CATO NETWORKS | SOLUTION BRIEF

Universal Zero Trust Network Access

AVANTAGES CLÉS

Sécurisez l’accès partout

Connectez sans effort tout type d’utilisateur à l’échelle mondiale sans limites d’infrastructure ni retards opérationnels.

Contenez les menaces

Ajustez en continu l’accès basé sur le zero trust en utilisant l’identité, la posture des appareils et des signaux de risque en temps réel.

Simplifiez les opérations

Réduisez la charge administrative en appliquant une politique unique pour tous les types d’utilisateurs, d’appareils et de lieux.

Défi

Le périmètre de l’entreprise a disparu. Les employés, les sous-traitants et les partenaires accèdent désormais à des applications décentralisées depuis n’importe où sur n’importe quel appareil. Les VPN legacy ne peuvent pas suivre. Les organisations se retrouvent à assembler plusieurs politiques, laissant des lacunes de sécurité et permettant un accès latéral à travers les applications. Le défi n’est plus de connecter les utilisateurs au réseau, mais de contrôler l’accès aux applications dans un monde où la frontière du réseau n’existe plus.

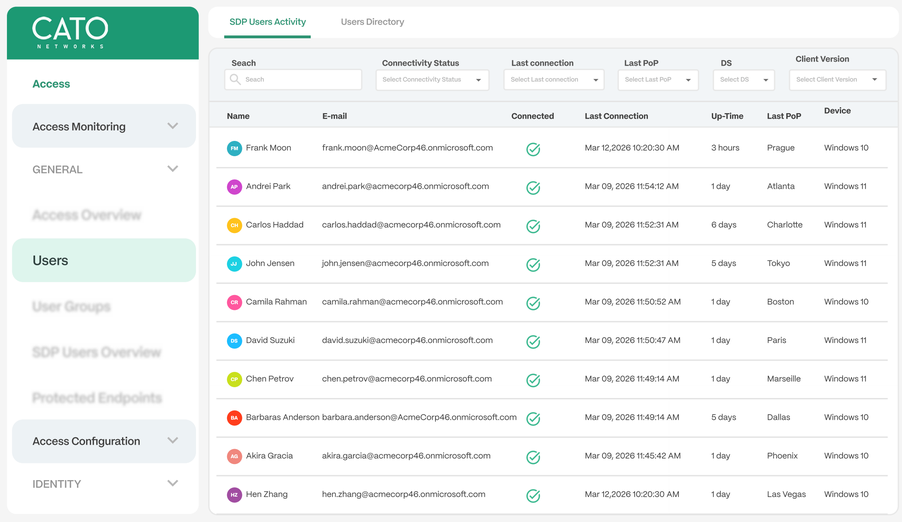
Solution

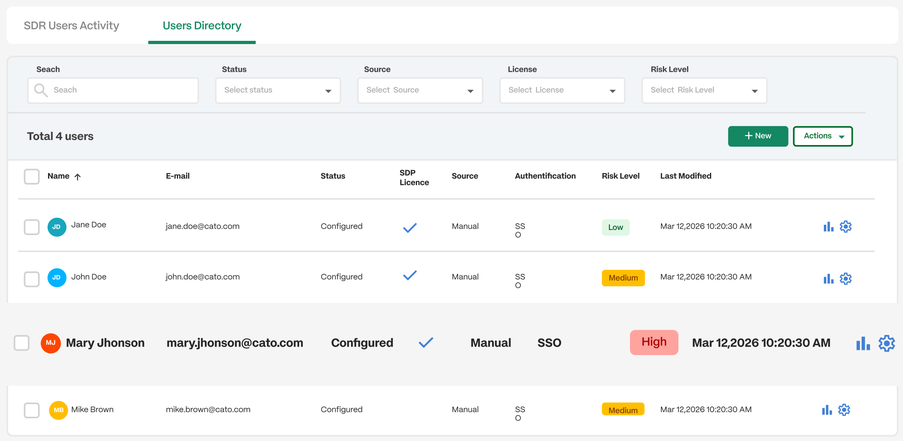
Cato Universal ZTNA offre un accès sécurisé au niveau des applications sans exposer le réseau. Une politique unique basée sur le risque, contrôle l’accès pour tous les utilisateurs, appareils et applications via la plateforme cloud mondiale de Cato, réduisant le risque cyber, simplifiant la gestion des accès et permettant une productivité en toute sécurité pour l’ensemble de l’organisation.

Accès Zero Trust. Simplifié.

Une politique unique partout

Réduisez le risque cyber tout en simplifiant l’accès sécurisé pour l’ensemble de l’organisation. Cato applique une politique centralisée à tous les utilisateurs, appareils, applications et lieux, en utilisant un moteur cloud-native qui inspecte le trafic, utilise l’identité et le contexte, et fournit des contrôles de sécurité consistants à l’échelle mondiale sans solutions désynchronisées et fragmentées.



