



# wiki Webinar

by **inetum.**  
realdolmen

**inetum.**  
realdolmen  
Positive digital flow

## Microsoft Secure Score

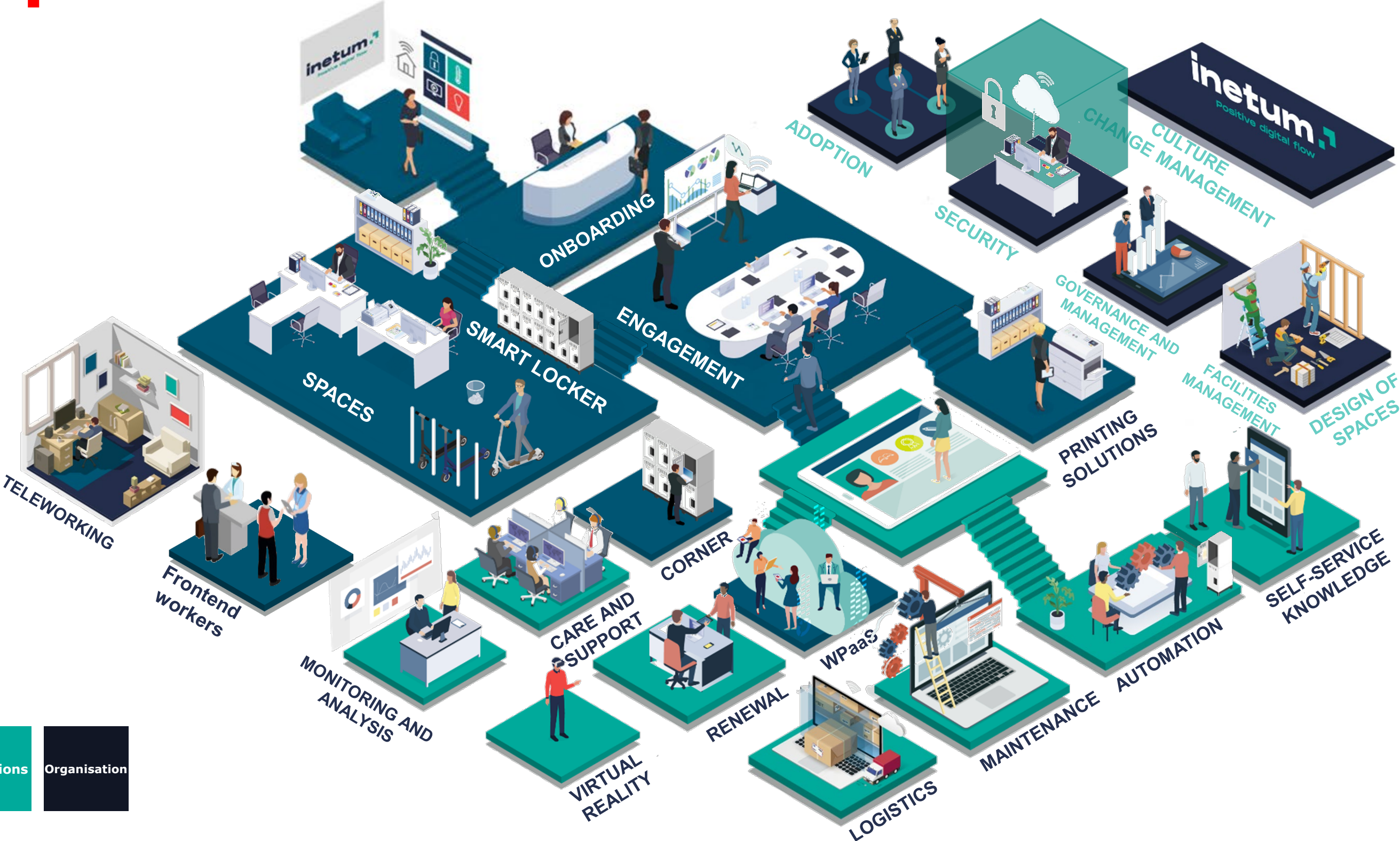


# Praktische afspraken

- Vragen via chat
- Iedereen op mute
- Q&A na de presentatie
- Evaluatie met link naar de slides worden na het event doorgestuurd



# And... What does an Intelligent Workplace include?



# M365 Secure Score Webinar

## Wie ben ik?



- Wim Van Clapdurp
- Werkzaam als Microsoft 365 security en modern workplace consultant.
- focus vooral op security via Microsoft Defender
- reeds 22 jaar in ICT sector

# M365 Secure Score Webinar

## Wat is Secure Score?

- Centraal dashboard met aanbevelingen om je security level te verhogen
- Ga naar : <https://security.microsoft.com/securescore>

# M365 Secure Score Webinar

CONTOSO demo

← admin@m365x36986996.onmicrosoft.com

### Enter password

Password

[Forgot my password](#)

**Sign in**

Contoso

Microsoft 365 Defender

- Home
- Incidents & alerts
- Hunting
- Actions & submissions
- Threat analytics
- Secure score**
- Learning hub
- Trials

