nic

2019

Artificial Edition

6-8 February

Protect your front door:
Use Conditional Access and MFA

to keep corporate data secure and your users productive at the same time

Marius A. Skovli

CTGlobal Principal Consultant and
Microsoft Enterprise Mobility MVP

mas@ctglobalservices.com
@MariusSkovli

Agenda

- Protecting my front door?
- Azure Multi-factor Authentication and Conditional Access
  - Configure MFA
  - Configure CA in General
  - Configure CA for Outlook
  - Configure CA for Co-Management

- #DemoHeavy

Digital transformation is driving change

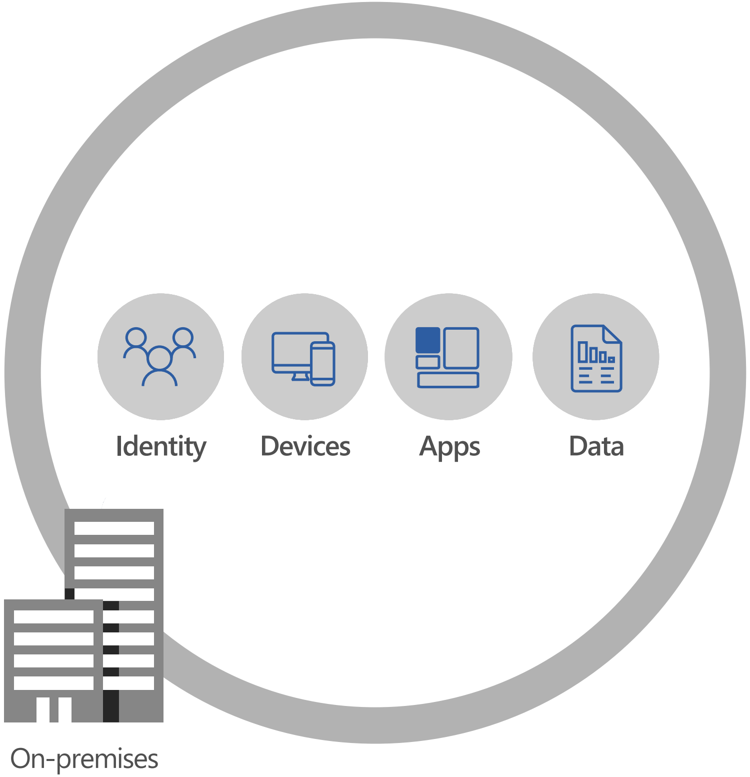
41% of employees say mobile business apps change how they work

85% of enterprise organizations keep sensitive information in the cloud

80% of employees use non-approved SaaS apps for work

NIC

The security perimeter has changed



Protect at the front door

81%

of hacking breaches leverage stolen and/or weak passwords

Verizon 2017 Data Breach Investigation Report

What is Multi-Factor Authentication?

- Multiple factors are required for sign-In
  - Familiar to consumer cloud service users such as the Microsoft Account
  - Simple block to password compromise from another location
  - Addresses regulatory compliance and high risk user scenarios
  - AKA two-factor, 2FA, MFA, strong authentication
- Two or more of the following factors:
  - Something you know – a password or PIN
  - Something you have – a phone, credit card or hardware token
  - Something you are – a fingerprint, hand geometry, retinal scan or other biometric
  - Stronger when using two different channels (out-of-band)
- Types of multi-factor authentication:

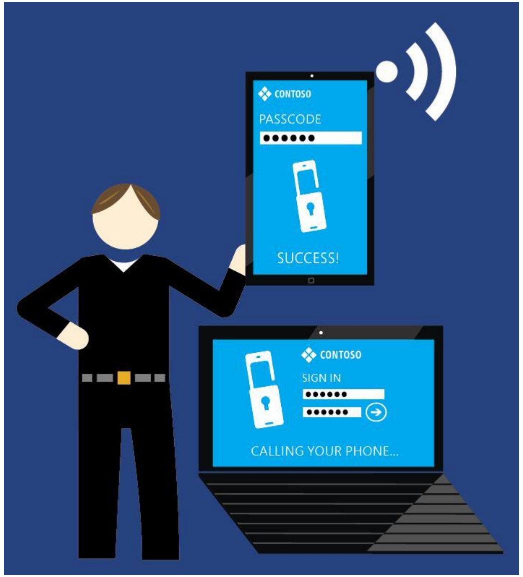
Hardware OTP Tokens
Certificates
Smart Cards
Phone-Based Authentication:

Phone Call, Text Message, and Push
Software OTP Tokens

Microsoft Azure Multi-Factor Authentication flavors

- Supports
  - Phone Calls
  - Text Messages
  - Mobile Apps (iOS, Android)

- Users manage their own authentication methods and phone numbers



Demo

- Configure Azure MFA
- Azure Authenticator app
- Logon to Teams (Browser) with MFA
- Force MFA on impossible logon (Identity Protection)
- Trusted locations
- Terms of use

How much control do you have over access?

Who is accessing? What is their role? Is the account compromised?

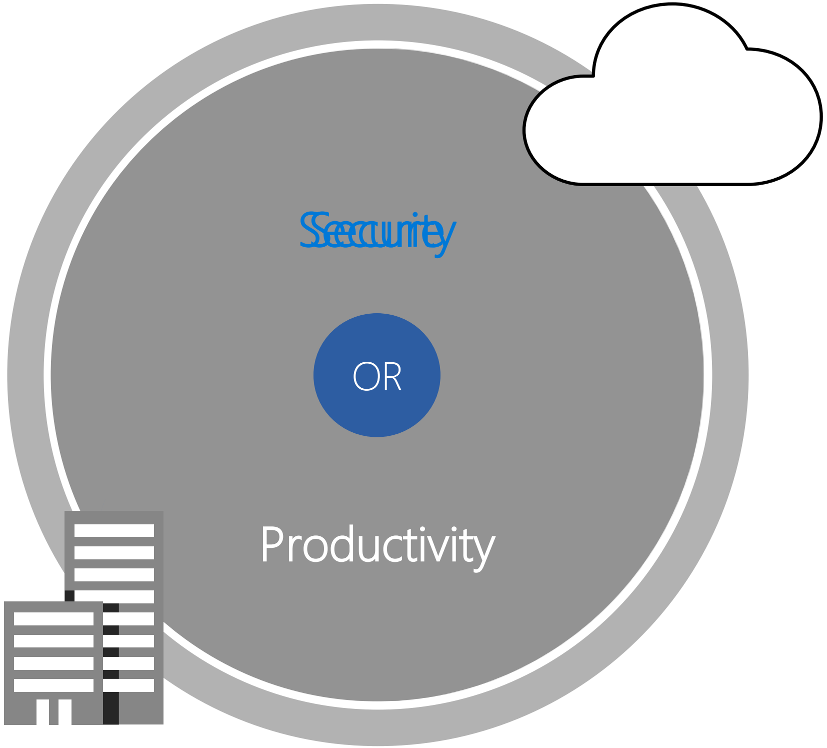
Where is the user based? From where is the user signing in? Is the IP anonymous?

Which app is being accessed? What is the business impact?

Is the device healthy? Is it managed? Has it been in a botnet?

What data is being accessed? Is it classified? Is it allowed off premises?

