Sécurisation Tenant M365

Microsoft 365 : Socle d'une nouvelle dimension de sécurité pour votre organisation

Microsoft 365

adista

Better be secured

1. Authentification multi-facteurs
   Accès conditionnel
2. Stratégie de défense Emails
   Gestion des groupes et défense O365
3. Sauvegarde de la donnée
4. Gestion du parc matériel
5. Confidentialité, conformité et intégrité du patrimoine informationnel

Un accompagnement sur mesure by adista

Better be authenticated

1

Authentification multi-facteurs
Accès conditionnel

- Méthodes d'authentification
- Environnements de confiance
- Profils d'accès aux applications et système d'information
- Stratégie de connexion accès distants
- Stratégie de connexions à risques
- Stratégie d'alertes et actions préventives

2

Stratégie de défense Emails
Gestion des groupes et défense O365

3

Sauvegarde de la donnée

4

Gestion du parc matériel

5

Confidentialité, conformité et intégrité du patrimoine informationnel

- Any Time
- Any Where
- Any Device
- Any Content
- Protéger
- Gouverner
- Réguler
- Sécuriser

adista

Authentification sécurisée

Microsoft Authenticator

L'utilisation de l'authentification multi-facteurs présente de nombreux avantages compte tenu des problématiques actuelles liées à l'évolution des modes de travail, mais aussi dans le cadre de la cybersécurité et des nouvelles réglementations en vigueur.

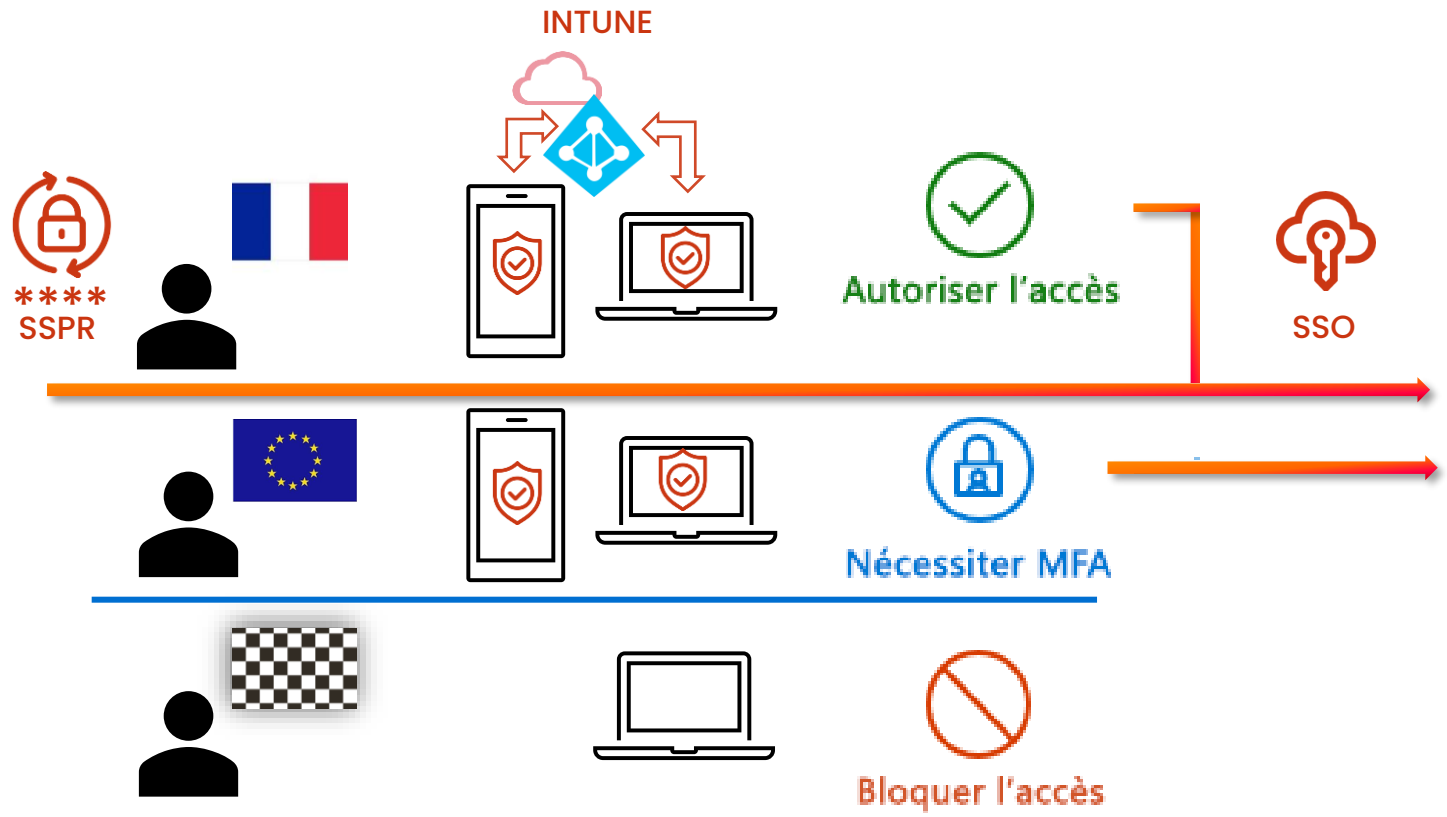
- **Prévenir les cyberattaques**
  La solution MFA permet de sécuriser instantanément les données et les ressources informatiques contre le vol d'identité, l'usurpation de compte et le phishing.