# M365 Secure Score Webinar



## Microsoft Secure Score

Overview Recommended actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

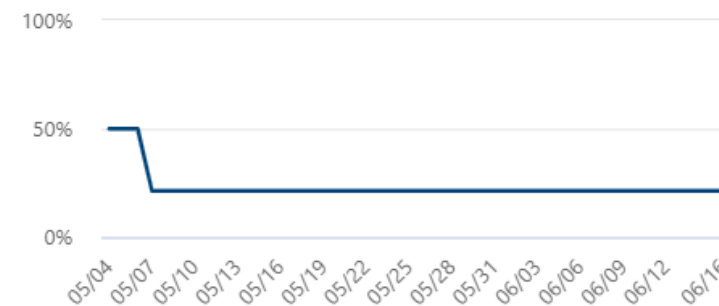


Your secure score

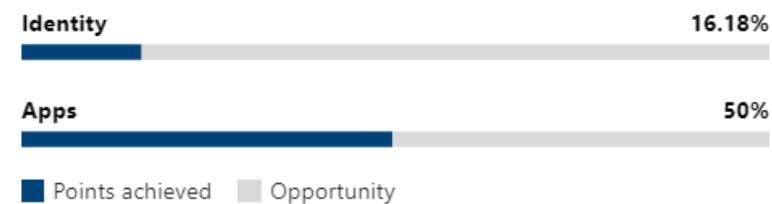
Include ▼

### Secure Score: 21.3%

14.06/66 points achieved



Breakdown points by: Category ▼



Actions to review



Top recommended actions

Recommended action	Score impact	Status	Category
Require MFA for administrative roles	+15.15%	<input type="radio"/> To address	Identity
Ensure all users can complete multi-factor authentication for secure ac...	+13.64%	<input type="radio"/> To address	Identity
Enable policy to block legacy authentication	+12.12%	<input type="radio"/> To address	Identity
Turn on user risk policy	+10.61%	<input type="radio"/> To address	Identity
Turn on sign-in risk policy	+10.61%	<input type="radio"/> To address	Identity
Do not allow users to grant consent to unmanaged applications	+6.06%	<input type="radio"/> To address	Identity

# M365 Secure Score Webinar

## Microsoft Secure Score

Overview **Recommended actions** History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters:

Export

18 items

Search

Filter

Group by

Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product
<input type="checkbox"/> 1	Require MFA for administrative roles	+15.15%	0/10	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/> 2	Ensure all users can complete multi-factor authentication for ...	+13.64%	0/9	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/> 3	Enable policy to block legacy authentication	+12.12%	0/8	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/> 4	Turn on user risk policy	+10.61%	0/7	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/> 5	Turn on sign-in risk policy	+10.61%	0/7	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/> 6	Do not allow users to grant consent to unmanaged applicatio...	+6.06%	0/4	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/> 7	Configure which users are allowed to present in Teams meeti...	+3.03%	0/2	<input type="radio"/> To address	No	Yes	Apps	Microsoft Teams
<input type="checkbox"/> 8	Only invited users should be automatically admitted to Team...	+3.03%	1/2	<input type="radio"/> To address	No	Yes	Apps	Microsoft Teams
<input type="checkbox"/> 9	Turn on customer lockbox feature	+1.52%	0/1	<input type="radio"/> To address	No	Yes	Apps	Exchange Online



# M365 Secure Score Webinar



## Require MFA for administrative roles

To address

Edit status & action plan Manage tags

**General** Implementation History (1)

### Description

Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.

### Implementation status

You have 0 out of 7 users with administrative roles registered and protected with MFA.

### User impact

First, users with administrative roles need to register for MFA. After each admin is registered, your policies then determine when they're prompted for the additional authentication factors.

#### Users affected

All of your Microsoft 365 users with administrator roles

[Manage in Microsoft Azure](#)

Share

### Details

Points achieved 0/10

#### History

1 events

#### Category

Identity

#### Product

Azure Active Directory

#### Protects against

[Password Cracking](#), [Account Breach](#),  
[Elevation of Privilege](#)



# M365 Secure Score Webinar

Home > Conditional Access

## Conditional Access | Policies

Azure Active Directory

- Overview (Preview)
- Policies**
- Insights and reporting
- Diagnose and solve problems
- Manage
- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context (Preview)

+ New policy

What If Refresh Got feedback?

Search policies

Add filters

2 out of 2 policies found

Policy Name ↑↓	State ↑↓	Creation Date ↑↓	Modified Date ↑↓
<a href="#">Exchange Online Requires Compliant Device</a>	Off	5/4/2022, 11:29:36 PM	...
<a href="#">Office 365 App Control</a>	Off	5/4/2022, 11:29:40 PM	...

# M365 Secure Score Webinar

[Home](#) > [Conditional Access](#) >

**New** ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Enable policy

Report-only On Off

Create

[Home](#) > [Conditional Access](#) >

**New** ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

Require MFA for all Admin ✓

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Enable policy

Report-only On Off

Create

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

What does this policy apply to?

Users and groups

Include Exclude

None

All users

Select users and groups

All guest and external users ⓘ

Directory roles ⓘ

0 selected

Select at least one role

Users and groups

# M365 Secure Score Webinar

**Built-in directory roles**

- Application administrator
- Attack simulation administrator
- Attribute assignment administrator
- Attribute definition administrator
- Authentication administrator
- Authentication policy administrator
- Azure AD joined device local administrator
- Azure DevOps administrator
- Azure Information Protection administrator

admin

0 selected

Select at least one role

Users and groups

**Built-in directory roles**

- Application administrator
- Attack simulation administrator
- Attribute assignment administrator
- Attribute definition administrator
- Authentication administrator
- Authentication policy administrator
- Azure AD joined device local administrator
- Azure DevOps administrator
- Azure Information Protection administrator

admin

56 selected

Users and groups

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.  
[Learn more](#)

What does this policy apply to?

