

IDENTITY DAYS

28 octobre 2021 - PARIS



@IdentityDays #identitydays2021

Merci à tous nos partenaires !



onelogin



yubico

ManageEngine



Exakis Nelite





Sécuriser votre Tenant Microsoft 365 et votre Azure AD en quelques minutes

Guillaume MATHIEU, Jean-François FERNANDEZ
Loic VEIRMAN, Sébastien PAULET
Seyfallah TAGREROUT, Sylvain CORTES

Guillaume MATHIEU

Directeur Technique Flexsi



AGENDA DE LA CONFÉRENCE

- La gouvernance des données
- Microsoft 365 Defender for O365
- Le Modern Workplace
- Le modèle de délégation Zero Trust
- Harden AD, le moteur
- Harden, la Preview



Jean-François FERNANDEZ

Responsable Technique Flexsi

Loic VEIRMAN

Manager BU CVC-IT

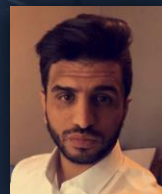


Sébastien PAULET

M365 Evangéliste AEROW

Seyfallah TAGREROUT

CEO STC Consulting – Cloud & Security
Architect

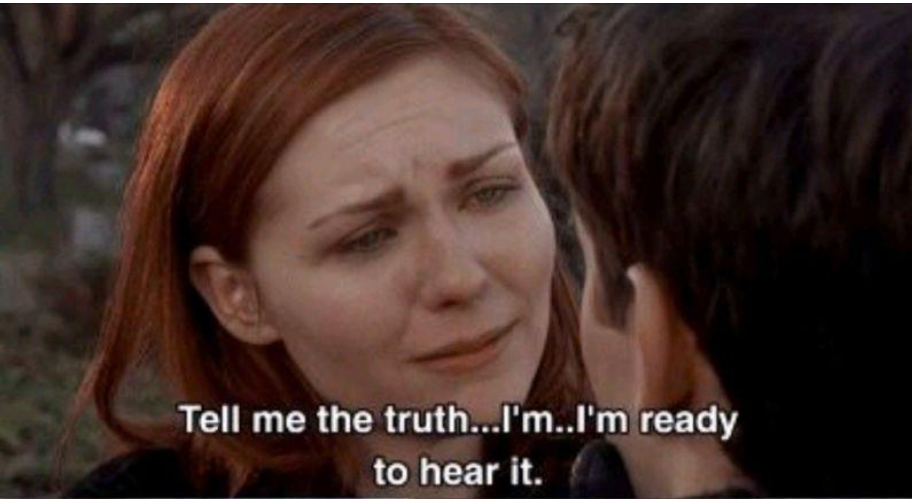


Sylvain CORTES

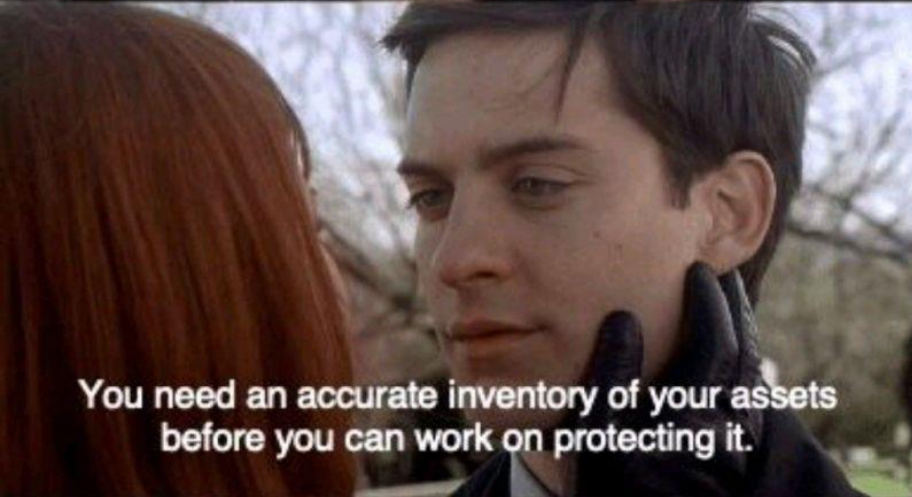
AD CyberSecurity Guru



La gouvernance des données



Tell me the truth...I'm...I'm ready
to hear it.