- **Promouvoir la mobilité et la productivité des employés**
  Sécuriser l'accès au système d'information et aux applications de l'organisation ou la connexion à distance au réseau via un VPN, sans dépendre d'un matériel spécifique.

- **Conforme aux exigences réglementaires**
  La réglementation en matière de sécurité des données est de plus en plus stricte, entraînant d'importants enjeux de conformité dans la gestion et la protection des données personnelles et d'organisation.

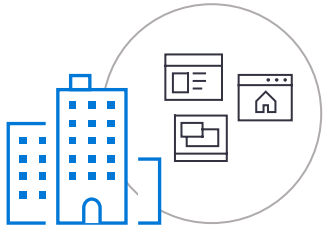
- **Expérience utilisateur optimisée**
  Simplifier l'expérience de connexion en permettant à vos utilisateurs de se connecter très rapidement et facilement, depuis n'importe quel appareil, et n'importe où avec ou sans mots de passes.

Accès conditionnels
AMÉLIORER VOTRE SÉCURITÉ



Microsoft Cloud

+ 3 000
Cloud SaaS apps



On-premises apps

Better be compliant

1

Authentification multi-facteurs
Accès conditionnel

2

Stratégie de défense Emails
Gestion des groupes et défense O365

- Stratégie de défense avancée des emails
- Gestion des rôles administrateurs
- Stratégie de partage externe
- Collaboration / Synchronisation cross tenant
- Cycle de vie des équipes Teams
- Stratégie des groupes de sécurité
- Stratégie de création des équipes Teams
- Cartographie des droits utilisateurs / groupes

3

Sauvegarde de la donnée

4

Gestion du parc matériel

5

Confidentialité, conformité et intégrité du patrimoine informationnel

- URL Cachées
- Redirections d'URL
- Logos altérés
- Usurpation de nom
- Domaine voisin
- Images distantes

adista

Protection des emails

vade

Face à des attaques de plus en plus sophistiquées, la protection de vos boîtes mail demande une nouvelle approche.

Vade utilise l'intelligence artificielle et notamment l'apprentissage automatique pour réaliser une analyse comportementale en temps réel de l'origine, du contenu et du contexte des emails.

- Intégration complète à l'environnement Microsoft 365

- Protection contre le phishing : L'analyse comportementale basé sur des algorithmes de machine learning permet d'analyser et de détecter les email frauduleux mettant en œuvre des mécanismes de contournement des solutions basé sur de l'analyse de signature

- Protection contre le spear phishing : L'intelligence artificielle, et notamment la détection d'anomalies et le natural language processing, permettent de repérer les tentatives d'usurpation d'identité et les structures malveillantes des emails frauduleux

- Lutte contre les malware et les ransomware : L'exploitation des données sur les menaces issues de la protection de plus d'un milliard de boîtes aux lettres permet de détecter et de bloquer les malwares et ransomwares les plus sophistiqués

