Microsoft

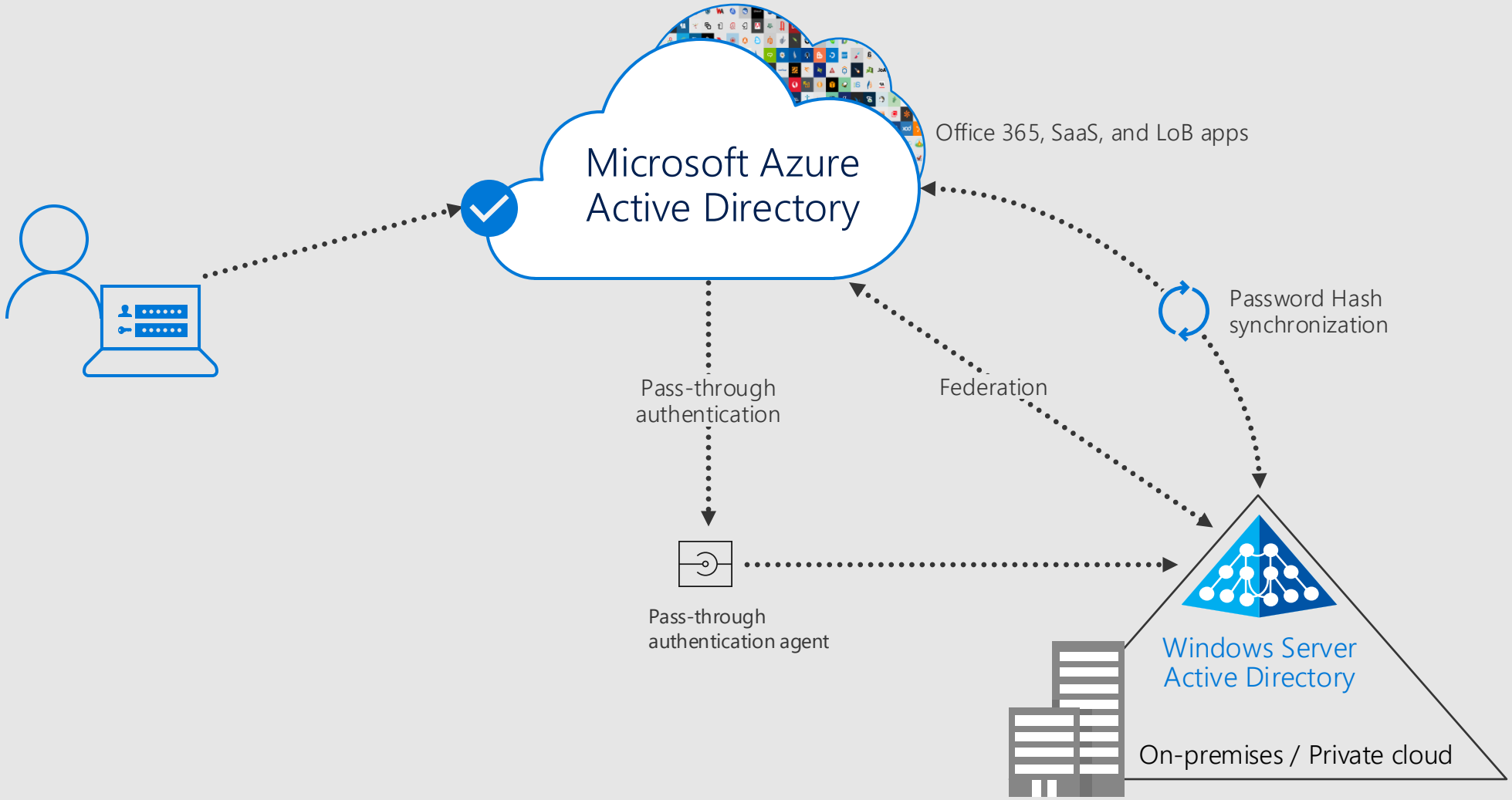
Leverage the cloud to strengthen your on-premises Active Directory security

Charity Shelbourne
Mark Morowczynski (@markmorow)
Program Managers-Identity Division

Agenda

- Protect your AD infrastructure
- Protect your AD passwords
- Password-less with Active Directory

What does Hybrid look like?



Azure AD Connect Health

Protect and monitor your **on-premises** identity infrastructure

Alerts

Monitor health of identity servers and receive alert notifications in email

Security Reporting

Detect risky IP addresses and analyze failed requests

Usage Analytics

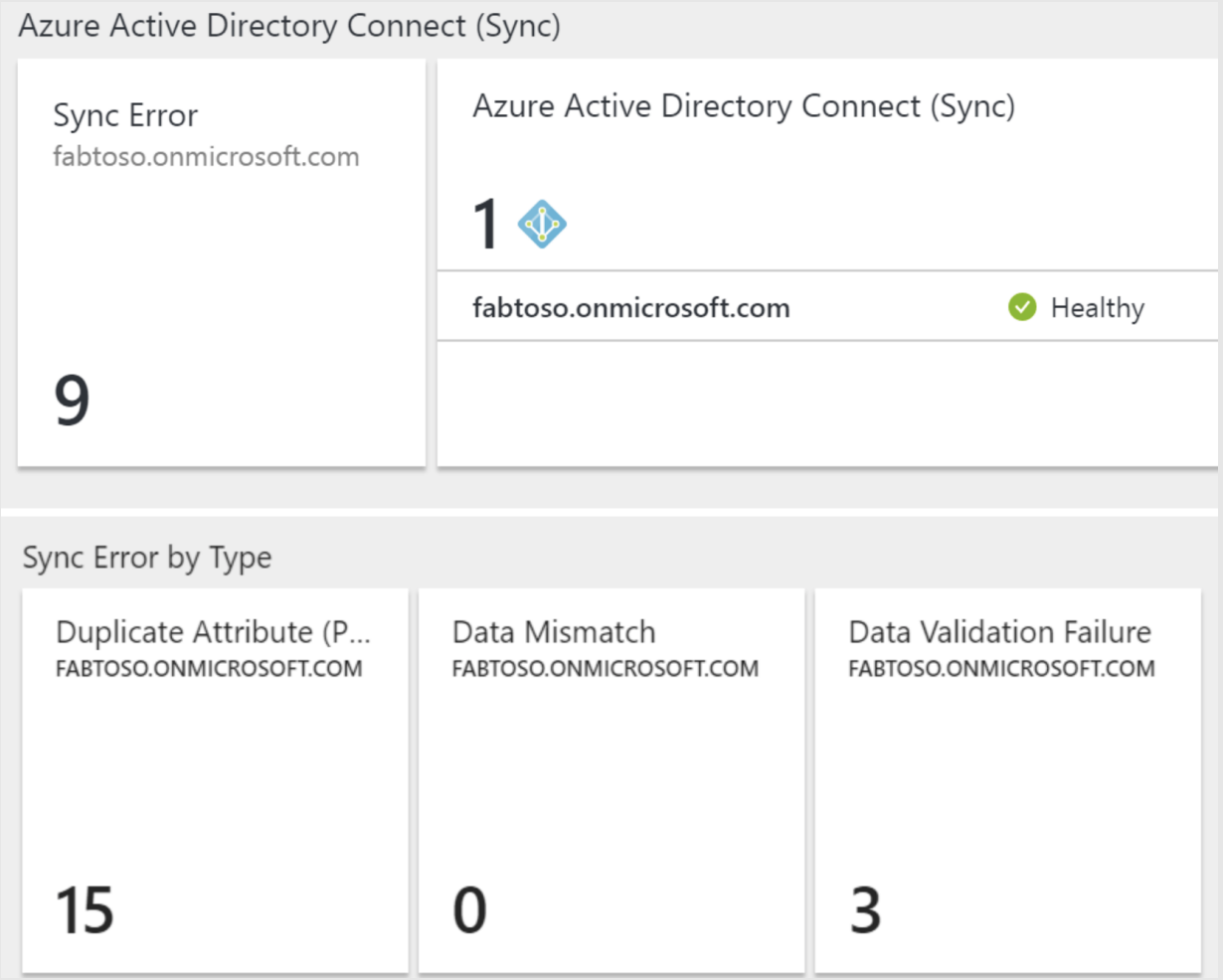
Analyze with different pivots such as app, users, network location

Performance Monitoring

View performance data trends and sync operational insights.

