CHIMERE

Votre accès réseau, nouvelle génération

CHIMERE

Chimere fournit une solution ZTNA (Zero-Trust Network Access) 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.

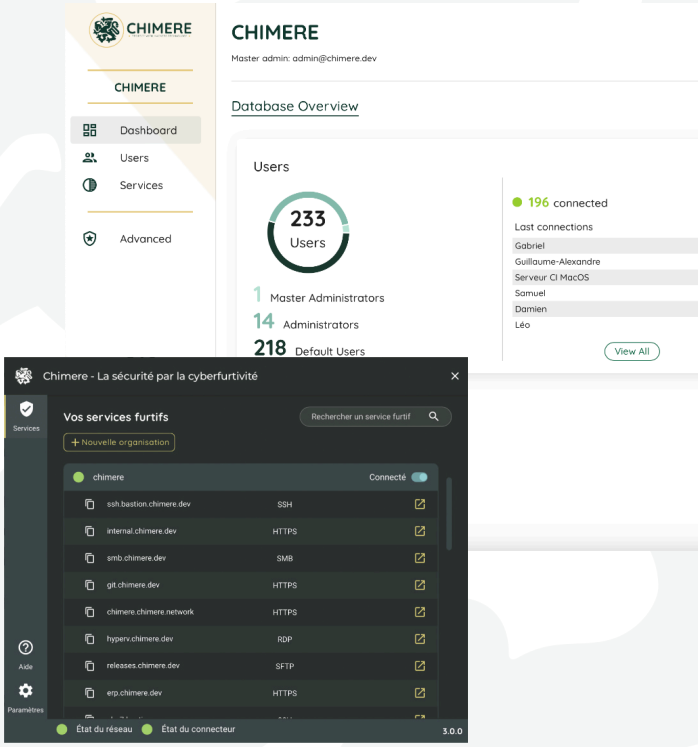
La solution se positionne comme une alternative efficace aux VPNs d'entreprise et aux pare-feux. Elle facilite le nomadisme numérique, le télétravail, et les accès prestataires.

ZERO-TRUST ET ZERO TIERS DE CONFIANCE

Grâce au réseau Chimere, nativement Zero-Trust, sans tiers de confiance, vous n'avez plus à faire confiance au fournisseur de votre solution d'accès distant. Il est impossible d'inspecter ce qui transite sur le réseau. Vous restez maîtres de vos données, de votre infrastructure et totalement indépendants.

POURQUOI CHIMERE ?

- Permettez à vos collaborateurs en mobilité et en télétravail d'accéder au SI
- Accédez aux systèmes de vos clients, sans ouvrir de port sur internet
- Rendez accessible ce qui était jusqu'alors interdit
- Fournissez des accès à vos prestataires sans passer par le VPN
- Rendez votre passerelle VPN invisible
- Administrez toutes les machines de votre parc, en un clic



NOUVELLE ERE DE L'ACCES DISTANT

Le Zero-Trust Network Access propose une vision nouvelle de l'accès distant au réseau d'entreprise. Avec la solution ZTNA de Chimere, nous vous proposons d'aller plus loin et d'adopter le **vrai Zero-Trust** !

- ✓ Suppression de l'exposition des services d'internet et réduction significative des risques d'intrusion
- ✓ Chiffrement de bout en bout : Zero Trust **confidentialité** et **intégrité**
- ✓ Traçabilité totale des utilisateurs customer-side : Zero-Trust **traçabilité**
- ✓ Infrastructure ZTNA décentralisée, multi-cloud et participative : Zero-Trust **disponibilité**

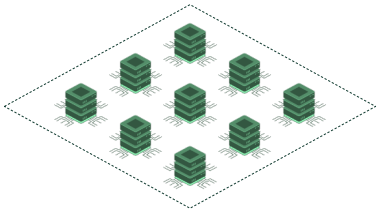
Chimere Cyberstealth®

4 composants pour mettre en place votre accès réseau Zero-Trust *by design*

RESEAU

Le réseau Zero-Trust Chimere

Opéré par Chimere, le réseau permet de mettre en relation les utilisateurs et les services protégés sans accorder de confiance à Chimere. Le vrai Zero-Trust.

