IDENTITY DAYS

28 octobre 2021 - PARIS

@IdentityDays #identitydays2021

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com

IDENTITY DAYS

28 octobre 2021 - PARIS

Cloud hybride et Zero Trust

Protection des Identités, des authentifications, des accès et des données
Vers un modèle d'Identités SecOps complet pour l'entreprise

''Du mythe à la réalité"

Jean-Francois Apréa
IT & Cloud Architect | Microsoft MVP
AZ IT Consulting - A partner of SPIE ICS

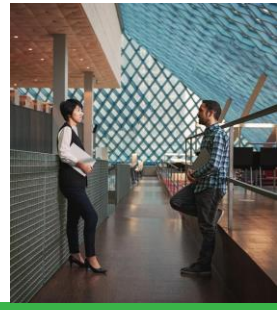
Seyfallah Tagrerout
IT & Cloud Architect | Microsoft MVP
STC Consulting (Switzerland)

Agenda

Zero Trust?

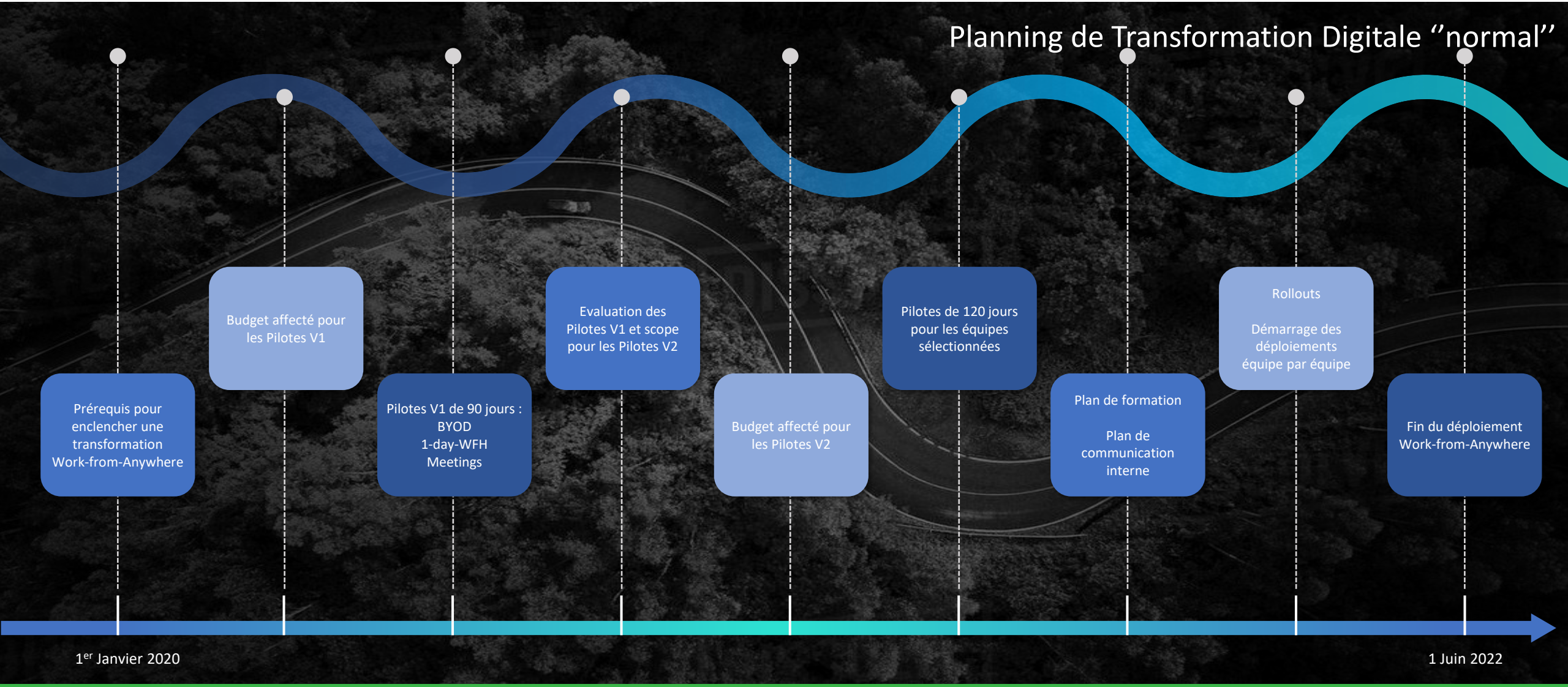
It’s urgent to go, because it’s urgent to be really protected!

- AAD + Accès Conditionnels + Defender = Microsoft Zero Trust
- Protection des Identités Azure et On-Premise
- Protection des comptes privilégiés (PIM)
- Comptes de récupération d’urgence Azure
- Authentifications FIDO2 et Passwordless
- Microsoft Defender 365 : Endpoints, Identités, O365, Azure
- Microsoft Cloud App Security (MCAS)
- Secured-Core PC ‘’from Chip to Cloud’’
- Bonnes pratiques et Plan d’actions en 12 étapes



1 Zero Trust : Pourquoi est-ce si important ?

Avant le COVID-19



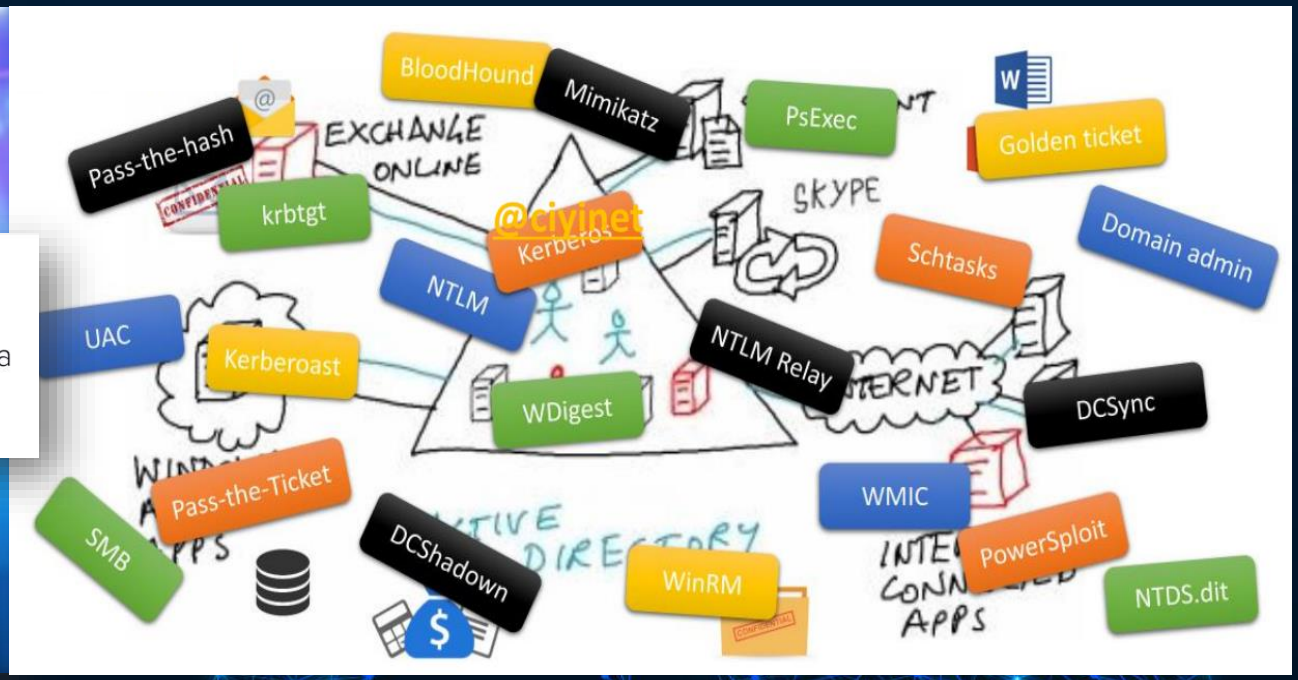
A cause du COVID-19

Ere COVID-19, infrastructure On-Premise et Cybercriminalité

Augmentation continue du risque Cyber

12 Aug 2021

IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach

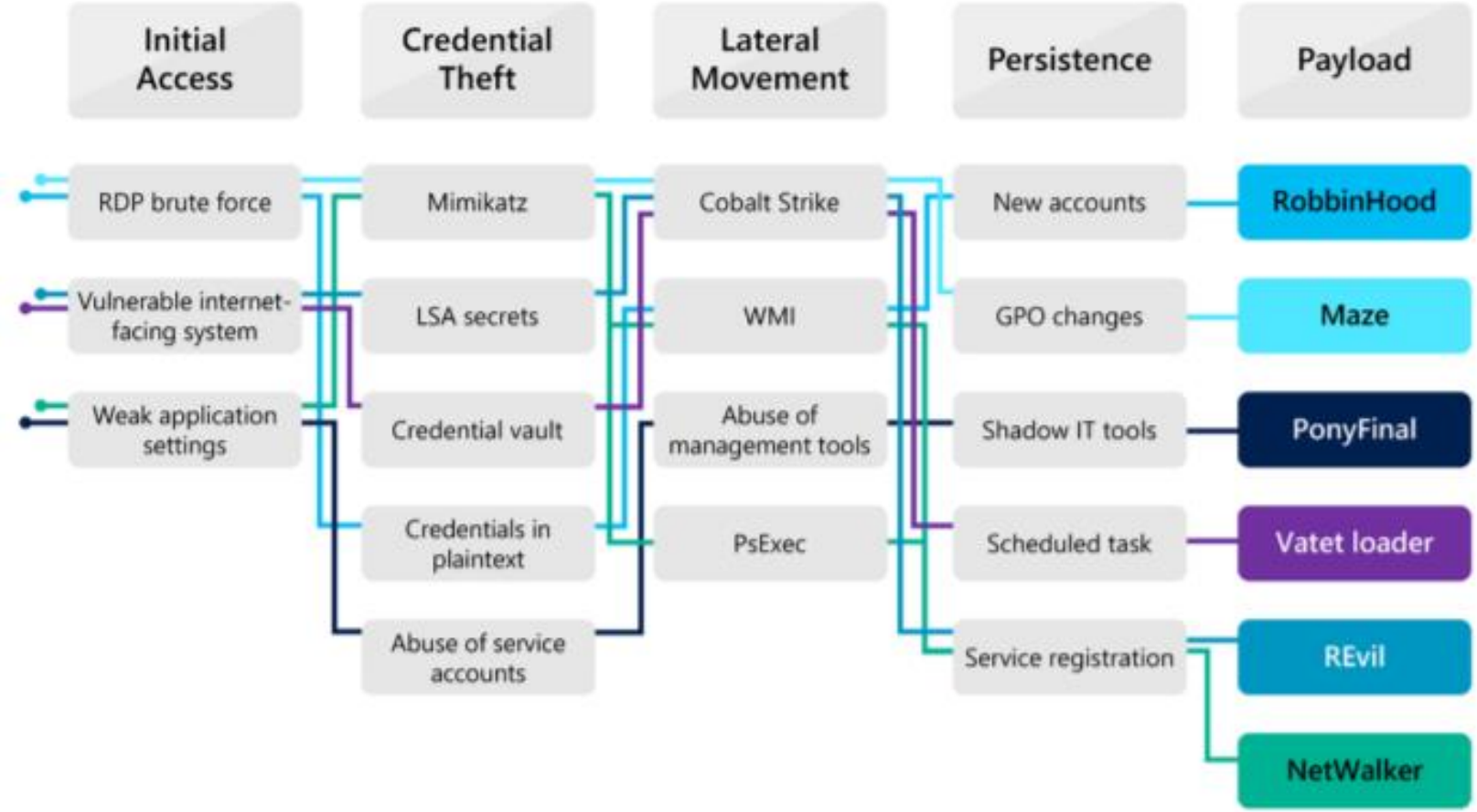


AD et Exchange sont les maillons faibles de 90% des entreprises !

Environnement On-Premise

Cybercriminalité : Ransomwares "de + en + sophistiqués"

Ransomware operations attack pattern detail observed by Microsoft Threat Protection intelligence in early 2020. Payloads might vary, but mitigations apply across all varieties.