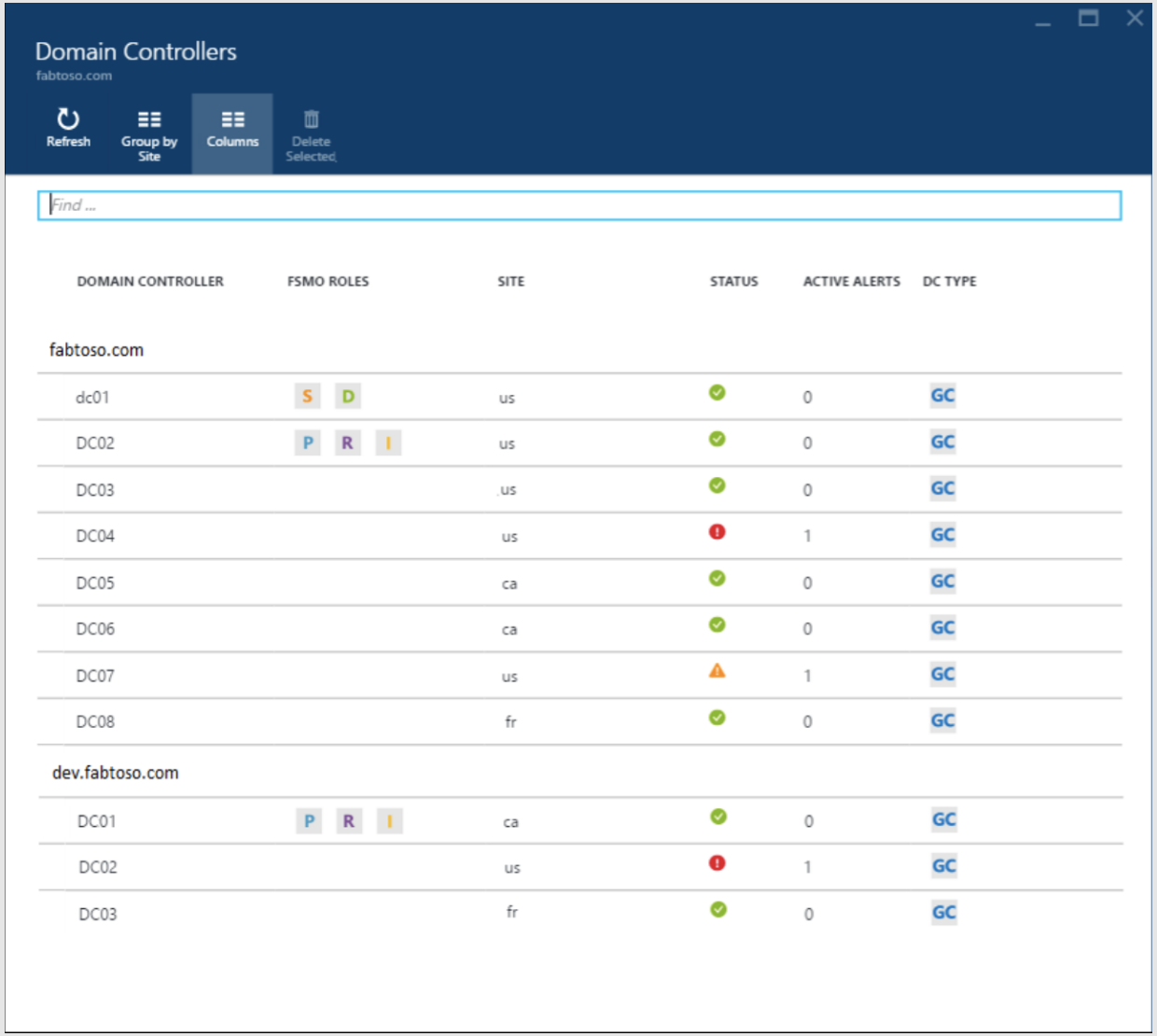
Azure AD Connect Health for Sync

- Built-in to Azure AD Connect!
- Sync Insights and Performance trends
- Sync Attribute Error Reporting
  - Duplicate Attributes- proxyAddress and UPN
  - Softmatch Fail
  - Unsupported characters
  - Large Attributes
- Resolution recommendations as well

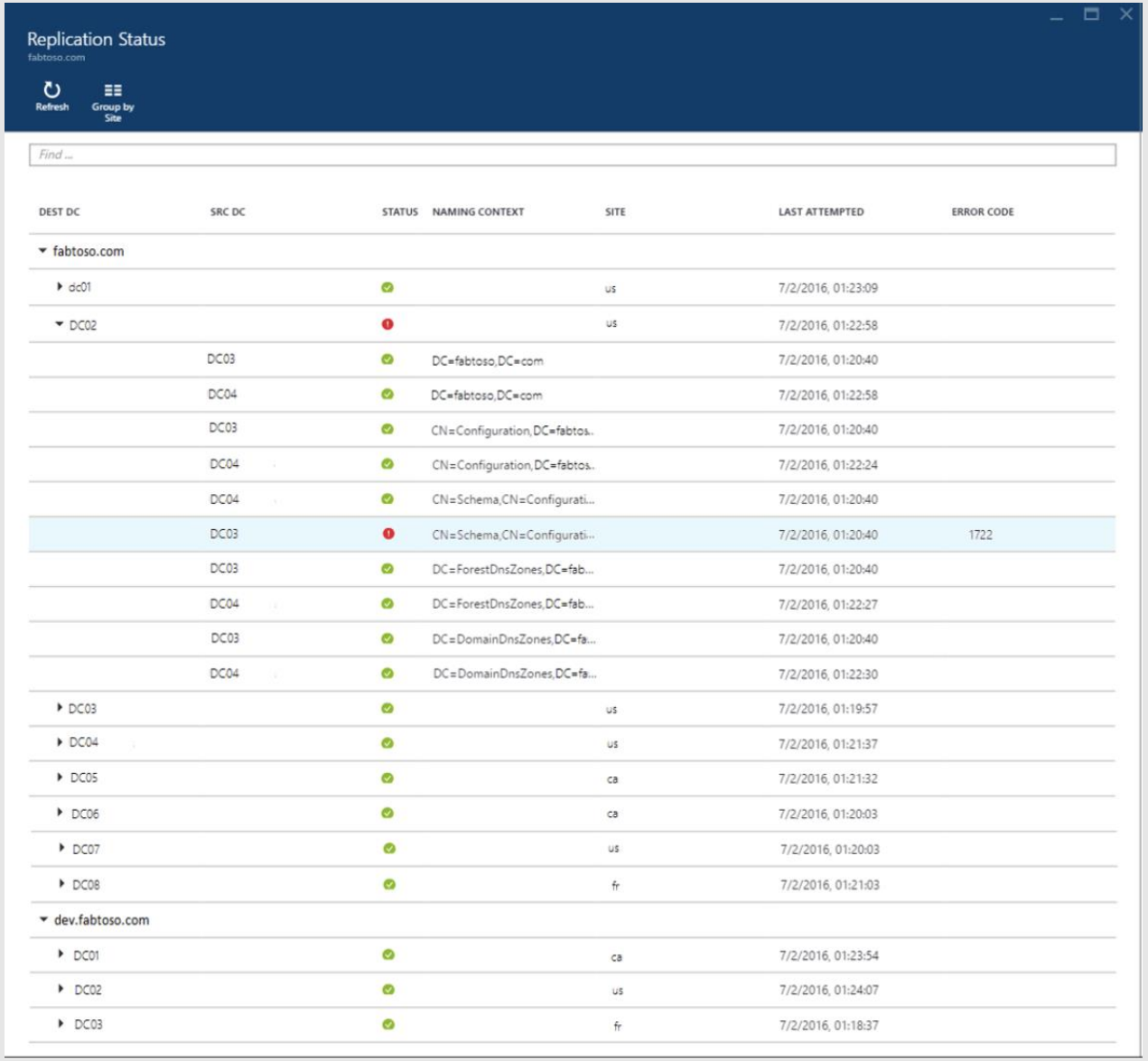


Azure AD Connect Health for Active Directory

- Agent installed on Domain Controllers
- Server 2008 R2-2019, including Server Core
- Outbound connectivity req, but can go through proxy
- Also can get perf and replication dashboard



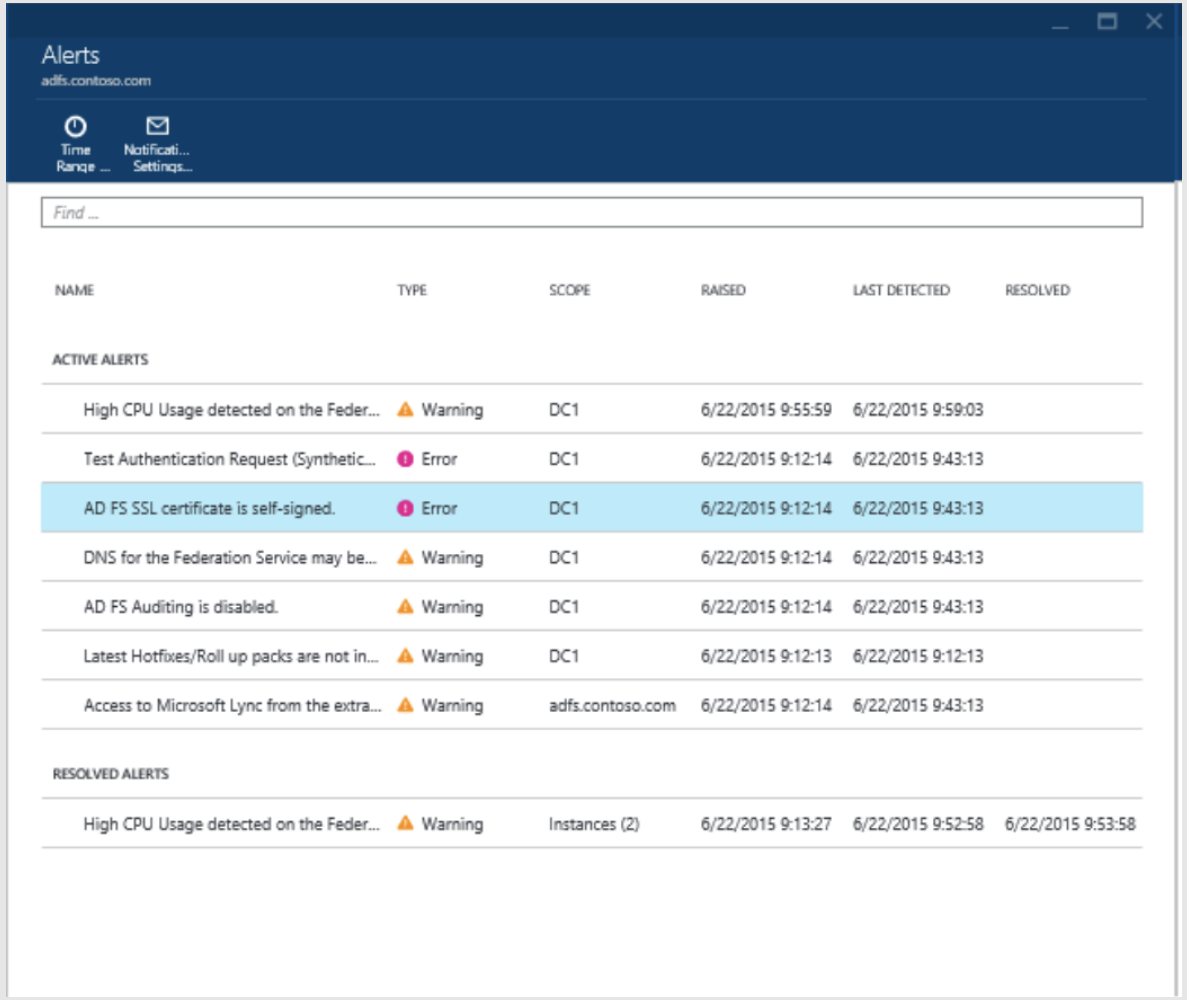
Azure AD Connect Health DS Dashboards



DEST DC	SRC DC	STATUS	NAMING CONTEXT	SITE	LAST ATTEMPTED	ERROR CODE
fabtoso.com						
dc01		✓		us	7/2/2016, 01:23:09	
DC02		!		us	7/2/2016, 01:22:58	
	DC03	✓	DC=fabtoso,DC=com		7/2/2016, 01:20:40	
	DC04	✓	DC=fabtoso,DC=com		7/2/2016, 01:22:58	
	DC03	✓	CN=Configuration,DC=fabtos..		7/2/2016, 01:20:40	
	DC04	✓	CN=Configuration,DC=fabtos..		7/2/2016, 01:22:24	
	DC04	✓	CN=Schema,CN=Configurati...		7/2/2016, 01:20:40	
	DC03	!	CN=Schema,CN=Configurati...		7/2/2016, 01:20:40	1722
	DC03	✓	DC=ForestDnsZones,DC=fab...		7/2/2016, 01:20:40	
	DC04	✓	DC=ForestDnsZones,DC=fab...		7/2/2016, 01:22:27	
	DC03	✓	DC=DomainDnsZones,DC=fa...		7/2/2016, 01:20:40	
	DC04	✓	DC=DomainDnsZones,DC=fa...		7/2/2016, 01:22:30	
DC03		✓		us	7/2/2016, 01:19:57	
DC04		✓		us	7/2/2016, 01:21:37	
DC05		✓		ca	7/2/2016, 01:21:32	
DC06		✓		ca	7/2/2016, 01:20:03	
DC07		✓		us	7/2/2016, 01:20:03	
DC08		✓		fr	7/2/2016, 01:21:03	
dev.fabtoso.com						
DC01		✓		ca	7/2/2016, 01:23:54	
DC02		✓		us	7/2/2016, 01:24:07	
DC03		✓		fr	7/2/2016, 01:18:37	