You need an accurate inventory of your assets
before you can work on protecting it.

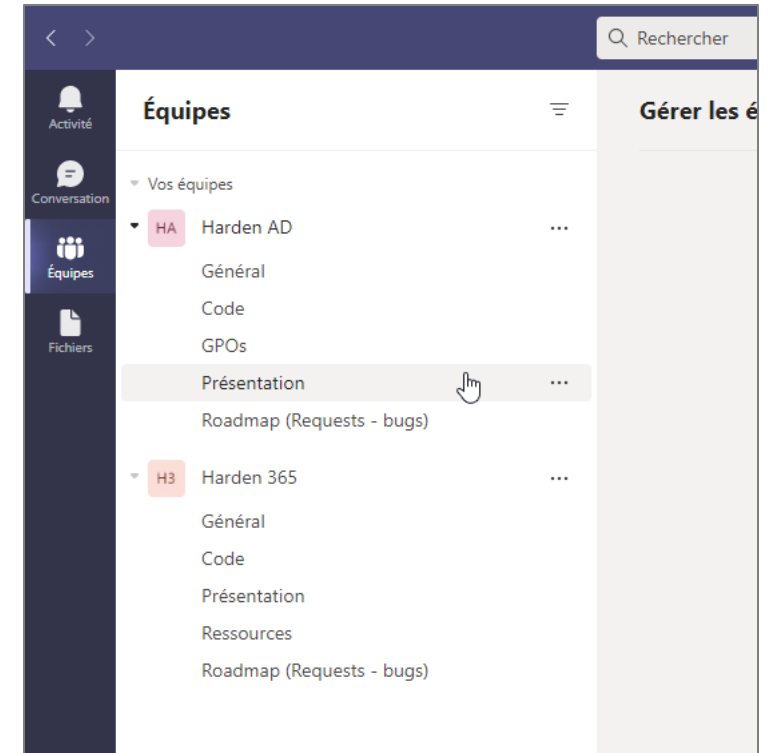


Besoins de classer

- Usage
 - Faciliter la recherche
- Conformité
 - Gestion des périodes de rétention (suppression automatique / conservation des traces)
 - Répartition géographique
- Sécurité
 - Protection des données sensibles (leaks)

