



Solution de
protection des identités



Les plateformes IAM modernes (Entra ID, Okta, Ping, etc.) offrent des contrôles de sécurité comme **MFA** & **Accès conditionnel**, pour des applications cloud modernes ou des applications sur site qui peuvent être placées derrière un proxy.

Mais certains **angles morts** critiques de la sécurité des identités restent encore non couvertes.



Les **angles morts** courants de la sécurité des identités.

Systèmes et protocoles critiques qui ne prennent pas en charge le **MFA**

En particulier les ressources qui s'authentifient sur **Active Directory** (par exemple, outils en ligne de commande, systèmes legacy, infrastructures).

Difficultés à cartographier et protéger les **comptes de service**

Un inventaire incomplet et des dépendances inconnues les rendent **difficile à protéger**.

La sécurité **des accès à privilège** est incomplète et souvent contournée

La rotation des mots de passe est **complexe** dans certains cas. Les utilisateurs empruntent souvent des identifiants et contournent le **PAM**.

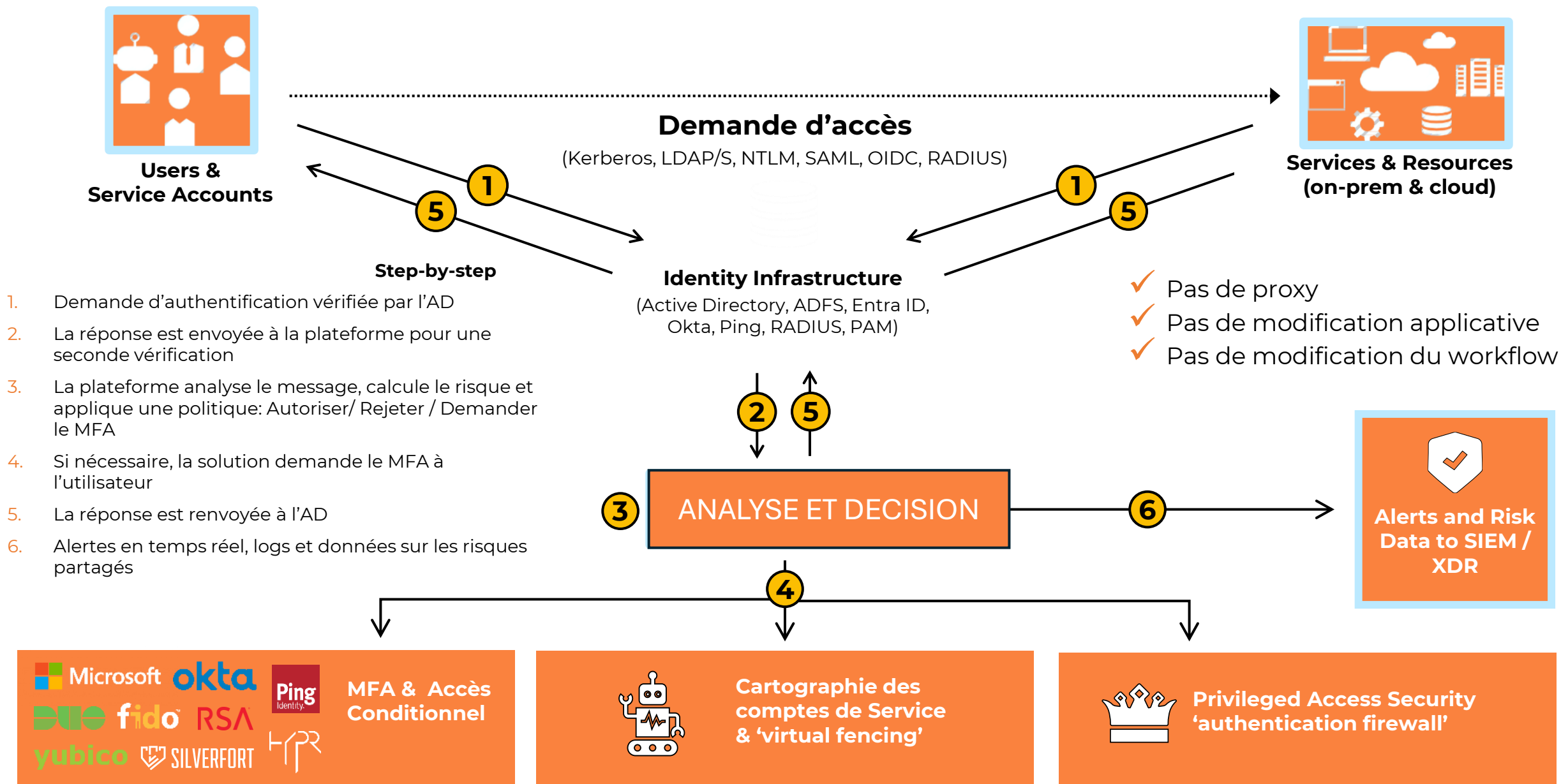
Lacunes dans **la découverte et la visibilité**

Vous ne pouvez pas protéger ce que vous ne connaissez pas. Sur site, dans le cloud, et partout ailleurs.



