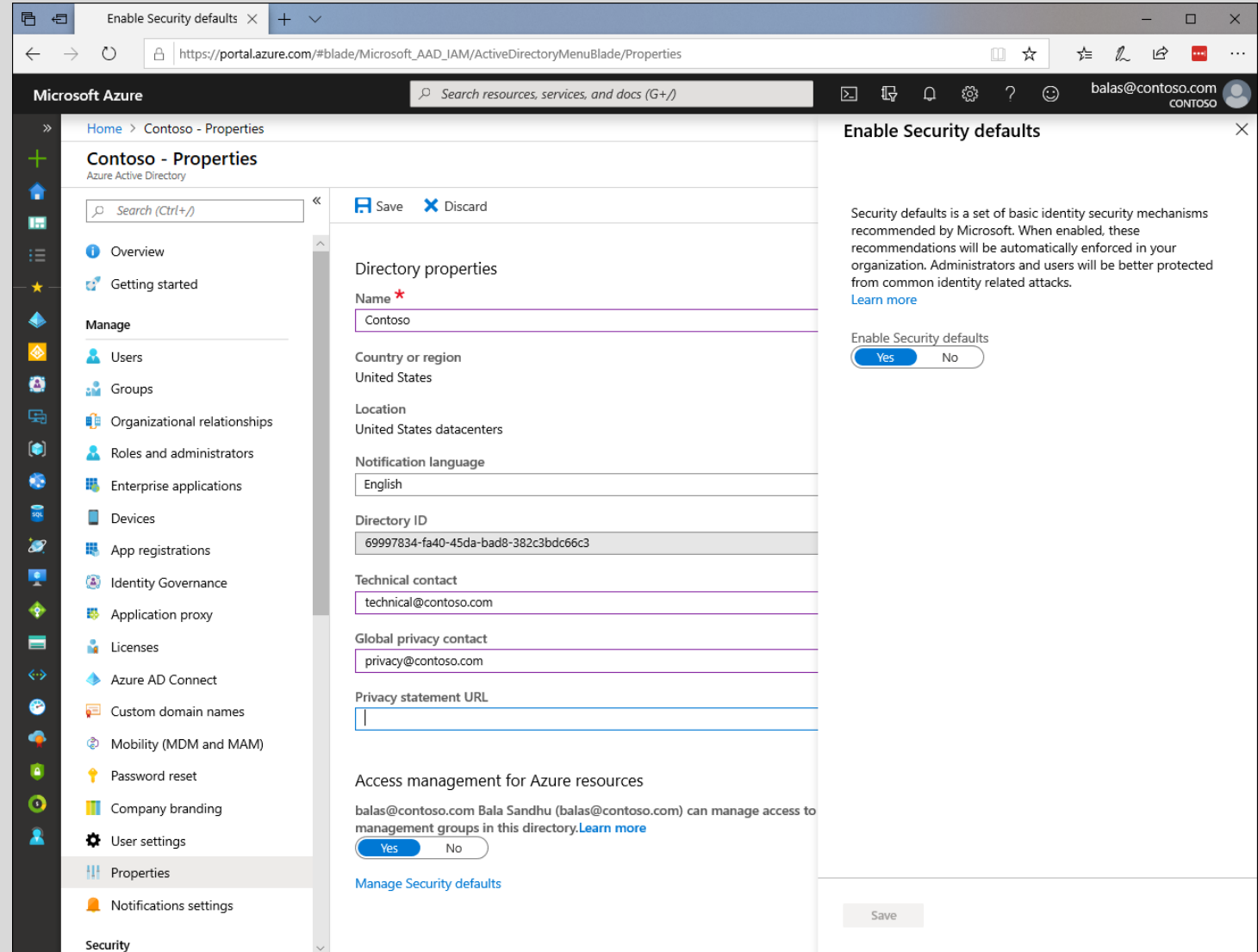
Enables MFA for all users AND blocks legacy auth tenant wide

It's FREE!!!

aka.ms/enableMFA

## Secure by default

New tenants will have security defaults enabled by default



# Go Do's!

## Today

- Enable MFA for your Admins!
  - Better yet, use PIM!
- Turn on PHS!
- Enable Password Protection in Audit Mode

## Next week

- Start looking at legacy auth logs
- Start planning your DC upgrades
- Create your resilient access control strategy

## Next Month

- Enable Password Protection
- Enable User Risk
  - Block or Password Reset
- Start testing FIDO2
- Start disabling legacy auth
- Enable Sign-In Risk policy
- Implement resilient access control strategy



# Thank you.

Follow Microsoft Azure AD



**[aka.ms/enableMFA](https://aka.ms/enableMFA)**  
...it's free!