Source: Microsoft Digital Defense Report, September 2020
Human-operated ransomware attacks: A preventable disaster

News Microsoft Cybercriminalité

Source: Microsoft Digital Defense Report, October 2021

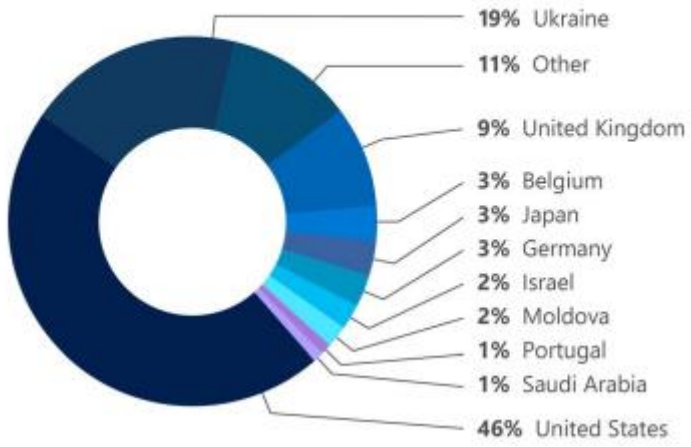
Microsoft Digital Defense Report OCTOBER 2021

MDDR octobre 2021 | 128 pages à lire absolument

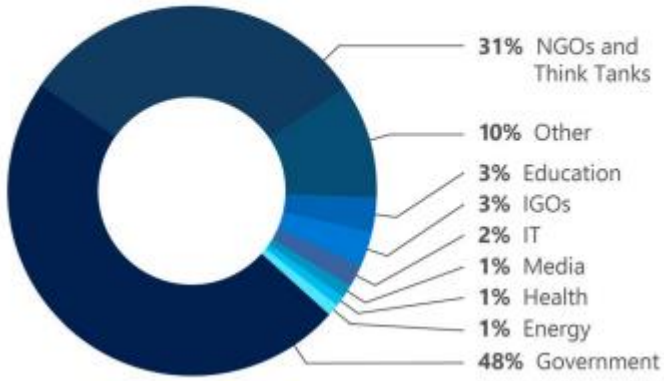
- Update 2021 sur l'état de cybercriminalité
- Menaces sur les états nations
- Menaces sur les chaînes d'approvisionnement et la sécurité IoT
- Menaces sur la sécurité des environnements hybrides
- Désinformation et informations exploitables

- Nouveaux ransomware en mode RaaS
- Modèle de double extorsion : vol + publication
- Généralisation du paiement via crypto-monnaie
  Cibles : Entreprises 79% et Consommateurs 21%
- 168K sites de phishing stoppés par MS en 2021
- Plus d'espionnage que de destruction de données

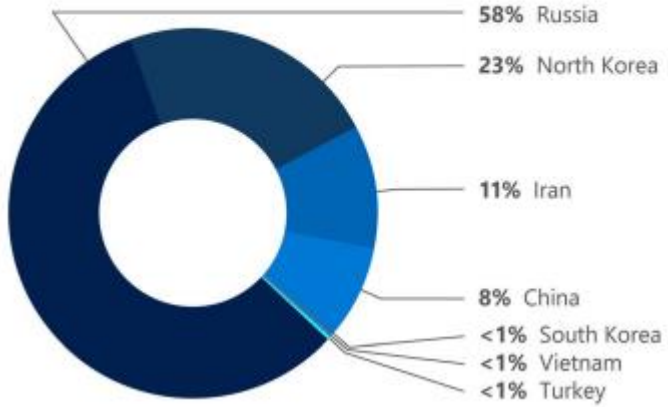
Most targeted countries (July 2020-June 2021)



Most targeted sectors (July 2020-June 2021)



Attacks by country of origin (July 2020-June 2021)



Annonce du 25 aout 2021 : Acquisition de RiskIQ et CloudKnox | Budget sécurité Microsoft porté à 20B$ sur 5 ans (x4)

2

Zero Trust : Concept & Principes

Protection des accès de bout-en-bout et Risques Cyber

Zero Trust : Never trust and Always verify

Vérification explicite

- Identités
- Emplacements réseaux
- Etat de santé
- Classification des données
- Comportements et Anomalies

Privilèges d'accès minimums

- Accès JIT & JEA
- Stratégies de risques
- Protection des données

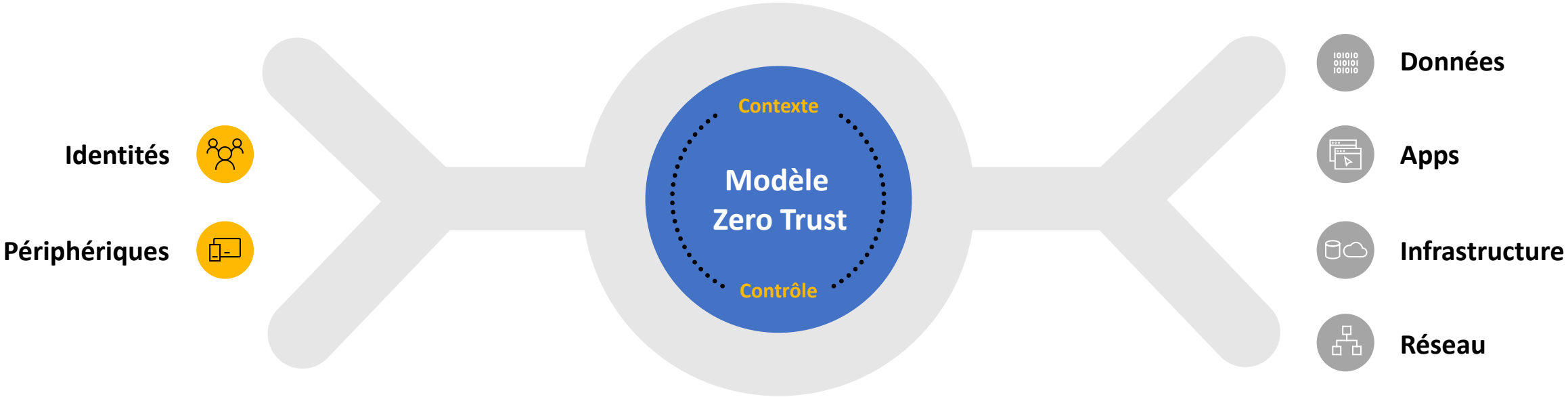
Suppose une violation

- Minimisation des menaces
- Limitation des mouvements latéraux
- Micro-segmentation & Réseaux
- Contrôle de session de bout en bout

Aujourd'hui, une stratégie Zero Trust est un impératif !

Zero Trust : Never trust and Always verify

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

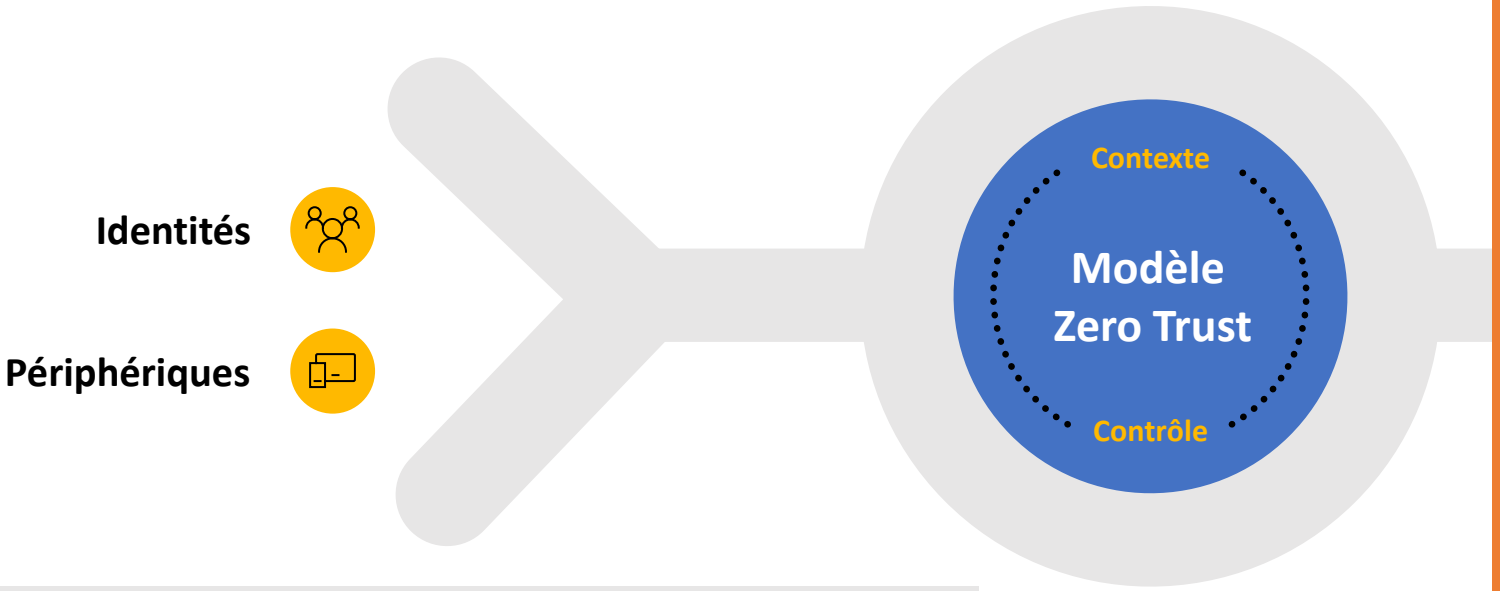


Visibilité | Analytics | Automation

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

Pourquoi implémenter un modèle Zero Trust ?

Cadre complet pour sécuriser les identités
et les périphériques utilisés par les utilisateurs



1/3 des attaques proviennent du Phishing
Attaques sur les mots de passe : +230% en 2021

des violations impliquent l'utilisation de mots de passe perdus ou volés

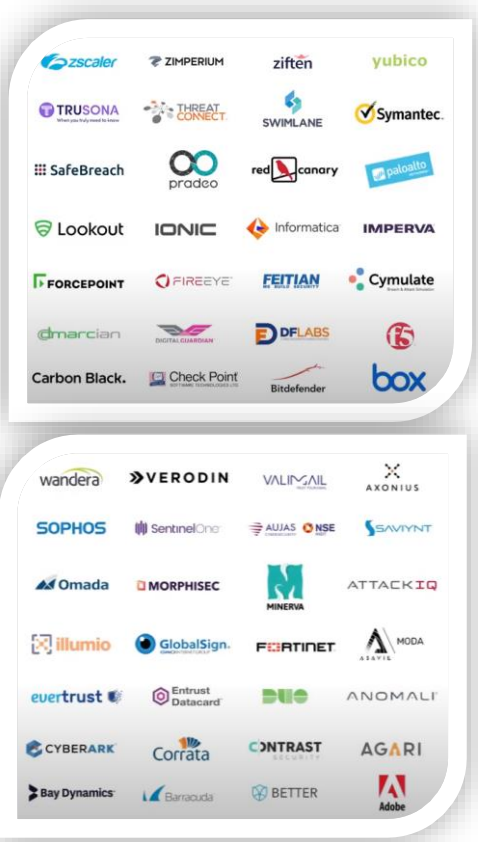
des périphériques de type BYOD ne sont pas sécurisés par l'IT

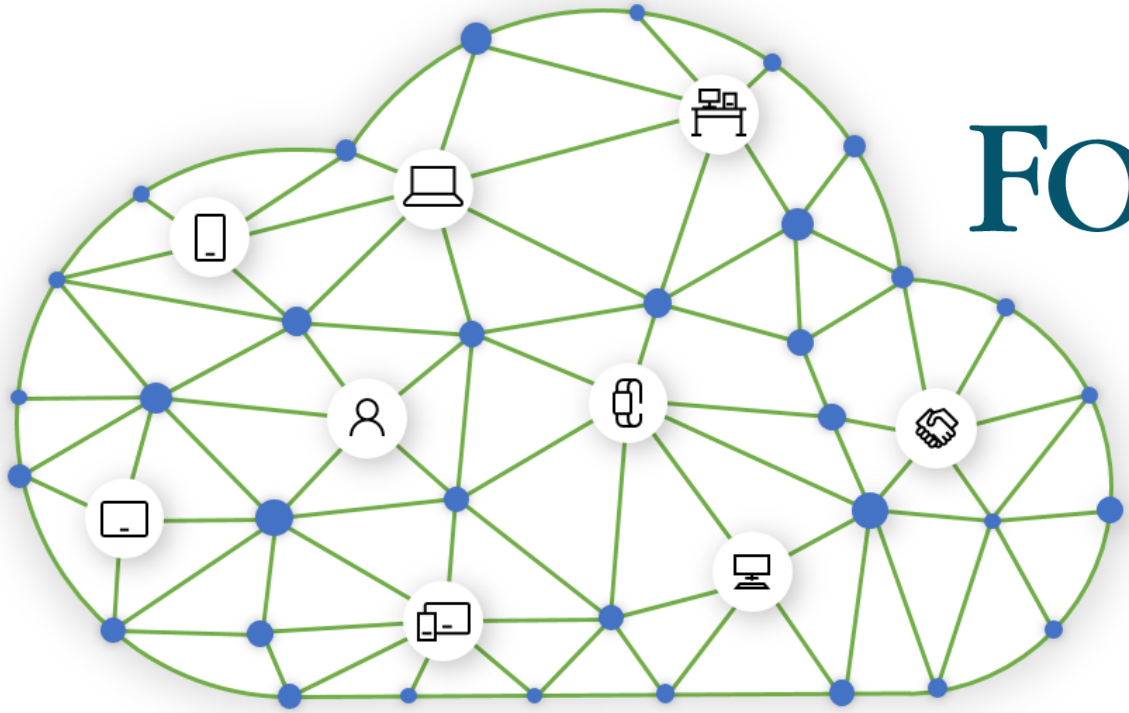
attaques de mots de passe par seconde !

