CHIMERE Cyberstealth®

Solution de Zero Trust Network Access française 🇫🇷 et européenne 🇪🇺

Zero Trust Network Access, le VPN nouvelle génération

Le paysage de la cybersécurité évolue rapidement, et avec lui, les méthodes d'accès aux ressources informatiques. Le VPN, longtemps considéré comme la solution de référence pour sécuriser l'accès aux réseaux d'entreprise, montre aujourd'hui ses limites face aux nouvelles menaces. C'est dans ce contexte qu'émerge le Zero Trust Network Access (ZTNA), une approche moderne et plus sécurisée de l'accès à distance.

> **65% des entreprises en Europe ont besoin de fournir un accès distant vers leur système d'information à leur collaborateurs, partenaires, prestataires ou clients.**

Le Zero Trust Network Access s'impose progressivement comme la solution de référence pour sécuriser l'accès aux applications et aux ressources d'entreprise. En adoptant cette approche, les organisations peuvent **réduire les risques liés aux cyberattaques, améliorer la flexibilité de leur infrastructure et offrir une meilleure expérience aux utilisateurs**. Le ZTNA n'est pas seulement une évolution du VPN, c'est une révolution dans la manière d'envisager la cybersécurité moderne.

«Le Zero trust (ZT) est le terme désignant un ensemble évolutif de paradigmes de cybersécurité qui déplacent les défenses des périmètres statiques basés sur le réseau pour se concentrer sur les utilisateurs, les assets et les ressources.» - *NIST, Zero Trust Architecture, 2020*

«Le ZTNA améliore la flexibilité, l'agilité et l'évolutivité, permettant aux écosystèmes numériques de fonctionner sans exposer les services directement à Internet, réduisant ainsi les risques d'attaques par déni de service distribué.» - *Gartner, ZTNA Market Guide, 2019*

Chimere Cyberstealth®, votre solution d'accès distant nouvelle génération

Chimere fournit une solution de Zero Trust Network Access (ZTNA) française et européenne permettant d'interconnecter de façon sécurisée des appareils et des applications à travers internet, sans les exposer et en assurant leur isolation. La solution est une alternative efficace aux VPN d'entreprise et facilite le nomadisme numérique, le télétravail, et les accès prestataires.

Le vrai «Zero Trust»

Avec le réseau Zero Trust Chimere, vous contrôlez finement les appareils et les utilisateurs qui accèdent à vos applications d'entreprise. Chimere s'assure que les appareils connectés à votre système d'information sont conformes à la politique de sécurité que vous définissez, tout en apportant une garantie d'accès réseau moindre privilège. Chimere permet de ne pas faire confiance par défaut, et vérifie en continue les droits d'accès et les politiques de sécurité.

Pourquoi Chimere ?

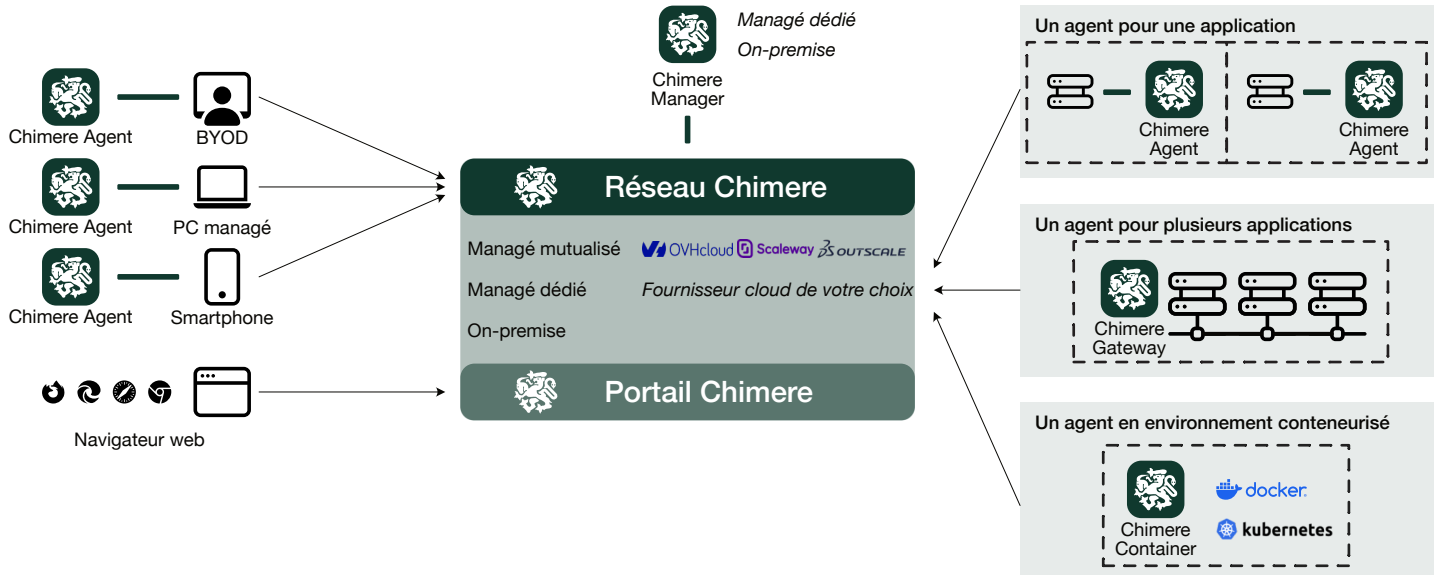
- Une solution d'accès distant conçue pour les usages et les menaces d'aujourd'hui et de demain.
- Chimere est **déployable en parallèle des solutions existantes** (VPN, MPLS, SD-WAN) sans interruption des services, évitant des modifications complexes et coûteuses de l'infrastructure réseau.
- Le principe de moindre privilège natif de Chimere assure que les utilisateurs et les appareils n'accèdent qu'aux ressources du réseau qui leur sont nécessaires. Cette micro-segmentation assure **une surface d'attaque réseau minimale**.
- Les ressources ne sont plus accessibles publiquement sur Internet. Chimere **masque les applications et services**, ce qui empêche leur découverte.
- Chimere offre une **connexion fluide, rapide et sécurisée**, améliorant la productivité des collaborateurs.
- Chimere réduit les risques liés aux terminaux et utilisateurs compromis par des **politiques de sécurité conditionnant l'accès aux ressources** à un utilisateur et un appareil conforme (absence de malware, OS à jour, zone géographique, etc.).
- Avec l'augmentation du télétravail et du BYOD (Bring Your Own Device), Chimere offre un **accès sécurisé depuis n'importe où**, sans nécessiter de connexions réseau complexes.
- À travers des **logs détaillés et une analyse en temps réel**, Chimere permet une meilleure détection et réponse aux menaces, améliorant la posture de cybersécurité globale.
- Chimere aide à **répondre aux exigences des réglementations** (NIS 2, GDPR, ISO 27001, etc.) en assurant une gestion rigoureuse des accès et en limitant les expositions superflues.
- En réduisant la dépendance aux VPN traditionnels, aux appliances physiques et aux configurations complexes de pare-feu, Chimere **entraine une baisse des coûts de gestion et de support IT**.