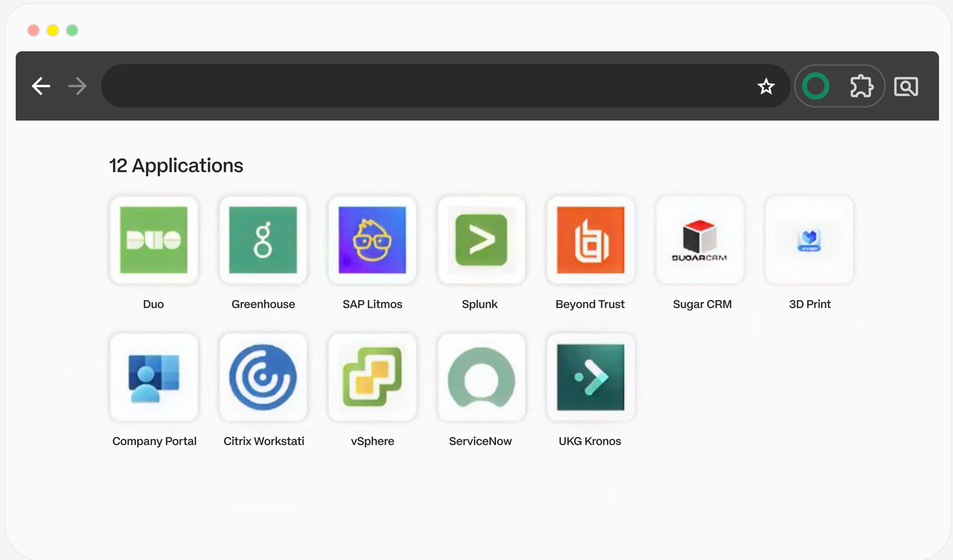


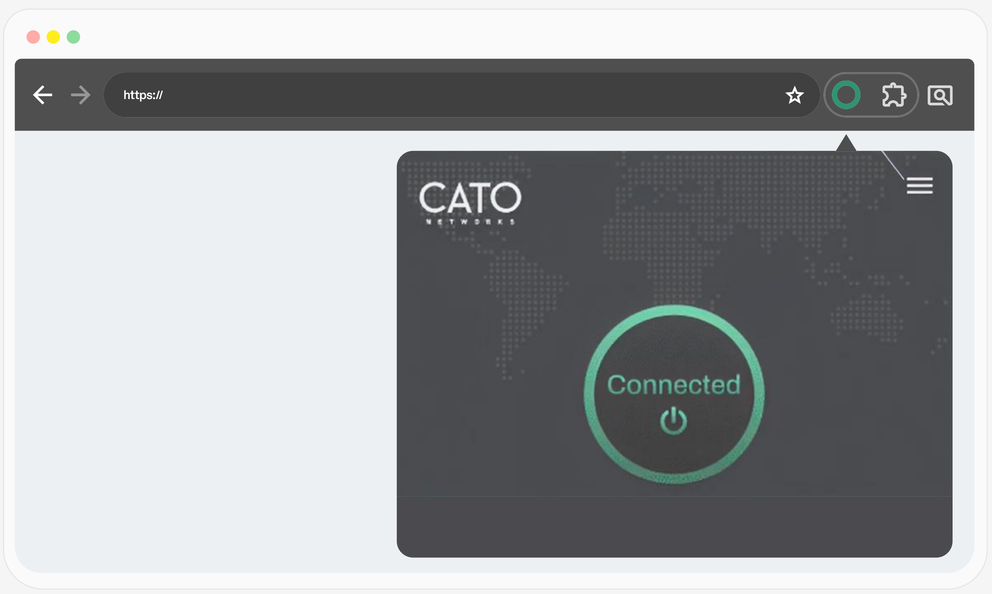
Contrôle d’accès basé sur le risque

Limitez le risque au niveau des endpoints et prévenez les violations en veillant à ce que seuls les appareils conformes avec une posture de device validée en continu, un statut de sécurité et un emplacement spécifiques aient un accès autorisé. La conformité des appareils, la version du système d’exploitation et les profils de sécurité des endpoints sont surveillés, et les sessions sont instantanément fermées si les profils ne sont plus conformes.

Segmentation au niveau de l’application

Empêchez les mouvements latéraux pour réduire la surface d’attaque en connectant les utilisateurs uniquement aux applications approuvées au lieu du réseau complet. Bloquez les mouvements est/ouest et les attaques provenant de stratégies d’attaque sophistiquées lentes et discrètes.





Accès sécurisé aux appareils non gérés

Étendez la connectivité sécurisée aux sous-traitants, partenaires et appareils non gérés et sans client. L’Enterprise Browser et l’extension de navigateur de Cato peuvent restreindre les téléchargements, les uploads et le copier/coller tout en appliquant l’ensemble de la pile de sécurité CASB/DLP de Cato pour protéger l’appareil, l’application et le réseau.

Évolutivité par conception

Permet aux organisations de maintenir un accès sécurisé et la continuité des activités tout en accélérant la croissance et l’agilité opérationnelle en tirant parti d’une architecture cloud-native qui prend instantanément en charge de nouveaux utilisateurs, des intégrations de fusions et acquisitions, et des demandes de travail à distance non prévues sans mises à niveau d’infrastructure.

