2023, mots de passe un mal encore nécessaire ?

LES JOURNÉES DE LA CYBER

2 & 3 MARS 2023
Campus Région du Numérique

LES JOURNÉES DE LA CYBER

Table ronde co-animée par

Hicham BEN HASSINE
Directeur

algosecure
Keep It Safe and Secure

Fabrice DIDIER
RSSI

dimo SOFTWARE

Victor SORGUES
RSSI

SynAApS

Pascal HENRY
RSSI

ESKER

1. Préambule
2. Politique de mots de passe
3. Coffre-fort de mots de passe
4. Comptes à privilèges
5. Fédération d'identité
6. Authentification multi-facteurs

Agenda

LES JOURNÉES DE LA CYBER

2 & 3 MARS 2023
Campus Région du Numérique

Préambule

A quoi sert un mot de passe ?

- C'est une méthode d'**authentification**

  Si **je suis le seul** à connaitre un secret, cela prouve mon identité

- Ce n'est pas une méthode d'**autorisation**

  Un mot de passe n'est pas une gestion des droits

Préambule

Est-ce qu'un mot de passe est encore nécessaire ?

Simplicité de mise en œuvre par les applications

Compatible avec tous **les SI historiques**

Mais des alternatives ou compléments existent :

- La biométrie
- Les mots de passe éphémères - One Time Password (OTP)
- Les certificats
- Les supports physiques

Politique de mots de passe

LES JOURNÉES DE LA CYBER

Politique de mots de passe – limites

Le mot de passe a ses **limites** car le **risque cyber** lié à l'authentification à largement évolué :

- **Fuites** d'identifiants et de mots de passe à répétition (**Password Leak**)
  Prévention : utiliser des dictionnaires et services pour bloquer les mots de passe interdits et compromis
- Tentatives d'authentification par **force brute** par des robots (**Password Spraying**)
  Prévention : contrôler le contenu (ou l'entropie) du mot de passe
- Multiplication et **réutilisation** des identifiants/mots de passe pour un utilisateur du SI
  Prévention : utiliser un **coffre-fort** de mots de passe ou limiter leur nombre en créant une **fédération d'identité**

Point d'attention : la réponse « **Sécurité** » doit s'adapter aux nouvelles pratiques des attaquants

Politique de mots de passe – état de l'art

Recommandations (**NIST 800-63B** – Révision 3 de Juin 2017 / *Révision 4 en cours*) :

- **Réduire la complexité** demandée à l'utilisateur basée sur les catégorie de caractères
- **Evaluer la qualité intrinsèque** du mot de passe
  - Bloquer les mots de passe **compromis** (fuites de donnée – publiques ou privé)
  - Bloquer les mots de passe appartenant à des **dictionnaires** (contextuels et mots interdits)
  - Bloquer l'utilisation des mots de passe **répétitifs ou incrémentaux** (**Password Cracking**)
- **Augmenter la longueur** des mots de passe
- Utiliser un mot de passe **unique** à chaque compte.
- **Arrêter d'imposer le renouvellement automatique** du mot passe (sauf si compromission)

Point d'attention : La veille. Il est indispensable de pouvoir **surveiller la compromission** ou non d'un mot de passe.

Politique de mots de passe – AD

Outils historique et le plus répandu dans un écosystème Microsoft :

- L'annuaire **Active Directory** (**AD**)
- Politique **limitée** dans sa version on-premise (mode On/Off)
- Nécessite des **outils tiers** pour permettre un suivis plus global et étendre les critères d'acceptation

Moyens de mise en œuvre :

- **FGPP** (**AD**) pour configurer des politiques fines, sur des groupes, utilisateurs particuliers
- **LAPS** (**AD**) pour les comptes locaux
- **MSAD** (**AD**) pour les comptes de services (quand c'est compatible….)
- Outils de comparaisons de hash pour détecter les compromissions

Politique de mots de passe – autres

RETEX d'outils pour l'implémentation d'une politique étendue :

Outils n°1 – **Audit** de l'existant (*SpecOps Password Auditor*)

- Outil **autonome et gratuit** – S'installe sur un poste client. Requiert un compte « admin »
- **Visualisation** directe et génération d'un **rapport d'audit** de la politique et des mots de passe
- **Conformité** de votre politique par rapport à ANSSI, CNIL, NIST, NCSC, PCI v4, BSI et Hitrust

Outils n°2 – **Amélioration** de l'existant (*SpecOps Password Policy*)

- Outil **payant** qui s'intègre dans le SI, en **complément** de Microsoft **AD**
- Définition d'une politique de **gestion avancée** des mots de passe (conforme à NIST)

  RSSI : Nouveaux critères de contenu, d'expiration et de compromission (dictionnaires, …)

  Utilisateur : Accompagnement du changement (expérience utilisateur). Vue claire des critères non respectés lors du changement de mot de passe, via une page Web ou directement dans l'interface du système Windows grâce à un agent déployé

Politique de mots de passe – bilan

Un mot de passe doit rester **secret**

Mais

- Le **SI** de l'entreprise s'étends avec d'avantage d'applications
- L'utilisateur n'a pas la **capacité** à mémoriser tous ses mots de passe

Que peut-on faire pour **aider** l'utilisateur ?

- **Coffre-fort** de mots de passe
- **Fédération d'identité**

Coffre-fort de mots de passe

LES JOURNÉES DE LA CYBER

Coffre-fort de mots de passe

Choix en fonction de **l'usage**

- **Nombre** d'utilisateurs, de sites
- **Environnement** (Windows, MacOS , Linux, iOS, Android)
- **Collaboratif** (notion de secrets partagés), haute disponibilité
- Type d'application de consultation (site web, Desktop, Mobile)
- Extension pour navigateur web (auto remplissage)
- Mode de déploiement (poste de travail, serveur on-premise, Saas)

Intégration dans la sécurité du **SI**

- Authentification en SSO, double facteur
- Traçabilité, conformité
- API (intégration avec des outils de gestion d'accès aux serveurs)

Point d'attention : proscrire le gestionnaire de mots de passe intégré aux navigateurs web