Azure AD Connect Health for ADFS

- Installed on WAP and ADFS servers
- Common issues such as missing updates, cert expiring
- Also performance monitoring and usage analysis
- Risky IP Report critical for Password Spray detection



NAME	TYPE	SCOPE	RAISED	LAST DETECTED	RESOLVED
ACTIVE ALERTS					
High CPU Usage detected on the Feder...	Warning	DC1	6/22/2015 9:55:59	6/22/2015 9:59:03	
Test Authentication Request (Synthetic...	Error	DC1	6/22/2015 9:12:14	6/22/2015 9:43:13	
AD FS SSL certificate is self-signed.	Error	DC1	6/22/2015 9:12:14	6/22/2015 9:43:13	
DNS for the Federation Service may be...	Warning	DC1	6/22/2015 9:12:14	6/22/2015 9:43:13	
AD FS Auditing is disabled.	Warning	DC1	6/22/2015 9:12:14	6/22/2015 9:43:13	
Latest Hotfixes/Roll up packs are not in...	Warning	DC1	6/22/2015 9:12:13	6/22/2015 9:12:13	
Access to Microsoft Lync from the extra...	Warning	adfs.contoso.com	6/22/2015 9:12:14	6/22/2015 9:43:13	
RESOLVED ALERTS					
High CPU Usage detected on the Feder...	Warning	Instances (2)	6/22/2015 9:13:27	6/22/2015 9:52:58	6/22/2015 9:53:58

Risky IP Report

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

- Look at Unique Users Attempted and Bad Password Error count per IP for password spray
- Remember Azure AD will ONLY see the SUCESSFUL logins when you are federated for now…

ADFS Sign-Ins in Azure AD- First Half of 2020

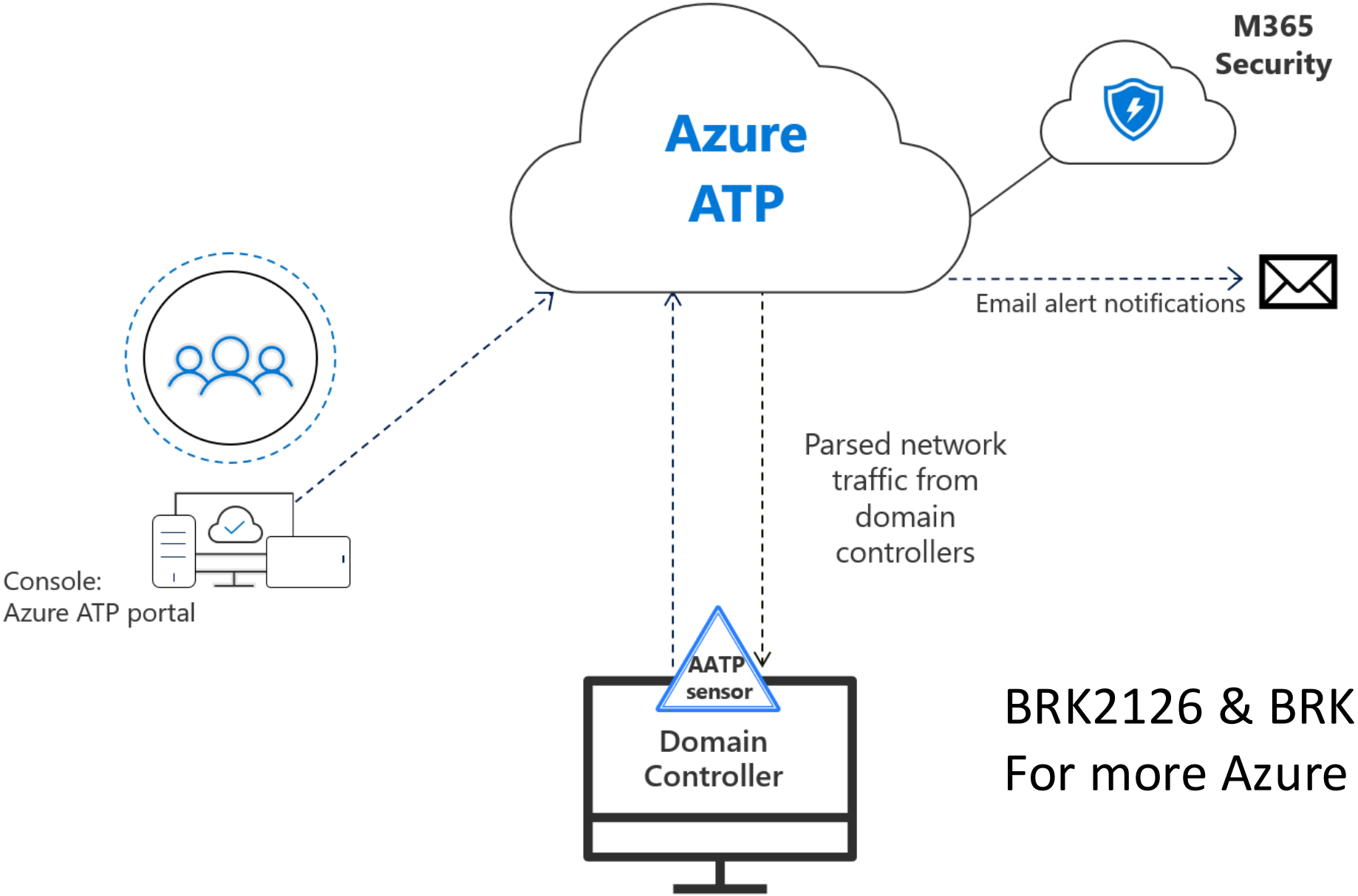
Date : **Last 1 month** | Show dates as: **Local** | User : **Zhanna Voloshina** | Token issuer type : **Federated (ADFS)** | Add filters

Date	Request ID	User	Application	Status	IP address	Location	Conditional acce...	Token issuer type
11/5/2019, 9:58:56 AM	383f6d21-45f8-4ed1-...	Zhanna Voloshina	urn:federation:Micros...	Success	10.221.133.3		Not Applied	Federated (ADFS)
11/4/2019, 2:55:54 PM	4e2c9581-213d-41ee...	Zhanna Voloshina	urn:federation:Micros...	Success	10.166.26.9		Not Applied	Federated (ADFS)
11/4/2019, 2:55:11 PM	1d9394c2-8a08-4c07...	Zhanna Voloshina	urn:federation:Micros...	Success	10.166.26.9		Not Applied	Federated (ADFS)

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only (Preview) | Additional Details

Date	11/4/2019, 1:59:30 PM	User	Zhanna Voloshina	Token issuer type	Federated (ADFS)
Request ID	f2eae539-3107-4739-a3fb-d155b1243861	Username	zhvolosh@microsoft.com	Token issuer name	msft.sts.microsoft.com
Correlation ID	17d0bbf6-43f1-472e-b0d9-351561e818d6	User ID	c1b5046d-f0a8-4085-b211-4f4ee616435a	Latency	N/A
Status	Success	Alternate sign-in name	zhvolosh@microsoft.com		
		Application	urn:federation:MicrosoftOnline		
		Application ID			
		Resource	urn:federation:MicrosoftOnline		
		Resource ID			
		Client app	N/A		