Source: "Microsoft Airlift October 2021"
Source: "Verizon 2020 Data Breach Investigations Report"
Source: "Mobile security—the 60 percent problem" Brian Peck, Zimperium, April 7, 2020

Zero Trust : Never trust and Always verify

Microsoft Intelligent Security Association





FORRESTER®

Microsoft

Google

"Le futur de la cybersécurité est dans le cloud." [1]

[1] https://go.forrester.com/blogs/tech-titans-google-and-microsoft-are-transforming-cybersecurity/

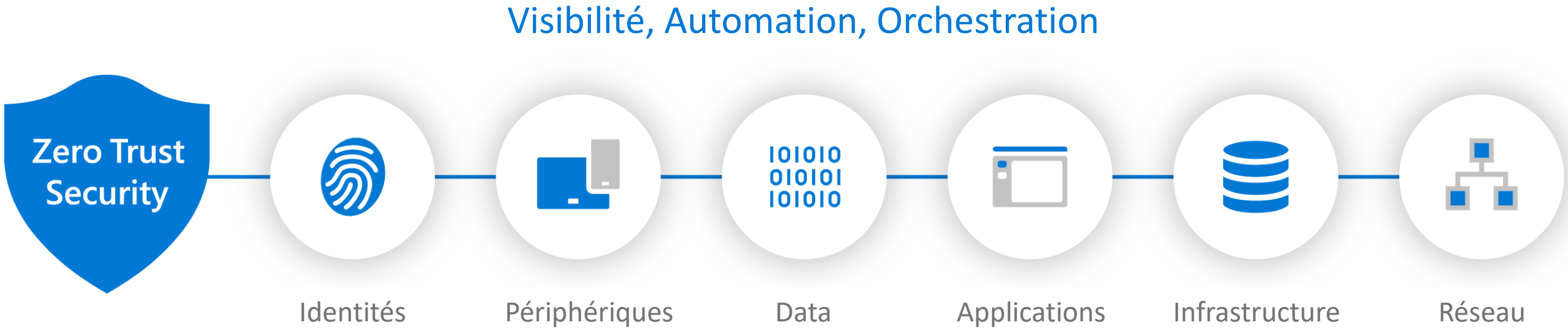
3

Zero Trust : Les Identités au centre de l'IT

Comment implémenter le modèle Zero Trust dans votre entreprise ?

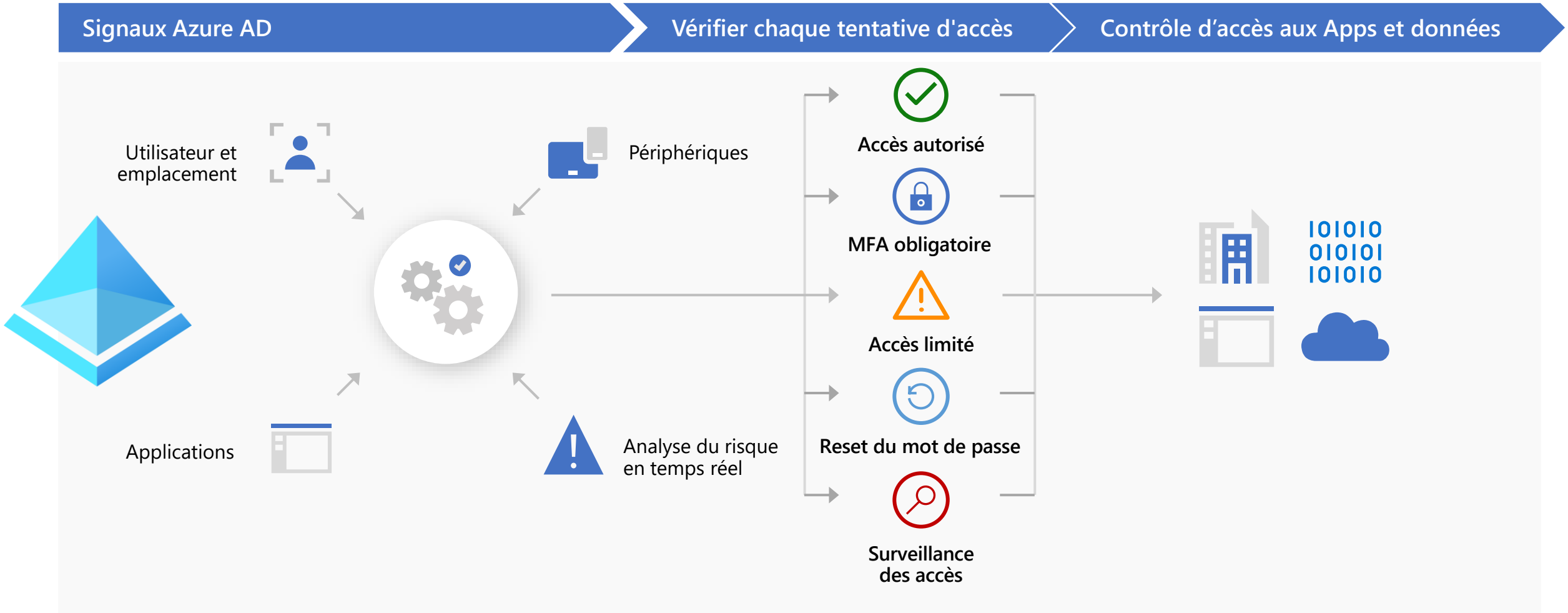
Identités, Authentifications, Accès conditionnels et Protection des Ressources

Zero Trust : Zoom sur l'implémentation Microsoft

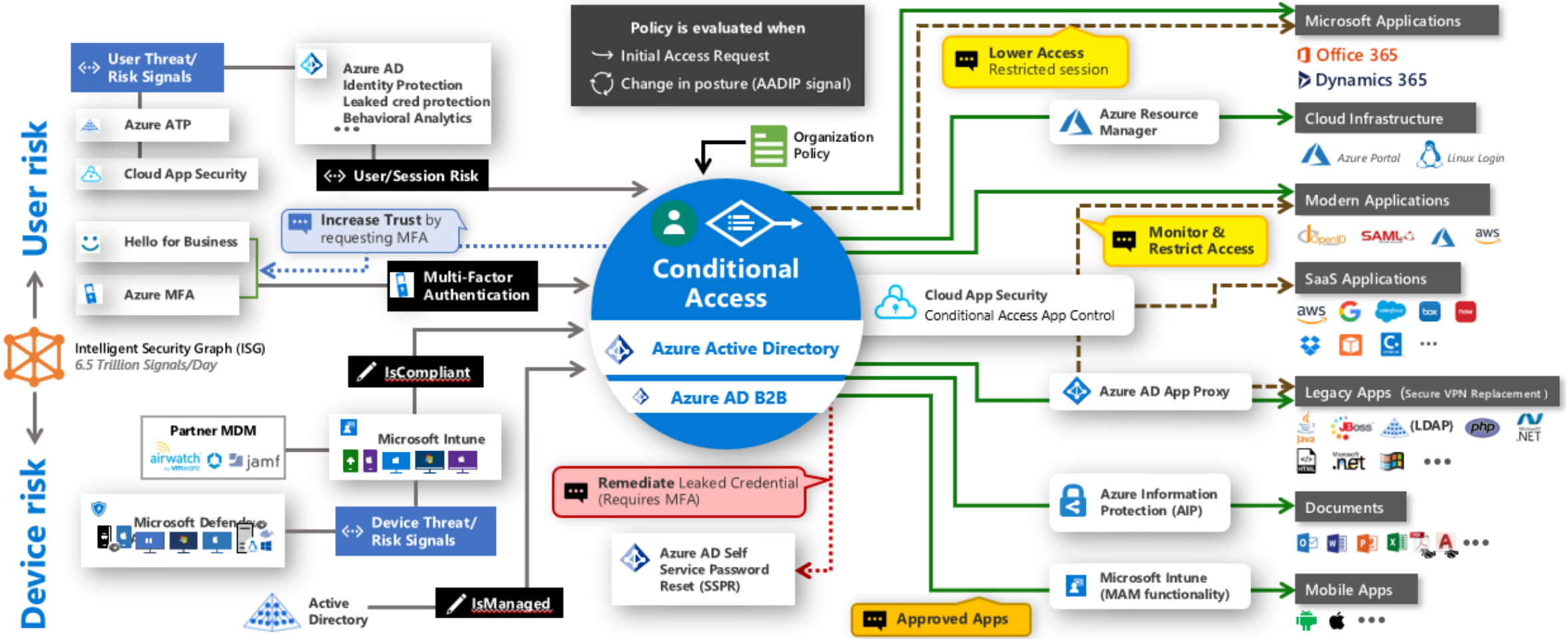


https://aka.ms/zerotrust
https://www.microsoft.com/en-us/security/business

Zero Trust : Azure AD et le contrôle des accès



Zero Trust : Zoom sur Azure AD Conditional Access



Signals
to make an informed decision

Decisions
based on organizational policy

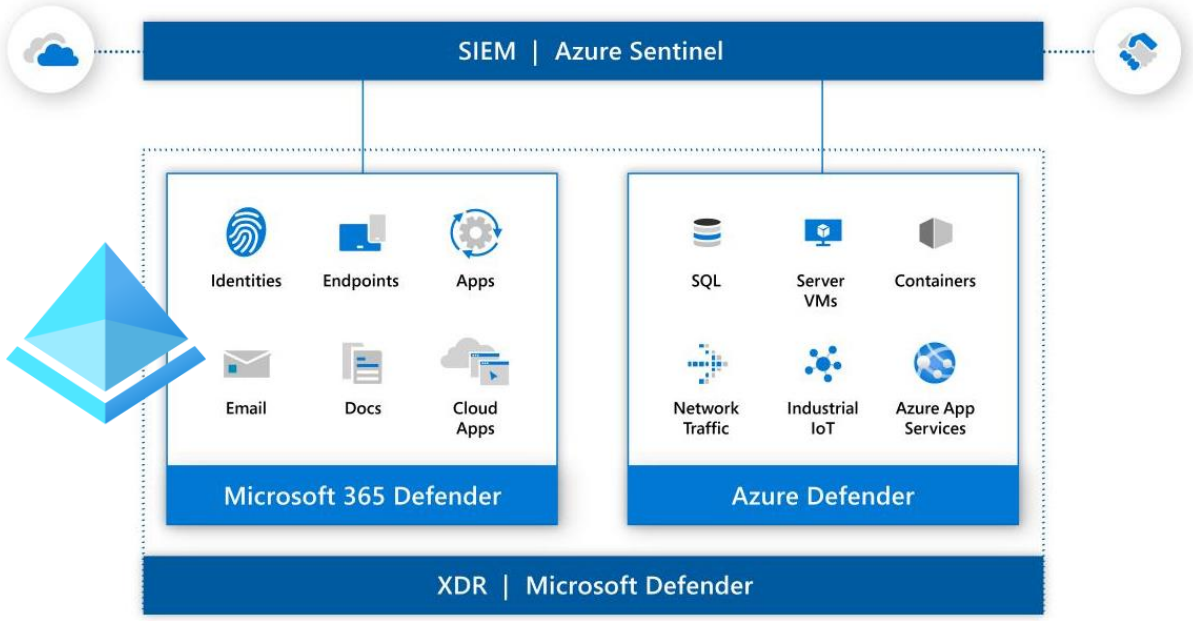
Enforcement
of policy across resources

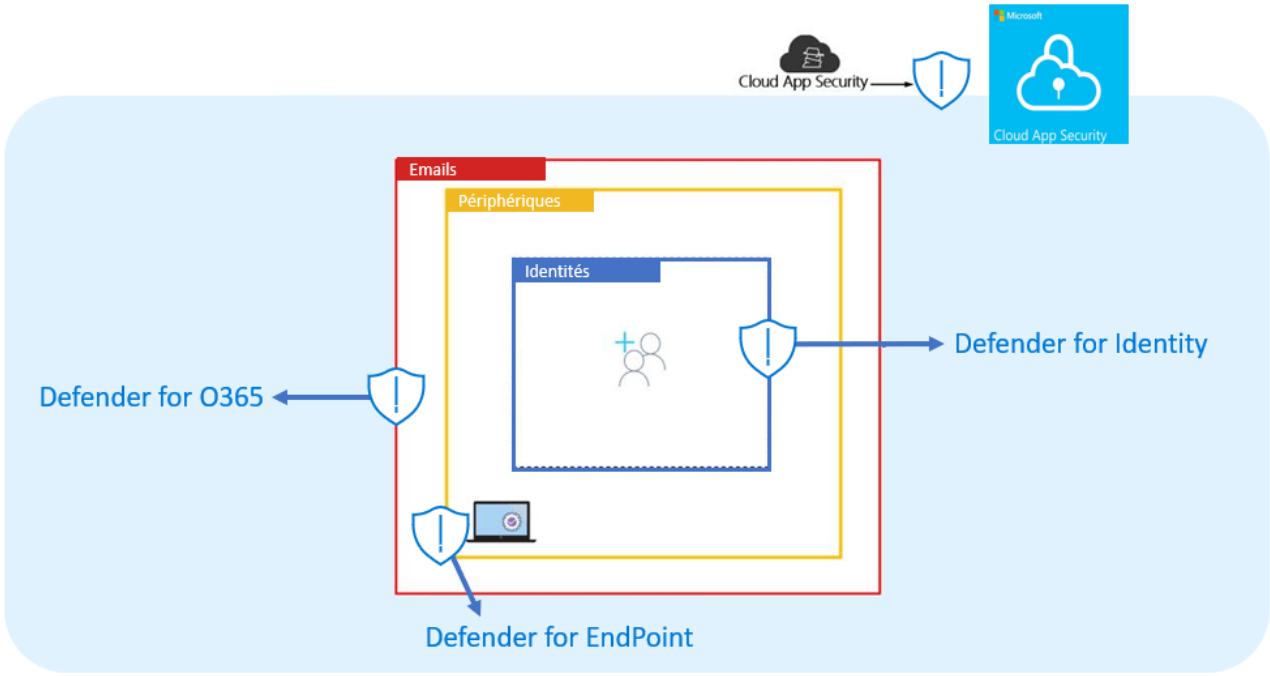
4 Déploiement d'une stratégie Zero Trust Microsoft