Modèles de Teams

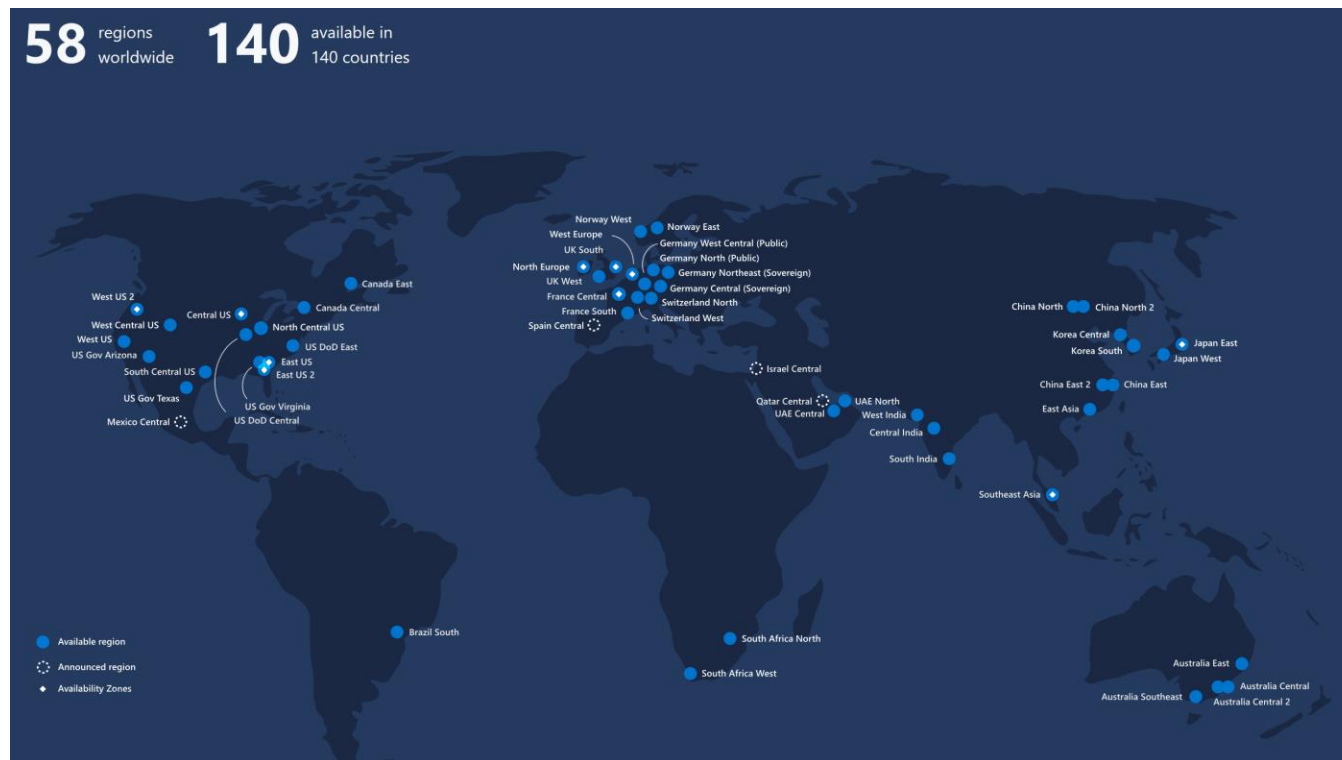
- Création de modèles Teams pour :
 - Uniformiser le classement
 - Initier l'usage de Teams avec les bonnes pratiques
 - Réponse à des scénarios collaboratifs (ex : projets)



- Harden365 : création de modèles types métiers

Localisation des données

- Par défaut : Tout dans une même région avec des subtilités par service



```
AadGraphNotifications/EUGB01
SharePoint/FRA-104-0007
M365LabelAnalytics/NA001
MIPEXchangeSolutions/NA001
M365CommunicationCompliance/NA001
ProjectProgramsAndPortfolios/NA001
MicrosoftThreatProtection/NA001
UniversalStoreService/NA001
AccessControlServiceS2S/EU
AccessControlServiceS2S/EU2
AccessControlServiceS2S/EU3
BecWSClients/*
DirectoryToCosmos/EU001
Metro/NA001
SMIT/NA002
ExchangeOnlineProtection/emea01-04
MicrosoftCommunicationsOnline/EMEA-1E-M1
Sway/NA001
YammerEnterprise/NA008
AzureAnalysis/SDF
WindowsAzure/EMEA001
ProjectWorkManagement/PROD_EU_Org_Ring_152
PowerAppsService/NA001
ProcessSimple/NA001
TeamspaceAPI/NA001
OfficeForms/NA001
MicrosoftStream/NA001
Adallom/EU001
Deskless/NA001
MicrosoftOffice/NorthAmerica7
PowerBI/EU001
RMSOnline/EU
BDM/NA014
AadAllTenantsNotifications/EUGB04
To-Do/NA001
exchange/FRAP264-002-01
CRM/EMEA106
Bing/NA001
MicrosoftKaizala/NA001
WhiteboardServices/NA001
ccibotsprod/NA001
```

Rétention des contenus

- Deux outils
 - Retention policies (par BAL/O4B/SP)
 - Retention labels (par email/fichier)
- 3 comportements
 - Suppression automatique à la fin de la période de rétention (w/wo workflow)
 - Conservation automatique de toute modification (PHL)
 - Rien (pour classement seulement)

The screenshot shows a document management interface. At the top, there's a header with 'Documents contrats' and several icons. Below this, the document title 'Contrat Accompagnement et ...' is displayed with a close button. The date '02/09/2020' is shown. Under 'ID de document', the value 'DEMOSPT-1504233608-1' is listed. The 'État de validation' section has a placeholder 'Entrez une valeur ici'. The 'Appliquer l'étiquette de rétention' section features a dropdown menu currently set to 'Aucun'. The dropdown list is open, showing options: 'Aucun Effacer l'étiquette', 'Donnée personnelle FR', 'Etiquette de retention 20200603', and 'Conserver pendant 7 années'. A 'Plus de détails' link is at the bottom of the dropdown. The 'Activité' section is partially visible at the bottom.