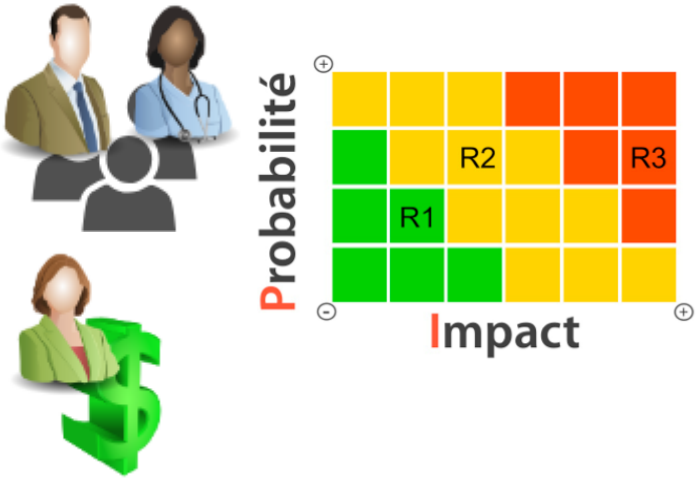
Comptes à privilèges

LES JOURNÉES DE LA CYBER

Comptes à privilèges - risques

Comptes **Techniques :**

- Comptes **Administrateur**
  - Infrastructure : Serveurs , annuaires, SGBD, Middleware
  - Cloud (SaaS / IaaS / PaaS)
  - Applicatif
- Comptes de **services**
- Comptes **applicatifs**



Comptes **Fonctionnels :**

- RH, Comptabilité / Achats, Communication

L'analyse du **contexte** doit définir les comptes dit à « privilèges »

Comptes à privilèges - risques

Risques

- Atteinte à la **disponibilité** (totale ou partielle) du SI
  - Disponibilité des composants
  - Perte / Corruption d'informations
- Atteinte à **l'intégrité** (totale ou partielle) du SI
  - Vols / falsification d'informations
  - Perte / falsification de traçabilité, d'imputabilité

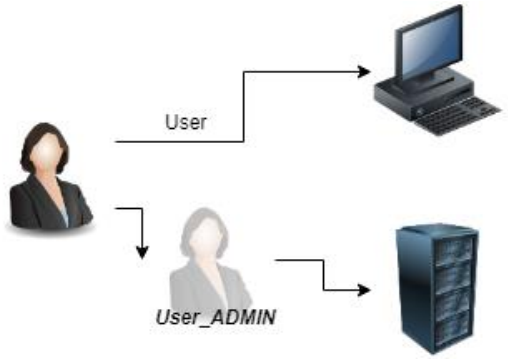
… en fait, à peu près tous les risques imaginables sur (depuis) un **SI** si un compte à privilège est corrompu

Moyens d'attaque

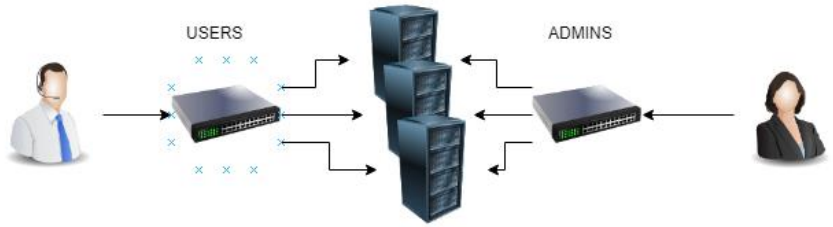
- Abus de privilèges : attaque « interne »
- Vol de compte : Secrets faibles, Postit, Spear phishing…
- Vol de « session » : Verrouillage de session, Cookies, …
- Élévation de privilèges

Comptes à privilèges – réduction du risque

Mise en place de moyens de gestion « **classiques** »



- **Gestion** (et suivi) des comptes et des privilèges
  - Difficultés de maitriser tous les comptes à privilèges
- **Verrouillage** / expiration de sessions
  - Dissociation des comptes avec et sans privilèges
    - Des référentiels ?
    - Des terminaux ?
- **Rotation** des secrets
  - Attention aux politiques et au nombre de référentiels
- Authentification **forte** (2FA, MFA)
- **Restrictions** réseau : Réseau (VLAN) d'administration dédié