Approche ''Etape par étape'' et RETEX

Zero Trust : Azure AD P1/P2 + M365 Defender

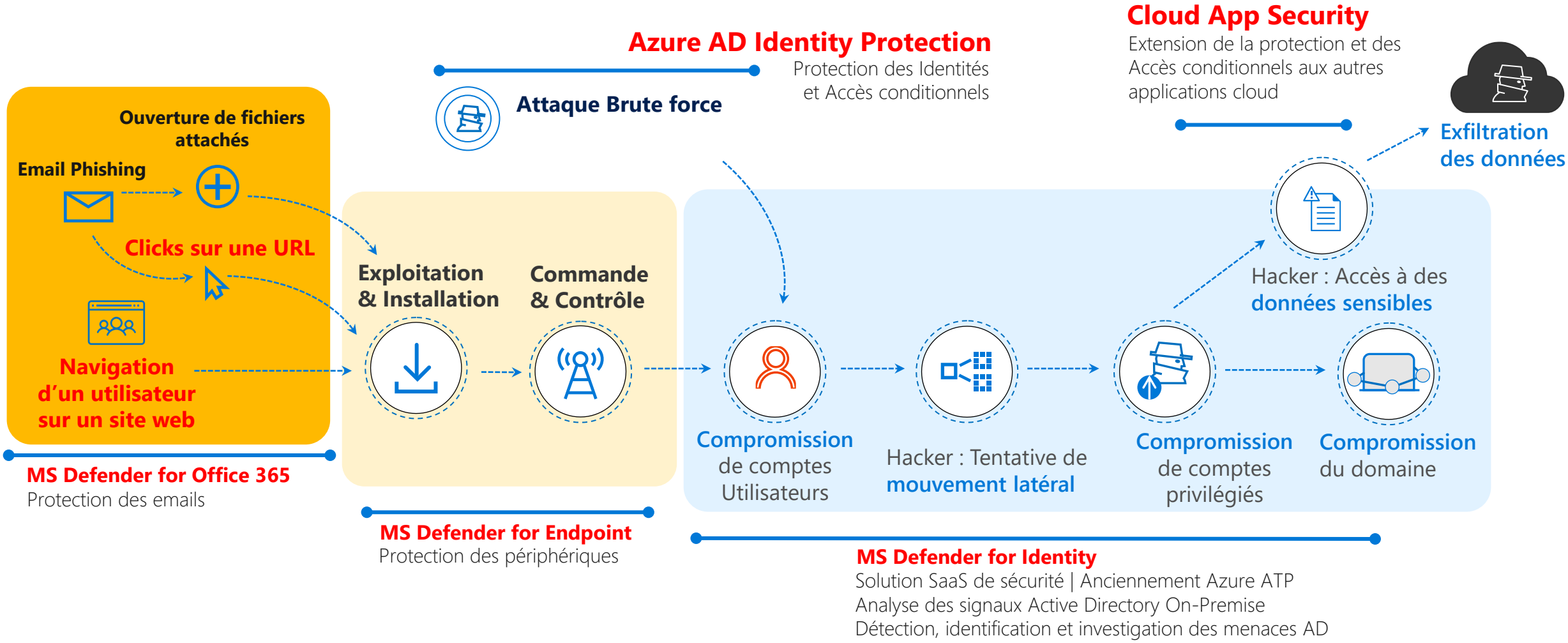
eXtended Detection and Response





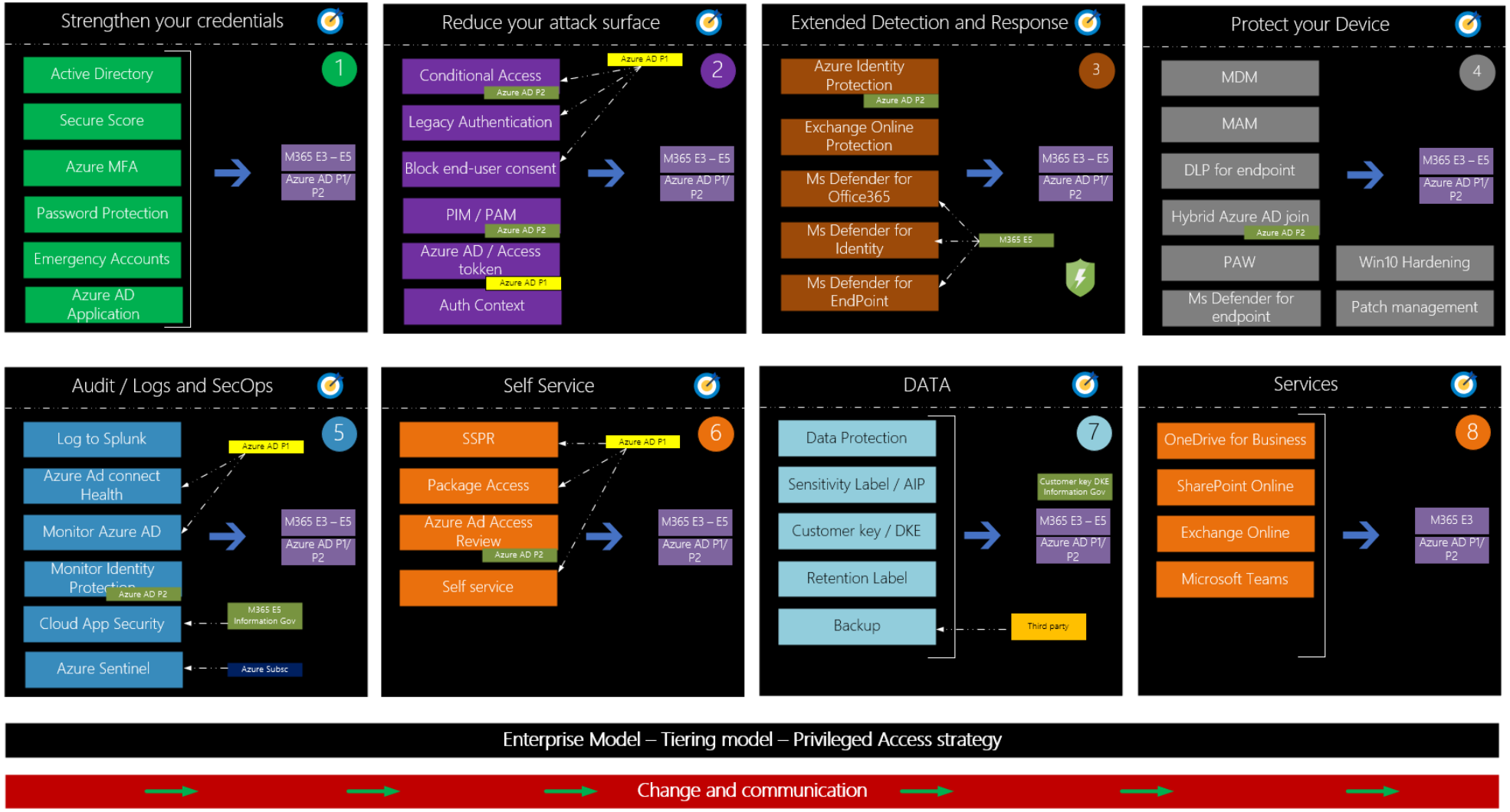
Zero Trust : Protection XDR avec M365 Defender

Détection à tous les stades de l'attaque



Déploiement d'une stratégie Zero Trust

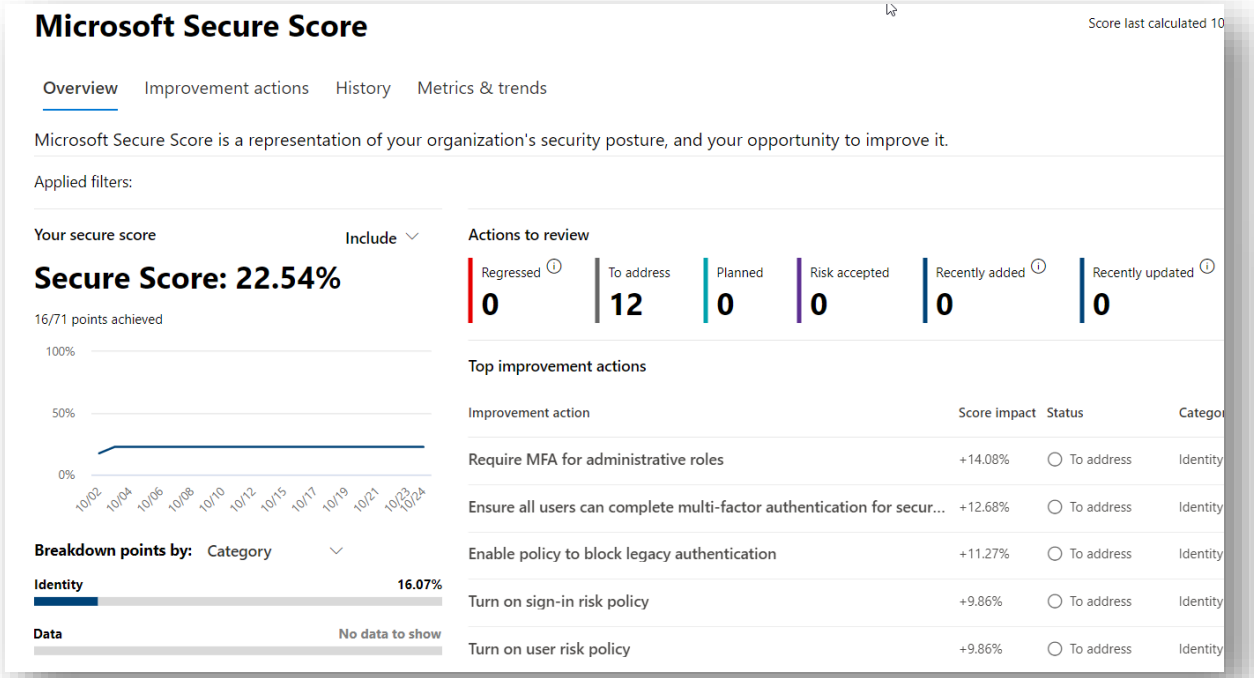
Approche étape par étape et recommandations