chimere.eu

contact@chimere.eu

+33 (0) 6 51 86 55 19

Une solution adaptée pour toutes les architectures



L'AGENT CHIMERE, UN COMPOSANT UNIQUE POUR ACCÉDER AUX SERVICES ET LES PUBLIER

L'agent Chimere est responsable du **chiffrement de bout-en-bout**, des vérifications de **conformité de l'appareil** et de l'établissement des liens sécurisés.

- Lorsqu'installé sur les appareils des utilisateurs ayant besoin d'accéder aux services et applications de l'organisation, il participe à **l'authentification de l'utilisateur** et la **vérification du contexte** tout en permettant l'**accès transparent aux ressources**.
- Lorsqu'installé sur un serveur, il permet la mise à disposition des services et applications aux utilisateurs autorisés. Avec des flux exclusivement sortants vers le réseau Chimere, **il n'expose aucun port**. Il est également configurable en **mode «passerelle»** pour permettre la connexion vers des applications hébergées sur des serveurs distincts.

LE CHIMERE MANAGER, UN SERVICE UNIQUE D'ADMINISTRATION CENTRALISÉE

Centre de contrôle, le manager est une application web permettant de configurer les utilisateurs, les services, les droits d'accès, les politiques de sécurité et la journalisation.

Unique et dédié pour chaque organisation, le Chimere Manager peut être déployé en mode managé ou on-premise.

LE RÉSEAU CHIMERE, UNE INFRASTRUCTURE ZERO CONFIANCE RÉSILIENT À LA COMPROMISSION

Le réseau Chimere est l'infrastructure intermédiaire entre les utilisateurs et les services. Résilient à la compromission, vos applications sont en **sûreté totale, empêchant les attaques par rebond, la découverte des applications publiées ou la récolte d'informations sur vos systèmes**. Le vrai « Zero Trust ».

Ce réseau, multicloud, est proposé en mode managé, mutualisé ou dédié, ou encore on-premise.

LE PORTAIL CHIMERE, UN ACCÈS SANS AGENT VIA LE NAVIGATEUR

Le portail Chimere permet aux utilisateurs d'accéder directement, **sans installation**, aux applications et services web de l'organisation.

Accessible depuis un simple navigateur, il **s'intègre au contrôle d'accès centralisé** du Manager et applique les mêmes accès conditionnels que l'agent Chimere.

LE BASTION CHIMERE, LE POINT CENTRAL POUR LES ACCÈS D'ADMINISTRATION

Le bastion Chimere gère **tous les accès d'administration** (RDP, SSH, VNC, etc.) à travers un point unique et sécurisé.

Il assure le chiffrement de bout-en-bout, l'application des politiques de sécurité et l'**enregistrement des sessions** pour répondre aux exigences de conformité et de traçabilité.

Chimere, entreprise spin-off du groupe Thales, est le seul «pure player» européen du Zero Trust Network Access. Conçue à partir des travaux de recherches modélisant les architectures Zero Trust, la solution Chimere Cyberstealth® implémente les mécanismes les plus robustes, à la pointe de la technologie. Innovant par nature et labellisée *Deeptech*, Chimere travaille avec un écosystème riche pour concevoir la solution qui répondra au mieux à vos attentes, même les plus exigeantes. Enfin, en tant qu'entreprise française et européenne, vous apporter enfin une solution de cybersécurité souveraine française et européenne est au cœur de notre mission.