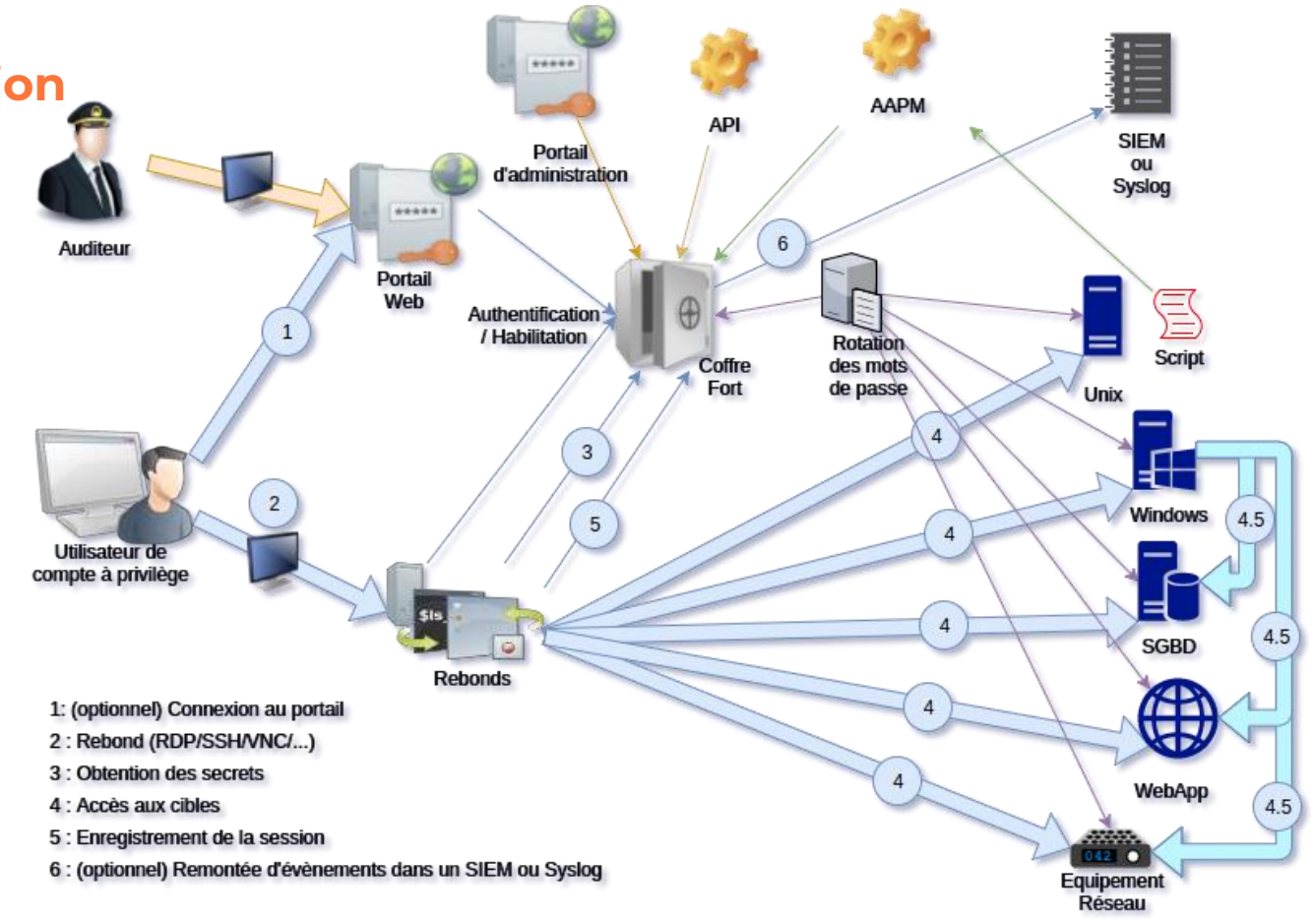


Comptes à privilèges – réduction du risque

Mise en place d'un **bastion d'administration**

- Changement de compte
- Rupture de flux
- Traçabilité
- Imputabilité
- Gestion des secrets

....



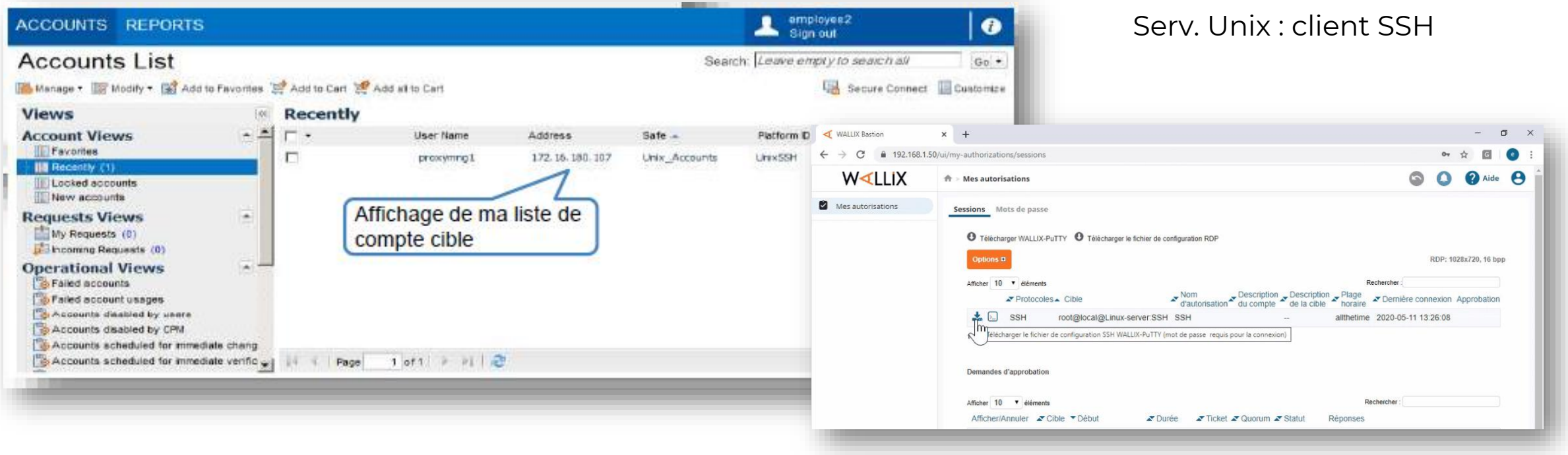
Comptes à privilèges – réduction du risque