Sécurité des emails
COMPARATIF

		EOP	ATP
Menaces identifiées			
Protection basique axée sur la signature			
Spam blacklistés	✓	✓	✓
Malware blacklistés	✓	✓	✓
Phishing blacklistés	✓	✓	✓
Menaces non identifiées			
Détection de Malware/Phishing/Spam en 0day			
IP Basique/Nom de Domaine/e-Reputation des URL	✓	✓	✓
Machine learning & heuristique / basique	✓	✓	✓
Analyse de réputation / complexe	✓	✓	✓
Détection et Protection Anti-Phishing			
Exploration de l'URL en temps réel	✓	✓	✓
Protection contre les URL malicieuses	✓	✓	✓
Demande de données sensibles	✓	✓	✓
Détection d'usurpation d'identité avérée	✓	✓	✓
Détection d'un expéditeur similaire lors de l'usurpation	✓	✓	✓
Confort Utilisateur			
Classification des emails à faible priorité	✓	!	!
Désinscription en 1 clic	✓	✗	✗
Désinscription avancée	✓	✗	✗

EOP = Exchange Online Protection

ATP = Advance Threat Protection

! = Limité au spam uniquement et non aux autres messages à faible priorité (newsletters, notifications de réseaux sociaux, etc.)

Better be saved

1. Authentification multi-facteurs
   Accès conditionnel
2. Stratégie de défense Emails
   Gestion des groupes et défense O365
3. Sauvegarde de la donnée
4. Gestion du parc matériel
5. Confidentialité, conformité et intégrité du patrimoine informationnel

- Emails
- Contacts
- Calendriers
- SharePoint
- Teams
- OneDrive

adista

Restore BACKUP service

Office 365
VEEAM

Les données de votre organisation ont de la valeur, il est important de les sauvegarder.

Microsoft 365 comprend des mécanismes de rétention.
Dans ce contexte, Adista vous propose le service Veeam Backup qui vous permet de sauvegarder les données Exchange (email, contact, calendrier), Sharepoint (où seront stockés vos dossiers et fichiers), Teams, et les OneDrive personnels des utilisateurs.

Ce service permet de sauvegarder quotidiennement vos données pendant 365 jours glissants

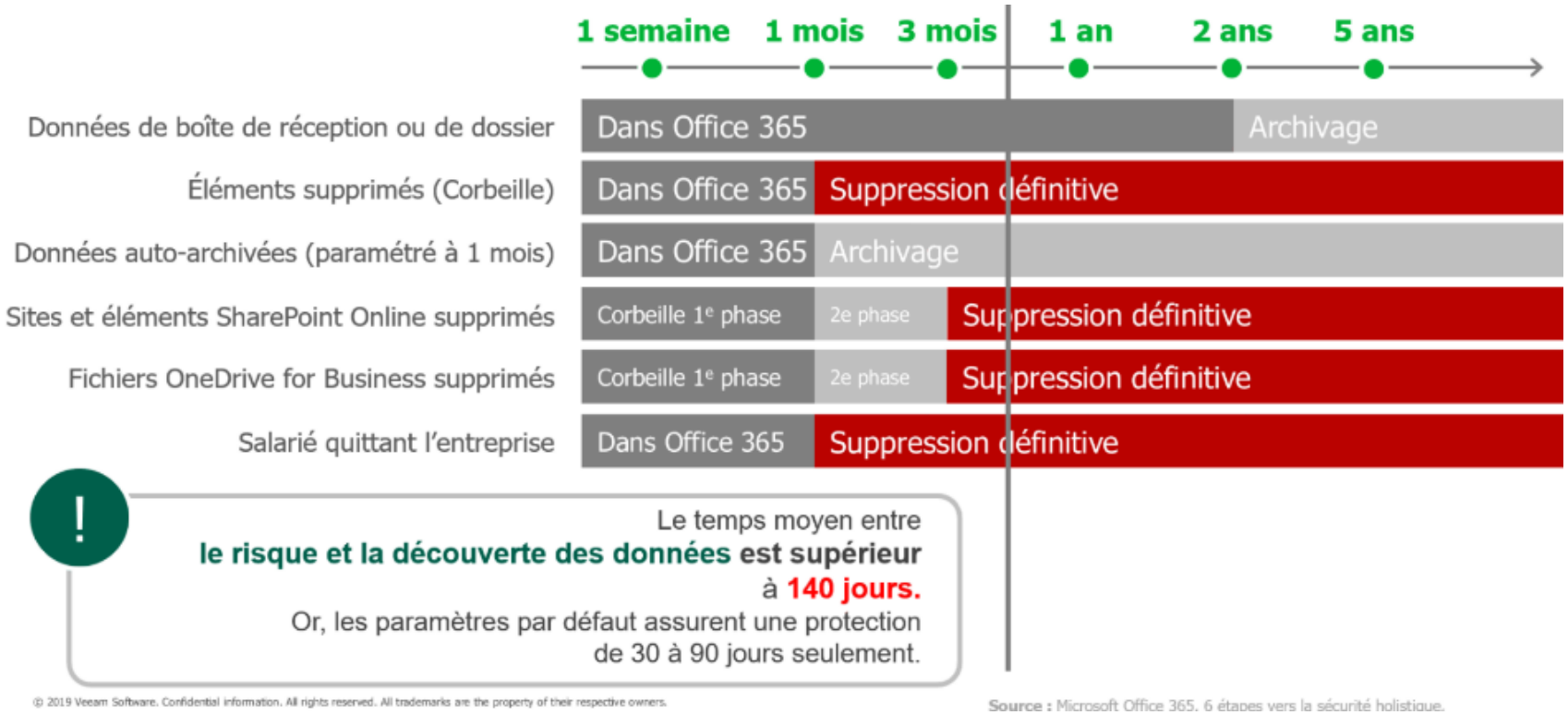
Vous conservez la propriété de vos données à tout moments.