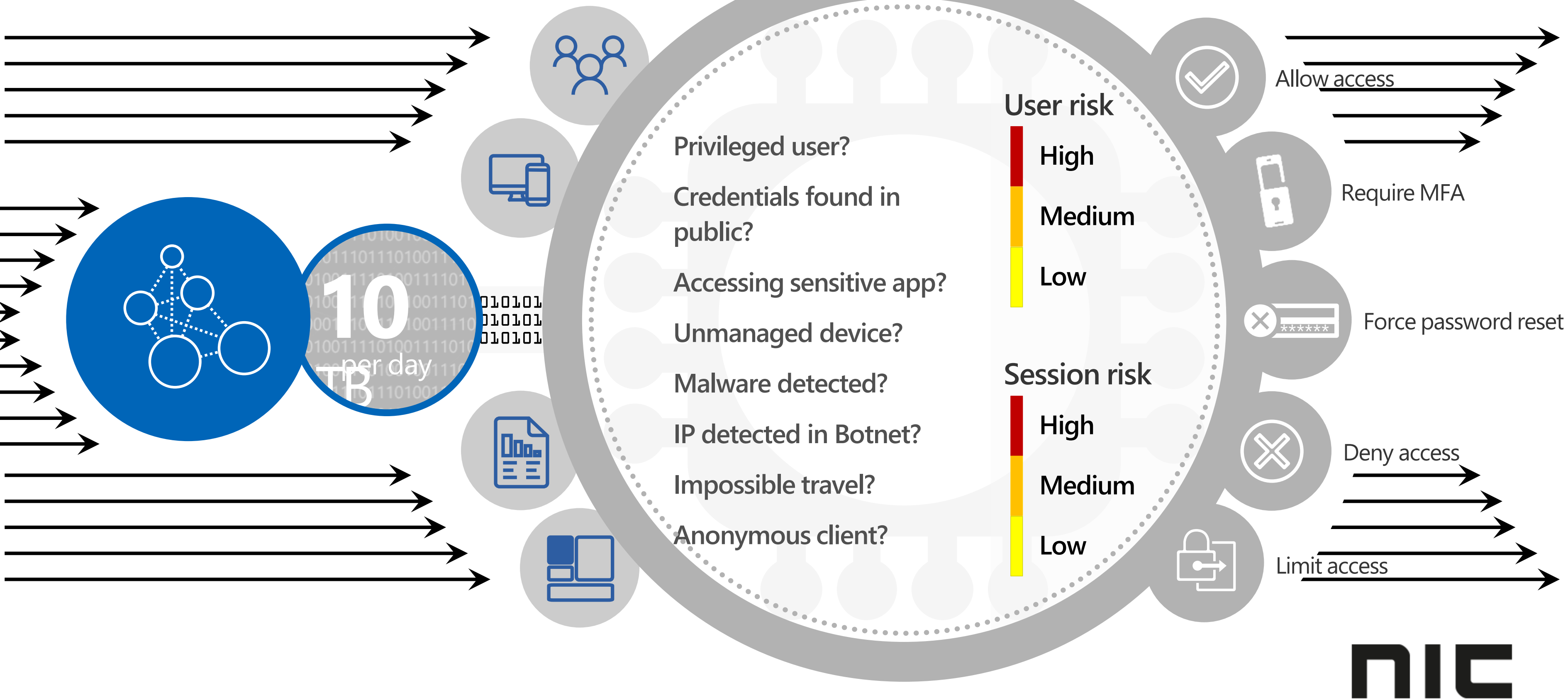
How do we enable productivity without compromising security?



It’s a delicate balance between productivity & security

The security you need integrated with the productivity tools you want

Conditional Access = IF THEN



Privileged user?

Credentials found in public?

Accessing sensitive app?

Unmanaged device?

Malware detected?

IP detected in Botnet?

Impossible travel?

Anonymous client?