Users and groups

Include  Exclude

Select the users and groups to exempt from the policy

All guest and external users ⓘ

Directory roles ⓘ

Users and groups

Select excluded users

0 users and groups selected

Select at least one user or group

# M365 Secure Score Webinar

## Select excluded users

Users and groups

admin



MOD Administrator  
admin@M365x36986996.onmicrosoft.com

### Selected items

No items selected

Select

Dit is enkel nodig voor een breakglass account.

# M365 Secure Score Webinar

## New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Require MFA for all Admin ✓

Assignments

Users or workload identities ⓘ

[Specific users included and specific users excluded](#)

✗ "Select users and groups" must be configured

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

Enable policy

Report-only On Off

Create

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps ▾

Include Exclude

- None
- All cloud apps
- Select apps

⚠ Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.

# M365 Secure Score Webinar

## Grant ×

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ  
[See list of approved client apps](#)

Require app protection policy ⓘ  
[See list of policy protected client apps](#)

Require password change ⓘ

For multiple controls

Require all the selected controls

Require one of the selected controls

Select

# M365 Secure Score Webinar



Enable policy

Report-only On Off

Don't lock yourself out! We recommend applying a policy to a small set of users first to verify it behaves as expected. We also recommend excluding at least one administrator from this policy. This ensures that you still have access and can update a policy if a change is required. Please review the affected users and apps.

Exclude current user, admin@xxxxxxxxxxxxxxxxxxxxxx, from this policy.

I understand that my account will be impacted by this policy. Proceed anyway.

Create



# M365 Secure Score Webinar

Policy Name ↑↓	State ↑↓	Creation Date ↑↓	Modified Date ↑↓
<a href="#">Exchange Online Requires Compliant Device</a>	Off	5/4/2022, 11:29:36 PM	...
<a href="#">Office 365 App Control</a>	Off	5/4/2022, 11:29:40 PM	...
<a href="#">Require MFA for all Admin</a>	Report-only		...



# M365 Secure Score Webinar

## Require MFA for administrative roles

General **Implementation** History (1)

### Prerequisites

✓ You have Azure Active Directory Premium P2.

### Next steps

If you are using **Azure Active Directory Free** versions with Office 365 or other SAAS/Web applications integrated with Azure Active Directory, then we suggest you enable "security defaults"

"Security defaults" achieves multiple objectives:

1. Requiring all users to register for Azure AD Multi-Factor Authentication.
2. Requiring administrators to do multi-factor authentication.
3. Blocking legacy authentication protocols.
4. Requiring users to do multi-factor authentication when necessary.
5. Protecting privileged activities like access to the Azure portal.

[Learn more about how to turn on security defaults.](#)

If you have invested in **Azure Active Directory Premium P1 or P2** licenses individually or as a part of another license like:

- Microsoft 365 E3/E5
- Enterprise Mobility + Security (EMS) E3/E5
- Microsoft 365 Business Premium

You can enable Conditional Access policies to enable custom policy enforcement for selected users or applications, under specific conditions



NOTE: Security defaults and Conditional Access cannot be used side by side.

Manage in Microsoft Azure

Share

# M365 Secure Score Webinar

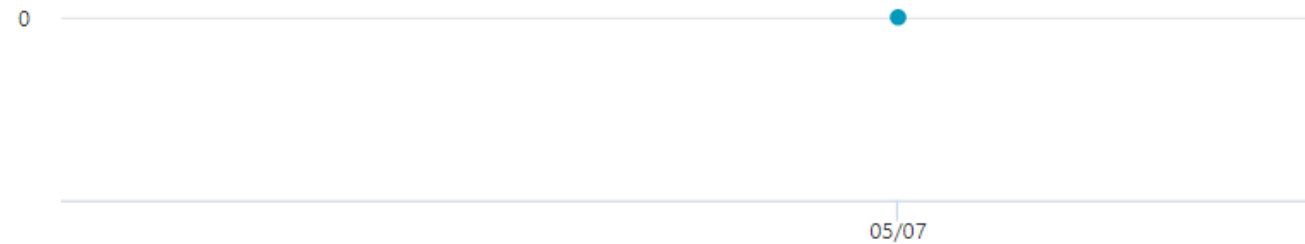
## Require MFA for administrative roles

 Edit status & action plan  Manage tags

General Implementation History (1)

View changes to this recommended action. "Require MFA for administrative roles".

### Point changes over time



### Activity

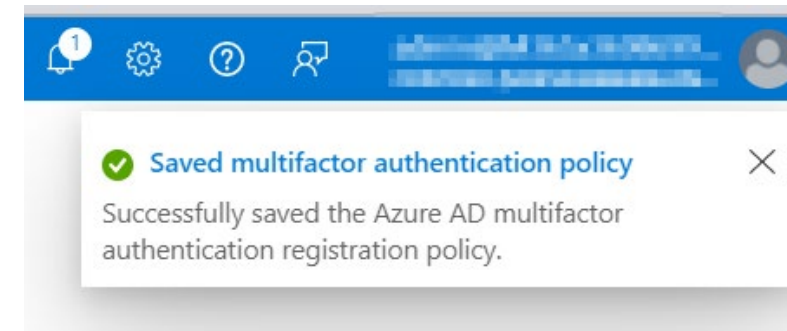
05/07 This action has become relevant (score -0 points)

Manage in Microsoft Azure

 Share 

## Implementation status

You have 0 out of 35 users registered and protected with MFA.