Nous pouvons restaurer, transférer vos données emails, fichiers, … en cas de

- Crash de votre système d'informations ou de Microsoft
- Restauration d'un ensemble de données supprimées
- Transfert « *rapide* » de vos données vers un tenant temporaire suite à un piratage, ransomware, …
- Transfert de vos données vers un autre environnement fonctionnel que Microsoft

Stratégies de rétention

QU'EST-CE QUE MICROSOFT SAUVEGARDE EXACTEMENT ?



Source : Microsoft Office 365. 6 étapes vers la sécurité holistique.

Better be managed

1

Authentification multi-facteurs
Accès conditionnel

2

Stratégie de défense Emails
Gestion des groupes et défense O365

3

Sauvegarde de la donnée

4

Gestion du parc matériel

- Conformité de l'appareil
- Encryptions des données
- Sécurisation par profil utilisateurs
- Déploiement d'applications
- Inventaire et gestion à distance
- Déploiement Autopilote

5

Confidentialité, conformité et intégrité du patrimoine informationnel

- Sécurisation du parc matériel
- Gestion des profils utilisateurs
- Conformité d'accès utilisateurs
- Auto-déploiement des postes
- Déploiement d'applications
- Inventaire facilité
- Stratégie zéro trust

adista

Gestion du matériel

Microsoft Intune

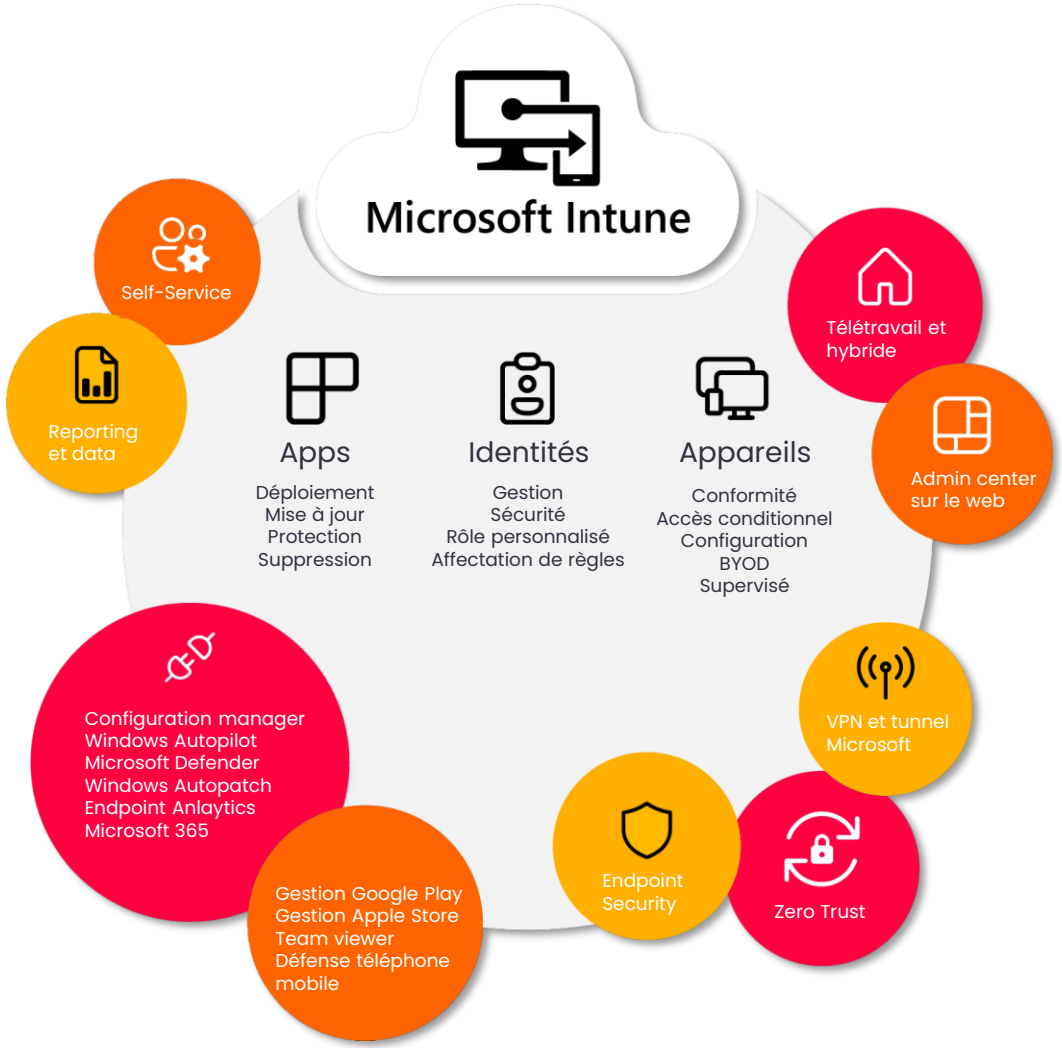
Intune est un service cloud interopérable pour fournir une gestion complète des appareils mobiles.

Intune vous permet de disposer d'un travail mobile productif en éliminant les failles de sécurité dans et en dehors de votre organisation.