Exemple de **bastion d'administration**

Connexion directe

Serv. Windows : client RDP

Serv. Unix : client SSH



Comptes à privilèges – bastion

WALLIX TRACE, AUDIT & TRUST

Centrify

PROVEIT

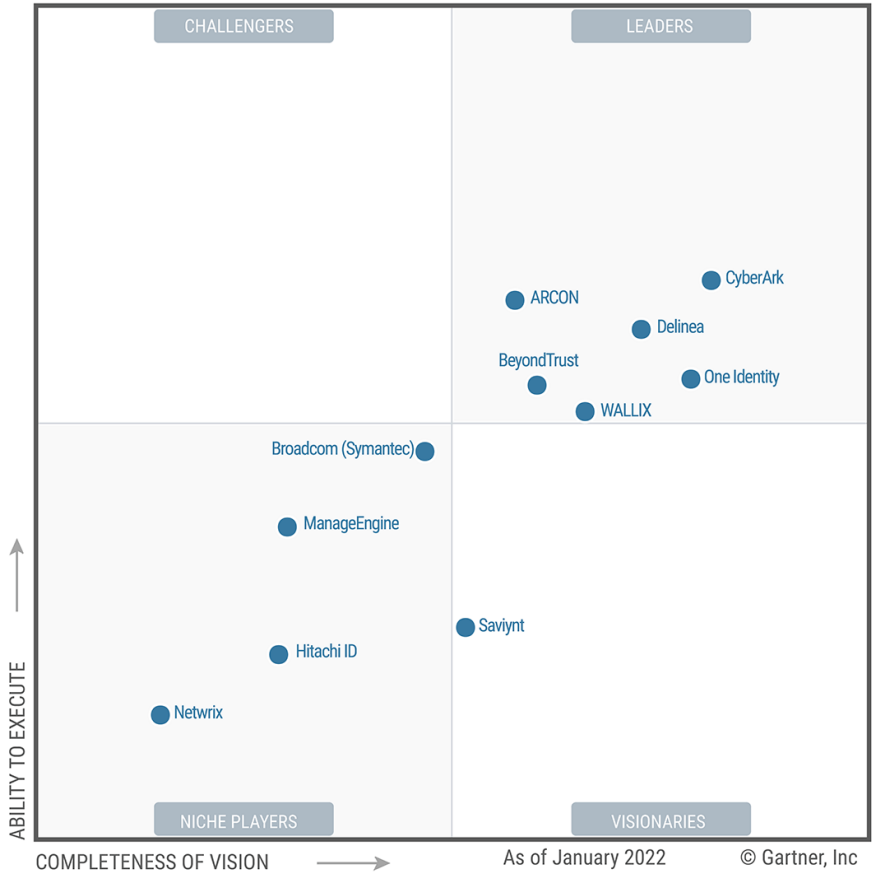
CYBERARK

BeyondTrust

ONE IDENTITY

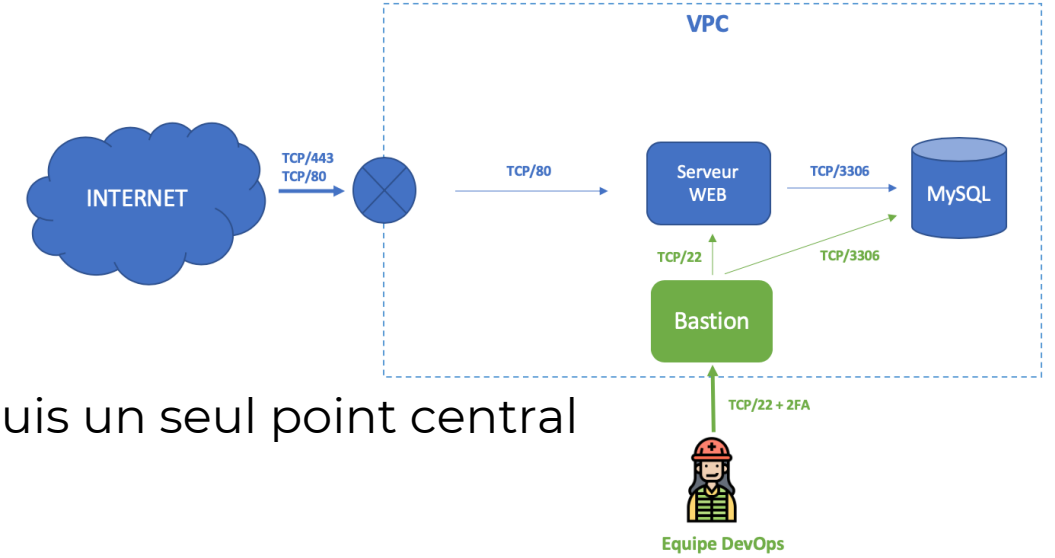
thycotic

Figure 1 : Magic Quadrant pour la gestion des accès privilégiés



Comptes à privilèges – bastion dans un SI

Apports du **bastion** d'administration



Gestion centralisée des accès à privilèges :

- Qui a accès à quoi , quand, par quels protocoles
- Au départ de l'entreprise, les accès sont retirés depuis un seul point central

Traçabilité des comptes à privilèges :

- Répondre à la question « qui fait quoi »
- Pouvoir investiguer suite à des incidents de production ou de sécurité

Gestion des mots de passe : séquestre et rotation selon des politiques

Donner des **accès temporaires** à des fournisseurs externes

Pour certaines populations, définir des **plages horaires** autorisées

Comptes à privilèges – bastion dans un SI

Risques projet

Sponsor : ce n'est pas uniquement un projet technique, mais aussi et surtout un projet ORGANISATIONNEL et transverse

Conduite du changement :

- Identification (acteurs, cibles, contraintes, impact/dépendances des autres briques….)
- Adhésion à la solution

Le bastion ne doit pas être un **SPOF** dans le **SI :**

- Redondance des rebonds
- Solution en HA - DR

Économique : Le coût produit n'est pas forcément le plus important (coûts d'infrastructure, intégration, exploitation, gestion du changement / impact …)

Fédération d’identité

LES JOURNÉES DE LA CYBER

Fédération d'identité

Une réponse unique à un double enjeu business et technique

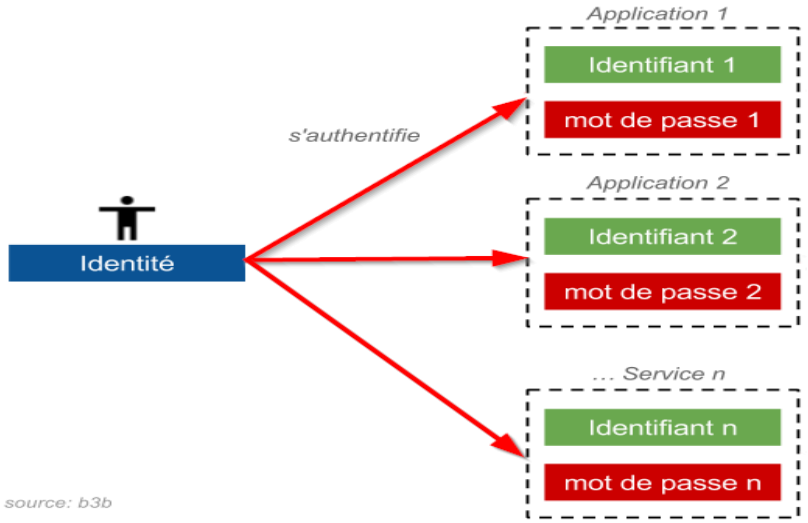
La fédération d'identité est un moyen **simple** pour des organisations de **partager** des informations à propos d'un utilisateur, le but étant qu'il puisse **naviguer entre différents services** après s'être authentifié **une seule et unique fois** auprès d'un **tiers de confiance** garant de son identité.