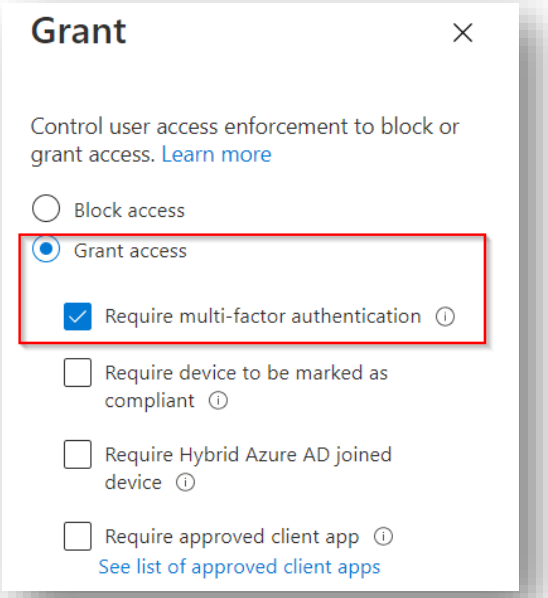


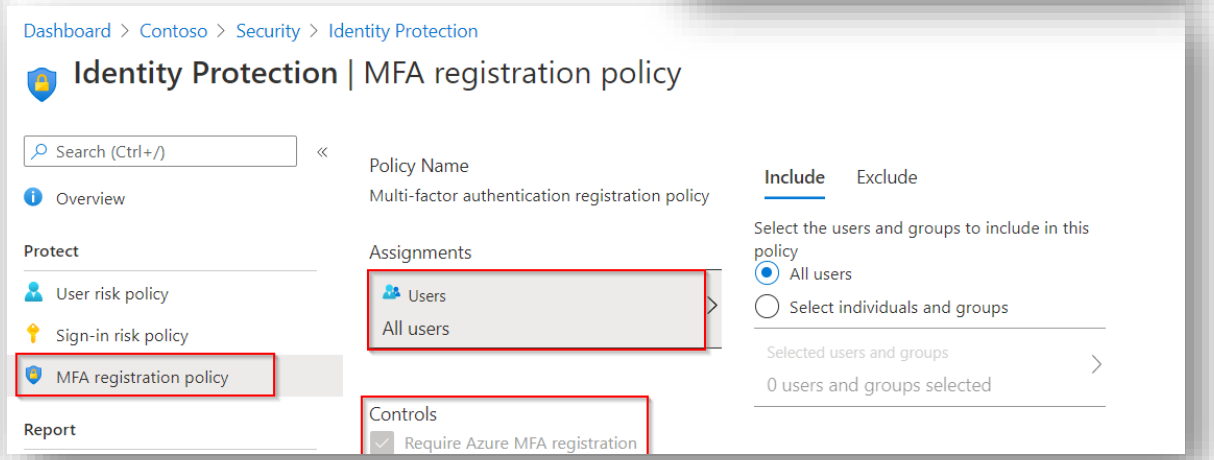
1. Renforcez vos secrets

Approche étape par étape et recommandations

Utilisez Microsoft Secured Score + déployez MFA + activez Identity Protection (P2)







2. Renforcez vos secrets entre AD et Azure AD

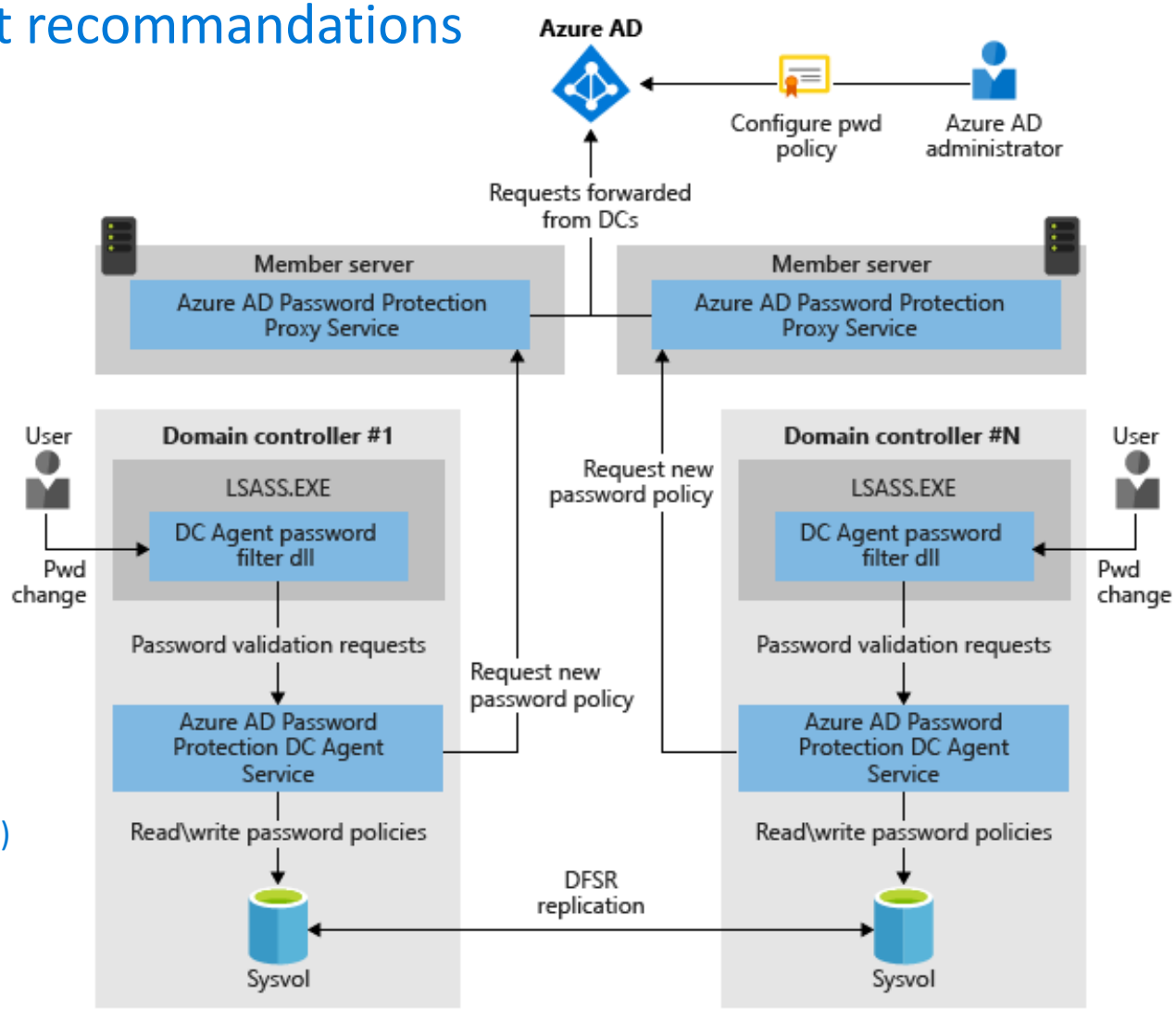
Approche étape par étape et recommandations

Déployez Azure AD Smart Lockout

- Pour les comptes cloud Azure AD
- Et aussi pour les comptes hybrides

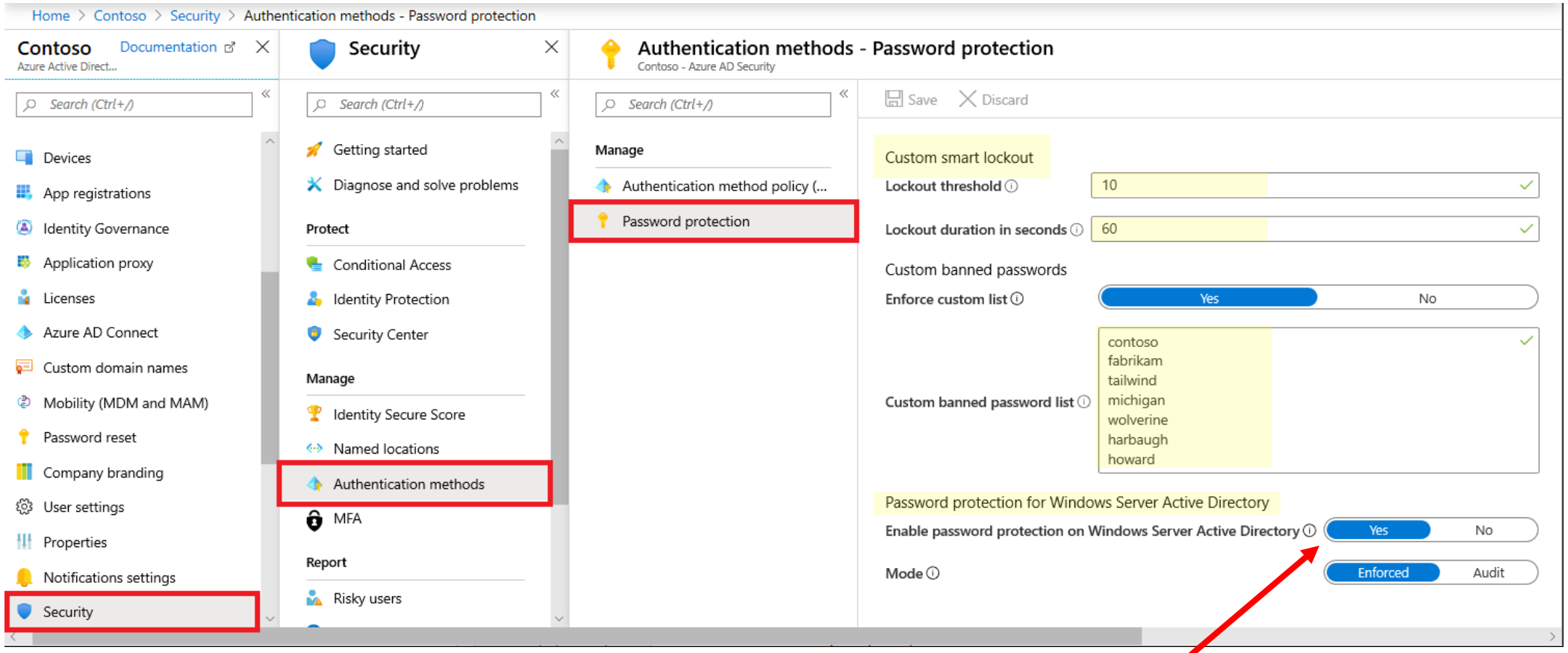
Déployez l'authentification sans mot de passe

- Clés de sécurité FIDO2
- Microsoft Authenticator (Android / iOS)



2. Renforcez vos secrets entre AD et Azure AD

Approche étape par étape et recommandations



Déployez l'authentification sans mot de passe

Déployez Azure AD Smart Lockout

3. Renforcez vos secrets : Comptes d'accès d'urgence Azure AD

Approche étape par étape et recommandations (Break Glass Accounts)

Créez DEUX comptes de secours

- Seulement dans Azure AD
- Ne pas activer de synchronisation
- Ne pas utiliser MFA
- Ne pas utiliser de clés FIDO2

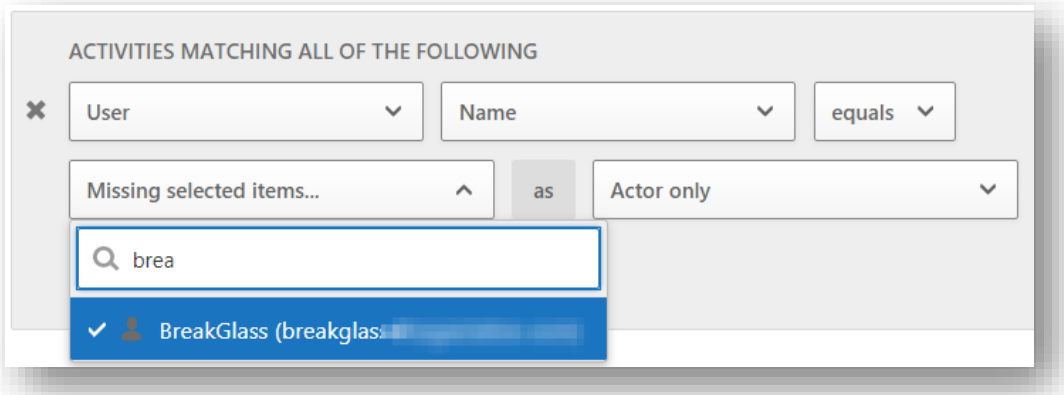
Désactiver l'expiration du mot de passe

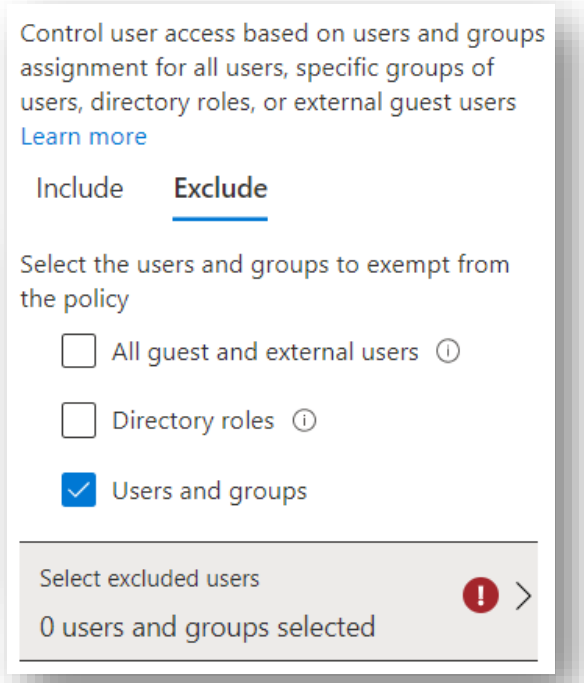
```
Set-MsolUser -UserPrincipalName
breakglass@domain.onmicrosoft.com
-PasswordNeverExpires $true
```