- Définissez des règles et configurez des politiques pour une gamme d'appareils, qu'ils soient personnels ou supervisé par l'organisation en mode de fonctionnement BYOD (Bring Your Own Device)
- Contrôlez les accès des utilisateurs et des appareils. Protégez les données de votre organisation en contrôlant les informations auxquelles les utilisateurs peuvent accéder et celles qu'ils peuvent partager.
- Assurez-vous que les appareils utilisés par les membres de votre organisation sont conformes à vos exigences de sécurité. Si les appareils ne sont pas conformes, vous pourrez appliquer des alertes, des messages ou des actions automatisées pour minimiser les risques.

Microsoft Intune

A QUOI ÇA SERT EXACTEMENT ?



Better be confidential

1

Authentification multi-facteurs
Accès conditionnel

2

Stratégie de défense Emails
Gestion des groupes et défense O365

3

Sauvegarde de la donnée

4

Gestion du parc matériel

5

Confidentialité, conformité et intégrité du patrimoine informationnel

- Stratégie de rétention légale
- Stratégie d'alerte activité suspecte
- Stratégie d'audit d'activité sur le tenant
- Stratégie contre la perte de données
- Stratégie de sensibilité de la donnée

- Sécurisation des partages
- Niveau d'accès utilisateur invité
- Niveau de confidentialité
- Cycle de vie documentaire
- Alertes/actions en temps réel
- Prévention pertes de données
- Chiffrement

adista

Gouvernance de la donnée

Microsoft Azure
Information Protection

La multiplication des canaux d'informations et des sources de données impliquent une supervision complexe.

- Analyser vos données

  Identifiez les informations importantes dans le Cloud et votre environnement local.