A screenshot of a notification in the Microsoft Azure portal. The notification is titled "Saved multifactor authentication policy" and contains the text "Successfully saved the Azure AD multifactor authentication registration policy." The notification is displayed in a white box with a green checkmark icon and a close button (X) in the top right corner. The background shows the Azure portal interface with a blue header bar containing navigation icons and a user profile icon.

# M365 Secure Score Webinar

<input checked="" type="checkbox"/>	13	Do not expire passwords	+12.12%	8/8	<input checked="" type="checkbox"/> Completed	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/>	14	Remove TLS 1.0/1.1 and 3DES dependencies	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Apps	Exchange Online
<input type="checkbox"/>	15	Designate more than one global admin	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Identity	Azure Active Directory
<input type="checkbox"/>	16	Restrict dial-in users from bypassing a meeting lobby	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Apps	Microsoft Teams
<input type="checkbox"/>	17	Limit external participants from having control in a Teams me...	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Apps	Microsoft Teams
<input type="checkbox"/>	18	Restrict anonymous users from starting Teams meetings	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Apps	Microsoft Teams

# M365 Secure Score Webinar



## Do not expire passwords

✔ Completed

 Edit status & action plan  Manage tags

General Implementation History (1)

### Prerequisites

✔ You have Azure Active Directory Premium P2.

### Next steps

In the [Microsoft 365 admin center](#) go to Settings > Org Settings > Security & privacy. Then uncheck the box "Set user passwords to expire after a number of days", this will help you set the password policy to never let passwords expire. You must be a global admin to edit the password policy.

If your organization has an on-premise implementation, it is recommended that you set status for this action to "Resolved through alternate mitigation."

### Learn more

[Set the password expiration policy for your organization](#)

[Password policy recommendations for Office 365](#)

Manage in Microsoft Azure

 Share 

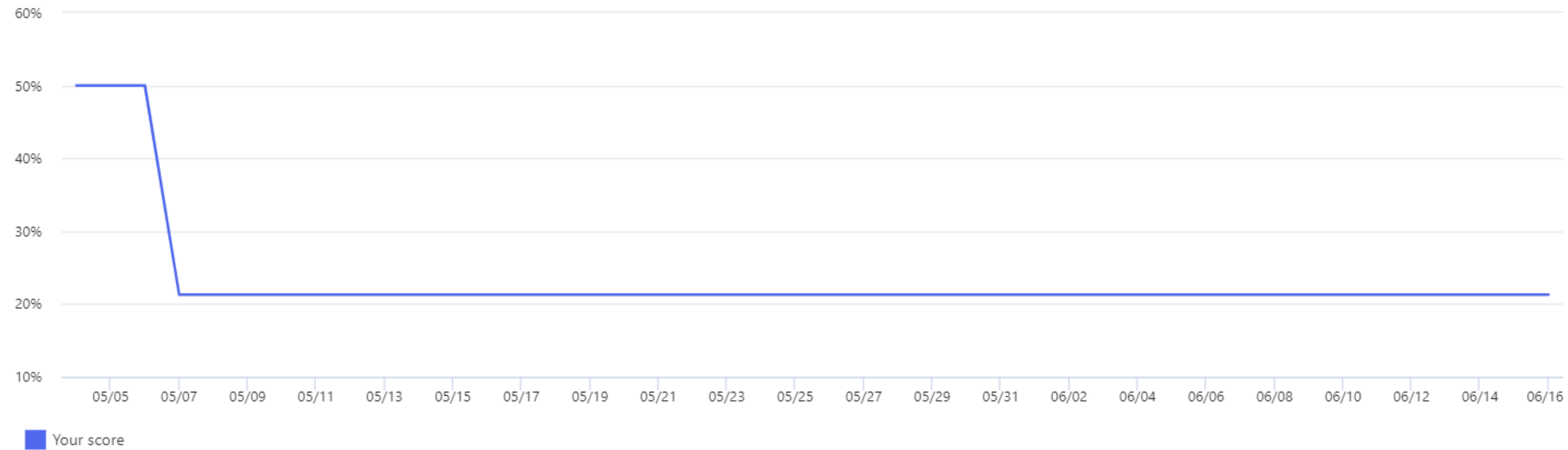


# M365 Secure Score Webinar

## Microsoft Secure Score

Overview Recommended actions History Metrics & trends


▼ **28.7%**



# M365 Secure Score Webinar





## Microsoft Secure Score

 Your score



Applied filters:

 Export

13 items

 90 days 

 Filter

 Group by 

Date/Time	Activity	Resulting points	Category	Attributed to
May 8, 2022 5:00 PM	0.00 points regressed for <a href="#">Enable self-service password reset</a> because 33 more users are affected	0.06/1	Identity	System
May 7, 2022 5:00 PM	+1.00 points score change because <a href="#">Remove TLS 1.0/1.1 and 3DES dependencies</a> has become r...	1/1	Apps	System
May 7, 2022 5:00 PM	+0.00 points score change because <a href="#">Use limited administrative roles</a> has become relevant	0/1	Identity	System
May 7, 2022 5:00 PM	-0.00 points score change because <a href="#">Turn on user risk policy</a> has become relevant	0/7	Identity	System
May 7, 2022 5:00 PM	+1.00 points score change because <a href="#">Designate more than one global admin</a> has become relevant	1/1	Identity	System
May 7, 2022 5:00 PM	-0.00 points score change because <a href="#">Enable policy to block legacy authentication</a> has become rel...	0/8	Identity	System
May 7, 2022 5:00 PM	-0.00 points score change because <a href="#">Ensure all users can complete multi-factor authentication fo...</a>	0/9	Identity	System
May 7, 2022 5:00 PM	-0.00 points score change because <a href="#">Require MFA for administrative roles</a> has become relevant	0/10	Identity	System
May 7, 2022 5:00 PM	+0.06 points score change because <a href="#">Enable self-service password reset</a> has become relevant	0.06/1	Identity	System
May 7, 2022 5:00 PM	+8.00 points score change because <a href="#">Do not expire passwords</a> has become relevant	8/8	Identity	System

# M365 Secure Score Webinar

## Products included in Secure Score

- Microsoft 365 (including Exchange Online)
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Defender for Cloud Apps
- Microsoft Teams

## Security defaults

Microsoft Secure Score has updated improvement actions to support [security defaults in Azure Active Directory](#), which make it easier to help protect your organization with pre-configured security settings for common attacks.

If you turn on security defaults, you'll be awarded full points for the following improvement actions:

- Ensure all users can complete multi-factor authentication for secure access (9 points)
- Require MFA for administrative roles (10 points)
- Enable policy to block legacy authentication (7 points)



# M365 Secure Score Webinar

## Disable Security Defaults?

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Properties' page for an Azure Active Directory tenant named 'Contoso'. The 'Properties' page includes fields for 'Name' (Contoso), 'Country or region' (United States), 'Location' (United States datacenters), 'Notification language' (English), 'Directory ID' (69997834-fa40-45da-bad8-382c3bdc66c3), 'Technical contact' (technical@contoso.com), 'Global privacy contact' (privacy@contoso.com), and 'Privacy statement URL'. A 'Manage Security defaults' link is visible at the bottom of the page.

On the right side, a dialog box titled 'Enable Security defaults' is open. It contains the following text: 'Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks. [Learn more](#)'. Below the text, there are two radio buttons: 'Yes' (selected) and 'No'. The dialog box also has a 'Save' button at the bottom.

Red boxes highlight the 'Properties' link in the left-hand navigation pane, the 'Manage Security defaults' link at the bottom of the main content area, and the 'Enable Security defaults' dialog box on the right.

# M365 Secure Score Webinar

## Wie kan aan dit portaal?

### **Read and write roles**

With read and write access, you can make changes and directly interact with Secure Score. You can also assign read-only access to other users.

- Global administrator
- Security administrator
- Exchange administrator
- SharePoint administrator

### **Read-only roles**

With read-only access, you aren't able to edit status or notes for an improvement action, edit score zones, or edit custom comparisons.

- Helpdesk administrator
- User administrator
- Service support administrator
- Security reader
- Security operator
- Global reader

# M365 Secure Score Webinar

## Weetjes:

Hoe vaak wordt de Secure score geüpdatet?

De score zal **1 maal per dag** aangepast worden (rond 1:00 AM PST dit is 10:00 AM onze tijd). Indien je aanpassingen maakt op een item dat 'gemeten' wordt zal de score automatisch aanpassen de volgende dag.

Het kan tot 48 uur duren eer de aanpassingen reflecteren in jouw score.

Hoe lang bestaat secure score al?

Secure score is reeds in 2017 uitgebracht

Hoe hoog scoor je maximaal?

Als je alle security recommendations volgt kom je uit op een secure score van ongeveer 67%

Je kan tot bvb 80% geraken.

Hiervoor zal wel gebruik moeten gemaakt worden van additionele settings of zal er een beleid nodig zijn.