Activez un audit renforcé sur ces deux comptes

- Azure Log Analytics
- Azure Sentinel
- Cloud App Security (MCAS)

Désactivez les accès conditionnels





Stockez les mots de passe de ces comptes de secours dans plus de 1 coffre fort

Stockage en plusieurs parties

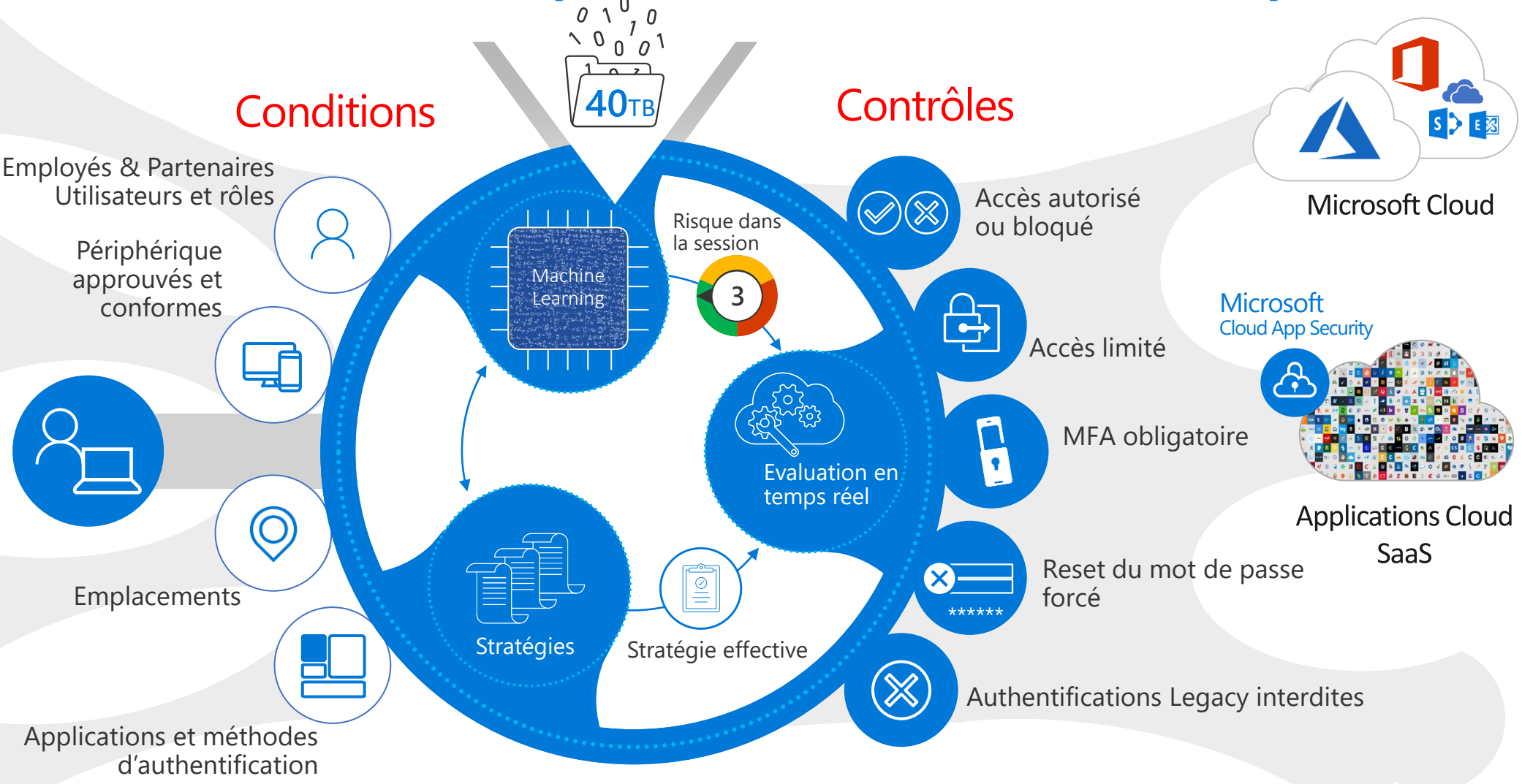
4. Réduisez votre exposition / surface d'attaque

- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Géo-location
- Réseau d'entreprise

- Apps. Browser
- Apps Clientes



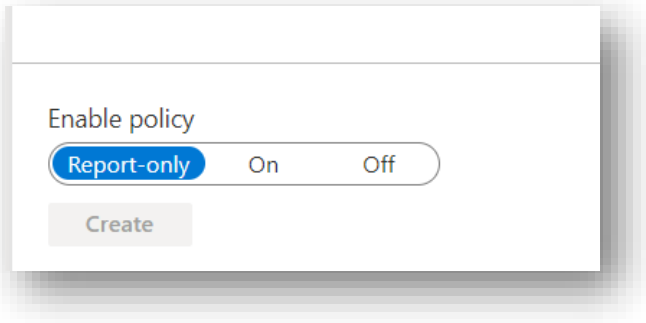
Utilisez les Accès conditionnels comme un ''Super firewall'' pour tous les accès

4. Réduisez votre exposition / surface d'attaque

Utilisez les Accès conditionnels comme un ''Super firewall'' pour tous les accès

Bonnes pratiques Accès conditionnels

- Toujours tester le comportement avant
- What if?
- Mode ''Rapport seulement''



Area	Description
Authentication Policies	- Enforce MFA for All administrators - Enforce MFA for all standard user - Enforce MFA for all Guest users - Block Legacy authentication - Reduce attack surface
Device Access Policies	- Block unsupported device platform - Require managed devices (endpoint Manager) – Admin station - Require approved app for mobile access (MAM) - Require managed devices - Specific conditional access for Mac Os (if needed)
Strict Security Policies	- Block MFA registration from untrusted location - Require Term of use for: All Administrator / Guest Access / Consultants - Control Sign-in Frequency - Disable persistent browser - Block foreign locations - Require trusted location for all admins - User Risk-based and Sign-in Risk based (via Identity Protection) - Authentication context ➔ PIM / MIP labeled SharePoint site / Cloud app security upload and download - Privileged access via filters for Devices

5. Protégez vos comptes Azure à forts privilèges

Utilisez PIM (Privileged Identity Management (Azure AD P2)

Bonnes pratiques PIM

1. Activez PIM pour les comptes privilégier
2. Activez PIM pour tous les rôles d'administration (Zero Trust)
3. Configurez chaque rôle avec le MFA
4. Pour un compte Global Admin, accordez 2H max (Zero Trust)
5. Pensez à la durée par défaut | Permanent pour les partenaires
6. Configurez les notifications par email pour tracer les usages
7. Configurez les Access Reviews pour PIM toute les semaines

6. Protégez vos Contrôleurs de domaine AD

Utilisez Microsoft Defender for Identity (anciennement ATA)

Microsoft

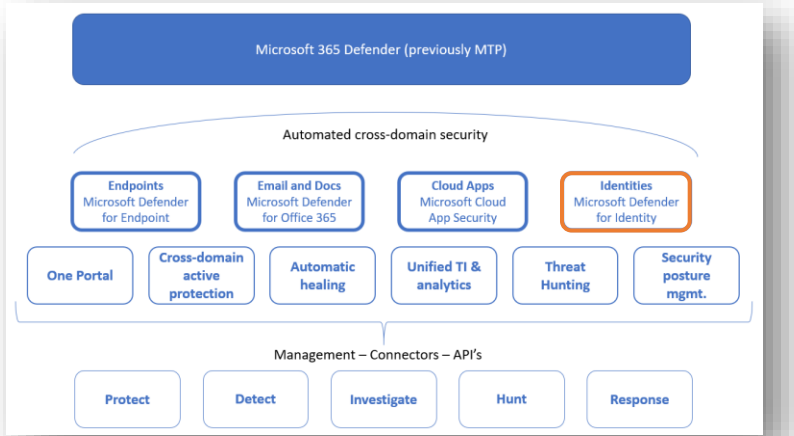
Microsoft Advanced Threat Analytics

Solution installée On-Premise
Server ATA Center
Seulement 1 version / an
Pas de détection DC Shadow
ATA Gateway vs Light Gateway
Inclus avec EMS E3

Microsoft

Microsoft Defender for Identity

Protection SaaS hyperscale dans Azure
Intégration MCAS
Support multi forêts
Détection des DC Shadow
MAJ continues en mode SaaS
ATA Sensor & ATA Sensor Standalone
Inclus avec EMS E5, M365 E5 et M365 Security E5



Machine Learning

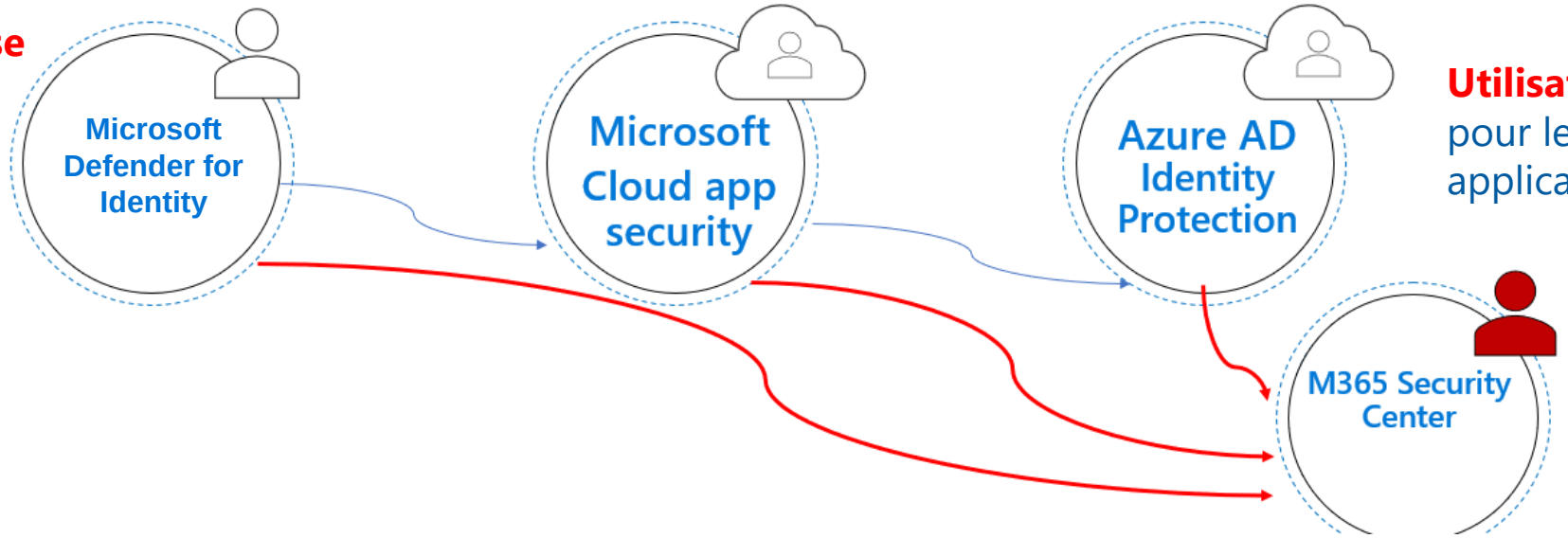
Protection

7. Audit & Log pour l'investigation

Adoptez un modèle SecOps

Comportement des
Identités On-Premise

Comportement des
Identités SaaS sur les applications Cloud



Utilisateurs à risques
pour les utilisateurs et applications Cloud

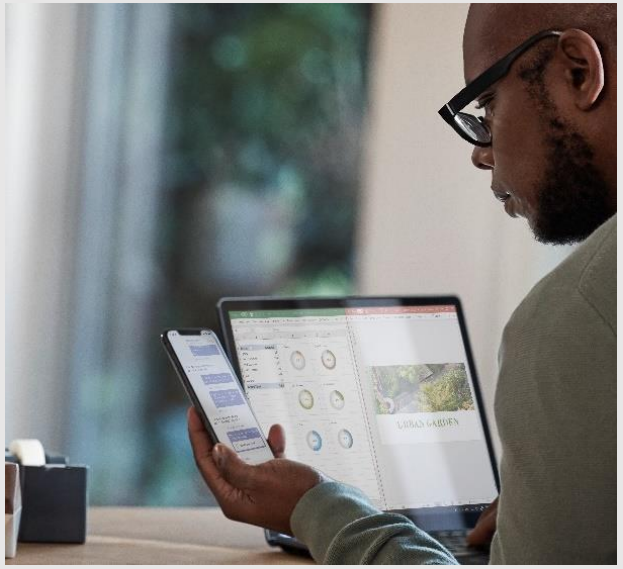
1. **Pour vos VIP / IT Admins, déployez Azure AD P2 ou M365 E5 ou M365 E5 Security**
2. **Déployez Microsoft Cloud App Security (MCAS)**
3. **Utilisez M365 Security Center inclus avec M365 E5**

5

Sécurisation des Authentifications
Sécurisation des Opérations d'administration

Passez au mode Passwordless avec quelque chose que vous avez
+ quelque chose que vous êtes ou que vous connaissez !