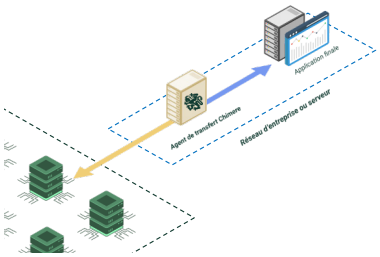


- ✓ Multi-cloud sur OVH et Scaleway
- ✓ Communications chiffrées de bout-en-bout. Personne ne peut voir ce qui transite, pas même Chimere.
- ✓ Accès aux applications sécurisées réalisés par clefs cryptographiques. Seuls vos utilisateurs peuvent découvrir et accéder aux services. Ni Chimere, ni le fournisseur de cloud, ni aucun autre intermédiaire n'ont cette possibilité.

SERVEUR

L'agent de transfert

Opéré par le client, l'agent de transfert permet de mettre à disposition les services et applications sécurisés aux utilisateurs.

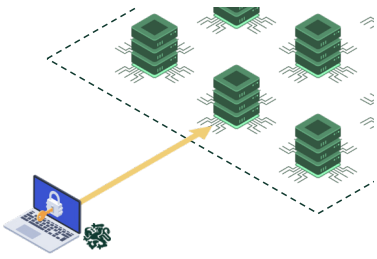


- ✓ Connecté à l'application finale
- ✓ Connecté au réseau Chimere via des flux TLS exclusivement sortants
- ✓ Installé sur le serveur qui porte le service final ou en mode proxy

UTILISATEUR

L'agent utilisateur

L'agent utilisateur permet à un utilisateur d'accéder aux applications et services sécurisés de son organisation, pour lesquels il dispose des droits.



- ✓ Accès aux applications en toute transparence
- ✓ Compatible avec n'importe quel navigateur ou client lourd
- ✓ On-boarding automatisé et autonome

ADMINISTRATEUR

La console Chimere Manager

Opéré par le client, le manager Chimere gère les utilisateurs, les services et les clefs cryptographiques associées à chacun.

- ✓ Hébergé au choix par le client ou par Chimere
- ✓ Provisioning automatisé avec des fournisseurs d'identité tiers (via SCIM)
- ✓ Mode utilisateurs standalone
- ✓ Propage et révoque les droits d'accès aux applications en temps réel

Quelles sont les différences entre le VPN et le ZTNA ?

Le VPN (Virtual Private Network) et le ZTNA (Zero Trust Network Access) sont deux technologies utilisées pour sécuriser l'accès aux ressources informatiques. Les VPNs, combinés aux pares-feux sont aujourd'hui encore considérés comme l'état de l'art dans certaines entreprises. Néanmoins, le ZTNA renverse progressivement la tendance au travers de ses approches différentes et plus adaptées aux menaces actuelles :

Fonctionnement

- Le VPN établit une connexion sécurisée entre un utilisateur et un réseau privé, en général, le réseau d'une entreprise.
- Le ZTNA, en revanche, crée des frontières d'accès logiques autour d'applications spécifiques plutôt que d'accorder un accès complet au réseau. Il applique des politiques de sécurité basées sur l'identité et le contexte de l'utilisateur plutôt que sur son emplacement ou son appartenance au réseau.

Portée

- Le VPN permet à l'utilisateur d'accéder à l'ensemble du réseau d'une organisation de manière sécurisée, comme s'il était physiquement connecté au réseau local.
- Le ZTNA restreint l'accès à des applications spécifiques en fonction des besoins de l'utilisateur et des politiques de sécurité définies, sans donner un accès général au réseau. Il apporte nativement une politique d'accès moindre privilèges.

Modèle de sécurité

- Le VPN repose souvent sur un modèle de sécurité de type "confiance mais vérification", où une fois que l'utilisateur est authentifié, il est généralement autorisé à accéder à toutes les ressources du réseau.
- Le ZTNA suit le modèle de sécurité "ne jamais faire confiance, toujours vérifier", où l'accès est accordé sur la base de politiques granulaires qui vérifient continuellement l'identité, le contexte et la conformité de l'utilisateur avant d'autoriser l'accès à une application spécifique.