Principe de fonctionnement

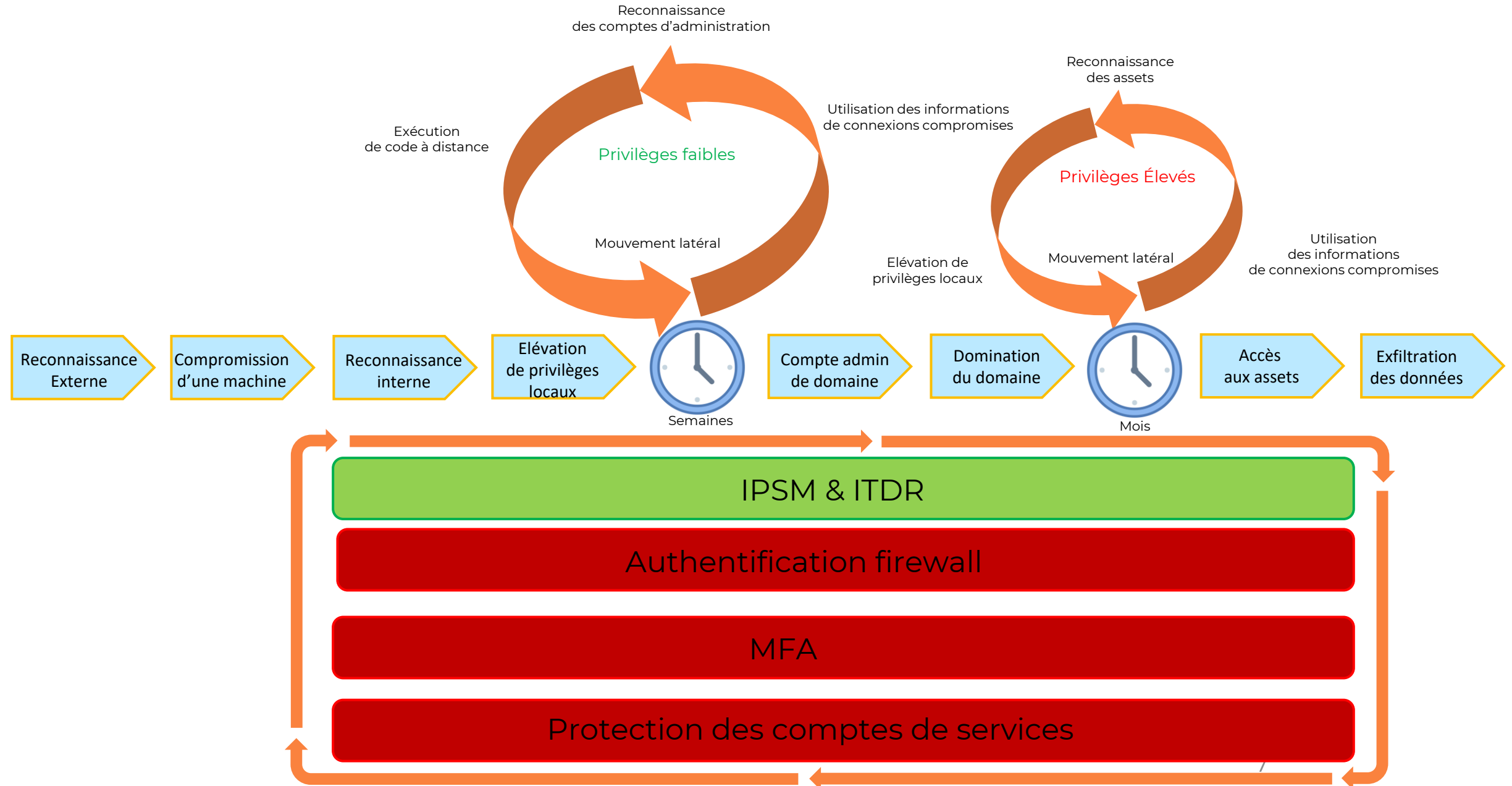




Compléments



Protection de l'ensemble de la KillChain AD



Exemples de cas d'usage



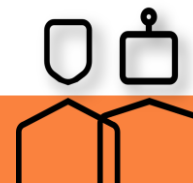
Protection Active Directory

Découvrir en temps réel et surveiller les authentifications sur tous vos comptes de l'AD



Accès Privilégiés sécurisés

Etendre la couverture de votre MFA aux authentifications LDAP, Kerberos ou NTLM



Comptes de service

Sécuriser les comptes de service sans rotation des mots de passe ni modification de l'application



ZeroTrust AD (Tiering model)

Attaques sur les identités comme les mouvements latéraux et déclenchement du MFA/Blocage comme réponse en temps réel



www.sasety.com