User risk

- 🟥 High
- 🟧 Medium
- 🟨 Low

Session risk

- 🟥 High
- 🟧 Medium
- 🟨 Low

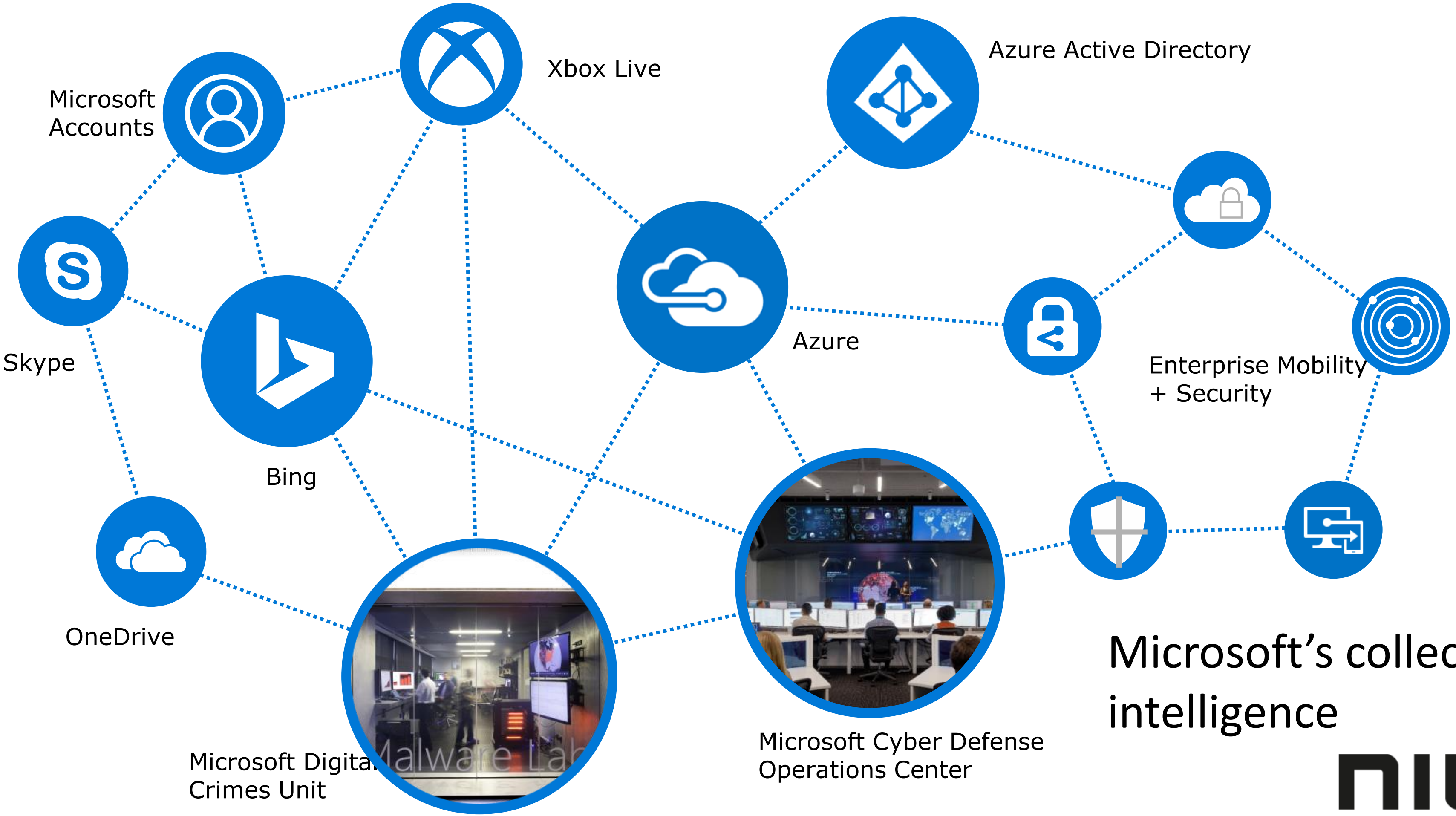
Allow access

Require MFA

Force password reset

Deny access

Limit access



Microsoft Accounts

Xbox Live

Azure Active Directory

Skype

Bing

Azure

Enterprise Mobility + Security

OneDrive

Microsoft Digital Crimes Unit

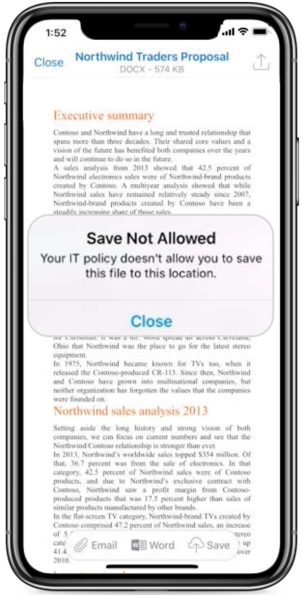
Microsoft Cyber Defense Operations Center

Microsoft’s collective intelligence

Demo

- Conditional Access
  - Policies in AAD CA – Global Administrators
  - Policies in AAD CA - Teams
  - Policies in AAD CA - Enterprise Apps
  - Policies in AAD CA - Internal website (Azure App proxy EA)
  - Policies in AAD CA - Teams

Why Outlook mobile versus built-in apps



Northwind Traders Proposal

DOCX - 574 KB

Executive summary

Contoso and Northwind have a long and trusted relationship that spans more than three decades. Their shared core values and a vision of the future has benefited both companies over the years and will continue to do so in the future.