# M365 Secure Score Webinar



## Live demo

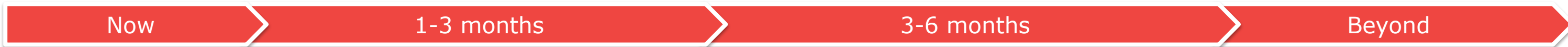
Dit is een live demo op een demo tenant

# M365 Secure Score Webinar

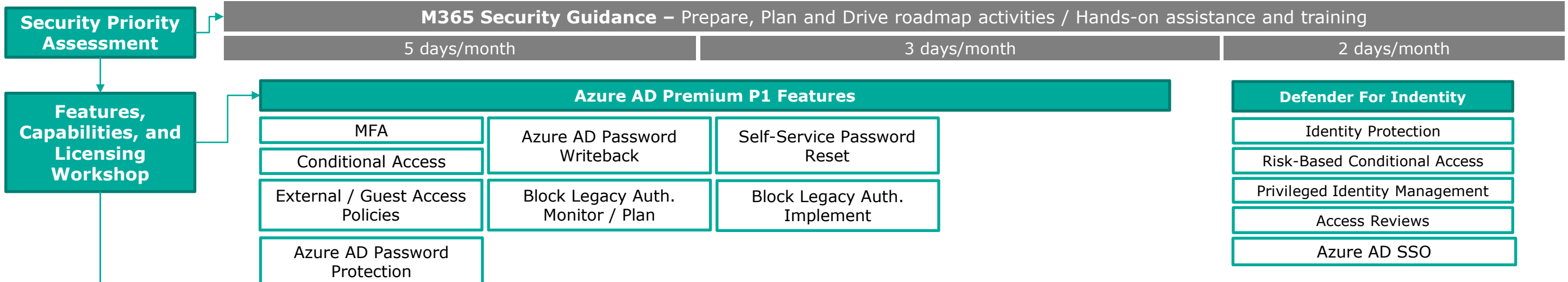


## Next Steps

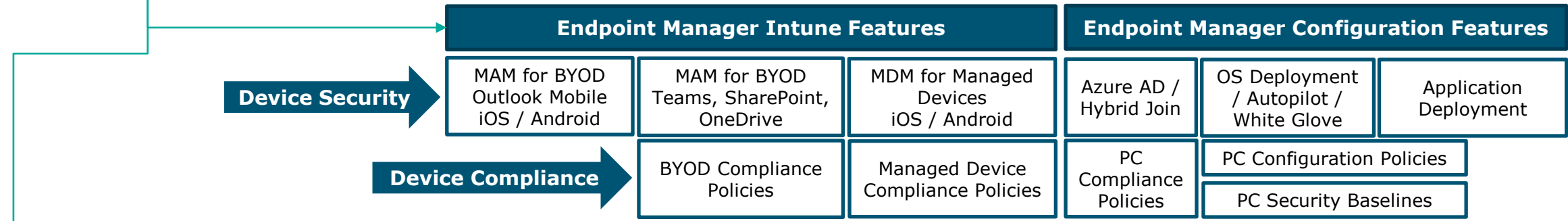
# Microsoft 365 Security



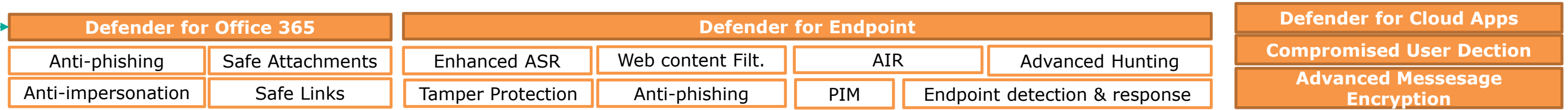
## Identity



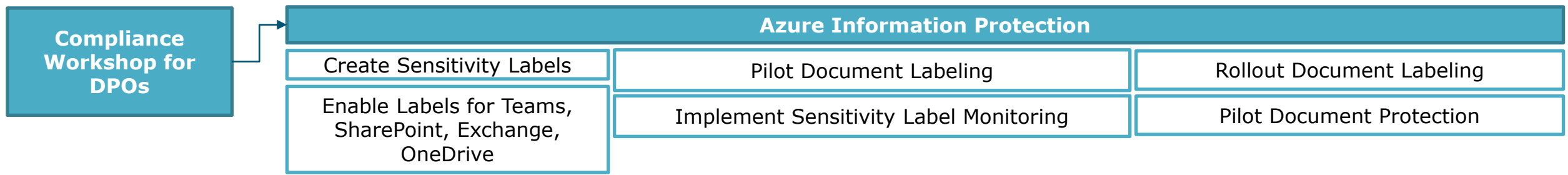
## Device



## Threat

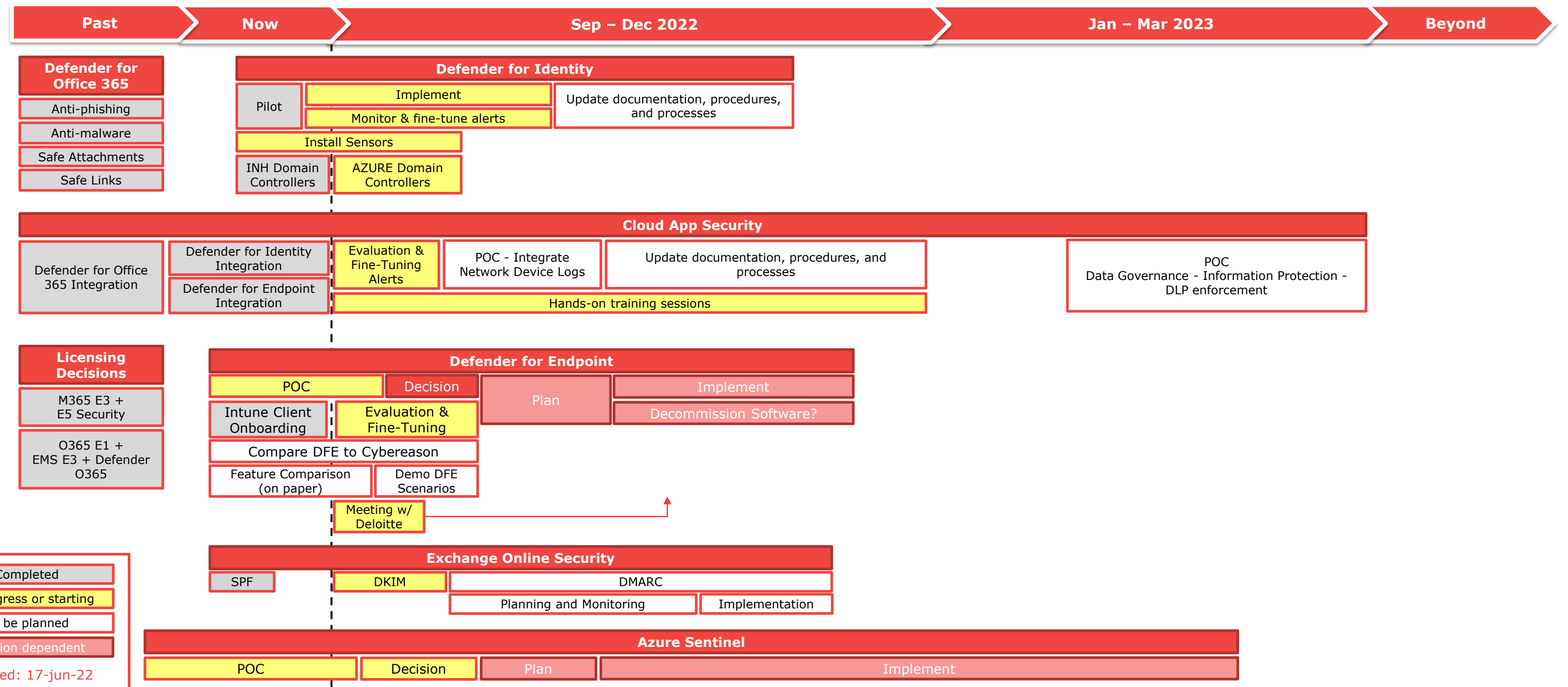


## Data

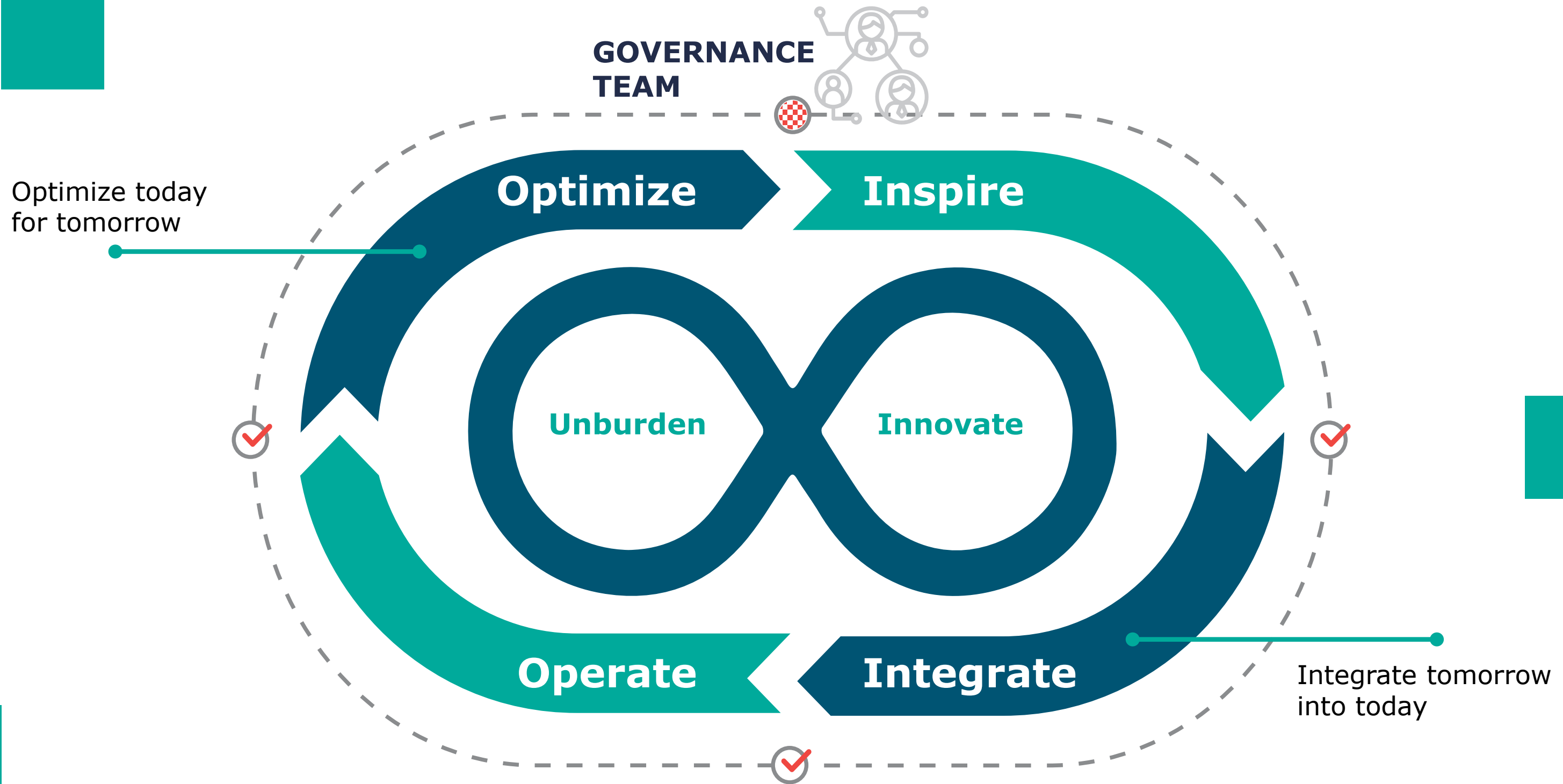


# Threat Protection

## Microsoft 365 Security



In order to **keep your balance**, you must **keep moving**





**GOVERNANCE  
TEAM**



**Optimize**

**Inspire**

**Unburden**

**Innovate**

**Operate**

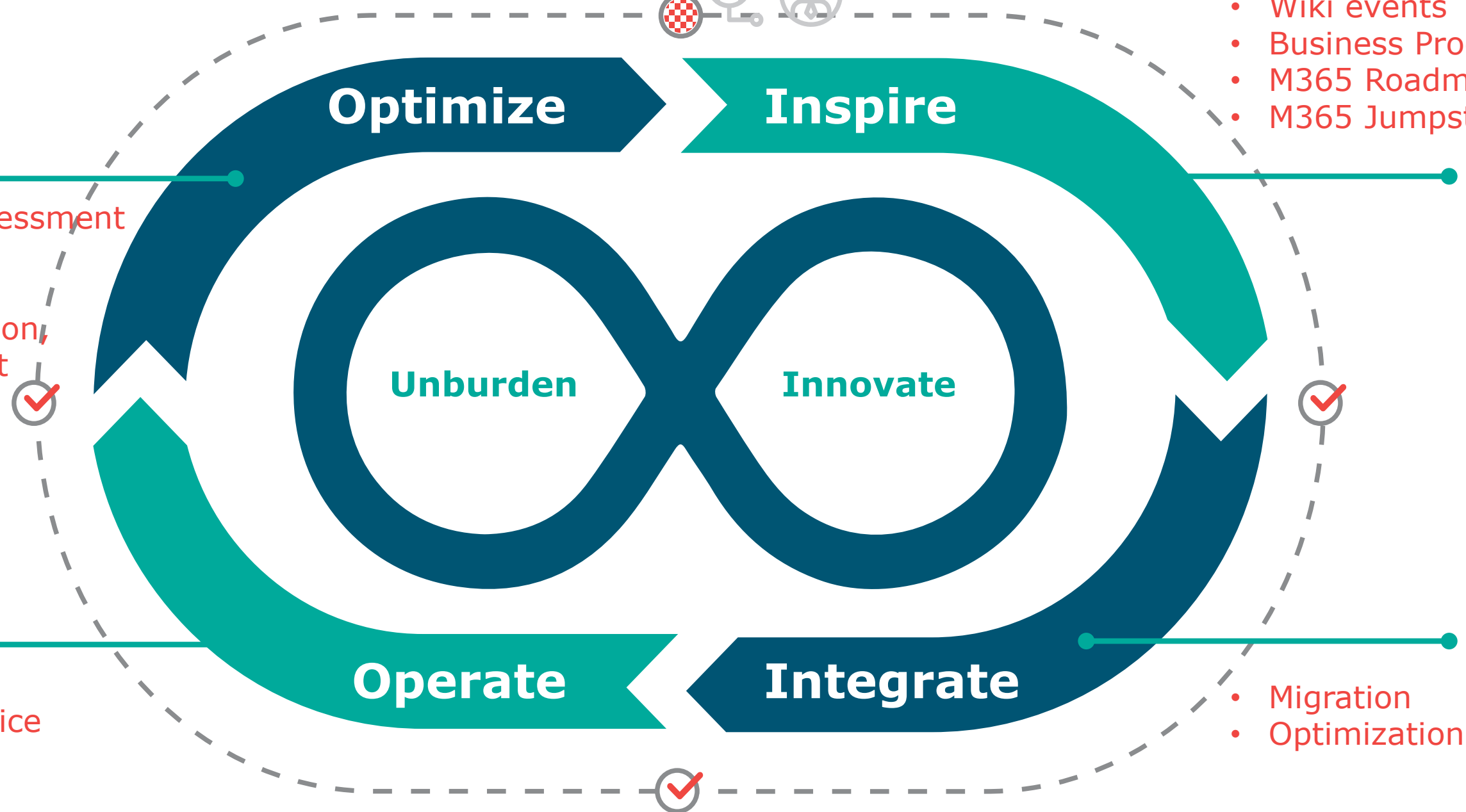
**Integrate**

- Wiki events
- Business Productivity Roadmap
- M365 Roadmap
- M365 Jumpstart

- Security Priority Assessment
- Calling Assessment
- Proactive Services