Sécurisez vos Identités avec Seamless SSO et Passwordless



Authentification sans mot de passe

- Microsoft Authenticator
- Windows Hello
- Clés de sécurité FIDO2
- Biometrics

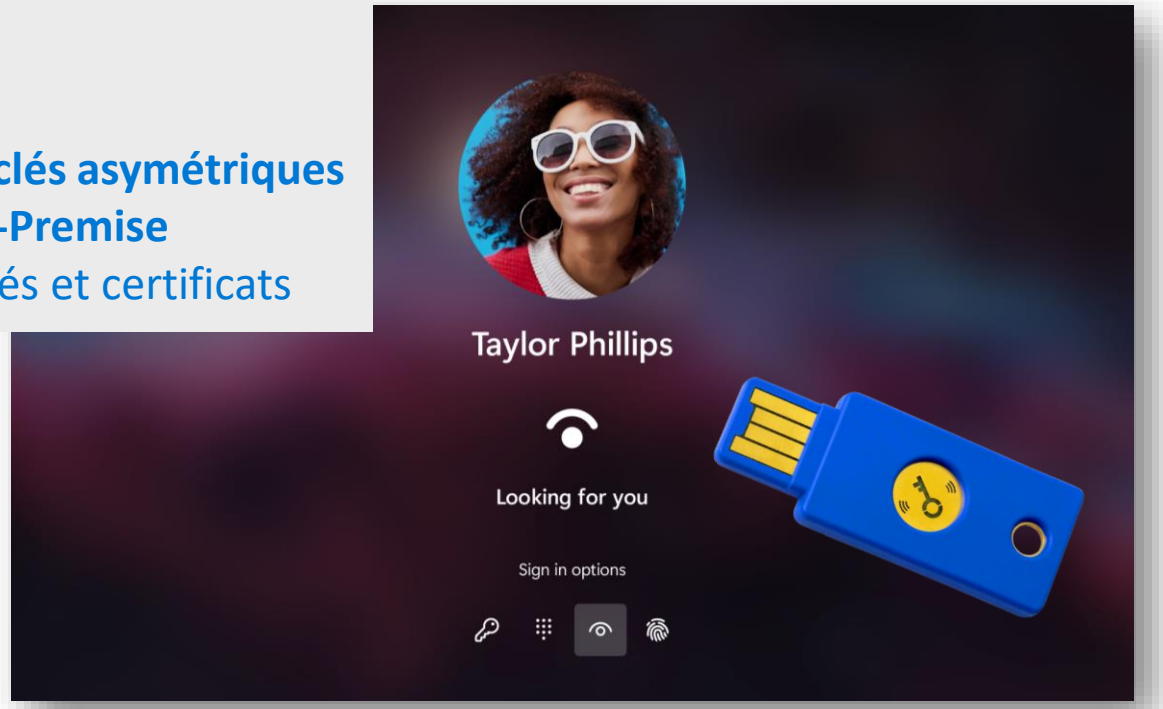
- Push notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

MFA empêche plus de 99.9% des attaques sur les identités

Windows Hello for Business : 1 composant de sécurité essentiel !

Fonctionnalités d'entreprise

- **Authentification forte à 2 facteurs**
- Modèle d'authentification via **paire de clés asymétriques**
- Environnements **cloud**, **hybrides** ou **On-Premise**
- Nombreuses options : paramètres de clés et certificats



Fonctionnalités de base

- Super expérience utilisateur
- Biométrie et/ou code PIN
  - Logon ''Plug'n Play'' de plusieurs caméras externes (ports et dock stations)
  - Nouveau protocole ESS (Enhanced Sign-in Security) supporté via VBS + TPM 2.0 pour la connexion sécurisées des caméras et lecteurs d'empreintes (protection du ring -1)
- **Est-ce sécurisé ?**
  - La biométrie ne quitte jamais le périphérique
  - La clé privée n'est jamais partagée
  - Les secrets, la clé privée sont générés et stockés dans la puce TPM

News pour Q1 2022 | Update pour Windows 10 et 11

Pour les déploiements hybrides, **les exigences PKI** et la **nécessité de synchroniser les clés AAD vers AD seront bientôt supprimées !**

Zero Trust : From Silicon to Cloud

Protection via une racine matérielle de confiance

Défense contre les attaques contre le firmware

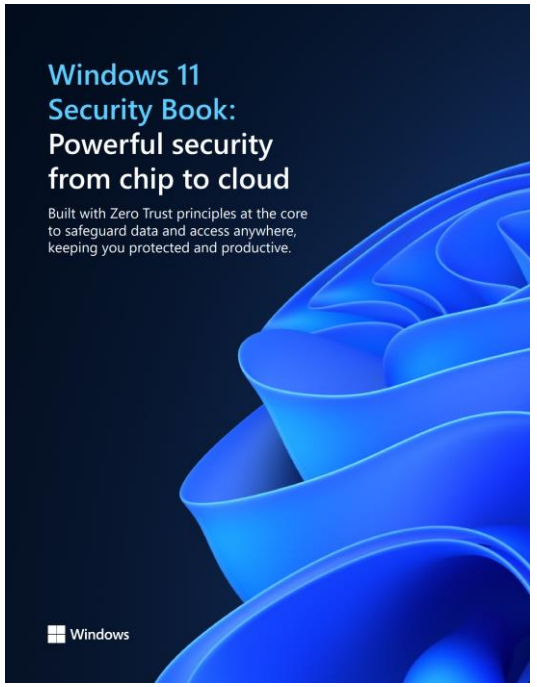
Bloque les accès à tout code non-approuvé

Protège les identités des menaces externes

Pour les VIP et IT Admins (PAW Workstations), utilisez Windows 10/11 Entreprise

- Activez VBS (Virtualization Based Security) / activé par défaut sous W11 (clean install)
- Fonctionnalités inclues dans VBS : HVCI, Credential Guard, System Guard, Secure BIO, Virtual TPM, Secure Lunch

Même avec des logiciels malveillants exécutés dans le noyau Windows, les secrets et le code exécutés dans VBS ne peuvent pas être divulgués ou falsifiés



Windows 11 Security book

Windows 11 Security show

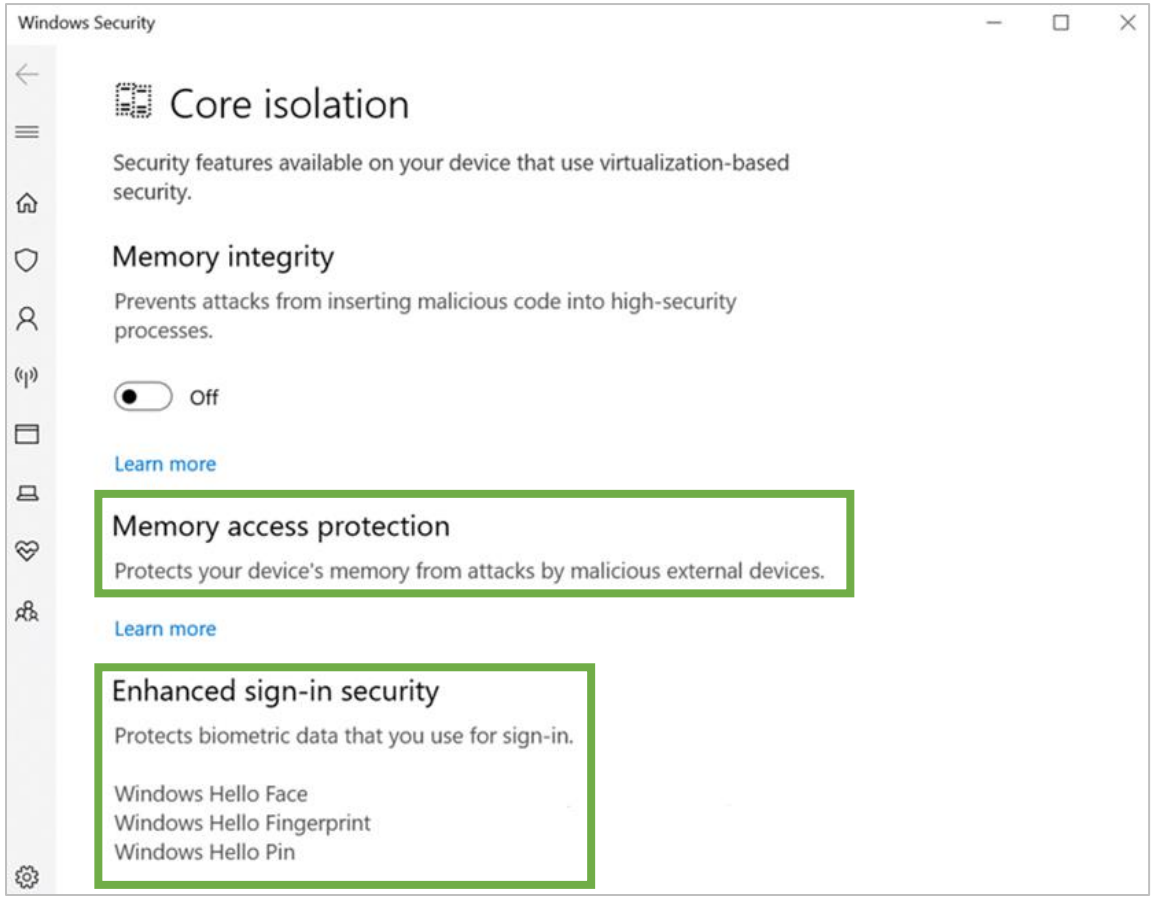
October 4, 2021

Windows 11 offers chip to cloud protection to meet the new security challenges of hybrid work

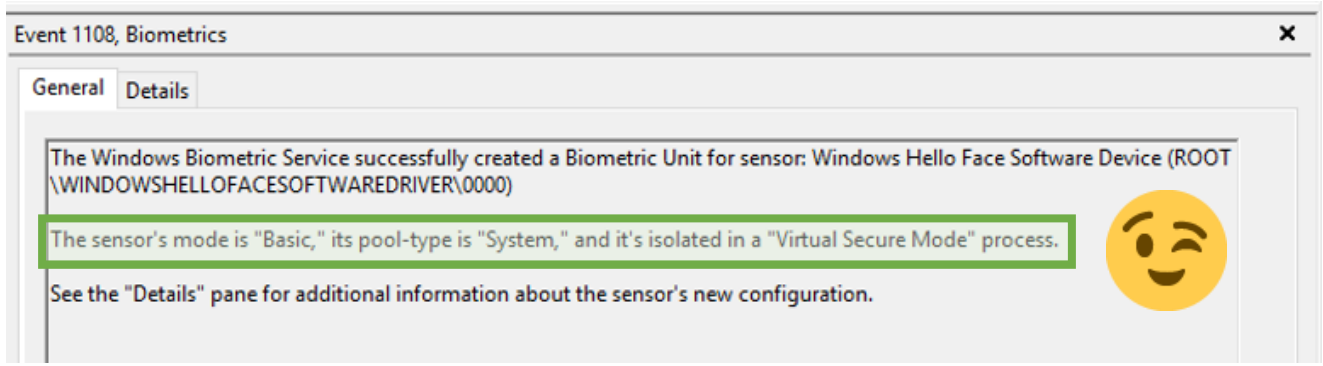
Microsoft Security Blog on Windows 11

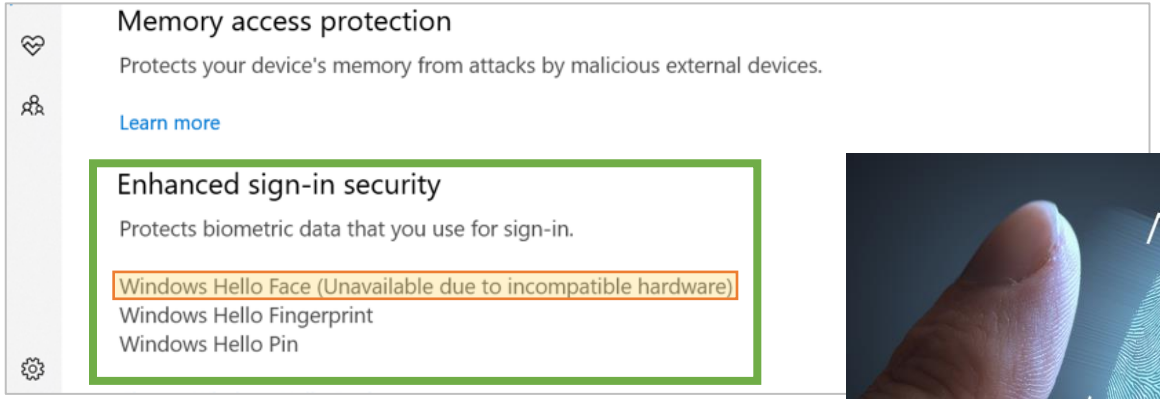
Windows Hello for Business with Enhanced Sign-in Security