Documents contrats

Contrat Accompagnement et ...

02/09/2020

ID de document

DEMOSPT-1504233608-1

État de validation

Entrez une valeur ici

Appliquer l'étiquette de rétention

Aucun

Aucun Effacer l'étiquette

Donnée personnelle FR

Etiquette de retention 20200603

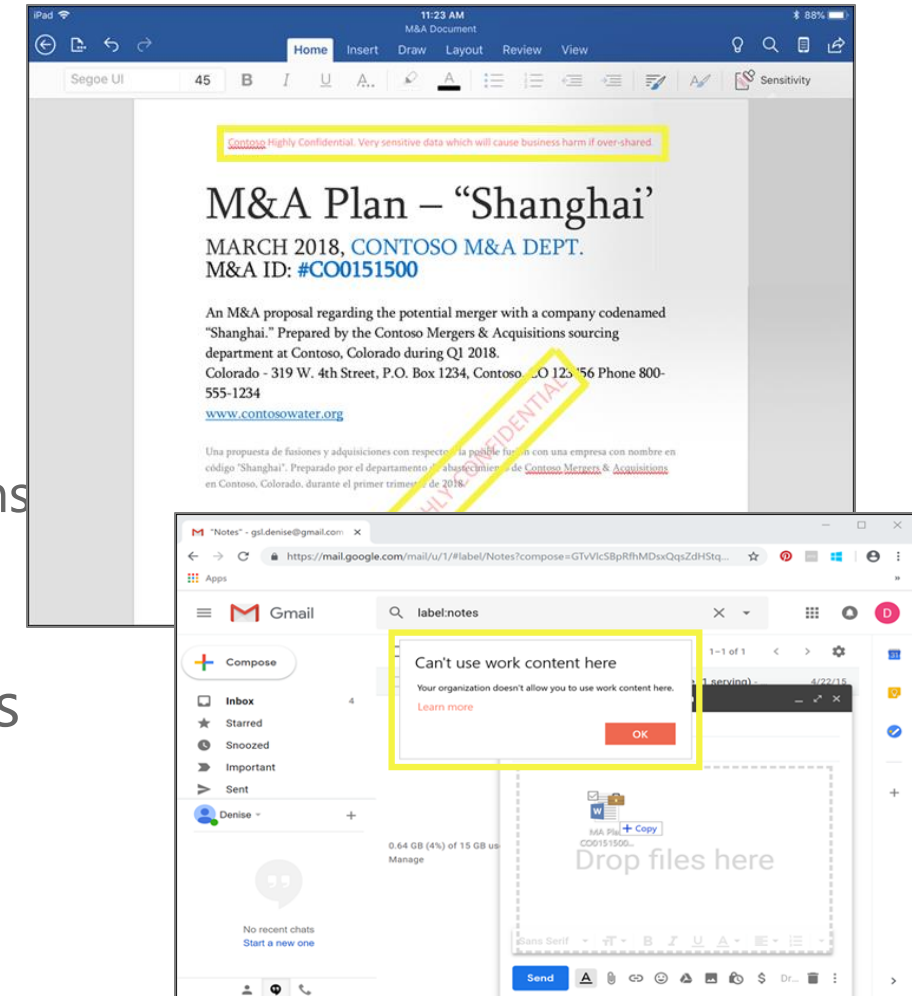
Conserver pendant 7 années

Plus de détails

Activité

Sécurisation des contenus : Sensitivity labels

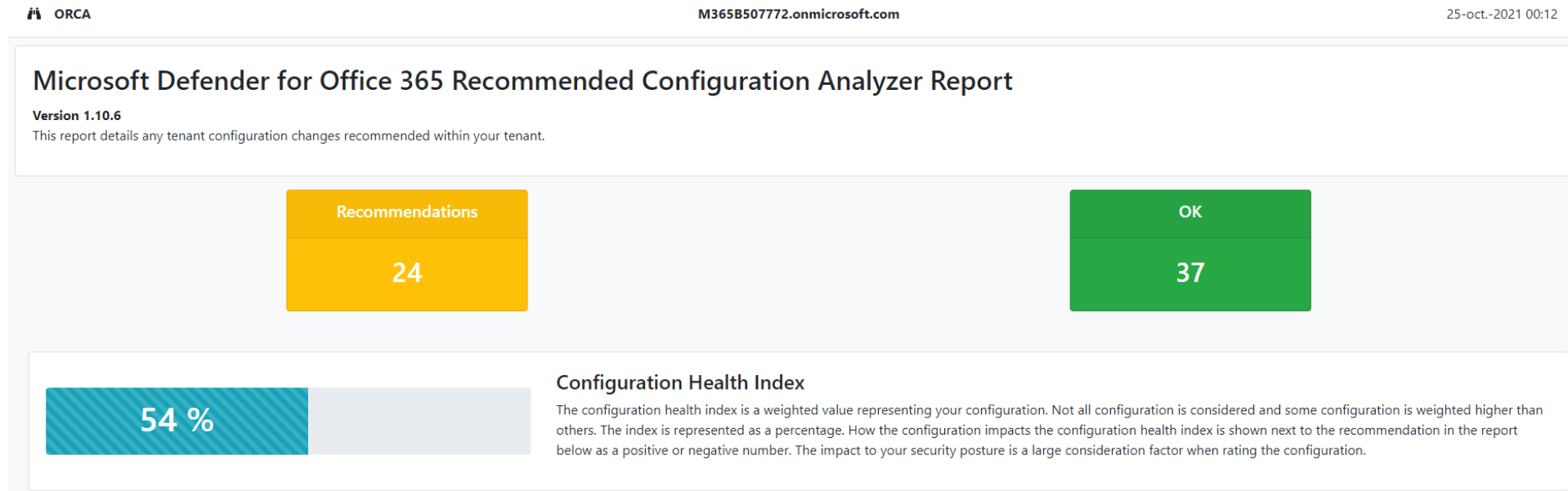
- Application manuelle ou auto (règle ou IA *)
- Chiffrement des fichiers à la volée
 - Impossible à ouvrir si pas authentifié/ pas autorisé
- Restriction des permissions
 - Bloquer le copier/coller, impression, capture écran, trans
- Texte en filigramme
- Bloquer la copie sur clé USB / usage sur services non M365
- Application sur des Groupes O365/Teams





Microsoft Defender for O365

Audit du tenant avec ORCA



<https://www.powershellgallery.com/packages/ORCA/1.10.6>

[Microsoft recommendations for EOP and Defender for Office 365 security settings - Office 365 | Microsoft Docs](#)

Microsoft Defender for O365

Anciennement Office 365 ATP



Plan 1



Plan 2

Anti Spam
Anti Malware
Anti Spoofing
Anti Phishing
Safe Links
Safe Attachments
Safe Documents



-  [Anti-Spam Policies](#)
-  [Advanced Threat Protection Policies](#)
-  [DKIM](#)
-  [Malware Filter Policy](#)
-  [Transport Rules](#)
-  [Zero Hour Autopurge](#)
-  [Tenant Settings](#)
-  [Connectors](#)



Le Modern Workplace

Modern Workplace

Azure AD join :

- ✓ Pilotage via Intune (règles Harden AD)
- ✓ Lightweight LAPS solution for Intune
- ✓ Conformité via Intune.