Azure ATP Architecture



BRK2126 & BRK2127

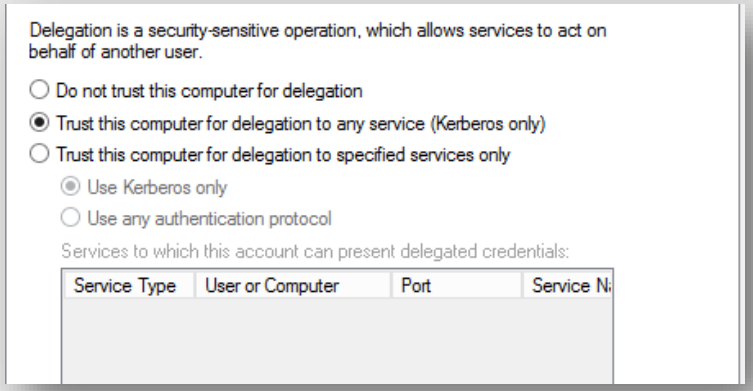
For more Azure ATP

Risky configurations = Lower security

Clear text authentication

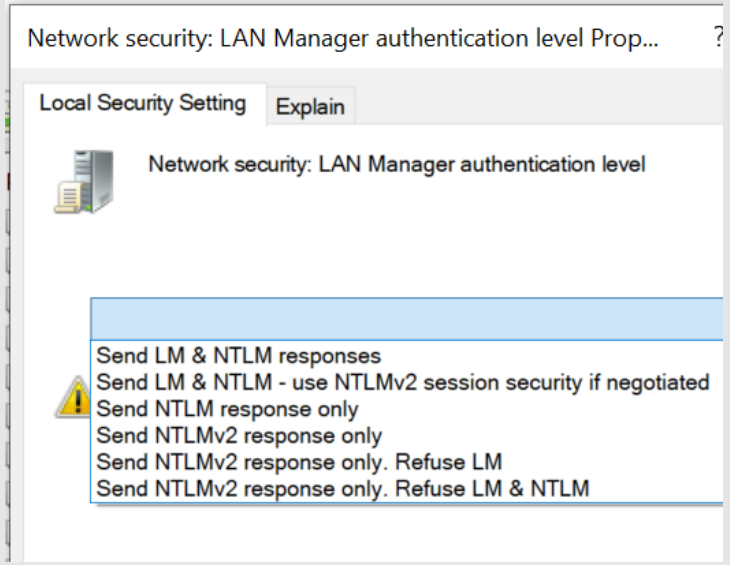
Exposed Passwords

Unconstrained delegation rights



Rogue Impersonation

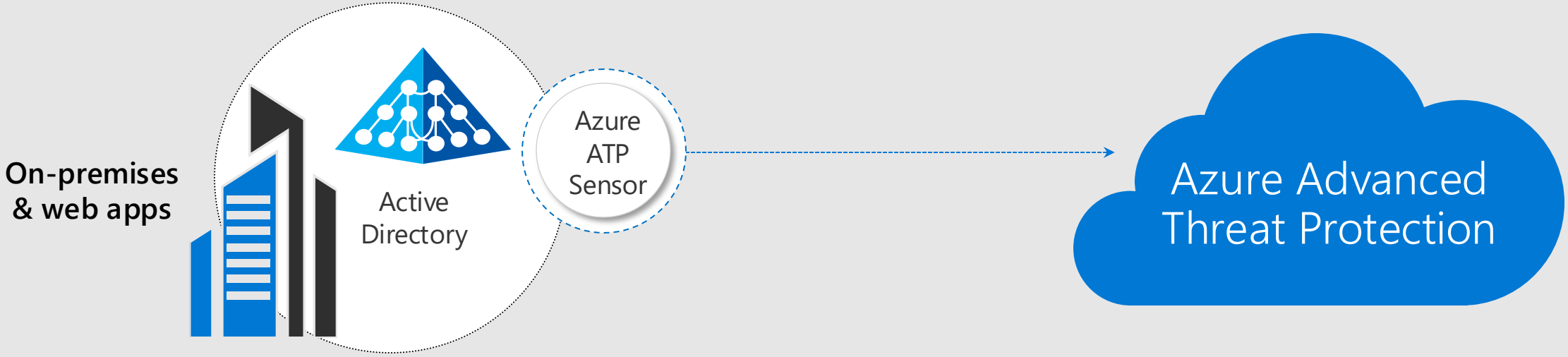
Legacy authentication in use



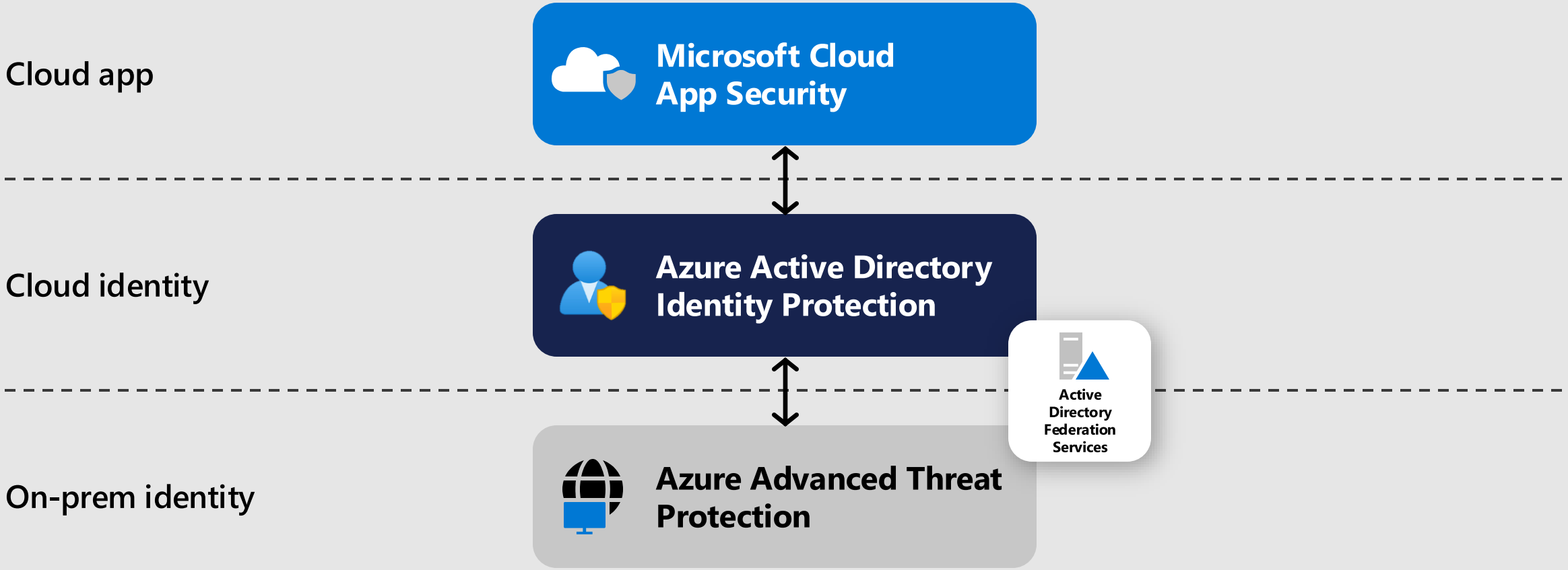
Easier to Attack

Azure ATP Data Sources and Technologies

NETWORK TRAFFIC ANALYTICS	SECURITY EVENTS & ACTIVE DIRECTORY DATA	USER BEHAVIOR ANALYTICS	CLOUD BASED REAL-TIME DETECTIONS
Inspect network traffic: NTLM, Kerberos, LDAP, RPC, DNS, SMB	Inspect events, event tracing and profile active directory entities	Profile users & entities behavior, identify behavior anomalies	Data enrichment and correlation in the cloud, for real time detections



End-to-end Identity Protection



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

Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > Identity Protection - Overview > Risky users

Risky users

Learn more | Download | Select all | Confirm user(s) compromised | Dismiss user(s) risk | Refresh | Columns

Welcome to Azure AD Identity Protection's advanced 'Risky users' view. Click to go back to the old experience. →

Show dates as: **Local** | Risk level : **High, Medium, Low** | Status : **Active** | Add filters

User	Risk state	Risk level	Risk last updated
Caleb Baker	At risk	Low	10/29/2019, 1:17:43 AM
Audrey Oliver	At risk	Medium	10/25/2019, 5:31:02 PM
Anna Barhudarian	At risk	High	10/17/2019, 2:51:38 PM
Rajat Luthra	At risk	Low	10/11/2019, 2:18:40 PM
Gia Luthra	Confirmed compromised	High	10/7/2019, 2:35:11 PM
Peter Eckardt	At risk	High	10/7/2019, 5:23:25 AM
Chris Donovan	At risk	High	10/7/2019, 2:04:00 AM

Details

User's sign-ins | User's risky sign-ins | User's risk detections | Reset password | Confirm user compromised | Dismiss user risk | Block user | Investigate with Azure ATP

Basic info | Recent risky sign-ins | Detections not linked to a sign-in | Risk history

User	Audrey Oliver	Risk state	At risk	Office location	
Roles	Global admin	Risk level	Medium	Department	Sales
Username	audrey.oliver@wingtiptoysonline.com	Details	-	Mobile phone	
User ID	bab8aed7-6f64-4cf2-8d58-49c36888f05e	Risk last updated	10/25/2019, 5:31:02 PM		

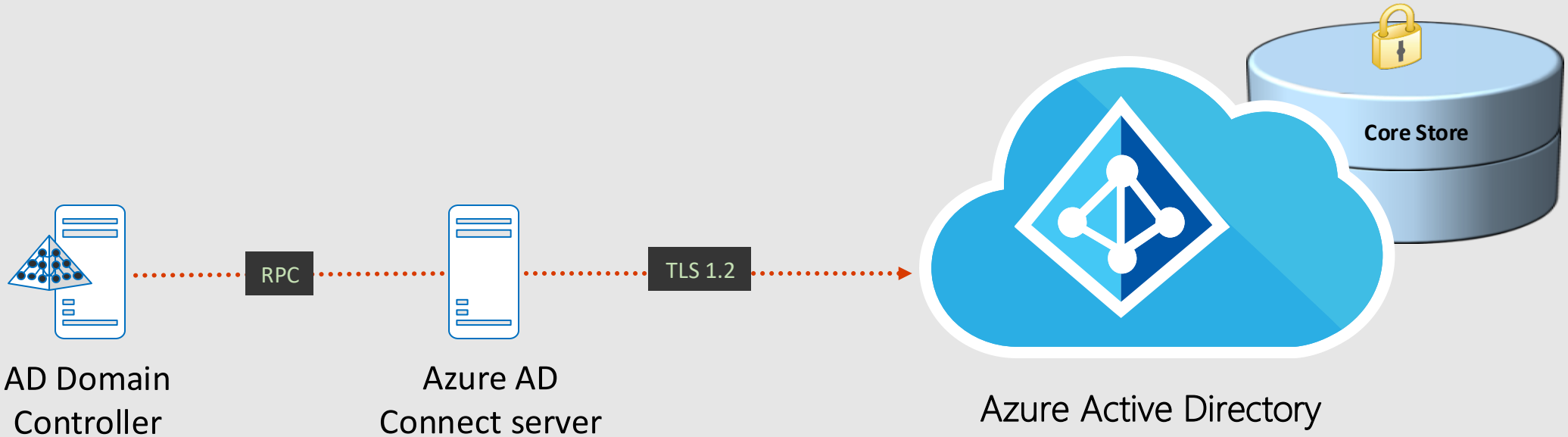
Agenda

- Protect your AD infrastructure
- Protect your AD passwords
- Password-less with Active Directory

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



MD4 Hash (Password)

PBKDF2 (salt + MD4(password), 1000)