A sales analysis from 2013 showed that 42.5 percent of Northwind electronics sales were of Northwind-brand products created by Contoso. A multiyear analysis showed that while Northwind sales have remained relatively steady since 2007, Northwind-brand products created by Contoso have been a steadily increasing share of those sales.

Save Not Allowed

Your IT policy doesn't allow you to save this file to this location.

Close

Ohio that Northwind was the place to go for the latest stereo equipment.

In 1975, Northwind became known for TVs too, when it released the Contoso-produced CR-113. Since then, Northwind and Contoso have grown into multinational companies, but neither organization has forgotten the values that the companies were founded on.

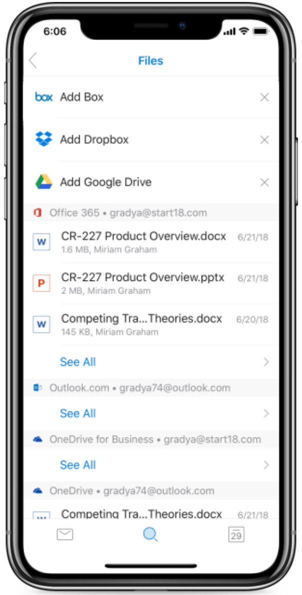
Northwind sales analysis 2013

Setting aside the long history and strong vision of both companies, we can focus on current numbers and see that the Northwind/Contoso relationship is stronger than ever.

In 2013, Northwind's worldwide sales topped $354 million. Of that, 36.7 percent was from the sale of electronics. In that category, 42.5 percent of Northwind sales were of Contoso products, and due to Northwind's exclusive contract with Contoso, Northwind saw a profit margin from Contoso-produced products that was 17.5 percent higher than sales of similar products manufactured by other brands.

In the flat-screen TV category, Northwind-brand TVs created by Contoso comprised 47.2 percent of Northwind sales, an increase of 5

2010.



Office 365 • gradya@start18.com

W	CR-227 Product Overview.docx 1.6 MB, Miriam Graham	6/21/18
P	CR-227 Product Overview.pptx 2 MB, Miriam Graham	6/21/18
W	Competing Tra...Theories.docx 145 KB, Miriam Graham	6/20/18

See All

Outlook.com • gradya74@outlook.com

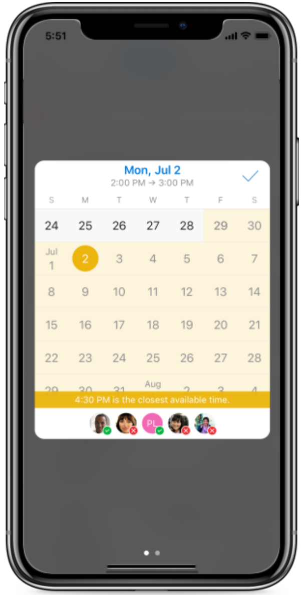
See All

OneDrive for Business • gradya@start18.com

See All

OneDrive • gradya74@outlook.com

Competing Tra...Theories.docx 6/21/18

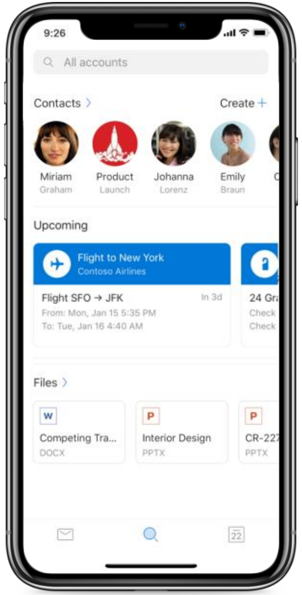


Mon, Jul 2

2:00 PM → 3:00 PM

S	M	T	W	T	F	S
24	25	26	27	28	29	30
Jul 1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

4:30 PM is the closest available time.