Azure AD Hybrid Join :

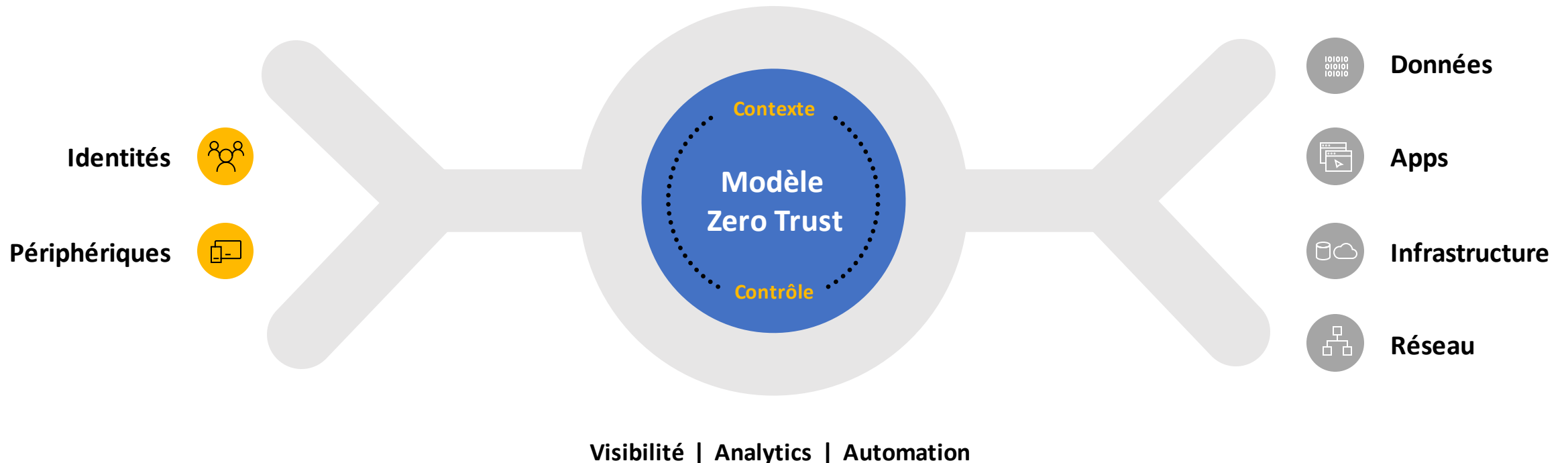
- ✓ Pilotage via les GPO / Intune
- ✓ Laps
- ✓ Conformité via Intune.



Le modèle Zéro Trust

Zero Trust : **Never trust and Always verify**

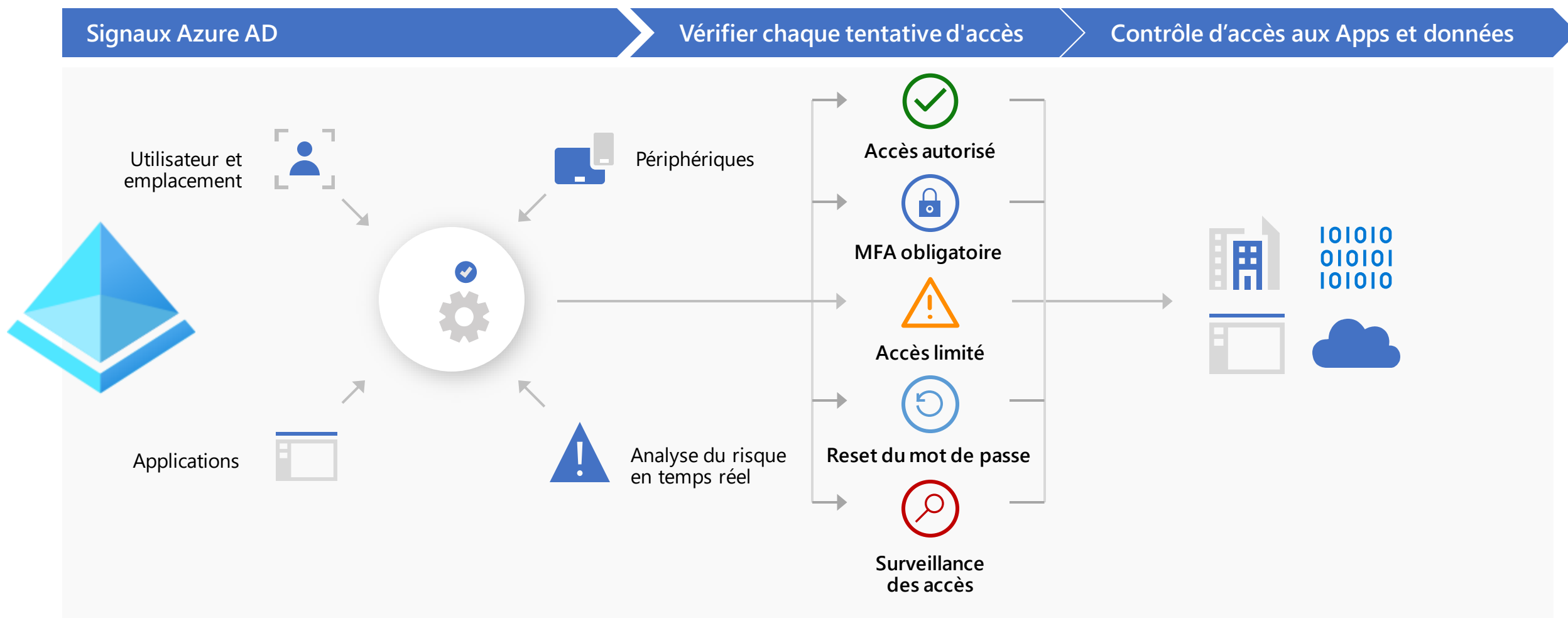
Vérification **explicite** | Privilèges d'accès **minimums** | Suppose une **violation**