Visibilité et contrôle

- Avec le VPN, une fois qu'un utilisateur est connecté, il peut potentiellement accéder à toutes les ressources du réseau, ce qui peut rendre difficile la surveillance et le contrôle précis de l'accès.
- Le ZTNA offre une visibilité et un contrôle plus granulaires, car il permet de restreindre l'accès à des applications spécifiques en fonction de règles de sécurité définies, ce qui permet une meilleure gestion des risques et une réduction de la surface d'attaque.

Exposition

- Le VPN expose une passerelle sur internet qui peut elle-même être vulnérable. La passerelle VPN est logicielle ou matérielle et nécessite une maintenance à la charge de l'entreprise.
- Le ZTNA n'expose aucune ressource de l'entreprise. L'infrastructure ZTNA est, quand à elle, exposée mais est entièrement gérée et maintenue par le fournisseur. Dans le cas de Chimere, cette infrastructure ZTNA est résiliente à la compromission.

Gartner

ZTNA Market Guide, 2019

“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.”

NIST

Zero Trust Architecture, Special Publication, 2020

“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. ”

Pourquoi le ZTNA de Chimere ?

Aujourd'hui, des dizaines de fournisseurs de solutions de ZTNA existent, mais aucun ne propose l'intégralité de ces fonctionnalités hormis Chimere.

Chiffrement de bout-en-bout

Cette approche de sécurité garantit que les données sont chiffrées dès leur point d'origine et ne sont déchiffrées qu'à leur destination finale, assurant ainsi une protection maximale contre les menaces potentielles. En utilisant le chiffrement de bout-en-bout, nous vous assurons que seuls les utilisateurs autorisés peuvent accéder aux données, **pas même nous**.

Résilience à la compromission

Contrairement aux autres fournisseurs, nous avons développé une approche unique qui garantit que la sécurité et la fonctionnalité du réseau à disposition de nos clients restent **intactes même en cas de compromission**. Cette résilience est rendue possible grâce à notre architecture distribuée et la non détention des clefs cryptographiques d'accès aux services par Chimere.

Disponibilité

Avec un réseau **décentralisé et distribué** sur différentes infrastructures indépendantes, nous vous offrons une disponibilité inégalée, vous assurant ainsi une connectivité fiable et ininterrompue.

Souveraineté

Nous sommes une entreprise française et européenne. Dans le contexte actuel de réglementations, de plus en plus strictes en matière de protection des données, nous comprenons que pour nombre d'entre vous, la souveraineté des données et des échanges est un aspect crucial de votre stratégie de sécurité. Vous apporter enfin **une solution de cybersécurité souveraine française et européenne** est au cœur de notre mission.

Tous ces aspects vous apportent un **vrai Zero-Trust** que vous ne trouverez nulle part ailleurs.

Devenez cyberfurtif et échappez aux cyberattaques

Le Zero-Trust Network Access rend invisibles vos applications sur internet et au sein de votre réseau d'entreprise. En devenant indétectables, vos services réseaux disparaissent de la liste des points d'entrée utilisables par les attaquants.

Gérez les droits d'accès simplement et en temps réel

En un clic, permettez à l'intégralité de vos collaborateurs, vos sous-traitants, et vos clients d'accéder de façon sécurisée et partout dans le monde à vos actifs. La propagation et la révocation des droits d'accès sont immédiates : administrer n'a jamais été aussi facile.

Empêchez les attaquants de se déplacer dans le réseau

Chimere apporte nativement une micro-segmentation qui empêche tout mouvement latéral, même si votre réseau est compromis. En appliquant le principe du ZTNA à vos applications d'entreprise, vous assurez une connexion point-à-point entre vos collaborateurs et leurs applications à la différence des VPN d'entreprise avec lesquels les utilisateurs ont accès à une partie ou l'intégralité du réseau.

https://chimere.eu

contact@chimere.eu