Protection via code en Ring -1 + puce TPM 2.0



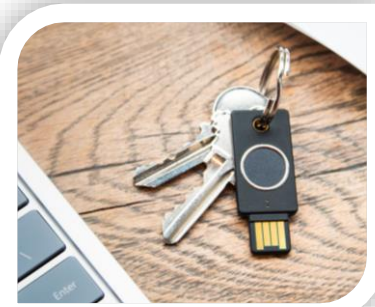
Windows 10 (octobre 2020) et > + Pilotes compatibles ESS
Activation via GPO, Intune ou SCCM





https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-enhanced-sign-in-security

YubiKey Bio : Le passwordless sans code Pin



YubiKey Bio

FIDO-only + Biométrie

WebAuthn

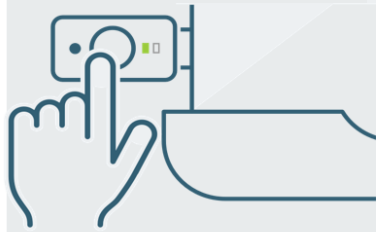
FIDO2

U2F

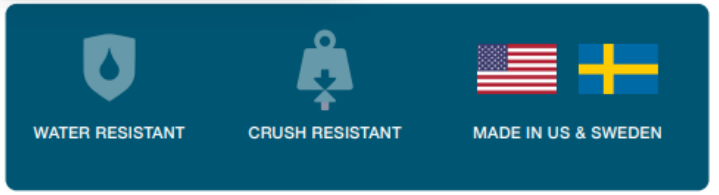
Note : Pas de NFC

1. Insérez la clé

2. La LED clignote + contrôle de l'empreinte



3. La LED s'arrête de clignoter
L'utilisateur est authentifié



- Biométrie et code PIN
- Support FIDO : FIDO U2F, WebAuthn et FIDO2
- Windows, macOS, Chrome OS, Linux, Chrome & Edge
- Formats USB-A and USB-C

Jusqu'à 5 empreintes
Code Pin après 3 échecs personnalisable de 1 à 10 tentatives

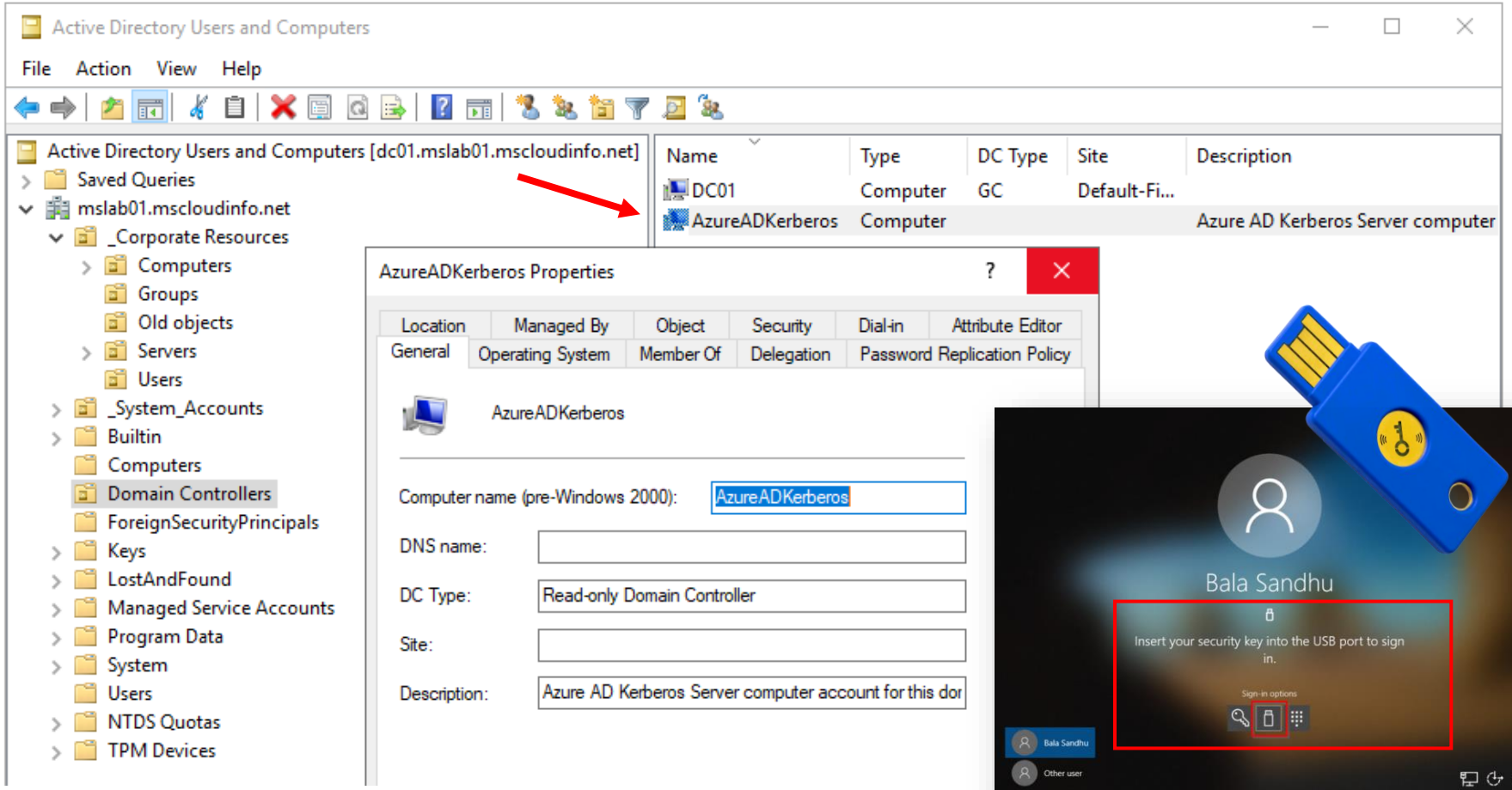
- Zero violation de comptes
- Logons 4 x plus rapides
- Super expérience utilisateur
- Fiabilité et sécurité
- Déploiement rapide
- Réduction des coûts IT
- Approuvé en UE et aux US

Sécurisez vos crédentials Active Directory sous Windows 10/11

SSO Azure AD et SSO pour Windows en mode Hybrid Azure AD Joined

Recommandé pour les VIP et IT Administrators

- Protection des Secrets sensibles
- Lorsque le téléphone ne peut pas être utilisé comme un second facteur



6

Zero Trust pour votre Entreprise “Etape par étape”

Commencez simplement avec une nouvelle approche (mindset)

Zero Trust : En priorité, sécurisez les utilisateurs hybrides !

1

Les utilisateurs doivent utiliser des **méthodes d'authentifications fortes**

2

Seuls des **périphériques conformes et approuvés** sont autorisés

3

Créez des stratégies **d'accès conditionnels** basées sur le **contexte et les risques**

4

Protégez les ressources avec la **gestion du cycle de vie des accès**

Implémentez Zero Trust en 12 étapes "à votre rythme"

"Démarrez simplement en pensant Hybride … sans jamais oublier votre environnement Active Directory!"

Configurez des accès sécurisés pour tous les types d'utilisateurs

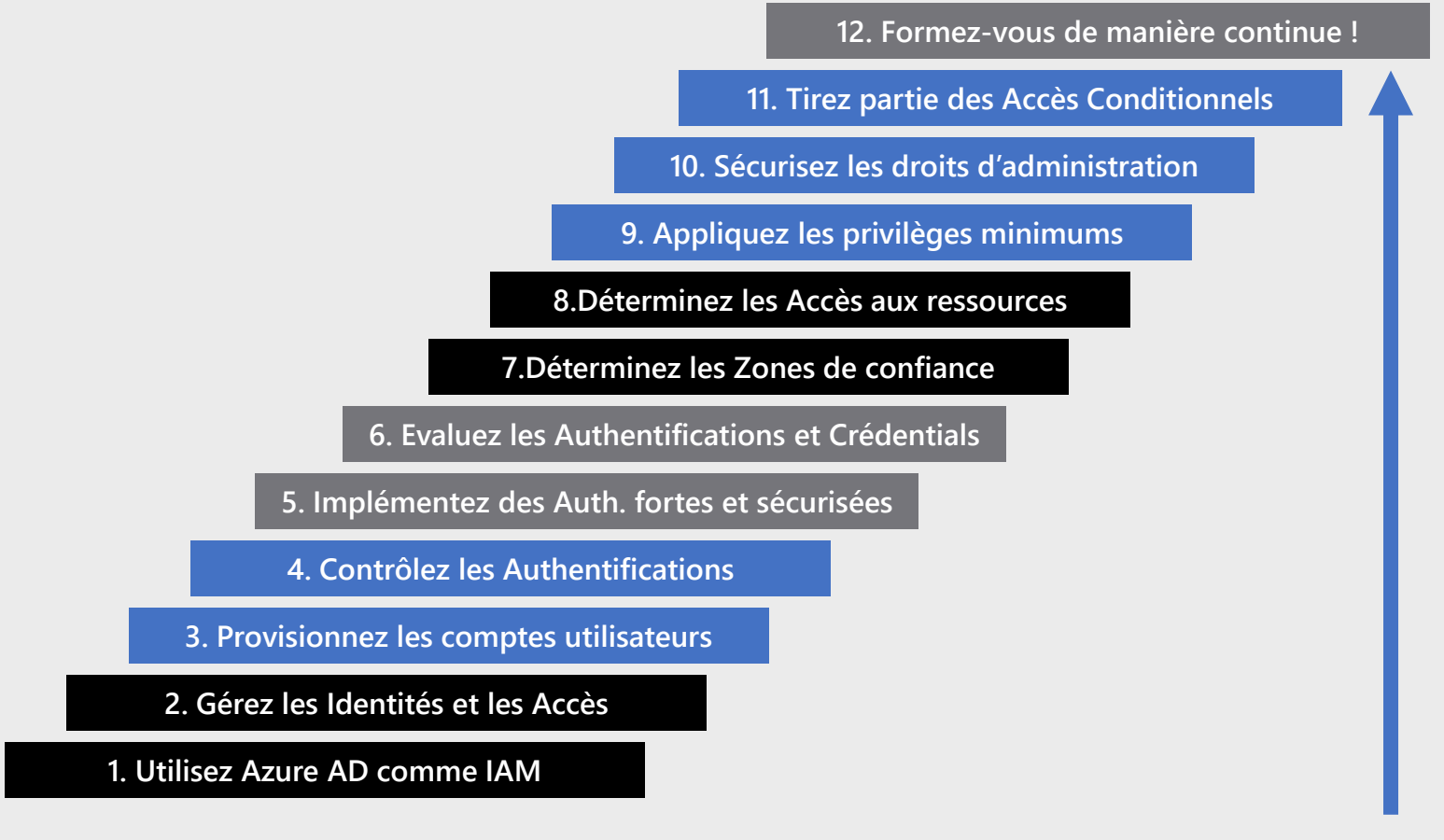
Expérience sécurisée pour tous les utilisateurs

Sécurisez l'environnement hybride

Authentifications fortes, accès conditionnels et stratégies intelligentes

Modernisez la gestion des identités et des périphériques

Consolidation puis retrait de l'infrastructure legacy



Pour finir, notre "To-do list" Zero Trust

Documentation Microsoft !
Zero Trust Document Center https://docs.microsoft.com/en-us/security/zero-trust/

Surveillez votre Secure Score Azure AD
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score

Intégrez vos applications dans Azure AD
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration

Enable PHS ou PTA
Activez le Seamless SSO et minimisez l'utilisation d'ADFS (SAML)

Azure MFA + Passwordless avec FIDO2 (Yubico)

Utilisez PIM

Utilisez Azure AD Identity Protection pour les VIP
Comptes à privilèges | comptes de secours | MFA | Passwordless

Security Update Guide: Patch and patch again!
https://msrc.microsoft.com/update-guide/

Accès conditionnels
MFA pour les invités
MFA pour tous les utilisateurs
Test | What If?
Stratégies d'accès et emplacements approuvés

Rapports - SecOps
Périphériques
Logs Azure AD (Sign-ins et applications)
Utilisateurs à risques : connexions, emplacements, IP, GPS
Cloud App Security
Azure Sentinel

Mots de passe
SSPR - Smart Lockout Azure AD / Active Directory
Protection des mots de passe

Education & Communication avec les utilisateurs
Formation interne / Bonnes pratiques Cyber

Démo & Questions

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com