Flight to New York

Contoso Airlines

Flight SFO → JFK In 3d

From: Mon, Jan 15 5:35 PM

To: Tue, Jan 16 4:40 AM

24 Gr

Check

Check

Competing Tra... DOCX

Interior Design PPTX

CR-227 PPTX

Security

Modern authentication, App Protection, Conditional Access

Office 365 Integration

Word, Excel, PowerPoint
OneDrive and Skype for Business

Organize on the go

Scheduling Free/Busy
Time to leave reminders

Intelligence

People, org view, LinkedIn
Travel summary cards

Why Block Legacy Authentication?

- 350K compromised accounts in April 2018 due to password spray, 200K in the last month.
- Nearly 100% of password spray attacks we see are from legacy authentication
- Blocking legacy authentication reduces compromise rate by 66%
- https://aka.ms/PasswordSprayBestPractices

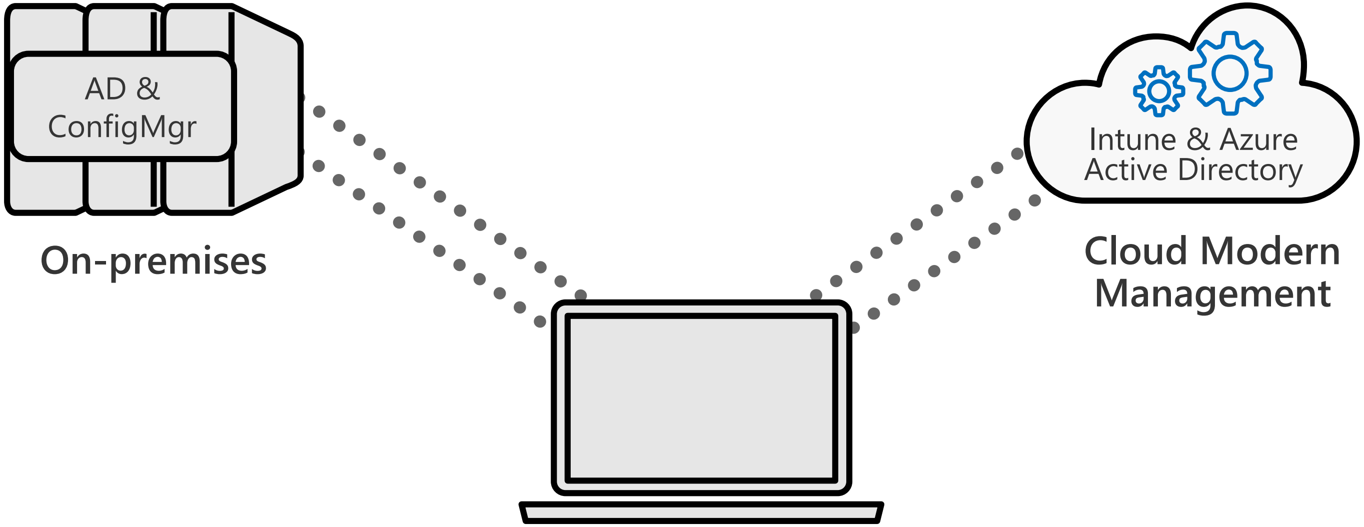
Why should I care about Disabling Legacy Auth?

- Did you not see the previous slide? ☺
- CA is designed based on controlling token issuance in modern auth (plus EAS legacy authentication)
- CA also relies on device authentication for device compliance controls.
- Legacy authentication doesn’t support device authentication, thus breaking CA.

Demo

- Conditional Access
  - Policies in AAD CA - Force Outlook Mobile
  - Policies in AAD CA - Force Outlook Mobile EAS
  - Policies in AAD CA - Outlook Block Basic Auth

Co-Management


AD & ConfigMgr

On-premises

Intune & Azure Active Directory

Cloud Modern Management

Demo

- Co-Management and Conditional Access
  - Compliance Workload
  - Intune Compliance policies
  - CA Device compliance
    - Teams in Windows (and let’s do iOS as well ☺)

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2019