Zero tolérance sécurité

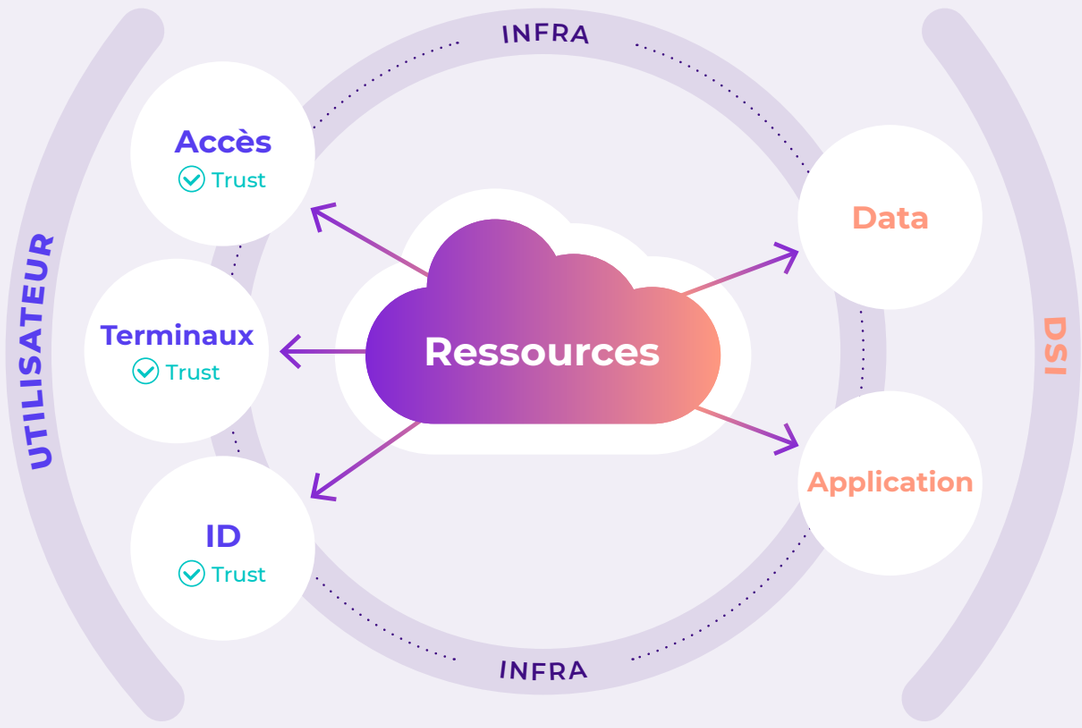
Retour ↑

#Platform

- **Unifier la gestion des identités**, des accès et renforcer la sécurité
- **Se protéger des vecteurs d'attaque**, notamment hameçonnage, vulnérabilité IT et arnaque au président
- **Combattre les effets des risques sécuritaires :** perturbation de la production, compromission, rançon, perte d'image

Remise en cause de la confiance implicite*

- Analyse comportementale privilégiée
- Implémentation de mécanisme de sécurité : Identité hybride, accès conditionnel, authentification multi facteurs ...
- Généralisation des points de contrôles : identité, terminal, application, réseau ...



255%
d'augmentation des attaques par ransomware, par an

54%
des entreprises françaises attaquées en 2021

47%
des télétravailleurs piégés par le phishing

Bénéfices

1. **Authentification simplifiée** et fluide pour l'utilisateur
2. **Protection de ses données**
3. **Maîtrise des politiques de sécurité** de l'entreprise
4. **Visibilité** sur les attaques
5. **Protection** contre les risques sécuritaires

Success story

Opérateur mobile

Besoin | Accentuer la sécurité au travers d'une plateforme unifiée contre toute attaque cybercriminelle.

Réponses | Identification, détection et investigation des menaces avancées. Mise en place de Microsoft Defender & Microsoft Defender for Identity pour gérer les vulnérabilités, protéger les appareils, détecter et répondre aux incidents.

Bénéfices |
- Contrôle centralisé de la cybersécurité
- Meilleure visibilité des menaces
- Réduction des coûts

Offres passerelles

- Virtual Desktop
- Unified endpoint management

L'atout Workplace Infra Innovation

- Proposer une vision **ambitieuse du support IT**
- Associer expérience utilisateur et **optimisation financière**