aka.ms/aadphs

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

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

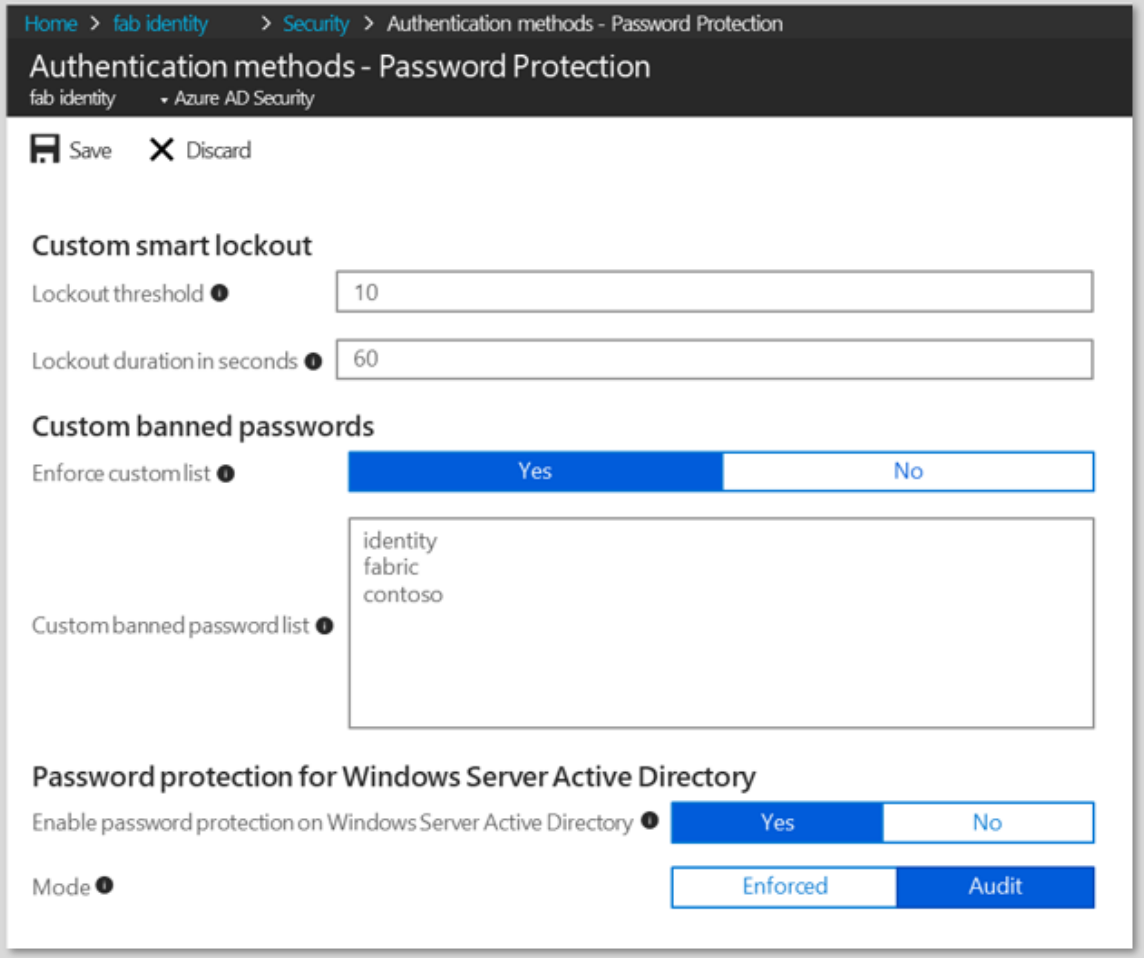
1,000 words and phrases unique to your organization. Do NOT put variations!

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.



Banned
Password Lists

$\neq$

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

$3curePP@$$w0rd8

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

Combined list:

$3curePP@$$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

$3curePP@$$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

"secure" "password"

1 Global and custom lists are combined

2 All inputs normalized

3 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

"secure" "password"

1 + 1 + 1

3 points = Weak Password!!

1 Global and custom lists are combined

2 All inputs normalized

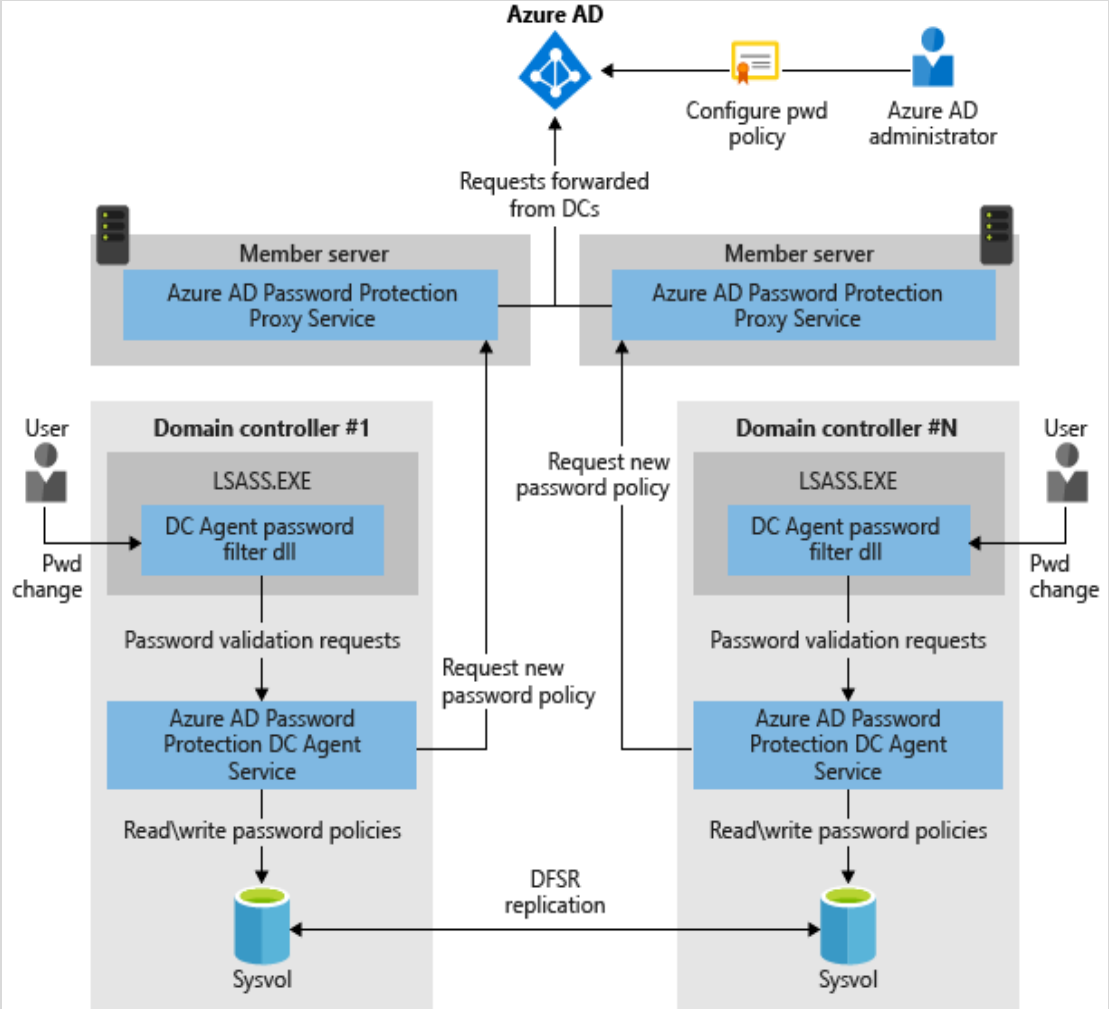
3 Identify banned passwords

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

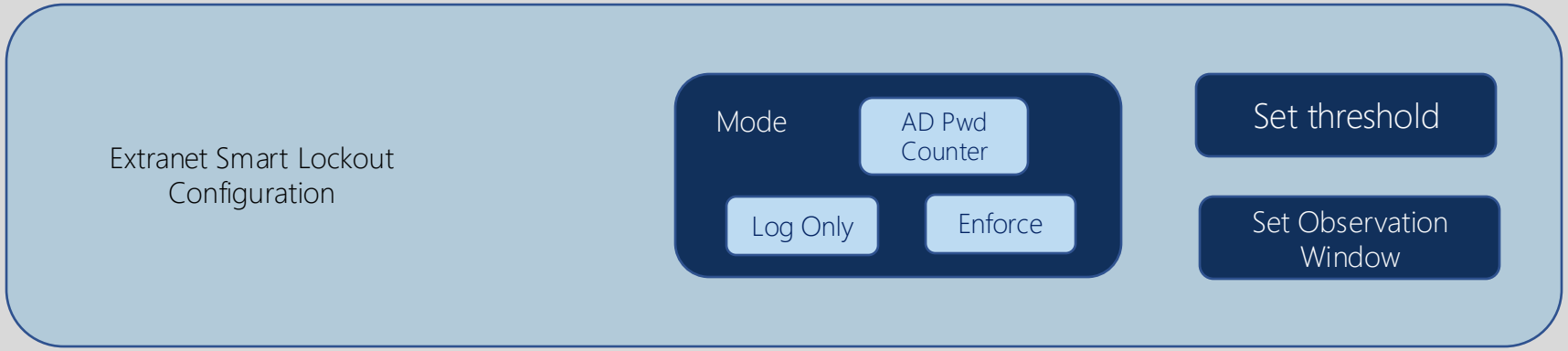
"what if" mode – logs when password would have been rejected

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

AD FS Extranet Smart Lockout

Protect users from extranet account lockouts due to password spray attacks

ESL differentiates sign-in attempts from a valid user vs an attempted attack, locking out attackers and allowing valid users to keep using their accounts.



Available for AD FS 2016 and 2019

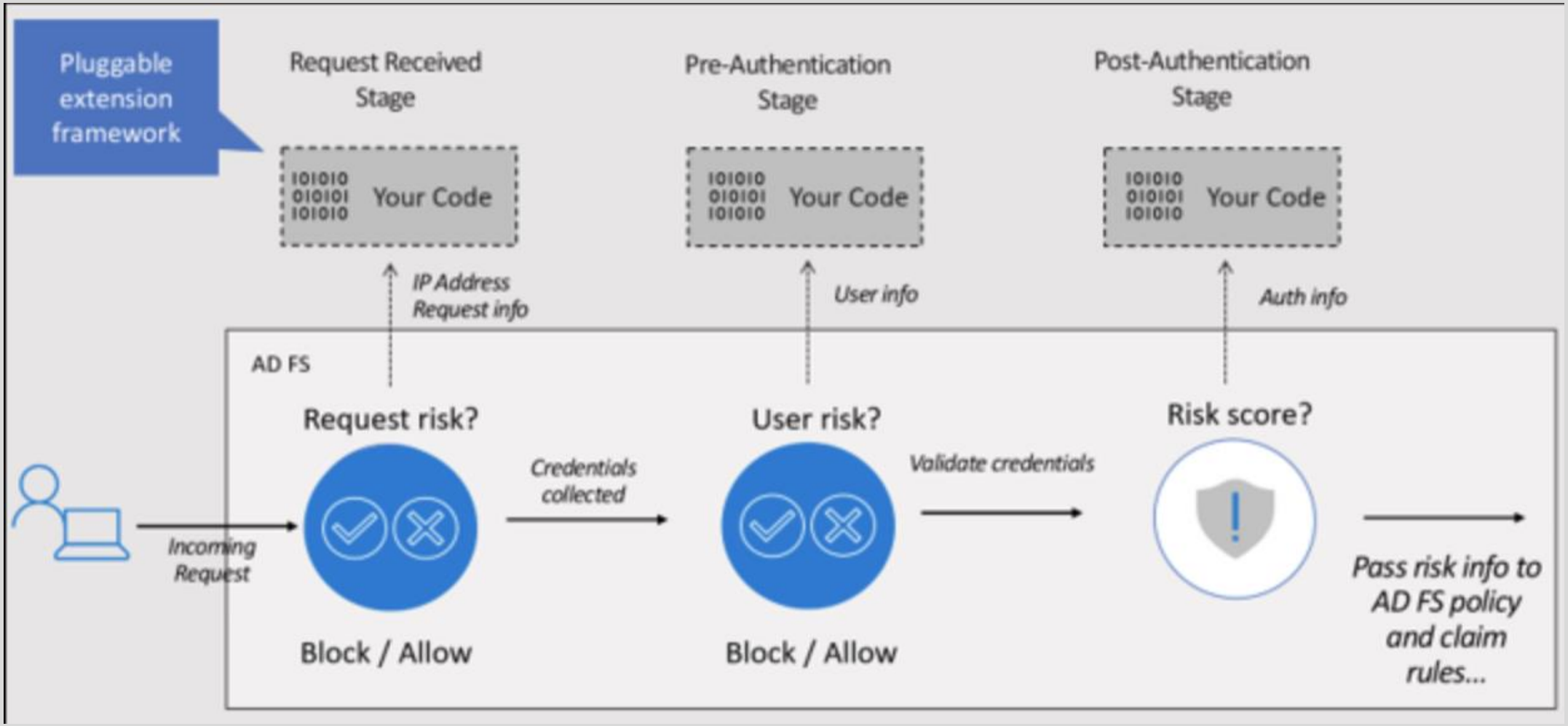
New features for AD FS 2019:

- Customize separate lockout thresholds for familiar locations vs unknown IP addresses
- Protect users while configuring smart lockout in ‘log only’ mode to continue enforcing ‘soft lockout’ behavior

ADFS 2019 Risk Assessment Model

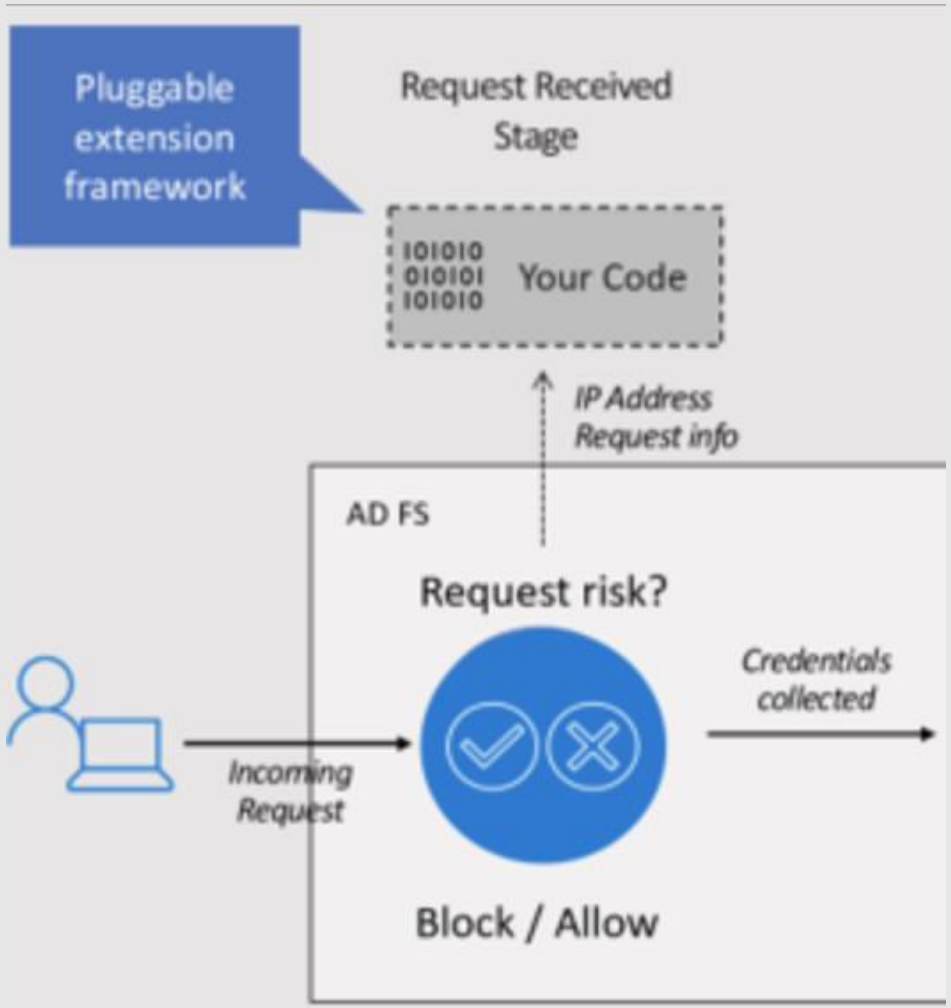
- Build your own plug-ins to block or assign a risk score at 3 different stages of the request.
  - Request Received
  - Pre-Authentication
  - Post-Authentication
- .NET 4.7 and later, Visual Studio
- Sample code-https://github.com/Microsoft/adfs-sample-RiskAssessmentModel-RiskyIPBlock
- Use Azure AD Identity protection or your own threat intel feed

ADFS 2019 Risk Assessment Model



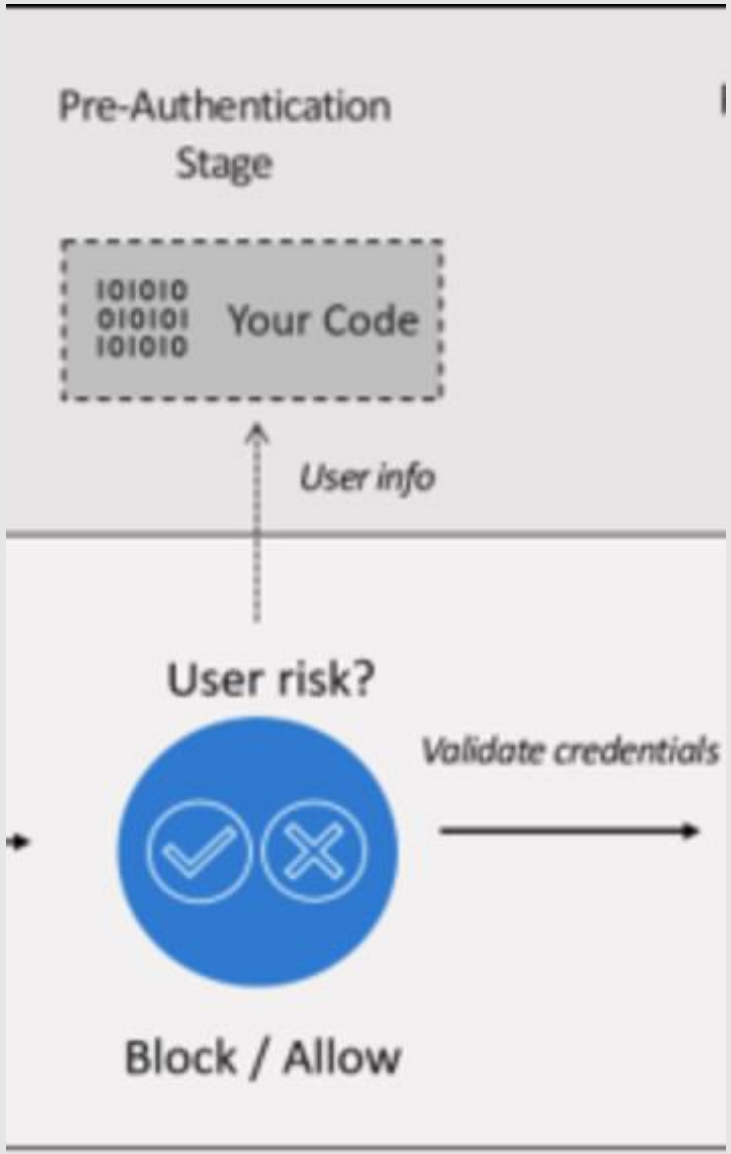
Request Received Stage

- BEFORE credentials are collected
- Request context
  - IP Address
  - HTTP method
  - Proxy or DNS
- Example: Reading IP address, Using Risky IP from ADFS Connect Health or other source to drop



Pre-Authentication Stage

- User provides credentials but BEFORE ADFS evaluates them
- Request Context
  - Security Context- User Token, User Identifier, etc
  - Protocol Context- Auth Protocol, ClientID, ResourceID
- Example: High risk user in Identity Protection, block the sign-in entirely



Post-Authentication Stage

- AFTER ADFS has performed authentication
- Request Context
  - Success or Failure of the login
- Example: Pass the risk score down the pipeline for other action/decision. Requiring MFA if user is medium risk

Sample Code Example

- Calling Identity Protection riskyUsers API
- Update documentation with sample code soon

```
static RiskyList GetRiskyUsers(string tokenType, string accessToken)
{
    var riskyReq = HttpWebRequest.Create("https://graph.microsoft.com/beta/riskyUsers");
    riskyReq.Headers.Add("Authorization", String.Format("{0} {1}", tokenType, accessToken));

    var responseRisky = riskyReq.GetResponse();
    Dictionary<string, object> RiskyjsonResponse = new Dictionary<string, object>();
    using (Stream stream = responseRisky.GetResponseStream())
    {
        StreamReader reader = new StreamReader(stream, Encoding.UTF8);
        String responseString = reader.ReadToEnd();
        JavaScriptSerializer json_serializer = new JavaScriptSerializer();
        return json_serializer.Deserialize<RiskyList>(responseString);
    }
}
```

ADFS 2019 Pre-Auth Risk Assessment Module

Charity Shelbourne

ADFS 2019 Risk Assessment Model Best Practices

- Think about the authentication latency on user experience
  - Latency impact will be on how long the risk assessment logic takes
  - TEST! TEST! TEST!
- Avoid process wide locks, this will cause ADFS to no longer process is parallel
- Provide logging and auditing so it shows up in the normal ADFS logs
- Don’t forget your OPS Processes!- As you add, remove, update your source, you need to update the plug-in