Fédération d'identité – sans fédération

Une personne physique possède en théorie pour chaque écosystème (entreprise, maison, …) **une identité informatique unique**

Il s'agit habituellement d'un code, une clé, qui lui permet d'être **identifié** de manière unique

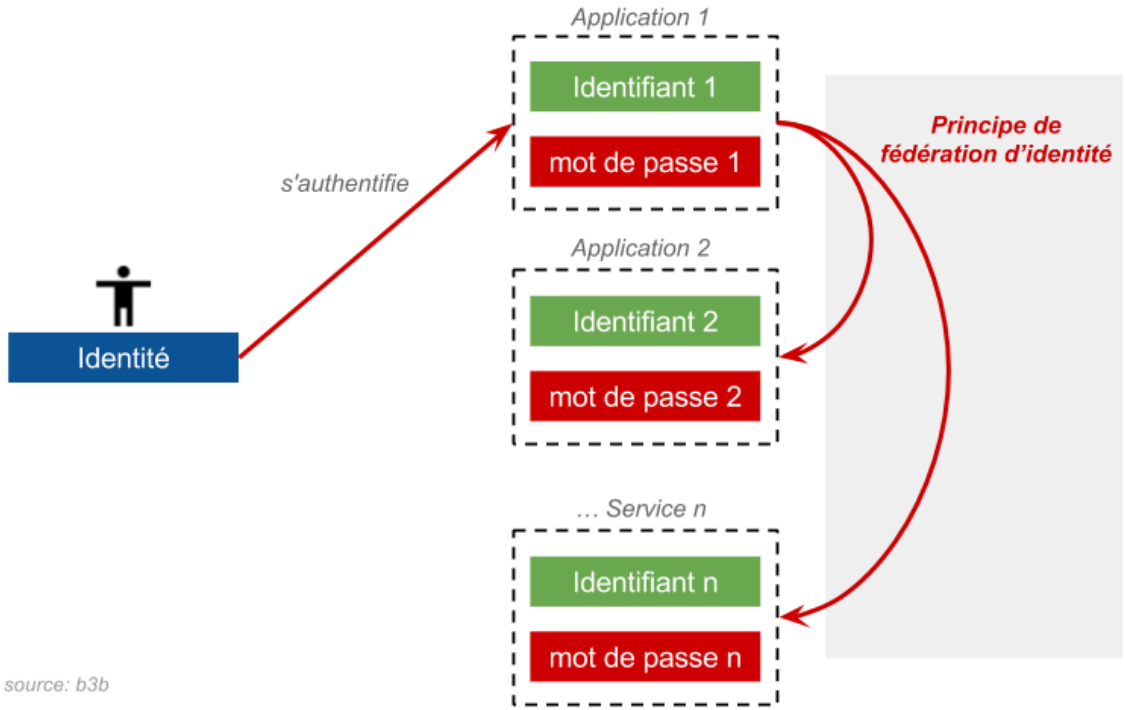
Le plus souvent cette identité s'exprime sous la forme d'un couple **Identifiant / Mot de passe**



Fédération d'identité – avec fédération

Le but de la fédération d'identité est donc de pallier cette problématique que nous rencontrons qui est la **multiplication des authentifications** nécessaires pour accéder aux applications.

Elle propose un point **d'authentification unique** à chaque utilisateur.



Fédération d'identité – composants

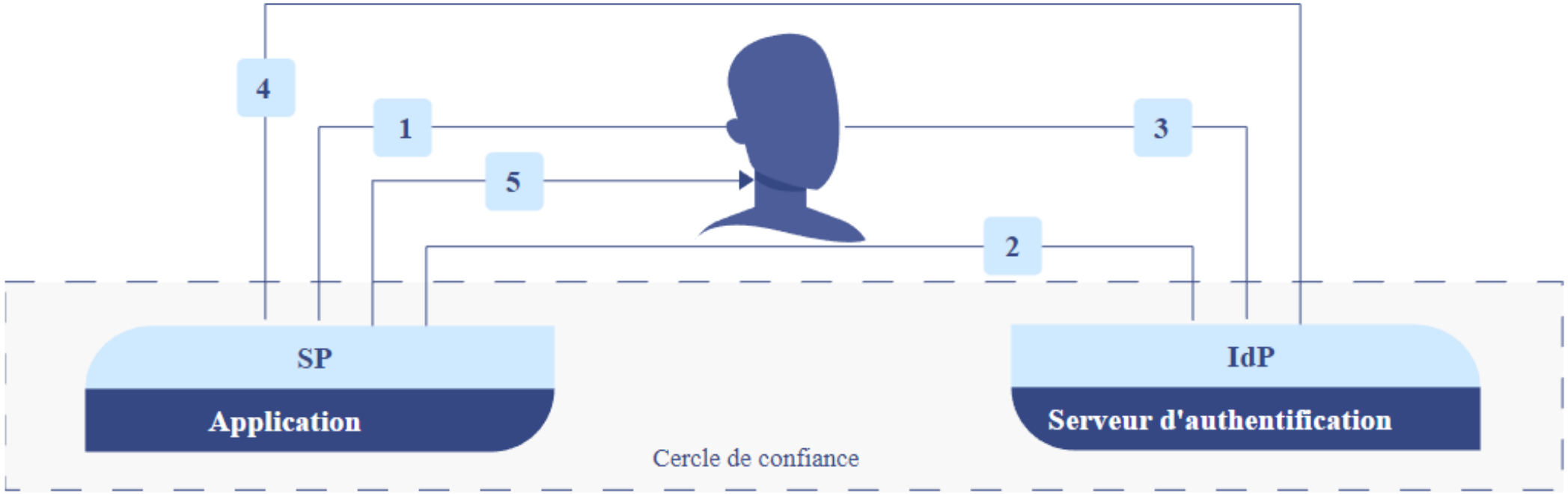
Pour mettre en place une **fédération d'identité**, il est nécessaire de reconnaître **trois acteurs** et d'identifier les différents flux entre eux :

- **L'utilisateur** : il s'agît de la personne qui interagit via son navigateur web. Il a une unique identité numérique associée à plusieurs attributs et souhaite accéder à une application protégée.

- **Le fournisseur d'identité** (**IDP**) : il est l'élément central de l'architecture. Il est chargé d'authentifier les utilisateurs. Il vérifie les facteurs d'authentification de l'utilisateur et fournit la preuve de son identité. Il est aussi en charge des autorisations d'accès aux attributs.