- Protéger vos données

  Protégez vos données sur l'ensemble de leur cycle de vie en appliquant des étiquettes de sensibilité liées à des actions de protection comme le chiffrement, les restrictions d'accès, les marquages visuels et plus encore.

- Prévenir les pertes de données

  Appliquez un ensemble cohérent de stratégies de protection contre la perte de données dans le Cloud, dans vos environnements locaux et sur vos points de terminaison afin de surveiller, prévenir et traiter les activités à risque impliquant des données sensibles.

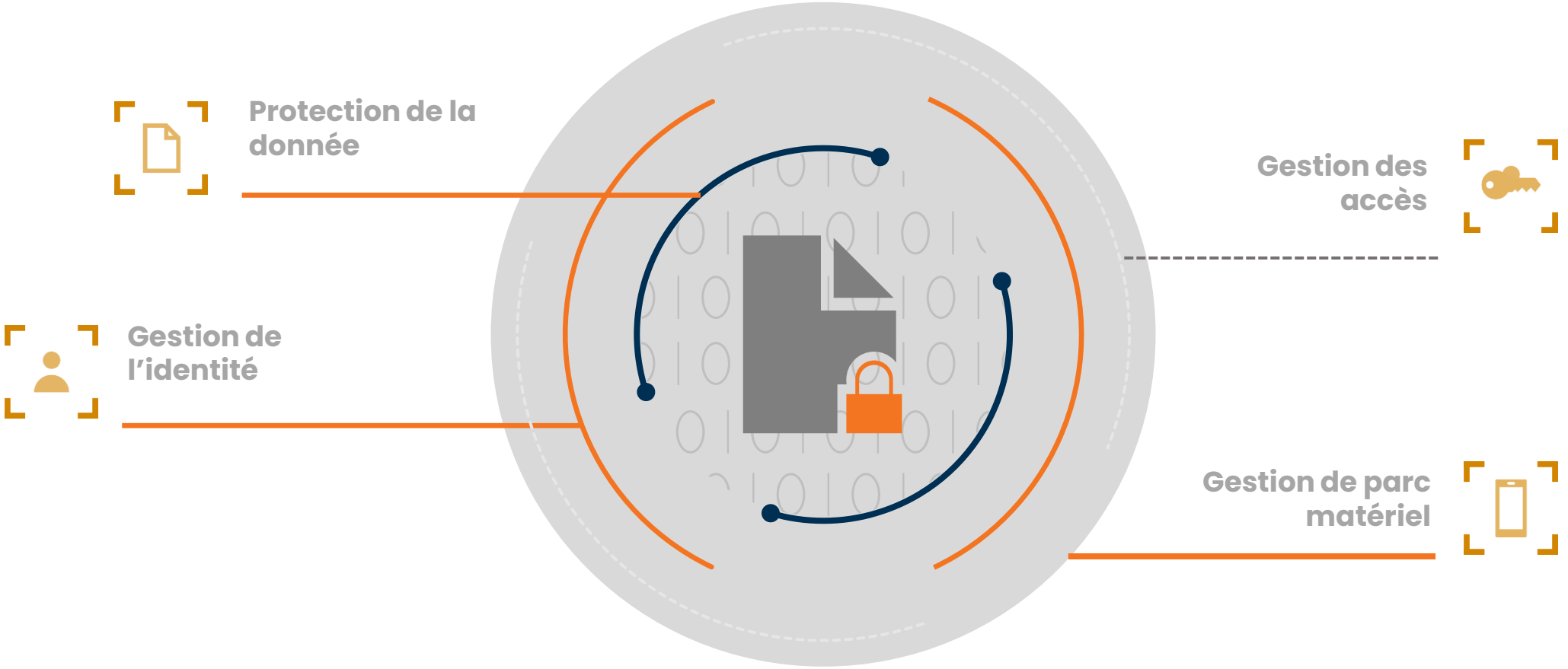
- Gouverner vos données

  Gérez le cycle de vie des informations et les enregistrements de manière intelligente grâce à la gestion sur place, les stratégies automatisées, la destruction défendable et les connecteurs de données prédéfinis.

Gouvernance de la donnée

UNE STRATÉGIE DE CONFIDENTIALITÉ ET DE PRÉVENTION

Zéro trust
UNE STRATÉGIE DE DÉFENSE EN PROFONDEUR



Merci