Principaux cas d’usage

Remplacement des VPN legacy

Modernisez les contrôles d’accès avec un accès applicatif plus simple et plus sécurisé, capable d’évoluer avec la croissance.

Segmentation est/ouest

Isolez les utilisateurs/applications pour empêcher les mouvements latéraux, réduisant l’impact des violations.

Atteindre la conformité

Contrôlez l’accès aux applications sensibles pour soutenir la conformité réglementaire et protéger les données

Accès aux appareils non gérés

Politique de menace et d’accès intégralement appliquée aux utilisateurs sans client et aux appareils BYOD.

Reconnaissance de l’industrie

« 98 % des tentatives de mouvement latéral ont été bloquées, montrant les fortes capacités de défense interne de Cato. »

FROST & SULLIVAN [Rapport sur l’efficacité de la sécurité]

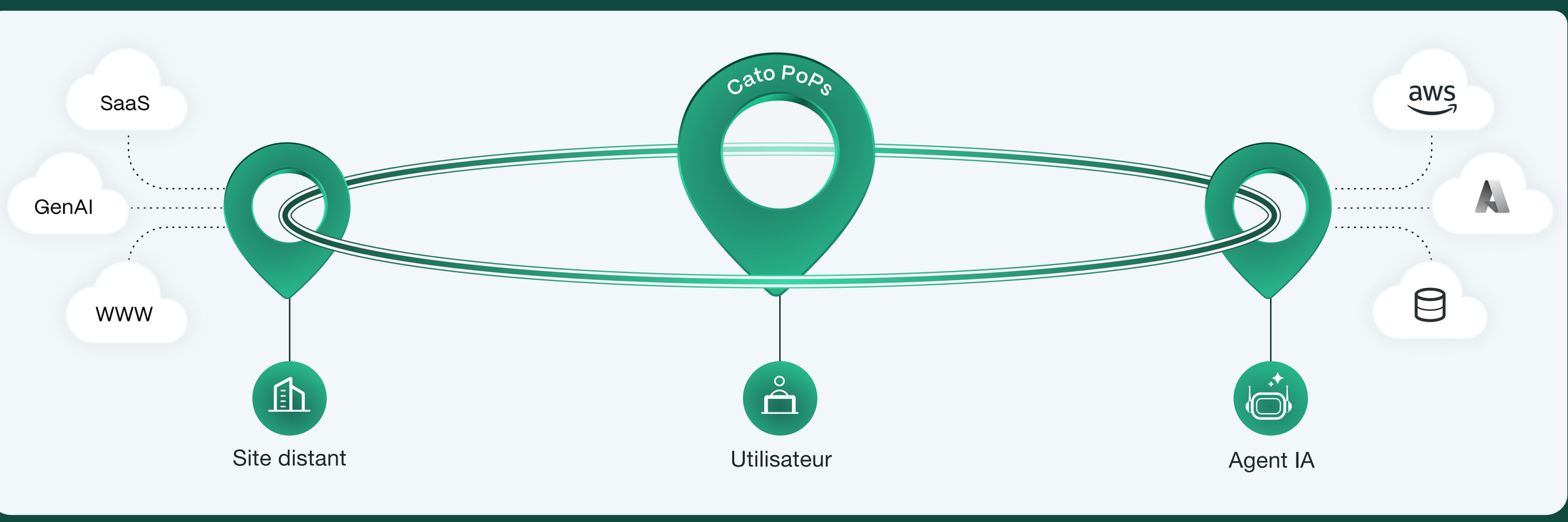
« [Cato SASE a généré] des économies de main-d’œuvre de 2 millions de dollars grâce à une productivité et des résultats améliorés. »

FORRESTER® [Rapport TEI de Forrester]

La plateforme SASE de Cato

Commencez la transformation de votre réseau et de votre sécurité là où les besoins sont les plus urgents Vous exploiterez ensuite toute la puissance du Cato SASE Cloud : conçu nativement pour le SASE auto-optimisé avec un moteur single pass, un datalake unique et une application uniforme des politiques.

Moteur cloud single pass | Gestion unifiée | Politique unique | Datalake unique | Backbone privé mondial



À propos de Cato Networks

Cato Networks, leader du SASE et de la sécurité de l’IA, fournit un accès sécurisé et Zero Trust partout à des milliers de clients dans le monde. Conçue pour les organisations fonctionnant sur tous les environnements cloud et hybrides, la plateforme Cato unifie le réseau, la sécurité et l’accès, fournissant cela comme des capacités élastiques et modulaires que les organisations peuvent facilement adopter et développer au fil du temps. Cato combine le Cato Cloud, un réseau mondial conçunativement pour le SASE, avec une expérience opérationnelle simplifiée, le tout livré via une plateforme robuste et assistée par l’IA. Avec Cato, les organisations se modernisent en toute confiance, opèrent avec une plus grande résilience et innovent plus rapidement, sans complexité ni risque supplémentaires.