- Training, user adoption, change management

- Managed Services
- Workplace as a Service

- Migration
- Optimization



# Contacteer voor :

- Microsoft Security Priority Assessment
- Microsoft 365 Identity and Device Best Practices Workshop
- Microsoft Security Roadmap Assistance



## Security Priority Assessment Microsoft 365

All aspects of security in your environment are important, but you don't have enough resources to focus on them all? Making the **right choices** and seeing results quickly is not easy.

**Identifying** security priorities in the context of available features and related initiatives in your organization offers a way to get "un-stuck" and **start improving** security **now**.



## The Road to M365 Security

## Security Roadmap Assistance Microsoft 365

All aspects of security in your environment are important, but you don't have enough resources to focus on them all? Making the **right choices** and seeing results quickly is not easy.

Knowing what your goals are is a first step, but a goal without a plan is just a wish. This follow-up to our "Security priority Assessment", will help you **implement** the discovered security improvements in an **Agile** manner, realizing your security goals at your pace, with the help of **M365 Security Experts**.

## Contacteer ons via:

- [products@inetum-realdolmen.world](mailto:products@inetum-realdolmen.world)
- Uw vertrouwde contactpersoon bij Inetum-Realdolmen

Bestel online via:  
[store.inetum-realdolmen.world](https://store.inetum-realdolmen.world)

**inetum**   
realdolmen  
Positive digital flow

**inetum.world**

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |  
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |  
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |  
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE