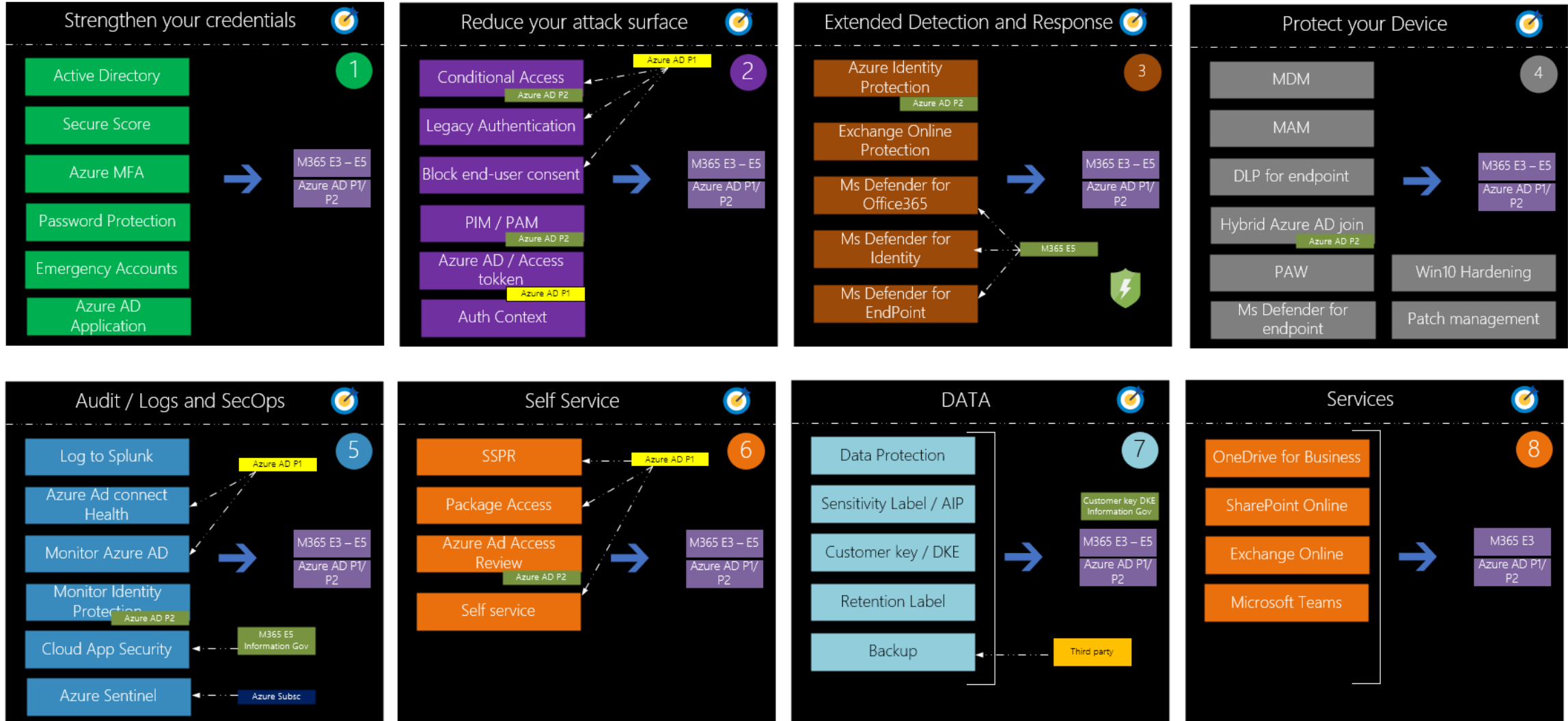
Un cadre de sécurité **MODERNE** basé sur les **Identités** et les **Périphériques**



Zero Trust : Azure AD et le contrôle des accès



Security model - Microsoft 365



Enterprise Model – Tiering model – Privileged Access strategy

Change and communication



Harden, le moteur

Structures des fichiers

The image displays two Windows File Explorer windows side-by-side, illustrating the file structure of the HardenAD project.

Left Window: SecureAD (C:\Users\LOIC\Documents\GitHub\SecureAD)

- Configs
 - Configuration_HardenAD.xml
 - Configuration_HardenAD.xsd
 - logo_harden.txt
 - TasksSequence_HardenAD.xml
 - TasksSequence_HardenAD.xsd
- Inputs
- Logs
- Modules
- Outputs
- Tools
 - HardenAD.ps1
- LICENSE
- README.md

Right Window: Debug

Name	Date modified	Type
Debug_Convert-MigrationTable.log	27/10/2021 21:43	Text Document
Debug_Import-WmiFilters.log	27/10/2021 21:43	Text Document
Debug_Install-LAPS.log	27/10/2021 21:45	Text Document
Debug_New-AdministrationAccounts.log	27/10/2021 21:43	Text Document
Debug_New-AdministrationGroups.log	27/10/2021 21:43	Text Document
Debug_New-GpoObject.log	27/10/2021 21:45	Text Document
Debug_New-M365OrganizationalUnits.log	27/10/2021 21:43	Text Document
Debug_New-ScheduleTasks.log	27/10/2021 21:45	Text Document
Debug_Publish-MigrationTable.log	27/10/2021 21:43	Text Document
Debug_Reset-GroupMembership.log	27/10/2021 21:45	Text Document
Debug_Set-ADRecycleBin.log	27/10/2021 21:43	Text Document
Debug_Set-DefaultObjectLocation.log	27/10/2021 21:43	Text Document
Debug_Set-GpoCentralStore.log	27/10/2021 21:43	Text Document
Debug_Set-LapsScripts.log	27/10/2021 21:45	Text Document
Debug_Set-msDSMachineAccountQuota...	27/10/2021 21:43	Text Document
Debug_Set-SiteLinkNotify.log	27/10/2021 21:43	Text Document
Debug_Set-TreeOU.log	27/10/2021 21:43	Text Document
Debug_Update-PreferenceXML.log	27/10/2021 21:43	Text Document
welcome.txt	16/10/2021 16:28	Text Document

Le fichier XML



TasksSequence_HardenAD.xml



One more thing...



HARDEN³⁶⁵

Protect your data in minutes

Une première version de la solution Harden 365 devrait être disponible premier trimestre 2022.



Rejoignez-nous, contactez nous :
contact@harden.world

IDENTITY DAYS

28 octobre 2021 - PARIS



@IdentityDays #identitydays2021

Merci à tous nos partenaires !



onelogin



yubico

ManageEngine



Exakis Nelite