- **Le fournisseur de service** (**SP**) : il s'assure de l'identité de l'utilisateur et peut avoir besoin des attributs de l'utilisateur.

Fédération d'identité – composants



1 Requête utilisateur

2 Redirection de l'utilisateur vers l'IdP

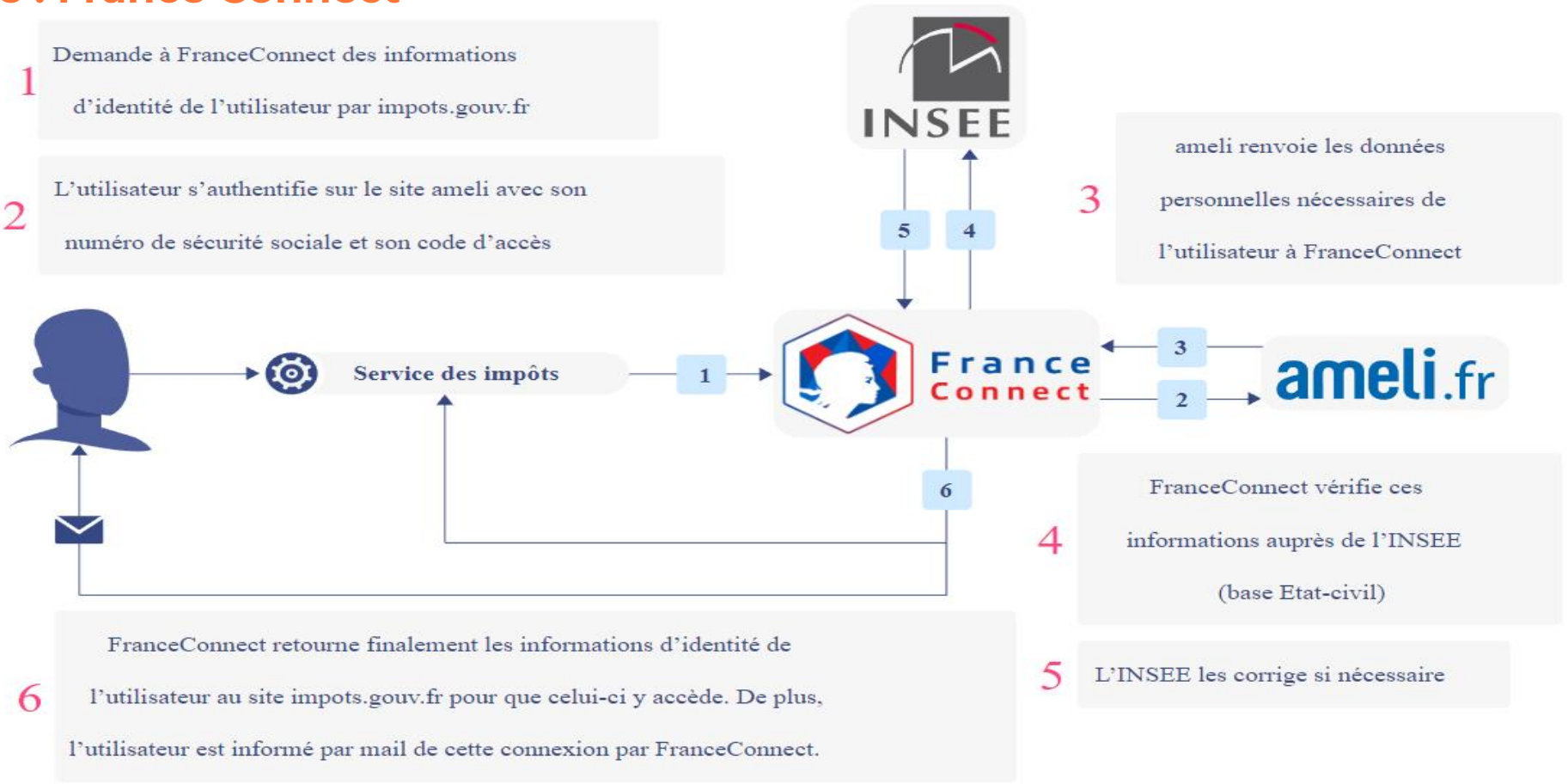
3 Authentification

4 Réponse de l'IdP avec un jeton

5 Accès à l'application

Fédération d'identité

Exemple : France Connect



Fédération d'identité – protocoles

La fédération d'identité peut utiliser **différents protocoles** :

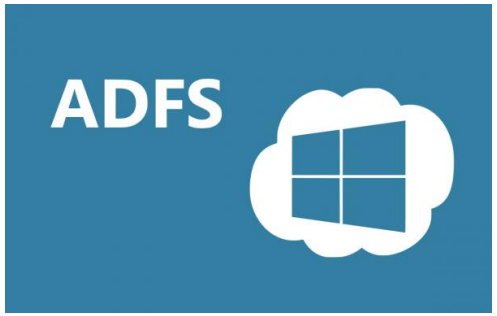
- **SAML**
- **WS-Fédération**
- **OpenID Connect (OAuth 2.0 *)**

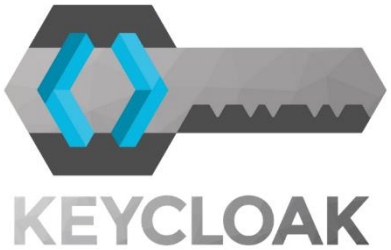
** Le protocole OAuth 2.0 est de plus en plus utilisé car il est très simple à mettre en place, géré par la majorité des IDP et adapté aux contraintes des smartphones.*

Fédération d'identité – bilan

Avantages	Inconvénients
• Des technologie **fiables**, normalisées et éprouvées • Une **simplicité** pour l'utilisateur final • Une **maitrise** de l'authentification pour les entreprises (respect des politiques de sécurité) • Les **avantages des SSO classiques** transposés aux applications web distantes	• Une **concentration du risque** non négligeable si la partie technique n'est pas maitrisée • Des solutions plus ou moins **onéreuses** • Un **manque de compatibilité** avec des applications **Web legacy** (interopérabilité)

Fédération d'identité – Exemples IDP





Authentification multi-facteurs

LES JOURNÉES DE LA CYBER

Authentification multi-facteurs

Que fournit l'Active Directory (**AD**) de Microsoft ?

