neomia pulse

Identity Control &
MultiFactor Authentication
IC-MFA
Biométrie Comportementale & Analyse Contextuelle propulsée par de l'Intelligence Artificielle

La cybercriminalité et les vols de données augmentent quotidiennement. Les entreprises et organismes publics, sont une cible de choix. Il n'a jamais été aussi important de prévenir les risques de sécurité à grande échelle, en commençant par la base, **l'identité.** C'est une tâche ardue, compte tenu de l'étendue des métiers, des usages et des localisations des collaborateurs.

Les défis actuels

La situation actuelle est principalement basée sur **l'authentification simple (login, mots de passe),** parfois renforcée par un système MFA, qui s'appuie essentiellement sur des tokens ou des devices physiques.
Il est très difficile de maintenir en parallèle des politiques de sécurité permettant de combiner un niveau de sécurité fort et d'adresser tous les cas d'usage.
La vérification d'identité peut être réalisée sur deux séquences différentes. **La connexion, et la surveillance** lors de la réalisation d'actions critiques.
La vérification d'identité biométrique est la plus résiliente dans les 3 composantes de l'authentification (ce que je sais, ce que je possède, ce que je suis).
Pour répondre aux enjeux d'universalité, d'acceptation par les utilisateurs, de facilité de déploiement et de coût, il est important d'amener une capacité d'identité biométrique, **sans device ni token.**

Les solutions doivent répondre de manière simple à ces questions :

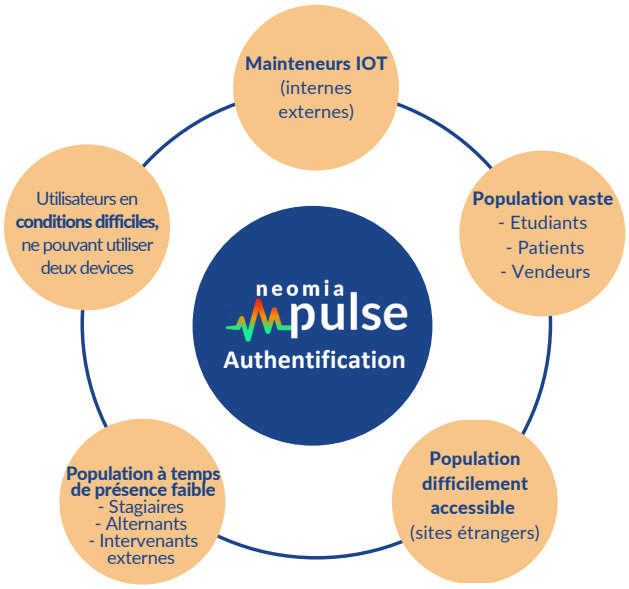
- L'utilisateur connecté est-il bien l'utilisateur légitime ?
- L'utilisateur est-il bien le même tout le long d'une connexion ?
- Les données sont-elles saisies par un utilisateur, par un processus automatisé ou un robot ?
- La machine utilisée est-elle sans risque ?
- L'approche ne doit laisser aucun doute sur la possibilité d'usurpation d'identité, ni compromission de session.

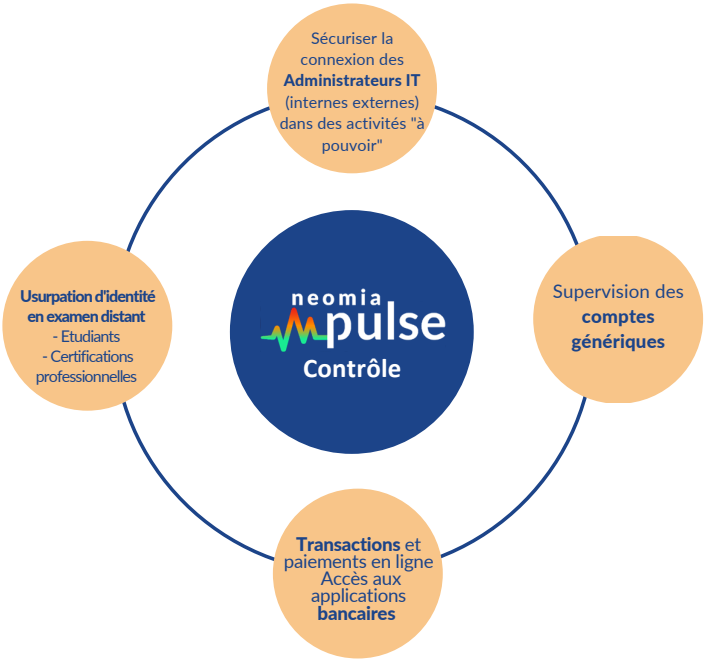
neomia Pulse, une approche novatrice propulsée par l'Intelligence Artificielle

Neomia Pulse authentifie d'une manière transparente et sans friction les utilisateurs, détecte et bloque toutes les activités suspectes grâce à la combinaison de la biométrie comportementale et l'analyse contextuelle.
neomia Pulse collecte en temps réel :

- des données comportementales (dynamique de frappe, mouvements de la souris, utilisation d'un écran tactile, ...) ;
- des données contextuelles liées à l'équipement utilisé (données physiques, logicielles, temporelles et géographiques).

Neomia Pulse, les cas d'usage





Neomia Pulse s'intègre très facilement

Pulse propose une intégration à différents niveaux

- Intégration par API avec vos systèmes actuels de gestion des identités.
- Pulse intègre les protocoles de dernière génération ; SAML / OIDC, pour se connecter sans contraintes à votre IDP.

Neomia Pulse permet de

Supprimer les risques associés aux mots de passe ainsi qu'à l'authentification statique

Détecter l'utilisation d'identités volées ou fictives

Améliorer la sécurité et l'expérience utilisateur avec une approche continue sans friction

Définir et mettre en œuvre des mesures efficaces en cas d'activités suspectes

neomia Pulse s'adresse à tout type d'organisation

Editeurs de logiciels

Fournisseurs SaaS

Organisations avec applications internes

Opérateurs d'Importance Vitale

neomia pulse

3 Rue Paul-Henri SPAAK, 68390 SAUSHEIM
contact@neomia.ai
03 89 33 58 20