Agenda

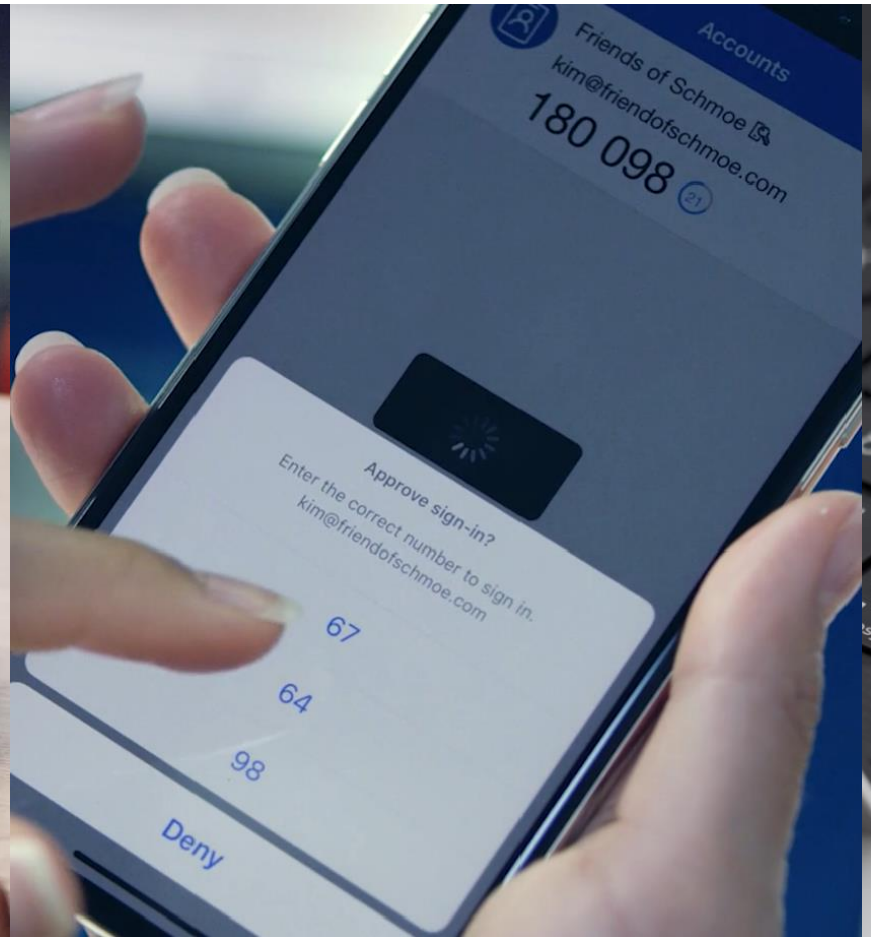
- Protect your AD infrastructure
- Protect your AD passwords
- Password-less with Active Directory

Getting to a world without passwords

High security, convenient methods of strong authentication

Windows Hello

Microsoft Authenticator



FIDO2 Security Keys

FIDO2

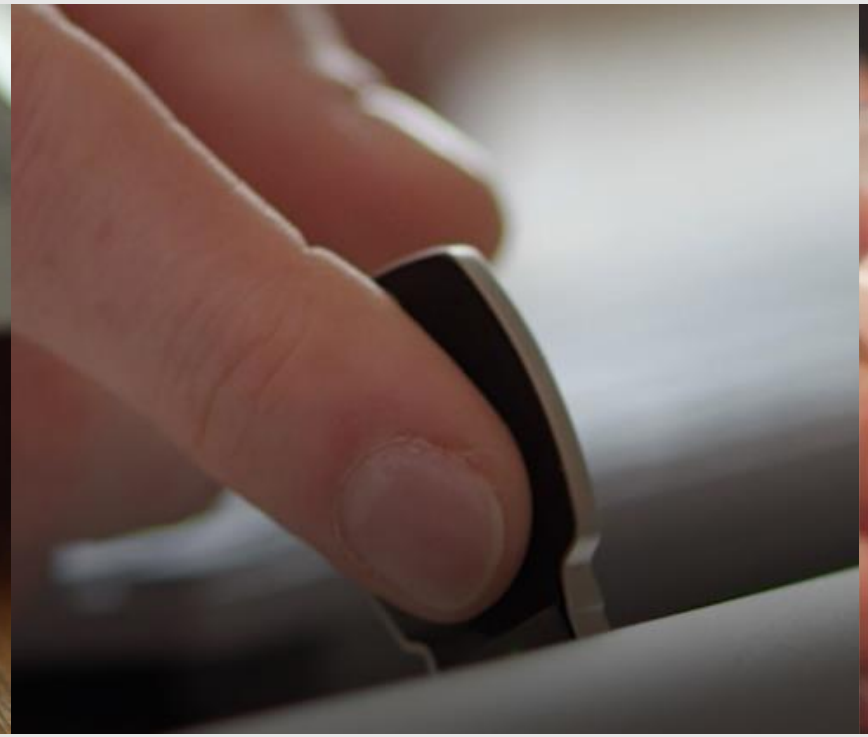
- Standards-based Passwordless authentication
- WebAuthN and CTAP(Client To Authenticator Protocol) standards are final
- Public/Private Key infrastructure
  - Private keys are securely stored on the device
- Local gesture (e.g., biometric, PIN) required
- Data bound to a single device

Passwordless with FIDO2 security keys

Open standards that allow innovative offerings from partners, serving broad range of user needs

USB/NFC Key

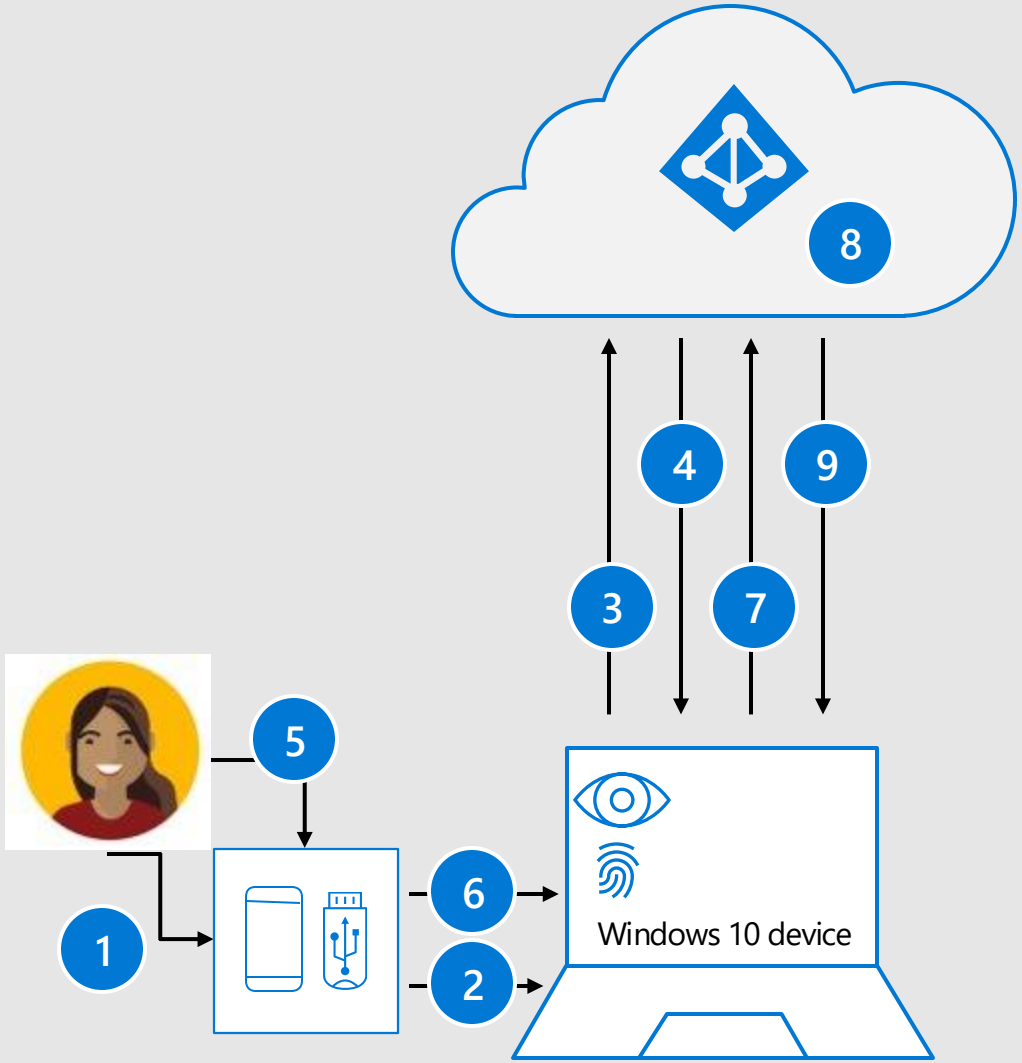
USB Biometric Key



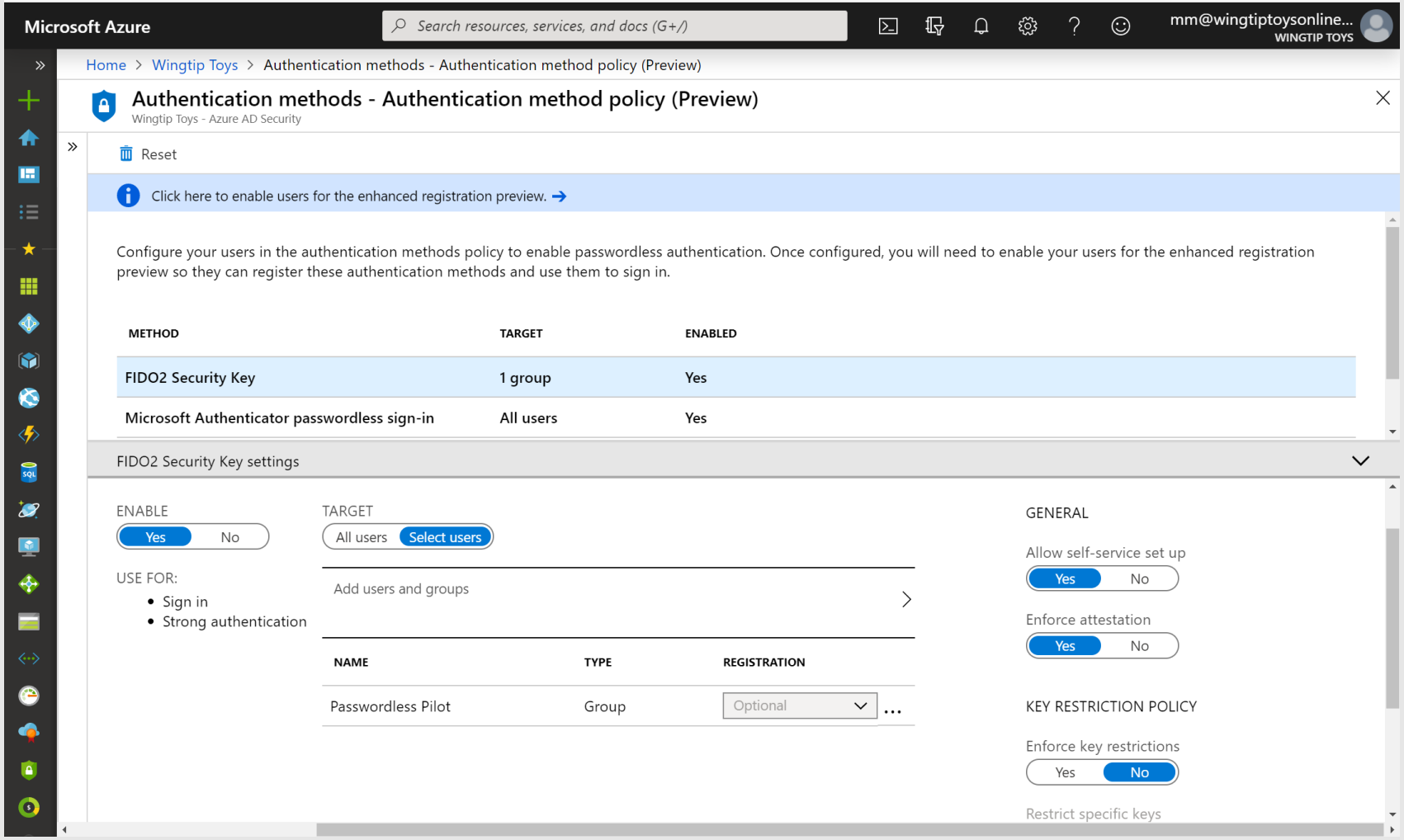
NFC Badge

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 signature
9. Azure AD returns PRT to enable access to cloud resources