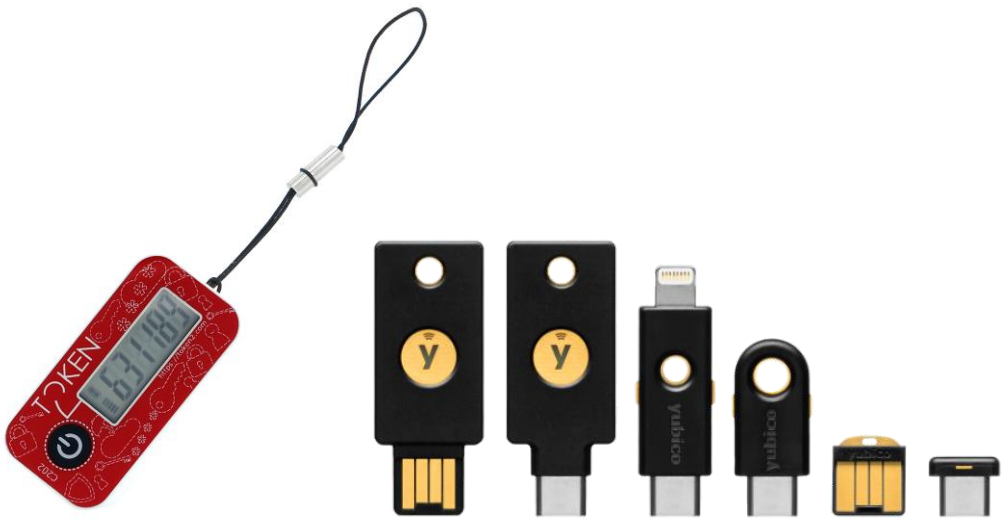
- On-premise ➔ pas de gestion native du multi-facteur dans **AD** (outils tiers nécessaires)
- Azure AD (ou Hybride) ➔ offre des possibilités (débute avec la licence AD Azure P1)

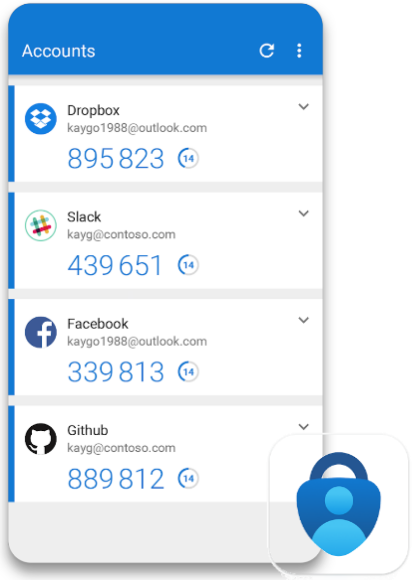
Avantages	Inconvénients
• Recommandée en tant que **bonne pratique** • **Renforce** la sécurité (gestion du risque de vol des identifiants)	• **Gestion du changement** de l'expérience utilisateur et nouvelle politique à créer • **Phase d'enregistrement** des utilisateurs • **Frustration** utilisateur d'avoir un second facteur (attention à la **« MFA Fatigue »**) • **Helpdesk** (gestion des incidents causés par le second facteur)

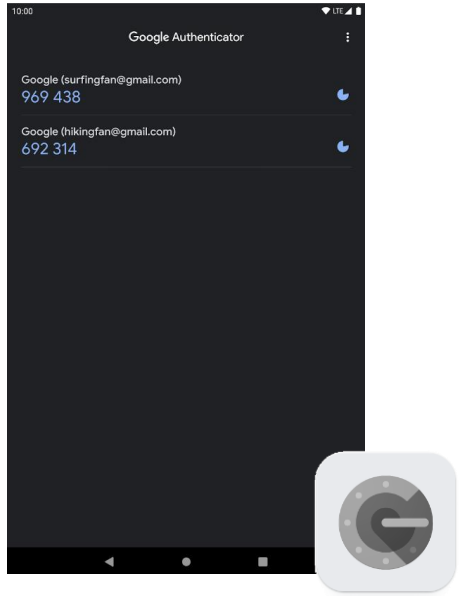
Authentification multi-facteurs

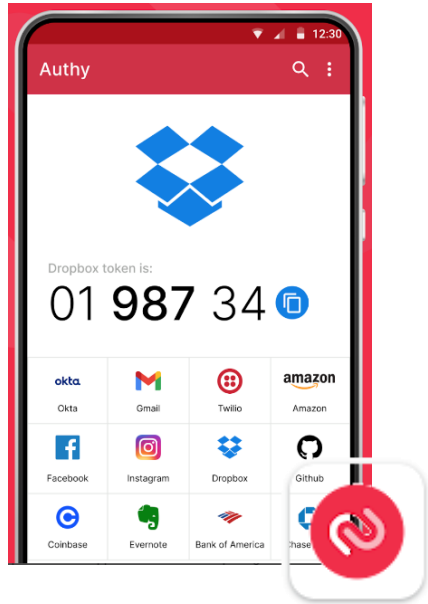
Choix du périphérique qui joue le rôle du second facteur :

- **Physique** ➔ un objet en plus qu'il garder avec soi et ne faut pas perdre
- **Virtuel** ➔ un périphérique que les utilisateurs possèdent déjà et dont ils prennent soin







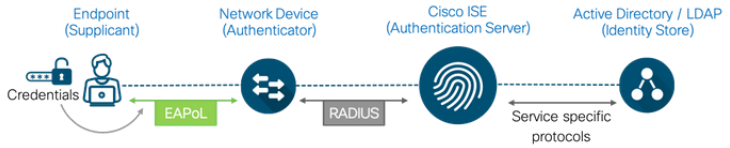


Authentification multi-facteurs

RETEX d'implémentation :

802.1X pour les prises réseaux filaires et le réseau sans-fil

Server (RADIUS) inclus dans Microsoft Windows Server



OTP pour les accès VPN (n'est **plus recommandé** à cause du canal de transmission)

Nécessite une solution tierce payante pour l'émission du « secret » via SMS ou e-mail

TOTP pour les accès VPN (**recommandé**)

Nécessite une application « légère » tierce gratuite de type Authenticator

Multiples formats pour Microsoft Azure AD

Nécessite un terminal mobile : envoi d'un SMS ou réception d'un appel vocal directement géré par Microsoft Azure, OTP, TOTP, HOTP, notification de type « push », correspondance des nombres (à compter du 27 février 2023)

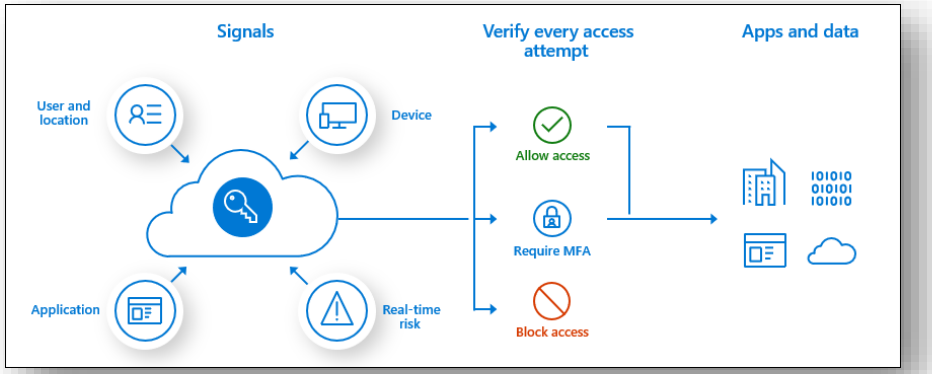
Authentification multi-facteurs

RETEX : accès conditionnel grâce à Microsoft Azure AD

La demande du second facteur est conditionnée par l'évaluation du risque (Licence AD Azure P2)

Exemple de **règles** pour le 2FA :

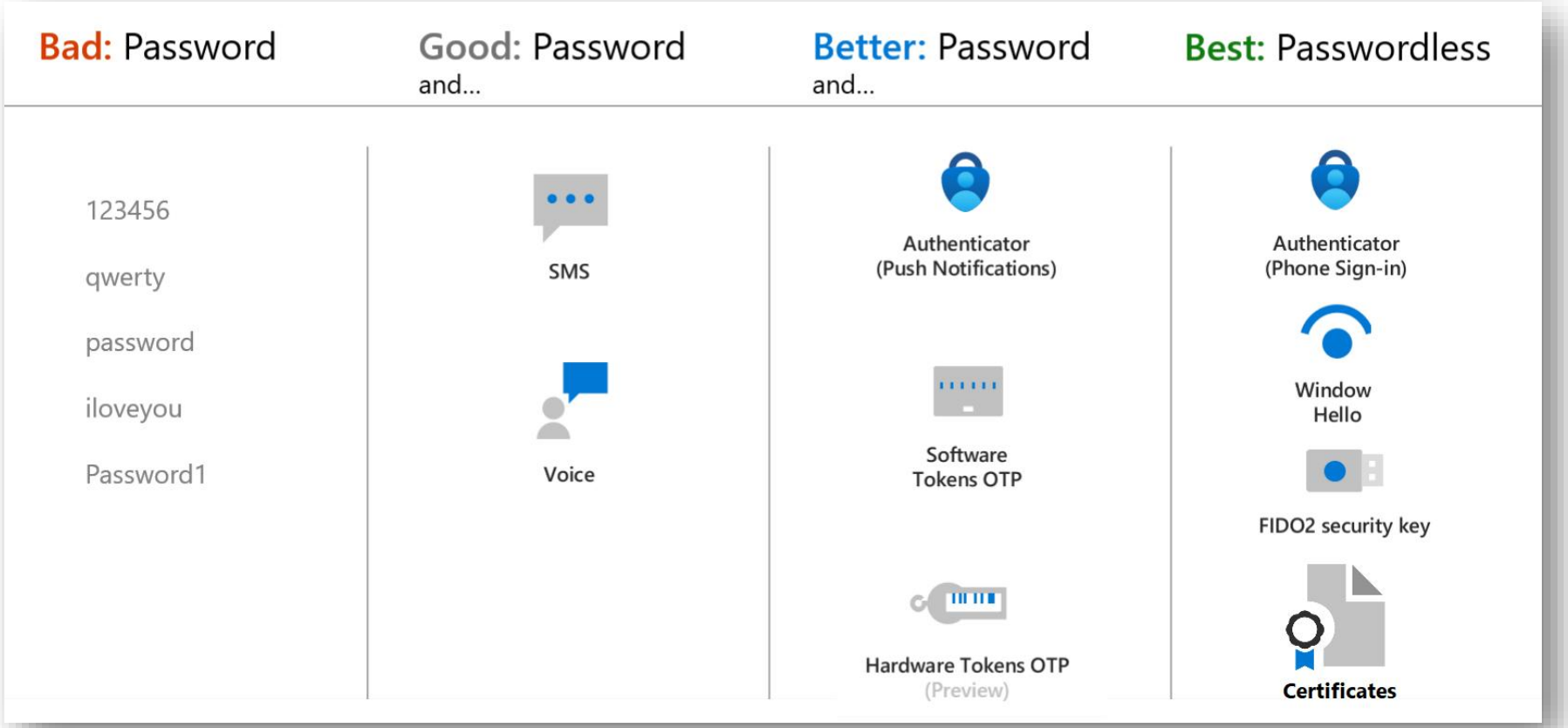
- **Délais** avant de le demander
- Uniquement pour certaines **applications**
- A chaque fois pour une certaine **population** d'utilisateur
- Uniquement depuis un **lieu/emplacement** (IP Source)
- Depuis un **périphérique géré** ou non par l'entreprise



Conclusion

LES JOURNÉES DE LA CYBER

Conclusion


Bad: Password
Good: Password
and...
Better: Password
and...
Best: Passwordless
123456
qwerty
password
iloveyou
Password1
SMS
Voice
Authenticator
(Push Notifications)
Software
Tokens OTP
Hardware Tokens OTP
(Preview)
Authenticator
(Phone Sign-in)
Window
Hello
FIDO2 security key
Certificates

Merci pour votre attention

LES JOURNÉES DE LA CYBER