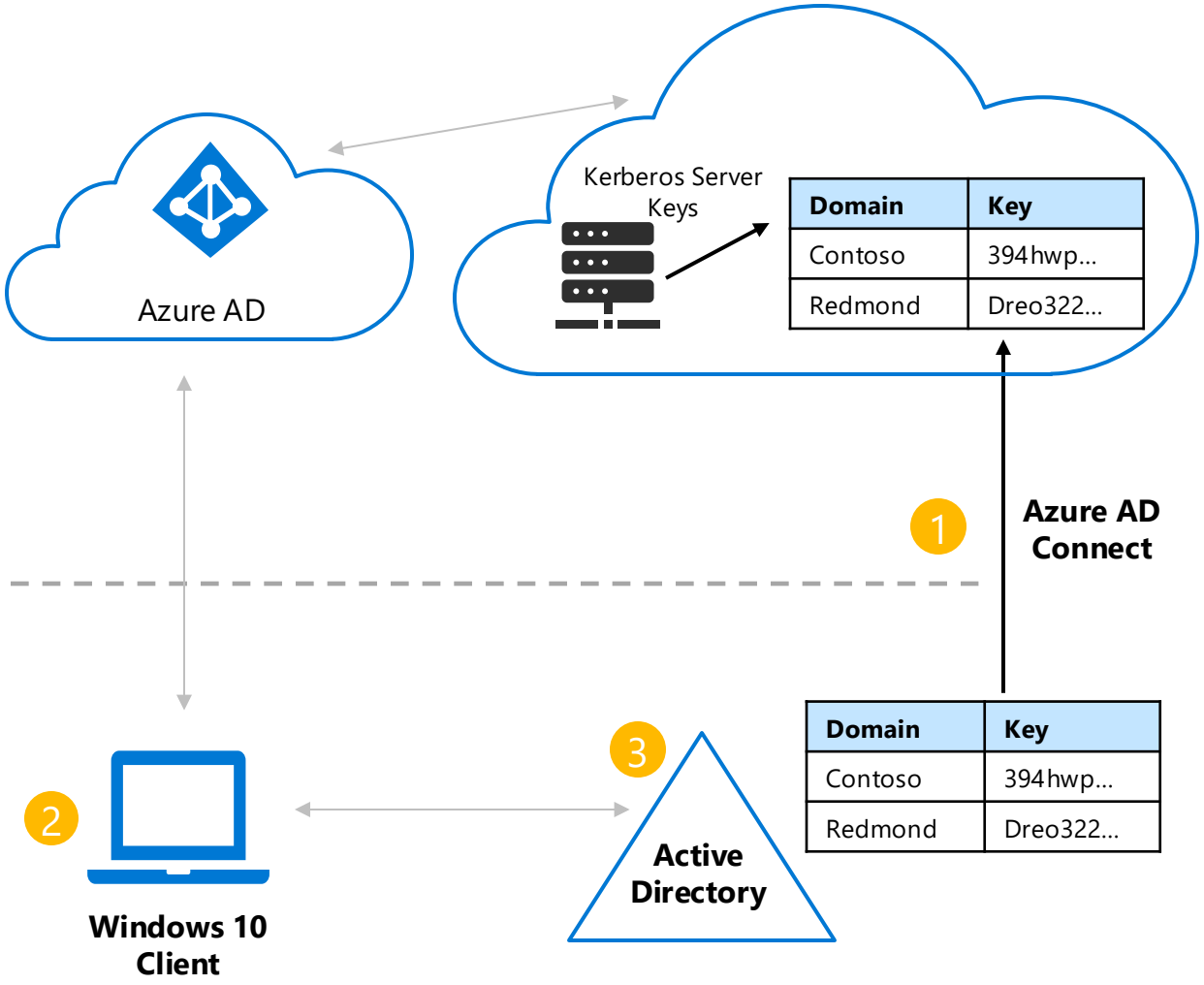
Authentication methods management



Microsoft

FIDO2 public preview expanding to Hybrid environments (Early 2020)

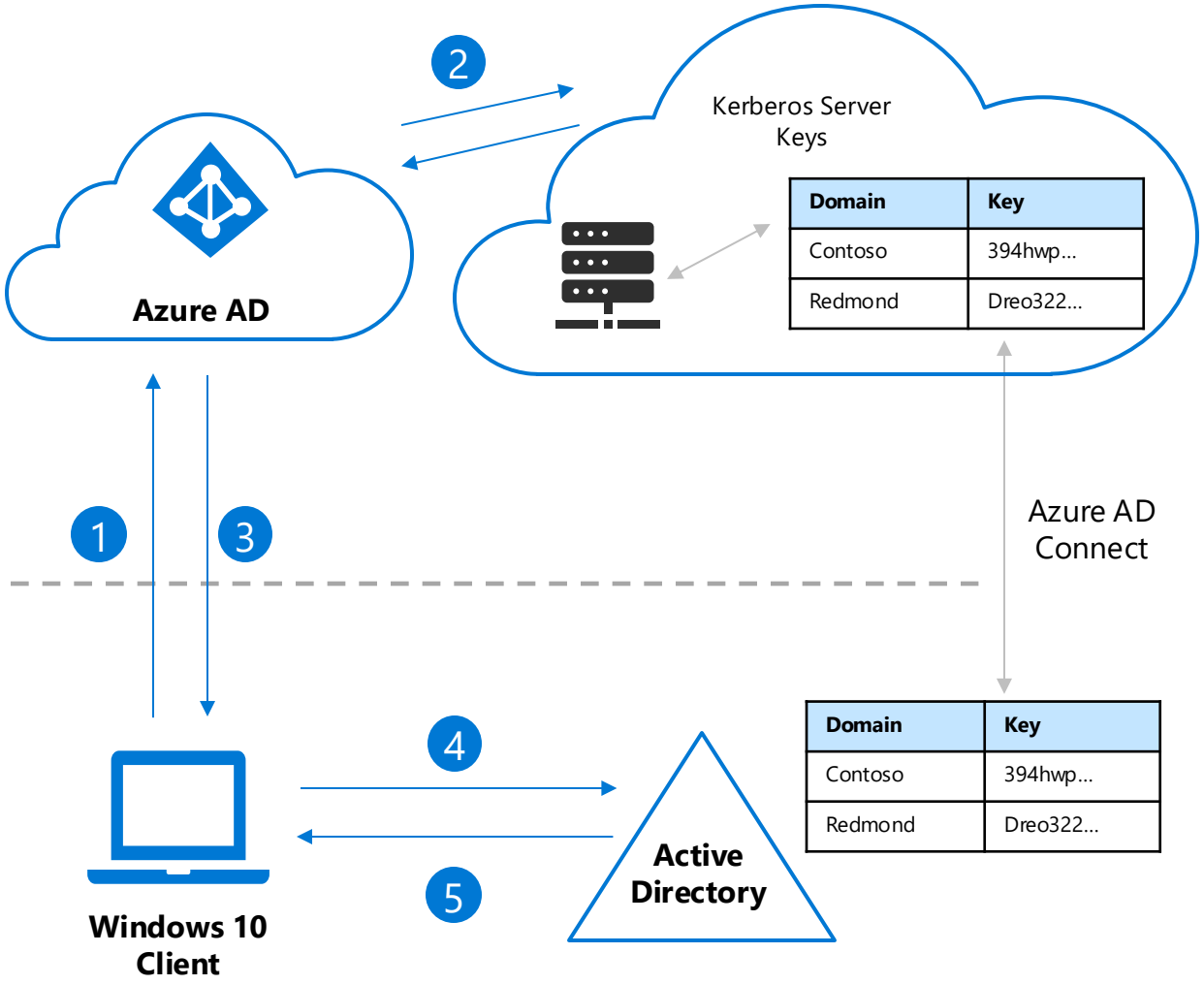
Deployment Components



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

No additional licensing required

Authentication



1. User authenticates to Azure AD with a FIDO2 security key.
2. Azure AD checks the tenant for a Kerberos server key matching the user's on-premises AD Domain.
   - Azure AD Generates a partial Kerberos Ticket Granting Ticket (TGT) for the users on-premises AD Domain. The TGT contains only the user SID. No authorization data (groups) are included in the TGT.
3. The partial TGT is returned to the Windows along with Azure AD Primary Refresh Token (PRT).
4. Windows contacts on-premises AD Domain Controller and trades the partial TGT for a full TGT.
5. Windows now has Azure AD PRT and a full Active Directory TGT.

FIDO2 Auth with Active Directory

Charity Shelbourne


Recycle Bin
Microsoft Teams
Microsoft Edge
Windows 10 Enterprise Insider Preview
Evaluation copy. Build 19504.rs_onecore_ens_id.191020-1700
Type here to search
11:57 AM
10/28/2019

Deployment Tips

- No Domain or Forest Functional Level required but..
- Patch all your 2016/2019 DCs
- Test/Pilot-Use an isolated site with patched servers/clients
- Does not work with RDP yet..
  - Instead use Citrix with Azure AD integration for FIDO. Then use FAS to login to the back end server

Go do now!

- Today
  - If ADFS, deploy Connect Health. Evaluate ADDS Connect Health and deploy.
  - Turn on PHS!
  - Turn on AAD Password Protection (audit)
  - Enable Hybrid AAD Join as prep for WHFB
  - Upgrade DC's to 2016/2019.
  - Upgrade ADFS to 2019
  - Deploy Azure ATP (license requirement)
- Within 3 months
  - Enable AAD Password Protection & update password policy to be at 12 month expiry
  - Pilot and deploy WHFB for new Win10
  - Evaluate Authenticator Passwordless and FIDO